

Grandstream Networks, Inc.

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, retail environments, and remote workers. Both models support 2.4GHz 2×2:2 and 5GHz 3×3:2 MU-MIMO with beamforming and XTRA Range technology, delivering maximum network throughput, extended Wi-Fi coverage, and seamless wireless Mesh networking.

Equipped with a 1.3GHz dual-core processor, these routers support Wi-Fi speeds up to 3Gbps and up to 256 wireless clients, making them ideal for streaming 4K UHD, online gaming, video conferencing, and smart automation.

For secure remote access, the routers include built-in VPN support, enterprise-grade encryption, unique security certificates, and random default Wi-Fi/VPN passwords. Both models support Deep Packet Inspection (DPI) for traffic stats and application detection, along with advanced firewall features such as URL filtering to block unsafe or inappropriate content.

While both units share these capabilities, the GWN7062ET includes 2 FXS ports for VoIP telephony, making it a strong choice for small businesses with voice service needs.

Management is streamlined through the built-in Web GUI, GDMS Networking, and GWN Manager for both cloud and on-premise control.

The routers also support mobile app management using the Grandstream Home app, which is the recommended platform for convenient remote administration.

By combining high-speed Wi-Fi, intelligent QoS, Mesh networking, VPN, and robust security, the GWN7062E(T) series provides a reliable and scalable solution for modern home and business networking needs.

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 <i>*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.</i>	
Frequency Bands	● 2.4GHz radio: 2412-2483.5MHz ● 5GHz radio: 5150-5895MHz <i>*Not all frequency bands can be used in all regions</i>	
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 <i>*Maximum power varies by country, frequency band and MCS rate</i>	
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	Supports up to 4 standard SSIDs, plus 1 dedicated Guest Wi-Fi SSID (total of 5).	
Concurrent Wireless Clients	Up to 256 concurrent clients	
Networking Interfaces	3x autosensing 10/100/1000Mbps Ethernet ports	
Analog Telephone FXS Ports	—	2x RJ11 FXS <i>*All ports have lifeline capability in case of power outage; number of ports can be expanded by peering with an FXS gateway</i>
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°C to 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)*90mm(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

Service Ports

The **GWN7062E** and **GWN7062ET** routers use the following service ports. These ports enable features such as remote management, device discovery, secure UI access, and portal-based authentication services:

Port	Protocol	Description
14	UDP	Used for automatic discovery of GWN Access Points within the local network (proprietary protocol).
22	TCP	Secure Shell (SSH) used for CLI access and remote command-line management.
53	UDP	Built-in DNS service for hostname resolution on the local network.
80	TCP	HTTP access; used as an initial entry point and redirects to HTTPS (port 443).
443	TCP	HTTPS web interface; provides secure access to the GWN management UI.
8080	TCP	Captive portal redirect for guest access and authentication workflows.
8443	TCP	Encrypted web authentication; used for secure access to captive portal and guest services.
9443	TCP	Business portal services, such as voucher-based log downloads and extended access features.
7443	TCP	Switch management port used internally for switching component control.

Service Ports

Note:

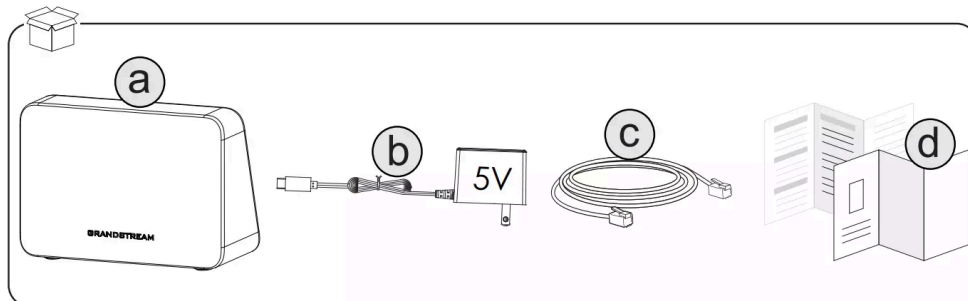
These ports apply specifically to the GWN7062E and GWN7062ET models documented in this manual.

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.

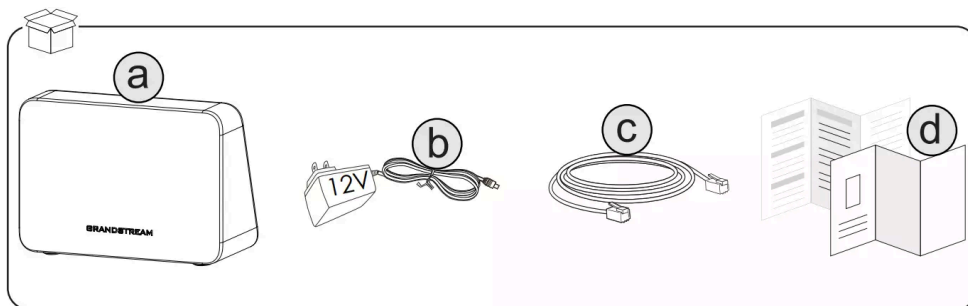
Package Contents

○ GWN7062E



GWN7062E Package Contents

○ GWN7062ET



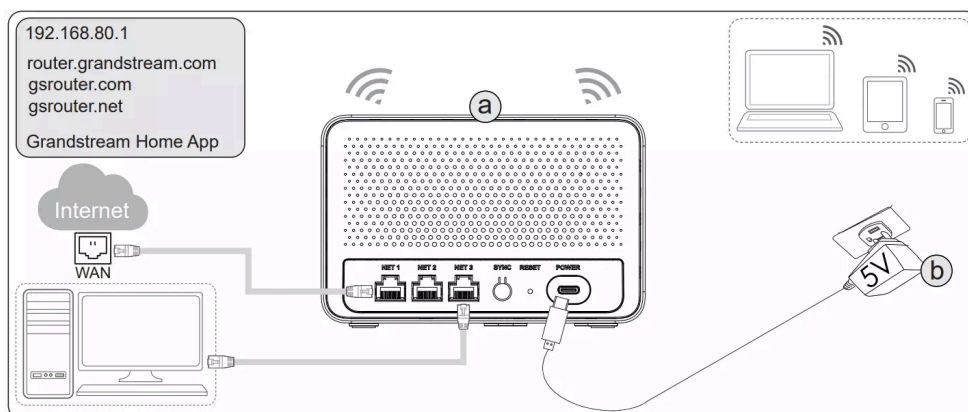
GWN7062ET Package Contents

Powering and Connecting

This section explains how to properly connect the **GWN7062E** and **GWN7062ET** to power, WAN, and devices.

○ GWN7062E

1. Connect the **WAN port** to the uplink.
2. Plug in the **power adapter** and turn the unit on.
3. Wait until the device is powered up and Wi-Fi is active (Wi-Fi LEDs will blink).
4. Use a computer or mobile device to connect to the default SSID or LAN port.

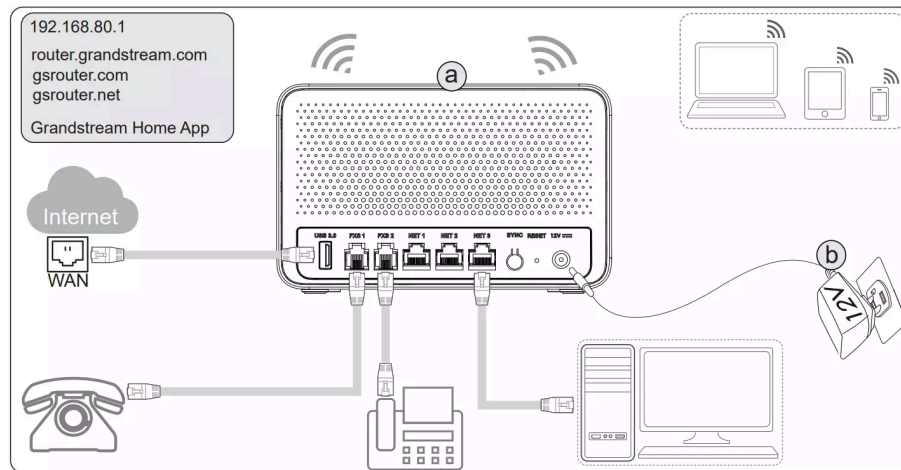


GWN7062E Ports

○ GWN7062ET

1. Connect the **WAN port** to the uplink.

2. If needed, connect phones to the **FXS ports**.
3. Plug in the **power adapter** and power on the device.
4. Connect your PC or mobile device to the default SSID or via LAN.



GWN7062ET Ports

Scan the QR Code

To easily set up, manage your router, and quickly connect to Wi-Fi using your phone, scan the QR code on the device label with the **Grandstream Home App**.



Scan the QR Code

Steps:

1. **Download the Grandstream Home App** from the App Store or Google Play: [Grandstream Home App Guide](#)
2. Launch the app and sign in or register.
3. Tap the “+” icon to add a new device.
4. Scan the **QR code** located on the bottom of the router.
5. Follow the steps provided in the app to complete device setup.

For more details on app features, configuration options, and remote management tools, visit the full guide: [Grandstream Home – User Guide](#)

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 damage 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:

System LED Status	Indication
Off	The router is powered off.
Solid Blue	● Internet is connected. ● Normal operation. ● Mesh network successfully established. ● Wireless Relay or Wireless Bridge mode is enabled and connected to an upstream Wi-Fi network.
Flashing Blue	● Configuration is being applied. ● Restoring configuration.
Flashing Pink	● When the main router scans for sub-routers, the main router’s pink LED flashes slowly, and the sub-router’s pink LED also flashes slowly when detected by the main router. ● When the main router is actively adding (pairing) a sub-router, both the main router’s and sub-router’s pink LEDs flash faster, indicating the pairing process is in progress.
Solid Pink	● The router has detected a WAN connection, but the Quick Setup Wizard has not been completed yet. ● The device is in Mesh standby mode ready for pairing, but the Mesh process hasn’t been started.
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. ● Wireless Relay or Wireless Bridge mode is enabled, but no uplink SSID is currently connected.

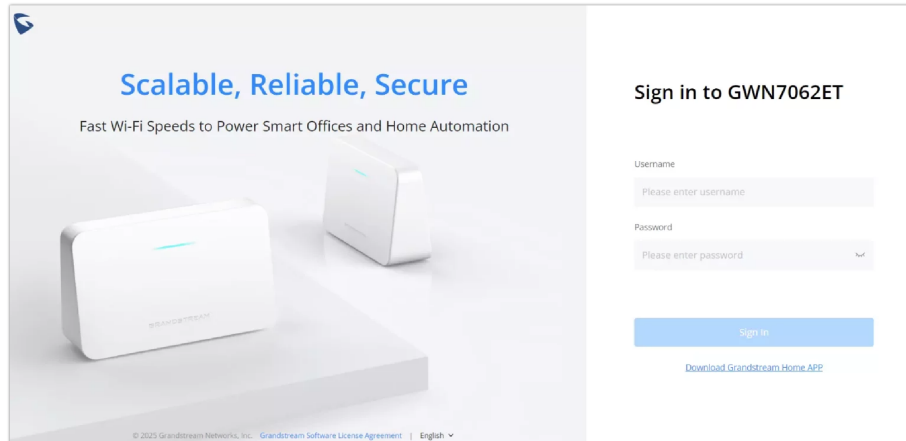
Flashing Yellow	No Internet connection.
-----------------	-------------------------

LED Indicators

Use the WEB GUI

Access WEB GUI

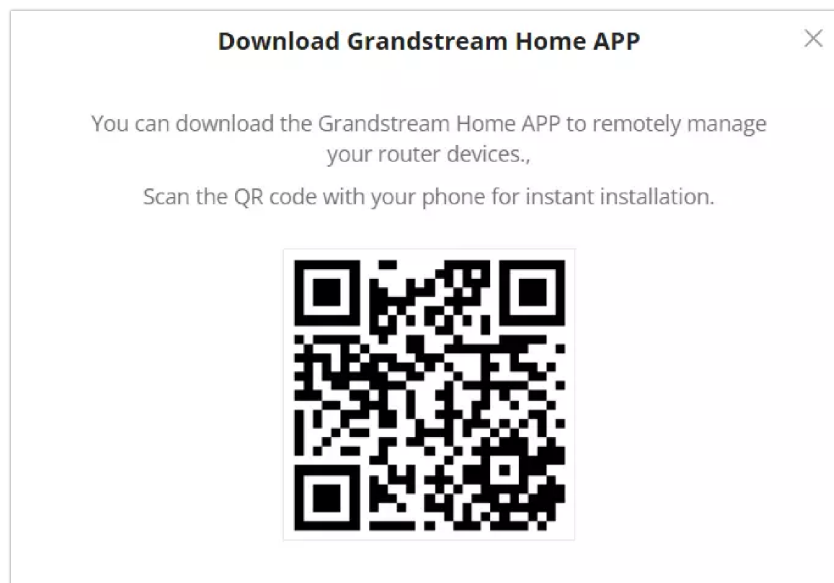
The router's embedded Web server responds to HTTPS GET/POST requests. Embedded HTML pages allow users to configure the device through a Web browser such as Microsoft IE, Mozilla Firefox, or Google Chrome.



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.



Web GUI Login Page

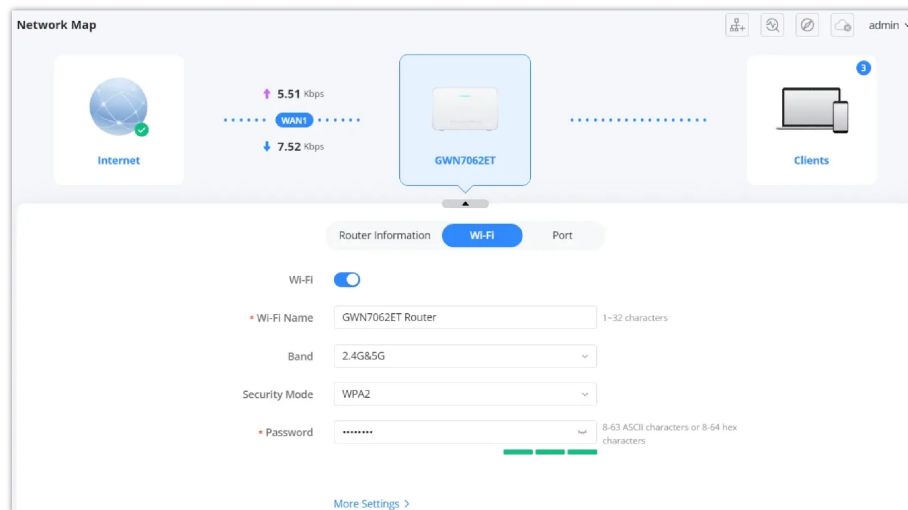
Clicking the **"Download Grandstream Home APP"** link will open a QR code pop-up. This QR code redirects users to a download page where they can choose to install the app on:

- **Android®** via the Google Play Store
- **iOS®** via the Apple App Store

📖 For full setup and management instructions, refer to the official app guide: [Grandstream Home App User Guide](#)

At first boot or after a factory reset, users will be asked to change the default administrator and user passwords before accessing the device's 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, the **Network Map** page will be displayed. This page contains general information and the status of the router, and allows quick configuration of the main Wi-Fi settings. On the Wi-Fi tab, the Wi-Fi toggle can be used to enable or disable the wireless function of the device. When Wi-Fi is disabled, the device operates only as a wired router, and no wireless SSIDs are broadcast. From this page, users can also configure the Wi-Fi name (SSID), band (2.4G&5G, 2.4G and 5G), security mode (Open, WPA/WPA2, WPA2, WPA2/WPA3, WPA3), and password.



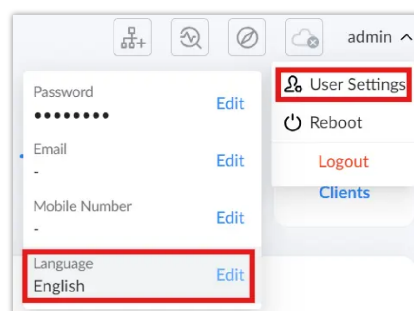
WEB GUI Configuration

Web UI Language

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

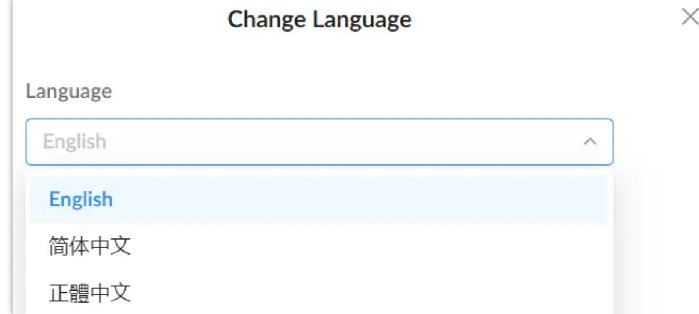
Steps to Change the Language:

1. **Locate User Settings:** In the top-right corner of the web interface, click on the **admin** (or current username) dropdown menu and select **User Settings**.



Change language

2. **Access Language Options:** In the User Settings sub-menu, click the **Edit** link next to the **Language** field.
3. **Select a Language:** A **Change Language** window will appear. Choose the desired language from the dropdown list.



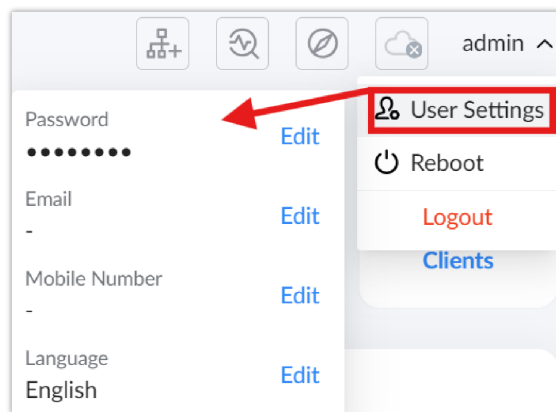
Change language

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

Note: Each user can now configure their own independent language preference. When switching between different user accounts, the interface will automatically change according to the specific logged-in user's settings.

User Settings

The **User Settings** menu allows for quick configuration of personal information for the currently logged-in user.



User Settings

From this menu, you can edit the following fields:

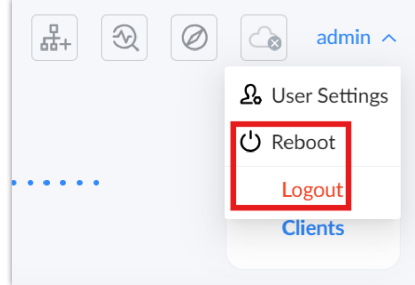
- **Password:** Update your account login credentials.
- **Email:** Configure an email address associated with the user account.
- **Mobile Number:** Set or update a mobile contact number.
- **Language:** Choose your preferred display language for the Web UI.

Tip: For comprehensive configuration of multiple users and detailed permissions, please refer to the **Advanced > System > User Management** section.

Rebooting or Logging Out

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

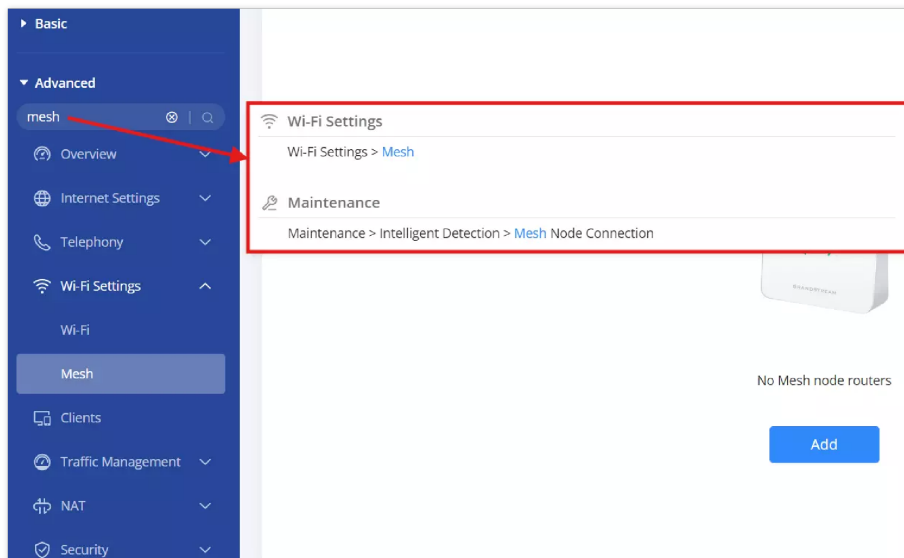
- **Reboot:** Click on **Reboot** to restart the router. This will temporarily disconnect all network connections and may take a few minutes to complete.
- **Logout:** Click on **Logout** to securely exit the web interface. You will need to log in again to access the settings.



Rebooting or Logging Out

Search

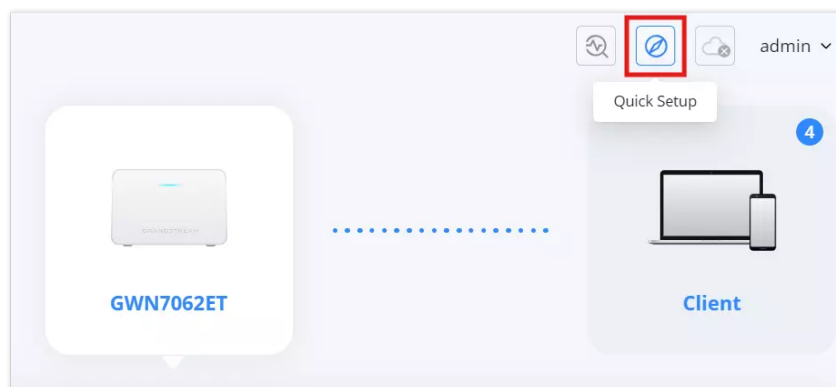
To make it easier for the user to find a particular option quickly, the device's web UI has a search feature. Users can access this feature by clicking on the search bar at the top of the left-hand menu under Advanced and typing the desired option name.



Search

Quick setup

If the user missed the Setup Wizard on the first boot of the 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. The **Wi-Fi** toggle at the top of the page can be used to enable or disable the wireless function during Quick Setup. The user specifies a **Wi-Fi Name (SSID)** within the allowed character range, selects the **Band** (2.4G & 5G, 2.4G, or 5G), and configures the **Security Mode** to ensure a secure connection (for example, WPA2/WPA3). A strong **Wi-Fi password** (8-63 ASCII characters or 8-64 hex 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

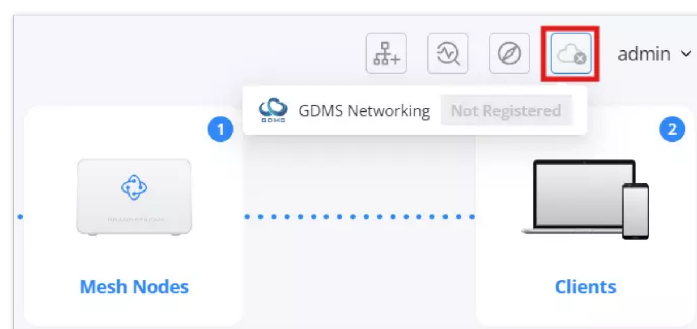
4. Automatic Upgrade

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

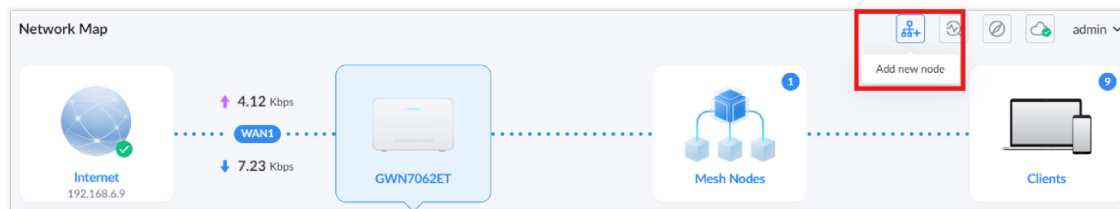
Benefits of GDMS Networking:

- **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](#)

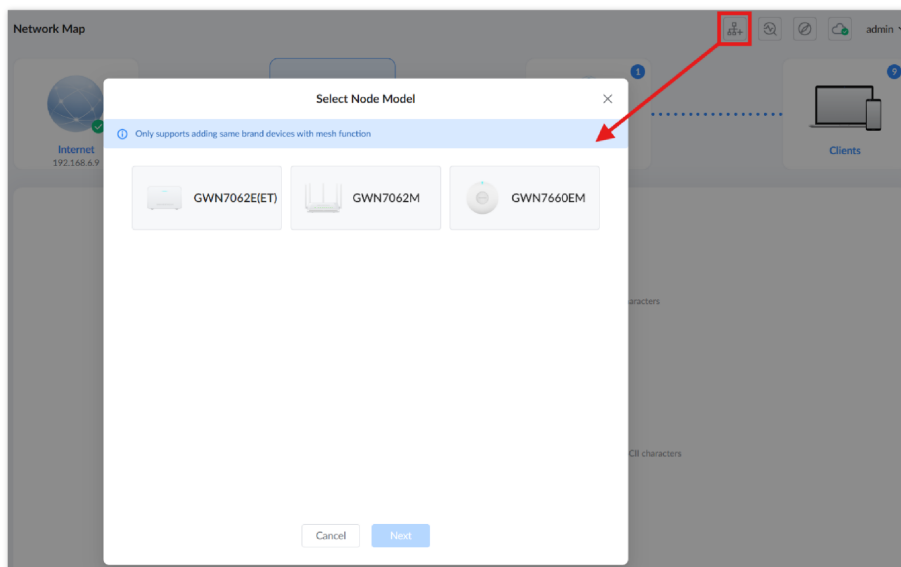
Mesh Network Shortcut

A Mesh Network shortcut is available in the top-right corner of the Network Map page, allowing users to quickly access the Mesh router adding workflow. This shortcut provides a convenient entry point for adding a new router to the Mesh network without navigating through the full Advanced menu.



Mesh Network Shortcut

Clicking the **Add New Router** shortcut opens the Mesh adding page, where users can start the process of adding a new node to the existing Mesh network.



Mesh Network Shortcut Add New Router

For detailed Mesh configuration, preparation requirements, and wired or wireless pairing 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 overview of the router's connection status, current internet speed, and connected clients.
- **Traffic Statistics:** Real-time monitoring of bandwidth usage across your network.
- **QoS (Quality of Service):** Tools to prioritize traffic for certain apps or devices, improving network performance.
- **HomeCare:** Includes Parental Control, SafeSearch, and basic firewall rules for better control and security.
- **Management Platform:** Offers management through:
 - **Grandstream Home App (Recommended)** – Scan the QR code or [click here](#) to learn how to manage your router using the mobile app (available on Android® and iOS®).
 - **Cloud Access** – Optional integration with Grandstream's cloud platform (GDMS.Cloud) or on-premise (GWN Manager) for extended configuration.

- **FXS Settings (GWN7062ET only):** Provides quick access to configure FXS port account settings for analog telephone connections.

This mode is ideal for home users, remote workers, and small businesses seeking essential network functionality with simple setup and mobile-first control.

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.

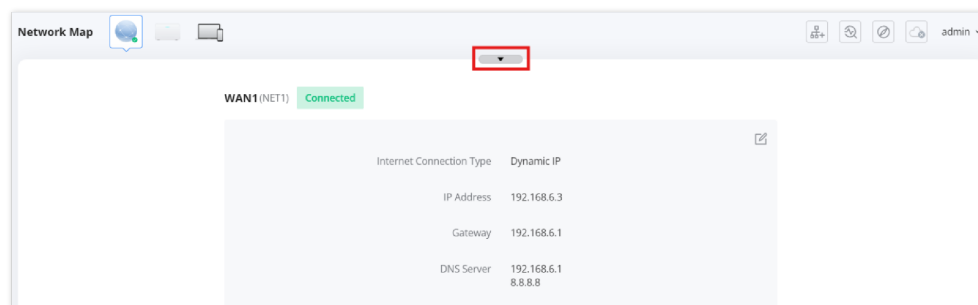
To navigate to the **Network Map**:

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

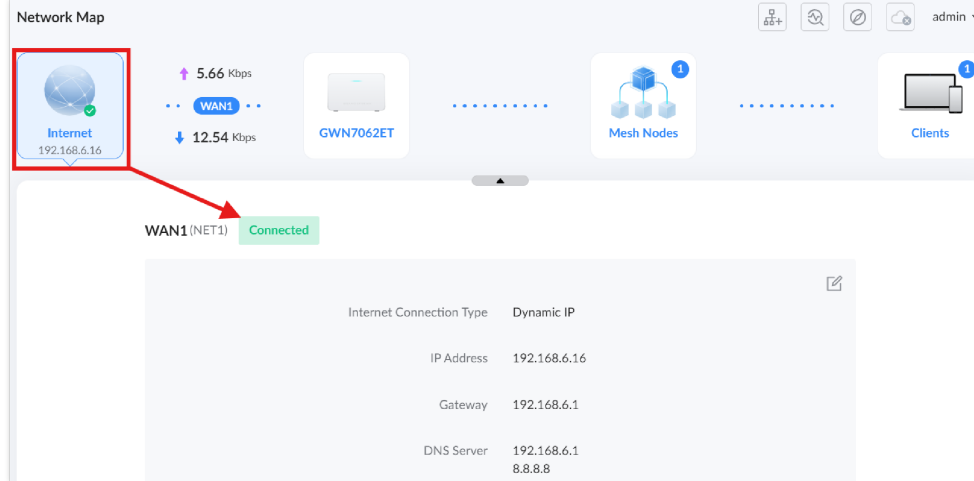
How to Use the Collapse/Expand Feature:

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

The **Internet** icon on the Network Map provides a real-time status of the router's gateway connectivity. The icon includes a status indicator and displays the current WAN IPv4 address directly beneath the label for immediate reference.



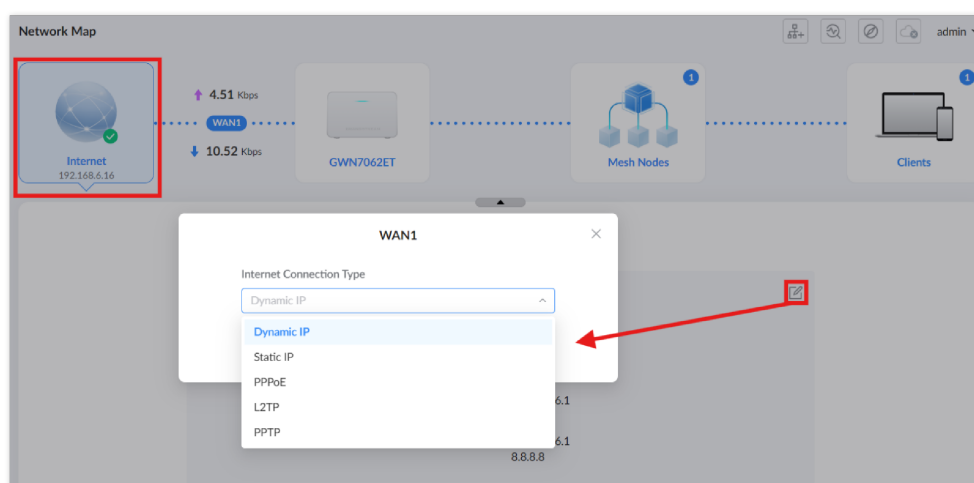
Network Map Internet

Clicking the **Internet** icon expands a detailed information panel. This panel provides the following technical data:

- **Connection Status:** Displays the current state of the WAN interface (e.g., **Connected**) and identifies the specific physical port in use (e.g., **WAN1 (NET1)**).
- **Internet Connection Type:** Indicates the protocol used to establish the connection, such as **Dynamic IP**, **Static IP**, or **PPPoE**.
- **IP Address:** The public or gateway IP address assigned to the router.
- **Gateway:** The IP address of the next-hop device or ISP gateway.
- **DNS Server:** The addresses of the DNS servers currently resolving domain names for the network.

WAN Configuration

To modify the internet connection parameters, click the **Edit (Pencil Icon)** in the top-right corner of the details panel.



Network Map Internet Edit WAN

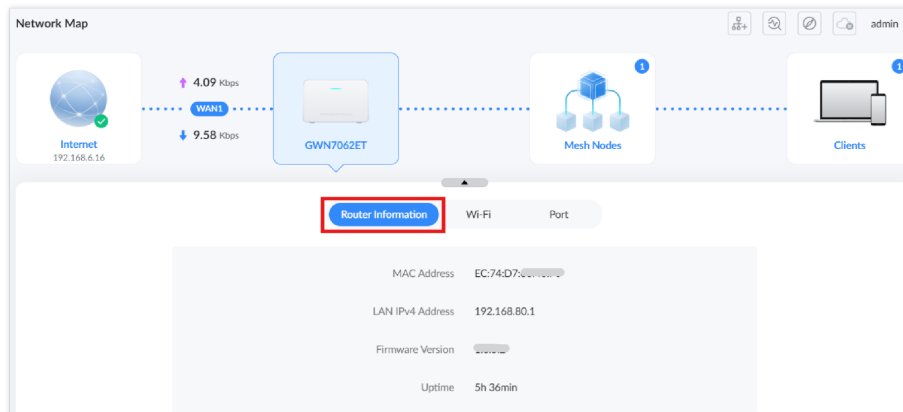
A configuration window will appear, allowing the selection of the **Internet Connection Type** based on the ISP's requirements:

Connection Type	Description
Dynamic IP	The router automatically obtains an IP address via DHCP. This is the standard configuration for most residential and business environments.
Static IP	Requires manual entry of a fixed IP address, subnet mask, gateway, and DNS servers.
PPPoE	Requires a service-provider-issued username and password to establish the connection.
L2TP	A tunneling protocol that requires a server address and authentication credentials.
PPTP	An alternative tunneling protocol requiring a server address and authentication credentials.

Primary Router Information

Displays essential details about the router, including:

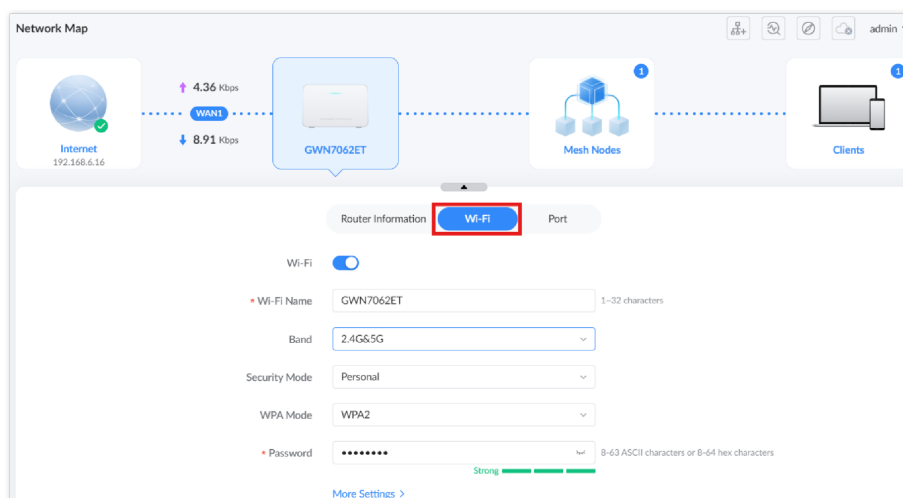
- **MAC Address:** The unique identifier assigned to the router.
- **LAN IPv4 Address:** The internal IP address used for local network communication.
- **Software Version:** Indicates the firmware version currently installed.
- **Uptime:** Shows how long the router has been running since the last restart.



Network Map Router Information

Wi-Fi Setting

The **Wi-Fi** tab allows for the direct management of the primary wireless network settings. To access these settings, click on the **Primary Router** icon (e.g., GWN7062ET) in the Network Map and select the **Wi-Fi** button.



Network Map Wi Fi

Field	Description
Wi-Fi	A toggle switch to enable or disable the wireless radio. When disabled, the router stops broadcasting all SSIDs and functions as a wired-only gateway.
Wi-Fi Name	Enter the Service Set Identifier (SSID) for the wireless network. Supports 1–32 characters.
Band	Select the operating frequency for the SSID. Options include 2.4G&5G (Dual-band), 2.4G , or 5G .
Security Mode	Defines the general security type for the network, such as Personal .
WPA Mode	Specifies the encryption protocol used for the connection, such as WPA2 or WPA2/WPA3 .

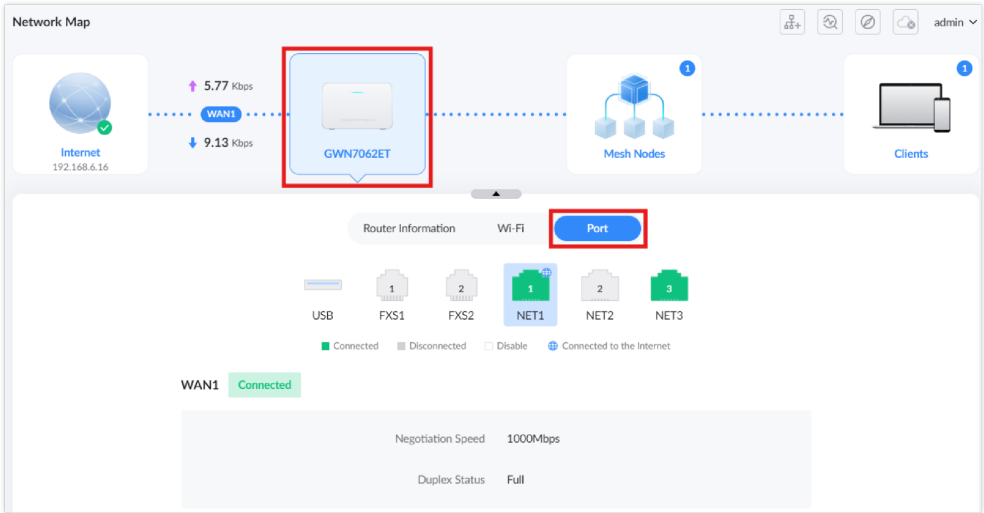
Field	Description
Password	Set or modify the security key for the Wi-Fi network. Supports 8–63 ASCII characters or 8–64 hexadecimal characters. A real-time strength meter indicates the security level of the chosen password.

Network Map – Wi-Fi

For advanced configurations, such as creating additional SSIDs, hidden networks, or adjusting channel widths, click the **More Settings** link at the bottom of the panel.

Port Status

The **Port** tab provides real-time visualization of the router’s physical interfaces, including Ethernet, telephony (FXS), and USB ports. This tool allows for the immediate verification of physical connectivity and link speeds.



Network Map Primary Router Port

To access these details, click on the **Primary Router** icon in the Network Map and select the **Port** button.

Visual Status Indicators

The operational state of each port is identified by specific color-coded icons and symbols:

- **Connected (Green):** The port has an active physical link with a connected device.
- **Disconnected (Grey):** The port is active, but no physical connection is detected.
- **Disable (White/Empty):** The port has been manually disabled within the system configuration.
- **Connected to the Internet (Globe Overlay):** A blue globe icon appears on the port currently serving as the active WAN gateway.

Port Technical Details

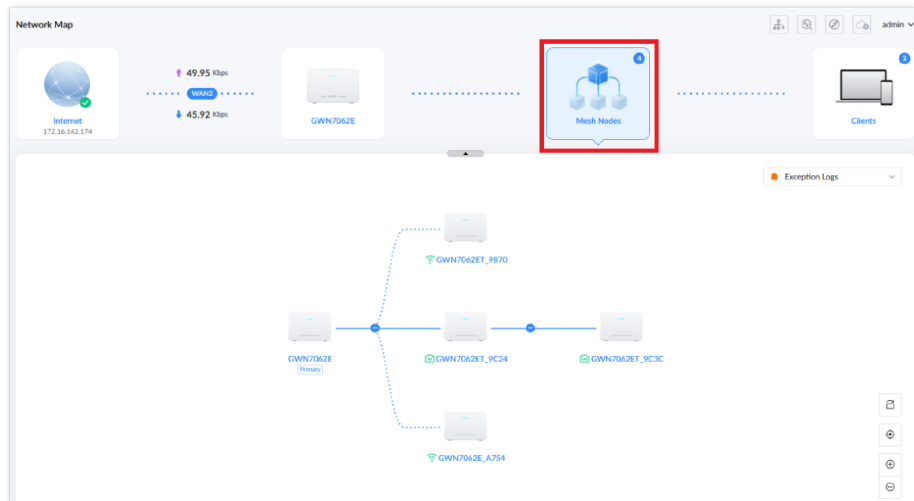
When a port is selected, the panel displays the following technical parameters for that specific interface:

Parameter	Description
WAN/LAN Status	Confirms the current logical state of the port (e.g., Connected).
Negotiation Speed	Displays the actual data rate established between the router and the connected device (e.g., 1000Mbps).
Duplex Status	Indicates the communication mode, typically Full (allowing simultaneous two-way transmission) or Half .

Network Map – Primary Router – Port

Mesh Nodes

The **Mesh Nodes** section provides an interactive visual representation of the mesh network topology. This interface allows administrators to monitor the health of the mesh network, understand device relationships, and manage individual satellite nodes.



