



User Guide

Manage Gateway via the Omada Controller

About this Guide

Omada Controller offers centralized and efficient management for configuring enterprise networks comprised of gateways, switches, wireless access points (APs), optical line terminals (OLTs), and more. This guide provides information for centrally managing gateway via the Omada Controller. Please read this guide carefully before operation.

For instructions about how to use the Omada Controller, refer to the [Omada Controller User Guide](#). For instructions about how to manage other types of devices via the Omada Controller, refer to the relevant user guides.

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 the Omada Controller may vary due to your region, controller type and version, and device model. 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.
- This guide uses the specific formats to highlight special messages. The following table lists the notice icons that are used throughout this guide.

In this guide, the following conventions are used:

Controller	Stands for the Omada On-Premises Controller and the Omada Cloud-Based Controller.
On-Premises Controller	Includes the Omada Software Controller (also referred to as the Omada Network Application), Omada Hardware Controller, and Omada Integrated Gateway (Controller).
Cloud-Based Controller/ Omada Central	The Omada Cloud-Based Controller is now referred to as the Omada Network system on the Omada Central. Note that the Omada Central integrates the Omada Network system and Omada Guard system. The Omada Network system works as an Omada Controller to manage network devices (gateways, switches, access points, OLTs, and more), while the Omada Guard system works as a VMS system to manage surveillance devices (security cameras, NVRs, and more). This guide involves instructions about the Omada Network system. For instructions about the Omada Guard system, refer to the Omada Guard User Guide.
Note:	The note contains the helpful information for a better use of the controller.

Configuration Guidelines:

Provide guidelines for the feature and its configurations.

More Resources

Main Site	https://www.omadanetworks.com/
Video Center	https://support.omadanetworks.com/video/
Documents	https://support.omadanetworks.com/document/
Product Support	https://support.omadanetworks.com/product/
Technical Support	https://support.omadanetworks.com/contact-support/

For technical support, the latest software, and management app, visit <https://support.omadanetworks.com/>.

CONTENTS

About this Guide

Manage the Gateway

Properties Window.....	1
Device Management Window	2

Configure General Settings

Configure Internet Settings (Only for 5G Gateways)

Configure Wireless Settings (Only for Certain Gateways)

Radio Settings.....	8
WLAN Settings.....	9
Advanced Settings.....	10

SIM Configurations (Only for Gateways with SIM Card)

PIN Management.....	12
Statistics	12
SMS Message	14
SMS Settings.....	15

Transmission Settings

Network Security settings:

MAC Filtering	18
IP-MAC Binding.....	19

Configure Advanced Settings

General.....	21
DNS	22
Dynamic DNS.....	22
DNS Proxy.....	25
DNS Cache.....	26
UPnP	28
IPTV	29

1 Manage the Gateway

Launch the controller and access a site. Go to [Devices](#) > [Device List](#). In the device list, click the gateway, then you can monitor and manage it in the Properties window and Device Management window.

1.1 Properties Window

The Properties window displays the device's basic information, port status, health status, connection information, and more.

Note: The available functions in the window may vary by device type, model, and status.

The screenshot shows the 'Device List' tab in a network management interface. At the top, there are three summary cards: 'Gateway' (Good - 9), 'Switches' (1/0/0/0), and 'APs' (2/0/0/0). Below these is a search bar and filters for 'All (4)', 'Gateway/Switches (2)', 'OLTs (0)', and 'APs (2)'. A table lists four devices: 6C-4C, A8-2S, B8-FB, and B8-FB, all with status 'CONNECTED'. To the right, the 'Properties' window for the 6C-4C device is open, showing its status as 'CONNECTED' for 37 days, 16h, 31m, and 55s. It also displays port status (Used Port: 2/7), a 'Manage Device' button, and a 'Device 24h health' section with a green bar indicating good health. Below the health bar, there are sections for Temperature (49°C), CPU (1%), and Memory (41%). At the bottom, there is a 'Connection' section with 'Device' and 'Client' tabs.

DEVICE NAME	SERIAL NUMBER	MAC ADDRESS	IP ADDRESS	STATUS
6C-4C			192.168.124.1	CONNECTED
A8-2S			192.168.124.100	CONNECTED
B8-FB			192.168.124.101	CONNECTED
B8-FB			192.168.124.112	CONNECTED

Quick Operations

Click the  icon and choose an operation to quickly operate the device.

Custom Upgrade

Click [Browse](#) and choose a file from your computer to upgrade the device. After upgraded, the device will reboot and be readopted by the controller.

Download Device Info

If the device has an abnormality, you can download the device information and provide it to our R&D personnel to analyze the problem.

Note: Firmware updates are required for earlier devices to obtain complete information.

Move to Site

Select a site which the device will be moved to. After moving to another site, device configurations on the prior site will be replaced by that on the new site, and its traffic history will be cleared.

Force Provision

Click [Force Provision](#) to synchronize the configurations of the device with the controller. The device will lose connection temporarily, and be adopted to the controller again to get the configurations from the controller.

Forget This Device	Click Forget and then the device will be removed from the controller. Once forgotten, all configurations and history related to the device will be wiped out.
ISP Upgrade	(Only for 4G/5G models) Click Browse to select the ISP upgrade file and click Upgrade to upgrade the ISP information. You can download the latest ISP upgrade file from https://support.omadanetworks.com.

Network Tools

Click the  icon and choose a network tool to analyze the network.

Network Check	Test the device connectivity via ping or traceroute.
Terminal	Open Terminal to execute CLI or Shell commands.

1.2 Device Management Window

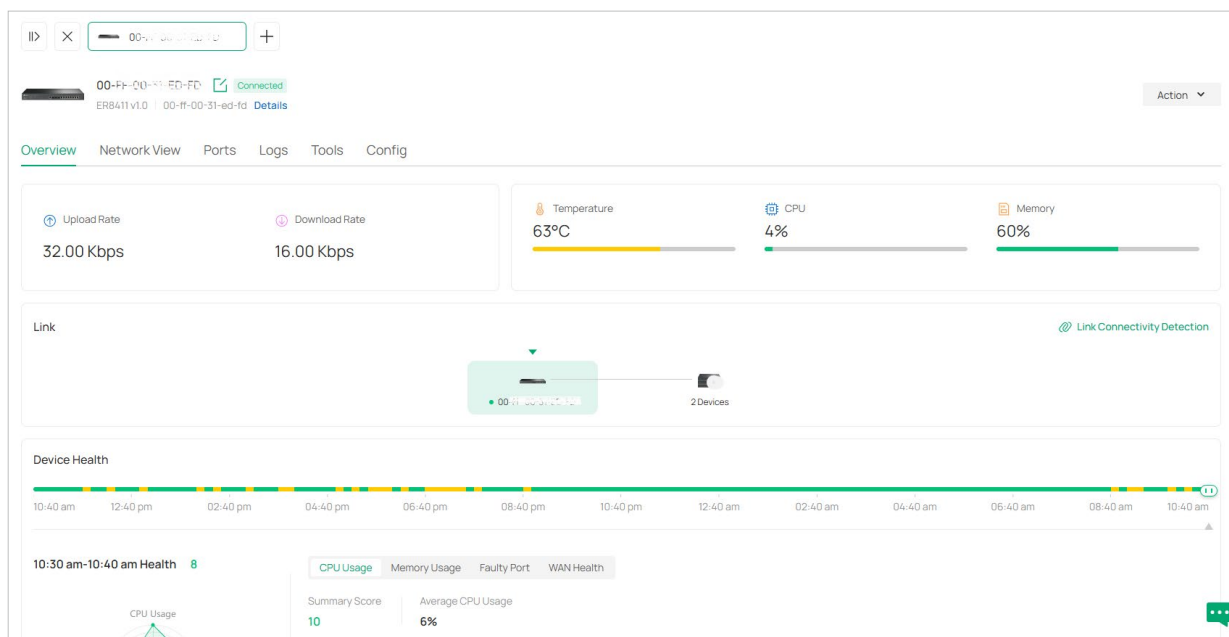
Click **Manage Device** to open the Device Management window to view more device details and change device settings.

