User Guide

Omada 5G Outdoor Gateway
(In IP Passthrough Mode)

CONTENTS

About This Guide

This User Guide provides information for managing Omada 5G Outdoor Gateway in the default IP Passthrough mode. Please read this guide carefully before operation.

By default, the IP Passthrough mode is enabled. If you disable IP Passthrough at Network > WAN > CellularWAN, the gateway will be switched to the Router mode. The functions available in the Router mode are different, and you can refer to the Omada Gateway_User Guide(New VI) at https://support.omadanetworks.com/document/ for detailed instructions.

Intended Readers

This Guide is intended for network managers familiar with IT concepts and network terminologies.

Conventions

When using this guide, notice that features available in Omada 5G Outdoor Gateway may vary by software version. Availability of Omada 5G Outdoor Gateway may also vary by region or ISP. All images, steps, and descriptions in this guide are only examples and may not reflect your actual experience.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied. Users must take full responsibility for their application of any products.

In this Guide, the following conventions are used:

- The symbol stands for Note. Notes contain suggestions or references that helps you make better use of your device.
- **Menu Name > Submenu Name > Tab** page indicates the menu structure. **Status > Traffic Statistics > Interface Statistics** means the Interface Statistics page under the Traffic Statistics menu option that is located under the Status menu.
- **Bold** font indicates a button, toolbar icon, menu or menu item.

More Information

- The latest software and documentations can be found at Download Center at https://support.omadanetworks.com/.
- The Installation Guide (IG) can be found where you find this guide or inside the package of the gateway.
- Specifications can be found on the product page at https://www.omadanetworks.com.
- Our Technical Support contact information can be found at the Contact Technical Support page at https://support.omadanetworks.com/.

Part 1

Accessing the Gateway

CHAPTERS

1 Determine the Management Method

Before building your network, choose a proper method to manage your gateway based on your actual network situation. The gateway supports two configuration options: Standalone Mode or Controller Mode.

- Controller Mode

If you want to configure and manage a large-scale network centrally, which consists of mass devices such as access points, switches, and gateways, Controller Mode is recommended. In Controller Mode, the gateway can be centrally configured and monitored via Omada SDN Controller.

To prepare the gateway for Omada SDN Controller Management, refer to Controller Settings. For detailed instructions about the network topology in such situations and how to use Omada SDN Controller, refer to the User Guide of Omada SDN Controller. The guide can be found on the download center of our official website: https://support.omadanetworks.com/document/.

- Standalone Mode

If you have a relatively small-sized network and only one or just a small number of devices need to be managed, Standalone Mode is recommended. In Standalone Mode, you can access and manage the gateway using the GUI (Graphical User Interface, also called web interface in this text). The gateway uses two built-in web servers, HTTP server and HTTPS server, for user authentication.

This User Guide introduces how to configure and monitor the gateway in Standalone Mode.

Note:

The GUI is inaccessible while the gateway is managed by a controller. To turn the gateway back to Standalone Mode and access its GUI, you can forget the gateway on the controller or reset the gateway.

2 Web Interface Access

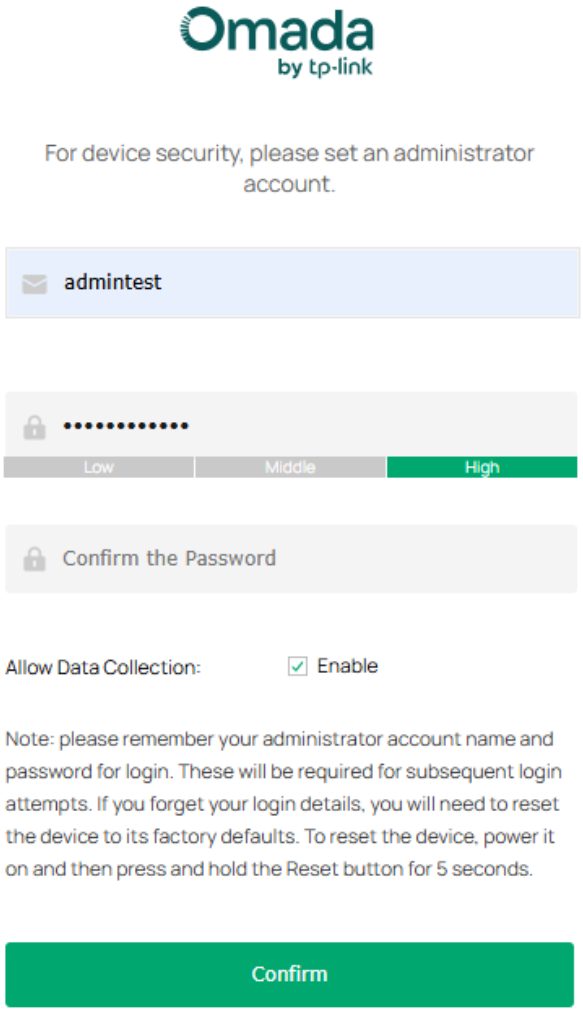
The following example shows how to log in via the web browser.

1) Connect to the gateway using the default SSID printed on the label at the bottom of the gateway or connect a PC to a LAN port of the gateway with an RJ45 port properly. If your computer is configured with a fixed IP address, change it to “Obtain an IP address automatically“.
2) Open a web browser and type https://mobile.omada.net in the address field of the browser, then press the Enter key.

Figure 2-1 Enter the gateway's Domain Name in the Browser

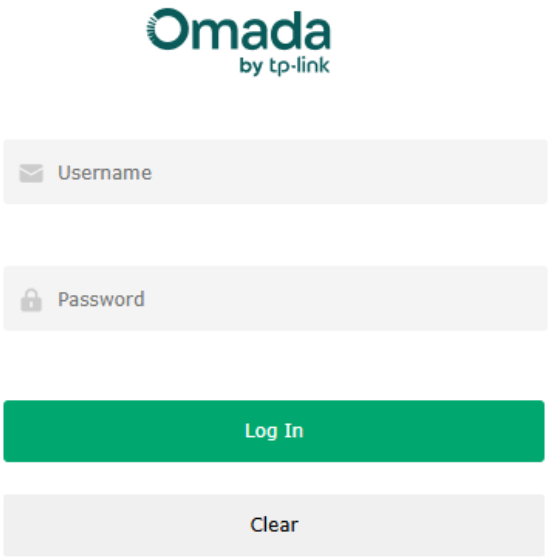
3) Create a username and a password for subsequent login attempts.

Figure 2-2 Create a Username and a Password



4) Use the username and password set above to log in to the webpage.

Figure 2-3 Login Authentication



5) After a successful login, the main page will appear, and you can configure the function by clicking the setup menu on the left side of the screen.

Part 2

Viewing Status Information

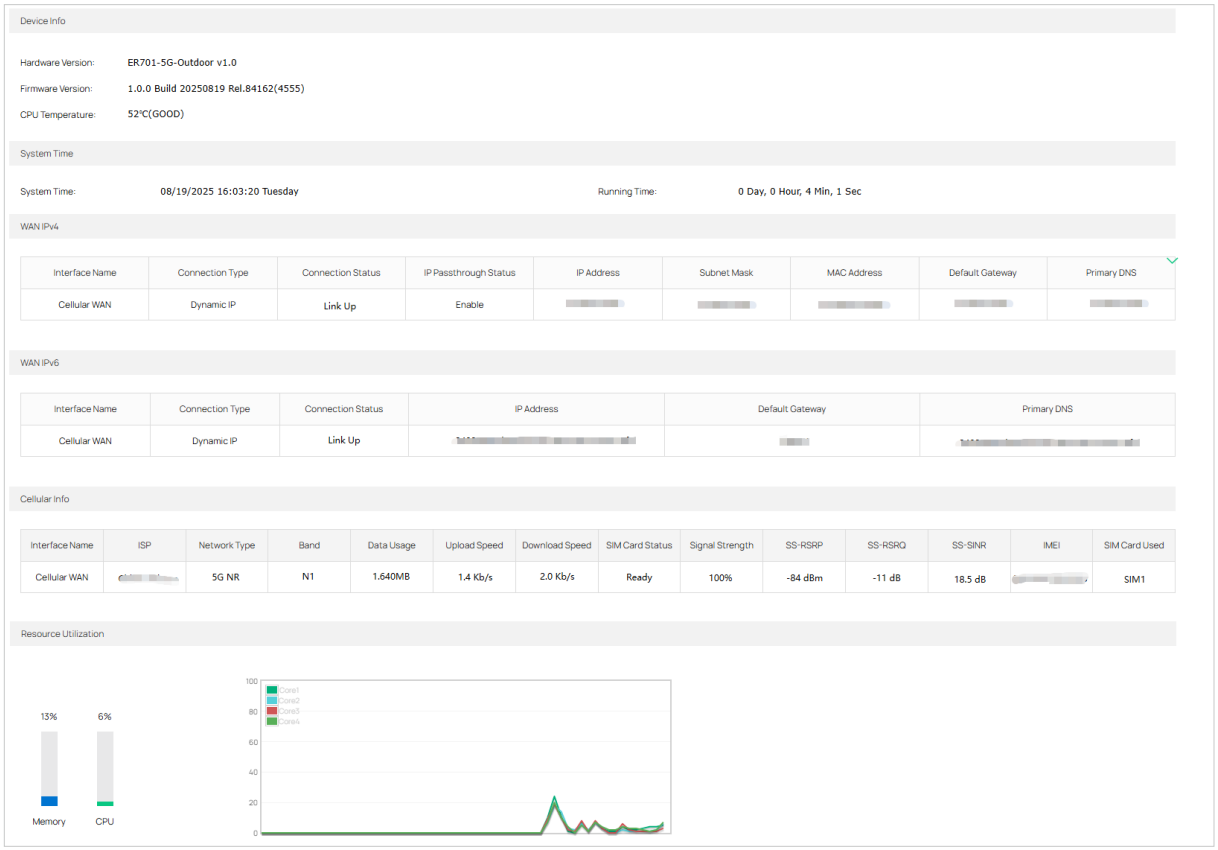
CHAPTERS

1 System Status

The System Status page displays the basic system information (like the hardware version, firmware version and system time) and the running information (like the WAN interface status, cellular info, memory utilization and CPU utilization). This page may vary depending on your model.

Choose the menu **Status > System Status > System Status** to load the following page.

Figure 1-1 System Status



2 Cellular Info

Cellular Info displays detailed cellular information including the Module Information, SIM Status, IP Passthrough Enable, Cellular Status and Service Information, and the signal information table .

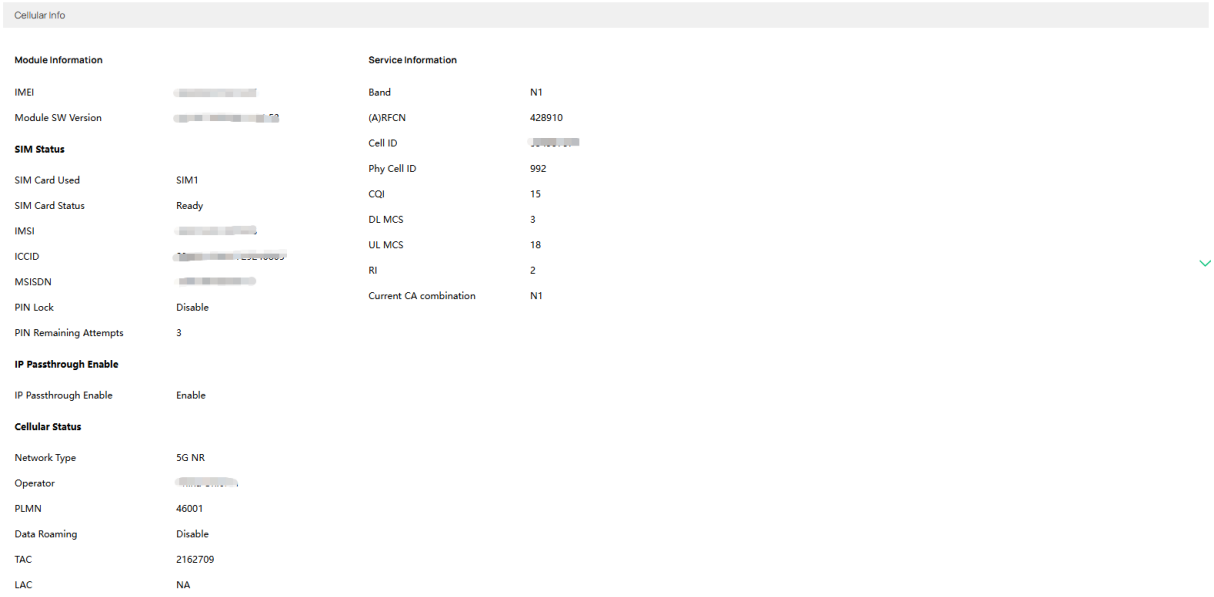
With the Cellular Info function, you can:

- View the cellular information.
- View the signal information.

2.1 Viewing the Cellular Information

Choose the menu **Status > Cellular Info** to load the following page. In the Cellular Info section, you can view the following parameters.

Figure 2-1 Celluar Info



IMEI	Displays the International Mobile Equipment Identity of this device.
Module SW Version	Displays the software version of the cellular network module.
SIM Card Used	Displays the SIM card currently in use.
SIM Card Status	Displays the status of the SIM card.
IMSI	International Mobile Subscriber Identity. An IMSI is a number that identifies a cellphone plan subscriber. Usually stored on SIM card.

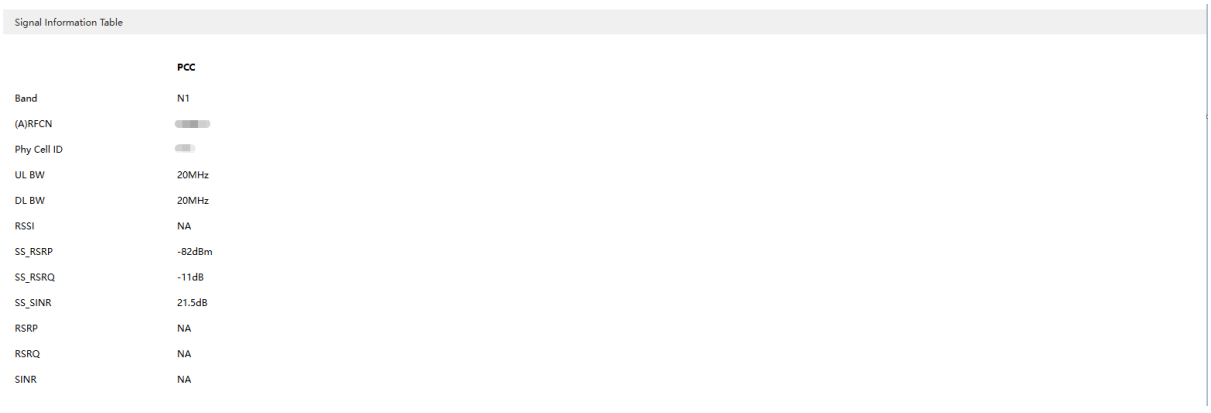
ICCID	Integrated Circuit Card ID, a globally unique serial number that identifies the SIM card. It is a 19 or 20-digit number usually printed on the back of the SIM card.
MSISDN	Mobile Station Integrated Services Digital Network. It is the phone number which identifies a device during calls or data sessions.
PIN Lock	A PIN (Personal Identification Number) code is a key to a SIM card. Without the PIN code, you cannot use the SIM card. It displays Enable if the service provider requires you to enter a PIN to use the SIM card. It displays Disable if the service provider lets you use the SIM without inputting a PIN, or you disable PIN Lock in Network > Cellular > PIN Management.
PIN Remaining Attempts	Displays the number of attempts remaining to enter your PIN before your ISP blocks your SIM card.
IP Passthrough Enable	Displays whether the IP Passthrough mode is enabled. You can go to Network > WAN > Cellular WAN > IP Passthrough Management to configure the settings.
Cellular Status	Displays the status of the cellular Internet connection.
Network Type	Displays the type of the mobile network to which this device is connecting.
Operator	Displays the name of the service provider.
PLMN	Displays the PLMN (Public Land Mobile Network) number.
Data Roaming	Displays if data roaming is enabled on this device. Data roaming lets you use your device in an area which is not covered by your service provider. Enable data roaming to keep your device connected to the internet when you are traveling outside the geographical coverage area of the network to which you are registered.
TAC	Tracking Area Code, the TAC of the current cell.
LAC	Location Area Code (LAC), which identifies a location area within a PLMN.
Band	Displays the band the network is working on.
(A)RFCN	This displays the Radio Frequency Channel Number of DL carrier frequency used by the mobile network to which this device is connected. For WCDMA, it indicates the UARFCN (UTRA Absolute Radio-Frequency Channel Number). For LTE, it indicates the EARFCN (E-UTRA Absolute Radio-Frequency Channel Number). For 5G, it indicates the NR-ARFCN (New Radio Absolute Radio-Frequency Channel Number).
Cell ID	Cell Identifier, the Cell ID of the current cell.
Phy Cell ID	Physical Cell Identifier, PCI of the current cell.
CQI	Channel Quality Indication, an indicator conveying the data on communication channel quality.

DL MCS	Downlink MCS(Modulation and Coding Scheme). A higher MCS means higher transmission efficiency, which is related to network signal quality.
UL MCS	Uplink MCS(Modulation and Coding Scheme). A higher MCS means higher transmission efficiency, which is related to network signal quality.
RI	Displays the Rank Indication, one of the control information that a UE will report to eNodeB (Evolved Node-B) on either PUCCH (Physical Uplink Control Channel) or PUSCH (Physical Uplink Shared Channel) based on uplink scheduling.
Current CA combination	Displays the combination of CA.

2.2 Viewing the Signal Information

Choose the menu **Status > Cellular Info** to load the following page. In the Signal Information Table section, you can view the following parameters.

Figure 2-2 Signal Information Table



Band	Displays the band the network is working on.
(A)RFCN	This displays the Radio Frequency Channel Number of DL carrier frequency used by the mobile network to which this device is connected. For WCDMA, it indicates the UARFCN (UTRA Absolute Radio-Frequency Channel Number). For LTE, it indicates the EARFCN (E-UTRA Absolute Radio-Frequency Channel Number). For 5G, it indicates the NR-ARFCN (New Radio Absolute Radio-Frequency Channel Number).
Phy Cell ID	Physical Cell Identifier, PCI of the current cell.