Network Map Mesh Nodes

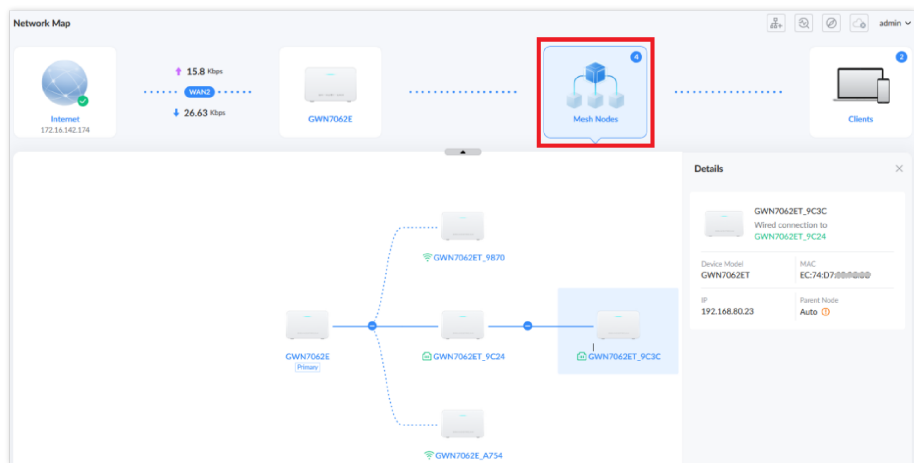
Interactive Topology Map

The topology diagram uses distinct visual cues to indicate connection types and network hierarchy:

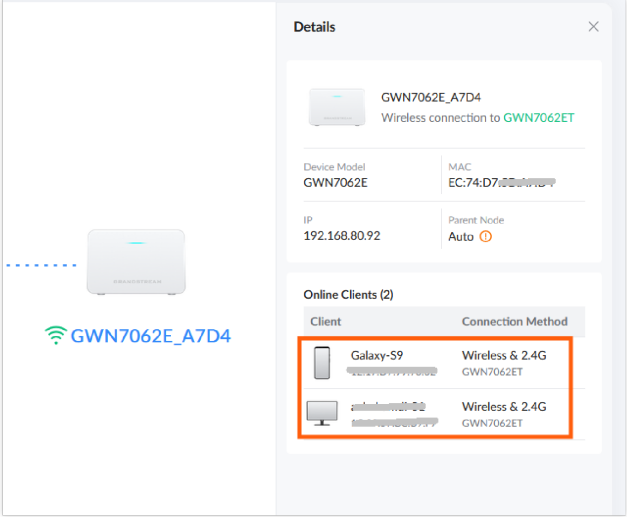
- **Connection Indicators:** Solid lines represent a **Wired** backhaul connection, while dotted lines represent a **Wireless** mesh connection.
- **Wired/Wireless Icons:** Node names are accompanied by icons (e.g., a green Wi-Fi symbol for wireless or a green Ethernet port symbol for wired) to immediately identify their current backhaul status.
- **Customizable Layout:** Nodes can be reorganized via drag-and-drop. Use the floating toolbar on the bottom right to **Save** the layout, **Center** the view, or **Zoom** in/out.

Node Details and Management

Clicking on any node in the map opens a **Details** panel on the right side of the screen, providing specific hardware and connection data for that device. The Details panel also displays the online clients connected through the selected Mesh node. The Online Clients list shows each client name, MAC address, connection method, wireless band, and the Mesh node used for the connection.



Network Map Mesh Nodes



Network Map Mesh Nodes Online Clients

Field	Description
Status Overview	Confirms the connection type and identifies the parent node (e.g., "Wired connection to GWN7062ET_9C24").
Device Model	Displays the specific hardware model of the node.
MAC	The unique physical identifier (Media Access Control address) of the device.
IP	The current local IP address assigned to the node.
Parent Node	Displays the current parent assignment. By default, this is set to Auto , allowing the system to determine the best path. Administrators can manually select a parent node here to optimize the mesh structure.
Online Clients	Displays the clients currently connected through the selected Mesh node, including the client name, MAC address, connection method, wireless band, and Mesh node used for the connection.

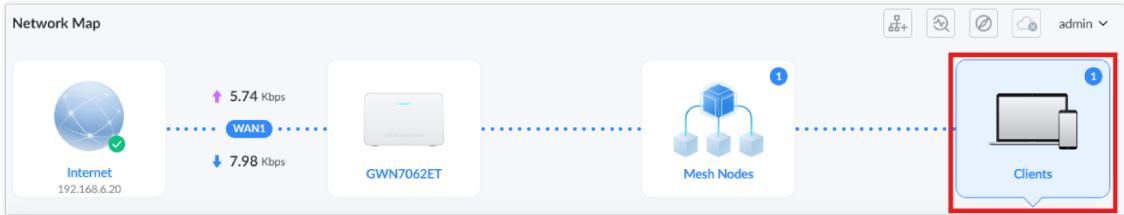
Network Map – Mesh Nodes

Exception Logs

The **Exception Logs** button (located at the top right of the diagram) provides a specialized log for mesh-specific events. This is used to track node disconnections, weak signal warnings, or parent-node switching, assisting in troubleshooting mesh stability.

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

Name	IP Address	Connect Time	Real-time Rate	Device Node	Operations
jelmokhliss-01 E8:F4:08:...	IPv4:192.168.80.235 IPv6:-	-	↑ Obps ↓ Obps	GWN7062ET EC:74:D7:...	   

Managing Connected Devices:

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

- **Edit (Pencil Icon):** Modify the device name or other settings.
- **Add to Blocklist (Prohibited Icon):** Adds the selected device to the blocklist to restrict its network access.
- **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.

For more options check the [Clients](#) section.

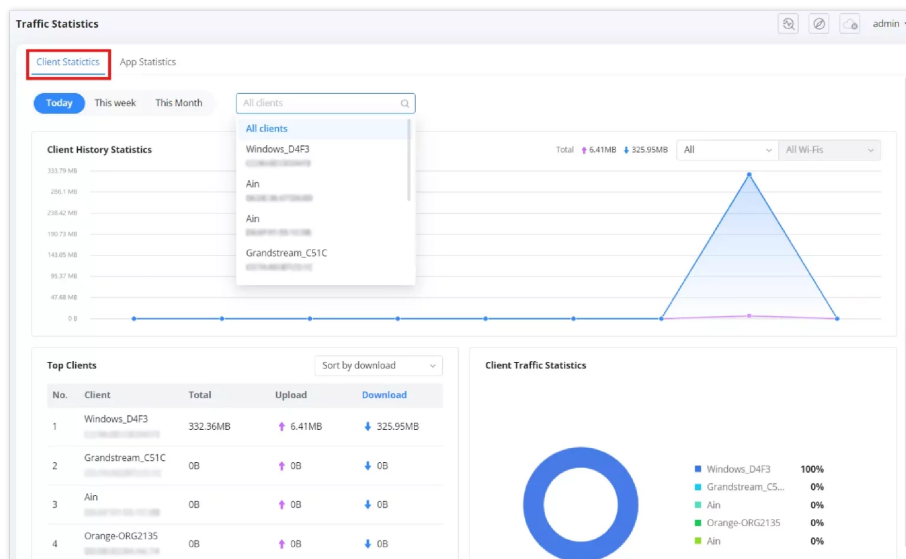
Traffic Statistics

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

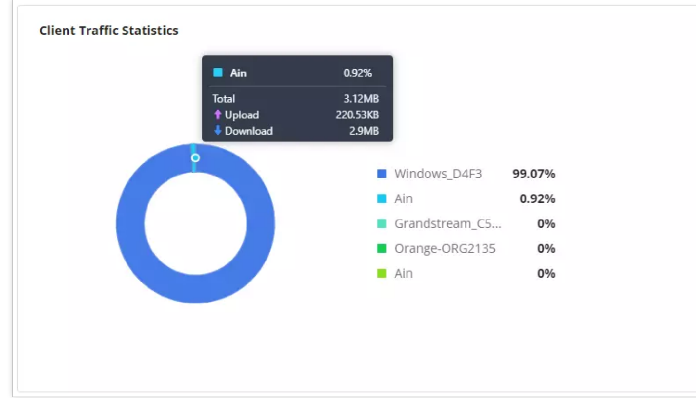
This tab displays **network usage per device**, allowing users to track bandwidth consumption for individual clients.

- **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.

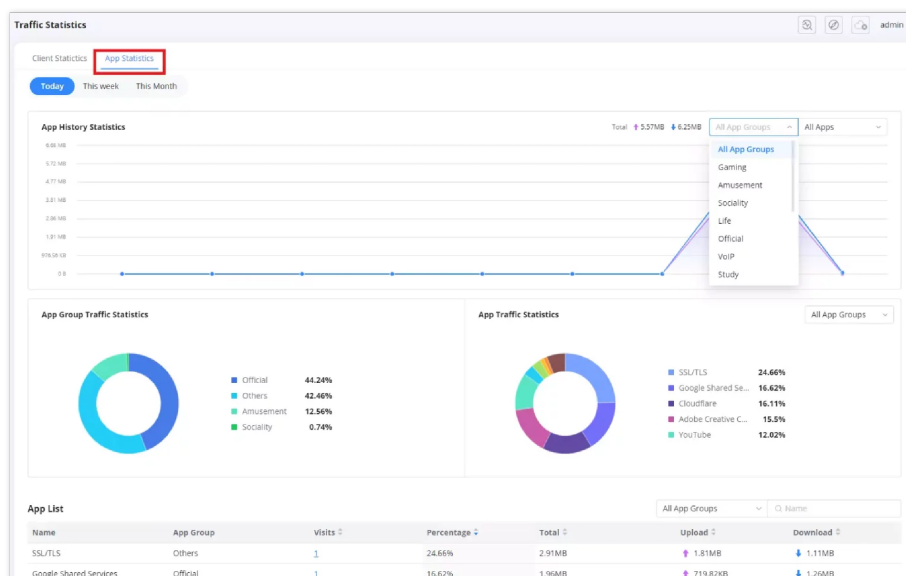


Traffic Statistics Client Statistics Part 2

App Statistics

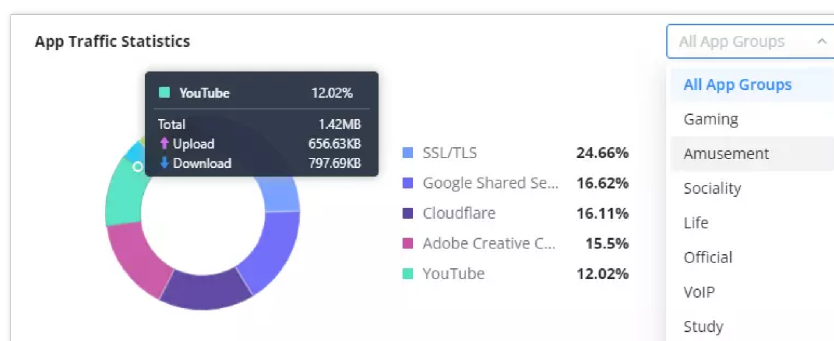
This tab provides a breakdown of network usage based on application types, enabling better traffic management and prioritization.

- **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 on this page to hover over graphs for more details or more info.



Traffic Statistics App Statistics part 2

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** then enable the WAN interface.
- Ensure that bandwidth settings are properly configured for QoS to function effectively.

QoS

QoS function

Enable

WAN Bandwidth Settings

Obtain bandwidth information from your ISP. It is recommended to set the bandwidth slightly below the peak.

WAN	Enable	Maximum Upload Bandwidth	Maximum Download Bandwidth
WAN1	Enable	100 Mbps	200 Mbps

Priority Surfing Mode

Auto Mode Game First Video First Web First

Cancel Save

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.
- **Enable:** Enables or disables QoS bandwidth control for the selected WAN interface. When enabled, the configured maximum upload and download bandwidth values are applied to that WAN connection.
- **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.

Note: If more than one WAN interface is configured, the maximum upload and download bandwidth can be set separately for each WAN interface, such as WAN1 and WAN2.

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.
- **General Settings:** Option to block internet access for unmanaged devices that are not subject to parental control rules.

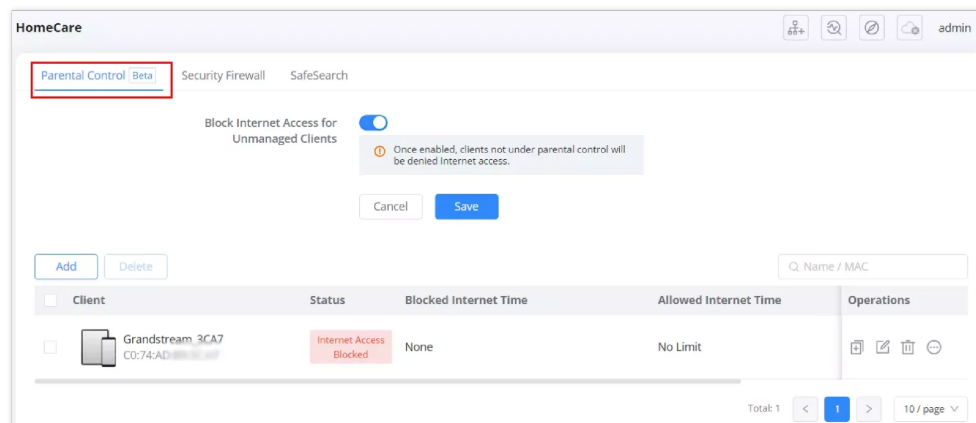
To configure **Parental Control**, navigate to **Basic** → **HomeCare** → **Parental Control** and use the available options to set restrictions, add devices, or customize browsing rules.

Parental Control

The **Parental Control** section allows 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 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.

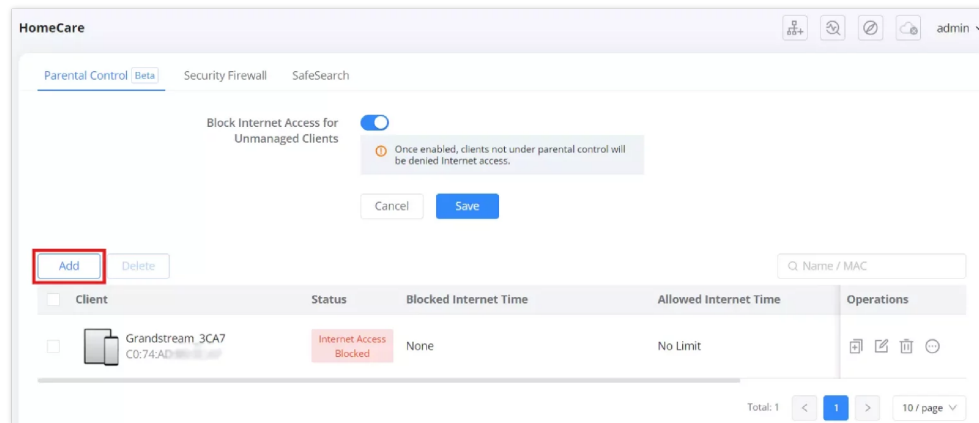
Navigating to Add a Client:

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 ClientDevice

Selecting or Manually Adding a Device

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

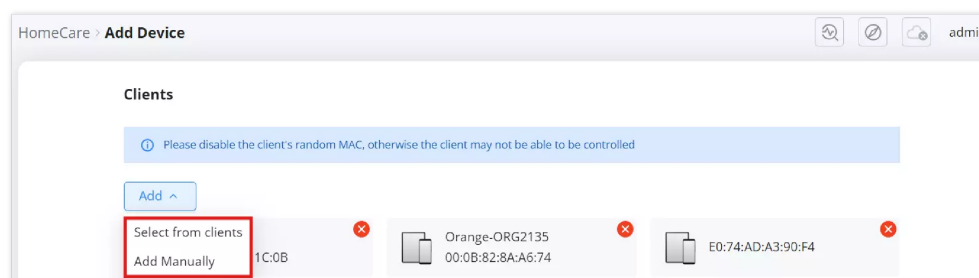
1. **Select from Clients** – Choose a device that is already connected to the router from the available list.
2. **Add Manually** – Enter the MAC address of a device that is not currently connected but needs to be managed under Parental Control.

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 deviceclient 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**:

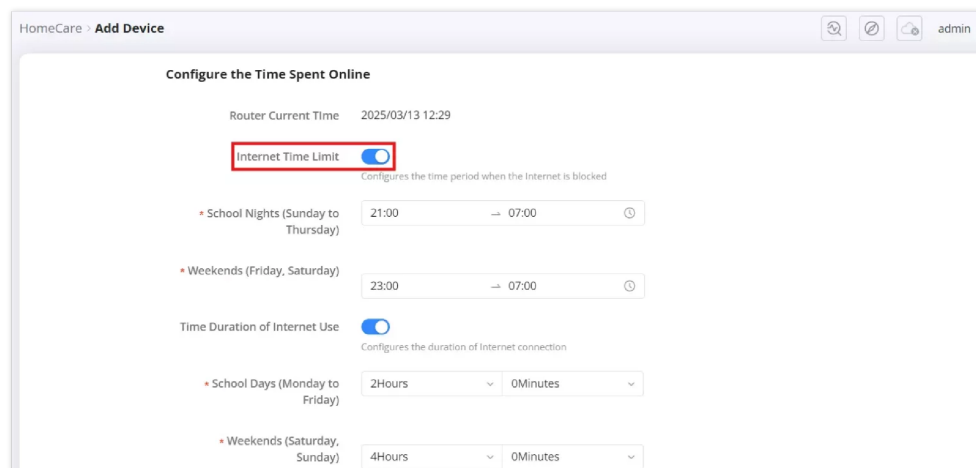
- Set restricted hours for **school nights (Sunday to Thursday)**.
- Define blocked times for **weekends (Friday and Saturday)**.

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

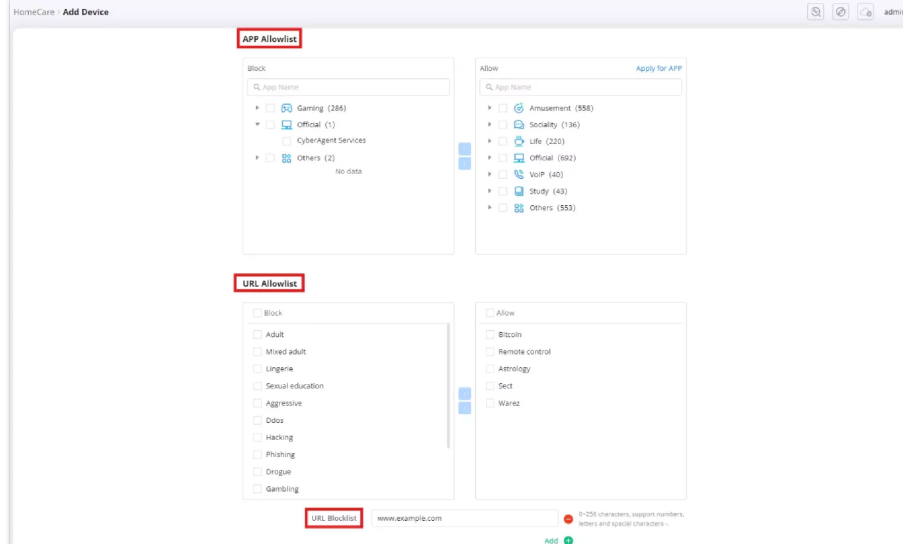
Configuring App and URL Filtering

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 AppURL allow or block

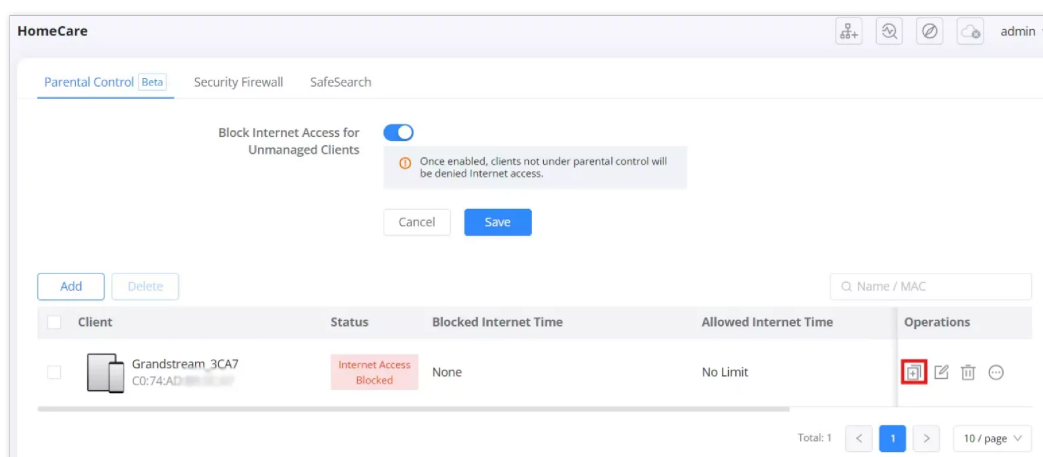
Applying Parental Control Settings to a New Device

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

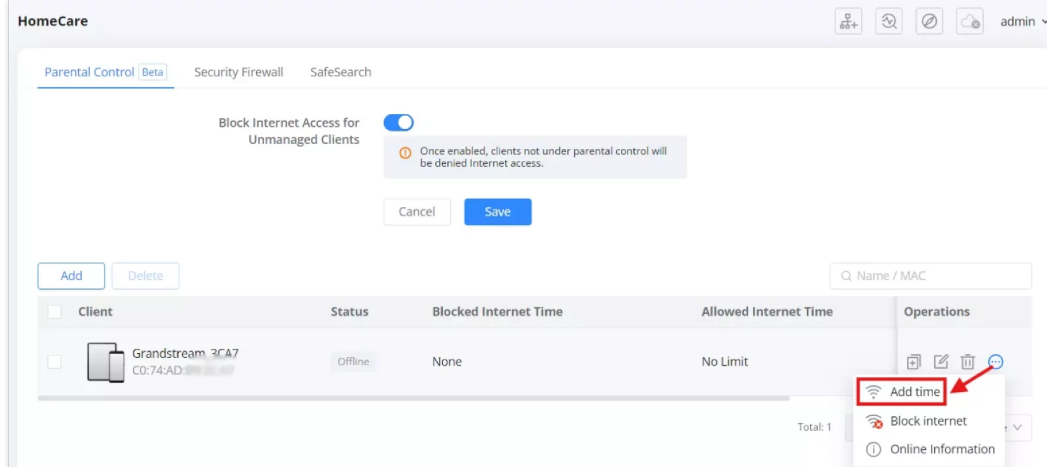
Parental Control – Block Internet and Add Time Options

The **Parental Control** page in **HomeCare** features enhanced control tools for managing internet access per device. Each connected device appears as a row with control icons represented by three dots

Once you click the dots for any listed client, you can choose between:

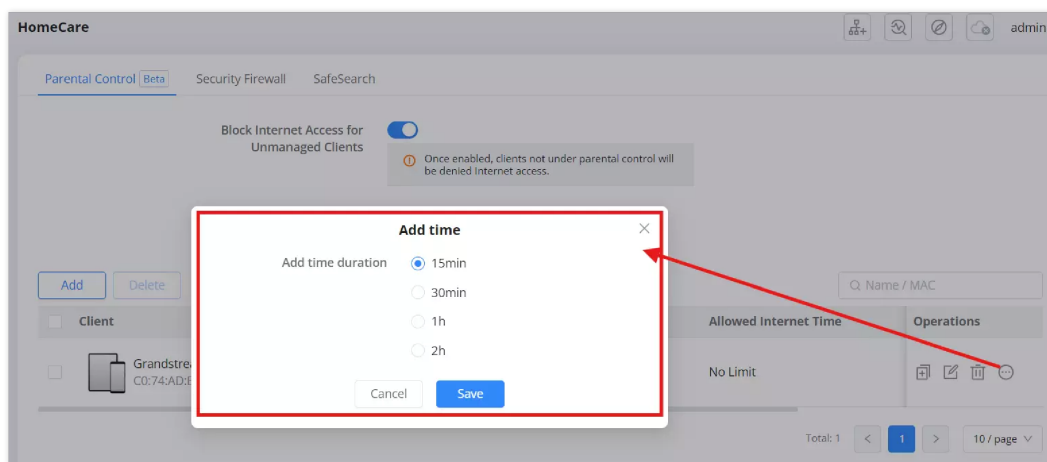
1. Add Time

Clicking **Add Time** opens a pop-up that lets you temporarily allow a device to connect to the internet during a defined time slot. This is ideal for managing screen time or temporary access.



Parental Control Add time

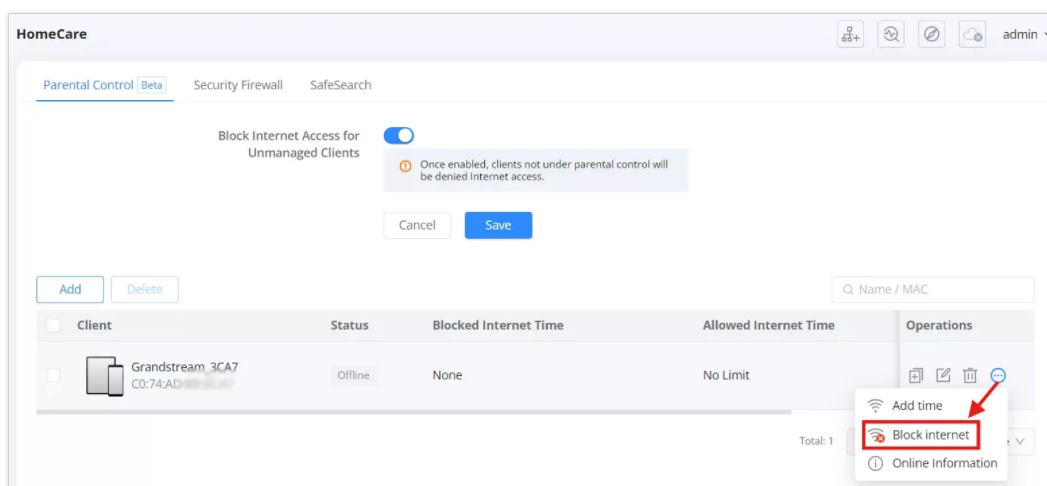
Then the user can select a specific internet access duration (15min, 30min, 1h, 2h) from the "Add time" dialog.



Parental Control Add time

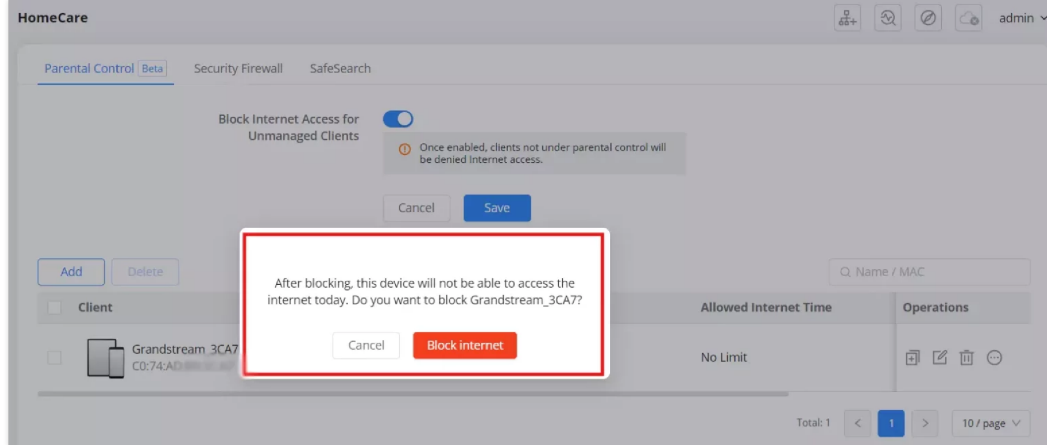
2. Block Internet

Clicking **Block Internet** from the client's three-dot menu allows you to immediately deny that device access to the internet for the rest of the day.



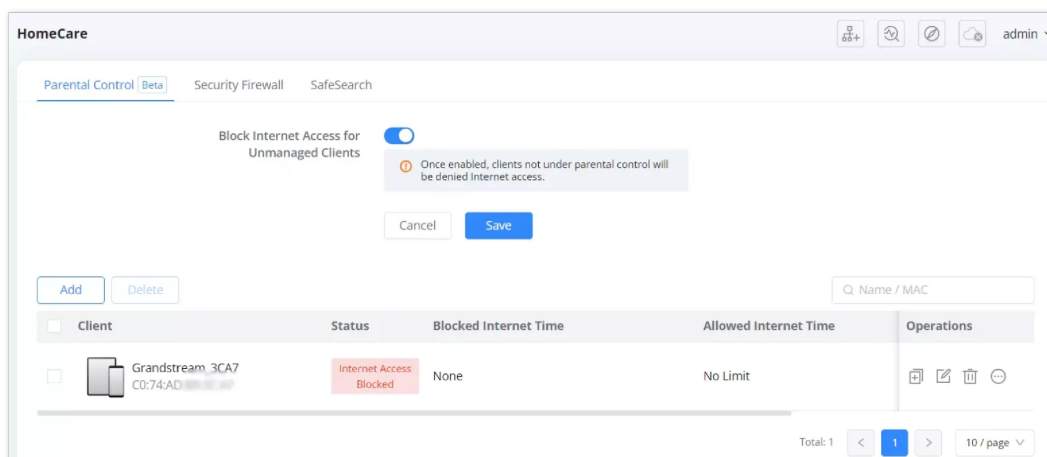
Parental Control Block Internet

Once selected, a confirmation pop-up appears to ensure the admin intends to block internet access for the selected client.



Parental Control Block Internet

After confirmation, the client's row is visually updated with a red badge showing **Internet Access Blocked** under the "Status" column.



Parental Control Internet Access Blocked

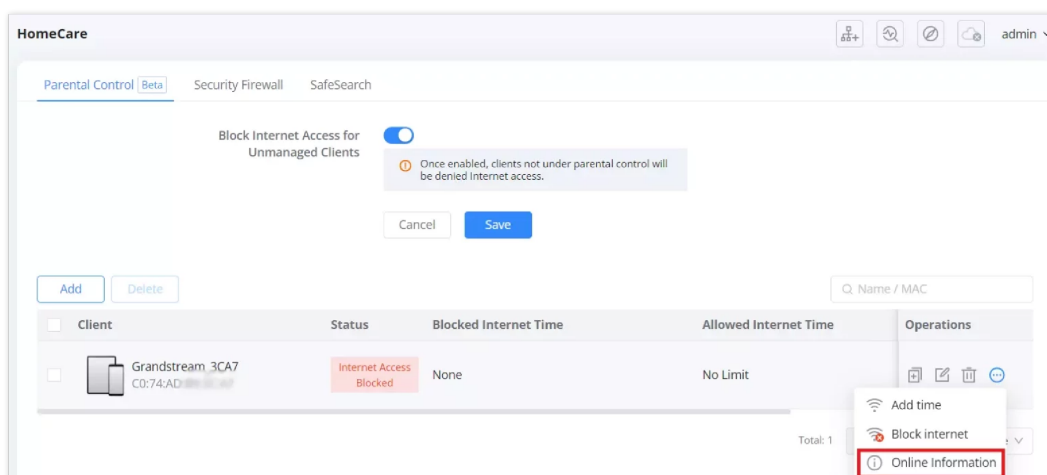
3. Online Information

The **Online Information** page under Parental Control provides detailed usage statistics for each managed client. Administrators can review internet time, data usage, and application traffic, and optionally block specific apps directly from this page.

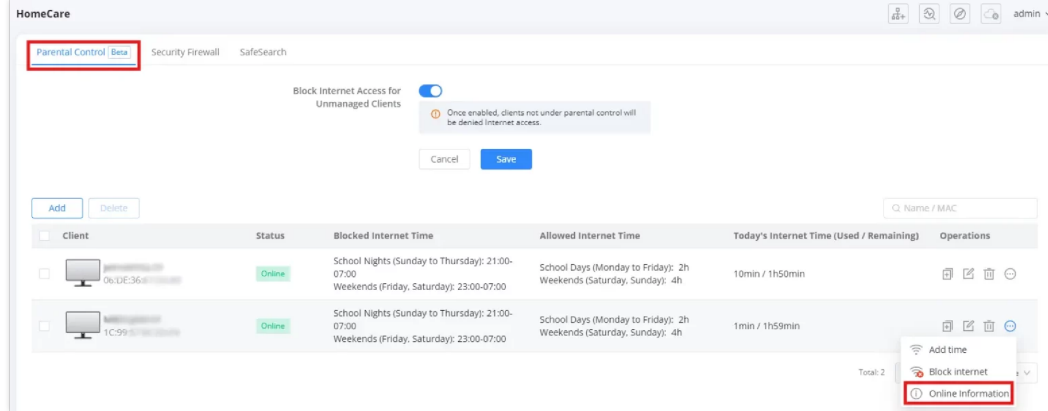
Accessing Online Information

1. Navigate to **Basic** → **HomeCare** → **Parental Control**.
2. In the client list, locate the device you want to inspect.
3. Click the **three-dot (⋮)** menu under the **Operations** column.
4. Select **Online Information**.

The Online Information page can be opened whether the client's status is **Online** or **Internet Access Blocked**.



Parental Control Internet Access Blocked



Parental Control Client Status Online

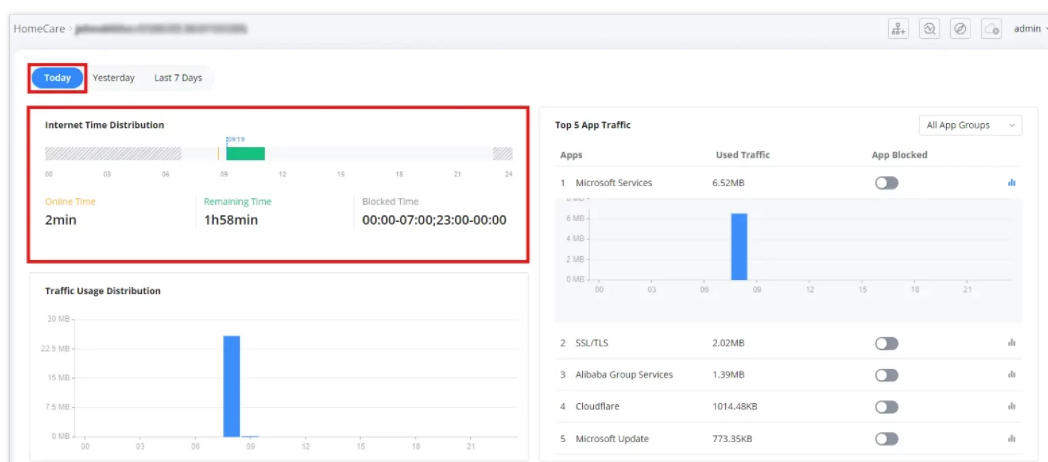
When opened, the page displays a breadcrumb such as:

HomeCare > [Client Name] ([MAC Address]) and provides three time-range tabs:

- **Today**
- **Yesterday**
- **Last 7 Days**

Today / Yesterday – Internet Time & Usage Overview

On the **Today** and **Yesterday** tabs, the layout is identical. The page shows how long the client has been online, how much time is remaining (based on Parental Control limits), and when internet access is blocked.



Client Online Information Today

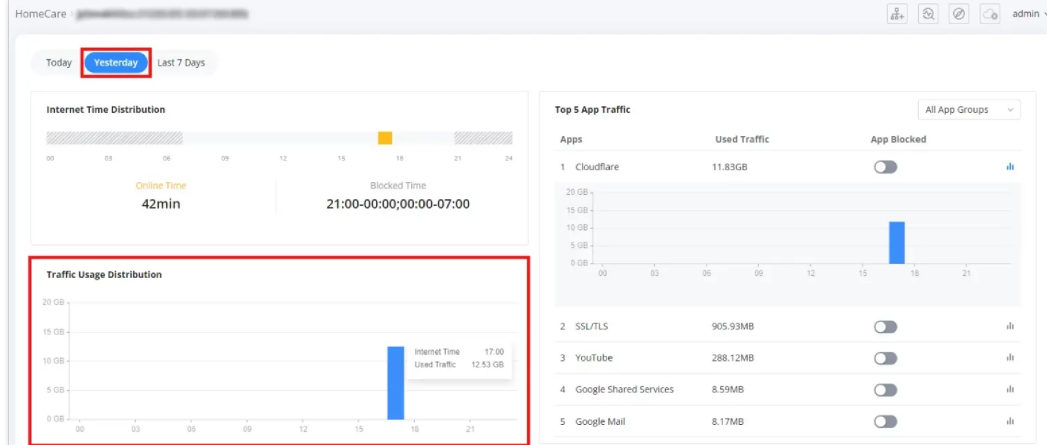
Internet Time Distribution

- Displays a 24-hour bar showing:
 - **Online Time**: total time the client has been connected during the selected day.
 - **Remaining Time**: remaining allowed time for that day, if a daily limit is configured.
 - **Blocked Time**: periods where internet access is blocked by the configured schedule (for example, school nights or bedtime hours).

This helps visualize when the device was online, how much time is still available, and when access is restricted.

Traffic Usage Distribution

- Shows a chart of **data usage over the day** for the selected client.
- Each bar represents the amount of traffic used during a specific time period.
- Hovering over a bar displays a tooltip with additional details such as:
 - **Used Traffic**
 - **Internet Time** during that period.



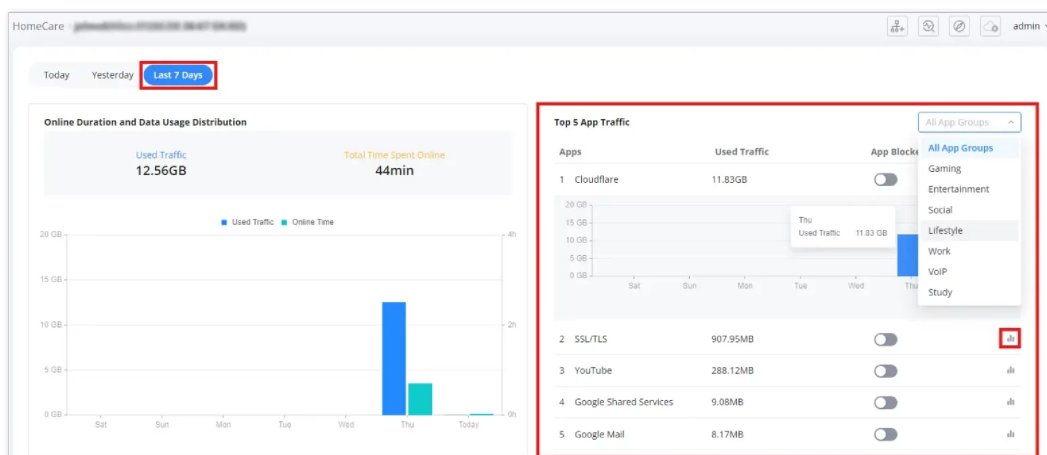
Client Online Information Yesterday

Top 5 App Traffic

- List the **top five applications or services** used by the client for the selected day.
- For each app, the following information is shown:
 - App name**
 - Used Traffic**
 - App Blocked** toggle
- The **App Blocked** switch can be used to immediately block or allow that application for the selected client.
- An **All App Groups** drop-down allows filtering by categories such as **Gaming, Entertainment, Social, Lifestyle, Work, VoIP, and Study**, so administrators can quickly focus on specific types of applications.

Last 7 Days – Aggregated Usage

The **Last 7 Days** tab shows a summary of the client's activity over the previous seven days.



Last 7 Days Aggregated Usage

Online Duration and Data Usage Distribution

- Displays the total usage for the selected client across the last seven days, including:
 - Used Traffic** (cumulative data usage for the period)
 - Total Time Spent Online** (total online duration over the last 7 days)
- A bar chart below shows daily values, typically indicating:
 - Used Traffic** per day
 - Online Time** per day

This view helps administrators quickly identify days with unusually high data consumption or long online periods.

Top 5 App Traffic (Last 7 Days)

- Shows the top applications used by the client during the last seven days, with:
 - App name**
 - Used Traffic** over the 7-day period

- **App Blocked** toggle
- The **All App Groups** drop-down can again be used to filter applications by category (Gaming, Entertainment, Social, etc.).
- Clicking the **three-bar (details) icon** next to an application expands additional information about that app's usage pattern within the selected time range.
- The **App Blocked** switch allows administrators to block or unblock an application directly from this list, applying the change to the selected client.

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

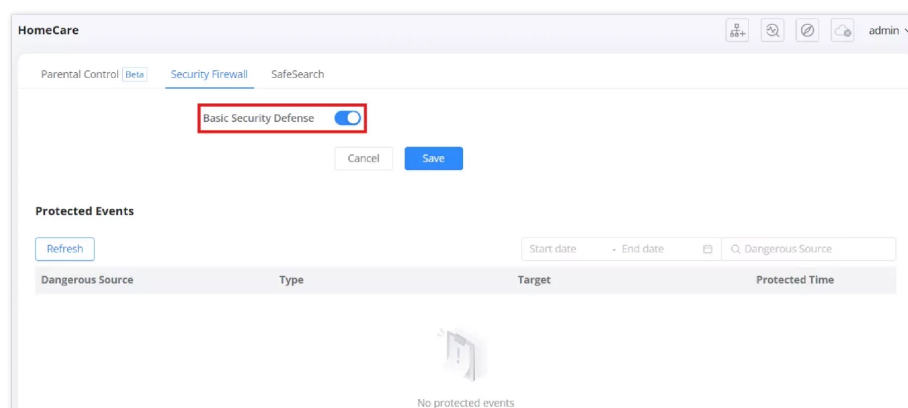
The **Security Firewall** feature under HomeCare provides **basic network security** by detecting and preventing potential threats, helping to protect connected devices from malicious attacks.

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.