In the management window, you can click + and select one or more devices to open new management windows, click the  icon in the top left to minimize the windows to the  icon in the right side, and click the  icon to reopen the minimized windows.

You can also click each tab to monitor and manage the device. The tabs available may vary by model.

Overview

In **Overview**, you can get an overview of the device, such as device status, link status, online time, current clients, and more.



Network View

In **Network View**, you can check the network information of the device, such as configured networks, routing table, port forwarding status, and more.

II> X [Device Icon] +

ER7206 v2.20

CONNECTED

Details

Action ▾

Overview

Network View

Ports

Logs

Tools

Config

Networks

Routing Table

Port Forwarding Status

Session Limit

QoS Data

Search Networks/IP

NETWORKS	IPv4/IPv6	TX BYTES	RX BYTES	CLIENTS
Default	192.168.0.1	10.6 GB	474.2 MB	2
2333	192.168.38.1	1.2 GB	88.5 MB	0
12333333333	192.168.30.1	1.2 KB	0	0
2-5.8.20	192.168.10.1	0	0	0
123	192.168.123.1	0	0	0
_Test201	192.168.201.1	0	0	0
_test301	192.168.46.1	0	0	0
vlan_4000	192.168.175.1	0	0	0

Ports

In **Ports**, you can view the port status and statistics and edit port settings.

II> X [Device Icon] +

ER7206 v2.20

CONNECTED

Details

Action ▾

Overview

Network View

Ports

Logs

Tools

Config

USB

SFP

2

3

4

5

6

10/100 Mbps

1000 Mbps

Disabled

Disconnected

LAN

WAN

Mirroring

Config

Statistics

PORT	NAME	DNS SERVER	IPv4/IPv6	PoE	SPEED	DUPLEX	CONNECTION	IPv4 DIAL UP	UPLOAD/DOWNLOAD PKTS	ACTION
1	SFP WAN/LAN1	0.0.0.0 0.0.0.0/-	0.0.0.0/-	-	Auto	Auto	-	Link Down	↑ 0 ↓ 0	
2	WAN2	192.168.110.1 0.0.0.0/-	192.168.110.196/-	-	Auto	Auto	-	Connected	↑ 4765262 ↓ 12671976	
3	WAN/LAN3	-/-	-/-	-	Auto	Auto	-	-	↑ 3455593 ↓ 1588978	
4	WAN/LAN4	-/-	-/-	-	Auto	Auto	98-03-8E-BE-8D-39 - WAN/LAN4	-	↑ 9686294 ↓ 4464158	

To configure a port, click the edit icon in the Action column. Port settings may vary by port type.

Status	Check the box to enable the port.
PoE Mode	Select the PoE mode: Off or 8.2.3at/af.
Link Speed	Select the speed mode for the port. Auto: The port negotiates the speed and duplex automatically. Manual: Specify the speed and duplex from the drop-down list manually.

Mirroring

Mirroring is used to analyze network traffic and troubleshoot network problems.

With Mirroring configured, the gateway will send a copy of traffic passing through the specified mirrored ports to the current port.

To use this function, enable this option to set the current port as the mirroring port, specify one or multiple mirrored ports, and specify the directions of the traffic to be mirrored in the **Mirror Mode**:

Ingress and Egress: Both the incoming and outgoing packets through the mirrored ports will be copied to the mirroring port.

Ingress: The packets received by the mirrored ports will be copied to the mirroring port.

Egress: The packets sent by the mirrored ports will be copied to the mirroring port.

Native VLAN

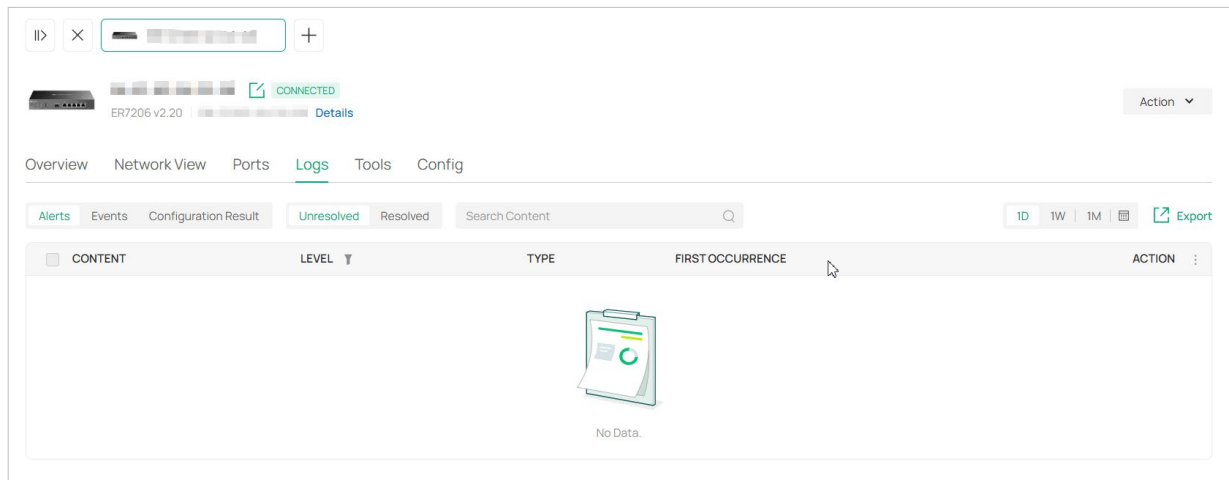
Select the Port VLAN Identifier (PVID) for the port.

Flow Control

With this option enabled, when a device gets overloaded it will send a PAUSE frame to notify the peer device to stop sending data for a specified period of time, thus avoiding the packet loss caused by congestion.

