JetWave 2310/2311 Series

Industrial Cellular Router/ IP Gateway

User Manual

V1.2 Jan. 2017

Copyright

About This Manual

This user manual is intended to guide professional installer to install the JetWave 2310 and how to configure the device. It includes procedures to assist you in avoiding unforeseen problems.

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 wordings is very important you must avoid.

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

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 beep 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

Chapter 1

Introduction

Chapter 1 Introduction

1.1 Introduction

The user manual is applied to Korenix JetWave 2310/2311 Series Industrial Cellular Router / IP Gateway. The JetWave 2310 is an industrial grade Cellular Router / IP gateway which enables Ethernet access over 3G/LTE network. The JetWave 2311 is an industrial grade Cellular + 802.11n 2.4G WIFI IP Gateway. The product series is equipped with one embedded 3G/LTE module to support different cellular communication bands. The 802.11n 2.4G WIFI in JetWave 2311 series can be the cellular offload solution to reduce the communication cost.

JetWave 2310/2311 Product Series:

Model Name	Description
JetWave 2310-HSPA	Industrial Cellular Router/Gateway, 2Xge, 3G UMTS/HSPA+ Five-Band
JetWave 2310-LTE-E	Industrial Cellular Router/Gateway, 2Xge, LTE 800(20)/900(8)/1800(3)/2600(7)
JetWave 2310-LTE-U	Industrial Cellular Router/Gateway, 2Xge, LTE 700(17)/850(5)/AWS(4)/1900(2)
JetWave 2311-HSPA	Industrial Cellular plus 802.11n 2.4G WIFI IP Gateway, 2Xge, UMTS/HSPA+ Five-Band
JetWave 2311-LTE-E	Industrial Cellular plus 802.11n 2.4G WIFI IP Gateway, 2Xge, LTE 800(20)/900(8)/1800(3)/2600(7)

For detail product specification, please download the latest datasheet from Korenix web site.

1.2 Product Package

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

Package:

JetWave 2310/2311 Unit

Default Antenna (Volume is different in different model)

Din-Rail Mounting Kit

6-pin Power Input connector

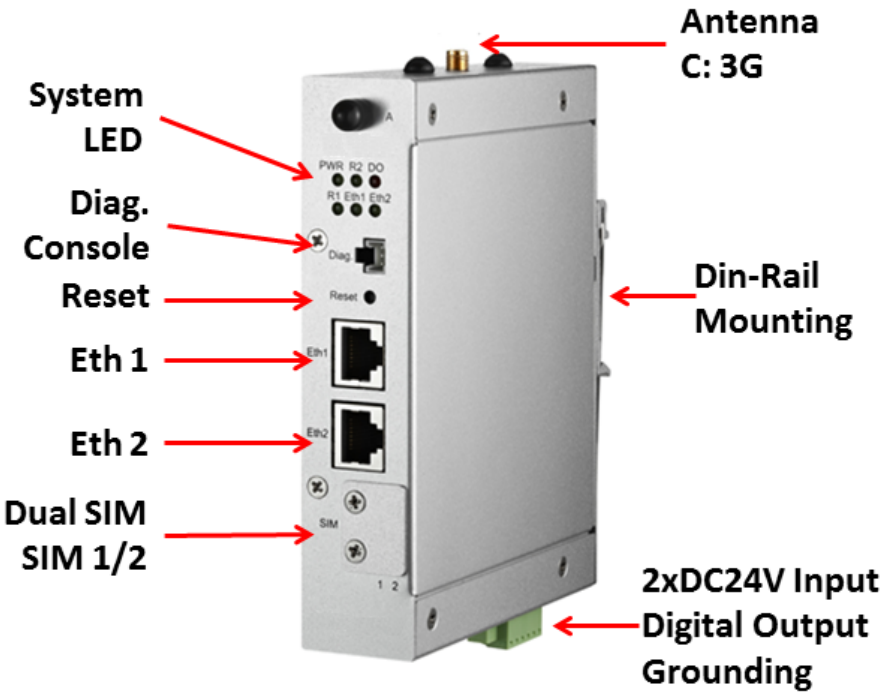
Quick Installation Guide

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

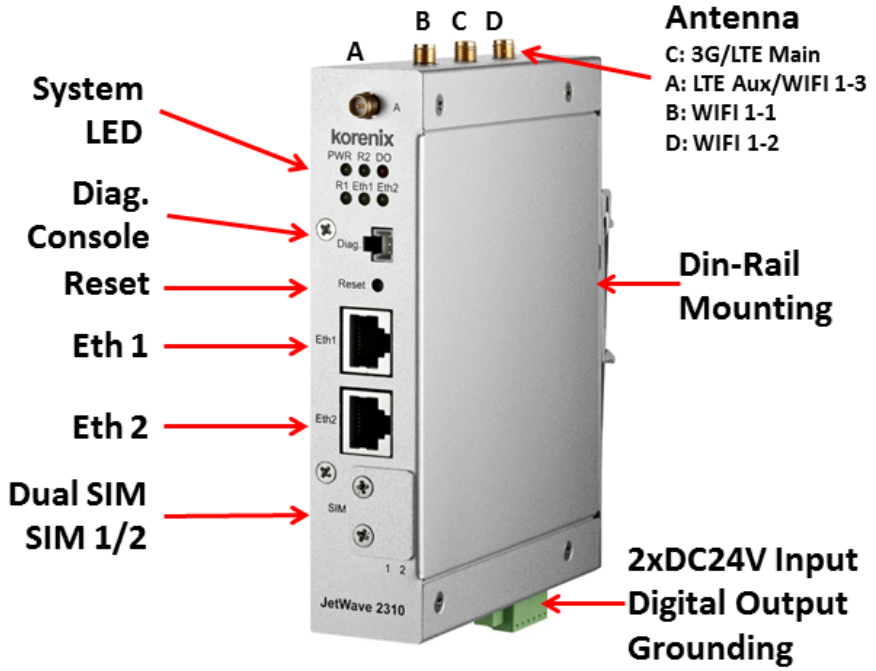
Note 1: Check the Korenix web site order information for new accessories, new version user manual, MIB file, firmware and Utility.

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.

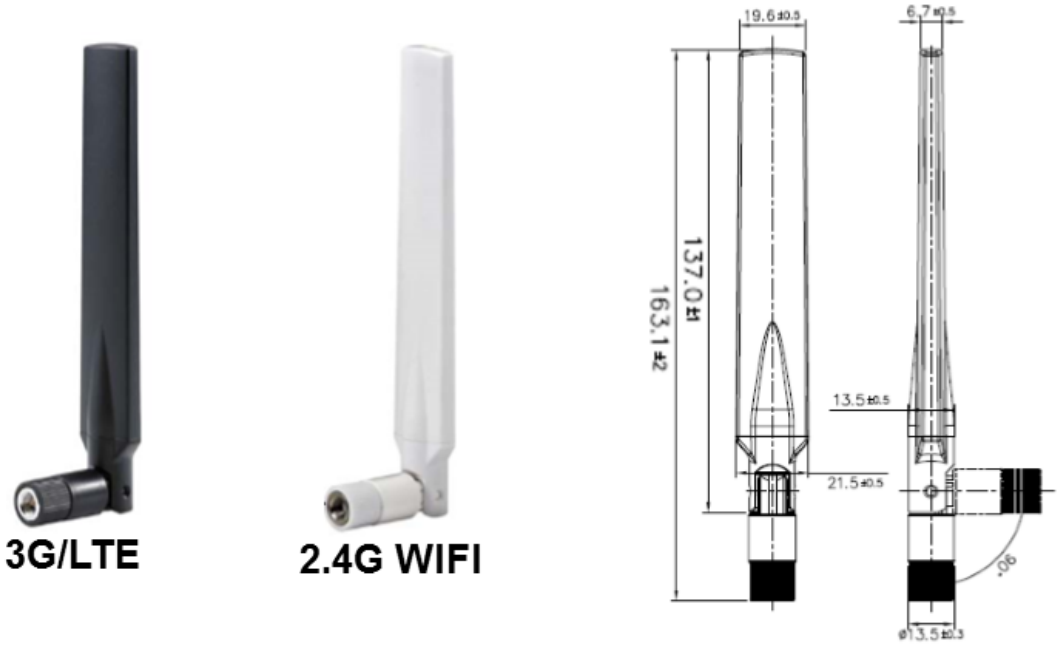
1.3 JetWave 2310/2311 Series Appearance



JetWave 2310 (JetWave 2310-HSPA) Appearance



JetWave 2311 Series Appearance



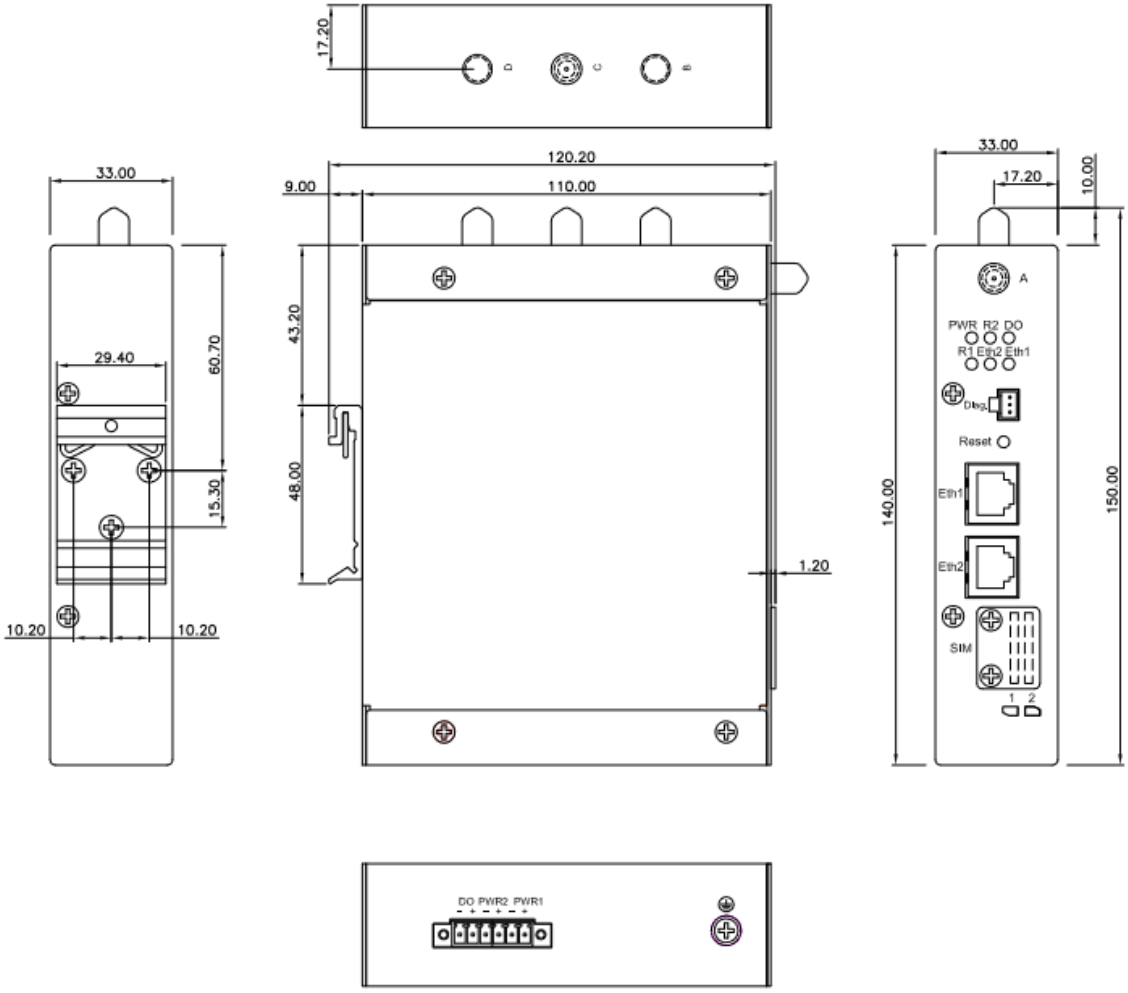
JetWave 2310/2311 Default Antenna Appearance/Dimension

Antenna	*2310-HSPA*	*2310-LTE-E/U*	*2311-HSPA*	*2311-LTE-E*
A		LTE-Aux	WIFI 1-3	LTE-Aux
B			WIFI 1-1	WIFI 1-1
C	3G	LTE-Main	3G	LTE-Main
D			WIFI 1-2	WIFI 1-2
Total Volume	1	2	4	4

1.4 JetWave 2310/2311 Series Major Features

- Industrial Slim Size Cellular Router/IP Gateway
- Next Generation Long Term Evolution (LTE) technology, 2x2 DL-MIMO, max. 100MDL/50M UL, compatible with UMTS/HSPA+ (LTE Models)
- Five band UMTS/HSPA+ (3G HSPA models)
- Dual SIM for Carrier Provider Redundant
- Dual Gigabit Ethernet Port HW-Based NAT Routing/Bridging
- VPN/Firewall/DMZ and Secure VPN Connectivity
- IEEE 802.11n 2.4G WIFI for more coverage, up to 3T3R MIMO, 450Mbps (2311 Series)
- 3G/LTE and WIFI/WAN Redundant/Auto-offload
- LAN/WIFI to 3G/LTE Routing
- Remote management by Web GUI, SNMP, Auto IP Report, Korenix View, Korenix NMS
- Dual 24V(12~48V) DC Redundant
- Wide Operating Temperature

1.5 JetWave 2310/2311 Dimension



Chapter 2

Hardware Installation

Chapter 2 Hardware Installation

This chapter describes safety precautions and product information before installing JetWave 2310 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 Wireless AP/Client/Router/Gateway 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

1. To keep you safe and install the hardware properly, please read and follow these safety precautions.
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. When the system is operational with extended Radio cable, avoid signal lost of the cable.
5. When you exchanged to high gain antenna, avoid standing directly in front of high gain antenna. Strong RF fields are present when the transmitter is on.

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

   The above safety precautions are applied to all Wireless product installation.

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 12 to 24 AWG.
3. The typical and suggest power source is DC 24V, the acceptable range is range from 12~48V. Please note that while you connect 48VDC, make sure the inrush voltage shall be under 10% tolerance (52.8V).
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.

2.3 I/O Configuration

2.3.1 Wiring your Ethernet Port

There are two Gigabit Ethernet ports. The 2 ports are standard RJ-45 form factor. They 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.

Available 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 an Heavy Industrial EMC certificated product and 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.

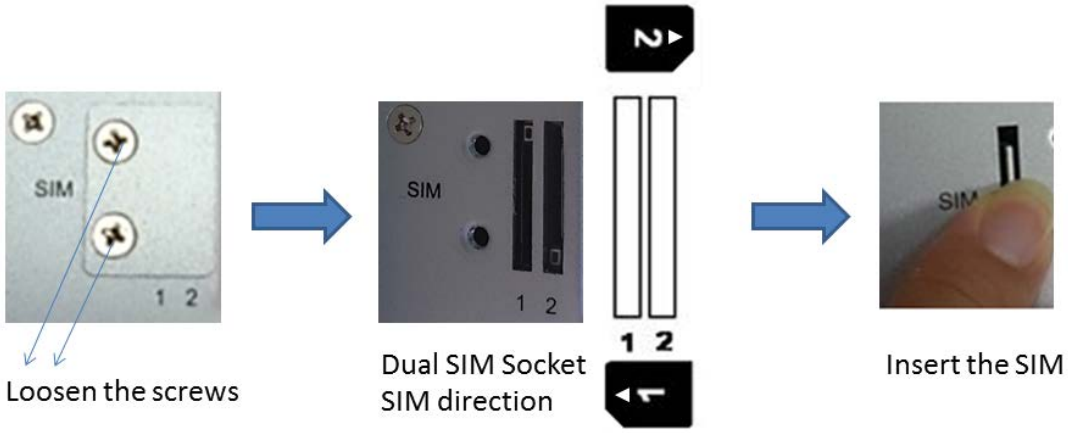
2.3.2 Reset

There is one Reset button located on the front of the device. This is design 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 JetWave 2310 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 3G Redundant and you can configure SIM 2 as startup or backup SIM socket, please go to Web GUI – 3G to modify the setting.

Note: The 3G Redundant is only available while you insert two SIM cards into the socket. If you only insert one, please DO NOT enable 3G Redundant.

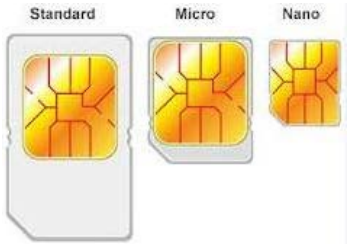
Note: You should not select the empty SIM and press “Connect” for the empty socket in Web GUI. The system can’t support this error configuration. The system may display warming message and you must re-select correct SIM, it may request system reboot after changed.

SIM Types:

The supported SIM card is standard SIM card. If your ISP provide you Micro-SIM or Nano-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.

The micro-SIM carry board. Put the Micro-SIM card to the standard SIM card type carry board and plug into the system.

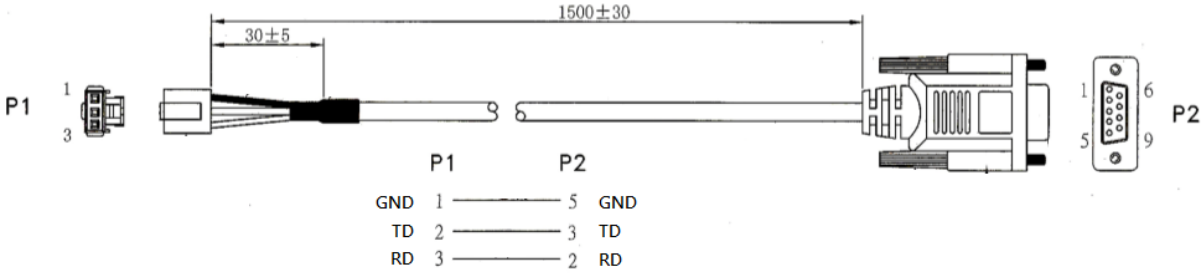
Note: While you prepare to plug in the SIM card, please remember to power off the system first. This is a MUST step, it allows the JetWave 2310 system to detect the SIM card while booting up.

Note: The SIM 1 is the default SIM socket.

2.3.4 Diag. Console

There is one 3-pin console **reserved for engineering diagnostic** in the bottom of the device. The 3 pin indicates below pin assignment of the typical RS-232 serial connection. You can wire the cable by yourself or purchase from Korenix.

	Pin 1	Pin 2	Pin 3
Diag. Socket	GND(Ground)	Receive Data (RD)	Transmit Date (TD)
D-Sub 9	GND(Ground)	Transmit Date (TD)	Receive Data (RD)



2.3.5 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 24 AWG.

