



Industrial Wireless PoE Switch-LTE Series

JetWave2714GF

Industrial Cellular + 2GT PSE +

2G SFP Gigabit PoE Switch

User Manual

V1.0 May. 2018

Copyright

Copyright © 2017 all rights reserved. No part of this publication may be reproduced, adapted, stored in a retrieval system, translated into any language, or transmitted in any form or by any means without the written permission of the supplier.

About This Manual

This user manual provides the following notes:

1. The Declaration of Conformity policy and manufacturer information.
2. The Safety Precaution and important notification.
3. The technical specification of the product.
4. The instruction on how to install and configure your product.

Please read this document carefully and only trained and qualified personnel should be allowed to install, replace, or service this equipment.

Conventions

For your attention on important parts, special characters and patterns are used in this manual:



Note:

This indicates an important note that you must pay attention to.

The Blue Wording is important note that you must pay attention to.

The Blue Wording with Big Case is very important note you must pay more attention to.



Warning:

This indicates a warning or caution that you have to abide.

The Red wording is very important you must avoid.

Bold: Indicates the function, important words, and so on.

Declaration of Conformity

R&TTE Directive 1999/5/EC

The product may be operated in all European Union countries. The R&TTE (1995/5/EC) Directive requires that apparatus bears the CE mark as an attestation of compliance with the R&TTE Directive. While you see the CE Marking print in our product, it indicates the product conform to the requirement of the R&TTE Directive.

We provide formal declaration of R&TTE for Wireless product in our web site, different product may conform to different standards of Health & Safety, EMC, Radio and other specific standard. You can download the formal document of the product in our Web site or apply from our Sales/Technical people.

Safety Precautions

General Notification
<ul style="list-style-type: none"> ● Only operate the device according to the technical specification. You can find the information from the product datasheet, user manual...etc. ● Read the installation instructions before connecting the system to the power source. ● If you don't get exact info you need, you can contact our technical people. Only trained and qualified personnel should be allowed to install, replace, or service this equipment.
<ul style="list-style-type: none"> ● The devices are designed for operation with extra-low voltage (SELV). Connect the unit only to DC power source that complies with the safety extra-low voltage (SELV) requirements in IEC/EN 60950 based safety standards. (Not included 110V input model)
<p>Solely connect the power supply that corresponds to the type of your device. For power connection, make sure the following requirement are met:</p> <ul style="list-style-type: none"> ● The DC power circuit of the product is usually not isolated design circuit. In practical, it is suggested to use isolated DC power design PSU for field installation. Besides the PSU selection, well digital/earth grounding is also important before power on the system. ● The Power Supply conforms to the overvoltage category I or II. ● The output voltage of the AC/DC to DC Power Supply conforms to the range of the input voltage of the equipment. ● The connection cables used are permitted for the specified electronic voltage, current, wire diameter and temperature range. (Wire Diameter of AC voltage is at least 0.75mm, AWG18. For DC voltage, it is at least 1.0mm, AWG16.) ● Follow the power installing instruction of the user manual, it indicates the input voltage, pin assignment, connection circuit and notice. ● The Power Supply must be well installed, includes grounded and other notices which are defined in its instruction guide. ● Only switch on the supply voltage to the device if the housing is closed, the terminal blocks are wired up correctly and the terminal blocks are connected.

- The equipment must be grounded. Ground the device before connecting the cables, antennas and power supply. The grounding of the equipment and DC Power Supply may be different in some applications, then, you must ground them separately.
- Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

Environment & Housing

- **Hot surface.** Avoid touching the device while it is operating.
- Only operate the device at the specified ambient temperature and humidity. The temperature of the surrounding air means a distance of up to 5cm from the device. While installing multiple devices within the cabinet, remains suitable width between the devices is **MUST** for better heat dispersing.
- Better install the device in the vertical position, with the upper antenna connections pointing upward, lower antenna pointing downward.
- Install the device in a cabinet or in an operating site with limited access, the metal cabinet will filter the radio signals, use the extended antenna cable and install the external antenna in free space helps to get better Radio signal.
- Only technicians authorized by the manufacturer are permitted to open the housing. Without the manufacturer permitted, open the housing means the product is not warrantied and no responsible for any unexpected risk.

Installation

If you are installing the wireless equipment in the field box or outdoor area, for your safety as well as others', please seek assistance from a professional installer who has received safety training on the hazards involved. Keep safety as well as performance in mind when selecting your installation site, especially where there are electric power and phone lines.

Please note the following things as well:

- ◆ Do not use a metal ladder;
- ◆ Do not work on a wet or windy day;
- ◆ Wear shoes with rubber soles and heels, rubber gloves, long sleeved shirt or jacket.

- If you are installing the equipment in the indoor office or factory, be aware of the power source and grounding must be well installed. The professional Wireless IT Engineer can provide service for AP location, channel and field plan to get better performance and coverage.
- Connect the equipment which meets the IP degree of protection requirements for the application case.

- Read the Radio output power, receiver sensitivity, antenna gain specification before installing. The shipped products and antenna conforms to the R&TTE and allowed to be used in all European countries. You can read the related technical specification from the product datasheet or user manual.
- When installing external antennas, the Radio Output power and antenna gain value must be allowed according to the regulations of the country.
- When the system is operational with high gain antenna, avoid standing directly in front of it. Strong RF fields are present when the transmitter is on.
- When the system is operational with high gain antenna in short distance, adjust the radio output lower. Strong output power plus high gain antenna is not good installation for short distance transmission.

- You are responsible for undertaking suitable lightning protection.
- Install over voltage protector devices on every outdoor Ethernet cable.
- Protect each antenna installed outside with lightning protection devices, ex: lightning arrester.

Note that Field EMD (Lightning) DAMAGE IS NOT COVERED UNDER WARRANTY.

Federal Communication Commission Interference Statement

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.

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.

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.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

To avoid the possibility of exceeding radio frequency exposure limits, you shall keep a distance of at least 100cm between you and the antenna of the installed equipment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Content

Content 9

Chapter 1 Introduction 2

1.1 Introduction 2

1.2 Product Package 3

1.3 Major Features 4

1.4 Dimension 4

Chapter 2 Hardware Installation 7

2.1 Professional Installation Required 7

 2.1.1 Safety Precautions 7

2.2 Power Installation 8

 2.2.1 DC Input 8

2.3 I/O Configuration 9

 2.3.1 Wiring your Ethernet Port 9

 2.3.2 Reset 9

 2.3.3 SIM Socket 10

 2.3.4 Digital Output 11

 2.3.5 Ground 11

2.4 LED Indication 12

2.5 Antenna 12

 2.5.1 Antenna Placement 12

 2.5.2 LTE Antenna Specifications 13

2.6 Antenna Installation 13

2.7 Mounting 15

 2.7.1 Mounting the device 15

 2.7.2 Mounting the default antenna for vibration environment 15

 2.7.3 Mounting the SMA-Type external antenna 15

 2.7.4 Mounting the N-Type external antenna: 15

2.8 Select the external antenna 16

2.9 Option Antenna Mounting Accessory 17

Chapter 3 Prepare for Management	19
3.1 Basic Factory Default Settings	19
3.2 System Requirements	20
3.3 How to Login the Web-based Interface	20
3.4 Fail to login the Web GUI.....	21
Chapter 4 Web GUI Configuration	24
4.1 Status.....	24
4.1.1 Information.....	24
4.1.2 Network Flow (Statistics):.....	26
4.1.3 ARP Table.....	26
4.1.4 DHCP Client List.....	27
4.2 System	28
4.2.1 Basic Settings	28
4.2.2 IP Settings	29
4.2.3 LAN Setting	30
4.2.4 Time Settings.....	30
4.2.5 Relay Setting	31
4.2.6 DDNS Setting	32
4.2.7 Traffic shaping	32
4.2.8 Outbound Firewall.....	33
4.2.9 Inbound Firewall	36
4.2.10 NAT Settings.....	37
4.3 Power Over Ethernet Configuration.....	39
4.3.1 PoE control.....	39
4.3.2 PoE Schedule.....	41
4.3.3 PoE Status	42
4.4 Switch Configuration.....	42
4.4.1 Port Status.....	42
4.4.2 Port Control	43
4.4.3 VLAN Configuration	44

4.4.4	Rate Control	46
4.4.5	Port Statistics.....	47
4.5	Traffic Prioritization	47
4.5.1	QoS Setting	48
4.5.2	Cos-Queue Mapping.....	49
4.5.3	DSCP-Queue Mapping	49
4.6	Multicast Filtering.....	50
4.6.1	IGMP Snooping	51
4.6.2	IGMP Query.....	52
4.7	Network Redundancy	53
4.7.1	STP Port Configuration	53
4.7.2	STP Port Configuration	55
4.7.3	STP Information.....	55
4.7.4	Redundant Ring Configuration.....	56
4.7.5	Redundant Ring Information	57
4.7.6	Redundant GW.....	58
4.7.7	VRRP	59
4.8	Cellular.....	61
4.8.1	Basic Settings.....	61
4.8.2	SIM Security	64
4.8.3	Mobile Manager Setting	65
4.9	VPN	66
4.9.1	Status	67
4.9.2	OpenVPN Client	68
4.9.3	OpenVPN Server	71
4.9.4	Port Forwarding	73
4.9.5	VPN Certificate	74
4.9.6	IPSec.....	74
4.10	Security.....	77
4.10.1	Port Security	77
4.11	Management.....	78

4.11.1 OPCUA Setting	78
4.11.2 Remote Settings.....	79
4.11.3 SMTP Configuration	82
4.11.4 Login Settings	83
4.11.5 Firmware Upgrade.....	83
4.11.6 Configuration File	84
4.11.7 Remote IP Scan	84
4.11.8 Topology Discovery	85
4.12 Tools	86
4.12.1 System Log.....	86
4.12.2 Ping Watchdog.....	87
4.12.3 Ping	88
4.13 Main Entry.....	88
4.13.1 Save	89
4.13.2 Logout	89
4.13.3 Reboot.....	90
Chapter 5 Configuration – SNMP, View Utility	92
5.1 SNMP.....	92
5.1.1 What is SNMP?	92
5.1.2 Management Information Base (MIB):.....	93
5.2 Command Line Interface (CLI).....	94
5.2.1 Show Command Set:.....	95
5.2.2 Set Command Set:	98
5.2.3 Delete Command Set:.....	100
5.3 i-View Utility.....	101
5.3.1 Device Discovery:.....	101
5.3.2 Basic Tools Shortcut:	101
Chapter 6 Troubleshooting	104
6.1 General Question	104
6.1.1 How to know the MAC address of the product?.....	104

6.1.2	What if I would like to reset the unit to default settings?	104
6.1.3	What if I can not access the Web-based management interface?	104
6.2	Cellular	104
6.2.1	What if the Cellular connection is not stable, poor performance after associating with the base station?	105
6.2.2	What if the Cellular connection is always disconnected, how to resolve it?	105
6.2.3	Why the backup Cellular connection is not active?	106
6.3	Appendix	107
6.3.1	ASCII	107
Revision History		108



Chapter 1

Introduction

Chapter 1 Introduction

1.1 Introduction

The user manual is applied to Industrial Wireless PoE Switch-LTE series. The Industrial Wireless PoE Switch-LTE series is an industrial grade Cellular LTE Router with multiple PoE and SFP Fiber Ethernet Ports. The product equips with next generation 4G Long Term Evolution (LTE) module, which supports up to 100M DL and 50M DL, two Gigabit 802.3at PoE Ports supports up to 30W power source to power devices.

Two 100/1000Base-X SFP Fiber port design provides great flexibility for field installation. The LAN switch ports supports flexibility for field installation. The LAN switch ports supports wire speed switch, Ring Redundancy Protocol, 256 VLANs, QoS traffic prioritizing and can be integrated with Managed Switch.

The product supports Cellular communication features, such as the multiple ports to LTE NAT routings, dual SIM standby, SNMP, LLDP and Mobile Manager Server for remote monitoring. The OPC UA is designed for industrial M2M communication, a popular protocol for industrial automation and M2M applications.

The product also provide different type VPN Client technology and 1-1 OpenVPN Server for secure M2M connectivity. The product supports dual 54V(50-57V)DC input, Digital Output and -40~75°C wide operating temperature.

Model Name	4G LTE	3G UMTS/ HSPA	SIM	USB/DO/COM
JetWave2714GF-LTE-E	LTE-E	Backward Compatible	2	1 x DO
JetWave2714GF-LTE-U	LTE-U	Backward Compatible	2	1 x DO

Model Name	Ethernet	Operating Temp.
JetWave2714GF-LTE-E	2xGT 802.3at PoE + 2x 100/1000M SFP	-40~75°C
JetWave2714GF-LTE-U	2xGT 802.3at PoE + 2x 100/1000M SFP	-40~75°C

- LTE-E: 800(20)/900(8)/1800(3)/2600(7)/2100(1)MHz, Backward compatible WCDMA FDD Band 8/3/1
- LTE-U: 700(13)/700(17)/850(5)/AWS(4)/1900(2)MHz, Backward compatible WCDMA FDD Band 5/4/2

1.2 Product Package

The product package you have received should contain the following items.

Package:

Product Unit

Quick Installation Guide

Default Antennas, 2x LTE (Black color)

Din-Rail Mounting Kit (Pre-installed)

6-pin Power Input connector

Note: Please download the Utility, User Manual from our Web Site.

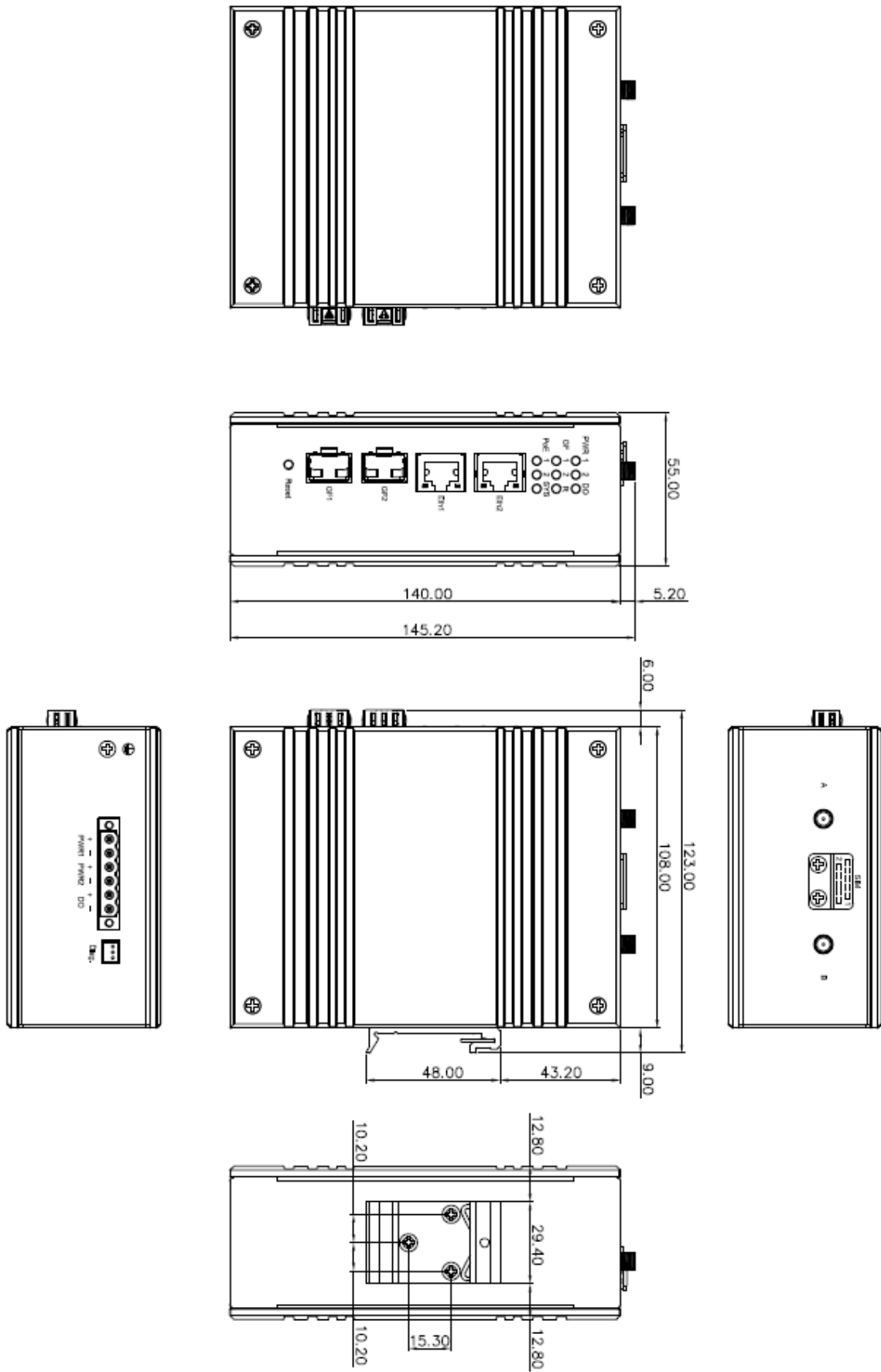
Note 1: Check the web site order information for new accessories, new version user manual, MIB file, firmware and Utility.

Note 2: Different model may have different number of the accessories. If you are not familiar with the feature of the accessories, please consult with our Sales or Technical Service Engineer.

1.3 Major Features

- Long Term Evolution (LTE) technology, 2x2 DL-MIMO, max. 100MDL/50M UL
- 2xGigabit 802.3at PoE ports, 2x100/1000Base-X SFP fiber ports, Wire-speed Switching
- IEEE 802.3at Power Source Equipment, up to 30W, per port, Link Partner Detection Protocol, Power, budget control, PD Auto Reset
- Support Ring Redundancy protocol, 256 VLAN and QoS can be integrated with our Managed Switch
- Support LAN to LTE NAT Routing, Dual SIM Redundancy, Ring Redundant Gateway, Virtual Router Redundancy Procotol(VRRP)
- NAT/Firewall/DMZ and Secure VPN Connectivity
- OPCuA for Industrial M2M Communication, SNMPv2c/v3 for NMS, LLDP, Mobile IP Management
- Dual DC 54V input, -40~75°C operating temperature
- R&TTE, EN 50121-4(TBD), NEMA TS-2(TBD), UL (TBD)

1.4 Dimension





Chapter 2

Hardware Installation

Chapter 2 Hardware Installation

This chapter describes safety precautions and product information before installing JetWave2714GF-LTE Series.

2.1 Professional Installation Required

1. Please seek assistance from a professional installer for field installation or professional IT Engineer for indoor installation. These engineers must be well trained in the RF installation and knowledgeable for the LTE setup and field plan.
2. The product is distributed through distributors and system installers with professional technicians and will not be sold directly through retail stores.

2.1.1 Safety Precautions

To keep you safe and install the hardware properly, please refer to the safety precautions in the front pages of this manual. **The Safety Precautions described in the front pages include General Notification, Power Source & Grounding Notification, Environment & Housing Notification and Installation Notification.**

Additional Notification for the product:

1. The DC power circuit of the product is not isolated design circuit. In practical, it is suggested to use isolated DC power design PSU for field installation. Besides the PSU selection, well digital/earth grounding is also important before power on the system. Connect the Ethernet Cables, Antennas or Antenna RF Cables, Serial Cable, Digital Output circuit, Ground and Power Terminal Block well before powering on.
2. If you are installing the product in the field box, for your safety as well as others', please seek assistance from a professional installer who has received safety training on the hazards involved. Keep safety as well as performance in mind when selecting your installation site, especially where there are electric power and phone lines. Please note the following things as well:
 - ◆ Do not use a metal ladder
 - ◆ Do not work on a wet or windy day
 - ◆ Wear shoes with rubber soles and heels, rubber gloves, long sleeved shirt or jacket.
3. If you are installing the product in the indoor office or factory, be aware of the power source and

grounding must be well installed. The professional Wireless IT Engineer can provide service for location, antenna and field plan to get better performance and coverage.

4. You are responsible for undertaking suitable lightning protection. Install over voltage protector devices on every outdoor Ethernet cable. Protect antennas installed outside with lightening protection devices, ex: lightening arrester.

Note that Field EMD (Lightning) DAMAGE IS NOT COVERED UNDER WARRANTY.

2.2 Power Installation

The system provides dual DC power input.

2.2.1 DC Input

1. There is one 6-pin terminal block within the package, 4 of them are applied for screwing the dual DC wires. It is a good practice to turn off the system power, and to unplug power terminal block before making wire connections.
2. Insert the positive and negative wires into the V+ and V- contact on the terminal block connector. Tighten the wire-clamp screws to prevent DC wires from being loosened. The range of the suitable electric wire is from 19 to 24 AWG.
3. The typical and suggest power source is DC 54V
4. The dual DC power can be redundant. You can connect one power to typical power source and the other to battery/UPS as backup.
5. If you connect the wrong positive/negative wires, the system would not be power on or cause unexpected error. Please avoid this in field installation.

Note: The DC power circuit of the product is not isolated design circuit. In practical, it is suggested to use isolated DC power design PSU for field installation. Besides the PSU selection, well digital/grounding is also important before power on the system.

2.3

2.3 I/O Configuration

2.3.1 Wiring your Ethernet Port

There are 4 Gigabit Ethernet ports, 2 standard RJ-45, IEEE802.3 at 30W High power PoE ports and 2 SFP type Fiber Interface for LAN.

The standard RJ-45 form factor copper ports can support 10Base-TX, 100Base-TX and 1000Base-T. All the Ethernet ports will auto-detect the signal from connected devices to negotiate the link speed and duplex mode. Auto MDI/MDIX allows users to connect another switch, hub or workstation without changing straight through or crossover cables. In some cases, the MDI/MDI-X may requests the connected device support auto-negotiation.

The 2 SFP type Fiber ports support 100Base-X and 1000Base-X speed. The default speed setting is 1000Mbps. If you want to plug in 100M SFP Fiber transceiver, you MUST change the speed to 100Mbps in management interface first.

Available Ethernet Cable Type:

10Base-T: 2-pair UTP/STP Cat. 3, 4, 5 cable (100m)

100 Base-TX: 2/4-pair UTP/STP Cat. 5 cable (100m)

1000 Base-T: 4-pair UTP/STP Cat. 5 cable (100m)

Cable Request in Harsh environment: CAT 5E/CAT 6 is preferred for Data transmission.

