Outdoor IIoT BSU
Outdoor WiFi LoRa BSU
OOP851-00L42

User Manual

Outdoor WiFi LoRa BSU

Outdoor WiFi LoRa BSU

Outdoor WiFi LoRa BSU

Chapter 1 Introduction

1.1 Introduction

Congratulations on your purchase of this outstanding product: OOP851 Outdoor WiFi LoRa BSU. For wireless M2M (Machine to Machine) applications, AMIT Outdoor WiFi LoRa BSU is absolutely the right choice. With built-in 8-channel LoRa gateway, your deployed LoRa end-nodes can easily connected to the gateway, and your application server / customer server can access to the data transferred from the end-nodes, and further make adequate control on your needs.

To be working well in different outdoor environment, OOP851 series products equip an IP67 compliant plastic/metal housing, and also with anti-UV coating on it. Together with its wall and pole mounting kit, it is easy and flexible to install in various outdoor sites. Built in an 802.3at standard compliant PoE (Power over Ethernet) PD, it's easy to power up this outdoor router via an Ethernet cable and a standard PoE power supply unit.

Main Features:
- Built-in 802.11ac/11n 5G/2.4GHz selectable WiFi module for wireless uplink applications.
- Embedded an 8-channel LoRa gateway module for connecting with multiple LoRa nodes.
- LoRaWAN Compliance gateway, forward received LoRa packets to network server.
- Provide one Gigabit Ethernet port for comprehensive LAN connection.
- Support the robust remote or local management to monitor network.
- Designed by robust and easy-to-mount IP67 metal body for outdoor environment.

Before you install and use this product, please read this manual in detail for fully exploiting the functions of this product.

Outdoor WiFi LoRa BSU

1.2 Contents List

1.2.1 Package Contents
#Standard Package

Items	Description	Contents	Quantity
1	OOP851-00L42 Outdoor WiFi LoRa BSU		1pcs
2-1	Mounting Bracket		1pcs
2-2	Stalnless Metal Ring		2pcs
2-3	Screw M6*L16 WasherID6.6*OD11.8*T1.5 Sprlng ID6.4*OD9.6*T1.6		4pcs
2-4	ScrewØ5.9*L24.5 Plactic FixingØ6.7*30.5		4pcs
3	Cable Gland		1pcs
4	Ootdoor Cellular/ LoRa Antenna		1pcs
5	WIFI 2.4/5G Ootdoor Antenna		2pcs

Outdoor WiFi LoRa BSU

1.2.2 Optional Accessories

#Optional parts (these parts are sold separately)

Items	Description	Contents	Comments
1	**802.3at Compliant PoE Power Injector (Gigabit, 30W)**		Standard 802.3 af/at compliant
2	**Compatible Passive PoE Power Injector (Gigabit, 30W)**		Passive PoE Injector AMIT ODG/ODP series only

These parts are sold separately. If necessary, please contact us via sales@amit.com.tw

Outdoor WiFi LoRa BSU

1.3 Hardware Configuration

➢ Lower-side View

| N-Type Jack (Female) Conncctor for WiFi 2.4G/5GHz Ant. | LED Indicators / Reset Button | N-Type Jack (Female) Conncctor for WiFi 2.4G/5GHz Ant. |

Auto MDI/MDIX RJ45 Port, PoE Input
1x GE LAN to connect local devices
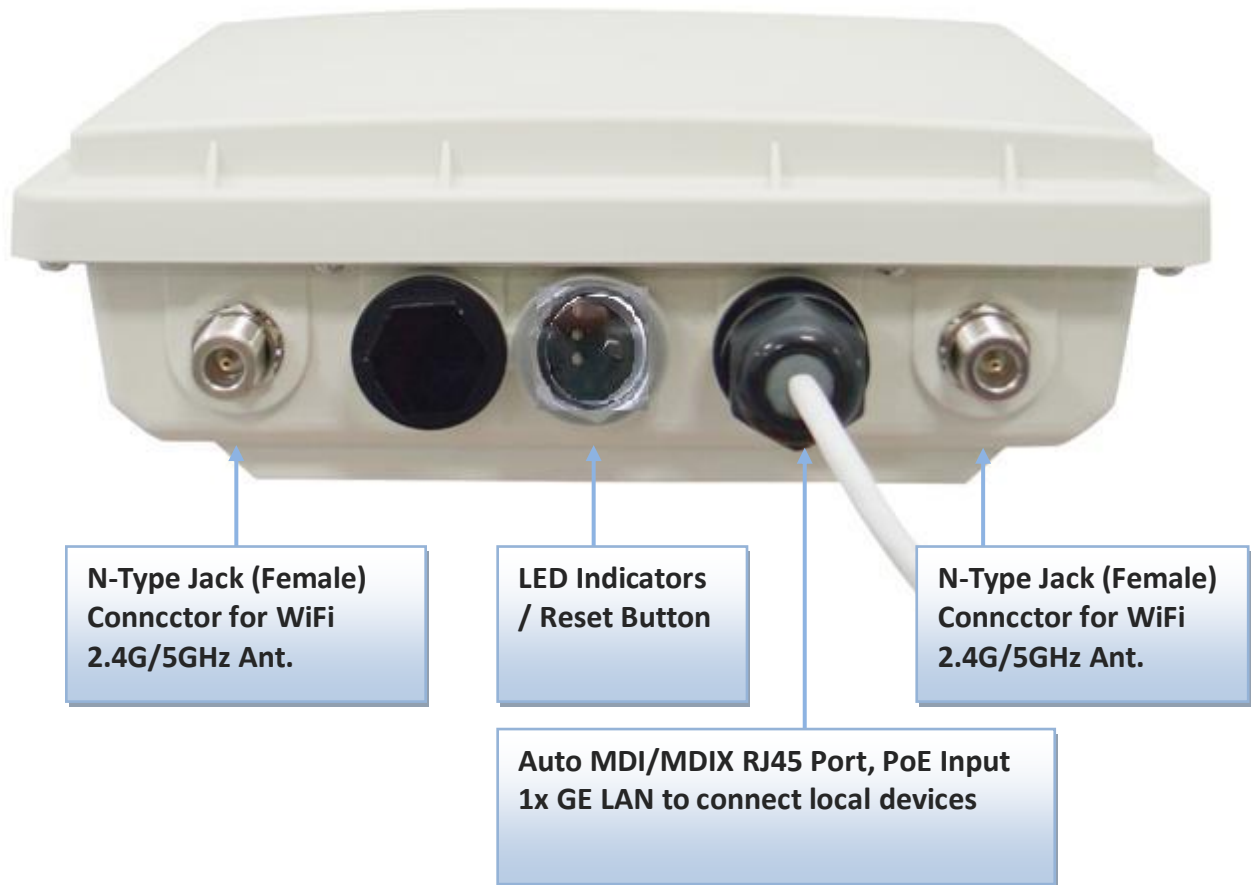
※Reset Button
The RESET button provides user with a quick and easy way to restore the default setting. Press the RESET button continuously for 6 seconds, and then release it. The device will restore to factory default settings.

Outdoor WiFi LoRa BSU

➢ Front View

N-Type Jack (Female) Conncctor for LoRa Ant

N-Type Jack (Female) Conncctor for WiFi 2.4G/5GHz Ant.

N-Type Jack (Female) Conncctor for WiFi 2.4G/5GHz Ant.

Outdoor WiFi LoRa BSU

➢ Bottom View

Wall Mounting Kit

Outdoor WiFi LoRa BSU

1.4 LED Indication

Uplink

LoRa

Status

LED Icon	Indication	LED Color	Description
Uplink	Uplink Status	Green	**OFF:**Uplink is disconnected **ON:** Uplink is connected **Flash:** Data packet transferred via Uplink connection
LoRa	LoRa Status	Green	**OFF:** LoRa Gateway is disabled **Green and Steady ON:** LoRa Gateway is enabled.
Status	Power Status	Green	**OFF:** Device is powered off **Flash (per second):** Device works normally **Fast Flash:** Device is in Recover Mode or abnormal situation

1.5 Installation & Maintenance Notice

1.5.1 SYSTEM REQUIREMENTS

Network Requirements	• An Gigabit Ethernet RJ45 cable • IEEE 802.11a/b/g/n/ac wireless network • IEEE 802.11a/b/g/n/ac wireless clients • 10/100/1000 Ethernet adapter on PC
Web-based Configuration Utility Requirements	**Computer with the following:** • Windows®, Macintosh, or Linux-based operating system • An installed Ethernet adapter **Browser Requirements:** • Internet Explorer 6.0 or higher • Chrome 2.0 or higher • Firefox 3.0 or higher • Safari 3.0 or higher

1.5.2 WARNING

Attention

● Only use the PoE Injector that is compliant to the power rating of the the product. Using a different voltage rating power adaptor is dangerous and may damage the product.

● Do not open or repair the case yourself. If the product is too hot, turn off the power immediately and have it repaired at a qualified service center.

Outdoor WiFi LoRa BSU

Federal Communication Commission Interference Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FOR PORTABLE DEVICE USAGE (<20m from body/SAR needed)

Radiation Exposure Statement:

The product comply with the FCC portable RF exposure limit set forth for an uncontrolled environment and are safe for intended operation as described in this manual. The further RF exposure reduction can be achieved if the product can be kept as far as possible from the user body or set the device to lower output power if such function is available.

FOR MOBILE DEVICE USAGE (>20cm/low power)

Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

FOR COUNTRY CODE SELECTION USAGE (WLAN DEVICES)

Note: The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all WiFi product marketed in US must fixed to US operation channels only.

1.5.3 HOT SURFACE CAUTION

CAUTION: The surface temperature for the metallic enclosure can be very high!
Especially after operating for a long time, installed at a closed cabinet without air conditioning support, or in a high ambient temperature space.
DO NOT touch the hot surface with your fingers while servicing!!

1.5.4 Product Information for CE RED Requirements

The following product information is required to be presented in product User Manual for latest CE RED requirements. [1]

(1) Frequency Band & Maximum Power

Band	Operating Frequency	Max. Output Power (EIRP)
868M	863 - 870MHz	100 mW
2.4G	2.4 – 2.4835 GHz	100 mW
5G	5.15 – 5.25 GHz	200 mW

(2) 5150 ~ 5350MHz In Door Use Statements
This product equips the IEEE 802.11ac compliance 5GHz wireless radio module. According to the RED requirement, the channels covered in the 5150 ~ 5350 MHz frequency band are In Door Use Only.

(3) Contries List for Restrictions (for products with 5GHz radio)

For EU/EFTA, this product can be used in all EU member states and EFTA countries.

AT	BE	BG	CH	CY	CY	DK
DE	EE	EL	ES	FI	FR	HR
HU	IE	IT	LT	LU	LV	MT
NL	NO	PL	PT	RO	SI	SK
SE	TR	UK				

(4) DoC Information
You can get the DoC information of this product from the following URL:
http://www.amitwireless.com/products-doc/

(5) RF Exposure Statements
The antenna of the product, under normal use condition, is at least 20 cm away from the body of user.

---

[1] The information presented in this section is ONLY valid for the EU/EFTA regional version. For those non-CE/EFTA versions, please refer to the corresponding product specification.

Outdoor WiFi LoRa BSU

(6) Unit Mounting Notice

The product is suitable for mounting at heights <= 2m (approx. 6 ft), or in a cabinet.

Ensure the unit is fixed tightly to reduce the likelyhood of injury due to exposure to mechanical hazards if dropped.

(7) Manufacture Information

Manufacture Name: AMIT Wireless Inc.

Manufacture Address: No. 28, Lane 31, Sec. 1, Huandong Rd., Xinshi Dist., Tainan 74146, Taiwan (R.O.C.)

Outdoor WiFi LoRa BSU

1.6 Hardware Installation

This chapter describes how to install and configure the hardware

1.6.1 Mount the Kits

The OOP851 series product can be mounted on wall or pole. It has designed with wall-mount bracket for attaching to the wall, or fixing on a pole by metal rings.

Wall Mount Bracket

Metal Ring for Pole Mount

Combined together
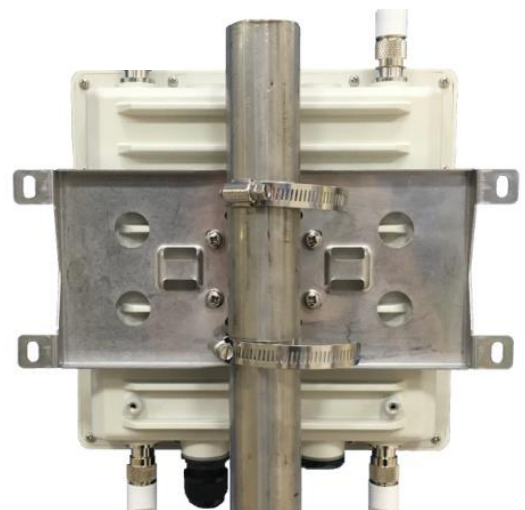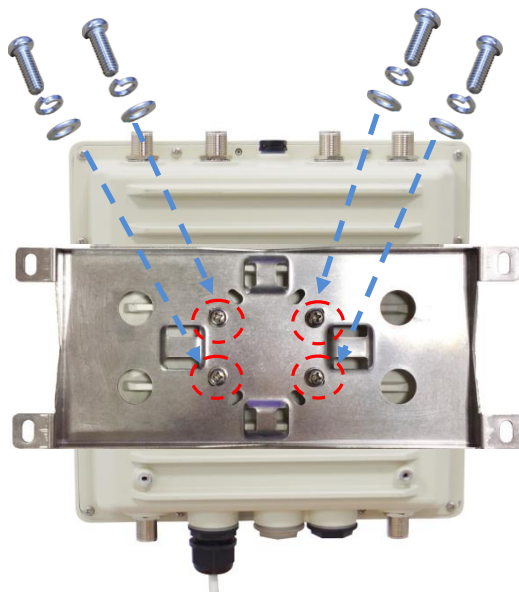
Outdoor WiFi LoRa BSU

1.6.2 Connecting PoE Power

The OOP851 series product is designed to be powered by IEEE 802.3at compliant PoE Injector, or proprietary passive PoE Injector that is listed in optional parts in Section 1.2.2. **Use other 3rd-party's passive PoE Injector is dangerous and may cause damage to the device.** Please follow instructions below to connect PoE power to this device.

Step 1:
Remove RJ45 cover.
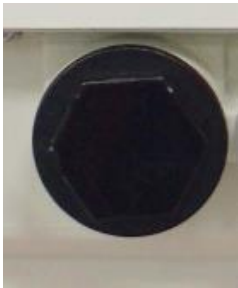
Step 2:
Plug Ethernet cable into RJ-45 connector and under the cable gland

Step 3:
Insert RJ45 Ethernet cable firmly and settle cable in the fillister

Step 4:
Put back cable gland to the housing and fasten cable gland firmly

Step 5:
Connect the other RJ45 plug of the Ethernet cable to RJ45 connector (marked as P+D/OUT) of the PoE Injector.

Step 6:
Connect the power cord of PoE Injector to an AC power socket.

1.6.3 Connecting to the Network or a Host

The OOP851 series products provide one Gigabit PoE LAN port to connect to the PoE power supply via a RJ45 cable as described in Section 1.6.2. The PoE LAN port can auto detect the transmission speed on the network and configure itself automatically. The device is powered from the PoE Injector via a RJ45 cable and PoE LAN port. Besides, use another RJ45 cable to connect the Data/IN port of PoE Injector to your computer's network port. In this way, you can use two RJ45 Ethernet cables to provide power source for the device and connect it to the host PC's Ethernet port for configuring or troubleshooting the device.

1.6.4 Setup by Configuring WEB UI
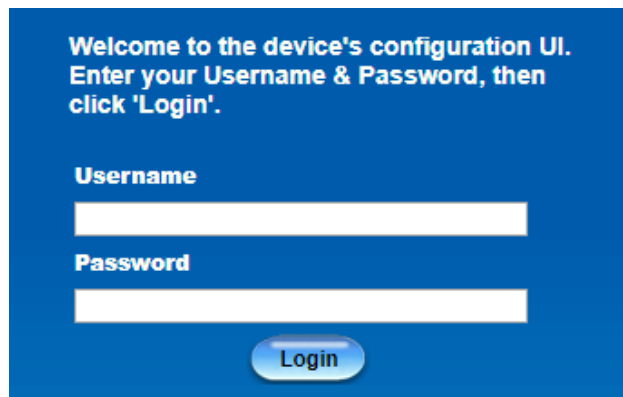
You can browse web UI to configure the device.

Type in the IP Address (**http://192.168.123.254**)[2]

When you see the login page, enter the user name and password and then click **'Login'** button.
The default setting for both username and password is **'admin'**.
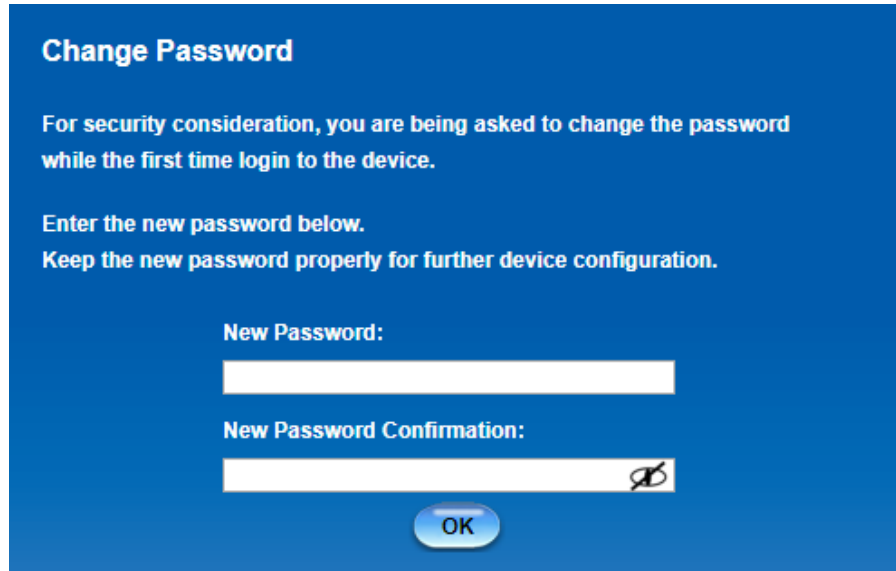
For the security consideration, you will be asked to change the loging password while the first time login to the device.

---

2 The default LAN IP address of this gateway is 192.168.123.254. If you change it, you need to login by using the new IP address.

After that, you will be asked to login again with the new password.

Note 1: Keep the login password properly for further device configuration.

Note 2: If, someday, you lose or forget the login password, the ONLY way to remedy is to recover the device to its factory default settings via long-pressing the Reset button.

Note 3: Under such situation, your device configuration will be erased accordingly. So, In addition to keep the login password, you may have to backup the device donfiguration and keep it properly for any unexpected accidence.

Chapter 2 Basic Network

2.1 WAN & Uplink

The gateway provides one WAN interface to let all client hosts in Intranet of the gateway access the the uplink network or Internet. But ISPs in the world apply various connection protocols to let gateways or user's devices dial in ISPs and then link to the Internet via different kinds of transmit media.

So, the WAN Connection lets you specify the WAN Physical Interface and Internet Setup for Intranet to access Internet. For each WAN interface, you must specify its physical interface first and then its Internet setup to connect to uplink network or Internet.

Outdoor WiFi LoRa BSU

2.1.1 Physical Interface
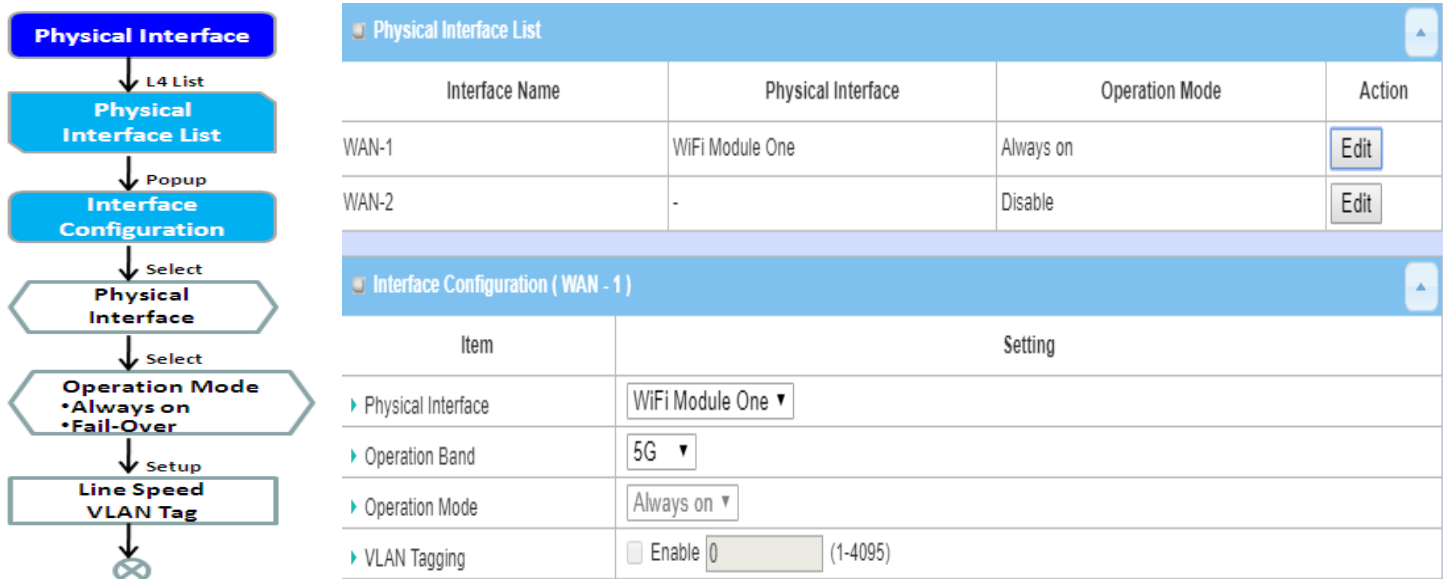
M2M gateways are usually equipped with various WAN interfacess to support different WAN connection scenario for requirement. You can configure the WAN interface one by one to get proper internet connection setup. **Refer to the product specification for the available WAN interfaces in the product you purchased.**

The first step to configure one WAN interface is to specify which kind of connection media to be used for the WAN connection, as shown in "Physical Interface" page.

In "Physical Interface" page, there are two configuration windows, "Physical Interface List" and "Interface Configuration". "Physical Interface List" window shows all the available physical interfaces. After clicking on the "Edit" button for the interface in "Physical Interface List" window the "Interface Configuration" window will appear to let you configure a WAN interface.

Physical Interface:

- **Ethernet WAN:** The gateway has one RJ45 WAN port that can be configured to be WAN connections. You can directly connect to external DSL modem or setup behind a firewall device.
- **WiFi Uplink WAN:** For the product with WiFi Uplink function, one WiFi module can be configured to be WAN connections. For the WiFi module with Uplink function activated, you can further create some uplink profiles for ease of connecting to an uplink network.

Operation Mode:

There are three option items "Always on", "Failover", and "Disable" for the operation mode setting. For the product with single WAN & Uplink interface, only "Always on" option is available.

Always on: Set this WAN interface to be active all the time. When two or more WAN are established at

Outdoor WiFi LoRa BSU

"Always on" mode, outgoing data will through these WAN connections base on load balance policies.

Physical Interface Setting

Go to **Basic Network > WAN > Physical Interface** tab.

The Physical Interface allows user to setup the physical WAN interface and to adjust WAN's behavior.

Note: Numbers of available WAN Interfaces can be different for the purchased gateway.

Physical Interface List			
Interface Name	Physical Interface	Operation Mode	Action
WAN-1	WiFi Module One	Always on	Edit

When **Edit** button is applied, an **Interface Configuration** screen will appear. WAN-1 interface is used in this example.

Interface Configuration:

Interface Configuration (WAN - 1)	
Item	Setting
▸ Physical Interface	WiFi Module One ⌄
▸ Operation Band	5G ⌄
▸ Operation Mode	Always on ⌄
▸ VLAN Tagging	☐ Enable 0 (1-4095)

Interface Configuration		
Item	**Value setting**	**Description**
Physical Interface	1. A Must fill setting 2. WAN-1 is the primary interface and is factory set to Always on.	Select one expected interface from the available interface dropdown list. It can be **Etherent** or **WiFi Module**.
Operation Band	1. A Must fill setting	If WiFi Module is specified as the physical interface, the Operation Band

	2. **5G** is selected by default.	item will be displayed for radio band selection. Specify the radio band for WiFI uplink connection. If the WiFi module in use is a 2.4G/5GHz selectable module, please select one band for uplink connection.
Operation Mode	A Must fill setting	Define the operation mode of the interface. Select **Always on** to make this WAN always active. (Note: for WAN-1, only **Always on** option is available.)
VLAN Tagging	Optional setting	Check **Enable** box to enter tag value provided by your ISP. Otherwise uncheck the box. *Value Range*: 1 ~ 4095. Note: This feature is NOT available for 3G/4G WAN connection.

Outdoor WiFi LoRa BSU

2.1.2 Internet Setup
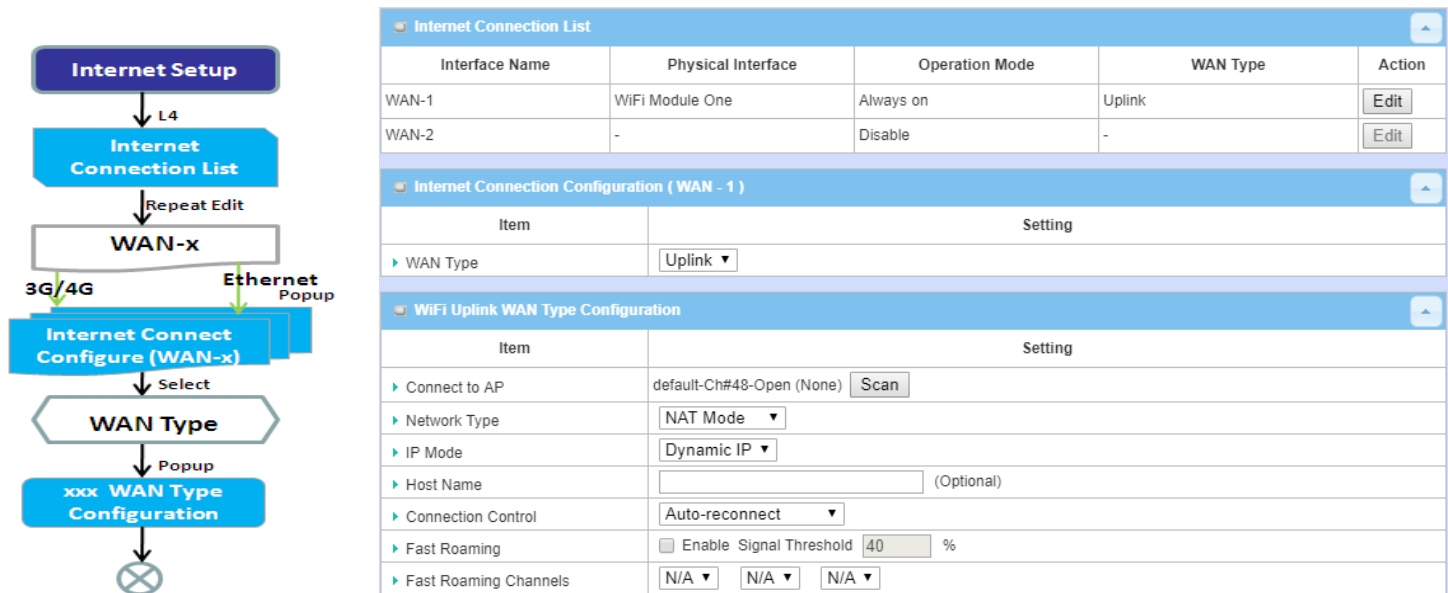
After specifying the physical interface for each WAN connection, administrator must configure their connection profile to meet the dial in process of ISP, so that all client hosts in the Intranet of the gateway can access the Internet.

In "Connection Setup" page, there are some configuration windows: "Internet Connection List", "Internet Connection Configuration", "WAN Type Configuration" and related configuration windows for each WAN type. For the Internet setup of each WAN interface, you must specify its WAN type of physical interface first and then its related parameter configuration for that WAN type.

After clicking on the "Edit" button of a physical interface in "Internet Setup List" window, the "Internet Connection Configuration" window will appear to let you specify which kind of WAN type that you will use for that physical interface to make an Internet connection. Based on your chosen WAN type, you can configure necessary parameters in each corresponding configuration window.

Outdoor WiFi LoRa BSU

Internet Connection List - Ethernet WAN

WAN Type for Ethernet Interface:

Ethernet is the most common WAN and uplink interface for M2M gateways. Usually it is connected with xDSL or cable modem for you to setup the WAN connection. There are various WAN types to connect with ISP.

- **Static IP:** Select this option if ISP provides a fixed IP to you when you subsribe the service. Usually is more expensive but very importat for cooperate requirement.
- **Dynamic IP:** The assigned IP address for the WAN by a DHCP server is different every time. It is cheaper and usually for consumer use.
- **PPP over Ethernet:** As known as PPPoE. This WAN type is widely used for ADSL connection. IP is usually different for every dial up.
- **PPTP:** This WAN type is popular in some countries, like Russia.
- **L2TP :** This WAN type is popular in some countries, like Israel.

Configure Ethernet WAN Setting

When **Edit** button is applied, **Internet Connection Configuration** screen will appear. WAN-1 interface is used in this example.

Outdoor WiFi LoRa BSU

WAN Type = Dynamic IP

When you select it, "Dynamic IP WAN Type Configuration" will appear. Items and setting is explained below

Dynamic IP WAN Type Configuration		
Item	**Value setting**	**Description**
Host Name	An optional setting	Enter the host name provided by your Service Provider.
ISP Registered MAC Address	An optional setting	Enter the MAC address that you have registered with your service provider. Or Click the **Clone** button to clone your PC's MAC to this field. Usually this is the PC's MAC address assigned to allow you to connect to Internet.

WAN Type= Static IP

When you select it, "Static IP WAN Type Configuration" will appear. Items and setting is explained below

Outdoor WiFi LoRa BSU

Static IP WAN Type Configuration		
Item	**Value setting**	**Description**
WAN IP Address	A Must filled setting	Enter the WAN IP address given by your Service Provider
WAN Subnet Mask	A Must filled setting	Enter the WAN subnet mask given by your Service Provider
WAN Gateway	A Must filled setting	Enter the WAN gateway IP address given by your Service Provider
Primary DNS	A Must filled setting	Enter the primary WAN DNS IP address given by your Service Provider
Secondary DNS	An optional setting	Enter the secondary WAN DNS IP address given by your Service Provider

WAN Type= PPPoE

When you select it, "PPPoE WAN Type Configuration" will appear. Items and setting is explained below

PPPoE WAN Type Configuration		
Item	**Value setting**	**Description**
PPPoE Account	A Must filled setting	Enter the PPPoE User Name provided by your Service Provider.
PPPoE Password	A Must filled setting	Enter the PPPoE password provided by your Service Provider.
Primary DNS	An optional setting	Enter the IP address of Primary DNS server.
Secondary DNS	An optional setting	Enter the IP address of Secondary DNS server.
Service Name	An optional setting	Enter the service name if your ISP requires it
Assigned IP Address	An optional setting	Enter the IP address assigned by your Service Provider.

Outdoor WiFi LoRa BSU

WAN Type= PPTP

When you select it, "PPTP WAN Type Configuration" will appear. Items and setting is explained below

PPTP WAN Type Configuration		
Item	**Value setting**	**Description**

IP Mode	A Must filled setting	Select either Static or Dynamic IP address for PPTP Internet connection.
		● When **Static IP Address** is selected, you will need to enter the **WAN IP Address**, **WAN Subnet Mask,** and **WAN Gateway**.
		  ■ **WAN IP Address** (A Must filled setting)**:** Enter the WAN IP address given by your Service Provider.
		  ■ **WAN Subnet Mask** (A Must filled setting)**:** Enter the WAN subnet mask given by your Service Provider.
		  ■ **WAN Gateway** (A Must filled setting)**:** Enter the WAN gateway IP address given by your Service Provider.
		● When **Dynamic IP** is selected, there are no above settings required.

Server IP Address/Name	A Must filled setting	Enter the PPTP server name or IP Address.
PPTP Account	A Must filled setting	Enter the PPTP username provided by your Service Provider.
PPTP Password	A Must filled setting	Enter the PPTP connection password provided by your Service Provider.
Connection ID	An optional setting	Enter a name to identify the PPTP connection.
MPPE	An optional setting	Select **Enable** to enable MPPE **(**Microsoft Point-to-Point Encryption) security for PPTP connection.

Outdoor WiFi LoRa BSU

WAN Type= L2TP

Item	Setting
☑ Internet Connection Configuration (WAN - 1)	▲
▸ WAN Type	L2TP ▾

When you select it, "L2TP WAN Type Configuration" will appear. Items and setting is explained below

Item	Setting
☐ L2TP WAN Type Configuration	▲
▸ IP Mode	Dynamic IP Address ▾
▸ Server IP Address / Name	
▸ L2TP Account	
▸ L2TP Password	
▸ Service Port	User-defined ▾ 1702
▸ MPPE	☐ Enable

L2TP WAN Type Configuration		
Item	**Value setting**	**Description**
IP Mode	A Must filled setting	Select either Static or Dynamic IP address for L2TP Internet connection. ● When **Static IP Address** is selected, you will need to enter the **WAN IP Address**, **WAN Subnet Mask,** and **WAN Gateway**. ■ **WAN IP Address** (A Must filled setting)**:** Enter the WAN IP address given by your Service Provider. ■ **WAN Subnet Mask** (A Must filled setting)**:** Enter the WAN subnet mask given by your Service Provider. ■ **WAN Gateway** (A Must filled setting)**:** Enter the WAN gateway IP address given by your Service Provider. ● When **Dynamic IP** is selected, there are no above settings required.
Server IP Address/Name	A Must filled setting	Enter the L2TP server name or IP Address.
L2TP Account	A Must filled setting	Enter the L2TP username provided by your Service Provider.
L2TP Password	A Must filled setting	Enter the L2TP connection password provided by your Service Provider.
Service Port	A Must filled setting	Enter the service port that the Internet service. There are three options can be selected : ● **Auto:** Port will be automatically assigned. ● **1701 (For Cisco)**: Set service port to port 1701 to connect to CISCO server. ● **User-defined**: enter a service port provided by your Service Provider.
MPPE	An optional setting	Select **Enable** to enable MPPE **(**Microsoft Point-to-Point Encryption) security for PPTP connection.

Outdoor WiFi LoRa BSU

Ethernet Connection Common Configuration
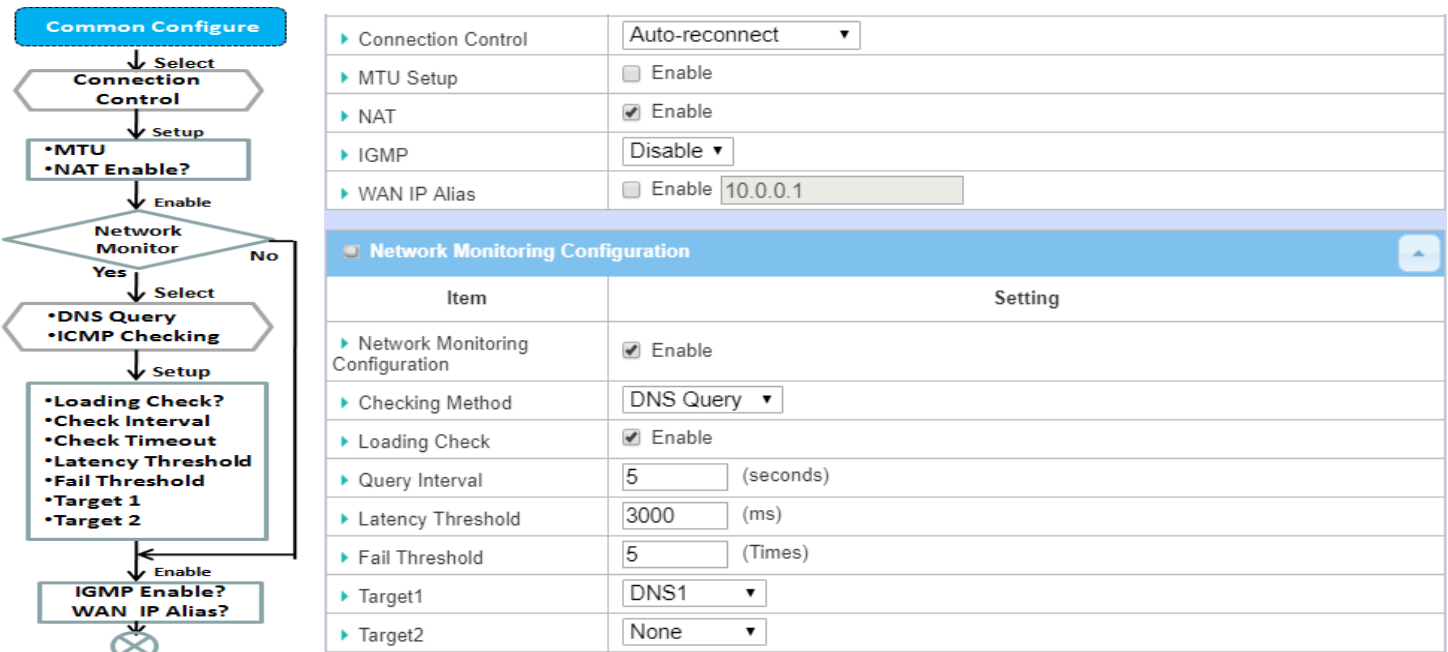
There are some important parameters to be setup no matter which Ethernet WAN type is selected. You should follow up the rule to configure.

Connection Control.
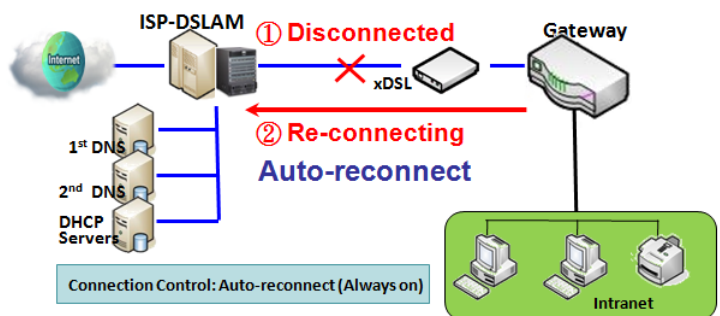
Auto-reconnect: This gateway will establish Internet connection automatically once it has been booted up, and try to reconnect once the connection is down. It's recommended to choose this scheme if for mission critical applications to ensure full-time Internet connection.
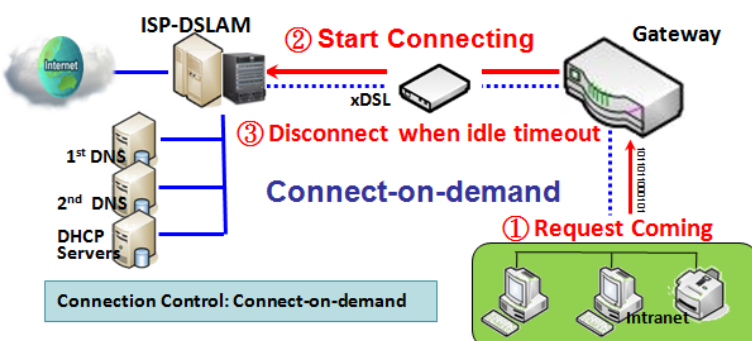
Connect-on-demand: This gateway won't start to establish Internet connection until local data is going to be sent to WAN side. After normal data transferring between LAN and WAN sides, this gateway will disconnect WAN connection if idle time reaches value of Maximum Idle Time.

Outdoor WiFi LoRa BSU
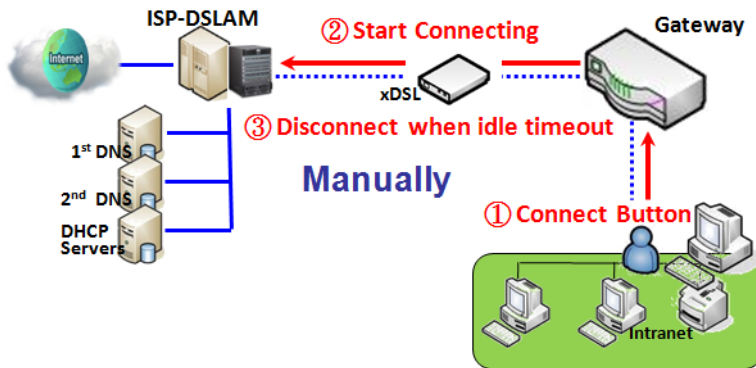
Manually: This gateway won't start to establish WAN connection until you press "Connect" button on web UI. After normal data transferring between LAN and WAN sides, this gateway will disconnect WAN connection if idle time reaches value of Maximum Idle Time.

Please be noted, if the WAN interface serves as the primary one for another WAN interface in Failover role, the Connection Control parameter will not be available to you to configure as the system must set it to "Auto-reconnect (Always on)".

Network Monitoring
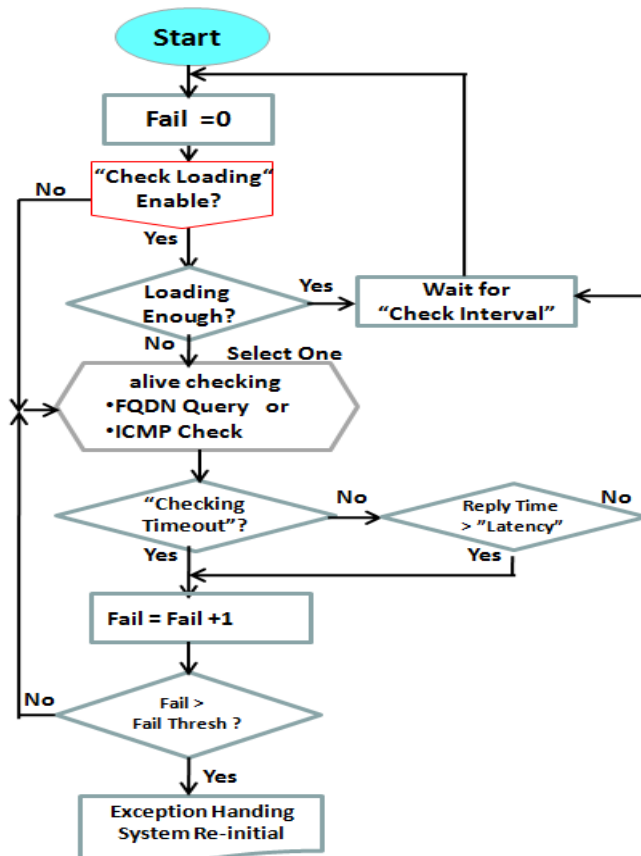
It is necessary to monitor connection status continuous. To do it, "ICMP Check" and "FQDN Query" are used to check. When there is trafiic of connection, checking packet will waste bandwidth. Response time of replied packets may also increase. To avoid "Network Monitoring" work abnormally, enabling "Checking Loading" option will stop connection check when there is traffic. It will wait for another "Check Interval" and then check loading again.

When you do "Network Monitoring", if reply time longer than "Latency" or even no response longer than "Checking Timeout", "Fail" count will be increased. If it is continuous and "Fail" count is more than "Fail Threshold", gateway will do exception handing process and re-initial this connection again . Otherwise, network monitoring process will be start again.

Outdoor WiFi LoRa BSU

Set up "Ethernet Common Configuration"

Ethernet WAN Common Configuration		
Item	**Value setting**	**Description**
Connection Control	A Must filled setting	There are three connection modes. • **Auto-reconnect** enables the router to always keep the Internet connection on. • **Connect-on-demand** enables the router to automatically re-establish Internet connection as soon as user attempts to access the Internet. Internet connection will be disconnected when it has been inactive for a specified idle time. • **Connect Manually** allows user to connect to Internet manually**.** Internet connection will be inactive after it has been inactive for specified idle time.
Maximum Idle Time	1. An Optional setting 2. By default **600** seconds is filled-in	Specify the maximum Idle time setting to disconnect the internet connection when the connection idle timed out. _**Value Range**_: 300 ~ 86400. **Note**: This field is available only when **Connect-on-demand** or **Connect Manually** is selected as the connection control scheme.
MTU Setup	1. An Optional setting 2. **Uncheck** by default	Check the Enable box to enable the MTU (Maximum Transmission Unit) limit, and specify the **MTU** for the 3G/4G connection. **MTU** refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. _**Value Range**_: 1200 ~ 1500.
MTU Setup	1. A Must filled setting 2. **Auto** (value zero) is set by default 3. Manual set range 1200~1500	**MTU** refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. When set to **Auto** (value '0'), the router selects the best MTU for best Internet connection performance.
NAT	1. An optional setting 2. NAT is enabled by default	Enable NAT to apply NAT on the WAN connection. Uncheck the box to disable NAT function.
IGMP	1. A Must filled setting 2. Disable is set by default	Enable IGMP (Internet Group Management Protocol) would enable the router to listen to IGMP packets to discover which interfaces are connected to which device. The router uses the interface information generated by IGMP to reduce bandwidth consumption in a multi-access network environment to avoid flooding the entire network.
WAN IP Alias	1. An optional setting 2. **Uncheck** by default	Enable **WAN IP Alias** then enter the IP address provided by your service provider. **WAN IP Alias** is used by the device router and is treated as a second set of WAN IP to provide dual WAN IP address to your LAN network.

Outdoor WiFi LoRa BSU

Network Monitoring Configuration		
Item	**Value setting**	**Description**
Network Monitoring Configuration	1. An optional setting 2. Box is checked by default	Check the **Enable** box to activate the network monitoring function.
Checking Method	1. An Optional setting 2. **DNS Query** is set by default	Choose either **DNS Query** or **ICMP Checking** to detect WAN link. With **DNS Query**, the system checks the connection by sending DNS Query packets to the destination specified in Target 1 and Target 2. With **ICMP Checking**, the system will check connection by sending ICMP request packets to the destination specified in Target 1 and Target 2.
Loading Check	1. An optional setting 2. Box is checked by default	Check the **Enable** box to activate the loading check function. Enable Loading Check allows the gateway to ignore unreturned DNS queries or ICMP requests when WAN bandwidth is fully occupied. This is to prevent false link-down status.
Query Interval	1. An Optional setting 2. **5 seconds** is selected by default.	Specify a time interval as the DNS **Query Interval**. **Query Interval** defines the transmitting interval between two DNS Query or ICMP checking packets. With **DNS Query,** the system checks the connection by sending DNS Query packets to the destination specified in Target 1 and Target 2. *Value Range*: 2 ~ 14400.
Check Interval	1. An Optional setting 2. **5 seconds** is selected by default.	Specify a time interval as the ICMP **Checking Interval**. **Query Interval** defines the transmitting interval between two DNS Query or ICMP checking packets. With **ICMP Checking,** the system will check connection by sending ICMP request packets to the destination specified in Target 1 and Target 2. *Value Range*: 2 ~ 14400.
Latency Threshold	1. An Optional setting 2. **3000 ms** is set by default	Enter a number of detecting disconnection times to be the threshold before disconnection is acknowledged. **Latency Threshold** defines the tolerance threshold of responding time. *Value Range*: 2000 ~ 3000 seconds.
Fail Threshold	1. An Optional setting 2. **5 times** is set by default	Enter a number of detecting disconnection times to be the threshold before disconnection is acknowledged. **Fail Threshold** specifies the detected disconnection before the router

		recognize the WAN link down status. ***Value Range:*** 1 ~ 10 times.
Target 1	1. An Optional filled setting 2. **DNS1** is selected by default	**Target1** specifies the first target of sending DNS query/ICMP request. **DNS1**: set the primary DNS to be the target. **DNS2**: set the secondary DNS to be the target. **Gateway**: set the Current gateway to be the target. **Other Host**: enter an IP address to be the target.
Target 2	1. An Optional filled setting 2. **None** is selected by default	**Target1** specifies the second target of sending DNS query/ICMP request. **None:** no second target is required. **DNS1**: set the primary DNS to be the target. **DNS2**: set the secondary DNS to be the target. **Gateway**: set the Current gateway to be the target. **Other Host**: enter an IP address to be the target.
Save	*N/A*	Click **Save** to save the settings.
Undo	*N/A*	Click **Undo** to cancel the settings.

Outdoor WiFi LoRa BSU

Internet Connection – WFi Uplink WAN

If the device connects to Internet through WiFi Uplink, this section will help you to complete WiFi Uplink connection setup.

Go to **Basic Network > WAN & Uplink > Internet Setup** tab.

WiFi Uplink interface: The Uplink network is a wireless network, and the gateway can connect to the Uplink network through WiFi connection.

If you have the access permission to a certain wireless network, you can setup a WiFi Uplink connection by using the gateway device. This gateway can support 802.11ac/n/g/b data connection, and it can connect to a wireless network (access point) under the regular infrastrature mode.

Internet Connection List				
Interface Name	Physical Interface	Operation Mode	WAN Type	Action
WAN-1	Ethernet	Always on	Static IP	Edit
WAN-2	WiFi Module One	Always on	Uplink	Edit
WAN-3	-	Disable	-	Edit
WAN-4	-	Disable	-	Edit

Configure WiFi Uplink Setting

When **Edit** button is applied, **Internet Connection Configuration** screen will appear. WAN-2 interface is used in this example.

Internet Connection Configuration (WAN - 2)	
Item	Setting
▶ WAN Type	Uplink ▾

Internet Connection Configuration		
Item	**Value setting**	**Description**
WAN Type	1. A Must filled setting. 2. **Uplink** is selected by default.	From the dropdown box, select Internet connection method for WiFi Uplink Connection. Only **Uplink** is available.

Outdoor WiFi LoRa BSU

WiFi Uplink

WiFi Uplink WAN Type Configuration	
Item	Setting
▶ Connect to AP	Only_For_Monkey-Ch#1-WPA2-PSK (AES) [Scan] [Edit]
▶ Network Type	NAT Mode ▾
▶ IP Mode	Dynamic IP ▾
▶ Host Name	[ ] (Optional)
▶ Connection Control	Connect Manually ▾
▶ Maximum Idle Time	86400 (seconds)
▶ Fast Roaming	☐ Enable Signal Threshold 40 %
▶ Fast Roaming Channels	N/A ▾ N/A ▾ N/A ▾

WiFi Uplink WAN Type Configuration		
Item	**Value setting**	**Description**
Connect to AP	N/A	Display the information of AP for connecting. You can Click the **Scan** button and select a AP for the uplink network. Besides, you can also create uplink profile(s) for ease of connecting to an available Uplink network. Refer to **Basic Network > WiFi > Uplink Profile** tab.
Network Type	1. A Must filled setting 2. **NAT Mode** is selected by default.	Select the expected network type for the WiFi Uplink connection. It can be **NAT Mode**, **Bridge Mode**, or **NAT Disable**. When **NAT Mode** is selected, the NAT function is activated on the Wireless Uplink connection; When **Bridge Mode** is selected, the bridge function is activated on the Wireless Uplink connection; The supporting of bridge mode depends on the product specification, if the purchased device doesn't support the bridge mode, it will be greyed out from selection. When **NAT Disable** is selected, the NAT function is deactivated on the Wireless Uplink connection, and it can function as a router with manually configured routing setting.
IP Mode	1. A Must filled setting 2. **Dynamic IP** is selected by default.	Specify the IP mode for the wireless uplink Interface. It can be **Dynamic IP** or **Static IP**. When **Dynamic IP** is selected, the device will request a IP from the Uplink Network as the IP for the uplink interface ; When **Static IP** is selected, you have to manually configure the IP address settings for the uplink interface. The settings include IP address, subnet mask, gateway, and primary/secondary DNS.
Connection Control	A Must filled setting	There are three connection modes. • **Auto-reconnect (Always on)** enables the router to always keep the Internet connection on. • **Connect-on-demand** enables the router to automatically re-establish Internet connection as soon as user attempts to access the Internet. Internet connection will be disconnected when it has been inactive for a specified idle time. • **Connect Manually** allows user to connect to Internet manually**.**

		Internet connection will be inactive after it has been inactive for specified idle time.
Maximum Idle Time	1. An Optional setting 2. By default **600** seconds is filled-in	Specify the maximum Idle time setting to disconnect the internet connection when the connection idle timed out. ***Value Range***: 300 ~ 86400. **Note**: This field is available only when **Connect-on-demand** or **Connect Manually** is selected as the connection control scheme.
Fast Roaming	1. An Optional setting 2. **Unchecked** is selected by default.	Click the **Enable** checkbox to activate the fast roaming function. In addition, you can also specify a threshold value for changing from one AP to another near-by AP. The default threshold value is 40%. ***Value Range***: 30 ~ 60%.
Fast Roaming Channels	1. An Optional setting 2. **N/A** is selected by default.	You can specify up to three channels for WiFi Uplink fast roaming function. If you don't specify any channel, the WiFi uplink will just operate on original connection channel.