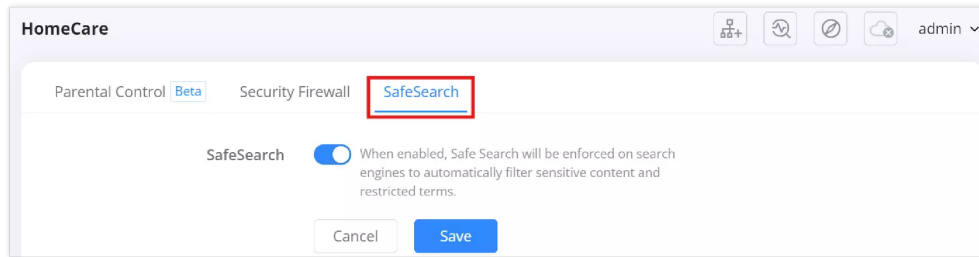
SafeSearch

The SafeSearch feature is designed to help protect users, especially children, by blocking explicit or sensitive search results across supported search engines.

► Accessing SafeSearch

To access this feature:

1. Log in to the Web UI.
2. Navigate to **Basic > HomeCare**.
3. Click on the **SafeSearch** tab.



SafeSearch

► Enabling SafeSearch

You will see a simple toggle switch labeled **SafeSearch**. When enabled:

- The router will enforce search filters on major search engines.
- This helps restrict access to adult content, inappropriate keywords, and sensitive search results.

After enabling the feature, click **Save** to apply changes.

Management Platform

Grandstream Home

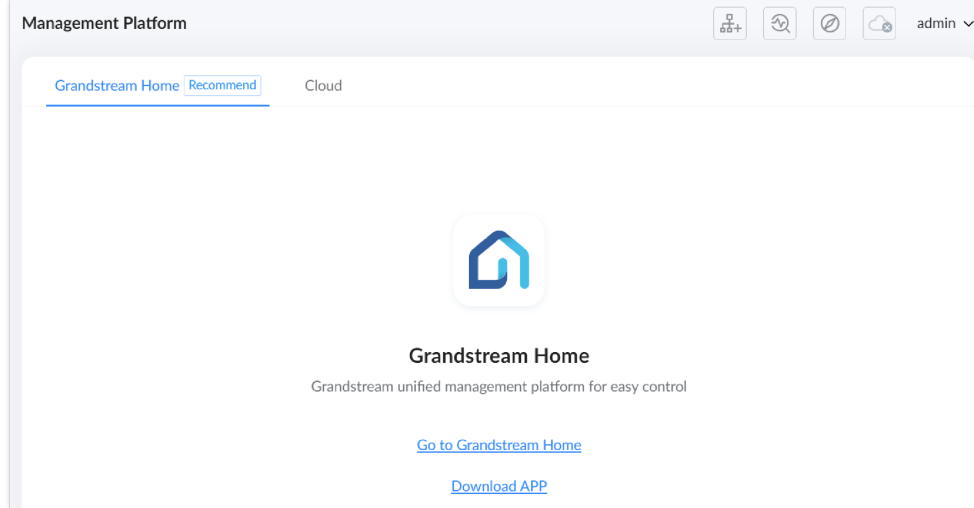
Grandstream Home is a simplified mobile-based platform designed for easy router control and setup within the local network. It's ideal for home users and small offices who want fast access to essential features without needing cloud registration or advanced configuration.

Key Features:

- Easy router setup in just a few taps
- Real-time monitoring of internet status and connected devices
- Mesh setup and pairing
- Parental Control
- Wi-Fi settings management
- Local notifications & diagnostics

How to Access:

1. Open the router's Web UI.
2. Go to **Basic → Management Platform → Grandstream Home**.
3. From this page, you can choose from the following access methods:
4. **Go to Grandstream Home:** Click this link to be directly routed to the official Grandstream Home web portal for centralized management.
5. **Download APP:** Click this link to display a QR code. Scan the code with your smartphone to download and install the Grandstream Home App for Android™ or iOS®.



Grandstream Home App

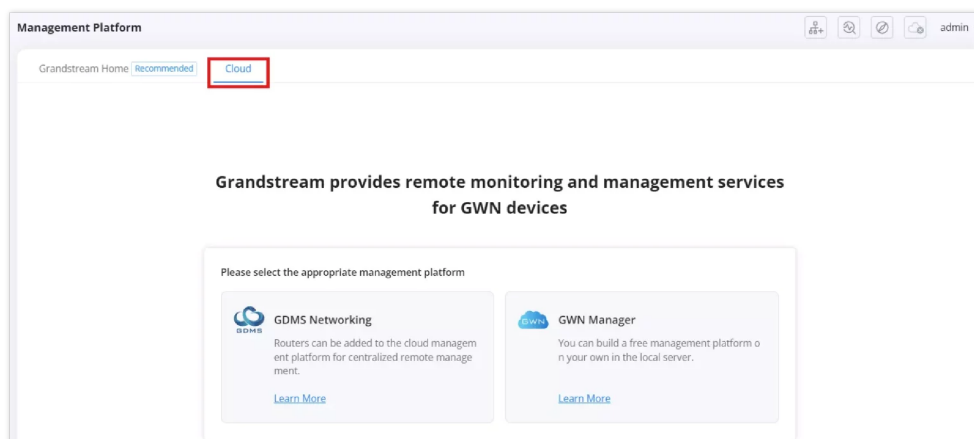


Grandstream Home App

For full usage instructions, please visit the official guide: [Grandstream Home User Guide](#)

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

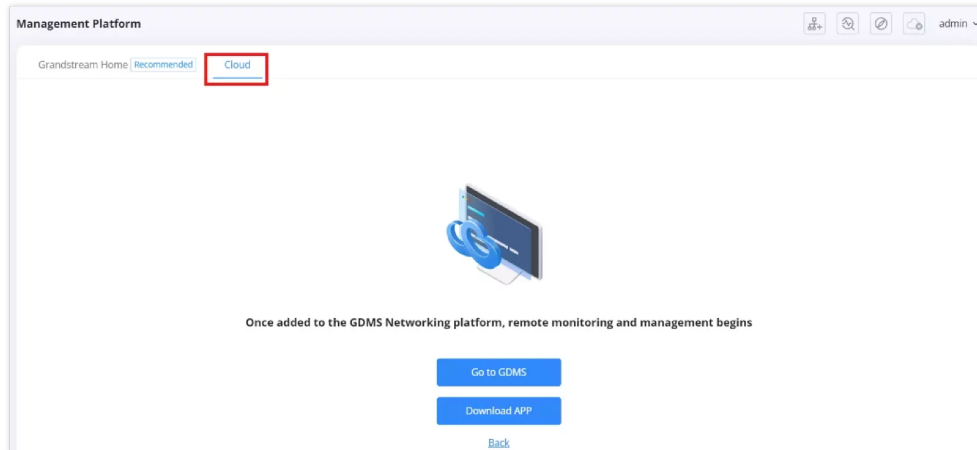
Users can choose between:

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.

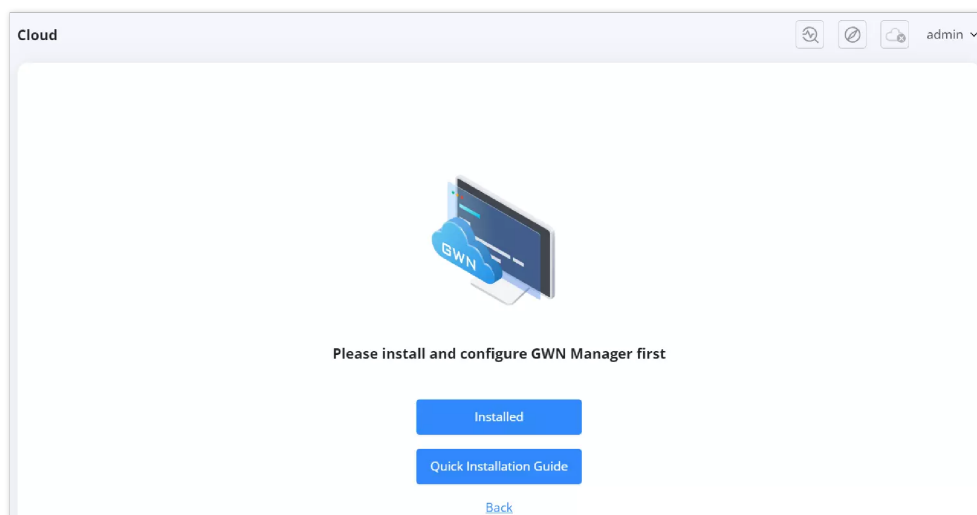
This integration allows network administrators to efficiently manage multiple devices remotely while ensuring real-time monitoring and configuration capabilities.

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

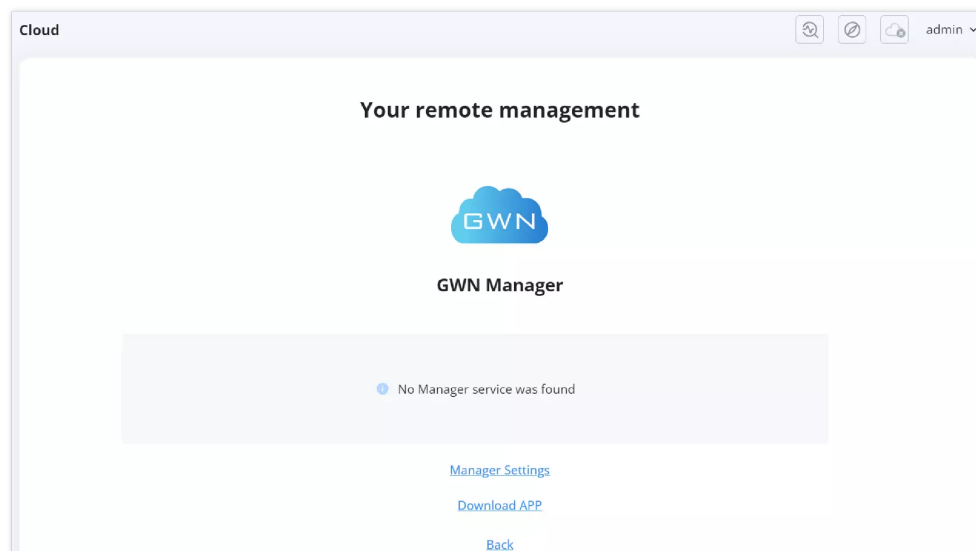


Cloud GWN Manager

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.

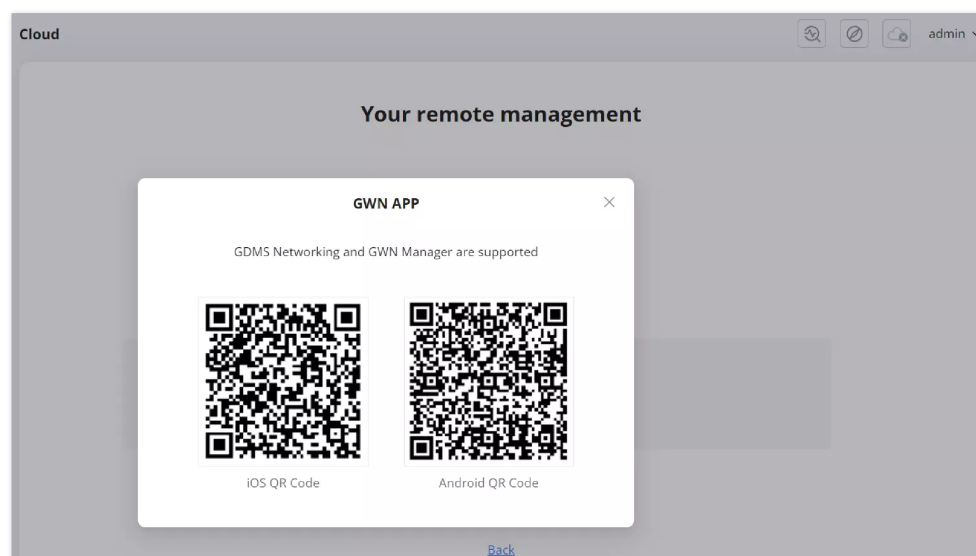
- **Download APP** – Install the mobile app for GWN Manager.



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**.

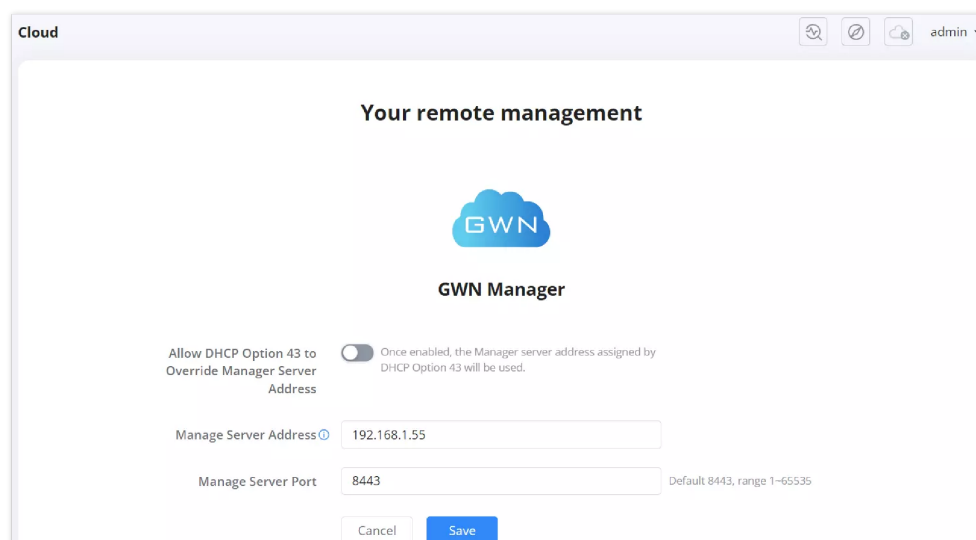


Cloud GWN Manager GWN App QR code

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.



FXS Settings – Basic

The **FXS Settings** page provides a simplified interface for the rapid configuration of analog phone ports on the primary router. This allows for essential telephony setup without navigating through advanced system menus.

Note: FXS port configuration is only supported on the primary router. For granular configurations, advanced SIP features, or managing ports on mesh nodes, please refer to the [\[Telephony – FXS Settings\]](#) section.

FXS Settings

Field	Description
FXS1 / FXS2	Select the specific physical analog port to configure.
User ID	The SIP account username provided by the VoIP service provider (0–64 characters).
Authenticate ID	The ID used for SIP authentication, usually the same as the User ID (0–64 characters).
Password	The authentication password for the SIP account.
Display Name	The name shown to the recipient during outgoing calls (0–64 characters).
Use and Sync Templates	Choose which predefined telephony template to apply to this port (Template 1 or Template 2).
SIP Registration Server	The IP address or Fully Qualified Domain Name (FQDN) of the SIP server/IPPBX.

Quick FXS Configuration Parameters

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:** Displays a detailed dashboard of the router’s performance, connection status, and system information.
- **Internet Settings:** Provides WAN, LAN, DHCP, static IP, PPPoE, and related internet configuration options.
- **Telephony (GWN7062ET only):** Provides configuration for FXS ports and VoIP-related settings.
- **Wi-Fi Settings:** Allows configuration of SSIDs, encryption types, security protocols, wireless bands, guest Wi-Fi, and general Wi-Fi behavior.
- **Mesh:** Provides Mesh network management, including Mesh node status, topology, and parent node configuration.
- **Clients:** Allows monitoring and management of connected client devices.

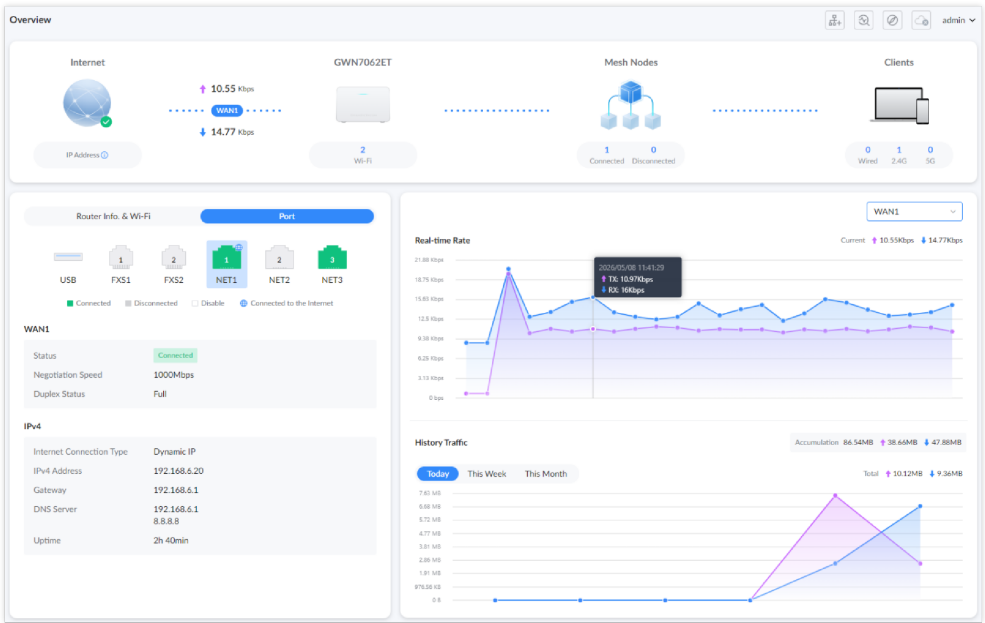
- o **Traffic Management:** Provides bandwidth control, traffic shaping, QoS, and WAN bandwidth settings.
- o **NAT:** Provides NAT-related features such as port forwarding, DMZ, UPnP, ALG, and related forwarding rules.
- o **Security:** Provides security features such as firewall, access control, IP exception, URL filtering, and basic security defense settings.
- o **VPN:** Provides secure remote access through supported VPN protocols, including L2TP, PPTP, OpenVPN, WireGuard, and IPsec.
- o **IPv6:** Provides configuration options for IPv6 WAN and LAN network settings.
- o **Captive Portal:** Provides guest network access control and authentication options.
- o **Maintenance:** Provides firmware upgrade, backup, restore, diagnostics, and maintenance-related functions.
- o **System:** Provides system-level settings such as user management, logs, time settings, access control, and system configuration.

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 serves as a centralized, real-time dashboard, providing a comprehensive snapshot of the router’s operational status, connectivity hierarchy, and network performance. This interactive interface allows administrators to monitor traffic trends and navigate directly to specific configuration menus.



Overview part 1

The dashboard is designed for high-level monitoring with integrated shortcuts:

- o **Icon Navigation:** Clicking on the **Internet**, **Router**, **Mesh Nodes**, or **Clients** icons at the top of the page redirects the user to their respective detailed management pages.
- o **Dynamic Graphs:** Hovering the cursor over any point on the **Real-time Rate** or **History Traffic** graphs reveals precise data values and timestamps.
- o **Time Filtering:** Statistical data can be toggled between **Today**, **This Week**, or **This Month** to analyze long-term network trends.

Dashboard Components:

1. Network Status Overview The top section displays the live topology and current throughput:

- o **Internet:** Displays the current **IPv4** and **IPv6** gateway addresses directly on the map for immediate reference.
- o **Connectivity Stats:** Shows live upload (TX) and download (RX) speeds, alongside counts for connected Mesh Nodes and Clients (categorized by Wired, 2.4G, and 5G).

2. Router Information & Port Status The secondary panel allows users to toggle between two views:

- **Router Info. & Wi-Fi:** Displays the MAC address, LAN IP, and system uptime. It also includes a summary table of active SSIDs, their operating bands, and their respective **Security Mode** and **WPA Mode**.
- **Port Status:** Provides a visual representation of the physical interfaces. The status of each port is identified by color and icon:
 - **Connected (Green):** Active physical link.
 - **Disconnected (Grey):** Port is active but no device is detected.
 - **Disable (White):** Port is manually turned off.
 - **Connected to the Internet (Globe Icon):** Identifies the port currently serving as the WAN interface.

3. Performance Analytics The right-hand panels focus on data throughput:

- **Real-time Rate:** An interactive line graph showing live bandwidth consumption.
- **History Traffic:** Summarizes total data accumulation (Upload/Download) for the selected period.

Mesh Network Monitoring:

The **Mesh** section provides a detailed table of all paired nodes in the network.

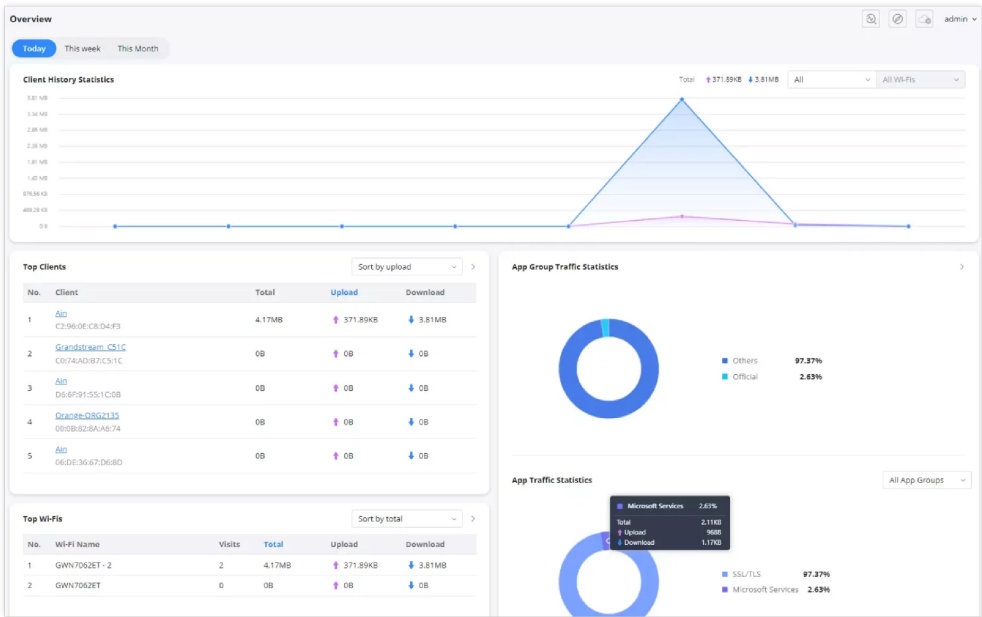
Mesh							
Device	Online Clients	Device Model	MAC Address	IP Address	GWN7062E	Status	
GWN7062ET_9870		GWN7062ET	EC:74:D7:88:88:88	192.168.80.40	Auto	Connected	
GWN7062ET_9C24		GWN7062ET	EC:74:D7:88:88:88	192.168.80.252	Auto	Connected	
GWN7062ET_9C3C		GWN7062ET	EC:74:D7:88:88:88	192.168.80.23	Auto	Connected	
GWN7062E_A754		GWN7062E	EC:74:D7:58:88:88	192.168.80.217	Auto	Connected	

Overview part 2

- **Parent Node Column:** This column identifies the connection path for each satellite node. When set to **Auto**, the system displays the parent node currently selected based on optimal network conditions. Hovering over the info icon provides further connection details.
- **Quick Diagnostics:** Click the diagnostic icon to jump to mesh-specific troubleshooting tools.

Traffic & Client Statistics

The bottom of the dashboard provides granular insights into who and what is using the network bandwidth.



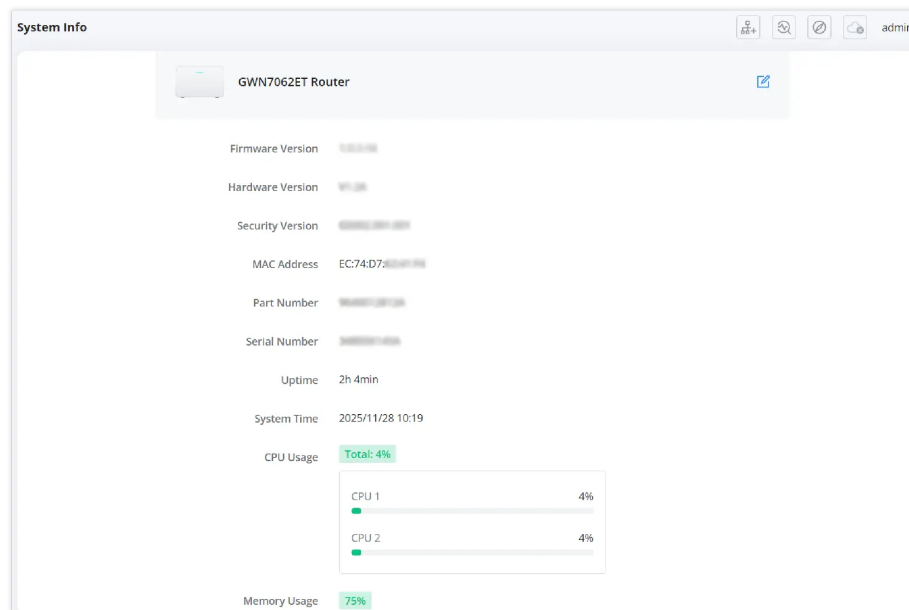
Overview part 3

- **Top Clients & Wi-Fis:** Lists the most active devices and SSIDs. Users can sort these lists by **Total**, **Upload**, or **Download** traffic to identify bandwidth-heavy users.
- **App Group & App Traffic:** Pie charts provide a visual breakdown of traffic by category (e.g., Microsoft Services, SSL/TLS, etc.). This helps administrators understand the distribution of network resources across different services.

System Info

The following details are displayed on this page:

- **Device Model:** Identifies the router model, e.g., **GWN7062ET**.
- **Firmware Version:** Displays the installed firmware version.
- **Hardware Version:** Indicates the router's hardware revision.
- **Security Version:** Displays the current security patch level included in the installed firmware. This helps verify if the router has the latest security updates and fixes.
- **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.
- **CPU Usage:** Shows the overall CPU usage (Total) as well as usage per CPU core, helping monitor current processing load on the device.
- **Memory Usage:** Displays the percentage of system memory currently in use.



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.

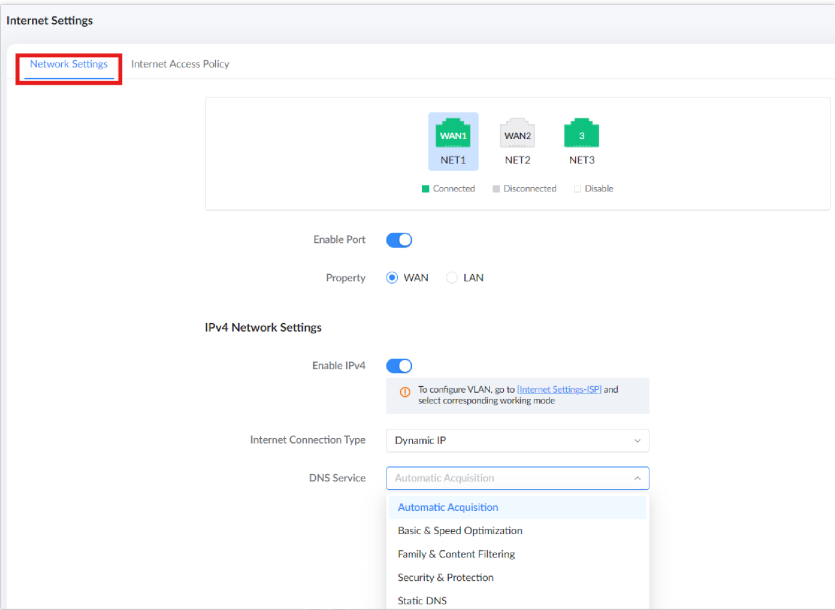
Internet Settings

Internet Setting

The **Internet Settings** page provides centralized management for physical port assignment, Wide Area Network (WAN) protocols, and multi-WAN traffic distribution for the GWN7062E and GWN7062ET routers. The interface is organized into functional tabs for granular network control.

Network Settings

The **Network Settings** tab manages the logical properties of the physical Ethernet interfaces. Each port is adaptive and can be logically assigned as either a WAN or LAN interface.



Internet Setting → Network Settings → WAN Settings

Field	Description
Enable Port	Master toggle to activate or deactivate the physical interface. When disabled, the port is rendered unusable regardless of whether its assigned role is WAN or LAN.
Property	Defines the logical role of the port as either WAN (Uplink) or LAN (Local Network).
Enable IPv4	When a port’s role is WAN, this switch specifically enables or disables the IPv4 network for that interface. Note: The IPv6 network is managed independently under Advanced → IPv6 .
Internet Connection Type	Select the protocol required by the ISP: Dynamic IP , Static IP , PPPoE , L2TP , or PPTP .
DNS Service	Allows the selection of predefined DNS provider profiles. Options include: • Automatic Acquisition: Obtains DNS automatically from the ISP . • Basic & Speed Optimization: Optimized for general performance . • Family & Content Filtering: Blocks inappropriate or adult content . • Security & Protection: Focused on blocking malicious domains . • Static DNS: Manual entry of preferred DNS server addresses. For a detailed breakdown of server addresses and specific use cases for each profile, refer to the DNS Service.

Port and Network Configuration Parameters

Note: When a port is assigned as a WAN, refer to the **ISP** section for specific VLAN tagging and working mode configurations.

Advanced Settings & Link Tracking

The lower portion of the tab contains hardware-level and link health monitoring configurations.

Advanced Settings

MAC Address of WAN Port

Use the default address

MAC Address

Use the default address

Use the MAC address of current management PC

Use custom MAC address

Link Tracking

Tracking Mode

☐ System Default

☒ Custom

* Detection Method

☐ Ping Target IP

☐ DNS Target Host

* Detection Threshold (times)

3

* Timeout (sec)

5

* Detection Interval (sec)

10

Advanced Settings Link Tracking

Advanced Settings: Some Internet Service Providers (ISPs) lock your internet connection to the specific hardware MAC address of the first device connected to their modem. If you are installing this new router and the internet will not connect, you can change the MAC address to bypass this ISP restriction:

MAC Address Option	Description & Use Case
Use the default address	The router uses its own factory-assigned MAC. Use this standard setting if your ISP does not use MAC binding.
Use the MAC address of current management PC	Clones the MAC address of the computer you are currently using to access the router. Use this if your computer was previously plugged directly into the ISP modem and had internet access.
Use custom MAC address	Allows you to manually type a specific MAC address. Use this if you are replacing an old router you can type the old router's MAC address here so the ISP still recognizes your connection.

Link Tracking: Link Tracking continuously monitors the health of your WAN connection to ensure it is actually online and transmitting data. This is critical for triggering Multi-WAN failover if the primary connection drops.

Link Tracking Parameter	Description
Tracking Mode	System Default: Uses the router's built-in parameters to check connectivity. Custom: Allows you to define the exact rules for when the router decides the internet is offline.
Detection Method	(Custom Mode) Choose how the router checks the connection: by sending a Ping (ICMP) to a target IP, or/and sending a DNS query to a target host.
Detection Threshold (times)	(Custom Mode) The number of consecutive failed checks required before the router officially marks the WAN link as disconnected.
Timeout (sec)	(Custom Mode) The maximum time the router will wait for a reply to a single Ping or DNS request before considering that specific attempt a failure.
Detection Interval (sec)	(Custom Mode) The time duration between each connectivity check (e.g., sending a Ping every 10 seconds).

Internet Access Policy

When multiple WAN interfaces are enabled, the **Internet Access Policy** tab defines how the router distributes traffic across the available links to optimize performance and ensure connectivity.

Load Balance Mode

In this mode, the router distributes outgoing network sessions across all active WAN interfaces simultaneously to maximize total throughput

The screenshot shows the 'Internet Settings' window with the 'Internet Access Policy' tab selected. Under 'Policy Mode', 'Load Balance' is chosen. A warning message states: 'Once VPN or policy route is configured, VPN and policy route will take precedence.' Below, 'Traffic Load Weight' is set to 1 for both WAN1 and WAN2. A dropdown menu for WAN2 is open, showing options from 1 to 8. 'Cancel' and 'Save' buttons are at the bottom.

Internet Access Policy Load Balance

Note: *Routing Precedence: To ensure traffic reaches its intended destination accurately, the router follows a strict routing hierarchy. Any established VPN tunnels or specific Policy Routes occupy a higher level of priority than general Load Balance settings. If a network session matches a VPN or Policy Route rule, the system will bypass the assigned weights and follow the specific routing instruction.*

Traffic Load Weight: Adjusts the proportion of traffic assigned to each interface (WAN1 vs. WAN2). The weight can be configured from 1 to 10 for each WAN. Higher values increase the weight ratio, meaning that specific interface will process a larger share of network sessions. These weights should be allocated based on the actual bandwidth capacity of each connection to ensure efficient data flow.

Failover Mode

This mode designates a primary path for all network traffic while holding an alternate interface in standby to ensure the network remains online if the primary link fails.

Internet Settings

Network Settings

Internet Access Policy

Policy Mode ⓘ

☐ Load Balance

☒ Failover

Preferred Interface

☒ WAN1

☐ WAN2

Alternate Interface

☐ WAN1

☒ WAN2

Failback ⓘ

☒

Cancel

Save

Internet Access Policy Failover

Field	Description
Preferred Interface	Identifies the primary WAN connection intended for normal operations.
Alternate Interface	Identifies the standby WAN connection that will automatically take over if the preferred link becomes unreachable.
Failback	Toggle to control automated recovery behavior. When enabled, if the Preferred Interface recovers while the Alternate Interface is in use, the system will automatically switch all network traffic back to the primary link to ensure the prioritized connection is used whenever it is healthy.

Internet Access Policy – 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

MAC Address

192.168.80.1

• IP Address

192.168.80.1

• Subnet Mask

255.255.255.0

Cancel

Save

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 Service

DHCP Server Address Binding

DHCP Service ☒

* Address Pool 192.168.80.2 - 192.168.80.254

* Release Time(m) 120 Range 60-2880

* Default Gateway 192.168.80.1

Preferred DNS Server 8.8.8.8

Alternative DNS Server 1.1.1.1

Cancel Save

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.

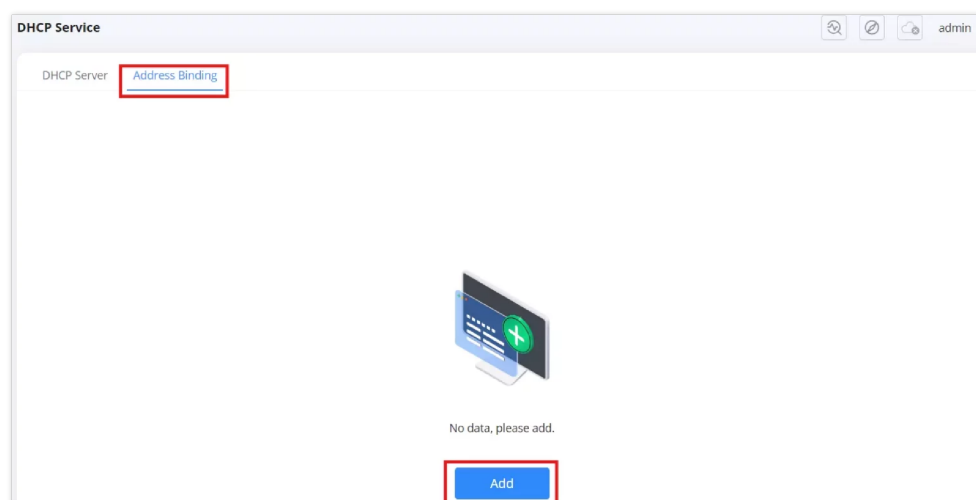
Navigating to the Address Binding Page

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.

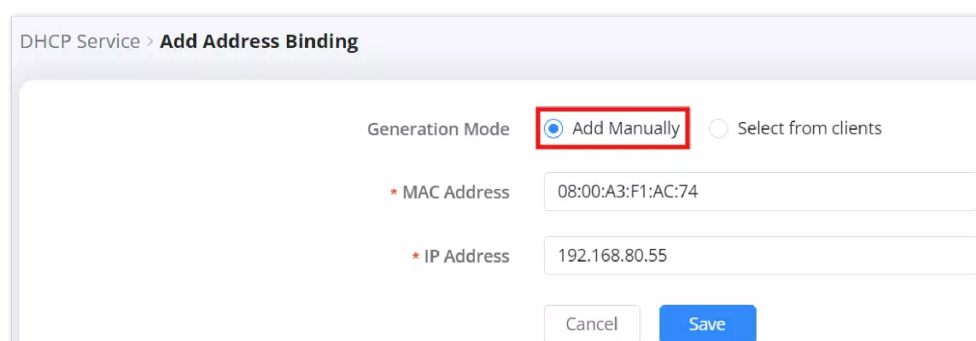
1. Click on **Add** to create a new address binding.
2. A new window appears with two configuration options:
 - **Add Manually** – Enter the **MAC address** and **IP address** manually.
 - **Select from Clients** – Choose a device from the **list of connected clients**, and the system will auto-fill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

DHCP Service > Add Address Binding

Generation Mode ☐ Add Manually ☒ Select from clients

* Client Name Ain (06:DE:36:67:D6:8D)

* IP Address

Ain
C2:96:0E:C8:D4:F3

Ain
06:DE:36:67:D6:8D

Ain
D6:6F:91:55:1C:0B

Grandstream_C51C
C0:74:AD:B7:C5:1C

Orange-ORG2135

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.

DNS Service

The DNS Service page acts as a technical directory for the various DNS provider profiles available within the router's WAN configuration menus. It provides transparency by allowing administrators to verify the specific server addresses and intended use cases for each service before selecting them in the network settings.

DNS Service Name	Description	IPv4 DNS Server	IPv6 DNS Server
Google	A global public DNS provided by Google, offering fast resolution and high stability.	8.8.8.8 8.8.4.4	2001:4860:4860:8888 2001:4860:4860:8844
OpenDNS	A Cisco service providing secure and reliable DNS resolution.	208.67.222.222 208.67.220.220	2620:119:35:35 2620:119:53:53
DNS.SB	A German public DNS service with servers worldwide, designed to provide low-latency resolution.	45.11.45.11 185.222.222.222	2a09:: 2a11::
Cloudflare DNS	A DNS service jointly launched by Cloudflare and APNIC, promising no user query logging, strong anti-...	1.1.1.1 1.0.0.1	2606:4700:4700::1111 2606:4700:4700:1001
Neustar UltraDNS	Public DNS provided by Neustar (USA), emphasizing high service reliability and rapid response.	64.6.64.6 64.6.65.6	2620:74:1b::1:1 2620:74:1c::2:2
AdGuard	Features fast response times and extensive global coverage.	94.140.14.140 94.140.14.141	2a10:50c0::1:ff 2a10:50c0::2:ff
FreeDNS	Provides basic free domain name resolution services.	37.235.1.174 37.235.1.177	2a00:dfc0::1 2a00:dfc0::2
SafeSurfer DNS	Focuses on security protection and provides reliable domain name resolution.	104.155.237.225 104.197.28.121	2001:4860:4860:8888 2001:4860:4860:8844

Basic & Speed Optimization

Family & Content Filtering

Security & Protection

DNS Service

Field	Description
DNS Service Name	The identifier for the supported DNS provider.

Field	Description
Description	Outlines the specialized function of the profile, such as speed optimization, ad-blocking, or malicious domain protection.
IPv4 DNS Server	The public IPv4 addresses the router will use for hostname resolution if this profile is selected.
IPv6 DNS Server	The public IPv6 addresses the router will use for hostname resolution if this profile is selected.

DNS Service Directory Columns

To assist in matching a provider to specific network requirements, the directory organizes services into three functional groups:

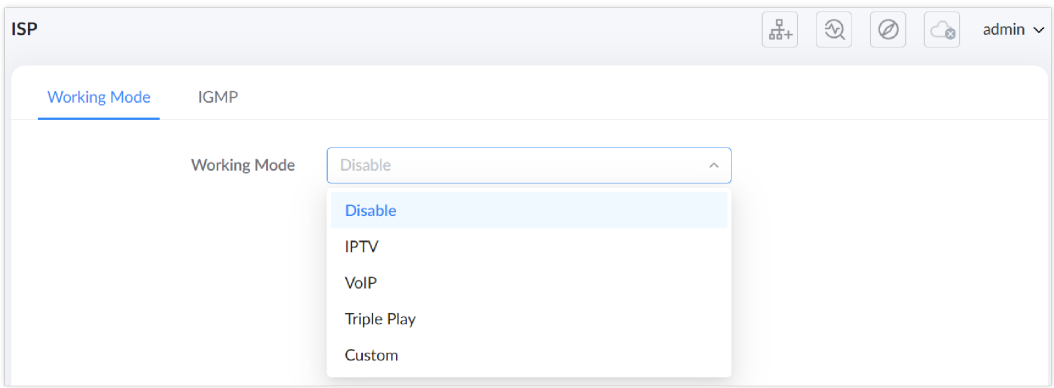
- **Basic & Speed Optimization:** Profiles optimized for general performance, high stability, and low-latency resolution. This category includes widely used providers such as **Google**, **Cloudflare**, and **OpenDNS**.
- **Family & Content Filtering:** Profiles specifically designed to block inappropriate or adult content to provide a comprehensive family network protection layer.
- **Security & Protection:** Profiles focused on blocking known malicious domains and providing enhanced security against online threats.

This centralized reference page ensures that users understand the technical impact of their DNS resolution choices within the internet connection settings.

ISP

The **ISP** 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** → **ISP** → **Working Mode** to configure the settings.



ISP Working mode

Selecting a Working Mode

In the **ISP** 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.
***Note:** Triple Play is not supported when two WAN ports are configured.*
- **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

The **IPTV Mode** allows for the logical shunting of specific physical LAN ports to act as dedicated bridges for television set-top boxes (STB). This enables the STB to communicate directly with the ISP’s IPTV headend, bypassing the router’s NAT and firewall to obtain its own IP address.