Wiring STP Cable: STP (Shielded Twisted Pair) cable is preferred. The device is usually install in harsh environment, part of the EMS protection are based on STP cable, for example the Surge protection of front Ethernet ports. STP cable can provide better field protection. It is MUST for the device installation in harsh environment.

2.3.2 Reset

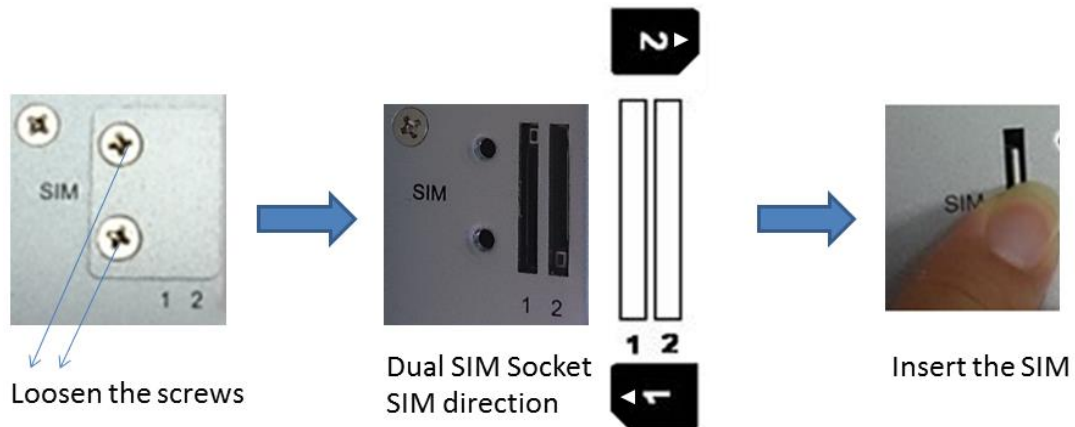
There is one Reset button located on the front of the device. This is designed for user to reboot the system (0~3 seconds) or reset the configuration to default setting (above 7 seconds) in the front of the device.

For some condition, you may need to activate the gateway after installed and hard to unplug/plug the power connector. For example, you forgot insert the SIM before power on, or the system failure to connect 3G base station due to some errors, the "Reset" button allows you reboot the

system in the front panel directly.

2.3.3 SIM Socket

The JetWave2714GF-LTE-E provides dual external SIM (Subscriber Identity Module) socket to store the cellular SIM card. Loosen the screw and then you can plug in the SIM card.



Insert the SIM

- ▶ Unlock the front plate of Dual SIM Socket
- ▶ Insert the SIM card into SIM 1 (**Default startup SIM Socket is SIM 1**) before power on system.
- ▶ The system may take around 1 minute to startup. It searches the SIM card in SIM1 socket and automatically connects to your carrier provider.
- ▶ If the cellular connection is not connected, please go to Web GUI to check the 3G Status and Settings.
- ▶ If you want to use dual SIM socket, it is better to insert the two SIM cards into the system before power on the system. After that enable Cellular Redundant and you can configure SIM 2 as startup or backup SIM socket, please go to Web GUI - Cellular to modify the setting.

Note: The Cellular Redundant is only available while you insert two SIM cards into the socket. If you only insert one, please DO NOT enable Cellular Redundant.

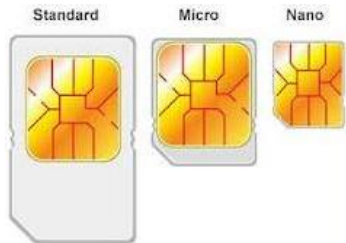
Note: You should not select the empty SIM and press "Connect" for the empty socket in Web GUI. The system can't support this error configuration. The system may display warning message and you must re-select correct SIM, it may request system reboot after changed.

SIM Types:

The supported SIM card is Nano-SIM card. If your carrier provider provides you standard SIM or Micro-SIM, please find the SIM card format carry board for the SIM socket.



The example of the standard SIM card.



The Major type SIM card.

Please DO NOT stick too stick patch on the carry board, if may affect the detection of the SIM card.

Note: While you prepare to plug in the SIM card, please remember to power off the system first. This is a MUST step, it allows the system to detect the SIM card while booting up.

Note: The SIM 1 is the default SIM socket.

2.3.4 Digital Output

The system provides 1 digital output. It is also known as Relay Output. The relay contacts are energized (open) for normal operation and will close for fault conditions. The fault conditions include power failure, Ethernet port link break or other pre-defined events which can be configured in the management interface.

Wiring digital output is exactly the same as wiring power input. Insert the positive and negative wires into the V+ and V- contact on the terminal block connector. Tighten the wire-clamp screws to prevent the wires from being loosened. The range of the suitable electric wire is from 12 to 19 AWG.

2.3.5 Ground

To ensure the system will not be damaged by noise or any electrical shock, you must make exact connection with the Earth Ground. There is one earth ground screw on the bottom side of the device. Loosen the earth ground screw then tighten the screw after earth ground wire is connected.

Note: Well Ground is MUST. Connect the Ethernet cable, Antenna, extended antenna cable and Ground before power on the system. Grounding is important and MUST in field.

2.4 LED Indication

The following table indicates the LED of your device.

LED	Indication	LED	Indication
PWR	PWR1/PWR2 Status Green ON = Power is enough and on Green OFF = No power	DO	Digital Output Status Red ON = The Relay is ON. It may indicate the alarm of specific events. Red OFF = The Relay is OFF
GF	Fiber Port GF1/GF2 Status Green Blinking = GF is Activating Green ON = GF is Link Up. Green OFF = No link	R	Boot Status Green Blinking = Booting Green ON = LTE connected Green OFF = Boot finished
PoE	PoE Output Status Green ON = Delivering PoE power Green OFF = No PD is attached	SYS	System Status Green ON = Power ON Green OFF = Power OFF
ETH	Eth1/Eth2 Status Green ON = Port is Link Up. Green Blinking = Port is Activating Orange color LED is NOT in use.		

2.5 Antenna

The JetWave2714GF-LTE series supports up to 2 antenna sockets. The product attaches LTE antennas inside the package.

2.5.1 Antenna Placement

The placement of the antennas is listed as below:

Antenna	JetWave2714GF-LTE-E	JetWave2714GF-LTE-U
A	LTE-Aux	LTE-Aux
B	LTE-Main	LTE-Main
Total Volume	2	2

Note: There are black covers covered on non-used hole of the mechanical. Please do NOT remove them.

2.5.2 LTE Antenna Specifications

Below figure is the specification of the attached 3G/LTE Antenna.

The Antenna is wide-temperature design; however, it is not water-proof design. If you want to install it in outdoor area, please select water-proof outdoor antenna.

Specifications

Frequency range	824 -894 MHz	900-960 MHz	1710-1880MHz	1910-2170 MHz
Peak gain	1.5dBi	1.0dBi	2.0dBi	4.0dBi
Average gain	-2.5 dBi	-3.5 dBi	-2.5 dBi	-2.0 dBi
VSWR	4.0 : 1 Max.			
Polarization	Linear, vertical			
Impedance	50 Ω			
Connector	RP SMA PLUG			

Environmental & Mechanical Characteristics

Temperature	-40°C to +85°C
Humidity	95% @ 25°C



2.6 Antenna Installation

The product attaches default cellular Antennas. You can install it to the SMA connector directly.

The Antenna Table:

The product supports maximum 2 antenna socket, the SMA type antenna socket is located on the front and top, you can see A, B, wording on the housing.

The table shows the functionality of each SMA socket. Place the correct antenna to the correct socket. The Black color antenna is for Cellular communication, it should be install in A and B..

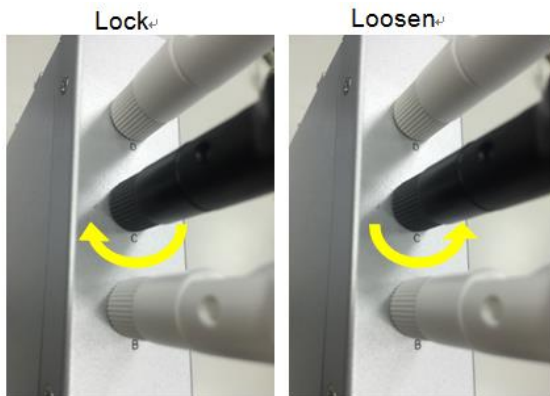
Antenna	JetWave2714GF-LTE-E	JetWave2714GF-LTE-U
A	LTE-Aux	LTE-Aux
B	LTE-Main	LTE-Main
Total Volume	2	2

If you only have one antenna or you only need one stream for transmission, you MUST place the antenna to LTE Main.

Lock the Antenna

The direction to lock the antenna is clockwise direction. The antenna socket is on-board design, it can provide better protection avoid the antenna contact lost in vibration environment.

Note that the counter-clockwise direction will loosen the antenna immediately.



For vibration environment, it is still suggested you install the antenna at non-vibration or low vibration place and connect it by extended Radio cable antenna to the device.

In another practical case, we usually mount the device within the field box to protect water, rain or other reasons, and mount its antennas outside the box. This is because the radio signal MUST be filtered by the metal field box if you install the AP within the box.

JetWave2714GF-LTE-E provides the external antenna mounting kit, extended radio cable as

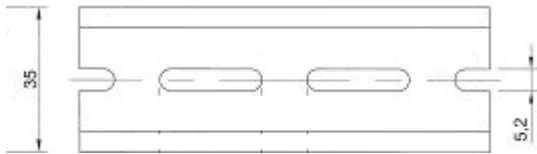
optional accessory. While you need it, you can purchase from Vendor.

For how to mounting the antenna plate, please refer to the chapter 2.7.

2.7 Mounting

2.7.1 Mounting the device

The product supports Din-Rail mounting. The Din-Rail mounting kit is Din 35 compliant and pre-installed in the back of the AP. Mount the product to the 35mm height Din Rail.



2.7.2 Mounting the default antenna for vibration environment

You can purchase our external antenna mount kit accessories. There are antenna mounting L plates and extended RF cable package to ease such mounting installation need. The antenna mounting L plate is available for both N-Type and SMA type antenna.

2.7.3 Mounting the SMA-Type external antenna

If the default antenna is not suitable for your environment, you can purchase the external antenna per your environment need. While selecting the SMA-type external antenna, you must notice that the antenna should support the correct band in your country for radio transmission. You can choose SMA-type antenna and follow the same steps as “Mounting the default antenna on unit” to install your antenna.

2.7.4 Mounting the N-Type external antenna:

If the default antenna is not suitable for your environment, for example the outdoor area, you can purchase the external water-proof N-Type antenna. While selecting the N-type external antenna, you must notice that the frequency band of antenna must comfort to the radio band you

connected.

While mounting the N-Type external antenna, you must need one SMA to N-Type connector or RF cable. Beware that our socket on board is **RP-SMA Female**. That means the end of the extended RF cable to our system should be RP-SMA Male.



Normally, while you purchase the external N-Type antenna, it usually attached antenna mounting kit. If it doesn't provide, the external antenna mounting L plate is available for both SMA and N-Type antenna, you can purchase the external antenna mounting kit from us, please contact with your sales.

2.8 Select the external antenna

Normally, the attached Cellular Antenna is available for most of the indoor applications. Once you install your product in a low signal environment and hope to using the external antenna, Consult your system integrator or our technical support engineer to choose the suitable external antenna with SMA-type or N-Type connector for your application. Different antenna supports different bands, polarization and different range of coverage.

Select the External Cellular Antenna:

Gain: It affects the system performance.

Direction: Typical type includes Omni-Directional or Directional antenna. Check the antenna zone in its specification.

Connector: Check what type it is, for example N-Type, SMA Male/Female.

Antenna Alignment:

- a. Follow the instruction of the antenna installation guide and install the antenna well.
- b. Connect your laptop to the Ethernet port and Install Cellular Speed Test tool in your laptop or connect to the carrier provider's web page, some of them provide the tool in their web site.
- c. Adjust the antenna location, run the Speed Test tool to check the result after changed the location or direction.

Lightning Arrestor:

While you install the external antenna in outside area, the Arrestor is a must accessory to avoid the environment attack through the antenna. The arrestor protects the insulation and conductors of the system from the damaging effects of lightning.

 **Note:**

When prepare the external antenna, make sure the antenna can support 3G connection
Most of high gain external antenna is installed in higher place than AP, get low power lost antenna cable in advance.

While installing the AP within metal field box, connect the extended antenna cable to outside the box is must to avoid the Radio lost.

2.9 Option Antenna Mounting Accessory

The product also provides external antenna mounting plate as optional accessory.

Optional Accessory:

Antenna Mounting L Plate

90cm RG316 Extended SMA Type Radio Cable (Indoor Use)

Antenna Mounting L Plate



90cm RG316 Extended SMA type Radio cable



Note: Consult our sales while you need water-proof outdoor RF cable.

Below figure shows the optional External Antenna Mounting Kit

- a) **Wall-mount Antenna L Plate Kits:** This plate supports SMA or N-Type connector, you can wall-mount it with the attached screws.
- b) **External Radio Cable:** The cable is SMA Male Reverse to SMA Female Reverse RF cable.



Chapter 3

Prepare for Management

Chapter 3 Prepare for Management

The JetWave2714GF-LTE-E Series supports Web GUI Configuration.

The Simple Network Management Protocol (SNMP), Telnet and Diagnostic Interface for management and Window Utility helps you discover the device cross network, basic IP setting, firmware management...etc. The SNMP, Telnet and Utility will be provided in phase 2 firmware.

This chapter describes the preparation for management. In your first time access the device, you can refer to the Basic Factory Default Settings to know the default settings and the default IP of the device. The chapter also tells you how to login the Web-based interface, Diagnostic Console. If you forget IP address you changed, you can use i-View Utility (refer to next chapter) to discover the devices' IP address and then access it.

3.1 Basic Factory Default Settings

We'll elaborate the JetWave2714GF-LTE-E Series basic factory default settings. You can re-acquire these parameters by default. This info is easier for you to find the device and access the product's configuration interface. For further info, please refer to configuration guide of the feature set.

Table 1 JetWave2714GF-LTE-E Basic Factory Default Settings

Features		Factory Default Settings
Username		admin
Password		admin
Model Name		JetWave2714GF-LTE (depends on which model you access)
LAN IP Address (Default)		
IP Address		192.168.10.1
Subnet Mask		255.255.255.0
DHCP Server Setting	DHCP Server	Enable
	DHCP IP Range Start	192.168.10.100
	DHCP IP Range End	192.168.10.200
	DHCP Subnet Mask	255.255.255.0
	DHCP Gateway	192.168.10.1
	(Refer to the System – IP Setting for further info.)	
Diagnostic CLI	Console Type	3-pin (Tx, Rx, GND) in internal Refer to the appendix B, RS232 to 3-pin pin assignment. Reserved for Engineering Diagnostic.
	Baud Rate	115,200

	Parameter	N, 8, 1
Cellular (3G/LTE)	SIM Socket	Default: SIM 1
	Cellular Redundant	Disable. Note: Only available when insert two SIM card.
	Cellular Connect	Automatically after SIM insert and Power on.
	Others SIM Settings	According to your SIM card setting.
	SIM Security	None.

3.2 System Requirements

Before configuration, please make sure your system meets the following requirements:

- A computer coupled with 10/100/1000 Base-T(X) adapter;
- Configure the computer with a static IP address of 192.168.10.x (X cannot be 0, 1, nor 255), as the default IP address of JetWave2714GF-LTE-E Series is 192.168.10.1. Connect the computer to the LAN port, GT1 ~GT2.
- A Web browser on PC for configuration such as Microsoft Internet Explorer 6.0 or above, Google Chrome or Firefox.

Note: If you want to do throughput test, not just configure the switch, please notice that the throughput of the high performance and low performance CPU must be different.

3.3 How to Login the Web-based Interface

The system provides you with user-friendly Web-based management tool.

Open IE and enter the IP address (Default LAN IP: **192.168.10.1**) into the address field. You will see the WELCOME page as below.

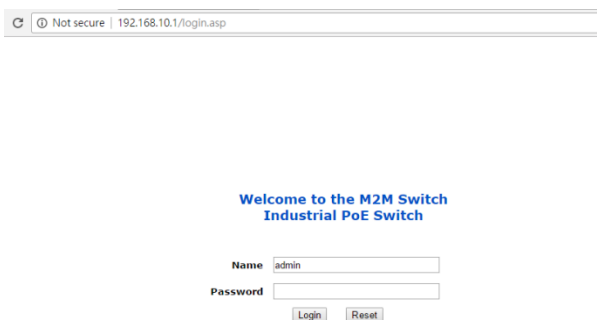


Figure - Login Page

Enter the name of Account (Default: **admin**) and password (Default: **admin**) respectively and click “**Login**” to login the main page of the device. As you can see, this management interface provides main options in the above, which are **Status, System, Power Over Ethernet, Switch Configuration, Traffic Prioritization, Multicast Filtering, Network Redundancy, Wireless, Cellular, VPN, Security, Management, Tools, Save, Reboot** and **Logout**.

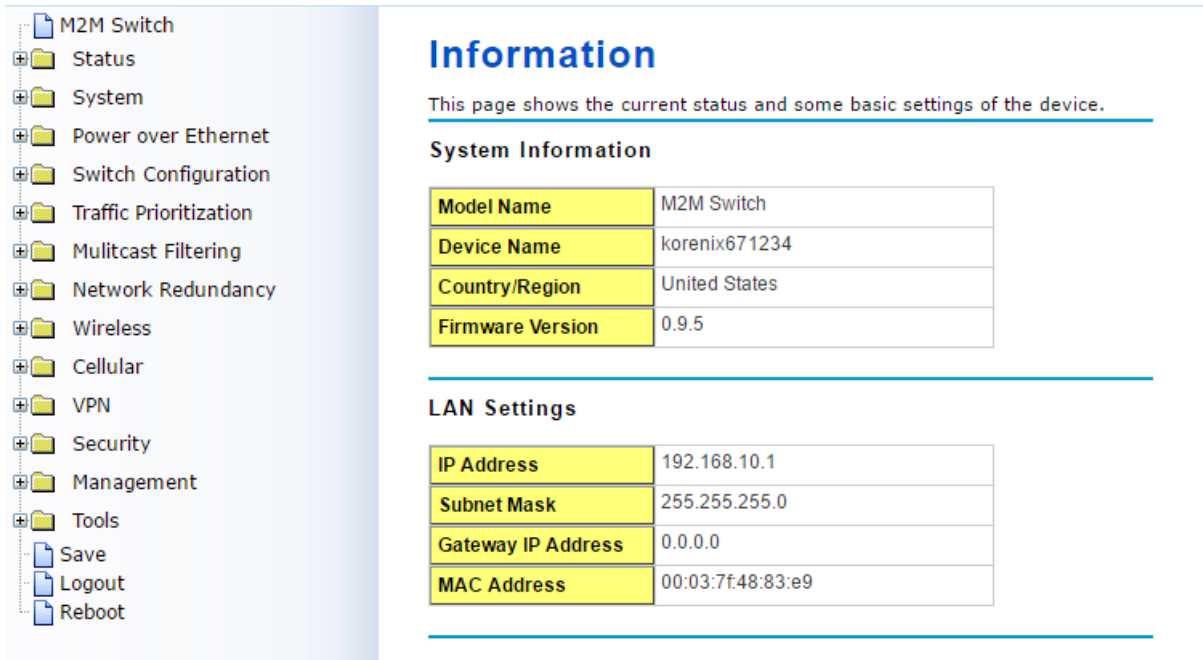


Figure - Main Page

Note:

The username and password are case-sensitive!

3.4 Fail to login the Web GUI

If you failed to login the web GUI, there are something you can do for troubleshooting.

1. Normally, you can access the device by using any kind of Window based Web browser, such as Microsoft Internet Explorer, Google Chrome, Firefox..., to configure and interrogate the product from anywhere on the network. If you failed access in either of the above Web browser, this might be the interoperability issue among your PC, OS version, Web browser and our product. You can try another Web browser as first self-aid, it usually works.
2. Please disable the firewall setting of your browser. The firewall setting may block the connection from your PC to the device. Note that after finished the setting, re-enable your firewall to protect your PC.
3. Check the IP Setting, your PC and managed device must be located within the same subnet.
4. Check whether the connected ports are connected well. Or if the ports are assigned to different IP

addresses.

5. The Web UI connection session of the device will be logged out automatically if you don't give any input after 30 seconds. After logged out, you should re-login and key in correct user name and password again.
6. Please contact technical engineer once you have problem for login.



Chapter 4

Web GUI Configuration

Chapter 4 Web GUI Configuration

This chapter describes the Web GUI for Software Configuration.

4.1 Status

The Status feature set includes **Information**, **Network Flow**, **ARP Table**, **DHCP Client List** and **Association List**. It allows you to see the information of the device.

4.1.1 Information

This page shows the current status and some basic setting of the device.

The screenshot shows the Web GUI for the M2M PoE Switch-LTE-E. On the left is a navigation tree with the following items: M2M PoE Switch-LTE-E, Status (expanded), Information, Network Flow, ARP Table, DHCP Client List, System, Switch Configuration, Traffic Prioritization, Network Redundancy, Cellular, VPN, Security, Management, Tools, Save, Logout, and Reboot. The main content area is titled "Information" and contains the following sections:

Information
This page shows the current status and some basic settings of the device.

System Information

Model Name	M2M PoE Switch-LTE-E
Device Name	devName
Firmware Version	0.5

LAN Settings

IP Address	192.168.10.1
Subnet Mask	255.255.255.0
Gateway IP Address	0.0.0.0
MAC Address	00:12:77:ff:55:02

Cellular Settings

SIM	1
Provider	NONE
APN	internet
Service Type	No Service
IMEI	358709050430440
Signal Strength	0 dBm
SIM1 Status	SIM Not Inserted
SIM2 Status	SIM Not Inserted
Connection Status	Disconnected

System Information: The Model Name, Device Name, and Firmware version number.

LAN Settings: It shows the IP Address, Subnet Mask, Gateway IP Address and MAC Address of the LAN interface.

Cellular Settings: It shows the SIM number, Carrier Provider name, APN name, Service Type, IMEI number, Signal strength, SIM1 status, SIM2 status and Connection status.