Network Minitoring

Network Monitoring Configuration Item	Value setting	Description
Network Monitoring Configuration	1. An optional setting 2. Box is checked by default	Check the **Enable** box to activate the network monitoring function.
Checking Method	1. An Optional setting 2. **DNS Query** is set by default	Choose either **DNS Query** or **ICMP Checking** to detect WAN link. With **DNS Query**, the system checks the connection by sending DNS Query packets to the destination specified in Target 1 and Target 2. With **ICMP Checking**, the system will check connection by sending ICMP request packets to the destination specified in Target 1 and Target 2.
Loading Check	1. An optional setting 2. Box is checked by default	Check the **Enable** box to activate the loading check function. Enable Loading Check allows the gateway to ignore unreturned DNS queries or ICMP requests when WAN bandwidth is fully occupied. This is to prevent false link-down status.

Query Interval	1. An Optional setting 2. **5 seconds** is selected by default.	Specify a time interval as the DNS **Query Interval**. **Query Interval** defines the transmitting interval between two DNS Query or ICMP checking packets. With **DNS Query,** the system checks the connection by sending DNS Query packets to the destination specified in Target 1 and Target 2. ***Value Range***: 2 ~ 14400.
Check Interval	1. An Optional setting 2. **5 seconds** is selected by default.	Specify a time interval as the ICMP **Checking Interval**. **Query Interval** defines the transmitting interval between two DNS Query or ICMP checking packets. With **ICMP Checking,** the system will check connection by sending ICMP request packets to the destination specified in Target 1 and Target 2. ***Value Range***: 2 ~ 14400.
Latency Threshold	1. An Optional setting 2. **3000 ms** is set by default	Enter a number of detecting disconnection times to be the threshold before disconnection is acknowledged. **Latency Threshold** defines the tolerance threshold of responding time. ***Value Range***: 2000 ~ 3000 seconds.
Fail Threshold	1. An Optional setting 2. **5 times** is set by default	Enter a number of detecting disconnection times to be the threshold before disconnection is acknowledged. **Fail Threshold** specifies the detected disconnection before the router recognize the WAN link down status. ***Value Range***: 1 ~ 10 times.
Target 1	1. An Optional filled setting 2. **DNS1** is selected by default	**Target1** specifies the first target of sending DNS query/ICMP request. **DNS1**: set the primary DNS to be the target. **DNS2**: set the secondary DNS to be the target. **Gateway**: set the Current gateway to be the target. **Other Host**: enter an IP address to be the target.
Target 2	1. An Optional filled setting 2. **None** is selected by default	**Target1** specifies the second target of sending DNS query/ICMP request. **None:** no second target is required. **DNS1**: set the primary DNS to be the target. **DNS2**: set the secondary DNS to be the target. **Gateway**: set the Current gateway to be the target. **Other Host**: enter an IP address to be the target.
Save	*N/A*	Click **Save** to save the settings.
Undo	*N/A*	Click **Undo** to cancel the settings.

2.2 LAN & VLAN

This section provides the configuration of LAN and VLAN. VLAN is an optional feature, and it depends on the product specification of the purchased gateway.

2.2.1 Ethernet LAN
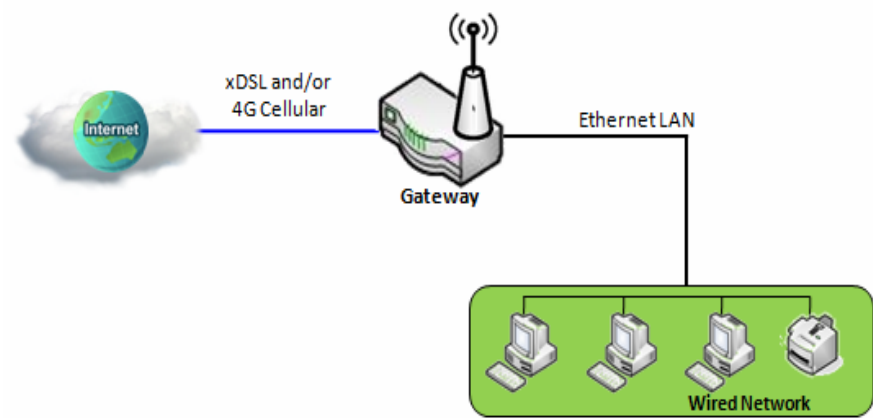
The Local Area Network (LAN) can be used to share data or files among computers attached to a network. Following diagram illustrates the network that wired and interconnects computers.

Please follow the following instructions to do IPv4 Ethernet LAN Setup.

Configuration Item	Value setting	Description
IP Mode	N/A	It shows the LAN IP mode for the gateway according the related configuration. **Static IP**: If there is at least one WAN interface activated, the LAN IP mode is fixed in Static IP mode. **Dynamic IP**: If all the available WAN inferfaces are disabled, the LAN IP mode can be Dynamic IP mode.
LAN IP Address	1. A Must filled setting 2. 192.168.123.254 **is set by default**	Enter the local IP address of this device. The network device(s) on your network must use the LAN IP address of this device as their Default Gateway. You can change it if necessary. **Note**: *It's also the IP address of web UI. If you change it, you need to type new IP address in the browser to see web UI*.
Subnet Mask	1. A Must filled setting 2. **255.255.255.0 (/24)** is set	Select the subnet mask for this gateway from the dropdown list. Subnet mask defines how many clients are allowed in one network or subnet.

	by default	The default subnet mask is 255.255.255.0 (/24), and it means maximum 254 IP addresses are allowed in this subnet. However, one of them is occupied by LAN IP address of this gateway, so there are maximum 253 clients allowed in LAN network. ***Value Range***: 255.0.0.0 (/8) ~ 255.255.255.252 (/30).
Save	N/A	Click the **Save** button to save the configuration
Undo	N/A	Click the **Undo** button to restore what you just configured back to the previous setting.

Create / Edit Additional IP

This gateway provides the LAN IP alias function for some special management consideration. You can add additional LAN IP for this gateway, and access to this gateway with the additional IP.

	Additional IP	Add	Delete					▲	✖
ID		Name		Interface	IP Address	Subnet Mask	Enable	Action	

When **Add** button is applied, **Additional IP Configuration** screen will appear.

Additional IP Configuration	▲ ✖
Item	Setting
▶ Name	[ ]
▶ Interface	lo ▾
▶ IP Address	[ ]
▶ Subnet Mask	255.255.255.0 (/24) ▾
▶ Enable	☐
	Save

Configuration Item	Value setting	Description
Name	.1 An Optional Setting	Enter the name for the alias IP address.
Interface	1. A Must filled setting 2. **lo** is set by default	Specify the Interface type. It can be **lo** or **br0**.
IP Address	1. An Optional setting 2. 192.168.123.254 **is set by default**	Enter the addition IP address for this device.
Subnet Mask	1. A Must filled setting 2. **255.255.255.0 (/24)** is set by default	Select the subnet mask for this gateway from the dropdown list. Subnet mask defines how many clients are allowed in one network or subnet. The default subnet mask is 255.255.255.0 (/24), and it means maximum 254 IP addresses are allowed in this subnet. However, one of them is occupied by LAN

		IP address of this gateway, so there are maximum 253 clients allowed in LAN network. ***Value Range*****:** 255.0.0.0 (/8) ~ 255.255.255.255 (/32).
Save	NA	Click the **Save** button to save the configuration

2.2.2 VLAN (not supported)

Not supported feature for the purchased product, leave it as blank.

2.2.3 DHCP Server

➢ **DHCP Server**

The gateway supports up to 4 DHCP servers to fulfill the DHCP requests from different VLAN groups (please refer to VLAN section for getting more usage details). And there is one default setting for whose LAN IP Address is the same one of gateway LAN interface, with its default Subnet Mask setting as "255.255.255.0", and its default IP Pool ranges is from ".100" to ".200" as shown at the DHCP Server List page on gateway's WEB UI.
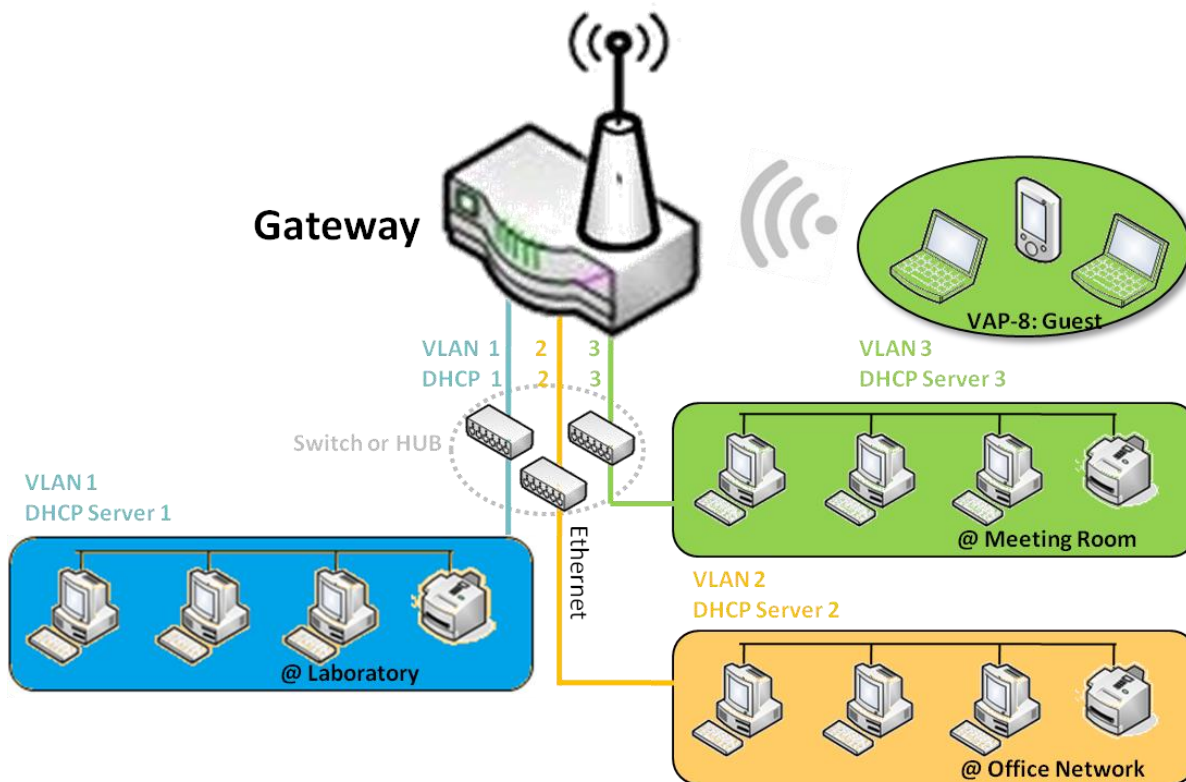
User can add more DHCP server configurations by clicking on the "Add" button behind "DHCP Server List", or clicking on the "Edit" button at the end of each DHCP Server on list to edit its current settings. Besides, user can select a DHCP Server and delete it by clicking on the "Select" check-box and the "Delete" button.

Outdoor WiFi LoRa BSU

➢ Fixed Mapping

User can assign fixed IP address to map the specific client MAC address by select them then copy, when targets were already existed in the **DHCP Client List**, or to add some other Mapping Rules by manually in advance, once the target's MAC address was not ready to connect.
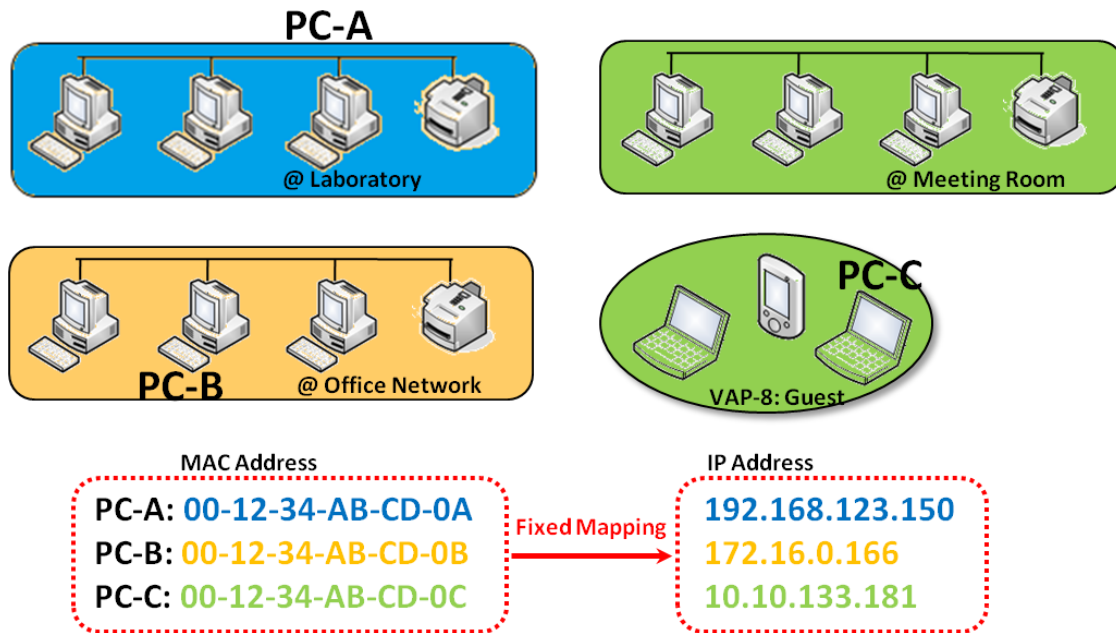
Outdoor WiFi LoRa BSU

DHCP Server Setting

Go to **Basic Network > LAN & VLAN > DHCP Server** Tab.

The DHCP Server setting allows user to create and customize DHCP Server policies to assign IP Addresses to the devices on the local area network (LAN).

Create / Edit DHCP Server Policy

The gateway allows you to custom your DHCP Server Policy. If multiple LAN ports are available, you can define one policy for each LAN (or VLAN group), and it supports up to a maximum of 4 policy sets.

DHCP Server Name	LAN IP Address	Subnet Mask	IP Pool	Lease Time	Domain Name	Primary DNS	Secondary DNS	Primary WINS	Secondary WINS	Gateway	Enable	Actions
DHCP 1	192.168.66.1	255.255.254.0	192.168.66.100-192.168.66.200	900		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	✓	Edit / Fixed Mapping

When **Add** button is applied, **DHCP Server Configuration** screen will appear.

Item	Setting
▸ DHCP Server Name	DHCP 2
▸ LAN IP Address	192.168.2.1
▸ Subnet Mask	255.255.255.0 (/24) ▾
▸ IP Pool	Starting Address: / Ending Address:
▸ Lease Time	86400 seconds
▸ Domain Name	(Optional)
▸ Primary DNS	(Optional)
▸ Secondary DNS	(Optional)
▸ Primary WINS	(Optional)
▸ Secondary WINS	(Optional)
▸ Gateway	(Optional)

Outdoor WiFi LoRa BSU

DHCP Server Configuration		
Item	**Value setting**	**Description**
DHCP Server Name	1. String format can be any text 2. A Must filled setting	Enter a DHCP Server name. Enter a name that is easy for you to understand.
LAN IP Address	1. IPv4 format. 2. A Must filled setting	The LAN IP Address of this DHCP Server.
Subnet Mask	255.0.0.0 (/8) is set by default	The Subnet Mask of this DHCP Server.
IP Pool	1. IPv4 format. 2. A Must filled setting	The IP Pool of this DHCP Server. It composed of Starting Address entered in this field and Ending Address entered in this field.
Lease Time	1. Numberic string format. 2. A Must filled setting	The Lease Time of this DHCP Server. ***Value Range***: 300 ~ 604800 seconds.
Domain Name	String format can be any text	The Domain Name of this DHCP Server.
Primary DNS	IPv4 format	The Primary DNS of this DHCP Server.
Secondary DNS	IPv4 format	The Secondary DNS of this DHCP Server.
Primary WINS	IPv4 format	The Primary WINS of this DHCP Server.
Secondary WINS	IPv4 format	The Secondary WINS of this DHCP Server.
Gateway	IPv4 format	The Gateway of this DHCP Server.
Server	The box is unchecked by default.	Click **Enable** box to activate this DHCP Server.
Save	N/A	Click the **Save** button to save the configuration
Undo	N/A	Click the **Undo** button to restore what you just configured back to the previous setting.
Back	N/A	When the **Back** button is clicked the screen will return to the DHCP Server Configuration page.

Create / Edit Mapping Rule List on DHCP Server

The gateway allows you to custom your Mapping Rule List on DHCP Server. It supports up to a maximum of 64 rule sets. When **Fix Mapping** button is applied, the **Mapping Rule List** screen will appear.

When **Add** button is applied, **Mapping Rule Configuration** screen will appear.

Outdoor WiFi LoRa BSU

Mapping Rule Configuration		
Item	**Value setting**	**Description**
MAC Address	1. MAC Address string format 2. A Must filled setting	The MAC Address of this mapping rule.
IP Address	1. IPv4 format. 2. A Must filled setting	The IP Address of this mapping rule.
Rule	The box is unchecked by default.	Click **Enable** box to activate this rule.
Save	N/A	Click the **Save** button to save the configuration
Undo	N/A	Click the **Undo** button to restore what you just configured back to the previous setting.
Back	N/A	When the **Back** button is clicked the screen will return to the **DHCP Server Configuration** page.

View / Copy DHCP Client List

When **DHCP Client List** button is applied, **DHCP Client List** screen will appear.

When the DHCP Client is selected and **Copy to Fixed Mapping** button is applied. The IP and MAC address of DHCP Client will apply to the Mapping Rule List on specific DHCP Server automatically.

Enable / Disable DHCP Server Options

The **DHCP Server Options** setting allows user to set **DHCP OPTIONS 66**, **72**, or **114**. Click the **Enable** button to activate the DHCP option function, and the DHCP Server will add the expected options in its sending out

DHCPOFFER DHCPACK packages.

Option	Meaning	RFC
66	TFTP server name	[RFC 2132]
72	Default World Wide Web Server	[RFC 2132]
114	URL	[RFC 3679]

Create / Edit DHCP Server Options

The gateway supports up to a maximum of 99 option settings.

When **Add**/**Edit** button is applied, **DHCP Server Option Configuration** screen will appear.

DHCP Server Option Configuration		
Item	**Value setting**	**Description**
Option Name	1. String format can be any text 2. A Must filled setting.	Enter a DHCP Server Option name. Enter a name that is easy for you to understand.
DHCP Server Select	Dropdown list of all available DHCP servers.	Choose the DHCP server this option should apply to.
Option Select	1. A Must filled setting.	Choose the specific option from the dropdown list. It can be **Option 66**, **Option**

	2. **Option 66** is selected by default.	**72**, **Option 144**, **Option 42**, **Option 150**, **or Option 160**. **Option 42** for ntp server; **Option 66** for tftp; **Option 72** for www; **Option 144** for url;

<table>
<tr><td rowspan="2">Type</td><td rowspan="2">Dropdown list of DHCP server option value's type</td><td colspan="2">Each different options has different value types.</td></tr>
<tr><td rowspan="2">66</td><td>Single IP Address</td></tr>
<tr><td>Type</td><td></td><td>Single FQDN</td></tr>
</table>

Type	Dropdown list of DHCP server option value's type	Each different options has different value types.	
		66	Single IP Address
			Single FQDN
		72	IP Addresses List, separated by ","
		114	Single URL
		42	IP Addresses List, separated by ","
		150	IP Addresses List, separated by ","
		160	Single IP Address
			Single FQDN

Value	1. IPv4 format 2. FQDN format 3. IP list 4. URL format 5. A Must filled setting	Should conform to Type :	
		Type	**Value**
		66 Single IP Address	IPv4 format
		66 Single FQDN	FQDN format
		72 IP Addresses List, separated by ","	IPv4 format, separated by ","
		114 Single URL	URL format

Enable	The box is unchecked by default.	Click **Enable** box to activate this setting.
Save	*NA*	Click the **Save** button to save the setting.
Undo	*NA*	When the **Undo** button is clicked the screen will return back with nothing changed.

Create / Edit DHCP Relay

The gateway supports up to a maximum of 6 DHCP Relay configurations.

When **Add/Edit** button is applied, **DHCP Relay Configuration** screen will appear.

Outdoor WiFi LoRa BSU

DHCP Relay Configuration		
Item	**Value setting**	**Description**
Agent Name	1. String format can be any text 2. A Must filled setting.	Enter a DHCP Relay name. Enter a name that is easy for you to understand. ***Value Range***: 1~64 characters.
LAN Interface	1. A Must filled setting. 2. **LAN** is selected by default.	Choose a LAN Interface for the dropdown list to apply with the DHCP Relay function.
WAN Interface	1. A Must filled setting. 2. **WAN-1** is selected by default.	Choose a WAN Interface for the dropdown list to apply with the DHCP Relay function. It can be the available WAN interface(s), and L2TP connection.
Server IP	1. A Must filled setting. 2. **null** by default.	Assign a **DHCP Server IP Address** that the gateway will relay the DHCP requests to the assigned DHCP server via specified WAN interface.
DHCP OPTION 82	The box is unchecked by default.	Click **Enable** box to activate DHCP OPTION 82 function. Option 82 is organized as a single DHCP option that contains circuit-ID information known by the relay agent. If the relayed DHCP server required the such information, you have to enable it, otherwise, just leave it as unchecked.
Enable	The box is unchecked by default.	Click **Enable** box to activate this setting.
Save	*NA*	Click the **Save** button to save the setting.
Undo	*NA*	When the **Undo** button is clicked the screen will return back with nothing changed.

2.3 WiFi

The gateway provides WiFi interface for mobile devices or BYOD devices to connect for Internet/Intranet accessing. WiFi function is usually modulized design in a gateway, and there can be single or dual modules within a gateway. The WiFi system in the gateway complies with IEEE 802.11ac/11n/11g/11b standard in 2.4GHz or 5GHz single band or 2.4G/5GHz concurrent dual bands of operation. There are several wireless operation modes provided by this device. They are: "**AP Router Mode**", "**WDS Only Mode**", and "**WDS Hybrid Mode**". You can choose the expected mode from the wireless operation mode list.

There are some sub-sections for you to configure the WiFi function, including "Basic Configuration" and "Advanced Configuration". In Basic Configuration section, you have to finish almost all the settings for using the WiFi function. And the Advanced Configuration section provides more parameters for advanced user to fine tune the connectivity performance for the WiFi function.

Outdoor WiFi LoRa BSU

2.3.1 WiFi Configuration
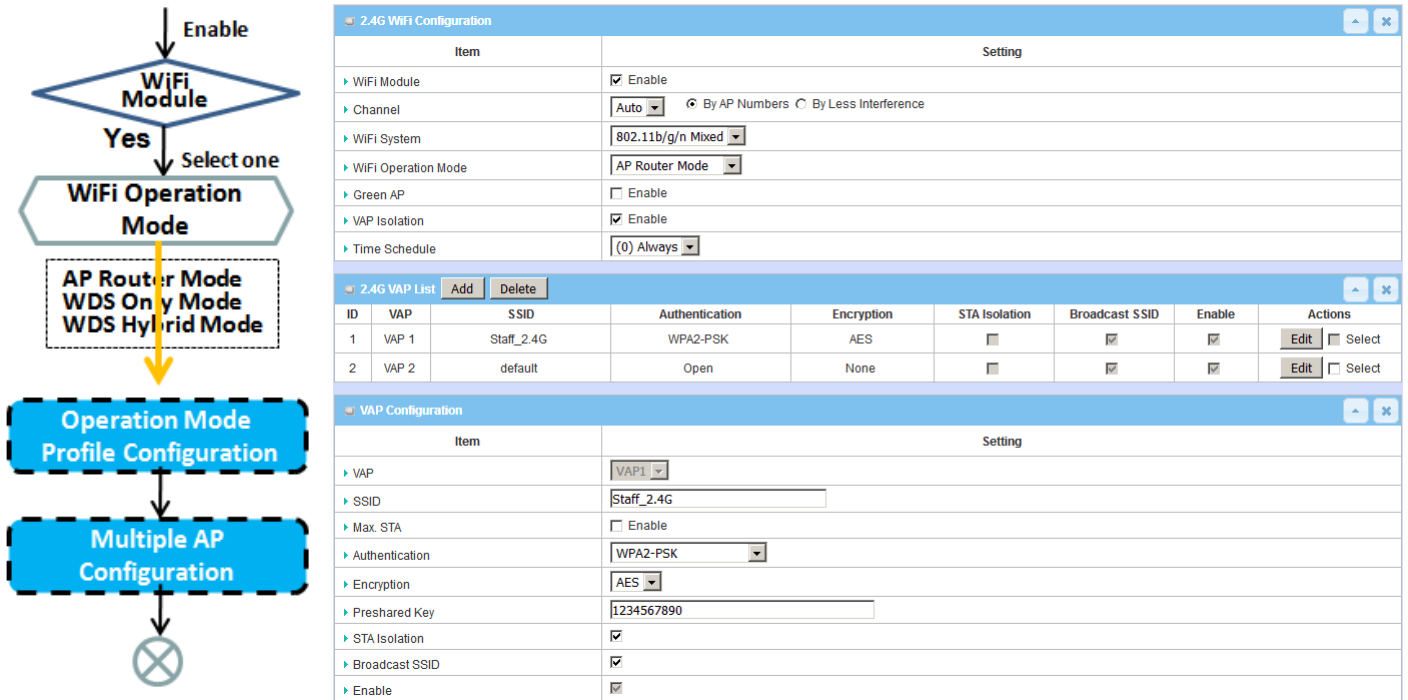
Due to optional module(s) and frequency band, you need to setup module one by one. For each module, you need to specify the operation mode, and then setup the virtual APs for wireless access.

In addition, if you configured the WiFi Uplink function in the **Basic Network > WAN & Uplink > Physical Interface** tab, the WiFi uplink function is activated. However, for the wireless LAN function of the module worked under WiFi uplink operation, it also provides AP Router function for local wireless clients to connect to wireless uplink network via the gateway.

Hereunder are the scenarios for each wireless operation mode, you can get how it works, and what is the difference among them. To connect your wireless devices with the wireless gateway, make sure your application scenario for WiFi network and choose the most adequate operation mode.

Outdoor WiFi LoRa BSU

AP Router Mode
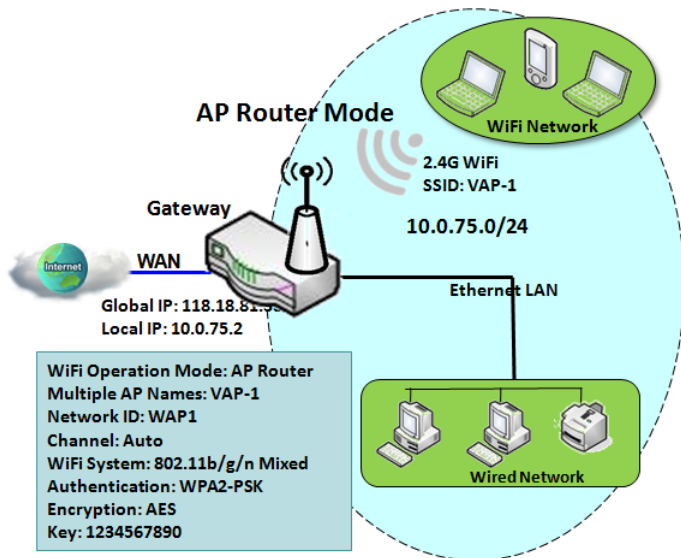
This mode allows you to get your wired and wireless devices connected to form the Intranet of the wireless gateway, and the Intranet will link to the Internet with NAT mechanism of the gateway. So, this gateway is working as a WiFi AP, but also a WiFi hotspot for Internet accessing service. It means local WiFi clients can associate to it, and go to Internet. With its NAT mechanism, all of wireless clients don't need to get public IP addresses from ISP.

WDS Only Mode
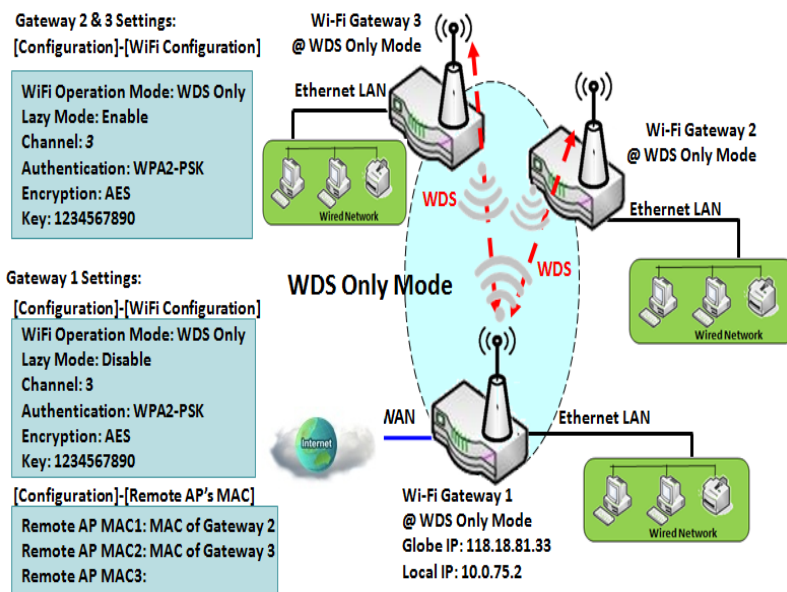
WDS (Wireless Distributed System) Only mode drives a WiFi gateway to be a bridge for its wired Intranet and a repeater to extend distance. You can use multiple WiFi gateways as a WiFi repeater chain with all gateways setup as "WDS Only" mode. All gateways can communicate with each other through WiFi. All wired client hosts within each gateway can also communicate each other in the scenario. Only one gateway within repeater chain can be DHCP server to provide IP for all wired client hosts of every gateway which being disabled DHCP server. This gateway can be NAT router to provide internet access

The diagram illustrates that there are two wireless gateways 2, 3 running at "WDS Only" mode. They both use channel 3 to link to local Gateway 1 through WDS. Both gateways connected by WDS need to setup the remote AP MAC for each other. All client hosts under gateway 2, 3 can request IP address from the DHCP server at gateway 1. Besides, wireless Gateway 1 also execute the NAT mechanism for all client hosts Internet accessing.

Outdoor WiFi LoRa BSU

WDS Hybrid Mode

Gateway 2 / AP 1 Settings:
[Configuration]-[WiFi Configuration]

WiFi Operation Mode: WDS Hybrid
Lazy Mode: Enable
Multiple AP Names: VAP1
Network ID: Extended-WiFi
Channel: *same as Router 1*
Authentication: *same as Router 1*
Encryption: *same as Router 1*
Key: *same as Router 1*

Gateway 1 Settings:
[Configuration]-[WiFi Configuration]

WiFi Operation Mode: WDS Hybrid
Lazy Mode: Disable
Multiple AP Names: VAP1
Network ID: Extended-WiFi
Channel: 3
Authentication: WPA2-PSK
Encryption: AES
Key: 1234567890

[Configuration]-[Remote AP's MAC]

Remote AP MAC1: MAC of Router 2
Remote AP MAC2: MAC of AP 1
Remote AP MAC3:
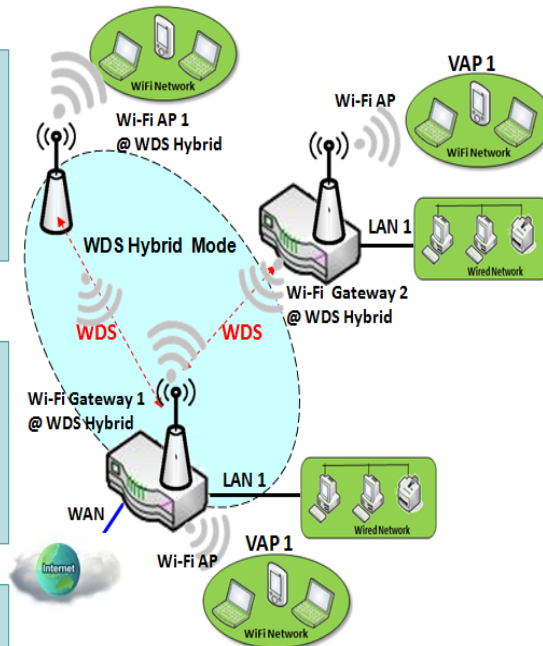
WDS hybrid mode includes both WDS and AP Router mode. WDS Hybrid mode can act as an access point for its WiFi Intranet and a WiFi bridge for its wired and WiFi Intranets at the same time. Users can thus use the features to build up a large wireless network in a large space like airports, hotels or campus.

The diagram illustrates Gateway 1, Gateway 2 and AP 1 connected by WDS. Each gateway has access point function for WiFi client access. Gateway 1 has DHCP server to assign IP to each client hosts. All gateways and AP are under WDS hybrid mode. To setup WDS hybrid mode, it need to fill all configuration items similar to that of AP-router and WDS modes.

Multiple VAPs

Gateway Settings:

WiFi Operation Mode: AP Router
VAP1
SSID: VAP-1
Authentication: WPA2-PSK
Encryption: TKIP
Key: 1234567890

VAP2
SSID: VAP-2
Authentication: WPA2-PSK
Encryption: TKIP
Key: 1234567890

VAP3
SSID: VAP-3
Authentication: WPA2
Encryption: TKIP
RADIUS Server IP: 192.168.168.
RADIUS Server Port: 1812
RADIUS Shared Key
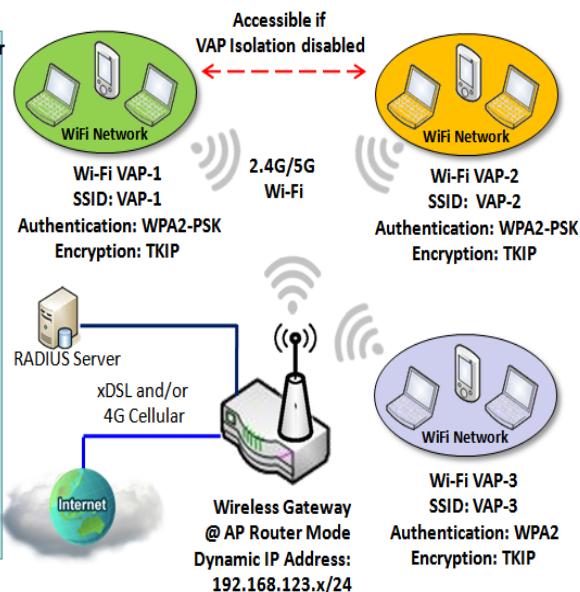
VAP (Virtual Access Point) is function to partition wireless network into multiple broadcast domains. It can simulate multiple APs in one physical AP. This wireless gateway supports up to 8 VAPs. For each VAP, you need to setup SSID, authentication and encryption to control Wi-Fi client access.

Besides, there is a VAP isolation option to manage the access among VAPs. You can allow or blocks communication for the wireless clients connected to different VAPs. As shown in the diagram, the clients in VAP-1 and VAP-2 can communicate to each other when VAP Isolation is disabled.

Outdoor WiFi LoRa BSU

Wi-Fi Security - Authentication & Encryption
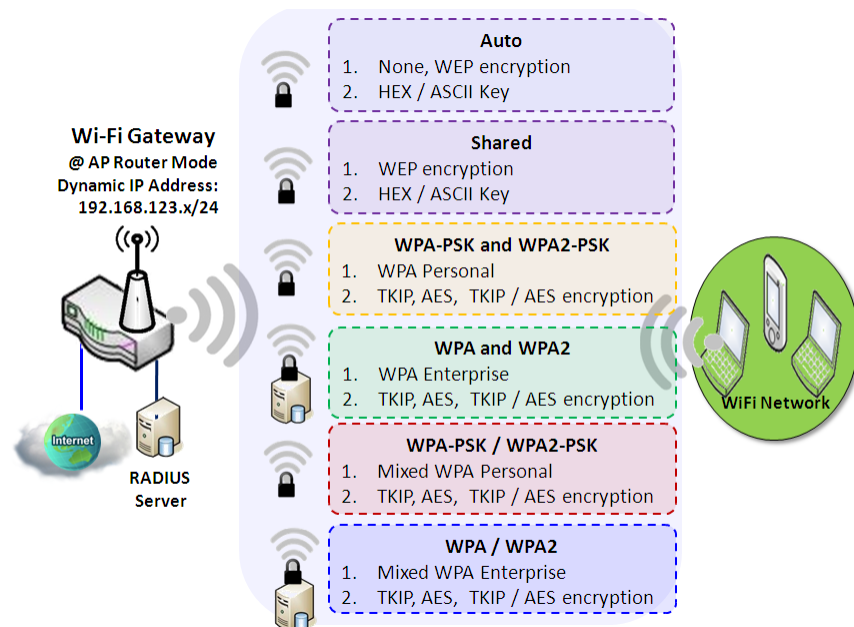
Wi-Fi security provides complete authentication and encryption mechanisms to enhance the data security while your data is transferred wirelessly over the air. The wireless gateway supports Shared, WPA-PSK / WPA2-PSK and WPA / WPA2 authentication. You can select one authentication scheme to validate the wireless clients while they are connecting to the AP. As to the data encryption, the gateway supports WEP, TKIP and AES. The selected encryption algorithm will be applied to the data while the wireless connection is established.

Outdoor WiFi LoRa BSU

WiFi Configuration Setting

The WiFi configuration allows user to configure 2.4GHz or 5GHz WiFi settings.

Go to **Basic Network > WiFi > WiFi Module One** Tab. If the gateway is equipped with two WiFi modules, there will be another **WiFi Module Two**. You can do the similar configurations on both WiFi modules.

Basic Configuration

Basic Configuration	
Item	**Setting**
▶ Operation Band	2.4G Single Band ▾

Basic Configuration		
Item	**Value setting**	**Description**
Operation Band	A Must filled setting	Specify the intended operation band for the WiFi module. Basically, this setting is fixed and cannot be changed once the module is integrated into the product. However, there is some module with selectable band for user to choose according to his network environment. Under such situation, you can specify which operation band is suitable for the application.

Configure WiFi Setting

2.4G WiFi Configuration	
Item	**Setting**
▶ WiFi Module	☑ Enable
▶ Channel	Auto ▾ ⦿ By AP Numbers ○ By Less Interference
▶ WiFi System	802.11b/g/n Mixed ▾
▶ WiFi Operation Mode	AP Router Mode ▾

Configuring Wi-Fi Settings		
Item	**Value setting**	**Description**
WiFi Module	The box is checked by default	Check the **Enable** box to activate Wi-Fi function.
Channel	1. A Must filled setting. 2. **Auto** is selected be default.	Select a radio channel for the VAP. Each channel is corresponding to different radio band. The permissible channels depend on the **Regulatory Domain**. There are two available options when **Auto** is selected: • **By AP Numbers** The channel will be selected according to AP numbers (The less, the better). • **By Less Interference**

		The channel will be selected according to interference. (The lower, the better).
WiFi System	A Must filled setting	Specify the preferred WiFi System. The dropdown list of **WiFi system** is based on **IEEE 802.11** standard. ● **2.4G WiFi** can select b, g and n only or mixed with each other. ● **5G WiFi** can select a, n and ac only or mixed with each other.
WiFi Operation Mode		Specify the **WiFi Operation Mode** according to your application. Go to the following table for **AP Router Mode**, **WDS Only Mode**, and **WDS Hybrid Mode** settings. Note: The available operation modes depend on the product specification.

In the following, the specific configuration description for each WiFi operation mode is given.

Note: If you configured the WiFi Uplink function in the **Basic Network > WAN & Uplink > Physical Interface** tab, the WiFi uplink function is activated. However, for the wireless LAN function of the module worked under WiFi uplink operation, the **WiFi Operation Mode** is fixed to **WiFi Uplink**, and also provides AP Router function for local wireless clients to connect to wireless uplink network via the gateway.

AP Router Mode [WiFi Uplink Mode] & VAPs Configuration

For the AP Router mode, or WiFi Uplink mode, the device not only supports **stations connection** but also the **router function**. The **WAN** port and the **NAT** function are **enabled**.

▶ WiFi Operation Mode	AP Router Mode ▼
▶ Green AP	☐ Enable
▶ VAP Isolation	☑ Enable
▶ Time Schedule	(0) Always ▼

AP Router Mode		
Item	**Value setting**	**Description**
Green AP	The box is unchecked by default.	Check the **Enable** box to activate **Green AP** function.
VAP Isolation	The box is checked by default.	Check the **Enable** box to activate this function. By default, the box is checked; it means that stations which associated to different VAPs cannot communicate with each other.
Profile	The box is unchecked by default.	Check the **Enable** box to enable the activate profile setting. Note: This setting is only available in WiFi Uplink operation mode.
Time Schedule	A Must filled setting	Apply a specific **Time Schedule** to this rule; otherwise leave it as **(0) Always**. If the dropdown list is empty ensure **Time Schedule** is pre-configured. Refer to **Object Definition** > **Scheduling > Configuration** tab.

Outdoor WiFi LoRa BSU

ID	VAP	SSID	Authentication	Encryption	STA Isolation	Broadcast SSID	Enable	Actions
1	VAP 1	Staff_2.4G	WPA2-PSK	AES	☐	☑	☑	Edit ☐ Select

2.4G VAP List [Add] [Delete]

By default, VAP 1 is enabled and security key is required to connect to the gateway wirelessly to enhance the security level and prevent unexpected access of un-authorized devices.

The default wifi key is printed on both the device label and the Security Card. It is created randomly and differs from devices. So, you can connected to the VAP1 (SSID: Staff_2.4G) with the provided key.

However, it is strongly recommanded that you have to change the security key to a easy-to-remember one by clicking the Edit button.

Click **Add** / **Edit** button in the VAP List screen to create or edit the settings for a VAP. A VAP Configuration screen will appear.

For VAP 1:

VAP Configuration

Item	Setting
▶ VAP	VAP1 ▾
▶ SSID	Staff_2.4G
▶ Max. STA	☐ Enable
▶ Authentication	WPA2-PSK ▾
▶ Encryption	AES ▾
▶ Preshared Key	1234567890
▶ STA Isolation	☑
▶ Broadcast SSID	☑
▶ Enable	☑

For others:

Outdoor WiFi LoRa BSU

Item	Setting
▶ VAP	VAP2 ▾
▶ SSID	default
▶ Max. STA	☐ Enable
▶ Authentication	Open ▾
▶ Encryption	None ▾
▶ STA Isolation	☐
▶ Broadcast SSID	☐
▶ Enable	☐

VAP Configuration

Item	Value setting	Description
SS ID	1. String format : Any text	Enter the SSID for the VAP, and decide whether to broadcast the SSID or not. The **SSID** is used for identifying from another AP, and client stations will associate with AP according to SSID.
Max. STA	The box is unchecked by default.	Check this box and enter a limitation to limit the maximum number of client station. The box is unchecked by default. It means no special limitation on the number of connected STAs.
Authentication	1. A Must filled setting 2. VAP1: **WPA2-PSK** is selected be default; Others: **Open** is selected be default.	For security, there are several authentication methods supported. Client stations should provide the key when associate with this device.
		When **Open** is selected The check box named **802.1x** shows up next to the dropdown list. ● **802.1x** (The box is unchecked by default) When **802.1x** is enabled, it means the client stations will be authenticated by RADIUS server. **RADIUS Server IP** (The default IP is 0.0.0.0) **RADIUS Server Port** (The default value is 1812) **RADIUS Shared Key**
		When **Shared** is selected The pre-shared WEP key should be set for authenticating.
		When **Auto** is selected The device will select **Open** or **Shared** by requesting of client automatically. The check box named **802.1x** shows up next to the dropdown list. ● **802.1x** (The box is unchecked by default) When **802.1x** is enabled, it means the client stations will be authenticated by RADIUS server. **RADIUS Server IP** (The default IP is 0.0.0.0) **RADIUS Server Port** (The default value is 1812) **RADIUS Shared Key**
		When **WPA** or **WPA2** is selected They are implementation of IEEE 802.11i. **WPA** only had implemented part of IEEE 802.11i, but owns the better **compatibility**.

		WPA2 had fully implemented 802.11i standard, and owns the highest **security**. ● **RADIUS Server** The client stations will be authenticated by RADIUS server. **RADIUS Server IP** (The default IP is 0.0.0.0) **RADIUS Server Port** (The default value is 1812) **RADIUS Shared Key**
		When **WPA / WPA2** is selected It owns the same setting as **WPA** or **WPA2**. The client stations can associate with this device via **WPA** or **WPA2**.
		When **WPA-PSK** or **WPA2-PSK** is selected It owns the same encryption system as WPA or WPA2. The authentication uses pre-shared key instead of RADIUS server.
		When **WPA-PSK / WPA2-PSK** is selected It owns the same setting as **WPA-PSK** or **WPA2-PSK**. The client stations can associate with this device via **WPA-PSK** or **WPA2-PSK**.
Encryption	1. A Must filled setting. 2. VAP1: **AES** is selected be default; Others: **None** is selected be default.	Select a suitable encryption method and enter the required key(s). The available method in the dropdown list depends on the Authentication you selected. **None** It means that the device is open system without encrypting. **WEP** Up to 4 WEP keys can be set, and you have to select one as current key. The key type can set to **HEX** or **ASCII**. If **HEX** is selected, the key should consist of (0 to 9) and (A to F). If **ASCII** is selected, the key should consist of ASCII table. **TKIP** TKIP was proposed instead of WEP without upgrading hardware. Enter a Pre-shared Key for it. The length of key is from 8 to 63 characters. **AES** The newest encryption system in WiFi, it also designed for the fast 802.11n high bitrates schemes. Enter a Pre-shared Key for it. The length of key is from 8 to 63 characters. You are recommended to use **AES** encryption instead of any others for security. **TKIP / AES** **TKIP / AES** mixed mode. It means that the client stations can associate with this device via **TKIP** or **AES**. Enter a Pre-shared Key for it. The length of key is from 8 to 63 characters.
STA Isolation	VAP1: The box is checked by default; Others: unchecked by default.	Check the **Enable** box to activate this function. By default, the box is checked; it means that stations which associated to the same VAP cannot communicate with each other.
Broadcast SSID	VAP1: The box is checked by default; Others: unchecked by default.	Check the **Enable** box to activate this function. If the broadcast SSID option is enabled, it means the SSID will be broadcasted, and the stations can associate with this device by scanning SSID.
Enable	VAP1: The box is checked by default; Others: unchecked by default.	Check the **Enable** box to activate this VAP.
Save	N/A	Click the **Save** button to save the current configuration.
Undo	N/A	Click the **Undo** button to restore configuration to previous setting before saving.
Apply	N/A	Click the **Apply** button to apply the saved configuration.

Outdoor WiFi LoRa BSU

Outdoor WiFi LoRa BSU

WDS Only Mode

For the WDS Only mode, the device only bridges the connected wired clients to another WDS-enabled WiFi device which the device associated with. That is, it also means the no wireless clients stat can connect to this device while WDS Only Mode is selected.

▶ WiFi Operation Mode	WDS Only Mode ▾
▶ Green AP	☐ Enable
▶ Time Schedule	(0) Always ▾
▶ Scan Remote AP's MAC List	[Scan]
Remote AP MAC 1	[ ]
Remote AP MAC 2	[ ]
Remote AP MAC 3	[ ]
Remote AP MAC 4	[ ]

WDS Only Mode		
Item	**Value setting**	**Description**
Green AP	The box is unchecked by default.	Check the **Enable** box to activate **Green AP** function.
Time Schedule	A Must filled setting	Apply a specific **Time Schedule** to this rule; otherwise leave it as **(0) Always**. If the dropdown list is empty ensure **Time Schedule** is pre-configured. Refer to **Object Definition** > **Scheduling** > **Configuration** tab.
Scan Remote AP's MAC List	N/A	Press the **Scan** button to scan the spatial AP information, and then select one from the AP list, the MAC of selected AP will be auto filled in the following Remote AP MAC table.
Remote AP MAC 1~4	A Must filled setting	Enter the remote AP's MAC manually, or via auto-scan approach, The device will bridge the traffic to the remote AP when associated successfully.

ID	VAP	SSID	Authentication	Encryption	STA Isolation	Broadcast SSID	Enable	Actions
1	VAP 1	Staff_2.4G	WPA2-PSK	AES	☐	☑	☑	[Edit] ☐ Select

By default, VAP 1 is enabled and security key is required to connect to the gateway wirelessly to enhance the security level and prevent unexpected access of un-authorized devices.

The default wifi key is printed on both the device label and the Security Card. It is created randomly and differs from devices. So, you can connected to the VAP1 (SSID: Staff_2.4G) with the provided key.

However, it is strongly recommanded that you have to change the security key to a easy-to-remember one by clicking the Edit button.

Outdoor WiFi LoRa BSU

Under **WDS Only** mode, only VAP1 is available for further specifying the required authentication and Encryption settings. Click **Edit** button in the VAP List screen and a VAP Configuration screen will appear for you to configure the required settings

Item	Setting
▶ VAP	VAP1 ▾
▶ SSID	Staff_2.4G
▶ Max. STA	☐ Enable
▶ Authentication	WPA2-PSK ▾
▶ Encryption	AES ▾
▶ Preshared Key	1234567890
▶ STA Isolation	☑
▶ Broadcast SSID	☑
▶ Enable	☑

For the detail description about VAP configuration, please refer to the description stated in AP-Router section.

Outdoor WiFi LoRa BSU

WDS Hybrid Mode

For the WDS Hybrid mode, the device bridges all the wired **LAN** and **WLAN** clients to another WDS or WDS hybrid enabled WiFi devices which the device associated with.

▶ WiFi Operation Mode	WDS Hybrid Mode ▾
▶ Lazy Mode	☐ Enable
▶ Green AP	☐ Enable
▶ VAP Isolation	☑ Enable
▶ Time Schedule	(0) Always ▾
▶ Scan Remote AP's MAC List	Scan
Remote AP MAC 1	
Remote AP MAC 2	
Remote AP MAC 3	
Remote AP MAC 4	

WDS Hybrid Mode		
Item	**Value setting**	**Description**
Lazy Mode	The box is checked by default.	Check the **Enable** box to activate this function. With the function been enabled, the device can auto-learn WDS peers without manually entering other AP's MAC address. But at least one of the APs has to fill remote AP MAC addresses.
Green AP	The box is unchecked by default.	Check the **Enable** box to activate **Green AP** function.
VAP Isolation	The box is checked by default.	Check the **Enable** box to activate this function. By default, the box is checked; it means that stations which associated to different VAPs cannot communicate with each other.
Time Schedule	A Must filled setting	Apply a specific **Time Schedule** to this rule; otherwise leave it as **(0) Always**. If the dropdown list is empty ensure **Time Schedule** is pre-configured. Refer to **Object Definition** > **Scheduling > Configuration** tab.
Scan Remote AP's MAC List	Available when Lazy Mode disabled.	Press the **Scan** button to scan the spatial AP information, and then select one from the AP list, the MAC of selected AP will be auto filled in the following Remote AP MAC table.
Remote AP MAC 1~4	Available when Lazy Mode disabled.	Enter the remote AP's MAC manually, or via auto-scan approach, The device will bridge the traffic to the remote AP when associated successfully.

	2.4G VAP List Add Delete							
ID	VAP	SSID	Authentication	Encryption	STA Isolation	Broadcast SSID	Enable	Actions
1	VAP 1	Staff_2.4G	WPA2-PSK	AES	☑	☑	☑	Edit ☐ Select

By default, VAP 1 is enabled and security key is required to connect to the gateway wirelessly to enhance the security level and prevent unexpected access of un-authorized devices.

Outdoor WiFi LoRa BSU

The default wifi key is printed on both the device label and the Security Card. It is created randomly and differs from devices. So, you can connected to the VAP1 (SSID: Staff_2.4G) with the provided key.
However, it is strongly recommanded that you have to change the security key to a easy-to-remember one by clicking the Edit button.

Under **WDS Hybrid** mode, the VAP function is available and you can further specifying the required VAP settings for connecting with wireless client devices.

Click **Add** / **Edit** button in the VAP List screen to create or edit the settings for a VAP. A VAP Configuration screen will appear.

For VAP 1:

Item	Setting
▶ VAP	VAP1 ▾
▶ SSID	Staff_2.4G
▶ Max. STA	☐ Enable
▶ Authentication	WPA2-PSK ▾
▶ Encryption	AES ▾
▶ Preshared Key	1234567890
▶ STA Isolation	☑
▶ Broadcast SSID	☑
▶ Enable	☑

Outdoor WiFi LoRa BSU

For others:

Item	Setting
▸ VAP	VAP2 ▾
▸ SSID	default
▸ Max. STA	☐ Enable
▸ Authentication	Open ▾
▸ Encryption	None ▾
▸ STA Isolation	☐
▸ Broadcast SSID	☐
▸ Enable	☐

VAP Configuration

For the detail description about VAP configuration, please refer to the description stated in AP-Router section.

Outdoor WiFi LoRa BSU

2.3.2 Wireless Client List

The **Wireless Client List** page shows the information of wireless clients which are associated with this device.

Go to **Basic Network > WiFi > Wireless Client List** Tab.