Working ModeIPTV

Connect the modem to the main router as shown in the following figure

Modem

Router

STB

TV

Internet Port

WAN1

IPTV Port

NET1

NET2

NET3

ISP

Malaysia-Maxis 1

802.1Q Tag

Internet VLAN

621

Internet VLAN 802.1p

0

IPTV VLAN

823

IPTV VLAN 802.1p

0

Triple Play IPTV

Field	Description
Internet Port	Select the physical WAN interface (e.g., WAN1) assigned to receive the incoming multi-service uplink from the ISP modem/ONT.
IPTV Port	Designate which physical LAN ports (NET1, NET2, or NET3) will be bridged to the IPTV VLAN. Devices connected to these selected ports are isolated from the standard local network to receive the dedicated video stream.
ISP	Pre-configured profiles for regional service providers (e.g., Malaysia-Maxis 1) that automatically populate necessary tagging parameters. Selecting None allows for manual entry of VLAN IDs.
802.1Q Tag	Master toggle to enable or disable the application of VLAN headers to traffic leaving the internet port.
Internet VLAN	The unique VLAN ID required by the ISP for general data traffic.
Internet VLAN 802.1p	Sets the priority bit (CoS) for data. Standard traffic typically uses priority 0.
IPTV VLAN	The unique VLAN ID assigned by the ISP to identify the television stream.
IPTV VLAN 802.1p	Sets the priority bit for video traffic. High priority values ensure the stream remains stable during network congestion.

IPTV Configuration Parameters

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.

Working Mode: VoIP

Connect the modem to the main router as shown in the following figure

Modem: LAN LAN LAN

Router: WAN NET 1, VoIP NET 2, NET 3

Phone

* Internet Port: ☒ WAN1

* VoIP Port: ☒ NET1 ☐ NET2 ☐ NET3

* ISP: Select ISP

Internet VLAN:

Internet VLAN 802.1p:

802.1Q Tag: ☐

VoIP VLAN:

VoIP VLAN 802.1p:

Cancel Save

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**.

Working Mode

Custom

* Internet Port

WAN1

802.1Q Tag

* WAN VLAN

20

Range 2~4094

* WAN VLAN 802.1p

4

Range 0-7. 7 is the highest priority.

NET Bridge

NET

VLAN

802.1p

NET2

6

5

Add

Cancel

Save

Triple Play Custom

IGMP

The **IGMP** tab manages multicast traffic handling to ensure efficient delivery of IPTV streams and prevent unnecessary flooding of data across the local network.

ISP

Working Mode

IGMP

IGMP Proxy

Enable

* Internet Port

WAN1

IGMP Version

Auto

* Query Interval (secs)

125

IGMP Snooping

Enable

Multicast to unicast

* Monitoring Port

* Internet Port

WAN1

IGMP

IGMP Proxy: When enabled, the router acts as an intermediary between local IPTV clients and the ISP’s multicast router, managing group membership requests to ensure the correct streams are delivered.

Field	Description
Enable	Master toggle to activate the IGMP Proxy service.
Internet Port	Select the physical WAN interface that serves as the source for the incoming multicast stream.
IGMP Version	Defines the version of the Internet Group Management Protocol used. Select Auto to allow the router to negotiate the version (V1, V2, or V3) with the ISP gateway.
Query Interval (secs)	Sets the frequency at which the router sends out IGMP host queries to verify active group memberships. (Default: 125).

IGMP Snooping: IGMP Snooping allows the router to “listen” to IGMP join and leave messages. By maintaining a map of which devices are requesting multicast data, the router ensures traffic is only sent to the specific physical ports where an IPTV client is active.

Field	Description
Enable	Master toggle to activate IGMP Snooping on the local network.
Multicast to unicast	Converts multicast streams into unicast packets for specific clients. This is primarily used to improve performance and stability on wireless networks or for devices that handle unicast traffic more efficiently.
Monitoring Port	Specify the physical port number used to monitor and track multicast data conversion.
Internet Port	Identifies the WAN port associated with the snooping service.

IGMP Snooping Configuration

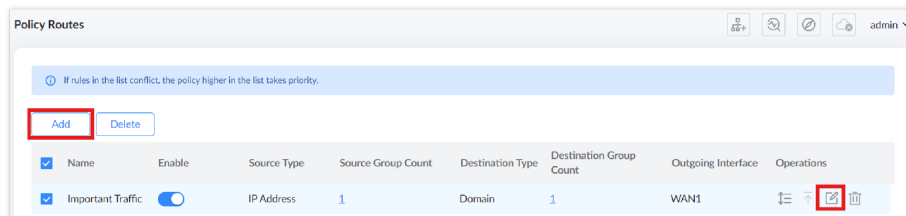
Policy Routes

Policy Routes function as a high-precision traffic control system, allowing you to bypass general load-balancing rules for specific data paths. By pairing a **Source** (who is sending) with a **Destination** (where it’s going), you can surgically direct traffic from certain devices or domains through a designated WAN interface. This is essential for prioritizing mission-critical applications such as ensuring specific workstations always use the most stable fiber link while letting standard web traffic follow general policies. Rules are executed in a strict **top-down sequence**, meaning the higher a rule appears in the list, the more authority it has.

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

Adding or Editing a Policy Route

Click the **Add** button to create a new routing rule, or click the **Edit** icon (pencil) in the **Operations** column to modify an existing one.



Policy Routes Add

- **Priority Logic:** The system processes rules from top to bottom. If multiple rules conflict, the one at the top of the list takes precedence.
- **Rule Management:** Use the **Operations** column to change the priority order (Up/Down arrows), edit settings, or delete rules.
- **Group Summary:** The **Source Group Count** and **Destination Group Count** columns show how many items (IPs, Clients, or Domains) are bundled into a single rule.

Configuring a Policy Route

The **Add/Edit Policy Route** window allows you to define traffic paths by pairing a **Source** with a **Destination**. By using the **Add (+)** icon, you can include multiple specific addresses or domains within a single rule to keep your routing list clean and organized.

Policy Routes · Edit Policy Route

Name

Important Traffic

1–64 characters

Enable

☒

Source Type

☐ All
☒ IP Address
☐ Client

Source IP Address

192.168.20.0

–

Add

+

Destination Type

☐ All
☐ IP Address
☒ Domain

Domain

youtube.com

–

Add

+

Outgoing Interface

☒ WAN1
☐ WAN2

Match Next Rule on Failure

☒

Configuring a Policy Route Example 1

Policy Routes · Edit Policy Route

Name

Important Traffic

1–64 characters

Enable

☒

Source Type

☐ All
☐ IP Address
☒ Client

Generation Mode

☐ Select from clients
☒ Add Manually

ⓘ

If the client use random MAC address, the MAC address will be inaccurate. Please disable random MAC address function on client side [\[How to disable?\]](#)

MAC Address

e.g. 08:00:20:0A:8C:6D

–

Add

+

Destination Type

☐ All
☒ IP Address
☐ Domain

Destination IP Address

–

Add

+

Outgoing Interface

☒ WAN1
☐ WAN2

Match Next Rule on Failure

☒

Configuring a Policy Route Example 2

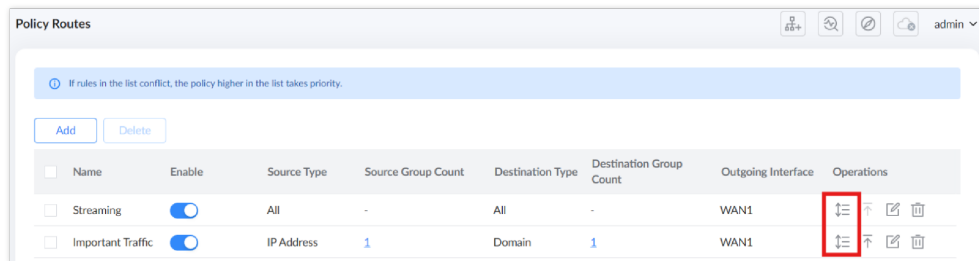
Field	Description
Name	Enter a descriptive name for the rule (1–64 characters).
Enable	Toggle to activate the routing rule.
Source Type	• All: Applies to every device. • IP Address: Enter a specific IP. Use Add (+) to include multiple source IPs. • Client: Select from the Connected Clients list or Add Manually to enter a MAC address. Use Add (+) to include multiple client devices. Note: 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.
Destination Type	All: Targets all traffic. IP Address: Enter a specific destination IP. Use Add (+) to include multiple target IPs. Domain: Enter a service address (e.g., youtube.com). Use Add (+) to include multiple domains. Note: Destination Type supports up to 65 unique IP addresses and domains.

Field	Description
Outgoing Interface	Designate WAN1 or WAN2 as the primary path for this traffic.
Match Next Rule on Failure	When enabled, if the selected WAN interface is down, the system will move to the next rule in the list to find an alternate path instead of dropping the traffic.

Policy Route Configuration Parameters

Managing Policy Priority

The router processes policy routes in a strict top-down hierarchy. If a network session matches multiple rules, the one located higher in the list will be executed first.



Managing Policy Priority

Adjusting Rule Order: To ensure critical traffic is handled correctly, you can manually adjust the priority of existing rules using the icons in the **Operations** column:

- **Reorder (Drag & Drop):** Click and hold the **Reorder** icon (three lines with arrows) to drag a policy to a new position in the list.
- **Move to Top:** Click the **Up Arrow** icon to immediately move a specific policy to the very top of the list, giving it the highest priority.

Telephony

The **Telephony** section is available when the primary router is **GWN7062ET**. It provides configuration options for analog phone services through the router's FXS ports, including direct IP dialing, FXS port management, SIP templates, accessibility features, phone audio settings, and ringtone behavior.

To access Telephony settings, navigate to: **Advanced** → **Telephony**

The Telephony menu includes the following pages:

Basic Settings

FXS Settings

Template Settings

Ringtone

Basic Settings

The **Basic Settings** page provides general telephony configuration for the current main router and sub-routers. Users can configure the WAN interface used for telephony behavior, enable IP address direct dialing, define WAN-side dial-in restrictions, configure logout behavior, enable DHCP Option 120 registration override, and configure STUN settings.

Basic Settings

Interface ☒ Auto ☐ WAN1

IP Address Direct Dialing ☒

Allowed WAN-side Dial-in IP Addresses

IP Address

IP Subnet

IP Range

Logout Scope ☐ Single ☒ All

Allow DHCP Option 120 to Override Registration Address ☒

STUN Settings

STUN Server Address

STUN Server Port Default 3478, range 1024–65535

STUN Refresh Interval (s) Default 60, range 10–160

Telephony Basic Settings

Field	Description
Interface	Selects the WAN interface used for telephony-related operation. Available options are Auto , WAN1 , and WAN2 .
IP Address Direct Dialing	Enables direct dialing by IP address. Once enabled, users can place direct calls using IP addresses.
Allowed WAN-side Dial-in IP Addresses	Configures the WAN-side IP addresses allowed to initiate direct IP dialing. Select the address type, such as IP Address , IP Subnet , or IP Range , then enter the corresponding address information. Click Add to add another allowed WAN-side dial-in IP address entry, or click the minus icon to remove an entry.
Logout Scope	Defines how the extension registration is cleared from the server. Single unregisters only the selected extension registration. All clears all registrations for the extension so the device can register again.
Allow DHCP Option 120 to Override Registration Address	When enabled, the registration address assigned by DHCP Option 120 is used.
STUN Server Address	Specifies the STUN server address used for NAT traversal.
STUN Server Port	Specifies the STUN server port. The default value is 3478 , with a supported range of 1024–65535 .
STUN Refresh Interval (s)	Specifies the STUN refresh interval in seconds. The default value is 60 , with a supported range of 10–160 .

Telephony – Basic Settings

FXS Settings

The **FXS Settings** page displays all FXS ports for the main router and sub-routers, along with their current configuration. From this page, users can view the assigned device node, enable or disable each FXS port, check the assigned template, and open the edit page for detailed port configuration.

FXS Settings

FXS Port	Device Node	Enable	User ID	Authenticate ID	Template	Operations
FXS1	GWN7062ET Primary EC:74:D7:...	☒	-	-	Template 1	Edit
FXS2	GWN7062ET Primary EC:74:D7:...	☒	-	-	Template 2	Edit

FXS Settings

Column	Description
FXS Port	Displays the available FXS port, such as FXS1 or FXS2 .
Device Node	Displays the router node associated with the FXS port.
Enable	Turns the selected FXS port on or off.
User ID	Displays the SIP user ID configured for the FXS port.
Authenticate ID	Displays the authentication ID configured for the FXS port.
Template	Displays the template assigned to the FXS port, such as Template 1 or Template 2 .
Operations	Provides the edit option for opening the detailed FXS configuration page.

FXS Settings

To edit an FXS port, click the **Edit** icon in the **Operations** column.

FXS Settings Edit FXS

FXS1

Not Registered

Primary node:GWN7062ET (EC:74:D7:)

Template

Template 1

Template 2

Account Settings

User ID

0~64 characters

Authenticate ID

0~64 characters

Password

0~64 characters

Display Name

0~64 characters

Cancel

Save

FXS Settings Edit FXS

The **Edit FXS** page displays the selected FXS port, its registration status, the associated primary node, the port enable switch, the assigned template, and the account settings used by the FXS port.

Field	Description
FXS Port Status	Displays the selected FXS port and its current registration status.
Primary Node	Displays the primary node associated with the selected FXS port.
Enable	Turns the selected FXS port on or off.
Template	Selects the template used by the FXS port. Available options are Template 1 and Template 2 .
User ID	Enter the SIP user or extension number used by the FXS port. Supports 0–64 characters .
Authenticate ID	Enter the SIP authentication ID used by the account. Supports 0–64 characters .
Password	Enter the SIP account password. Supports 0–64 characters .
Display Name	Enter the caller display name used by the FXS port. Supports 0–64 characters .

FXS Settings – Edit FXS

Template Settings

The **Template Settings** page allows users to configure two reusable telephony templates: **Template 1** and **Template 2**. Each FXS port can then be assigned to one of these templates from the **FXS Settings** edit page. This avoids repeating the same SIP, accessibility, and phone behavior settings for each port, because apparently even routers deserve reusable logic.

Each template includes three configuration tabs:

- SIP Settings
- Accessibility
- Phone Settings

SIP Settings

The **SIP Settings** tab is used to configure SIP registration, proxy servers, NAT traversal, transport protocol, SIP port behavior, RTP behavior, and SRTP.

Template Settings

Template 1Template 2

SIP SettingsAccessibilityPhone Settings

Registration & Proxy

SIP Registration Server

Secondary SIP Registration Server

Prioritize Primary SIP Server

Outbound Proxy Server

Secondary Outbound Proxy Server

NAT Traversal

NAT Traversal

Advanced Settings

Unregistered Dialing

SIP Transport Protocol

Random SIP Port

SIP Port

SIP OPTIONS

Random RTP Port

SRTP

Template Settings SIP Settings

Field	Description
Interface	Selects the WAN interface used for telephony-related operation. Available options are Auto , WAN1 , and WAN2 .
IP Address Direct Dialing	Enables direct dialing by IP address. Once enabled, users can place direct calls using IP addresses.
Allowed WAN-side Dial-in IP Addresses	Configures the WAN-side IP addresses allowed to initiate direct IP dialing. Select the address type, such as IP Address , IP Subnet , or IP Range , then enter the corresponding address information. Click Add to add another allowed WAN-side dial-in IP address entry, or click the minus icon to remove an entry.
Logout Scope	Defines how the extension registration is cleared from the server. • Single: unregisters only the selected extension registration • All: clears all registrations for the extension so the device can register again.
Allow DHCP Option 120 to Override Registration Address	When enabled, the registration address assigned by DHCP Option 120 is used.
STUN Server Address	Specifies the STUN server address used for NAT traversal.

STUN Server Port	Specifies the STUN server port. The default value is 3478 , with a supported range of 1024–65535 .
STUN Refresh Interval (s)	Specifies the STUN refresh interval in seconds. The default value is 60 , with a supported range of 10–160 .

Accessibility

2.

The **Accessibility** tab is used to configure call accessibility and supplementary service behavior, including anonymous call handling, call waiting, call hold, MWI, forwarding, DND, and emergency call options.

Template Settings Accessibility

Field	Description
Anonymous Call	Enables anonymous calling behavior.
Reject Anonymous Calls	Rejects calls from anonymous callers when enabled.
Call Waiting	Enables call waiting for the analog phone connected to the FXS port.
Call Hold	Enables call hold.
Message Waiting Indication (MWI)	Enables message waiting indication.
MWI Type	Selects the MWI type. Available options shown are FSK and NEON .
Subscribe for MWI	Enables subscription for message waiting indication.
Unconditional Forwarding	Enables unconditional call forwarding.
Unconditional Forwarding Feature Code	Defines the feature code used for unconditional forwarding. The value shown is *72 .
Busy Forwarding	Enables call forwarding when the line is busy.
Busy Forwarding Feature Code	Defines the feature code used for busy forwarding. The value shown is *90 .
No Answer Forwarding	Enables call forwarding when the call is not answered.
No Answer Forwarding Feature Code	Defines the feature code used for no-answer forwarding. The value shown is *92 .
Do Not Disturb (DND) Mode	Enables Do Not Disturb mode.
Emergency Call	Enables emergency call behavior.

The following service codes are supported for SRTP, Call Waiting, DND, and forwarding behavior:

Function	Feature Code	Remark
Enable SRTP	*16	The code is not displayed on the web page, but remains valid.
Disable SRTP	*17	The code is not displayed on the web page, but remains valid.
Enable Call Waiting	*51	The code is not displayed on the web page, but remains valid.
Disable Call Waiting	*50	The code is not displayed on the web page, but remains valid.
Enable Do Not Disturb (DND) Mode	*78	The code is not displayed on the web page, but remains valid.
Disable Do Not Disturb (DND) Mode	*79	The code is not displayed on the web page, but remains valid.
Set unconditional forwarding number	*72	The code is displayed on the web page and takes effect only when Unconditional Forwarding is enabled.
Cancel unconditional forwarding	*73	The code is not displayed on the web page and takes effect only when Unconditional Forwarding is enabled.
Set busy forwarding number	*90	The code is displayed on the web page and takes effect only when Busy Forwarding is enabled.
Cancel busy forwarding	*91	The code is not displayed on the web page and takes effect only when Busy Forwarding is enabled.
Set no-answer forwarding number	*92	The code is displayed on the web page and takes effect only when No Answer Forwarding is enabled.
Cancel no-answer forwarding	*93	The code is not displayed on the web page and takes effect only when No Answer Forwarding is enabled.

Phone Settings

3.

The **Phone Settings** tab is used to configure audio gain, line interface behavior, jitter buffer behavior, buffer length, and DTMF method for analog phones connected to the FXS ports.

Template Settings

Template 1Template 2

SIP SettingsAccessibilityPhone Settings

Volume Settings

RX Gain (dB)TX Gain (dB)

Voice Encoding Settings

SLIC SettingsUSA 1 (Bell Standard 600ohms)

Jitter BufferFixedAdaptiveNetEQ

Buffer LengthHighMediumLow

DTMF MethodAuto

Template Settings Phone Settings

Field	Description
RX Gain (dB)	Adjusts the receive audio gain.
TX Gain (dB)	Adjusts the transmit audio gain.
SLIC Settings	Selects the subscriber line interface circuit setting. The visible selected option is USA 1 (Bell Standard 600ohms) .
Jitter Buffer	Selects the jitter buffer mode. Available options shown are Fixed , Adaptive , and NetEQ .
Buffer Length	Selects the buffer length. Available options are High , Medium , and Low .
DTMF Method	Selects the DTMF method. The visible selected option is Auto .

Template Settings – Phone Settings

Ringtone

The **Ringtone** page is used to configure tone region behavior and prompt language for analog phones connected to the FXS ports. Users can either use automatic region-based tones or define custom tone values manually.

Ringtone

Tone RegionAuto-configure by RegionCustom

Prompt LanguageEnglish

Ringtone Auto configure by Region

Field	Description
Tone Region	Select Auto-configure by Region to use region-based tone settings automatically.

Ringtone – Auto-configure by Region

When **Custom** is selected, the page displays editable tone fields for dial tone, ringback tone, busy tone, and call waiting tone.

Ringtone

Tone Region

☐ Auto-configure by Region
 ☒ **Custom**

* Dial Tone ⓘ

f1=350@-6,f2=440@-6,c=0/0;

* Ringback Tone ⓘ

f1=440@-6,f2=480@-6,c=2000/4000;

* Busy Tone ⓘ

f1=480@-6,f2=620@-6,c=500/500;

* Call Waiting Tone ⓘ

f1=440@-6,c=300/2000-300/2000-0/0;

Prompt Language

English

Ringtone Custom

Field	Description
Tone Region	Select Custom to manually configure tone values.
Dial Tone	Defines the custom dial tone. The visible value is f1=350@-6,f2=440@-6,c=0/0;
Ringback Tone	Defines the custom ringback tone. The visible value is f1=440@-6,f2=480@-6,c=2000/4000;
Busy Tone	Defines the custom busy tone. The visible value is f1=480@-6,f2=620@-6,c=500/500;
Call Waiting Tone	Defines the custom call waiting tone. The visible value is f1=440@-6,c=300/2000-300/2000-0/0;

Ringtone – Custom

The **Prompt Language** option defines the language used for voice prompts played through analog phones connected to the FXS ports. Select the preferred language for the voice prompts from the drop-down list.

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**.

The **Wi-Fi** page lists all configured Wi-Fi networks, including the **default SSID(s)**. For each SSID, the **Enable** column provides a switch that can be used to quickly turn that Wi-Fi network **on or off**. When a Wi-Fi network is disabled, its SSID is no longer broadcast and connected wireless clients are disconnected from that network.

Wi-Fi

admin

Add

Wi-Fi Name	Enable	Band	Security Mode	WPA Mode	WPA Encryption Type	Captive Portal	Clients Count	Total Traffic	TX/RX Traffic	Operations
GWN7062ET		2.4G	Personal	WPA2	AES	Disable	0	0B		

Wi Fi page

Adding a New Wi-Fi Network:

Click **Add** to create a new Wi-Fi network, or click **Edit** to modify an existing Wi-Fi network.

Wi-Fi > Edit Wi-Fi

Basic Settings

Wi-Fi ☒

Wi-Fi Name GWN7062ET

Band ☒ 2.4G&5G ☐ 2.4G ☐ 5G

Security Mode ☐ Open ☒ Personal ☐ Enterprise

WPA Mode WPA2

WPA Encryption Type AES

Password ••••••••

Strong

Advanced Settings

Hide Wi-Fi ☐

Captive Portal Disable

Disable Wi-Fi Regularly

Professional Settings ☐ General ☒ Custom

When 'Custom' is selected, custom rules must be reset.
[\[Settings\]](#)

Add Wi Fi

Field	Description
Wi-Fi	Enables or disables the Wi-Fi network.
Wi-Fi Name	Enter the Wi-Fi network name, also known as the SSID.
Band	Select the wireless band used by the SSID. Available options shown are 2.4G&5G , 2.4G , and 5G .
Security Mode	Select the security mode used by the Wi-Fi network. Available options shown are Open , Personal , and Enterprise .
WPA Mode	Select the WPA mode used by the Wi-Fi network. The visible selected value is WPA2 .
WPA Encryption Type	Select the WPA encryption type used by the Wi-Fi network. The visible selected value is AES .
Password	Enter the Wi-Fi password. This field is required when the selected security mode requires authentication.
Hide Wi-Fi	Prevents the SSID from being broadcast when enabled.
Captive Portal	Selects the captive portal policy applied to the Wi-Fi network.
Disable Wi-Fi Regularly	Enables scheduled Wi-Fi disabling based on the configured time range and frequency.
Professional Settings	Select General to use the router's default Wi-Fi behavior, or select Custom to apply the advanced profile configured under Advanced → Wi-Fi Settings → General Settings → Professional Settings . When Custom is selected, custom rules must be reset.

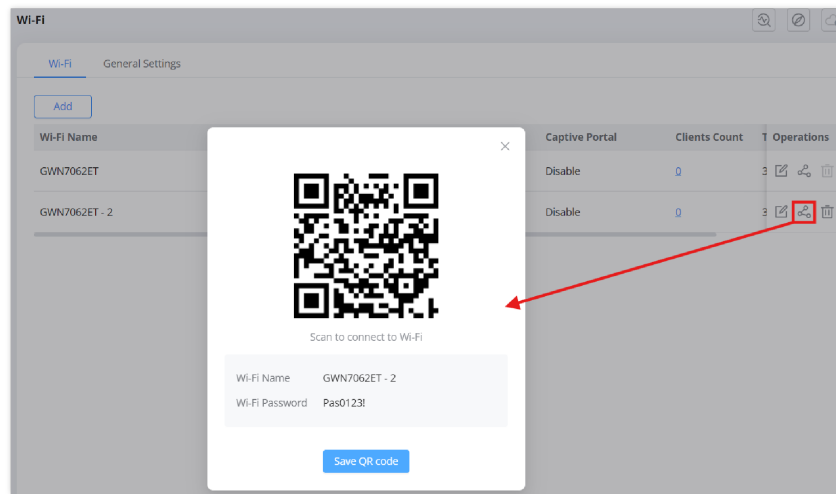
Add Wi-Fi

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**.

- o **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.

Guest Wi-Fi

The **Guest Wi-Fi** feature allows administrators to configure an isolated wireless SSID for visitors. This network operates separately from the main SSIDs, enhancing security by keeping guest traffic segmented from the LAN and internal devices.

To access the configuration page, navigate to: **Advanced** → **Wi-Fi Settings** → **Guest Wi-Fi**

Guest Wi-Fi

Guest Wi-Fi ☒

* Wi-Fi Name

GWN_6343F0_Guest

Band

☒ 2.4G&5G
 ☐ 2.4G
 ☐ 5G

Security Mode

☐ Open
 ☒ Personal
 ☐ Enterprise

WPA Mode

WPA2

WPA Encryption Type

AES

* Password

.....

Strong

Advanced Settings

Captive Portal

Disable

Professional Settings

☐ General
 ☒ Custom

When 'Custom' is selected, custom rules must be reset.

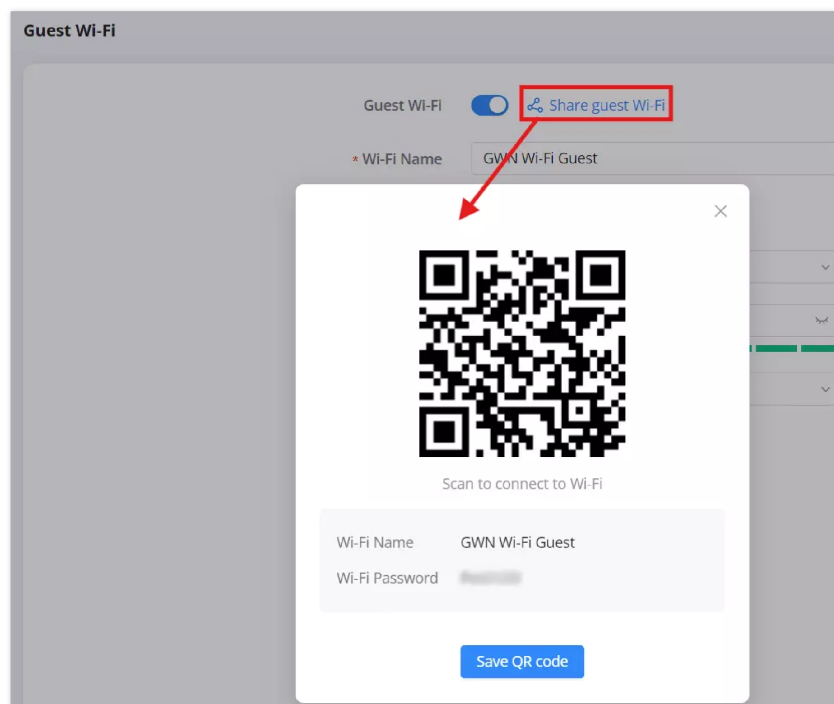
[Settings](#)

Guest Wi Fi page

The following settings are available:

Field	Description
Guest Wi-Fi	Enables or disables the guest Wi-Fi network.
Wi-Fi Name	Enter the broadcast name for the guest network.
Band	Select the wireless band used by the guest SSID. Available options shown are 2.4G&5G , 2.4G , and 5G .
Security Mode	Select the security mode used by the guest Wi-Fi network. Available options shown are Open , Personal , and Enterprise .
WPA Mode	Select the WPA mode used by the guest Wi-Fi network. The displayed example uses WPA2 .
WPA Encryption Type	Select the WPA encryption type used by the guest Wi-Fi network. The displayed example uses AES .
Password	Set the password used to connect to the guest Wi-Fi network. This field is required when the selected security mode requires authentication.
Captive Portal	Select the captive portal policy applied to the guest Wi-Fi network.
Professional Settings	Select General to use the router's default Wi-Fi behavior for the guest network, or select Custom to apply the advanced profile configured under Advanced → Wi-Fi Settings → General Settings → Professional Settings . When Custom is selected, custom rules must be reset.

Additionally, Guest Wi-Fi can be shared using a QR code. The QR code contains the SSID and password, allowing users to connect to the guest network without entering the information manually.



Share Guest Wi Fi password

Wi-Fi General Settings

The **General Settings** page provides advanced controls for optimizing overall Wi-Fi performance. From this page, administrators can configure **Wi-Fi5 compatibility**, **channel width**, **channel selection**, **radio power**, and **dynamic optimization** for both the **2.4GHz** and **5GHz** bands, ensuring a stable and interference-free wireless environment.

Navigating to General Setting

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

General Settings

Common Settings Professional Settings

Wi-Fi5 Compatible ☐

Turning this off will optimize Wi-Fi speed, but some devices may not be able to connect.

Configuration Item	2.4G	5G
Channel Width	20MHz	80MHz
Channel Switch	Auto	Auto
Channel	1 x + 12 ...	36 x + 15 ...
Radio Power	High	High

Dynamic Optimization ☒

Cancel Save

Channel Quality One-Click Optimization

Channel (2.4G)

9 12 4 11 6 7 10

Channel (5G)

104 116 120 124 128 60 108

Wi Fi General Common Settings

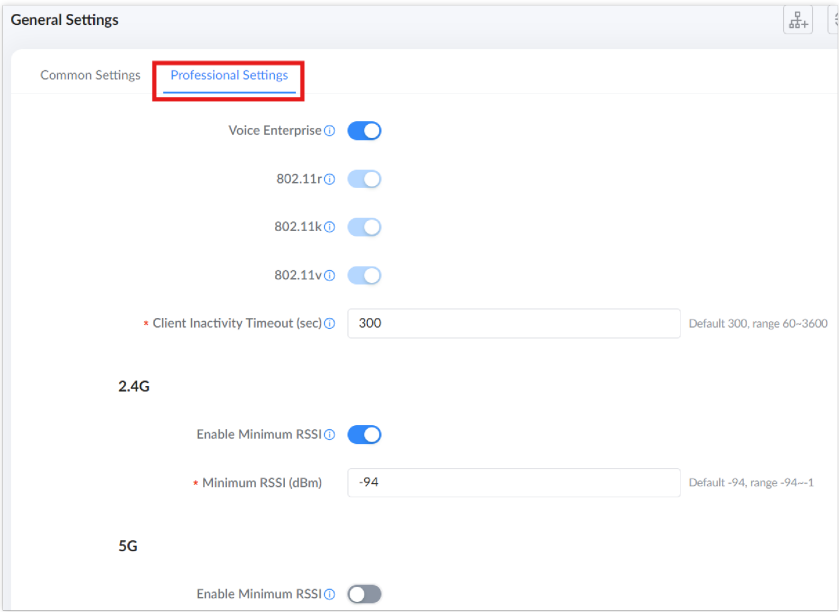
Available Configuration Options:

- **Wi-Fi5 Compatible**
 - Enables compatibility with Wi-Fi 5 (802.11ac).
 - When disabled, Wi-Fi rates are optimized for performance, but some older devices may not be able to connect.
- **Channel Width**
 - Adjusts the channel width for both 2.4GHz and 5GHz bands.
 - Common options include:
 - 2.4GHz: 20MHz (recommended for stability).
 - 5GHz: 40MHz or 80MHz (wider channels enable higher throughput, but may be more sensitive to interference).
- **Channel Switch**
 - Controls how the router handles channel switching (for example, automatic switching based on the environment or fixed behavior depending on the available mode).
- **Channel**
 - Set to Auto to let the router dynamically choose the best channel based on the environment.
 - Or manually assign a channel to reduce interference or align with a specific deployment plan.
- **Radio Power**
 - Sets the transmission power level for each band (for example High, Medium, or Low).
 - Useful for managing coverage range and minimizing interference in multi-device or multi-AP environments.
- **Dynamic Optimization**
 - When enabled, automatically optimizes Wi-Fi channels based on interference and congestion levels.
 - The router can adjust parameters to maintain better performance as conditions change.
- **One-Click Optimization**
 - Manually triggers Wi-Fi optimization by scanning the environment and applying the best available wireless settings.
 - Helpful after changing physical layout, adding new APs, or noticing interference.
- **Channel Quality Monitoring**
 - Displays the current channel quality for both 2.4GHz and 5GHz.
 - Helps administrators identify noisy or congested channels and adjust Channel, Channel Width, or Radio Power accordingly.

Professional Settings

The **Professional Settings** tab under **Advanced** → **Wi-Fi Settings** → **General Settings** → **Professional Settings** defines advanced Wi-Fi behavior applied to SSIDs where **Professional Settings** is set to **Custom** on the Wi-Fi or Guest Wi-Fi pages.

Voice Enterprise, **802.11r**, **802.11k**, **802.11v**, and **Client Inactivity Timeout** apply to both **2.4G** and **5G** bands. Separate **Minimum RSSI** controls are available for each band.



Wi Fi General Professional Settings

Refer to the table below for more details about each field:

Field	Description
Voice Enterprise	Optimizes Wi-Fi parameters for latency-sensitive voice traffic, improving call quality and roaming for VoIP devices.
802.11r	Enables Fast BSS Transition to reduce handoff time when clients roam between access points using the same SSID.
802.11k	Enables neighbor reports so clients can discover and select better access points when roaming.
802.11v	Enables BSS transition management to help steer clients toward more suitable access points or bands, improving load balancing and roaming stability.
Client Inactivity Timeout (sec)	Specifies how long an idle client can remain associated before being disconnected. The default value is 300, with a supported range of 60–3600 seconds.
2.4G – Enable Minimum RSSI	Enables minimum RSSI control for clients connected on the 2.4G band.
2.4G – Minimum RSSI (dBm)	Enables minimum RSSI control for clients connected on the 2.4G band.
5G – Enable Minimum RSSI	Enables minimum RSSI control for clients connected on the 5G band.
5G – Minimum RSSI (dBm)	Sets the minimum allowed RSSI value for the 2.4G band. The default value is -94, with a supported range of -94~1.

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.

Mesh Capacity and Topology Rules:

The router supports adding up to 16 total Mesh nodes to a single network. To ensure network stability and prevent bottlenecks, the following connection limits apply:

- **Wired Parent Requirement:** Any router acting as a parent node must use a physical Ethernet connection.
- **Wireless Sub-Node Limit:** A single wired parent node can support a maximum of **3 wireless sub-nodes**.
- **Expanding the Network:** To build a larger mesh (up to the 16-node limit), you must deploy multiple wired parent nodes on the same network (e.g., 4 wired parents each supporting 3 wireless sub-nodes) or hardwire your nodes directly.

With Mesh Networking, users can:

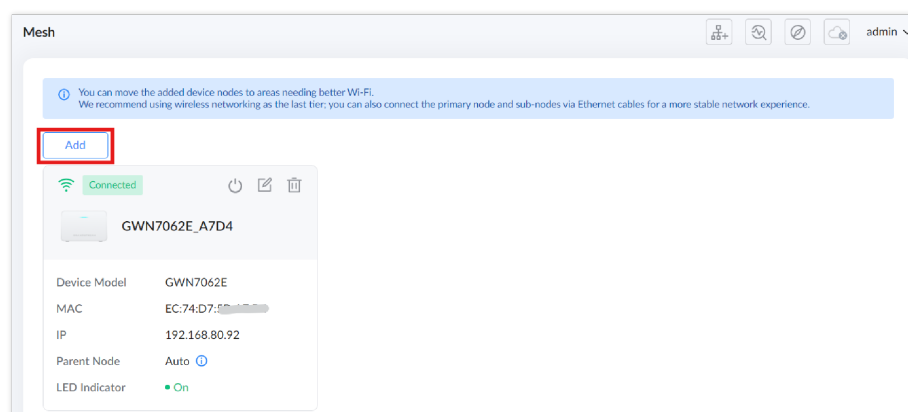
- Extend Wi-Fi coverage seamlessly by adding more routers.
- Optimize signal strength and network stability using intelligent routing.
- Avoid the need for additional Ethernet cables.
- Ensure a self-healing network where traffic automatically reroutes in case of link failure.

1. Accessing the Mesh Networking Feature

Navigate to **Advanced** → **Mesh** to access the Mesh configuration page.

2. Adding a New Router to the Mesh Network

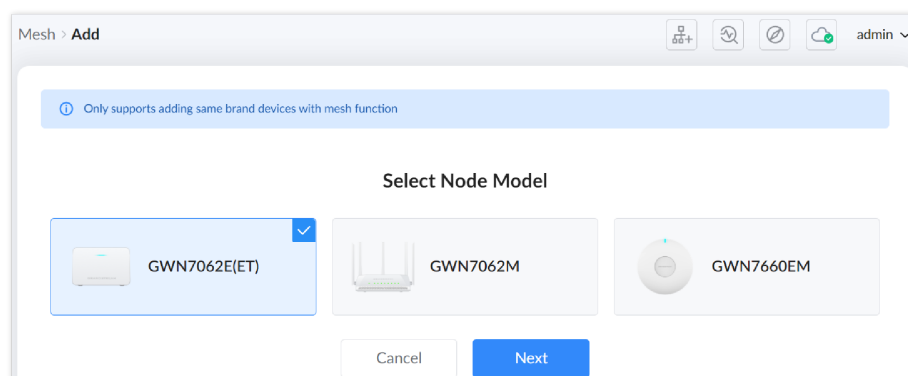
- Click on the **"Add"** button to begin the process of adding a new node router to the mesh.
- A prompt will appear detailing the **preparations required** before adding the new router.



Mesh Add sub router

Select the model of the Mesh node to be added. The system supports adding same-brand devices with Mesh functionality, including **GWN7062E(T)**, **GWN7062M**, and **GWN7660EM**.

Click Next to continue with the Mesh node pairing process.

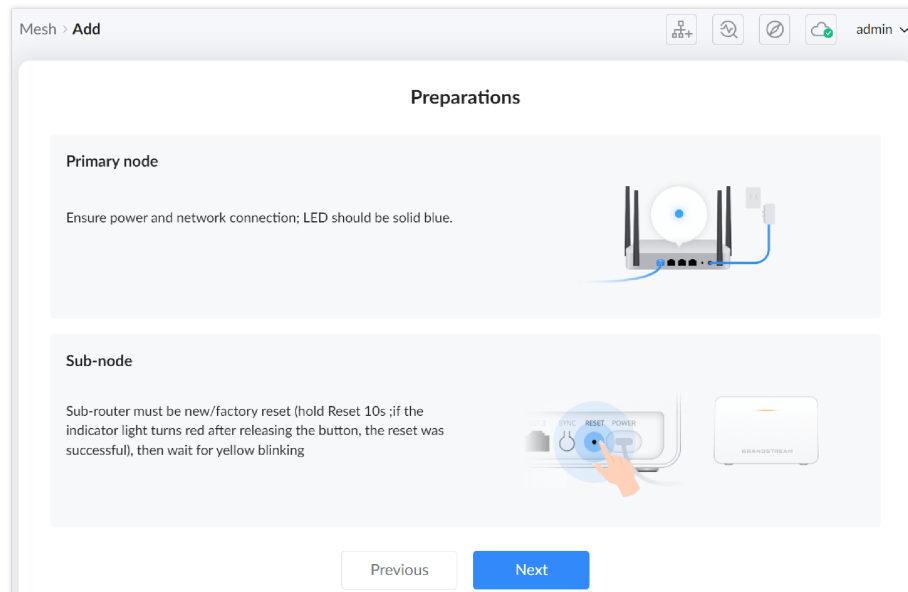


Mesh Select the model

3. Preparing the Router for Mesh Connection

Before beginning Mesh pairing, follow these steps:

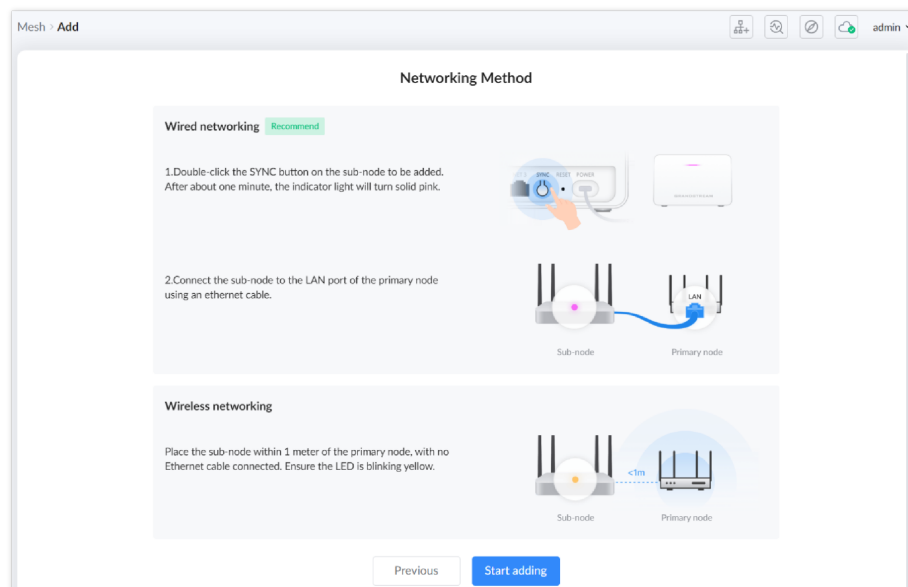
- The **main router** must have a **WAN or uplink cable** connected and must be **provisioned** (initial setup wizard completed). Its LED should be **solid blue**.
- The **sub-router** must be **factory reset**. Once reset, its LED should blink **yellow**.