Cellular Settings	
SIM	1
Provider	VIBO
APN	internet
Service Type	UMTS
IMEI	358884050574461
Signal Strength	-99 dBm(Low)
SIM1 Status	SIM OK
SIM2 Status	SIM Not Inserted
Connection Status	Connected
IP Address	10.144.251.129

SIM: The SIM card number. 1 or 2 is depends on which SIM you selected in Cellular Basic Settings.

Provider: The name of the ISP.

APN: The APN (Access Point Name) name provided by your ISP.

Note: Some of the ISP asks specific APN name, you have to configure in Basic Settings first, please refer to the instruction in next page.

Service Type: After 3G/LTE connected, the connected ISP will update the service type here. The possible types are GSM, UMTS, GSM w/EGPRS, UMTS w/HSDPA, UMTS w/HSDPA and HSUPA, E-UTRAN, Unknown, No Service (default value)

Note: The cellular service is mainly applied for HSPA/LTE data communication. The rest of services are backward compatible service to avoid lost while HSPA/LTE is not available.

IMEI: It shows the International Mobile Equipment Identity (IMEI) of the Cellular module.

Signal Strength: The signal strength to the remote connected base station. If the signal strength shows low, please change the AP/Gateway location or mounting the antenna in better location.

Below are the signal strength definitions in our system:

0 dBm (Default value while no connection, or Read the Signal Strength error.)

-113 dBm or less (Low)

-51 dBm or greater (Excellent)

Not known or not detectable

SIM Status:

SIM OK: The SIM card is okay to use.

SIM not inserted: The SIM card is not inserted.

SIM PIN Locked: The SIM card is locked due to PIN error. It may be caused by error typing PIN password many times. Please check with your ISP to resolve the issue.

SIM is deactivated: The SIM card may have some problem. Please check with your ISP to resolve the issue.

Connection Status:

Connected: The 3G/LTE interface is connected to the base station.

Not Connected: The 3G/LTE interface is not connected to the base station.

IP Address: The IP Address assigned by the ISP. While the 3G/LTE is connected, the IP address will display here. If there is no 3G/LTE connection, the field will be hidden.

4.1.2 Network Flow (Statistics):

This page shows the packet counters for transmission and reception, it includes system current device interfaces: **Cellular** interface. Cellular means 3G or LTE.

The screenshot shows a web interface titled "Statistics". Below the title is a description: "This page shows the packet counters for transmission and reception regarding to wireless and ethernet networks." There is a "Poll Interval" field set to "5" with a unit of "(0-65534) sec", and buttons for "Set Interval" and "Stop". Below this is a table with columns "Received" and "Transmitted". Under the "Cellular" section, the table shows "Total Packets" and "Total Bytes" both at 0. A "Refresh" button is located at the bottom.

	Received	Transmitted
Cellular		
Total Packets	0	0
Total Bytes	0	0

Poll Interval: The poll interval time setting, range from 0~65524 seconds. If you want to change the poll interval time, press “Stop” and then enter new value, press “Set Interval” to activate.

Set Interval: Set new Interval time after enter new poll interval time.

Stop: Stop polling the associated clients.

Refresh: Refresh the table.

4.1.3 ARP Table

This table shows the ARP table.

The screenshot shows a web interface titled "ARP Table". Below the title is a description: "This table shows ARP table." There is a table with columns "IP Address", "MAC Address", and "Interface". The table contains one entry: IP Address 192.168.10.95, MAC Address 08:9E:01:BF:A8:87, and Interface br0. A "Refresh" button is located at the bottom.

IP Address	MAC Address	Interface
192.168.10.95	08:9E:01:BF:A8:87	br0

IP Address: The IP Address learnt from the interface.

MAC Address: The MAC Address learnt from the interface.

Interface: The interface which learnt the ARP packet (IP and MAC Address).

Refresh: Refresh the table.

4.1.4 DHCP Client List

This table shows the assigned IP address, MAC address and expire timer of the connected DHCP client device.

DHCP Clients
This table shows the assigned IP address, MAC address and time expired for each DHCP leased client.

IP Address	MAC Address	Time Expired(s)
192.168.10.100	68:76:4f:f3:86:78	86398

Refresh

IP Address: The assigned IP address of the connected DHCP client device.

MAC Address: The MAC Address of the connected DHCP client device.

Time Expired(s): The DHCP expire timer connected DHCP client device. Time unit is second. The number can be changed in DHCP Server Lease Time setting.

Refresh: Refresh the table.

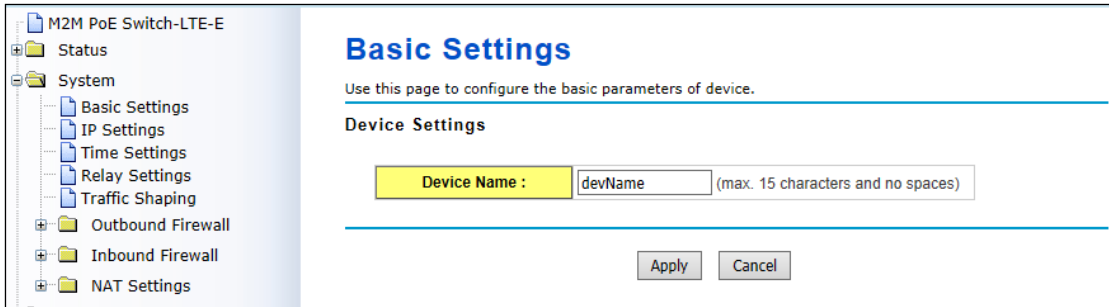
4.2 System

For users who use the JetWave2714GF-LTE-E for the first time, it is recommended that you begin configuration from the “**System**” feature set pages shown below:

In System pages, there are some configuration pages for the system settings. These setups include Basic Settings, IP Settings, Time Settings, Relay Settings, Traffic Shaping, Outbound/Inbound Firewall Settings and NAT Settings, these features are introduced in below pages.

4.2.1 Basic Settings

Use this page to configure the basic parameters of the device.



The screenshot displays the 'Basic Settings' configuration page. On the left, a navigation tree shows the following structure:

- M2M PoE Switch-LTE-E
 - Status
 - System
 - Basic Settings
 - IP Settings
 - Time Settings
 - Relay Settings
 - Traffic Shaping
 - Outbound Firewall
 - Inbound Firewall
 - NAT Settings

The main content area is titled 'Basic Settings' and includes the instruction: 'Use this page to configure the basic parameters of device.' Below this, the 'Device Settings' section features a text input field labeled 'Device Name' with the value 'devName' and a note '(max. 15 characters and no spaces)'. At the bottom of the page, there are 'Apply' and 'Cancel' buttons.

Device Name: User could give a name for identifying a particular outdoor access point in here.

It allows maximum 15 characters and no spaces.

4.2.2 IP Settings

Use this page to configure the IP related parameters for **LAN** interfaces. Here you may change the setting for IP address, subnet mask, Default Gateway, DNS, Static IP or DHCP Server settings...etc.

IP Settings

Use this page to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP address, subnet mask, DHCP, etc..

LAN IP Address Assignment

<input type="radio"/> Use DHCP <input checked="" type="radio"/> Use Static IP Address	
IP Address :	<input type="text" value="192.168.10.1"/>
Subnet Mask :	<input type="text" value="255.255.255.0"/>
Gateway Ip Address :	<input type="text" value="0.0.0.0"/>
DNS 1 :	<input type="text" value="8.8.8.8"/>
DNS 2 :	<input type="text" value="0.0.0.0"/>

LAN Settings :

DHCP Server :	<input type="text" value="Enabled"/> ▼
DHCP IP Address Range Start :	<input type="text" value="192.168.10.100"/>
DHCP IP Address Range End :	<input type="text" value="192.168.10.200"/>
DHCP Subnet Mask :	<input type="text" value="255.255.255.0"/>
DHCP Gateway :	<input type="text" value="192.168.10.1"/>
WINS1 :	<input type="text" value="0.0.0.0"/>
WINS2 :	<input type="text" value="0.0.0.0"/>
Primary DNS Server :	<input type="text" value="8.8.8.8"/>
Secondary DNS Server :	<input type="text" value="0.0.0.0"/>
Lease Time(15-44640 Minutes) :	<input type="text" value="1440"/>

4.2.3 LAN Setting

IP Address: The IP Address field allows you to set the device's IP address manually.

Subnet Mask: This is the subnet mask address for your LAN interface. Set the IP subnet mask manually.

DHCP Server: Enabled / Disabled (Default Setting is Enable)

After the DHCP Server Enabled, you can continue assign the Start IP and End IP of the DHCP IP Address Range, the device allows you assign up to one Class C, 255 IP Addresses. Since the maximum connection session is 64, configuring 64 IP addresses is enough for the need.

You can also configure the **Subnet Mask, DHCP Gateway, WINS, Primary/Secondary DNS, Servers' IP Address** and **Least Time** of the assigned IP addresses.

4.2.4 Time Settings

Use this page to configure the **Time Settings**. You can configure current time, time zone and configure NTP protocol to synchronize system time with a public time server over the internet.

Current Time: You can manually type the current time or get the time from you PC. Click “**Get PC time**”, the current time will be updated according to your PC’s time.

Time Zone: Select the time zone of your country from the dropdown list.

NTP: You can select “**Enable NTP client update**” in this page, then the NTP feature will be activated and synchronize from the remote time server.

NTP Server: Select the time server from the “NTP Server” dropdown list or manually input the IP address of available time server into “Manual IP”.

Press “**Apply**” to activate the settings.

4.2.5 Relay Setting

Use this page to configure the Link Failure Relay.

Select **GT1**, **GT2**, **GF1**, and **GF2** port or all of link failure and press “Apply” to activate the settings.

Relay Settings

You can bind the events to Relay.

Relay:	
Link Failure:	Port <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4

4.2.6 DDNS Setting

Use this page to configure the parameters for DDNS (Dynamic Domain Name System) client. Since Not every carrier provider provide fixed IP service and the dynamic IP address of cellular interface may be changed very often, it's hard to remotely manage the devices' IP address. Then you can use DDNS domain name instead fixed IP address. You can apply the DDNS domain name, User Name and password from the companies which provide DDNS service through internet. The device now supports "dyndns.org", "freedns.afraid.org" and "no-ip.com" services.

DDNS Settings

Use this page to configure the parameters for DDNS(Dynamic Domain Name System) client.

Enable DDNS Client

Server:	dyndns.org ▼	
Domain Name:	dyndns.org dyndns.org(custom)	<input type="text"/>
User Name:	dyndns.org(static) freedns.afraid.org	<input type="text"/>
Password:	no-ip.com	<input type="text"/>
Confirm Password:	<input type="text"/>	

Apply Cancel

Use this page to configure the DDNS settings. Select the Server, the Domain Name, User Name and Password you applied.

4.2.7 Traffic shaping

Use this page to specify the incoming and outgoing traffic limit.

Enable Traffic Shaping: Select the item to activate the feature. After enabled it, you can continue configure the "Incoming Traffic Limit", "Incoming Traffic Burst", "Outgoing Traffic Limit" and "Outgoing Traffic Burst" with K bits per second.

Traffic Shaping

Use this page to specify the incoming and outgoing traffic limit.

Enable Traffic Shaping

Incoming Traffic Limit:	1024000	kbit/s
Incoming Traffic Burst:	20	kBytes
Outgoing Traffic Limit:	1024000	kbit/s
Outgoing Traffic Burst:	20	kBytes

Press “**Apply**” to activate the settings.

4.2.8 Outbound Firewall

The follow Firewall Settings pages to configure the Firewall setting. There are different types firewall settings, you can enable the setting, configure the rules, check the table you configured and Delete Selected/All rules.

Src IP Filtering: Source IP addresses Filtering from your LAN to Internet through the gateway.

Dest IP Filtering: Destination IP addresses Filtering from the LAN to Internet through the gateway.

Src Port Filtering: Source Ports Filtering from the LAN to Internet through the gateway.

Dest Port Filtering: Destination Ports Filtering from the LAN to Internet through the gateway.

- **Source IP Filtering**

Entries in this table are used to restrict certain types of data packets from your local network to internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Select “**Enable Source IP Filtering**”, type the “**Local IP Address**” and “**Comment**” (note for the entry) and then press “**Apply**” to activate the settings.

Source IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Enable Source IP Filtering

Local IP Address:	
Comment:	

Apply
Cancel

Local IP Address	↕	Comment	↕	Select	Edit
------------------	---	---------	---	--------	------

Delete Selected
Delete All
Refresh

After applied, the Web GUI will show “Change settings successfully”. Click “**OK**” and then you can see the new entry shown in the below table.

- **Destination IP Filtering**

Entries in this table are used to restrict the computers in LAN from accessing certain websites in WAN according to IP address.

Select “**Enable Destination IP Filtering**”, type the “**Destination IP Address**” and “**Comment**” (note for the entry) and then press “**Apply**” to activate the settings.

Destination IP Filtering

Entries in this table are used to restrict the computers in LAN from accessing certain websites in WAN according to IP address.

Enable Destination IP Filtering

Destination IP Address:

Comment:

Apply Cancel

Destination IP Address	Comment	Select	Edit
------------------------	---------	--------	------

Delete Selected Delete All Refresh

After applied, the Web GUI will show “Change settings successfully”. Click “**OK**” and then you can see the new entry shown in the below table.

- **Source Port Filtering**

Entries in this table are used to restrict certain ports of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Select “**Enable Source Port Filtering**”, type the “**Port Range**” of below “**Protocol**” type, the protocol type can be **UDP, TCP or Both**. Type the “**Comment**” (note for the entry) and then press “**Apply**” to activate the settings.

Source Port Filtering

Entries in this table are used to restrict certain ports of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Enable Source Port Filtering

Port Range: -

Protocol: Both ▾

Comment:

Apply Cancel

Source Port Range ▾	Protocol ▾	Comment ▾	Select	Edit
80-88	TCP+UDP		<input type="checkbox"/>	Edit

Delete Selected Delete All Refresh

After applied, the Web GUI will show “Change settings successfully”. Click “**OK**” and then you can see the new entry shown in the below table.

- **Destination Port Filtering**

Entries in this table are used to restrict certain ports of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Destination Port Filtering

Entries in this table are used to restrict certain ports of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Enable Destination Port Filtering

Port Range: -

Protocol: Both ▾

Comment:

Apply Cancel

Dest Port Range ▾	Protocol ▾	Comment ▾	Select	Edit
23	TCP	Telnet only	<input type="checkbox"/>	Edit

Delete Selected Delete All Refresh

Select “**Enable Destination Port Filtering**”, type the “**Port Range**” of below “**Protocol**” type, the protocol type can be **UDP, TCP or Both**. Type the “**Comment**” (note for the entry) and then press “**Apply**” to activate the settings.

After applied, the Web GUI will show “Change settings successfully”. Click “**OK**” and then you can see the new entry shown in the below table.

4.2.9 Inbound Firewall

Inbound Filtering is used to restrict any access from Internet to the Gateway. Only the applied entries in “**Remote Management Exception**” list can access the gateway.

Enable Inbound Firewall: After enabled inbound firewall, it means that all the IP address from the Internet can NOT access the gateway. You can configure “**Remote Management Exception**” for exceptional items that includes **Web, Telnet, SSH** and **SNMP**.

Exception: The exception table allows you to configure the exception list.

Src IP Address: The entry allows you to configure the source IP address from Internet.

Src Port Range: The source port range of the above IP address.

Dest Port Range: The destination port range of the above IP address. [Destination port range can NOT be empty!](#) You should set a value between 1~65535.

Comment: Note for the entry.

Press “**Apply**” to activate the settings.

After applied, the Web GUI will show “Change settings successfully”. Click “OK” and then you can see the new entry shown in the below table.

4.2.10 NAT Settings

NAT is the abbreviation of “Network Address Translation”, it is a methodology of modifying network address information in IP packet headers while they are in transit across a Gateway/Router for the purpose of remapping one IP address space into another. The simple type of NAT provides one to one translation of IP address. It can be used to interconnect two IP networks, normally one network is for Local Area Network and the other network is for Wide Area Network/Internet.

Use the “NAT Settings” pages to configure the NAT setting. There are two main configuration pages, “Port Forwarding”, “DMZ” and “Advanced”.

- **Port Forwarding**

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway’s NAT firewall.

Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway’s NAT firewall.

<input checked="" type="checkbox"/> Enable Port Forwarding	
Public Port Range:	<input type="text"/> - <input type="text"/>
IP Address:	<input type="text"/>
Protocol:	Both ▾
Port Range:	<input type="text"/> - <input type="text"/>
Comment:	<input type="text"/>

Public Port Range	Local IP Address	Protocol	Port Range	Comment	Select	Edit

Select “Enable Port Forwarding” and then type the parameters to create the port forwarding entries.

Public Port Range: Configure the port range which will be public to WAN/Internet. You can configure one or a range of TCP/UDP port number.

IP Address: Configure the IP Address of the LAN PC. The traffic from the public port range will be redirected to this IP address.

Protocol: Configure TCP, UDP or Both (TCP + UDP) protocol type.

Port Range: Configure the port range of the LAN, the traffic from the public port will be redirected to these port.

Comment: Add information of the entry.

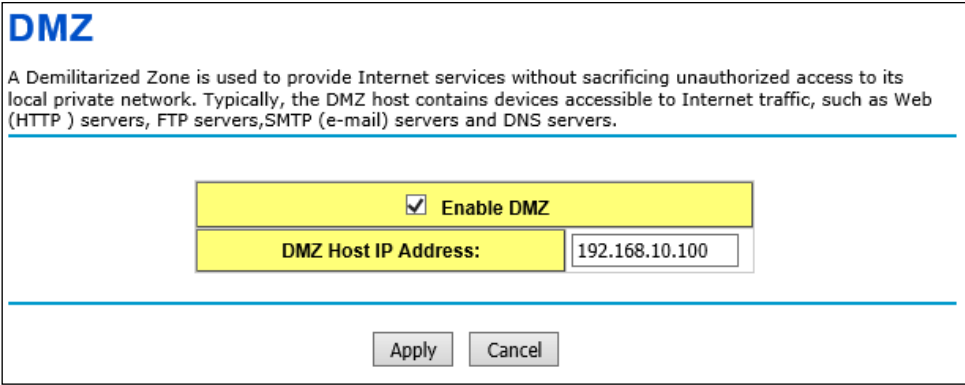
Press “**Apply**” to activate the settings. After applied, there is one popup screen shows you already configured new entry. And then you can see the entries you configure in below.

You can press “**Delete Selected**” to delete selected entries, or “**Delete All**” to delete all entries.

Press “**Refresh**” to update the table.

- **DMZ**

A **Demilitarized Zone** is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains device accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.



The image shows a configuration dialog box titled "DMZ". It contains a descriptive paragraph: "A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers,SMTP (e-mail) servers and DNS servers." Below the text is a yellow button with a checked checkbox and the label "Enable DMZ". Underneath is a label "DMZ Host IP Address:" followed by a text input field containing "192.168.10.100". At the bottom of the dialog are two buttons: "Apply" and "Cancel".

Select “**Enable DMZ**” and assign the IP address of the “**DMZ Host IP Address**”. This is the DMZ computer’s IP address. If you configure the DMZ function for your office network, please make sure this is agreed by the IT administrator.

Press “**Apply**” to activate the settings.

- **Advanced**

The **NAT Advanced** setting will randomize the NAT port mapping.

NAT Advanced setting

Random Port : enable it then nat port mapping will be randomized.

Random Port :	Enabled ▾
----------------------	-----------

4.3 Power Over Ethernet Configuration

The Power over Ethernet is one of the key features of the switch, each PoE port compliant with both 802.3af and 802.3at. The Power Over Ethernet Configuration pages helps you configure PoE Control, PoE Schedule and Check PoE Status.

4.3.1 PoE Control

4.3.2 PoE Schedule

4.3.3 PoE Status

4.3.1 PoE control

The PoE Control page include there major steps, PoEsystem configuration, PoE Port configuration and PD Status alive detection.

- **PoE System Configuration**

PoE Control

System Configuration

PoE System

Power Budget (W) :	<input type="text" value="0"/>
Warning Water Level (%) :	<input type="text" value="0"/>

PoE System: Enable or Disable the system's PoE function. While you want to use PoE function, this is the first step you should enabled.

Budget (W): The maximum output budget of the PoE function. The device support 2 802.3at PoE port, the maximum power budget is 60W.

Warning Water Level(%): The warning level is for system warning to alerts user when PoE system

drawing power that meet the warning level user defined

- **PoE Port Configuration**

Port Configuration

Port	Mode	Powering Mode	Budget(W)	Priority
1	Disabl ▼	802.3af ▼	31	Critica ▼
2	Disabl ▼	802.3af ▼	31	Critica ▼

Apply Cancel

Mode: Enable/Disable the port’s PoE function. You can also enable Priority mode here and configure time table in PoE Schedule setting.

Powering Mode: 802.3af, 802.3at(2-event) and forced mode. Forced mode will ignore the classification behaviors and deliver power to the connected power. While using the forced mode, be noted that you should carefully and check your connected device can support.

Budget (W): It allows user to assign PoE budget of the port. The invalid value is range from 1~31W.

Power priority: it supports 3 levels, Critical, High and low. If the system PoE consumption is over the budget, the PoE system will turn off low priority port first, then high and critical will be the last.

- **PD Status Detection**

PD Status Detection

Enable PD Status Detection

PD	IP Address	Cycle Time(s)	Delete
1	192.168.10.100	300	<input type="checkbox"/>
2			<input type="checkbox"/>

Apply Cancel

The PoE Switch supports the useful function to detect the connected PD status. While the connected device is failure, the system will reset the PoE of the port as the first step aid for field engineer. You can define the setting in this page.

IP address: The IP address of the connected PD of the port.

Cycle time(s): This is the time reserved per duration of PD reboot in second, the invalid time is 10~3600, step by 10 seconds. You can measure the PD reboots duration time first. Normally, the IP camera will take at least 40~50 seconds. Once you define this function, the PoE Switch will turn-off PoE power while connected PD does not echo the request. After the duration time (cycle time), the PoE switch will

start request PD again. This function also named link partner line detection (LPLD).

Delete: Click Delete and Apply can delete the settings.