Select Target WiFi

Item	Setting
▶ Module Select	One ▼
▶ Operation Band	2.4G ▼
▶ Multiple AP Names	All ▼

Target Configuration		
Item	**Value setting**	**Description**
Module Select	A Must filled setting.	Select the WiFi module to check the information of connected clients. For those single WiFi module products, this option is hidden.
Operation Band	A Must filled setting.	Specify the intended operation band for the WiFi module. Basically, this setting is fixed and cannot be changed once the module is integrated into the product. However, there is some module with selectable band for user to choose according to his network environment. Under such situation, you can specify which operation band is suitable for the application.
Multiple AP Names	1. A Must filled setting. 2. **All** is selected by default.	Specify the VAP to show the associated clients information in the following Client List. By default, All VAP is selected.

Show Client List

The following Client List shows the information for wireless clients that is associated with the selected VAP(s).

IP Address Configuration & Address	Host Name	MAC Address	Mode	Rate	RSSI0	RSSI1	Signal	Interface

Target Configuration		
Item	**Value setting**	**Description**
IP Address Configuration & Address	N/A	It shows the Client's IP address and the deriving method. **Dynamic** means the IP address is derived from a DHCP server. **Static** means the IP address is a fixed one that is self-filled by client.
Host Name	N/A	It shows the host name of client.
MAC Address	N/A	It shows the MAC address of client.
Mode	N/A	It shows what kind of **Wi-Fi system** the client used to associate with this device.

Rate	N/A	It shows the **data rate** between client and this device.
RSSI0, RSSI1	N/A	It shows the RX sensitivity (RSSI) value for each radio path.
Signal	N/A	The **signal strength** between client and this device.
Interface	N/A	It shows the VAP ID that the client associated with.
Refresh	N/A	Click the **Refresh** button to update the Client List immediately.

Outdoor WiFi LoRa BSU

2.3.3 Advanced Configuration

This device provides advanced wireless configuration for professional user to optimize the wireless performance under the specific installation environment. Please note that if you are not familiar with the WiFi technology, just leave the advanced configuration with its default values, or the connectivity and performance may get worse with improper settings.

Go to **Basic Network > WiFi > Advanced Configuration** Tab.

Select Target WiFi

Target WiFi	
Item	**Setting**
▶ Module Select	One ▼
▶ Operation Band	2.4G ▼

Target Configuration		
Item	**Value setting**	**Description**
Module Select	A Must filled setting.	Select the WiFi module to check the information of connected clients. For those single WiFi module products, this option is hidden.
Operation Band	A Must filled setting.	Specify the intended operation band for the WiFi module. Basically, this setting is fixed and cannot be changed once the module is integrated into the product. However, there is some module with selectable band for user to choose according to his network environment.

Setup Advanced Configuration

Advanced Configuration	
Item	**Setting**
▶ Regulatory Domain	(36, 40, 44, 48, 149, 153, 157, 161, 165)
▶ Beacon Interval	100 Range: (1~1000 msec)
▶ DTIM Interval	3 Range: (1~255)
▶ RTS Threshold	2347 Range: (1~2347)
▶ Fragmentation	2346 Range: (256~2346)
▶ WMM	☑ Enable
▶ Short GI	400ns ▼
▶ TX Rate	Best ▼
▶ RF Bandwidth	Auto ▼
▶ Transmit Power	100% ▼
▶ 5G Band Steering	☐ Enable
▶ WIDS	☐ Enable

Outdoor WiFi LoRa BSU

▸ Dynamic Frequency Selection	☑ Enable

Advanced Configuration		
Item	**Value setting**	**Description**
Regulatory Domain	The default setting is according to where the product sale to	It limits the available radio channel of this device. The permissible channels depend on the **Regulatory Domain**.
Beacon Interval	100	It shows the time interval between each beacon packet broadcasted. The beacon packet contains **SSID**, **Channel ID** and **Security setting**.
DTIM Interval	3	A **DTIM (Delivery Traffic Indication Message)** is a countdown informing clients of the next window for listening to broadcast message. When the device has buffered broadcast message for associated client, it sends the next DTIM with a DTIM value.
RTS Threshold	2347	**RTS (Request to send) Threshold** means when the packet size is over the setting value, then active **RTS** technique. RTS/CTS is a **collision avoidance** technique. It means RTS **never** activated when the threshold is set to **2347**.
Fragmentation	2346	Wireless frames can be divided into smaller units (fragments) to **improve performance** in the presence of RF interference at the limits of RF coverage.
WMM	The box is checked by default	**WMM (WiFi Multimedia)** can help control **latency** and **jitter** when transmitting **multimedia content** over a wireless connection.
Short GI	By default **400ns** is selected	**Short GI (Guard Interval)** is defined to set the sending interval between each packet. Note that lower **Short GI** could **increase** not only the **transition rate** but also **error rate**.
TX Rate	By default **Best** is selected	It means the **data transition rate**. When **Best** is selected, the device will choose a proper **data rat**e according to **signal strength**.
RF Bandwidth	By default **Auto** is selected	The setting of RF bandwidth limits the maximum data rate.
Transmit Power	By default **100%** is selected	Normally the wireless transmitter operates at 100% power. By setting the **transmit power** to control the WiFi **coverage**.
5G Band Steering	The box is unchecked by default	When the client station associate with 2.4G WiFi, the device will send the client to 5G WiFi automatically if the client is available on accessing this 5G Wi-Fi band. This option is only available on the module that supports 5GHz band.
WIDS	The box is unchecked by default	The WIDS (Wireless Intrusion Detection System) will analyze all packets and make a statistic table in WiFi status. Go to **Status** > **Basic Network** > **WiFi** tab for detailed WIDS status.
Dynamic Frequency Selection	The box is checked by default	**Dynamic Frequency Selection (DFS)** is a legally required feature for all WiFi devices that share the 5 GHz band with radar. DFS enables a gateway to detect radar signals and switch their operating frequency to prevent interference. This process ensures that radar systems send and receive accurate information. **Note**: Dynamic Frequency Selection (DFS) option is only available for the WiFi module with 5GHz radio.
Save	N/A	Click the **Save** button to save the current configuration.
Undo	N/A	Click the **Undo** button to restore configuration to previous setting before saving.

Outdoor WiFi LoRa BSU

2.3.4 Uplink Profile

This device provides WiFi Uplink function for connecting to a wireless access point just like connected to a wired WAN or cellular WAN connection. It can operate as a NAT gateway and link the devices wirelessly to the uplink network or hosts.

To connect to the wireless access point, user has to enable the wireless Uplink function for a certain WiFi Module (refer to **Basic Network > WAN & Uplink > Physical Interface**, **Internet Setup** tabs) first, and then configure the Uplink profile(s) for the access point to be connected to in the **Uplink Profile** page.

Go to **Basic Network > WiFi > Uplink Profile** tab for configuring the Uplink Profile page.

Uplink Profile Setting

Item	Setting
▶ Profile	☐ Enable
▶ Module Select	One ▾
▶ Operation Band	2.4G ▾
▶ Priority	⦿ By Signal Strength ○ By User-defined
▶ Current Profile	

Setting Item	Value setting	Description
Profile	1. A Must filled setting. 2. **Unchecked** by default.	Check the **Enable** box to activate the profile function. It is available only when the selected WiFi module is configured at WiFi Uplink mode.
Module Select	A Must filled setting.	Select the WiFi module to check or configure the expected uplink profile(s). For those single WiFi module products, this option is hidden.
Operation Band	A Must filled setting.	Specify the intended operation band for the WiFi module. Basically, this setting is fixed and cannot be changed once the module is integrated into the gateway product. However, there are some module with selectable band for user to choose according to his network environment. Under such situation, you can specify which operation band is suitable for the application.
Priority	1. A Must filled setting. 2. **By Signal Strength** is selected by default.	Specify the network selection methodology for connectin to an available wireless uplink network. It can be **By Signal Strength** or **By User-defined** priority. When **By Signal Strength** is selected, the gateway will try to connect to the available uplink network whose wireless signal strength is the strongest. When **By User-defined** is selected, the gateway will try to connect to the available uplink network whose priority is the highest (1 is the highest priority, and 16 is the lowest priority).
Current Profile	N/A	After enabling Profile and connecting by a certain uplink profile, the profile name will be displayed.

Outdoor WiFi LoRa BSU

Note: to apply the defined Uplink profile(s) for the gateway to find a best fit profile for connecting to a certain uplink network, user has to **Enable** the Profile auto-connect function (Refer to **Basic Network > WiFi > (Module 1/ Module 2) WiFi Configuration** tab.

Create/Edit Uplink Profile

The Profile List shows the settings for the created uplink profiles. The information includes Profile Name, SSID, Channel, Authentication, Encryption, MAC Address, Signal Strength, Priority, and Enable.

When **Add** button is applied, **Profile Configuration** screen will appear.

Profile Configuration		
Item	**Value setting**	**Description**
Profile Name	1. String format can be any text 2. A Must filled setting	Enter a profile name for the uplink network specified below. It is a name that is easy for you to understand. ***Value Range*: 1 ~ 64 characters.**
Network ID (SSID)	1. String format : Any text 2. The box is checked by default.	Enter the SSID for the VAP, and decide whether to broadcast the SSID or not. The **SSID** is used for identifying from another AP, and client stations will associate with AP according to SSID. If the broadcast SSID option is enabled, it means the SSID will be broadcasted, and the stations can associate with this device by scanning SSID.
Channel	1. A Must filled setting. 2. **Auto** is selected by default.	Select a radio channel for the VAP. Each channel is corresponding to different radio band. The permissible channels depend on the **Regulatory Domain**. There are two available options when **Auto** is selected: ● **By AP Numbers**

75

Outdoor WiFi LoRa BSU

		The channel will be selected according to AP numbers (The less, the better). ● **By Less Interference** The channel will be selected according to interference. (The lower, the better).
Authentication	1. A Must filled setting 2. **Open** is selected by default.	Specify the authentication method for connecting with the uplink network. It can be **Open**, **Shared**, **WPA-SPK**, or **WPA2-PSK**. When **Open** is selected, the preshared WEP key could be set for authentication; When **Shared** is selected, the preshared WEP key should be set for authentication; When **WPA-PSK** or **WPA2-PSK** is selected, The the TKIP or AES preshared key should be set for authentication;
Encryption	1. A Must filled setting. 2. **None** is selected by default.	Select a suitable encryption method and enter the required key(s). The available method in the dropdown list depends on the Authentication you selected. **None** It means that the device is open system without encrypting. **WEP** Up to 4 WEP keys can be set, and you have to select one as current key. The key type can set to **HEX** or **ASCII**. If **HEX** is selected, the key should consist of (0 to 9) and (A to F). If **ASCII** is selected, the key should consist of ASCII table. **TKIP** TKIP was proposed instead of WEP without upgrading hardware. Enter a Preshared Key for it. The length of key is from 8 to 63 characters. **AES** The newest encryption system in WiFi, it also designed for the fast 802.11n high bitrates schemes. Enter a Preshared Key for it. The length of key is from 8 to 63 characters. You are recommended to use **AES** encryption instead of any others for security.
MAC Address	1. MAC Address string Format 2. A Must fill setting	Specify the **MAC Address** of the access point (with the Network ID) to be connected to.
Priority	1. An Optional filled setting. 2. **16** is set by default.	Specify a priority setting for the uplink profile when the **By User-defined** methodology is selected. The priority value can be 1 ~ 16. 1 is the highest priority, and 16 is the lowest priority).
Enable	The box is checked by default.	Click the **Enable** box to activate this profile.
Save	N/A	Click the **Save** button to save the configuration.
Undo	N/A	Click the **Undo** button to restore what you just configured back to the previous setting.
Back	N/A	When the **Back** button is clicked, the screen will return to the Profile List page.

Instead of manually enter the information for the uplink network, you can alslo click the **Scan** button to get the available wireless networks around the device, and select one as the uplink network.

When the **Scan** button is applied, **Wireless AP List** will appear after few seconds.

Outdoor WiFi LoRa BSU

SSID	Channel	Quality	Authentication	Encryption	MAC Address	Select
Wireless AP List						
Guest_2.4G	1	86%		None	02:50:78:56:79:15	○
WIN	1	100%	WPA2-PSK	AES	00:60:64:cb:f5:f6	○
amit02	1	63%	WPA2-PSK	AES	00:50:18:21:e2:17	○
Guest_2.4G	1	5%		None	1a:50:18:33:55:66	○
lan test_24_1	1	86%	WPA2-PSK	AES	00:50:18:56:79:15	○
lan test_24_3	1	89%	WPA2-PSK	AES	02:50:28:56:79:15	○
lan test_24_5	1	86%	WPA2-PSK	AES	02:50:48:56:79:15	○
lan test_24_7	1	86%	WPA2-PSK	AES	02:50:68:56:79:15	○

Once you selected an AP from the AP list, the channel, SSID, Authentication, Encryption, and MAC address will be automatically filled into the profile, you just have to enter a key for the uplink connection, if required.

2.4 IPv6 (not supported)

Not supported feature for the purchased product, leave it as blank.

Outdoor WiFi LoRa BSU

2.5   Port Forwarding

Network address translation (NAT) is a methodology of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device. The technique was originally used for ease of rerouting traffic in IP networks without renumbering every host. It has become a popular and essential tool in conserving global address space allocations in face of IPv4 address exhaustion. The product you purchased embeds and activates the NAT function. You also can disable the NAT function in **[Basic Network]-[WAN & Uplink]-[Internet Setup]-[WAN Type Configuration]** page.
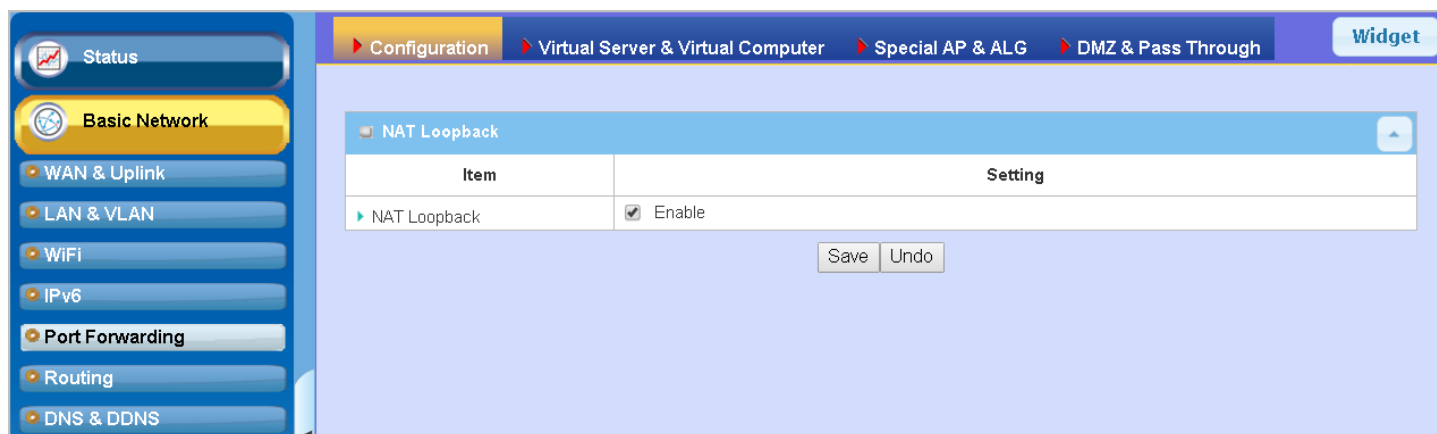
Usually all local hosts or servers behind corporate gateway are protected by NAT firewall. NAT firewall will filter out unrecognized packets to protect your Intranet. So, all local hosts are invisible to the outside world. Port forwarding or port mapping is function that redirects a communication request from one address and port number combination to assigned one. This technique is most commonly used to make services on a host residing on a protected or masqueraded (internal) network available to hosts on the opposite side of the gateway (external network), by remapping the destination IP address and port number

2.5.1 Configuration

NAT Loopback

This feature allows you to access the WAN global IP address from your inside NAT local network. It is useful when you run a server inside your network. For example, if you set a mail server at LAN side, your local devices can access this mail server through gateway's global IP address when enable NAT loopback feature. On either side are you in accessing the email server, at the LAN side or at the WAN side, you don't need to change the IP address of the mail server.

Configuration Setting

Go to **Basic Network > Port Forwarding > Configuration** tab.

The NAT Loopback allows user to access the WAN IP address from inside your local network.

Enable NAT Loopback

Configuration Item	Value setting	Description
NAT Loopback	The box is checked by default	Check the **Enable** box to activate this NAT function
Save	N/A	Click the **Save** button to save the settings.
Undo	N/A	Click the **Undo** button to cancel the settings

2.5.2 Virtual Server & Virtual Computer

There are some important Pot Forwarding functions implemented within the gateway, including "Virtual Server", "NAT loopback" and "Virtual Computer".

It is necessary for cooperate staffs who travel outside and want to access various servers behind office gateway. You can set up those servers by using "Virtual Server" feature. After trip, if want to access those servers from LAN side by global IP, without change original setting, NAT Loopback can achieve it.

"Virtual computer" is a host behind NAT gateway whose IP address is a global one and is visible to the outside world. Since it is behind NAT, it is protected by gateway firewall. To configure Virtual Computer, you just have to map the local IP of the virtual computer to a global IP.

Outdoor WiFi LoRa BSU

Virtual Server & NAT Loopback

Network-A

Gateway
Global IP: 118.18.81.33
Local IP: 10.0.75.2

1. Configure E-mail Server (10.0.75.101) as a Virtual Server.
2. Remote User access E-mail Server with Gateway Global IP (118.18.81.33).
3. With NAT Loopback enabled, Local User can access local E-mail Server with Global IP (118.18.81.33) as well.

E-mail Server 10.0.75.101

Local User 10.0.75.100

File Server
Global IP: 118.18.81.44
Local IP: 10.0.75.102
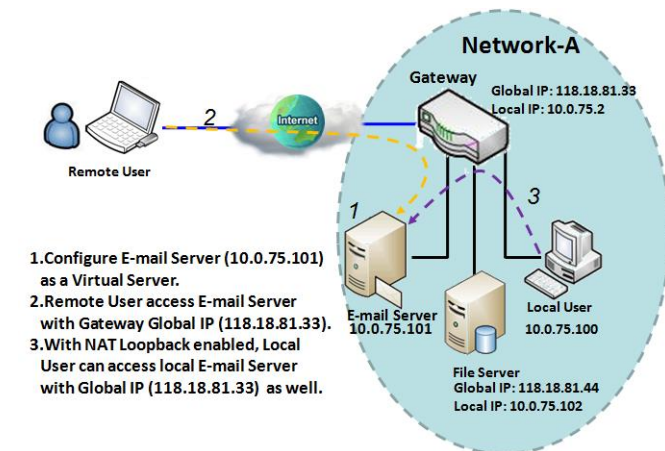
"Virtual Server" allows you to access servers with the global IP address or FQDN of the gateway as if they are servers existed in the Internet. But in fact, these servers are located in the Intranet and are physically behind the gateway. The gateway serves the service requests by port forwarding the requests to the LAN servers and transfers the replies from LAN servers to the requester on the WAN side. As shown in example, an E-mail virtual server is defined to be located at a server with IP address 10.0.75.101 in the Intranet of Network-A, including SMTP service port 25 and POP3 service port 110. So, the remote user can access the E-mail server with the gateway's global IP 118.18.81.33 from its WAN side. But the real E-mail server is located at LAN side and the gateway is the port forwarder for E-mail service.

NAT Loopback allows you to access the WAN global IP address from your inside NAT local network. It is useful when you run a server inside your network. For example, if you set a mail server at LAN side, your local devices can access this mail server through gateway's global IP address when enable NAT loopback feature. On either side are you in accessing the email server, at the LAN side or at the WAN side, you don't need to change the IP address of the mail server.

Virtual Computer

Network-A

Gateway
Global IP: 118.18.81.33
Local IP: 10.0.75.2

1. Configure File Server as a Virtual Computer by Global IP (118.18.81.44).
2. Remote User access File Server as by global IP (118.18.81.44) directly

E-mail Server 10.0.75.101

Local User 10.0.75.100

File Server
Global IP: 118.18.81.44
Local IP: 10.0.75.102
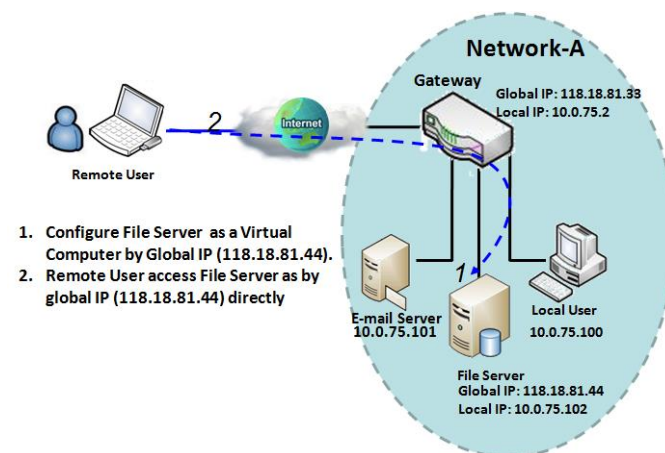
"Virtual Computer" allows you to assign LAN hosts to global IP addresses, so that they can be visible to outside world. While so, they are also protected by the gateway firewall as being client hosts in the Intranet. For example, if you set a FTP file server at LAN side with local IP address 10.0.75.102 and global IP address 118.18.82.44, a remote user can access the file server while it is hidden behind the NAT gateway. That is because the gateway takes care of all accessing to the IP address 118.18.82.44, including to forward the access requests to the file server and to send the replies from the server to outside world**.**

Outdoor WiFi LoRa BSU

Virtual Server & Virtual Computer Setting

Go to **Basic Network > Port Forwarding > Virtual Server & Virtual Computer** tab.

Enable Virtual Server and Virtual Computer

Item	Setting
▸ Virtual Server	☐ Enable
▸ Virtual Computer	☑ Enable

Configuration Item	Value setting	Description
Virtual Server	The box is unchecked by default	Check the **Enable** box to activate this port forwarding function
Virtual Computer	The box is checked by default	Check the **Enable** box to activate this port forwarding function
Save	N/A	Click the **Save** button to save the settings.
Undo	N/A	Click the **Undo** button to cancel the settings.

Create / Edit Virtual Server

The gateway allows you to custom your Virtual Server rules. It supports up to a maximum of 20 rule-based Virtual Server sets.

ID	WAN Interface	Server IP	Source IP	Protocol	Public Port	Private Port	Time Schedule	Enable	Actions

When **Add** button is applied, **Virtual Server Rule Configuration** screen will appear.

Outdoor WiFi LoRa BSU

Virtual Server Rule Configuration		
Item	**Value setting**	**Description**
WAN Interface	1. A Must filled setting 2. Default is **ALL**.	Define the selected interface to be the packet-entering interface of the gateway. If the packets to be filtered are coming from **WAN-x** then select **WAN-x** for this field. Select **ALL** for packets coming into the gateway from any interface. It can be selected **WAN-x** box when **WAN-x** enabled. **Note**: The available check boxes (**WAN-1** ~ **WAN-4**) depend on the number of WAN interfaces for the product.
Server IP	A Must filled setting	This field is to specify the IP address of the interface selected in the WAN Interface setting above.
Source IP	1. A Must filled setting 2. By default **Any** is selected	This field is to specify the **Source IP address**. Select **Any** to allow the access coming from any IP addresses. Select **Specific IP Address** to allow the access coming from an IP address. Select **IP Range** to allow the access coming from a specified range of IP address.
Protocol	1. A Must filled setting 2. **TCP & UDP** is selected by default.	When **"ICMPv4"** is selected It means the option "Protocol" of packet filter rule is ICMPv4. Apply **Time Schedule** to this rule, otherwise leave it as **Always**. (refer to **Scheduling setting** under **Object Definition**) Then check **Enable** box to enable this rule. When **"TCP"** is selected It means the option "Protocol" of packet filter rule is TCP. **Public Port** selected a predefined port from **Well-known Service**, and **Private Port** is the same with **Public Port** number. **Public Port** is selected **Single Port** and specify a port number, and **Private Port** can be set a **Single Port** number. **Public Port** is selected **Port Range** and specify a port range, and **Private Port** can be selected **Single Port** or **Port Range**. *Value Range*: 1 ~ 65535 for Public Port, Private Port.

When **"UDP"** is selected

It means the option "Protocol" of packet filter rule is UDP.

Public Port selected a predefined port from **Well-known Service**, and **Private Port** is the same with **Public Port** number.

Public Port is selected **Single Port** and specify a port number, and **Private Port** can be set a **Single Port** number.

Public Port is selected **Port Range** and specify a port range, and **Private Port** can be selected **Single Port** or **Port Range**.

Value Range: 1 ~ 65535 for Public Port, Private Port.

When **"TCP & UDP"** is selected

It means the option "Protocol" of packet filter rule is TCP and UDP.

Public Port selected a predefined port from **Well-known Service**, and **Private Port** is the same with **Public Port** number.

Public Port is selected **Single Port** and specify a port number, and **Private Port** can be set a **Single Port** number.

Public Port is selected **Port Range** and specify a port range, and **Private Port** can be selected **Single Port** or **Port Range**.

Value Range: 1 ~ 65535 for Public Port, Private Port.

When **"GRE"** is selected

It means the option "Protocol" of packet filter rule is GRE.

When **"ESP"** is selected

It means the option "Protocol" of packet filter rule is ESP.

When **"SCTP"** is selected

It means the option "Protocol" of packet filter rule is SCTP.

When **"User-defined"** is selected

It means the option "Protocol" of packet filter rule is User-defined.

For **Protocol Number**, enter a port number.

Time Schedule	1. An optional filled setting 2. **(0) Always** Is selected by default.	Apply Time Schedule to this rule; otherwise leave it as (0) Always. (refer to Scheduling setting under Object Definition)
Rule	1. An optional filled setting 2.The box is unchecked by default.	Check the Enable box to activate the rule.
Save	N/A	Click the **Save** button to save the settings.
Undo	N/A	Click the **X** button to cancel the settings and return to previous page.

Outdoor WiFi LoRa BSU

Create / Edit Virtual Computer

The gateway allows you to custom your Virtual Computer rules. It supports up to a maximum of 20 rule-based Virtual Computer sets.

ID	Global IP	Local IP	Enable	Actions

When **Add** button is applied, **Virtual Computer Rule Configuration** screen will appear.

Global IP	Local IP	Enable
		☐

Virtual Computer Rule Configuration		
Item	**Value setting**	**Description**
Global IP	A Must filled setting	This field is to specify the IP address of the WAN IP.
Local IP	A Must filled setting	This field is to specify the IP address of the LAN IP.
Enable	N/A	Then check **Enable** box to enable this rule.
Save	N/A	Click the **Save** button to save the settings.

2.5.3 DMZ & Pass Through

DMZ (De Militarized Zone) Host is a host that is exposed to the Internet cyberspace but still within the protection of firewall by gateway device. So, the function allows a computer to execute 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications. In some cases when a specific application is blocked by NAT mechanism, you can indicate that LAN computer as a DMZ host to solve this problem.

The DMZ function allows you to ask the gateway pass through all normal packets to the DMZ host behind the NAT gateway only when these packets are not expected to receive by applications in the gateway or by other client hosts in the Intranet. Certainly, the DMZ host is also protected by the gateway firewall. Activate the feature and specify the DMZ host with a host in the Intranet when needed.

Item	Setting
▶ DMZ	☑ Enable ☑ All ☐ WAN-1 ☐ WAN-2 ☐ WAN-3 ☐ WAN-4 DMZ Host : 10.0.75.100
▶ Pass Through Enable	☑ IPSec ☑ PPTP ☑ L2TP

DMZ Scenario

Global IP:118.18.81.33
Local IP: 10.0.75.2
Gateway
Remote User 2
1.Set X Server as DMZ Host
2.Request X server service by Gateway Global IP
3.Gateway redirect service request to DMZ host: 10.0.75.100
DMZ Host 10.0.75.100
X Server

When the network administrator wants to set up some service daemons in a host behind NAT gateway to allow remote users request for services from server actively, you just have to configure this host as DMZ Host. As shown in the diagram, there is an X server installed as DMZ host, whose IP address is 10.0.75.100. Then, remote user can request services from X server just as it is provided by the gateway whose global IP address is 118.18.81.33. The gateway will forward those packets, not belonging to any configured virtual server or applications, directly to the DMZ host.

Outdoor WiFi LoRa BSU

VPN Pass through Scenario
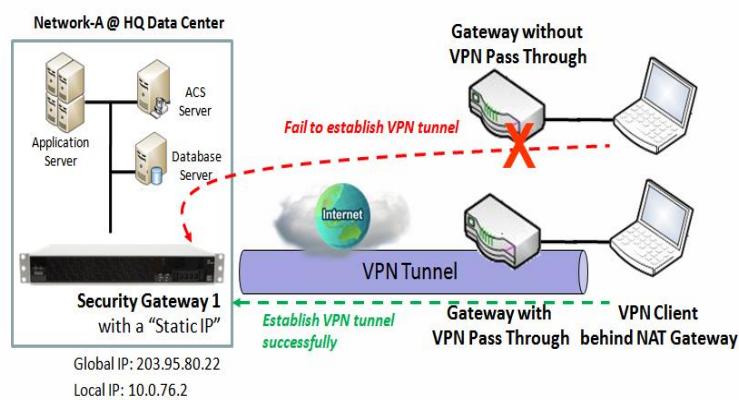
Since VPN traffic is different from that of TCP or UDP connection, it will be blocked by NAT gateway. To support the pass through function for the VPN connections initiating from VPN clients behind NAT gateway, the gateway must implement some kind of VPN pass through function for such application. The gateway support the pass through function for IPSec, PPTP, and L2TP connections, you just have to check the corresponding checkbox to activate it.

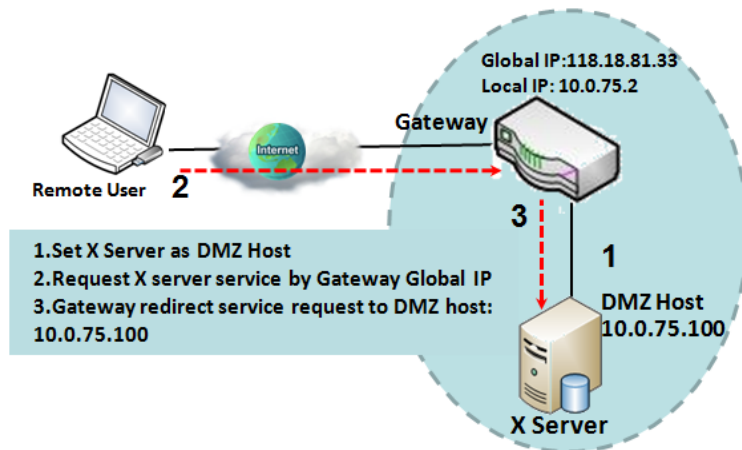## *DMZ & Pass Through Setting*

Go to **Basic Network > Port Forwarding > DMZ & Pass Through** tab.

The DMZ host is a host that is exposed to the Internet cyberspace but still within the protection of firewall by gateway device.

Enable DMZ and Pass Through

Configuration Item	Value setting	Description
DMZ	1. A Must filled setting 2. Default is **ALL**.	Check the **Enable** box to activate the DMZ function Define the selected interface to be the packet-entering interface of the gateway, and fill in the IP address of Host LAN IP in **DMZ Host** field . If the packets to be filtered are coming from **WAN-x** then select **WAN-x** for this field. Select **ALL** for packets coming into the router from any interfaces. It can be selected **WAN-x** box when **WAN-x** enabled.

		Note: The available check boxes (**WAN-1** ~ **WAN-4**) depend on the number of WAN interfaces for the product.
Pass Through Enable	The boxes are checked by default	Check the box to enable the pass through function for the **IPSec**, **PPTP**, and **L2TP**.
		With the pass through function enabled, the VPN hosts behind the gateway still can connect to remote VPN servers.
Save	N/A	Click the **Save** button to save the settings.
Undo	N/A	Click the **Undo** button to cancel the settings

2.6 Routing
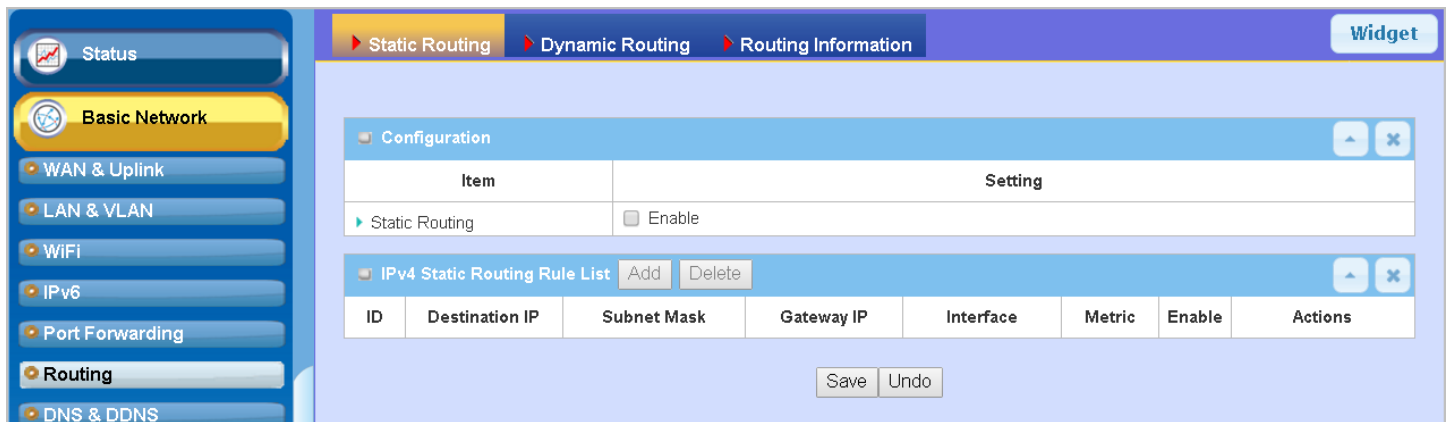
If you have more than one router and subnet, you will need to enable routing function to allow packets to find proper routing path and allow different subnets to communicate with each other. Routing is the process of selecting best paths in a network. It is performed for many kinds of networks, like electronic data networks (such as the Internet), by using packet switching technology. The routing process usually directs forwarding on the basis of routing tables which maintain a record of the routes to various network destinations. Thus, constructing routing tables, which are held in the router's memory, is very important for efficient routing. Most routing algorithms use only one network path at a time.

The routing tables record your pre-defined routing paths for some specific destination subnets. It is **static routing**. However, if the contents of routing tables record the obtained routing paths from neighbor routers by using some protocols, such as RIP, OSPF and BGP. It is **dynamic routing**. These both routing approaches will be illustrated one after one. In addition, the gateway also built in one advanced configurable routing software Quagga for more complex routing applications, you can configure it if required via Telnet CLI.

Outdoor WiFi LoRa BSU

2.6.1 Static Routing

"Static Routing" function lets you define the routing paths for some dedicated hosts/servers or subnets to store in the routing table of the gateway. The gateway routes incoming packets to different peer gateways based on the routing table. You need to define the static routing information in gateway routing rule list.
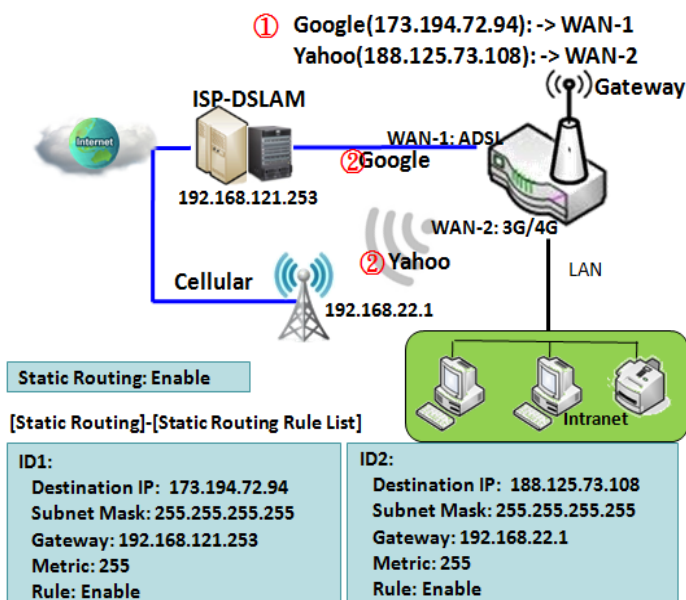
When the administrator of the gateway wants to specify what kinds of packets to be transferred via which gateway interface and which peer gateway to their destination. It can be carried out by the "Static Routing" feature. Dedicated packet flows from the Intranet will be routed to their destination via the pre-defined peer gateway and corresponding gateway interface that are defined in the system routing table by manual.

As shown in the diagram, when the destination is Google access, rule 1 set interface as ADSL, routing gateway as IP-DSLAM gateway 192.168.121.253. All the packets to Google will go through WAN-1. And the same way applied to rule 2 of access Yahoo. Rule 2 sets 3G/4G as interface.

Outdoor WiFi LoRa BSU

Static Routing Setting

Go to **Basic Network** > **Routing** > **Static Routing** Tab.

There are three configuration windows for static routing feature, including "Configuration", "Static Routing Rule List" and "Static Routing Rule Configuration" windows. "Configuration" window lets you activate the global static routing feature. Even there are already routing rules, if you want to disable routing temporarily, just uncheck the Enable box to disable it. "Static Routing Rule List" window lists all your defined static routing rule entries. Using "Add" or "Edit" button to add and create one new static routing rule or to modify an existed one.

When "**Add**" or "**Edit**" button is applied, the "Static Routing Rule Configuration" window will appear to let you define a static routing rule.

Enable Static Routing

Just check the **Enable** box to activate the "Static Routing" feature.

Item	Setting
▸ Static Routing	☑ Enable

Static Routing Item	Value setting	Description
Static Routing	The box is unchecked by default	Check the **Enable** box to activate this function

Create / Edit Static Routing Rules

The Static Routing Rule List shows the setup parameters of all static routing rule entries. To configure a static routing rule, you must specify related parameters including the destination IP address and subnet mask of dedicated host/server or subnet, the IP address of peer gateway, the metric and the rule activation.

ID	Destination IP	Subnet Mask	Gateway IP	Interface	Metric	Enable	Actions

The gateway allows you to custom your static routing rules. It supports up to a maximum of 64 rule sets. When **Add** button is applied, **Static Routing Rule Configuration** screen will appear, while the **Edit** button at the end

Outdoor WiFi LoRa BSU

of each static routing rule can let you modify the rule.

IPv4 Static Routing		
Item	**Value setting**	**Description**
Destination IP	1. IPv4 Format 2. A Must filled setting	Specify the Destination IP of this static routing rule.
Subnet Mask	255.255.255.0 (/24) is set by default	Specify the Subnet Mask of this static routing rule.
Gateway IP	1. IPv4 Format 2. A Must filled setting	Specify the Gateway IP of this static routing rule.
Interface	Auto is set by default	Select the Interface of this static routing rule. It can be **Auto**, or the available WAN / LAN interfaces.
Metric	1. Numberic String Format 2. A Must filled setting	The Metric of this static routing rule. *Value Range*: 0 ~ 255.
Rule	The box is unchecked by default.	Click **Enable** box to activate this rule.
Save	NA	Click the **Save** button to save the configuration
Undo	NA	Click the **Undo** button to restore what you just configured back to the previous setting.
Back	NA	When the **Back** button is clicked the screen will return to the Static Routing Configuration page.

2.6.2 Dynamic Routing
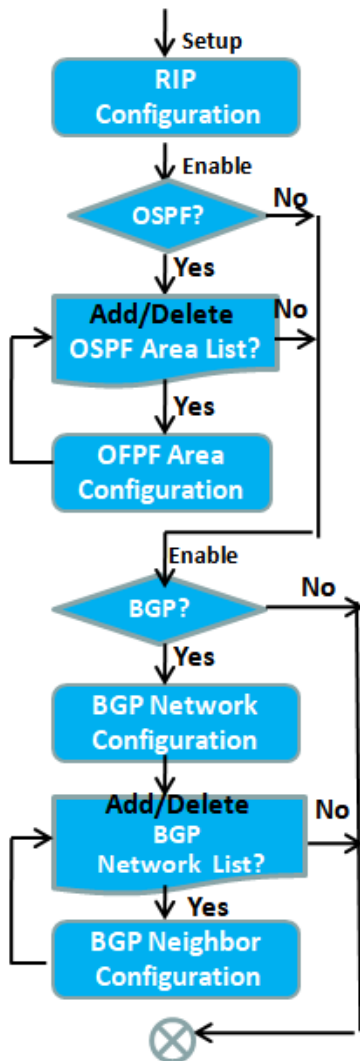
RIP Configuration			
Item	**Setting**		
▸ RIP Enable	Disable ▾		

OSPF Configuration	
Item	**Setting**
▸ OSPF	☐ Enable
▸ Router ID	
▸ Authentication	None ▾
▸ Backbone Subnet	

OSPF Area List	Add	Delete		
ID	**Area Subnet**	**Area ID**	**Enable**	**Actions**

OSPF Area Configuration	
Item	**Setting**
▸ Area Subnet	
▸ Area ID	
▸ Area	☐ Enable
	Save

BGP Configuration	
Item	**Setting**
▸ BGP	☐ Enable
▸ ASN	
▸ Router ID	

BGP Network List	Add	Delete	
ID	**Network Subnet**	**Enable**	**Actions**

BGP Neighbor List	Add	Delete		
ID	**Neighbor IP**	**Remote ASN**	**Enable**	**Actions**

Dynamic Routing, also called adaptive routing, describes the capability of a system, through which routes are characterized by their destination, to alter the path that the route takes through the system in response to a change in network conditions.

This gateway supports dynamic routing protocols, including RIPv1/RIPv2 (Routing Information Protocol), OSPF (Open Shortest Path First), and BGP (Border Gateway Protocol), for you to establish routing table automatically. The feature of dynamic routing will be very useful when there are lots of subnets in your network. Generally speaking, RIP is suitable for small network. OSPF is more suitable for medium network. BGP is more used for big network infrastructure.

Outdoor WiFi LoRa BSU

The supported dynamic routing protocols are described as follows.

RIP Scenario
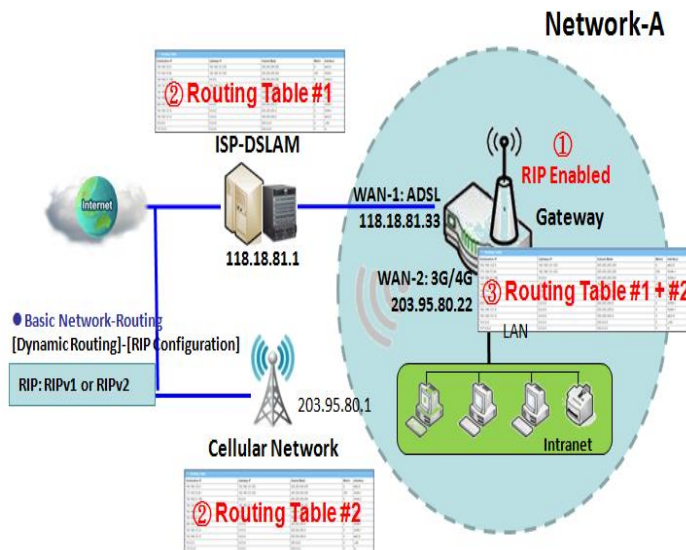
The Routing Information Protocol (RIP) is one of the oldest distance-vector routing protocols, which employs the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops allowed for RIP is 15. This hop limit, however, also limits the size of networks that RIP can support. A hop count of 16 is considered an infinite distance, in other words the route is considered unreachable. RIP implements the split horizon, route poisoning and hold-down mechanisms to prevent incorrect routing information from being propagated.

OSPF Scenario
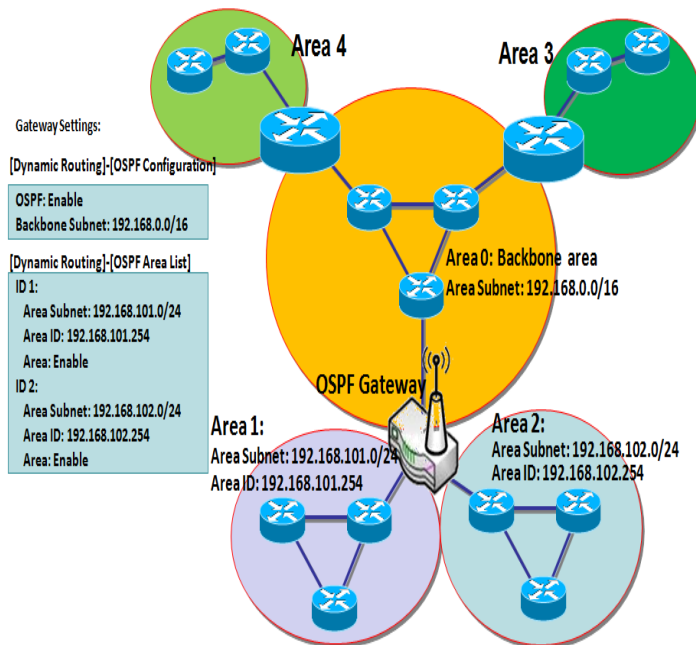
Open Shortest Path First (OSPF) is a routing protocol that uses link state routing algorithm. It is the most widely used interior gateway protocol (IGP) in large enterprise networks. It gathers link state information from available routers and constructs a topology map of the network. The topology is presented as a routing table which routes datagrams based solely on the destination IP address.

Network administrator can deploy OSPF gateway in large enterprise network to get its routing table from the enterprise backbone, and forward routing information to other routers, which are no linked to the enterprise backbone. Usually, an OSPF network is subdivided into routing areas to simplify administration and optimize traffic and resource utilization.

As shown in the diagram, OSPF gateway gathers routing information from the backbone gateways in area 0, and will forward its routing information to the routers in area 1 and area 2 which are not in the backbone.

Outdoor WiFi LoRa BSU

BGP Scenario
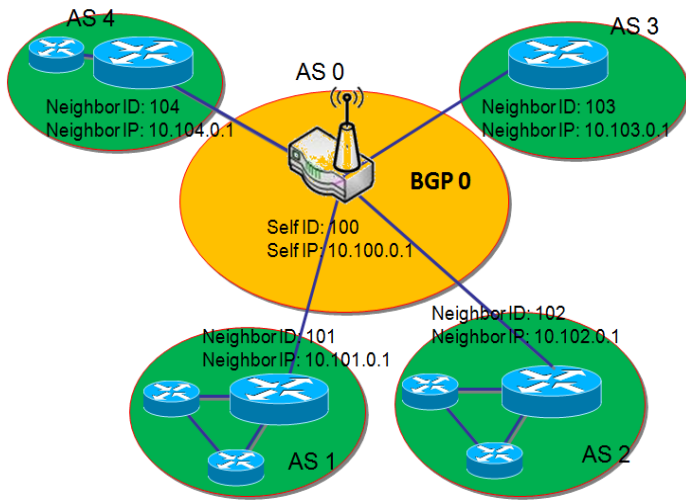
Border Gateway Protocol (BGP) is a standard exterior gateway protocol designed to exchange routing and reachability information between autonomous systems (AS) on the Internet. It usually makes routing decisions based on paths, network policies, or rule-sets.

Most ISPs use BGP to establish routing between one another (especially for multi-homed). Very large private IP networks also use BGP internally. The major BGP gateway within one AS will links with some other border gateways for exchanging routing information. It will distribute the collected data in AS to all routers in other AS.

As shown in the diagram, BGP 0 is gateway to dominate AS0 (self IP is 10.100.0.1 and self ID is 100). It links with other BGP gateways in the Internet. The scenario is like Subnet in one ISP to be linked with the ones in other ISPs. By operating with BGP protocol, BGP 0 can gather routing information from other BGP gateways in the Internet. And then it forwards the routing data to the routers in its dominated AS. Finally, the routers resided in AS 0 know how to route packets to other AS.

Outdoor WiFi LoRa BSU

Dynamic Routing Setting

Go to **Basic Network** > **Routing** > **Dynamic Routing** Tab.

The dynamic routing setting allows user to customize RIP, OSPF, and BGP protocol through the router based on their office setting.

In the "Dynamic Routing" page, there are several configuration windows for dynamic routing feature. They are the "RIP Configuration" window, "OSPF Configuration" window, "OSPF Area List", "OSPF Area Configuration", "BGP Configuration", "BGP Neighbor List" and "BGP Neighbor Configuration" window. RIP, OSPF and BGP protocols can be configured individually.

The "RIP Configuration" window lets you choose which version of RIP protocol to be activated or disable it. The "OSPF Configuration" window can let you activate the OSPF dynamic routing protocol and specify its backbone subnet. Moreover, the "OSPF Area List" window lists all defined areas in the OSPF network. However, the "BGP Configuration" window can let you activate the BGP dynamic routing protocol and specify its self ID. The "BGP Neighbor List" window lists all defined neighbors in the BGP network.

RIP Configuration

The RIP configuration setting allows user to customize RIP protocol through the router based on their office setting.

Item	Setting
▸ RIP Enable	Disable ▾

RIP Configuration		
Item	**Value setting**	**Description**
RIP Enable	Disable is set by default	Select **Disable** will disable RIP protocol. Select **RIP v1** will enable RIPv1 protocol. Select **RIP v2** will enable RIPv2 protocol.

OSPF Configuration

The OSPF configuration setting allows user to customize OSPF protocol through the router based on their office setting.

Outdoor WiFi LoRa BSU

OSPF Configuration	
Item	**Setting**
▶ OSPF	☐ Enable
▶ Router ID	
▶ Authentication	None ▾
▶ Backbone Subnet	

OSPF Configuration		
Item	**Value setting**	**Description**
OSPF	Disable is set by default	Click **Enable** box to activate the OSPF protocol.
Router ID	1. IPv4 Format 2. A Must filled setting	The Router ID of this router on OSPF protocol
Authentication	None is set by default	The Authentication method of this router on OSPF protocol. Select **None** will disable Authentication on OSPF protocol. Select **Text** will enable Text Authentication with entered the Key in this field on OSPF protocol. Select **MD5** will enable MD5 Authentication with entered the ID and Key in these fields on OSPF protocol.
Backbone Subnet	1. Classless Inter Domain Routing (CIDR) Subnet Mask Notation. (Ex: 192.168.1.0/24) 2. A Must filled setting	The Backbone Subnet of this router on OSPF protocol.

Create / Edit OSPF Area Rules

The gateway allows you to custom your OSPF Area List rules. It supports up to a maximum of 32 rule sets.

OSPF Area List Add Delete				▲
ID	**Area Subnet**	**Area ID**	**Enable**	**Actions**

When **Add** button is applied, **OSPF Area Rule Configuration** screen will appear.

Outdoor WiFi LoRa BSU

Item	Setting
▸ Area Subnet	
▸ Area ID	
▸ Area	☐ Enable
	Save

OSPF Area Configuration

Item	Value setting	Description
Area Subnet	1. Classless Inter Domain Routing (CIDR) Subnet Mask Notation. (Ex: 192.168.1.0/24) 2. A Must filled setting	The Area Subnet of this router on OSPF Area List.
Area ID	1. IPv4 Format 2. A Must filled setting	The Area ID of this router on OSPF Area List.
Area	The box is unchecked by default.	Click **Enable** box to activate this rule.
Save	N/A	Click the **Save** button to save the configuration

Outdoor WiFi LoRa BSU

BGP Configuration

The BGP configuration setting allows user to customize BGP protocol through the router setting.

Item	Setting
▶ BGP	☐ Enable
▶ ASN	
▶ Router ID	

BGP Network Configuration		
Item	**Value setting**	**Description**
BGP	The box is unchecked by default	Check the **Enable** box to activate the BGP protocol.
ASN	1. Numberic String Format 2. A Must filled setting	The ASN Number of this router on BGP protocol. ***Value Range***: 1 ~ 4294967295.
Router ID	1. IPv4 Format 2. A Must filled setting	The Router ID of this router on BGP protocol.

Create / Edit BGP Network Rules

The gateway allows you to custom your BGP Network rules. It supports up to a maximum of 32 rule sets.

BGP Network List Add Delete

ID	Network Subnet	Enable	Actions

When **Add** button is applied, **BGP Network Configuration** screen will appear.

Item	Setting
▶ Network Subnet	IP : 255.255.255.0 (/24) ▾
▶ Network	☐ Enable

Save

Item	Value setting	Description
Network Subnet	1. IPv4 Format	The Network Subnet of this router on BGP Network List. It composes of entered

	2. A Must filled setting	the IP address in this field and the selected subnet mask.
Network	The box is unchecked by default.	Click **Enable** box to activate this rule.
Save	N/A	Click the **Save** button to save the configuration

Create / Edit BGP Neighbor Rules

The gateway allows you to custom your BGP Neighbor rules. It supports up to a maximum of 32 rule sets.

BGP Neighbor List Add Delete				▲
ID	**Neighbor IP**	**Remote ASN**	**Enable**	**Actions**

When **Add** button is applied, **BGP Neighbor Configuration** screen will appear.