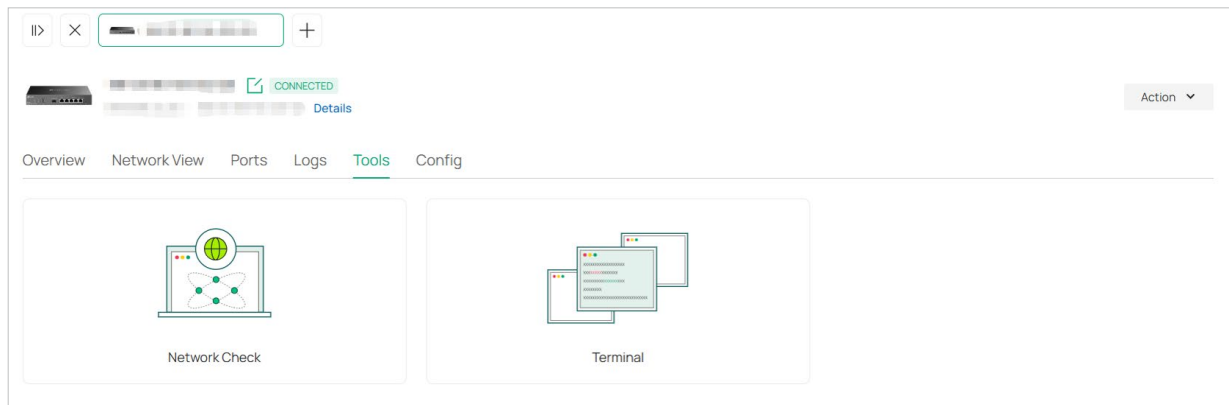
Logs

In **Logs**, you can check the logs of the device, such as alerts, events, and configuration result.



Tools

In **Tools**, you can use network tools to test the device connectivity and open Terminal to execute CLI or Shell commands.



2 Configure General Settings

In General Settings, you can specify the device name, control the LED, configure the device address, and more.

To configure general settings of a gateway, follow the steps below:

1. Launch the controller and access a site.
2. Go to [Devices](#) > [Device List](#). In the device list, click a gateway, click [Manage Device](#) and go to [Config](#) > [General](#).
3. Configure the parameters.

General

Name

Description
(Optional)

LED
☒ Use Site Settings
☐ On
☐ Off

Device Labels

Please Select...

Remember Device
☒ Use Site Settings
☐ On
☐ Off ⓘ

Others

SNMP
Manage

Location

Contact

Device Address

Address
Refresh (Optional)

Longitude/Latitude

Longitude
Latitude

(Optional)

Apply
Cancel

Name	Specify a name of the device.
Description	(Optional) Enter a description for identification.
LED	Select the way that device's LEDs work. Use Site Settings: The device's LED will work following the settings of the site. On/Off: The device's LED will keep on/off.
Device Labels	Select a label from the drop-down list or create a new label to categorize the device.
Remember Device	With this function, the controller will remember this device. After device reset and power-on, the controller will automatically adopt the device if the controller can find it.
SNMP	Configure SNMP to write down the location and contact detail. You can also click Manage to jump to Network Config > General Settings > SNMP .

Device Address	Configure the address, longitude, and latitude according to where the site is located. These fields are optional.
----------------	---

3 Configure Internet Settings (Only for 5G Gateways)

In Radios, you can control how and what type of radio signals the wireless gateway emits.

To configure radio settings of a gateway, follow the steps below:

1. Launch the controller and access a site.
2. Go to [Devices > Device List](#). In the device list, click a gateway, click [Manage Device](#) and go to [Config > Internet](#).
3. Configure the Cellular WAN and SIM dial-up settings as needed.

WAN Mode

Gateway Model

ER701-5G-Outdoor v1.0

Online Detection Interval

custom

Custom Time

10

Seconds

(1-3600)

Edit Cellular WAN

Description

(Optional)

Mobile Data

☒

SIM Priority

☒ SIM1

☐ SIM2

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.

SIM1 Dial-up Settings

APN Profile

☒ Auto

☐ Manual

Data Roaming

☐

Network Mode

5G/4G/3G

Dial-up

100

(100 - 3552s)

SIM2 Dial-up Settings

APN Profile

☒ Auto

☐ Manual

Data Roaming

☐

Network Mode

5G/4G/3G

Dial-up

100

(100 - 3552s)

Apply

Cancel

Online Detection Interval	Select how often the WAN ports detect WAN connection status. If you don't want to enable online detection, select Disable, and you can also select Custom to specify the time.
	Online Detection results will influence whether Load Balancing and Link Backup features take effect. The smaller the online detection interval, the faster Load Balancing and Link Backup features will respond, and meanwhile more detection packets will be sent.

Description	(Optional) Enter a description for identification.
-------------	--

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.
SIM1/SIM2 Dial-up Settings	
APN Profile	Select Auto or Manual. If auto is selected, the gateway will use the profile automatically assigned. If manual is selected, you can select the APN file you created before, and you can click Manage APN Profile to create new files.
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.
Dial-up	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.

4 Configure Wireless Settings (Only for Certain Gateways)

4.1 Radio Settings

In Radios, you can control how and what type of radio signals the wireless gateway emits.

To configure radio settings of a gateway, follow the steps below:

1. Launch the controller and access a site.
2. Go to [Devices](#) > [Device List](#). In the device list, click a gateway, click [Manage Device](#) and go to [Config](#) > [Wireless](#) > [Radios](#).
3. Select each band and configure the parameters. Different models support different bands.

The screenshot shows the 'Radios' configuration page. At the top, there are two tabs: '2.4 GHz' and '5 GHz'. The '2.4 GHz' tab is active. Below the tabs, the 'Status' section has a checkbox labeled 'Enable' which is checked. The 'Wireless Mode' is set to 'Auto', 'Channel Width' is '20 MHz', 'Channel' is '6 (2437 MHz)', and 'Tx Power' is 'High'. At the bottom, there are 'Apply' and 'Cancel' buttons.

Status If you disable the frequency band, the radio on it will turn off.

Wireless Mode	Specify the wireless mode of the band. Different bands have different available options. We recommend using the default value.
Channel Width	Specify the channel width of the band. Different bands have different available options. We recommend using the default value.
Channel	Specify the operation channel of the device to improve wireless performance. If you select Auto for the channel setting, the device scans available channels and selects the channel where the least amount of traffic is detected.
Tx Power	Specify the Tx Power (Transmit Power) in the 4 options: Low, Medium, High and Custom. The actual power of Low, Medium and High are based on the minimum transmit power (Min. Txpower) and maximum transmit power (Max. TxPower), which may vary in different countries and regions. Low: $\text{Min. TxPower} + (\text{Max. TxPower} - \text{Min. TxPower}) * 20\%$ (round off the value) Medium: $\text{Min. TxPower} + (\text{Max. TxPower} - \text{Min. TxPower}) * 60\%$ (round off the value) High: Max. TxPower Custom: Specify the value manually.

4.2 WLAN Settings

To configure WLAN settings of a gateway, follow the steps below:

1. Launch the controller and access a site.
2. Go to **Devices > Device List**. In the device list, click a gateway, click **Manage Device** and go to **Config > Wireless > WLANs**.
3. Configure the parameters.