UL BW	Uplink Bandwidth, the bandwidth which is used for transmission of signals from the device to the base station.
DL BW	Downlink Bandwidth, the bandwidth which is used for transmission of signals from the base station to the device.
RSSI	The strength of the cellular signal between an associated cellular station and this device.
RSRP	The current RSRP (Reference Signals Received Power) value. It is a measurement of the received power level in an LTE cell network.
RSRQ	The current RSRQ (Reference Signal Receiving Quality) value. It is a measurement of the received quality.
SINR	The Signal to Interference plus Noise Ratio (SINR) in dB. It is also a measurement of signal quality and is used by the UE (User Equipment) to calculate the Channel Quality Indicator (CQI) that it reports to the network. A negative value means more noise than signal.
SS_RSRP	SS reference signal received power. It is a measurement of the received power level in a NR cell network.
SS_RSRQ	SS reference signal received quality. It is a measurement of the received quality in a NR cell network.
SS_SINR	SS Signal to Interference and Noise Ratio.

3 Traffic Statistics

Traffic Statistics displays detailed information relating to the data traffic of interfaces and IP addresses. You can monitor the traffic and locate faults according to this information.

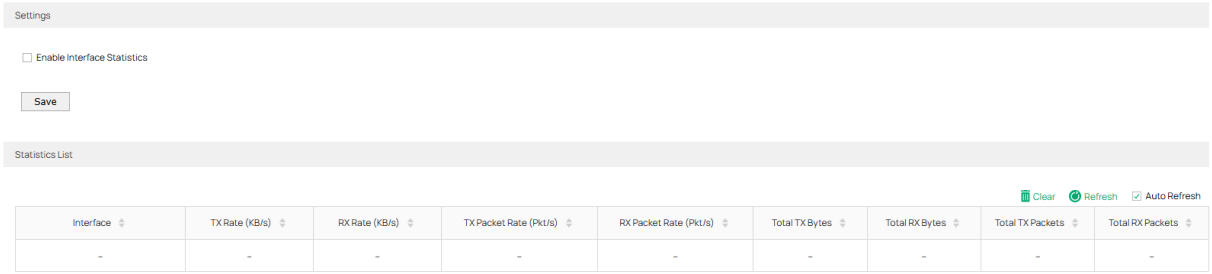
With the Traffic Statistics function, you can:

- View the traffic statistics on each interface.
- Specify an IP address range, and view the traffic statistics of the IP addresses in this range.

3.1 Viewing the Interface Statistics

Choose the menu **Status > Traffic Statistics > Interface Statistics** to load the following page.

Figure 3-1 Interface Statistics



Enable **Interface Statistics**, then you can view the detailed traffic information of each interface in the statistics list.

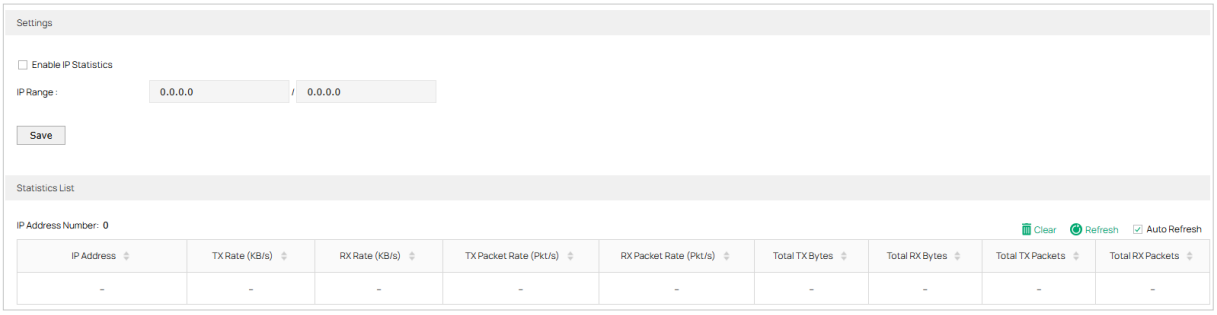
TX Rate (KB/s)	Displays the rate for transmitting data in kilobytes per second.
RX Rate (KB/s)	Displays the rate for receiving data in kilobytes per second.
TX Packet Rate (Pkt/s)	Displays the rate for transmitting data in packets per second.
RX Packet Rate (Pkt/s)	Displays the rate for receiving data in packets per second.
Total TX Bytes	Displays the bytes of packets transmitted on the interface.
Total RX Bytes	Displays the bytes of packets received on the interface.
Total TX Packets	Displays the number of packets transmitted on the interface.
Total RX Packets	Displays the number of packets received on the interface.

You can enable **Auto Refresh** or click **Refresh** to get the latest statistics information, or click **Clear** to clear the current statistics information.

3.2 Viewing the IP Statistics

Choose the menu **Status > Traffic Statistics > IP Statistics** to load the following page.

Figure 3-2 IP Statistics



Follow these steps to view the traffic statistics of the specific IP addresses:

1) In the **Settings** section, enable IP Statistics and specify an IP range to monitor.

Enable IP Statistics	Check the box to enable IP Statistics.
IP Range	Specify an IP range. The gateway will monitor the packets whose source IP addresses or destination IP addresses are in this range, and display the statistics information in Statistics List.

2) In the **Statistics List** section, view the detailed traffic information of the IP addresses.

IP Address Number	Displays the number of active users whose IP address is in the specified IP range.
TX Rate (KB/s)	Displays the rate for transmitting data in kilobytes per second.
RX Rate (KB/s)	Displays the rate for receiving data in kilobytes per second.
TX Packet Rate (Pkt/s)	Displays the rate for transmitting data in packets per second.
RX Packet Rate (Pkt/s)	Displays the rate for receiving data in packets per second.
Total TX Bytes	Displays the bytes of packets transmitted by the user who owns the IP address.
Total RX Bytes	Displays the bytes of packets received by the user who owns the IP address.

You can enable **Auto Refresh** or click **Refresh** to get the latest statistics information, or click **Clear** to clear the current statistics information.

Part 3

Configuring Wireless Settings

CHAPTERS

1 Overview

The Wireless module provides basic wireless functions, including checking wireless connection details, and configuring wireless parameters .

1.1 Supported Features

Status

You can check the parameters of the gateway's wireless network (radio settings) and the details about the connected clients.

Wireless Settings

Wireless networks enable wireless clients to access the internet. Once a wireless network is set up, the gateway typically broadcast the network name (SSID) in the air, and wireless clients can connect to the network and access the internet. In this module, you can configure wireless settings, and configure MAC filtering.

2 Wireless Status

You can check the parameters of the gateway's wireless network (radio settings) and the details about the connected clients.

2.1 View Gateway's Wireless Settings

Choose the menu **Wireless** > **Status** > **Wireless** to load the following page.

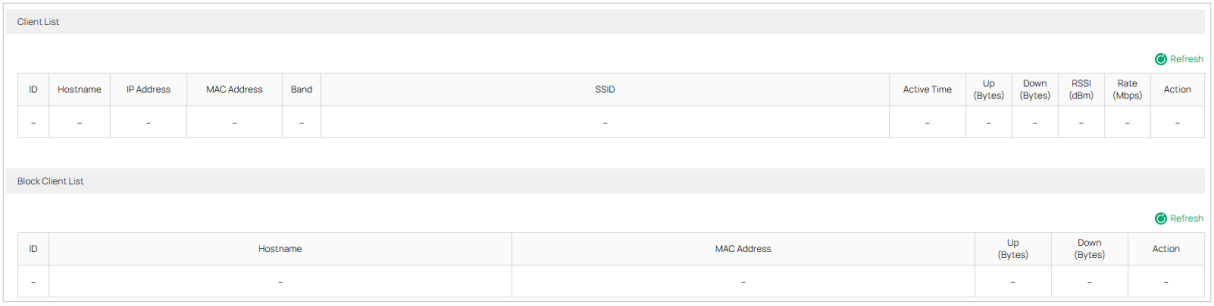
Figure 2-1 Viewing the Wirelesss Settings

2.4GHz Wireless Radio	Displays whether the wireless function is enabled on the radio band.
Channel Frequency	Displays the channel and frequency which are currently used by the gateway.
Channel Width	Displays the channel width which is currently used by the gateway.
IEEE802.11 Mode:	Displays the IEEE802.11 protocol currently used by the gateway.
Max TX Rate	Displays the maximum physical rate of the gateway.
Tx Power	Displays the transmit power of the gateway.

2.2 View Client Details

Choose the menu **Wireless** > **Status** > **Client** to load the following page.

Figure 2-2 Viewing Client Details



Client List	Click User	Guest to select the client type (User or Guest), and view the following parameters. Click Refresh to get the latest status of the Client List.
Block Client List	Allows you to view the information of the clients that have been blocked, and resume the client's access. Click Refresh to get the latest status of the Block Client List.

3 Wireless Settings

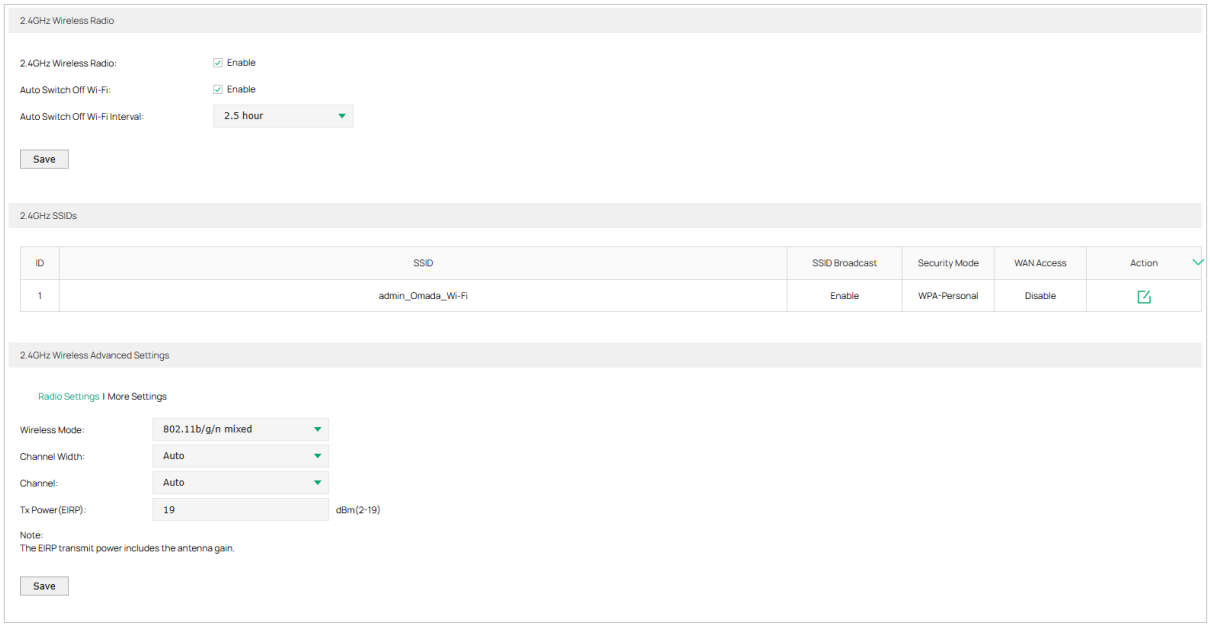
Wireless networks enable wireless clients to access the internet. Once a wireless network is set up, the gateway typically broadcast the network name (SSID) in the air, and wireless clients can connect to the network. In this module, you can configure wireless settings, and configure MAC filtering.

3.1 Wireless Settings Access

Wireless Settings Access allows you to view and edit the information of the wireless networks, and configure the wireless networks' advanced settings, such as Radio Settings.

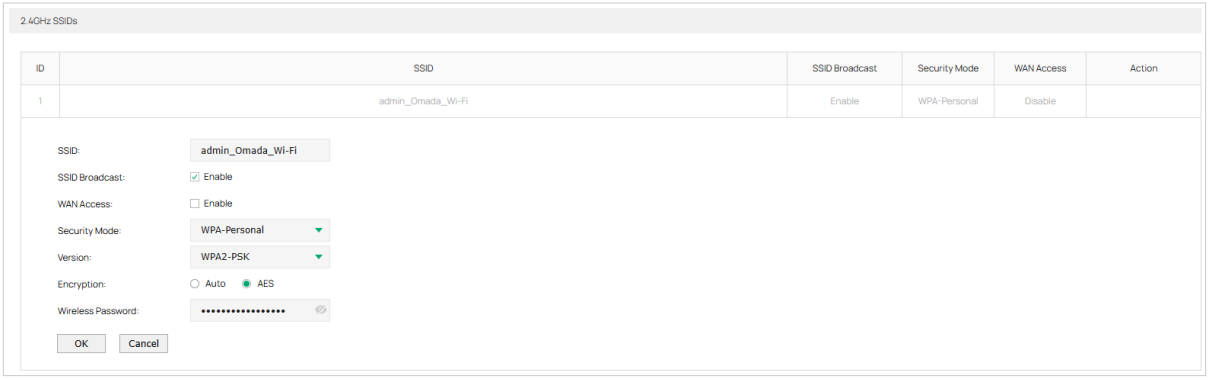
Choose the menu **Wireless** > **Wireless Settings** > **Wireless Settings Access** to load the following page and configure the following parameters.

Figure 3-1 Configuring the Wireless Settings Access



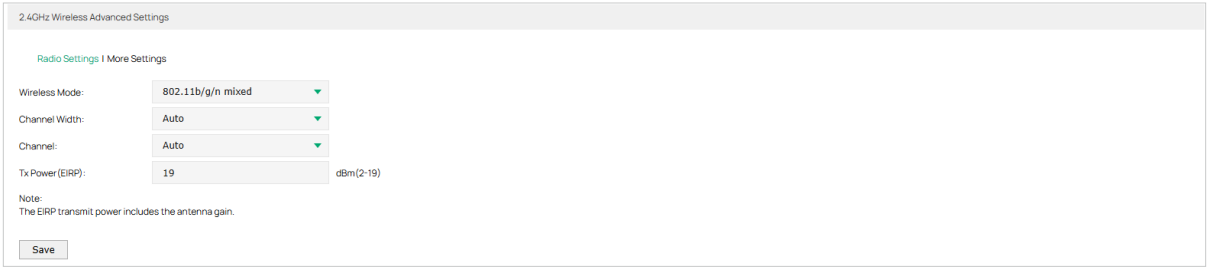
2.4GHz Wireless Radio	Check the box to enable the 2.4GHz wireless radio before configuring the wireless parameters. Only when this option is enabled will the wireless radio on 2.4GHz works.
Auto Switch Off Wi-Fi	Check the box and set the **Auto Switch Off Wi-Fi Interval**, the wireless network will automatically turn off after the set time.
Auto Switch Off Wi-Fi Interval	Select the time interval for the 2.4G radio to automatically turn off. Options include: 1h, 2.5h, 4h.

In the 2.4GHz SSIDs section, click the Edit icon in the Action column to modify the following parameters.



SSID	Specify the network name (SSID) to identify the wireless network. The wireless clients choose the SSID on their WLAN settings page to connect to the wireless network.
SSID Broadcast	When enabled, the gateway broadcast the SSID in the air, and the SSID will appear in the list of available wireless networks. When disabled, users must enter the SSID manually to connect to the wireless network.
WAN Access	When enabled, clients connected to the SSID can access the internet.
Security Mode	Select the encryption method for the wireless network based on needs. **None:** With None selected, the clients can access the wireless network without authentication, which is suitable for scenarios with lower security requirements. **WPA-Personal:** WPA-Personal is based on a pre-shared key. It is characterized by high safety and simple settings, so it is mostly used by common households and small businesses.
Version	If the Security Mode is set to WPA-Personal, select the WPA version (WPA/WPA2-PSK, WPA-PSK, and WPA2-PSK), and then configure the encryption type and wireles password.
Encryption	Select the WPA encryption type. **Auto:** The gateway automatically determines the encryption type during authentication. **AES:** AES stands for Advanced Encryption Standard.
Wireless Password	Specify a password for the clients to connect to the wireless network.

Go to the 2.4GHz Wireless Advanced Settings to configure Radio Settings and More Settings.



■ Radio Settings

Radio settings directly control the behavior of the radio in the gateway and its interaction with the physical medium; that is, how and what type of signal the gateway emits. Configure the following parameters, and click **Save**.

Wireless Mode	Select the IEEE 802.11 mode the radio uses. **802.11n only:** Only 802.11n clients can connect to the gateway. **802.11b/g mixed:** Both 802.11b and 802.11g clients can connect to the gateway. **802.11b/g/n mixed:** All of 802.11b, 802.11g, and 802.11n clients operating in the 2.4GHz frequency can connect to the gateway.
Channel Width	Select the channel width of the gateway. Available options include **Auto**, **20MHz**, and **40MHz**.
Channel	Select the channel used by the gateway. For example, 1/2412MHz means that the channel is 1 and the frequency is 2412MHz. By default, the channel is selected as **Auto**, and we recommend that you keep the default setting.
Tx Power (EIRP)	Specify the transmit power value. If this value is set to be larger than the maximum transmit power that is allowed by the local regulation, the regulated maximum transmit power will be applied in the actual situation.

Note:
In most cases, it is unnecessary to use the maximum transmit power. Specifying a larger transmit power than needed may cause interference to the neighborhood. Also, it consumes more power and reduces the longevity of the device.

■ More Settings

To improve the network's stability, reliability, and communication efficiency, configure the following parameters based on your needs. Configure the following parameters, and click **Save**.

Beacon Interval	Beacons are transmitted periodically by the gateway to announce the presence of a wireless network for the clients. **Beacon Interval** determines the time interval of the beacons sent by the gateway. You can specify a value between 40 and 100ms. The default is 100ms.