BGP Neighbor Configuration	▲ ✕
Item	**Setting**
▶ Neighbor IP	
▶ Remote ASN	
▶ Neighbor	☐ Enable
	Save

BGP Neighbor Configuration		
Item	**Value setting**	**Description**
Neighbor IP	1. IPv4 Format 2. A Must filled setting	The Neighbor IP of this router on BGP Neighbor List.
Remote ASN	1. Numberic String Format 2. A Must filled setting	The Remote ASN of this router on BGP Neighbor List. ***Value Range*: 1 ~ 4294967295.
Neighbor	The box is unchecked by default.	Click **Enable** box to activate this rule.
Save	N/A	Click the **Save** button to save the configuration

Outdoor WiFi LoRa BSU

2.6.3 Routing Information

The routing information allows user to view the routing table and policy routing information. Policy Routing Information is only available when the Load Balance function is enabled and the Load Balance Strategy is By User Policy.

Go to **Basic Network > Routing > Routing Information** Tab.

Routing Table

Destination IP	Subnet Mask	Gateway IP	Metric	Interface
100.105.167.72	255.255.255.252	0.0.0.0	0	WAN-2
192.168.66.0	255.255.255.0	0.0.0.0	0	LAN
192.168.127.0	255.255.255.0	0.0.0.0	0	WAN-1
169.254.0.0	255.255.0.0	0.0.0.0	0	LAN
127.0.0.0	255.0.0.0	0.0.0.0	0	lo

Routing Table Item	Value setting	Description
Destination IP	N/A	Routing record of Destination IP. IPv4 Format.
Subnet Mask	N/A	Routing record of Subnet Mask. IPv4 Format.
Gateway IP	N/A	Routing record of Gateway IP. IPv4 Format.
Metric	N/A	Routing record of Metric. Numeric String Format.
Interface	N/A	Routing record of Interface Type. String Format.

Policy Routing Information

Policy Routing Source	Source IP	Destination IP	Destination Port	WAN Interface
Load Balance	-	-	-	-

Policy Routing Information Item	Value setting	Description
Policy Routing Source	N/A	Policy Routing of Source. String Format.
Source IP	N/A	Policy Routing of Source IP. IPv4 Format.
Destination IP	N/A	Policy Routing of Destination IP. IPv4 Format.
Destination Port	N/A	Policy Routing of Destination Port. String Format.
WAN Interface	N/A	Policy Routing of WAN Interface. String Format.

2.7 DNS & DDNS

How does user access your server if your WAN IP address changes all the time? One way is to register a new domain name, and maintain your own DNS server. Another simpler way is to apply a domain name to a third-party DDNS service provider. The service can be free or charged. If you want to understand the basic concepts of DNS and Dynamic DNS, you can refer to Wikipedia website[3],[4].

2.7.1 DNS & DDNS Configuration

Dynamic DNS
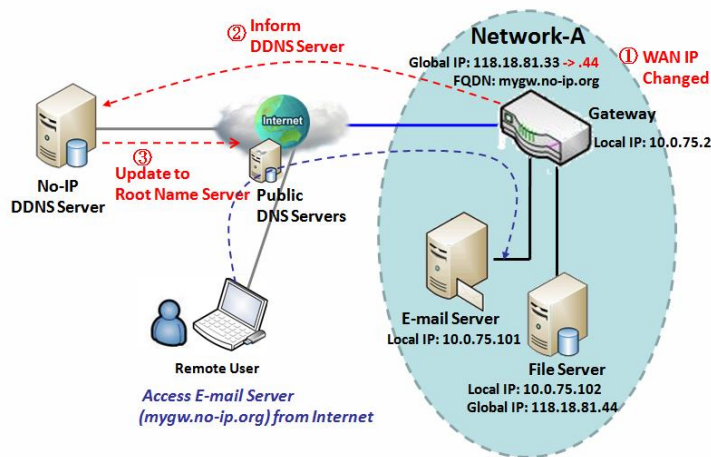
To host your server on a changing IP address, you have to use dynamic domain name service (DDNS). Therefore, anyone wishing to reach your host only needs to know the domain name. Dynamic DNS will map the name of your host to your current IP address, which changes each time you connect your Internet service provider.

The Dynamic DNS service allows the gateway to alias a public dynamic IP address to a static domain name, allowing the gateway to be more easily accessed from various locations on the Internet. As shown in the diagram, user registered a domain name to a third-party DDNS service provider (NO-IP) to use DDNS function. Once the IP address of designated WAN interface has changed, the dynamic DNS agent in the gateway will inform the DDNS server with the new IP address. The server automatically re-maps your domain name with the changed IP address. So, other hosts or remote users in the Internet world are able to link to your gateway by using your domain name regardless of the changing global IP address.

---

3 http://en.wikipedia.org/wiki/Domain_Name_System
4 http://en.wikipedia.org/wiki/Dynamic_DNS

Outdoor WiFi LoRa BSU

DNS & DDNS Setting

Go to **Basic Network** > **DNS & DDNS** > **Configuration** Tab.

The DNS & DDNS setting allows user to setup Dynamic DNS feature and DNS redirect rules.

Setup Dynamic DNS

The gateway allows you to custom your Dynamic DNS settings.

Dynamic DNS	
Item	**Setting**
▸ DDNS	☐ Enable
▸ WAN Interface	WAN-1 ▾
▸ Provider	DynDNS.org(Dynamic) ▾
▸ Host Name	
▸ User Name / E-Mail	
▸ Password / Key	

DDNS (Dynamic DNS) Configuration		
Item	**Value setting**	**Description**
DDNS	The box is unchecked by default	Check the **Enable** box to activate this function.
WAN Interface	WAN 1 is set by default	Select the WAN Interface IP Address of the gateway.
Provider	**DynDNS.org (Dynamic)** is set by default	Select your DDNS provider of Dynamic DNS. It can be **DynDNS.org(Dynamic)**, **DynDNS.org(Custom)**, **NO-IP.com**, etc...
Host Name	1. String format can be any text 2. A Must filled setting	Your registered host name of Dynamic DNS. ***Value Range***: 0 ~ 63 characters.
User Name / E-Mail	1. String format can be any text 2. A Must filled setting	Enter your User name or E-mail addresss of Dynamic DNS.
Password / Key	1. String format can be any text 2. A Must filled setting	Enter your Password or Key of Dynamic DNS.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Outdoor WiFi LoRa BSU

Setup DNS Redirect

DNS redirect is a special function to redirect certain traffics to a specified host. Administator can manage the internet / intranet traffics that are going to access some restricted DNS and force those traffics to be redirected to a specified host.

Item	Setting
▸ DNS Redirect	☐ Enable

DNS Redirect (header over the panel)

Item	Value setting	Description
DNS Redirect	The box is unchecked by default	Check the **Enable** box to activate this function.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

If you enabled the DNS Redirect function, you have to further specify the redirect rules. According to the rules, the gateway can redirect the traffic that matched the DNS to corresponding pre-defined IP address.

ID	Mapping Rule	Condition	Description	Enable	Action

When **Add** button is applied, **Redirect Rule** screen will appear.

Redirect Rule — Save

Item	Setting	
Mapping Rule	Domain Name	IP
	(* for Any)	
Condition	Always	
Description		
Enable	☐ Enable	

Redirect Rule Configuration

Item	Value setting	Description
Domain Name	1. String format can be any text	Enter a domain name to be redirect. The traffic to specified domain name will be redirect to the following IP address.

105

	2. A Must filled setting	**Value Range**: at least 1 character is required; '*' for any.
IP	1. IPv4 format 2. A Must filled setting	Enter an IP Address as the target for the DNS redirect.
Condition	1. A Must filled setting **2. Always is selected by default.**	Specify when will the DNS redirect action can be applied. It can be **Always**, or **WAN Block**. **Always:** The DNS redirect function can be applied to matched DNS all the time. **WAN Block:** The DNS redirect function can be applied to matched DNS only when the WAN connection is disconneced, or un-reachable.
Description	1. String format can be any text 2. A Must filled setting	Enter a brief description for this rule. **Value Range**: 0 ~ 63 characters.
Enable	The box is unchecked by default	Click the **Enable** button to activate this rule.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Chapter 3 Object Definition

3.1 Scheduling

Scheduling provides ability of adding/deleting time schedule rules, which can be applied to other functionality.

3.1.1 Scheduling Configuration

Go to **Object Definition > Scheduling > Configuration** tab.

ID	Rule Name	Actions

Time Schedule List [Add] [Delete]

Button description		
Item	**Value setting**	**Description**
Add	N/A	Click the **Add** button to configure time schedule rule
Delete	N/A	Click the **Delete** button to delete selected rule(s)

When **Add** button is applied, Time Schedule Configuration and Time Period Definition screens will appear.

Time Schedule Configuration

Item	Setting
▸ Rule Name	
▸ Rule Policy	Inactivate ▾ the Selected Days and Hours Below.

Time Schedule Configuration		
Item	**Value Setting**	**Description**
Rule Name	String: any text	Set rule name
Rule Policy	Default Inactivate	Inactivate/activate the function been applied to in the time period below

Outdoor WiFi LoRa BSU

Time Period Definition			
ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	-- choose one --		
2	-- choose one --		
3	-- choose one --		
4	-- choose one --		
5	-- choose one --		
6	-- choose one --		
7	-- choose one --		
8	-- choose one --		

Time Period Definition		
Item	**Value Setting**	**Description**
Week Day	Select from menu	Select everyday or one of weekday
Start Time	Time format (hh :mm)	Start time in selected weekday
End Time	Time format (hh :mm)	End time in selected weekday
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings
Refresh	N/A	Click the **Refresh** button to refresh the time schedule list.

3.2 User (not supported)

Not supported feature for the purchased product, leave it as blank.

3.3 Grouping (not supported)

Not supported feature for the purchased product, leave it as blank.

3.4 External Server

Go to **Object Definition > External Server > External Server** tab.

The External Server setting allows user to add external server.

Create External Server

☐ External Server List	Add	Delete				▲
ID	Server Name	Server Type	Server IP/FQDN	Server Port	Server Enable	Actions

When **Add** button is applied, **External Server Configuration** screen will appear.

☐ External Server Configuration	▲ ✕
Item	**Setting**
▶ Server Name	
▶ Server Type	Email Server ▾ User Name: Password:
▶ Server IP/FQDN	
▶ Server Port	25
▶ Server	☑ Enable
	Save Undo

Outdoor WiFi LoRa BSU

External Server Configuration		
Item	**Value setting**	**Description**
Sever Name	1. String format can be any text 2. A Must filled setting	Enter a server name. Enter a name that is easy for you to understand.
Server Type	A Must filled setting	Specify the Server Type of the external server, and enter the required settings for the accessing the server.
		Email Server (A Must filled setting) : When **Email Server** is selected, **User Name**, and **Password** are also required. **User Name** (String format: any text) **Password** (String format: any text)
		RADIUS Server (A Must filled setting) : When **RADIUS Server** is selected, the following settings are also required. Primary : **Shared Key** (String format: any text) Authentication Protocol (By default CHAP is selected) Session Timeout (By default **1**) The values must be between 1 and 60. Idle Timeout: (By default 1) The values must be between 1 and 15. Secondary : **Shared Key** (String format: any text) Authentication Protocol (By default CHAP is selected) Session Timeout (By default **1**) The values must be between 1 and 60. Idle Timeout: (By default 1) The values must be between 1 and 15.
		Active Directory Server (A Must filled setting) : When **Active Directory Server** is selected, **Domain** setting is also required. **Domain** (String format: any text)
		LDAP Server (A Must filled setting) : When **LDAP Server** is selected, the following settings are also required. **Base DN** (String format: any text) **Identity** (String format: any text) **Password** (String format: any text)
		UAM Server (A Must filled setting) : When **UAM Server** is selected, the following settings are also required. **Login URL** (String format: any text) **Shared Secret** (String format: any text) **NAS/Gateway ID** (String format: any text) **Location ID** (String format: any text) **Location Name** (String format: any text)

		TACACS+ Server (A Must filled setting) : When **TACACS+ Server** is selected, the following settings are also required. **Shared Key** (String format: any text) **Session Timeout** (String format: any number) The values must be between 1 and 60.
		SCEP Server (A Must filled setting) : When **SCEP Server** is selected, the following settings are also required. **Path** (String format: any text, By default **cgi-bin** is filled) **Application** (String format: any text, By default **pkiclient.exe** is filled)
		FTP(SFTP) Server (A Must filled setting) : When **FTP(SFTP) Server** is selected, the following settings are also required. **User Name** (String format: any text) **Password** (String format: any text) **Protocol** (Select **FTP** or **SFTP**) **Encryprion** (Select **Plain, Explicit FTPS** or **Implicit FTPS**) **Transfer mode** (Select **Passive** or **Active**)
Server IP/FQDN	A Must filled setting	Specify the IP address or FQDN used for the external server.
Server Port	A Must filled setting	Specify the Port used for the external server. If you selected a certain server type, the default server port number will be set. For **Email Server** 25 will be set by default; For **Syslog Server**, port 514 will be set by default; For **RADIUS Server**, port 1812, 1823 will be set by default; For **Active Directory Server**, port 389 will be set by default; For **LDAP Server**, port 389 will be set by default; For **UAM Server**, port 3990, 4990 will be set by default; For **TACACS+ Server**, port 49 will be set by default; For **SCEP Server**, port 80 will be set by default; For **FTP(SFTP) Server**, port 21 will be set by default; For **LoRa Server**, port 1700 will be set by default; ***Value Range*: 1 ~ 65535.**
Account Port	1. A Must filled setting **2. 1813 is set by default**	Specify the accounting port used if you selected external RADIUS server. ***Value Range*: 1 ~ 65535.**
Server	The box is checked by default	Click **Enable to** activate this External Server.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings
Refresh	N/A	Click the **Refresh** button to refresh the external server list.

3.5 Certificate

In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document used to prove ownership of a public key. The certificate includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are genuine. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner[5].

In a typical public-key infrastructure (PKI) scheme, the signer is a certificate authority (CA), usually a company such as VeriSign which charges customers to issue certificates for them. In a web of trust scheme, the signer is either the key's owner (a self-signed certificate) or other users ("endorsements") whom the person examining the certificate might know and trust. The device also plays as a CA role.

Certificates are an important component of Transport Layer Security (TLS, sometimes called by its older name SSL), where they prevent an attacker from impersonating a secure website or other server. They are also used in other important applications, such as email encryption and code signing. Here, it can be used in IPSec tunneling for user authentication.

3.5.1 Configuration

The configuration setting allows user to create Root Certificate Authority (CA) certificate and configure to set enable of SCEP. Root CA is the top-most certificate of the tree, the private key of which is used to "sign" other certificates.

Go to **Object Definition > Certificate > Configuration** tab.

Create Root CA

☐ Root CA Generate					▲ ✖
ID	Name	Subject	Issuer	Vaild To	Action

When **Generate** button is applied, **Root CA Certificate Configuration** screen will appear. The required information to be filled for the root CA includes the name, key, subject name and validity.

---

5 http://en.wikipedia.org/wiki/Public_key_certificate.

Outdoor WiFi LoRa BSU

Root CA Certificate Configuration	
Item	**Setting**
▸ Name	[ ]
▸ Key	Key Type : [RSA ▾] Key Length : [512-bits ▾] Digest Algorithm : [MD5 ▾]
▸ Subject Name	Country(C) : [ ] State(ST) : [ ] Location(L) : [ ] Organization(O) : [ ] Organization Unit(OU) : [ ] Common Name(CN) : [ ] E-mail : [ ]
▸ Validity Period	[20-years ▾]

| Root CA Certificate Configuration		
Item	**Value setting**	**Description**
Name	1. String format can be any text 2. A Must filled setting	Enter a Root CA Certificate name. It will be a certificate file name
Key	A Must filled setting	This field is to specify the key attribute of certificate. **Key Type** to set public-key cryptosystems. It only supports RSA now. **Key Length** to set s the size measured in bits of the key used in a cryptographic algorithm. **Digest Algorithm** to set identifier in the signature algorithm identifier of certificates
Subject Name	A Must filled setting	This field is to specify the information of certificate. **Country(C)** is the two-letter ISO code for the country where your organization is located. **State(ST)** is the state where your organization is located. **Location(L)** is the location where your organization is located. **Organization(O)** is the name of your organization. **Organization Unit(OU)** is the name of your organization unit. **Common Name(CN)** is the name of your organization. **Email** is the email of your organization. It has to be email address style.
Validity Period	A Must filled setting	This field is to specify the validity period of certificate.

Outdoor WiFi LoRa BSU

Setup SCEP

Item	Setting
▶ SCEP	☐ Enable
▶ Automatically re-enroll aging certificates	☐ Enable

SCEP Configuration

Item	Value setting	Description
SCEP	The box is unchecked by default	Check the **Enable** box to activate SCEP function.
Automatically re-enroll aging certificates	The box is unchecked by default	When **SCEP** is activated, check the **Enable** box to activate this function. It will be automatically check which certificate is aging. If certificate is aging, it will activate SCEP function to re-enroll automatically.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Outdoor WiFi LoRa BSU

3.5.2 My Certificate

My Certificate includes a Local Certificate List. Local Certificate List shows all generated certificates by the root CA for the gateway. And it also stores the generated Certificate Signing Requests (CSR) which will be signed by other external CAs. The signed certificates can be imported as the local ones of the gateway.

Self-signed Certificate Usage Scenario
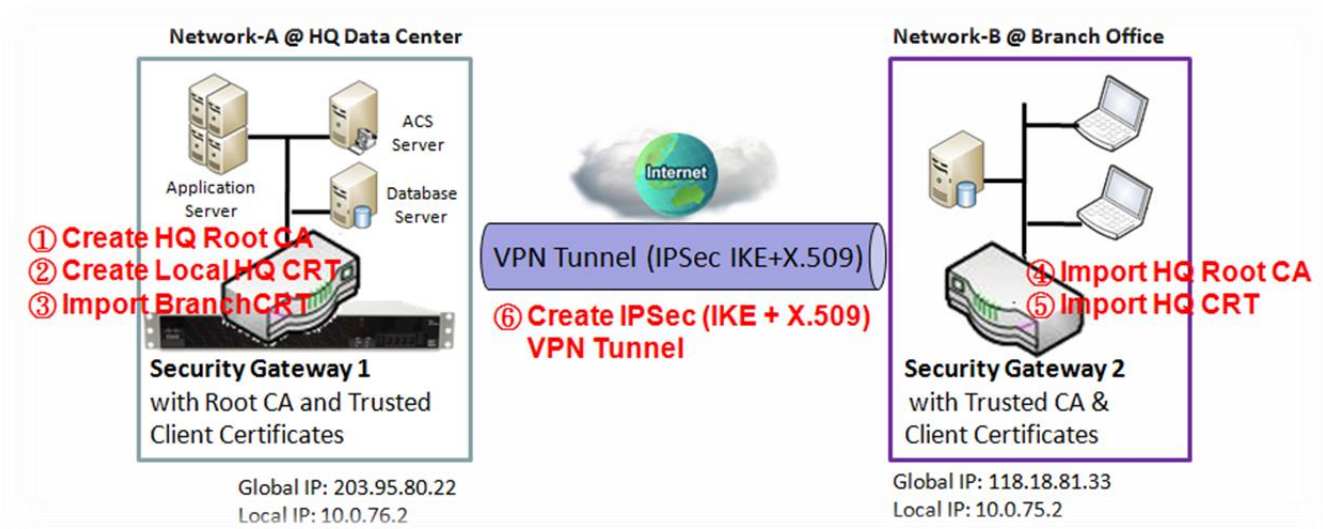
Scenario Application Timing

When the enterprise gateway owns the root CA and VPN tunneling function, it can generate its own local certificates by being signed by itself or import any local certificates that are signed by other external CAs. Also import the trusted certificates for other CAs and Clients. In addition, since it has the root CA, it also can sign Certificate Signing Requests (CSR) to form corresponding certificates for others. These certificates can be used for two remote peers to make sure their identity during establishing a VPN tunnel.

Scenario Description

Gateway 1 generates the root CA and a local certificate (HQCRT) signed by itself. Import a trusted certificate (BranchCRT) –a BranchCSR certificate of Gateway 2 signed by root CA of Gateway 1.

Gateway 2 creates a CSR (BranchCSR) to let the root CA of the Gateway 1 sign it to be the BranchCRT certificate. Import the certificate into the Gateway 2 as a local certificate. In addition, also import the certificates of the root CA of the Gateway 1 into the Gateway 2 as the trusted ones. (Please also refer to following two sub-sections)

Establish an IPSec VPN tunnel with IKE and X.509 protocols by starting from either peer, so that all

client hosts in these both subnets can communicate with each other.

Parameter Setup Example

For Network-A at HQ

Following tables list the parameter configuration as an example for the "My Certificate" function used in the user authentication of IPSec VPN tunnel establishing, as shown in above diagram. The configuration example must be combined with the ones in following two sections to complete the whole user scenario.

Use default value for those parameters that are not mentioned in the tables.

Configuration Path	[My Certificate]-[Root CA Certificate Configuration]
Name	*HQRootCA*
Key	Key Type: *RSA* Key Length: *1024-bits*
Subject Name	Country(C): *TW* State(ST): *Taiwan* Location(L): *Tainan* Organization(O): *AMITHQ* Organization Unit(OU): *HQRD* Common Name(CN): *HQRootCA* E-mail: *hqrootca@amit.com.tw*

Configuration Path	[My Certificate]-[Local Certificate Configuration]
Name	*HQCRT* Self-signed: ■
Key	Key Type: *RSA* Key Length: *1024-bits*
Subject Name	Country(C): *TW* State(ST): *Taiwan* Location(L): *Tainan* Organization(O): *AMITHQ* Organization Unit(OU): *HQRD* Common Name(CN): *HQCRT* E-mail: *hqcrt@amit.com.tw*

Configuration Path	[IPSec]-[Configuration]
IPSec	■ *Enable*

Configuration Path	[IPSec]-[Tunnel Configuration]
Tunnel	■ *Enable*
Tunnel Name	*s2s-101*
Interface	*WAN 1*
Tunnel Scenario	*Site to Site*
Operation Mode	*Always on*

Configuration Path	[IPSec]-[Local & Remote Configuration]
Local Subnet	*10.0.76.0*
Local Netmask	*255.255.255.0*
Full Tunnel	*Disable*
Remote Subnet	*10.0.75.0*
Remote Netmask	*255.255.255.0*
Remote Gateway	*118.18.81.33*

Outdoor WiFi LoRa BSU

Configuration Path	[IPSec]-[Authentication]
Key Management	*IKE+X.509* Local Certificate: *HQCRT* Remote Certificate: *BranchCRT*
Local ID	*User Name Network-A*
Remote ID	*User Name Network-B*

Configuration Path	[IPSec]-[IKE Phase]
Negotiation Mode	*Main Mode*
X-Auth	*None*

For Network-B at Branch Office

Following tables list the parameter configuration as an example for the "My Certificate" function used in the user authentication of IPSec VPN tunnel establishing, as shown in above diagram. The configuration example must be combined with the ones in following two sections to complete the whole user scenario.

Use default value for those parameters that are not mentioned in the tables.

Configuration Path	[My Certificate]-[Local Certificate Configuration]
Name	*BranchCRT* Self-signed: □
Key	Key Type: *RSA* Key Length: *1024-bits*
Subject Name	Country(C): *TW* State(ST): *Taiwan* Location(L): *Tainan* Organization(O): *AMITBranch* Organization Unit(OU): *BranchRD* Common Name(CN): *BranchCRT* E-mail: *branchcrt@amit.com.tw*

Configuration Path	[IPSec]-[Configuration]
IPSec	■ *Enable*

Configuration Path	[IPSec]-[Tunnel Configuration]
Tunnel	■ *Enable*
Tunnel Name	*s2s-102*
Interface	*WAN 1*
Tunnel Scenario	*Site to Site*
Operation Mode	*Always on*

Configuration Path	[IPSec]-[Local & Remote Configuration]
Local Subnet	*10.0.75.0*
Local Netmask	*255.255.255.0*
Full Tunnel	*Disable*
Remote Subnet	*10.0.76.0*

Remote Netmask	*255.255.255.0*
Remote Gateway	*203.95.80.22*

Configuration Path	[IPSec]-[Authentication]
Key Management	*IKE+X.509* Local Certificate: *BranchCRT* Remote Certificate: *HQCRT*
Local ID	*User Name Network-B*
Remote ID	*User Name Network-A*

Configuration Path	[IPSec]-[IKE Phase]
Negotiation Mode	*Main Mode*
X-Auth	*None*

Scenario Operation Procedure

In above diagram, "Gateway 1" is the gateway of Network-A in headquarters and the subnet of its Intranet is 10.0.76.0/24. It has the IP address of 10.0.76.2 for LAN interface and 203.95.80.22 for WAN-1 interface. "Gateway 2" is the gateway of Network-B in branch office and the subnet of its Intranet is 10.0.75.0/24. It has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN-1 interface. They both serve as the NAT security gateways.

Gateway 1 generates the root CA and a local certificate (HQCRT) that is signed by itself. Import the certificates of the root CA and HQCRT into the "Trusted CA Certificate List" and "Trusted Client Certificate List" of Gateway 2.

Gateway 2 generates a Certificate Signing Request (BranchCSR) for its own certificate (BranchCRT) (Please generate one not self-signed certificate in the Gateway 2, and click on the "View" button for that CSR. Just downloads it). Take the CSR to be signed by the root CA of Gateway 1 and obtain the BranchCRT certificate (you need rename it). Import the certificate into the "Trusted Client Certificate List" of the Gateway 1 and the "Local Certificate List" of Gateway 2.

Gateway 2 can establish an IPSec VPN tunnel with "Site to Site" scenario and IKE and X.509 protocols to Gateway 1.

Finally, the client hosts in two subnets of 10.0.75.0/24 and 10.0.76.0/24 can communicate with each other.

Outdoor WiFi LoRa BSU

My Certificate Setting

Go to **Object Definition > Certificate > My Certificate** tab.

The My Certificate setting allows user to create local certificates. In "My Certificate" page, there are two configuration windows for the "My Certificate" function. The "Local Certificate List" window shows the stored certificates or CSRs for representing the gateway. The "Local Certificate Configuration" window can let you fill required information necessary for corresponding certificate to be generated by itself, or corresponding CSR to be signed by other CAs.

Create Local Certificate

ID	Name	Subject	Issuer	Vaild To	Actions

Local Certificate List Add Import Delete

When **Add** button is applied, **Local Certificate Configuration** screen will appear. The required information to be filled for the certificate or CSR includes the name, key and subject name. It is a certificate if the "Self-signed" box is checked; otherwise, it is a CSR.

Item	Setting
▸ Name	Self-signed : ☐
▸ Key	Key Type : RSA ▾ Key Length : 1024-bits ▾ Digest Algorithm : SHA-1 ▾
▸ Subject Name	Country(C) : State(ST) : Location(L) : Organization(O) : Organization Unit(OU) : Common Name(CN) : E-mail :
▸ Extra Attributes	Challenge Password: Unstructured Name:
▸ SCEP Enrollment	Enable: ☐ SCEP Server: --- Option --- ▾ Add Object CA Certificate: amit-IDG761AM-JH.crt ▾ CA Encryption Certificate: --- Option --- ▾ (Optional) CA Identifier: (Optional)

Outdoor WiFi LoRa BSU

Local Certificate Configuration		
Item	**Value setting**	**Description**
Name	1. String format can be any text 2. A Must filled setting	Enter a certificate name. It will be a certificate file name If **Self-signed** is checked, it will be signed by root CA. If **Self-signed** is not checked, it will generate a certificate signing request (CSR).
Key	A Must filled setting	This field is to specify the key attributes of certificate. **Key Type** to set public-key cryptosystems. Currently, only RSA is supported. **Key Length** to set the length in bits of the key used in a cryptographic algorithm. It can be 512/768/1024/1536/2048. **Digest Algorithm** to set identifier in the signature algorithm identifier of certificates. It can be MD5/SHA-1.
Subject Name	A Must filled setting	This field is to specify the information of certificate. **Country(C)** is the two-letter ISO code for the country where your organization is located. **State(ST)** is the state where your organization is located. **Location(L)** is the location where your organization is located. **Organization(O)** is the name of your organization. **Organization Unit(OU)** is the name of your organization unit. **Common Name(CN)** is the name of your organization. **Email** is the email of your organization. It has to be email address setting only.
Extra Attributes	A Must filled setting	This field is to specify the extra information for generating a certificate. **Challenge Password** for the password you can use to request certificate revocation in the future. **Unstructured Name** for additional information.
SCEP Enrollment	A Must filled setting	This field is to specify the information of SCEP. If user wants to generate a certificate signing request (CSR) and then signed by SCEP server online, user can check the **Enable** box. Select a **SCEP Server** to identify the SCEP server for use. The server detailed information could be specified in External Servers. Refer to **Object Definition** > **External Server** > **External Server**. You may click **Add Object** button to generate, and the settings are the same as those defined in **Section 3.4 External Server**. Select a **CA Certificate** to identify which certificate could be accepted by SCEP server for authentication. It could be generated in Trusted Certificates. Select an optional **CA Encryption Certificate**, if it is required, to identify which certificate could be accepted by SCEP server for encryption data information. It could be generated in Trusted Certificates. Fill in optional **CA Identifier** to identify which CA could be used for signing certificates.
Save	N/A	Click the **Save** button to save the configuration.
Back	N/A	When the **Back** button is clicked, the screen will return to previous page.

Outdoor WiFi LoRa BSU

When **Import** button is applied, an Import screen will appear. You can import a certificate from an existed certificate file, or directly paste a PEM encoded string as the certificate.

Import		
Item	**Value setting**	**Description**
Import	A Must filled setting	Select a certificate file from user's computer, and click the **Apply** button to import the specified certificate file to the gateway.
PEM Encoded	1. String format can be any text 2. A Must filled setting	This is an alternative approach to import a certificate. You can directly fill in (Copy and Paste) the PEM encoded certificate string, and click the **Apply** button to import the specified certificate to the gateway.
Apply	N/A	Click the **Apply** button to import the certificate.
Cancel	N/A	Click the **Cancel** button to discard the import operation and the screen will return to the My Certificates page.

Outdoor WiFi LoRa BSU

3.5.3 Trusted Certificate

Trusted Certificate includes Trusted CA Certificate List, Trusted Client Certificate List, and Trusted Client Key List. The Trusted CA Certificate List places the certificates of external trusted CAs. The Trusted Client Certificate List places the others' certificates what you trust. And the Trusted Client Key List places the others' keys what you trusted.

Self-signed Certificate Usage Scenario

Scenario Application Timing (same as the one described in "My Certificate" section)

When the enterprise gateway owns the root CA and VPN tunneling function, it can generate its own local certificates by being signed by itself. Also imports the trusted certificates for other CAs and Clients. These certificates can be used for two remote peers to make sure their identity during establishing a VPN tunnel.

Scenario Description (same as the one described in "My Certificate" section)

Gateway 1 generates the root CA and a local certificate (HQCRT) signed by itself. Import a trusted certificate (BranchCRT) –a BranchCSR certificate of Gateway 2 signed by root CA of Gateway 1.

Gateway 2 creates a CSR (BranchCSR) to let the root CA of the Gateway 1 sign it to be the BranchCRT certificate. Import the certificate into the Gateway 2 as a local certificate. In addition, also imports the certificates of the root CA of Gateway 1 into the Gateway 2 as the trusted ones. (Please also refer to "My Certificate" and "Issue Certificate" sections).

Establish an IPSec VPN tunnel with IKE and X.509 protocols by starting from either peer, so that all client hosts in these both subnets can communicate with each other.

Parameter Setup Example (same as the one described in "My Certificate" section)

Outdoor WiFi LoRa BSU

For Network-A at HQ

Following tables list the parameter configuration as an example for the "Trusted Certificate" function used in the user authentication of IPSec VPN tunnel establishing, as shown in above diagram. The configuration example must be combined with the ones in "My Certificate" and "Issue Certificate" sections to complete the setup for the whole user scenario.

Configuration Path	[Trusted Certificate]-[Trusted Client Certificate List]
Command Button	*Import*

Configuration Path	[Trusted Certificate]-[Trusted Client Certificate Import from a File]
File	*BranchCRT.crt*

For Network-B at Branch Office

Following tables list the parameter configuration as an example for the "Trusted Certificate" function used in the user authentication of IPSec VPN tunnel establishing, as shown in above diagram. The configuration example must be combined with the ones in "My Certificate" and "Issued Certificate" sections to complete the setup for the whole user scenario.

Configuration Path	[Trusted Certificate]-[Trusted CA Certificate List]
Command Button	*Import*

Configuration Path	[Trusted Certificate]-[Trusted CA Certificate Import from a File]
File	*HQRootCA.crt*

Configuration Path	[Trusted Certificate]-[Trusted Client Certificate List]
Command Button	*Import*

Configuration Path	[Trusted Certificate]-[Trusted Client Certificate Import from a File]
File	*HQCRT.crt*

Scenario Operation Procedure (same as the one described in "My Certificate" section)

In above diagram, the "Gateway 1" is the gateway of Network-A in headquarters and the subnet of its Intranet is 10.0.76.0/24. It has the IP address of 10.0.76.2 for LAN interface and 203.95.80.22 for WAN-1 interface. The "Gateway 2" is the gateway of Network-B in branch office and the subnet of its Intranet is 10.0.75.0/24. It has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN-1 interface. They both serve as the NAT security gateways.

In Gateway 2 import the certificates of the root CA and HQCRT that were generated and signed by

Outdoor WiFi LoRa BSU

Gateway 1 into the "Trusted CA Certificate List" and "Trusted Client Certificate List" of Gateway 2.

Import the obtained BranchCRT certificate (the derived BranchCSR certificate after Gateway 1's root CA signature) into the "Trusted Client Certificate List" of the Gateway 1 and the "Local Certificate List" of the Gateway 2. For more details, refer to the Network-B operation procedure in "My Certificate" section of this manual.

Gateway 2 can establish an IPSec VPN tunnel with "Site to Site" scenario and IKE and X.509 protocols to Gateway 1.

Finally, the client hosts in two subnets of 10.0.75.0/24 and 10.0.76.0/24 can communicate with each other.

Outdoor WiFi LoRa BSU

Trusted Certificate Setting

Go to **Object Definition > Certificate > Trusted Certificate** tab.

The Trusted Certificate setting allows user to import trusted certificates and keys.

Import Trusted CA Certificate

ID	Name	Subject	Issuer	Vaild To	Actions

Trusted CA Certificate List [Import] [Delete] [Get CA]

When **Import** button is applied, a **Trusted CA import** screen will appear. You can import a Trusted CA certificate from an existed certificate file, or directly paste a PEM encoded string as the certificate.

Trusted CA Certificate Import from a File [Apply] [Cancel]

瀏覽... 未選擇檔案。

Trusted CA Certificate Import from a PEM [Apply] [Cancel]

Trusted CA Certificate List		
Item	**Value setting**	**Description**
Import from a File	A Must filled setting	Select a CA certificate file from user's computer, and click the **Apply** button to import the specified CA certificate file to the gateway.
Import from a PEM	1. String format can be any text 2. A Must filled setting	This is an alternative approach to import a CA certificate. You can directly fill in (Copy and Paste) the PEM encoded CA certificate string, and click the **Apply** button to import the specified CA certificate to the gateway.
Apply	N/A	Click the **Apply** button to import the certificate.
Cancel	N/A	Click the **Cancel** button to discard the import operation and the screen will return to the Trusted Certificates page.

Outdoor WiFi LoRa BSU

Instead of importing a Trusted CA certificate with mentioned approaches, you can also get the CA certificate from the SECP server.

If **SCEP** is enabled (Refer to **Object Definition** > **Certificate** > **Configuration**), you can click **Get CA** button, a Get CA Configuration screen will appear.

Get CA Configuration	
Item	Setting
▶ SCEP Server	--- Option --- ▼ Add Object
▶ CA Identifier	[ ] (Optional)

Get CA Configuration		
Item	**Value setting**	**Description**
SCEP Server	A Must filled setting	Select a **SCEP Server** to identify the SCEP server for use. The server detailed information could be specified in External Servers. Refer to **Object Definition** > **External Server** > **External Server**. You may click **Add Object** button to generate.
CA Identifier	1. String format can be any text	Fill in optional **CA Identifier** to identify which CA could be used for signing certificates.
Save	N/A	Click **Save** to save the settings.
Close	N/A	Click the **Close** button to return to the Trusted Certificates page.

Import Trusted Client Certificate

Trusted Client Certificate List Import Delete					
ID	Name	Subject	Issuer	Vaild To	Actions

When **Import** button is applied, a **Trusted Client Certificate Import** screen will appear. You can import a Trusted Client Certificate from an existed certificate file, or directly paste a PEM encoded string as the certificate.

Outdoor WiFi LoRa BSU

Trusted Client Certificate Import from a File [Apply] [Cancel]

瀏覽... 未選擇檔案。

Trusted Client Certificate Import from a PEM [Apply] [Cancel]

Trusted Client Certificate List		
Item	**Value setting**	**Description**
Import from a File	A Must filled setting	Select a certificate file from user's computer, and click the **Apply** button to import the specified certificate file to the gateway.
Import from a PEM	1. String format can be any text 2. A Must filled setting	This is an alternative approach to import a certificate. You can directly fill in (Copy and Paste) the PEM encoded certificate string, and click the **Apply** button to import the specified certificate to the gateway.
Apply	N/A	Click the **Apply** button to import certificate.
Cancel	N/A	Click the **Cancel** button to discard the import operation and the screen will return to the Trusted Certificates page.

Import Trusted Client Key

Trusted Client Key List [Import] [Delete]

ID	Name	Actions

When **Import** button is applied, a **Trusted Client Key Import** screen will appear. You can import a Trusted Client Key from an existed file, or directly paste a PEM encoded string as the key.

Outdoor WiFi LoRa BSU

Trusted Client Key List		
Item	**Value setting**	**Description**
Import from a File	A Must filled setting	Select a certificate key file from user's computer, and click the **Apply** button to import the specified key file to the gateway.
Import from a PEM	1. String format can be any text 2. A Must filled setting	This is an alternative approach to import a certificate key. You can directly fill in (Copy and Paste) the PEM encoded certificate key string, and click the **Apply** button to import the specified certificate key to the gateway.
Apply	N/A	Click the **Apply** button to import the certificate key.
Cancel	N/A	Click the **Cancel** button to discard the import operation and the screen will return to the Trusted Certificates page.

3.5.4 Issue Certificate

When you have a Certificate Signing Request (CSR) that needs to be certificated by the root CA of the device, you can issue the request here and let Root CA sign it. There are two approaches to issue a certificate. One is from a CSR file importing from the managing PC and another is copy-paste the CSR codes in gateway's web-based utility, and then click on the "Sign" button.

If the gateway signs a CSR successfully, the "Signed Certificate View" window will show the resulted certificate contents. In addition, a "Download" button is available for you to download the certificate to a file in the managing PC.

Self-signed Certificate Usage Scenario
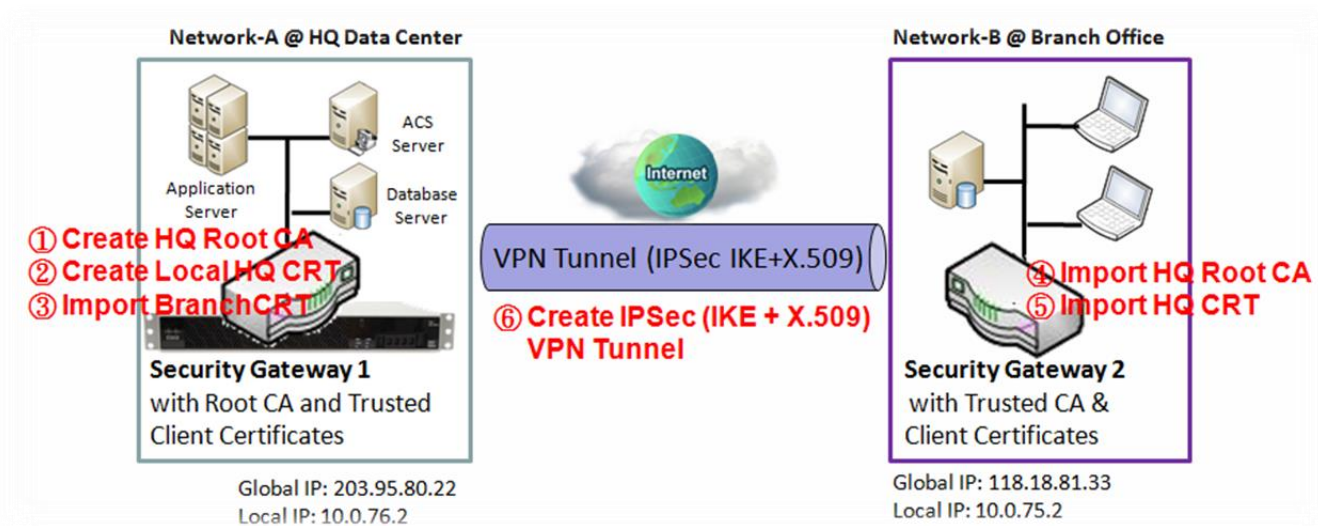
Scenario Application Timing (same as the one described in "My Certificate" section)

When the enterprise gateway owns the root CA and VPN tunneling function, it can generate its own local certificates by being signed by itself. Also imports the trusted certificates for other CAs and Clients. These certificates can be used for two remote peers to make sure their identity during establishing a VPN tunnel.

Scenario Description (same as the one described in "My Certificate" section)

Gateway 1 generates the root CA and a local certificate (HQCRT) signed by itself. Also imports a trusted certificate (BranchCRT) –a BranchCSR certificate of Gateway 2 signed by root CA of Gateway 1.

Gateway 2 creates a CSR (BranchCSR) to let the root CA of the Gateway 1 sign it to be the BranchCRT certificate. Import the certificate into the Gateway 2 as a local certificate. In addition, also imports the certificates of the root CA of the Gateway 1 into the Gateway 2 as the trusted ones. (Please also refer

to "My Certificate" and "Trusted Certificate" sections).

Establish an IPSec VPN tunnel with IKE and X.509 protocols by starting from either peer, so that all client hosts in these both subnets can communicate with each other.

Parameter Setup Example (same as the one described in "My Certificate" section)

For Network-A at HQ

Following tables list the parameter configuration as an example for the "Issue Certificate" function used in the user authentication of IPSec VPN tunnel establishing, as shown in above diagram. The configuration example must be combined with the ones in "My Certificate" and "Trusted Certificate" sections to complete the setup for whole user scenario.

Configuration Path	[Issue Certificate]-[Certificate Signing Request Import from a File]
Browse	*C:/BranchCSR*
Command Button	*Sign*

Configuration Path	[Issue Certificate]-[Signed Certificate View]
Command Button	*Download* (default name is "issued.crt")

Scenario Operation Procedure (same as the one described in "My Certificate" section)

In above diagram, the "Gateway 1" is the gateway of Network-A in headquarters and the subnet of its Intranet is 10.0.76.0/24. It has the IP address of 10.0.76.2 for LAN interface and 203.95.80.22 for WAN-1 interface. The "Gateway 2" is the gateway of Network-B in branch office and the subnet of its Intranet is 10.0.75.0/24. It has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN-1 interface. They both serve as the NAT security gateways.

Gateway 1 generates the root CA and a local certificate (HQCRT) that is signed by itself. Import the certificates of the root CA and HQCRT into the "Trusted CA Certificate List" and "Trusted Client Certificate List" of Gateway 2.

Gateway 2 generates a Certificate Signing Request (BranchCSR) for its own certificate BranchCRT to be signed by root CA (Please generate one not self-signed certificate in the Gateway 2, and click on the "View" button for that CSR. Just downloads it). Take the CSR to be signed by the root CA of the Gateway 1 and obtain the BranchCRT certificate (you need rename it). Import the certificate into the "Trusted Client Certificate List" of the Gateway 1 and the "Local Certificate List" of the Gateway 2.

Gateway 2 can establish an IPSec VPN tunnel with "Site to Site" scenario and IKE and X.509 protocols to Gateway 1.

Finally, the client hosts in two subnets of 10.0.75.0/24 and 10.0.76.0/24 can communicate with each other.

Outdoor WiFi LoRa BSU

Issue Certificate Setting

Go to **Object Definition > Certificate > Issue Certificate** tab.

The Issue Certificate setting allows user to import Certificate Signing Request (CSR) to be signed by root CA.

Import and Issue Certificate

Certificate Signing Request (CSR) Import from a File		
Item	**Value setting**	**Description**
Certificate Signing Request (CSR) Import from a File	A Must filled setting	Select a certificate signing request file you're your computer for importing to the gateway.
Certificate Signing Request (CSR) Import from a PEM	1. String format can be any text 2. A Must filled setting	Enter (copy-paste) the certificate signing request PEM encoded certificate to the gateway.
Sign	N/A	When root CA is exist, click the **Sign** button sign and issue the imported certificate by root CA.

Chapter 4 Field Communication (not supported)

Not supported feature for the purchased product, leave it as blank.

Chapter 5 Security

5.1 VPN

A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefitting from the functionality, security and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. The tunnel technology supports data confidentiality, data origin authentication and data integrity of network information by utilizing encapsulation protocols, encryption algorithms, and hashing algorithms.
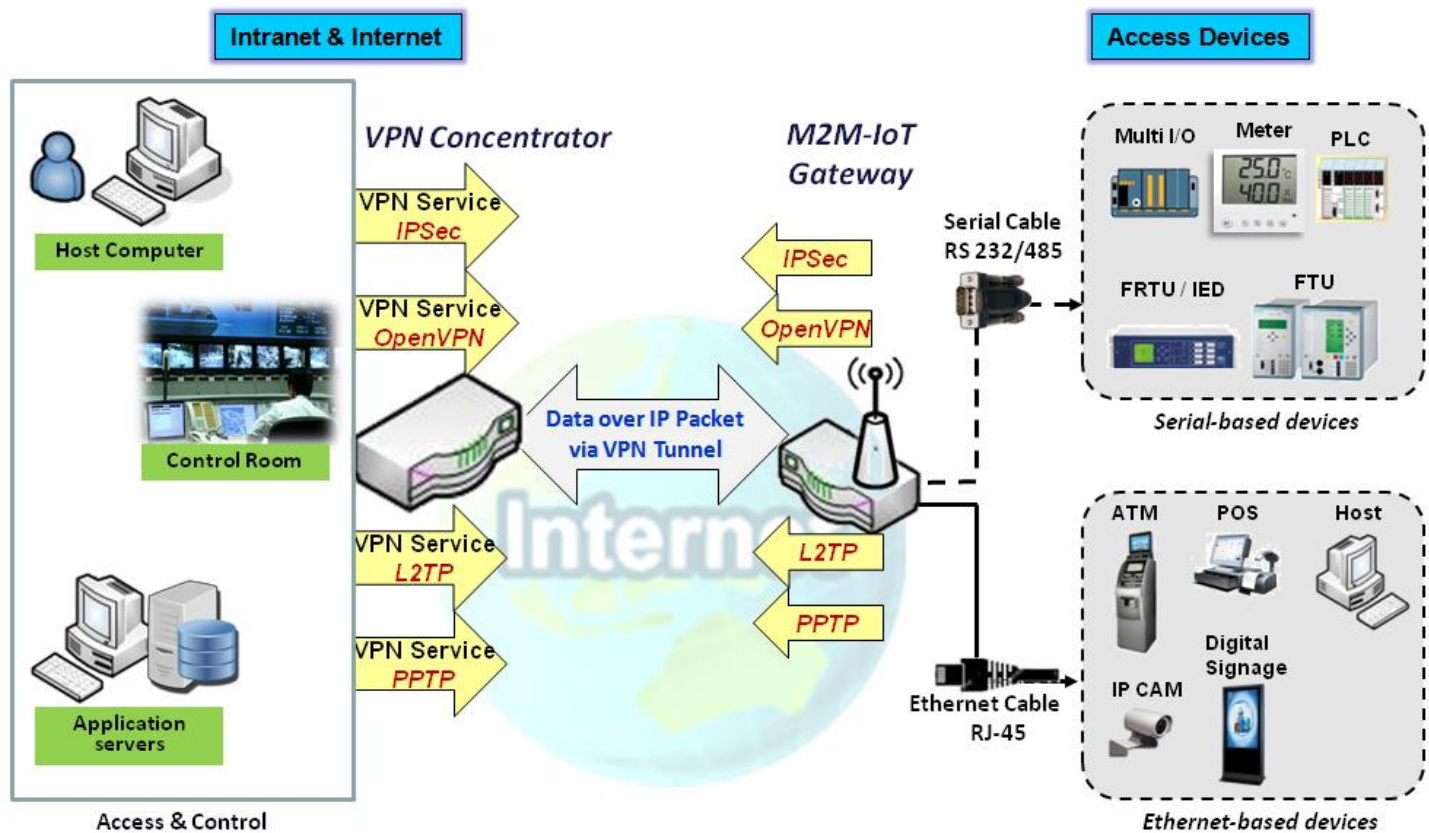
The product series supports different tunneling technologies to establish secure tunnels between multiple sites for data transferring, such as IPSec, OpenVPN, L2TP (over IPSec), PPTP and GRE. Besides, some advanced functions, like Full Tunnel, Tunnel Failover, Tunnel Load Balance, NetBIOS over IPSec, NAT Traversal and Dynamic VPN, are also supported.

Outdoor WiFi LoRa BSU

5.1.1 IPSec

Internet Protocol Security (IPSec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPSec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.

An IPSec VPN tunnel is established between IPSec client and server. Sometimes, we call the IPSec VPN client as the initiator and the IPSec VPN server as the responder. This gateway can be configured as different roles and establish number of tunnels with various remote devices. Before going to setup the VPN connections, you may need to decide the scenario type for the tunneling.

IPSec Tunnel Scenarios
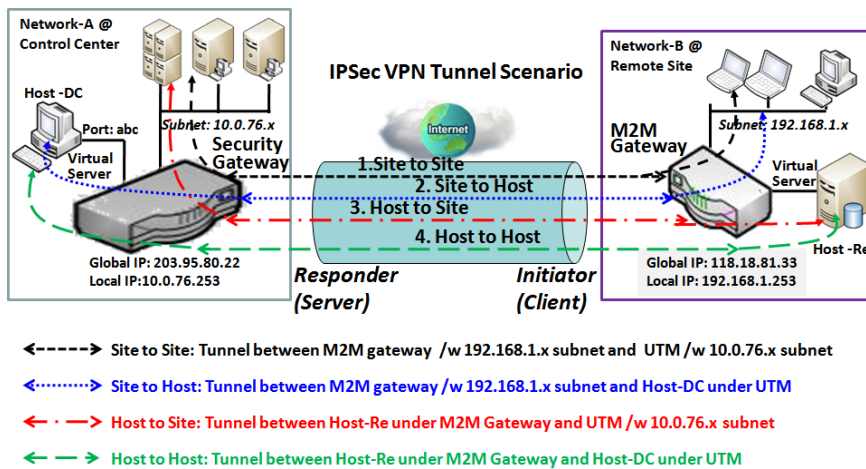
To build IPSec tunnel, you need to fill in remote gateway global IP, and optional subnet if the hosts behind IPSec peer can access to remote site or hosts. Under such configuration, there are four scenarios:

Site to Site: You need to setup remote gateway IP and subnet of both gateways. After the IPSec tunnel established, hosts behind both gateways can communication each other through the tunnel.

Site to Host: Site to Host is suitable for tunneling between clients in a subnet and an application server (host). As in the diagram, the clients behind the M2M gateway can access to the host "Host-DC" located in the control center through Site to Host VPN tunnel.

Host to Site: On the contrast, for a single host (or mobile user to) to access the resources located in an intranet, the Host to Site scenario can be applied.

Host to Host: Host to Host is a special configuration for building a VPN tunnel between two single hosts.

Outdoor WiFi LoRa BSU

IPSec Setting

Go to **Security > VPN > IPSec** tab.

The IPSec Setting allows user to create and configure IPSec tunnels.

Enable IPSec

Configuration	
Item	**Setting**
▶ IPSec	☐ Enable
▶ Max. Concurrent IPSec Tunnels	16

Configuration Window		
Item	**Value setting**	**Description**
IPsec	Unchecked by default	Click the **Enable** box to enable IPSec function.
Max. Concurrent IPSec Tunnels	Depends on Product specification.	The specified value will limit the maximum number of simultaneous IPSec tunnel connection. The default value can be different for the purchased model.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Create/Edit IPSec tunnel

Ensure that the IPSec enable box is checked to enable before further configuring the IPSec tunnel settings.

IPSec Tunnel List	Add	Delete	Refresh				
ID	Tunnel Name	Interface	Remote Gateway	Remote Subnet	Status	Enable	Actions

When **Add/Edit** button is applied, a series of configuration screens will appear. They are Tunnel Configuration, Local & Remote Configuration, Authentication, IKE Phase, IKE Proposal Definition, IPSec Phase, and IPSec Proposal Definition. You have to configure the tunnel details for both local and remote VPN devices.