2.3.6 Ground

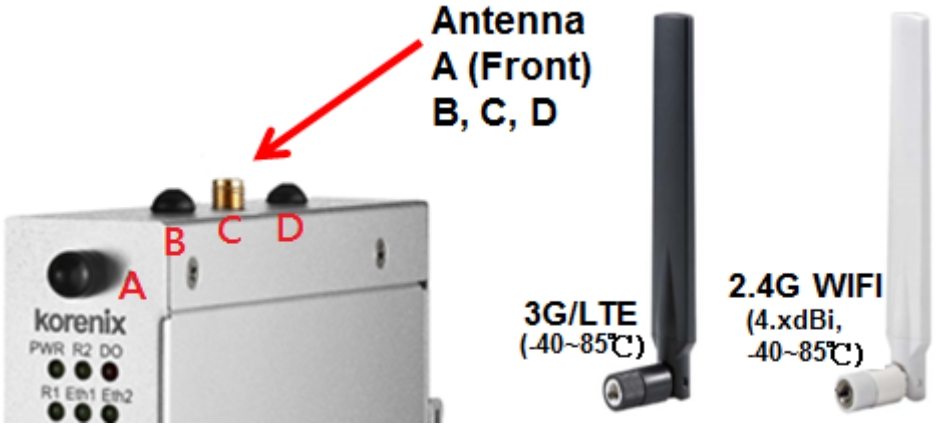
To ensure the system will not be damaged by noise or any electrical shock, you must make exact connection with the Earth Ground. There is one earth ground screw on the bottom side of the device. Loosen the earth ground screw then tighten the screw after earth ground wire is connected.

2.4 Antenna

The JetWave 2310 series supports up to 4 antenna sockets for 2310/2311 series. The product attaches 3G/LTE and WIFI antennas inside the package.

2.4.1 Antenna Placement

The placement of the antennas is listed as below:



Ant.	*2310-HSPA*	*2310-LTE-E/U*	*2311-HSPA*	*2311-LTE-E*
A		**LTE-Aux**	**WIFI 1-3**	**LTE-Aux**
B			WIFI 1-1	WIFI 1-1
C	3G	LTE-Main	3G	LTE-Main
D			WIFI 1-2	WIFI 1-2
Total Volume	1	2	4	4

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

For example, the JetWave 2310-HSPA supports one 3G antenna only, it uses antenna number C as the 3G Antenna socket and the other holes are covered. This is reverse SMA type antenna socket. Please connect your 3G Antenna to the antenna number C.

Note: Below are the easy ways to identify the antenna for reference:

a. The Antenna C is designed for 3G or LTE Main.

b. Antenna B and D are designed for 1st and 2nd WIFI radio.

c. The Antenna A may have different usage to support LTE-Aux. or the 3rd WIFI (3T3R) of the JetWave 2311 Series.

d. The black color antenna is 3G or LTE antenna, the white color is 2.4G WIFI antenna.

e. If want to change the Antenna number setting in Web GUI, refer to the 4.3.3 Wireless Advanced Setting.

2.4.2 3G/LTE Antenna Specifications

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

The Antenna is wide-temperature design, however, 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℃ to +85℃
Humidity	95% @ 25℃

2.4.3 WIFI Antenna Specification

Below figure is the specification of the attached WIFI Antenna.

The Antenna is wide-temperature design, however, if you want to install it in outdoor area, please select water-proof outdoor antenna.

Specifications

Frequency (MHz)	2400-2500
Peak gain(dBi)	4
VSWR	2.0 : 1 Max.
Polarization	Linear, vertical
Impedance	50 Ω
Connector	RP SMA PLUG

Environment & Mechanical Characteristics

Temperature	-40℃ to +85℃
Humidity	95% @ 25℃

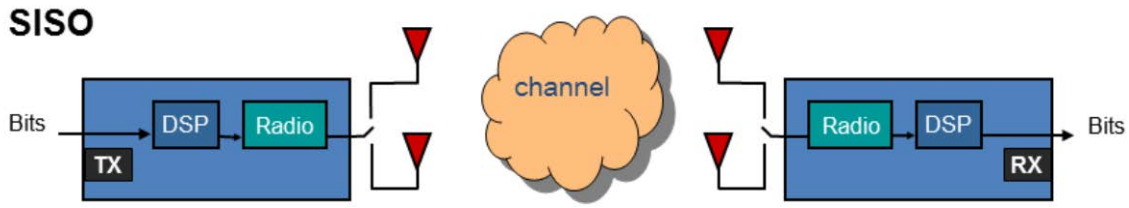
2.4.4 WIFI MIMO Introduction

The JetWave 2311 series WIFI radio supports IEEE 802.11n Multiple-input Multiple-output (short of MIMO) technology. The JetWave 2311-HSPA can support up to 3T3T MIMO, which means 3 Transmit 3 Receive, it can reach up to 450Mbps, triple times communication performance than traditional 1T1R SISO (Single-in Single-out).

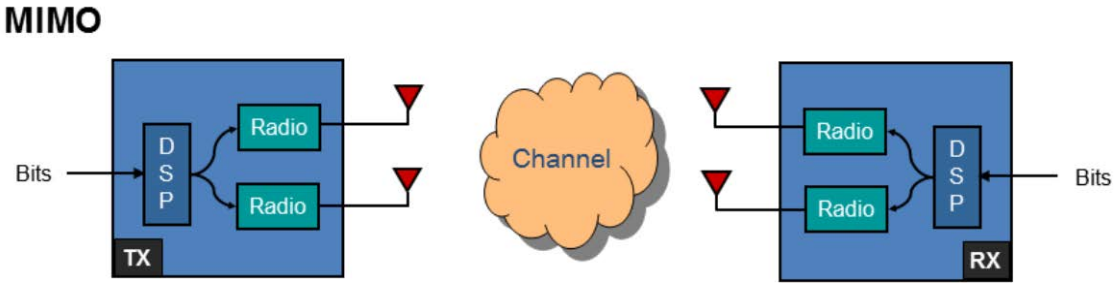
What is MIMO:

With the rising data rates and signal congestion, the MIMO is the proposed radio technology in IEEE 802.11n and accepted popularly. MIMO is short of the Multiple-Input and Multiple-Output, is the use of multiple antennas at both the transmitter and receiver to increase the wireless communication bandwidth, for example the 2T2R means 2 Transmitter and 2 receiver, then the bandwidth is double than SISO. MIMO technology offers significant increases in data throughput without additional bandwidth or increased transmit radio power.

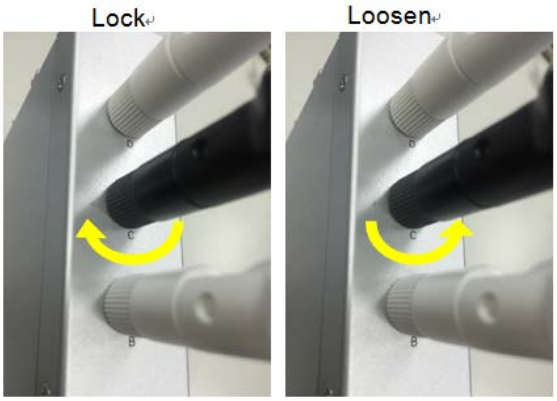
The below figure shows the SISO technology, each transmitter and receiver has single radio:



The below figure shows the MIMO technology, the transmitter and receiver spread the total transmit power to 2 (or more) different radio antenna for communication.



2.5 Antenna Installation



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.

Korenix provides the external antenna mounting kit, extended radio cable as optional accessory. While you need it, you can purchase from Korenix.

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

2.6 LED Indicator

The following table indicates the LED of your device.

LED	Indication	LED	Indication
PWR	**Power** Status Green ON = System ON	**R1**	**Radio 1 (3G/ 4G)** Status OFF = Booting Green Blinking = System is ready Green ON = Radio 1 is activated
R2	Status of the **Radio Number 2** Green ON = Radio 2 is activated *Note 1: NOT Support in JetWave 2310	**Eth 1**	**Ethernet Port 1** Status. Green ON = Eth 1 is Link Up. Green Blinking = Eth 1 is Activating
DO	**Digital Output** Status Red ON = The Relay is ON. It may indicate the alarm of specific events.	**Eth 2**	**Ethernet Port 2** Status. Green ON = Eth 2 is Link Up. Green Blinking = Eth 2 is Activating
Note 1: R1/R2 is the radio number. R1 is the first Radio, 3G Radio, this is applied for JetWave 2310 and 2311. R2 is the second Radio, WIFI Radio. This is applied to JetWave 2311 only.			

2.7 Mounting

2.7.1 Mounting the device

The JetWave 2310 series supports Din-Rail mounting. The Din-Rail mounting kit is Din 35 compliant and pre-installed in the back of the AP.

The JetWave 2310 series also provide 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.

2.7.1 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.

2.7.2 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 3G antenna and follow the same steps as “Mounting the default antenna on unit” to install your antenna.

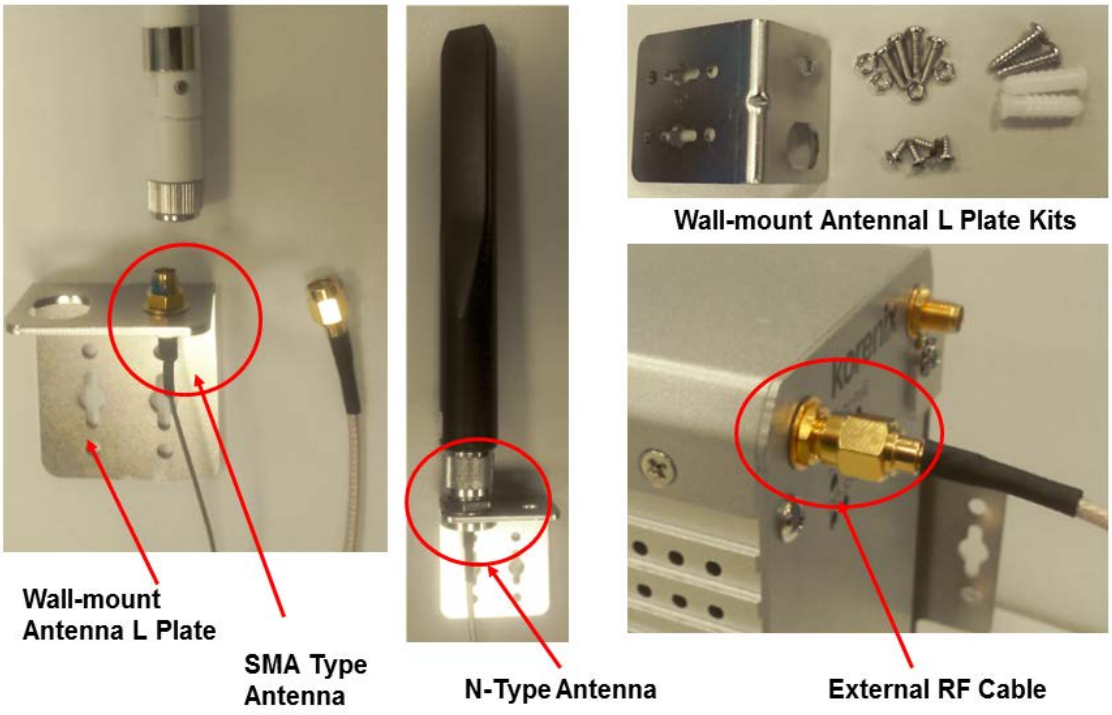
2.7.3 Mounting the N-Type external antenna:

While selecting the N-type external antenna, you must notice that the antenna should support 3G radio transmission. The JetWave external antenna mounting L plate is available for both SMA and N-Type antenna, purchase the external antenna mounting kit from your sales.

2.7.4 Below figure shows the optional External Antenna Mounting Kit

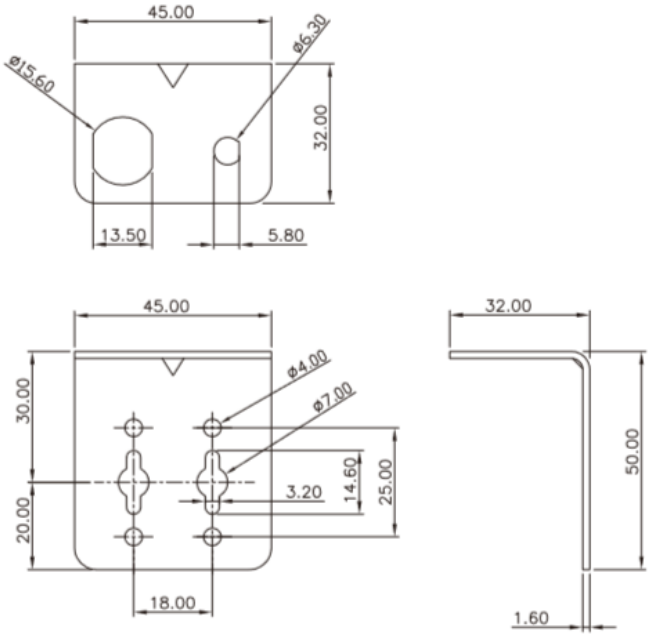
a) **Wall-mount Antenna L Plate Kits:** This plate supports SMA or N-Type connector, you can wall-mount it with the attached screws.

b) **External Radio Cable:** The cable is SMA Male Reverse to SMA Female Reverse RF cable.



(Reference Photo: The same as the JetWave 3220 Series)

Wall-mount Antenna L Plate Dimension (The same as JetWave 3200/3300/3400 Series)



JetWave 3200/3300/3400 Series
Wall-mount Antenna L Plate Dimension

2.8 Using the External Antenna

Normally, the attached 3G Antenna is available for most of the application. 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 3G 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 3G 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. For example the JWA-Arrestor-5803 is 0-6G Arrestor for N-Type Antenna.

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.

Chapter 3

Prepare for Management

Chapter 3 Prepare for Management

Both JetWave 2310/2311 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 Korenix 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 JetWave 2310 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 switch's configuration interface. For further info, please refer to configuration guide of the feature set.

Table 1 JetWave 2300 Basic Factory Default Settings

Features		Factory Default Settings
Username		admin
Password		admin
Model Name		JetWave2310-HSPA (depends on which model you access)
Device Name		korenixXXXXXX (X represents the last 6 digits of Ethernet MAC address)
Time Settings		Current Time
Cellular is NOT activated		2015.01.01
Cellular is activated		Get Cellular time
LAN IP Address (Default)		
IP Address		192.168.10.1
Subnet Mask		255.255.255.0
DHCP Server Setting	DHCP Server	Disable
	DHCP IP Range Start	0.0.0.0
	DHCP IP Range End	0.0.0.0
	DHCP Subnet Mask	0.0.0.0

	DHCP Gateway	0.0.0.0
	(Refer to the System – IP Setting for further info.)	
Diagnostic CLI	Console Type	3-pin (Tx, Rx, GND) Refer to the appendix B, RS232 to 3-pin pin assignment. Reserved for Engineering Diagnostic. (Check with Korecare@korenix.com)
	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.
WIFI (JetWave 2311)	Wireless Mode	Client
	SSID	JetWave2300_1
	802.11 Mode	802.11G/N
	Channel Mode	20MHz
	Antenna Number	Three (JetWave 2311-HSPA) Two (JetWave 2311-LTE)

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 JetWave 2310 Series is 192.168.10.1.

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: **192.168.10.1**) into the address field. You will see the WELCOME page as below.

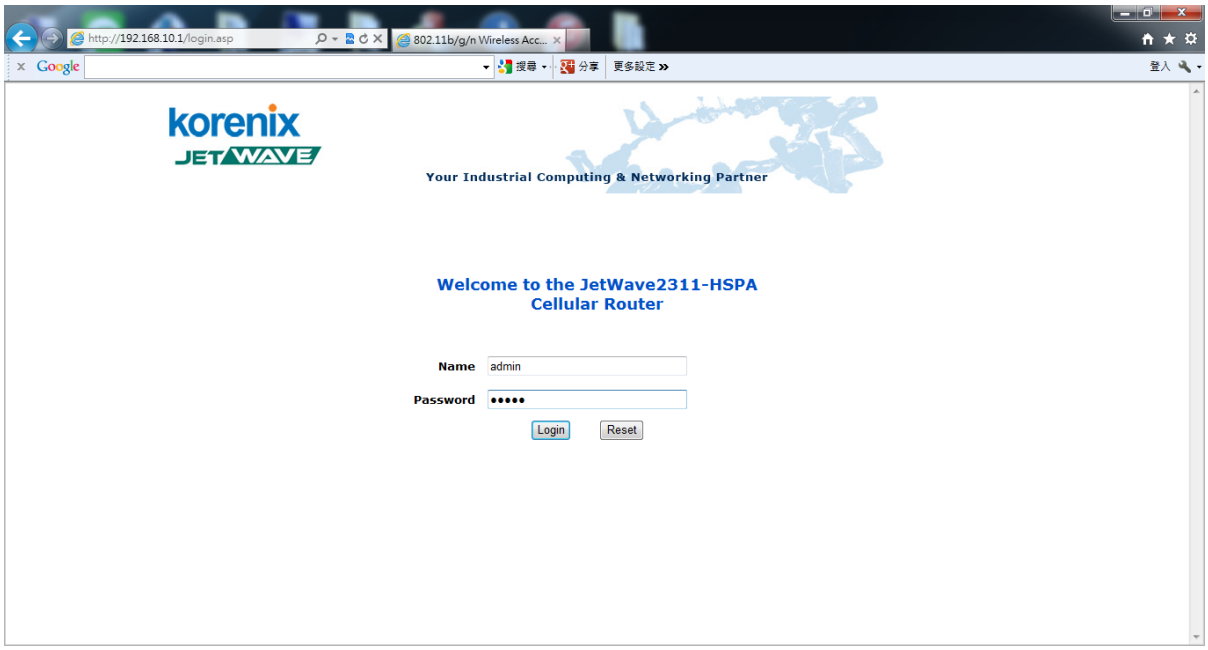


Figure – Login Page

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**, **Cellularf**, **Management**, **Tools**, **Save, Reboot** and **Logout**.

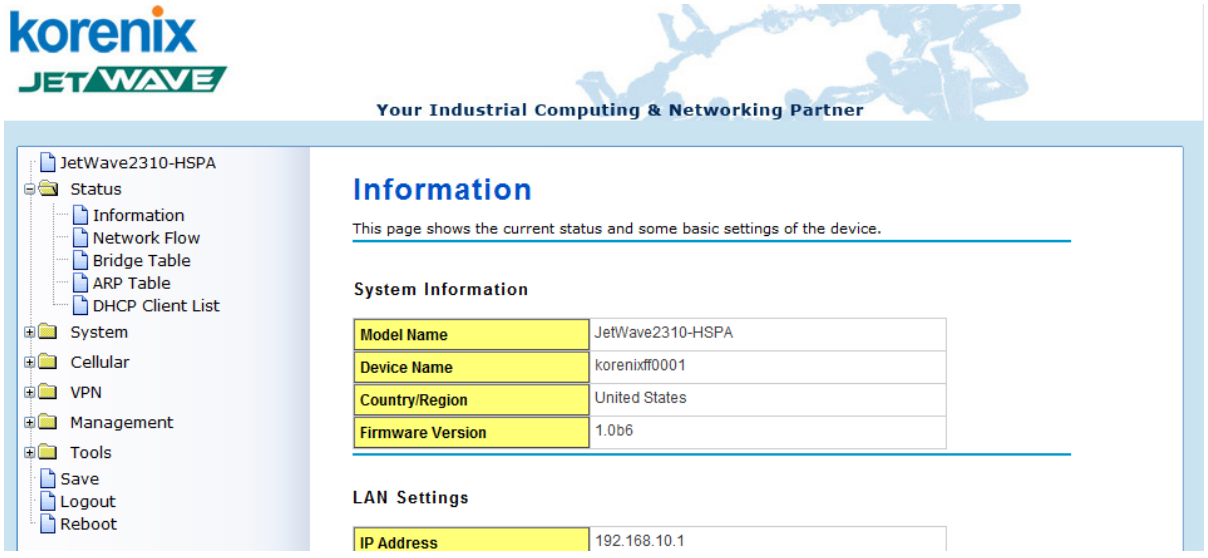


Figure – Main Page

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. Korenix web management page is developed by JAVA. It allows you to use a standard web-browser such as Microsoft Internet Explorer, or Mozila, to configure and interrogate the switch from anywhere on the network. The IE 5.0 or later versions do not allow Java applets to open sockets by default. Users have to directly modify the browser settings to selectively enable Java applets to use network ports.
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. The new JAVA version may have different security policy in different versions, please contact Korenix engineer (Korecare@korenix.com) once you have problem for login.