DTIM Period	The DTIM (Delivery Traffic Indication Message) is contained in some Beacon frames. It indicates whether the gateway has buffered data for client devices. The **DTIM Period** indicates how often the clients served by this gateway should check for buffered data still on the gateway awaiting pickup. You can specify the value between 1-255 Beacon Intervals. The default value is 1, indicating that clients check for buffered data at every beacon. An excessive DTIM interval may reduce the performance of multicast applications, so we recommend you keep the default value.
RTS Threshold	RTS/CTS (Request to Send/Clear to Send) is used to improve the data transmission efficiency of the network with hidden nodes, especially when there are lots of large packets to be transmitted. When the size of a data packet is larger than the **RTS Threshold**, the RTS/CTS mechanism will be activated. As a result, before sending a data packet, the client will send an RTS packet to the gateway to request data transmitting. And then the gateway will send a CTS packet to inform other clients to delay their data transmitting. In this way, packet collisions can be avoided. For a busy network with hidden nodes, a low threshold value will help reduce interference and packet collisions. But for a not-so-busy network, a too low threshold value will cause bandwidth wasting and reduce the data throughput. The recommended and default value is 2347 bytes.
Fragmentation Threshold	The fragmentation function can limit the size of packets transmitted over the network. If the size of a packet exceeds the **Fragmentation Threshold**, the fragmentation function is activated and the packet will be fragmented into several packets. Fragmentation helps improve network performance if properly configured. However, a too low fragmentation threshold may result in poor wireless performance caused by the extra work of dividing up and reassembling of frames and increased message traffic. The recommended and default value is 2346 bytes.

3.2 MAC Filtering

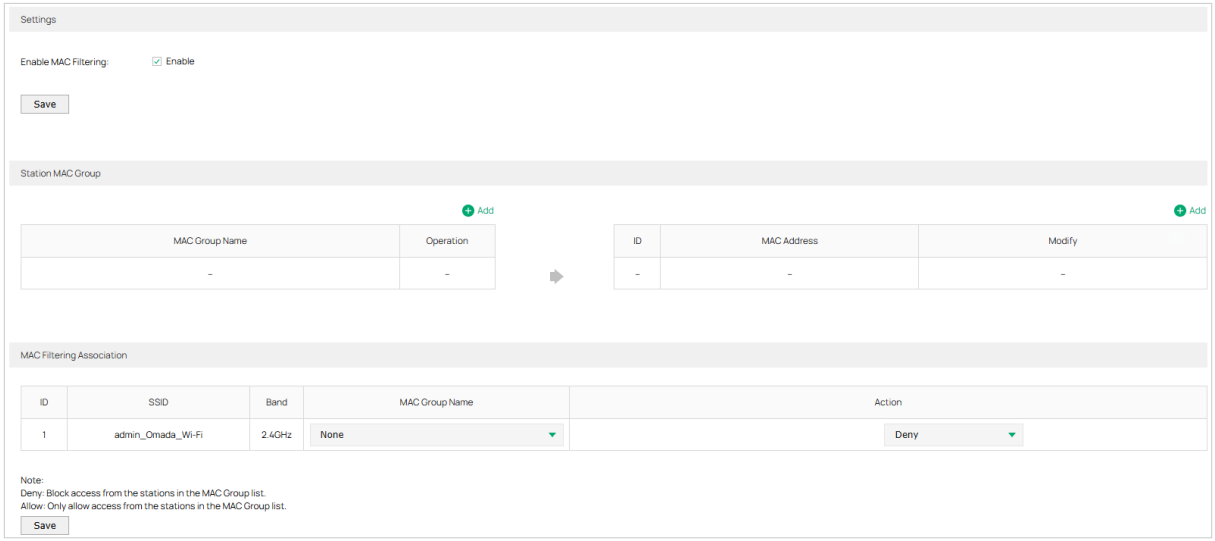
MAC Filtering is used to allow or block clients with specific MAC addresses to access the network. With this feature, you can effectively control clients' access to the wireless network according to your needs.

To complete MAC filtering settings, follow these steps:

1) In **Settings**, check the box of **Enable MAC Filtering**.
2) In **Station MAC Group**, click **Create Groups**, create a new MAC group, and add the MAC address of the hosts to be filtered to the MAC group.
3) In **MAC Filtering Association**, configure the filtering rule

Choose the menu **Wireless** > **Wireless Settings** > **MAC Filtering** to load the following page.

Figure 3-2 Configuring MAC Filtering



In **Settings** section, Check the box to enable **MAC Filtering,** and click **Save.**

In **Station MAC Group** section, click **Create Groups**, and two boxes will appear, which allow you to create a MAC group first, and add the MAC addresses to the MAC group.

Add (above the Operation column)	Click **Add** to create a new MAC group. Click to select a group to move the arrow to point the other box to add MAC addresses.
MAC Group	Specify a name for the MAC Group, and click **OK**.
MAC Group Name	Displays all the MAC groups you have created.
Add (above the Modify column)	Click to add MAC address to the specific group.
MAC Address	Enter the MAC address to be filtered in the format XX-XX-XX-XX-XX-XX, and OK. In the same way, you can add more MAC addresses to the selected MAC group. And you can also view all the added MAC addresses here.
Modify	Edit or delete the selected MAC address.

In **MAC Filtering Association** section, specify the filtering rule, then click **Save**.

SSID	Displays the SSIDs that you can set the filtering rule.
Band	Displays the SSIDs that you can set the filtering rule.
MAC Group Name	Select a MAC group to be filtered from the drop-down list.
Action	Specify the filtering rule (Allow/Deny) for the selected MAC group from the drop-down list, and click **Save.**

Part 4

Configuring Network

CHAPTERS

1 Overview

The Network module provides basic gateway functions, including WAN connection, DHCP service, VLAN and more.

1.1 Supported Features

WAN

WAN ports connect to the internet. You can configure the WAN port for your network.

Cellular

You can upgrade the ISP information, configure the PIN code and data settings.

LAN

When the LAN ports of the gateway connect to your local network devices, the gateway functions as the gateway, which allows those devices to connect to the internet.

MAC

You can change the default MAC address of the WAN port according to your needs.

Switch

The gateway supports some basic switch port management functions, like Flow Control and Port Negotiation, to help you monitor the traffic and manage the network effectively.

VLAN

VLAN enables you to divide the LAN into multiple logical networks and control the traffic among them in a convenient and flexible way. The LAN can be logically segmented by departments, application, or types of users, without regard to geographic locations.

IPv6

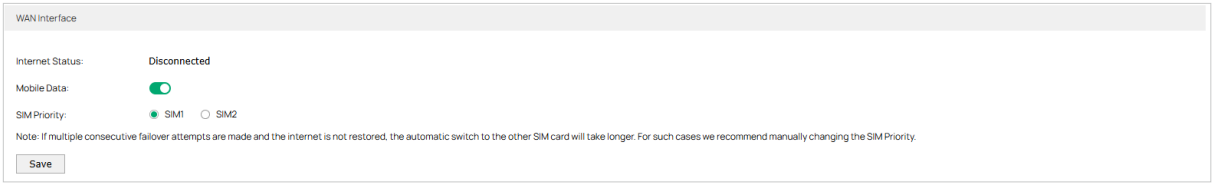
IPv6 is the next-generation network protocol following IPv4. You can configure IPv6 network for the gateway if your ISP supports IPv6. IPv6 network won't cause conflict with your current IPv4 network.

2 WAN Configuration

WAN ports connect to the internet. By default, the gateway is using cellular WAN. You can enable mobile data, configure the SIM priority and SIM card settings.

2.1 Configuring the WAN Interface

Choose the menu **Network** > **WAN** > **Cellular WAN** to load the following page. In the **WAN Interface** section, configure the following parameters.



Internet Status	Displays whether the gateway is connected to the internet.
Mobile Data	It is enabled by default. You can disable it to block internet access.
SIM Priority	Set which SIM card is used first. SIM Priority takes effect only when the device is powered on and the priority is changed. If only one SIM card is inserted, this card is used by default.

Note:

If multiple consecutive failover attempts are made and the internet is not restored, the automatic switch to the other SIM card will take longer. For such cases we recommend manually changing the SIM Priority.

2.2 Configuring the IP Passthrough Management

Choose the menu **Network** > **WAN** > **Cellular WAN** to load the following page. In the **IP Passthrough Management** section, configure the following parameters.

Note:

By default, the IP Passthrough mode is enabled. If you disable IP Passthrough, the gateway will be switched to the Router mode. The functions available in the Router mode are different, and you can refer to the Omada Gateway_User Guide(New VI) at https://support.omadanetworks.com/document/ for detailed instructions.

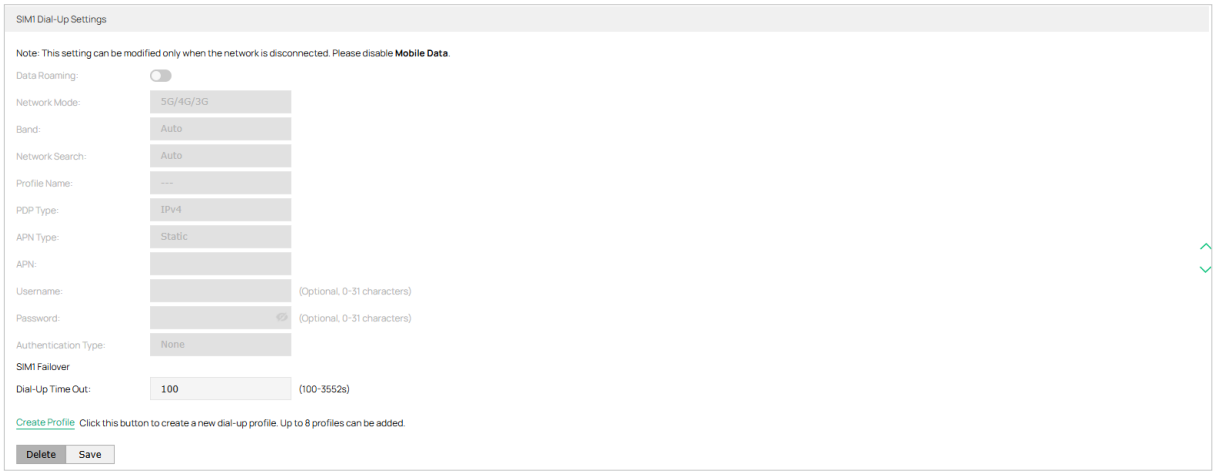
IP Passthrough	IP Passthrough allows a LAN computer on the local network of the gateway to have access to web services using the public IP address. When IP Passthrough is configured, all traffic is forwarded to the LAN computer and will not go through NAT. It is enabled by default. Changing the IP Passthrough settings may affect the network setting of client devices.
IP Passthrough Mode	**Dynamic:** Select this mode to allow traffic to be forwarded to the first LAN computer on the local network of the gateway. **Fixed:** Select this mode to specify a computer (for example, Client A) by entering its MAC address in the **To Fixed MAC field**.

2.3 Configuring the SIM Dial-Up Settings

In the **Dial-up Settings** section, enter the corresponding parameters for SIM1 and SIM2, and then click **Save**. This settings can be modified only when the network is disconnected. Disable Mobile Data before configuring the following parameters.

Note:

If you are not familiar with this, keep the default option or contact your carrier for more details.



Data Roaming	It is disabled by default. If disabled, data service usage is not allowed while roaming. If enabled, data service is allowed while roaming, but significant roaming charges may apply.
Network Mode	You can choose a network mode according to your mobile network standard and current network conditions. The following modes are supported, 5G/4G/3G, 5G-SA, 5G-NSA/4G, 4G/3G, 4G Only, and 3G Only.
Band	Select the band selection type as you need. **Auto:** The device will automatically choose available cellular frequency bands nearby based on advanced band selection algorithms. **Manual:** The device will automatically search for available cellular frequency bands. Then you can select specific bands as needed.

Create Profile	Click to create a new dial-up profile. Up to 8 profiles can be added.
Network Search	Select the network connection type as you need. **Auto:** The device will automatically establish connection once it's started. **Manual:** When you select Manual and click Search, the device will search for mobile networks automatically and you can choose a network with better performance to access, which is related or have corporation with the network provider of your SIM.
Profile Name	The name of the profile you've selected.
PDP Type	Select the type of your PDP (Packet Data Protocol). PDP Type is the type of the IP address assigned to the PDP during 'PDP context activation' procedure. You can select IPv4, or IPv6, or IPv4&IPv6.
APN	Access Point Name, provided by your ISP. You need to set APN only after selecting the static APN type. You are recommended to keep the default value.
Username/ Password	Enter the username and password provided by your ISP. These fields are case-sensitive. You are recommended to keep the default value.
Authentication Type	Some ISPs need a specific authentication type, confirm it with your ISP or keep the default value. **None:** No authentication is required. **PAP:** Password Authentication Protocol. The protocol allows a device to establish authentication with a peer using a two-way handshake. Select this option if your ISP requires this authentication type. **CHAP:** Challenge Handshake Authentication Protocol. The protocol allows a device to establish authentication with a peer using a three-way handshake and periodically checking the peer's identity. Select this option if your ISP requires this authentication type.
SIM1/SIM2 Failover Dial-Up Time Out	Set the dial-up timeout (100 to 3552 seconds). If the connection is not successfully established within the specified time, the gateway will use the other SIM card to connect to the internet.

3 Cellular Configuration

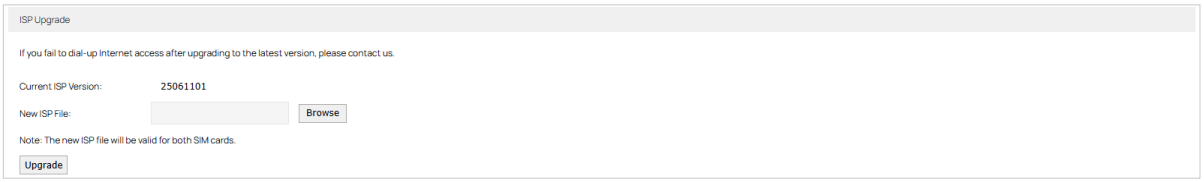
Configure the cellular related parameters for your network.

- Configure the ISP Upgrade.
- Configure the PIN Management.
- Configure the Data Settings

3.1 Configuring the ISP Upgrade

Choose the menu **Network** > **Cellular** > **ISP Upgrade** to load the following page.

Figure 3-1 Configuring the ISP Upgrade



Follow the steps to upgrade ISP information

1) Download the latest ISP upgrade file from the Support page at www.omadanetworks.com to your computer.
2) Click **Browse** to locate and select the latest file.
3) Click **Upgrade**.

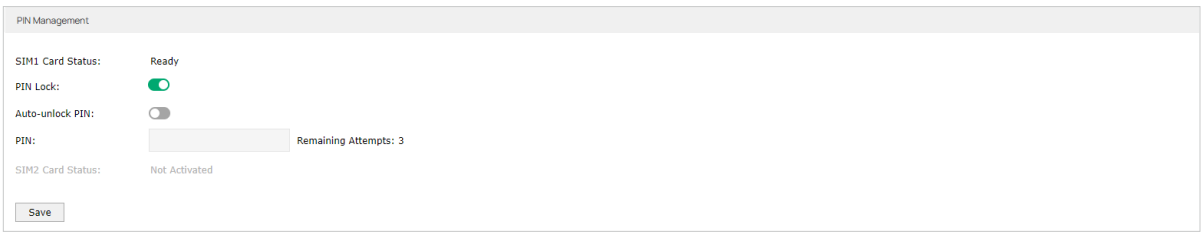
3.2 Configuring the PIN Management

Choose the menu **Network** > **Cellular** > **PIN Management** to load the following page and configure the following parameters.

Note:

In this module, you can enter the PIN to unlock the active SIM card, and preset a PIN for the inactive card.

Figure 3-2 Configuring the PIN Management



SIM Card Status	Displays the status of your SIM card.
PIN Lock	You can select whether to enable this function or not. Once the PIN Lock function is enabled, every time you start the device with this SIM card inserted, you need to enter the PIN code. However, you can enable the Auto-unlock PIN function to avoid this hassle..
Auto-unlock PIN	When the PIN code is required upon device restarting, it will be validated automatically once. If validation failed, you need to enter the PIN code on the PIN Management page.
PIN	Personal Identification Number of the SIM card. It consists of 4-8 digits.
PUK	PIN Unlocked Key. It consists of 8 digits.
Remaining Attempts	Displays how many attempts are left for you to try entering the PIN or PUK code. You have 3 attempts at most for entering the PIN code and 10 attempts at most for entering the PUK code.

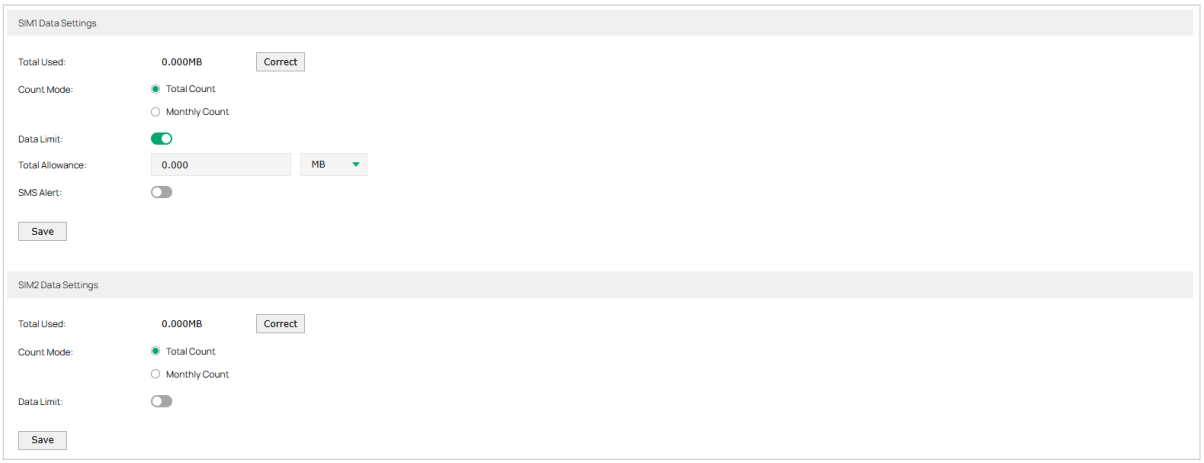
3.3 Configuring the Data Settings

You can view the data statistics and set a data limit to better control your data usage so that you will not exceed the data package provided by your carrier.