Note: During the PoE operating, the surface will accumulate heat and caused surface temperature becomes higher than ambient temperature. Do remember don't touch device surface during PoE operating

4.3.2 PoE Schedule

The PoE Scheduling control is a powerful function to help you save power and money. You need to configure PoE Scheduling and select a target port manually to enable this function.

PoE Schedule

PoE Schedule on

Time	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
00:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
01:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
02:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
03:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
04:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
05:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
06:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
07:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
08:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
09:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
14:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
15:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
16:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
17:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
18:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
19:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
20:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
21:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
22:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
23:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The Power over Ethernet schedule supports hourly and weekly base PoE schedule configuration. Selecte the target port and marking the time frame, then click Apply to activate the PoE scheduling function. The PoE port will working as the predefined behavior and follows the system clock. As this

result, be sure the system clock have configured as your local time for the reference of scheduling control.

4.3.3 PoE Status

The PoE Status page shows the operating status of each PoE Port. The information includes PoE mode, Powering Status, PD class, Power Budget(W), Power Consumption(W), Voltage and Current of the connected device. Following port 2 is an example of one PoE IP Camera.

PoE Status

Port	Mode	Status	Class	Budget(W)	Consumption(W)	Voltage(V)	Current(mA)
1	Schedule	Off	---	---	0.0	0.0	0.0
2	Enable	Powering	Class2	7	2.33	46.7	50.0

Refresh

4.4 Switch Configuration

The Switch Configuration group helps you to enable/disable port status, configure port auto-negotiation, speed, and duplex, flow control, rate limit control and VLAN. It also allows you to view port status and port statistics.

Following commands are included in this group:

4.4.1 Port Status

4.4.2 Port Control

4.4.3 VLAN Configuration

4.4.4 Rate Control

4.4.5 Port Statistics

4.4.1 Port Status

Port Status shows you current port status.

Port Status

Port	Link	Speed/Duplex	Flow Control	SFP Vendor	Wavelength	Distance
1	Up	1000 Full	Disable	---	---	---
2	Up	100 Full	Disable	---	---	---
3	Down	1000 Full	Disable	---	---	---
4	Down	1000 Full	Disable	---	---	---

Refresh

Link: Up or Down.

Speed/Duplex: Port speed (10, 100 or 1000) and duplex (Full or half).

Flow Control: The status of flow control.

SFP Vendor: Vendor name of the SFP transceiver you plugged.

Wavelength: The wave length of the SFP transceiver you plugged.

Distance: The distance of the SFP transceiver you plugged.

Refresh: Reload the all port information.

Note: Most of the SFP transceivers provide vendor information which allows your switch to read it. The UI can display vendor name, wavelength and distance of all SFP transceiver family. If you see Unknown info, it may mean that the vendor doesn't provide their information or that the information of their transceiver can't be read.

4.4.2 Port Control

Select the port you want to configure and make changes to the port.

PortControlSetup

Use this page to configure the switch. To change SFP speed you need to save configuration to flash and reboot the system to make it effective

Port	State	Speed/Duplex	Flow Control
1	Enable ▼	AutoNegotiation ▼	Disable ▼
2	Enable ▼	AutoNegotiation ▼	Disable ▼
3	Enable ▼	1000 ▼	Disable ▼
4	Enable ▼	1000 ▼	Disable ▼

Apply

Cancel

State: Enable or disable the state of this port. The default setting is Enable which means all the ports are workable when you receive the device.

Speed/Duplex: You can configure port speed and duplex mode at each port.

1, 2: Factory Default is “**Autonegotiation**”, it will based on transmission to auto negotiate the speed and duplex mode. You can also select **10 Full**, **10 Half**, **100 Full** or **100 Half**.

3, 4: The ports represent the SFP fiber ports. Factory default is **1000**, it means the port is in gigabit speed. Need to configure to **100** if you use 100M SFP transceiver.

Flow Control: Enable or disable Flow Control. Enable means that you need to activate the flow control function of the remote network device in order to let the flow control of that corresponding port on the switch to work. “Disable” means that you don’t need to activate the flow control function of the remote network device, as the flow control of that corresponding port on the switch will work anyway.

Press “**Apply**” to activate settings.

Note: It is necessary to reset system, if the SFP configuration was changed.

4.4.3 VLAN Configuration

JetWave2714GF-LTE-E supports 802.1Q VLAN. 802.1Q VLAN is also known as Tag-Based VLAN. This Tag-Based VLAN allows VLAN to be created across different switches. IEEE 802.1Q tag-based VLAN makes use of VLAN control information stored in a VLAN header attached to IEEE 802.3 packet frames. This tag contains a VLAN Identifier (VID) that indicates which VLAN a frame belongs to. Since each switch only has to check a frame’s tag, without the need to dissect the contents of the frame, this also saves a lot of computing resources within the switch.

VLAN Configuration group enables you to Add/Remove static VLAN, configure Management VLAN ID, Port PVID, Egress parameters and view VLAN table.

VLAN Configuration

PVID Setting

Port	1	2	3	4
PVID	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>

Management VLAN ID :	<input type="text" value="1"/> (1-4094)
----------------------	---

Add Static VLAN

VLAN ID	1	2	3	4
<input type="text"/>	<input type="button" value="Untag ▼"/>	<input type="button" value="Untag ▼"/>	<input type="button" value="Untag ▼"/>	<input type="button" value="Untag ▼"/>

Static VLAN Overview

Vlan ID	1	2	3	4	Select	Edit
1	Untag	Untag	Untag	Untag	<input type="checkbox"/>	<input type="button" value="Edit"/>

PVID Setting: PVID is the abbreviation of the Port VLAN ID. Enter port VLAN ID here. PVID allows the switches to identify which port belongs to which VLAN. To keep things simple, it is recommended that PVID is equivalent to VLAN IDs. The values of PVIDs are from 1 to 4095. But, 1 and 4095 are reserved. You can't input these 2 PVIDs. 1 is the default value. 2 to 4094 are valid and available in this column. Type the PVID you'd like to configure here.

Press "**Apply**" to activate settings.

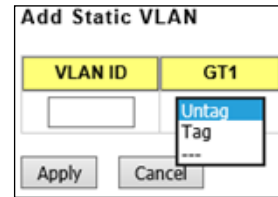
Management VLAN ID: The management VLAN ID is the VLAN ID of the CPU interface so that only member ports of the management VLAN can ping and access the switch. The default management VLAN ID is 1.

Add Static VLAN: Assign VLAN ID for new VLAN, and specify the egress (outgoing) rule to be Untag or Tag on each port.

Untag: Indicates that egress/outgoing frames are not VLAN tagged.

Tag: Indicates that egress/outgoing frames are to be VLAN tagged.

-- : Not available



Press “**Apply**” to activate settings.

Static VLAN Overview: The table shows static VLAN status.

Select: Check “Select” with “**Delete Selected**” to delete the selected entry.

Edit: Edit entries for the Route Entry.

Delete all: Delete the all entries.

Refresh: Reload the table.

4.4.4 Rate Control

“**Limit Packet Type and Rate**” is a form of flow control used to enforce a strict bandwidth limit at a port. You can program separate transmit (Egress Rule) and receive (Ingress Rule) rate limits at each port, and even apply the limit to certain packet types.

Rate Control

Ingress Rate : Range is from 1 Mbps to 1000 Mbps and Zero means no limit. Increments of 1Mbps. Egress Rate : 1 Mbps to 100 Mbps, increments of 1Mbps. 100 Mbps to 1000 Mbps, increments of 10Mbps. Zero means no limit.

Limit Packet Type and Rate

Port	Ingress Rule		Egress Rule	
	Packet Type	Rate(Mbps)	Packet Type	Rate(Mbps)
1	Broadcast Only ▼	10	All	0
2	Broadcast Only ▼	10	All	0
3	Broadcast Only ▼	10	All	0
4	Broadcast Only ▼	10	All	0

Apply Cancel

Packet type: You can select the packet type that you want to filter. The packet types of the Ingress Rule listed here include **All**, **Broadcast Only**, **Broadcast/Multicast** and **Broadcast/ Multicast/ Unknown Unicast**. The packet types of the Egress Rule (outgoing) only support all packet types.

Rate: This column allows you to manually assign the limit rate of the port. Valid values are from 1Mbps-1000Mbps, and Zero means no limit.

Ingress Rate: Increments of 1Mbps.

Egress Rate: 1 Mbps to 100 Mbps, increments of 1Mbps. 100 Mbps to 1000 Mbps, increments of 10Mbps.

Click on “**Apply**” to apply the configuration.

4.4.5 Port Statistics

In this page, you can view operation statistics for each port.

Port Statistics

Port	Link	Rx Good	Rx Bad	Rx Abort	Tx Good	Tx Bad	Collision	Select
1	Up	26956	0	0	17739	0	0	<input type="checkbox"/>
2	Up	499	0	0	472	0	0	<input type="checkbox"/>
3	Down	0	0	0	0	0	0	<input type="checkbox"/>
4	Down	0	0	0	0	0	0	<input type="checkbox"/>

The statistics that can be viewed include **Link State**, **Rx Good**, **Rx Bad**, **Rx Abort**, **Tx Good**, **Tx Bad** and **Collision**. Rx means the received packet while Tx means the transmitted packets.

Select: Check “Select” with “**Delete Selected**” to delete the selected entry.

Delete all: Delete the all Route entries.

Refresh: Reload to refresh the counts.

Note: If you see many Bad, Abort or Collision counts increased, that may mean your network cable is not connected well, the network performance of the port is poor...etc. Please check your network cable, Network Interface Card of the connected device, the network application, or reallocate the network traffic...etc.

4.5 Traffic Prioritization

Quality of Service (QoS) provides traffic prioritization mechanism which allows users to deliver

better service to certain flows. QoS can also help to alleviate congestion problems and ensure high-priority traffic is delivered first. This section allows you to configure Traffic Prioritization settings for each port with regard to setting priorities. JetWave2714GF-LTE-E supports 4 physical queues, weighted fair queuing (WRR) and Strict Priority scheme, which follows 802.1p COS tag and IPv4 TOS/DiffServ information to prioritize the traffic of your industrial network.

4.5.1 QoS Setting

Queue Scheduling: You can select the Queue Scheduling rule as follows:

8,4,2,1 weighted fair queuing scheme: This is also known as WRR (Weight Round Robin). JetWave2714GF-LTE-E will follow 8:4:2:1 rate to process the packets in a queue from the highest priority to the lowest. For example, the system will process 8 packets with the highest priority in the queue, 4 with middle priority, 2 with low priority, and 1 with the lowest priority at the same time.

Strict priority scheme: Packets with higher priority in the queue will always be processed first, except that there is no packet with higher priority.

QoS Setting

Queue Scheduling

- 8,4,2,1 weighted fair queuing scheme
- Strict priority scheme

Port Setting

Port	CoS	Trust Mode
1	0 ▼	CoS Only ▼
2	0 ▼	CoS Only ▼
3	0 ▼	CoS Only ▼
4	0 ▼	CoS Only ▼

Apply Cancel

Port Setting:

CoS: this column is to indicate default port priority value for untagged or priority-tagged frames. When JetWave2714GF-LTE-E receives the frames, it attaches the value to the CoS field of the incoming

VLAN-tagged packets. User can select 0,1,2,3,4,5,6 or 7 to the port

Port	CoS	CoS Only
GT1	0	DSCP Only
GT2	0	CoS First
		DSCP First

Trust Mode: Indicate Queue Mapping types for you to select.

CoS Only: Port priority will only follow CoS-Queue Mapping you have assigned.

DSCP Only: Port priority will only follow DSCP-Queue Mapping you have assigned.

CoS first: Port priority will follow CoS-Queue Mapping first, and then DSCP-Queue Mapping rule.

Default priority type is CoS First. The system will provide default CoS-Queue table to which you can refer for the next command.

DSCP first: Port priority will follow DSCP-Queue Mapping first, and then CoS-Queue Mapping rule.

After configuration, press “**Apply**” to enable the settings.

4.5.2 Cos-Queue Mapping

This page is to change CoS values to Physical Queue mapping table. Since the switch fabric of JetWave2714GF-LTE-E supports 4 physical queues, Lowest, Low, Middle and High. Users should therefore assign how to map CoS value to the level of the physical queue. In JetWave2714GF-LTE-E, users can freely assign the mapping table or follow the suggestion of the 802.1p standard. It uses 802.1p suggestion as default values. You can find CoS values 1 and 2 are mapped to physical Queue 0, the lowest queue. CoS values 0 and 3 are mapped to physical Queue 1, the low/normal physical queue. CoS values 4 and 5 are mapped to physical Queue 2, the middle physical queue. CoS values 6 and 7 are mapped to physical Queue 3, the high physical queue.

CoS-Queue Mapping

CoS	0	1	2	3	4	5	6	7
Queue	1	0	0	1	2	2	3	3

Note : Queue 3 is the highest priority queue in using Strict Priority scheme.

4.5.3 DSCP-Queue Mapping

This page is to change DSCP values to Physical Queue mapping table. Since the switch fabric of JetWave2714GF-LTE-E only supports 4 physical queues, Lowest, Low, Middle and High. Users should therefore assign how to map DSCP value to the level of the physical queue. In JetWave2714GF-LTE-

E, users can freely change the mapping table to follow the upper layer 3 switch or routers' DSCP setting.

DSCP-Queue Mapping

DSCP	0	1	2	3	4	5	6	7
Queue	1 ▾	1 ▾	1 ▾	1 ▾	1 ▾	1 ▾	1 ▾	1 ▾
DSCP	8	9	10	11	12	13	14	15
Queue	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾
DSCP	16	17	18	19	20	21	22	23
Queue	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾
DSCP	24	25	26	27	28	29	30	31
Queue	1 ▾	1 ▾	1 ▾	1 ▾	1 ▾	1 ▾	1 ▾	1 ▾
DSCP	32	33	34	35	36	37	38	39
Queue	2 ▾	2 ▾	2 ▾	2 ▾	2 ▾	2 ▾	2 ▾	2 ▾
DSCP	40	41	42	43	44	45	46	47
Queue	2 ▾	2 ▾	2 ▾	2 ▾	2 ▾	2 ▾	2 ▾	2 ▾
DSCP	48	49	50	51	52	53	54	55
Queue	3 ▾	3 ▾	3 ▾	3 ▾	3 ▾	3 ▾	3 ▾	3 ▾
DSCP	56	57	58	59	60	61	62	63
Queue	3 ▾	3 ▾	3 ▾	3 ▾	3 ▾	3 ▾	3 ▾	3 ▾

Note : Queue 3 is the highest priority queue in using Strict Priority scheme.

After configuration, press “**Apply**” to enable the settings.

4.6 Multicast Filtering

For multicast filtering, the Switch uses IGMP Snooping technology. IGMP (Internet Group Management Protocol) is an Internet Protocol that provides a way for internet device to report its multicast group membership to adjacent routers. Multicasting allows one computer on the internet to send data to a multitude of other computers that have identified themselves as being interested in receiving the originating computers data. Multicasting is useful for such applications as updating the address books of mobile computer users in the field, sending out newsletters to a distribution list, and broadcasting streaming media to an audience that has tuned into the event by setting up multicast group membership. In effect, IGMP Snooping manages multicast traffic by making use of switches, routers, and hosts that support IGMP. Enabling IGMP Snooping allows the ports to detect IGMP queries, report packets, and manage multicast traffic through the switch. IGMP has three fundamental types of messages, as shown below:

Message	Description
Query	A message sent from the querier (an IGMP router or a switch) which asks for a response from each host that belongs to the multicast group.
Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host has quit as a member of a specific multicast group.

You can enable IGMP Snooping and IGMP Query functions here. You will see the information of the IGMP Snooping function in this section, including different multicast groups' VID and member ports, and IP multicast addresses that range from 224.0.0.0 to 239.255.255.255. In this section, Force filtering can determined whether the switch flooding unknown multicast or not. Following commands are included in this group:

4.6.1 IGMP Snooping

4.6.2 IGMP Query

4.6.1 IGMP Snooping

This page is to enable IGMP Snooping feature, assign IGMP Snooping for specific VLAN, and view IGMP Snooping table from dynamic learnt or static manual key-in.

IGMP Snooping

Enable IGMP Snooping

VLAN Overview

Vlan ID	IGMP Snooping	Select
1	Disabled	<input type="checkbox"/>

Select All

IGMP Snooping Table

IP Address	VID	1	2	3	4

Enable IGMP Snooping: You can click the checkbox and Apply to Enable the IGMP Snooping here.

VLAN Overview: You can assign IGMP Snooping to for specific VLAN. You can enable IGMP Snooping for some VLANs so that some of the VLANs will support IGMP Snooping and others won't.

IGMP Snooping Table: The table shows the multicast group IP Address, VID and member ports of the current working multicast stream in this device.

4.6.2 IGMP Query

IGMP Query

IGMP Query on Management VLAN

Version :	Version 2 ▼
Query Interval(s):	125
Query Maximum Response Time(s):	10

This page allows users to configure IGMP Query feature. Since the Switch can only be configured by

member ports of the management VLAN, IGMP Query can only be enabled on the management VLAN. If you want to run IGMP Snooping feature in several VLANs, you should notice that whether each VLAN has its own IGMP Querier first. The IGMP querier periodically sends query packets to all end-stations on the LANs or VLANs that are connected to it. For networks with more than one IGMP querier, a switch with the lowest IP address becomes the IGMP querier.

IGMP Query Version: In IGMP Query version selection, you can select V1, V2 or Disable. V1 means IGMP V1 General Query and V2 means IGMP V2 General Query. The query will be forwarded to all multicast groups in the VLAN. Disable allows you to disable IGMP Query.

Query Interval(s): The period of query sent by querier.

Query Maximum Response Time: The span querier detect to confirm there are no more directly connected group members on a LAN. Once you finish configuring the settings, click on Apply to apply your configuration.

4.7 Network Redundancy

It is critical for industrial applications that network remains non-stop. JetWave2714GF-LTE-E supports STP, RSTP and Redundant Ring technology.

- 4.7.1 STP configuration
- 4.7.2 STP Port configuration
- 4.7.3 STP information
- 4.7.4 Redundant Ring Configuration
- 4.7.5 Redundant Ring Information
- 4.7.6 Redundant GW
- 4.7.7 VRRP

4.7.1 STP Configuration

This page allows user to select the STP mode and configure the global STP/RSTP Bridge Configuration. The STP mode includes the STP, RSTP and Disable. Please select the STP mode for your system first. The default mode is RSTP enabled.

STP Configuration

STP Mode

Bridge Configuration

Bridge Address	0003.7f48.83e9
Bridge Priority	32768 ▼
Max Age	20 ▼
Hello Time	2 ▼
Forward Delay	15 ▼

Bridge Configuration

Bridge Address: This shows the switch's MAC address.

Bridge Priority (0-61440): RSTP uses bridge ID to determine the root bridge, the bridge with the highest bridge ID becomes the root bridge. The bridge ID is composed of bridge priority and bridge MAC address. So that the bridge with the highest priority becomes the highest bridge ID. If all the bridge ID has the same priority, the bridge with the lowest MAC address will then become the root bridge.

Note: The bridge priority value must be in multiples of 4096. A device with a lower number has a higher bridge priority. Ex: 4096 is higher than 32768.

Note: The Web GUI allows user select the priority number directly. This is the convenient of the GUI design. When you configure the value through the CLI or SNMP, you may need to type the value directly.

Please follow the $n \times 4096$ rules for the Bridge Priority.

Max Age (6-40): Enter a value from 6 to 40 seconds here. This value represents the time that a bridge will wait without receiving Spanning Tree Protocol configuration messages before attempting to reconfigure.

If the device is not the root bridge, and if it has not received a hello message from the root bridge in an amount of time equal to Max Age, then device will reconfigure itself as a root bridge. Once two or more devices on the network are recognized as a root bridge, the devices will renegotiate to set up a new spanning tree topology.

Hello Time (1-10): Enter a value from 1 to 10 seconds here. This is a periodic timer that drives the switch to send out BPDU (Bridge Protocol Data Unit) packet to check current STP status.

The root bridge of the spanning tree topology periodically sends out a "hello" message to other devices

on the network to check if the topology is “healthy”. The “hello time” is the amount of time the root has waited during sending hello messages.

Forward Delay Time (4-30): Enter a value between 4 and 30 seconds. This value is the time that a port waits before changing from Spanning Tree Protocol learning and listening states to forwarding state.

This is the amount of time the device will wait before checking to see if it should be changed to a different state.

Once you have completed your configuration, click on Apply to apply your settings.

Note: You must observe the following rule to configure Hello Time, Forwarding Delay, and Max Age parameters.

$$2 \times (\text{Forward Delay Time} - 1 \text{ sec}) \geq \text{Max Age Time} \geq 2 \times (\text{Hello Time value} + 1 \text{ sec})$$

4.7.2 STP Port Configuration

This page allows you to configure the port parameter after enabled STP or RSTP.

Port Configuration

Select the port you want to configure and you will be able to view current setting and status of the port.

STP Port Configuration

Port	STP State	Path Cost	Port Priority
1	Enable ▼	2000	128 ▼
2	Enable ▼	2000	128 ▼
3	Enable ▼	2000	128 ▼
4	Enable ▼	2000	128 ▼

Apply Cancel

STP State: Enable or Disable the STP/RSTP of the port. Default is Enable.

Path Cost: Enter a number between 1 and 200,000,000. This value represents the “cost” of the path to the other bridge from the transmitting bridge at the specified port.

Priority: Enter a value between 0 and 240, using multiples of 16. This is the value that decides which port should be blocked by priority in a LAN.

4.7.3 STP Information

This page allows you to see the information of the root switch and port status.

STP Information

Root Information

Root Address	0003.7f48.83e9
Root Priority	32768
Root Port	N/A
Root Path Cost	0
Max Age	20 second(s)
Hello Time	2 second(s)
Forward Delay	15 second(s)

Port Information

Port	Role	Port State	Path Cost	Port Priority
1	Designated	Forwarding	20000	128
2	Designated	Forwarding	20000	128
3	Disabled	Blocking	20000	128
4	Disabled	Blocking	20000	128

Refresh

Root Information: You can see Root Bridge Address, Root Priority, Root Port, Root Path Cost and the Max Age, Hello Time and Forward Delay of BPDU sent from the root switch.