Outdoor WiFi LoRa BSU

Tunnel Configuration Window		
Item	**Value setting**	**Description**
Tunnel	Unchecked by default	Check the **Enable** box to activate the IPSec tunnel
Tunnel Name	1. A Must fill setting 2. String format can be any text	Enter a tunnel name. Enter a name that is easy for you to identify. **Value Range:** 1 ~ 19 characters.
Interface	1. A Must fill setting 2. **WAN 1** is selected by default	Select the interface on which IPSec tunnel is to be established. It can be the available WAN and LAN interfaces.
Tunnel Scenario	1. A Must fill setting 2. **Site to site** is selected by default	Select an IPSec tunneling scenario from the dropdown box for your application. Select **Site-to-Site**, **Site-to-Host**, **Host-to-Site**, or **Host-to-Host**. If LAN interface is selected, only **Host-to-Host** scenario is available. With **Site-to-Site** or **Site-to-Host** or **Host-to-Site**, IPSec operates in tunnel mode. The difference among them is the number of subnets. With **Host-to-Host**, IPSec operates in transport mode.
Tunel TCP MSS	1. An optional setting 2. **Auto** is set by default	Select from the dropdown box to define the size of Tunel TCP MSS. Select **Auto**, and all devices will adjust this parameter automatically. Select **Manual, and** specify an expected vaule for Tunel TCP MSS. **Value Range:** 64 ~ 1500 bytes.
ICMP Keep Alive	1. An optional setting 2. **Unchecked** by default	Check the **Enable** box to activate the ICMP keep alive function for the tunnel. If the keep alive function is enabled, you have to define the numner of fail trials, check interval, and source/destination IP address for the ICMP packets. **Value Range:** 1~999 for fail trials and time interval.
Encapsulation Protocol	1. A Must fill setting 2. **ESP** is selected by default	Select the Encapsulation Protocol from the dropdown box for this IPSec tunnel. Available encapsulations are **ESP** and **AH**.
IKE Version	1. A Must fill setting 2. **v1** is selected by default	Specify the IKE version for this IPSec tunnel. Select **v1** or **v2**.

Outdoor WiFi LoRa BSU

Local & Remote Configuration				
Item		**Setting**		
	ID	Subnet IP Address	Subnet Mask	Actions
▸ Local Subnet List	1	192.168.66.0	255.255.255.0(/24) ▾	Delete
	Add			
	ID	Subnet IP Address	Subnet Mask	Actions
▸ Remote Subnet List	1		255.255.255.0(/24) ▾	Delete
	Add			
▸ Remote Gateway			(IP Address/FQDN)	

Local & Remote Configuration Window		
Item	**Value setting**	**Description**
Local Subnet List	A Must fill setting	Specify the Local Subnet IP address and Subnet Mask. Click the Add or Delete button to add or delete a Local Subnet. Note_1: When Dynamic VPN option in Tunnel Scenario is selected, there will be only one subnet available. Note_2: When Host-to-Site or Host-to-Host option in Tunnel Scenario is selected, Local Subnet will not be available. Note_3: When Hub and Spoke option in Hub and Spoke is selected, there will be only one subnet available.
Remote Subnet List	A Must fill setting	Specify the Remote Subnet IP address and Subnet Mask. Click the Add or Delete button to add or delete Remote Subnet setting.
Remote Gateway	1. A Must fill setting. 2. Format can be a ipv4 address or FQDN	Specify the Remote Gateway.

Authentication	
Item	**Setting**
▸ Key Management	IKE+Pre-shared Key ▾ (Min. 8 characters)
▸ Local ID	Type: User Name ▾ ID: (Optional)
▸ Remote ID	Type: User Name ▾ ID:

Authentication Configuration Window		
Item	**Value setting**	**Description**
Key Management	1. A Must fill setting 2. Pre-shared Key 8 to 32 characters.	Select Key Management from the dropdown box for this IPSec tunnel. **IKE+Pre-shared Key:** user needs to set a key (8 ~ 32 characters). **IKE+X.509:** user needs Certificate to authenticate. IKE+X.509 will be available only when Certificate has been configured properly. Refer to Certificate section of this manual and also **Object Definition > Certificate** in web-based utility.
Local ID	An optional setting	Specify the Local ID for this IPSec tunnel to authenticate. Select **User Name** for Local ID and enter the username. The username may include but can't be all numbers. Select **FQDN** for Local ID and enter the FQDN. Select **User@FQDN** for Local ID and enter the User@FQDN.

		Select **Key ID** for Local ID and enter the Key ID (English alphabet or number).
Remote ID	An optional setting	Specify the Remote ID for this IPSec tunnel to authenticate. Select **User Name** for Remote ID and enter the username. The username may include but can't be all numbers. Select **FQDN** for Local ID and enter the FQDN. Select **User@FQDN** for Remote ID and enter the User@FQDN. Select **Key ID** for Remote ID and enter the Key ID (English alphabet or number). Note: Remote ID will be not available when Dynamic VPN option in Tunnel Scenario is selected.

IKE Phase Window

Item	Value setting	Description
Negotiation Mode	Main Mode is set by default default	Specify the Negotiation Mode for this IPSec tunnel. Select **Main Mode** or **Aggressive Mode**.
X-Auth	None is selected by default	Specify the X-Auth role for this IPSec tunnel. Select Server, Client, or None. Selected None no X-Auth authentication is required. Selected Server this gateway will be an X-Auth server. Click on the X-Auth Account button to create remote X-Auth client account. Selected Client this gateway will be an X-Auth client. Enter User name and Password to be authenticated by the X-Auth server gateway. Note: X-Auth Client will not be available for Dynamic VPN option selected in Tunnel Scenario.
Dead Peer Detection (DPD)	1. Checked by default 2. Default Timeout 180s and Delay 30s	Click **Enable** box to enable **DPD** function. Specify the **Timeout** and **Delay** time in seconds. ***Value Range***: 0 ~ 999 seconds for **Timeout** and **Delay**.
Phase1 Key Life Time	1. A Must fill setting 2. Default 3600s 3. Max. 86400s	Specify the Phase1 Key Life Time. ***Value Range***: 30 ~ 86400.

IKE Proposal Definition Window

Outdoor WiFi LoRa BSU

Item	Value setting	Description
IKE Proposal Definition	A Must fill setting	Specify the Phase 1 Encryption method. It can be DES / 3DES / AES-128 / AES-192 / AES-256. Specify the Authentication method. It can be None / MD5 / SHA1 / SHA2-256. Specify the DH Group. It can be None / Group1 / Group2 / Group5 / Group14 / Group15 / Group16 / Group17 / Group18. Check **Enable** box to enable this setting

IPSec Phase	
Item	Setting
▸ Phase2 Key Life Time	28800 (seconds) (Max. 86400)

IPSec Phase Window

Item	Value setting	Description
Phase2 Key Life Time	1. A Must fill setting 2. 28800s is set by default 3. Max. 86400s	Specify the Phase2 Key Life Time in second. ***Value Range***: 30 ~ 86400.

IPSec Proposal Definition				
ID	Encryption	Authentication	PFS Group	Definition
1	AES-128 ▾	SHA1 ▾		☑ Enable
2	AES-128 ▾	MD5 ▾	Group 2 ▾	☑ Enable
3	DES ▾	SHA1 ▾		☑ Enable
4	3DES ▾	SHA1 ▾		☑ Enable

IPSec Proposal Definition Window

Item	Value setting	Description
IPSec Proposal Definition	A Must fill setting	Specify the Encryption method. It can be DES / 3DES / AES-128 / AES-192 / AES-256. Note: None is available when Encapsulation Protocol is set as **AH**. Specify the Authentication method. It can be None / MD5 / SHA1 / SHA2-256. Note: None and SHA2-256 are available only when Encapsulation Protocol is set as **ESP**; they are not available for **AH** Encapsulation. Specify the PFS Group. It can be None / Group1 / Group2 / Group5 / Group14 / Group15 / Group16 / Group17 / Group18. Click **Enable** to enable this setting
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Back	N/A	Click **Back** to return to the previous page.

Create/Edit Dynamic VPN Server List

Similar to create an IPSec VPN Tunnel for site/host to site/host scenario, when **Add** / **Edit** button is applied a series of configuration screen will appear. They are Tunnel Configuration, Local & Remote Configuration, Authentication, IKE Phase, IKE Proposal Definition, IPSec Phase, and IPSec Proposal Definition. You have to configure the tunnel details for the gateway as a Dynamic VPN server.

Note: For the purchased gateway, you can configure one Dynamic VPN server for each WAN interface.

Tunnel Configuration Window		
Item	**Value setting**	**Description**
Tunnel	Unchecked by default	Check the **Enable** box to activate the Dynamic IPSec VPN tunnel.
Tunnel Name	1. A Must fill setting 2. String format can be any text	Enter a tunnel name. Enter a name that is easy for you to identify. ***Value Range***: 1 ~ 19 characters.
Interface	1. A Must fill setting 2. **WAN 1** is selected by default	Select WAN interface on which IPSec tunnel is to be established.
Tunnel Scenario	1. A Must fill setting 2. **Tunnel Mode** is selected by default	Select the Dynamic IPSec tunneling scenario. It can be **Tunnel Mode** or **Transport Mode**.
Encapsulation Protocol	1. A Must fill setting 2. **ESP** is selected by default	Select the Encapsulation Protocol from the dropdown box for this IPSec tunnel. Available encapsulations are **ESP** and **AH**.
IKE Version	1. A Must fill setting 2. **v1** is selected by default	Specify the IKE version for this IPSec tunnel.

Outdoor WiFi LoRa BSU

Local & Remote Configuration Window		
Item	**Value setting**	**Description**
Local Subnet	A Must fill setting	Specify the Local Subnet IP address.
Local Netmask	A Must fill setting	Specify the Local Subnet Mask.

Authentication Configuration Window		
Item	**Value setting**	**Description**
Key Management	1. A Must fill setting 2. Pre-shared Key 8 to 32 characters.	Select Key Management from the dropdown box for this IPSec tunnel. **IKE+Pre-shared Key**: user needs to set a key (8 ~ 32 characters).
Local ID	An optional setting	Specify the Local ID for this IPSec tunnel to authenticate. Select **User Name** for Local ID and enter the username. The username may include but can't be all numbers. Select **FQDN** for Local ID and enter the FQDN. Select **User@FQDN** for Local ID and enter the User@FQDN. Select **Key ID** for Local ID and enter the Key ID (English alphabet or number).
Remote ID	An optional setting	Specify the Remote ID for this IPSec tunnel to authenticate. Select **User Name** for Remote ID and enter the username. The username may include but can't be all numbers. Select **FQDN** for Local ID and enter the FQDN. Select **User@FQDN** for Remote ID and enter the User@FQDN. Select **Key ID** for Remote ID and enter the Key ID (English alphabet or number). Note: Remote ID will be not available when Dynamic VPN option in Tunnel Scenario is selected.

For the rest IKE Phase, IKE Proposal Definition, IPSec Phase, and IPSec Proposal Definition settings, they are the same as that of creating an IPSec Tunnel described in previous section. Please refer to the related description.

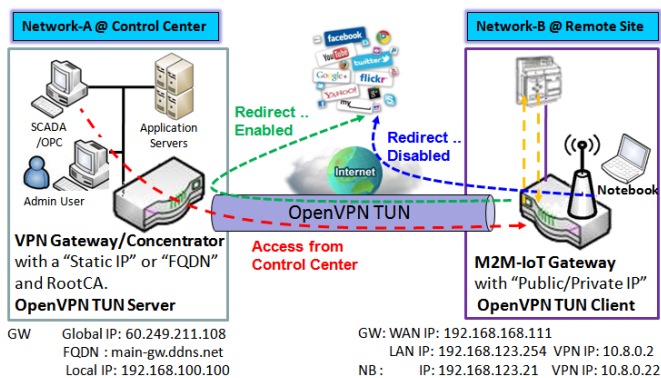# Outdoor WiFi LoRa BSU

5.1.2 OpenVPN

OpenVPN is an application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange. It is capable of traversing network address translators (NATs) and firewalls.

OpenVPN allows peers to authenticate each other using a Static Key (pre-shared key) or certificates. When used in a multi-client-server configuration, it allows the server to release an authentication certificate for every client, using signature and certificate authority. It uses the OpenSSL encryption library extensively, as well as the SSLv3/TLSv1 protocol, and contains many security and control features.

OpenVPN Tunneling is a Client and Server based tunneling technology. The OpenVPN Server must have a Static IP or a FQDN, and maintain a Client list. The OpenVPN Client may be a mobile user or mobile site with public IP or private IP, and requesting the OpenVPN tunnel connection. The product supports both OpenVPN Server and OpenVPN Client features to meet different application requirements.

There are two OpenVPN connection scenarios. They are the TAP and TUN scenarios. The product can create either a layer-3 based IP tunnel (TUN), or a layer-2 based Ethernet TAP that can carry any type of Ethernet traffic. In addition to configuring the device as a Server or Client, you have to specify which type of OpenVPN connection scenario is to be adopted.

OpenVPN TUN Scenario

Network-A @ Control Center
SCADA /OPC
Application Servers
Admin User
Redirect .. Enabled
Redirect .. Disabled
Internet
OpenVPN TUN
Access from Control Center
VPN Gateway/Concentrator with a "Static IP" or "FQDN" and RootCA.
OpenVPN TUN Server

Network-B @ Remote Site
Notebook
M2M-IoT Gateway with "Public/Private IP"
OpenVPN TUN Client

GW	Global IP: 60.249.211.108	GW: WAN IP: 192.168.168.111
	FQDN : main-gw.ddns.net	LAN IP: 192.168.123.254 VPN IP: 10.8.0.2
	Local IP: 192.168.100.100	NB : IP: 192.168.123.21 VPN IP: 10.8.0.22

1. M2M-IoT Gateway (as OpenVPN TUN Client) connects to peer VPN Gateway/Concentrator (as OpenVPN TUN Server).
2. M2M-IoT Gateway will be assigned 10.8.0.2 IP Address after OpenVPN TUN Connection establilshed. (10.8.0.x is a virtual subnet)
3. Local networked device will get a virtual IP 10.8.0.x if its traffic goes through the OpenVPN TUN connection (when NAT disabled & Redirect Internet Traffic enabled).
4. SCADA Server in Control Center can access remote attached device(s) with the assigned IP Address 10.8.0.2.

The term "TUN" mode is referred to routing mode and operates with layer 3 packets. In routing mode, the VPN client is given an IP address on a different subnet than the local LAN under the OpenVPN server. This virtual subnet is created for connecting to any remote VPN computers. In routing mode, the OpenVPN server creates a "TUN" interface with its own IP address pool which is different to the local LAN. Remote hosts that dial-in will get an IP address inside the virtual network and will have access only to the server where OpenVPN resides.
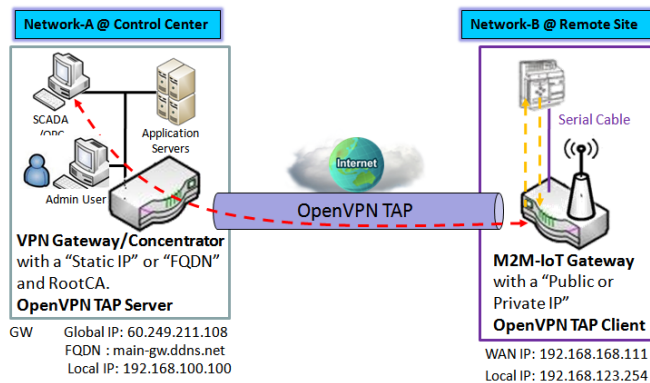
If you want to offer remote access to a VPN server from client(s), and inhibit the access to remote LAN resources under VPN server, OpenVPN TUN mode is the simplest solution.

As shown in the diagram, the M2M-IoT Gateway is configured as an OpenVPN TUN Client, and connects to an

Outdoor WiFi LoRa BSU

OpenVPN UN Server. Once the OpenVPN TUN connection is established, the connected TUN client will be assigned a virtual IP (10.8.0.2) which is belong to a virtual subnet that is different to the local subnet in Control Center. With such connection, the local networked devices will get a virtual IP 10.8.0.x if its traffic goes through the OpenVPN TUN connection when Redirect Internet Traffic settings is enabled; Besides, the SCADA Server in Control Center can access remote attached serial device(s) with the virtual IP address (10.8.0.2).

OpenVPN TAP Scenario

Network-A @ Control Center

SCADA /OPC
Application Servers
Admin User

VPN Gateway/Concentrator
with a "Static IP" or "FQDN" and RootCA.
OpenVPN TAP Server

GW   Global IP: 60.249.211.108
      FQDN : main-gw.ddns.net
      Local IP: 192.168.100.100

Internet

OpenVPN TAP

Network-B @ Remote Site

Serial Cable

M2M-IoT Gateway
with a "Public or Private IP"
OpenVPN TAP Client

WAN IP: 192.168.168.111
Local IP: 192.168.123.254

1. M2M-IoT Gateway (as OpenVPN TAP Client) connects to peer VPN Gateway/Concentrator (as OpenVPN TAP Server).
2. M2M-IoT Gateway will be assigned 192.168.100.210 IP Address after OpenVPN TAP Connection estabilshed. (same subnet as in Control Center)
3. SCADA Server in Control Center can access remote attached device(s) with the assigned IP Address 192.168.100.210.

The term "TAP" is referred to bridge mode and operates with layer 2 packets. In bridge mode, the VPN client is given an IP address on the same subnet as the LAN resided under the OpenVPN server. Under such configuration, the OpenVPN client can directly access to the resources in LAN. If you want to offer remote access to the entire remote LAN for VPN client(s), you have to setup OpenVPN in "TAP" bridge mode.

As shown in the diagram, the M2M-IoT Gateway is configured as an OpenVPN TAP Client, and connects to an OpenVPN TAP Server. Once the OpenVPN TAP connection is established, the connected TAP client will be assigned a virtual IP (192.168.100.210) which is the same subnet as that of local subnet in Control Center. With such connection, the SCADA Server in Control Center can access remote attached serial device(s) with the virtual IP address (192.168.100.210).

Outdoor WiFi LoRa BSU

Open VPN Setting

Go to **Security > VPN > OpenVPN** tab.

The OpenVPN setting allows user to create and configure OpenVPN tunnels.

Enable OpenVPN

Enable OpenVPN and select an expected configuration, either server or client, for the gateway to operate.

Configuration		
Item	**Value setting**	**Description**
OpenVPN	The box is unchecked by default	Check the **Enable** box to activate the OpenVPN function.
Server/ Client	Server Configuration is selected by default.	When **Server** is selected, as the name indicated, server configuration will be displayed below for further setup. When **Client** is selected, you can specify the client settings in another client configuration window.

Outdoor WiFi LoRa BSU

As an OpenVPN Server

If **Server** is selected, an OpenVPN Server Configuration screen will appear. **OpenVPN Server Configuration** window can let you enable the OpenVPN server function, specify the virtual IP address of OpenVPN server, when remote OpenVPN clients dial in, and the authentication protocol.

Item	Setting
▸ OpenVPN	☑ Enable
▸ Server / Client	Server ▾
▸ OpenVPN Configuration file	☐ Enable Export client.ovpn

Configuration		
Item	**Value setting**	**Description**
OpenVPN Configuration File	1. An Optional setting. 2. The box is unchecked by default.	Click the **Enable** box to activate the export feature of OpenVPN Client configuration to a .ovpn file. You have to further click the **Export** button to get the configuration file.

The OpenVPN Server supports up to 4 TUN / TAP tunnels at the same time.

OpenVPN Server Configuration		
Item	**Value setting**	**Description**
OpenVPN Server	The box is unchecked by default.	Click the **Enable** to activate OpenVPN Server functions.
Protocol	1. A Must filled setting 2. By default **TCP** is selected.	Define the selected **Protocol** for connecting to the OpenVPN Server. • Select **TCP , or UDP** -> The TCP protocol will be used to access the OpenVPN Server, and **Port** will be set as 4430 automatically. • Select **UDP** -> The UDP protocol will be used to access the OpenVPN Server, and **Port** will be set as 1194 automatically.
Port	1. A Must filled setting 2. By default **4430** is set.	Specify the **Port** for connecting to the OpenVPN Server. ***Value Range**: 1 ~ 65535.*
Tunnel Scenario	1. A Must filled setting 2. By default **TUN** is selected.	Specify the type of **Tunnel Scenario** for connecting to the OpenVPN Server. It can be **TUN** for TUN tunnel scenario, or **TAP** for TAP tunnel scenario.
Authorization Mode	1. A Must filled setting 2. By default **TLS** is selected.	Specify the authorization mode for the OpenVPN Server. • **TLS** ->The OpenVPN will use TLS authorization mode, and the following items **CA Cert.**, **Server Cert.** and **DH PEM** will be displayed.

		CA Cert. could be generated in Certificate. Refer to **Object Definition** > **Certificate** > **Trusted Certificate**. **Server Cert.** could be generated in Certificate. Refer to **Object Definition** > **Certificate** > **My Certificate**. • **Static Key** ->The OpenVPN will use static key (pre-shared) authorization mode, and the following items **Local Endpoint IP Address**, **Remote Endpoint IP Address** and **Static Key** will be displayed. Note: Static Key will be available only when TUN is chosen in Tunnel Scenario.
Local Endpoint IP Address	A Must filled setting	Specify the virtual **Local Endpoint IP Address** of this OpenVPN gateway. ***Value Range***: The IP format is 10.8.0.x, the range of x is 1~254. Note: Local Endpoint IP Address will be available only when Static Key is chosen in Authorization Mode.
Remote Endpoint IP Address	A Must filled setting	Specify the virtual **Remote Endpoint IP Address** of the peer OpenVPN gateway. ***Value Range***: The IP format is 10.8.0.x, the range of x is 1~254. Note: Remote Endpoint IP Address will be available only when Static Key is chosen in Authorization Mode.
Static Key	A Must filled setting	Specify the **Static Key**. Note: Static Key will be available only when Static Key is chosen in Authorization Mode.
Server Virtual IP	A Must filled setting	Specify the **Server Virtual IP**. ***Value Range***: The IP format is 10.y.0.0, the range of y is 1~254. Note: Server Virtual IP will be available only when TLS is chosen in Authorization Mode.
DHCP-Proxy Mode	1. A Must filled setting 2. The box is checked by default.	Check the **Enable** box to activate the **DHCP-Proxy Mode**. Note: DHCP-Proxy Mode will be available only when TAP is chosen in Tunnel Device.
IP Pool	A Must filled setting	Specify the virtual **IP pool** setting for the OpenVPN server. You have to specify the **Starting Address** and **Ending Address** as the IP address pool for the OpenVPN clients. Note: IP Pool will be available only when TAP is chosen in Tunnel Device, and DHCP-Proxy Mode is unchecked (disabled).
Gateway	A Must filled setting	Specify the **Gateway** setting for the OpenVPN server. It will be assigned to the connected OpenVPN clients. Note: Gateway will be available only when TAP is chosen in Tunnel Device, and DHCP-Proxy Mode is unchecked (disabled).
Netmask	By default **- select one -** is selected.	Specify the **Netmask** setting for the OpenVPN server. It will be assigned to the connected OpenVPN clients. ***Value Range***: 255.255.255.0/24 (only support class C) Note_1: Netmask will be available when TAP is chosen in Tunnel Device, and DHCP-Proxy Mode is unchecked (disabled). Note_2: Netmask will also be available when TUN is chosen in Tunnel Device.
Redirect Default Gateway	1. An Optional setting. 2. The box is unchecked by default.	Check the **Enable** box to activate the **Redirect Default Gateway** function.
Encryption Cipher	1. A Must filled setting. 2. By default **Blowfish** is selected.	Specify the **Encryption Cipher** from the dropdown list. It can be **Blowfish/AES-256/AES-192/AES-128/None.**
Hash Algorithm	By default **SHA-1** is selected.	Specify the **Hash Algorithm** from the dropdown list. It can be **SHA-1/MD5/MD4/SHA2-256/SHA2-512/None/Disable.**

Outdoor WiFi LoRa BSU

LZO Compression	By default **Adaptive** is selected.	Specify the **LZO Compression** scheme. It can be **Adaptive/YES/NO/Default.**
Multicast	1. An Optional setting. 2. The box is checked by default.	Check the **Enable** box to activate the **Multicast** function. Note: Multicast function is only available for TAP tunnel scenario.
Persis Key	1. An Optional setting. 2. The box is checked by default.	Check the **Enable** box to activate the **Persis Key** function.
Persis Tun	1. An Optional setting. 2. The box is checked by default.	Check the **Enable** box to activate the **Persis Tun** function.
Advanced Configuration	N/A	Click the **Edit** button to specify the **Advanced Configuration** setting for the OpenVPN server. If the button is clicked, **Advanced Configuration** will be displayed below.
Save	N/A	Click **Save** to save the settings.
Undo	N/A	Click **X** to cancel the changes and return to last page.

Outdoor WiFi LoRa BSU

When **Advanced Configuration** is selected, an OpenVPN Server Advanced Configuration screen will appear.

Item	Setting
▶ TLS Cipher	None ▼
▶ TLS Auth. Key	(Optional)
▶ Client to Client	☑ Enable
▶ Duplicate CN	☑ Enable
▶ Tunnel MTU	1500
▶ Tunnel UDP Fragment	0
▶ Tunnel UDP MSS-Fix	☐ Enable
▶ CCD-Dir Default File	
▶ Client Connection Script	
▶ Additional Configuration	

OpenVPN Server Advanced Configuration

OpenVPN Server Advanced Configuration		
Item	**Value setting**	**Description**
TLS Cipher	1. A Must filled setting. 2. **TLS-RSA-WITH-AES128-SHA** is selected by default	Specify the **TLS Cipher** from the dropdown list. It can be **None / TLS-RSA-WITH-RC4-MD5 / TLS-RSA-WITH-AES128-SHA / TLS-RSA-WITH-AES256-SHA / TLS-DHE-DSS-AES128-SHA / TLS-DHE-DSS-AES256-SHA.** Note: TLS Cipher will be available only when TLS is chosen in Authorization Mode.
TLS Auth. Key	1. An Optional setting. 2. String format: any text	Specify the **TLS Auth. Key.** Note: TLS Auth. Key will be available only when TLS is chosen in Authorization Mode.
Client to Client	The box is checked by default	Check the **Enable** box to enable the traffics among different OpenVPN Clients. Note: Client to Client will be available only when TLS is chosen in Authorization Mode
Duplicate CN	The box is checked by default	Check the **Enable** box to activate the **Duplicate CN** function. Note: Duplicate CN will be available only when TLS is chosen in Authorization Mode
Tunnel MTU	1. A Must filled setting 2. The value is **1500** by default	Specify the **Tunnel MTU.** *Value Range: 0 ~ 1500.*
Tunnel UDP	1. A Must filled setting	Specify the **Tunnel UDP Fragment.** By default, it is equal to **Tunnel MTU**.
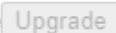
Fragment	2. The value is **1500** by default	***Value Range***: 0 ~ 1500. Note: Tunnel UDP Fragment will be available only when UDP is chosen in Protocol.
Tunnel UDP MSS-Fix	1. An Optional setting. 2. The box is unchecked by default.	Check the **Enable** box to activate the **Tunnel UDP MSS-Fix** Function. Note: Tunnel UDP MSS-Fix will be available only when UDP is chosen in Protocol.
CCD-Dir Default File	1. An Optional setting. 2. String format: any text	Specify the **CCD-Dir Default File.** ***Value Range***: 0 ~ 256 characters.
Client Connection Script	1. An Optional setting. 2. String format: any text	Specify the **Client Connection Script.** ***Value Range***: 0 ~ 256 characters.
Additional Configuration	1. An Optional setting. 2. String format: any text	Specify the **Additional Configuration.** ***Value Range***: 0 ~ 256 characters.

Outdoor WiFi LoRa BSU

As an OpenVPN Client

If **Client** is selected, the configuration screen will be changed as below and an OpenVPN Client List screen appear.

OpenVPN Configuration		
Item	**Value setting**	**Description**
OpenVPN	The box is unchecked by default	Check the **Enable** box to activate the OpenVPN function.
Server/ Client	Server Configuration is selected by default.	When **Server** is selected, as the name indicated, server configuration will be displayed below for further setup. When **Client** is selected, you can specify the client settings in another client configuration window.
OpenVPN Configuration file	1. An Optional setting. 2. The box is unchecked by default.	Click the **Enable** box to activate the OpenVPN Client configuration via a pre-defined configuration file. You have to further specify the **Interface** to be applied, and click the **Upgrade** button to upload the configuration from a .ovpn file. If you enabled this function, you can't add any OpenVPN clients manually.

When **Add** button is applied, OpenVPN Client Configuration screen will appear. **OpenVPN Client Configuration** window let you specify the required parameters for an OpenVPN VPN client, such as "OpenVPN Client Name", "Interface", "Protocol", "Tunnel Scenario", "Remote IP/FQDN", "Remote Subnet", "Authorization Mode", "Encryption Cipher", "Hash Algorithm" and tunnel activation.

Outdoor WiFi LoRa BSU

OpenVPN Client Configuration		
Item	**Value setting**	**Description**
OpenVPN Client Name	A Must filled setting	The **OpenVPN Client Name** will be used to identify the client in the tunnel list. *Value Range*: 1 ~ 32 characters.
Interface	1. A Must filled setting 2. By default **WAN-1** is selected.	Define the physical interface to be used for this OpenVPN Client tunnel.
Protocol	1. A Must filled setting 2. By default **TCP** is selected.	Define the **Protocol** for the OpenVPN Client. • Select **TCP** ->The OpenVPN will use TCP protocol, and **Port** will be set as 443 automatically. • Select **UDP** -> The OpenVPN will use UDP protocol, and **Port** will be set as 1194 automatically.
Port	1. A Must filled setting 2. By default **443** is set.	Specify the **Port** for the OpenVPN Client to use. *Value Range*: 1 ~ 65535.
Tunnel Scenario	1. A Must filled setting 2. By default **TUN** is selected.	Specify the type of **Tunnel Scenario** for the OpenVPN Client to use. It can be **TUN** for TUN tunnel scenario, or **TAP** for TAP tunnel scenario.
Remote IP/FQDN	A Must filled setting	Specify the **Remote IP/FQDN** of the peer OpenVPN Server for this OpenVPN Client tunnel. Fill in the IP address or FQDN.
Remote Subnet	1. An Optional setting. 2. The box is unchecked by default.	Check the **Enable** box to activate remote subnet function, and specify **Remote Subnet** of the peer OpenVPN Server for this OpenVPN Client tunnel. Fill in the remote subnet address and remote subnet mask.
Redirect Internet Traffic	1. An Optional setting. 2. The box is unchecked by default.	Check the **Enable** box to activate the **Redirect Internet Traffic** function.

NAT	1. An Optional setting. 2. The box is checked by default.	Check the **Enable** box to activate the **NAT** function.
Authorization Mode	1. A Must filled setting 2. By default **TLS** is selected.	Specify the authorization mode for the OpenVPN Server. • **TLS** ->The OpenVPN will use TLS authorization mode, and the following items **CA Cert.**, **Client Cert.** and **Client Key** will be displayed. **CA Cert.** could be selected in Trusted CA Certificate List. Refer to **Object Definition** > **Certificate** > **Trusted Certificate**. **Client Cert.** could be selected in Local Certificate List. Refer to **Object Definition** > **Certificate** > **My Certificate**. **Client Key** could be selected in Trusted Client key List. Refer to **Object Definition** > **Certificate** > **Trusted Certificate**. • **Static Key** ->The OpenVPN will use static key authorization mode, and the following items **Local Endpoint IP Address**, **Remote Endpoint IP Address** and **Static Key** will be displayed.
Local Endpoint IP Address	A Must filled setting	Specify the virtual **Local Endpoint IP Address** of this OpenVPN gateway. ***Value Range:*** The IP format is 10.8.0.x, the range of x is 1~254. Note: Local Endpoint IP Address will be available only when Static Key is chosen in Authorization Mode.
Remote Endpoint IP Address	A Must filled setting	Specify the virtual **Remote Endpoint IP Address** of the peer OpenVPN gateway. ***Value Range:*** The IP format is 10.8.0.x, the range of x is 1~254. Note: Remote Endpoint IP Address will be available only when Static Key is chosen in Authorization Mode.
Static Key	A Must filled setting	Specify the **Static Key**. Note: Static Key will be available only when Static Key is chosen in Authorization Mode.
Encryption Cipher	By default **Blowfish** is selected.	Specify the **Encryption Cipher.** It can be **Blowfish/AES-256/AES-192/AES-128/None.**
Hash Algorithm	By default **SHA-1** is selected.	Specify the **Hash Algorithm.** It can be **SHA-1/MD5/MD4/SHA2-256/SHA2-512/None/Disable.**
LZO Compression	By default **Adaptive** is selected.	Specify the **LZO Compression** scheme. It can be **Adaptive/YES/NO/Default.**
Multicast	1. An Optional setting. 2. The box is checked by default.	Check the **Enable** box to activate the **Multicast** function. Note: Multicast function is only available for TAP tunnel scenario.
Persis Key	1. An Optional setting. 2. The box is checked by default.	Check the **Enable** box to activate the **Persis Key** function.
Persis Tun	1. An Optional setting. 2. The box is checked by default.	Check the **Enable** box to activate the **Persis Tun** function.
Advanced Configuration	N/A	Click the **Edit** button to specify the **Advanced Configuration** setting for the OpenVPN server. If the button is clicked, **Advanced Configuration** will be displayed below.
Tunnel	The box is unchecked by default	Check the **Enable** box to activate this OpenVPN tunnel.
Save	N/A	Click **Save** to save the settings.
Undo	N/A	Click **X** to cancel the changes and return to last page.

Outdoor WiFi LoRa BSU

When **Advanced Configuration** is selected, an OpenVPN Client Advanced Configuration screen will appear.


OpenVPN Advanced Client Configuration		
Item	**Value setting**	**Description**
TLS Cipher	1. A Must filled setting. 2. **TLS-RSA-WITH-AES128-SHA** is selected by default	Specify the **TLS Cipher** from the dropdown list. It can be **None / TLS-RSA-WITH-RC4-MD5 / TLS-RSA-WITH-AES128-SHA / TLS-RSA-WITH-AES256-SHA / TLS-DHE-DSS-AES128-SHA / TLS-DHE-DSS-AES256-SHA.** Note: TLS Cipher will be available only when TLS is chosen in Authorization Mode.
TLS Auth. Key	1. An Optional setting. 2. String format: any text	Specify the **TLS Auth. Key** for connecting to an OpenVPN server, if the server required it. Note: TLS Auth. Key will be available only when TLS is chosen in Authorization Mode.
User Name	An Optional setting.	Enter the **User account** for connecting to an OpenVPN server, if the server required it. Note: User Name will be available only when TLS is chosen in Authorization Mode.
Password	An Optional setting.	Enter the **Password** for connecting to an OpenVPN server, if the server required it. Note: User Name will be available only when TLS is chosen in Authorization Mode.
Bridge TAP to	By default **VLAN 1** is selected	Specify the setting of "**Bridge TAP to**" to bridge the TAP interface to a certain local network interface or VLAN. Note: Bridge TAP to will be available only when TAP is chosen in Tunnel Scenario and NAT is unchecked.

Firewall Protection	The box is unchecked by default.	Check the box to activate the **Firewall Protection** function. Note: Firewall Protection will be available only when NAT is enabled.
Client IP Address	By default **Dynamic IP** is selected	Specify the virtual IP Address for the OpenVPN Client. It can be **Dynamic IP/Static IP.**
Tunnel MTU	1.A Must filled setting 2.The value is 1500 by default	Specify the value of **Tunnel MTU.** ***Value Range***: 0 ~ 1500.
Tunnel UDP Fragment	The value is 1500 by default	Specify the value of **Tunnel UDP Fragment.** ***Value Range***: 0 ~ 1500. Note: Tunnel UDP Fragment will be available only when UDP is chosen in Protocol.
Tunnel UDP MSS-Fix	The box is unchecked by default.	Check the **Enable** box to activate the **Tunnel UDP MSS-Fix** function. Note: Tunnel UDP MSS-Fix will be available only when UDP is chosen in Protocol.
nsCerType Verification	The box is unchecked by default.	Check the **Enable** box to activate the **nsCerType Verification** function. Note: nsCerType Verification will be available only when TLS is chosen in Authorization Mode.
TLS Renegotiation Time (seconds)	The value is 3600 by default	Specify the time interval of **TLS Renegotiation Time.** ***Value Range***: -1 ~ 86400.
Connection Retry(seconds)	The value is -1 by default	Specify the time interval of **Connection Retry.** The default -1 means that it is no need to execute connection retry. ***Value Range***: -1 ~ 86400, and -1 means no retry is required.
DNS	By default **Automatically** is selected	Specify the setting of **DNS.** It can be **Automatically/Manually.**
Additional Configuration	An Optional setting.	Enter optional configuration string here. Up to 256 characters is allowable. ***Value Range***: 0 ~ 256 characters.
Save	N/A	Click **Save** to save the settings.
Undo	N/A	Click **X** to cancel the changes and return to last page.

5.2 Firewall
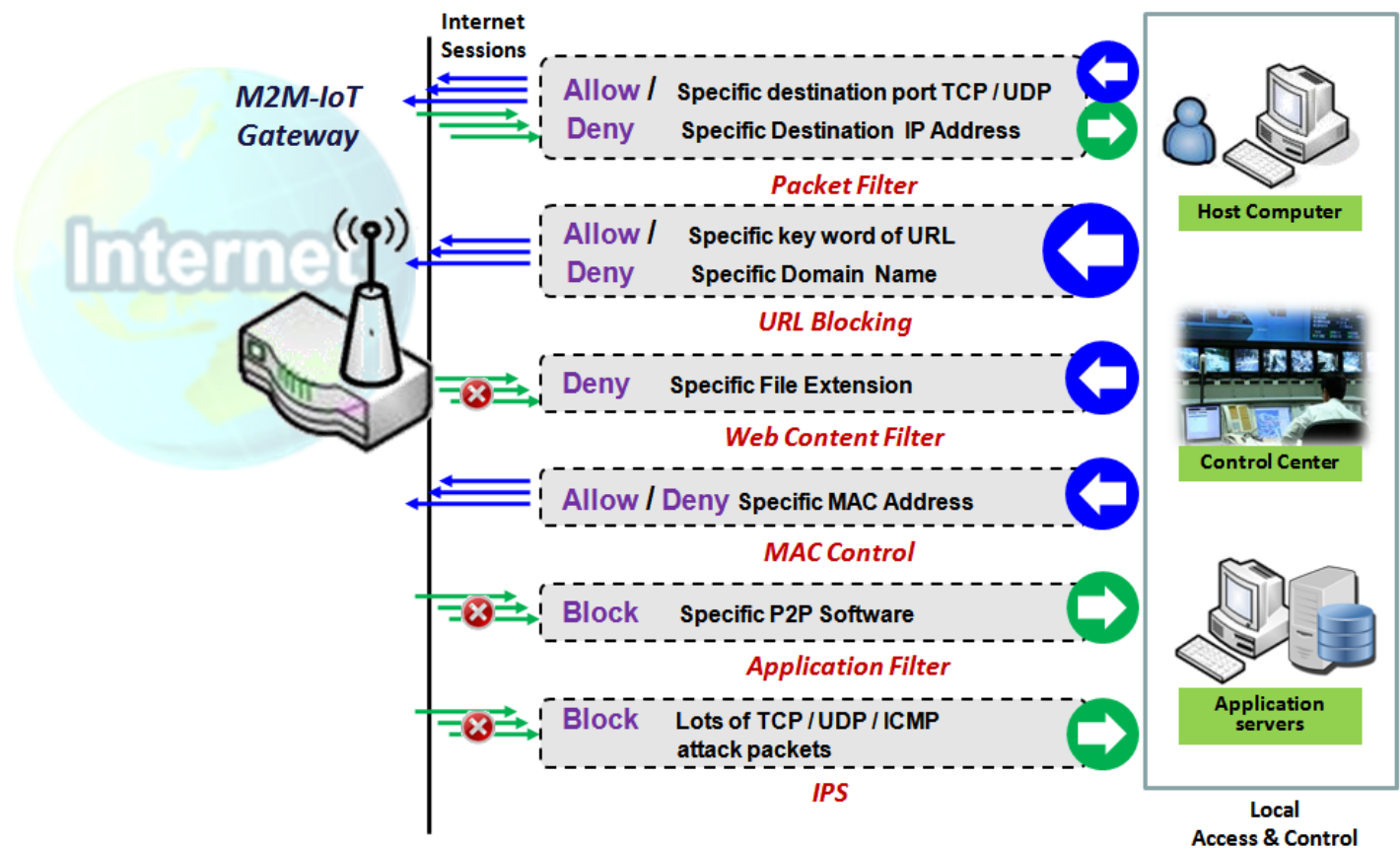
The firewall functions include Packet Filter, URL Blocking, Content Filter, MAC Control, Application Filter, IPS and some firewall options. The supported function can be different for the purchased gateway.

5.2.1 Packet Filter (not supported)

Not supported feature for the purchased product, leave it as blank.

5.2.2 URL Blocking (not supported)

Not supported feature for the purchased product, leave it as blank.
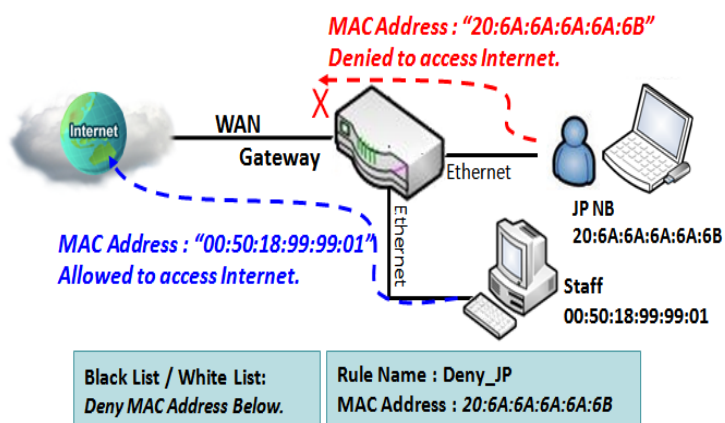
5.2.3 MAC Control

"MAC Control" function allows you to assign the accessibility to the gateway for different users based on device's MAC address. When the administrator wants to reject the traffics from some client hosts with specific MAC addresses, he can use the "MAC Control" function to reject with the black list configuration.

MAC Control with Black List Scenario

As shown in the diagram, enable the MAC control function and specify the "MAC Control Rule List" is a black list, and configure one MAC control rule for the gateway to deny the connection request from the "JP NB" with its own MAC address 20:6A:6A:6A:6A:6B.

System will block the connecting from the "JP NB" to the gateway but allow others.

Outdoor WiFi LoRa BSU

MAC Control Setting

Go to **Security > Firewall > MAC Control** Tab.

The MAC control setting allows user to create and customize MAC address policies to allow or reject packets with specific source MAC address.

Enable MAC Control

Configuration Window		
Item	**Value setting**	**Description**
MAC Control	The box is unchecked by default	Check the **Enable** box to activate the MAC filter function
Black List / White List	Deny MAC Address Below is set by default	When **Deny MAC Address Below** is selected, as the name suggest, packets specified in the rules will be blocked –black listed. In contrast, with **Allow MAC Address Below**, you can specifically white list the packets to pass and the rest will be blocked.
Log Alert	The box is unchecked by default	Check the **Enable** box to activate to activate Event Log.
Known MAC from LAN PC List	N/A	Select a MAC Address from LAN Client List. Click the **Copy to** to copy the selected **MAC Address** to the filter rule.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Outdoor WiFi LoRa BSU

Create/Edit MAC Control Rules

The gateway supports up to a maximum of 20 filter rule sets. Ensure that the MAC Control is enabled before we can create control rules.

When **Add** button is applied, **Filter Rule Configuration** screen will appear.

MAC Control Rule Configuration Item	Value setting	Description
Rule Name	1. String format can be any text 2. A Must fill setting	Enter a MAC Control rule name. Enter a name that is easy for you to remember.
MAC Address (Use: to Compose)	1. MAC Address string Format 2. A Must fill setting	Specify the **Source MAC Address** to filter rule.
Time Schedule	A Must fill setting	Apply **Time Schedule** to this rule; otherwise leave it as **(0) Always**. If the dropdown list is empty, ensure **Time Schedule** is pre-configured. Refer to **Object Definition > Scheduling > Configuration tab**
Enable	The box is unchecked by default.	Click **Enable** box to activate this rule, and then save the settings.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

5.2.4 Content Filter (not supported)

Not supported feature for the purchased product, leave it as blank.

5.2.5 Application Filter (not supported)

Not supported feature for the purchased product, leave it as blank.

5.2.6 IPS

To provide application servers in the Internet, administrator may need to open specific ports for the services. However, there are some risks to always open service ports in the Internet. In order to avoid such attack risks, it is important to enable IPS functions.

Intrusion Prevention System (IPS) is network security appliances that monitor network and/or system activities for malicious activity. The main functions of IPS are to identify malicious activity, log information about this activity, attempt to block/stop it and report it. You can enable the IPS function and check the listed intrusion activities when needed. You can also enable the log alerting so that system will record Intrusion events when corresponding intrusions are detected.

IPS Scenario
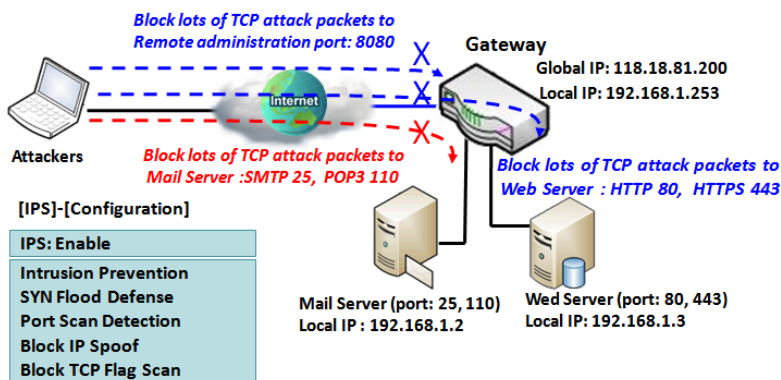
As shown in the diagram, the gateway serves as an E-mail server, Web Server and also provides TCP port 8080 for remote administration. So, remote users or unknown users can request those services from Internet. With IPS enabled, the gateway can detect incoming attack packets, including the TCP ports (25, 80, 110, 443 and 8080) with services. It will block the attack packets and let the normal access to pass through the gateway

Outdoor WiFi LoRa BSU

IPS Setting

Go to **Security > Firewall > IPS** Tab.

The Intrusion Prevention System (IPS) setting allows user to customize intrusion prevention rules to prevent malicious packets.

Enable IPS Firewall

Configuration Window		
Item	**Value setting**	**Description**
IPS	The box is unchecked by default	Check the **Enable** box to activate IPS function
Log Alert	The box is unchecked by default	Check the **Enable** box to activate to activate Event Log.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Setup Intrusion Prevention Rules

The router allows you to select intrusion prevention rules you may want to enable. Ensure that the IPS is enabled before we can enable the defense function.

Outdoor WiFi LoRa BSU

Setup Intrusion Prevention Rules		
Item Name	**Value setting**	**Description**
SYN Flood Defense	1. A Must filled setting	Click **Enable** box to activate this intrusion prevention rule and enter the traffic threshold in this field.
UDP Flood Defense	2. The box is unchecked by default. 3. Traffic threshold is set to 300 by default	Click **Enable** box to activate this intrusion prevention rule and enter the traffic threshold in this field.
ICMP Flood Defense	4. The value range can be from 10 to 10000.	Click **Enable** box to activate this intrusion prevention rule and enter the traffic threshold in this field. *Value Range*: 10 ~ 10000.
Port Scan Defection	1. A Must filled setting 2. The box is unchecked by default. 3. Traffic threshold is set to 200 by default 4. The value range can be from 10 to 10000.	Click **Enable** box to activate this intrusion prevention rule and enter the traffic threshold in this field. *Value Range*: 10 ~ 10000.
Block Land Attack **Block Ping of Death** **Block IP Spoof** **Block TCP Flag Scan** **Block Smurf** **Block Traceroute** **Block Fraggle**	The box is unchecked by default.	Click **Enable** box to activate this intrusion prevention rule.

Outdoor WiFi LoRa BSU

Attack		
ARP Spoofing Defence	1. A Must filled setting 2. The box is unchecked by default. 3. Traffic threshold is set to 300 by default 4. The value range can be from 10 to 10000.	Click **Enable** box to activate this intrusion prevention rule and enter the traffic threshold in this field. ***Value Range***: 10 ~ 10000.
Save	NA	Click **Save** to save the settings
Undo	NA	Click **Undo** to cancel the settings

5.2.7 Options

Firewall Options		
Item	**Setting**	
▶ Stealth Mode	☐ Enable	
▶ SPI	☑ Enable	
▶ Discard Ping from WAN	☐ Enable	

Remote Administrator Host Definition							
ID	Interface	Protocol	IP	Subnet Mask	Service Port	Enable	Action
1	All WAN	HTTPS	Any IP	N/A	443	☐	Edit
2	All WAN	HTTPS	Any IP	N/A	443	☐	Edit
3	All WAN	HTTPS	Any IP	N/A	443	☐	Edit
4	All WAN	HTTPS	Any IP	N/A	443	☐	Edit
5	All WAN	HTTPS	Any IP	N/A	443	☐	Edit

There are some additional useful firewall options in this page.

"Stealth Mode" lets gateway not to respond to port scans from the WAN so that makes it less susceptible to discovery and attacks on the Internet. "SPI" enables gateway to record the packet information like IP address, port address, ACK, SEQ number and so on while they pass through the gateway, and the gateway checks every incoming packet to detect if this packet is valid.

"Discard Ping from WAN" makes any host on the WAN side can`t ping this gateway. And finally, "Remote Administrator Hosts" enables you to perform administration task from a remote host. If this feature is enabled, only specified IP address(es) can perform remote administration.

Outdoor WiFi LoRa BSU

Enable SPI Scenario
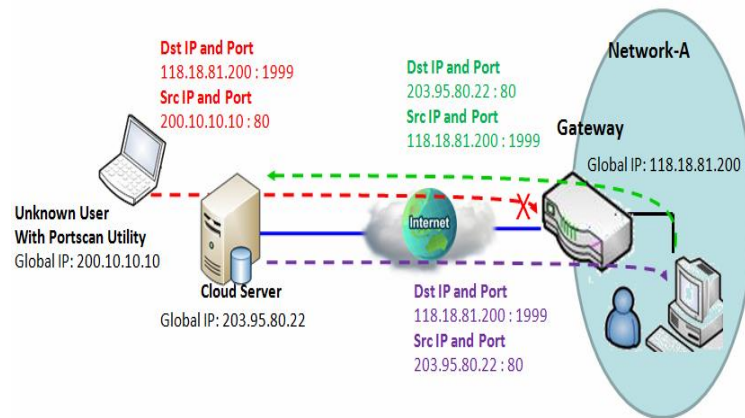
As shown in the diagram, Gateway has the IP address of 118.18.81.200 for WAN interface and 192.168.1.253 for LAN interface. It serves as a NAT gateway. Users in Network-A initiate to access cloud server through the gateway. Sometimes, unknown users will simulate the packets but use different source IP to masquerade. With the SPI feature been enabled at the gateway, it will block such packets from unknown users.

Discard Ping from WAN & Remote Administrator Hosts Scenario
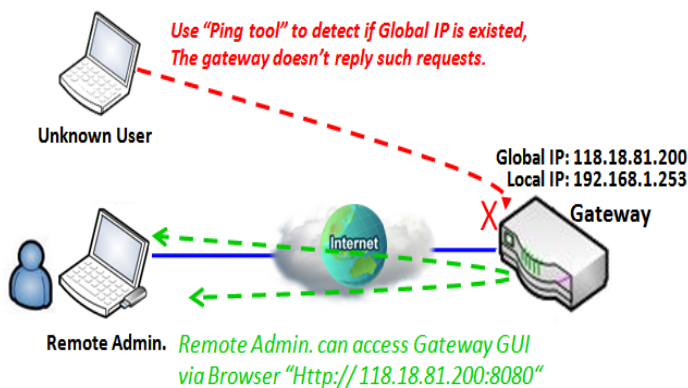
"Discard Ping from WAN" makes any host on the WAN side can`t ping this gateway reply any ICMP packets. Enable the Discard Ping from WAN function to prevent security leak when local users surf the internet.

Remote administrator knows the gateway's global IP, and he can access the Gateway GUI via TCP port 8080.

Outdoor WiFi LoRa BSU

Firewall Options Setting

Go to **Security > Firewall > Options** Tab.

The firewall options setting allows network administrator to modify the behavior of the firewall and to enable Remote Router Access Control.

Enable Firewall Options

Firewall Options		
Item		Setting
▶ Stealth Mode		☐ Enable
▶ SPI		☑ Enable
▶ Discard Ping from WAN		☐ Enable

Firewall Options		
Item	**Value setting**	**Description**
Stealth Mode	The box is unchecked by default	Check the **Enable** box to activate the Stealth Mode function
SPI	The box is checked by default	Check the **Enable** box to activate the SPI function
Discard Ping from WAN	The box is unchecked by default	Check the **Enable** box to activate the Discard Ping from WAN function

Define Remote Administrator Host

The router allows network administrator to manage router remotely. The network administrator can assign specific IP address and service port to allow accessing the router via designated WAN interface.