The data usage is for reference only, and the specific data shall be subject to the operator.

Choose the menu **Network** > **Cellular** > **Data Settings** to load the following page.

Figure 3-3 Configuring the Data Settings



Select a SIM card and follow the steps below to set the data limit:

1) Toggle on **Data Limit**.
2) Enter the total allowance provided by your carrier. When your data usage reaches the allowance, the device will automatically disconnect from the internet.
3) Enter the usage alert percentage. When your data usage reaches this proportion of the total allowance, you will receive a message.
4) Enter the phone number via which you will receive the alert message. You will also receive a message if the device automatically disconnects from the internet when your data usage reaches the allowance.

5) Toggle on **Monthly Count** and enter the start date if you want to view the monthly data used and set a monthly data limit.

6) Click **Save**.

Parameters

Monthly Used/ Total Used	Displays the total traffic/monthly traffic used according to the set traffic billing method.
Correct	Correct the traffic used (according to the billing method, total traffic/monthly traffic).
Count Mode	Select the count mode, total count or monthly count. Monthly count needs to select start date for each monthly count cycle.
Start Date	The start date of the monthly count cycle. For example: 2nd, indicating that the monthly count cycle is from the 2nd of this month to the 1st of the next month.
Total Allowance/ Monthly Allowance	How much traffic is allowed to use for a month or in total.
SMS Alert	The SMS alert switch of the data limit, if the data limit function is turned on and the SMS altert is turned on, when the usage alert of the set data allowance is reached or the set data allowance is reached, the SMS alert will be sent.
Usage Alert	Usage alert. For example, when 80% of the data allowance is reached, an SMS alert will be sent.
Alert SMS Phone Number	The number for receiving alert SMS.
Send Text Message	Send a test SMS to confirm that the number can be used to receive alert SMS.

4 LAN Configuration

The LAN port is used to connect to the LAN clients, and works as the default gateway for these clients. You can configure the DHCP server for the LAN clients, and clients will automatically be assigned to IP addresses if the method of obtaining IP addresses is set as "Obtain IP address automatically".

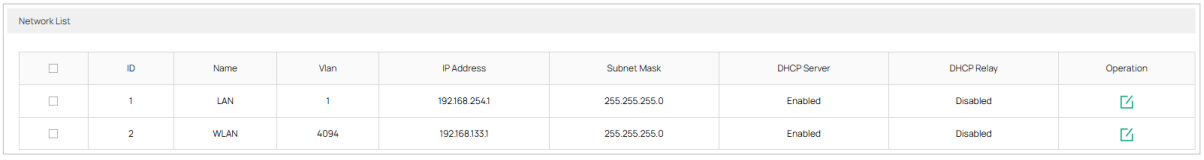
For LAN configuration, you can:

- Configure the IP address of the LAN port.
- Configure the DHCP server.

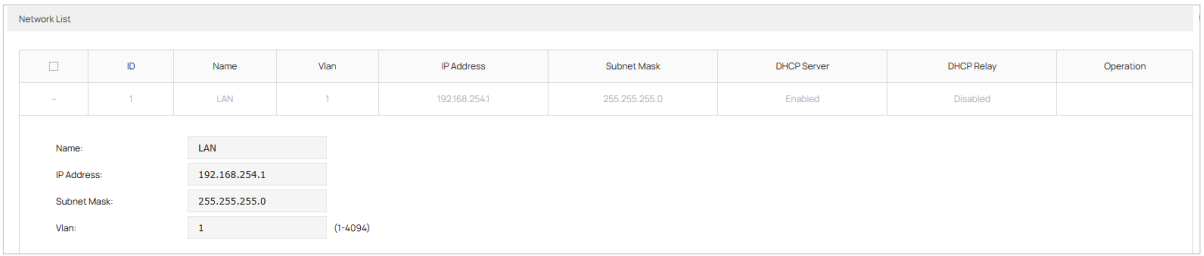
4.1 Configuring the LAN IP

Choose the menu **Network** > **LAN** > **LAN** to load the following page.

Figure 4-1 Configuring the LAN network



In the **Network List** section, click the Edit icon in the Operation column to configure the LAN network parameters.

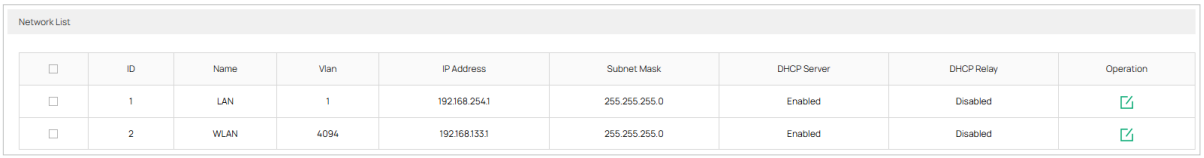


Name	Specify a name for the LAN network.
IP Address	Enter the IP address of the LAN port. To make your local network devices connect to the internet, you need to set the IP address of the LAN port as the default gateway of those devices.
Subnet Mask	Enter the subnet mask of the LAN port (255.255.255.0 by default). The IP addresses of all devices which connect to the LAN ports should be in the same subnet as the IP address of the LAN port.
VLAN	Specify the VLAN of the LAN port, only the devices in the specified VLAN can access and manage the gateway.

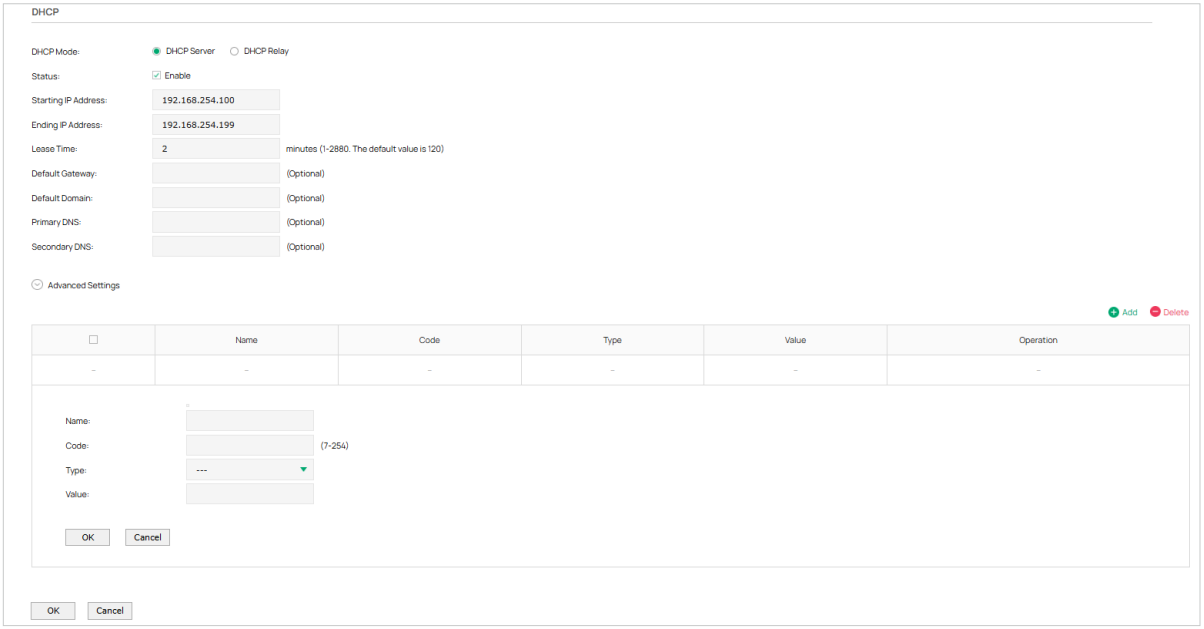
4.2 Configuring the DHCP

Choose the menu **Network** > **LAN** > **LAN** to load the following page.

Figure 4-2 Configuring the LAN network



In the **DHCP** section, configure the following parameters.



DHCP Mode -- DHCP Server

If you select DPCP Server as DHCP Mode, the DHCP server of the gateway will assign IP addresses to the LAN clients. Configure the following parameters.

Status: Check the box to enable DHCP Server.

Starting IP Address / Ending IP Address: Enter the starting IP address and ending IP address of the DHCP server's IP pool. The IP pool defines the range of IP addresses that can be assigned to the LAN clients. Note that the starting IP address and ending IP address should be in the same subnet as the IP address of the LAN port.

Lease Time: Specify the lease time for DHCP clients. Lease time defines how long the clients can use the IP address assigned by the DHCP server. Generally, the client will automatically request the DHCP server for extending the lease time before the lease expired. If the request fails, the client will have to stop using that IP address when the lease finally expired, and try to get a new IP address from another DHCP server.

Default Gateway: (Optional) Enter the default gateway which is assigned by the DHCP server. It is recommended to enter the IP address of the LAN port.

Default Domain: (Optional) Enter the domain name of your network.

Primary DNS / Secondary DNS: (Optional) Enter the DNS server address provided by your ISP. If you are not clear, please consult your ISP.

Click Advanced Settings to display the DHCP Options.

DHCP NTP Server: (Option 42) Enter one or two DHCP NTP Server addresses to get the system time from internet. Use "," to divide addresses.

DHCP Network Boot: (Option 67) Enter the value for DHCP Option 67. It specifies the boot file name.

DHCP Time Offset: (Option 2) Enter the time offset of the DHCP client's subnet in seconds from the UTC time.

DHCP TFTP Server: (Option 66) Enter the TFTP server address for file transfer.

DHCP WPAD URL: (Option 252) Enter the DHCP WPAD (Web Proxy Auto-Discovery) URL for the DHCP client to configure its proxy settings.

DHCP Mode -- DHCP Server	**Option60:** (Optional) Enter the value for DHCP Option 60. DHCP clients use this field to optionally identify the vendor type and configuration of a DHCP client. Mostly, it is used in the scenario where the APs apply for different IP addresses from different servers according to the needs. For detailed information, please consult the vendor. For TP-Link, this entry should be TP-Link. **Option138:** (Optional) Enter the value for DHCP Option 138. It is used in discovering the devices by the Omada controller. **Option150:** (Optional) Enter the value for DHCP Option 150. It specifies the TFTP server information and supports multiple TFTP server IP addresses. **Option159:** (Optional) Enter the value for DHCP Option 159. This option is used to configure a set of ports bound to a shared IPv4 address. **Option160:** (Optional) Enter the value for DHCP Option 160. This option is used to configure DHCP captive portal. **Option176:** (Optional) Enter the value for DHCP Option 176. This option is used to configure parameters for IP phones. **Option242:** (Optional) Enter the value for DHCP Option 242. This option is used to provide the TMS address automatically. To add a DHCP option entry, click the Add buton, specify the option name and code, select the oprtion type from the list, enter its value, and clcik OK to save the settings.
DHCP Mode -- DHCP Relay	If you select DHCP Relay as DHCP Mode, the gateway will relay DHCP requests from LAN clients to the DHCP server in another network. Then the DHCP server will assign IP addresses to the LAN clients. Configure the following parameters. **Status:** Check the box to enable DHCP Relay. **Server Address:** Enter the IP address of the DHCP server.

4.3 Viewing the DHCP Client List

Choose the menu **Network** > **LAN** > **DHCP Client List** to load the following page.

Figure 4-3 Viewing the DHCP Client List

Here you can view the DHCP client list.

Client Name	Displays the host name of the DHCP client. It should be composed of digits, English letters, dashes and underscores only.
MAC Address	Displays the MAC address of the client.
Assigned IP Address	Displays the IP address assigned to the client.

Lease Time	Displays the remaining lease time of the assigned IP address. After the lease expires, the IP address will be re-assigned.

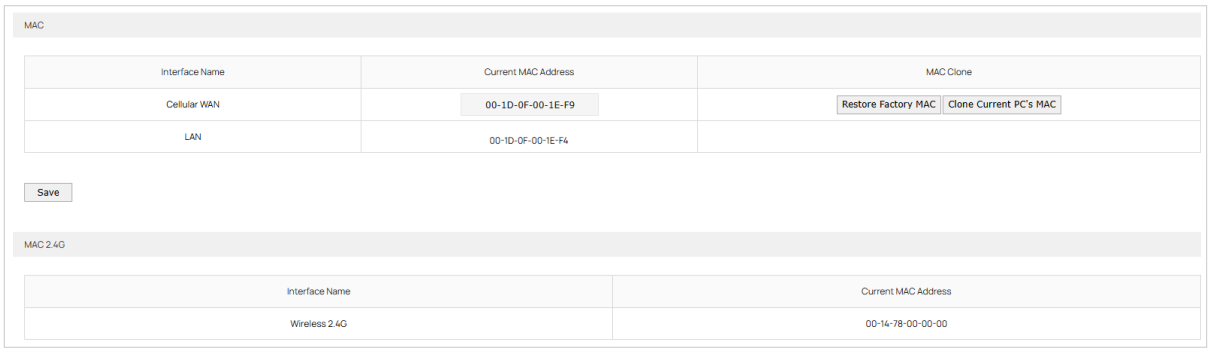
5 MAC Configuration

Generally, the MAC address does not need to be changed. However, in the following situations, you may need to change the MAC address of the WAN port.

In the condition that your ISP has bound your account to the MAC address of the dial-up device, if you want to replace the dial-up device with this gateway, you can just set the MAC address of this gateway's WAN port the same as that of the previous dial-up device for a normal internet connection.

Choose the menu **Network** > **MAC** > **MAC** to load the following page.

Figure 5-1 Configuring MAC Address



Configure the MAC address of the WAN port according to your need, then click **Save**.

Interface Name	Displays the WAN port and LAN port.
Current MAC Address	Configure the MAC address of the WAN port.
MAC Clone	MAC Clone provides a shortcut to changing the MAC Address. **Restore Factory MAC**: Click this button to restore the MAC address to the factory default value. **Clone Current PC's MAC**: Click this button to clone the MAC address of the PC you are currently using to configure the gateway. It's only available for the WAN ports.

Note:

When cloning current management host's MAC on the WAN port, the management PC should be connected to the LAN port.

6 Switch Configuration

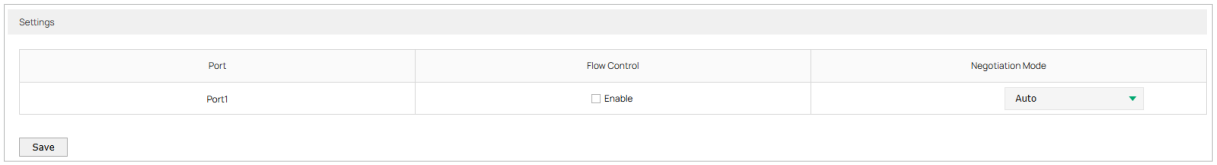
The gateway provides some basic switch port management function, including **Port Config** and **Port Status**.

6.1 Configuring Port Config

You can configure the flow control and negotiation mode for the port.

Choose the menu **Network** > **Switch** > **Port Config** to load the following page.

Figure 6-1 Configuring Flow Control and Negotiation



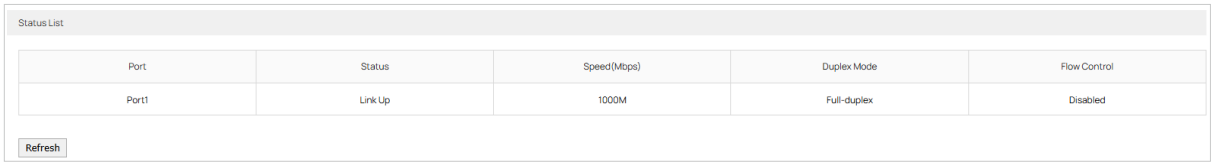
Configure the flow control and negotiation mode for a port.

Flow Control	Check the box to enable the flow control function. Flow Control is the process of managing the data transmission of the sender to avoid the receiver getting overloaded.
Negotiation Mode	Select the Negotiation Mode for the port. You can select Auto (Auto-negoation), or manually select the speed and duplex mode.

6.2 Viewing Port Status

Choose the menu **Network** > **Switch** > **Port Status** to load the following page.

Figure 6-2 Viewing Port Status



Status	Displays the port status. **Link Down**: The port is not connected. **Link Up**: The port is working normally.
Speed (Mbps)	Displays the port speed.
Duplex Mode	Displays the duplex mode of the port, including Full-duplex and Half-duplex.
Flow Control	Displays the status of Flow Control you have set for this port. Flow Control is enabled only when both the port and its connected device have Flow Control enabled.

7 VLAN Configuration

In IP Passthrough mode, the gateway's LAN port is in VLAN 1. In the VLAN module, you can modify the VLAN settings.

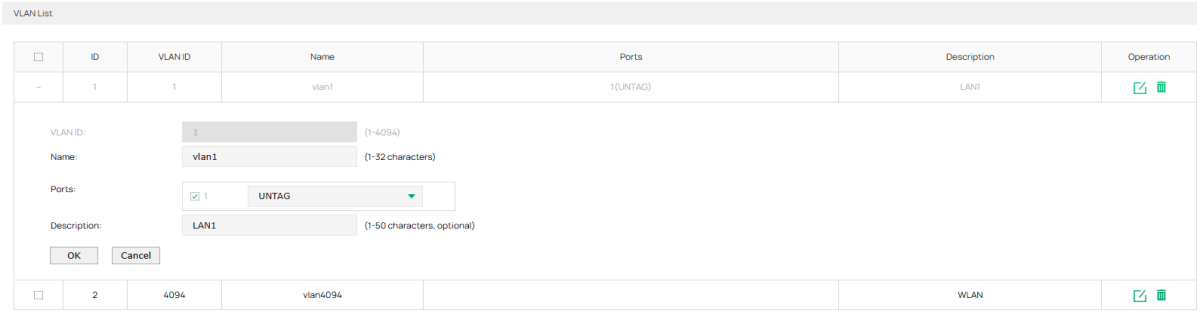
For VLAN configuration, you can:

- Modify the VLAN settings.
- Configure the PVID of the ports.

7.1 Modifying the VLAN Settings

Choose the menu **Network** > **VLAN** > **VLAN**, click the Edit icon in the Operation column to load the following page and configure the following parameters.