The screenshot shows the 'WLANs' configuration page. It includes the following fields and options:

- Network Name (SSID):** A text input field containing 'Omada_2.4GHz_000000'.
- Band:** Three radio buttons for '2.4 GHz' (selected), '5 GHz', and '6 GHz'.
- Security:** A dropdown menu showing 'WPA-Personal'.
- WPA Mode:** A dropdown menu showing 'WPA2-PSK / AES'.
- Security Key:** A text input field with masked characters '.....' and a toggle icon.
- SSID Broadcast:** A checkbox labeled 'Enable' which is checked.
- WAN Access:** A checkbox labeled 'Enable' which is unchecked, with a help icon.
- MAC Filter:** A section with a minus icon, a label 'MAC Filter' with a help icon, and a checkbox labeled 'Enable' which is unchecked.
- Buttons:** 'Apply' and 'Cancel' buttons at the bottom left.

Network Name (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.
Band	Select the wireless band.

Security	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. When this option is selected, set the WPA mode and the security key.
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.
MAC Filter	Only 11ac and above products support this function. You can select a policy to allow or deny the connections from specific MAC addresses. Allow List: Allow connections from MAC Address(es) below. Blocks all others. Deny List: Blocks connections from MAC Address(es) below. Allows all others. You can click Manage MAC Groups to add or delete MAC addresses.

4.3 Advanced Settings

In Advanced, you can configure Load Balance, QoS, and OFDMA to improve network performance.

To configure advanced wireless settings of a gateway, follow the steps below:

1. Launch the controller and access a site.
2. Go to [Devices](#) > [Device List](#). In the device list, click a gateway, click [Manage Device](#) and go to [Config](#) > [Wireless](#) > [Advanced](#).

3. Select each band and configure the parameters. Different models support different bands.

Advanced

2.4 GHz

5 GHz

Load Balance

Maximum Associated Clients ☐ Enable

RSSI Threshold ☐ Enable ⓘ

QoS

Unscheduled Automatic Power Save Delivery ☒ Enable ⓘ

OFDMA

OFDMA ☐ Enable ⓘ

Apply

Cancel

Load Balance

Load Balance controls the clients associated to the device.

Max Associated Clients: Enable this function and specify the maximum number of connected clients. If the number of connected clients reaches the specified value, the device will disconnect those with weaker signals to make room for other clients requesting connections.

RSSI Threshold: Enable this function and enter the threshold of RSSI (Received Signal Strength Indication). If a client's signal strength is weaker than the threshold, the client will lose connection with the device.

QoS

QoS optimize the performance when handling differentiated wireless traffics, including traditional IP data, VoIP (Voice-over Internet Protocol), and other types of audio, video, streaming media.

Unscheduled Automatic Power Save Delivery: Abbreviation as U-APSD, this function greatly improves the energy-saving capacity of clients to extend their battery life, and reduces the latency of traffic flow that is delivered over the wireless media.

OFDMA

(Only for AP supporting 802.11 ax or later standards) Enable this feature to enable multiple users to transmit data simultaneously, and it will greatly improves speed and efficiency. Note that the benefits of OFDMA can be fully enjoyed only when the clients support OFDMA.

5 SIM Configurations (Only for Gateways with SIM Card)

5.1 PIN Management

In PIN Management, you can view the SIM card used and its status.

To view the SIM status, follow the steps below:

1. Launch the controller and access a site.
2. Go to [Devices](#) > [Device List](#). In the device list, click a gateway, click [Manage Device](#) and go to [Config](#) > [SIM Config](#) > [PIN Management](#).

5.2 Statistics

In Statistics, you can have a overview of the total/monthly statistics calculated according to the billing/counting method you set. You can click the edit icon to correct the statistics.

To configure WLAN settings of a gateway, follow the steps below:

1. Launch the controller and access a site.
2. Go to [Devices](#) > [Device List](#). In the device list, click a gatewa, click [Manage Device](#) and go to [Config](#) > [SIM Config](#) > [Statistics](#).
3. Configure the parameters.

[SIM 1 Statistics](#)

[SIM 2 Statistics](#)

 **Total Data Usage**
115.924 MB 

 **Monthly SMS Messages**
0 

SIM Data

Billing Method

☒ Total ☐ Monthly

Data Limit

☐

SMS Messages

Counting Method

☐ Total ☒ Monthly

Start Date

1

st

 (1-31)

SMS Quota Limit

☐

[Apply](#)

[Cancel](#)

For SIM data settings, configure the following parameter:

Billing Method	Select the billing method, Total count or Monthly count. If you select the Monthly count, select a Start Date for each monthly count cycle. For example, 2nd indicates that the monthly count cycle is from the 2nd of this month to the 1st of the next month.
Data Limit	Specify whether to enable the data limit function. If turned on, the network will be disconnected when your data usage reaches the allowance.
Total Allowance/ Monthly Allowance	Enter the total/monthly allowance provided by your carrier. The device will automatically disconnect from the internet when your data usage reaches the allowance.
Data Limit Alert	Specify whether to enable the SMS alert of data limit. If turned on, the alert message will be sent when your data usage reaches the set allowance percentage or the set allowance.
Usage Alert	Set the usage alert percentage. The alert message will be sent when your data usage reaches the set allowance percentage.
Alert SMS Phone Number	Enter the phone number to receive the SMS alert message when your data usage reaches the set allowance percentage or the set allowance.
Send Test Message	Send a test SMS to confirm that the number can receive the SMS alert message.

For SIM message settings, configure the following parameter:

Counting Method	Select the counting method, Total count or Monthly count. If you select the Monthly count, select a Start Date for each monthly count cycle. For example, 2nd indicates that the monthly count cycle is from the 2nd of this month to the 1st of the next month.
SMS Quota Limit	Specify whether to enable the SMS quota limit function. If turned on, your device will be unable to send SMS messages when your SMS quantity reaches the allowance.
Total Allowance/ Monthly Allowance	Enter the total/monthly allowance provided by your carrier. Your device will be unable to send SMS messages when your SMS quantity reaches the allowance.
SMS Quota Alert	Specify whether to enable the SMS alert of SMS limit. If turned on, the alert message will be sent when your SMS quantity reaches the set allowance percentage. Note that the alert messages will also be counted in your SMS quantity.

Usage Alert	Set the usage alert percentage. The alert message will be sent when your SMS quantity reaches the set allowance percentage.
Alert SMS Phone Number	Enter the phone number to receive the SMS alert message when your SMS quantity reaches the set allowance percentage.
Send Test Message	Send a test SMS to confirm that the number can receive the SMS alert message.

5.3 SMS Message

In this section, you check the messages you have received and sent for each card.

1. Launch the controller and access a site.
2. Go to [Devices > Device List](#). In the device list, click a gateway, click [Manage Device](#) and go to [Config > SIM Config > SMS Message](#).
3. Configure the parameters.

SIM 1 Message

SIM 2 Message

SMS Inbox Message

Refresh Clear All

FROM	MESSAGE	Date	ACTION
 No Data.			

SMS Outbox Message

Export Refresh Create New Message

 SIM 1 is not activated and the configuration will take effect only when SIM 1 is activated and supports SMS.