Outdoor WiFi LoRa BSU

ID	Interface	Protocol	IP	Subnet Mask	Service Port	Enable	Action
1	All WAN	HTTPS	Any IP	N/A	443	☐	Edit
2	All WAN	HTTPS	Any IP	N/A	443	☐	Edit
3	All WAN	HTTPS	Any IP	N/A	443	☐	Edit
4	All WAN	HTTPS	Any IP	N/A	443	☐	Edit
5	All WAN	HTTPS	Any IP	N/A	443	☐	Edit

Remote Administrator Host Definition		
Item	**Value setting**	**Description**
Protocol	**HTTPS** is set by default	Select **HTTP** or **HTTPS** method for remote administration.
IP	A Must filled setting	This field is to specify the remote host to assign access right for remote access. Select **Any IP** to allow any remote hosts Select **Specific IP** to allow the remote host coming from a specific subnet. An IP address entered in this field and a selected **Subnet Mask** to compose the subnet**.**
Service Port	1. 80 for HTTP by default 2. 443 for HTTPS by default	This field is to specify a Service Port to HTTP or HTTPS connection. *Value Range*: 1 ~ 65535.
Enabling the rule	The box is unchecked by default.	Click **Enable** box to activate this rule.
Save	N/A	Click **Enable** box to activate this rule then save the settings.
Undo	N/A	Click **Undo** to cancel the settings

Chapter 6 Administration

6.1 Configure & Manage
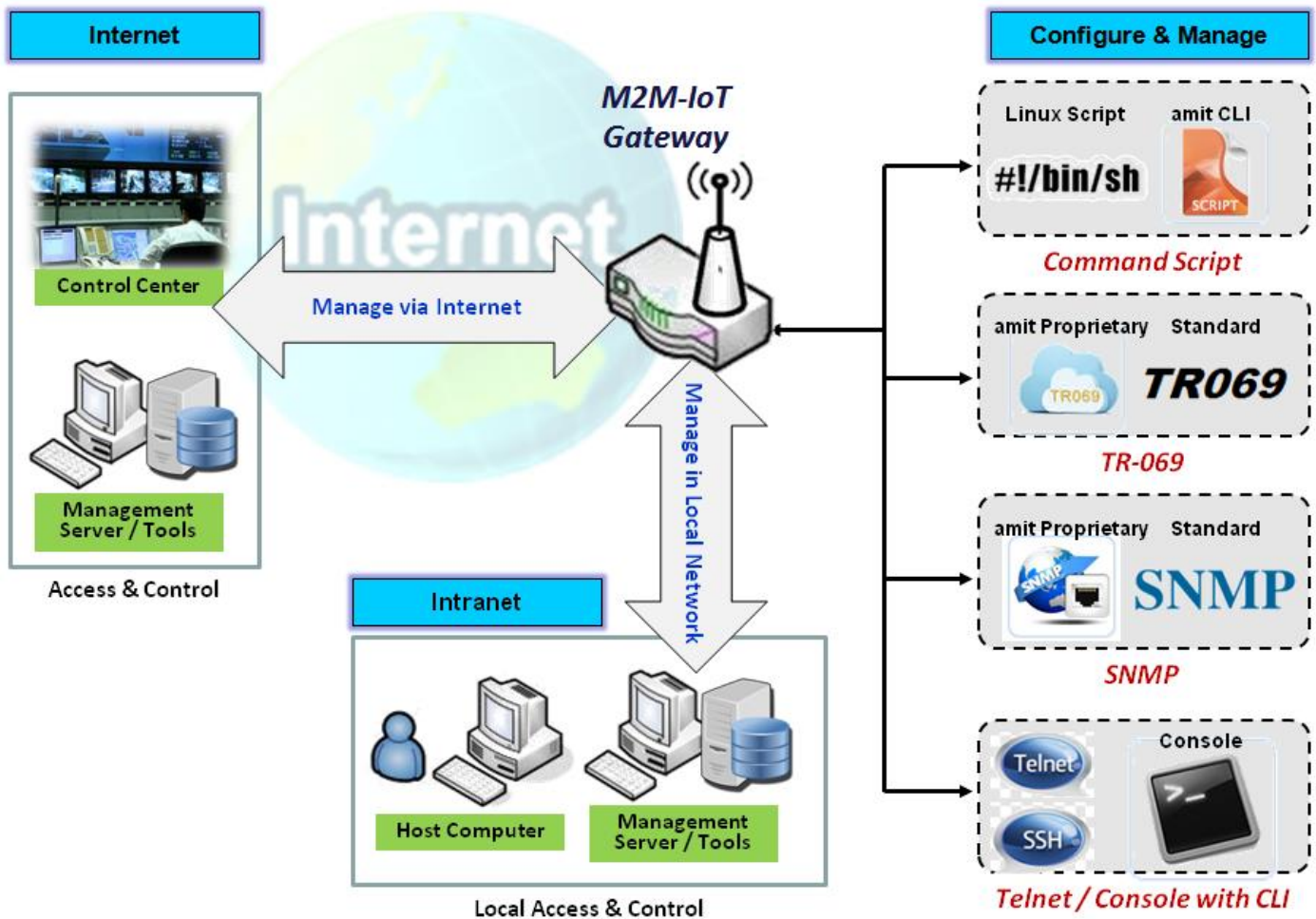
Configure & Manage refers to enterprise-wide administration of distributed systems including (and commonly in practice) computer systems. Centralized management has a time and effort trade-off that is related to the size of the company, the expertise of the IT staff, and the amount of technology being used. This device supports many system management protocols, such as Command Script, TR-069, SNMP, and Telnet with CLI. You can setup those configurations in the "Configure & Manage" section.

Outdoor WiFi LoRa BSU

6.1.1 Command Script

Command script configuration is the application that allows administrator to setup the pre-defined configuration in plain text style and apply configuration on startup.

Go to **Administration > Command Script > Configuration** Tab.
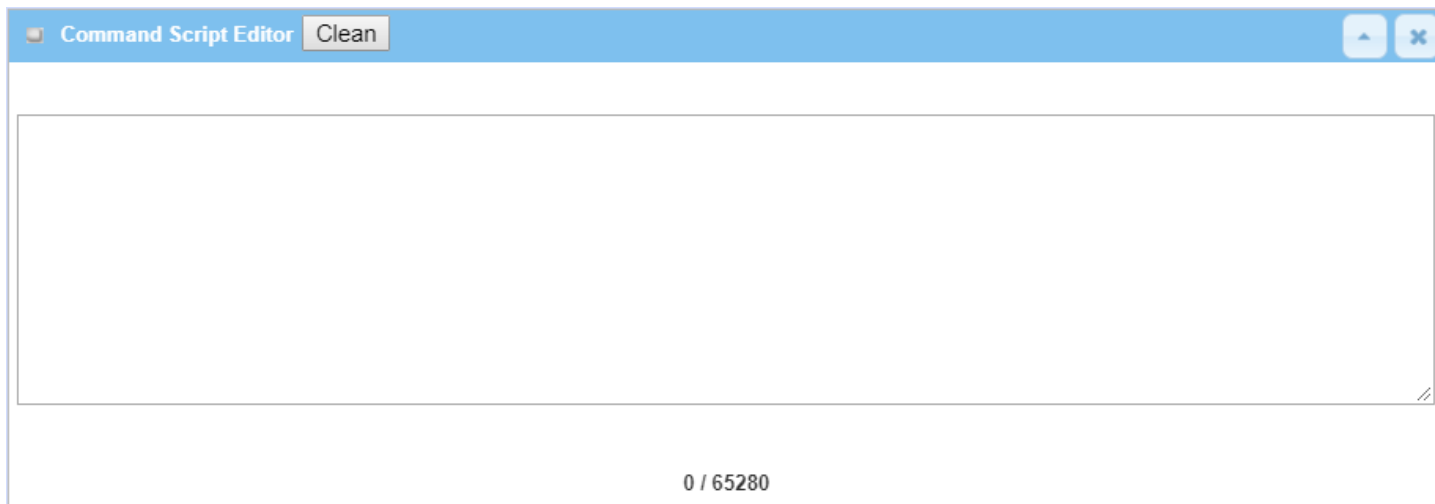
Enable Command Script Configuration

Configuration Item	Value setting	Description
Command Script	The box is unchecked by default	Check the **Enable** box to activate the Command Script function.
Backup Script	N/A	Click the **Via Web UI** or **Via Storage** button to backup the existed command script in a .txt file. You can specify the script file name in **Script Name** below.
Upload Script	N/A	Click the **Via Web UI** or **Via Storage** button to Upload the existed command script from a specified .txt file.
Script Name	1.An Optional setting **2.Any valid file name**	Specify a script file name for script backup, or display the selected upload script file name. **Value Range**: 0 ~ 32 characters.
Version	1.An Optional setting 2.Any string	Specify the version number for the applied Command script. **Value Range**: 0 ~ 32 characters.
Description	1.An Optional setting 2.Any string	Enter a short description for the applied Command script.
Update time	N/A	It records the upload time for last commad script upload.

Outdoor WiFi LoRa BSU

Edit/Backup Plain Text Command Script

You can edit the plain text configuration settings in the configuration screen as above.

Plain Text Configuration		
Item	**Value setting**	**Description**
Clean	NA	Clean text area. (You should click **Save** button to further clean the configuration already saved in the system.)
Backup	NA	Backup and download configuration.
Save	NA	Save configuration

The supported plain text configuration items are shown in the following list. For the settings that can be executed with standard Linux commands, you can put them in a script file, and apply to the system configure with **STARTUP** command. For those configurations without corresponding Linux command set to configure, you can configure them with proprietary command set.

Configuration Content		
Key	**Value setting**	**Description**
OPENVPN_ENABLED	1 : enable 0 : disable	Enable or disable OpenVPN Client function.
OPENVPN_DESCRIPTION	A Must filled Setting	Specify the tunnel name for the OpenVPN Client connection.
OPENVPN_PROTO	udp tcp	Define the **Protocol** for the OpenVPN Client. • Select **TCP** or **TCP /UDP** ->The OpenVPN will use TCP protocol, and **Port** will be set as 443 automatically. • Select **UDP** -> The OpenVPN will use UDP protocol, and **Port** will be set as 1194 automatically.
OPENVPN_PORT	A Must filled Setting	Specify the **Port** for the OpenVPN Client to use.
OPENVPN_REMOTE_IPADDR	IP or FQDN	Specify the **Remote IP/FQDN** of the peer OpenVPN Server for this OpenVPN Client tunnel. Fill in the IP address or FQDN.
OPENVPN_PING_INTVL	seconds	Specify the time interval for OpenVPN keep-alive checking.

OPENVPN_PING_TOUT	seconds	Specify the timeout value for OpenVPN Client keep-alive checking.
OPENVPN_COMP	Adaptive	Specify the **LZO Compression** algorithm for OpenVPN client.
OPENVPN_AUTH	Static Key/TLS	Specify the authorization mode for the OpenVPN tunnel. • **TLS** ->The OpenVPN will use TLS authorization mode, and the following items **CA Cert.**, **Client Cert.** and **Client Key** need to specify as well.
OPENVPN_CA_CERT	A Must filled Setting	Specify the Trusted CA certificate for the OpenVPN client. It will go through Base64 Conversion.
OPENVPN_LOCAL_CERT	A Must filled Setting	Specify the local certificate for OpenVPN client. It will go through Base64 Conversion.
OPENVPN_LOCAL_KEY	A Must filled Setting	Specify the local key for the OpenVPN client. It will go through Base64 Conversion.
OPENVPN_EXTRA_OPTS	Options	Specify the extra options setting for the OpenVPN client.
IP_ADDR1	Ip	Ethernet LAN IP
IP_NETM1	Net mask	Ethernet LAN MASK
PPP_MONITORING	1 : enable 0 : disable	When the Network Monitoring feature is enabled, the router will use DNS Query or ICMP to periodically check Internet connection – connected or disconnected.
PPP_PING	0 : DNS Query 1 : ICMP Query	With **DNS Query,** the system checks the connection by sending DNS Query packets to the destination specified in PPP_PING_IPADDR. With **ICMP Query,** the system will check connection by sending ICMP request packets to the destination specified in PPP_PING_IPADDR.
PPP_PING_IPADDR	IP	Specify an IP address as the target for sending DNS query/ICMP request.
PPP_PING_INTVL	seconds	Specify the time interval for between two DNS Query or ICMP checking packets.
STARTUP	Script file	For the configurations that can be configured with standard Linux commands, you can put them in a script file, and apply the script file with STARTUP command. For example, STARTUP=#!/bin/sh STARTUP=echo "startup done" > /tmp/demo

Plain Text System Configuration with Telnet

In addition to the web-style plain text configuration as mentioned above, the gateway system also allow the configuration via Telnet CLI. Administrator can use the proprietary telnet command "***txtConfig***" and related action items to perform the plain system configuration.

The command format is: txtConfig (action) [option]

Action	Option	Description
clone	*Output file*	Duplicate the configuration content from database and stored as a configuration file. (ex: *txtConfig clone /tmp/config*) The contents in the configuration file are the same as the plain text commands mentioned above. This action is exactly the same as performing the "Backup" plain text configuration.

|		
commit	a existing file	Commit the configuration content to database. (ex: *txtConfig commit /tmp/config*)
enable	*NA*	Enable plain text system config. (ex: *txtConfig enable*)
disable	*NA*	Disable plain text system config. (ex: *txtConfig disable*)
run_immediately	*NA*	Apply the configuration content that has been committed in database. (ex: *txtConfig run_immediately*)
run_immediately	a existing file	Assign a configuration file to apply. (ex: *txtConfig run_immediately /tmp/config*)

Outdoor WiFi LoRa BSU

6.1.2 TR-069

TR-069 (Technical Report 069) is a Broadband Forum technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices, like this gateway device. As a bidirectional SOAP/HTTP-based protocol, it provides the communication between customer-premises equipment (CPE) and Auto Configuration Servers (ACS). The Security Gateway is such CPE.

TR-069 is a customized feature for ISP. It is not recommend that you change the configuration for this. If you have any problem in using this feature for device management, please contact with your ISP or the ACS provider for help. At the right upper corner of TR-069 Setting screen, one "[Help]" command let you see the same message about that.

Scenario - Managing deployed gateways through an ACS Server
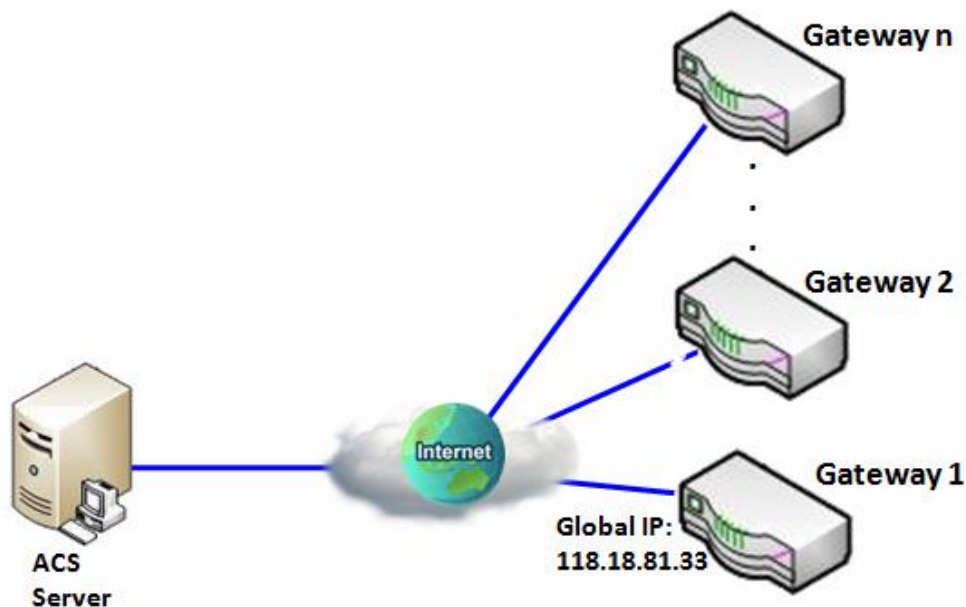
Scenario Application Timing

When the enterprise data center wants to use an ACS server to manage remote gateways geographically distributed elsewhere in the world, the gateways in all branch offices must have an embedded TR-069 agent to communicate with the ACS server. So that the ACS server can configure, FW upgrade and monitor these gateways and their corresponding Intranets.

Scenario Description

The ACS server can configure, upgrade with latest FW and monitor these gateways.

Remote gateways inquire the ACS server for jobs to do in each time period.

The ACS server can ask the gateways to execute some urgent jobs.

Outdoor WiFi LoRa BSU

Parameter Setup Example

Following tables list the parameter configuration as an example for the Gateway 1 in above diagram with "TR-069" enabling.

Use default value for those parameters that are not mentioned in the tables.

Configuration Path	[TR-069]-[Configuration]
TR-069	■ *Enable*
ACS URL	**http://qa.acslite.com/cpe.php**
ACS User Name	*ACSUserName*
ACS Password	*ACSPassword*
ConnectionRequest Port	*8099*
ConnectionRequest User Name	*ConnReqUserName*
ConnectionRequest Password	*ConnReqPassword*
Inform	■ *Enable Interval 900*

Scenario Operation Procedure

In above diagram, the ACS server can manage multiple gateways in the Internet. The "Gateway 1" is one of them and has 118.18.81.33 IP address for its WAN-1 interface.

When all remote gateways have booted up, they will try to connect to the ACS server.

Once the connections are established successfully, the ACS server can configure, upgrade with latest FW and monitor these gateways.

Remote gateways inquire the ACS server for jobs to do in each time period.

If the ACS server needs some urgent jobs to be done by the gateways, it will issue the "Connection Request" command to those gateways. And those gateways make immediate connections in response to the ACS server's immediate connection request for executing the urgent jobs.

Outdoor WiFi LoRa BSU

TR-069 Setting

Go to **Administration > Configure & Manage > TR-069** tab.

In "TR-069" page, there is only one configuration window for TR-069 function. In the window, you must specify the related information for your security gateway to connect to the ACS. Drive the function to work by specifying the URL of the ACS server, the account information to login the ACS server, the service port and the account information for connection requesting from the ACS server, and the time interval for job inquiry. Except the inquiry time, there are no activities between the ACS server and the gateways until the next inquiry cycle. But if the ACS server has new jobs that are expected to do by the gateways urgently, it will ask these gateways by using connection request related information for immediate connection for inquiring jobs and executing.

Enable TR-069

TR-069		
Item	**Value setting**	**Description**

TR-069	The box is unchecked by default	Check the **Enable** box to activate TR-069 function.
Interface	**WAN-1** is selected by default.	When you finish set basic network WAN-1 ~ WAN-n, you can choose WAN-1 ~ WAN-n When you finish set Security > VPN > IPSec/OpenVPN/PPTP/L2TP/GRE, you can choose IPSec/OpenVPN/PPTP/L2TP/GRE tunnel, the interface just like "IPSec #1"
Data Model	**ACS Cloud Data Model** is selected by default.	Select the TR-069 dat model for the remote management. **Standard** : the ACS Server is a standard one, which is fully comply with TR-069. **ACS Cloud Data Model** : Select this data model if you intend to use Cloud ACS Server to managing the deployed gateways.
ACS URL	A Must filled setting	You can ask ACS manager provide ACS URL and manually set
ACS Username	A Must filled setting	You can ask ACS manager provide ACS username and manually set
ACS Password	A Must filled setting	You can ask ACS manager provide ACS password and manually set
ConnectionRequest Port	1. A Must filled setting. 2. By default **8099** is set.	You can ask ACS manager provide ACS ConnectionRequest Port and manually set *Value Range*: 0 ~ 65535.
ConnectionRequest UserName	A Must filled setting	You can ask ACS manager provide ACS ConnectionRequest Username and manually set
ConnectionRequest Password	A Must filled setting	You can ask ACS manager provide ACS ConnectionRequest Password and manually set
Inform	1. The box is checked by default. 2. The Interval value is **300** by default.	When the **Enable** box is checked, the gateway (CPE) will periodicly send inform message to ACS Server according to the **Interval** setting. *Value Range*: 0 ~ 86400 for Inform Interval.
Certification Setup	The **default** box is selected by default	You can leave it as **default** or select an expected certificate and key from the drop down list. Refer to **Object Definition > Certificate** Section for the Certificate configuration.
Save	N/A	Click **Save** to save the settings.
Undo	N/A	Click **Undo** to cancel the modifications.

When you finish set **ACS URL ACS Username ACS Password,** your gateway (CPE, Client Premium Equipment) can send inform to ACS Server.

When you finish set **ConnectionRequest Port ConnectionRequest Username ConnectionRequest Password**, ACS Server can ask the gateway (CPE) to send inform to ACS Server.

Enable STUN Server

Outdoor WiFi LoRa BSU

| STUN Settings Configuration		
Item	**Value setting**	**Description**
STUN	The box is checked by default	Check the **Enable** box to activate STUN function.
Server Address	1. String format: any IPv4 address 2. It is an optional item.	Specify the IP address for the expected STUN Server.
Server Port	1. An optional setting 2.**3478** is set by default	Specify the port number for the expected STUN Server. *Value Range*: 1 ~ 65535.
Keep Alive Period	1. An optional setting 2.**0** is set by default	Specify the keep alive time period for the connection with STUN Server. *Value Range*: 0 ~ 65535.
Save	N/A	Click **Save** to save the settings.
Undo	N/A	Click **Undo** to cancel the modifications.

6.1.3 SNMP

In brief, SNMP, the Simple Network Management Protocol, is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

In typical SNMP uses, one or more administrative computers, called managers, have the task of monitoring or managing a group of hosts or devices on a computer network. Each managed system executes, at all times, a software component called an agent which reports information via SNMP to the manager.

SNMP agents expose management data on the managed systems as variables. The protocol also permits active management tasks, such as modifying and applying a new configuration through remote modification of these variables. The variables accessible via SNMP are organized in hierarchies. These hierarchies, and other metadata (such as type and description of the variable), are described by Management Information Bases (MIBs).

The device supports several public MIBs and one private MIB for the SNMP agent. The supported MIBs are as follow: MIB-II (RFC 1213, Include IPv6), IF-MIB, IP-MIB, TCP-MIB, UDP-MIB, SMIv1 and SMIv2, SNMPv2-TM and SNMPv2-MIB, and AMIB (a Proprietary MIB)

SNMP Management Scenario
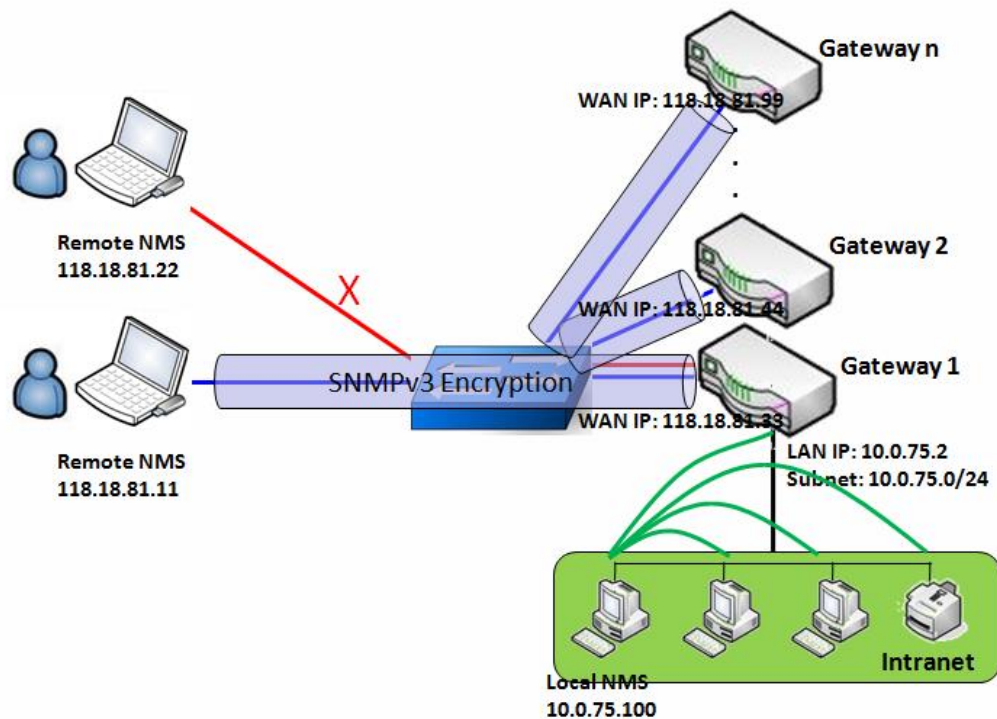
Scenario Application Timing

There are two application scenarios of SNMP Network Management Systems (NMS). Local NMS is in

the Intranet and manage all devices that support SNMP protocol in the Intranet. Another one is the Remote NMS to manage some devices whose WAN interfaces are connected together by using a switch or a router with UDP forwarding. If you want to manage some devices and they all have supported SNMP protocol, use either one application scenario, especially the management of devices in the Intranet. In managing devices in the Internet, the TR-069 is the better solution. Please refer to last sub-section.

Scenario Description

The NMS server can monitor and configure the managed devices by using SNMP protocol, and those devices are located at where UDP packets can reach from NMS.

The managed devices report urgent trap events to the NMS servers.

Use SNMPv3 version of protocol can protected the transmitting of SNMP commands and responses.

The remote NMS with privilege IP address can manage the devices, but other remote NMS can't.

Parameter Setup Example

Following tables list the parameter configuration as an example for the Gateway 1 in above diagram with "SNMP" enabling at LAN and WAN interfaces.

Use default value for those parameters that are not mentioned in the tables.

Configuration Path	[SNMP]-[Configuration]
SNMP Enable	■ *LAN* ■ *WAN*
Supported Versions	■ *v1* ■ *v2c* ■ *v3*
Get / Set Community	*ReadCommunity / WriteCommunity*
Trap Event Receiver 1	*118.18.81.11*
WAN Access IP Address	*118.18.81.11*

Configuration Path	[SNMP]-[User Privacy Definition]		
ID	1	2	3
User Name	*UserName1*	*UserName2*	*UserName3*
Password	*Password1*	*Password2*	*Disable*
Authentication	*MD5*	*SHA-1*	*Disable*
Encryption	*DES*	*Disable*	*Disable*
Privacy Mode	*authPriv*	*authNoPriv*	*noAuthNoPriv*
Privacy Key	*12345678*	*Disable*	*Disable*
Authority	*Read/Write*	*Read*	*Read*
Enable	■ *Enable*	■ *Enable*	■ *Enable*

Scenario Operation Procedure

In above diagram, the NMS server can manage multiple devices in the Intranet or a UDP-reachable network. The "Gateway 1" is one of the managed devices, and it has the IP address of 10.0.75.2 for

LAN interface and 118.18.81.33 for WAN-1 interface. It serves as a NAT router.

At first stage, the NMS manager prepares related information for all managed devices and records them in the NMS system. Then NMS system gets the status of all managed devices by using SNMP get commands.

When the manager wants to configure the managed devices, the NMS system allows him to do that by using SNMP set commands. The "UserName1" account is used if the manager uses SNMPv3 protocol for configuring the "Gateway 1". Only the "UserName1" account can let the "Gateway 1" accept the configuration from the NMS since the authority of the account is "Read/Write".

Once a managed device has an urgent event to send, the device will issue a trap to the Trap Event Receivers. The NMS itself could be one among them.

If you want to secure the transmitted SNMP commands and responses between the NMS and the managed devices, use SNMPv3 version of protocol.

The remote NMS without privilege IP address can't manage the "Gateway 1", since "Gateway 1" allows only the NMS with privilege IP address can manage it via its WAN interface.

Outdoor WiFi LoRa BSU

SNMP Setting

Go to **Administration > Configure & Manage > SNMP** tab.

The SNMP allows user to configure SNMP relevant setting which includes interface, version, access control and trap receiver.

Enable SNMP

SNMP Item	Value setting	Description
SNMP Enable	1.The boxes are unchecked by default	Select the interface for the SNMP and enable SNMP functions. When Check the **LAN** box, it will activate SNMP functions and you can access SNMP from LAN side; When Check the **WAN** box, it will activate SNMP functions and you can access SNMP from WAN side.
WAN Interface	1.A Must filled setting **2. ALL WANs is selected by default**	Specify the WAN interface that a remote SNMP host can access to the device. By default, **All WANs** is selected, and there is no limitation for the WAN inferface.
Supported Versions	1.A Must filled setting 2.The boxes are unchecked by default	Select the version for the SNMP When Check the **v1** box. It means you can access SNMP by version 1. When Check the **v2c** box. It means you can access SNMP by version 2c. When Check the **v3** box. It means you can access SNMP by version 3.
SNMP Port	1. String format: any	Specify the **SNMP Port**.

	port number 2. The default SNMP port is **161**. 3. A Must filled setting	You can fill in any port number. But you must ensure the port number is not to be used. *Value Range*: 1 ~ 65535.
Limited Remote Aceess IP	1. String format: any IPv4 address 2. It is an optional item.	Specify the **Remote Access IP** for WAN and check the box to enable it as well. Select **Specific IP Address**, and fill in a certain IP address. It means only this IP address can access SNMP from LAN/WAN side. Select **IP Range**, and fill in a range of IP addresses. It means the IP address within specified range can access SNMP from LAN/WAN side. If you left it as blank, it means any IP address can access SNMP from WAN side.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Create/Edit Multiple Community

The SNMP allows you to custom your access control for version 1 and version 2 user. The router supports up to a maximum of 10 community sets.

When **Add** button is applied, **Multiple Community Rule Configuration** screen will appear.

Multiple Community Rule Configuration		
Item	**Value setting**	**Description**
Community	1. **Read Only** is selected by default 2. A Must filled setting 3. String format: any text	Specify this version 1 or version v2c user's community that will be allowed **Read Only** (GET and GETNEXT) or **Read-Write** (GET, GETNEXT and SET) access respectively. The maximum length of the community is 32.
Enable	1.The box is checked by default	Click Enable to enable this version 1 or version v2c user.
Save	N/A	Click the **Save** button to save the configuration. But it does not apply to SNMP functions. When you return to the SNMP main page. It will show "Click on save button to apply your changes" remind user to click main page Save button.

Outdoor WiFi LoRa BSU

Undo	N/A	Click the **Undo** button to cancel the settings.
Back	N/A	Click the **Back** button to return to last page.

Create/Edit User Privacy

The SNMP allows you to custom your access control for version 3 user. The router supports up to a maximum of 128 User Privacy sets.

When **Add** button is applied, **User Privacy Rule Configuration** screen will appear.

User Privacy Rule Configuration Item	Value setting	Description
User Name	1. A Must filled setting 2. String format: any text	Specify the **User Name** for this version 3 user. ***Value Range*****:** 1 ~ 32 characters.
Password	1. String format: any text	When your **Privacy Mode** is **authNoPriv** or **authPriv**, you must specify the **Password** for this version 3 user. ***Value Range*****:** 8 ~ 64 characters.
Authentication	1. **None** is selected by default	When your **Privacy Mode** is **authNoPriv** or **authPriv**, you must specify the **Authentication** types for this version 3 user. Selected the authentication types **MD5/ SHA-1** to use.
Encryption	1. **None** is selected by default	When your **Privacy Mode** is **authPriv**, you must specify the **Encryption** protocols for this version 3 user.

		Selected the encryption protocols **DES / AES** to use.
Privacy Mode	1. **noAuthNoPriv** is selected by default	Specify the **Privacy Mode** for this version 3 user. Selected the **noAuthNoPriv**. You do not use any authentication types and encryption protocols. Selected the **authNoPriv**. You must specify the **Authentication** and **Password**. Selected the **authPriv**. You must specify the Authentication, Password, Encryption and Privacy Key.
Privacy Key	1. String format: any text	When your **Privacy Mode** is **authPriv**, you must specify the **Privacy Key** (8 ~ 64 characters) for this version 3 user.
Authority	1. **Read** is selected by default	Specify this version 3 user's **Authority** that will be allowed **Read Only** (GET and GETNEXT) or **Read-Write** (GET, GETNEXT and SET) access respectively.
OID Filter Prefix	1. The default value is 1 2. A Must filled setting 3. String format: any legal OID	The **OID Filter Prefix** restricts access for this version 3 user to the sub-tree rooted at the given OID. ***Value Range*:** 1 ~2080768.
Enable	1.The box is checked by default	Click **Enable** to enable this version 3 user.
Save	N/A	Click the **Save** button to save the configuration. But it does not apply to SNMP functions. When you return to the SNMP main page. It will show "Click on save button to apply your changes" remind user to click main page **Save** button.
Undo	N/A	Click the **Undo** button to cancel the settings
Back	N/A	Click the **X** button to return the last page.

Create/Edit Trap Event Receiver

The SNMP allows you to custom your trap event receiver. The router supports up to a maximum of 4 Trap Event Receiver sets.

When **Add** button is applied, **Trap Event Receiver Rule Configuration** screen will appear. The default SNMP Version is v1. The configuration screen will provide the version 1 must filled items.

Outdoor WiFi LoRa BSU

When you selected v2c, the configuration screen is exactly the same as that of v1, except the version.

When you selected v3, the configuration screen will provide more setting items for the version 3 Trap.

Trap Event Receiver Rule Configuration		
Item	**Value setting**	**Description**
Server IP	1. A Must filled setting 2. String format: any IPv4 address or FQDN	Specify the trap **Server IP** or **FQDN**. The DUT will send trap to the server IP/FQDN.
Server Port	1. String format: any port number 2. The default SNMP trap port is 162 3. A Must filled setting	Specify the trap **Server Port**. You can fill in any port number. But you must ensure the port number is not to be used. *Value Range*: 1 ~ 65535.
SNMP Version	1. **v1** is selected by	Select the version for the trap

190

	default	Selected the **v1**. The configuration screen will provide the version 1 must filled items. Selected the **v2c**. The configuration screen will provide the version 2c must filled items. Selected the **v3**. The configuration screen will provide the version 3 must filled items.
Community Name	1. A **v1** and **v2c** Must filled setting 2. String format: any text	Specify the **Community Name** for this version 1 or version v2c trap. ***Value Range:*** 1 ~ 32 characters.
User Name	1. A **v3** Must filled setting 2. String format: any text	Specify the **User Name** for this version 3 trap. ***Value Range:*** 1 ~ 32 characters.
Password	1. A **v3** Must filled setting 2. String format: any text	When your **Privacy Mode** is **authNoPriv** or **authPriv**, you must specify the **Password** for this version 3 trap. ***Value Range:*** 8 ~ 64 characters.
Privacy Mode	1. A **v3** Must filled setting 2. **noAuthNoPriv** is selected by default	Specify the **Privacy Mode** for this version 3 trap. Selected the **noAuthNoPriv**. You do not use any authentication types and encryption protocols. Selected the **authNoPriv**. You must specify the **Authentication** and **Password**. Selected the **authPriv**. You must specify the Authentication, Password, Encryption and Privacy Key.
Authentication	1. A **v3** Must filled setting 2. **None** is selected by default	When your **Privacy Mode** is **authNoPriv** or **authPriv**, you must specify the **Authentication** types for this version 3 trap. Selected the authentication types **MD5/ SHA-1** to use.
Encryption	1. A **v3** Must filled setting 2. **None** is selected by default	When your **Privacy Mode** is **authPriv**, you must specify the **Encryption** protocols for this version 3 trap. Selected the encryption protocols **DES / AES** to use.
Privacy Key	1. A **v3** Must filled setting 2. String format: any text	When your **Privacy Mode** is **authPriv**, you must specify the **Privacy Key** (8 ~ 64 characters) for this version 3 trap.
Enable	1.The box is checked by default	Click **Enable** to enable this trap receiver.
Save	N/A	Click the **Save** button to save the configuration. But it does not apply to SNMP functions. When you return to the SNMP main page. It will show "Click on save button to apply your changes" remind user to click main page **Save** button.
Undo	N/A	Click the **Undo** button to cancel the settings.
Back	N/A	Click the **X** button to return to last page.

Outdoor WiFi LoRa BSU

Specify SNMP MIB-2 System

If required, you can also specify the required information for the MIB-2 System.

SNMP MIB-2 System Configuration

Item	Value setting	Description
sysContact	1. An Optional filled setting 2. String format: any text	Specify the contact information for MIB-2 system. **Value Range**: 0 ~ 64 characters.
sysLocation	1. An Optional filled setting 2. String format: any text	Specify the location information for MIB-2 system. **Value Range**: 0 ~ 64 characters.

Edit SNMP Options

If you use some particular private MIB, you must fill the enterprise name, number and OID.

Options

Item	Value setting	Description
Enterprise Name	1. The default value is **Default** 2. A Must filled setting 3. String format: any text	Specify the **Enterprise Name** for the particular private MIB. **Value Range**: 1 ~ 10 characters, and only string with A~Z, a~z, 0~9, '–', '_'.
Enterprise Number	The default value is **12823** (Default Enterprise	Specify the **Enterprise Number** for the particular private MIB. **Value Range**: 1 ~2080768.

	Number) 2. A Must filled setting 3. String format: any number	
Enterprise OID	1. The default value is 1.3.6.1.4.1.**12823.4.4.9** (Default Enterprise OID) 2. A Must filled setting 3. String format: any legal OID	Specify the **Enterprise OID** for the particular private MIB. The range of the each OID number is 1-2080768. The maximum length of the enterprise OID is 31. The seventh number must be identical with the enterprise number.
Save	N/A	Click the **Save** button to save the configuration and apply your changes to SNMP functions.
Undo	N/A	Click the **Undo** button to cancel the settings.

6.1.4 Telnet & SSH

A command-line interface (CLI), also known as command-line user interface, and console user interface are means of interacting with a computer program where the user (or client) issues commands to the program in the form of successive lines of text (command lines). The interface is usually implemented with a command line shell, which is a program that accepts commands as text input and converts commands to appropriate operating system functions. Programs with command-line interfaces are generally easier to automate via scripting. The device supports both Telnet and SSH (Secure Shell) CLI with default service port 23 and 22, respectively.

Telnet & SSH Scenario
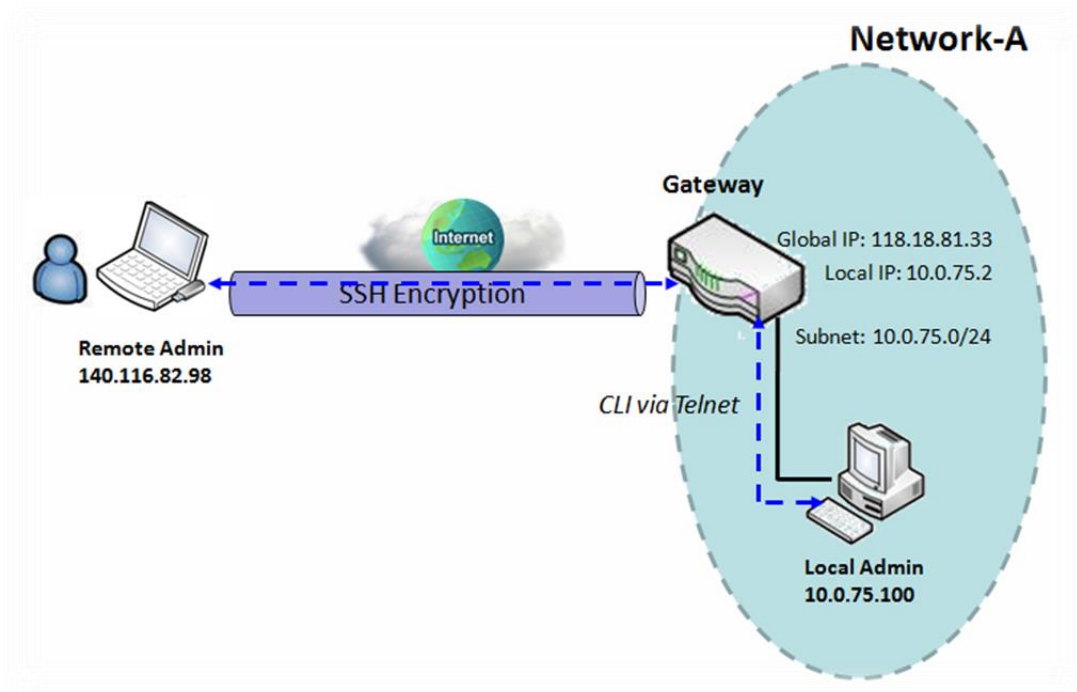
Scenario Application Timing

When the administrator of the gateway wants to manage it from remote site in the Intranet or Internet, he may use "Telnet with CLI" function to do that by using "Telnet" or "SSH" utility.

Scenario Description

The Local Admin or the Remote Admin can manage the Gateway by using "Telnet" or "SSH" utility with privileged user name and password.

The data packets between the Local Admin and the Gateway or between the Remote Admin and the Gateway can be plain texts or encrypted texts. Suggest they are plain texts in the Intranet for Local Admin to use "Telnet" utility, and encrypted texts in the Internet for Remote Admin to use "SSH"

utility.

Parameter Setup Example

Following table lists the parameter configuration as an example for the Gateway in above diagram with "Telnet with CLI" enabling at LAN and WAN interfaces.

Use default value for those parameters that are not mentioned in the table.

Configuration Path	[Telnet & SSH]-[Configuration]
Telnet	LAN: ∎ *Enable* WAN: ☐ *Enable* Service Port: *23*
SSH	LAN: ∎ *Enable* WAN: ∎ *Enable* Service Port: *22*

Scenario Operation Procedure

In above diagram, "Local Admin" or "Remote Admin" can manage the "Gateway" in the Intranet or Internet. The "Gateway" is the gateway of Network-A, and the subnet of its Intranet is 10.0.75.0/24. It has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN-1 interface. It serves as a NAT gateway.

The "Local Admin" in the Intranet uses "Telnet" utility with privileged account to login the Gateway.

Or the "Remote Admin" in the Internet uses "SSH" utility with privileged account to login the Gateway.

The administrator of the gateway can control the device as like he is in front of the gateway.

Outdoor WiFi LoRa BSU

Telnet & SSH Setting

Go to Administration > Configure & Manage > Telnet & SSH tab.

The Telnet & SSH setting allows administrator to access this device through the traditional Telnet or SSH Telnet program. Before you can telnet (login) to the device, please configure the related settings with care.

Configuration Item	Value setting	Description
Telnet	1. The LAN Enable box is checked by default. 2. By default **Service Port** is 23.	Check the **Enable** box to activate the Telnet function for connecting from LAN or WAN interfaces. You can set which number of **Service Port** you want to provide for the corresponding service. ***Value Range***: 1 ~65535.
SSH	3. The LAN Enable box is checked by default. 4. By default **Service Port** is 22.	Check the **Enable** box to activate the SSH Telnet function for connecting from LAN or WAN interfaces. You can set which number of **Service Port** you want to provide for the corresponding service. ***Value Range***: 1 ~65535.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Note: The Telnet/SSH login password is the same one as the administrator's login password for the device web GUI.

6.2 System Operation

System Operation allows the network administrator to manage system, settings such as web-based utility access password change, system information, system time, system log, firmware/configuration backup & restore, and reset & reboot.

6.2.1 Password & MMI

Go to **Administration > System Operation > Password & MMI** tab.

Setup Host Name

Host Name screen allows network administrator to setup / change the host name of the gateway. Click the **Modify** button and provide the new username setting.

Item	Setting
▸ Host Name	

Username Configuration		
Item	**Value setting**	**Description**
Host Name	1. An Optional setting 2. It is blanked by default	Enter the host name of the gateway.
Save	N/A	Click **Save** button to save the settings
Undo	N/A	Click **Undo** button to cancel the settings

Change UserName

Username screen allows network administrator to change the web-based MMI login account to access gateway. Click the **Modify** button and provide the new username setting.

Item	Setting
▸ Username	admin [Modify]
▸ New Username	
▸ Password	

Outdoor WiFi LoRa BSU

Username Configuration		
Item	**Value setting**	**Description**
Username	1. The default Username for web-based MMI is '**admin**'.	Display the current MMI login account (Username).
New Username	String: any text	Enter new Username to replace the current setting.
Password	String: any text	Enter current password to verify if you have the permission to change the username setting.
Save	N/A	Click **Save** button to save the settings
Undo	N/A	Click **Undo** button to cancel the settings

Change Password

Change password screen allows network administrator to change the web-based MMI login password to access gateway.

Password Configuration		
Item	**Value setting**	**Description**
Old Password	1. String: any text **2. The default password for web-based MMI is 'admin'.**	Enter the current password to enable you unlock to change password.
New Password	String: any text	Enter new password
New Password Confirmation	String: any text	Enter new password again to confirm
Save	N/A	Click **Save** button to save the settings
Undo	N/A	Click **Undo** button to cancel the settings

Change MMI Setting for Accessing

This is the gateway's web-based MMI access which allows administrator to access the gateway for management. The gateway's web-based MMI will automatically logout when the idle time has elapsed. The

setting allows administrator to enable automatic logout and set the logout idle time. When the login timeout is disabled, the system won't logout the administrator automatically.

MMI		
Item	Setting	
▸ Login	Password-Guessing Attack & MAX: 3 (times)	
▸ Login Timeout	☑ Enable 300 (seconds)	
▸ GUI Access Protocol	http/https ▾	
▸ HTTPs Certificate Setup	⦿ default ◯ Select from Certificate List Certificate: TrustedCert0 ▾ Key: TrustedKey0 ▾	
▸ HTTP Compression	☑ gzip ☐ deflate	
▸ HTTP Binding	☑ DHCP 1	
▸ System Boot Mode	Normal Mode ▾	

MMI Configuration Item	Value setting	Description
Login	3 times is set by default	Enter the login trial counting value. *Value Range*: 3 ~ 10. If someone tried to login the web GUI with incorrect password for more than the counting value, an warning message "*Already reaching maximum Password-Guessing times, please wait a few seconds!*" will be displayed and ignore the following login trials.
Login Timeout	The Enable box is checked, and 300 is set by default.	Check the Enable box to activate the auto logout function, and specify the maximum idle time as well. *Value Range*: 30 ~ 65535.
GUI Access Protocol	**http/https** is selected by default.	Select the protocol that will be used for GUI access. It can be **http/https**, **http only**, or **https only**.
HTTPs Certificate Setup	The **default** box is selected by default	If the https Access Protocol is selected, the HTTPs Certificate Setup option will be available for further configuration. You can leave it as default or select a expected certificate and key from the drop down list. Refer to **Object Definition > Certificate** Section for the Certificate configuration.
HTTP Compression	The box is unchecked by default.	Check the box (**gzip**, or **deflate**) if any comprerssion method is preferred.
HTTP Binding	1. An Optional setting 2. DHCP-1 is checked by default	Select the DHCP Server to bind with http access.
System Boot Mode	**Normal Mode** is selected by default.	Select the system boot mode that will be adopted to boot up the device. **Normal Mode**: It takes longer boot up time, with complete firmware image

Outdoor WiFi LoRa BSU

		check during the device booting.
Save	N/A	Click **Save** button to save the settings
Undo	N/A	Click **Undo** button to cancel the settings

6.2.2 System Information

System Information screen gives network administrator a quick look up on the device information for the purchades gateway.

Go to **Administration > System Operation > System Information** tab.

Item	Setting
▸ Model Name	VHG87BAM_0T001
▸ Device Serial Number	
▸ Kernel Version	2.6.36
▸ FW Version	0000Y90.J31_e32.BETA_04021700
▸ System Time	Thu, 18 Apr 2019 16:18:16 +0800
▸ Device Up-Time	15day 22hr 30min 35sec

System Information		
Item	**Value Setting**	**Description**
Model Name	N/A	It displays the model name of this product.
Device Serial Number	N/A	It displays the serial number of this product.
Kernel Version	N/A	It displays the Linux kernel version of the product
FW Version	N/A	It displays the firmware version of the product
Memory Usage	N/A	It displays the percentage of device memory utilization.
System Time	N/A	It displays the current system time that you browsed this web page.
Device Up-Time	N/A	It displays the statistics for the device up-time since last boot up.
Refresh	N/A	Click the **Refresh** button to update the system Information immediately.

6.2.3 System Time

The gateway provides manually setup and auto-synchronized approaches for the administrator to setup the system time for the gateway. The time supported synchronization methods can be Time Server, Manual, PC, Cellular Module, or GPS Signal. Select the method first, and then configure rest settings.

Instead of manually configuring the system time for the gateway, there are two simple and quick solutions for you to set the correct time information and set it as the system time for the gateway.

The first one is "Sync with Timer Server". Based on your selection of time zone and time server in above time information configuration window, system will communicate with time server by NTP Protocol to get system date and time after you click on the **Synchronize immediately** button.

The second one is "Sync with my PC". Select the method and the system will synchronize its date and time to the time of the administration PC.

Go to **Administration > System Operation > System Time** tab.

Synchronize with Time Server

System Time Configuration	
Item	**Setting**
▸ Synchronization method	Time Server ▾
▸ Time Zone	(GMT+00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▾
▸ Auto-synchronization	Time Server: [_____]
	Available Time Servers (RFC-868): Auto ▾
▸ Daylight Saving Time	☐ Enable
▸ NTP Service	☐ Enable
▸ Synchronize immediately	Active

System Time Information		
Item	**Value Setting**	**Description**
Synchronization method	1. A Must-filled item. 2. **Time Server** is selected by default.	Select the **Time Server** as the synchronization method for the system time.
Time Zone	1. A Must-filled item. 2. **GMT+00 :00** is selected by default.	Select a time zone where this device locates.
Auto-synchronization	1. A Must-filled item. 2. Auto is selected by	Enter the IP or FQDN for the NTP time server you expected, or leave it as auto mode so that the available server will be used for time synchronization one by

	default.	one.
Daylight Saving Time	1. It is an optional item. 2. Un-checked by default	Check the **Enable** button to activate the daylight saving function. When you enabled this function, you have to specify the start date and end date for the daylight saving time duration.
NTP Service	1. It is an optional item. 2. Un-checked by default	Check the **Enable** button to activate the NTP Service function. When you enabled this function, the gateway can provide NTP server service for its local connected devices.
Synchronize immediately	N/A	Click the **Active** button to synchronize the system time with specified time server immediately.
Save	N/A	Click the **Save** button to save the settings.
Refresh	N/A	Click the **Refresh** button to update the system time immediately.

Note: Remember to select a correct time zone for the device, otherwise, you will just get the UTC (Coordinated Universal Time) time, not the local time for the device.

Synchronize with Manually Setting

System Time Configuration	
Item	**Setting**
▶ Synchronization method	Manual ▼
▶ Time Zone	(GMT+00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▼
▶ Daylight Saving Time	☐ Enable
▶ Set Date & Time Manually	2019 ▼ / April ▼ / 18 ▼ (Year/Month/Day) 16 ▼ : 24 ▼ : 27 ▼ (Hour:Minute:Second)
▶ NTP Service	☐ Enable

System Time Information		
Item	**Value Setting**	**Description**
Synchronization method	1. A Must-filled item. 2. **Time Server** is selected by default.	Select the **Manual** as the synchronization method for the system time. It means administrator has to set the Date & Time manually.
Time Zone	1. A Must-filled item. 2. **GMT+00 :00** is selected by default.	Select a time zone where this device locates.
Daylight Saving Time	1. It is an optional item. 2. Un-checked by default	Check the **Enable** button to activate the daylight saving function. When you enabled this function, you have to specify the start date and end date for the daylight saving time duration.
Set Date & Time Manually	1. It is an optional item.	Manually set the date (Year/Month/Day) and time (Hour:Minute:Second) as the system time.
NTP Service	1. It is an optional item.	Check the **Enable** button to activate the NTP Service function.

	2. Un-checked by default	When you enabled this function, the gateway can provide NTP server service for its local connected devices.
Save	N/A	Click the **Save** button to save the settings.

Synchronize with PC

System Time Configuration	
Item	**Setting**
▶ Synchronization method	PC ▼
▶ NTP Service	☐ Enable
▶ Synchronize immediately	Active

System Time Information		
Item	**Value Setting**	**Description**
Synchronization method	1. A Must-filled item. 2. **Time Server** is selected by default.	Select **PC** as the synchronization method for the system time to let system synchronize its date and time to the time of the administration PC.
NTP Service	1. It is an optional item. 2. Un-checked by default	Check the **Enable** button to activate the NTP Service function. When you enabled this function, the gateway can provide NTP server service for its local connected devices.
Synchronize immediately	N/A	Click the **Active** button to synchronize the system time with specified time server immediately.
Save	N/A	Click the **Save** button to save the settings.
Refresh	N/A	Click the **Refresh** button to update the system time immediately.

Outdoor WiFi LoRa BSU

Synchronize with Cellular Time Service

System Time Configuration

Item	Setting
▸ Synchronization method	Cellular Module ▾
▸ Time Zone	(GMT+00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▾
▸ NTP Service	☐ Enable
▸ Synchronize immediately	Active

System Time Information		
Item	**Value Setting**	**Description**
Synchronization method	1. A Must-filled item. 2. **Time Server** is selected by default.	Select **Cellular Module** as the synchronization method for the system time to let system synchronize its date and time to the time provided from the connected mobile ISP. Note: this option is only available for the product with Cellular WAN interface.
Time Zone	1. A Must-filled item. 2. **GMT+00 :00** is selected by default.	Select a time zone where this device locates.
NTP Service	1. It is an optional item. 2. Un-checked by default	Check the **Enable** button to activate the NTP Service function. When you enabled this function, the gateway can provide NTP server service for its local connected devices.
Synchronize immediately	N/A	Click the **Active** button to synchronize the system time with specified time server immediately.
Save	N/A	Click the **Save** button to save the settings.
Refresh	N/A	Click the **Refresh** button to update the system time immediately.