Figure 7-1 Modifying the VLAN



VLAN ID	Enter a VLAN ID. The value ranges from 1 to 4094.
Name	Specify the name of the VLAN for easy identification.
Ports	Check the box to add the desired port to the VLAN and specify the port type in the specified VLAN. The port can be divided into two types: TAG or UNTAG. **TAG**: The egress rule of the packets transmitted by the port is tagged. **UNTAG**: The egress rule of the packets transmitted by the port is untagged. If the device connected to the port is an end device, like a PC or a server, the port type should be UNTAG, because end devices don't recognize tagged packets.
Description	(Optional) Enter a brief description for easy management and searching.

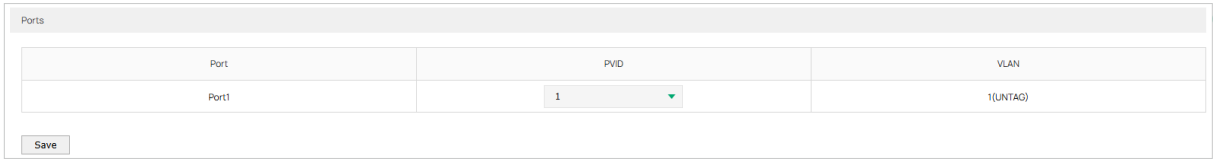
7.2 Configuring the PVID of a Port

PVID indicates the default VLAN for the corresponding port. Untagged packets which are received by the port are tagged with the PVID and then transmitted within the corresponding VLAN.

For example, if Port 2 is in both VLAN 10 and VLAN 20, and the PVID of the port is 10, when Port 2 receives an untagged packet from a PC, the packet is transmitted within VLAN 10, but cannot reach VLAN 20 directly.

To Configure the PVID of the port, choose the menu **Network** > **VLAN** > **Ports** to load the following page.

Figure 7-2 Configuring the PVID



Configure the PVID of the port, then click **Save**.

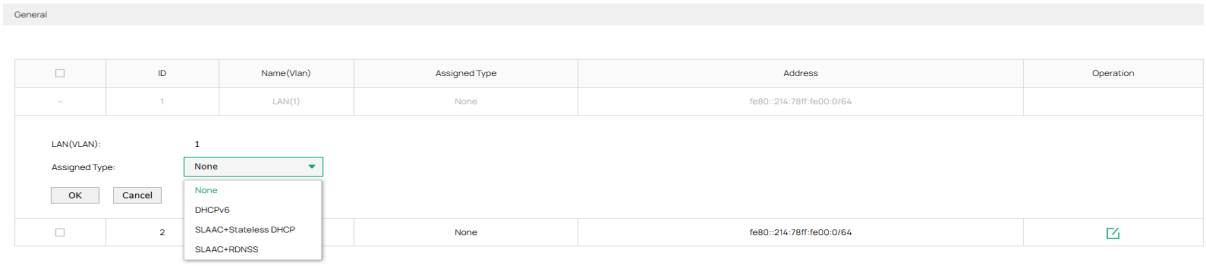
Port	Displays the port.
PVID	Specify the PVID for the port. PVID indicates the default VLAN for the corresponding port.
VLAN	Displays the VLAN(s) the port belongs to.

8 IPv6 Configuration

IPv6 is the next-generation network protocol following IPv4. You can configure IPv6 network for the gateway if your ISP supports IPv6. IPv6 network won't cause conflict with your current IPv4 network.

Choose the menu **Network** > **IPv6** > **LAN**, click the Edit icon in the Operation column to load the following page and configure the following parameters.

Figure 8-1 Select Assigned Type



In the **General** section, select the proper Assigned Type, which is determined by the compatibility of clients in your local network, and configure the parameters according to the requirements of your ISP. Then click **OK**.

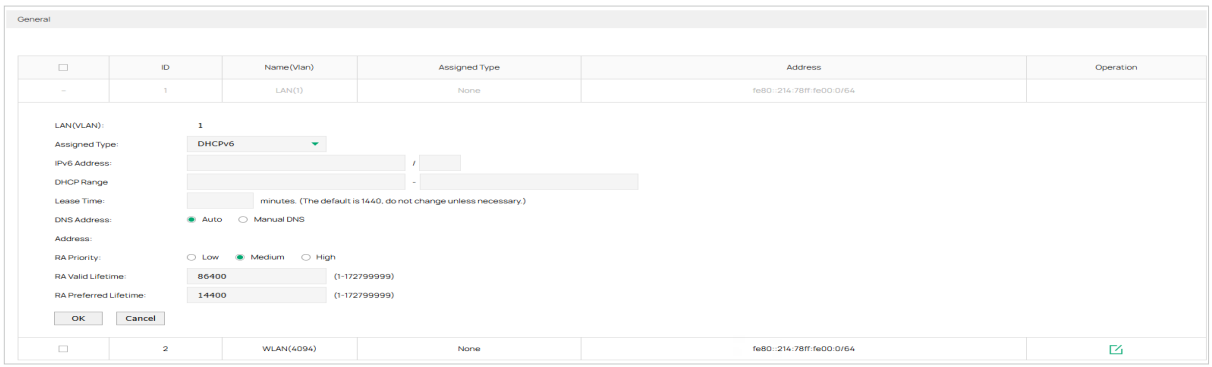
Assigned Type	Determines the method whereby the gateway assigns IPv6 addresses to the clients in your local network. Some clients may support only a few of these assigned types, so you should choose it according to the compatibility of clients in your local network.

Note:

- If Internet Connection Type of WAN / SFP WAN is selected as Pass-Through (Bridge), the IPv6 parameters of the LAN port and the other WAN ports cannot be configured.
- If Prefix Delegation of WAN / SFP WAN is enabled, the Address Prefix of LAN is automatically assigned by your ISP and you cannot designate an address prefix manually.

■ Configuring the DHCPv6

Figure 8-2 Configuring the DHCPv6

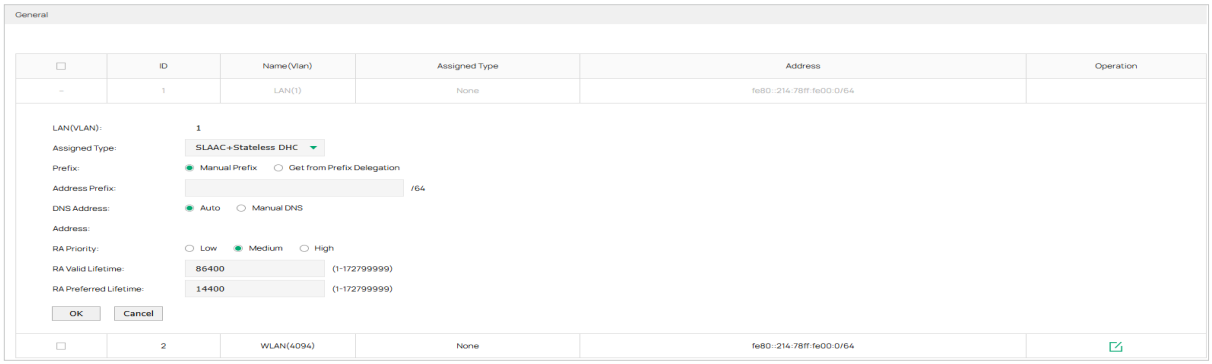


In **Assigned Type** section, select the connection type as DHCPv6. Enter the corresponding parameters and click **OK**.

IPv6 Address	Enter the IPv6 address and prefix length (subnet mask).
DHCP Range	Enter the starting and ending IPv6 address to define a range for the DHCPv6 server to assign dynamic IPv6 addresses.
Lease Time	The duration time in minutes when the assigned IPv6 address remains valid. Either keep the defualt 1440 minutes or change it if required.
DNS Address	Select a method to configure the DNS server for the LAN, with Auto selected, the DNS server addresses are automatically obtained. With Manual DNS selected, manually enter the primary and secondary DNS server addresses provided by your ISP.
Address	Displays the IPv6 address of the LAN port.
RA Priority	Specify the router priority to help a host choose its default gateway. If a host receives RA messages from multiple routers, it will select the router with the highest RA priority as the default gateway. In the case of routers with the same priority, it will select the router whose RA message is received first as the default gateway.
RA Valid Lifetime	Specify the validity lifetime of the prefix. The addresses automatically generated with the prefix can be used normally during the valid lifetime, and they will become invalid and be deleted after the valid lifetime expires.
RA Preferred Lifetime	Specify the preferred lifetime for stateless auto-configuration of addresses with the prefix. After the preferred lifetime expires, the addresses automatically configured by the hosts with this prefix will be abolished. A host cannot use an abolished address to establish a new connection, but it can still receive packets whose destination address is an abolished address. The RA Preferred Lifetime must be less than or equal to the RA Valid Lifetime.

■ Configuring the SLAAC+Stateless DHCP

Figure 8-3 Configuring the SLAAC+Stateless DHCP

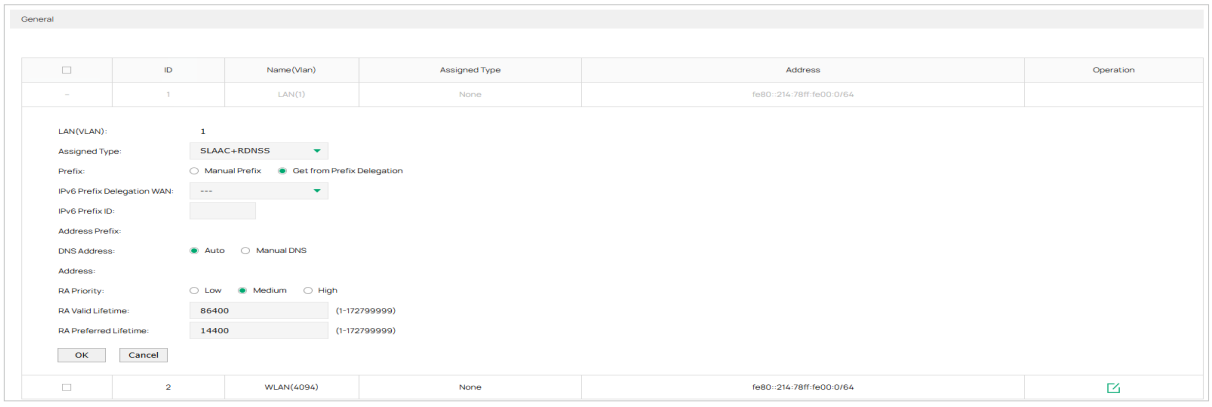


In **Assigned Type** section, select the connection type as SLAAC+Stateless DHCP. Enter the corresponding parameters and click **OK**.

Prefix	Configure the IPv6 address prefix for each client in the local network. WIth Manual Prifix selected, enter the prefix in the Address Prefix field. With Get from Prefix Delegation selected, select hte IPv6 Prefix Delegation WAN port, and enter the IPv6 Prefix ID to get a prefix delegation from the ISP.
IPv6 Prefix Delegation WAN	Enter the IPv6 Prefix Delegation WAN port and the IPv6 Prefix ID to get a prefix delegation from the ISP.
IPv6 Prefix ID	With Get from Prefix Delegation selected, enter the Prefix ID, which will be addred to the prefix to obtain a /64 subnet. The range of IPv6 Prefix ID is determined by Prefix Delegation Size and Prefix Length.
DNS Address	Select a method to configure the DNS server for the LAN. With Auto selected, the DNS server addresses are automatically obtained. With Manual DNS selected, manually enter the primary and secondary DNS server addresses provided by your ISP.
Address	Displays the IPv6 address automatically generated by Prefix.
RA Priority	Specify the router priority to help a host choose its default gateway. If a host receives RA messages from multiple routers, it will select the router with the highest RA priority as the default gateway. In the case of routers with the same priority, it will select the router whose RA message is received first as the default gateway.
RA Valid Lifetime	Specify the validity lifetime of the prefix. The addresses automatically generated with the prefix can be used normally during the valid lifetime, and they will become invalid and be deleted after the valid lifetime expires.
RA Preferred Lifetime	Specify the preferred lifetime for stateless auto-configuration of addresses with the prefix. After the preferred lifetime expires, the addresses automatically configured by the hosts with this prefix will be abolished. A host cannot use an abolished address to establish a new connection, but it can still receive packets whose destination address is an abolished address. The RA Preferred Lifetime must be less than or equal to the RA Valid Lifetime.

Configuring the SLAAC+RDNSS

Figure 8-4 Configuring the SLAAC+RDNSS



In **Assigned Type** section, select the connection type as SLAAC+RDNSS. Enter the corresponding parameters and click **OK**.

Prefix	Configure the IPv6 address prefix for each client in the local network. WIth Manual Prifix selected, enter the prefix in the Address Prefix field. With Get from Prefix Delegation selected, select hte IPv6 Prefix Delegation WAN port, and enter the IPv6 Prefix ID to get a prefix delegation from the ISP.
IPv6 Prefix Delegation WAN	Enter the IPv6 Prefix Delegation WAN port and the IPv6 Prefix ID to get a prefix delegation from the ISP.
IPv6 Prefix ID	With Get from Prefix Delegation selected, enter the Prefix ID, which will be addred to the prefix to obtain a /64 subnet. The range of IPv6 Prefix ID is determined by Prefix Delegation Size and Prefix Length.
DNS Address	Select a method to configure the DNS server for the LAN. With Auto selected, the DNS server addresses are automatically obtained. With Manual DNS selected, manually enter the primary and secondary DNS server addresses provided by your ISP.
Address	Displays the IPv6 address automatically generated by Prefix.
RA Priority	Specify the router priority to help a host choose its default gateway. If a host receives RA messages from multiple routers, it will select the router with the highest RA priority as the default gateway. In the case of routers with the same priority, it will select the router whose RA message is received first as the default gateway.
RA Valid Lifetime	Specify the validity lifetime of the prefix. The addresses automatically generated with the prefix can be used normally during the valid lifetime, and they will become invalid and be deleted after the valid lifetime expires.
RA Preferred Lifetime	Specify the preferred lifetime for stateless auto-configuration of addresses with the prefix. After the preferred lifetime expires, the addresses automatically configured by the hosts with this prefix will be abolished. A host cannot use an abolished address to establish a new connection, but it can still receive packets whose destination address is an abolished address. The RA Preferred Lifetime must be less than or equal to the RA Valid Lifetime.

Part 5

Configuring SMS

CHAPTERS

1 Overview

The SMS module lets you manage SMS usage, check inbox messages, send messages and configure gateway commands.

1.1 Supported Features

SMS Quota

Set SMS quota to better manage SMS usage so that it does not exceed your set quota.

SMS Inbox/Outbox Message

Check inbox and outbox messages, and send messages.

Router Command

Send specific commands via SMS to interact with the device, and only specific users are allowed to perform these interactions.

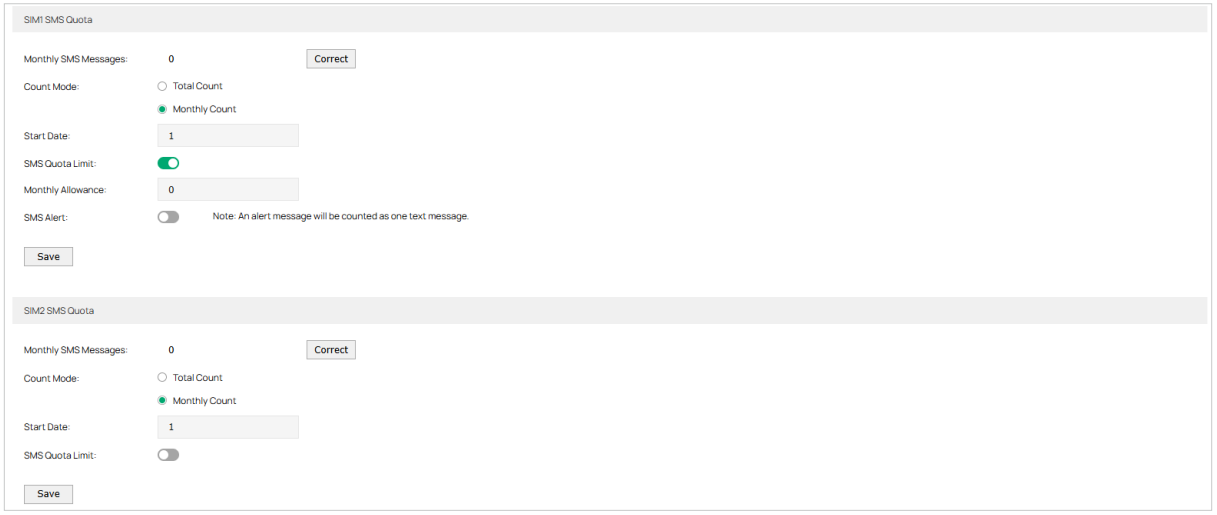
2 SMS Configuration

You can set SMS quota to better manage SMS usage. You can also set policies related to sending and receiving inboxes.

2.1 Configuring SMS Quota

Choose the menu **SMS** > **SMS Settings** > **SMS Quota**, select a SIM card and configure the **SMS Quota**.

Figure 2-1 Configuring the SMS Quota



Total SMS Messages	When Total Count mode is selected, set the Total SMS Messages, and the total number of SMS sent will be displayed here. Long text messages exceeding the set length are split into multiple messages for counting. You can manually adjust the number of messages sent.
Monthly SMS Messages	When Monthly Count mode is selected, the number of SMS sent every month will be displayed here. Long text messages exceeding the set length are split into multiple messages for counting. You can manually adjust the number of messages sent.
Count Mode	Select count mode: **Total Count:** The total number of text messages allowed to be sent. **Monthly Count:** The number of text messages allowed to be sent within a one-month cycle, monthly count needs to select the start date of each monthly count cycle.
Start Date	The start date of the monthly count cycle. For example: 2nd, indicating the monthly count cycle is from the 2nd of this month to the 1st of the next month.
Total Allowance	SMS allowance, that is, how many SMS messages are allowed to be sent.
SMS Quota Limit	Whether to enable the SMS quota function, if enabled, you will not be able to send SMS when the SMS quota is reached.