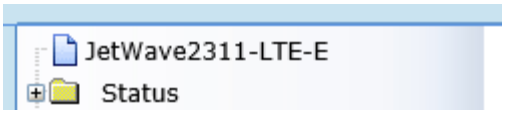
Chapter 4

Web GUI Configuration

Chapter 4 Web GUI Configuration

This chapter describes the Web GUI for Software Configuration.

In the top of the Web configuration tree, it shows the product name and the cellular communication type. Check whether this is the correct product first before start the following configuration.

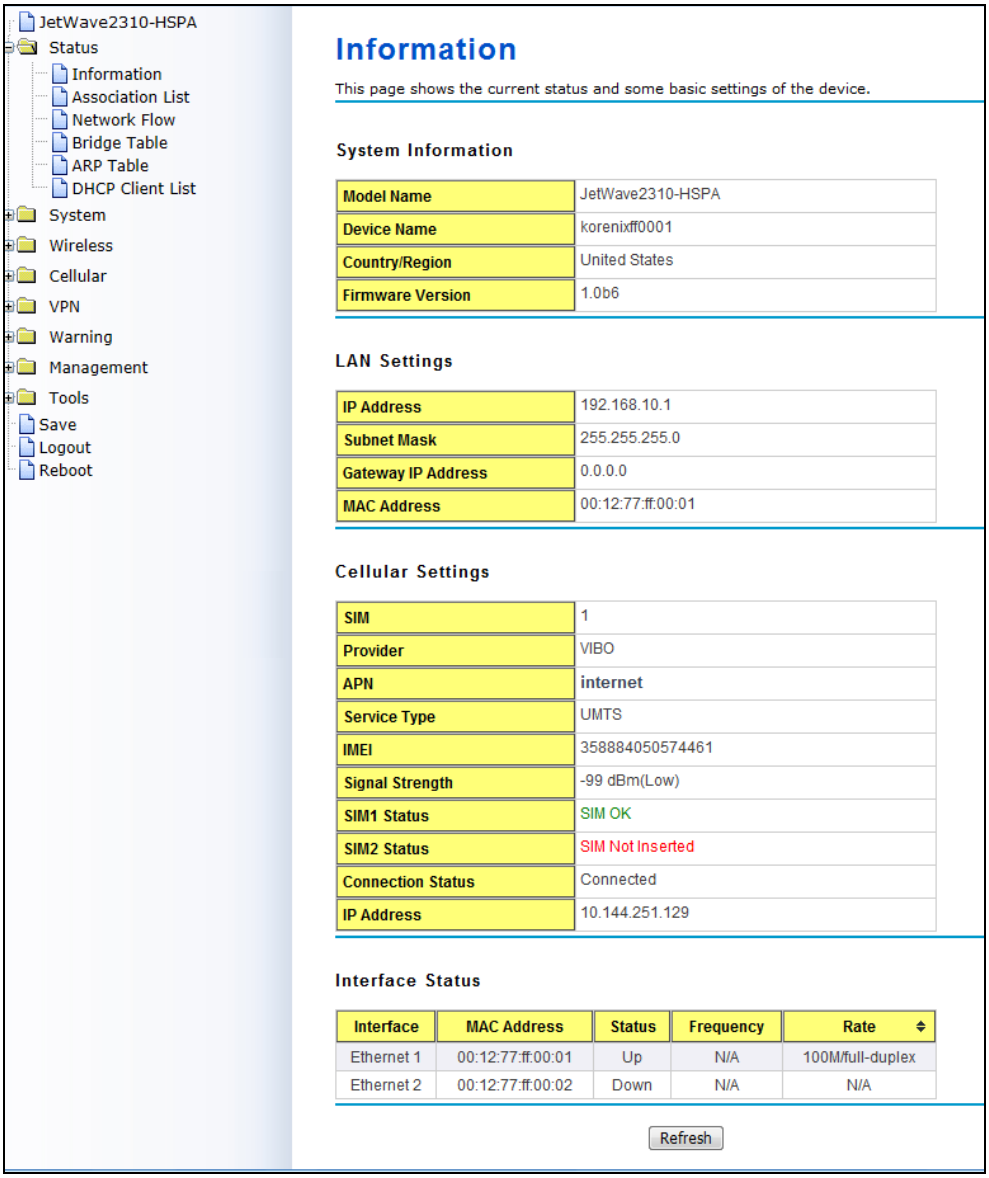


Ex: JetWave 2310-HSPA supports 3G UMTS/HSPA+. JetWave 2311-LTE-E supports the WIFI and LTE.

4.1 Status

The Status feature set includes **Information, Network Flow, Bridge Table, ARP Table** and **DHCP Client List**. The information 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.

System Information: The Model Name, Device Name, Country/Region you selected and Firmware version number.

LAN Setting: 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, SIM status, Connection status and IP address.

SIM: The SIM card number. 1 or 2 is pends on

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

which SIM you selected in 3G Basic Settings.

Provider: The name of the ISP.

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

Note that 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 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, Unknown, No Service(default value)

IMEI: This item shows the International Mobile Equipment Identity (IMEI) of the 3G 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 interface is connected to the base station.

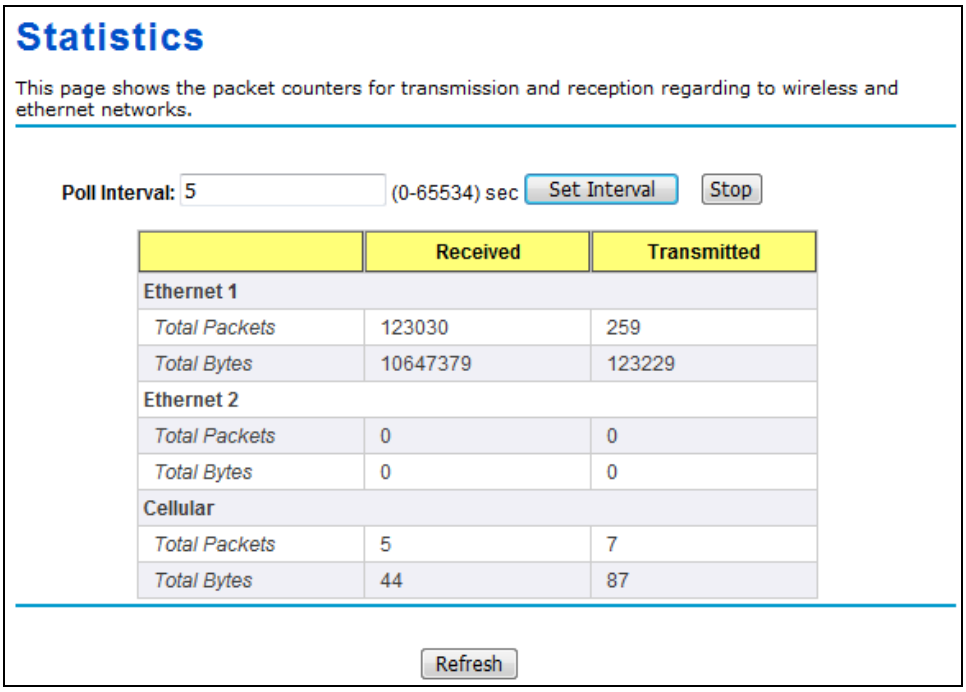
Not Connected: The 3G interface is not connected to the base station.

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

Interface Status: This table shows the Interface Name, MAC Address, Status, Frequency and Rate of the connected device.

4.1.2 Network Flow (Statistics):

This page shows the packet counters for transmission and reception regarding to wireless(include Wi-Fi or 3G/LTE) and Ethernet. Wireless 1 means WIFI traffic. Cellular means 3G or LTE.



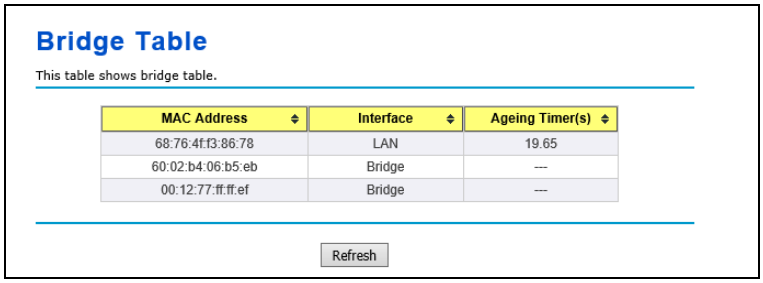
Poll Interval: The poll interval time setting, range from 0~65524 seconds. If you want to change the poll interval time, press “Stop” and then enter new value, press “Set Interval” to activate.

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

Stop: Stop polling the associated clients.

4.1.3 Bridge Table

This table shows bridge table.



MAC Address: The MAC address of the connected device.

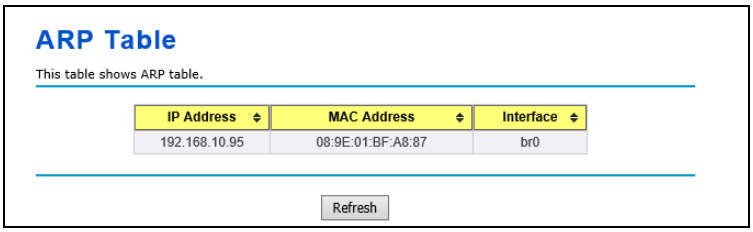
Interface: This field shows the interface which learnt the MAC Address.

Aging Timer(s): The aging time of this entry. If the MAC didn’t transmit any packet, the aging time will start counting, and delete the entry after aging timeout.

Refresh: Refresh the table.

4.1.4 ARP Table

This table shows the ARP table.



IP Address: The IP Address leant from the interface.

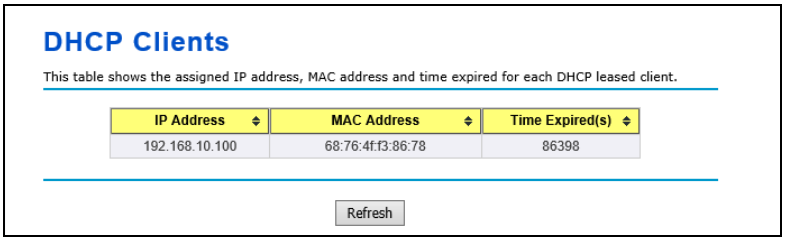
MAC Address: The MAC Address leant from the interface.

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

Refresh: Refresh the table.

4.1.5 DHCP Client List

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



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.

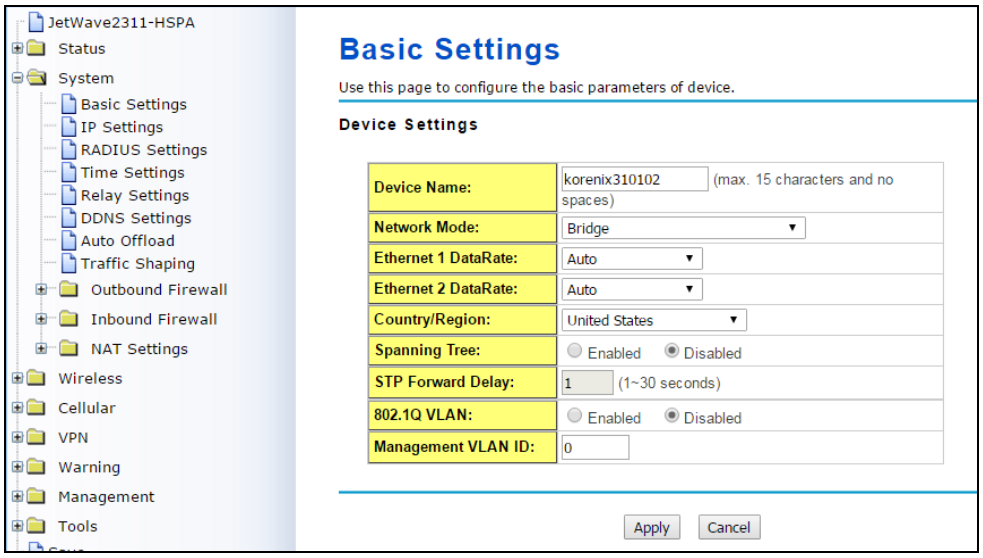
4.2 System

For users who use the JetWave 2310 series 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, RADIUS 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.



Device Name: User could give a name for identifying a particular outdoor access point in here. It allows maximum 15 characters and no spaces.

Network Mode: User could select "Bridge", "Router", "Auto Offload", and "Auto Offload – Eth to WIFI Bridge" mode depend on the application.

Bridge: Apply the system as bridge mode. In this mode, WIFI client and Ethernet ports are in the same broadcast domain.

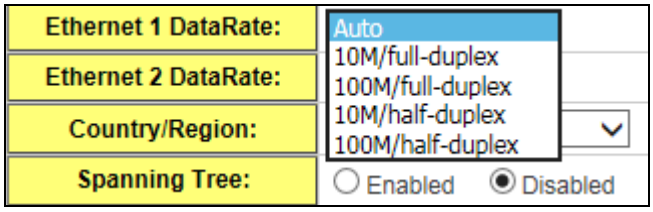
Router: Apply the system as router mode. In this mode, Ethernet port 1 is the WAN port. The Ethernet port 2 and WIFI client are in the same broadcast domain.

Auto Offload: Setup WIFI and Cellular path as the WAN port. WIFI is a wireless client mode and connects to AP as uplink path, and get IP address from base station as Cellular uplink

path. When WIFI performance is lower than threshold, the WAN path will go to Cellular path.

Auto Offload – Eth to WIFI Bridge: In this mode, WIFI is a wireless client mode and connects to AP as uplink path, and get IP address from base station as a Cellular uplink path. Ethernet port and WIFI client form a flat layer 2 network. It means the device, which connected to Ethernet port, is in the same subnet with WIFI client. When WIFI performance is lower than threshold, the WAN path will go to Cellular path.

Ethernet 1 Data Rate: Configure the Speed/Duplex of the port Eth 1. The default value, Auto means Auto-Negotiation. Force speed/duplex is available to setup here.



Ethernet 2 Data Rate: Configure the Speed/Duplex of the port Eth 2. The default value, Auto means Auto-Negotiation. Force speed/duplex is available to setup here.

Country/Region: Select the country you are installed.

Spanning Tree:

Spanning Tree Protocol (STP) is a link management protocol for AP which provides path redundancy while preventing loops in a network. STP allows only one active path at a time between the access points but establish the redundant link as a backup if the initial link fails.

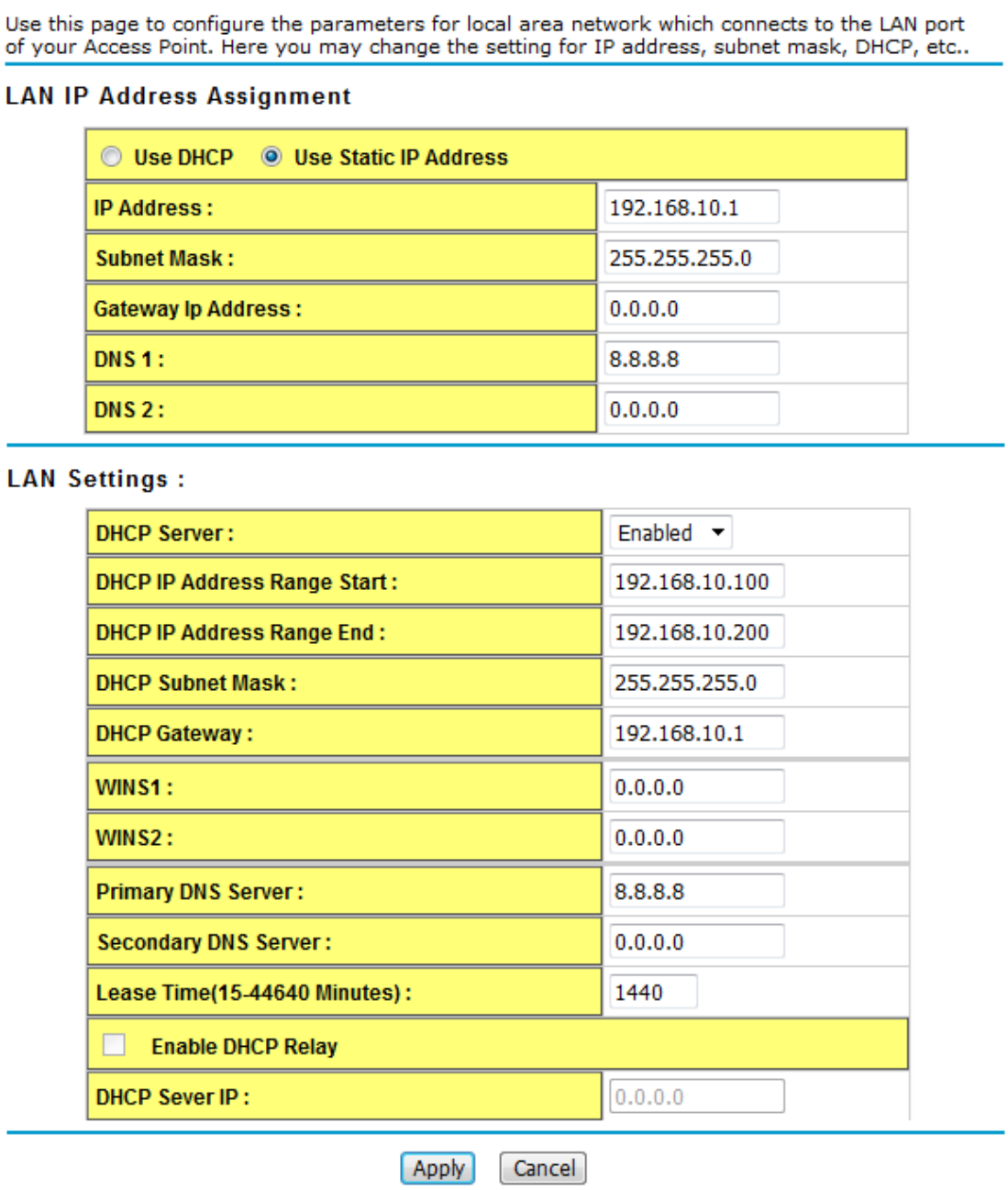
STP Forward Delay (1~30 Seconds): This is the Forward Delay value of the Spanning Tree protocol setting.

802.1Q VLAN: User can select enable 802.1Q VLAN function here.

Management VLAN ID: Here is the setting to decide which VLAN number included in the packet can access this device.

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.



LAN IP Address assignment:

Use DHCP: The device will get IP address and relation configuration from DHCP server.