Port Information: You can see Port Role, Port State, Path Cost and Port Priority of the STP ports.

4.7.4 Redundant Ring Configuration

This page allow user to create new Ring and edit Ring configuration.

Add New Ring

Ring ID	Name	Priority	Ring Port 1	Path Cost	Ring Port 2	Path Cost	Status
<input type="text"/>	<input type="text"/>	<input type="text" value="128"/>	GT1 <input type="button" value="v"/>	<input type="text" value="128"/>	GT2 <input type="button" value="v"/>	<input type="text" value="128"/>	Disable <input type="button" value="v"/>

Ring Configuration

ID	Name	Priority	Ring Port 1	Path Cost	Ring Port 2	Path Cost	Status	Select	Edit
1	Ring1	128	GF1	128	GF2	128	Disable	<input type="checkbox"/>	<input type="button" value="Edit"/>

Add New Ring:

Ring ID: Once a Ring is created. This appears and can NOT be changed.

Name: Type the name of the Ring. If it is not filled in when creating, it will be automatically named by

the rule “Ring ID”.

Priority: The switch with highest priority (highest value) will be automatically selected as Ring Master. If all of the switches have the same priority, the switch with the biggest MAC address will be selected as Ring Master.

Ring Port 1/ Ring Port 2: In a Ring, 2 ports should be selected to be Ring Ports. For Ring Master, one of the ring ports will become the forwarding port and the other one will become the blocking port.

Path Cost: Change the Path Cost of Ring Port. If this switch is the Ring Master of a Ring, then it determines the blocking port. The Port with higher Path Cost in the two ring ports will become the blocking port, If the Path Cost is the same, the port with larger port number will become the blocking port.

Status: To enable/disable the Ring. Please remember to enable the ring after you add it.

Press “**Apply**” to activate settings after Ring created.

Ring Configuration: Click on “Edit” to modify Ring configuration.

Select: Check “Select” with “**Delete Selected**” to delete the selected entry.

Edit: Edit entries of a Ring.

Delete all: Delete the all Route entries.

Refresh: Reload to refresh the counts.

4.7.5 Redundant Ring Information

The table shows the Multiple Super Ring information.

ID	Role	Status	RM MAC	Blocking Port	Role Transition count	Ring State Transition count
1	RM	Normal	0012.7700.1123	---	2	2

Refresh

ID: Ring ID.

Role: This Switch is RM or nonRM.

Status: If this field is Normal which means the redundancy is approved. If any one of the link in this Ring is broken, then the status will be Abnormal.

RM MAC: The MAC address of Ring Master of this Ring. It helps to find the redundant path.

Blocking Port: This field shows which is blocked port of RM.

Role Transition count: This means how many times this switch has changed its Role from nonRM to RM or from RM to nonRM.

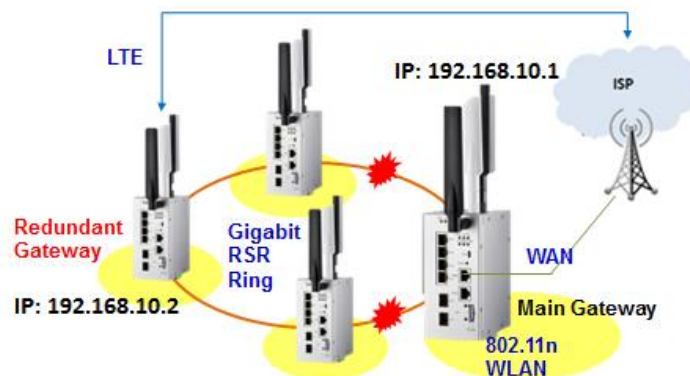
Ring State Transition count: This number means how many times the Ring status has been transformed between Normal and Abnormal state.

Press “**Refresh**” to reload MSR information.

4.7.6 Redundant GW

Redundant Gateway is a Ring redundancy feature when two links failure in a Ring.

Simple instance as below:



In the Rapid Super Ring, IP:192.168.10.1 device is the main gateway, other devices in the same Ring though its WAN port or Cellular interface for external Network transmission. Once there are two links failure or link down issue, other devices can not transmit datas to external Network and would keep the Gateway settings unless user change the settings on each device manually. To solve the problem, we implemented “Redundant Gateway”. When two links failure, Redundant Gateway device will create an internal virtual gateway (The same as original main gateway) so for other devices, the main gateway still existing and these devices can transmit datas to external Network via WAN/ Cellular interface of the Redundant Gateway device.

Redundant Gateway

These settings are only for redundant gateway setting.

Status:	Backup	
Redundant gateway:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
Gateway Address:	<input type="text" value="192.168.10.2"/>	
Ring ID :	<input type="text" value="1"/>	(1-31)
ARP Miss Count (Default:5):	<input type="text" value="5"/>	(0-65535)

Status: **Backup** or **Master**. Backup mode means the Ring status is normal. When two links failure, Redundant Gateway function will be trigger out and change to “Master” mode.

Redundant gateway: **Enable** or **disable** the function.

Gateway Address: Type the main gateway of the Redundant Ring.

Ring ID: The Ring number.

ARP Miss Count(Default:5): Type the ARP miss count. When Ring status is abnormal, system will transmit ARP packets in the Ring to check whether the main gateway still alive or not. If the ARP miss count is higher than the value that you set, the Redundant Gateway status will change to “Master” and replace the original gateway.

4.7.7 VRRP

The VRRP is short of Virtual Router Redundant Protocol. To further ensure the high reliability of an environment, the device also supports the VRRP protocol allowing the hosts to continuously direct traffic to the default gateway without change the default gateway configuration. In VRRP domain, the VRRP device should have the same Virtual Router ID, Virtual IP and Advertisement Interval time and choose one of the VRRP devices as the VRRP Master. The other becomes VRRP Backup to take over the VRRP Master immediately once the VRRP Master is done.

VRRP

The Virtual Router Redundancy Protocol (VRRP) eliminates the single point of failure inherent in the static default routed environment.

Enable VRRP

Virtual Router ID:	100
Virtual IP:	192.168.10.1
Priority:	255
Adv. Interval:	1
Preempt Mode:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

Apply Cancel

Virtual Router Interface Status

Select	Virtual ID	Virtual IP	Priority	Adv. Interval	Preempt	VRRP Status	VRRP Mac	Edit
<input type="checkbox"/>	100	192.168.10.1	255	1	Enable	Disable	00:00:5E:00:01:64	Edit

Delete Selected Delete All Refresh

Virtual Router ID: This is a virtual ID range from 1~255. The device within the same VRRP domain should have the same Virtual Router ID.

Virtual IP: This is the virtual IP of the VRRP domain. This is the Gateway IP of the clients.

Priority: VRRP priority is in the range of 0 to 255. The greater the number, the higher the priority. In VRRP domain, the VRRP device should have the same Virtual Router ID and Virtual IP and choose who should be the VRRP Master. The device equips with the highest priority will be selected as the VRRP Master. The priority setting can be manually changed, 1 to 254 are configurable. Priority 0 is reserved for special uses and priority 255 for the Virtual owner.

Adv. Interval: This field indicates how often the VRRP devices exchange the VRRP setting. The time unit is second, the default setting is 1 sec. In VRRP domain, the VRRP devices should have the same Adv. Interval as well.

Preempt Mode: While the VRRP Master link is failure, the VRRP Backup will take over its job immediately. However, while the VRRP master link is recovered, who should be the Master? The preempt decide whether the VRRP master should be recovered or not.

While the Preempt is **Enabled** and the interface is VRRP Master, the interface will be recovered.

While the Preempt is **Disabled** and the interface is VRRP Master, there is no change while the link is recovered. The VRRP Backup acts as the Master before restart the device.

4.8 Cellular

The “Cellular” feature set pages allow users to see the 3G/LTE Status, configure the Basic Setting, SIM Security, Connection Watchdog, Debug Mode and Mobile Manager Server Settings.

4.8.1 Basic Settings

The system supports Dual SIM socket, you can select SIM 1 or SIM 2 as the startup SIM socket, and configure whether the 2 SIM socket will Redundant with each other or not.

For cellular SIM settings, normally, you can connect the cellular Gateway to the ISP cellular network without configuring cellular setting. However, in some countries, before the cellular gateway can access the ISP’s cellular data network, you may need to enter the APN settings, User Name, Password, Authentication type... on the device. You can use this page to configure the parameters.

Basic Settings

Use this page to configure the parameters for Cellular.

Disable Cellular Interface

SIM Selection:	<input checked="" type="radio"/> SIM1 <input type="radio"/> SIM2
Cellular Redundant:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
SIM1 Settings	
APN:	<input type="text" value="internet"/>
User Name:	<input type="text"/>
Password:	<input type="text"/>
Authentication Type:	<input checked="" type="radio"/> CHAP <input type="radio"/> PAP
SIM2 Settings	
APN:	<input type="text" value="internet"/>
User Name:	<input type="text"/>
Password:	<input type="text"/>
Authentication Type:	<input checked="" type="radio"/> CHAP <input type="radio"/> PAP
Connection	
Connect:	<input type="button" value="Connect"/>
WAN Redundancy:	<input type="text" value="Fixed Cellular"/> ▼

Enable Auto IP Report

IP Report to URL:	<input type="text"/>
-------------------	----------------------

Disable Cellular Interface: You can disable the Cellular interface manually.

SIM Selection: SIM 1 means the SIM socket 1, you can see the ID in the front panel. SIM 2 means

the SIM socket 2. Select one of it as the startup SIM socket. SIM 1 is the default settings. Please insert the 3G SIM card to the SIM socket you select.

Cellular Redundant: While you enable Cellular Redundant, please insert the dual SIM cards into the two SIM socket before power on the system. Then the Dual SIM will be Redundant with each other while the primary Cellular connection is failed. The selected SIM number will be the primary SIM, the other one is backup SIM. The redundant timer is based on your settings of Reconnection Delay and Retries.

Note: The LTE module only can check the selected sim slot. Thus the unselected SIM2 slot shows inserted because the sim holder is inserted vice versa.

Note:

(1) The Cellular Redundant is only available while you insert two SIM cards into the socket. If you only insert one, the Cellular Redundant will not work.

(2) Please adjust the Reconnection Delay and Retires based on your application, if you requests shorter redundant time, you can modify the delay time or retires times.

SIM 1/ SIM 2 Settings:

Assign below setting for the specific SIM card.

SIM1 Settings	
APN:	internet
User Name:	
Password:	
Authentication Type:	<input checked="" type="radio"/> CHAP <input type="radio"/> PAP
SIM2 Settings	
APN:	internet
User Name:	
Password:	
Authentication Type:	<input checked="" type="radio"/> CHAP <input type="radio"/> PAP

APN: Every ISP has a specific APN (Access Point Name) assigned to its cellular network. The system can read this name from the SIM card. You can also find this setting by contacting your ISP to know this. Once you failed to connect your cellular network, this is the first way you can check. Please check with your ISP to know the APN and correctly input the setting through the page.

User Name: The user name for the Cellular connection. Normally, this is provided by your ISP.

Password: The password for the Cellular connection. Normally, this is provided by your ISP.

Authentication Type: You can select CHAP or PAP per your ISP request. Normally, this is provided by your ISP.

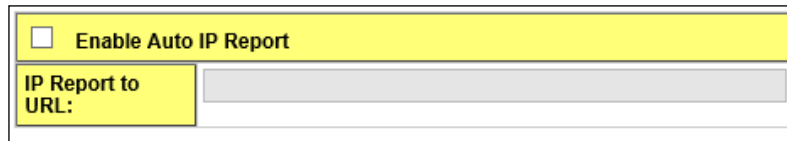
Connection	
Connect:	<input type="button" value="Connect"/>

Connect: You can press “Connect” to re-connect the Cellular connection of the selected SIM card. This progress may take 30 seconds. You will see below popup screen ask you wait 30 seconds.

Wait for Cellular connecting.
Please wait for 29 seconds before attempting to access the device again...

Note: You should not select the empty SIM and press “Connect” for the empty socket. This is error configuration.

Auto IP Report: Most of the ISP assigns the dynamic IP address to the Cellular clients and change the IP address every period of time. While you need to remotely control the gateway, you may need additional information generated from the remote Cellular client device. The Auto IP Report in JetWave2714GF-LTE-E can meet your need while you need to know the IP address from the product.



<input type="checkbox"/> Enable Auto IP Report	
IP Report to URL:	<input type="text"/>

Enable Auto IP Report: Press Enable Auto IP Report, the system will automatically update the system information to remote server/URL.

IP Report to URL: Type the correct URL here for your Gateway report to. You can build your own server, rent URL address from ISP or Google Cloud service also supports this functionality. Please check with your ISP or create through Google cloud.

Press “**Apply**” to activate the new setting.

4.8.2 SIM Security

This page allows you to assign the SIM security. If you (or ISP) already apply the PIN number to your SIM card, you need to configure the correct PIN number for your JetWave2714GF-LTE-E. After correctly enter the PIN number, you can start the Cellular connection or change the new PIN settings.

SIM Security Settings

SIM	1
SIM Status	SIM OK
Number of Retries Remaining:	3
SIM1 PIN:	<input type="text"/>
Confirm SIM1 PIN:	<input type="text"/>
Remember PIN:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
PIN Protection: Disable	Disable PIN ▼

4.8.3 Mobile Manager Setting

With Mobile Manager Utility can help you collect the IP Address after you installed the cellular devices in the remote field site. You can check the Mobile Manager Utility User Manual for detail operation and configuration. The device acts as the cellular router device, you can assign the target Server IP Address and specific port (TCP port), then the device will automatically update the current IP address and the new IP address once it is changed to the server.

Mobile Manager Settings

These settings are only for Mobile Manager remote management .

Server:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
Server Address:	<input type="text" value="60.251.55.126"/>	
Server Port:	<input type="text" value="2310"/>	(1-65535)
Control Port (Auto:0):	<input type="text" value="23001"/>	(0-65535)

Server: You can Enable or Disable the function. Default value is disabled.

Server Address: Type the Mobile Manager’s IP address in this field.

Server Port: The device will update info to server through this port. You can assign specific TCP port number.

Control Port: The Control Port (TCP port) allows you to connect to the device. You can assign specific TCP port number.

4.9 VPN

The “VPN” feature set pages allow users to configure the device as VPN client to connect to VPN server. It also allows users to configure 1-1 VPN Server service for one VPN client, with both the VPN server and client features can help you build one to one connection between two devices.

The current supported VPN type is OpenVPN. The OpenVPN is a full-featured SSL VPN which implements OSI layer 2 or 3 secure network extension using the industry standard SSL/TLS protocol, supports flexible client authentication methods based on certificates, smart cards, and/or username/password credentials, and allows user or group-specific access control policies using firewall rules applied to the VPN virtual interface.

The first step in building an OpenVPN 2.x configuration is to establish a PKI (public key infrastructure). PKI consists of a separate certificate (also known as a public key) and private key for the server and each client, and a master Certificate Authority (CA) certificate and key which are used to sign each of the server and client certificates.

In static encryption mode, each VPN client shares the same static key with OpenVPN server. In TLS encryption mode, each VPN client needs 3 keys, while VPN server needs 4 keys. The description of the 7 keys listed below.

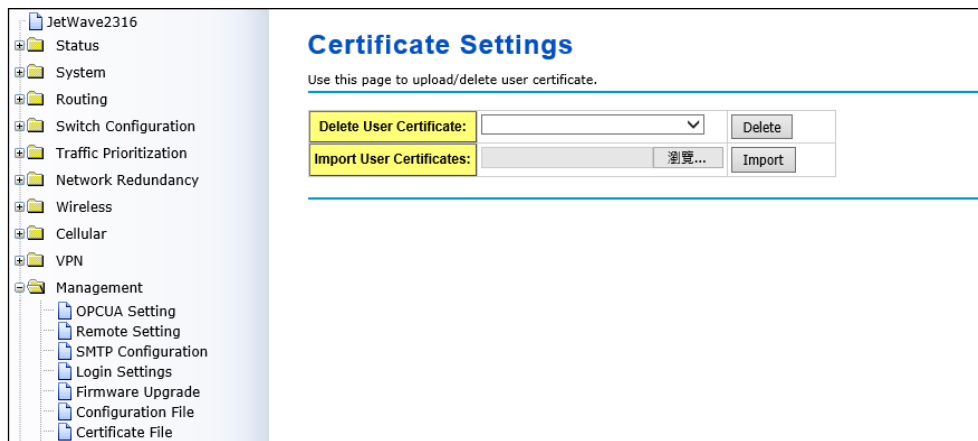
Filename	Needed By	Purpose	Secret
ca.crt	server + all clients	Root CA certificate	NO
ca.key	key signing machine only	Root CA key	YES
dh{n}.pem	server only	Diffie Hellman parameters	NO
server.crt	server only	Server Certificate	NO
server.key	server only	Server Key	YES

client.crt	client only	Client1 Certificate	NO
client.key	client only	Client key	YES

While the device acts as OpenVPN client. The ca.crt, client.crt and client.key are needed to establish OpenVPN tunnel as OpenVPN client.

Note: The file names of these keys are pre-defined and can't be changed.

Go to **VPN->VPN Certificate** Web configuration page to upload these keys. Import keys one by one in the page. Old certificate can also be deleted in the page.



The OpenVPN client configurations can be set in **VPN->OpenVPN client** web configuration page in below description.

Note: The settings should be consistent with OpenVPN server.

4.9.1 Status

This page shows VPN status. There are OpenVPN Client Information, OpenVPN Server Information and IPsec Information.

Information

This page shows the VPN status.

OpenVPN Client Information

Enabled	no
Connection Status	Disconnected

OpenVPN Server Information

Enabled	no
---------	----

IPsec Information

Enabled	no
Connection Status	Disconnected

Enabled:

yes: The VPN function already enabled.

no: The VPN function not enabled yet.

Connection Status:

Connected: The VPN connection is already built successfully.

Disconnected: The VPN not connect.

Tx / Rx Bytes:

You can see the transmission data volume in bytes after the VPN client is connected.

Press "**Refresh**" to reload VPN status.

4.9.2 OpenVPN Client

This page allows you to configure the OpenVPN settings. While the device acts as the VPN client, it must follow the VPN Server settings in most parameters. You need to check with the administrator of the VPN server first, then type the parameters to the below figure.

OpenVPN Client Settings

Use this page to configure the parameters for OpenVPN Client.

Enable OpenVPN Client Connection

Encryption Mode :	<input checked="" type="radio"/> Static <input type="radio"/> TLS	
Server Address (1) :	192.168.10.1	(IP or Domain Name)
Server Address (2) :	0.0.0.0	
Port :	1194	(1-65535)
Tunnel Protocol :	UDP	
Encryption Cipher :	Blowfish CBC	
Hash Algorithm :	SHA1	
ping-timer-rem :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
persist-tun :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
persist-key :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Use LZO Compression :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Keepalive :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Ping Interval :	10	(1-99999 seconds)
Retry Timeout :	60	(1-99999 seconds)
nobind :	<input checked="" type="checkbox"/>	
ifconfig :	Local : 10.8.0.2	Remote : 10.8.0.1
Route :	IP : 0.0.0.0	MASK : 0.0.0.0
Enable NAT :	<input type="checkbox"/>	
Save Log File :	Save...	

Encryption Mode: Select the encryption is Static or TLS.

Static Key: Use a pre-shared static key.

TLS: Use SSL/TLS + certificates for authentication and key exchange.

Remote Server IP (1): Input the IP address of VPN server.

Remote Server IP (2): Input the second IP address of VPN server if necessary.

Port: Input the port number that your VPN service used.

Note: you may need check your VPN server also has properly port setting.

Tunnel Protocol: You can choose use TCP or UDP to establish the VPN connection.

Encryption Cipher: Select the encryption cipher from Blowfish to AES in Pull-down menus.

Hash Algorithm: Select the hash algorithm.

Ping-timer-rem: Select enable or disable the ping-timer-rem, this function prevent unnecessary restart at server/client when network fail.

Persist-tun: Select enable or disable the persist-tun, enable this function will keep tun(layer 3)/tap(layer 2) device linkup after Keepalive timeout, default value is Enable.

Persist-key: Select enable or disable the persist-key, enable this function will keep the key

first use if VPN restart after Keepalive timeout, default value is Enable.

Use LZO Compression: Select use LZO Compression or not, this function compress data to decrease the traffic but also need more CPU effort, default value is Disable.

Keepalive: Select enable or disable keepalive function, this function is use to detect the status of connection, default value is Enable.

Ping Interval: Input the ping interval, the range can from 1~99999 seconds.

Retry Timeout: Input the retry timeout, the range can from 1~99999 seconds.

nobind: When click on nobind, VPN client don't need to bind to a specific local port number.

ifconfig: Input the tunnel IP address that VPN use.

Route: Input the route IP and MASK. This is the target IP domain you can access through the VPN tunnel.

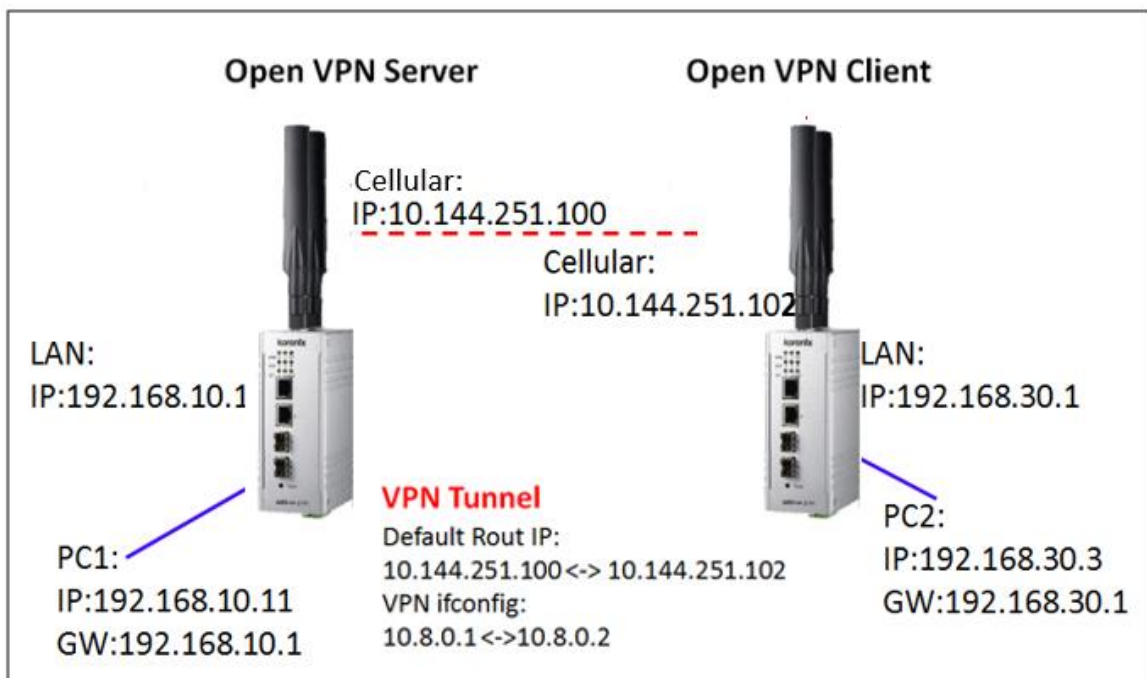
Enable NAT: Enable NAT(Network Address Translation).