Monthly Allowance	Monthly SMS allowance, that is, how many SMS messages are allowed to be sent before the next cycle.
SMS Alert	The SMS alert switch of the SMS quota, if the SMS quota function is turned on and the SMS alert is turned on, the SMS allowance alet message will be sent when the alert ratio reaches the set SMS allowance.
Usage Alert	Usage alert. For example, when 80% of the SMS allowance is reached, an SMS allowance alert message will be sent.
Alert SMS Phone Number	The number for receiving alert SMS receiving.
Send Test Message	Send a test message to confirm that the number can be used to receive SMS limit alert messages.

2.2 Configuring SMS Inbox Policy

Choose the menu **SMS** > **SMS Settings** > **SMS Inbox** to load the following page. Select the desired policy and click **Save** to save the settings.

Figure 2-1 Configuring the SMS Inbox Policy

If SMS inbox is full, delete the oldest SMS	When the inbox is full, delete the oldest SMS.
If SMS inbox is full, send e-mail alert to Administrator	When the inbox is full, an e-mail will be sent to the administrator, and the new SMS will be lost, and an alert email will be sent to administrator. You need to enable **Mail Notification Setup** in **System Tools > Mail Notification**, configure related parameters and check **SMS Alert** in **Enable Mail Notification**.
If SMS inbox is full, forward new SMS with e-mail to Administrator	When the inbox is full, forward new SMS with e-mail to Administrator. You need to enable **Mail Notification Setup** in **System Tools > Mail Notification**, configure related parameters and check **SMS Alert** in **Enable Mail Notification**.

3 SMS Inbox/Outbox Management

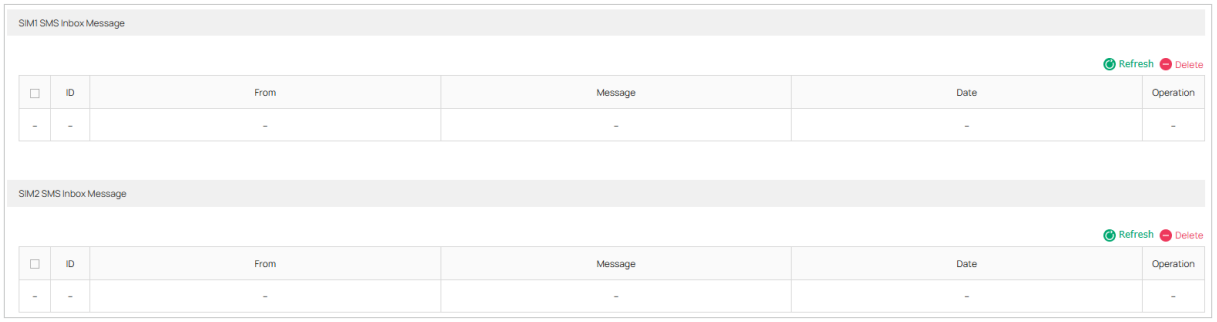
You can set SMS quota to better manage SMS usage. You can also set policies related to sending and receiving inboxes.

3.1 SMS Inbox Message

This box displays the messages you have received for each card.

Choose the menu **SMS** >**SMS Inbox Message** to load the following page.

Figure 3-1 Configuring the SMS Inbox Message



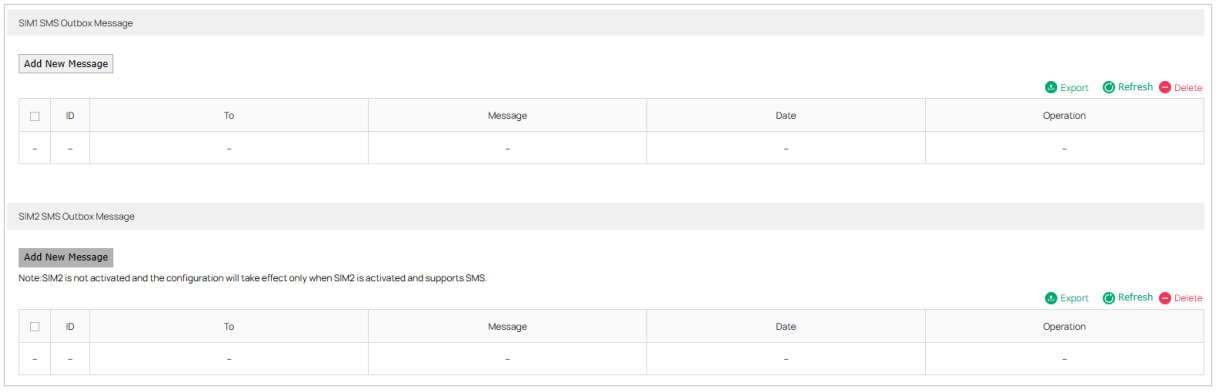
Refresh	Click to refresh the inbox.
Delete	Click to delete the messages you select.

3.2 SMS Outbox Message

This box displays the messages you have successfully sent from each card.

Choose the menu **SMS** >**SMS Outbox Message** to load the following page.

Figure 3-1 Configuring the SMS Outbox Message



Export	Click to export the required SMS to the local.

Refresh	Click to refresh the outbox.
Delete	Click to delete the messages you select.

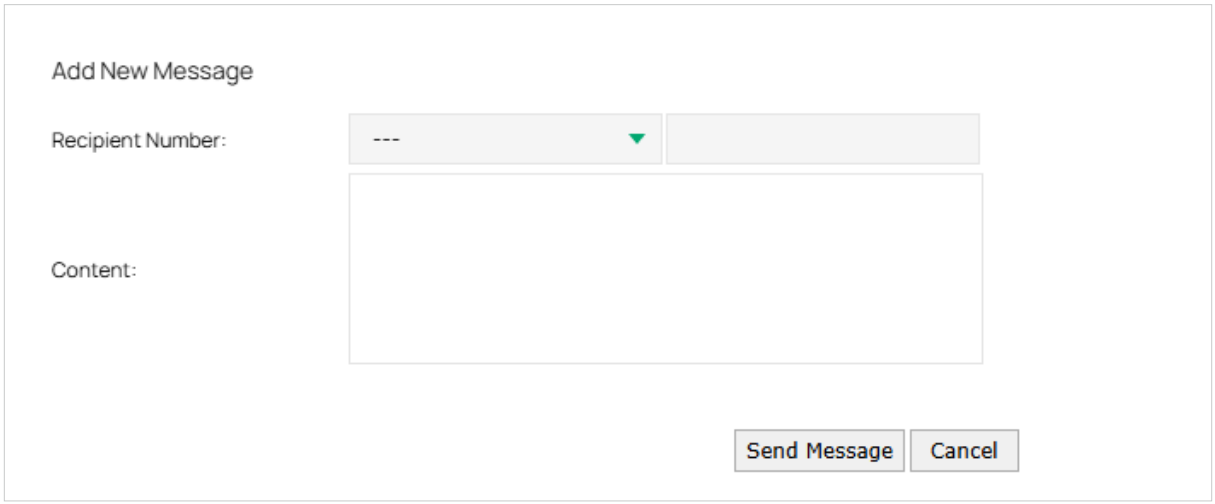
To send a message

Click **Add New Message** to send a message. Enter select the receiver's country code and enter the phone number and enter your message in the Content field. Click Send to send out your message.

Note:

When two SIM cards are inserted, only one card can be activated and used for internet connection. The other inactivated card cannot send or receive text messages.

Figure 3-2 Sending a Message

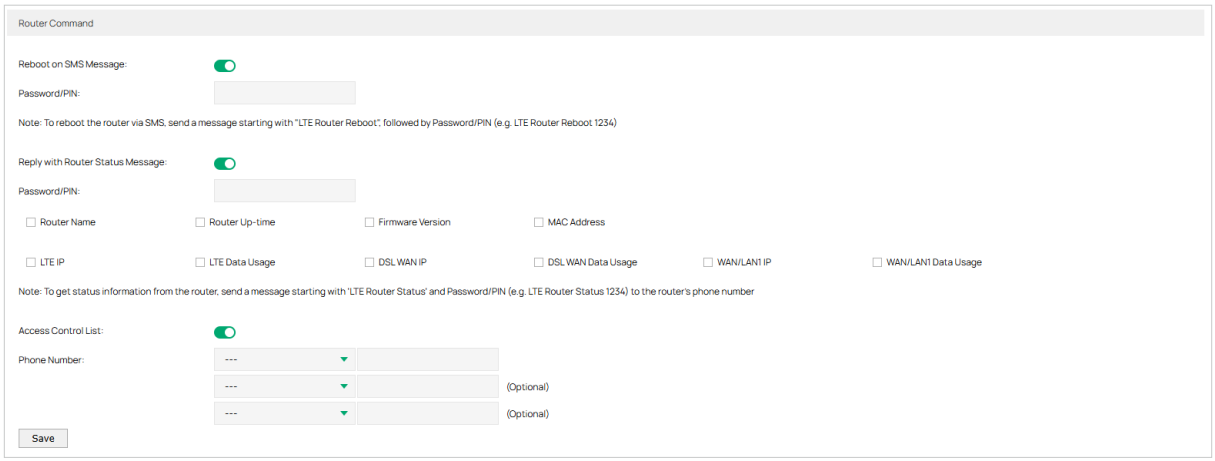


4 Router Command Configuration

You can send specific commands via SMS to interact with the device, and only specific users are allowed to perform these interactions.

Choose the menu **SMS** > **Router Command** to load the following page.

Figure 4-1 Configuring the Router Command



- **Reboot on SMS Message**

1) Enable **Reboot on SMS Message**, enter the password for the control of device restart via SMS.
2) To reboot the gateway via SMS, send a message starting with “LTE Router Reboot”, followed by Password/PIN (e.g. LTE Router Reboot 1234)

- **Reply with Router Status Message**

1) Enable **Reply with Router Status Message**, enter the password for viewing device-related information and WAN port-related information via SMS.
2) Check the types of information you want to review.
3) To get status information from the gateway, send a message starting with ‘LTE Router Status’ and Password/PIN (e.g. LTE Router Status 1234) to the gateway’s phone number.

- **Access Control List**

1) Enable **Access Control List** to enable the allow list of the above functions, and only allow users in the list to interact with the device.
2) Select the country code and enter the allowed phone numbers. Note that the international telephone area code needs to be added before the number.

Part 6

Configuring Transmission

CHAPTERS

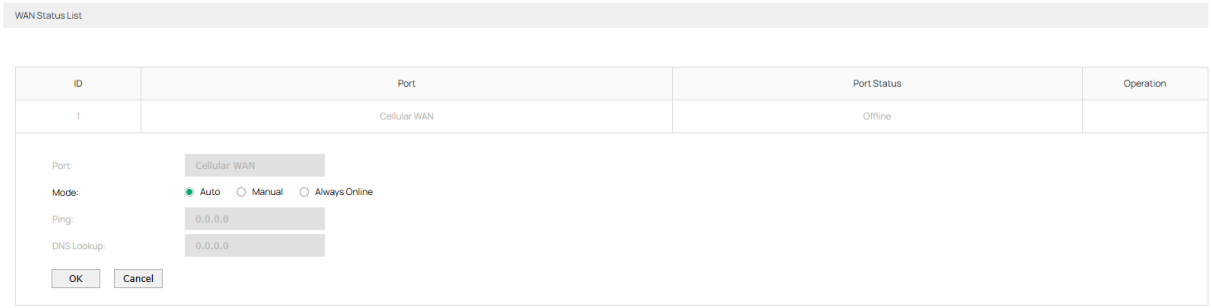
1 Overview

Online Detection is used to detect whether the 5G network is working normally. The gateway supports two SIM cards, when the network is abnormal, the gateway can switch between the two SIM cards to ensure a normal network.

2 Online Detection Configuration

Choose the menu **Transmission > Online Detection** and click the Edit button in the Operation column to load the following page and configure the following parameters.

Figure 2-1 Configuring Online Detection



Port	Displays the name of WAN Port.
Mode	Select the online detection mode. **Auto:** In this mode, the DNS server of the WAN port will be selected as the destination for DNS Lookup to detect whether the WAN is online. **Manual:** In this mode, you can configure the destination IP address for Ping and DNS Lookup manually to detect whether the WAN is online. **Always Online:** In this mode, the status of the port will always be online.
Ping	If Manual Mode is selected, specify the destination IP for Ping. The corresponding port will ping the IP address to detect whether the WAN port is online. 0.0.0.0 means Ping detection is disabled.
DNS Lookup	If Manual Mode is selected, specify the IP address of DNS server. The corresponding port will perform the DNS lookup using default domain name to detect whether the WAN port is online. 0.0.0.0 means DNS Lookup is disabled.

Part 7

Managing Services

CHAPTERS

1 Overview

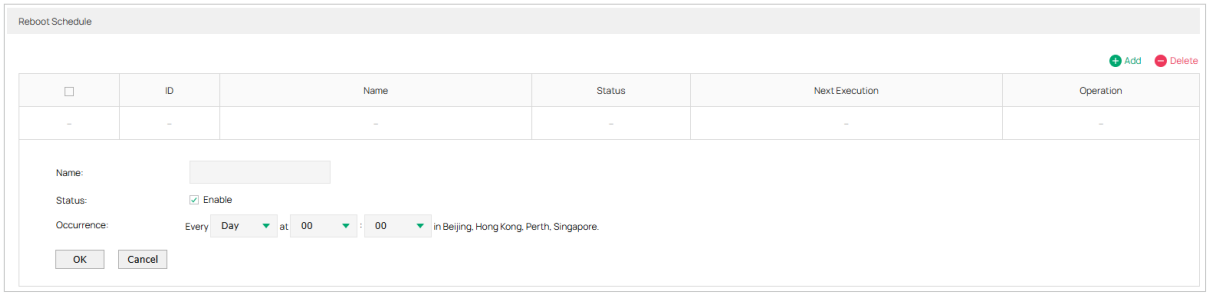
In Reboot Schedule, you can set schedules to reboot the connected devices periodically based on needs. You can configure the reboot schedule flexibly by creating multiple entries.

2 Reboot Schedule

In Reboot Schedule, you can set schedules to reboot the connected devices periodically based on needs. You can configure the reboot schedule flexibly by creating multiple entries. The system time can be set in **System Tools** > **Time Settings**.

Choose the menu **Services** > **Reboot Schedule**, click **Add** to load the following page and configure the following parameters.

Figure 2-1 Configuring Reboot Schedule



Name	Enter a name to identify the reboot schedule entry.
Status	Click the checkbox to enable the reboot schedule entry.
Occurrence	Specify the date and time for the devices to reboot.

Part 8

System Tools

CHAPTERS

1 Overview

1.1 Overview

The System Tools module provides several system management tools for users to manage the gateway.

1.2 Support Features

Admin Setup

Admin Setup is used to configure the parameters for users' login. With this function, you can modify the login account, specify the IP subnet and mask for remote access and specify the HTTP and HTTPS server port.

Management

The Management section is used to manage the firmware and the configuration file of the gateway. With this function, you can reset the gateway, backup and restore the configuration file, reboot the gateway and upgrade the firmware.

Controller Settings

With this feature configured, you can configure your gateway via Cloud-Based Controller.

SNMP

SNMP (Simple Network Management Protocol) is a standard network management protocol. It helps network managers to configure and monitor network devices. With SNMP, network managers can view and modify network device information, detect and analyze network error, and so on. The gateway supports SNMPv1 and SNMPv2c.

Diagnostics

Diagnostics is used to detect network errors and equipment failures. With this function, you can test the connectivity of the network with ping or traceroute command and inspect the gateway under the help of technicians.

LED Control

Manually control the LED status via the web.

Time Settings

Time Settings is used to configure the system time and the daylight saving time.

System Log

System Log is used to view the system log of the gateway. You can also configure the gateway to send the log to a server.

Mail Notification

You can configure mail-related parameters and choose the modules to apply these parameters to. Some modules will use the configuration information to send emails.

2 Admin Setup

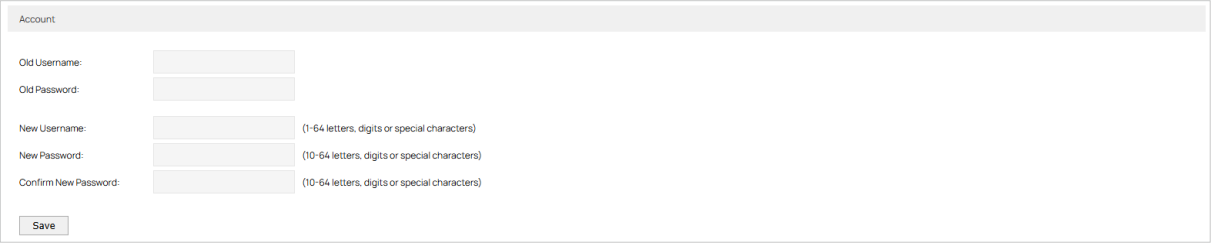
In Admin Setup module, you can configure the following features:

- Admin Setup
- Remote Management
- Remote Management for IP Passthrough
- System Settings

2.1 Admin Setup

Choose the menu **System Tools** > **Admin Setup** > **Admin Setup** to load the following page.

Figure 2-1 Modifying the Admin Account



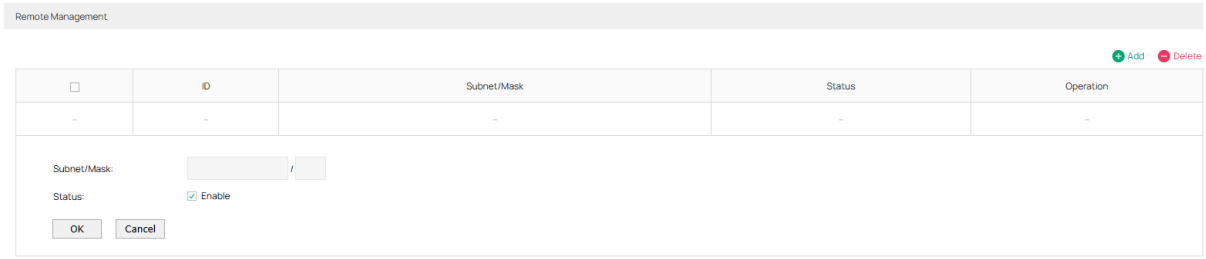
In the **Account** section, configure the following parameters and click **Save** to modify the admin account

Old Username	Enter the old username.
Old Password	Enter the old password.
New Username	Enter a new username.
New Password	Enter a new password.
Confirm New Password	Re-enter the new password for confirmation.