Preparing the Router for Mesh Connection

- While blinking yellow, **double-press the SYNC button** on the sub-router. After about 1 minute, the LED should turn **solid pink**, which means the device is in Mesh pairing mode.
- You can now proceed using **wired (recommended)** or **wireless (1-meter range)** pairing.

Once ready, click **“Start adding”** to detect and add the sub-router.

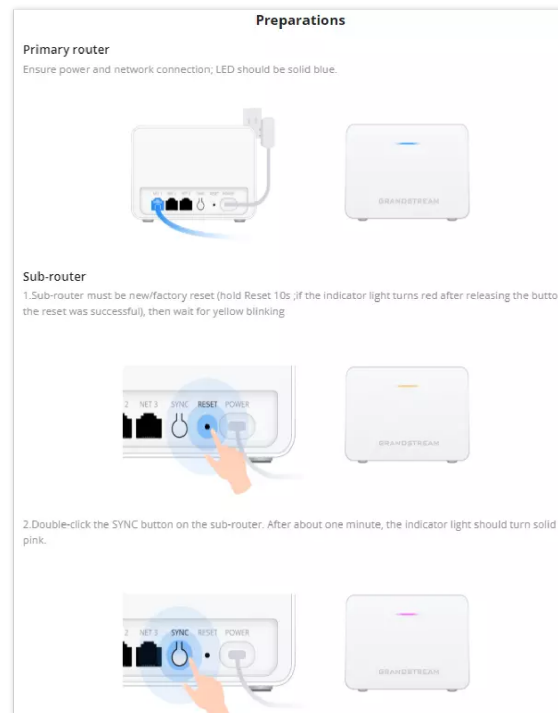


Preparing the Router for Mesh Connection

Clicking the **“View Help”** link will show the following requirements:

- **Main Router:**
 - Must be connected via WAN/uplink cable.
 - Must be provisioned (initial setup completed).
 - LED should be **solid blue**.
- **Node:**
 1. Must be either brand new or manually reset (hold RESET 10 sec → wait for **blinking yellow**).
 2. While blinking yellow, **double-click the SYNC button** only in wireless networking case.
 3. After ~1 minute, LED turns **solid pink**, indicating it's ready for Mesh pairing.

You can now start Mesh pairing using either a **wired** or **wireless** connection. If wireless, ensure both devices are **within 1 meter**.



Preparing the Router for Mesh Connection View Help

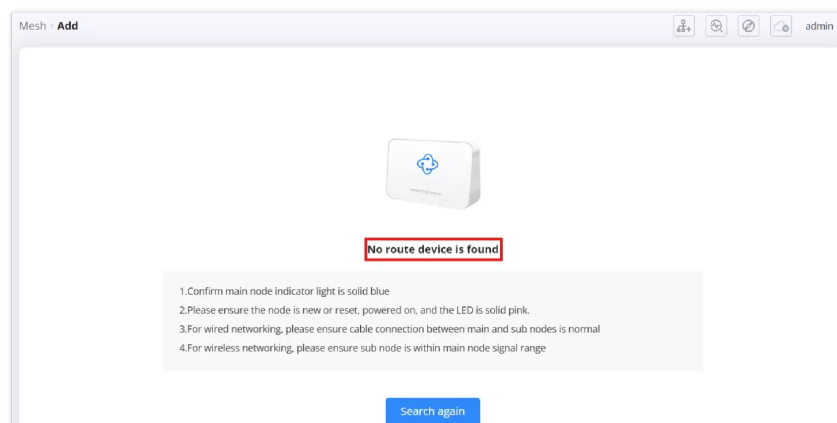
4. Searching for Available Node Routers

Once you click **Start Adding**, the main router will scan for sub-routers (node routers) ready to be paired. If **no devices are found**, ensure the following:

- The **main router** is provisioned, and its LED is **solid blue**.
- The **sub-router** has been **factory reset**, is **powered on**, and its LED is **solid pink** (Mesh pairing mode).
- If using **wired mode**, verify the Ethernet cable is securely connected between the LAN port of the sub-router and the main router.
- If using **wireless mode**, make sure the sub-router is placed **within 1 meter** of the main router.
- If needed, click **"Search again"** to retry the detection process.

Note:

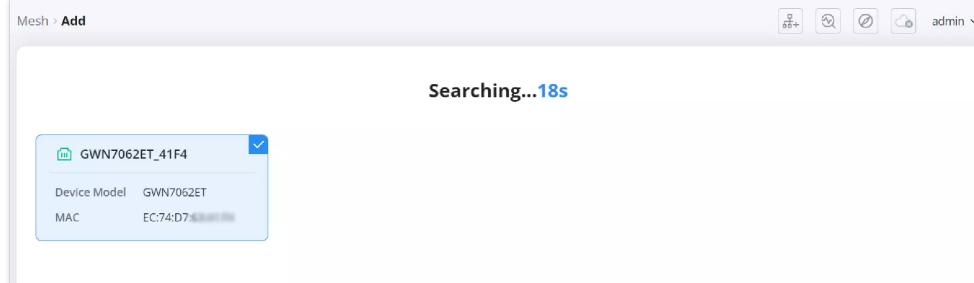
If the issue persists, repeat the reset and SYNC steps for the sub-router and ensure it's running the latest firmware that supports Mesh.



Mesh no router is found

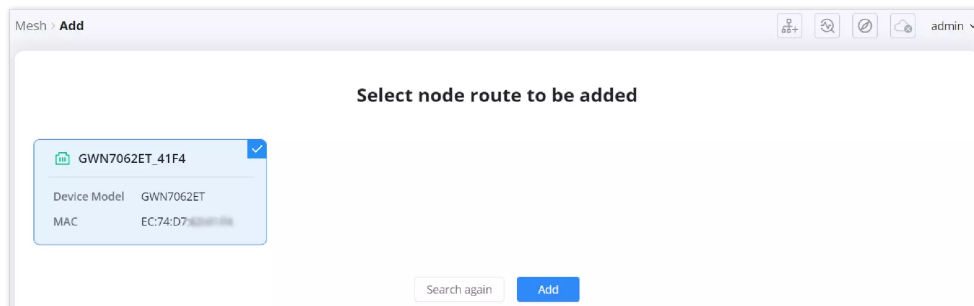
5. Selecting the Router to Add

When scanning begins, the main router searches for available node routers. If successful, the sub-router will appear in the list along with its model name and MAC address.



Mesh sub router is found

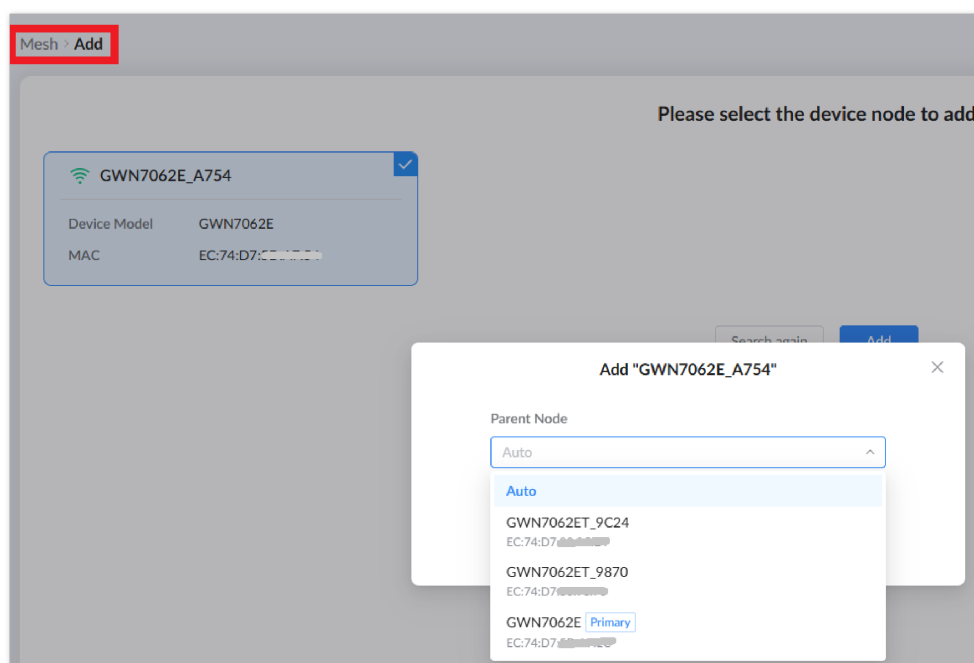
Once the sub-router is visible, select it by checking the box next to it, then click **“Add”** to begin the pairing process.



Mesh sub router is found add device

Once the **sub-router** (node router) is in Mesh pairing mode and detected by the main router, it will appear in the list. Follow the steps below to complete the pairing:

First select the parent node. (only if using wireless networking method)



Mesh sub router is found

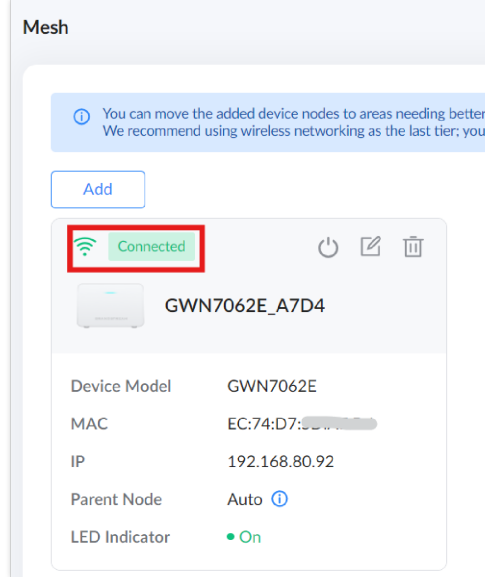
Note

To complete the pairing based on connection type:

- If using a wired connection, no further action is needed. The pairing will complete automatically.
- If using a wireless connection, press and hold the SYNC button on the sub-router for 3 seconds to finalize the pairing.

6. Confirmation of Successful Connection

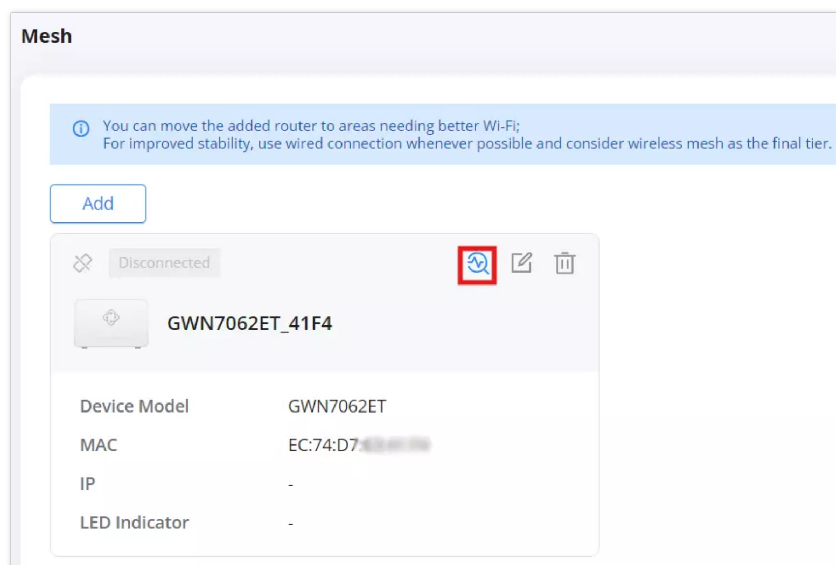
After a successful connection, the device status changes to **Connected**, showing IP, MAC address, model, and LED status. You can now reposition the sub-router for better Wi-Fi coverage as needed.



Mesh sub router is found device connected

7. 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.

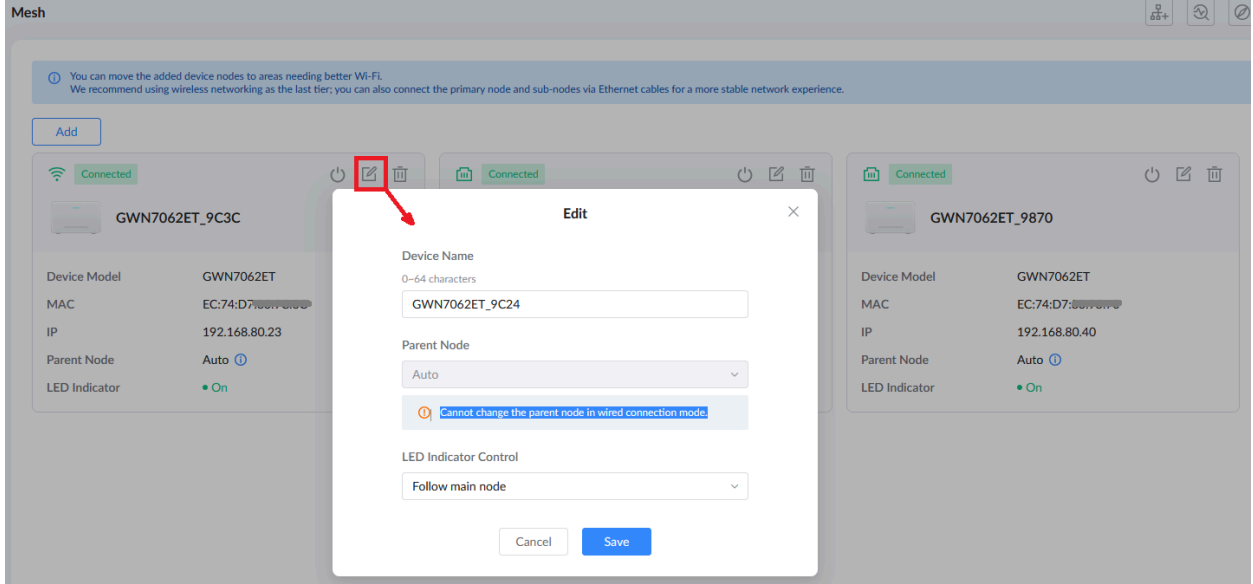


Mesh Diagnosing Connection Issues

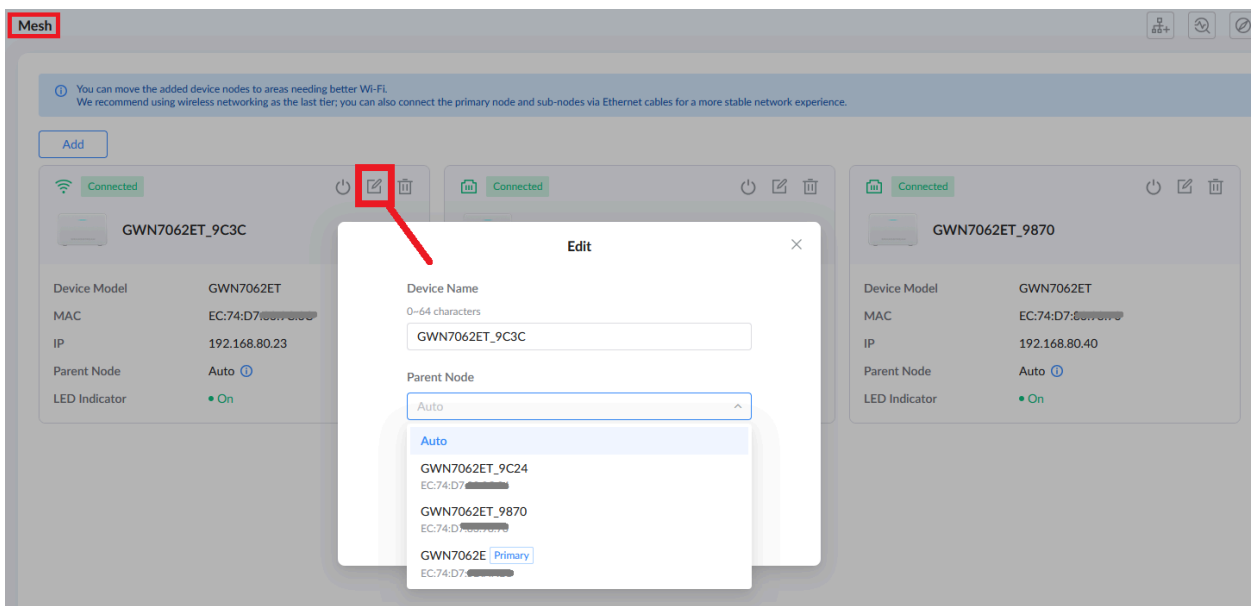
Editing a Mesh Node

The **Edit** window allows configuring the node display name, parent node, and LED indicator control. Parent node selection is available only when the connection mode supports it:

- For **wireless connections**, the parent node can be selected manually.
- For **wired connections**, the parent node is automatically set to **Auto** and cannot be changed. A warning message is displayed if attempted.



Edit Mesh Node Wired Connection Mode



Edit Mesh Node Parent Node Selection

Edit

Device Name
0~64 characters
GWN7062E_A7D4

Parent Node
Auto
ⓘ Cannot change the parent node in wired connection mode.

LED Indicator Control
Follow main node

Cancel Save

Parent Node Locked in Wired Connection Mode

Refer to the table below for details about each field in the Edit window:

Field	Description
Device Name	Configures the display name of the mesh node. Supports 0–64 characters.
Parent Node	Selects the upstream parent node used by the mesh node. Auto allows the system to select the parent automatically. This field is available only when manual parent selection is supported. In wired connection mode, the parent node is locked to Auto and cannot be changed.
LED Indicator Control	Configures how the LED behaves for the selected mesh node.
Wired Connection Mode Warning	Indicates that the parent node cannot be changed while the node is connected in wired connection mode.

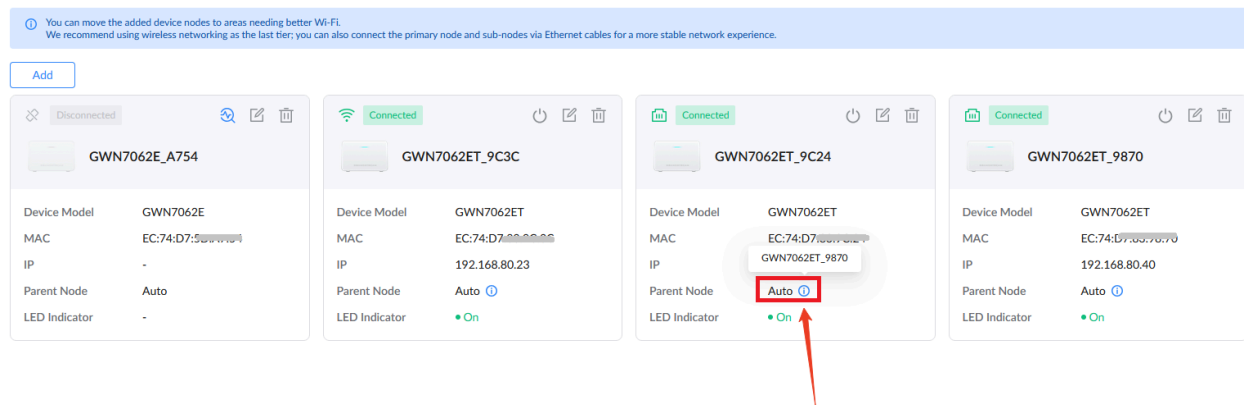
Editing a Mesh Node

Parent Node Behavior: The **Parent Node** field may be automatically assigned or locked depending on how the mesh node is added, connected, or supported by its model and firmware version.

- **Sub-node paired via SYNC button:** The parent node is set to **Auto** by default. If the node uses wireless networking, the parent node can be modified later from the web UI.
- **Auto selected when adding a wireless sub-node:** The router automatically selects the parent node. The parent node can be modified later if wireless networking still supports manual parent selection.
- **Current parent node deleted:** The sub-node switches back to **Auto**. If it uses wireless networking, the parent node can be modified later from the web UI.
- **Wired sub-node:** The parent node is set to **Auto** and cannot be changed.
- **Wireless sub-node changed to wired connection:** The parent node switches to **Auto** and cannot be changed.
- **GWN7062M with firmware 1.0.1.x or earlier:** The parent node is set to **Auto** and cannot be changed.
- **GWN7062E/ET with firmware 1.0.3.x or earlier:** The parent node is set to **Auto** and cannot be changed.
- **GW7660EM sub-node:** The parent node is set to **Auto** and cannot be changed.

Parent Node

The **Parent Node** field shows the upstream node used by each mesh node. When **Auto** is selected, the router automatically selects the parent node based on the mesh connection. Users can also select a specific available node when manual parent selection is supported.



Mesh Node List – Parent Node

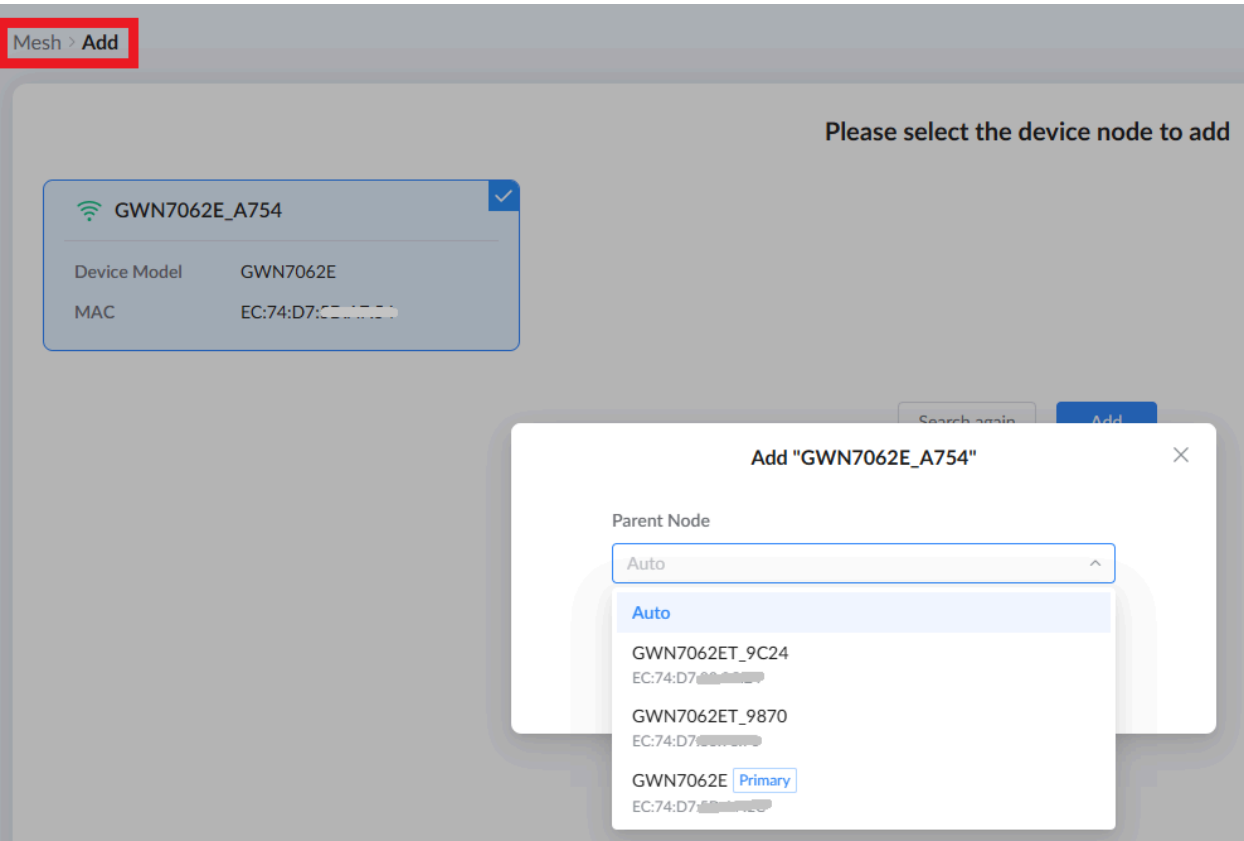
Each mesh node card displays the current **Parent Node** value. Hovering over the information icon can show the selected or detected parent node details.

Refer to the table below for more details about the Parent Node field on the Mesh page.

Field	Description
Parent Node	Displays the upstream parent node used by the mesh node. Auto allows the router to select the parent node automatically.

Adding a Mesh Node with a Parent Node

When adding a mesh node, the **Parent Node** field allows users to keep the selection on **Auto** or choose one of the available nodes from the list.



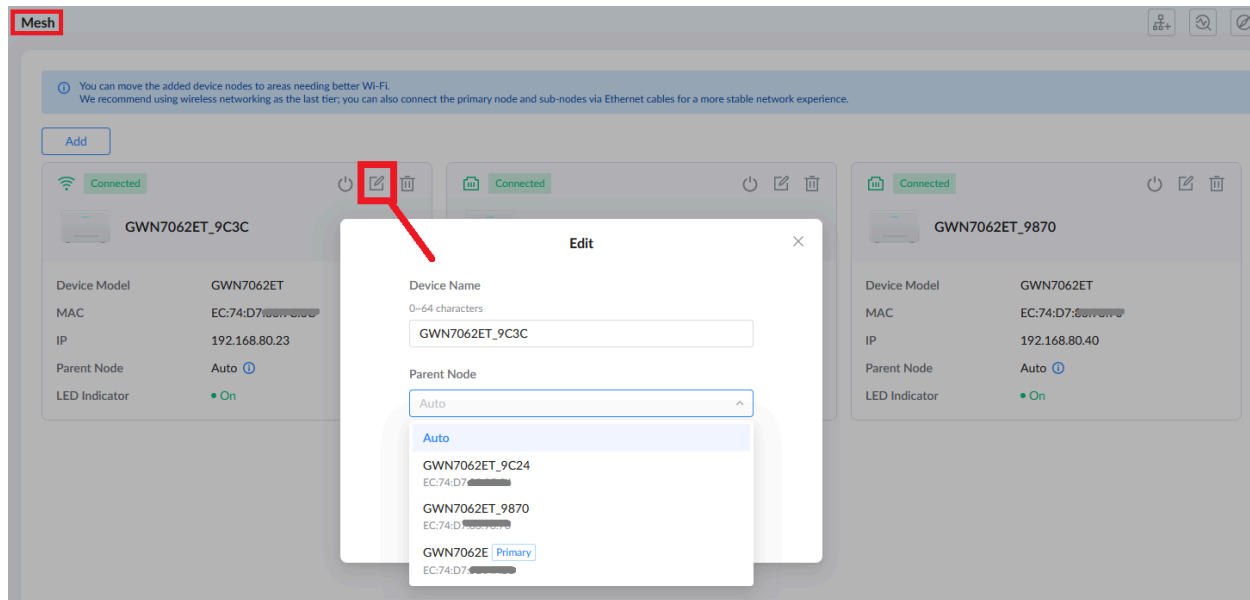
Add Mesh Node – Parent Node Selection

Refer to the table below for more details about the available Parent Node selection.

Field	Description
Auto	Allows the router to select the parent node automatically.
Available Mesh Nodes	Lists available mesh nodes that can be selected as the parent node.
Primary Node	Indicates the primary router when it is available as a parent node option.

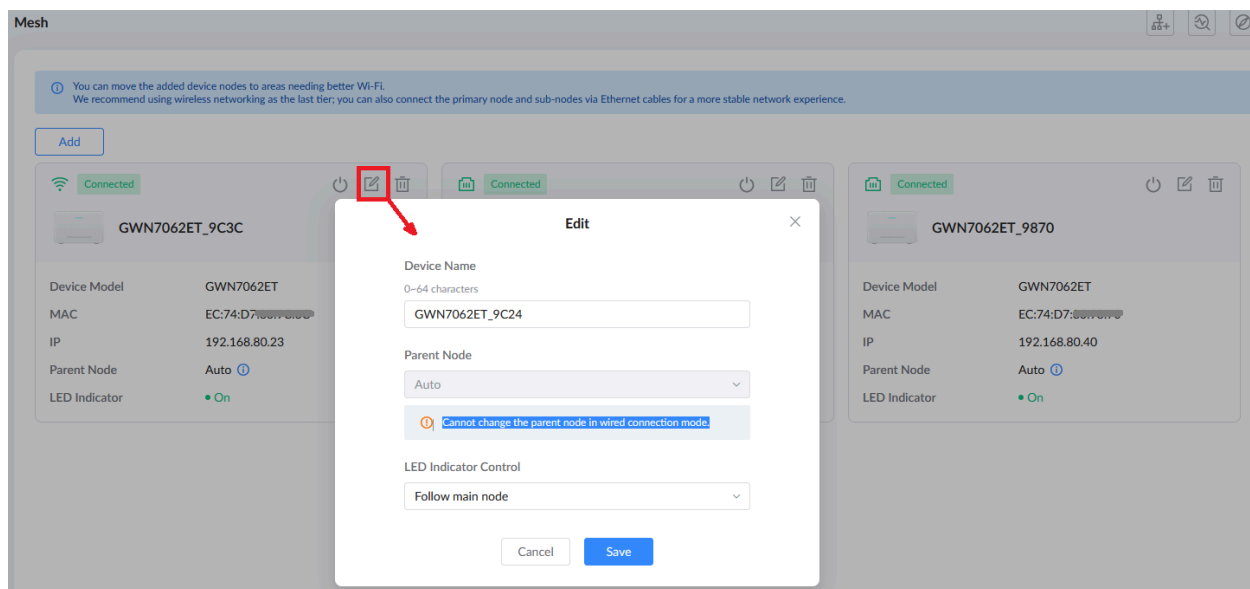
Editing the Parent Node

When editing a mesh node, the **Parent Node** field can be used to adjust the node parent when the connection mode allows manual parent selection.



Edit Mesh Node – Parent Node Selection

When the node is connected in wired connection mode, the **Parent Node** field is locked and the page displays a message indicating that the parent node cannot be changed in wired connection mode.



Edit Mesh Node – Parent Node Locked in Wired Connection Mode

Refer to the table below for more details about the Edit window fields.

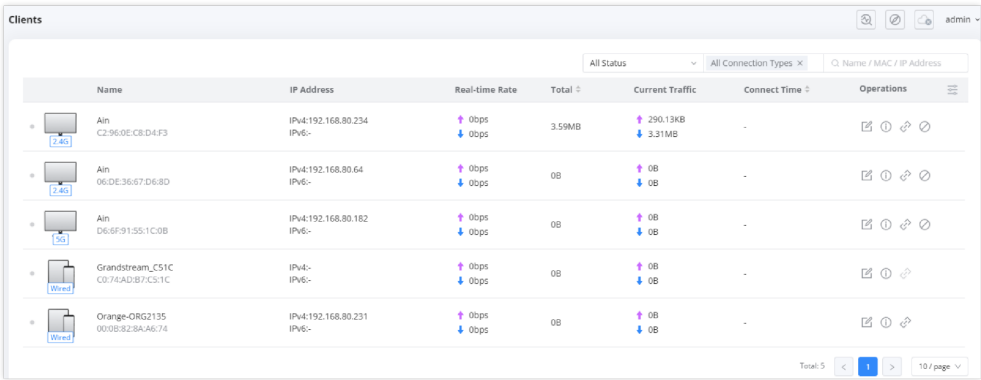
Field	Description
Device Name	Configures the display name of the mesh node. The field supports 0–64 characters.
Parent Node	Selects the upstream parent node for the mesh node. The field is locked when the node is connected in wired connection mode.
LED Indicator Control	Configures the LED indicator behavior for the selected mesh node.
Wired Connection Mode Warning	Indicates that the parent node cannot be changed while the mesh node is using wired connection mode.

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



The screenshot shows the 'Clients' page interface. At the top, there are filters for 'All Status', 'All Connection Types', and a search bar for 'Name / MAC / IP Address'. The main table has columns: Name, IP Address, Real-time Rate, Total, Current Traffic, Connect Time, and Operations. It lists five devices: three wireless (Ain) and two wired (Grandstream and Orange-ORG). Each device row shows its name, MAC address, IP address, real-time data rate (up/down arrows and 0bps), total data usage, current traffic (up/down arrows and 0B/250.13KB/3.31MB), and a set of operation icons (edit, info, refresh, delete).

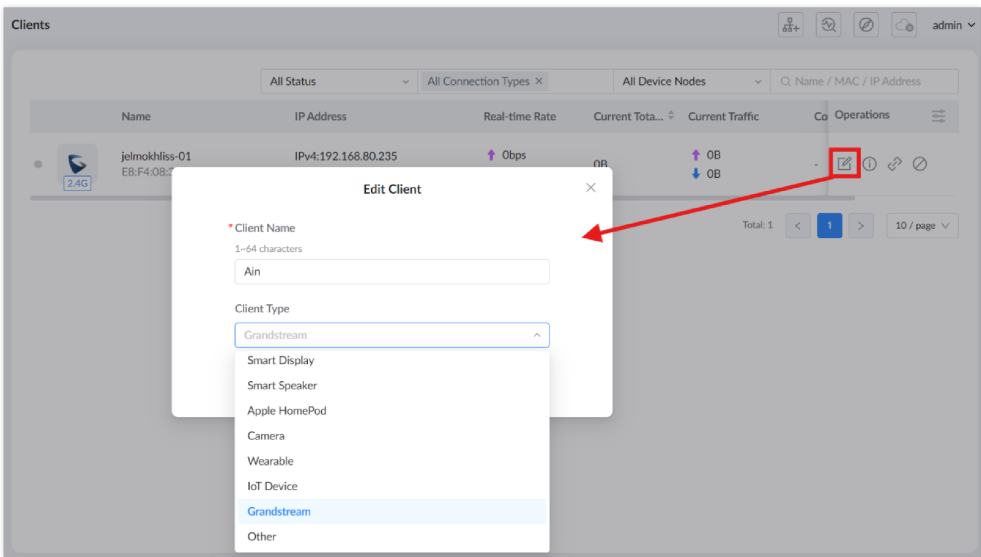
Name	IP Address	Real-time Rate	Total	Current Traffic	Connect Time	Operations
Ain C2:96:0E:CE:D4:F3	IPv4:192.168.80.234 IPv6:-	↑ 0bps ↓ 0bps	3.59MB	↑ 250.13KB ↓ 3.31MB	-	[Edit] [Info] [Refresh] [Delete]
Ain 06:DE:36:67:D6:8D	IPv4:192.168.80.64 IPv6:-	↑ 0bps ↓ 0bps	0B	↑ 0B ↓ 0B	-	[Edit] [Info] [Refresh] [Delete]
Ain D6:6F:91:55:1C:0B	IPv4:192.168.80.182 IPv6:-	↑ 0bps ↓ 0bps	0B	↑ 0B ↓ 0B	-	[Edit] [Info] [Refresh] [Delete]
Grandstream_CS1C C0:74:AD:B7:C5:1C	IPv4:- IPv6:-	↑ 0bps ↓ 0bps	0B	↑ 0B ↓ 0B	-	[Edit] [Info] [Refresh] [Delete]
Orange-ORG2135 00:0B:82:2A:A6:74	IPv4:192.168.80.231 IPv6:-	↑ 0bps ↓ 0bps	0B	↑ 0B ↓ 0B	-	[Edit] [Info] [Refresh] [Delete]

Clients page

Modifying a Client Name and Client Type

The client edit window allows users to update the client display name and assign a device type for easier identification in the client list.

Refer to the table below for more details about each field in the edit window.



The screenshot shows the 'Edit Client' dialog box overlaid on the Clients page. The dialog has two main fields: 'Client Name' with a text input containing 'Ain' and a character count '1-64 characters'; and 'Client Type' with a dropdown menu. The dropdown is open, showing options: Smart Display, Smart Speaker, Apple HomePod, Camera, Wearable, IoT Device, Grandstream (highlighted), and Other. A red arrow points from the 'Edit' icon in the table to the dialog box.

Clients edit name

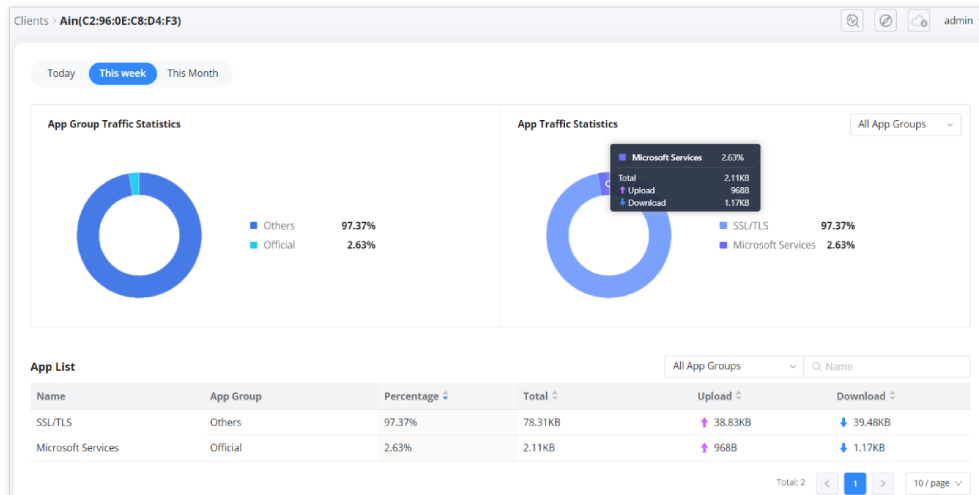
Field	Description
Client Name	Specifies the display name of the client. The name can contain 1–64 characters.

Field	Description
Client Type	Assigns a device category to the client, such as Smart Display, Smart Speaker, Apple HomePod, Camera, Wearable, IoT Device, Grandstream, or Other.

Modifying a Client Name and Client Type

Viewing Client Traffic Details

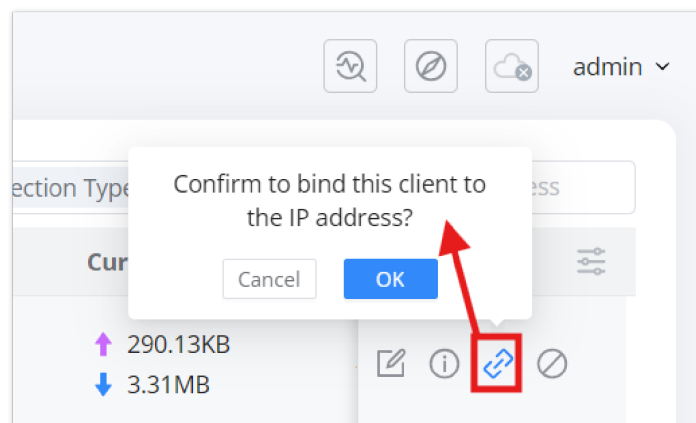
1. Click on the **Exclamation mark icon** next to a client entry.
2. This opens a **Client Traffic Overview** page with:
 - **Traffic statistics by app group**
 - **Data usage trends over time** (Today, This Week, or This Month)
 - **Breakdown of applications consuming network resources**



Clients View details

Binding a Static IP to a Client

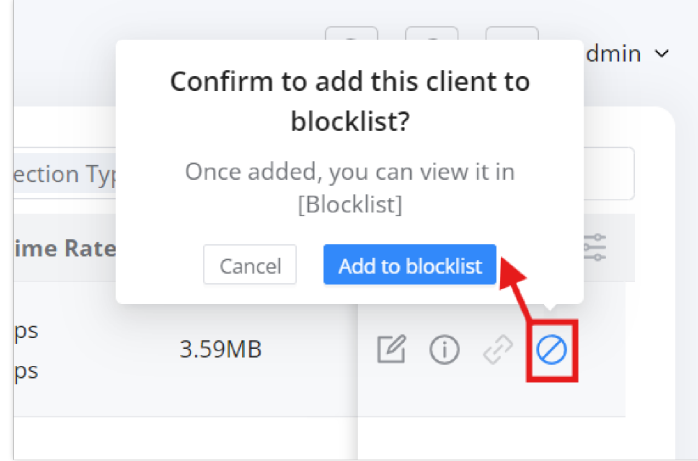
1. Click on the **Link (chain) icon** next to the client.
2. A confirmation prompt will appear: "Confirm to bind this client to the IP address?"
3. Click **OK** to assign a static IP to the client.



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 blacklist?"
3. Click **Add to blacklist** 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.

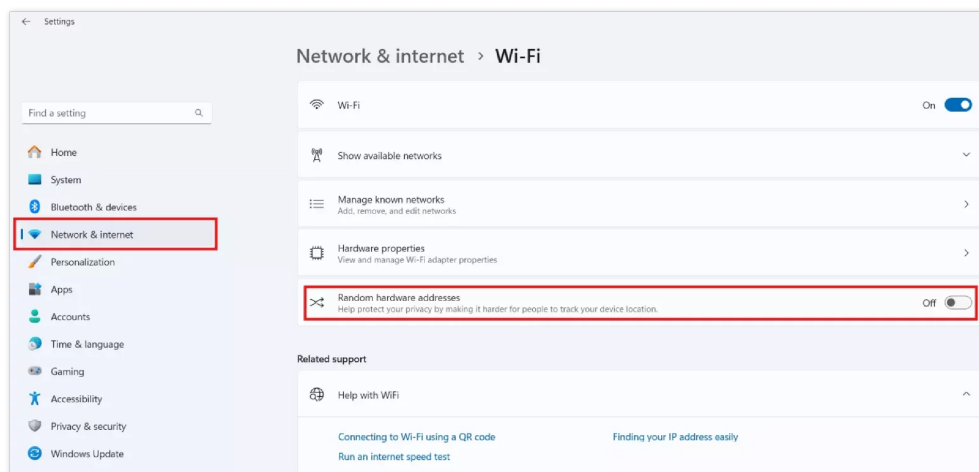
To ensure proper operation, users should **disable random MAC addresses** for their specific Wi-Fi network. Below is a general method to do so, followed by examples for **Windows®, iOS®, and Android®**.