Outdoor WiFi LoRa BSU

Synchronize with GPS Time Service

Item	Setting
▸ Synchronization method	GPS Signal ▾
▸ Time Zone	(GMT+00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▾
▸ NTP Service	☐ Enable
▸ Synchronize immediately	Active

System Time Information		
Item	**Value Setting**	**Description**
Synchronization method	1. A Must-filled item. 2. **Time Server** is selected by default.	Select **GPS Signal** as the synchronization method for the system time to let system synchronize its date and time to the time provided from the GNSS service. Note: this option is only available for the product with GNSS interface.
Time Zone	1. A Must-filled item. 2. **GMT+00 :00** is selected by default.	Select a time zone where this device locates.
NTP Service	1. It is an optional item. 2. Un-checked by default	Check the **Enable** button to activate the NTP Service function. When you enabled this function, the gateway can provide NTP server service for its local connected devices.
Synchronize immediately	N/A	Click the **Active** button to synchronize the system time with specified time server immediately.
Save	N/A	Click the **Save** button to save the settings.
Refresh	N/A	Click the **Refresh** button to update the system time immediately.

Outdoor WiFi LoRa BSU

6.2.4 System Log

System Log screen contains various event log tools facilitating network administrator to perform local event logging and remote reporting.

Go to **Administration > System Operation > System Log** tab.

View & Email Log History

View button is provided for network administrator to view log history on the gateway. **Email Now** button enables administrator to send instant Email for analysis.

View & Email Log History		
Item	**Value setting**	**Description**
View button	N/A	Click the **View** button to view Log History in Web Log List Window.
Email Now button	N/A	Click the **Email Now** button to send Log History via Email instantly.

Outdoor WiFi LoRa BSU

Time	Log
Apr 1 06:01:36	dnsmasq-dhcp[6016]: Ignoring domain amit.com.tw for DHCP host name NB-msnb
Apr 1 06:08:31	dnsmasq-dhcp[6016]: Ignoring domain amit.com.tw for DHCP host name NB-msnb
Apr 1 06:15:30	dnsmasq-dhcp[6016]: Ignoring domain amit.com.tw for DHCP host name NB-msnb
Apr 1 06:22:06	dnsmasq-dhcp[6016]: Ignoring domain amit.com.tw for DHCP host name NB-msnb
Apr 1 06:28:42	dnsmasq-dhcp[6016]: Ignoring domain amit.com.tw for DHCP host name NB-msnb
Apr 1 06:35:42	dnsmasq-dhcp[6016]: Ignoring domain amit.com.tw for DHCP host name NB-msnb
Apr 1 06:42:20	dnsmasq-dhcp[6016]: Ignoring domain amit.com.tw for DHCP host name NB-msnb

Web Log List Window		
Item	**Value Setting**	**Description**
Time column	N/A	It displays event time stamps
Log column	N/A	It displays Log messages

Web Log List Button Description		
Item	**Value setting**	**Description**
Previous	N/A	Click the **Previous** button to move to the previous page.
Next	N/A	Click the **Next** button to move to the next page.
First	N/A	Click the **First** button to jump to the first page.
Last	N/A	Click the **Last** button to jump to the last page.
Download	N/A	Click the **Download** button to download log to your PC in tar file format.
Clear	N/A	Click the **Clear** button to clear all log.
Back	N/A	Click the **Back** button to return to the previous page.

Web Log Type Category

Web Log Type Category screen allows network administrator to select the type of events to log and be displayed in the Web Log List Window as described in the previous section. Click on the View button to view Log History in the Web Log List window.

▸ Web Log Type Category   ☑ System ☑ Attacks ☑ Drop ☑ Login message ☐ Debug

Web Log Type Category Setting Window		
Item	**Value Setting**	**Description**
System	Checked by default	Check to log system events and to display in the Web Log List window.
Attacks	Checked by default	Check to log attack events and to display in the Web Log List window.
Drop	Checked by default	Check to log packet drop events and to display in the Web Log List window.
Login message	Checked by default	Check to log system login events and to display in the Web Log List window.

Debug	Un-checked by default	Check to log debug events and to display in the Web Log List window.

Email Alert

Email Alert screen allows network administrator to select the type of event to log and be sent to the destined Email account.

Email Alert Setting Window		
Item	**Value Setting**	**Description**
Enable	Un-checked by default	Check **Enable** box to enable sending event log messages to destined Email account defined in the E-mail Addresses blank space.
Server	N/A	Select one email server from the Server dropdown box to send Email. If none has been available, click the **Add Object** button to create an outgoing Email server. You may also add an outgoing Email server from Object Definition > External Server > External Server tab.
E-mail address	String : email format	Enter the recipient's Email address. Separate Email addresses with comma ',' or semicolon ' ;' Enter the Email address in the format of '*myemail@domain.com*'
Subject	String : any text	Enter an Email subject that is easy for you to identify on the Email client.
Log type category	Default unchecked	Select the type of events to log and be sent to the designated Email account. Available events are System, Attacks, Drop, Login message, and Debug.

Outdoor WiFi LoRa BSU

Syslogd

Syslogd screen allows network administrator to select the type of event to log and be sent to the designated Syslog server.

Syslogd	☐ Enable Server: --- Option --- ▼ Add Object
	Log type Category: ☐ System ☐ Attacks ☐ Drop ☐ Login message ☐ Debug

Syslogd Setting Window		
Item	**Value Setting**	**Description**
Enable	Un-checked by default	Check Enable box to activate the Syslogd function, and send event logs to a syslog server
Server	N/A	Select one syslog server from the Server dropdown box to sent event log to. If none has been available, click the **Add Object** button to create a system log server. You may also add an system log server from the Object Definition > External Server > External Server tab.
Log type category	Un-checked by default	Select the type of event to log and be sent to the destined syslog server. Available events are System, Attacks, Drop, Login message, and Debug.

Log to Storage

Log to Storage screen allows network administrator to select the type of events to log and be stored at an internal or an external storage.

Log to Storage	☑ Enable
	Select Device: Internal ▼
	Log file name: syslog
	Split file: ☐ Enable Size: 200 KB ▼
	Interval: ☐ Enable 1440 (1 ~ 10080 Minutes)
	Max Records: 3000 (5~10000)
	Download log file clear logs
	Log type Category: ☑ System ☑ Attacks ☑ Drop ☑ Login message ☑ Debug

Log to Storage Setting Window		
Item	**Value Setting**	**Description**
Enable	Un-checked by default	Check to enable sending log to storage.
Select Device	Internal is selected by default	Select internal or external storage.
Log file name	Un-checked by default	Enter log file name to save logs in designated storage.
Split file Enable	Un-checked by default	Check **enable** box to split file whenever log file reaching the specified limit.
Split file Size	**200 KB** is set by default	Enter the file size limit for each split log file. *Value Range*: 10 ~ 1000.
Interval Enable	Un-checked by default	Check **enable** box to enable the log interval setting.
Log Interval	**1440** is set by default	Enter the log interval setting. *Value Range*: 1 ~ 10080 Minute.
Max Records	**3000** is set by default	Enter the maximum number of records to be stored in the log storage. *Value Range*: 5 ~ 10000.
Log type category	Un-checked by default	Check which type of logs to send: System, Attacks, Drop, Login message, Debug

Log to Storage Button Description		
Item	**Value setting**	**Description**
Download log file	N/A	Click the **Download log file** button to download log files to a log.tar file.
Clear Logs	N/A	Click the **Clear logs** button to delete the log files from the storage.

6.2.5 Backup & Restore

In the Backup & Restore window, you can upgrade the device firmware when new firmware is available and also backup / restore the device configuration.

In addition to the factory default settings, you can also customize a special configuration setting as a customized default value. With this customized default value, you can reset the device to the expected default setting if needed.

Go to **Administration > System Operation > Backup & Restore** tab.

Item	Setting
▶ FW Upgrade	Via Web UI ▾ [FW Upgrade]
▶ Backup Configuration Settings	Download ▾ [Via Web UI]
▶ Auto Restore Configuration	☐ Enable [Save Conf.] [Clean Conf.] [Conf. Info.]
▶ Self-defined Logo	Download ▾ [Via Web UI] [Reset]
▶ Self-defined CSS	[Edit] : Download ▾ [Via Web UI] [Reset]

FW Backup & Restore		
Item	**Value Setting**	**Description**
FW Upgrade	**Via Web UI** is selected by default	If new firmware is available, click the **FW Upgrade** button to upgrade the device firmware **via Web UI**, or **Via Storage**. After clicking on the "FW Upgrade" command button, you need to specify the file name of new firmware by using "Browse" button, and then click "Upgrade" button to start the FW upgrading process on this device. If you want to upgrade a firmware which is from GPL policy, please check "Accept unofficial firmware"
Backup Configuration Settings	**Download** is selected by default	You can backup or restore the device configuration settings by clicking the *Via Web UI* button. **Download**: for backup the device configuration to a config.bin file. **Upload**: for restore a designated configuration file to the device. **Via Web UI**: to retrieve the configuration file via Web GUI.
Auto Restore Configuration	The **Enable** box is unchecked by default	Chick the **Enable** button to activate the customized default setting function. Once the function is activated, you can save the expected setting as a customized default setting by clicking the **Save Conf.** button, or clicking the **Clean Conf.** button to erase the stored customized configuration.

6.2.6 Reboot & Reset

For some special reason or situation, you may need to reboot the gateway or reset the device configuration to its default value. In addition to perform these operations through the Power ON/OFF, or pressing the reset button on the device panel, you can do it through the web GUI too.

Go to **Administration > System Operation > Reboot & Reset** tab.

In the Reboot & Reset window, you can reboot this device by clicking the "Reboot" button, and reset this device to default settings by clicking the "Reset" button.

System Operation	
Item	**Setting**
▸ Reboot	Now ▾ [Reboot]
▸ Reset to Default	[Reset]

System Operation Window		
Item	**Value Setting**	**Description**
Reboot	**Now** is selected by default	Chick the **Reboot** button to reboot the gateway immediately or on a pre-defined time schedule. **Now**: Reboot immediately **Time Schedule**: Select a pre-defined auto-reboot time schedule rule to reboot the auto device on a designated tim. To define a time schedule rule, go to **Object Definition > Scheduling > Configuration** tab.
Reset to Default	N/A	Click the **Reset** button to reset the device configuration to its default value.

6.3 FTP

The File Transfer Protocol (FTP) is a standard network protocol used to transfer computer files between a client and server on a computer network. FTP is built on a client-server model architecture and uses separate control and data connections between the client and the server. FTP users may authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it.

For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS). Besides, SSH File Transfer Protocol (SFTP) is sometimes also used instead, but is technologically different.

This gateway embedded FTP / SFTP server for administrator to download the log files to his computer or database. In the following two sections, you can configure the FTP server and create the user accounts that can login to the server. After login to the FTP server, you can browse the log directory and have the permission to download the stored log files and delete the files you have downloaded to make more storage space for further data logs.

The available log files can be system logs (refer to Administration > System Operation > System Log), Network Packets (refer to Administrator > Diagnostic > Packet Analyzer), Data Log (refer to Field Communication > Data Logging > Log File Management), and GNSS Log (refer to Service > Location Tracking > GNSS). With proper configuration for the various log functions that supported on your purchased product, you can download the log via FTP / SFTP connections.
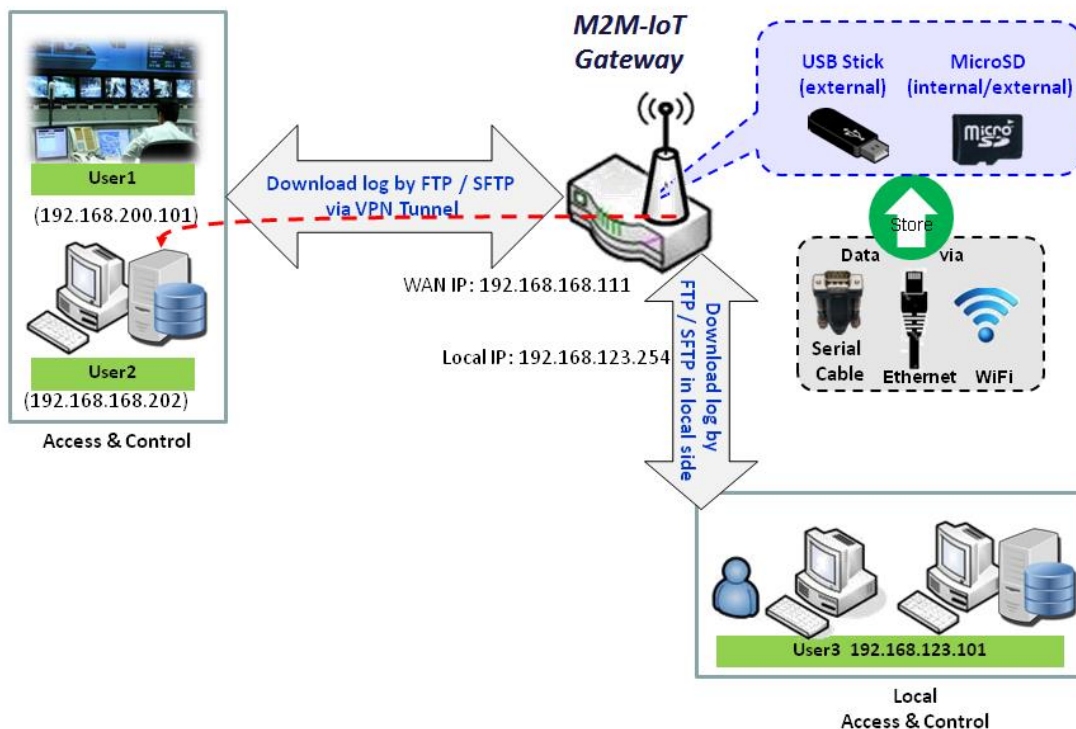
Outdoor WiFi LoRa BSU

6.3.1 Server Configuration

This section allows user to setup the embedded FTP and SFTP server for retrieving the interested log files.

Go to **Administration > FTP > Server Configuration** tab.

Enable FTP Server

Configuration Item	Value setting	Description
FTP	The box is unchecked by default.	Check **Enable** box to activate the embedded FTP Server function. With the FTP Server enabled, you can retrieve or delete the stored log files via FTP connection. **Note**: The embedded FTP Server is only for log downloading, so no any write permission is implemented for user file upload to the storage.
FTP Port	Port **21** is set by default	Specify a port number for FTP connection. The gateway will listen for incoming FTP connections on the specified port. *Value Range*: 1 ~ 65535.
Timeout	**300** seconds is set by default.	Specify the maximum timeout interval for the FTP connection. Supported range is 60 to 7200 seconds.
Max. Connections per IP	**2** Clients are set by default.	Specify the maximum number of clients from the same IP address for the FTP connection. Up to 5 clients from the same IP address is supported.
Max. FTP Clients	**5** Clients are set by default.	Specify the maximum number of clients for the FTP connection. Up to 32 clients is supported.
PASV Mode	Optional setting	Check the **Enable** box to activate the support of PASV mode for a FTP

		connection from FTP clients.
Port Range of PASV Mode	Port **50000** ~ **50031** is set by default.	Specify the port range to allocate for PASV style data connection. ***Value Range***: 1024 ~ 65535.
Auto Report External IP in PASV Mode	Optional setting	Check the **Enable** box to activate the support of overriding the IP address advertising in response to the PASV command.
ASCII Transfer Mode	Optional setting	Check the **Enable** box to activate the support of ASCII mode data transfers. Binary mode is supported by default.
FTPS (FTP over SSL/TLS)	Optional setting	Check the **Enable** box to activate the support of secure connections via SSL/TLS.

Enable SFTP Server

Configuration Item	Value setting	Description
SFTP	The box is unchecked by default.	Check **Enable** box to activate the embedded SFTP Server function. Furthermore, you can check the granted interface(s) for the SFTP connection, via **LAN**, **WAN**, or both. Besides, if any WAN interface is selected, you can further limit the hosts that can access to the WAN port via SFTP. The available options are: **any**, **Specific IP Address**, or **IP Range**. With the SFTP Server enabled, you can retrieve or delete the stored log files via secure SFTP connection.
SFTP Port	Default 22	Specify a port number for SFTP connection. The gateway will listen for incoming SFTP connections on the specified port. ***Value Range***: 1 ~ 65535.

6.3.2 User Account

This section allows user to setup user accounts for logging to the embedded FTP and SFTP server to retrieve the interested fog files.

Go to **Administration > FTP > User Account** tab.

Create/Edit FTP User Accounts

When **Add** button is applied, **User Account Configuration screen** will appear.

Configuration Item	Value setting	Description
User Name	String : non-blank string	Enter the user account for login to the FTP server. **_Value Range_**: 1 ~ 15 characters.
Password	String : no blank	Enter the user password for login to the FTP server.
Directory	N/A	Select a root directory after user login.
Permission	**Read/Write** is selected by default.	Select the Read/write permission. Note: The embedded FTP Server is only for log downloading, so no any write permission is implemented for user file upload to the storage, even **Read/Write** option is selected.
Enable	The box is checked by default.	Check the box to activate the FTP user account.

6.4 Diagnostic

This gateway supports simple network diagnosis tools for the administrator to troubleshoot and find the root cause of the abnormal behavior or traffics passing through the gateway. There can be a Packet Analyzer to help record the packets for a designated interface or specific source/destination host, and another Ping and Tracert tools for testing the network connectivity issues.

6.4.1 Diagnostic Tools

The Diagnostic Tools provide some frequently used network connectivity diagnostic tools (approaches) for the network administrator to check the device connectivity.

Go to **Administration > Diagnostic > Diagnostic Tools** tab.

Diagnostic Tools		
Item	**Value setting**	**Description**
Ping Test	Optional Setting	This allows you to specify an IP / FQDN, the Outer interface (auto, WAN, LAN, or VLAN), and LAN source (default, LAN, or VLAN) as well, so system will try to ping the specified device to test whether it is alive after clicking on the **Ping** button. A test result window will appear beneath it.
Tracert Test	Optional setting	Trace route (tracert) command is a network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an IP network. Trace route proceeds until all (three) sent packets are lost for more than twice, then the connection is lost and the route cannot be evaluated. First, you need to specify an IP / FQDN, the test interface (LAN, WAN, or Auto) and the protocol (UDP or ICMP), and by default, it is **UDP**. Then, system will try to trace the specified host to test whether it is alive after clicking on **Tracert** button. A test result window will appear beneath it.
Speed Test	Optional setting	This allows you to do a quick speed test for verifying the connectivity on specific interface.
Wake on LAN	Optional setting	Wake on LAN (WOL) is an Ethernet networking standard that allows a computer to be turned on or awakened by a network message. You can

		specify the MAC address of the computer, in your LAN network, to be remotely turned on by clicking on the **Wake up** command button.
Save	N/A	Click the **Save** button to save the configuration.

Outdoor WiFi LoRa BSU

6.4.2 Packet Analyzer

The Packet Analyzer can capture packets depend on user settings. User can specify interfaces to capture packets and filter by setting rule. Ensure the log storage is available (either embedded SD-Card or external USB Storage), otherwise **Packet Analyzer** cannot be enabled.

Go to **Administration > Diagnostic > Packet Analyzer** tab.

Configuration		
Item	**Value setting**	**Description**
Packet Analyzer	The box is unchecked by default.	Check **Enable** box to activate the Packet Analyzer function. If you cannot enable the checkbox, please check if the storage is available or not. Plug in the USB storage and then enable the Package Analyzer function.
File Name	1. An optional setting 2. Blank is set by default, and the default file name is **<Interface>_<Date>_<index>**.	Enter the file name to save the captured packets in log storage. If **Split Files** option is also enabled, the file name will be appended with an index code "**_<index>**". The extension file name is **.pcap**.
Split Files	1. An optional setting 2. The default value of **File Size** is 200 KB.	Check **enable** box to split file whenever log file reaching the specified limit. If the **Split Files** option is enabled, you can further specify the **File Size** and **Unit** for the split files. *Value Range*: 10 ~ 99999. NOTE: **File Size** cannot be less than 10 KB
Packet Interfaces	An optional setting	Define the interface(s) that **Packet Analyzer** should work on. At least, one interface is required, but multiple selections are also accepted. The supported interfaces can be: ● **WAN**: When the WAN is enabled at **Physical Interface**, it can be selected here. ● **ASY**: This means the serial communication interface. It is used to capture packets appearing in the **Field Communication**.

		Therefore, it can only be selected when specific field communication protocol, like Modbus, is enabled. Select **Binary mode** or **String mode** for the serial interface. ● **VAP**: This means the virtual AP. When WiFi and VAP are enabled, it can be selected here.
Save	N/A	Click the **Save** button to save the configuration.
Undo	N/A	Click the **Undo** button to restore what you just configured back to the previous setting.

Once you enabled the Packet Analyzer function on specific Interface(s), you can further specify some filter rules to capture the packets which matched the rules.

Capture Fitters		
Item	**Value setting**	**Description**
Filter	Optional setting	Check **Enable** box to activate the Capture Filter function.
Source MACs	Optional setting	Define the filter rule with **Source MACs**, which means the source MAC address of packets. Packets which match the rule will be captured. Up to 10 MACs are supported, but they must be separated with "**;**", e.g. AA:BB:CC:DD:EE:FF; 11:22:33:44:55:66 The packets will be captured when match any one MAC in the rule.
Source IPs	Optional setting	Define the filter rule with **Source IPs**, which means the source IP address of packets.

		Packets which match the rule will be captured. Up to 10 IPs are supported, but they must be separated with "**;**", e.g. 192.168.1.1; 192.168.1.2 The packets will be captured when match any one IP in the rule.
Source Ports	Optional setting	Define the filter rule with **Source Ports**, which means the source port of packets. The packets will be captured when match any port in the rule. Up to 10 ports are supported, but they must be separated with "**;**", e.g. 80; 53 ***Value Range*: 1 ~ 65535.**
Destination MACs	Optional setting	Define the filter rule with **Destination MACs**, which means the destination MAC address of packets. Packets which match the rule will be captured. Up to 10 MACs are supported, but they must be separated with "**;**", e.g. AA:BB:CC:DD:EE:FF; 11:22:33:44:55:66 The packets will be captured when match any one MAC in the rule.
Destination IPs	Optional setting	Define the filter rule with **Destination IPs**, which means the destination IP address of packets. Packets which match the rule will be captured. Up to 10 IPs are supported, but they must be separated with "**;**", e.g. 192.168.1.1; 192.168.1.2 The packets will be captured when match any one IP in the rule.
Destination Ports	Optional setting	Define the filter rule with **Destination Ports**, which means the destination port of packets. The packets will be captured when match any port in the rule. Up to 10 ports are supported, but they must be separated with "**;**", e.g. 80; 53 ***Value Range*: 1 ~ 65535.**

Chapter 7 Service

7.1 Cellular Toolkit (not supported)

Not supported feature for the purchased product, leave it as blank.

Outdoor WiFi LoRa BSU

7.2 Event Handling

Event handling is the application that allows administrator to setup the pre-defined events, handlers, or response behavior with individual profiles. With properly configuring the event handling function, administrator can easily and remotely obtain the status and information via the purchased gateway. Moreover, he can also handle and manage some important system related functions, even the field bus devices and D/O devices which are already well connected to.

The supported events are categorized into two groups: the **managing events** and **notifying events**.

The **managing events** are the events that are used to manage the gateway or change the setting / status of the specific functionality of the gateway. On receiving the managing event, the gateway will take action to change the functionality, collect the required status for administration, and also change the status of a certain connected field bus device simultaneously.

The **notifying events** are the events that some related objects have been triggered and take corresponding actions on the occurrence of the events. It could be an event generated from the connected sensor, or a certain connected field bus device for alerting the administrator something happened with Email, and SNMP Trap, etc...
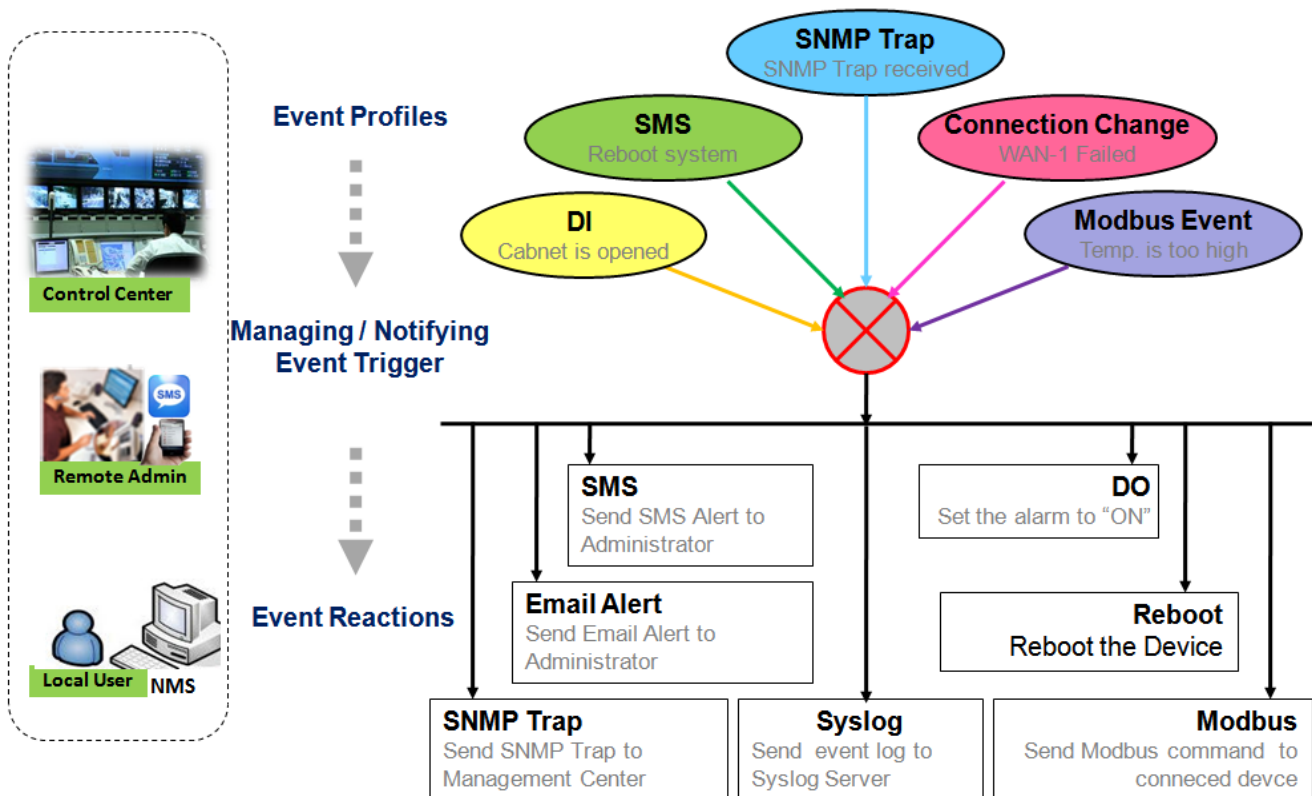
For ease of configuration, administrator can create and edit the common pre-defined managing / notifying event profiles for taking instant reaction on a certain event or managing the devices for some advanced useful purposes. For example, sending/receiving the field bus device status monitoring, digital sensors detection

controlling, and so on. All of such management and notification function can be realized effectively via the Event Handling feature.

The following is the summary lists for the provided profiles, and events:

(**Note**: The available profiles and events could be different for the purchased product.)

● Profiles (Rules):
  • Email Accounts
  • Digital Input (DI) profiles
  • Digital Output (DO) profiles
  • Modbus Managing Event profiles
  • Modbus Notifying Event profiles
  • Remote Host profiles

● Managing Events:
  • Trigger Type: SNMP Trap, and Digital Input (DI).
  • Actions: Get the Network Status; or Configure the LAN/VLAN behavior, WIFI behavior, NAT behavior, Firewall behavior, VPN behavior, System Management, Administration, Digital Output behavior, connected Modbus devices, and Remote Host.

● Notifying Events:
  • Trigger Type: Digital Input, Power Change, Connection Change (WAN, LAN & VLAN, WiFi, DDNS), Administration, Modbus, and Data Usage.
  • Actions: Notify the administrator with Syslog, SNMP Trap or Email Alert; Change the status of connected Digital Output or Modbus devices; Sending collected information to Remote Host.

To use the event handling function, First of all, you have to enable the event management setting and configure the event details with the provided profile settings. You can create or edit pre-defined profiles for individual managing / notifying events. The profile settings are separated into several items; they are the Email Service Definition, Digital Input (DI) Profile Configuration, Digital Output (DO) Profile Configuration, Modbus Definition, and Remote Host Configuration.

Then, you have to configure each managing / notifying event with identifying the event's trigger condition, and the corresponding actions (reaction for the event) for the event. For each event, more than one action can be activated simultaneously.

Outdoor WiFi LoRa BSU

7.2.1 Configuration

Go to **Service** > **Event Handling** > **Configuration** Tab.

Event handling is the service that allows administrator to setup the pre-defined events, handlers, or response behavior with individual profiles.

Create / Edit Email Service Account

Setup the Email Service Account for event notification. It supports up to a maximum of 5 accounts.

ID	Email Server	Email Addresses	Enable	Actions

You can click the **Add / Edit** button to configure the Email account.

Email Service Configuration

Item	Setting
▶ Email Server	--- Option --- ▼
▶ Email Addresses	
▶ Enable	☑ Enable
	Save

Email Service Configuration		
Item	**Value setting**	**Description**
Email Server	--- Option ---	Select an Email Server profile from **External Server** setting for the email account setting.
Email Addresses	1. Internet E-mail address format 2. A Must filled setting	Specify the Destination Email Addresses.
Enable	The box is unchecked by default.	Click **Enable** box to activate this account.
Save	NA	Click the **Save** button to save the configuration

Outdoor WiFi LoRa BSU

Create / Edit Remote Host Profile

Setup the Remote Host Profile. It supports up to a maximum of 10 profiles.

ID	Host Name	Host IP	Protocol Type	Port Number	Prefix Message	Suffix Message	Enable	Actions

You can click the **Add / Edit** button to configure the profile.

Item	Setting
▸ Host Name	
▸ Host IP	
▸ Protocol Type	TCP ▾
▸ Port Number	
▸ Prefix Message	
▸ Suffix Message	
▸ Enable	☐

Save

Remote Host Configuration		
Item	**Value setting**	**Description**
Host Name	1. String format 2. A Must filled setting	Specify the Remote Host profile name. **Value Range**: -1 ~ 64 characters.
Host IP	1. A Must filled setting 2.IP Address format.	Specify the IP address for the Remote Host. IPv4 Format.
Protocol Type	1. A Must filled setting 2. **TCP** is selected by default	Specify the protocol to access the Remote Host. It could be **TCP or UDP**.
Port Number	1. A Must filled setting	Specify the Port number for accessing the Remote Host. **Value Range**: 1 ~ 65535.
Prefix Message	1. String format 2. An Optional filled setting	Specify the Prefix Message string as pre-defined identification for accessing the remote host, if required. **Value Range**: -1 ~ 64 characters.
Suffix Message	1. String format 2. An Optional filled setting	Specify the Suffix Message string as pre-defined identification for accessing the remote host, if required. **Value Range**: -1 ~ 64 characters.
Enable	The box is unchecked by default.	Click **Enable** box to activate this profile setting.
Save	NA	Click the **Save** button to save the configuration
Undo	NA	Click the **Undo** button to restore what you just configured back to the previous setting.

7.2.2 Managing Events

Managing Events allow administrator to define the relationship (rule) among event trigger, handlers and response.

Go to **Service** > **Event Handling** > **Managing Events** Tab.

Enable Managing Events

Item	Setting
▸ Managing Events	☐ Enable

Configuration		
Item	**Value setting**	**Description**
Managing Events	The box is unchecked by default	Check the **Enable** box to activate the Managing Events function.

Create / Edit Managing Event Rules

Setup the Managing Event rules. It supports up to a maximum of 128 rules.

ID	Event Name	Event	Trigger Type	Description	Enable	Actions

When **Add** or **Edit** button is applied, the **Managing Event Configuration** screen will appear.

Outdoor WiFi LoRa BSU

Item	Setting
▶ Event Name	[ ]
▶ Event	None ▼ None ▼ None ▼
▶ Trigger Type	Period ▼
▶ Interval	0 (0~86400 seconds)
▶ Description	[ ]
▶ Action	☐ Network Status ☐ LAN&VLAN ☐ WiFi ☐ NAT ☐ Firewall ☐ VPN ☐ System Manage ☐ Administration ☐ Digital Output ☐ Modbus ☐ Remote Host
▶ Managing Event	☑ Enable

Save

Managing Event Configuration		
Item	**Value setting**	**Description**
Event	**None** by default	Specify the Event type (**SNMP Trap**, or **Digital Input**) and an event identifier / profile. Up to 3 event conditions can be specified for defining an event, and the event will be triggered when all the conditions hold simutaneously (AND relation). The supported Event types could be: **SNMP**: Select **SNMP Trap** and fill the message in the textbox to specify SNMP Trap condition; **Digital Input**: Select **Digital Input** and a DI profile you defined to specify a certain Digital Input condition; *Note: The available Event types could be different for the purchased product.*
Trigger Type	**Period** is selected by default	Specify the type of event trigger, either **Period** or **Once**. **Period**: Select **Period** and specify a time interval, the event will be repeatedly triggered on every time interval when the specified event condition holds. **Once**: Select **Once** and the event will be just triggered just one time when the specified event condition holds.
Interval	**0** is set by default	Specify the repeatedly event trigger time interval. ***Value Range***: 0 ~86400 seconds.
Description	String format : any text.	Enter a brief description for the Managing Event.

Action	All box is unchecked by default.	Specify **Network Status**, or at least one rest action to take when the expected event is triggered. **Network Status**: Select **Network Status** Checkbox to get the network status as the action for the event; **LAN&VLAN**: Select **LAN&VLAN** Checkbox and the interested sub-items (Port link On/Off), the gateway will change the settings as the action for the event; **WiFi**: Select **WiFi** Checkbox and the interested sub-items (WiFi radio On/Off), the gateway will change the settings as the action for the event; **NAT**: Select **NAT** Checkbox and the interested sub-items (Virtual Server Rule On/Off, DMZ On/Off), the gateway will change the settings as the action for the event; **Firewall**: Select **Firewall** Checkbox and the interested sub-items (Remote Administrator Host ID On/Off), the gateway will change the settings as the action for the event; **VPN**: Select **VPN** Checkbox and the interested sub-items (IPSec Tunnel ON/Off, PPTP Client On/Off, L2TP Client On/Off, OpenVPN Client On/Off), the gateway will change the settings as the action for the event; **GRE**: Select **GRE** Checkbox and the interested sub-items (GRE Tunnel On/Off), the gateway will change the settings as the action for the event; **System Manage**: Select **System Manage** Checkbox and the interested sub-items (WAN SSH Service On/Off, TR-069 On/Off), the gateway will change the settings as the action for the event; **Administration**: Select **Administration** Checkbox and the interested sub-items (Backup Config, Restore Config, Reboot, Save Current Setting as Default), the gateway will change the settings as the action for the event; **Digital Output**: Select **Digital Output** checkbox and a DO profile you defined as the action for the event; **Modbus**: Select **Modbus** checkbox and a Modbus Managing Event profile you defined as the action for the event; **Remote Host**: Select **Remote Host** checkbox and a Remote Host profile you defined as the action for the event; *Note: The available Event Type could be different for the purchased product.*
Managing Event	The box is unchecked by default.	Click **Enable** box to activate this Managing Event setting.
Save	*NA*	Click the **Save** button to save the configuration
Undo	*NA*	Click the **Undo** button to restore what you just configured back to the previous setting.

Outdoor WiFi LoRa BSU

7.2.3 Notifying Events

Go to **Service** > **Event Handling** > **Notifying Events** Tab.

Notifying Events Setting allows administrator to define the relationship (rule) between event trigger and handlers.

Enable Notifying Events

Item	Setting
▸ Notifying Events	☐ Enable

Configuration		
Item	**Value setting**	**Description**
Notifying Events	The box is unchecked by default	Check the **Enable** box to activate the Notifying Events function.

Create / Edit Notifying Event Rules

Setup your Notifying Event rules. It supports up to a maximum of 128 rules.

ID	Event Name	Event	Trigger Type	Description	Action	Time Schedule	Enable	Actions

When **Add** or **Edit** button is applied, the **Notifying Event Configuration** screen will appear.

Item	Setting
▸ Event Name	
▸ Event	None ▾ and None ▾ and None ▾
▸ Trigger Type	Period ▾
▸ Interval	0 (0~86400 seconds)
▸ Description	

Delay to send	[ ] (0~3600 seconds)
▸ Action	☐ Syslog ☐ SNMP Trap (Only Support v1 and v2c) ☐ Email Alert ☐ Remote Host ☐ System
▸ Time Schedule	(0) Always ▾
▸ Notifying Events	☑ Enable

Notifying Event Configuration		
Item	**Value setting**	**Description**
Event	**None** by default	Specify the Event type and an event identifier / profile. Up to 3 event conditions can be specified for defining an event, and the event will be triggered when all the conditions hold simutaneously (AND relation). The supported Event types could be: **WAN**: Select **WAN** and a trigger condition to specify a certain WAN Event; **LAN&VLAN**: Select **LAN&VLAN** and a trigger condition to specify a certain LAN&VLAN Event; **WiFi**: Select **WiFi** and a trigger condition to specify a certain WiFi Event; **DDNS**: Select **DDNS** and a trigger condition to specify a certain DDNS Event; **Administration**: Select **Administration** and a trigger condition to specify a certain Administration Event; **Remote Host**: Select **Remote Host** checkbox and a Remote Host profile you defined as the action for the event; *Note: The available Event types could be different for the purchased product.*
Trigger Type	**Period** is selected by default	Specify the type of event trigger, either **Period** or **Once**. **Period**: Select **Period** and specify a time interval, the event will be repeatedly triggered on every time interval when the specified event condition holds. **Once**: Select **Once** and the event will be just triggered just one time when the specified event condition holds.
Interval	**0** is set by default	Specify the repeatedly event trigger time interval. *Value Range*: 0 ~86400 seconds.
Description	String format : any text.	Enter a brief description for the Notifying Event.
Delay to Send	**Blank** by default	Specify a delay time, if required, to send out the notifying event once it had been triggered. *Value Range*: 0 ~3600 seconds.
Action	All box is unchecked by default.	Specify at least one action to take when the expected event is triggered. **Syslog**: Select **Syslog** and select/unselect the Enable Checkbox to as the action for the event; **SNMP Trap**: Select **SNMP Trap**, and the gateway will send out SNMP Trap to the defined SNMP Event Receivers as the action for the event; **Email Alert**: Select **Email Alert**, and the gateway will send out an Email to the defined Email accounts as the action for the event; **Remote Host**: Select **Remote Host** checkbox and a Remote Host profile you

		defined as the action for the event; **System**: Select **Reboot after 30 sec.** checkbox as the action for the event; *Note: The available Event Type could be different for the purchased product.*
Time Schedule	**(0) Always** is selected by default	Select a time scheduling rule for the Notifying Event.
Notifying Events	The box is unchecked by default.	Click **Enable** box to activate this Notifying Event setting.
Save	*NA*	Click the **Save** button to save the configuration
Undo	*NA*	Click the **Undo** button to restore what you just configured back to the previous setting.

7.3 LoRa

LoRa Technology

LoRa is a long range wireless data communication technology developed by Semtech. LoRa uses license-free sub-gigahertz radio frequency bands like 433 MHz, 868 MHz (Europe) and 915 MHz (North America). LoRa enables very-long-range transmissions (more than 10 km in rural areas) with low power consumption. The technology is presented in two parts — LoRa, the physical layer and LoRaWAN, the upper layers. [6]

Semtech builds LoRa Technology into its chipsets. These chipsets are then built into the commercial products, LoRa Gateway and LoRa Nodes, and integrated into LPWANs service by worldwide ISPs.

Application				
LoRaWAN MAC				
MAC options				
Class A		Class B		Class C
LoRa Modulation				
Regional ISM band				
EU 868	EU 433	US 915	AS 430	—

---

6 https://www.semtech.com/technology/lora/what-is-lora
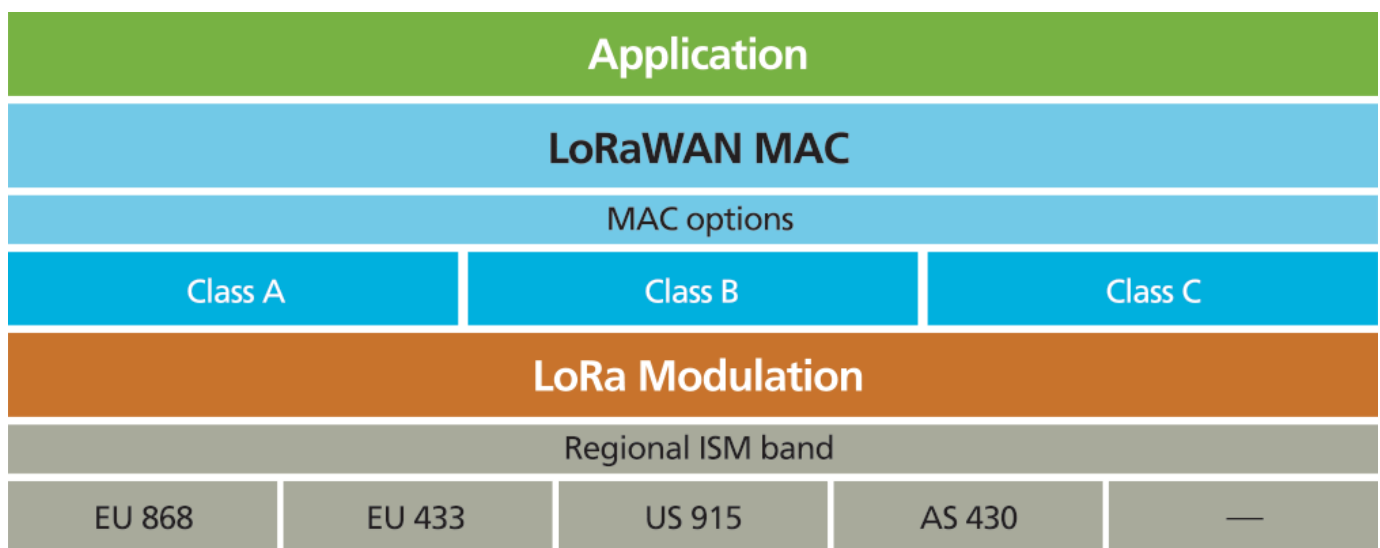
Outdoor WiFi LoRa BSU
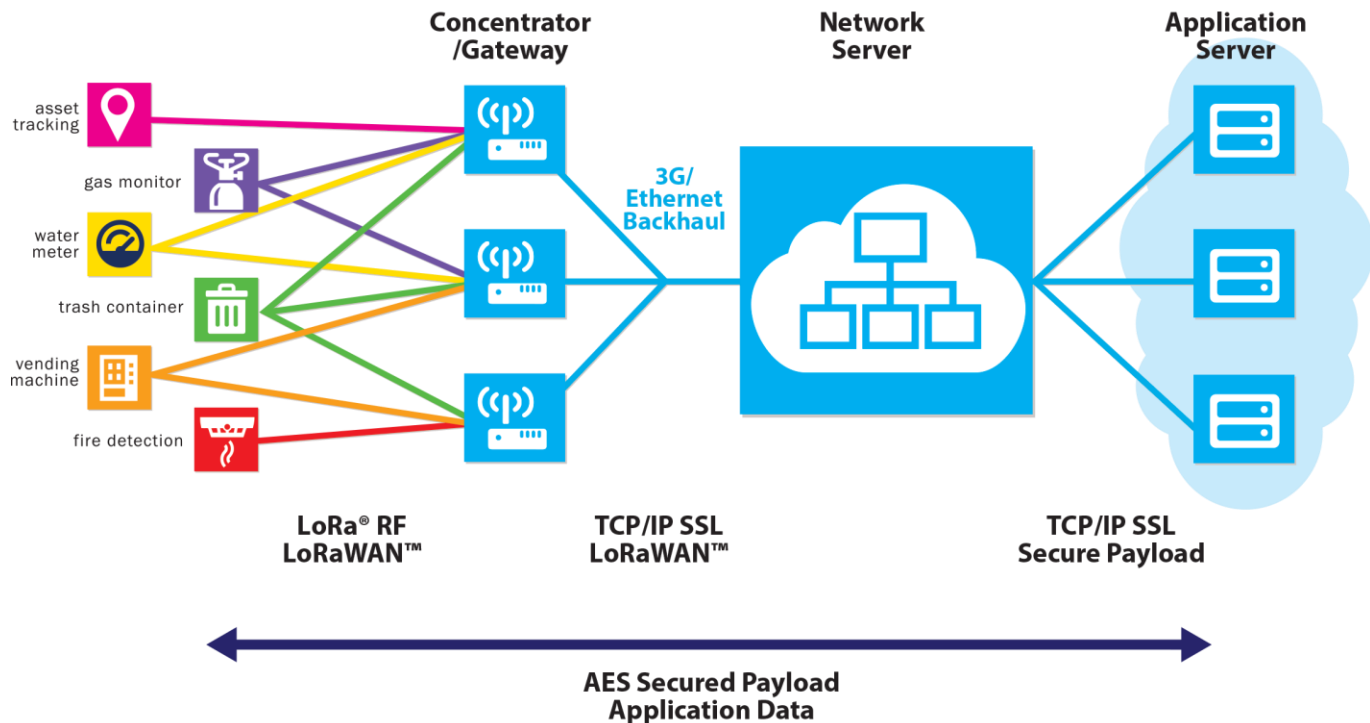
LoRaWAN Protocol

LoRaWAN is a protocol specification built on top of the LoRa technology developed by the LoRa Alliance. It uses unlicensed radio spectrum in the Industrial, Scientific and Medical (ISM) bands to enable low power, wide area communication between remote sensors and gateways connected to the network. This standard-based approach to building a LPWA network allows for quick set up of public or private IoT networks anywhere using hardware and software that is bi-directionally secure, interoperable and mobile, provides accurate localization, and works the way you expect.

LoRaWAN defines the communication protocol and system architecture for the network, while the LoRa physical layer enables the long-range communication link. LoRaWAN is also responsible managing the communication frequencies, data rate, and power for all devices. Devices in the network are asynchronous and transmit when they have data available to send. Data transmitted by an end-node device is received by multiple gateways, which forward the data packets to a centralized network server. The network server filters duplicate packets, performs security checks, and manages the network. Data is then forwarded to application servers.

As depicted in the LoRaWAN network diagram, all the application data between the end nodes and application server are AES-encrypted. The LoRa gateway and network server are merely responsible for data forwarding and security checks, they know nothing about the encrypted data transferred.

Outdoor WiFi LoRa BSU

7.3.1 LoRa Gateway

This product is integrated with an 8-channel LoRa Gateway module. With some basic configuration and specified an accompanied network server, the LoRa Gateway can connect with surrounding LoRa Nodes and forward the received data to Network Server for further processing.

LoRa Gateway Setting

Go to **Service > LoRa > LoRa Gateway** Tab.

The LoRa Gateway setting page enables user to configure the embedded LoRa gateway, and allow packet forwarding from LoRa nodes to Network Server, or from Network Server to LoRa Nodes.

LoRa Configuration

LoRa Configuration		
Item	**Value setting**	**Description**
LoRa Gateway	The box is unchecked by default	Check **Enable** box to activate the LoRa Gateway function.
MultiSF Channel	Some channels are selected by default	Select the RF channels to be activated. The LoRa gateway supports up to 8 LoRa channels, defined in **Radio0** and **Radio1**, for connecting with LoRa Nodes. For each Radio, you can select one sub band (four channels covered) to operate. **EU868 Frequency Plan:** 8 Sub-Bands for 863.3~863.9 / 864.1~864.7 / 864.9~865.5 / 865.7~866.3 / 866.5~867.1 / 867.3~876.9 / 868.1~868.7 / 868.9~869.5 MHz; and **Radio 0** is fixed at Sub-Band(868.1~868.7) **US915 Frequency Plan:** 8 Sub-Bands for 902.3~903.7 / 903.9~905.3 / 905.5~906.9 / 907.1~908.5 / 908.7~910.1 / 910.3~911.7 /911.9~913.3 / 913.5~914.9 MHz **AS923 Frequency Plan:** 5 Sub-Bands for 920.2~921.0 / 921.2~922.0 /

		922.2~923.0 / 923.2~924.0 / 924.0~924.8 MHz **Note 1**: The supported operation band list is hardware dependent. It depends on the hardware version and regional regulation. **Note 2**: The bandwidth is fixed at 125KHz.
Gateway ID	String format: EUI-64 MAC-like string, with eight 2-digit hex. numbers	Enter an unique ID for the LoRa Gateway. It will be used for communicating with Network Server. Please enter the WAN MAC for the device, and followed with two extra numbers. For example, WAN MAC is 00:50:18:00:08:FE, then imput "*00:50:18:00: 08:FE:11:22*" as the Gateway ID.
Keep Alive Interval	1. AMust filled setting. 2. **10** is selected by default.	Specify the time **interval** (seconds) to keep the connection alive between network server and LoRa gateway even there is no LoRa traffic. ***Value Range***: 10 ~ 999 seconds
Save	*NA*	Click the **Save** button to save the configuration

7.3.2 LoRa Network Server

For the small scale or private applications, you don't want to use third party's public LoRaWAN network service (bind to a certain LoRa Network Server, Application Server) that is provided by local Telco or ISP. In such case, you will need a private network server for collecting all the data from your deployed LoRa nodes.

This product is integrated with a private LoRa Network Server, and also a simplified Application Server. It supports up to 200 LoRa Nodes. If you intend to use the embedded network server for your private application, you have to proceed with following LoRa Network Server settings.

After that, the collected data from your LoRa nodes is collected and stored in an embedded SQL database. You can access to it with the LAN IP and port 9999.

Note: To customize your application with the product for two-way communication with the Class C LoRa nodes, you may need to get further SDK from the gateway vendor to link with your own application or managing platform.

LoRa Network Server

Go to **Service > LoRa > LoRa Network Server** Tab.

The LoRa Network Server setting page enables user to configure the LoRa network server, and optionally register the LoRa nodes to the internal LoRa Network Server, when available, to get permissible access.

LoRa Network Server Configuration

LoRa Configuration		
Item	**Value setting**	**Description**
LoRa Network Server	The box is unchecked by default	Check **Enable** box to activate the embedded LoRa Network Server.
Server Port	A Must filled setting Port **1700** set by default	Specify a **Port Number** as destination port for sending packets. *Value Range*: 1 ~ 65535.

Outdoor WiFi LoRa BSU

LoRa Message Database	The box is unchecked by default	Check **Enable** box to activate the embedded LoRa Message Database. The database can keep up to 600,000 records from connected LoRa nodes. Once the records exceed the limit, half of the records will be deleted for recording further messages.
Internal / External	Default value depends on product spec.	Specify the type of LoRa network server to be connected. **External**: Select a thirty LoRa network server, provided by the LoRa Networking Service Provider, to process the packets to/from the LoRa gateway. When the External server is selected, you have to further select a pre-defined server profile from the dropdown list, or click the **Add Object** button to define the server information to the external LoRa Network Server. Refer to **Section 3.4 External Server** for the details. **Internal**: Select the internal LoRa network server, embedded with the LoRa Gateway device to process the packets to/from the LoRa gateway. **Note**: Depending on the purchase model, the supported interface type could be **Internal** or **External**. Some model just supports **External** network server.

Register LoRa Nodes

If you enabled the internal LoRa Network Server, you have to further register all the LoRa Nodes that you are going to deploy in you application sites. It supports up to 200 LoRa Nodes. For the data packets coming from un-registered LoRa nodes, it will be ignored accordingly.

If you are not familiar with the following terms or items required for registering your LoRa node, you can refer to a good article that can be foud in a Blog in NEWIE VENTURES web page[7].

You can maintain and see all the registered LoRa nodes in the LoRa Node list.

ID	Device Name	Device Class	Device Description	Activation method	Enable	Actions

When **Add** or **Edit** button is applied, the **LoRa Node Configuration** screen will appear.