Use Static IP address: Allows user set the device's IP address and relation configuration manually.

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 WAN interface. Set the IP subnet mask manually.

Gateway IP address: Input the IP address of gateway that the device will refer.

DNS1: Input the first IP address of DNS server that the device will refer.

DNS2: Input the second IP address of DNS server that the device will refer.

LAN Settings:

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

DHCP Server Setting:

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.

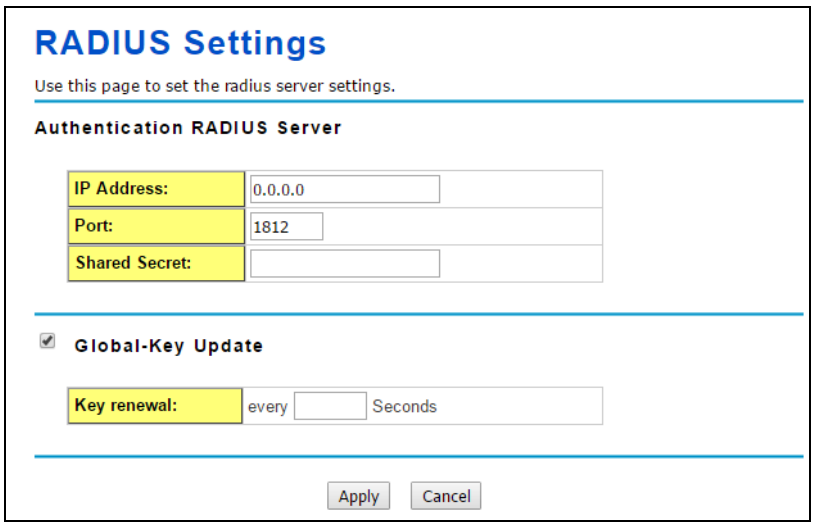
You can also configure the **Subnet Mask, DHCP Gateway, WIS, Primary/Secondary DNS Server**s' IP Address and **Least Time** of the assigned IP addresses.

Enable DHCP Relay:

You can also "**Enable DHCP Server**", click the "**Enable DHCP Relay**" and assign the "**DHCP Server IP"** address to activate the function.

4.2.3 RADIUS Settings

Use this page to configure the RADIUS Server Setting. RADIUS (Remote Authentication Dial-In User Service) is a server for remote user authentication and accounting; it plays a central role in the network in providing the capabilities of authenticating, authorizing, accounting, alarming and etc. It allows an organization to maintain user profiles in a central database that all remote servers can share.



Authentication RADIUS Server

IP Address: Enter the IP address of the Radius Server.

Port: Enter the TCP port number of the Radius Server; the default port number is 1812.

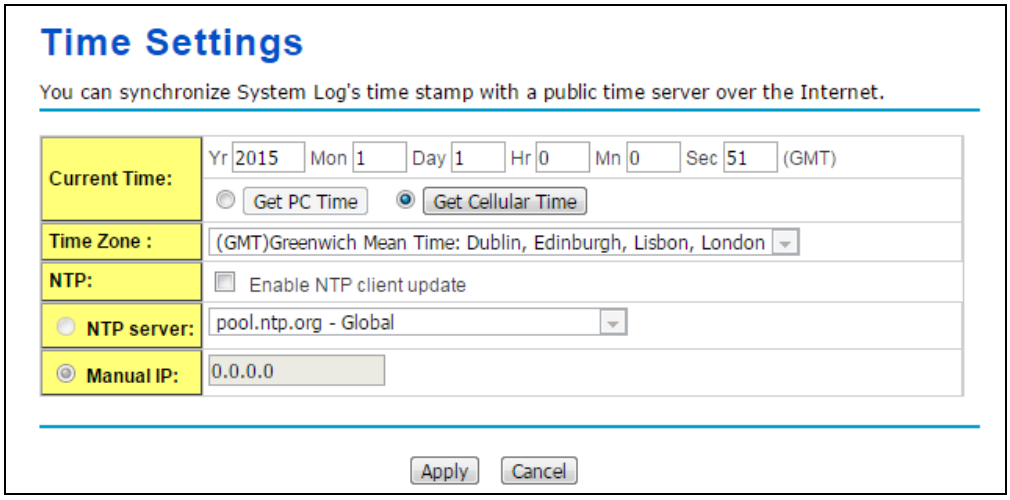
Shared Secret: This secret, which is composed of no more than 31 characters, is shared by the device and RADIUS server during authentication.

Global-Key Update: Check this option and specify the time interval between two global-key updates.

Key renewal: Set the time interval between two authentications. For the User Security, please go to Wireless Security Setting page (Refer to the 4.3.2)

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 your PC or Cellular ISP.

Get PC time: The current time will be updated according to your PC's time.

Get Cellular Time: The item appears when the system already connected to ISP (Internet Service Provider) through cellular interface, the current time will be updated according to ISP. Default setting is enabled when meet the condition.

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

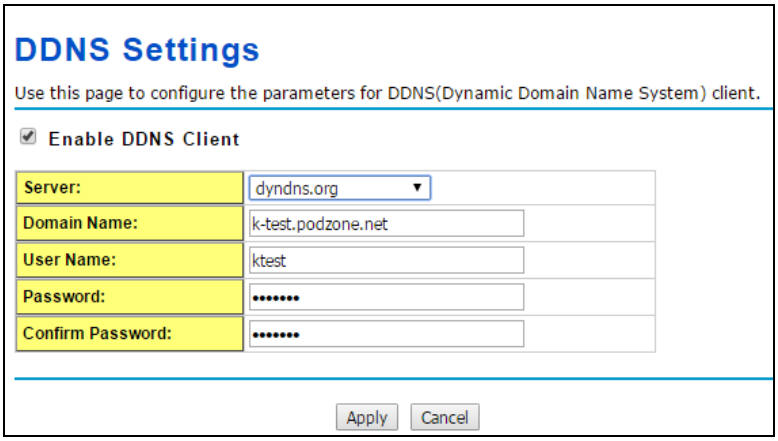
NTP: You can select **"Enable NTP client update"** in this page, then the NTP feature will be activated and synchronize from the remote time server.

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 Dynamic DNS

Use this page to configure the Dynamic DNS.



DDNS: Check the "Enable DDNS Client" box to active this feature.

Server: Choose your DDNS provider, Dyndns, NO-IP, or Freedns from drop down menu.

Domain Name: Enter the Name that you registered with your DDNS service provider.

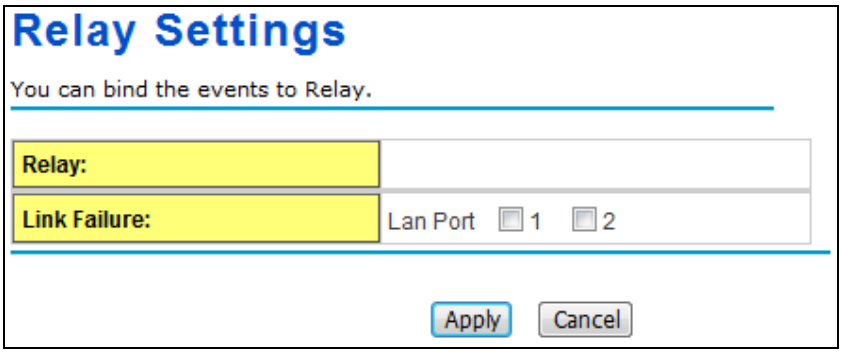
Username: Enter the Username for your DDNS account.

Password: Enter the Password for your DDNS account.

4.2.6 Relay Settings

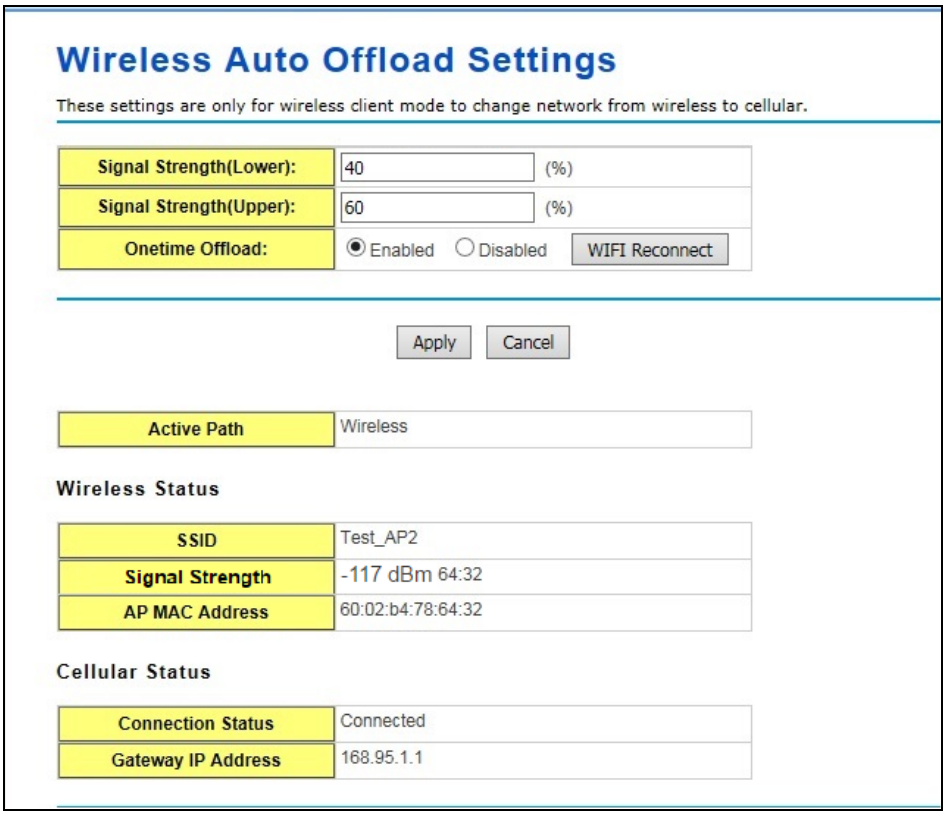
Use this page to configure the Link Failure Relay.

Select LAN Port 1 or Port 2 or both of link failure and press "**Apply**" to activate the settings.



4.2.7 Wireless Auto Offload Settings

This page helps you to enable Wireless Auto Offload. In addition to 3G/LTE, JetWave 2311 supports 802.11n WIFI Client mode. The loading of data traffic can be shared by 3G/LTE and WIFI to reduce the cellular cost. When the WIFI signal is poor or not available, the system automatically forwards traffic to the 3G/LTE interface.



Auto Offload function can only active when meet both conditions as below:

(1) Wireless (WIFI) Interface is configured as "Client" mode and is connected to the AP.

(2) Cellular Interface is already connected to Carrier Provider.

Signal Strength(Lower): When signal strength of WIFI connection lower than the ratio(ex. 40%), the outgoing traffic will be directed to cellular interface.

Signal Strength(Upper): When signal strength of WIFI connection is greater than the ratio (ex. 60%), the outgoing traffic will be directed to WIFI.

The difference between the Lower and Upper signal strength is a value similar to the delay time. While the active path is changed from WIFI to cellular interface, the active path will be changed only while the signal strength of WIFI is better than the value.

Onetime Offload: When enable **Onetime Offload**, it means the Auto Offload mechanism will be directed to cellular one time, it will not go back to WIFI automatically, unless press the "WIFI

Reconnect" button. *The "WIFI Reconnect" button only appear when enable* ***Onetime Offload****.*

Following are the status of the active path and the information of the Wireless and Cellular interface. These information helps you check whether the connected status easier.

Press **"Apply"** to activate the new settings. After applied, if the current WIFI signal is better than the lower Signal Strength, the WIFI connection will be the active path first.

Information:

Below figure displays the current status.

Active Path shows the current active path is **Wireless** or **Cellular**.

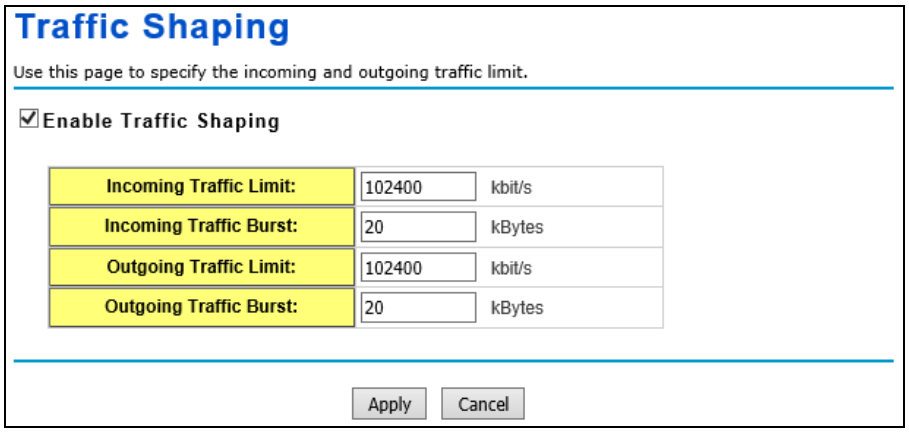
Wireless Status shows the SSID, MAC address of the connected AP, and IP address of gateway.

Cellular Status shows the connection status and IP address of gateway**.**

4.2.8 Traffic shaping

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

Enable Traffic Shaping: Select the "**Enable Traffic Shaping**" 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.



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

4.2.9 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 Select/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.

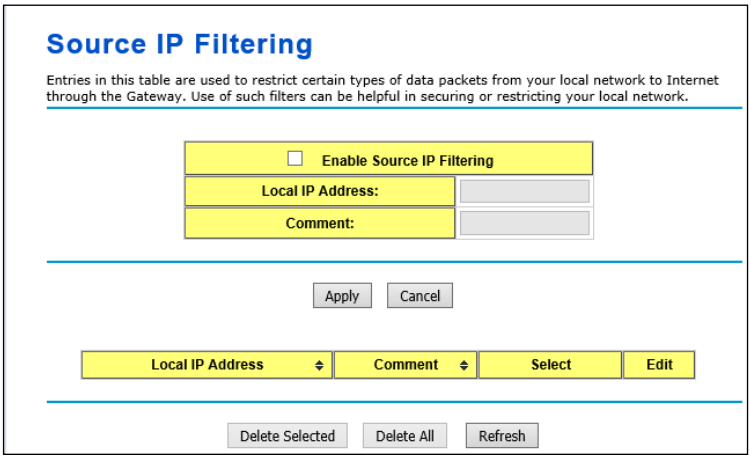
"**Src Port Filtering**": Source Ports Filtering from the LAN to Internet through the gateway.

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

- **Source IP Filtering**

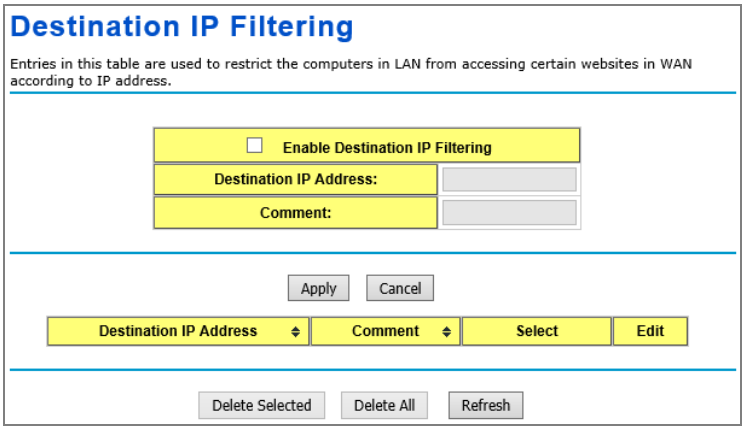
  Entries in this table are used to restrict certain types of data packets from your local network to internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

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



  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.

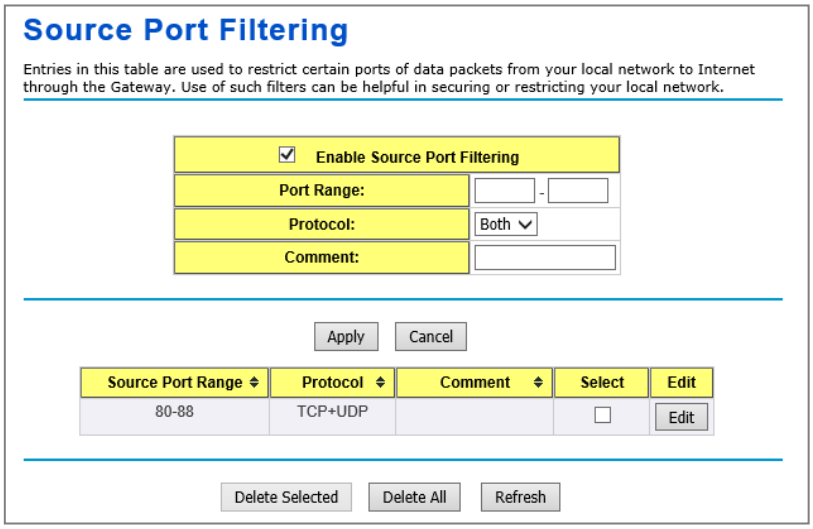
Select "**Enable Destination IP Filtering**", type the "**Destination IP Address**" and "**Comment**" (note for the entry) and then press "**Apply**" to activate the settings.

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**

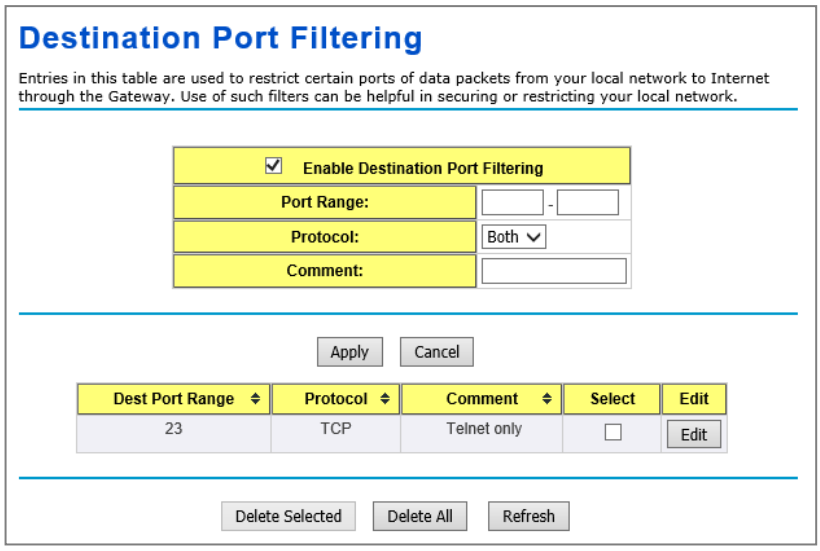
Entries in this table are used to restrict certain ports of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

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.



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.



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.

4.2.10 Inbound Firewall

"Inbound Filtering": Inbound Filtering is used to restrict any access from Internet to the LAN. Only the applied entries in **Exception** list can access the LAN from Internet through the gateway.

Enable Inbound Firewall: After enabled inbound firewall, it means that all the IP address from the Internet can NOT access the LAN through the gateway.