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.

o 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**.



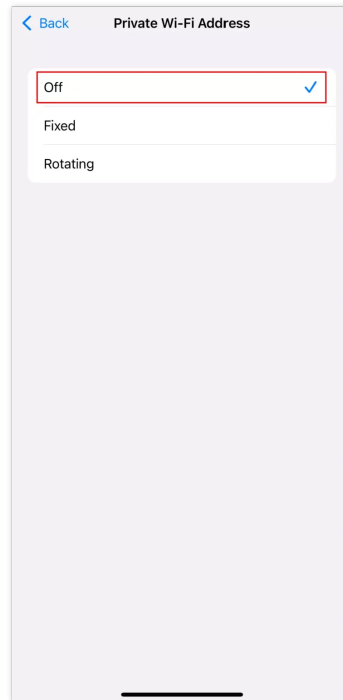
Disable Random MAC Address Windows® Example Windows® 1011

o 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**.

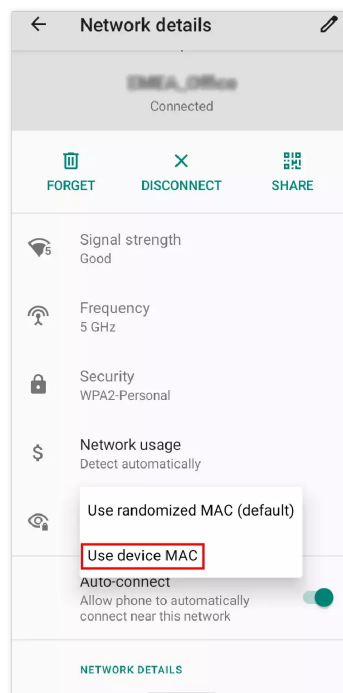


*Disable Random MAC Address iOS®
Example iOS® 14 and later*

◦ **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**.

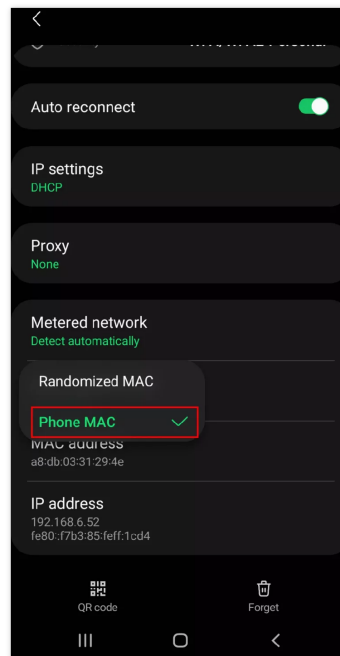


*Disable Random MAC Address Stock
Android*

Samsung® Devices:

1. **Go to** **Settings** > **Connections** > **Wi-Fi**.
2. Tap on your **connected network**.
3. Scroll to **MAC Address Type**.

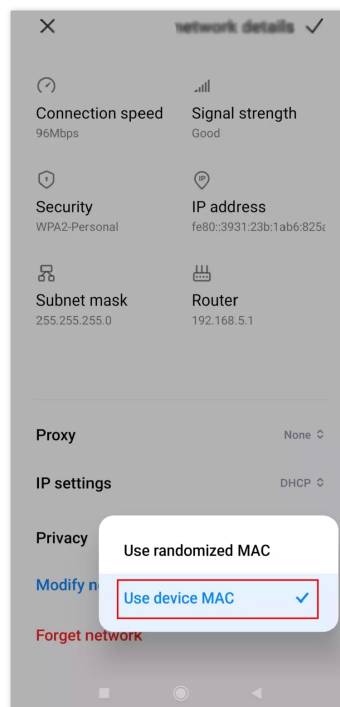
4. Select **Phone MAC** instead of **Randomized MAC**.



*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**.

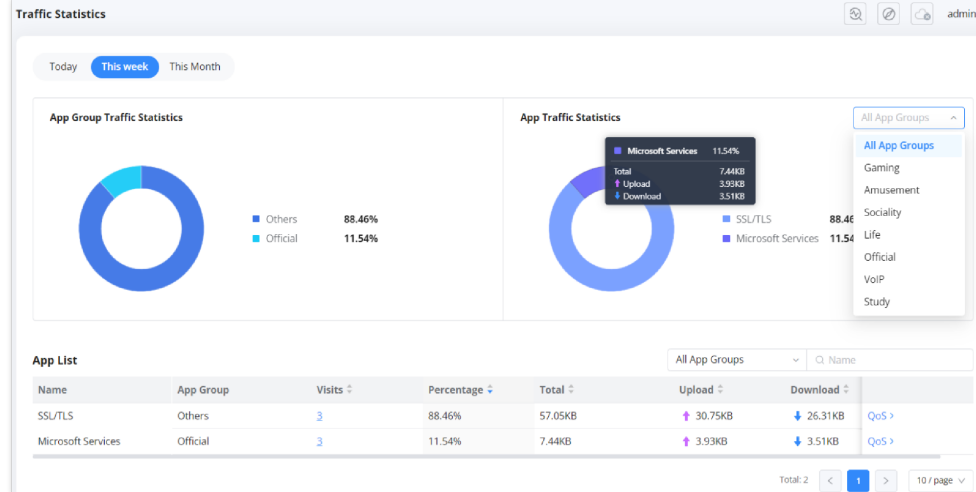


*Disable Random MAC Address Xiaomi
Devices*

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 allows users to optimize and control network traffic based on priority settings. It can allocate bandwidth to specific applications, clients, or traffic types, helping improve performance for critical services such as gaming, VoIP, and streaming.

Navigate to **Advanced** → **Traffic Management** → **QoS** to access the QoS settings.

The QoS page includes three tabs: **Basic Settings**, **APP QoS**, and **QoS Rules**. The **Basic Settings** tab is used to enable QoS, configure WAN bandwidth limits, and define bandwidth allocation for each priority level.

Basic Settings

In the **QoS function** section, enable QoS globally to activate traffic prioritization.

In the **WAN Bandwidth Settings** section, configure the upload and download bandwidth for each WAN interface. Each WAN interface also has its own **Enable** switch, allowing QoS bandwidth control to be enabled or disabled separately for **WAN1** and **WAN2**.

Important Note: Obtain bandwidth information from the ISP and configure the bandwidth values slightly below the peak bandwidth. If the bandwidth settings are not configured properly, QoS may not function as expected.

WAN	Enable	Maximum Upload Bandwidth	Maximum Download Bandwidth
WAN1	☒	200 Mbps	200 Mbps
WAN2	☒	100 Mbps	100 Mbps

Priority	Rewrite DSCP	Minimum Bandwidth	Maximum Bandwidth
0	56	40%	100%
1	48	20%	100%
2	40	15%	100%
3	32	8%	100%
4	24	7%	100%
5	16	5%	100%
6	8	3%	100%
7	0	2%	100%

QoS Basic Settings

Refer to the table below for more details about each field in the **Basic Settings** tab.

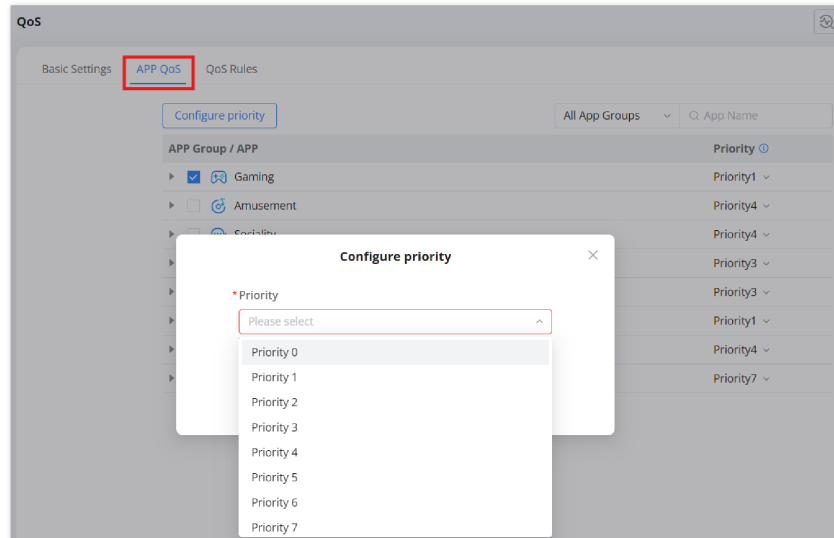
Field	Description
QoS Function – Enable	Enables or disables QoS globally.
WAN – Enable	Enables or disables QoS bandwidth control for the selected WAN interface.
Maximum Upload Bandwidth	Specifies the maximum upload bandwidth available on the selected WAN interface.
Maximum Download Bandwidth	Specifies the maximum download bandwidth available on the selected WAN interface.
Priority	Displays the QoS priority level. Priority 0 has the highest priority, while Priority 7 has the lowest priority.
Rewrite DSCP	Displays the DSCP value mapped to the corresponding priority level.
Minimum Bandwidth	Specifies the minimum bandwidth percentage reserved for traffic assigned to the priority level.
Maximum Bandwidth	Specifies the maximum bandwidth percentage allowed for traffic assigned to the priority level.

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.

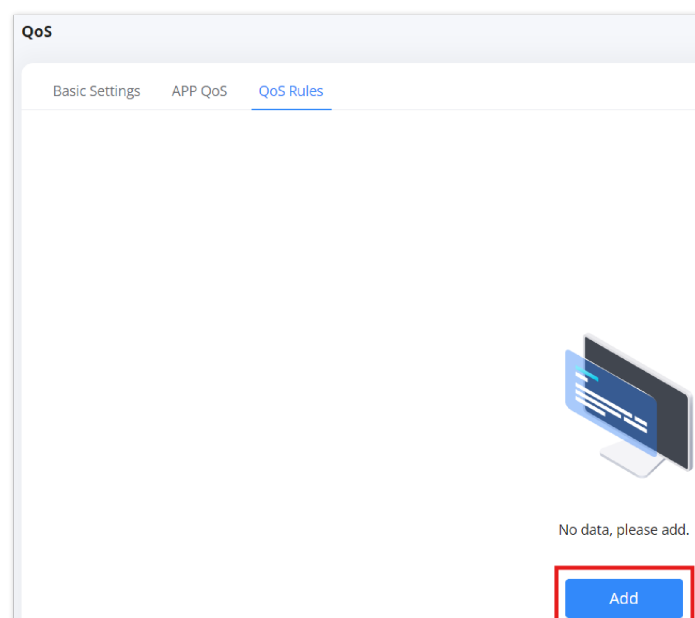
- The available priority levels range from **Priority 0 (highest) to Priority 7 (lowest)**.
- Users can classify traffic based on categories such as:
 - **Gaming**
 - **VoIP**
 - **Social Media**
 - **Streaming**
 - **Work & Study**
- Selecting a higher priority ensures better bandwidth allocation for 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

* Name: Higher Priority Clients (1-64 characters)

Enable: ☒

* Source: ☐ All clients ☒ Specified clients ☐ IP Address

* Client: Ain(C2:96:0E:C8:D4:F3) ×

* Destination: ☐ All traffic ☒ Apps ☐ Domain

* Apps: Gaming ×

* Priority ⓘ: Priority 5

Rewrite DSCP: 6

Cancel Save

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).

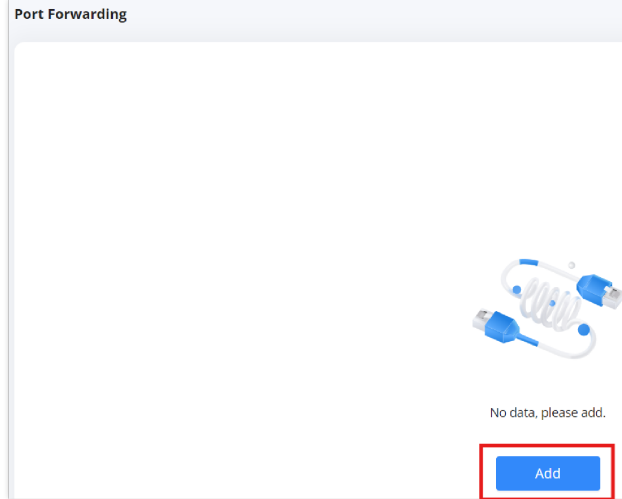
Accessing the Port Forwarding Page:

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:

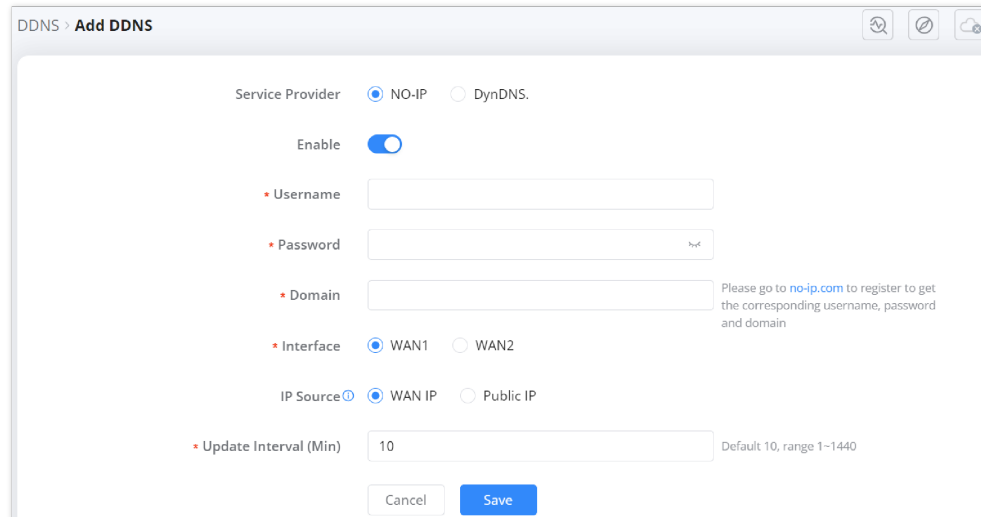
- **External Port Note:** This port is open to the internet, allowing external users to send requests.
- **Internal Port Note:** This is the destination port inside the local network. If a port range is specified, the difference between the starting and ending ports must remain consistent.

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.



The screenshot shows the 'Add DDNS' configuration window in a router's web interface. The window has a title bar with 'DDNS > Add DDNS' and three icons on the right. The configuration options are as follows:

- Service Provider:** Radio buttons for 'NO-IP' (selected) and 'DynDNS'.
- Enable:** A toggle switch that is turned on.
- Username:** A text input field with a red asterisk indicating it is required.
- Password:** A text input field with a red asterisk and a 'show/hide' icon on the right.
- Domain:** A text input field with a red asterisk. To its right, a note says: 'Please go to no-ip.com to register to get the corresponding username, password and domain'.
- Interface:** Radio buttons for 'WAN1' (selected) and 'WAN2'.
- IP Source:** Radio buttons for 'WAN IP' (selected) and 'Public IP'.
- Update Interval (Min):** A text input field containing '10'. To its right, a note says: 'Default 10, range 1~1440'.

At the bottom of the window are two buttons: 'Cancel' and 'Save'.

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:

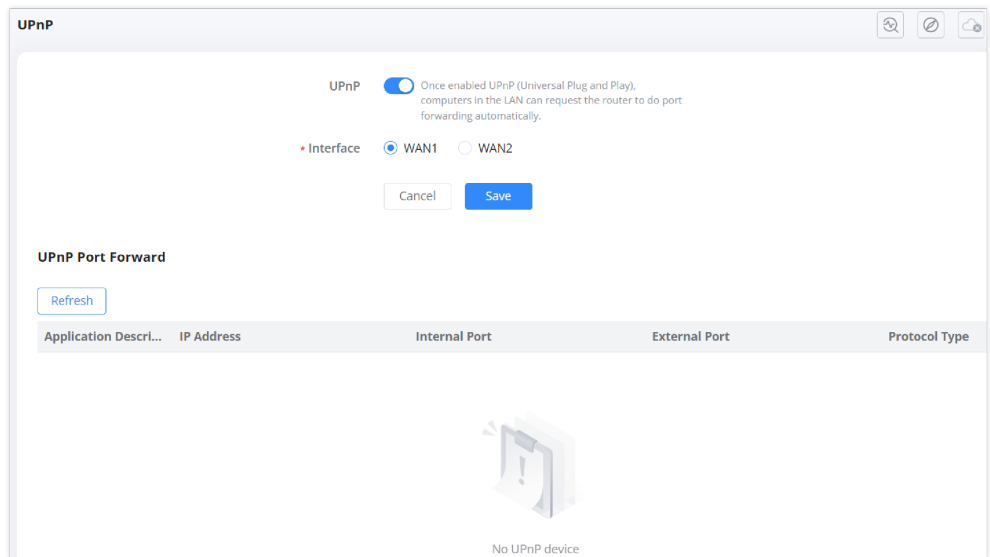
- Set the frequency for updating the DDNS record.
- Default: **10 minutes** (Range: **1 – 1440 minutes**).

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:

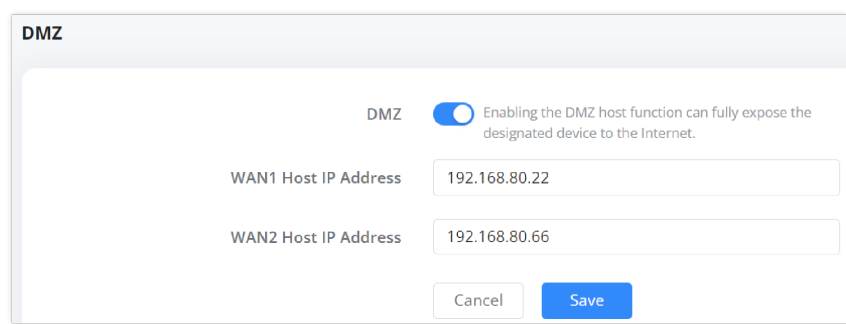
- While UPnP simplifies port forwarding, it may pose security risks if enabled without proper monitoring.
- It is recommended to **disable UPnP** if not actively used to prevent unauthorized applications from opening ports.
- Users can manually configure port forwarding for more control over network 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 a DMZ only when necessary** and for trusted devices.
- For enhanced security, consider **using Port Forwarding** instead of a 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**.

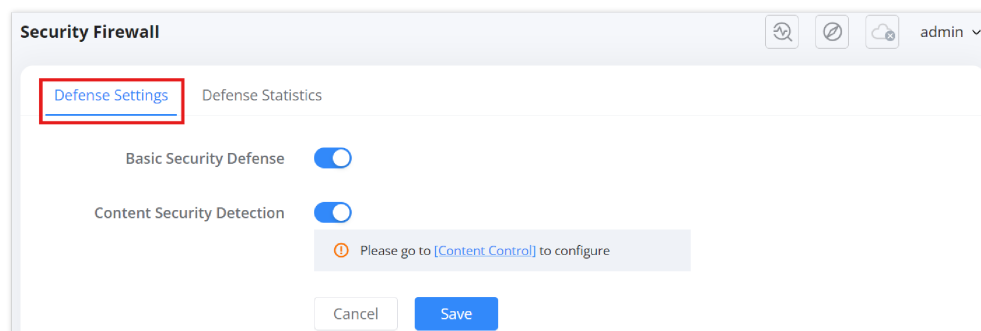
Defense Settings:

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:

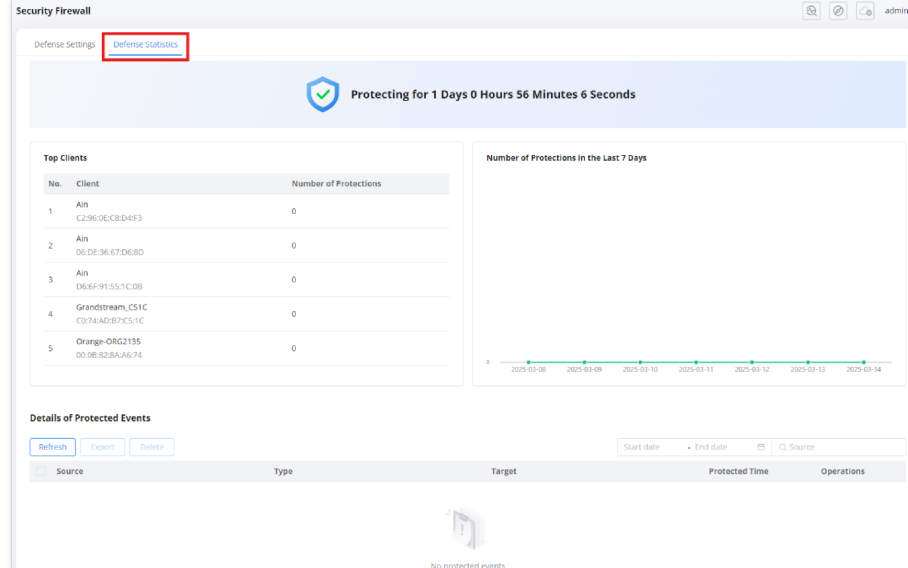
If Content Security Detection is enabled, users must configure content control settings separately by navigating to Security > Content Control.



Security Firewall Defense Settings

Defense Statistics

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



Security Firewall Defense Statistics

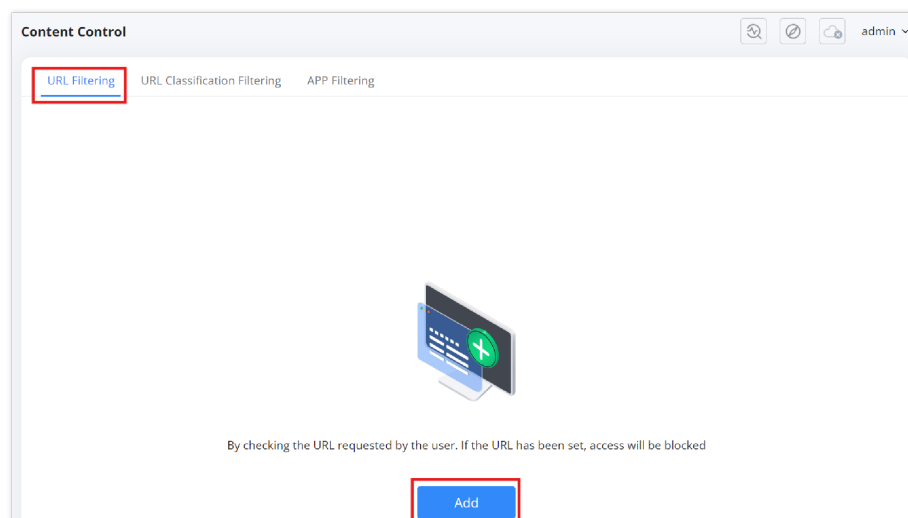
Key Metrics in Defense Statistics:

- **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 > Edit URL Filtering

Name: streaming (1-64 characters)

URL: www.youtube.com (1-256 characters, support numbers, letters and special characters)

www.netflix.com

Add

Cancel Save

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 Filtering | **URL Classification Filtering** | APP Filtering

Number of Classifications: 19 | Number of URLs: 219117

Allow Block

Classification Name	Number of URLs	Action
☐ Adult	93540	Block
☐ Mixed adult	150	Block
☐ Lingerie	132	Block
☐ Sexual education	12	Block
☐ Aggressive	144	Block
☐ Ddos	421	Allow
☐ Hacking	271	Allow
☒ Phishing	99790	Allow
☐ Drogue	602	Allow
☐ Gambling	5656	Allow
☐ Dangerous material	31	Allow
☐ Bitcoin	330	Allow
☐ Cryptojacking	16280	Allow
☐ Stalkerware	30	Allow
☐ Remote control	64	Allow

Content Control URL Classification Filtering

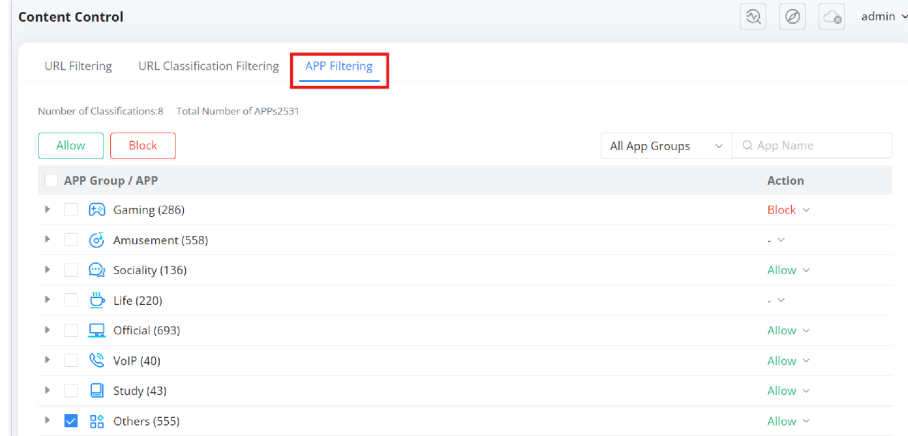
App Filtering

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.

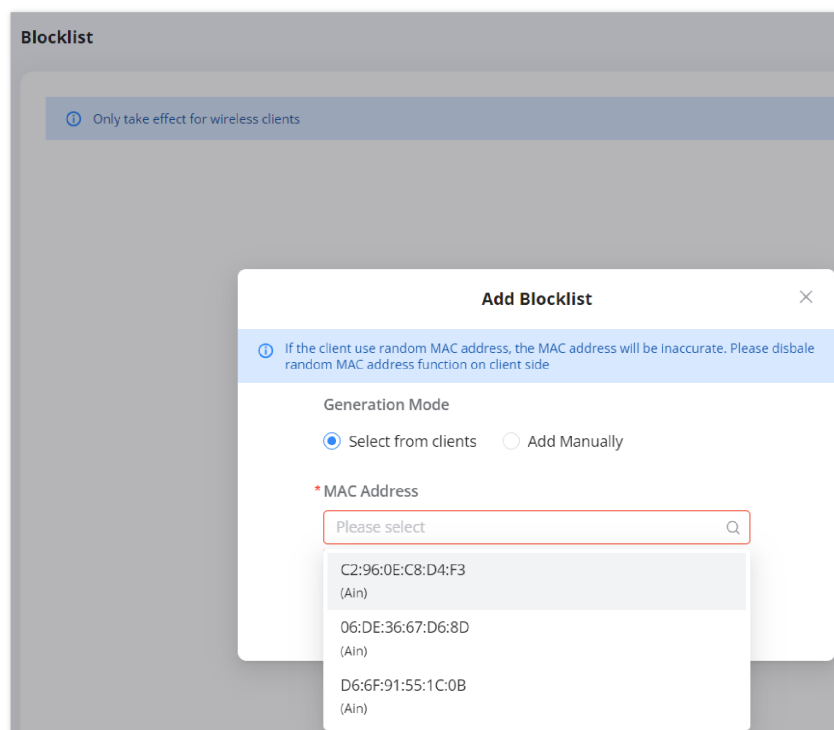


Content Control App Filtering

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:

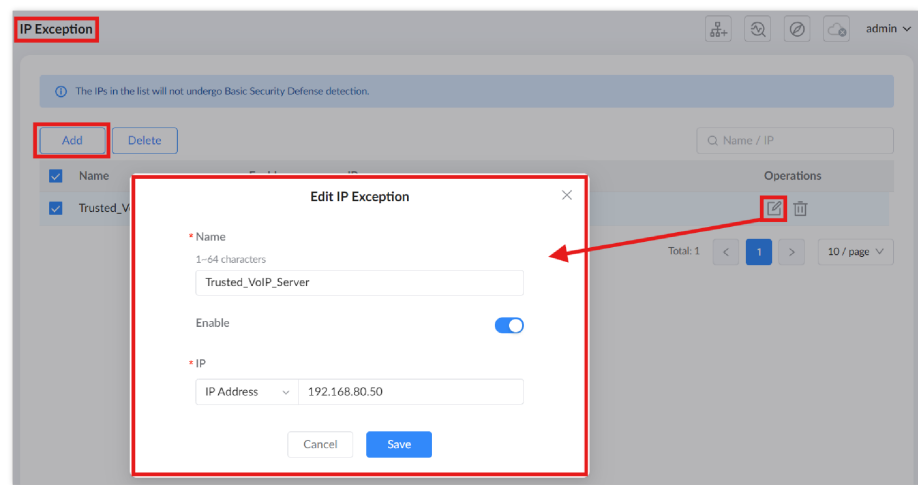
This feature requires devices to have a static MAC address to function properly. If your device is using a random MAC address, certain functions may not work as expected. To ensure compatibility, follow the steps in [Disabling Client Random MAC Address](#) to disable the random MAC feature on your device.

IP Exception

The **IP Exception** page allows users to define trusted IP entries that are excluded from **Basic Security Defense** detection. Entries in this list are not inspected by the Basic Security Defense feature.

Navigate to **Advanced** → **Security** → **IP Exception**.

To add an IP exception, click **Add** and configure the exception entry.



IP Exception

Refer to the table below for more details about each field.

Field	Description
Name	Specifies the name of the IP exception entry.
Enable	Enables or disables the IP exception entry.
IP	Specifies the IP entry to exclude from Basic Security Defense detection. The supported types include IP Address , IP Subnet , and IP Range .

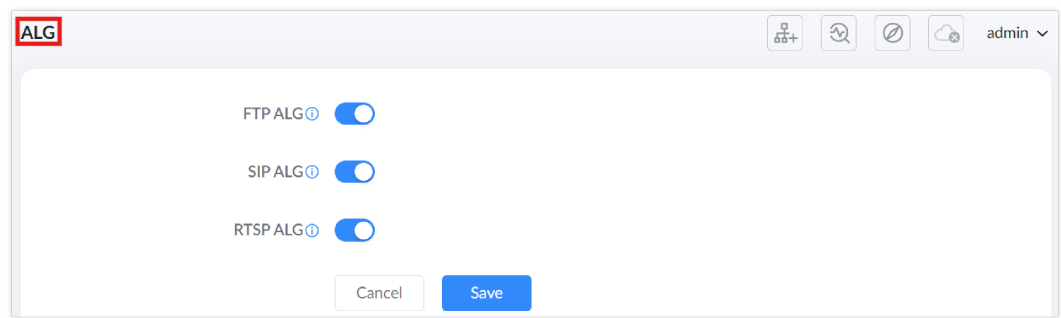
IP Exception

Existing IP exception entries can be edited or deleted from the **Operations** column.

ALG

The **ALG** page allows users to enable or disable Application Layer Gateway handling for supported protocols. ALG helps specific application protocols pass through NAT by assisting with protocol negotiation.

Navigate to **Advanced** → **Security** → **ALG** to access this page.



ALG

Refer to the table below for more details about each field.

Field	Description
FTP ALG	Enables FTP ALG to support TCP negotiation.
SIP ALG	Enables SIP ALG to support TCP/UDP negotiation.
RTSP ALG	Enables RTSP ALG to support TCP negotiation.

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®

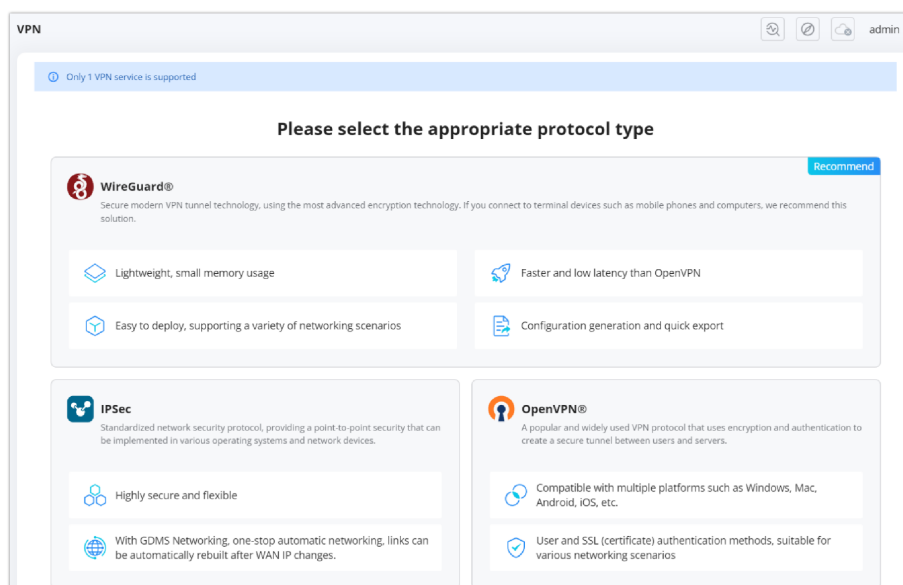
- A widely used VPN protocol with encryption and authentication features.
- Compatible with multiple platforms (Windows, Mac, Android, iOS).
- Supports user authentication via SSL certificates.

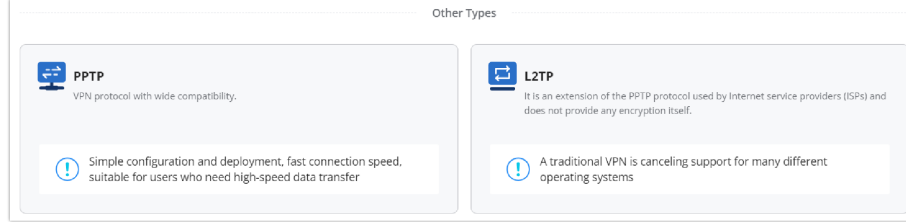
4. PPTP

- 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 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

The screenshot shows the 'WireGuard®' configuration screen in the Setup Wizard. The progress bar indicates the current step is 'Select Interface'. The configuration fields are as follows:

- Name**: WireGuard® (1-64 characters)
- Interface**: WAN2 (WAN)
- Local IP Address**: 192.168.49.1
- Subnet Mask**: 255.255.255.0 (Only support input range 255.255.255.0-255.255.255.255 is supported)

Buttons for 'Back' and 'Next' are at the bottom.

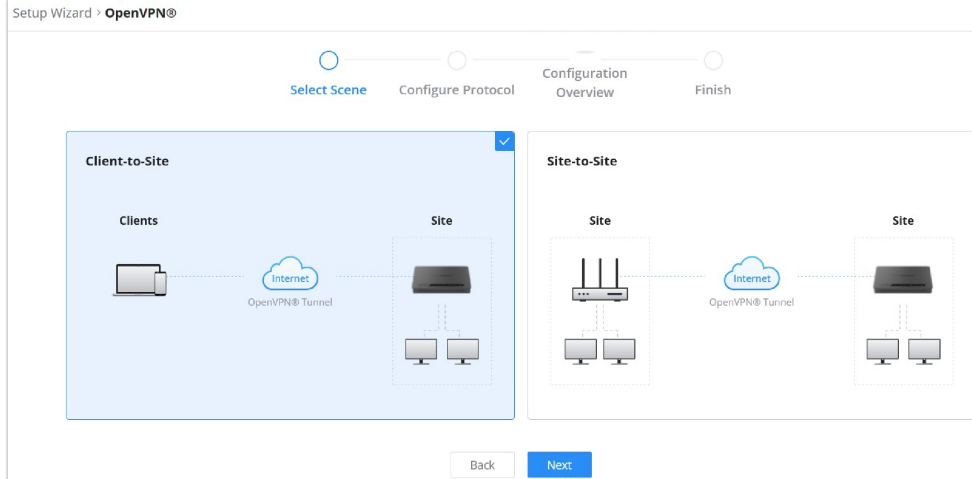
WireGuard® Example

◦ IPSec Setup Wizard

The screenshot shows the 'IPSec' configuration screen in the Setup Wizard. The progress bar indicates the current step is 'Select Scene'. The configuration is for a 'Site-to-Site' connection, showing two sites connected via an 'Internet' cloud and an 'IPSec Tunnel'. The 'Site-to-Site' option is selected with a checkmark. Buttons for 'Back' and 'Next' are at the bottom.

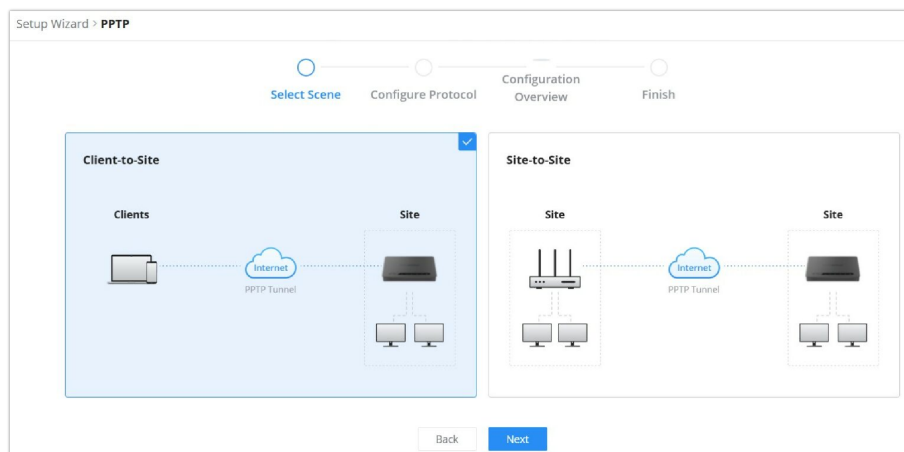
IPSec Example

◦ OpenVPN® Setup Wizard



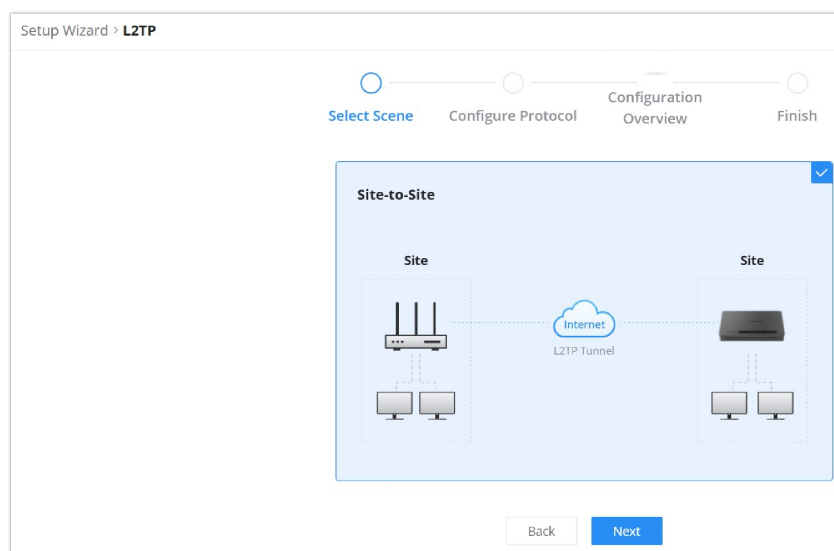
OpenVPN® Example

- o **PPTP Setup Wizard**



PPTP Example

- o **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**.

IPv6

WAN IPv6

Enable ☒

* Interface

☐ WAN1
☒ WAN2

The selected port is disabled. Please go to [Internet Settings](#) to enable it.

Internet Connection Type

☒ Dynamic IP
☐ Static IP
☐ PPPoE

DNS Service

Automatic Acquisition

Get PD prefix

☒

LAN IPv6

Enable ☒

IPv6 Address Prefix / Prefix Length

Automatic Acquisition

Interface ID

☒

* Customize Interface ID

IPv6 Address Assignment

Stateless DHCPv6

IPv6

WAN IPv6

This section manages IPv6 connectivity for the WAN interfaces.

IPv6

WAN IPv6

Enable ☒

* Interface

☐ WAN1
☒ WAN2

The selected port is disabled. Please go to [Internet Settings](#) to enable it.

Internet Connection Type

☒ Dynamic IP
☐ Static IP
☐ PPPoE

DNS Service

Automatic Acquisition

Get PD prefix

☒

LAN IPv6

Enable ☐

Cancel

Save

WAN IPv6 Get PD Prefix enabled

Refer to the table below for more details about each field.

Field	Description
Enable	Enables or disables IPv6 support on the selected WAN interface.
Interface	Selects the WAN interface used for IPv6 connectivity. WAN1: Applies the WAN IPv6 configuration to the WAN1 interface. WAN2: Applies the WAN IPv6 configuration to the WAN2 interface. If the selected WAN port is disabled, a warning message is displayed and the port must be enabled under Advanced → Internet Settings → Internet Settings before it can be used.

Field	Description
Internet Connection Type	Selects the IPv6 connection method. • Dynamic IP: Obtains IPv6 addressing automatically from the upstream network. • Static IP: Allows the IPv6 address information to be configured manually. • PPPoE: Used when the ISP requires PPPoE authentication for IPv6 service.
DNS Service	Selects how DNS servers are assigned for the WAN IPv6 connection. The available DNS service profiles can be reviewed under Advanced → Internet Settings → DNS Service. • Automatic Acquisition: Obtains DNS server information automatically. • Basic & Speed Optimization: Uses predefined DNS profiles optimized for general performance and stable resolution. • Family & Content Filtering: Uses DNS profiles designed to filter inappropriate or unwanted content. • Security & Protection: Uses DNS profiles focused on blocking malicious or unsafe domains. • Static DNS: Allows DNS servers to be configured manually.
Get PD prefix	Requests and uses a Prefix Delegation (PD) from the ISP. This is commonly used to assign IPv6 prefixes to the LAN side.