TO	MESSAGE	Date	ACTION
 No Data.			

SMS Inbox Message	Displays the messages you have received. You can click the Detail icon to view the SMS details.
SMS Outbox Message	Displays the messages you have successfully sent. You can click the Detail icon to view the SMS details, click Export to save outbox messages of specific time period locally, or click Create New Message to send a message.

5.4 SMS Settings

In **SMS Inbox/Outbox Policy**, you can set policies related to receiving inboxes.

- 1. Launch the controller and access a site.
- 2. Go to **Devices > Device List**. In the device list, click a gateway, click **Manage Device** and go to **Config > SIM Config > SMS Settings**.
- 3. Configure the parameters.

SMS Inbox/Outbox Policy

SMS Inbox/Outbox

☒ If SMS inbox/outbox is full, delete the oldest read SMS

☐ If SMS inbox/outbox is full, send e-mail alert to Administrator

☐ If SMS inbox/outbox is full, Forward new SMS with e-mail to Administrator

To ensure e-mail sending, please configure the Mail Server.

Apply

Cancel

SMS Inbox/Outbox	Select the SMS Inbox/Outbox Policy.
	If SMS inbox/outbox is full, delete the oldest read SMS: When the inbox/outbox is full, delete the oldest read SMS to receive the new SMS.
	If SMS inbox/outbox is full, send e-mail alert to Administrator: When the inbox/outbox is full, send an email to the administrator, and does not receive the new SMS. To ensure email sending, please configure the Mail Server.
	If SMS inbox/outbox is full, forward new SMS with e-mail to Administrator: When the inbox/outbox is full, forward the new SMS to the administrator via email. To ensure email sending, please configure the Mail Server.

In **Mail Server**, you can configure mail-related parameters. The SMS Inbox/Outbox Policy module will use the configuration information to send emails.

Mail Server

FROM

TO

SMTP Server

SSL

☐ Enable

SMTP Port

25

(1-65535)

Authentication

☐ Enable

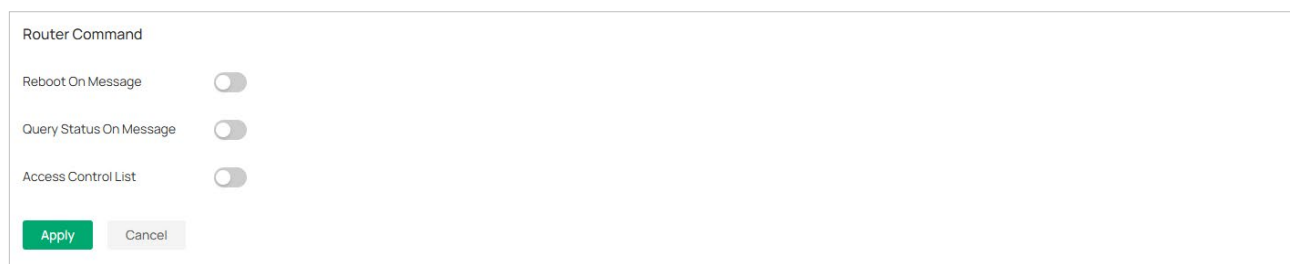
Apply

Cancel

FROM	Enter the email address of the sender.
TO	Enter the email address of the receiver, 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.
SSL	When enabled, the data will be transmitted based on the SSL protocol.
SMTP Port	Enter the port used by the SMTP server according to the instructions of your email service provider.
Authentication	If the login of the mailbox requires a username and authorization code, enable this option and configure the following parameters: User Name: Enter your email address as the username. Authorization Code: Enter the authorization code that enables a third party to log into the mailbox according to the instructions of your email service provider. Note that the authorization code is not the mailbox's password.

In **Router Command**, you can send specific commands via SMS to interact with the router, and only specific users are allowed to perform these interactions.



Router Command

Reboot On Message ☐

Query Status On Message ☐

Access Control List ☐

Apply Cancel

Reboot On Message	This feature is used to reboot the router via SMS. Enable this feature and enter the router's Password/PIN. Then you can send a message starting with "LTE Router Reboot", followed by the router's Password/PIN (e.g. LTE Router Reboot 1234) to reboot the router.
Query Status On Message	This feature is used to get status information from the router via SMS. Enable this feature, enter the router's Password/PIN, and choose the query contents. Then you can send a message starting with "LTE Router Status", followed by the router's Password/PIN (e.g. LTE Router Status 1234) to get status information from the router.
Access Control List	This feature is used to configure the allow phone number list of the above functions. Enable this feature, select the international telephone area code, and enter the phone number. You can add one or more phone numbers, and only these phone numbers can interact with the router via SMS.

6 Transmission Settings

For configuration instructions, refer to **Configure Network Transmission Settings** in the Omada Controller guide.

Routing	You can configure the following routing functions for the device. Static Route: Network traffic is oriented to a specific destination, and Static Route designates the next hop or interface where to forward the traffic. Policy Routing: Policy Routing designates which WAN port the router uses to forward the traffic based on the source, the destination, and the protocol of the traffic.
NAT	You can configure the following NAT functions for the device. Port Forwarding: Port Forwarding helps establish network connections between a host on the internet and the other in the LAN by letting the traffic pass through the specific port of the gateway. Without Port Forwarding, hosts in the LAN are typically inaccessible from the internet for the sake of security. ALG: ALG ensures that certain application-level protocols function appropriately through your gateway. One-to-One NAT: One-to-One NAT will establish a correspondence between a private IP and a public IP, allowing access to the device with the private IP through the corresponding public IP. Disable NAT: Disable NAT allows internal devices to obtain public IP addresses.
DHCP Reservation	DHCP Reservation allows you to reserve specific IP addresses for devices in your network, and centrally manage the IP addresses.
Bandwidth Control	Bandwidth Control optimizes network performance by limiting the bandwidth of specific sources.
Session Limit	Session Limit optimizes network performance by limiting the maximum sessions of specific sources.
Gateway QoS	Gateway QoS allows you to define service entries that will appear as matching conditions for you to choose when configuring the rules of related modules like QoS.

7 Network Security settings:

For configuration instructions of the following functions, refer to **Configure Network Security** in the Omada Controller guide.

ACL	ACL (Access Control List) allows a network administrator to create rules to restrict access to network resources. ACL rules filter traffic based on specified criteria such as source IP addresses, destination IP addresses, and port numbers, and determine whether to forward the matched packets.
URL Filtering	URL Filtering allows a network administrator to create rules to block or allow certain websites, which protects it from web-based threats, and deny access to malicious websites.
Application Control	DPI (Deep Packet Inspection) helps you identify, analyze, and control the traffic at the application layer in the network. DPI engine includes the latest application identification signatures to track which applications are using the most bandwidth. You can better manage and distribute network traffic usage through DPI.

IDS/IPS	IDS/IPS is a security mechanism that detects intrusions based on attack characteristics. It can detect malware, Trojan horses, worms, ActiveX and other attacks to protect the network security of users.
Firewall	Firewall is used to enhance the network security.