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

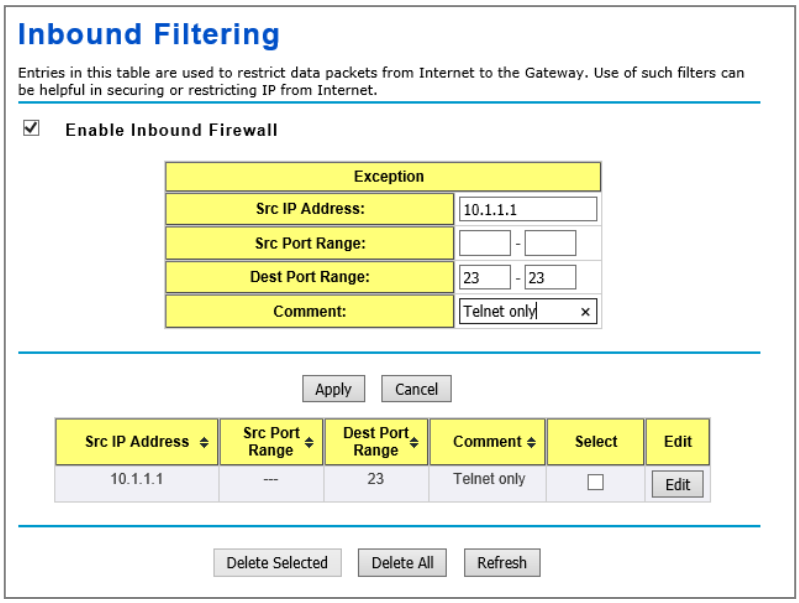
Src IP Address: The entry allows you to configure the source IP address from Internet.

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.

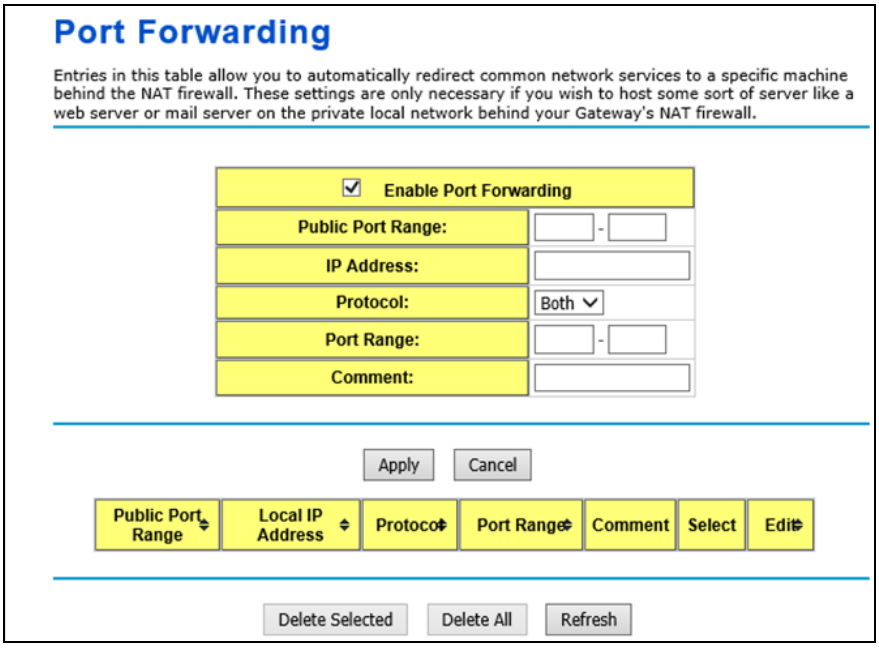
4.2.11 NAT Settings

NAT is the short 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**” and “**DMZ**”.

- **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.



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.

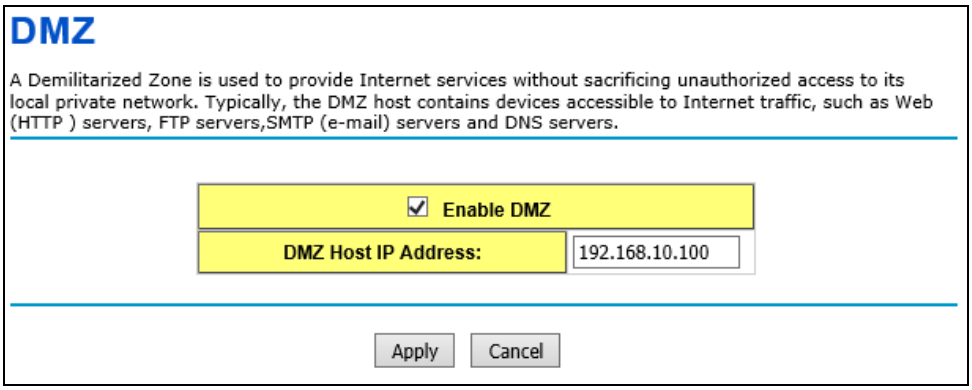
Comment: Add information of the entry.

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.



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.

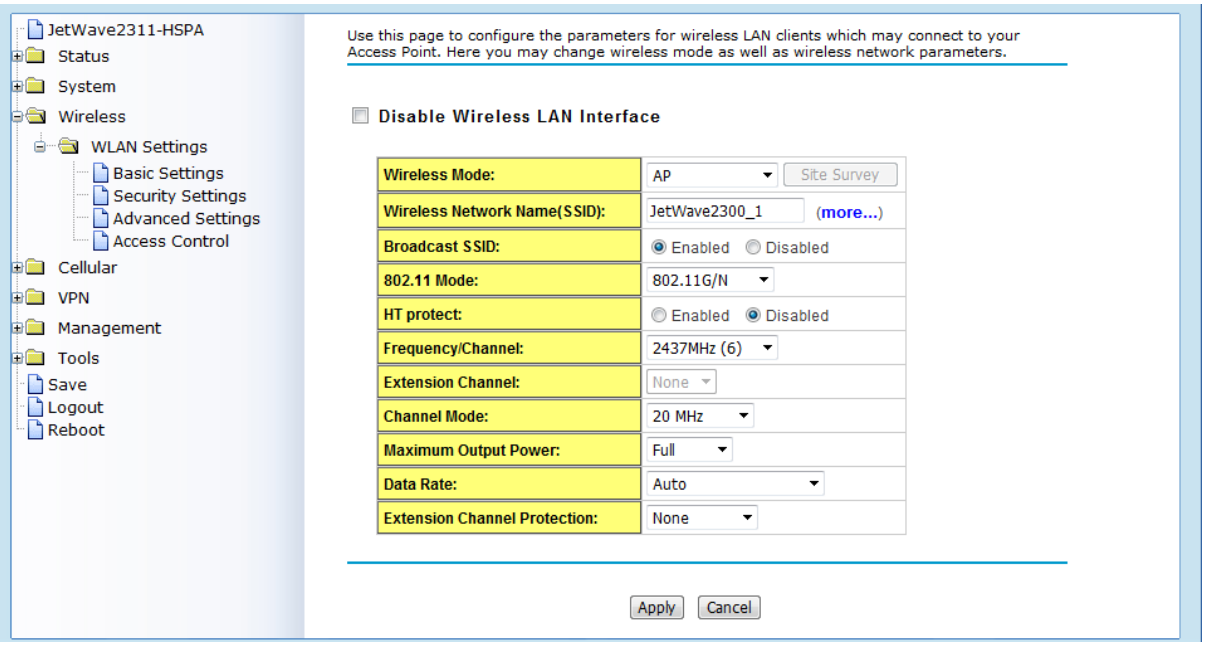
4.3 Wireless (for JetWave 2311 Series only)

The "**Wireless**" feature set pages allow users to configure the Wireless LAN configuration. The Wireless means the WIFI radio of the device.

JetWave 2311 support one WIFI and one 3G/LTE radio, you must configure WIFI features here and go to 3G/4G LTE page to configure other settings.

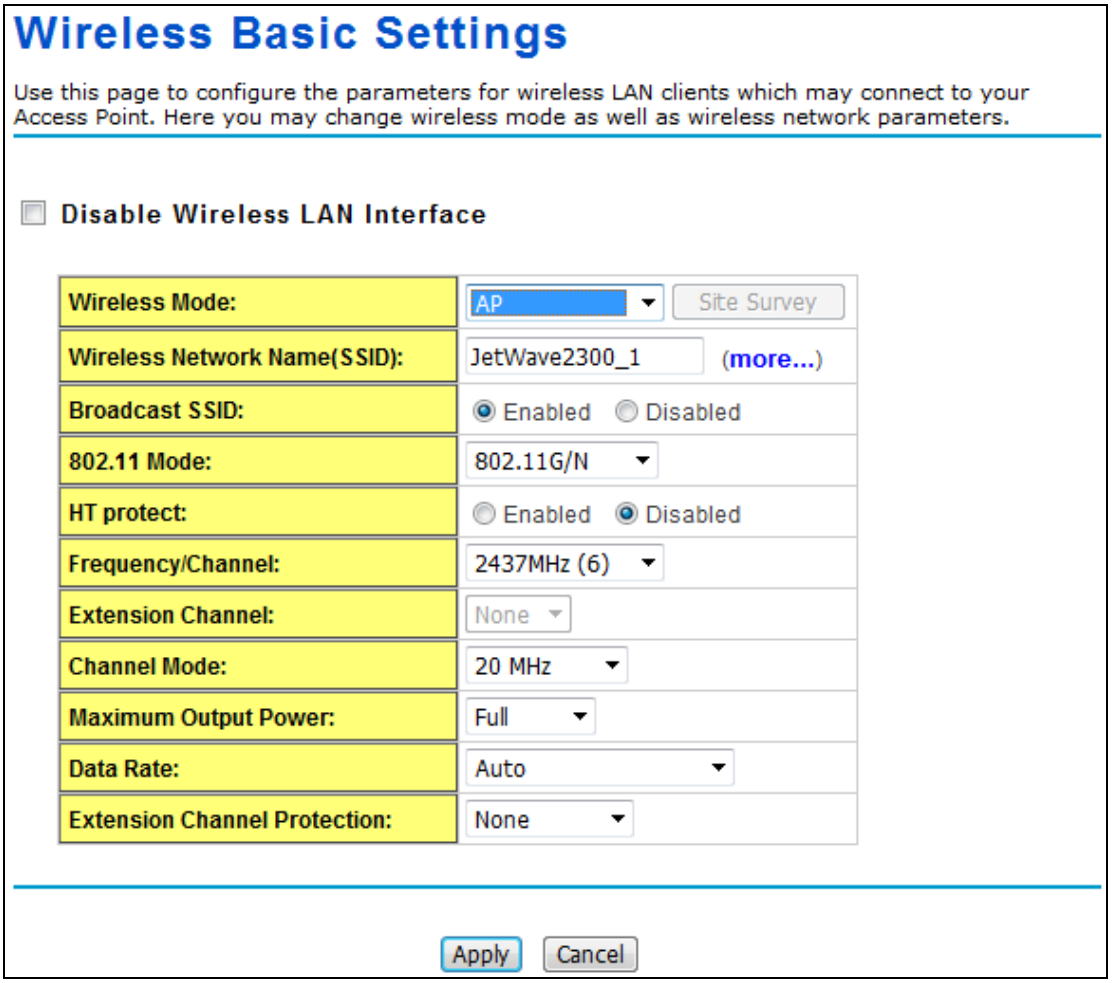
There are several settings such as the **Basic Settings**, **Security Setting**, **Advanced Setting and Access Control** can be configured in the Wireless Configuration.

The figure below shows the Web GUI of the JetWave 2311. The Wireless and 3G settings are separated to different feature set.



4.3.1 Wireless Basic Setting

Use this page to configure the parameters for Wireless LAN Interface of the device. Here you may change wireless interface modes and related parameters.



Disable Wireless LAN Interface: Check this option to disable WLAN interface, then the wireless module of the AP will stop working and no wireless device can connect to it.

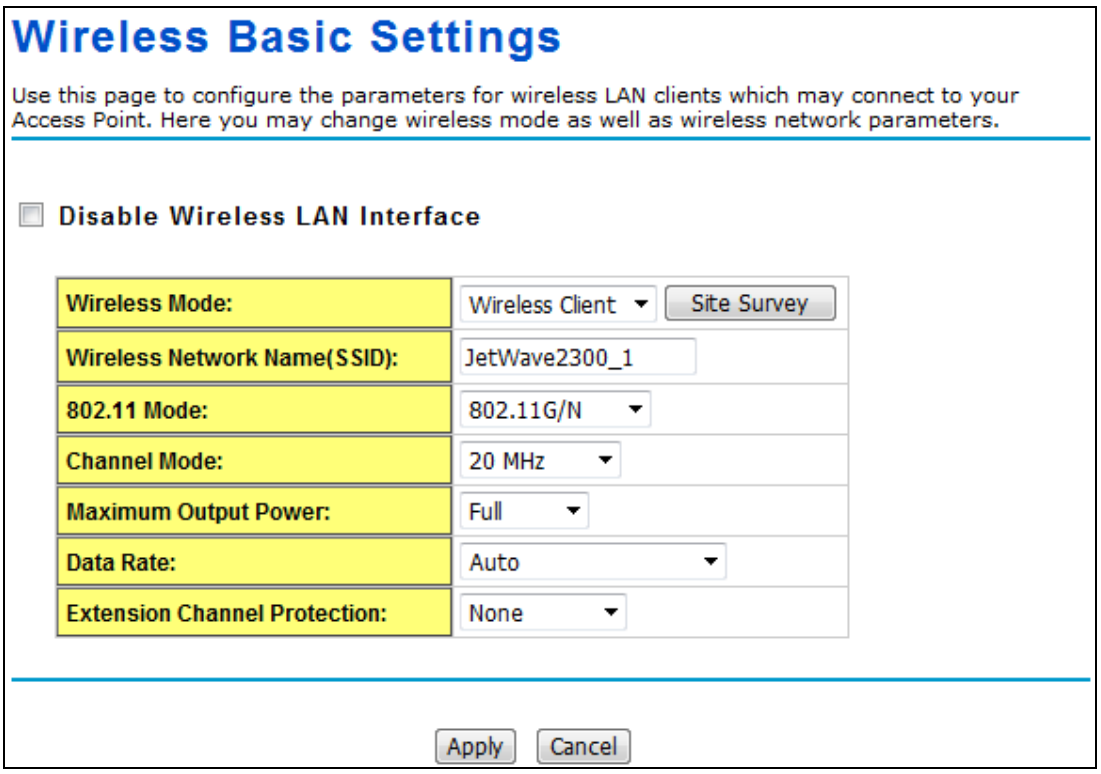
Wireless Mode: The below operating modes are available on this AP/Gateway.

AP: The AP works as the Access Point mode, it establishes a wireless coverage and receives connectivity from other wireless clients devices, the clients can search and connect to it.

In Wireless AP mode, you can configure the Wireless Network Name (SSID), Enable/Disable Broadcast SSID, select the 802.11 mode, HT Protect Enabled/Disabled, Frequency/Channel, Maximum Output Power (per chain), Data Rate and Extension Channel Protection. While the Wireless Client connect to the AP, the client must follow AP settings for communicating.

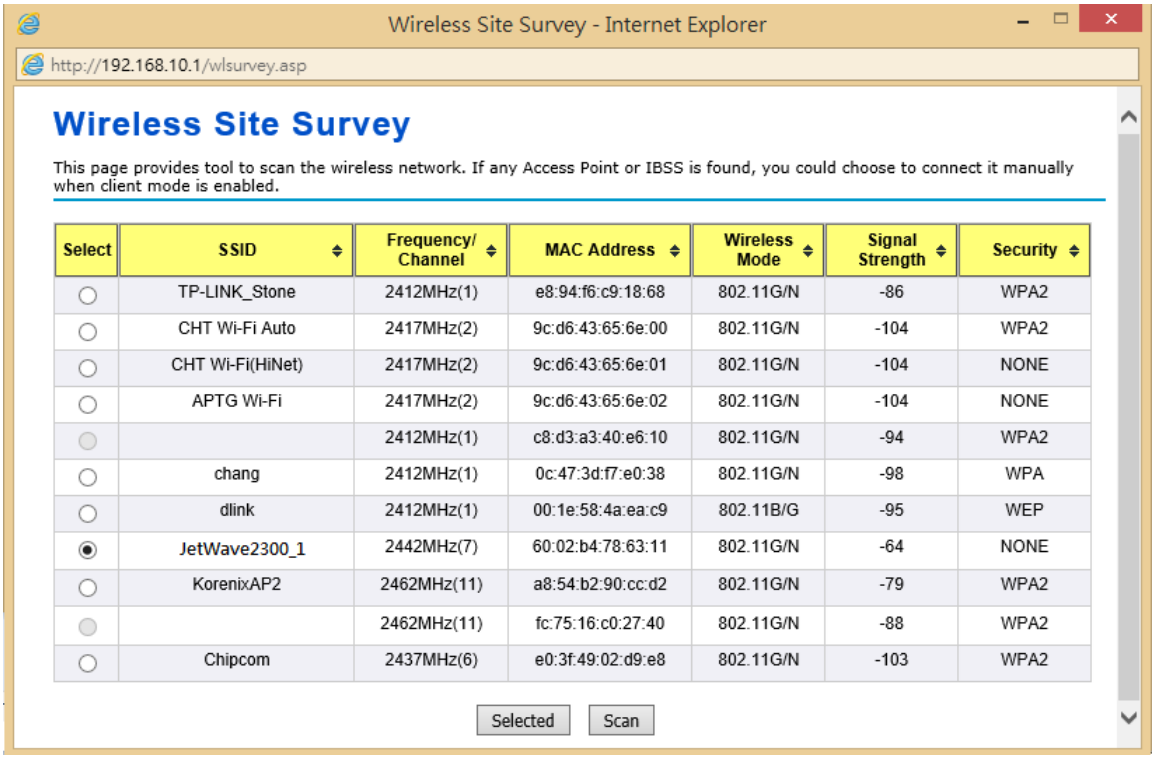
Wireless Client: The AP/Gateway is able to connect to the AP and thus join the wireless network around it. In Wireless Client mode, you can click "**Site Survey**" to find the best signal connected AP per your need. Or you can manually type the SSID you want to connect.

While in wireless client, please **note** that all the rest of Wireless Client settings must be the same as your AP settings.



Select **Site Survey** to select the target AP.

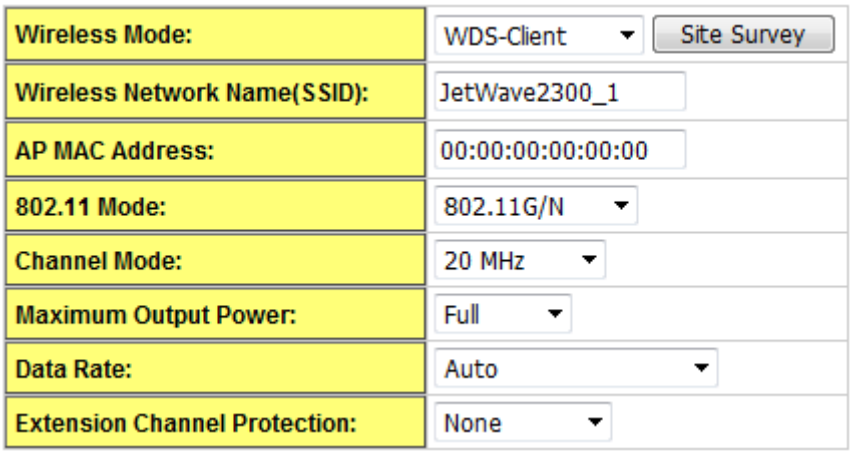
In below figure, you can find the **SSID: JetWave2300_1** is selected. Press "**Selected**" to activate the new setting, this Site Survey popup screen will then disappear. And the SSID in Wireless Basic Setting will be updated.