Save Log File: Save OpenVPN Client log file.

4.9.3 OpenVPN Server

To help you easier create the One to One Secure M2M (machine to machine) connection for the remote devices. The device supports both OpenVPN Server and OpenVPN Client. This Server setting allows you to configure the Secure M2M connection for one remote Client.

Below is the simple test setup for your reference. The red color line becomes a VPN Tunnel and the transmission data are secured. To configure the settings, you need to have IP plan of the 2 sites and the routing/VPN path first. Configure the device as Router mode and give the Ethernet ports specific IP as the default gateway for the connected devices (ex: PCs). For VPN Tunnel, you can choose Cellular interface. Type the connected IP in VPN ifconfig and apply/save the settings.



Note: To create the 1-1 VPN Tunnel you can follow below steps:

1. Define the IP of both ends and secure tunnel.
2. Select the general VPN Settings:
 - (1) Encryption Mode, Port, Tunnel protocol (Must)
 - (2) Select the Encryption Cipher, Hash Algorithm (Must)
 - (3) Keepalive, Ping Interval, Retry Timeout (option)
3. Type the ifconfig / Route of the tunnel & both ends.
 - (1) Tunnel: ifconfig (VPN Tunnel)
 - (2)Route: Target Route behind the Client/Server
4. Generate a Key and Upload the Key (Management -> Certificate File) to the system
5. Enable VPN & Apply to activate

6. Check Status
7. Save Settings

Please generate the key by VPN Server or 3rd party Key generation tool.

Enable OpenVPN Server Connection

Encryption Mode :	<input checked="" type="radio"/> Static <input type="radio"/> TLS	
Port :	<input type="text" value="1194"/>	(1-65535)
Tunnel Protocol :	UDP ▾	
Encryption Cipher :	Blowfish CBC ▾	
Hash Algorithm :	SHA1 ▾	
ping-timer-rem :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
persist-tun :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
persist-key :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Use LZO Compression :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Keepalive :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Ping Interval :	<input type="text" value="10"/>	(1-99999 seconds)
Retry Timeout :	<input type="text" value="60"/>	(1-99999 seconds)
ifconfig :	Local : <input type="text" value="10.8.0.1"/>	Remote : <input type="text" value="10.8.0.2"/>
Route :	IP : <input type="text" value="0.0.0.0"/>	MASK : <input type="text" value="0.0.0.0"/>
Save Log File :	<input type="button" value="Save..."/>	

Encryption Mode: Select the encryption is Static or TLS.

Static Key: Use a pre-shared static key.

TLS: Use SSL/TLS + certificates for authentication and key exchange.

Port: Input the port number that your VPN service used.

Tunnel Protocol: You can choose use TCP or UDP to establish the VPN connection.

Encryption Cipher: Select the encryption cipher from Blowfish to AES in Pull-down menus.

Hash Algorithm: Select the hash algorithm.

Ping-timer-rem: Select enable or disable the ping-timer-rem, this function prevent unnecessary restart at server/client when network fail.

Persist-tun: Select enable or disable the persist-tun, enable this function will keep tun(layer 3)/tap(layer 2) device linkup after Keepalive timeout, default value is Enable.

Persist-key: Select enable or disable the persist-key, enable this function will keep the key first use if VPN restart after Keepalive timeout, default value is Enable.

Use LZO Compression: Select use LZO Compression or not, this function compress data to decrease the traffic but also need more CPU effort, default value is Disable.

Keepalive: Select enable or disable keepalive function, this function is use to detect the status of connection, default value is Enable.

Ping Interval: Input the ping interval, the range can from 1~99999 seconds.

Retry Timeout: Input the retry timeout, the range can from 1~99999 seconds.

Ifconfig: Input the tunnel IP address that VPN use.

Route: Input the route IP and MASK. This is the target IP domain you can access through the VPN tunnel.

Save Log File: Save OpenVPN Server log file.

Press “Apply” to activate settings.

4.9.4 Port Forwarding

This page allow user to configure Port Forwarding rules on the OpenVPN Client tunnel.

Select “**Enable VPN Port Forwarding**” and then type the parameters to create the port forwarding entries.

Protocol: Configure Both (TCP + UDP), TCP or UDP protocol type.

Source IP Address: Type specific source IP address.

Destination Port or Range: Configure the port range of destination.(Destination is JetWave2714GF-LTE-E that you use)

Forwarding IP Address: Type specific forwarding IP address.

Forwarding Port or Range: Configure the port or range for forwarding device.

Press “**Apply**” to activate settings.

After configured VPN Port Forwarding, you can see the entries you configure in below. You can press “**Edit**” to modify the setting, click on “**Select**” and press “**Delete Selected**” to delete selected entries. Or “**Delete All**” to delete all entries. Press “**Refresh**” to update the table.

4.9.5 VPN Certificate

This page allow user to manage the user certificate file.

VPN Certificate Management

Use this page to upload/delete vpn certificate. Please import the correct vpn certificate files.
OpenVPN Server TLS Mode : ca.crt, server.key, server.crt, dh1024.pem
OpenVPN Client TLS Mode : ca.crt, client.key, client.crt
Static Mode : static.key

Delete VPN Certificate:	<input type="text"/>	<input type="button" value="Delete"/>
Import VPN Certificates:	<input type="text"/> 瀏覽...	<input type="button" value="Import"/>

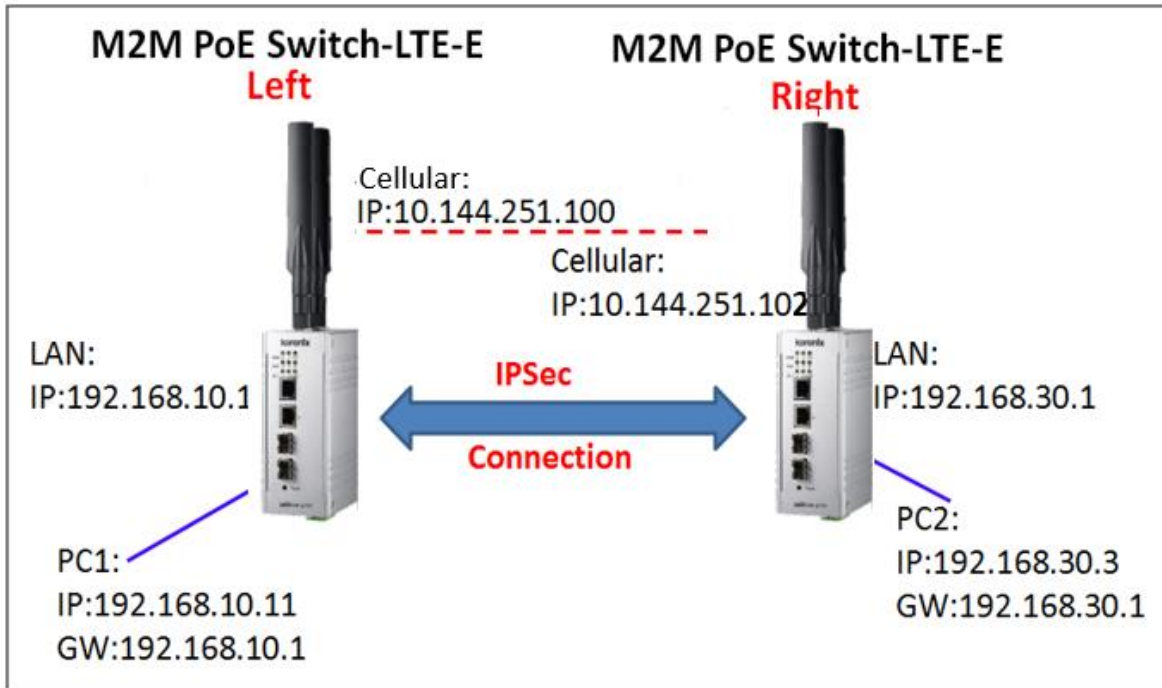
Import: Import the correct VPN Certificate.

Delete: Delete existing VPN Certificate.

4.9.6 IPsec

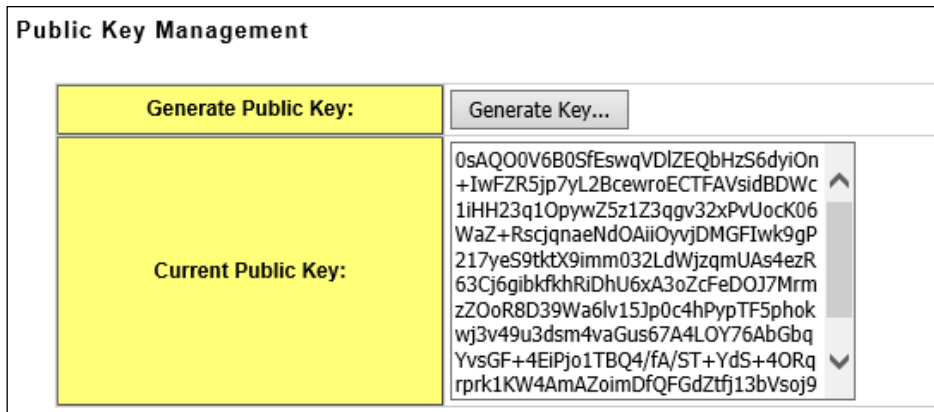
Use this page to configure the parameters for IPsec Connection. The VPN tunnel has two participants on its ends, called left and right, and which participant is considered left or right is arbitrary. You can configure various parameters for these two ends in this page.

Simple example about IPsec connection:



Public Key Management:

The content of current public key is displayed. New public key can be generated by pressing “**Generate key...**” button. An alert will be displayed to confirm the creation of new public key. Public key is used when the authentication method set to RSA key in the configuration of IPsec connection in bottom half of the page.



Click on “**IPsec Connection**” to enable IPsec function.

Enable IPsec Connection

Interfaces for IPsec to Use :	WAN
Authentication Method :	RSA Key
ESP Algorithm :	AES
Left - IP of network interface :	192.168.1.1
Left Source IP Address :	0.0.0.0
Left Subnet (network/netmask) :	(Ex : 192.168.10.0/24)
Left RSA Key :	
Right - IP of network interface :	192.168.1.2
Right Source IP Address :	0.0.0.0
Right Subnet (network/netmask) :	(Ex : 192.168.20.0/24)
Right RSA Key :	

Interfaces for IPsec to Use: Select the interface that can be interworking with VPN server, possible options are WAN/LAN/Cellular.

Authentication Method: Select authentication method, RSA key or .Shared secret.

Shared secret: Use a static shared secret key. Max. length is 25.

RSA key: use public/private key for encryption and decryption. Use public key generated in top-half page

ESP Algorithm: Select ESP (Encapsulating Security Payload) desired, AES/DES/3DES.

Left – IP of network interface: Left corresponds to right in IPsec point-to-point connection. The left and right IP settings should be the same in both IPsec endpoints. Enter interface IP address of left endpoint that can directly connected to right endpoint, for example, WAN port IP address or cellular IP address when using cellular network.

Left Source IP Address: As Left - IP of network interface, enter the LAN port interface IP address of left endpoint.

Left Subnet (network/netmask): Enter subnet mask of left endpoint in CIDR notation, for example, 192.168.10.0/24.

Left RSA Key: The attribute is only required when using RSA key authentication method. Using public key generated from top-half page.

Right- IP of network interface: Right corresponds to left in IPsec point-to-point connection. The left and right IP settings should be the same in both IPsec endpoints. Enter interface IP address of right

endpoint that can directly connected to left endpoint, for example, cellular IP address when using cellular network.

Right Source IP Address: As Right - IP of network interface, enter the LAN port interface IP address of right endpoint.

Right Subnet(network/netmask): Enter subnet mask of right endpoint in CIDR notation, for example, 192.168.20.0/24.

Right RSA Key: The attribute is only required when using RSA key authentication method. Using public key generated from top-half page.

Press “**Apply**” to activate settings.

4.10 Security

The JetWave2714GF-LTE-E provides Port Security for you to secure your connection.

4.10.1 Port Security

Port Security Port Security feature allows you to stop the MAC address learning for specific port. After stopping MAC learning, only the MAC address listed in Port Security List can access the switch and transmit/receive traffic. This is a simple way to secure your network environment and not to be accessed by hackers. This page allows you to enable Port Security and configure Port Security entry. Port Security State: Change Port Security State of the port to Enable first. Add Port Security Entry: Select the port, and type VID and MAC address. Format of the MAC address is xxxx.xxxx.xxxx. Ex: 0012.7701.0101. Max volume of one port is 10. So the system can accept 100 Port Security MAC addresses in total. Port Security List: This table shows you those enabled port security entries. You can click on Remove to delete the entry. Once you finish configuring the settings, click on Apply / Add to apply your configuration.

Port Security

Port Security State

Port	GT1	GT2	GF1	GF2
State	Disable ▾	Disable ▾	Disable ▾	Disable ▾

Apply

Add Port Security Entry

Port	VID	MAC Address
GT1 ▾	<input type="text"/>	<input type="text"/>

Add

Port Security Entry List All ▾

Port	VID	MAC Address	Select
Delete Selected			
Delete All			
Refresh			

4.11 Management

The “Management” feature set pages allow users to configure the Remote Setting, Password Setting, Firmware Upgrade, Configuration File Backup/Restore and Certificate File import.

4.11.1 OPCUA Setting

OPCUA is the abbreviation of OPC Unified Architecture. It is an industrial M2M communication protocol for interoperability developed. This page allow user to configure the parameters for OPCUA Server.

OPCUA Server Settings

Use this page to configure the parameters for OPCUA Server.

Enable OPCUA Server

Clear Certificate Key :	<input type="checkbox"/>
Port :	<input type="text" value="48020"/> (1-65535)
Change Password :	<input type="checkbox"/>
New Password:	<input type="password"/>
Confirm Password:	<input type="password"/>

Apply Cancel

Click on “**Enable OPCUA Server**” to enable the function.

Clear Certificate Key: Click to clear certificate key.

Port: Specifies the port number, range from 1 to 65535. Default value is 48020.

Click on “**Change Password**” to change the password, and then type new password at “**New Password**” and “**Confirm Password**” field.

Press “Apply” to activate setting.

4.11.2 Remote Settings

Use this page to set the Remote Management Privacy with selected Event Warning Type.

And this page also includes the configuration of SNMP settings V2c and V3.

Please make sure the configuration of SNMP should match between the device and SNMP server.

Remote Settings

Use this page to switch services of remote console.

Remote Management Privacy

Telnet SNMP SNMP Trap
 SSH Force HTTPS Email Alert

Event Warning Type

Authentication Fail Config Changed

Remote Management Privacy: You can select which kinds of remote service should be opened in your environment. The services include **Telnet**, **SNMP**, **SNMP Trap**, **SSH**, **Force HTTPS** and **E-mail Alert**. Select the service and press “**Apply**” to activate the settings.

Event Warning Type: The event warning type selection.

Authentication Fail: The client failure of authentication event.

Config Changed: The configuration of the AP/Gateway is changed event.

SNMP Settings:

SNMP Settings	
Protocol Version:	V2c ▾
Server Port:	161
Get Community:	public
Set Community:	private
Trap Destination:	0.0.0.0
Trap Community:	public

Protocol Version: Select the SNMP version, and keep it identical on the device and the SNMP manager. While you chose SNMPv3 and applied, you must configure the SNMPv3 User Name, Password and their Access type, Authentication and Privacy Protocol in below SNMPv3 User Profile.

Server Port: Change the server port for a service if needed; however you have to use the same port to use that service for remote management.

Get Community: Specify the password for the incoming Get and GetNext requests from the management station. By default, it is set to public and allows all requests.

Set Community: Specify the password for the incoming Set requests from the management station. By default, it is set to private.

Trap Destination: Specify the IP address of the station to send the SNMP traps to.

Trap Community: Specify the password sent with each trap to the manager. By default, it is set to public and allows all requests.

Configure SNMPv3 User Profile: For SNMP protocol version 3, you can click “**Configure SNMPv3 User Profile**” in blue to set the details of SNMPv3 user. Check “**Enable SNMPv3 Admin/User**” in advance and make further configuration.

Configure SNMPv3 User Profile

<input checked="" type="checkbox"/> Enable SNMPv3Admin	
User Name:	SNMPv3Admin
Password:	••••••••
Confirm Password:	••••••••
Access Type:	Read/Write ▾
Authentication Protocol:	MD5 ▾
Privacy Protocol:	None ▾
<input checked="" type="checkbox"/> Enable SNMPv3User	
User Name:	SNMPv3User
Password:	••••••••
Confirm Password:	••••~•••
Access Type:	Read Only ▾
Authentication Protocol:	MD5 ▾
Privacy Protocol :	None ▾

User Name

Specify a user name for the SNMPv3 administrator or user. Only the SNMP commands carrying this user name are allowed to access the device.

Password

Specify a password for the SNMPv3 administrator or user. Only the SNMP commands carrying this password are allowed to access the device.

Confirm Password

Input that password again to make sure it is your desired one.

Access Type

Select "Read Only" or "Read and Write" accordingly.

Authentication Protocol

Select an authentication algorithm. SHA authentication is stronger than MD5 but is slower.

Privacy Protocol

Specify the encryption method for SNMP communication. None, DES and None are available.

None: No encryption is applied.

DES: Data Encryption Standard, it applies a 58-bit key to each 64-bit block of data.

Note: [For security concern, it is recommended change the Community Name before you connect the AP to the network.](#) The experience engineer who familiar with SNMP protocol can easily discovery and change the configuration of the AP/Gateway through SNMP once you use the default communication name.

4.11.3 SMTP Configuration

JetWave2714GF-LTE-E supports E-mail Warning feature. The AP will send the occurred events to remote E-mail server. The receiver can then receive notification by E-mail. The E-mail warning is conformed to SMTP standard. This page allows you to enable E-mail Alert, assign the SMTP Server IP, Sender E-mail, and Receiver E-mail. If SMTP server requests you to authorize firstly, you can also set up the username and password in this page.

SMTP Settings

Use this page to setup Email Alert of remote console.

Configure SMTP Setting

SMTP Server IP:	<input style="width: 90%;" type="text"/>
Email Account:	<input style="width: 90%;" type="text"/>
Authentication Protocol:	None ▾
User Name:	<input style="width: 80%;" type="text"/>
Password:	<input style="width: 90%;" type="password"/>
Confirm Password:	<input style="width: 90%;" type="password"/>
Rcpt Email Address 1:	<input style="width: 90%;" type="text"/>
Rcpt Email Address 2:	<input style="width: 90%;" type="text"/>

SMTP Server IP: The IP address of the SMTP Server.

Email Account: The sender's Email Account.

Authentication Protocol: If SMTP server requests you to authorize first, select the Authentication Protocol and following User Name and Password.

User Name: The User Name of the Sender Email account.

Password: The Password of the Sender Email account.

Confirm Password: Confirm the Password of the Sender Email account.

Rcpt Email Address 1: The first Receiver's email address.

Rcpt Email Address 2: The second Receiver's email address.

Press “**Apply**” to activate the setting.

4.11.4 Login Settings

Use this page to set the user name and password of the AP. Type the **User Name**, **New Password** and **Confirm Password** again. Press “**Apply**” to activate the new password.

Login Settings

Use this page to set the user name and password of this Access Point.

User Name:	admin
New Password:	••••
Confirm Password:	••••

Apply Cancel

4.11.5 Firmware Upgrade

In this section, you can update the latest firmware for your device. We provides the latest firmware in our Web site. The new firmware may include new features, bug fixes or other software changes. We’ll also provide the release notes for the update as well.

From technical viewpoint, we suggest you use the latest firmware before installing the AP to the customer site.

Note: The system will be automatically rebooted after you finished upgrading new firmware. Please remind the attached users before you do this.

Firmware Upgrade

This page allows you upgrade the device firmware to a new version. Please do not power off the device during the upload because it may crash the system.

Select File: 浏览...

Upgrade Cancel

Firmware Upgrade:

Type the path of the firmware in **Select File** field, or click “**Browse...**” to browse the firmware file. Press “**Upgrade**” to upload the firmware file to the AP. After finishing transmitting the firmware, the system will copy the firmware file and replace the firmware in the flash.

Note: During the progress, please **DO NOT** power off your system.

4.11.6 Configuration File

JetWave2714GF-LTE-E provides Configuration File **Backup (Save Setting to File)**, **Restore (Load Setting from File)** and **Reset Setting to Default** features.

With Backup command, you can save current configuration file saved in the AP/Gateway's flash to admin PC. This will allow you to go to Restore command later to restore the configuration file back to the AP/Gateway. Before you restore the configuration file, you must place the backup configuration file to specific folder in the PC. Users can also browse the target folder and select existed configuration file. The AP/Gateway can then download this file back to the flash.

This "**Browse...**" mode is only provided by Web UI. For CLI, please type specific path of the configuration file.

Configuration File:

Configuration File

This page allows you to save current settings to a file or load the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default or reboot the device.

Load Settings from File:	<input style="width: 100%;" type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Upload"/>
Save Settings to File:	<input type="button" value="Save..."/>
Reset Settings to Default:	<input type="button" value="Reset"/> <input type="checkbox"/> Include IP Settings

Restore (Load Setting from File): Type the path of the configuration file or click "**Browse...**" to browse the firmware file. The Browse feature is only supported in Web GUI. Press "**Upload**" after the file is selected.