7.1 MAC Filtering

Overview

MAC Filtering can drop or allow packets from certain devices passing through the router based on the MAC address of the devices. After the MAC filtering policy and MAC filtering list are configured, the router will apply the filter policy to the packets matching the MAC address, and thus limit network traffic and manage network access behaviors.

Configuration

1. Launch the controller and access a site.
2. Go to [Device Config](#) > [Gateway](#) > [MAC Filtering](#) for all gateways in the site, or go to [Devices](#) > [Device List](#), and in the device list, click a gateway, click [Manage Device](#) and go to [Config](#) > [Network Security](#) > [MAC Filtering](#) for a specific gateway.
3. Enable [MAC Filtering](#) and configure the parameters.

Type	Select the mode of MAC Filtering. Allow packets with the MAC addresses listed below and deny the rest : Select to allow packets with the listed MAC address to pass through the router, and packets with other MAC addresses will be dropped. Deny packets with the MAC addresses listed below and allow the rest : Select to drop packets with the listed MAC address, and packets with other MAC addresses will be allowed to pass through the router.
Direction	Select All when you want to apply the policy to traffic both from LAN to LAN and from LAN to WAN. Select LAN -> WAN when you want to apply the policy only to traffic from LAN to WAN.

4. Click [Add MAC Filtering](#) to add MAC addresses or groups to the list.

Add MAC Filtering

Name

Policy

☒ MAC Group

☐ MAC Address

MAC Group

Please Select...

Create

Cancel

Name	Specify the name for the entry.
Policy	Choose MAC Group and specify the MAC groups of devices, then the MAC filtering policy will be applied to traffic with the MAC groups. Choose MAC Address and specify the MAC addresses of devices, then the MAC filtering policy will be applied to traffic with the MAC addresses.

7.2 IP-MAC Binding

Overview

ARP (Address Resolution Protocol) is used to map IP addresses to the corresponding MAC addresses so that packets can be delivered to their destinations. However, if attackers send ARP spoofing packets with false IP address-to-MAC address mapping entries, the device will update the ARP table based on the false ARP packets and record wrong mapping entries, which results in a breakdown of normal communication.

Anti ARP Spoofing can protect the network from ARP spoofing attacks. It works based on the IP-MAC Binding. These entries record the correct one-to-one relationships between IP addresses and MAC addresses. When receiving an ARP packet, the gateway checks whether it matches any of the IP-MAC Binding entries. If not, the gateway will ignore the ARP packets. In this way, the gateway maintains the correct ARP table.

Configuration

1. Launch the controller and access a site.
2. Go to [Device Config](#) > [Gateway](#) > [IP-MAC Binding](#) for all gateways in the site, or go to [Devices](#) > [Device List](#), and in the device list, click a gateway, click [Manage Device](#) and go to [Config](#) > [Network Security](#) > [IP-MAC Binding](#) for a specific gateway.

3. Enable **ARP Spoofing Defense** and configure general settings. Click **Apply**.

General

ARP Spoofing Defense

☒ Enable

☒ Permit the packets matching the IP-MAC Binding entries only

☒ Send GARP packets when ARP attack is detected

Interface

Please Select...

▼

Interval

1000ms

(1-10000)

Apply

Cancel

ARP Spoofing Defense	Check the box to globally enable ARP Spoofing Defense.
Permit the packets matching the IP-MAC Binding entries only	With this option enabled, when receiving a packet, the router will check whether the IP address, MAC address and receiving interface match any of the IP-MAC Binding entries. Only the matched packets will be forwarded. This feature can be enabled only when ARP Spoofing Defense is enabled.
Send GARP packets when ARP attack is detected	With this option enabled, the router will send GARP packets to the hosts if it detects ARP spoofing packets on the network. The GARP packets will inform the hosts of the correct ARP information, which is used to replace the wrong ARP information in the hosts. This feature can be enabled only when ARP Spoofing Defense is enabled.
Interface	Select the interface on which the entries will take effect.
Interval	Specify the time interval for sending GARP packets. The valid values are from 1 to 10000.

4. Click **Create New IP-MAC Binding Entry** and add an IP-MAC binding entry. Click **Apply**.

Create New IP-MAC Binding Entry

×

IP Address

.

.

.

MAC Address

-

-

-

-

-

Interface

Please Select...

▼

Description

(Optional)

Export to DHCP Address Reservation

☒ Enable

?

Status

☒ Enable

Apply

Cancel

IP Address	Specify the IP address to be bound.
------------	-------------------------------------

MAC Address	Specify the MAC address to be bound.
Interface	Select the interface on which the entries will take effect.
Description	(Optional) Enter a description for identification.
Export to DHCP Address Reservation	When enabled, the newly created IP-MAC Binding entry will be synchronized to DHCP Reservation list
Status	Enable the entry. Only when the status is enabled will the entry take effect.

8 Configure Advanced Settings

8.1 General

You can configure advanced settings to make better use of network resources.

1. Launch the controller and access a site.
2. Go to [Devices > Device List](#). In the device list, click a gateway, click [Manage Device](#) and go to [Config > Advanced > General](#).
3. Configure the parameters.

General

Hardware Offload ☒ Enable ⓘ

LLDP ☐ Use Site Settings ☒ On ☐ Off ⓘ

Echo Server ☒ Auto ☐ Custom

[Save](#) [Cancel](#)

Hardware Offload	With this feature enabled, packet forwarding performance will be improved and CPU utilization will be reduced. Note that this feature cannot take effect if the QoS is enabled.
LLDP	LLDP (Link Layer Discovery Protocol) can help discover devices..
Echo Server	Echo Server is used to test the connectivity and monitor the latency of the network automatically or manually. If you click Custom , enter the IP address or hostname of your custom server.

8.2 DNS

8.2.1 Dynamic DNS

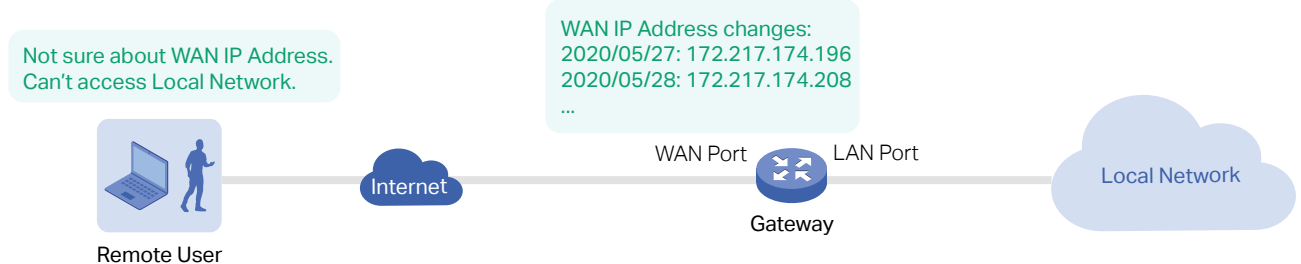
Overview

WAN IP Address of your gateway can change periodically because your ISP typically employs DHCP among other techniques. This is where Dynamic DNS comes in. Dynamic DNS assigns a fixed domain name to the WAN port of your gateway, which facilitates remote users to access your local network through WAN Port.