WDS-AP: WDS mode is usually implemented in Point to Point (P2P) connection. When

configuring P2P, one end should be WDS-AP and the other end should be WDS-Client. WDS-AP can also provide network access to general clients to act as an AP repeater.

WDS-Client: Select the WDS-Client mode. In WDS-Client mode, you must type the target WDS-AP's SSID and MAC address. With the setting, the traffic from the WDS-Client can Only transmit to the WDS-AP. Please note that the rest of other wireless/security settings must the same as the WDS-AP as well.



Wireless Network Name (SSID): This wireless network name is shared among all associated devices in your wireless network. Keep it identical on all those devices. Note that the SSID is case-sensitive and can not exceed 32 characters.

Broadcast SSID: Under AP mode, hiding network name is necessary when you are in a wireless environment that may have potential risk. By disabling broadcast SSID, the clients can not scan and find the AP/Gateway, so that malicious attack by some illegal clients could be avoided.

802.11 Mode: The AP/Gateway can communicate with wireless devices of 802.11n/g. You can also select **"802.11G Only"** or **"802.11 G/N"** and make it work under an appropriate wireless mode automatically. Different band has different settings as below.

Wireless Mode:	AP Site Survey
Wireless Network Name(SSID):	wds3200 (more...)
Broadcast SSID:	Enabled Disabled
802.11 Mode:	802.11G Only
Frequency/Channel:	2437MHz (6)
Maximum Output Power (per chain):	20 dBm
Data Rate:	Auto

Wireless Mode:	AP Site Survey
Wireless Network Name(SSID):	wds3200 (more...)
Broadcast SSID:	Enabled Disabled
802.11 Mode:	802.11G/N
HT protect:	Enabled Disabled
Frequency/Channel:	2437MHz (6)
Extension Channel:	None
Channel Mode:	20 MHz
Maximum Output Power (per chain):	20 dBm
Data Rate:	Auto
Extension Channel Protection:	None

HT Protect: Enable HT (High Throughput) protect to ensure HT transmission with MAC mechanism. Under 802.11n mode, wireless client can be divided into HT STA and Non-HT STA, among which the one with HT protect enabled gets higher throughput.

Frequency/Channel: Channel varies much as the available band differs from country to country. Select a proper operating channel in the drop-down list according to your situation.

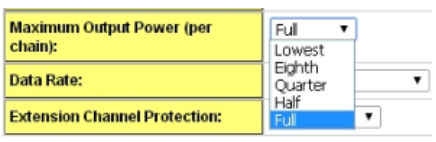
The 802.11G and 802.11G/N are 2.4G band which supports 12~13 channels.

802.11G/N

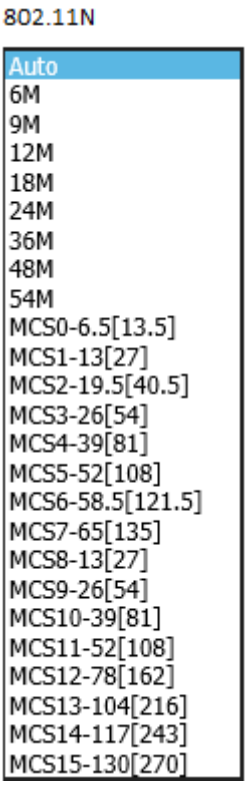
Auto
2412MHz (1)
2417MHz (2)
2422MHz (3)
2427MHz (4)
2432MHz (5)
2437MHz (6)
2442MHz (7)
2447MHz (8)
2452MHz (9)
2457MHz (10)
2462MHz (11)

Maximum Output Power (per chain): Specify the signal transmission power. The higher the output power is, the wider the signal can cover, but the power consumption will be greater accordingly. Usually "**Full**" with proper antenna is preferred.

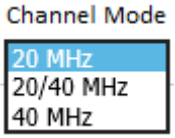
Half: 1/2 of Full (Full -3dBm), **Quarter:** 1/4 of Full (Full -6dBm), **Eighth**: 1/8 of Full (Full –9dBm).



Date Rate: Usually "**Auto**" is preferred. Under this rate, the AP/Gateway will automatically select the highest available rate to transmit. In some cases, however, like where there is no great demand for speed, you can have a relatively-low transmit rate for compromise of a long distance.



Channel Mode: Two levels are available: 20MHz and 20/40MHz. The latter one can enhance the data rate more effectively, but takes more bandwidth, thus cause potential interference.

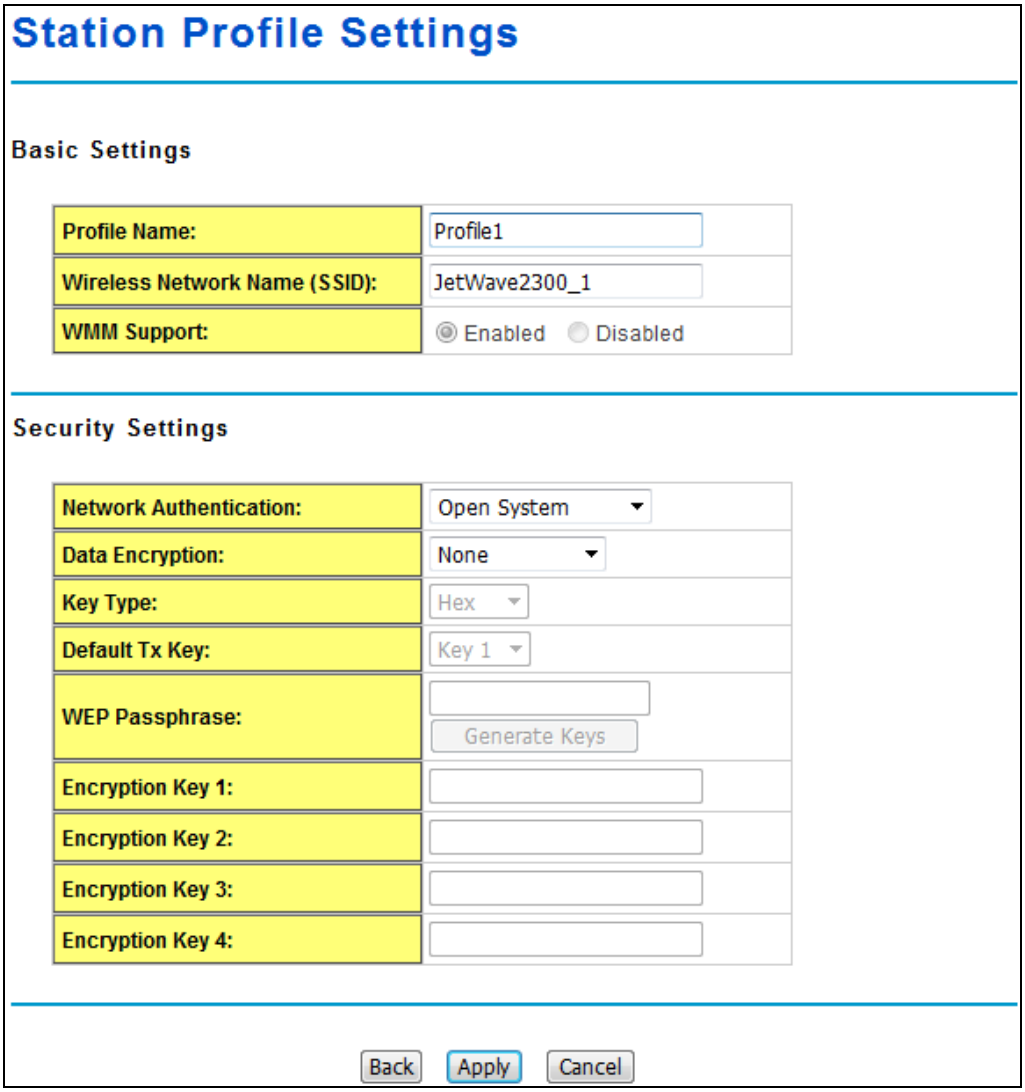


Extension Channel Protection: This is to avoid conflict with other wireless network and boost the ability of your device to catch all 802.11g transmissions. However, it may decrease wireless network performance. Compared to CTS-Self; the transmission amount of CTS-RTS is much lower.

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

4.3.2 Wireless Security Setting

The page allows you configure the Security Settings.



Basic Setting

Profile Name: The profile name of the settings.

Wireless Network Name(SSID): This is the same SSID of the AP/Gateway.

WMM Support: WMM (Wi-Fi Multimedia) is a subset of 802.11e. It allows wireless communication to define a priority limit on the basis of data type, thus those time-sensitive data, like video/audio data, may own a higher priority than common one.

In AP mode, you will have more settings as below.

Broadcast SSID: Normally, the SSID is broadcast and all the clients can search the SSID. For security concern, you can disable the Broadcast SSID function, then the clients can't search it and the client must type the correct AP's SSID to connect the AP. This is a simple security setting.

Wireless Separation: Wireless separation is an ideal way to enhance the security of network transmission. Under the AP mode, enable **"**Wireless Separation**"** can prevent the communication among associated wireless clients.

Security Setting

Network Authentication

Open System: It allows any device to join the network without performing any security check.

Shared Key: Data encryption and key are required for wireless authentication.

WPA with RADIUS: With warrant (username, password and etc.) offered by user, this kind of authentication can be realized with specific RADIUS server. This is the common way to be adopted in large enterprise network.

WPA2 with RADIUS: As a new version of WPA, only all the clients support WPA2, can it be available. If it is selected, AES encryption and RADIUS server is required.

WPA and WPA2 with RADIUS: If it is selected, AES & TKIP encryption and RADIUS server is required.

WPA-PSK: It is a simplified WPA mode with no need for specific authentication server. In this so-called WPA Pre-Shared Key, all you have to do is just pre-enter a key in each WLAN node and this is the common way to be adopted in large and middle enterprise as well as residential network.

WPA2-PSK: As a new version of WPA, only all the clients support WPA2, can it be available. If it is selected, the data encryption can only be AES and the passphrase is required.

WPA-PSK&WPA2-PSK: If it is selected, the data encryption will be AES & TKIP and the passphrase is required.

Data Encryption

If data encryption is enabled, the key is required and only sharing the same key with other wireless devices can the communication be established.

None: Available only when the authentication type is open system.

64 bits WEP: It is made up of 10 hexadecimal numbers.

128 bits WEP: It is made up of 26 hexadecimal numbers.

152 bits WEP: It is made up of 32 hexadecimal numbers. This is applied in Shared Key mode.

TKIP: Temporal Key Integrity Protocol, which is a kind of dynamic encryption, is co-used with

WPA-PSK.

AES: Advanced Encryption Standard, it is usually co-used with WPA2-PSK.

Eap Type: for WPA/WPA2 with Radius. The system supports **TTLS, LEAP, TLS, PEAP** and **MSCHAPv2, GTC** Eap types. Select the Eap type and type the **User Name**, **Password** for the WAP/WPA2 with Radius.

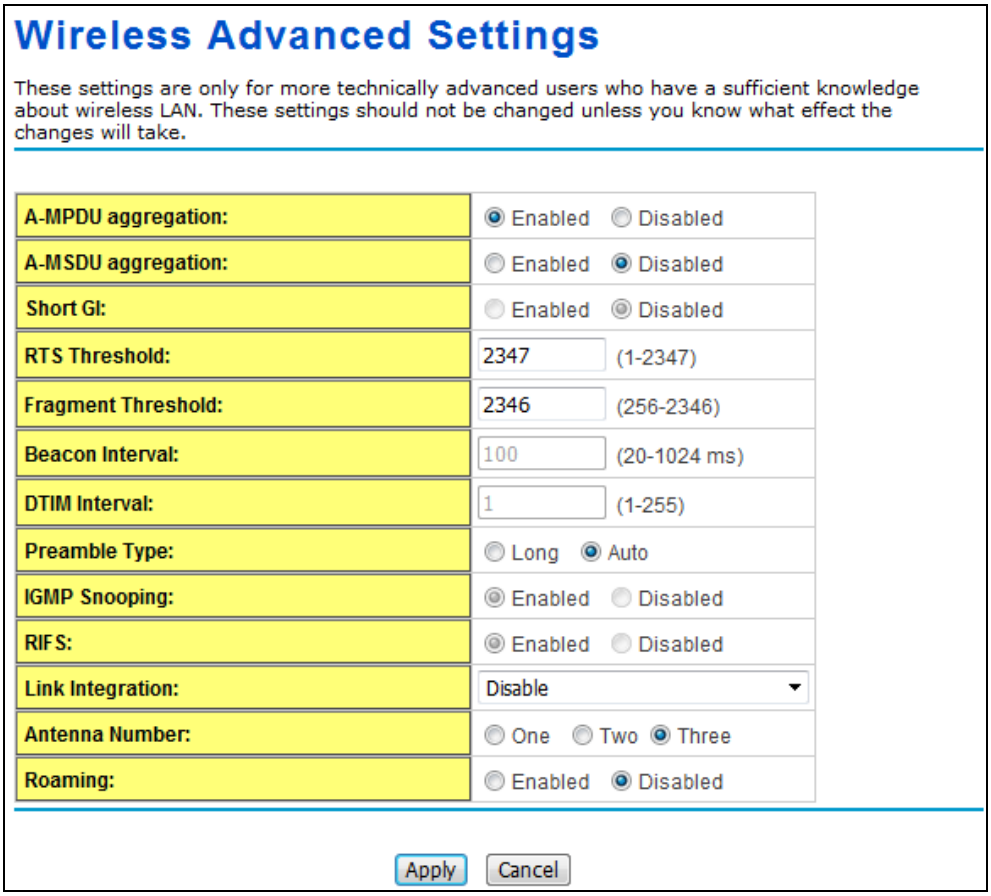
Press **"Apply"** to activate the setting.

Note:

- We strongly recommend you enable wireless security on your network!
- Only setting the same Authentication, Data Encryption and Key in the JetWave and other associated wireless devices, can the communication be established!

4.3.3 Wireless Advanced Setting

The page allows you to configure advanced wireless setting. These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. Some of these settings should not be changed unless you know what effect the changes will take. And some of the modification on them may negatively impact the performance of your wireless network.



A-MPDU/A-MSDU Aggregation: Under AP mode, the data rate of your AP could be enhanced greatly with this option enabled; however, if your wireless clients don't support A-MPDU/A-MSDU aggregation, it is recommended not to enable it.

Short GI: Under 802.11n mode, enable it (Short Guard Interval) to obtain better data rate if there is no negative compatibility issue.

RTS Threshold: The AP/Gateway sends RTS (Request to Send) frames to certain receiving station and negotiates the sending of a data frame. After receiving an RTS, that STA responds with a CTS (Clear to Send) frame to acknowledge the right to start transmission. The setting range is 0 to 2347 in byte.

Fragmentation Threshold: Specify the maximum size in byte for a packet before data is fragmented into multiple packets. Setting it too low may result in poor network performance. Leave it at its default of 2346 is recommended.

Beacon Interval: Specify the frequency interval to broadcast packets. Enter a value between 20 and 1024. The default value is 100ms.

DTIM Interval: DTIM, which stands for Delivery Traffic Indication Message, is contained in the data packets. It is for enhancing the wireless transmission efficiency. The default is set to 1. Enter

a value between 1 and 255.

Preamble Type: It defines some details on the 802.11 physical layer. "**Long**" and "**Short**" are available.

IGMP Snooping: IGMP snooping is the process of listening to IGMP network traffic. By enabling IGMP snooping, the AP will listen to IGMP membership reports, queries and leave messages to identify the ports that are members of multicast groups. Multicast traffic will only be forwarded to ports identified as members of the specific multicast group or groups.

RIFS: RIFS (Reduced Interframe Spacing) is a means of reducing overhead and thereby increasing network efficiency.

Link Integration: This is also known as **Link Fault Pass-Through**. This feature allows you to bind the Ethernet port 1 (Eth1) and Wireless LAN interface together. Once one of them fails, the other interface becomes down as well.

Disable: Disable the Link Integration.

LAN links WLAN: Single direction only while the LAN Ethernet port failure, the binding WLAN radio will be shut down.

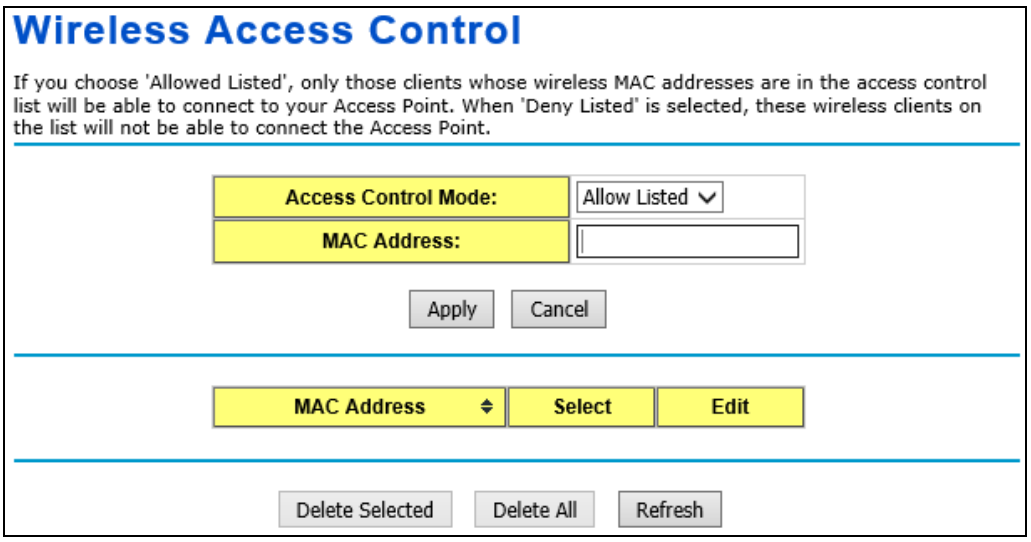
WLAN links LAN: Single direction only while the WLAN failure, the binding Ethernet port will become link down.

WLAN and LAN link each other: This is Bi-directional integration no matter while LAN Ethernet port failure or WLAN radio failure.

Antenna Number: The setting allows you configure One for 1T1R SISO, Two for 2T2R MIMO or Three for 3T3R MIMO. While you change the antenna number, please connect the antenna to the correct antenna sockets of the WIFI radio. Please refer to the 2.4.1 Antenna Placement table.

4.3.4 Wireless Access Control

This page allows you configure the **Wireless Access Control** list. You can configure **Allow** list or **Deny** list for your wireless network on the AP/Gateway.



Access Control Mode: Allow Listed or Deny Listed.

MAC Address: Type the MAC address of the client which you want to Allow or Deny.

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

The lower screen shows the Wireless Access Control list you configured. Press "**Delete Selected**" or '**Delete All**" to delete part of or all of the entries.

Press **"Refresh"** to refresh the table.