Backup (Save Setting to File): Press "**Save...**" to backup the configuration file to specific path/folder in your computer.

Reset Settings to Default: Press "**Reset**" can reset all the configurations, but not included default IP address to default settings. If you want to reset the IP address to default value, select "Include IP Settings".

4.11.7 Remote IP Scan

The page allow user to set remote IP Scan, it include **Cluster Name** and **IP Scan Password**.

With **Remote IP Scan**, it provides higher wireless security when use i-View management tool.

IP Scan

Use this page to set the remote ip scan of this Access Point.

Cluster Name:

Apply Cancel

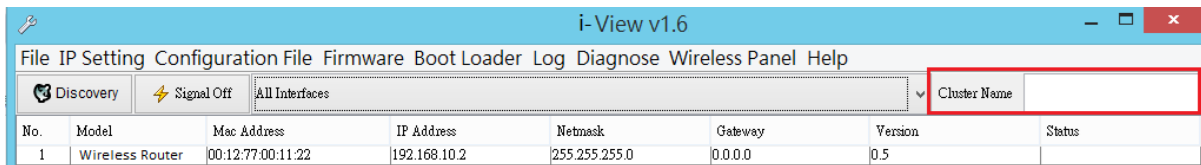
IP Scan Password:

Confirm Password:

Apply Cancel

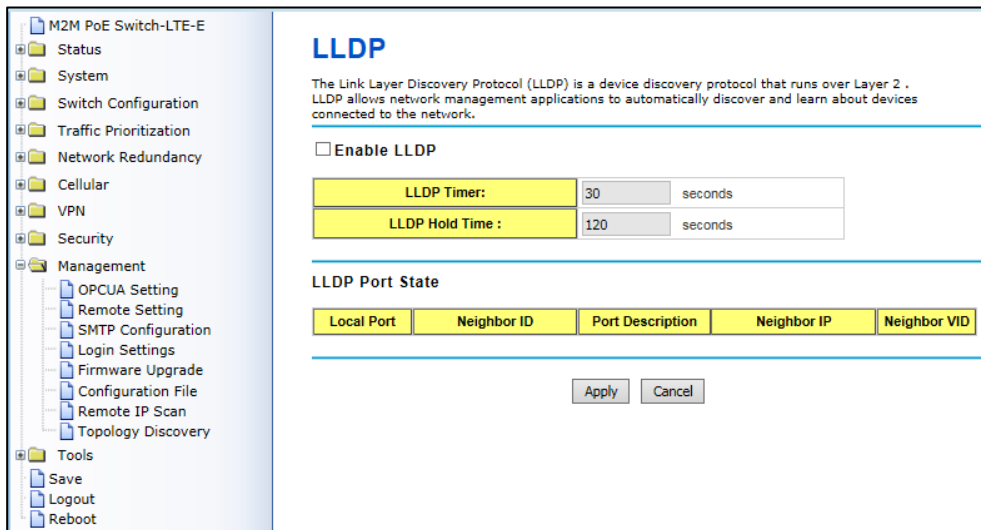
After set **Cluster Name**, i-View will not list device in Model filed unless user type the same Cluster name at i-View interface.

If set **Cluster Name** with **Password**, i-View will not list the device in Model filed unless user type the same Cluster name at i-View interface, if user already type the same Cluster Name at i-View tool interface, it will list devices but need to key in password if user want to modify configuration, such as Reboot, Load factory default, Change Cluster Name and Wireless panel settings.



4.11.8 Topology Discovery

JetWave2714GF-LTE-E supports topology discovery or LLDP (IEEE 802.1AB Link Layer Discovery Protocol) function that can help user to discovery multi-vendor's network device on same segment by NMS system which supports LLDP function; With LLDP function, NMS can easier maintain the topology map, display port ID, port description, system description, VLAN ID... Once the link failure, the topology change events can be updated to the NMS as well. The LLDP Port State can display the neighbor ID and IP learnt from the connected devices.



LLDP: Select Enable/Disable to enable/disable LLDP function.

LLDP Timer: the interval time of each LLDP and counts in second; the valid number is from 5 to 254, default is 30 seconds.

LLDP Hold time: The TTL (Time To Live) timer. The LLDP state will be expired once the LLDP is not received by the hold time. The default is 120 seconds.

Local port: the current port number that linked with neighbor network device.

Neighbor ID: the MAC address of neighbor device on the same network segment.

Neighbor IP: the IP address of neighbor device on the same network segment.

Neighbor VID: the VLAN ID of neighbor device on the same network segment.

4.12 Tools

The “Tools” feature set pages provides the additional useful tools.

4.12.1 System Log

System log is used for recording events occurred on the JetWave2714GF LTE-E, including station connection, disconnection, system reboot and etc.

System Log

Use this page to set remote log server and show the system log.

Enable Remote Syslog Server

IP Address:	0.0.0.0
Port:	514

#	Time	Source	Message
1	<14>2015- 1- 1 00:00:04	00:12:77:FF:00:07	WLAN[0] service started.
2	<14>2015- 1- 1 00:00:04	00:12:77:FF:00:07	WLAN[0] service stopped.
3	<14>2015- 1- 1 00:00:04	00:12:77:FF:00:07	WLAN[0] service started.

Enable Remote Syslog Server: Enable System log or not.

IP Address: Specify the IP address of the server.

Port: Specify the port number of the server.

Press “**Apply**” to activate settings.

It shows system log information in the bottom half of the page. Press “**Refresh**” to reload the log table or press “**Clear**” to delete log information.

4.12.2 Ping Watchdog

This is a simple tool great to reduce maintain cost for JetWave2714GF-LTE-E.

It will auto reboot itself when cannot ping the specific IP address.

Ping Watchdog

This page provides a tool to configure the Ping Watchdog. If the failcount of the Ping reaches to a specified value, the watchdog will reboot the device.

Enable Ping Watchdog

IP Address to Ping:	0.0.0.0
Ping Interval:	300 seconds
Startup Delay:	120 seconds(>120)
Failure Count To Reboot:	300

Enable Ping Watchdog: Check means enable ping watchdog function.

IP Address to Ping: input the IP address, it will ping this IP.

Ping Interval: Ping this IP every ping interval.

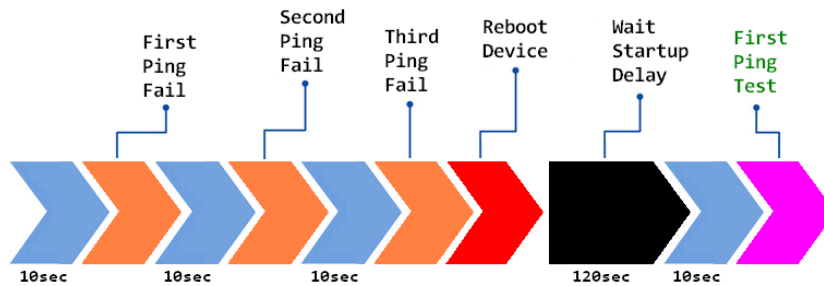
Startup Delay: It need time to boot, the startup delay use to buffer to prevent it continue to reboot itself.

Failure Count To Reboot: When ping fail reach the failure count that you input, it will reboot.

Press “Apply” to activate settings.

Below is the ping watchdog example:

<input checked="" type="checkbox"/> Enable Ping Watchdog	
IP Address to Ping:	192.168.1.10
Ping Interval:	10 seconds
Startup Delay:	120 seconds(>=120)
Failure Count To Reboot:	3



4.12.3 Ping

This is a simple Ping tool for you to check the status of remote station.

Type the target IP address in the “Destination: _____” field then press “Ping”.

The system will ping the remote station 4 times and list the ping result in the web GUI.

Ping

This page provides a tool to Ping IP address.

Destination:

```

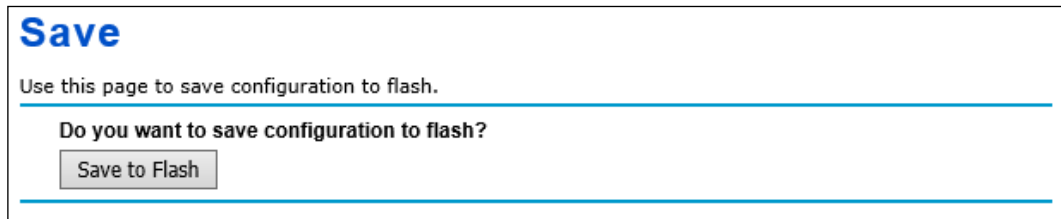
PING 192.168.10.95 (192.168.10.95): 56 data bytes
64 bytes from 192.168.10.95: icmp_seq=0 ttl=128 time=0.5 ms
64 bytes from 192.168.10.95: icmp_seq=1 ttl=128 time=0.6 ms
64 bytes from 192.168.10.95: icmp_seq=2 ttl=128 time=0.7 ms
64 bytes from 192.168.10.95: icmp_seq=3 ttl=128 time=0.5 ms

--- 192.168.10.95 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.5/0.5/0.7 ms
                    
```

The main entry provides the system tools, for example the Save the configuration, Logout and Reboot the system.

4.13.1 Save

Use this page to save configuration to flash. Every time while you finished the configuring the device, please remember to save the configuration to flash. Otherwise, the configuration will lost after reboot the system.



Save

Use this page to save configuration to flash.

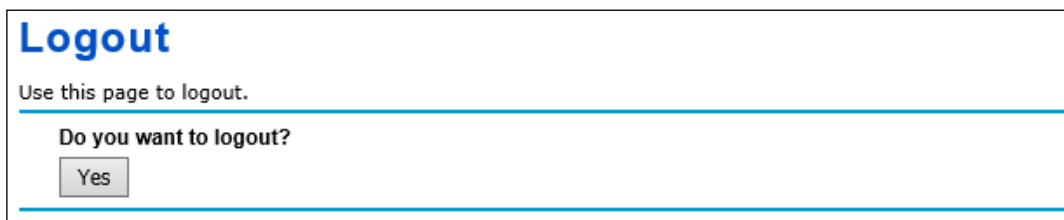
Do you want to save configuration to flash?

Press **“Save to Flash”** to save the configuration to flash.

4.13.2 Logout

After finished configuring and leave, please remember to Logout the system. Without Logout the system, the login session will not timeout for couple minutes, it is a risk that other user may login your system without password checking before timeout. Another affect is that the user can NOT access at the same time if someone already login the system.

Use this page to logout. Press **“Yes”** to logout.



Logout

Use this page to logout.

Do you want to logout?

4.13.3 Reboot

Use this page to reboot the system. Press “**Yes**” to reboot system.

Reboot

Use this page to Reboot.

Do you want to reboot?

The below warning message will appear after you reboot the system.

This device has been reboot, you have to login again.
Please wait for 72 seconds before attempting to access the device again...



Chapter 5 Configuration

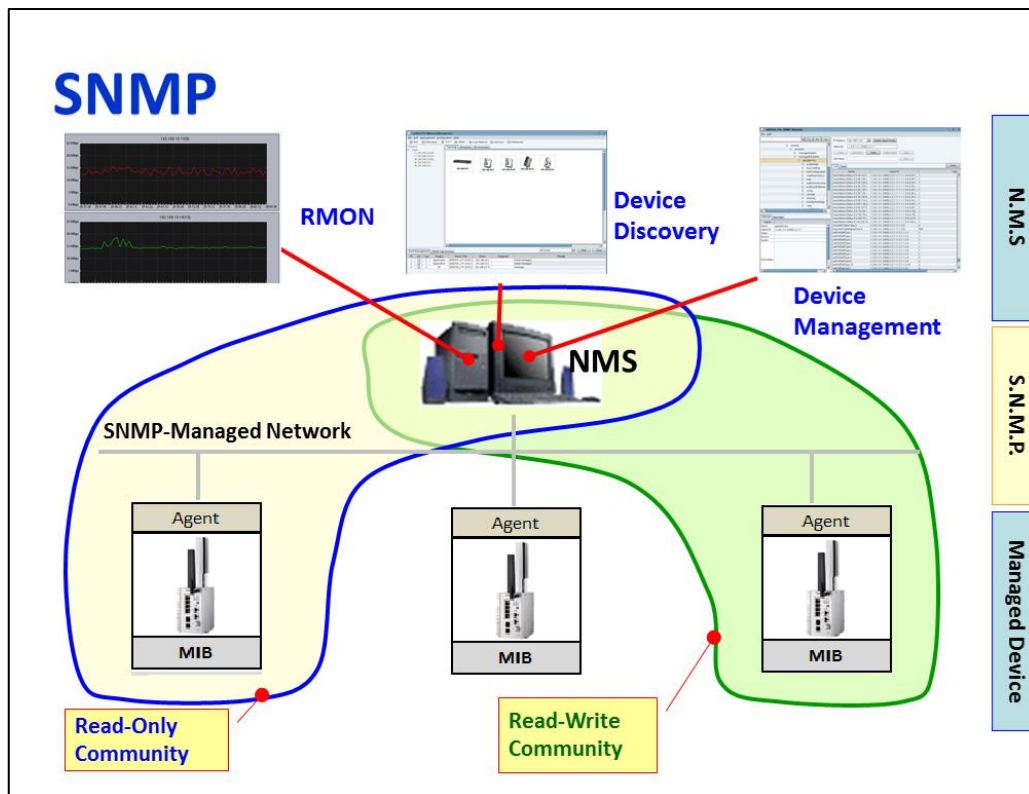
Chapter 5 Configuration – SNMP, View Utility

5.1 SNMP

5.1.1 What is SNMP?

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. This product series supports SNMP v1, v2c and V3.

Typical SNMP Architecture:



An SNMP managed network consists of two main components: Agent of the Managed Device and Manager (Network Management System, NMS).

Agent of the Managed Device: An agent is a management software module that resides in AP/Gateway. An agent translates the local management information (Management Information Base, MIB) from the managed device into a SNMP compatible format. In MIB, all the status and settings of the AP/Gateway has its own specific object ID (OID), the manager can read or write the value of the OID.

Manager (Network Management System, NMS): The manager is the console through the

network. Network Management System (NMS) is the typical management system to manage the SNMP compatible devices. It normally provides device discovery, management, remote monitoring on network (RMON), trap server...etc.

Community:

The community is similar to the password of SNMP, while the manager wants to manage the target device, they must have the same community name. The community includes 2 privileges, Read Only and Read and Write. With Read Only privilege, you only have the ability to read the values of MIB tables. Default community string is Public. With Read and Write privilege, you have the ability to read and set the values of MIB tables. Default community string is Private.

SNMP Setup:

Please refer to the **Remote Setting**.

5.1.2 Management Information Base (MIB):

Before you want to manage the JetWave2714GF-LTE-E through SNMP, please go to download the MIB files from our web site and compile all of them to the NMS. The AP/Gateway supports function based MIB, the same function/parameters in all the models have the same object ID (OID). The benefit is you just need to compile the MIB file one time even you purchase different models. While you purchase our new released models in the future, the MIB file can be applied as well. Once we provide new features for the MIB, you just need one time effort to update the MIB table for all the models.

There are some MIB files which are:

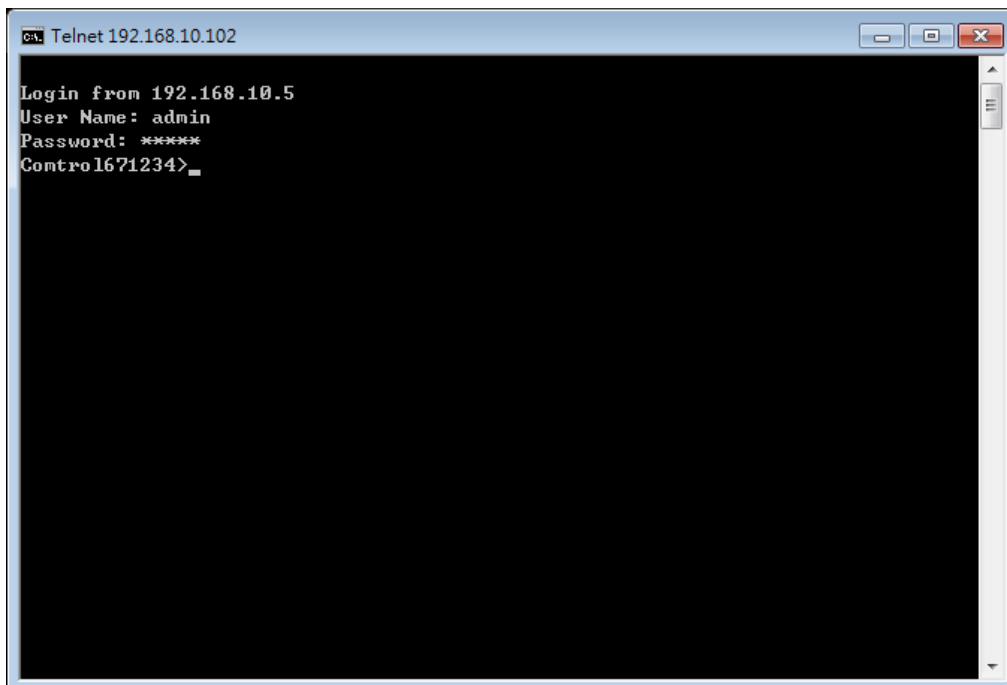
- a. WIRELESS-ACL-MIB.my: This is the ACL object MIB.
- b. WIRELESS-CELLULAR-MIB.my: This is the Cellular object MIB.
- c. WIRELESS-DEVICE-MIB.my: This is the Device Management object MIB.
- d. WIRELESS-EVENT-MIB.my: This is the Event/Trap MIB.
- e. WIRELESS-ROOT-MIB.my: This is the top level object MIB.
- f. WIRELESS-RELAY-MIB.my: This is the top level object MIB.
- g. WIRELESS-SERIAL-MIB.my: This is the Serial Port object MIB.
- h. WIRELESS-STATISTICS-MIB.my: This is the Serial Port object MIB.
- i. WIRELESS-SWITCH-MIB.my: This is the Serial Port object MIB.
- j. WIRELESS-SYSTEM-MIB.my: This is the System objects MIB.

(Please download the latest MIB file from web site.)

5.2 Command Line Interface (CLI)

The Cellular Router provides the Command Line Interface (CLI), you can access it through the console or Telnet. The Command Line Interface (CLI) is the user interface to the Cellular Router's embedded software system. You can view the system information, show the status, configure the switch and receive a response back from the system by keying in a command.

The below screen is the login screen of the Cellular Router. The default username/password is admin/admin, it is the same as Web GUI. Once you modified it from other configuration interface, please type the new name/password to login.



There are some different command sets. Each command sets has its own access ability and available command lines. These command sets are:

SHOW: This is "Read Only" command to show the current setting and status of the AP/Gateway.

SET: This is Write command to change the current setting.

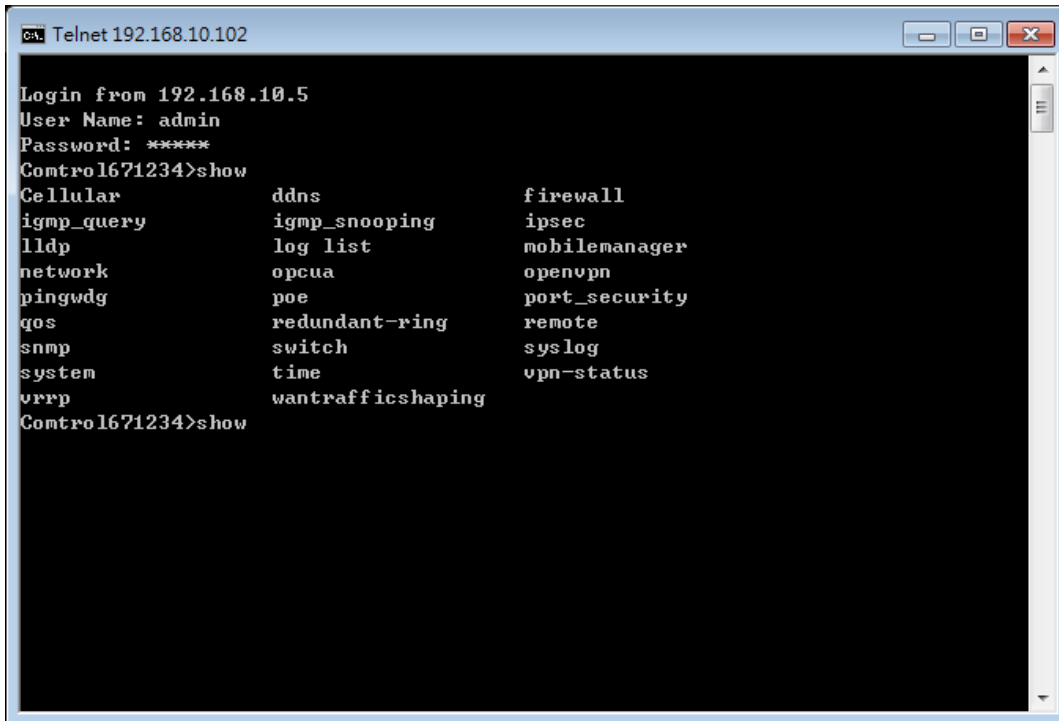
Del: This is Delete command to delete the applied settings.

Exit: To exit the CLI. It is logout command.

Note: Use "Tab" key can help you find the correct command and complete the command no matter you want to Read or Write easier.