IPv6 → WAN IPv6

Note:

When enabled, this option will also set the **LAN IPv6** → **IPv6 Address Prefix / Prefix Length** field to Automatic Acquisition. If disabled, users must manually input these fields in the LAN section.

LAN IPv6

This section configures IPv6 behavior within the local network.

LAN IPv6

Enable ☒

IPv6 Address Prefix / Prefix Length

IPv6 Address Prefix

Prefix Length

Prefix Length range 48~64

Interface ID

☒

Customize Interface ID

IPv6 Address Assignment

Stateless DHCPv6

Cancel

Save

LAN IPv6 Get PD prefix is disabled

- **Enable:** Enables IPv6 functionality for LAN.
- **IPv6 Address Prefix / Prefix Length:** Set to **Automatic Acquisition** or specify manually if needed.

Note:

This field is automatically filled if the Get PD prefix option is enabled in the WAN IPv6 section. Otherwise, it must be entered manually.

- **Interface ID:** Toggle to enable interface identifier customization. (*Auto-generate IPv6 address when disabled*)
 - **Customize Interface ID:** Appears only when the toggle is on.

- **IPv6 Address Assignment:**
 - **Stateless DHCPv6**
 - **Stateful DHCPv6**
 - **SLAAC** (if available)

This modular approach provides flexibility for both home users and enterprise setups with dual WAN deployments.

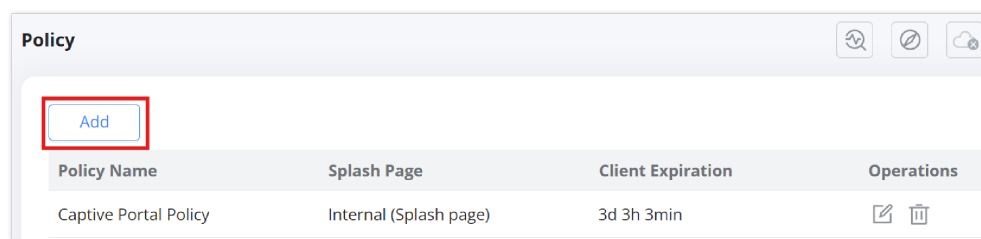
Captive Portal

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.

Policy > Add Policy

Policy Name: Captive Portal - policy (1-64 characters)

Splash Page: ☒ Internal ☐ External

Client Expiration: 7 day 3 hour 0 min

Client Idle Timeout (Min): Range 5-1440

Unauthenticated Client Timeout (Min): Range 1-1440

Daily Limit: ☒ Disable ☐ Limit by client ☐ Limit by authentication method

Splash Page Customization: Splash page

Login Page: ☒ Redirect to the original URL ☐ Redirect to an external page

HTTPS Redirection: ☐

Secure Portal: ☐

Pre Authentication Rule(s): Please enter IP or domain Add +

Post Authentication Rule(s): Please enter IP or domain Add +

Cancel Save

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

admin

Add

Welcome to GIN7062ET

Login for free

Login with password

Splash page

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.

Client	Wi-Fi Name	Authentication Type	Login Time	End Time	Authentication Status	Operations
Android-4 0A:B5:8F:28:E8:6B	portal	For Free	2025/03/14 16:31:07	2025/03/17 19:34:07	Authenticated	

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.

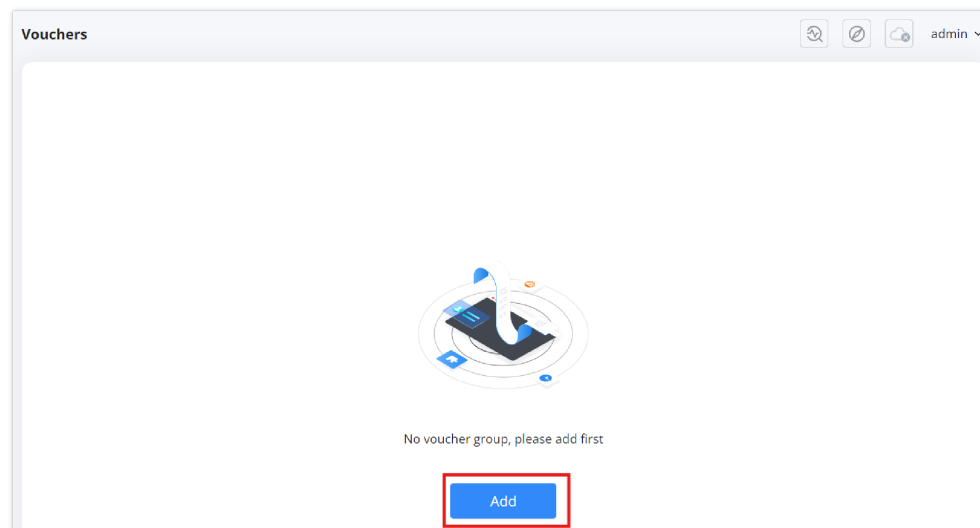
Vouchers

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.

Vouchers > Add Voucher Group

* Voucher Group Name: Guests Voucher (1-64 characters)

* Quantity: 100 (Range 1-100)

* Max Devices: 5 (Range 1-5)

Byte Limit: 5 (The range is 1-1024, if it is empty, there is no limit)

Traffic Allocation Method: ☒ Per Voucher ☐ Per Device

* Duration: 6 day 3 hour 24 min

* Valid Time (Days): 7 (Range 1-365)

Description: Vouchers for Guests (0-128 characters)

Cancel Save

AddEdit 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.

Vouchers							
Add							
Voucher Group Name	Voucher Quota	Duration	Byte Limit	Created Time	Expire Time	Description	Operations
Guests Voucher	0/100	6d 3h 24min	5GB/Per Voucher	2025/03/14 16:39:20	2025/03/21 16:39:20	Vouchers for Guests	

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 under **Maintenance** → **Upgrade** allows users to manage firmware updates for the main router and mesh device nodes. The page displays the current firmware version of the primary device, lists connected device nodes with their firmware versions, and provides options for manual or automatic firmware upgrades.

The device overview area shows the primary router and the available device nodes in the mesh network. Users can check the current firmware version of each device before starting an upgrade.

Upgrade

GWN7062E Primary

Current Version: 1.0.5.2

Detect New Version

Device Nodes (4)

GWN7062M_E318

1.0.1.89

GWN7062ET_9C3C

1.0.5.2

GWN7062ET_9C24

1.0.5.2

GWN7062ET_9B70

1.0.5.2

Upgrade via Manual Upload

Device Node

GWN7062E Primary

Upload firmware file to update (.bin)

Upgrade

Automatic Upgrade

Automatic Upgrade

☐

Cancel

Save

Upgrade page

Refer to the table below for more details about each field.

Field	Description
Primary Device	Displays the main router model and its current firmware version.
Device Nodes	Displays the connected mesh device nodes and the firmware version installed on each node.
Detect New Version	Checks whether a newer firmware version is available for the router or device nodes.
Device Node	Selects the device node to upgrade through manual firmware upload. The primary router and supported mesh nodes can be selected from the list.
Upload firmware file to update (.bin)	Uploads a firmware file in <code>.bin</code> format for the selected device node.
Upgrade	Starts the manual firmware upgrade process for the selected device and uploaded firmware file.
Automatic Upgrade	Enables scheduled firmware upgrade checks and installation based on the configured automatic upgrade settings.

Upgrade page

When a new firmware version is detected, the upgrade window displays the upgradeable device nodes and the available firmware version. Users can select the devices to upgrade from the list. The window also provides access to the firmware release information through the **See new features** link.

Upgrade

GWN7062ET Primary

Current Version: 1.0.5.2

Detect New Version

Device Nodes (1)

GWN7062E

1.0.3.25

See new features

GWN7062E_A7D4

1.0.3.25

See new features

Upgrade via Manual Upload

Device Node

GWN7062E Primary

Upload firmware file to update (.bin)

Upgrade

Automatic Upgrade

Automatic Upgrade

☐

Cancel

Save

New Firmware Version Available

Do not disconnect the network or power supply during download and installation. The device will be unable to connect to the network while the main node is being installed.

Upgradeable device node

☒

GWN7062E

New Version: 1.0.3.25

See new features

☒

GWN7062E_A7D4

New Version: 1.0.3.25

See new features

Cancel

Upgrade

Detect New Version

Important: Do not disconnect the network or power supply during firmware download or installation. The device may be unable to connect to the network while the main node is being installed.

Automatic Upgrade

The **Automatic Upgrade** section allows the router to check for and install firmware updates during a defined maintenance window. This helps keep the device firmware up to date while allowing administrators to control when upgrade activity can occur.

When **Automatic Upgrade** is enabled, the router displays the current system time, the scheduled upgrade time range, and the upgrade cycle settings.

Maintenance → Upgrade – Automatic Upgrade

Automatic Upgrade

Automatic Upgrade

☒

Router Current Time

2026/05/12 11:48:11

* Upgrade Time

00:00

→

01:00

* Upgrade Cycle

☒ Weekly

☐ Monthly

Sunday

▼

Automatic Upgrade

Refer to the table below for more details about each field.

Field	Description
Automatic Upgrade	Enables or disables scheduled firmware upgrade checks and installation.
Router Current Time	Displays the current time used by the router for scheduling automatic upgrades.
Upgrade Time	Defines the time window during which automatic upgrade activity can run.
Upgrade Cycle	Specifies how often the router checks for firmware updates. The available options are Weekly and Monthly .
Weekly	Runs the automatic upgrade check on the selected day of the week.
Monthly	Runs the automatic upgrade check on the selected day of the month.

Automatic Upgrade

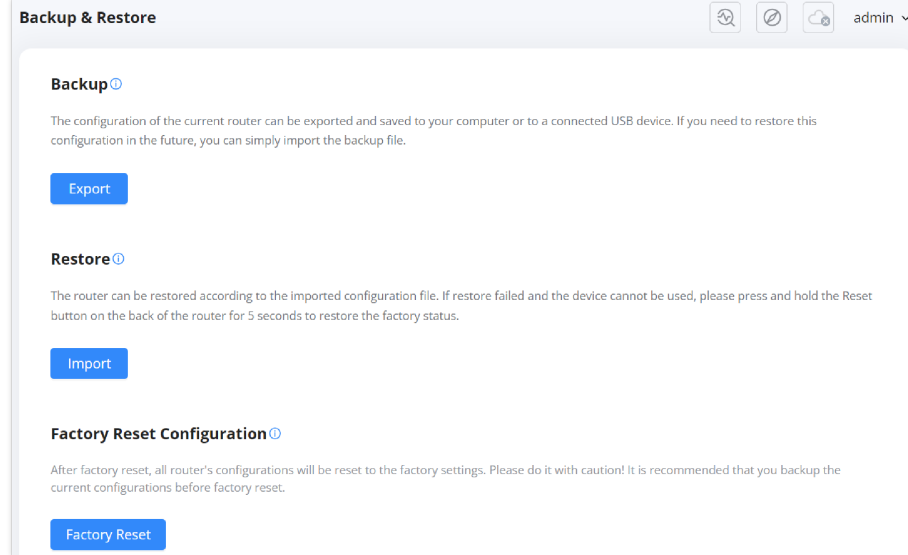
Note: Schedule automatic upgrades during low-traffic hours to reduce service interruption during firmware download and installation.

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.

Note: For security and operational purposes, please be aware that the backup `.bin` file does not include the following settings. These will need to be reconfigured manually if the device is restored:

- **Mesh Network Configurations:** Any configured Mesh network settings are excluded. Consequently, sections in the user interface that display Mesh nodes (such as the Network Map) will appear empty until the Mesh network is reconfigured.
- **Captive Portal Vouchers:** All generated vouchers used for Captive Portal authentication will not be saved.
- **TR-069 Credentials:** The connection request username, password, and port settings used for TR-069 remote management are excluded.
- **GWN Manager Settings:** The cloud management access settings (Manager Settings) are not retained in the backup file.
- **Maintenance Tunnel:** Any active maintenance tunnel configurations used for remote diagnostics will not be backed up.

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.

Ping / Traceroute

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

Steps to Use Ping / Traceroute:

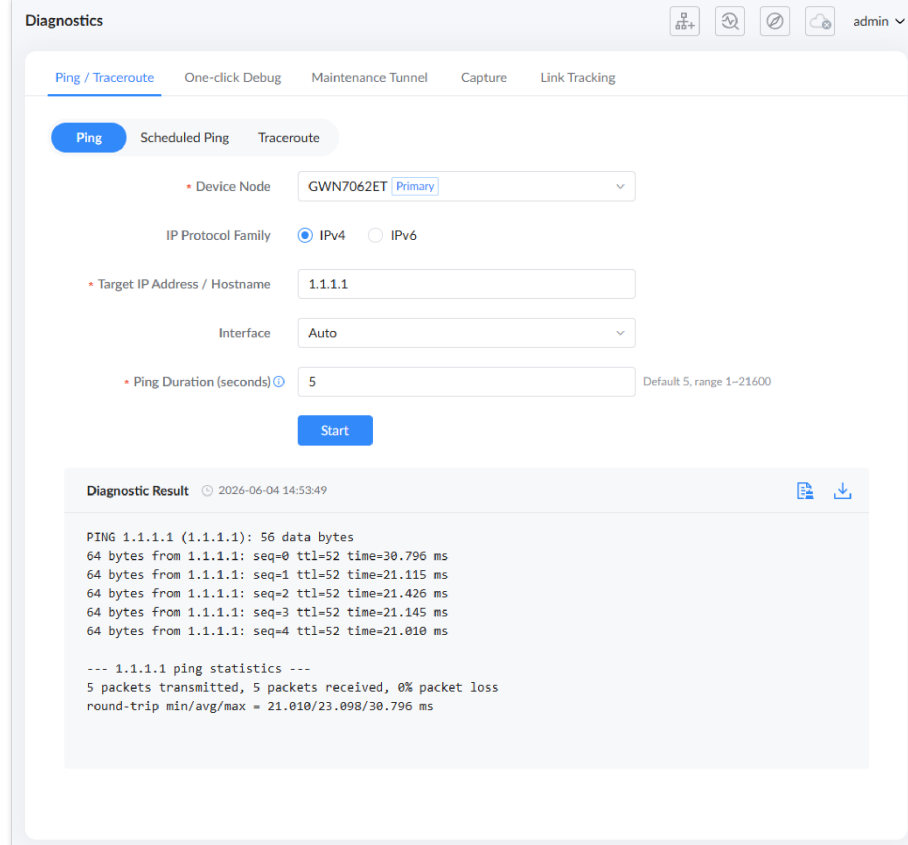
1. Select **Diagnostic Tools**:
 - **Ping (IPv4/IPv6)** – Checks if a device is reachable.
 - **Traceroute** – Traces the path packets take to a destination.
2. Enter **Target IP Address / Hostname**.
3. Select **Interface** (Auto by default).
4. Click **Start** to run the test.

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 PingTraceroute

One-click Debug

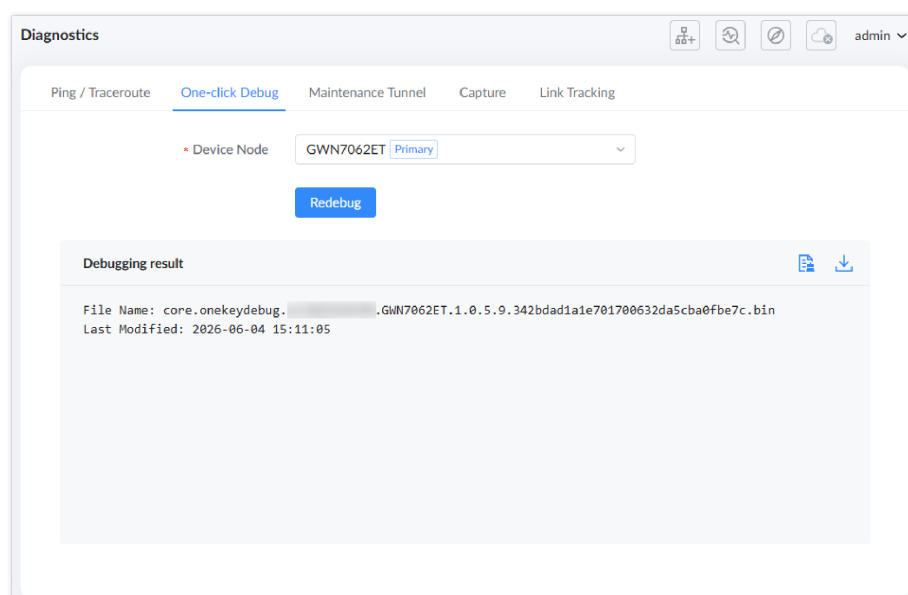
This feature automatically **collects system logs and diagnostic data** in a compressed file.

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

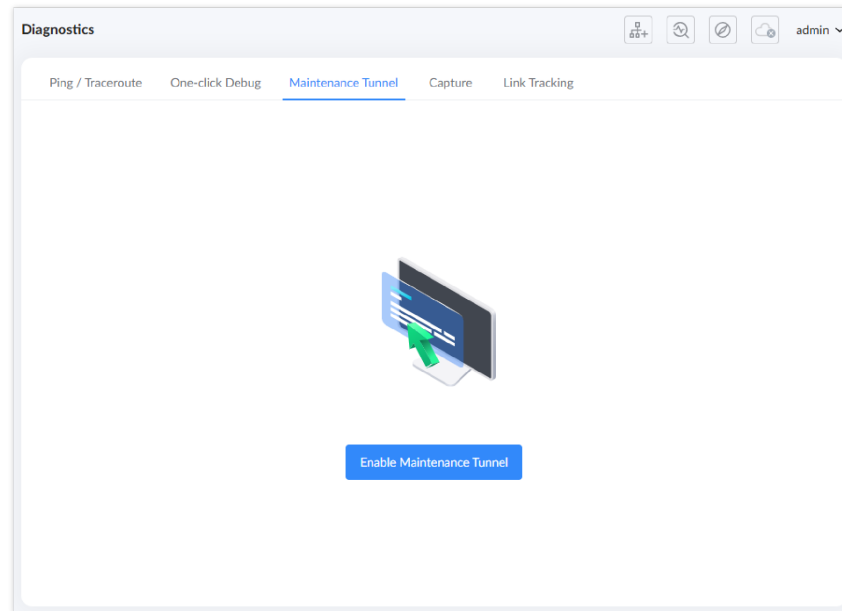
Maintenance Tunnel

In certain cases, Grandstream support may require remote access to the router to diagnose an issue. Enabling Maintenance Tunnel allows safe remote access.

Important

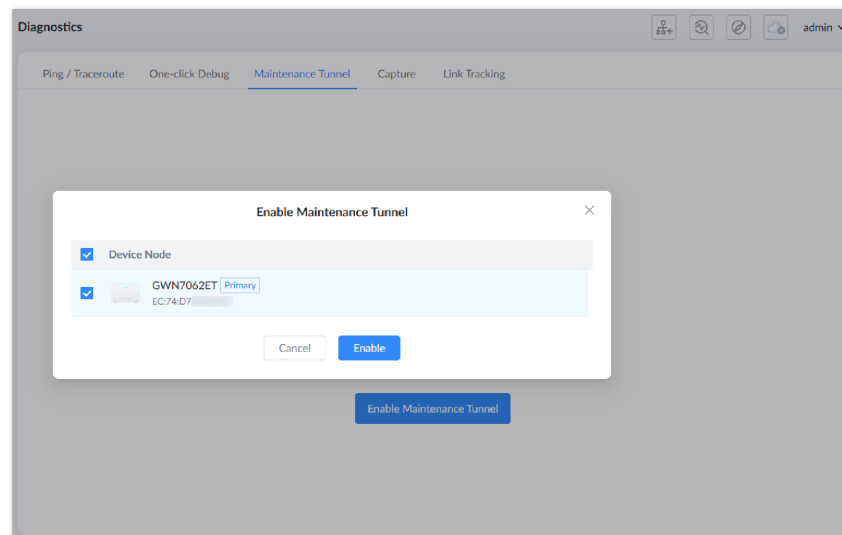
- We highly recommend disabling Maintenance Tunnel right after the diagnosis is completed.
- Maintenance Tunnel is automatically disabled after 48 hours of the time of enabling it.

1. To access Maintenance Tunnel configuration, navigate to **Advanced > Maintenance > Diagnostics > Maintenance Tunnel**, click “Enable Maintenance Tunnel”.



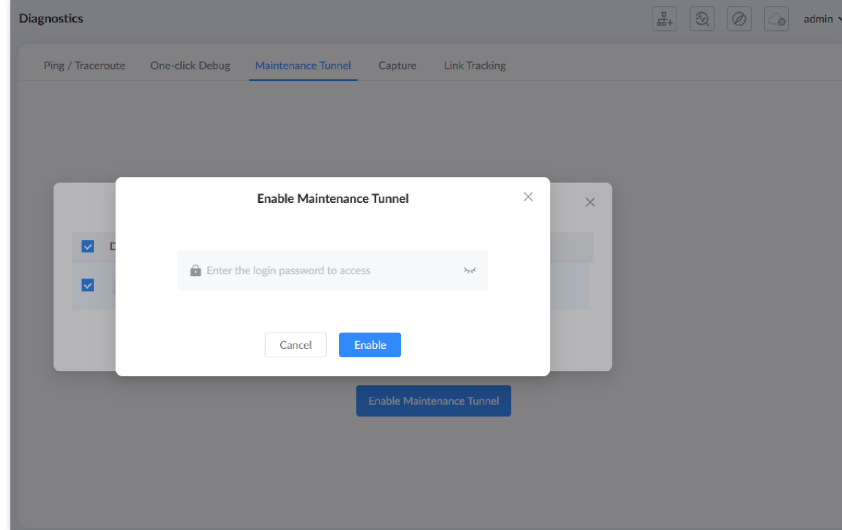
Maintenance Tunnel

2. Select the nodes on which the tunnel will be enabled.

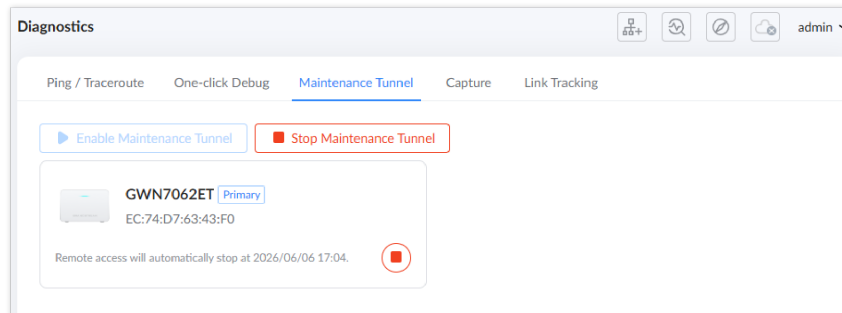


Select Nodes

3. Enter the administrator password, then click “Enable”.



Enable Maintenance Tunnel



Maintenance Tunnel Enabled

Capture

Packet capture feature allows to capture the traffic going through the router for diagnosis purposes.

Ping / Traceroute
One-click Debug
Maintenance Tunnel
Capture
Link Tracking

Interface
All

Capture Duration
1 minutes

Capture Rule
☒ Default
☐ Custom Rules

Traffic Direction
☒ Both
☐ Inbound
☐ Outbound

Protocol
Any

IP Address

Storage Location
Browser Download

Format
☒ cap
☐ tar

For long-term captures, the tar format is recommended to generate segmented files.

Start Capturing

Capture

Parameter	Description
Interface	Select the interface to capture the traffic from. Selecting “All” will result in capturing the traffic from all the interfaces.

Capture Duration	Define the capture duration.
Capture Rule	Enter the filters for the capture.
Traffic Direction	Select the traffic direction. • Both • Inbound • Outbound The default setting is Both.
Protocol	Select the protocols to capture. • Any • TCP • UDP • ICMP • IGMP The default setting is Any.
IP Address	Enter the IP address to use as a filter.
Storage Location	Select the storage location of the capture file. The default setting is Browser Download.
Format	Select the file format of the capture file. • cap • tar Note: For long-term captures, the tar format is recommended to generate segmented files. The default setting is cap.

Link Tracking

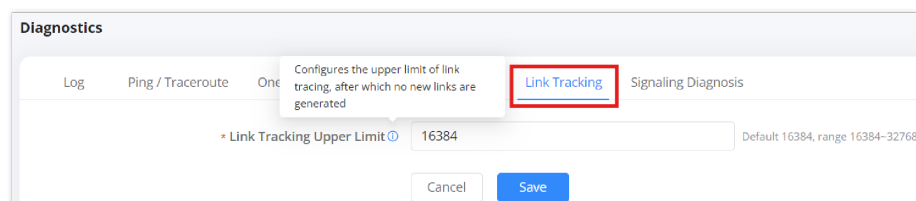
Monitors and controls **network connection limits**.

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

5. Signaling Diagnosis

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

Steps to Start Capturing:

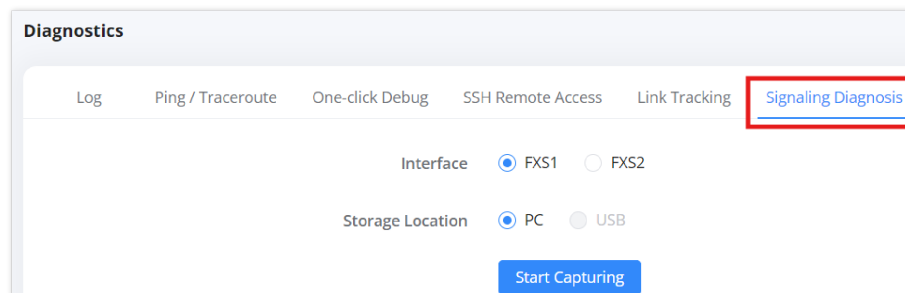
1. Select **Interface** (e.g., **FXS1**, **FXS2** for VoIP traffic).
2. Choose **Storage Location** (PC or USB).

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**:

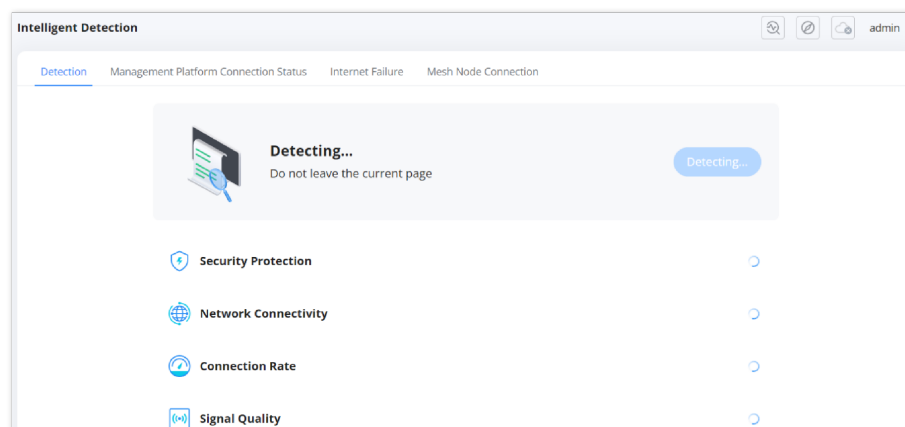
1. Log in to the router's web UI.
2. Navigate to **Maintenance** → **Intelligent Detection**.
3. Select the relevant tab to perform detection tests.

1. Detection Tab

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

How to Run a Detection Test:

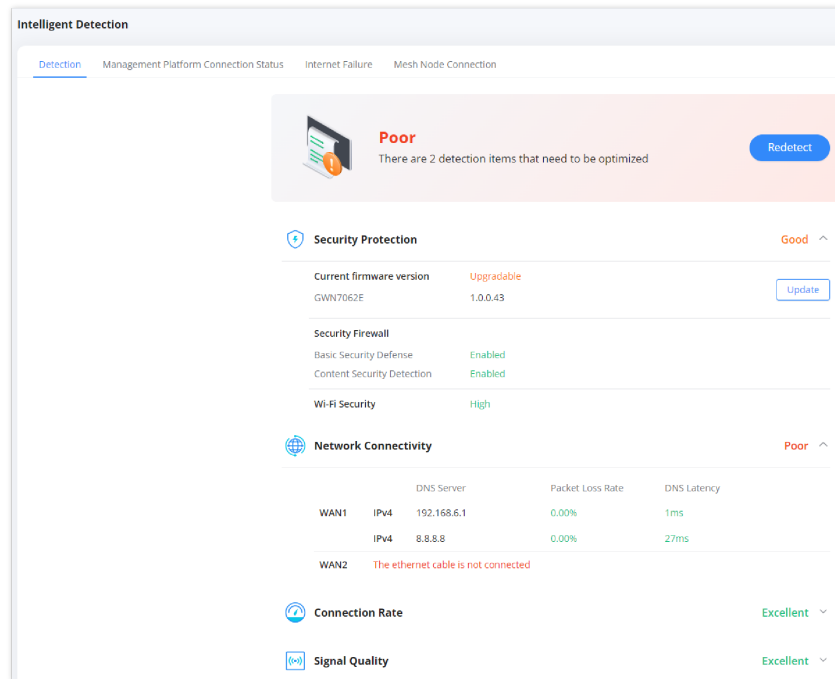
1. Click the **Detection** button.
2. The router runs diagnostics on the following areas:
 - **Security Protection** – Checks for firmware updates, firewall settings, and Wi-Fi security.
 - **Network Connectivity** – Analyzes DNS latency and packet loss.
 - **Connection Rate** – Monitors the status of 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**.



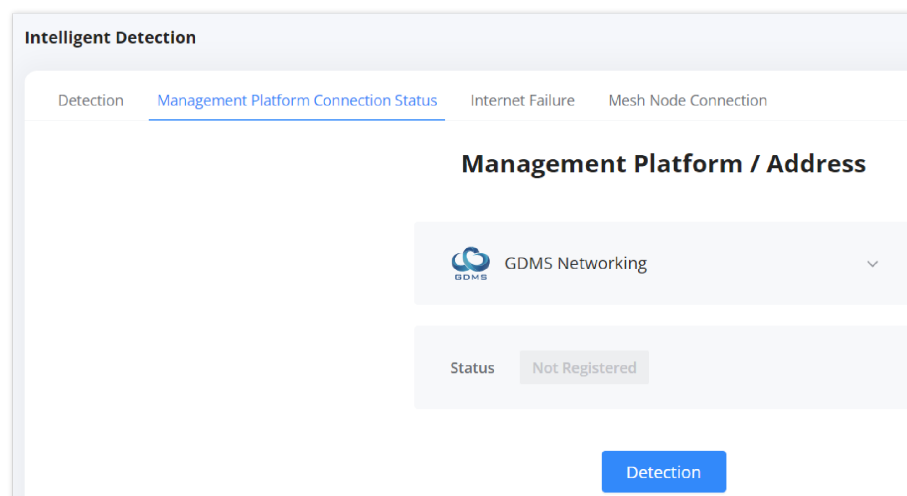
Intelligent Detection Detection Tab

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:

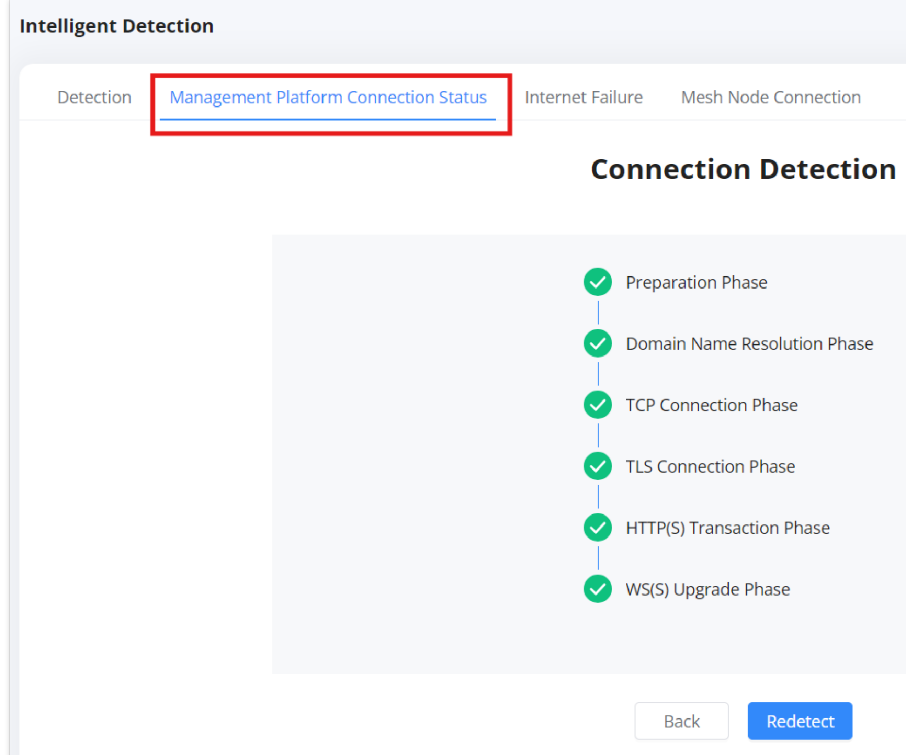
1. Click **Detection** to start the connection test.
2. The system verifies different **connection phases**:
 - **Preparation Phase**
 - **Domain Name Resolution Phase**
 - **TCP Connection Phase**
 - **TLS Connection Phase**
 - **HTTPS Transaction Phase**
 - **WebSocket Upgrade Phase**
3. If all phases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

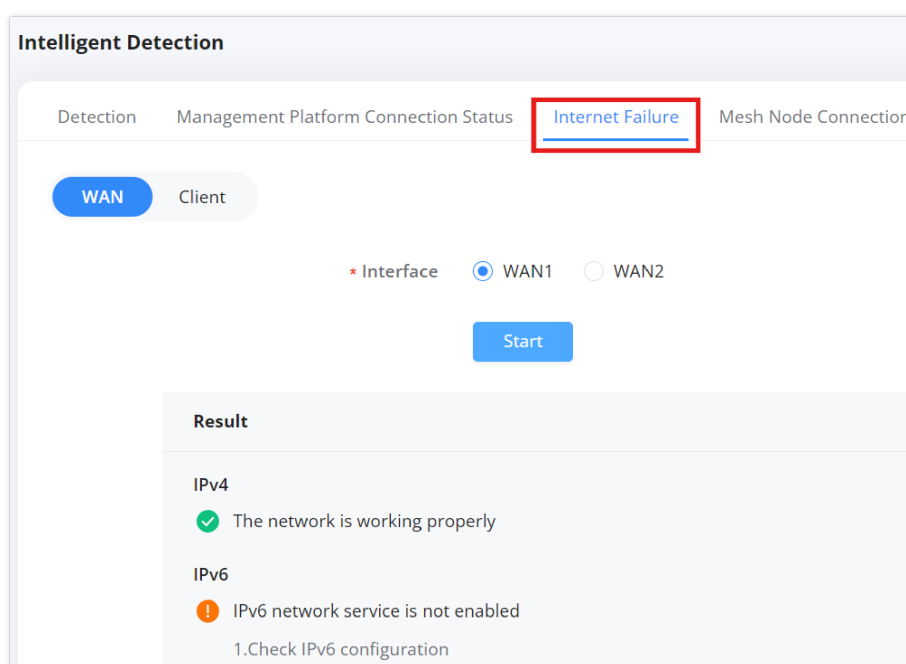
3. Internet Failure Detection

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:

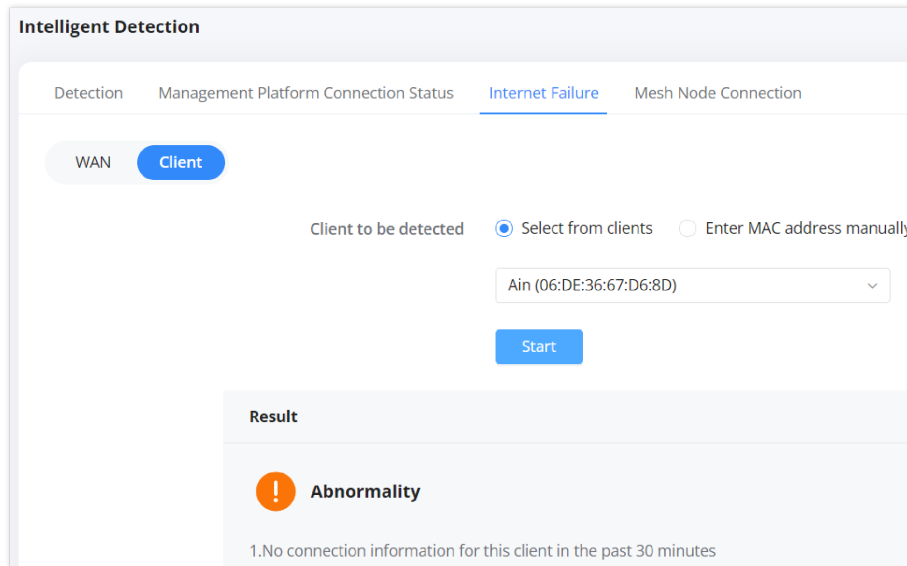
1. Select **Client** and choose a connected device from the list or enter a **MAC address manually**.

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.
- Troubleshoot **client device disconnections**.



Intelligent Detection Internet Failure

4. Mesh Node Connection

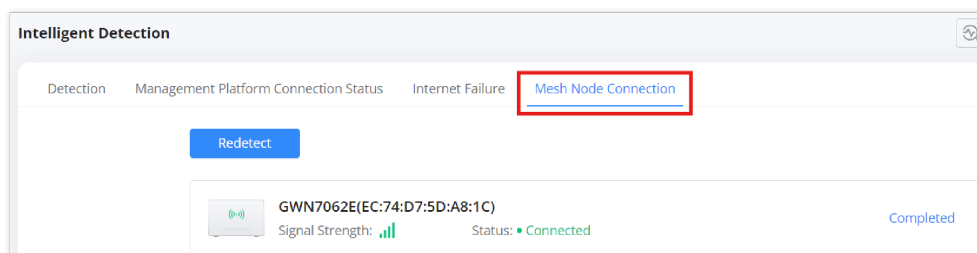
This tab checks the status of connected **mesh nodes** in a multi-router setup.

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**.
- Troubleshoot **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 ☒

ACS URL

ACS Username

ACS Password

Periodic Inform ☒ If enabled, the router will send connection Inform packets to ACS regularly.

Periodic Inform Interval (sec) Default: 86400

Connection Request Username

Connection Request Password

Connection Request Port Default: 7547, range 1-65535

CPE Cert File

CPE Cert Key

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

Log

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.
- **User** – Displays the user account associated with the log entry.
- **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.

Time	Severity	Platform	User	Address	Log Type	Details
2026-05-12 11:31:28	Notice	Local	admin	IPv4:192.168.5.248	Operation	action:check firmware
2026-05-12 11:28:36	Notice	Local	admin	IPv4:192.168.5.248	Operation	action:login
2026-05-12 10:58:39	Notice	Local	admin	IPv4:192.168.5.248	Operation	Update config(success) : s...
2026-05-12 10:50:29	Notice	Local	admin	IPv4:192.168.5.248	Operation	Update config(success) : s...
2026-05-12 10:44:49	Notice	Local	admin	IPv4:192.168.5.248	Operation	Update config(success) : s...
2026-05-12 10:44:45	Notice	Local	admin	IPv4:192.168.5.248	Operation	Update config(success) : s...
2026-05-12 10:44:29	Notice	Local	admin	IPv4:192.168.5.248	Operation	Update config(success) : s...
2026-05-12 10:44:26	Notice	Local	admin	IPv4:192.168.5.248	Operation	Update config(success) : s...
2026-05-12 10:44:18	Notice	Local	admin	IPv4:192.168.5.248	Operation	Update config(success) : s...
2026-05-12 10:43:48	Notice	Local	admin	IPv4:192.168.5.248	Operation	Update config(success) : s...

Diagnostics log page

Basic Settings

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.

Basic Settings

Device Current Time 2025/03/14 14:43:59

Country / Region Morocco

Time Zone (UTC+01:00) Brussels,Copenhagen,Madrid,Paris

NTP Server 0.pool.ntp.org
1.pool.ntp.org
Add

Language English

LED Indicator

LED Indicator ☒ Always On ☐ Always Off ☐ Disabled within the specified time

Reboot Schedule

Reboot Schedule ☒

Reboot Time 00:00 → 01:00

Frequency ☒ Weekly ☐ Monthly

Sunday

Cancel Save

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 allows users to configure how the router can be accessed and managed from the LAN side and WAN side. This includes HTTPS access, SSH access, WAN management access, allowed remote IP addresses, manager-related settings, and passwordless remote access options.

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 **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** – Optionally specify one or more external IPv4/IPv6 addresses that are allowed to access the router's HTTPS management from the WAN side. If left empty, there is **no restriction**, and any IP address can connect. When one or more addresses are configured, **only those IPs** will be able to access the router.

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.

Note: Up to **16 external IPv4/IPv6 addresses** can be added to the allowed access list. Only the configured IP addresses will be able to access the router's HTTPS management interface from the WAN side.

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.