2.2 Remote Management

Choose the menu **System Tools** > **Admin Setup** > **Remote Management** and click **Add** to load the following page.

Figure 2-2 Configuring Remote Management



In the **Remote Management** section, configure the following parameters and click **OK** to specify the IP subnet and mask for remote management.

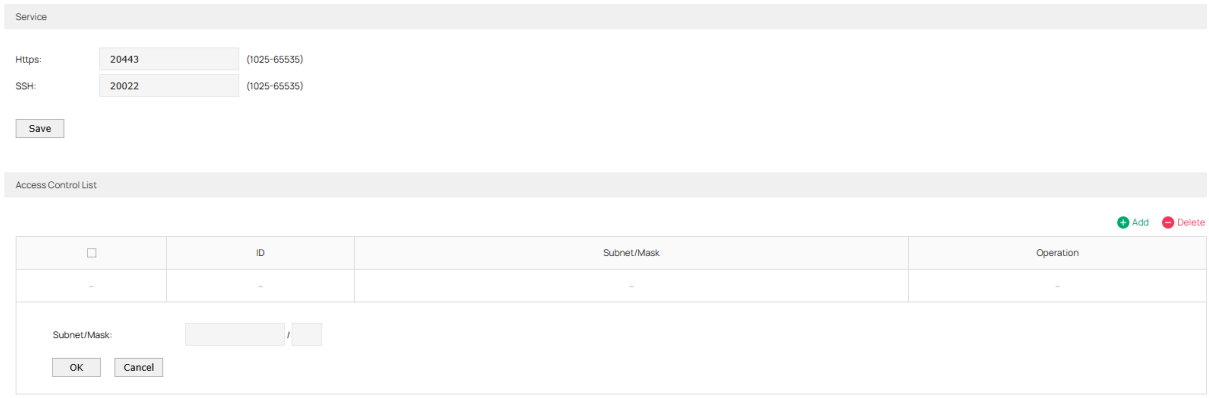
Subnet/Mask	Enter the IP Subnet and Mask of the remote host.
Status	Check the box to enable the remote management function for the remote host.

2.3 Remote Management for IP Passthrough

Remote management for IP Passthrough allows you to configure different server ports to remotely access the device in different ways.

Choose the menu **System Tools** > **Admin Setup** > **Remote Management for IP Passthrough** to load the following page.

Figure 2-3 Configuring Remote Management for IP Passthrough



Configure the parameters for the ways to access the management interface of the gateway. Click **Save.**

Https	Specify the https server port for web management. The port number should be different from other servers.
SSH	Specify the SSH server port for web management. The port number should be different from other servers.

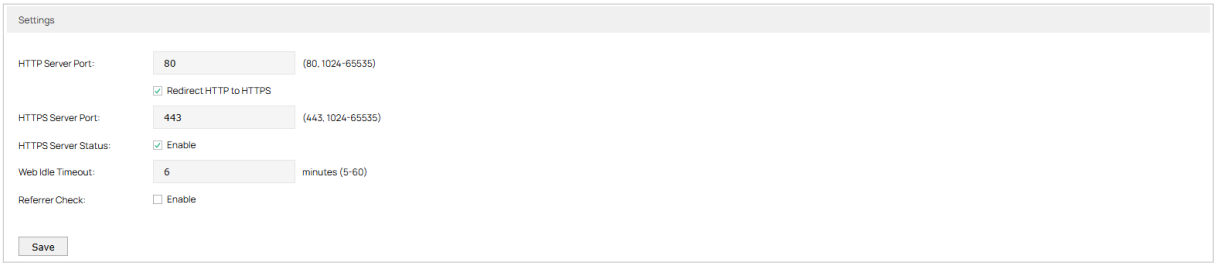
Click Add and configure the parameters. Click **OK.**

Subnet/Mask	Enter the subnet mask of the port that allows to access the device.

2.4 System Settings

Choose the menu **System Tools** > **Admin Setup** > **System Settings** to load the following page.

Figure 2-4 Configuring System Settings



In the **Settings** section, configure the following parameters and click **Save**.

HTTP Server Port	Specify the http server port for web management. The port number should be different from other servers. The default setting is 80. For example, if you change the http server port to 1600, you should access the interface by using IP address and the port number in the format of 192.168.0.1:1600.
Redirect HTTP to HTTPS	Check the box to enable the function, then you will access the web management interface by HTTPS protocol instead of HTTP protocol.
HTTPS Server Port	Specify the https server port for web management. The port number should be different from other servers. The default setting is 443. For example, if you change the https server port to 1600, you should access the interface by using IP address and the port number in the format of https://192.168.0.1:1600.
HTTPS Server Status	Check the box to enable HTTPS Server.
Web Idle Timeout	Enter a session timeout time for the device. The web session will log out for security if there is no operation within the session timeout time.
Referrer Check	Enabling Referrer Check can avoid CSRF (Cross-site request forgery) and improve the security of the device. When enabled, the referrer field and the message IP will be strictly verified. In some cases (such as using a domain name to access the device web), the referrer field verification will fail.

3 Management

In Management module, you can configure the following features:

- Factory Default Restore
- Backup & Restore
- Reboot
- Firmware Upgrade

3.1 Factory Default Restore

Choose the menu **System Tools** > **Management** > **Factory Default Restore** to load the following page.

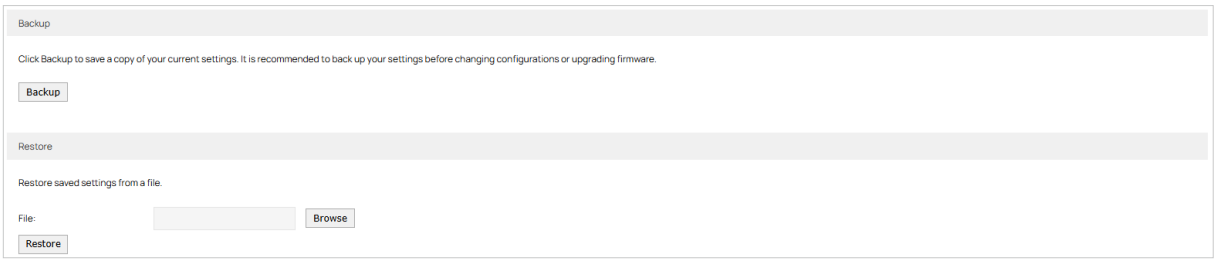
Figure 3-1 Reseting the Device

Click **Factory Restore** to reset the device.

3.2 Backup & Restore

Choose the menu **System Tools** > **Management** > **Backup & Restore** to load the following page.

Figure 3-2 Backup & Restore Page



Choose the corresponding operation according to your need:

1) In the **Backup** section, click **Backup** to save your current configuration as a configuration file and export the file to the host.
2) In the **Restore** section, select one configuration file saved in the host and click **Restore** to import the saved configuration to your gateway.

3.3 Reboot

Choose the menu **System Tools** > **Management** > **Reboot** to load the following page.

Figure 3-3 Rebooting the Device

Click **Reboot** to reboot the device.

3.4 Firmware Upgrade

Choose the menu **System Tools** > **Management** > **Firmware Upgrade** to load the following page.

Figure 3-4 Configure System Settings

Select one firmware file and click **Upgrade** to upgrade the firmware of the device.

4 Controller Settings

To make your controller adopt your gateway, make sure the gateway can be discovered by the controller. Controller Settings enable your gateway to be discovered in either of the following scenarios.

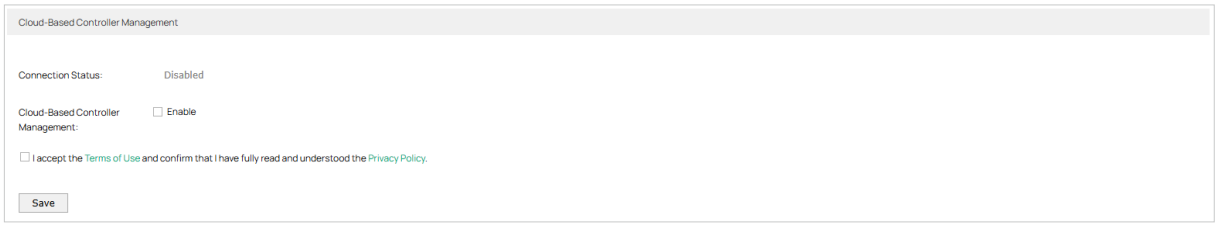
- If you are using Omada Cloud-Based Controller, Enable Cloud-Based Controller Management.
- If your gateway and controller are located in the same network, LAN and VLAN, the controller can discover and adopt the gateway without any controller settings. Otherwise, you need to inform the gateway of the controller's URL/IP address, and one possible way is to Configure Controller Inform URL.

For details about the whole procedure, refer to the User Guide of Omada SDN Controller. The guide can be found on the official website: https://support.omadanetworks.com/document/.

4.1 Enable Cloud-Based Controller Management

Choose the menu **System Tools** > **Controller Settings** page. In the Cloud-Based Controller Management section, enable **Cloud-Based Controller Management** and click **Save**. You can check the connection status on this page. Check the box before **I accept the Terms of Use and confirm that I have fully read and understood the Privacy Policy**.

Figure 4-1 Cloud-Based Controller Management



4.2 Configure Controller Inform URL

Choose the menu **System Tools** > **Controller Settings** page. In the Controller Inform URL section, Enter the inform URL or IP address of your controller to tell the gateway where to discover the controller and click **Save**.

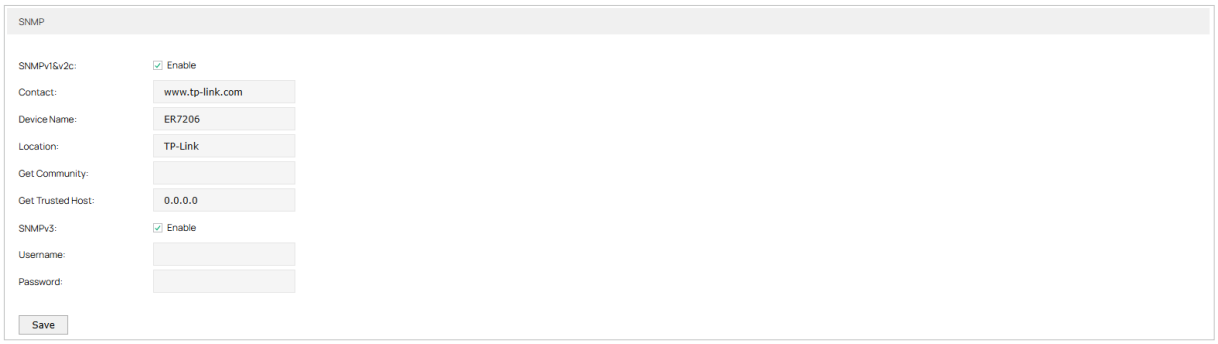
To get the inform URL of Cloud-Based Controller, click the controller on your Cloud Dashboard to reveal the Properties window, and then go to the Details tab.

Figure 4-2 Cloud-Based Controller Management

5 SNMP

Choose the menu **System Tools** > **SNMP** > **SNMP** to load the following page.

Figure 5-1 Configuring SNMP



Follow these steps to configure the SNMP function:

1) Choose the SNMP version and specify the corresponding parameter.
2) Configure the following parameters and click **Save**.

- If SNMPv1&v2c is enabled:

Contact	Enter the textual identification of the contact person for this the device, for example, contact or e-mail address.
Device Name	Enter a name for the device.
Location	Enter the location of the device. For example, the name can be composed of the building, floor number, and room location.
Get Community	Specify the community string for getting the read-only access to the device's SNMP information. When a manager tries to access the SNMP agent, the community helps authenticate the manage and establish trust between the manager and the agent.
Get Trusted Host	Enter the IP address that can serve as Get Community to read the SNMP information of this device.

- If SNMPv3 is enabled:

Username	With SNMPv3 selected, specify the username of your NMS (Network Management Station) to access the SNMP agent. You need to configure the username correspondingly on your NMS.
Password	With SNMPv3 selected, specify the password of your NMS (Network Management Station) to access the SNMP agent. You need to configure the password correspondingly on your NMS.

6 Diagnostics

In Diagnostics module, you can configure the following features:

- Diagnostics
- Remote Assistance

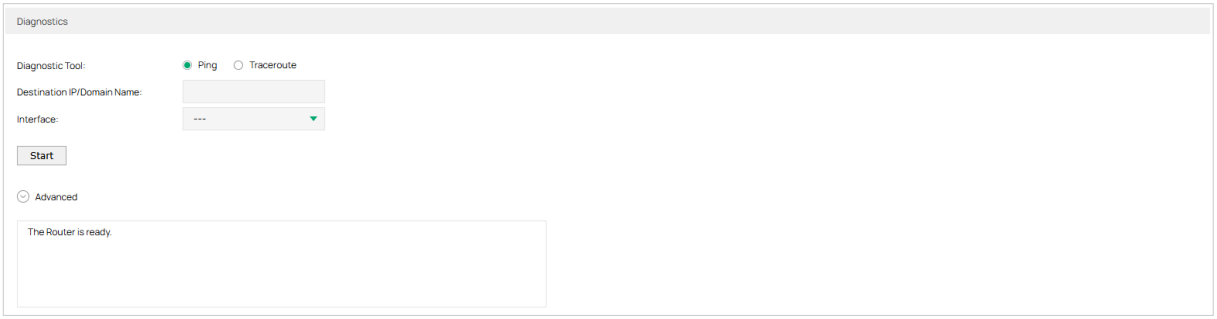
6.1 Diagnostics

Ping and traceroute are both used to test the connectivity between two devices in the network. In addition, ping can show the roundtrip time between the two devices directly and traceroute can show the IP address of gateways along the route path.

6.1.1 Configuring Ping

Choose the menu **System Tools** > **Diagnostics** > **Diagnostics** to load the following page.

Figure 6-1 Configuring Diagnostics



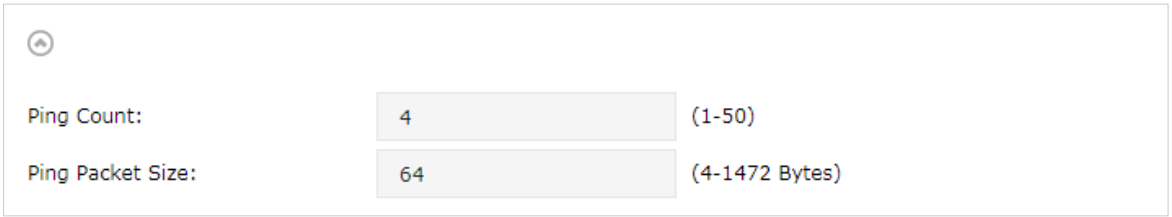
Follow these steps to configure Diagnostics:

1) In **Diagnostics** section, select **Ping** and configure the following parameters.

Diagnostic Tool	Select **Ping** to test the connectivity between the gateway and the desired device.
Destination IP/ Domain Name	Enter the IP address or the domain name that you want to ping or tracert.
Interface	Select the interface that sends the detection packets.

2) (Optional) Click **Advanced** and the following section will appear.

Figure 6-2 Advanced Parameters for Ping Method



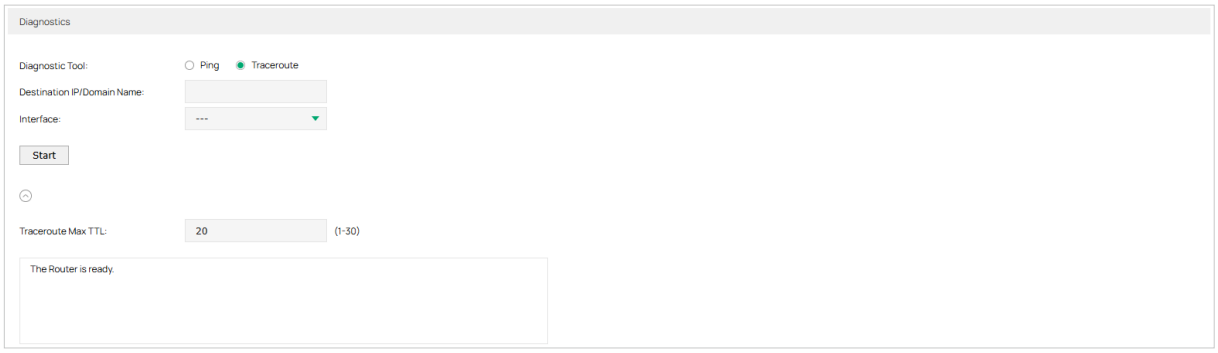
Ping Count	Specify the count of the test packets to be sent during the ping process.
Ping Packet Size	Specify the size of the test packets to be sent during the ping process.

3) Click **Start**.

6.1.2 Configuring Traceroute

Choose the menu **System Tools** > **Diagnostics** > **Diagnostics** to load the following page.

Figure 6-3 Configuring Diagnostics



Follow these steps to configure Diagnostics:

1) In **Diagnostics** section, select **Traceroute** and configure the following parameters.

Diagnostic Tool	Select **Traceroute** to test the connectivity between the gateway and the desired device.
Destination IP/ Domain Name	Enter the IP address or the domain name that you want to ping or tracert.
Interface	Select the interface that sends the detection packets.

2) (Optional) Click **Advanced**.

Traceroute MAX TTL	Specify the traceroute max TTL (Time To Live) during the traceroute process. It is the maximum number of the route hops the test packets can pass through.

3) Click **Start**.

6.2 Remote Assistance

Note:

Please make contact with the technicians before trying to use this function.

Choose the menu **System Tools** > **Diagnostics** > **Remote Assistance** to load the following page.

Figure 6-4 Remote Assistance Page

1) In the **Remote Assistance** section, check the box and click **Save** to enable the remote assistance function and then the technicians can access your gateway and help to solve the problems by SSH.
2) In the **Diagnostic Information** section, click **Export** to download a binary (.bin) file containing helpful information, and send it to the technicians for help.

7 LED Control

You can manually turn on or off the LED via a web browser.

Choose the menu **System Tools** > **LED Control**, check the box to turn on or off the LED.