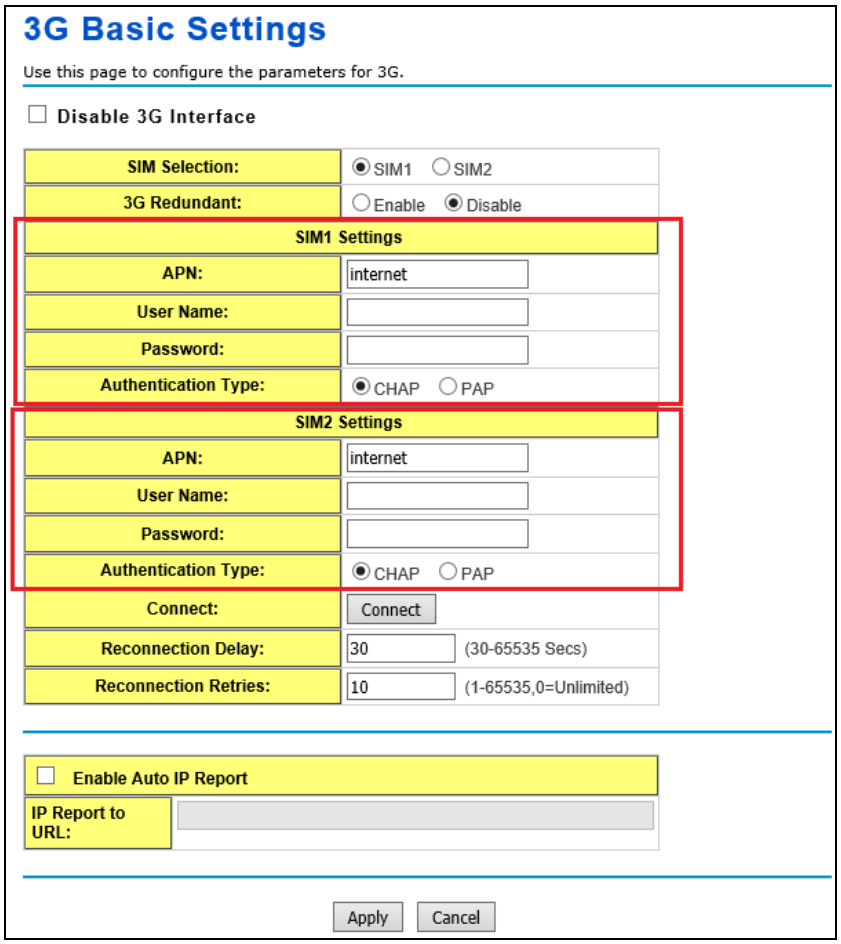
4.4 Cellular

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.

4.4.1 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 3G SIM settings, normally, you can connect the 3G Gateway to the ISP cellular network without configuring 3G setting. However, in some countries, before the 3G 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.



Disable 3G Interface: You can disable the 3G 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.

3G Redundant: While you enable 3G 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 3G 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.

3G Redundant Timer = Reconnection Delay x Reconnection Retries + Reset Module Time

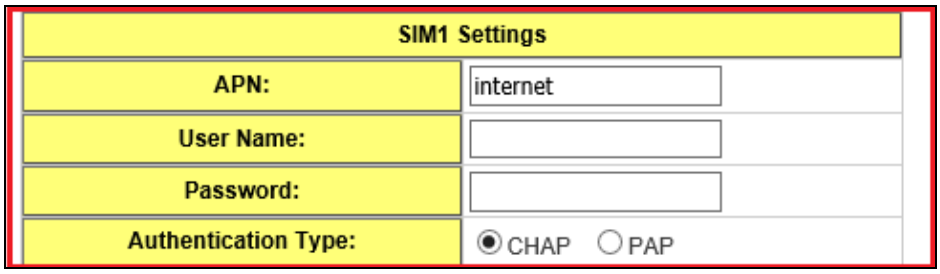
For example, while the SIM 1 connection is failure for (30 seconds x 10 times + 30 seconds), the SIM 2 will become primary SIM after **330** seconds. The system may take additional 30 seconds to exchange the SIM from SIM 1 to SIM 2.

Note: The 3G Redundant is only available while you insert two SIM cards into the socket. If you only insert one, the 3G Redundant will not work.

Note: 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.

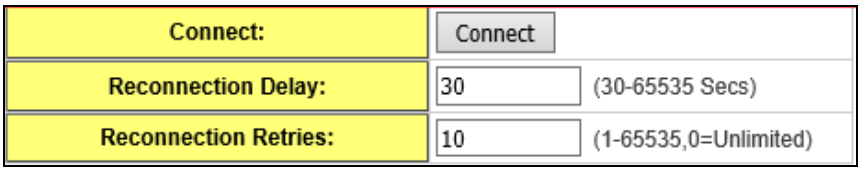


APN: Every ISP has a specific APN (Access Point Name) assigned to its cellular network. The system can read this name from the SIM card. You can also find this setting by contacting your ISP to know this. Once you failed to connect your 3G cellular network, this is the first way you can check. Please check with your ISP to know the APN and correctly input the setting through the page.

User Name: The user name for the 3G connection. Normally, this is provided by your ISP.

Password: The password for the 3G 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.



Connect: You can press "**Connect**" to re-connect the 3G connection of the selected SIM card. This progress may take 30 seconds. You will see below popup screen ask you wait 30 seconds.

Reconnection Delay: Reconnection Delay time is the delay time for each 3G Retry.

Reconnection Retries: This is the times of Reconnection Retry. While 3G is not connected, the system will retry the connection according to the Reconnection Delay time and Retry times.

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 3G 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 3G client device. The Auto IP Report in JetWave 2310 can meet your need while you need to know the IP address from the product.

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

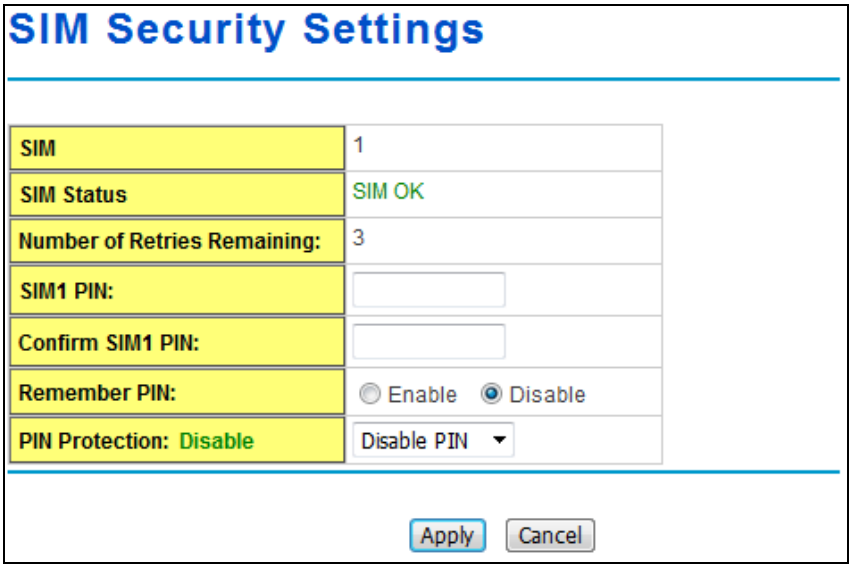
IP Report to URL: Type the correct URL here for your Gateway report to. You can build your own server, rent URL address from ISP or Google Cloud service also supports this functionality. Please check with your ISP or create through Google cloud.

Press **"Apply"** to activate the new setting.

4.4.2 SIM Security

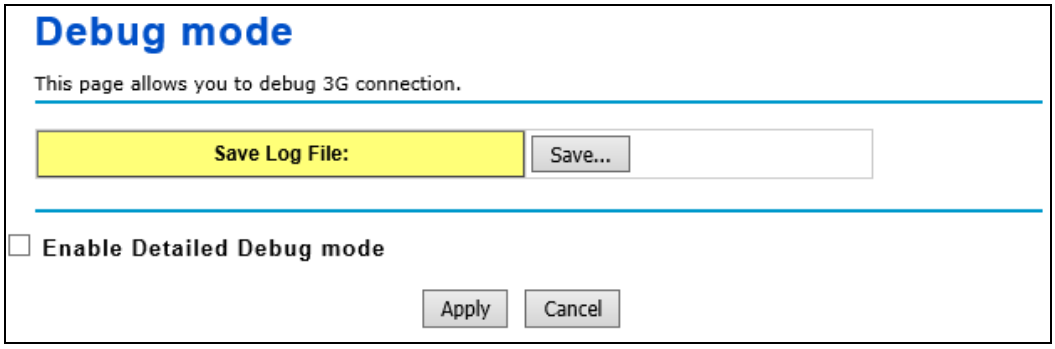
This page allows you to assign the SIM security. If you (or ISP) already apply the PIN number to your SIM card, you need to configure the correct PIN number for your AP/Gateway.

After correctly enter the PID number, you can start the 3G connection or change the new PIN settings.



4.4.3 Debug Mode

The page allows you to debug 3G connection. This is applied to JetWave 2310/2311-HSPA.



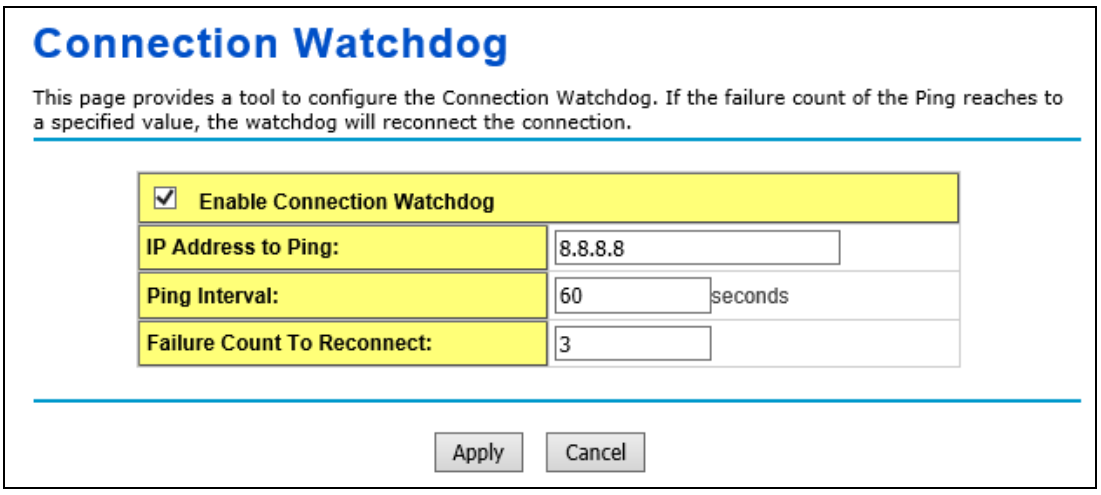
Select "**Enable Detailed Debug mode**" and press "**Apply**" to activate the debug mode.

Press "**Save…**" while the 3G connection is failure, you can know more about the 3GPP process done while 3G connection Retry.

4.4.4 Connection Watchdog

The page allows you to configure the connection watchdog.

In some country, the carrier provider may terminate your cellular connection while you don't transmit data for a period of time. This setting can help you keep the connection always alive.



Enable Connection Watchdog: Select it to enable the settings.

IP Address to Ping: Type the target IP Address. The device will ping the target by below settings.

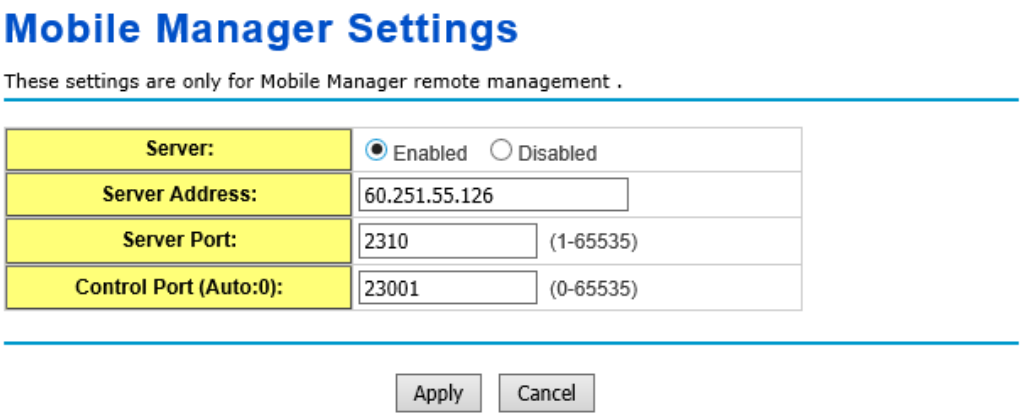
Ping Interval: The interval time of the ping.

Failure Count to Reconnect: The failure count to reconnect. If the failure count of the Ping

reaches the specified value, the watchdog will reconnect the cellular connection. It can help you keep the cellular connection always alive.

4.4.5 Mobile Manager Setting:

With Korenix 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.



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.

4.5 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 is used to sign each of the server and client certificates. Please refer to Korenix JetBox 5630 user manual for example PKI key generation.

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.

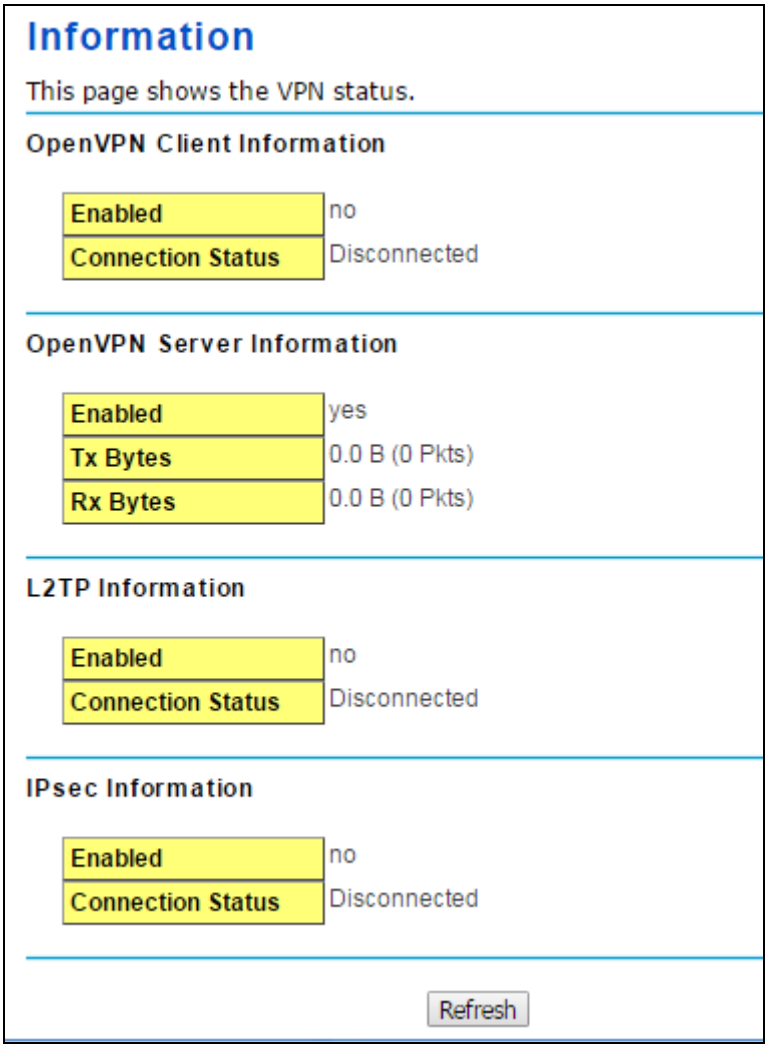
Go to **Management->Certificate File** Web configuration page to upload these keys. Import keys one by one in the page. Old certificate can also be deleted in the page.

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.

4.5.1 Status

This page shows the current VPN status. There is the status of VPN client, VPN server, L2TP, and IPsec VPN connection status.



Enabled:

yes: The VPN Client/VPN Server/L2TP/IPsec function already enabled.

No: The VPN Client/VPN Server/L2TP/IPsec function not enabled yet.

Connection Status:

Connected: The connection is already built successfully.

Disconnected: The connection is not built.

Tx / Rx Bytes:

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

4.5.2 L2TP Client

This page helps you to configure the L2TP settings. Layer2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs).

L2TP Client: Check the "Enable L2TP Client Connection" to active this feature

Server Address: Enter the L2TP Server IP address

Username: Enter the user name of L2TP client

Password: Enter the password of L2TP client

Redial: Enable/Disable the re-dial

Redial Timeout: Redial timeout

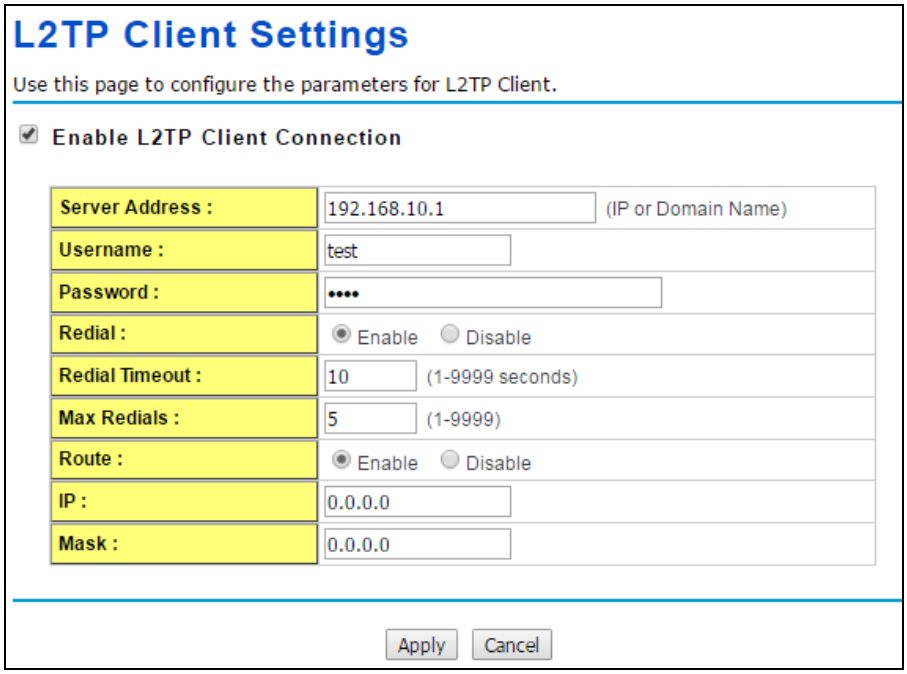
Max Redial: The maximum of Redial times

Route: Check if add remote subnet IP into static route

IP: Remote subnet IP address

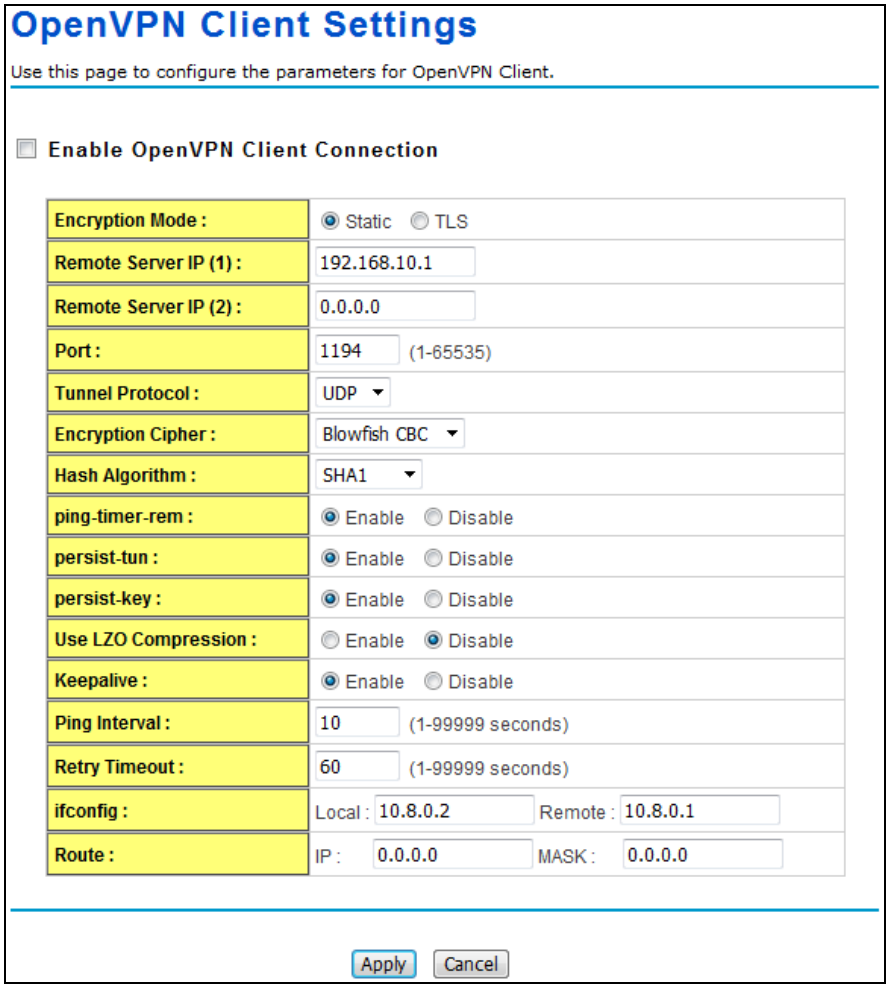
Mask: Remote subnet netmask address

Check VPN-> status Web configuration page after enabled to see the status of L2TP connection



4.5.3 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.