---

7 https://www.newieventures.com.au/blogtext/2018/2/26/lorawan-otaa-or-abp

Outdoor WiFi LoRa BSU

LoRa Node Configuration		
Item	**Value setting**	**Description**
Device Name	A Must filled setting Blanked by default	Enter an unique name / identifier of the LoRa node being registered. Please enter the WAN MAC for the device, and followed with two extra numbers. *Value Range*: 1~16 aplhanumeric characters; '-' and '_' are valid characters.
Device Class	A Must filled setting Class **A** is selected by default	Specify the device type of the LoRa node being registered. Currently, Class **A** and Class **C** devices are supported.
Device Description	An Optional filled setting Blanked by default	Enter a brief description for the LoRa node be registered.
Activation Method	A Must filled setting **OTAA** is selected by default	Specify the activation method of the LoRa node being registered. **OTAA** (Over-the-Air Activation) and **ABP** (Activation by Personalization) are supported. **OTAA**: OTAA is the preferred and most secure way to connect with network server. Devices perform a join-procedure with the network server, during

		which a dynamic Device Address is assigned and security keys (Network Session Key, APP Session Key) are negotiated with the device. **ABP**: ABP is a simpler activation method with fixed device address and security keys. For some device, it is manufactured with a hardcode Device Address as well as the security keys in the device. This means it can't worked with OTAA method. This strategy might seem simpler, because you skip the join procedure.
Device EUI	A Must filled setting Blanked by default	Enter a unique Device EUI for the LoRa node being registered. The EUI is provided by the device manufacture. ***Value Range***: 16 hexadecimal characters (0~9, A~F)
Application EUI	A Must filled setting Blanked by default	Enter an identifier as the Application EUI for the application you are deploying with the LoRa nodes. For using the private LoRa Network Server, you can define your own Application EUI. ***Value Range***: 16 hexadecimal characters (0~9, A~F)
App Key	A Must filled setting for OTAA scheme	Enter an Application Key, if OTAA actication is selected, to generate required session keys while the LoRa node joins or re-joins to the network. For using the private LoRa Network Server, you can define your own Application Key. ***Value Range***: 32 hexadecimal characters (0~9, A~F)
Device Address	A Must filled setting for ABP scheme	Enter a unique device address for the LoRa node being registered. It is required for ABP activation scheme. ***Value Range***: 8 hexadecimal characters (0~9, A~F)
Network Session Key	A Must filled setting for ABP scheme	Enter a network session key for the LoRa node being registered. The Network Server will use this key to decrypt the meta data that is transmitted from the registered LoRa nodes. It is required for ABP activation scheme. ***Value Range***: 32 hexadecimal characters (0~9, A~F)
APP Session Key	A Must filled setting for ABP scheme	Enter an application session key for the LoRa node being registered. The Application Server will use this key to decrypt the packet payload that is transmitted from the registered LoRa nodes. It is required for ABP activation scheme. ***Value Range***: 32 hexadecimal characters (0~9, A~F)
Enable	Unchecked by default	Check the Enable box to activate the parameters of the LoRa node being registered.
Save	*NA*	Click the **Save** button to save the configuration

Register LoRa Group Nodes

To deploy hundreds of LoRa nodes, you can register the LoRa nodes as group of LoRa nodes instead of registering one by one.

You can maintain and see all the registered LoRa group nodes in the LoRa Group Node list.

Outdoor WiFi LoRa BSU

When **Add** or **Edit** button is applied, the **LoRa Group Node Configuration** screen will appear.

LoRa Group Node Configuration		
Item	**Value setting**	**Description**
Device Name	A Must filled setting Blanked by default	Enter an unique name / identifier of the LoRa group node being registered. ***Value Range***: 1~16 aplhanumeric characters.
Device Class	A Must filled setting Class **A** is selected by default	Specify the device type of the LoRa node being registered. Currently, Class **A** and Class **C** devices are supported.
Device Description	An Optional filled setting Blanked by default	Enter a brief description for the LoRa group node be registered.
Activation Method	A Must filled setting **OTAA** is selected by default	Specify the activation method of the LoRa node being registered. **OTAA** (Over-the-Air Activation) and **ABP** (Activation by Personalization) are supported. **OTAA**: OTAA is the preferred and most secure way to connect with network server. Devices perform a join-procedure with the network server, during which a dynamic Device Address is assigned and security keys (Network Session Key, APP Session Key) are negotiated with the device.

		ABP: ABP is a simpler activation method with fixed device address and security keys. For some device, it is manufactured with a hardcode Device Address as well as the security keys in the device. This means it can't worked with OTAA method. This strategy might seem simpler, because you skip the join procedure.
Device Address start / Device Address end	A Must filled setting Blanked by default	Specify a range of Device address, by entering the start and end address, for the LoRa group nodes. For example, 12340000 as the start address, and 1234FFFF as the end address. Any LoRa Node with Device address in this range will be regarded as a registered node. The address is provided by the device manufacture. It is required for ABP activation scheme. **_Value Range_**: 8 hexadecimal characters (0~9, A~F)
Device EUI start / Device EUI end	A Must filled setting Blanked by default	Specify a range of Device EUI, by entering the start and end EUI, for the LoRa group nodes. For example, 1000123AB0100000 as the start EUI, and 1000123AB01FFFFF as the end EUI. Any LoRa Node with Device EUI in this range will be regarded as a registered node. The EUI is provided by the device manufacture. **_Value Range_**: 16 hexadecimal characters (0~9, A~F)
Application EUI	A Must filled setting Blanked by default	Enter an identifier as the Application EUI for the application you are deploying with the LoRa nodes. For using the private LoRa Network Server, you can define your own Application EUI. **_Value Range_**: 16 hexadecimal characters (0~9, A~F)
Network Session Key	A Must filled setting for ABP scheme	Enter a network session key for the LoRa node being registered. The Network Server will use this key to decrypt the meta data that is transmitted from the registered LoRa nodes. It is required for ABP activation scheme. **_Value Range_**: 32 hexadecimal characters (0~9, A~F)
APP Session Key	A Must filled setting for ABP scheme	Enter an application session key for the LoRa node being registered. The Application Server will use this key to decrypt the packet payload that is transmitted from the registered LoRa nodes. It is required for ABP activation scheme. **_Value Range_**: 32 hexadecimal characters (0~9, A~F)
Enable	Unchecked by default	Check the Enable box to activate the parameters of the LoRa node being registered.
Save	*NA*	Click the **Save** button to save the configuration

Outdoor WiFi LoRa BSU

7.3.3 Application Server

Go to **Service > LoRa > Application Server** Tab.

The Application Server setting page enables user to configure the embedded LoRa application server, and specify the information for the client server that the LoRa packet will be forward to for application-specific processing.

Specify Application Server

You can maintain and see all the available application server in the Application Server list. Up to 3 Application Server profile is supported.

ID	Application Name	Application EUI	CS FQDN	CS Port	Enable	Actions

Application Server List — Add | Delete

When **Add** or **Edit** button is applied, the **Application Server Configuration** screen will appear.

Application Server Configuration — Save | Undo

Item	Setting
▶ Application Name	
▶ Application EUI	
▶ CS FQDN	
▶ CS Port	
▶ Enable	☐

Application Server Configuration		
Item	**Value setting**	**Description**
Application Name	A Must filled setting Blanked by default	Enter the name for the application server. ***Value Range***: 1~16 aplhanumeric characters; '-' and '_' are valid characters.
Application EUI	A Must filled setting Blanked by default	Enter the corresponding Application EUI for the application server. All the decrypted payloads from connected LoRa nodes with the same Appication EUI setting will be forward to the designated application server. You have to further specify the CS FQDN and Port as the connmuication interface for final client applications ***Value Range***: 16 hexadecimal characters (0~9, A~F)
CS FQDN / **CS Port**	A Must filled setting Blanked by default	Enter the IP address or FQDN and port number for the clent application server. The application server will forward the decrypted payloads from the LoRa nodes to this designated client application server for application data processing.

		Value Range: 1 ~ 65535.
Enable	Unchecked by default	Check the Enable box to activate the application server setting.
Save	*NA*	Click the **Save** button to save the configuration

Chapter 8 Status

8.1 Dashboard
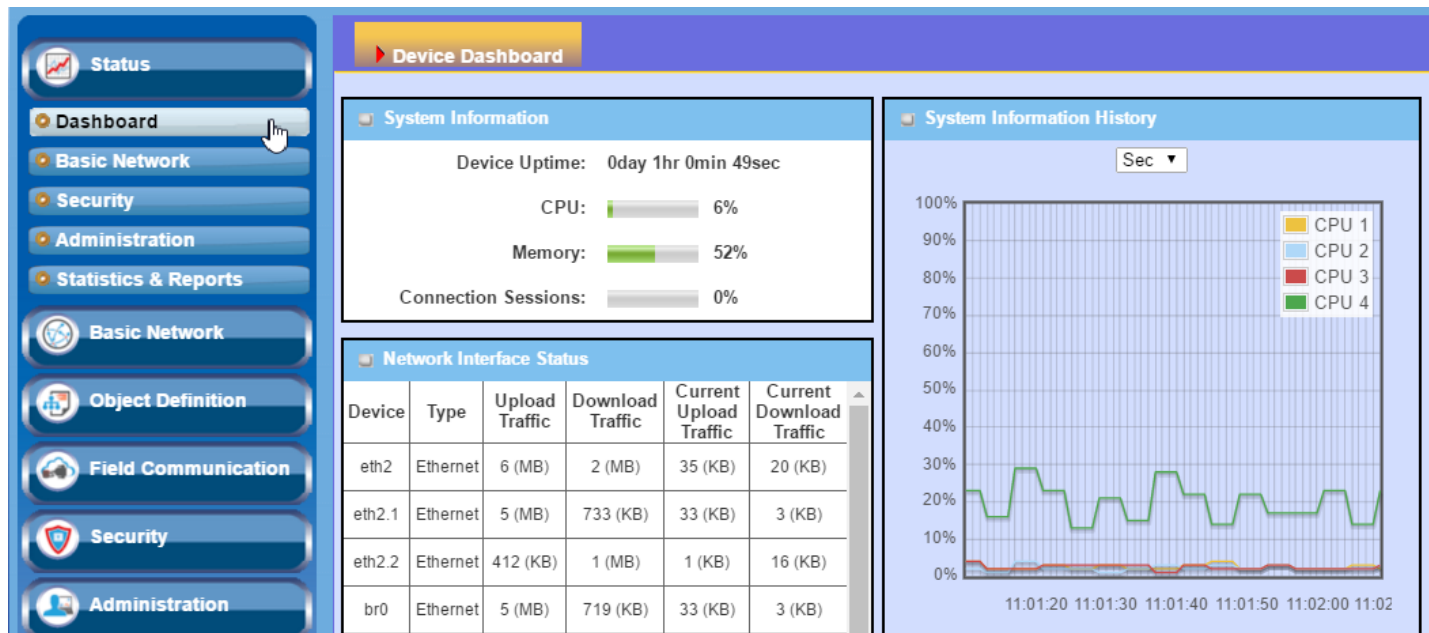
8.1.1 Device Dashboard

The **Device Dashboard** window shows the current status in graph or tables for quickly understanding the operation status for the gateway. They are the System Information, System Information History, and Network Interface Status. The display will be refreshed once per second.

From the menu on the left, select **Status > Dashboard > Device Dashboard** tab**.**

System Information Status

The **System Information** screen shows the device Up-time and the resource utilization for the CPU, Memory, and Connection Sessions.
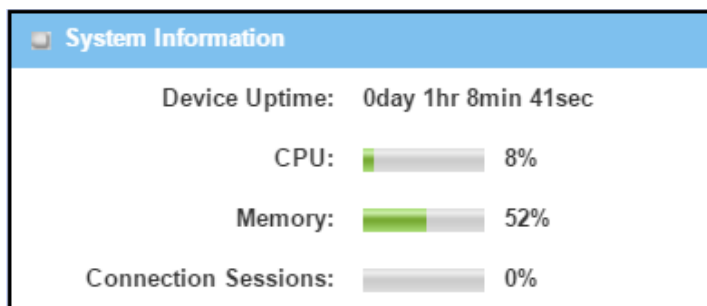
Outdoor WiFi LoRa BSU

System Information History

The **System Information History** screen shows the statistic graphs for the CPU and memory.
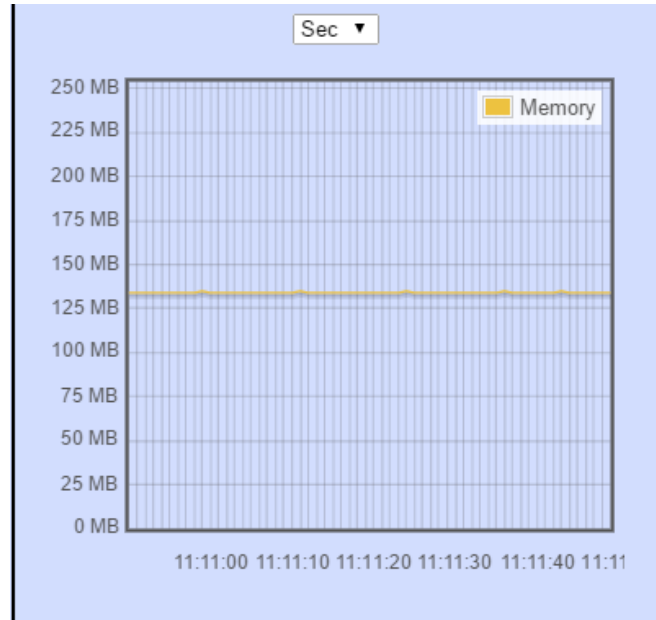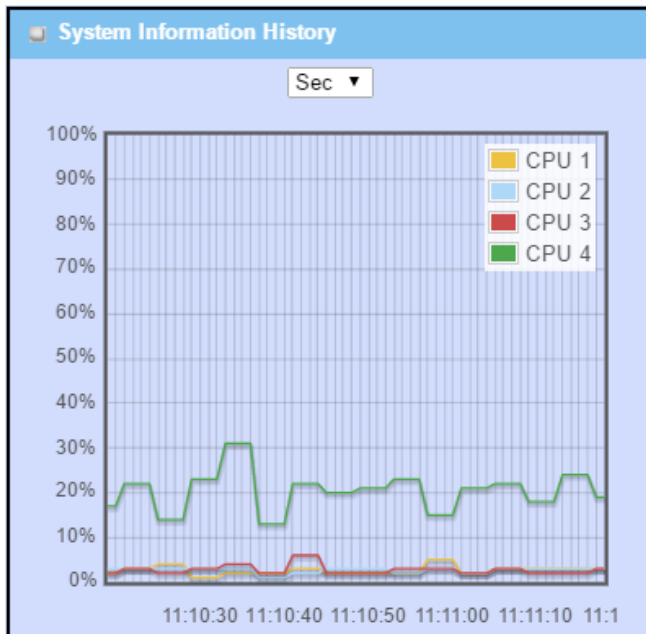
Network Interface Status

The **Network Interface Status** screen shows the statistic information for each network interface of the gateway. The statistic information includes the Interface Type, Upload Traffic, Download Traffic, and Current Upload / Download Traffic.

Device	Type	Upload Traffic	Download Traffic	Current Upload Traffic	Current Download Traffic
eth2	Ethernet	27 (MB)	15 (MB)	35 (KB)	19 (KB)
eth2.1	Ethernet	26 (MB)	2 (MB)	34 (KB)	3 (KB)
eth2.2	Ethernet	1 (MB)	12 (MB)	1 (KB)	15 (KB)
br0	Ethernet	26 (MB)	2 (MB)	33 (KB)	3 (KB)
ra0	Wireless LAN	0 (Bytes)	0 (Bytes)	0 (Bytes)	0 (Bytes)
rai0	Wireless LAN	0 (Bytes)	0 (Bytes)	0 (Bytes)	0 (Bytes)
ra7	Wireless LAN	0 (Bytes)	0 (Bytes)	0 (Bytes)	0 (Bytes)
	Wireless				

8.2 Basic Network

8.2.1 WAN & Uplink Status

Go to **Status > Basic Network > WAN & Uplink** tab.

The **WAN & Uplink Status** window shows the current status for different network type, including network configuration, connecting information, modem status and traffic statistics. The display will be refreshed on every five seconds.

WAN interface IPv4 Network Status

WAN interface IPv4 Network Status screen shows status information for IPv4 network.

ID	Interface	WAN Type	Network Type	IP Addr.	Subnet Mask	Gateway	DNS	MAC Address	Conn. Status	Action
WAN-1	WIFI Module 1	Uplink	NAT	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0, 0.0.0.0	02:50:18:26:F0:31	Disconnected -	Connect | Edit
WAN-2		Disable								Edit

WAN interface IPv4 Network Status		
Item	**Value setting**	**Description**
ID	N/A	It displays corresponding WAN interface WAN IDs.
Interface	N/A	It displays the type of WAN physical interface. Depending on the model purchased, it can be Ethernet, or WiFi.
WAN Type	N/A	It displays the method which public IP address is obtained from your ISP. Depending on the model purchased, it can be Static IP, Dynamic IP, PPPoE, PPTP, L2TP, or WiFi Uplink.
Network Type	N/A	It displays the network type for the WAN interface(s). Depending on the model purchased, it can be NAT, Routing, Bridge, or IP Pass-through.
IP Addr.	N/A	It displays the public IP address obtained from your ISP for Internet connection. Default value is 0.0.0.0 if left unconfigured.
Subnet Mask	N/A	It displays the Subnet Mask for public IP address obtained from your ISP for Internet connection. Default value is 0.0.0.0 if left unconfigured.
Gateway	N/A	It displays the Gateway IP address obtained from your ISP for Internet connection. Default value is 0.0.0.0 if left unconfigured.
DNS	N/A	It displays the IP address of DNS server obtained from your ISP for Internet connection. Default value is 0.0.0.0 if left unconfigured.
MAC Address	N/A	It displays the MAC Address for your ISP to allow you for Internet access. Note: Not all ISP may require this field.
Conn. Status	N/A	It displays the connection status of the device to your ISP. Status are Connected or disconnected.

		This area provides functional buttons.
Action	N/A	**Renew** button allows user to force the device to request an IP address from the DHCP server. Note: **Renew** button is available when DHCP WAN Type is used and WAN connection is disconnected. **Release** button allows user to force the device to clear its IP address setting to disconnect from DHCP server. Note: **Release** button is available when DHCP WAN Type is used and WAN connection is connected. **Connect** button allows user to manually connect the device to the Internet. Note: Connect button is available when Connection Control in WAN Type setting is set to Connect Manually (Refer to **Edit** button in **Basic Network > WAN & Uplink > Internet Setup**) and WAN connection status is disconnected. **Disconnect** button allows user to manually disconnect the device from the Internet. Note: **Connect** button is available when Connection Control in WAN Type setting is set to Connect Manually (Refer to **Edit** button in **Basic Network > WAN & Uplink > Internet Setup**) and WAN connection status is connected.

WAN interface IPv6 Network Status

WAN interface IPv6 Network Status screen shows status information for IPv6 network.

WAN Interface IPv6 Network Status						
ID	Interface	WAN Type	Link-local IP Address	Global IP Address	Conn. Status	Action
WAN-1		Disable				Edit

WAN interface IPv6 Network Status		
Item	**Value setting**	**Description**
ID	N/A	It displays corresponding WAN interface WAN IDs.
Interface	N/A	It displays the type of WAN physical interface. Depending on the model purchased, it can be Ethernet, or WiFi.
WAN Type	N/A	It displays the method which public IP address is obtained from your ISP. WAN type setting can be changed from **Basic Network > IPv6 > Configuration**.
Link-local IP Address	N/A	It displays the LAN IPv6 Link-Local address.
Global IP Address	N/A	It displays the IPv6 global IP address assigned by your ISP for your Internet connection.
Conn. Status	N/A	It displays the connection status. The status can be connected, disconnected and connecting.
Action	N/A	This area provides functional buttons. **Edit Button** when pressed, web-based utility will take you to the IPv6 configuration page. (**Basic Network > IPv6 > Configuration**.)

Outdoor WiFi LoRa BSU

LAN Interface Network Status

LAN Interface Network Status screen shows IPv4 and IPv6 information of LAN network.

IPv4 Address	IPv4 Subnet Mask	IPv6 Link-local Address	IPv6 Global Address	MAC Address	Action
192.168.66.1	255.255.254.0	fe80::250:18ff:fe3a:4a5f	/64	00:50:18:3A:4A:5F	Edit IPv4 | Edit IPv6

LAN Interface Network Status		
Item	**Value setting**	**Description**
IPv4 Address	N/A	It displays the current IPv4 IP Address of the gateway This is also the IP Address user use to access Router's Web-based Utility.
IPv4 Subnet Mask	N/A	It displays the current mask of the subnet.
IPv6 Link-local Address	N/A	It displays the current LAN IPv6 Link-Local address. This is also the IPv6 IP Address user use to access Router's Web-based Utility.
IPv6 Global Address	N/A	It displays the current IPv6 global IP address assigned by your ISP for your Internet connection.
MAC Address	N/A	It displays the LAN MAC Address of the gateway
Action	N/A	This area provides functional buttons. **Edit IPv4 Button** when press, web-based utility will take you to the Ethernet LAN configuration page. (**Basic Network > LAN & VLAN > Ethernet LAN** tab). **Edit IPv6 Button** when press, web-based utility will take you to the IPv6 configuration page. (**Basic Network > IPv6 > Configuration**.)

Interface Traffic Statistics

Interface Traffic Statistics screen displays the Interface's total transmitted packets.

ID	Interface	Received Packets(Mb)	Transmitted Packets(Mb)	Action
WAN-1	WIFI Module 1	0	0	Reset
WAN-2		-	-	

Interface Traffic Statistics		
Item	**Value setting**	**Description**
ID	N/A	It displays corresponding WAN interface WAN IDs.
Interface	N/A	It displays the type of WAN physical interface. Depending on the model purchased, it can be Ethernet, 3G/4G, etc...
Received Packets	N/A	It displays the downstream packets (Mb). It is reset when the device is

250

(Mb)		rebooted.
Transmitted Packets (Mb)	N/A	It displays the upstream packets (Mb). It is reset when the device is rebooted.

Outdoor WiFi LoRa BSU

8.2.2 LAN & VLAN Status

Go to **Status > Basic Network > LAN & VLAN** tab.

Client List

The **Client List** shows you the LAN Interface, IP address, Host Name, MAC Address, and Remaining Lease Time of each device that is connected to this gateway.

LAN Interface	IP Address	Host Name	MAC Address	Remaining Lease Time
Ethernet	Dynamic / 192.168.66.100	amit25613572	00-13-3B-0E-5B-1D	00:15:00

LAN Client List Item	Value setting	Description
LAN Interface	N/A	Client record of LAN Interface. String Format.
IP Address	N/A	Client record of IP Address Type and the IP Address. Type is String Format and the IP Address is IPv4 Format.
Host Name	N/A	Client record of Host Name. String Format.
MAC Address	N/A	Client record of MAC Address. MAC Address Format.
Remaining Lease Time	N/A	Client record of Remaining Lease Time. Time Format.

Outdoor WiFi LoRa BSU

8.2.3 WiFi Status

Go to **Status > Basic Network > WiFi** tab.

The **WiFi Status** window shows the overall statistics of WiFi VAP entries.

WiFi Virtual AP List

The WiFi Virtual AP List shows all of the virtual AP information on each WiFi module. The **Edit** button allows for quick configuration changes.

Op. Band	ID	WiFi Enable	Op. Mode	SSID	Channel	WiFi System	Auth.&Security	MAC Address	Action	
2.4G	VAP-1	☑	WiFi Uplink	Staff_2.4G	1	b/g/n Mixed	WPA2-PSK(AES)	00:50:18:3A:4A:5F	Edit	QR Code
2.4G	VAP-2	☑	WiFi Uplink	default	1	b/g/n Mixed	Open(None)	02:50:18:38:4A:5F	Edit	QR Code
2.4G	VAP-3	☐	WiFi Uplink	default	1	b/g/n Mixed	WPA2-PSK(AES)	02:50:18:39:4A:5F	Edit	QR Code
2.4G	VAP-4	☐	WiFi Uplink	default	1	b/g/n Mixed	WPA2-PSK(AES)	02:50:18:3A:4A:5F	Edit	QR Code
2.4G	VAP-5	☐	WiFi Uplink	default	1	b/g/n Mixed	WPA2-PSK(AES)	02:50:18:3B:4A:5F	Edit	QR Code
2.4G	VAP-6	☐	WiFi Uplink	default	1	b/g/n Mixed	WPA2-PSK(AES)	02:50:18:3C:4A:5F	Edit	QR Code
2.4G	VAP-7	☐	WiFi Uplink	default	1	b/g/n Mixed	WPA2-PSK(AES)	02:50:18:3D:4A:5F	Edit	QR Code

WiFi Virtual AP List		
Item	**Value setting**	**Description**
Op. Band	N/A	It displays the Wi-Fi Operation Band (2.4G or 5G) of VAP.
ID	N/A	It displays the ID of VAP.
WiFi Enable	N/A	It displays whether the VAP wireless signal is enabled or disabled.
Op. Mode	N/A	The Wi-Fi Operation Mode of VAP. Depends of device model, modes are AP Router, WDS Only and WDS Hybrid, Universal Repeater and Client.
SSID	N/A	It displays the network ID of VAP.
Channel	N/A	It displays the wireless channel used.
WiFi System	N/A	The WiFi System of VAP.
Auth. & Security	N/A	It displays the authentication and encryption type used.
MAC Address	N/A	It displays MAC Address of VAP.
Action	N/A	Click the **Edit** button to make a quick access to the WiFi configuration page. (**Basic Network > WiFi > Configuration** tab) The **QR Code** button allow you to generate QR code for quick connect to the VAP by scanning the QR code.

Outdoor WiFi LoRa BSU

WiFi Uplink Status

The WiFi Uplink Status shows all information of connected WiFi uplink network on each WiFi module..

SSID	BSSID	Channel	Security	RSSI0	RSSI1	Rate	Action
Only_For_Monkey	00:00:00:00:00:00	1	WPA2-PSK(AES)	0	0	0	Edit

WiFi Module One Uplink Status

Item	Value setting	Description
SSID	N/A	It displays the network ID of VAP.
BSSID	N/A	It displays the theBSSID for the connected wireless network.
Channel	N/A	It displays the wireless channel used.
Security	N/A	It displays the authentication and encryption setting for the WiFi uplink connection.
RSSI0, RSSI1	N/A	It displays the Rx sensitivity on each radio path..
Rate	N/A	It displays the link rate for the WiFi uplink connection.
Action	N/A	Click the **Edit** button to make a quick access to the WiFi uplink configuration page. (**Basic Network > WAN & Uplink > Internet Setup** tab)

WiFi IDS Status

The WiFi IDS Status shows all the WIDS statistics on each WiFi module.

Authentication Frame	Association Request Frame	Re-association Request Frame	Probe Request Frame	Disassociation Frame	Deauthentication Frame	EAP Request Frame	Malicious Data Frame	Action
0	0	0	0	0	0	0	0	Reset

WiFi IDS Status

Item	Value setting	Description
Authentication Frame	N/A	It displays the receiving Authentication Frame count.
Association Request Frame	N/A	It displays the receiving Association Request Frame count.
Re-association Request Frame	N/A	It displays the receiving Re-association Request Frame count.
Probe Request Frame	N/A	It displays the receiving Probe Request Frame count.
Disassociation Frame	N/A	It displays the receiving Disassociation Frame count.
Deauthentication Frame	N/A	It displays the receiving Deauthentication Frame count.
EAP Request Frame	N/A	It displays the receiving EAP Request Frame count.
Malicious Data Frame	N/A	It displays the number of receiving unauthorized wireless packets.

Action	N/A	Click the **Reset** button to clear the entire statistic and reset counter to 0.

Ensure WIDS function is enabled

Go to **Basic Network** > **WiFi** > **Advanced Configuration tab**

Note that the WIDS of **2.4GHz** or **5GHz WiFi** should be configured **separately**.

WiFi Traffic Statistic

The WiFi Traffic Statistic shows all the received and transmitted packets on each WiFi module.

WiFi Module One Traffic Statistics

Op. Band	ID	Received Packets	Transmitted Packets	Action
2.4G	VAP-1	269	80	Reset
2.4G	VAP-2	26	8	Reset
2.4G	VAP-3	0	0	Reset
2.4G	VAP-4	0	0	Reset
2.4G	VAP-5	0	0	Reset
2.4G	VAP-6	0	0	Reset
2.4G	VAP-7	0	0	Reset

WiFi Traffic Statistic		
Item	**Value setting**	**Description**
Op. Band	N/A	It displays the Wi-Fi Operation Band (2.4G or 5G) of VAP.
ID	N/A	It displays the VAP ID.
Received Packets	N/A	It displays the number of reveived packets.
Transmitted Packet	N/A	It displays the number of transmitted packets.
Action	N/A	Click the **Reset** button to clear individual VAP statistics.
Refresh Button	N/A	Click the **Refresh** button to update the entire VAP Traffic Statistic instantly.

Outdoor WiFi LoRa BSU
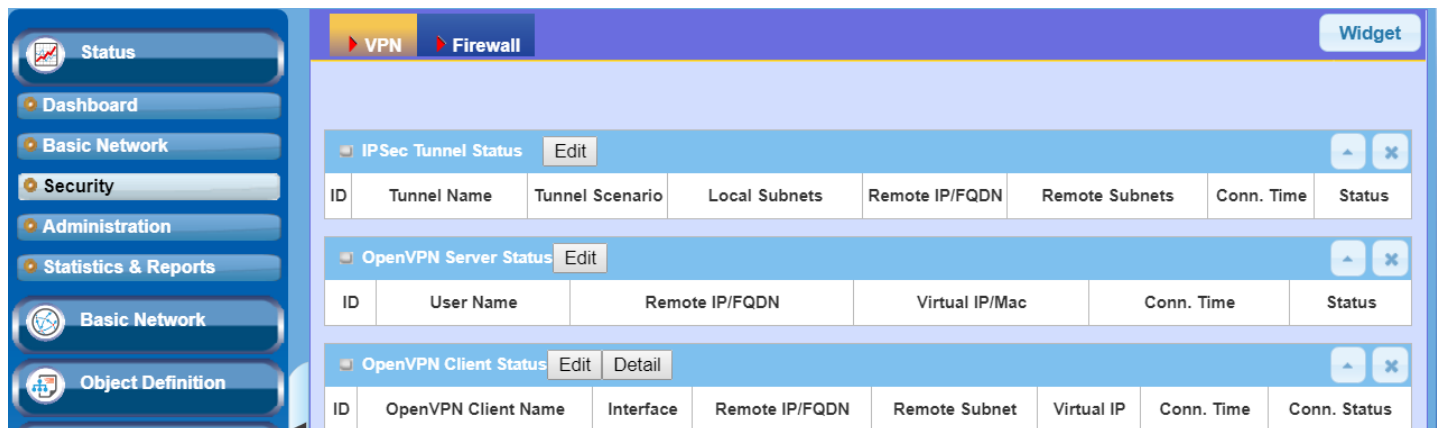
8.3 Security

8.3.1 VPN Status

Go to **Status > Security > VPN** tab.

The **VPN Status** widow shows the overall VPN tunnel status. The display will be refreshed on every five seconds.

IPSec Tunnel Status

IPSec Tunnel Status windows show the configuration for establishing IPSec VPN connection and current connection status.

IPSec Tunnel Status		
Item	**Value setting**	**Description**
Tunnel Name	N/A	It displays the tunnel name you have entered to identify.
Tunnel Scenario	N/A	It displays the Tunnel Scenario specified.
Local Subnets	N/A	It displays the Local Subnets specified.
Remote IP/FQDN	N/A	It displays the Remote IP/FQDN specified.
Remote Subnets	N/A	It displays the Remote Subnets specified.
Conn. Time	N/A	It displays the connection time for the IPSec tunnel.
Status	N/A	It displays the Status of the VPN connection. The status displays are Connected, Disconnected, Wait for traffic, and Connecting.
Edit Button	N/A	Click on Edit Button to change IPSec setting, web-based utility will take you to the IPSec configuration page. (**Security > VPN > IPSec** tab)

Outdoor WiFi LoRa BSU

OpenVPN Server Status

According to OpenVPN configuration, the **OpenVPN Server/Client Status** shows the status and statistics for the OpenVPN connection from the server side or client side.

ID	User Name	Remote IP/FQDN	Virtual IP/Mac	Conn. Time	Status

OpenVPN Server Status		
Item	**Value setting**	**Description**
User Name	N/A	It displays the Client name you have entered for identification.
Remote IP/FQDN	N/A	It displays the public IP address (the WAN IP address) of the connected OpenVPN Client
Virtual IP/MAC	N/A	It displays the virtual IP/MAC address assigned to the connected OpenVPN client.
Conn. Time	N/A	It displays the connection time for the corresponding OpenVPN tunnel.
Status	N/A	It displays the connection status of the corresponding OpenVPN tunnel. The status can be Connected, or Disconnected.

OpenVPN Client Status

ID	OpenVPN Client Name	Interface	Remote IP/FQDN	Remote Subnet	Virtual IP	Conn. Time	Conn. Status

OpenVPN Client Status		
Item	**Value setting**	**Description**
OpenVPN Client Name	N/A	It displays the Client name you have entered for identification.
Interface	N/A	It displays the WAN interface specified for the OpenVPN client connection.
Remote IP/FQDN	N/A	It displays the peer OpenVPN Server's Public IP address (the WAN IP address) or FQDN.
Remote Subnet	N/A	It displays the Remote Subnet specified.
TUN/TAP Read(bytes)	N/A	It displays the TUN/TAP Read Bytes of OpenVPN Client.
TUN/TAP Write(bytes)	N/A	It displays the TUN/TAP Write Bytes of OpenVPN Client.
TCP/UDP Read(bytes)	N/A	It displays the TCP/UDP Read Bytes of OpenVPN Client.
TCP/UDP Write(bytes)	N/A	It displays the TCP/UDP Write Bytes of OpenVPN Client. Connection
Conn. Time	N/A	It displays the connection time for the corresponding OpenVPN tunnel.
Conn. Status	N/A	It displays the connection status of the corresponding OpenVPN tunnel. The status can be Connected, or Disconnected.

Outdoor WiFi LoRa BSU

8.3.2 Firewall Status

Go to **Status > Security > Firewall Status** Tab.

The **Firewall Status** provides user a quick view of the firewall status and current firewall settings. It also keeps the log history of the dropped packets by the firewall rule policies, and includes the administrator remote login settings specified in the Firewall Options. The display will be refreshed on every five seconds.

By clicking the icon [+], the status table will be expanded to display log history. Clicking the **Edit** button the screen will be switched to the configuration page.

Packet Filter Status

▣ Packet Filters	Edit		▲ ✕
Activated Filter Rule	Detected Contents	IP	Time

Packet Filter Status		
Item	**Value setting**	**Description**
Activated Filter Rule	N/A	This is the Packet Filter Rule name.
Detected Contents	N/A	This is the logged packet information, including the source IP, destination IP, protocol, and destination port –the TCP or UDP. String format: Source IP to Destination IP : Destination Protocol (TCP or UDP)
IP	N/A	The Source IP (IPv4) of the logged packet.
Time	N/A	The Date and Time stamp of the logged packet. Date & time format. ("Month" "Day" "Hours":"Minutes":"Seconds")

Note: Ensure Packet Filter Log Alert is enabled.
Refer to **Security > Firewall > Packet Filter** tab. Check Log Alert and save the setting.

MAC Control Status

▣ MAC Control	Edit		▲ ✕
Activated Control Rule	Blocked MAC Addresses	IP	Time

MAC Control Status		
Item	**Value setting**	**Description**
Activated Control Rule	N/A	This is the MAC Control Rule name.

Blocked MAC Addresses	N/A	This is the MAC address of the logged packet.
IP	N/A	The Source IP (IPv4) of the logged packet.
Time	N/A	The Date and Time stamp of the logged packet. Date & time format. ("Month" "Day" "Hours":"Minutes":"Seconds")

Note: Ensure MAC Control Log Alert is enabled.

Refer to **Security > Firewall > MAC Control** tab. Check Log Alert and save the setting.

IPS Status

⬜ IPS Edit			▲ ✖
Detected Intrusion		IP	Time

IPS Firewall Status		
Item	**Value setting**	**Description**
Detected Intrusion	N/A	This is the intrusion type of the packets being blocked.
IP	N/A	The Source IP (IPv4) of the logged packet.
Time	N/A	The Date and Time stamp of the logged packet. Date & time format. ("Month" "Day" "Hours":"Minutes":"Seconds")

Note: Ensure IPS Log Alert is enabled.

Refer to **Security > Firewall > IPS** tab. Check Log Alert and save the setting.

Firewall Options Status

⬜ Options Edit				▲ ✖
Stealth Mode	SPI	Discard Ping from WAN	Remote Administrator Management	

Firewall Options Status		
Item	**Value setting**	**Description**
Stealth Mode	N/A	Enable or Disable setting status of Stealth Mode on Firewall Options. String Format: Disable or Enable
SPI	N/A	Enable or Disable setting status of SPI on Firewall Options. String Format : Disable or Enable
Discard Ping from WAN	N/A	Enable or Disable setting status of Discard Ping from WAN on Firewall Options. String Format: Disable or Enable
Remote Administrator Management	N/A	Enable or Disable setting status of Remote Administrator. If Remote Administrator is enabled, it shows the currently logged in administrator's source IP address and login user name and the login time.

	Format:
	IP : "Source IP", User Name: "Login User Name", Time: "Date time"
	Example:
	IP: 192.168.127.39, User Name: admin, Time: Mar 3 01:34:13

Note: Ensure Firewall Options Log Alert is enabled.

Refer to **Security > Firewall > Options** tab. Check Log Alert and save the setting.

8.4 Administration

8.4.1 Configure & Manage Status

Go to **Status > Administration > Configure & Manage** tab.

The **Configure & Manage Status** window shows the status for managing remote network devices. The type of management available in your device is depended on the device model purchased. The commonly used ones are the SNMP, TR-069, and UPnP. The display will be refreshed on every five seconds.

SNMP Linking Status

SNMP Link Status screen shows the status of current active SNMP connections.

User Name	IP Address	Port	Community	Auth. Mode	Privacy Mode	SNMP Version

SNMP Link Status		
Item	**Value setting**	**Description**
User Name	N/A	It displays the user name for authentication. This is only available for SNMP version 3.
IP Address	N/A	It displays the IP address of SNMP manager.
Port	N/A	It displays the port number used to maintain connection with the SNMP manager.
Community	N/A	It displays the community for SNMP version 1 or version 2c only.
Auth. Mode	N/A	It displays the authentication method for SNMP version 3 only.
Privacy Mode	N/A	It displays the privacy mode for version 3 only.
SNMP Version	N/A	It displays the SNMP Version employed.

SNMP Trap Information

SNMP Trap Information screen shows the status of current received SNMP traps.

Trap Level	Time	Trap Event

SNMP Trap Information		
Item	**Value setting**	**Description**
Trap Level	N/A	It displays the trap level.
Time	N/A	It displays the timestamp of trap event.
Trap Event	N/A	It displays the IP address of the trap sender and event type.

TR-069 Status

TR-069 Status screen shows the current connection status with the TR-068 server.

TR-069 Status		
	Link Status	
	Off	

TR-069 Status		
Item	**Value setting**	**Description**
Link Status	N/A	It displays the current connection status with the TR-068 server. The connection status is either On when the device is connected with the TR-068 server or Off when disconnected.

Outdoor WiFi LoRa BSU

8.4.2 Log Storage Status

Go to **Status > Administration > Log Storage** tab.

The **Log Storage Status** screen shows the status for selected device storage.

Log Storage Status

Log Storage Status screen shows the status of current the selected device storage. The status includes Device Description, Usage, File System, Speed, and status.

Device Select	Device Description	Usage	File System	Speed	Status

Outdoor WiFi LoRa BSU

8.5 Statistics & Report

8.5.1 Connection Session

Go to **Status > Statistics & Reports > Connection Session** tab.

**Internet Surfing Statistic** shows the connection tracks on this router.

User Name	Protocol	Internal IP & Port	MAC	External IP & Port	Duration Time
	UDP	192.168.127.58:3847		88.198.95.100:1194	2019/04/01 12:09~
	UDP	192.168.127.58:4486		192.168.123.10:53	2019/04/01 12:09~
	UDP	192.168.127.58:2899		192.168.123.10:53	2019/04/01 12:09~
	UDP	192.168.127.58:1251		192.168.123.10:53	2019/04/01 12:09~
	UDP	192.168.127.58:3145		192.168.123.10:53	2019/04/01 12:09~

Internet Surfing List (14 entries) — Previous | Next | First | Last | Export (.xml) | Export (.csv) | Refresh

Internet Surfing Statistic		
Item	**Value setting**	**Description**
Previous	N/A	Click the **Previous** button; you will see the previous page of track list.
Next	N/A	Click the **Next** button; you will see the next page of track list.
First	N/A	Click the **First** button; you will see the first page of track list.
Last	N/A	Click the **Last** button; you will see the last page of track list.
Export (.xml)	N/A	Click the **Export (.xml)** button to export the list to xml file.
Export (.csv)	N/A	Click the **Export (.csv)** button to export the list to csv file.
Refresh	N/A	Click the **Refresh** button to refresh the list.

Outdoor WiFi LoRa BSU

8.5.2 Network Traffic

Go to **Status > Statistics & Reports > Network Traffic** tab.

Network Traffic Statistics screen shows the historical graph for the selected network interface.

You can change the interface drop list and select the interface and sampling time interval you want to monitor.
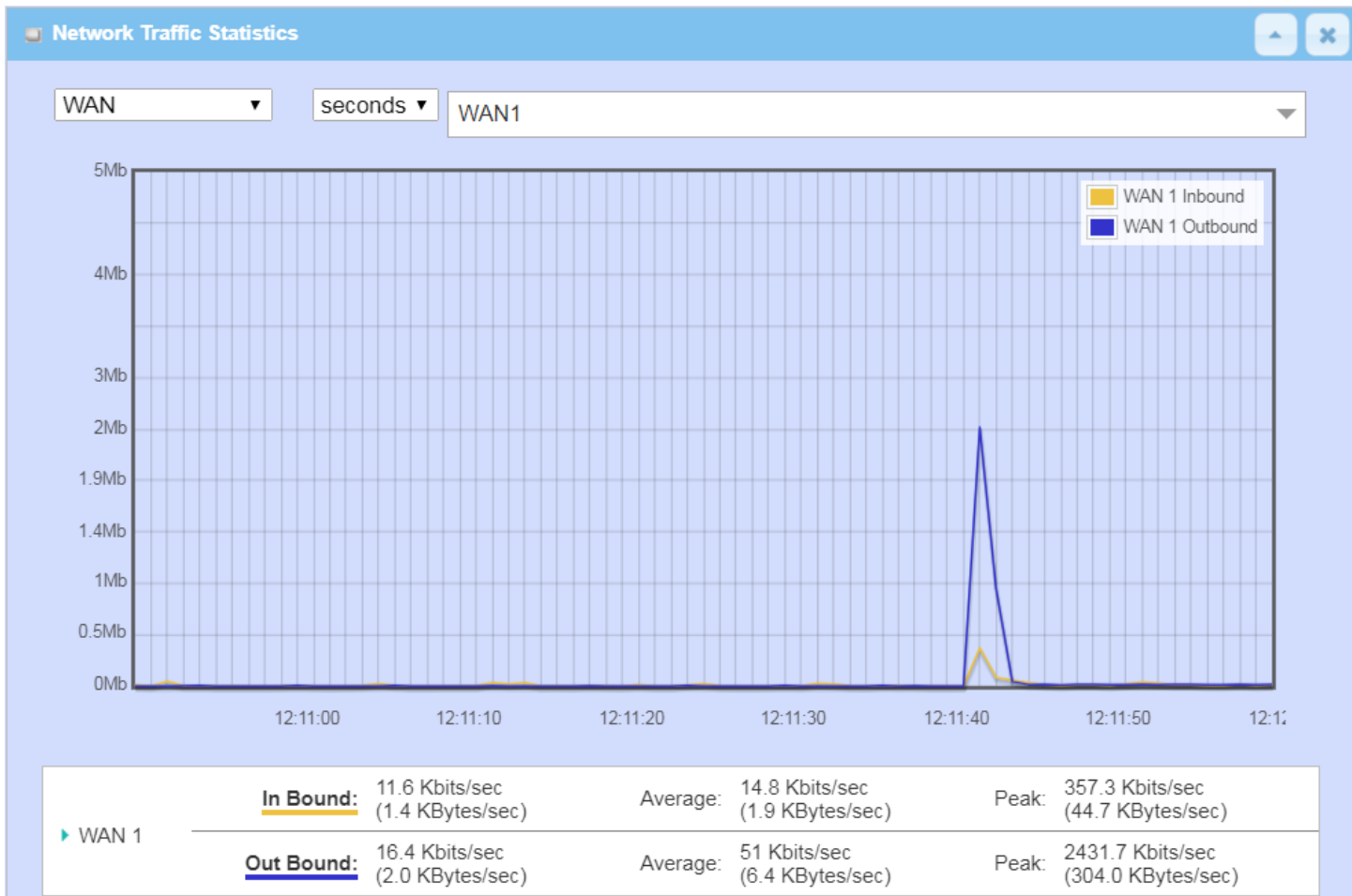
Outdoor WiFi LoRa BSU

8.5.3 Login Statistics

Go to **Status > Statistics & Reports > Login Statistics**

Login Statistics shows the login information.

User Name	Protocol Type	IP Address	Info	Duration Time
admin	HTTP	192.168.123.190	Admin	2018/01/01 00:00~
admin	HTTP	192.168.123.190	Admin	2018/01/01 00:02~
admin	HTTP	192.168.123.190	Login Fail	2019/06/05 16:30~
admin	HTTP	192.168.123.190	Admin	2019/06/05 16:30~

Device Manager Login Statistic		
Item	**Value setting**	**Description**
Previous	N/A	Click the **Previous** button; you will see the previous page of login statistics.
Next	N/A	Click the **Next** button; you will see the next page of login statistics.
First	N/A	Click the **First** button; you will see the first page of login statistics.
Last	N/A	Click the **Last** button; you will see the last page of login statistics.
Export (.xml)	N/A	Click the **Export (.xml)** button to export the login statistics to xml file.
Export (.csv)	N/A	Click the **Export (.csv)** button to export the login statistics to csv file.
Refresh	N/A	Click the **Refresh** button to refresh the login statistics.

Appendix A GPL WRITTEN OFFER

This product incorporates open source software components covered by the terms of third party copyright notices and license agreements contained below.

GPSBabel
Version 1.4.4
Copyright (C) 2002-2005 Robert Lipe<robertlipe@usa.net>
GPL License: https://www.gpsbabel.org/

Curl
Version 7.19.6
Copyright (c) 1996-2009, Daniel Stenberg, <daniel@haxx.se>.
MIT/X derivate License: https://curl.haxx.se/

OpenSSL
Version 1.0.2m
Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
GPL License: https://www.openssl.org/

brctl - ethernet bridge administration
Stephen Hemminger <shemminger@osdl.org>
Lennert Buytenhek <buytenh@gnu.org>
version 1.1
GNU GENERAL PUBLIC LICENSE Version 2, June 1991

tc - show / manipulate traffic control settings
Stephen Hemminger<shemminger@osdl.org>
Alexey Kuznetsov<kuznet@ms2.inr.ac.ru>
version iproute2-ss050330
GNU GENERAL PUBLIC LICENSE Version 2, June 1991

dhcp-fwd — starts the DHCP forwarding agent
Enrico Scholz <enrico.scholz@informatik.tu-chemnitz.de>
version 0.7
GNU GENERAL PUBLIC LICENSE Version 2, June 1991

lftp - Sophisticated file transfer program
Alexander V. Lukyanov <lav@yars.free.net>

version:4.5.x
Copyright (c) 1996-2014 by Alexander V. Lukyanov (lav@yars.free.net)

dnsmasq - A lightweight DHCP and caching DNS server.
Simon Kelley <simon@thekelleys.org.uk>
version:2.72
dnsmasq is Copyright (c) 2000-2014 Simon Kelley

socat - Multipurpose relay
Version: 2.0.0-b8
GPLv2
http://www.dest-unreach.org/socat/

LibModbus
Version: 3.0.3
LGPL v2
http://libmodbus.org/news/

LibIEC60870
GPLv2
Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
https://sourceforge.net/projects/mrts/

Openswan
Version: v2.6.38 GNU GENERAL PUBLIC LICENSE Version 2, June 1991
 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed.
https://www.openswan.org/

Opennhrp
Version: v0.14.1
OpenNHRP is an NHRP implementation for Linux. It has most of the RFC2332
and Cisco IOS extensions.
Project homepage: http://sourceforge.net/projects/opennhrp
Git repository: git://opennhrp.git.sourceforge.net/gitroot/opennhrp
 LICENSE
OpenNHRP is licensed under the MIT License. See MIT-LICENSE.txt for

additional details.

OpenNHRP embeds libev. libev is dual licensed with 2-clause BSD and GPLv2+ licenses. See libev/LICENSE for additional details.

OpenNHRP links to c-ares. c-ares is licensed under the MIT License.

https://sourceforge.net/projects/opennhrp/

IPSec-tools
Version: v0.8
No GPL be written
http://ipsec-tools.sourceforge.net/

PPTP
Version: pptp-1.7.1
GNU GENERAL PUBLIC LICENSE Version 2, June 1991
 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 675 Mass Ave, Cambridge, MA 02139, USA
 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed.
http://pptpclient.sourceforge.net/

PPTPServ
Version: 1.3.4
GNU GENERAL PUBLIC LICENSE Version 2, June 1991
 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 675 Mass Ave, Cambridge, MA 02139, USA
 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed. http://poptop.sourceforge.net/

L2TP
Version: 0.4
Copying All software included in this package is Copyright 2002 Roaring Penguin Software Inc. You may distribute it under the terms of the GNU General Public License (the "GPL"), Version 2, or (at your option) any later version.
http://www.roaringpenguin.com/

L2TPServ
Version: v 1.3.1 GNU GENERAL PUBLIC LICENSEVersion 2, June 1991
 Copyright (C) 1989, 1991 Free Software Foundation, Inc.59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed.

Outdoor WiFi LoRa BSU

http://www.xelerance.com/software/xl2tpd/

Mpstat: from sysstat, system performance tools for Linux
Version: 10.1.6
Copyright: (C) 1999-2013 by Sebastien Godard (sysstat <at> orange.fr)

SSHD: dropbear, a SSH2 server
Version: 0.53.1
Copyright: (c) 2002-2008 Matt Johnston

Libncurses: The ncurses (new curses) library is a free software emulation of curses in System V Release 4.0 (SVr4), and more.
Version: 5.9
Copyright: (c) 1998,2000,2004,2005,2006,2008,2011,2015 Free Software Foundation, Inc., 51 Franklin Street, Boston, MA 02110-1301, USA

MiniUPnP: The miniUPnP daemon is an UPnP IGD (internet gateway device) which provide NAT traversal services to any UPnP enabled client on the network.
Version: 1.7
Copyright: (c) 2006-2011, Thomas BERNARD

CoovaChilli is an open-source software access controller for captive portal (UAM) and 802.1X access provisioning.
Version: 1.3.0
Copyright: (C) 2007-2012 David Bird (Coova Technologies) <support@coova.com>

Krb5: Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography.
Version: 1.11.3
Copyright: (C) 1985-2013 by the Massachusetts Institute of Technology and its contributors

OpenLDAP: a suite of the Lightweight Directory Access Protocol (v3) servers, clients, utilities, and development tools.
Version: 2.4
Copyright: 1998-2014 The OpenLDAP Foundation

Samba3311: the free SMB and CIFS client and server for UNIX and other operating systems
Version: 3.3.11
Copyright: (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>

Outdoor WiFi LoRa BSU

NTPClient: an NTP (RFC-1305, RFC-4330) client for unix-alike computers
Version: 2007_365
Copyright: 1997, 1999, 2000, 2003, 2006, 2007 Larry Doolittle

exFAT: FUSE-based exFAT implementation
Version: 0.9.8
Copyright: (C) 2010-2012 Andrew Nayenko

ONTFS_3G: The NTFS-3G driver is an open source, freely available read/write NTFS driver for Linux, FreeBSD, Mac OS X, NetBSD, Solaris and Haiku.
Version: 2009.4.4
Copyright: (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

mysql-5_1_72: a release of MySQL, a dual-license SQL database server
Version: 5.1.72
Copyright: (c) 2000, 2013, Oracle and/or its affiliates
FreeRadius: a high performance and highly configurable RADIUS server
Version: 2.1.12
Copyright: (C) 1999-2011 The FreeRADIUS server project and contributors

Linux IPv6 Router Advertisement Daemon – radvd
Version: V 1.15
Copyright (c) 1996,1997 by Lars Fenneberg<lf@elemental.net>
BSD License: http://www.litech.org/radvd/

WIDE-DHCPv6
Dynamic Host Configuration Protocol for IPv6 (DHCPv6) clients, servers, and relay agents.
Version: 20080615
Copyright (C) 1998-2004 WIDE Project.
BSD License: https://sourceforge.net/projects/wide-dhcpv6/

Python version 2.7.12
This Python distribution contains no GNU General Public Licensed
(GPLed) code so it may be used in proprietary projects just like prior
Python distributions. There are interfaces to some GNU code but these
are entirely optional

OpenPAM Radula
This software was developed for the FreeBSD Project by ThinkSec AS and

Outdoor WiFi LoRa BSU

Network Associates Laboratories, the Security Research Division of
Network Associates, Inc. under DARPA/SPAWAR contract N66001-01-C-8035
("CBOSS"), as part of the DARPA CHATS research program.

ISC DHCP Version 4.3.5
Copyright (c) 2004-2016 by Internet Systems Consortium, Inc. ("ISC")