Figure 7-1 Getting Automatically from the Internet

8 Time Settings

In Time Settings module, you can configure the following features:

- System Time
- Daylight Saving Time

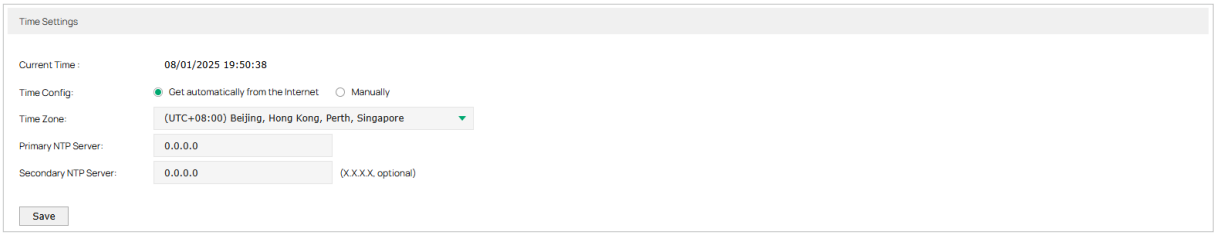
8.1 Setting the System Time

Choose one method to set the system time.

8.1.1 Getting time from the Internet Automatically

Choose the menu **System Tools** > **Time Settings** > **Time Settings** to load the following page.

Figure 8-1 Getting Automatically from the Internet



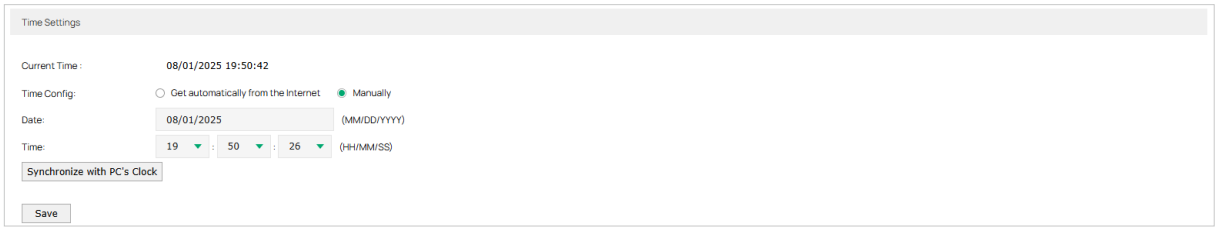
In the **Time Settings** section, configure the following parameters and click **Save**.

Current Time	Displays the current system time.
Time Config	Select **Get automatically from the Internet** to get the system time from the NTP server.
Time Zone	Select the time zone the device is in.
Primary NTP Server	Enter the IP address of the Primary NTP server.
Secondary NTP Server	Enter the IP address of the Secondary NTP server.

8.1.2 Setting the System Time Manually

Choose the menu **System Tools** > **Time Settings** > **Time Settings** to load the following page.

Figure 8-2 Setting the System Time Manually



In the **Time Settings** section, configure the following parameters and click **Save**.

Current Time	Displays the current system time.
Time Config	Select **Manually** to set the system time manually.
Date	Specify the date of the system.
Time	Specify the time of the system.
Synchronize with PC's Clock	Synchronize the system time of the gateway with PC's clock.

8.2 Setting the Daylight Saving Time

Choose one method to set the daylight saving time.

8.2.1 Predefined Mode

Choose the menu **System Tools** > **Time Settings** > **Time Settings** to load the following page.

Figure 8-3 Predefined Mode Page

In the **Daylight Saving Time** section, select one predefined DST schedule and click **Save**.

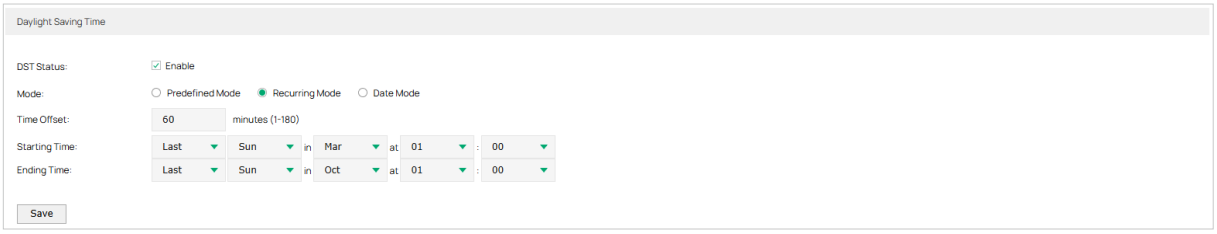
DST Status	Check the box to enable the DST function.
Mode	Select **Predefined Mode** to choose a predefined daylight saving time.
USA	Select the Daylight Saving Time of the USA. It is from 2: 00 a.m. on the Second Sunday in March to 2:00 a.m. on the First Sunday in November
Europe	Select the Daylight Saving Time of Europe. It is from 1:00 a.m. on the Last Sunday in March to 1:00 a.m. on the Last Sunday in October.

Australia	Select the Daylight Saving Time of Australia. It is from 2:00 a.m. on the First Sunday in October to 3:00 a.m. on the First Sunday in April.
New Zealand	Select the Daylight Saving Time of New Zealand. It is from 2:00 a.m. on the Last Sunday in September to 3:00 a.m. on the First Sunday in April.

8.2.2 Recurring Mode

Choose the menu **System Tools** > **Time Settings** > **Time Settings** to load the following page.

Figure 8-4 Recurring Mode Page



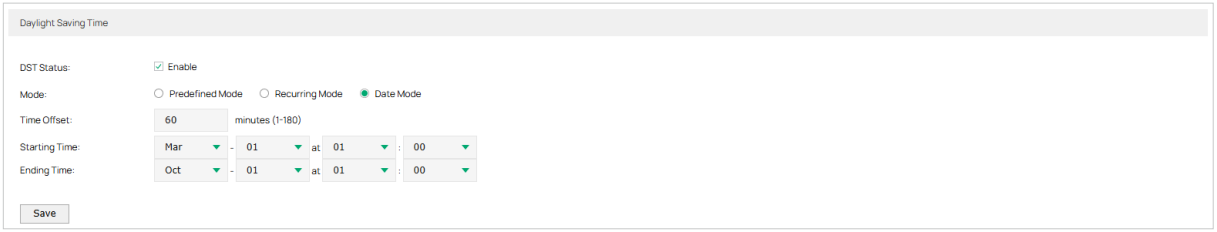
In the **Daylight Saving Time** section, configure the following parameters and click **Save**.

DST Status	Check the box to enable the DST function.
Mode	Select **Recurring Mode** to specify a cycle time range for the daylight saving time. This configuration will take effect every year.
Time Offset	Specify the time added in minutes when Daylight Saving Time takes effect.
Starting Time	Specify the starting time of Daylight Saving Time. The starting time is relative to standard time.
Ending Time	Specify the ending time of Daylight Saving Time. The ending time is relative to daylight saving time.

8.2.3 Date Mode

Choose the menu **System Tools** > **Time Settings** > **Time Settings** to load the following page.

Figure 8-5 Date Mode Page



In the **Daylight Saving Time** section, select one predefined DST schedule and click **Save**.

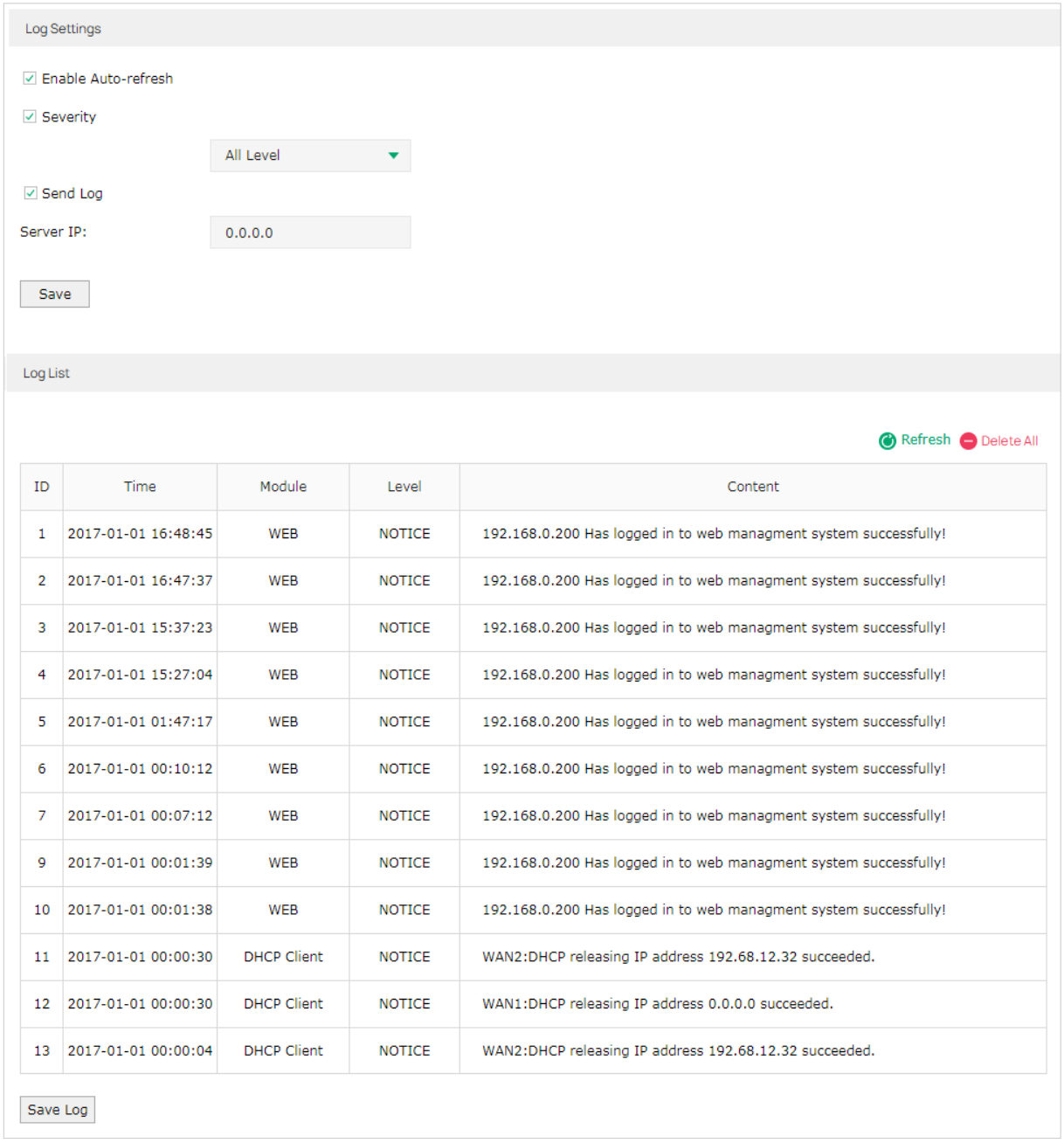
DST Status	Check the box to enable the DST function.

Mode	Select Date Mode to specify an absolute time range for the daylight saving time.
Time Offset	Specify the time added in minutes when Daylight Saving Time takes effect.
Starting Time	Specify the starting time of Daylight Saving Time. The starting time is relative to standard time.
Ending Time	Specify the ending time of Daylight Saving Time. The ending time is relative to daylight saving time.

9 System Log

Choose the menu **System Tools** > **System Log** > **System Log** to load the following page.

Figure 9-1 System Log Page



ID	Time	Module	Level	Content
1	2017-01-01 16:48:45	WEB	NOTICE	192.168.0.200 Has logged in to web managment system successfully!
2	2017-01-01 16:47:37	WEB	NOTICE	192.168.0.200 Has logged in to web managment system successfully!
3	2017-01-01 15:37:23	WEB	NOTICE	192.168.0.200 Has logged in to web managment system successfully!
4	2017-01-01 15:27:04	WEB	NOTICE	192.168.0.200 Has logged in to web managment system successfully!
5	2017-01-01 01:47:17	WEB	NOTICE	192.168.0.200 Has logged in to web managment system successfully!
6	2017-01-01 00:10:12	WEB	NOTICE	192.168.0.200 Has logged in to web managment system successfully!
7	2017-01-01 00:07:12	WEB	NOTICE	192.168.0.200 Has logged in to web managment system successfully!
9	2017-01-01 00:01:39	WEB	NOTICE	192.168.0.200 Has logged in to web managment system successfully!
10	2017-01-01 00:01:38	WEB	NOTICE	192.168.0.200 Has logged in to web managment system successfully!
11	2017-01-01 00:00:30	DHCP Client	NOTICE	WAN2:DHCP releasing IP address 192.68.12.32 succeeded.
12	2017-01-01 00:00:30	DHCP Client	NOTICE	WAN1:DHCP releasing IP address 0.0.0.0 succeeded.
13	2017-01-01 00:00:04	DHCP Client	NOTICE	WAN2:DHCP releasing IP address 192.68.12.32 succeeded.

Follow these steps to view the system log:

1) In the **Log Settings** section, configure the following parameters and click **Save**.

Enable Auto-refresh	Check the box to enable this function and the page will refresh automatically every 10 seconds.

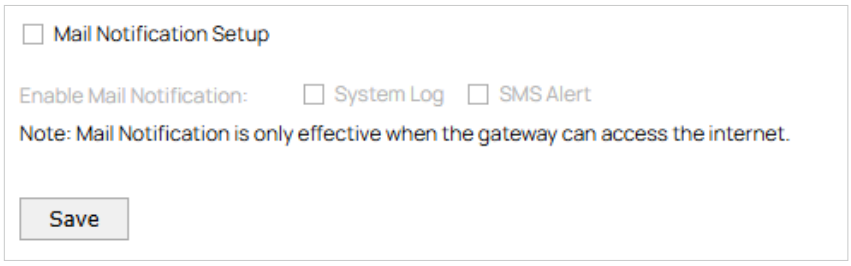
Severity	Enable Severity and specify the importance of the logs you want to view in the log list. **ALL Level**: Logs of all levels. **EMERGENCY**: Errors that render the gateway unusable, such as hardware errors. **ALERT**: Errors that must be resolved immediately, such as flash write errors. **CRITICAL**: Errors that put the system at risk, such as a failure to release memory. **ERROR**: Generic errors. **WARNING**: Warning messages, such as WinNuke attack warnings. **NOTICE**: Important notifications, such as IKE policy mismatches. **INFO**: Informational messages. **DEBUG**: Debug-level notifications, such as when the gateway receives a DNS packet.
Send Log	Enable the Send Log function and then the newly generated logs will be sent to the specified server.
Server IP	Specify the IP address of the server that the logs will be sent to.
Enable Auto Mail	With the Mail Server, the device can send the system logs. You need to enable Mail Notification Setup in **System Tools > Mail Notification**, configure related parameters and check System Log in Enable Mail.

2) (Optional) Click **Save Log** to save the current logs to the host.

10 Mail Notification

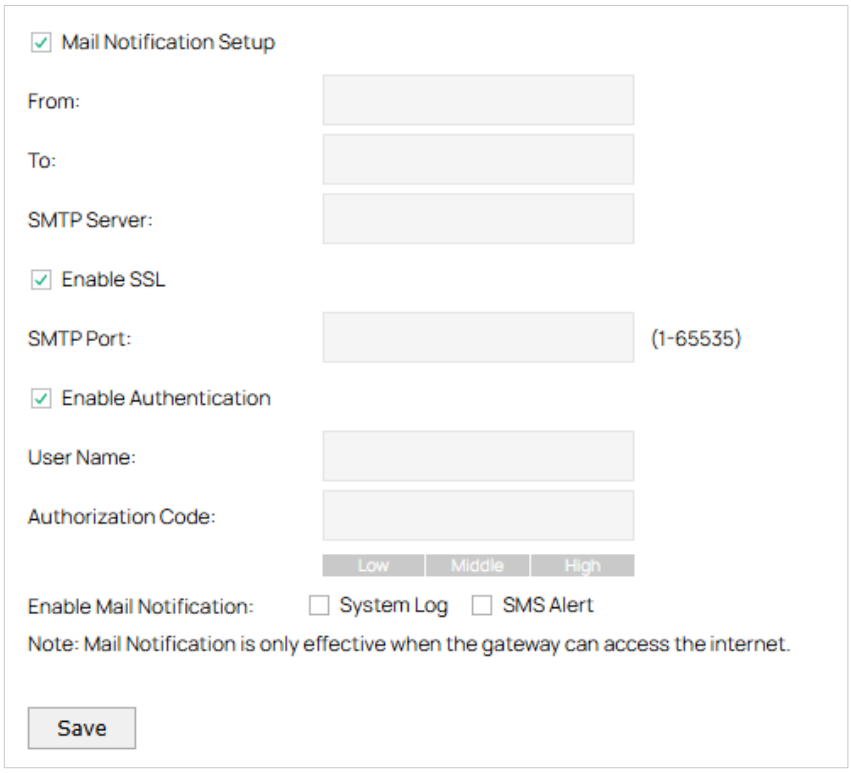
Choose the menu **System Tools** > **Mail Notification** to load the following page.

Figure 10-1 Mail Notification Page



Follow these steps to set up main notification:

1) Enable **Mail Notification Setup**, configure the following parameters and click **Save**.



Mail Notification Setup	Check the box to enable **Mail Notification**. Once enabled, you need to configure related parameters that will be used in **System Log** or **SMS Alert**.
From	Enter the email address used for sending the system log.
To	Enter the recipient's email address, which can be the same as or different from the sender's email address.
SMTP Server	Enter the domain name or IP address of the SMTP server.
Enable SSL	Enable this feature, and the data will be transmitted based on the SSL protocol.

Enable Authentication	Enable this feature if the login of the mailbox requires a username and authorization code.
User Name	Enter the email address used for sending the system log.
Authorization Code	Enter the authorization code that enables a third party to log in to the mailbox. Note that the authorization code is not the mailbox's password.
Enable Mail Notification	Configure related parameters, which will be used by the checked modules. **System Log:** When enabled, you can set the log information to be automatically sent by email in **System Tools** > **System Log**. **SMS Alert:** When enabled, if you select the second or third option in **SMS** > **SMS Settings** > **SMS Inbox**, an email reminder will be sent when the SMS inbox is full information.