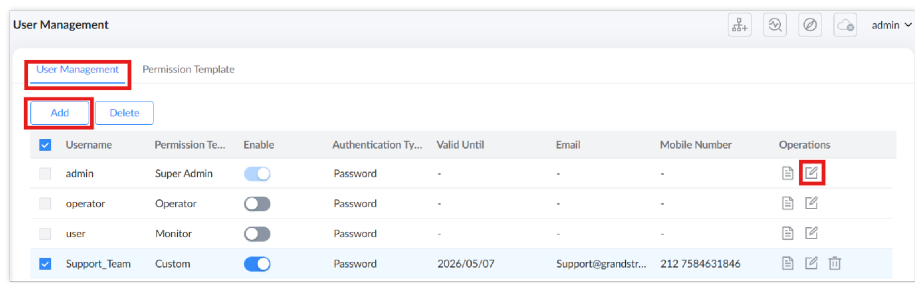
Access management Passwordless Remote Access

User Management

This feature enables the creation of multiple administrative accounts with customized access levels through role-based templates. Administrators can precisely control user privileges by assigning “Read/Write,” “Read-only,” or “No Permission” status to individual functional areas of the Web UI. The system ensures accountability by tracking login history and source IP addresses, while offering flexible security options such as automated account expiration and support for local or external authentication methods.

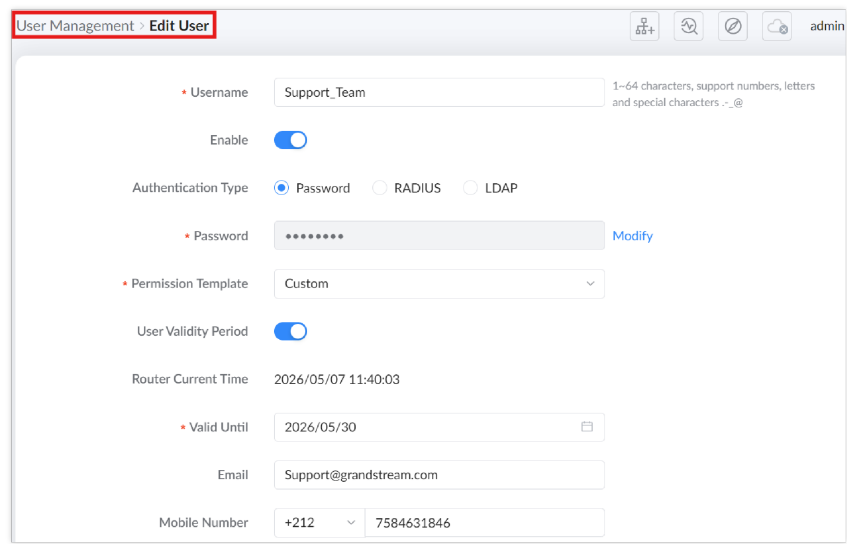
User Management Tab

The **User Management** tab displays a comprehensive list of all accounts authorized to access the router’s Web UI. This interface allows administrators to monitor account statuses, assigned roles, and audit login history at a glance.



User Management Tab

To create a new account, click the **Add** button. To modify an existing account, click the **Edit** icon in the **Operations** column.



Add/Edit User

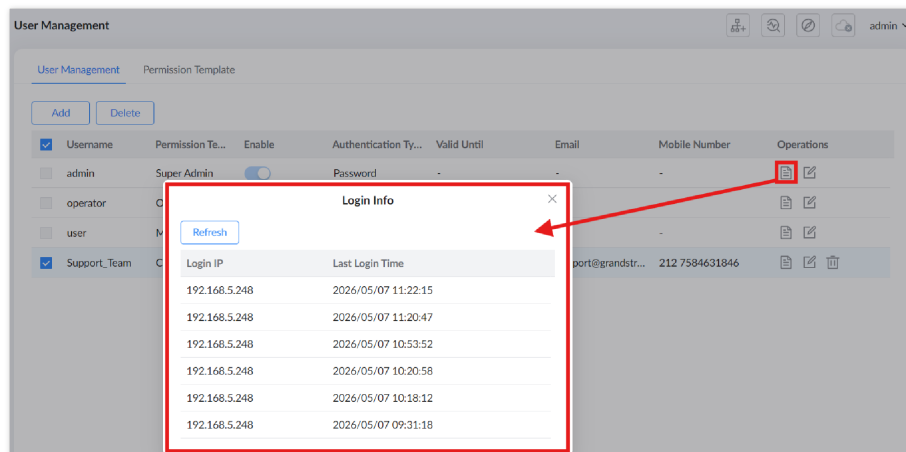
Field	Description
Username	Enter a unique login name for the account. Supports 1–64 characters, including numbers, letters, and special characters: . , - _ , @.
Enable	Toggle this switch to activate or deactivate the specific user account.
Authentication Type	Select the verification method for the user: • Password: Local authentication stored on the router. • RADIUS: Authentication via an external RADIUS server. • LDAP: Authentication via an external LDAP directory.
Password	Define the login password for the user. For existing accounts, click Modify to update the credentials.
Permission Template	Select the specific access role for the user from the dropdown menu. Built-in options typically include Operator , Monitor , or Custom .
User Validity Period	Enable this toggle to set a specific active lifespan for the account. This is recommended for temporary guest or technician access.
Router Current Time	Displays the router’s current synchronized system time to assist in setting accurate expiration dates.

Field	Description
Valid Until	Specifies the exact date when the account will automatically be disabled. This field is mandatory if User Validity Period is enabled.
Email	Input the email address associated with the user for contact and identification.
Mobile Number	Select the country code and enter the user's mobile contact number.

User Configuration Parameters

Auditing User Access

The system includes a dedicated auditing tool to track administrative activity. By clicking the **Log icon** under the **Operations** column, administrators can view the **Login Info** for any user.

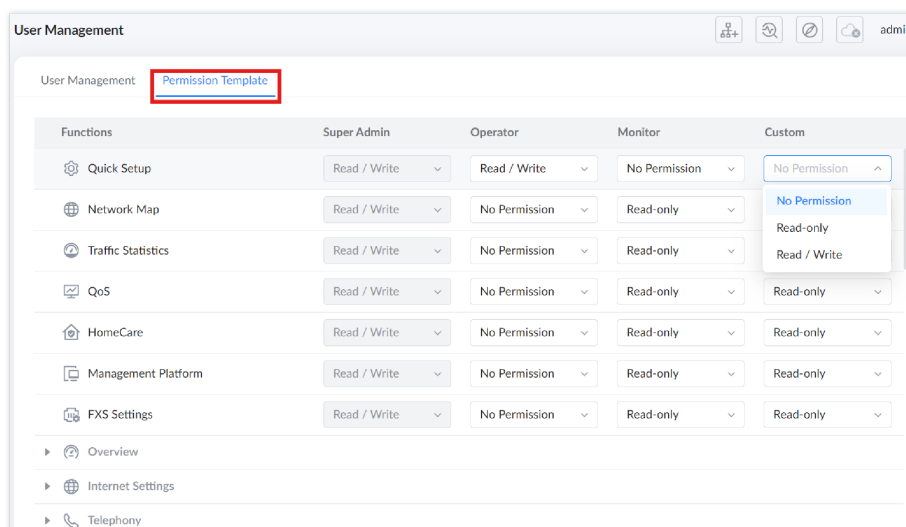


Auditing User Access

This pop-up provides a detailed history of the **Login IP** addresses and the **Last Login Time** for each session, ensuring complete accountability for system changes.

Permission Template

The **Permission Template** tab is the management center for Role-Based Access Control (RBAC). It allows administrators to define exactly which functional areas of the Web UI are visible and modifiable for specific roles. These templates are then assigned to individual users in the **User Management** tab to enforce security policies.



Permission Template

Function Permission Levels

For every feature and menu item listed in the **Functions** column, a specific access level can be assigned via the dropdown menus:

Level	Description
Read / Write	Grants full access. The user can view data and modify all settings within that section.
Read-only	Grants restricted access. The user can view status information and current configurations but cannot save changes or perform actions.
No Permission	Completely restricts access. The corresponding menu item is hidden from the user's interface sidebar.

Template Roles

The interface provides columns for four distinct roles, allowing for standardized permission sets across different types of users:

- **Super Admin:** The highest level of authority. This role is fixed at **Read / Write** for all functions and cannot be modified. It is the only role capable of managing other users and templates.
- **Operator:** A customizable template intended for staff members who handle regular network maintenance. This role is generally used for operational tasks such as Internet Settings, Wi-Fi Settings, and Maintenance, while higher-level permissions can be adjusted by the Super Admin based on the required access level.
- **Monitor:** A customizable template designed for observation-only roles. Most functions are typically set to **Read-only**.
- **Custom:** A fully flexible template that starts as a blank slate, allowing the Super Admin to precisely tailor permissions for unique scenarios.

The functions are organized into expandable categories (e.g., **Overview, Internet Settings, Telephony**) to allow for granular control over every sub-menu of the router.

Operation Mode

The **GWN7062E(T)** supports three different working modes under the **System > Operation Mode** section, allowing users to deploy the router in various network environments based on their needs:

1. **Router Mode** (Default)
2. **Wireless Relay Mode**
3. **Wireless Bridge Mode**

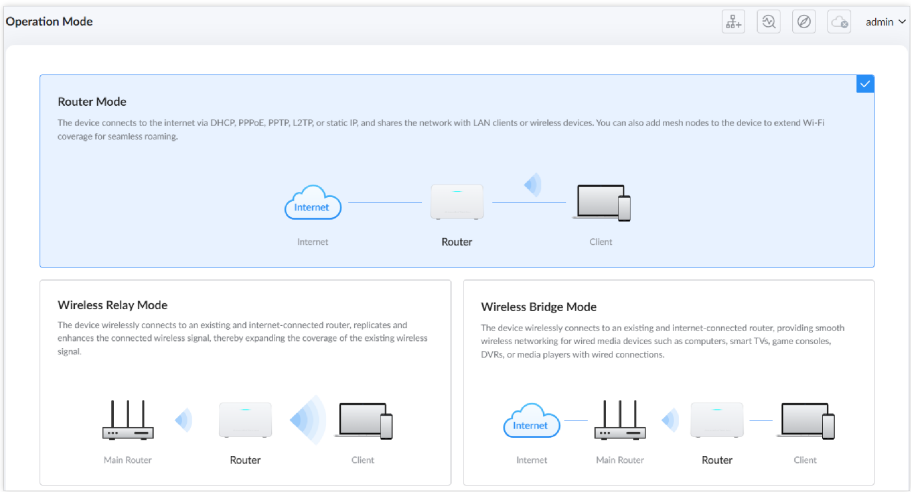
Each mode affects how the device connects to the upstream network and handles LAN traffic whether it's routing traffic, rebroadcasting existing Wi-Fi, or serving as a wireless bridge to wired devices.

Router Mode

This is the default mode. The device connects directly to the Internet via **DHCP, PPPoE, PPTP, L2TP, or Static IP**, then shares that connection with local clients either through Ethernet or Wi-Fi. Users can also add Mesh sub-nodes for broader coverage.

Usage Example:

Standard internet access with full routing and NAT capabilities. Ideal for homes and offices.



Wireless Relay Mode

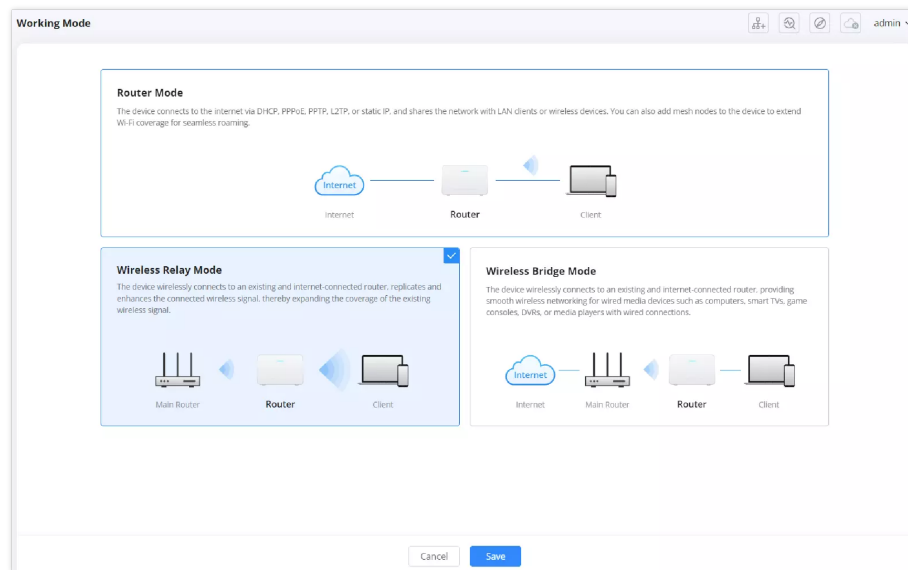
The GWN7062E(T) supports Wireless Relay Mode, allowing the device to connect wirelessly to an existing router and extend the wireless coverage. In this mode, all Ethernet ports on the device become LAN ports, and the device rebroadcasts the same SSID (network name) of the source router. Devices connected via LAN will obtain IP addresses from the main router.

Note

The user can still use FXS gateway when this mode is enabled.

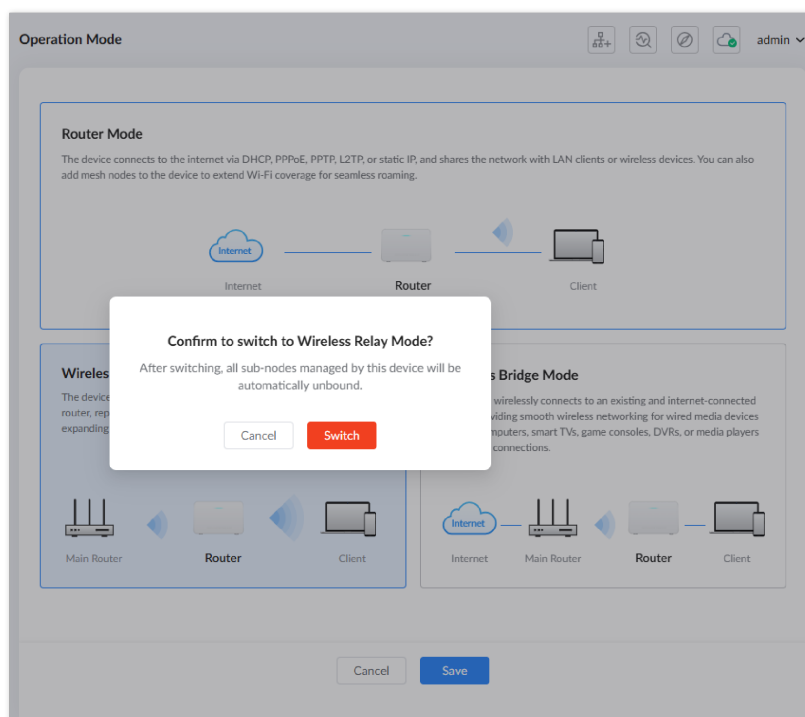
Steps to Configure Wireless Relay Mode:

Navigate to Working Mode. Go to **System > Working Mode** in the left menu. Select **Wireless Relay Mode** from the available options: Router Mode, Wireless Relay Mode, or Wireless Bridge Mode.



Working Mode page

Confirmation Prompt After selecting Wireless Relay Mode, a confirmation dialog will appear stating: "After switching, all sub-nodes managed by this device will be automatically unbound." Click **Switch** to proceed.



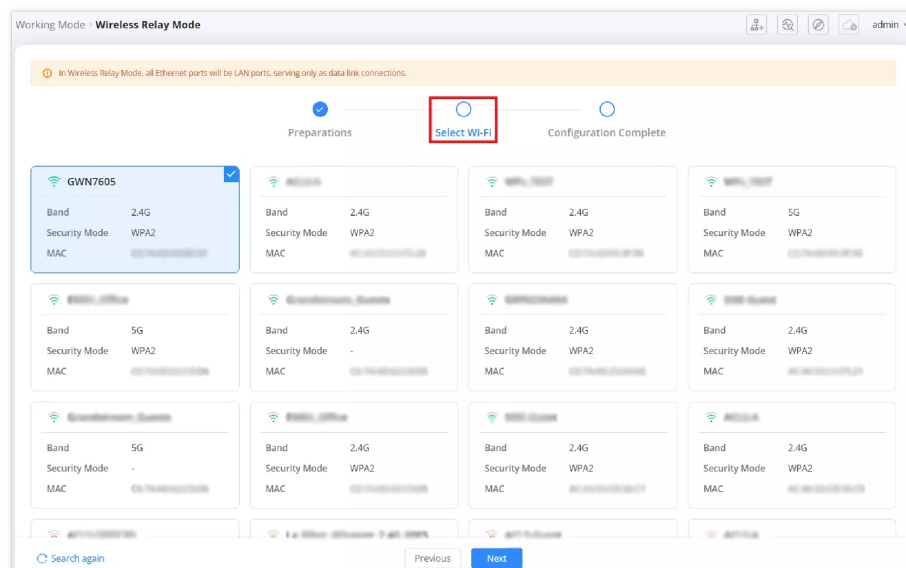
Working Mode Switching Prompt

Step 1 – Preparations The screen will guide you through preparations:

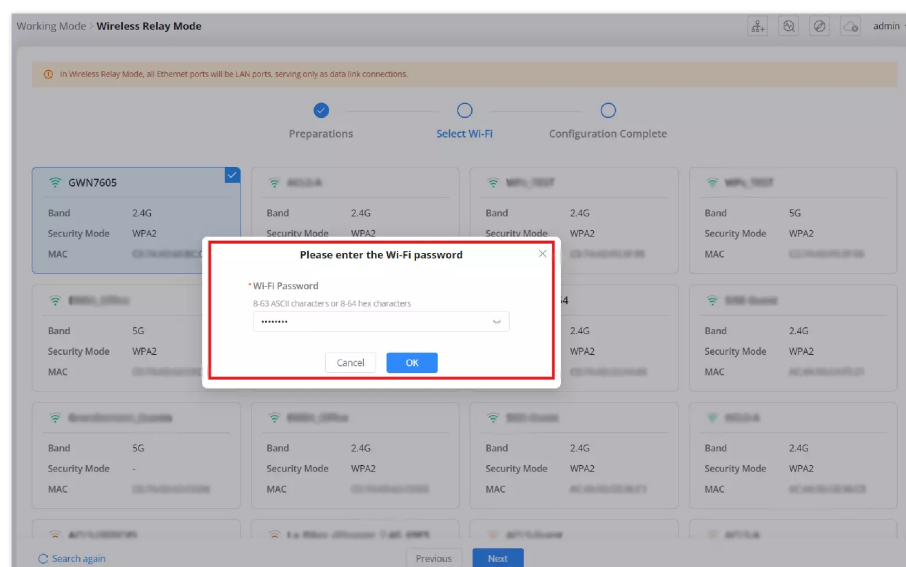
- Ensure a wireless network is available and that this device is placed within signal range.

-

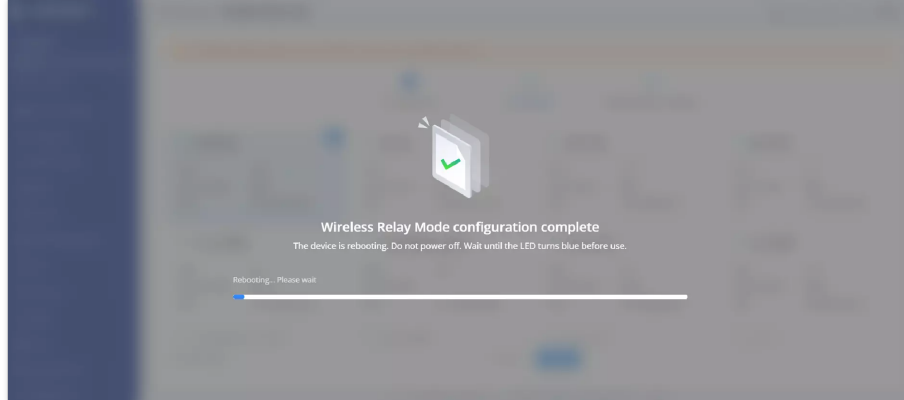
Step 2 – Select Wi-Fi. The device will scan for nearby Wi-Fi networks. Select the desired network (SSID) you wish the GWN7062E(T) to connect to.



Enter Wi-Fi Password. Once the SSID is selected, a prompt will appear requesting the Wi-Fi password. Enter the correct credentials and click **OK**.



Step 3 – Configuration Complete The device will now apply the settings and reboot. Do not power off the unit. Wait for the LED to turn solid blue before using the router.



Working Mode Wireless Relay Mode Rebooting

Note

- In this mode, the router replicates and extends the existing Wi-Fi network.
- All LAN ports can be used to connect wired clients, which will receive IP addresses from the main router.
- This is ideal for extending Wi-Fi coverage without using cables.

You have successfully configured Wireless Relay Mode.

Wireless Bridge Mode

The GWN7062E(T) supports **Wireless Bridge Mode**, allowing the device to wirelessly connect to an existing and internet-connected router. Once connected, the device disables its wireless broadcasting and converts all Ethernet ports into LAN ports for wired client connections. This mode is ideal for connecting wired-only devices such as smart TVs, DVRs, game consoles, and desktop computers to a remote Wi-Fi network.

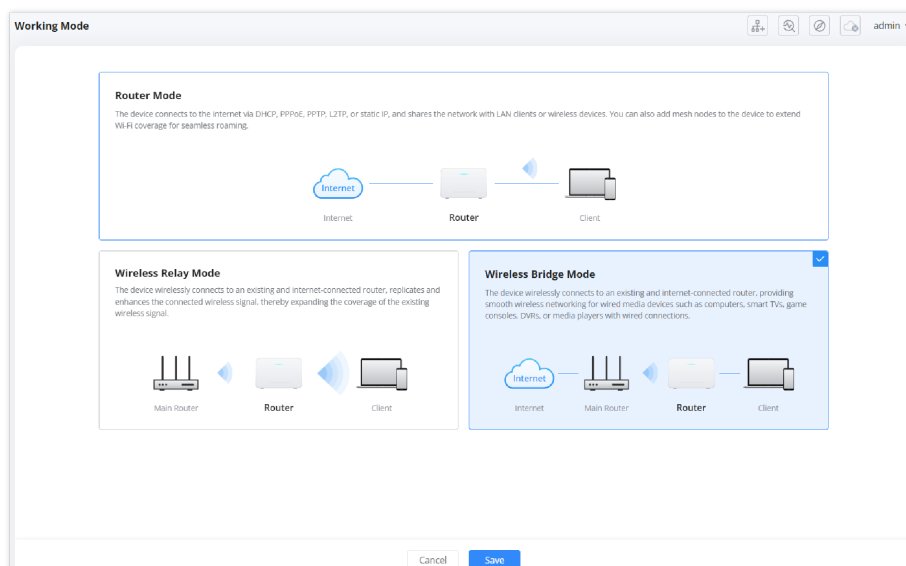
Note

- Wireless client bridge supports third-party access points.
- The user can still use FXS gateway when this mode is enabled.

To set up Wireless Bridge Mode:

1. Navigate to Working Mode

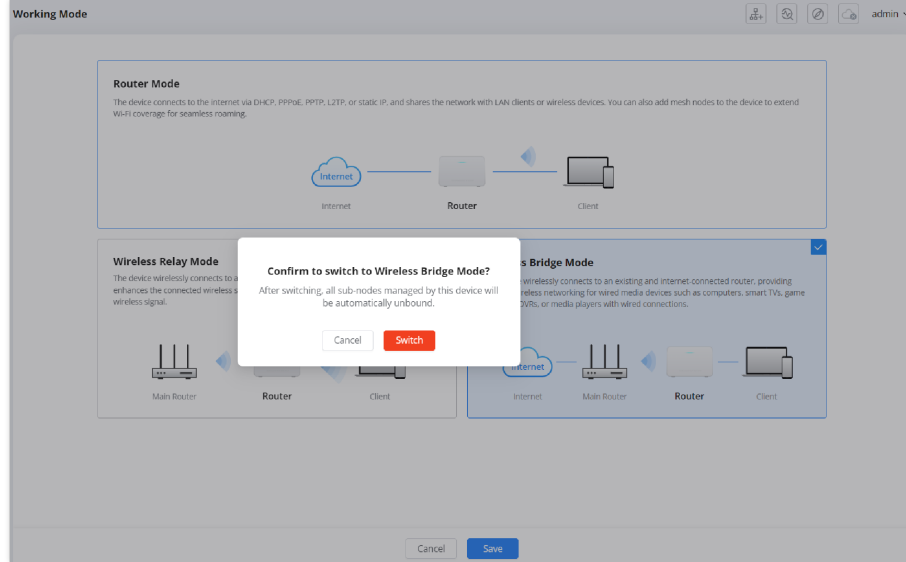
Go to **System > Working Mode**, then select **Wireless Bridge Mode** and click **Save**.



Working Mode Wireless Bridge Mode

2. Confirm Mode Switch

A prompt will appear stating that all sub-nodes managed by the device will be unbound. Click **Switch** to proceed.

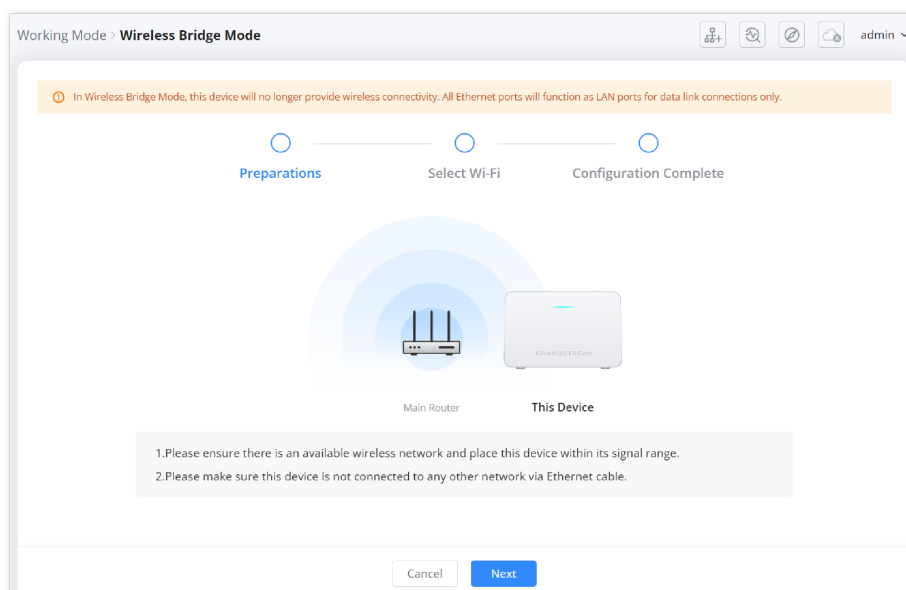


Working Mode Wireless Relay Mode Switch confirmation

3. Read Preparations

The screen will display key instructions:

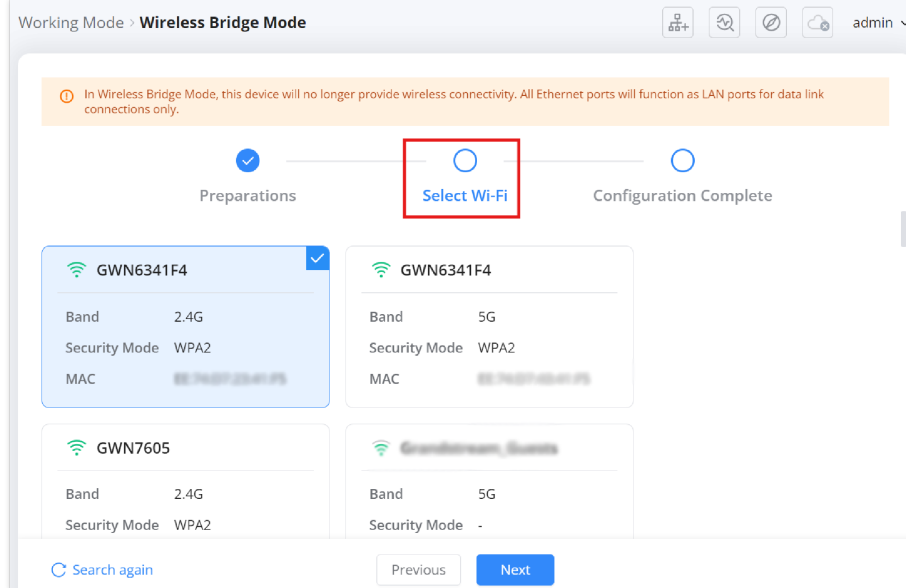
- The device will no longer provide wireless connectivity.
 - All Ethernet ports will serve as LAN ports for data transmission.
 - Ensure the device is not connected to any network via cable and is placed within Wi-Fi range of the main router.
- Click **Next** to continue.



Working Mode Wireless Relay Mode Preparations

4. Select Wi-Fi

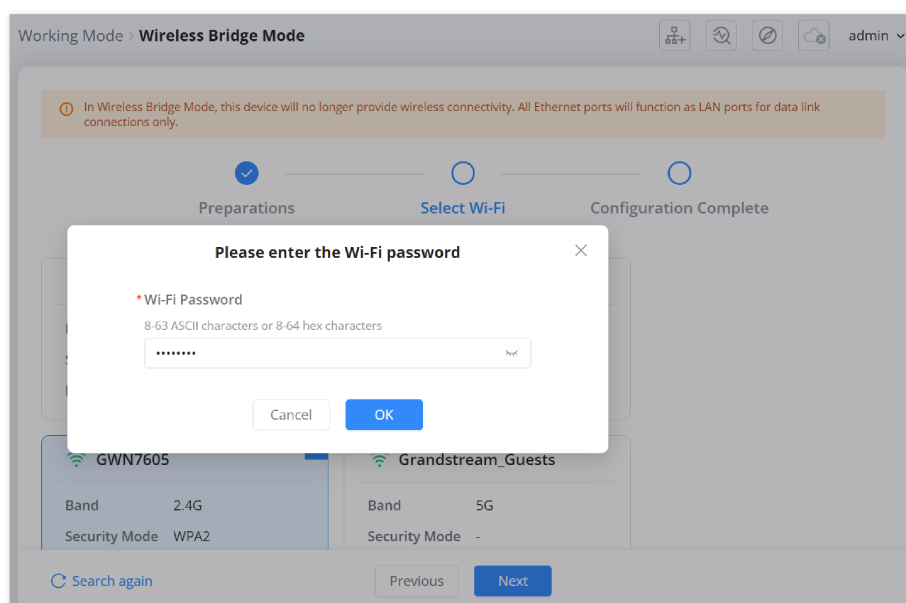
The device will scan for available Wi-Fi networks. Choose the network you want to connect to and click **Next**.



Working Mode Wireless Bridge Mode Select Wi Fi

5. Enter Wi-Fi Password

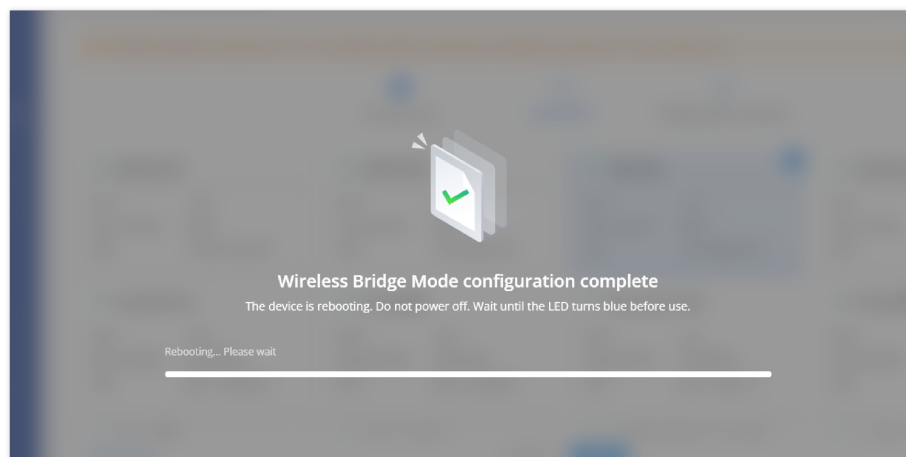
Enter the password of the selected Wi-Fi network and confirm by clicking **OK**.



Working Mode Wireless Bridge Mode Wi Fi Password

6. Reboot and Finish

The device will apply the settings and automatically reboot. Wait until the LED turns solid blue before using it. You can now connect wired clients to the router's LAN ports, and they will obtain IP addresses from the main router.



Working Mode Wireless Bridge Mode Rebooting

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 1.0.5.9

- Added ability to support DTMF on RFC4733 in GWN7062ET. [[Phone Settings](#)]
- Added support for client bridge with third-party AP. [[Operation Mode](#)]
- Added support for packet capture feature. [[Capture](#)]
- Added support to allow device to run as Wi-Fi client with FXS enabled. [[Wireless Relay Mode](#)][[Wireless Bridge Mode](#)]
- Added support to customize Dial, Busy, and Ringback Tones for GWN7062ET. [[Ringtone](#)]
- Improved Ping functionality to support longer duration, scheduled Ping, and save the results into files. [[Ping / Traceroute](#)]
- Added support for TLS and SRTP for SIP calls in FXS settings. [[Template Settings](#)]
- Added ability to modify DTMF method in GWN7062ET. [[Phone Settings](#)]
- Added the ability to configure the minimum RSSI level for the bands. [[Professional Settings](#)]

Firmware Version 1.0.5.2

- Added support for User Management and Permission Templates. [[User Management](#)]
- Added WAN IPv4 address display on the Network Map → Internet icon. [[Network Map](#)]
- Added Security Mode and WPA Mode on the Network Map → Wi-Fi tab. [[Network Map](#)]
- Added “Disabled” and “Connected to the Internet” status for the port on the Network Map → Port tab. [[Network Map](#)]
- Optimized Mesh Nodes topology with an interactive diagram, manual parent node selection, and Exception Logs. [[Network Map](#)]
- Added an enable/disable switch for each WAN under QoS → WAN Bandwidth Settings. [[QoS](#)]
- Added client type icons for devices within the HomeCare → Parental Control list. [[HomeCare](#)]
- Added a “Go to Grandstream Home” link to access the official web portal. [[Management Platform](#)]
- Added a quick FXS configuration page for the primary router. [[FXS Settings](#)]
- Added display of WAN-side IPv4 and IPv6 addresses on the Overview page. [[Overview](#)]
- Added Security Mode and WPA Mode columns to the Wi-Fi summary on the Overview page. [[Overview](#)]The **ISP** feature on the GWN7062E/ET
- Added “Disabled” and “Connected to the Internet” status indicators for physical ports on the Overview page. [[Overview](#)]
- Added a “Parent Node” column to the Mesh node list on the Overview page. [[Overview](#)]Policy routes allow network administrators to define
- Added “Enable” and “Disable” functions for ports. [[Internet Settings](#)]
- Added a “DNS Service” selection list to choose an existing DNS service. [[Internet Settings](#)]
- Renamed “Dual WAN Policy” to “Internet Access Policy” and transitioned it to a dedicated tab. [[Internet Access Policy](#)]
- Added a “Failback” function for Failover mode to automatically switch back to the primary interface upon recovery. [[Internet Access Policy](#)]
- Added a list of DNS services, describing the currently supported DNS services. [[DNS Service](#)]
- Removed the previous “Multicast to Unicast” option. [[ISP](#)]
- Added IGMP functionality, allowing configuration of IGMP Proxy and IGMP Snooping. [[IGMP](#)]
- Added support for configuring Source Type and Destination Type within policy routes. [[Policy Routes](#)]
- Added support for adjusting the priority order of the policy routes list. [[Policy Routes](#)]
- Added separate **Security Mode**, **WPA Mode**, and **WPA Encryption Type** fields when adding or editing Wi-Fi networks. [[Wi-Fi](#)]
- Updated **Telephony** with new submenu structure, including **Basic Settings**, **FXS Settings**, **Template Settings**, and **Ringtone**. [[Telephony](#)]
- Added reusable **Telephony Template Settings** for FXS ports, including SIP settings, accessibility features, phone settings, and ringtone configuration. [[Telephony](#)]

- Added separate **Security Mode**, **WPA Mode**, and **WPA Encryption Type** fields when adding or editing Guest Wi-Fi networks. [[Guest Wi-Fi](#)]
- Updated **Professional Settings** behavior so shared roaming and client timeout options apply to both **2.4G** and **5G**, with separate **Minimum RSSI** controls for each band. [[Wi-Fi General Settings](#)]
- Added support for adding up to 16 Mesh nodes. [[Mesh](#)]
- Added Parent Node information and selection behavior for Mesh nodes, including automatic parent node selection, manual parent node selection, and wired connection mode restrictions. [[Mesh](#)]
- Added **Client Type** selection when modifying a client name. [[Modifying a Client Name](#)]
- Added an enable/disable switch for each WAN under QoS WAN Bandwidth Settings. [[QoS](#)]
- Added IP Exception page to exclude specific IP addresses, subnets, or ranges from Basic Security Defense detection. [[IP Exception](#)]
- Added ALG page for enabling FTP ALG, SIP ALG, and RTSP ALG protocol negotiation helpers. [[ALG](#)]
- Added WAN port status warning and DNS Service selection for WAN IPv6 configuration. [[WAN IPv6](#)]
- Updated the Upgrade page to show device node firmware versions and upgradeable device node selection when detecting a firmware version. [[Upgrade](#)]
- Moved the Log section from Maintenance to System. [[Log](#)]
- Added the **User** column to the Log table. [[Log](#)]
- Added support for up to **16** WAN-side allowed access IP addresses in Access Management. [[Access Management](#)]
- Updated Access Management by removing the Admin Password and User Account tabs and adding support for up to **16** WAN-side allowed access IP addresses. [[Access Management](#)]

Firmware Version 1.0.3.25

- No major changes.

Firmware Version 1.0.3.23

- Added Wi-Fi enable/disable toggle on the **Network Map** → **Wi-Fi** tab. [[Access WEB GUI](#)] [[Quick setup](#)]
- Added enable/disable option for default SSID on **Wi-Fi Settings** → **Wi-Fi** page. [[Default SSID](#)]
- Redesigned **Online Information** page under **HomeCare** → **Parental Control** (per-client time & traffic statistics for Today / Yesterday / Last 7 Days). [[Parental Control](#)]
- Updated **System Info** page label from **Software Version** to **Firmware Version**. [[System Info](#)]
- Added **Professional Settings** profile for Wi-Fi / Guest Wi-Fi under **Wi-Fi Settings** → **General Settings** → **Professional Settings**. [[Professional Settings](#)]
- Added **Professional Settings (General / Custom)** option on **Wi-Fi Settings** → **Wi-Fi** and **Wi-Fi Settings** → **Guest Wi-Fi** pages. [[Guest Wi-Fi](#)] [[Wi-Fi](#)]
- Added **Channel Configuration** under **Wi-Fi Settings** → **General Settings** → **Common Settings** (available when Country/Region is set to USA or Canada). [[Chaneel Configuration](#)]
- Updated **System** → **Access Management** → **Access Control: IP Addresses Allowed to be Accessed** is now optional (empty = no restriction; specified IPs only = restricted access). [[IP Addresses Allowed to be Accessed](#)]
- Added the WAN Speed Test feature on GDMS. [[GDMS Networking](#)]
- Added the ability to provision the device via HTTP. [[GDMS Networking](#)]
- Disabled UNII-4 channels (including 169, 173, and 177) by default. [[Wi-Fi General Settings](#)]
- Added the ability to configure FXS when GWN7062ET is MESH RE. [[FXS Settings](#)]

Firmware Version 1.0.3.10

- No major changes.

Firmware Version 1.0.3.7

- Added support for Guest Wi-Fi. [[Guest Wi-Fi](#)]
- Added router service ports. [[Service Ports](#)]
- Updated LED indicators: solid blue and solid yellow behaviors added, flashing pink behavior revised. [[LED Indicators](#)]
- Updated web GUI login page. [[Access WEB GUI](#)]

- Updated Mesh configuration flow. [[Mesh](#)]
- Added Safe Search under HomeCare. [[SafeSearch](#)]
- Renamed “Cloud” section to “Management Platform” and added Grandstream Home. [[Management Platform](#)]
- Added Security Version under System Info. [[System Info](#)]
- Renamed “Triple Play” to “ISP”. [[ISP](#)]
- Modified FXS Settings layout. [[FXS Settings](#)]
- Updated IPv6 configuration page. [[IPv6](#)]
- Added Working Mode section with Wireless Relay and Bridge modes. [[Working Mode](#)]
- Changed button name and function from “Block” to “Block internet”, and “Allow” to “Add time” under *HomeCare* → *Parental Control* page. [[Parental Control](#)]
- Added support for “IP Address Direct Dialing” to the “Telephony” -> “Basic Settings” page. [[Telephony](#)]
- Deleted the “Outgoing Call Without Registration” from “FXS Settings” page. [[FXS Settings](#)]
- Changed Wi-Fi “General settings” location and added more items. [[Wi-Fi General Settings](#)]
- Added a text hint under WAN settings when the WAN is enabled: “To configure VLAN, go to [Internet settings ISP] and select corresponding working mode”. [[Internet Settings](#)]

Firmware Version 1.0.1.13

- Added support for Wi-Fi 5 compatibility mode option. [[Wi-Fi 5 Compatible](#)]
- Added configuration option for Wi-Fi radio transmit power. [[Wi-Fi 5 Compatible](#)]
- Added support for enforcing 802.1Q VLAN tagging through ISP Locking on GDMS Networking. [[GDMS Networking](#)]

Firmware Version 1.0.1.10

- No major changes.

Firmware Version 1.0.1.7

- This is the initial release.

All product names, logos, and brands mentioned in this document are the property of their respective owners. **Windows® is a registered trademark of Microsoft Corporation. iOS® is a registered trademark of Apple Inc. Android® is a registered trademark of Google LLC. Samsung® is a registered trademark of Samsung Electronics Co., Ltd.**