5.2.1 Show Command Set:

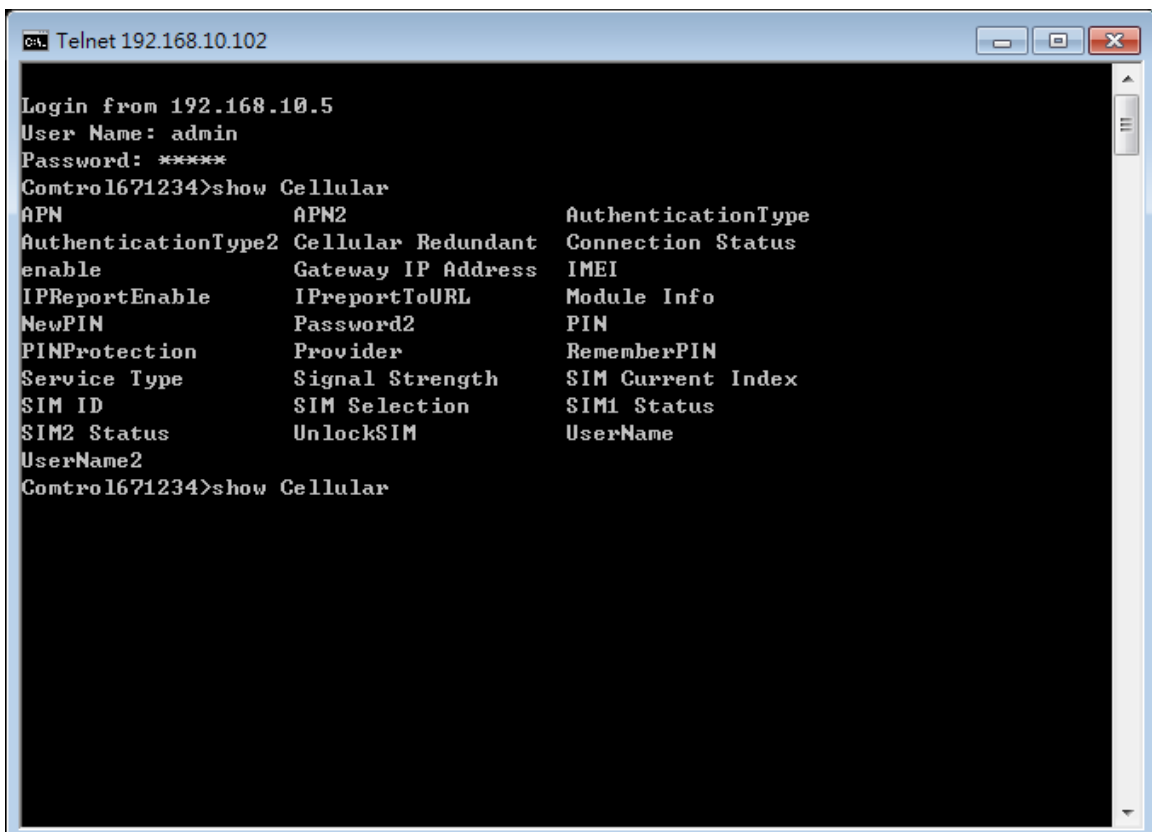
Type **Show** + “Tab↵” to see all the show command sets. The following command lines are available.



```

Telnet 192.168.10.102
Login from 192.168.10.5
User Name: admin
Password: *****
Comtrol671234>show
Cellular          ddns              firewall
igmp_query        igmp_snooping    ipsec
lldp              log_list         mobilemanager
network          opcua            openvpn
pingwdg          poe              port_security
qos              redundant-ring   remote
snmp             switch           syslog
system          time             vpn-status
vrrp            wantraffichaping
Comtrol671234>show
    
```

Type **Show Cellular** + “Tab↵” to see all the show cellular command lines.



```

Telnet 192.168.10.102
Login from 192.168.10.5
User Name: admin
Password: *****
Comtrol671234>show Cellular
APN                APN2              AuthenticationType
AuthenticationType2 Cellular Redundant Connection Status
enable            Gateway IP Address IMEI
IPReportEnable    IPreportToURL    Module Info
NewPIN           Password2         PIN
PINProtection     Provider          RememberPIN
Service Type      Signal Strength   SIM Current Index
SIM ID           SIM Selection     SIM1 Status
SIM2 Status      UnlockSIM         UserName
UserName2
Comtrol671234>show Cellular
    
```

SHOW Cellular Command Set:

Type **Show cellular** + “**Enter**” to see all the cellular information. The console print all the information for reference.

```

Comtrol671234>show Cellular
Cellular SIM Current Index : 1
Cellular Provider : NONE
Cellular Service Type : No Service
Cellular IMEI : 358709050126667
Cellular Signal Strength : 0 dBm
Cellular SIM1 Status : SIM Not Inserted
Cellular SIM2 Status : SIM Not Inserted
Cellular Connection Status : Disconnected
Cellular Gateway IP Address :
Cellular Module Info : Cinterion
 PLS8-E
 REVISION 02.011

Cellular SIM ID :
Cellular enable : Enabled
Cellular SIM Selection : 1
Cellular Cellular Redundant : Disabled
Cellular APN : internet
....
    
```

For example: Type **show Cellular A** + “**Tab**” to complete the commands, and then you can see the result.

```

Comtrol671234 >show Cellular A (+Tab)
APN APN2 AuthenticationType
Comtrol671234 >show Cellular AP (+Tab)
APN APN2
Comtrol671234 >show Cellular APN (+ Enter)

Cellular APN : internet (This is the result.)
    
```

SHOW POE Command Set:

```

Comtrol671234>show poe (+Tab)
pd-detect pd-status-detection port-1
    
```

port-2 **schedule** **status**
system **system-power-budget warning-water-level**

Control671234>show poe status

```
Control671234>
Control671234>show poe status
poe status
-----
Port      Mode      Status    Class    Budget(W)  Consumption(W)  Voltage(V)  Current(mA)
-----
1         Disable  Off       ---      ---        0.0           0.0         0.0
2         Disable  Off       ---      ---        0.0           0.0         0.0
Control671234>
```

Control671234>show poe port-1

Port 1 Configuration :

Mode **:** **Disable**
Powering Mode **:** **802.3af**
Budget(W) **:** **31**
Priority **:** **Critical**

SHOW SWITCH Command Set:

Control671234>show switch

switch gi1 state **:** **Enable**
switch gi1 speed **:** **AutoNegotiation**
switch gi1 flow-control **:** **Disable**
switch gi1 pvid **:** **1**
switch gi1 ingress_type **:** **Broadcast Only**
switch gi1 ingress_rate **:** **10**
switch gi1 egress_rate **:** **0**
switch gi2 state **:** **Enable**
switch gi2 speed **:** **AutoNegotiation**
switch gi2 flow-control **:** **Disable**
switch gi2 pvid **:** **1**
switch gi2 ingress_type **:** **Broadcast Only**
switch gi2 ingress_rate **:** **10**
switch gi2 egress_rate **:** **0**
switch gi3 state **:** **Enable**
switch gi3 speed **:** **1000**
switch gi3 flow-control **:** **Disable**
switch gi3 pvid **:** **1**
switch gi3 ingress_type **:** **Broadcast Only**
switch gi3 ingress_rate **:** **10**
switch gi3 egress_rate **:** **0**
switch gi3 vendor **:** **WESTERMO**
switch gi3 wavelength **:** **1310 nm**

```

switch gi3 distance      : 10000 m
switch gi4 state        : Enable
switch gi4 speed        : 1000
switch gi4 flow-control : Disable
switch gi4 pvid         : 1
switch gi4 ingress_type : Broadcast Only
switch gi4 ingress_rate : 10
switch gi4 egress_rate  : 0
switch gi4 vendor       : WESTERMO
switch gi4 wavelength   : 1310 nm
switch gi4 distance     : 10000 m
switch vlan manageID    : 1
    
```

String format : vlanid untag port_num tag port_num.

```

Ex : set switch vlan addvlan 2 untag 1,2 tag 3,4
switch vlan overview
Vlan ID   gi1      gi2      gi3      gi4
-----
1         ---      Untag   Untag   Untag
2         Untag   Untag   Tag     Tag
switch statistics overview
Port      Link      Rx Good  Rx Bad  Rx Abort  Tx Good  Tx Bad  Collision
-----
gi1       Down     8449    0       0         12536   0       0
gi2       Up       560614 0       0         44335   0       0
gi3       Down     0       0       0         0       0       0
gi4       Down     0       0       0         0       0       0
Comtrol671234>
    
```

5.2.2 Set Command Set:

Type **Set** + “Tab↵” to see all the write command sets. The following command lines are available



The most Set comment lines have the same functionality as the the Web GUI. Please read user manual to know all the features our Cellular Router supported. And the CLI is a different

way for you to complete the setting.

SET CELLULAR Command Set

Example: Set the Cellular Settings

```
Comtrol671234>set Cellular (+Tab)
APN                APN2                AuthenticationType
AuthenticationType2 Cellular Redundant Connect/Disconnect
enable            IPReportEnable    IPReportToURL
NewPIN            Password          Password2
PIN              PINProtection    RememberPIN
SIM Selection     UnlockSIM        UserName
UserName2
```

Example: Cellular Enable/Disable:

```
Comtrol671234>show Cellular enable
Cellular enable      : Disabled
Comtrol671234>set Cellular enable Enabled
Cellular enable      : Enabled
Comtrol671234>set Cellular enable Disabled
Cellular enable      : Disabled
Comtrol671234>
```

SET POE Command Set

Example: Set POE Settings

```
Comtrol671234>set poe (+Tab)
pd-detect          pd-status-detection port-1
port-2            schedule          system
system-power-budget warning-water-level
```

Example: Change POE Powering Mode:

```
Comtrol671234>show poe port-1
Port 1 Configuration :
Mode                :      Disable
Powering Mode       :      802.3at(2-Event)
Budget(W)           :      31
Priority             :      Cirtical
```

```
Comtrol671234>set poe (+Tab)
pd-detect          pd-status-detection port-1
port-2            schedule          system
system-power-budget warning-water-level
```

```
Comtrol671234>set poe port-1 powering-mode
802.3af            802.3at(2-Event)  forced
```

```
Comtrol671234>set poe port-1 powering-mode 802.3af
```

```
Comtrol671234>show poe port-1 status
Port 1 Configuration :
Mode                :      Disable
Powering Mode       :      802.3af
```


Budget(W) : 31
 Priority : Cirtical

SET SWITCH Command Set

Example: SET SWITCH Setting

```
Comtrol671234>set switch (+Tab)
gi1      gi2      gi3      gi4      statistics  vlan
```

Example: Enable/Disable port 3

```
Comtrol671234>show switch gi3 state
switch gi3 state      : Enable
```

```
Comtrol671234>set switch gi3 state Disable
switch gi3 state      : Disable
```

```
Comtrol671234>show switch gi3 state
switch gi3 state      : Disable
```

Example: Add SWICH vlan 2 port 1, 2 untag, port 3,4 tag:

String format : vlanid untag port_num tag port_num.

```
Comtrol671234>set switch vlan addvlan 2 untag 1,2 tag 3,4
ok!
```

```
Comtrol671234>show switch vlan
switch vlan manageID      : 1
String format : vlanid untag port_num tag port_num.
Ex : set switch vlan addvlan 2 untag 1,2 tag 3,4
```

```
switch vlan overview      :
Vlan ID  gi1    gi2    gi3    gi4
=====  =====  =====  =====  =====
1        Untag  Untag  Untag  Untag
2        Untag  Untag  Tag    Tag
```

Example: Remove port 1 from vlan 1:

```
Comtrol671234>set switch vlan addvlan 1 untag 2,3,4
ok!
```

```
Comtrol671234>show switch vlan overview
switch vlan overview      :
Vlan ID  gi1    gi2    gi3    gi4
=====  =====  =====  =====  =====
1        ---    Untag  Untag  Untag
2        Untag  Untag  Tag    Tag
```

5.2.3 Delete Command Set:

Type del + “Tab↵” to see all the delete command sets. The following command lines are available.

```
Comtrol671234>del
ipsec      log list  opcua     openvpn   remote
```

The log list can be deleted through CLI.

Control671234>del log list

5.3 i-View Utility

The i-View Utility provides you convenient tool to scan the network and configure the AP. Please connect your PC to port GT1, or GT2 (LAN) and start below steps to scan and configure.

5.3.1 Device Discovery:

Step 1: Open i-View Utility.

Step 2: Select the correct NIC (Network Interface Card) from the NIC list or remains the “All Interfaces”.

Step 3: Click “**Discovery**”, and then the Nodes and its IP address can be found and listed in Node list.

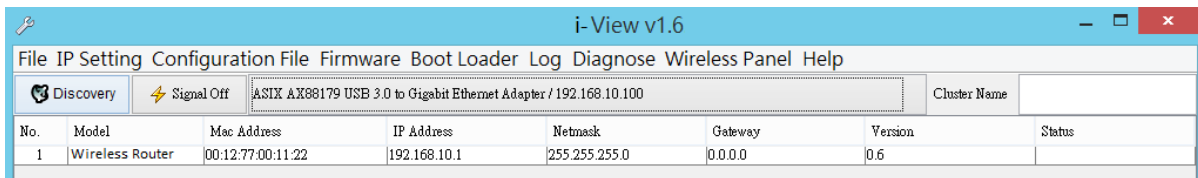
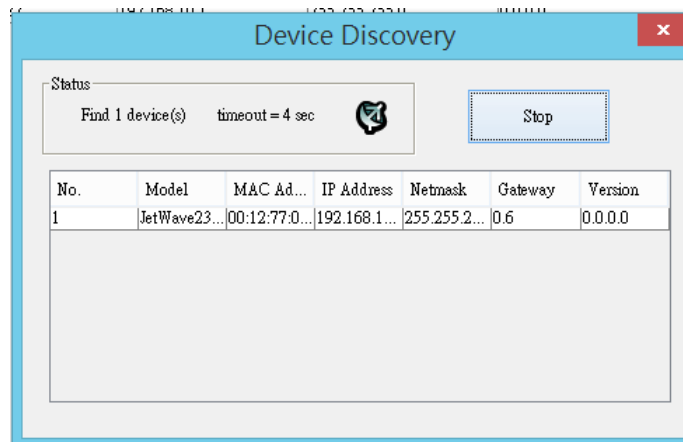


Figure: The main screen of the i-View Utility

Figure: The Device Discovery Screen, please wait couple seconds.



5.3.2 Basic Tools Shortcut:

After you scan the network, select the AP/Gateway and click Right key of mouse, you can see some tools.

- a. You can modify the IP address/Netmask directly on the field and then Click “**Change IP**“ to change the IP settings.
- b. Select multiple devices and click “**Auto-Assign IP**”, the popup screen will ask you type the IP Address range. You can assign new IP address for the selected devices.

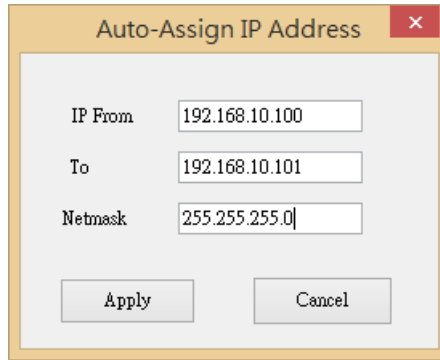
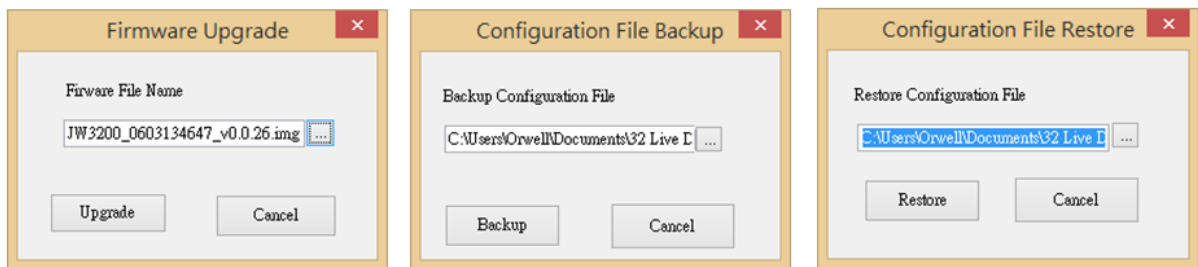
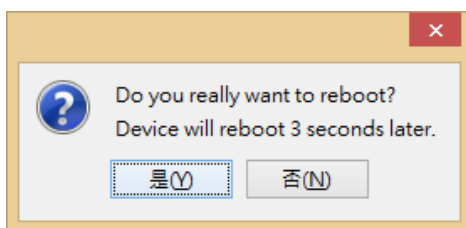


Figure: Assign the Auto-Assign IP Range.

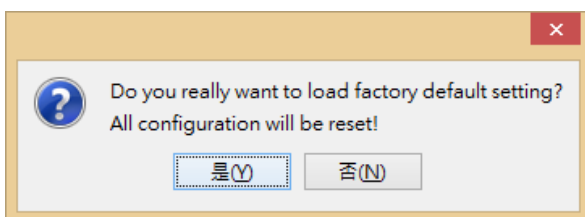
- c. You can enable DHCP client by “DHCP Client Enable”.
- d. You can upgrade firmware for single or multiple units by “**Firmware Upgrade**”. A popup screen will ask you select the target firmware file you’d like to upgrade.
- e. You can Backup/Restore the configuration file by “**Configuration File -> Backup/Restore**”. A popup screen will ask you select target configuration/target folder you’d like to backup or restore.



- f. Click “**Open Web GUI**” to access the web management interface.
- g. You can reboot the device by “**Reboot Device**”. A popup screen will ask you confirm again.



- h. You can restore to default configuration by “**Load Factory Default**”. A popup screen will ask you confirm again.



Note: You can also find these commands in the upper menu of the i-View Utility.



Chapter 6

Troubleshooting

Chapter 6 Troubleshooting

This chapter provides troubleshooting procedures for basic problems with the JetWave2714GF-LTE-E. For warranty assistance, contact your service provider or distributor for the process.

6.1 General Question

6.1.1 How to know the MAC address of the product?

MAC Address distinguishes itself by the unique identity among network devices. There are two ways available to know it.

Each device has a label posted on the side of the product. There are MAC addresses for Ethernet and Radio interfaces. On the Web-based management interface, you can view the MAC Address from “**Status**” -> “**Information**”. You can also see this in CLI or SNMP OID.

6.1.2 What if I would like to reset the unit to default settings?

You may restore factory default settings by click the “**Reset**” button above 7 seconds. By press Reset button, you will reset the IP address to default IP setting, LAN is 192.168.10.1.

Or you can reset the unit to default setting in Web GUI. You can reserve the IP address setting.

6.1.3 What if I can not access the Web-based management interface?

Please check the followings:

- Check whether the IP address of PC is correct (in the same network segment as the unit)
- Login the unit via other browsers such as Firefox, Google Chrome.
- Use i-View Utility to scan the AP and check/modify the IP address.
- If everything is correct, but, you still can't access the web GUI, we suggest you connect the console cable to do further checking. Please refer to the pin assignment in hardware installation chapter.
- Check whether the power supply is OK; Try to power on the unit again. If the web GUI can't be accessed issue occurred again, please contact our technical service engineer. We may ask you connect console cable and provide us more information.

6.2 Cellular

6.2.1 What if the Cellular connection is not stable, poor performance after associating with the base station?

- Please check the signal strength first. Once the signal strength is poor, the connection may be unstable. Even the connection is established, the performance is poor as well.
- You can move the device closed to the window or install external antenna outside the box/room/factory.
- If the distance between the Gateway and base station is far, the high gain antenna is an option to improve the transmission quality.
- Check whether the antenna supports the band you use or not? Normally, the outlook of the Cellular and WIFI antenna are the same.
- Check with the carrier provider and ask them check cellular connection condition of your site.
- Make sure the SIM card has enough quota/budget for both data upload and download. Some out-of-quota/budget card is only available for Download stream only.
- Make sure the maximum speed you applied from carrier provider. The remote connection will also reduce the performance. Make sure you have enough bandwidth from carrier provider.
- Download the screen message and debug message to our service engineer.
- Continuously ping one remote IP address through cellular connection for a while, once the ping is often timeout, check the status before leave the device on site.

6.2.2 What if the Cellular connection is always disconnected, how to resolve it?

- Make sure you insert the SIM card before power on the device. For 3G redundant, you MUST insert two SIM before power on the device.
- Make sure you insert the SIM card well, check the SIM status on Web GUI.
- Make sure the SIM card is available to support 3G connection. It is a simple way to insert it to smart phone for trail test.
- Make sure the SIM card has enough quota/budget for both data upload and download. Some out-of-quota/budget card is only available for voice only.
- Make sure the SIM settings. For example the APN number, SIM security...etc. In some countries, the carrier service provider asks customer input the correct APN name first. The APN

name may be different than its original setting. Please check the with your carrier service provider and type them correctly.

- Check whether the antenna supports 3G band or not? Normally, the outlook of the 3G and WIFI antennas are similar.
- Download the screen message and debug message to our service engineer.

6.2.3 Why the backup Cellular connection is not active?

- Make sure you insert the SIM card before power on the device. For Cellular redundant, you MUST insert two SIM before power on the device.
- Make sure the two SIM cards' setting and budget are all correct and enough.
- The backup SIM is activated after primary SIM failure for couple minutes. The default time is 10 minutes.

6.3 Appendix

6.3.1 ASCII

WEP can be configured with a 64-bit or 128-bit Shared Key (hexadecimal number or ACSII). As defined, hexadecimal number is represented by 0-9, A-F or a-f; ACSII is represented by 0-9, A-F, a-f or punctuation. Each one consists of two-digit hexadecimal.

ASCII Table

ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent
!	21	9	39	Q	51	i	69
"	22	:	3A	R	52	j	6A
#	23	;	3B	S	53	k	6B
\$	24	<	3C	T	54	l	6C
%	25	=	3D	U	55	m	6D
&	26	>	3E	V	56	n	6E
'	27	?	3F	W	57	o	6F
(28	@	40	X	58	p	70
)	29	A	41	Y	59	q	71
*	2A	B	42	Z	5A	r	72
+	2B	C	43	[5B	s	73
,	2C	D	44	\	5C	t	74
-	2D	E	45]	5D	u	75
.	2E	F	46	^	5E	v	76
/	2F	G	47	_	5F	w	77
0	30	H	48	`	60	x	78
1	31	I	49	a	61	y	79
2	32	J	4A	b	62	z	7A
3	33	K	4B	c	63	{	7B
4	34	L	4C	d	64		7C
5	35	M	4D	e	65	}	7D
6	36	N	4E	f	66	~	7E
7	37	O	4F	g	67		
8	38	P	50	h	68		

Revision History

Version	Description	Date	Editor
V1.0	1 st release for JetWave2714GF-LTE-E.	Oct, 2016	Orwell Hsieh Nobby Shen
V1.0a	Add DDNS, PoE, STP, VRRP sections, CLI	Mar 10, 2017	Orwell Hsieh Nobby Shen