Let's illustrate how Dynamic DNS works with the following figures.

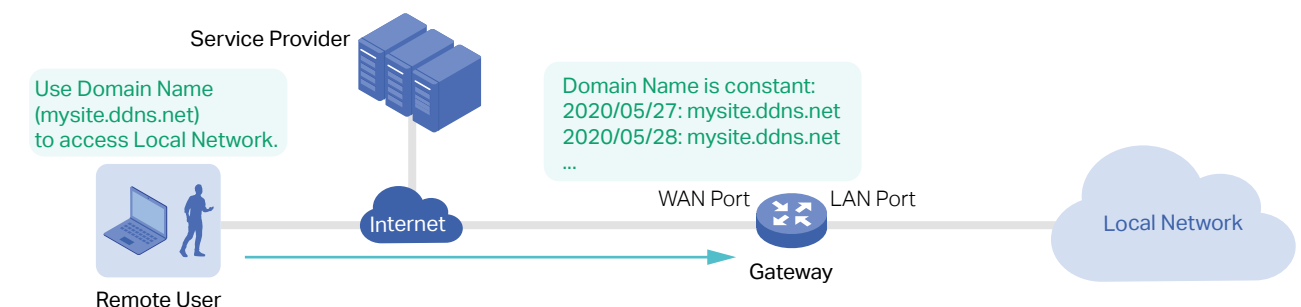
Before:

- WAN IP Address can change periodically, if it's dynamically assigned by the ISP using DHCP among other techniques.
- Remote User doesn't know what WAN IP Address is exactly at the moment, and cannot access Local Network.



After:

- Remote User can simply use Domain Name to access Local Network through WAN Port. In this example, Domain Name is `mysite.ddns.net`.

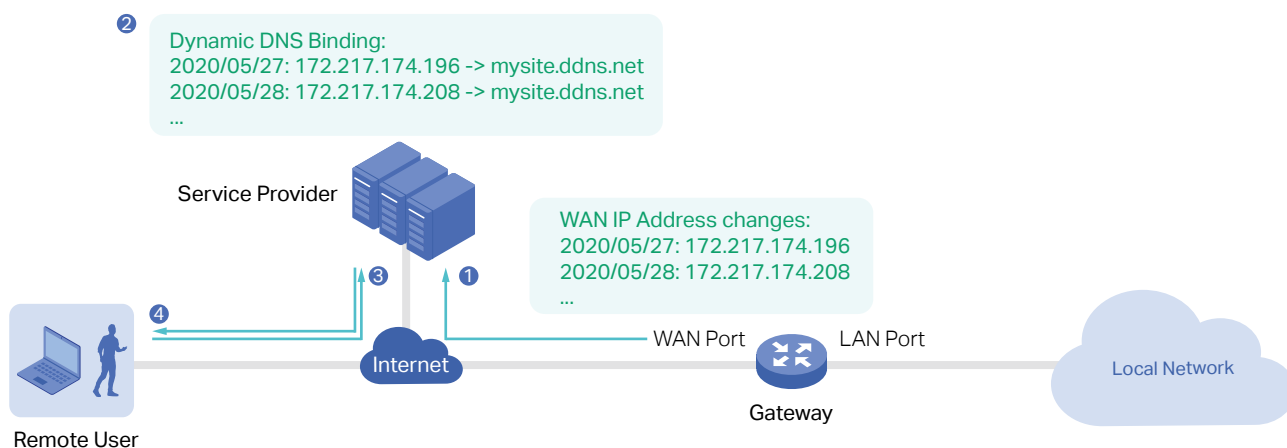


Prerequisite:

- Choose one [Service Provider](#) from the four that the controller supports, i.e. [DynDNS](#), [No-IP](#), [Peanuthull](#), [Comexe](#), [TP-Link Dynamic DNS](#).
- Register at your [Service Provider](#), then you get your [Username](#) and [Password](#).
- Get your [Domain Name](#) from your [Service Provider](#).

How Dynamic DNS works:

- 1 Gateway informs [Service Provider](#) of [WAN IP Address](#).
- 2 [Service Provider](#) binds [WAN IP Address](#) with [Domain Name](#) and keeps it updated as WAN IP Address changes.
- 3 Remote User requests for [WAN IP Address](#) by sending [Domain Name](#) to [Service Provider](#).
- 4 [Service Provider](#) replies with [WAN IP Address](#), which Remote User actually uses to access Local Network through [WAN Port](#).



Configuration

1. Launch the controller and access a site.
 1. Go to [Device Config](#) > [Gateway](#) > [DNS](#) > [Dynamic DNS](#) for all gateways in the site, or go to [Devices](#) > [Device List](#), and in the device list, click a gateway, click [Manage Device](#) and go to [Config](#) > [Advanced](#) > [DNS](#) > [Dynamic DNS](#) for a specific gateway.
2. Click [Create New Dynamic DNS Entry](#), to load the following page. Configure the parameters.

Create New Dynamic DNS Entry ⓘ

Service Provider

DynDNS

Status

☒ Enable

Interface

Username

Go To Register ⓘ

Password

Domain Name

Interval Mode

☒ Fixed
☐ Custom

Update Interval

Apply

Cancel

Service Provider	Select your service provider of Dynamic DNS. The Controller supports DynDNS, NO-IP, Peanuthull, Comexe and Custom.
Status	Enable or disable the Dynamic DNS entry.
Interface	Select the WAN Port which the Dynamic DNS entry applies to.
Username	Enter your username for the service provider. If you haven't registered at the service provider, click Go To Register .
Password	Enter your password for the service provider.
Domain Name	Enter the Domain Name which is provided by your service provider. Remote users can use the Domain Name to access your local network through WAN port.
Interval Mode	Choose to use fixed or custom interval.
Update Interval	Specify the update interval to report the changes of the WAN IP address for the DDNS service.
Update URL	Enter the URL provided by your DDNS service provider in format of "http://[USERNAME]:[PASSWORD]@api.cp.easydns.com/dyn/tomato.php?hostname=[DOMAIN]&myip=[IP]". The router will automatically update user information to the service provider.

- Click **Create**. The new entry will be listed. You can check the Dynamic DNS status in the STATUS column.

SERVICE PROVIDER	INTERFACE	STATUS	USERNAME	DOMAIN NAME	IP	UPDATE INTERVAL	LAST UPDATED	ENABLED	ACTION
DynDNS	WAN2	disconnect	■@yopmail.net	■	■	1 hour	Oct 26, 2025 11:44:47	☒	✎ 🗑

8. 2. 2 DNS Proxy

Overview

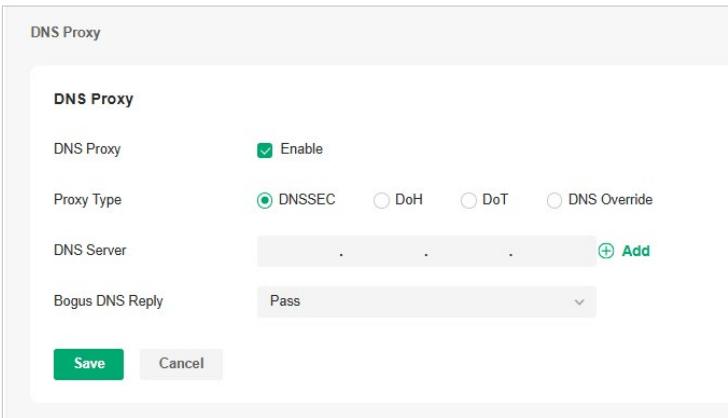
DNS Proxy provides the LAN side clients with the DNS query service. It forwards the DNS request from the LAN side clients to the selected upstream DNS server and forwards the DNS reply accordingly.

DNSSEC (DNS Security Extensions), DoT (DNS over TLS), DoH (DNS over Https), and DNS Override are security options for DNS Proxy. DNSSEC will verify the integrity of DNS records, and DoT / DoH will encrypt the query. DNS Override lets you choose your preferred DNS servers.

All the options need an upstream DNS server that supports them.

Configuration

1. Launch the controller and access a site.
2. Go to [Device Config](#) > [Gateway](#) > [DNS](#) > [DNS Proxy](#) for all gateways in the site, or go to [Devices](#) > [Device List](#), and in the device list, click a gateway, click [Manage Device](#) and go to [Config](#) > [Advanced](#) > [DNS](#) > [DNS Proxy](#) for a specific gateway.
3. Enable [DNS Proxy](#) and configure the parameters, then save the settings.



Proxy Type	Specify a security option to apply.
DNS Server	Specify the upstream DNS server which the DNS requests will be forwarded to. For DoT and DoH, the system provides some known public DNS servers that support these security options. For DoH, the upstream DNS servers are usually websites with https URLs. For DNSSEC and DoT, servers are usually IP address.
Bogus DNS Reply	This is an special option for DNSSEC. Choose to pass/drop the bogus reply if the integrity of DNS records failed to be verified (which means the DNS record may be modified and is not trustable).
Primary DNS Server	Specify the primary upstream DNS server.
Secondary DNS Server	Specify the secondary upstream DNS server.
Apply Network	Specify the effective LAN network to apply DNS Override.

8. 2. 3 DNS Cache

Overview

DNS caching further speeds up domain name translation/resolution by handling it for recently visited addresses before the request is sent to the internet. Even if your network can use a large number of public DNS servers for translation/resolution, it's still faster to have a local copy.

Configuration

1. Launch the controller and access a site.
2. Go to [Device Config > Gateway > DNS > DNS Cache](#) for all gateways in the site, or go to [Devices > Device List](#), and in the device list, click a gateway, click [Manage Device](#) and go to [Config > Advanced > DNS > DNS Cache](#) for a specific gateway.
3. Enable [DNS Cache](#) and set a TTL value according to your needs. Then save the settings.

DNS Cache

Enable DNS Cache

☒ Enable

TTL

seconds

(Optional, 1 - 86400)

Save

Cancel

TTL

Specify the time to live (TTL) value in seconds. When the life cycle of the DNS entry exceeds the TTL value, the DNS cache will be automatically cleared. The range is 1-86400. If it's not specified, the system will use the default TTL value of each DNS message.

4. Refresh the DNS Cache Table and check the DNS cache status. You can clear the cache information if necessary.

DNS Cache Table

IPv4

IPv6

Refresh

Clear

DOMAIN NAME	IP ADDRESS	TTL
a.root-servers.net		4

For a wireless gateway, you can configure Load Balance and QoS to make better use of network resources. Load Balance can control the client number associated to the device, while QoS can optimize the performance when handling differentiated wireless traffics, including traditional IP data, VoIP (Voice-over Internet Protocol), and other types of audio, video, streaming media.

Select each band and configure the following parameters and features.

Max Associated Clients	Enable this function and specify the maximum number of connected clients. If the connected client reaches the maximum number, the device will disconnect those with weaker signals to make room for other clients requesting connections.
RSSI Threshold	Enable this function and enter the threshold of RSSI (Received Signal Strength Indication). If the client's signal strength is weaker than the threshold, the client will lose connection with the device.
Unscheduled Automatic Power Save Delivery	When enabled, this function can greatly improve the energy-saving capacity of clients.
OFDMA	(Only for AP supporting 802.11 ax or later standards) Enable this feature to enable multiple users to transmit data simultaneously, and it will greatly improves speed and efficiency. Note that the benefits of OFDMA can be fully enjoyed only when the clients support OFDMA.

8.3 UPnP

Overview

UPnP (Universal Plug and Play) is essential for applications including multiplayer gaming, peer-to-peer connections, real-time communication (such as VoIP or telephone conference) and remote assistance, etc. With the help of UPnP, the traffic between the endpoints of these applications can freely pass the gateway, thus realizing seamless connections.

Configuration

- 1. Launch the controller and access a site.
- 2. Go to [Device Config](#) > [Gateway](#) > [UPnP](#) for all gateways in the site, or go to [Devices](#) > [Device List](#), and in the device list, click a gateway, click [Manage Device](#) and go to [Config](#) > [Advanced](#) > [UPnP](#) for a specific gateway.
- 3. Enable UPnP globally and configure the parameters. Then click [Apply](#).

UPnP ⓘ

UPnP

Interface

☐ USB Modem

☐ SFP WAN/LAN1

☐ WAN2

Networks

Please Select...

▼

Apply

Reset

Interface	Select the WAN port where UPnP takes effect.
Networks	Select the LAN interface where UPnP takes effect.

8.4 IPTV

Overview

IPTV includes two sections: IGMP and IPTV. In IGMP settings, you can enable IGMP proxy to detect multicast group membership information and thus the router is able to forward multicast packets based upon the information. IPTV settings allows you to enable Internet/IPTV/Phone service provided by your ISP.

Configuration

- 1. Launch the controller and access a site.
- 2. Go to [Device Config](#) > [Gateway](#) > [IPTV](#) for all gateways in the site, or go to [Devices](#) > [Device List](#), and in the device list, click a gateway, click [Manage Device](#) and go to [Config](#) > [Advanced](#) > [IPTV](#) for a specific gateway.
- 3. Enable [IGMP Proxy](#) and configure the parameters.

IGMP

IGMP Proxy

IGMP Version

v2

IGMP Interface

WAN2

IGMP Proxy	Enable IGMP Proxy. IGMP Proxy sends IGMP querier packets to the LAN ports to detect if there is any multicast member connected to the LAN ports.
IGMP Version	Select the IGMP version as V2 or V3. The default is IGMP V2.
IGMP Interface	Select the WAN port on which the IGMP Proxy takes effect.

- 4. If you want to configure the IPTV settings, enable [IPTV](#) and choose the mode as Bridge or Custom according to your ISP. Then configure the corresponding parameters.

Note: The IPTV section will be hidden if your device is an earlier version that does not support this feature.