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.

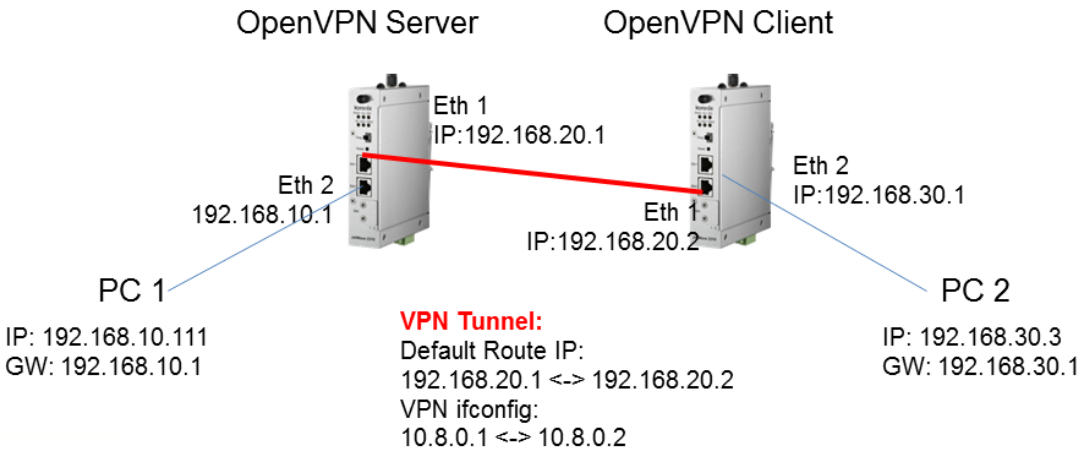
Ifconfig: Input the tunnel IP address that VPN use.

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

4.5.4 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.

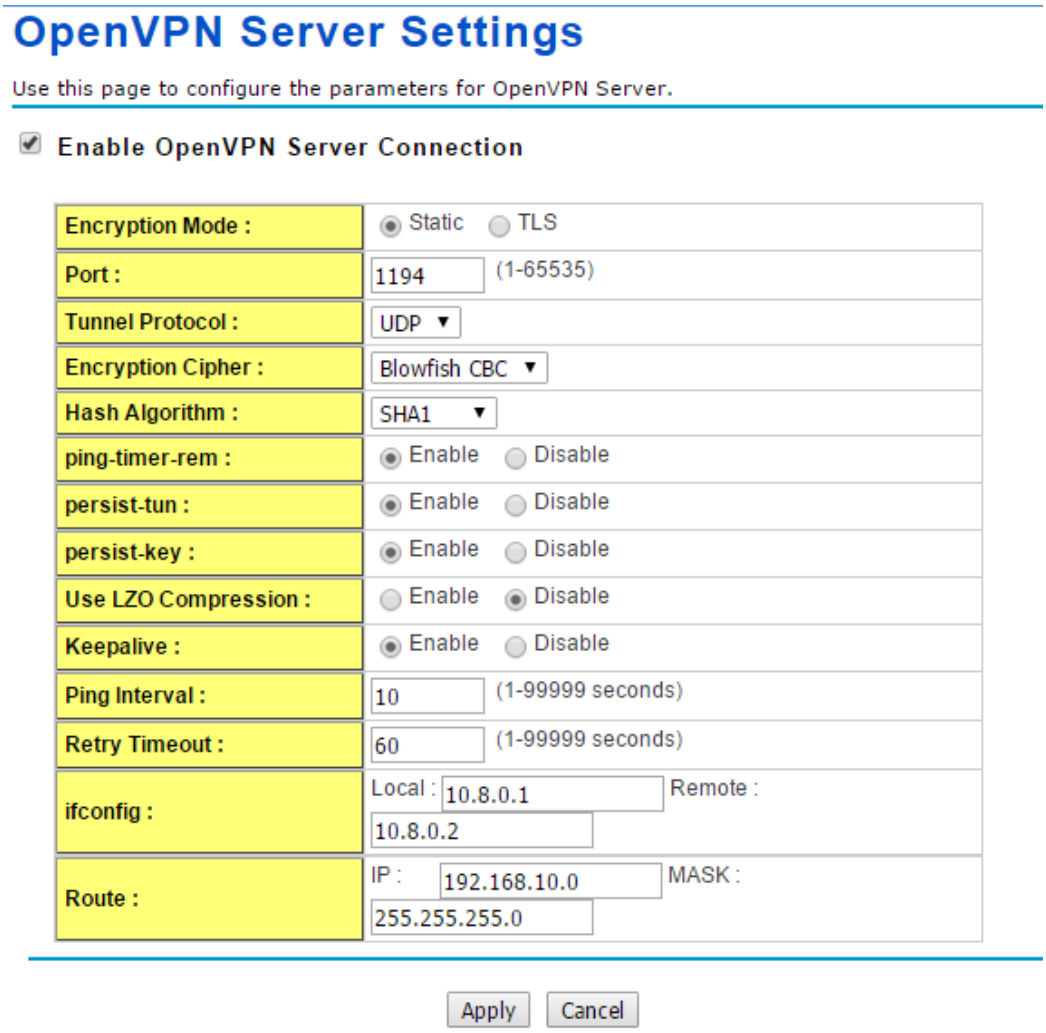
Below is the simple test setup for your reference. The red color line becomes a VPN Tunnel and the transmission data are secured. To configure the settings, you need to have IP plan of the 2 sites and the routing/VPN path first. Configure the device as Router mode and give the Ethernet ports specific IP as the default gateway for the connected devices (ex: PCs). For VPN Tunnel, you can choose Ethernet port 1 (WAN) or WIFI or 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 (ex: JetBox 5630) or 3rd party Key generation tool.



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.

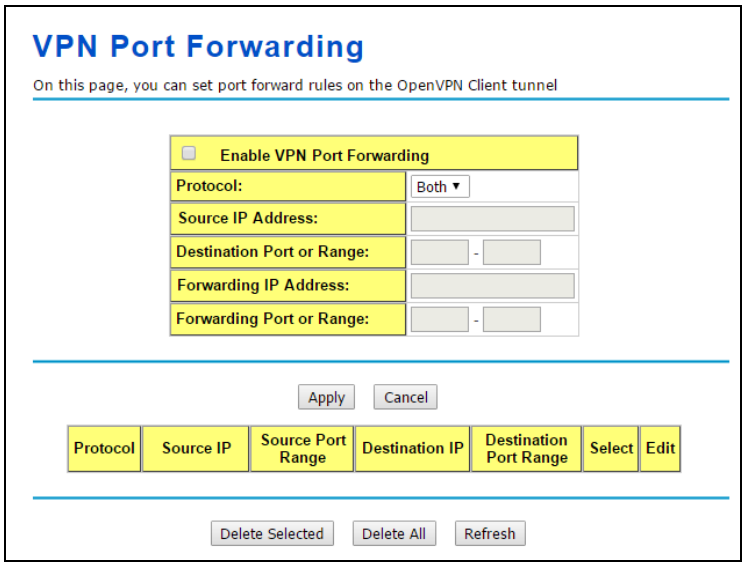
Retry Timeout: Input the retry timeout, the range can from 1~99999 seconds.

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.

4.5.5 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 JetWave 2316 that you use)

Forwarding IP Address: Type specific forwarding IP address.

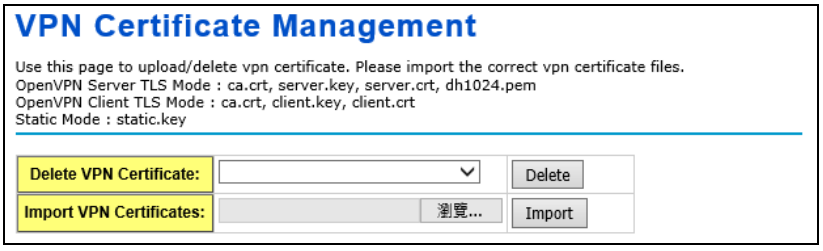
Forwarding Port or Range: Configure the port or range for forwarding device.

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.

4.5.6 VPN Certificate

This page allow user to manage the user certificate file.



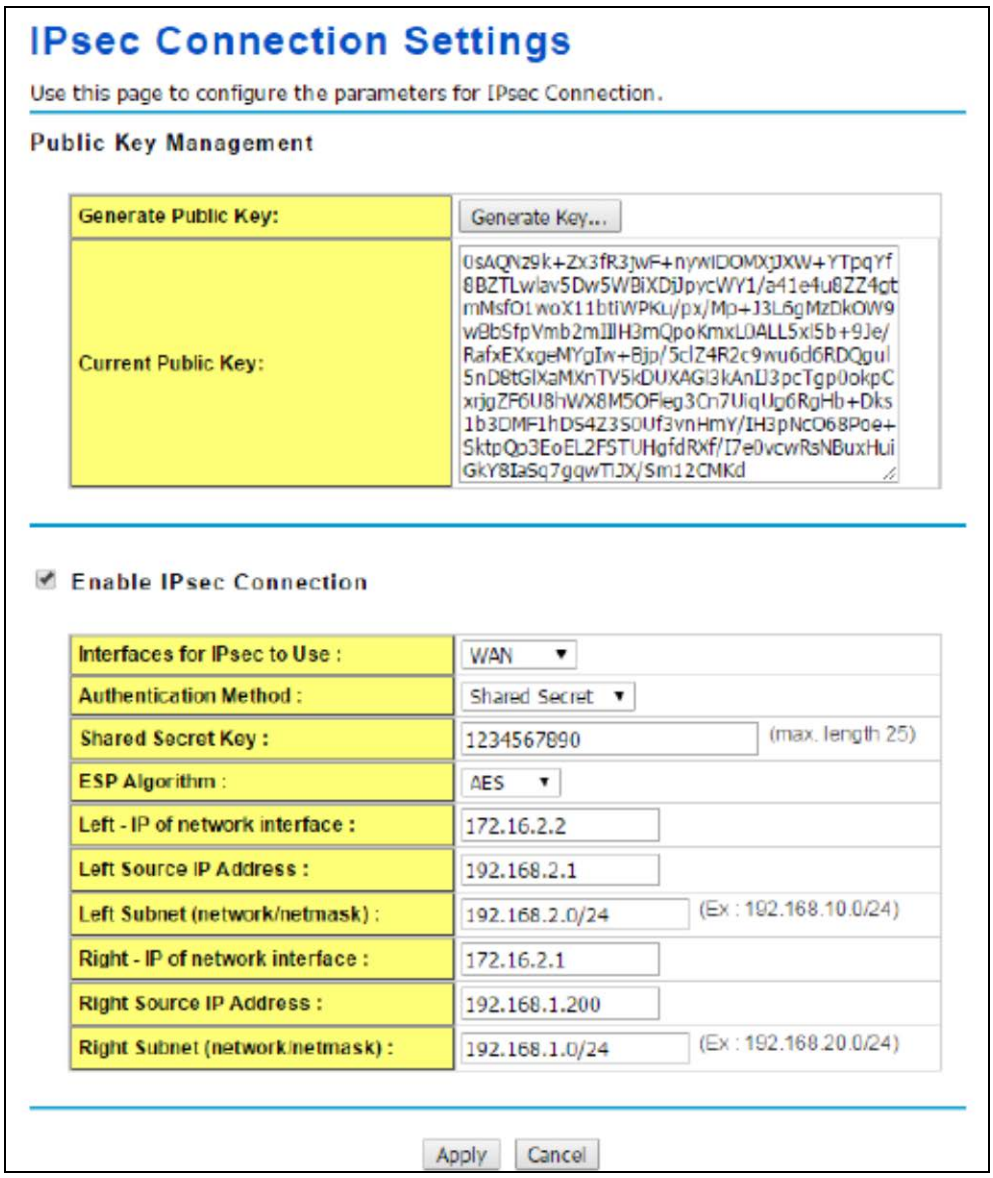
Import: Import the correct VPN Certificate.

Delete: Delete existing VPN Certificate.

4.5.7 IPsec

This page help user to setup IPsec.

IPsec: Check the “Enable IPsec Connection” to active IPsec connection.



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, shared key or RSA key..

Shared Key: Use a pre-shared static key.

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

Shared secret key: The attribute is displayed when using static key. Maximum length is 25

characters

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 in router mode or cellular IP address when using cellular network.

Left Source IP Address: 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, WAN port IP address in router mode or cellular IP address when using cellular network

Right Source IP Address: 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

Check VPN-> status Web configuration page after enabled to see the status of IPsec connection

4.6 Warning

The "**Warning**" feature pages allows user to configure Basic Setting, SMTP Configuration, and SMS Configuration.

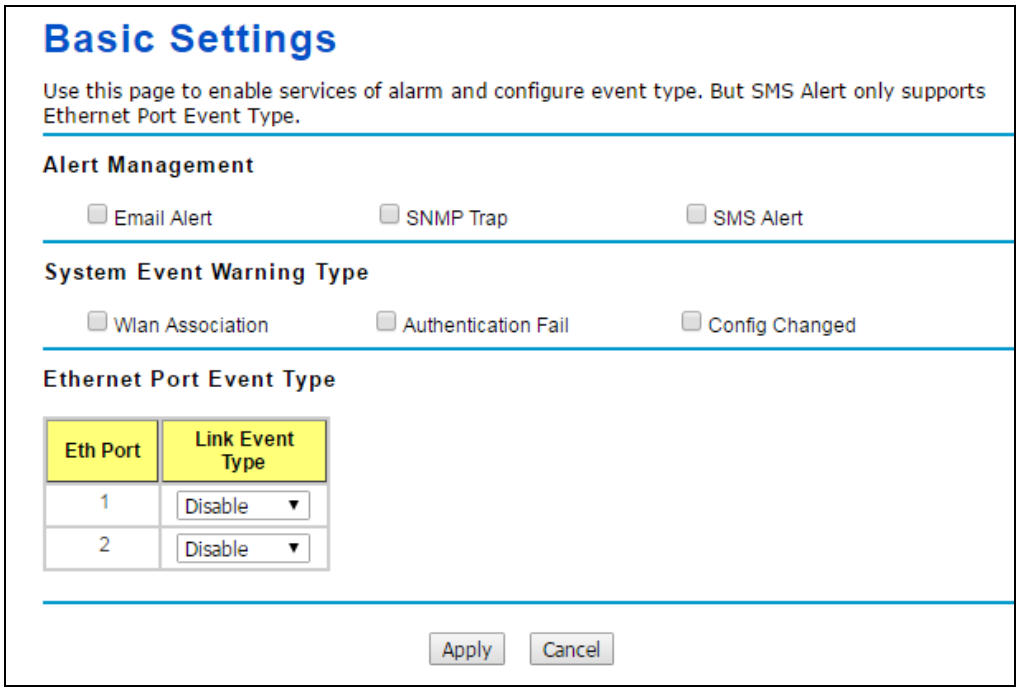
4.6.1 Basic Setting

This page allows user to manage notification message types and methods. The notification methods

include “Email Alert”, “SNMP Trap”, and “SMS Alert”, and user can decide message types (Wlan Association, Authentication, and Config changed), which needs to notification.

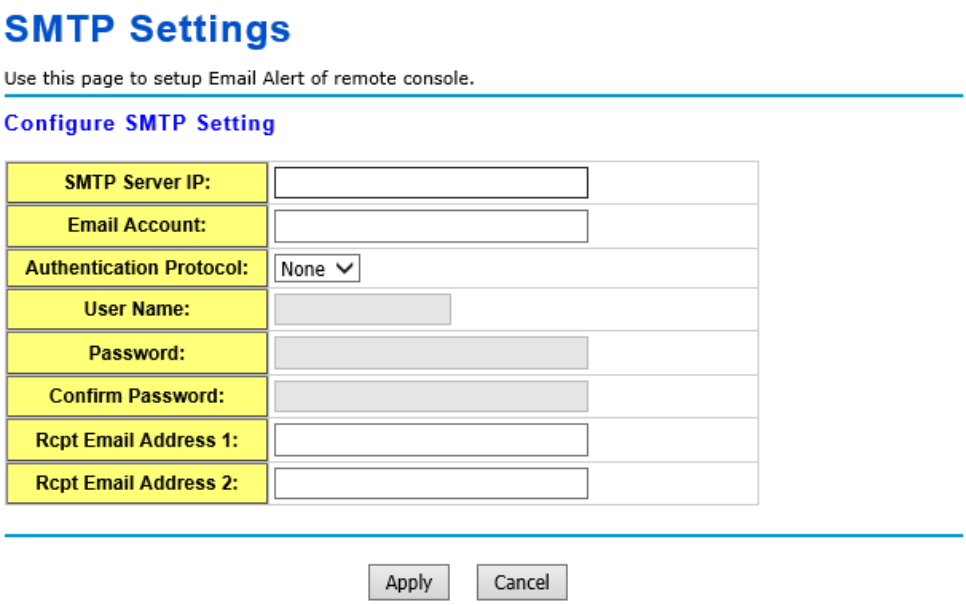
Note: SMS Alert only supports Ethernet Port Event Type

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



4.6.2 SMTP Configuration

The AP/Gateway supports E-mail Warning feature. The AP/Gateway 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 first, you can also set up the username and password in this page.



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.

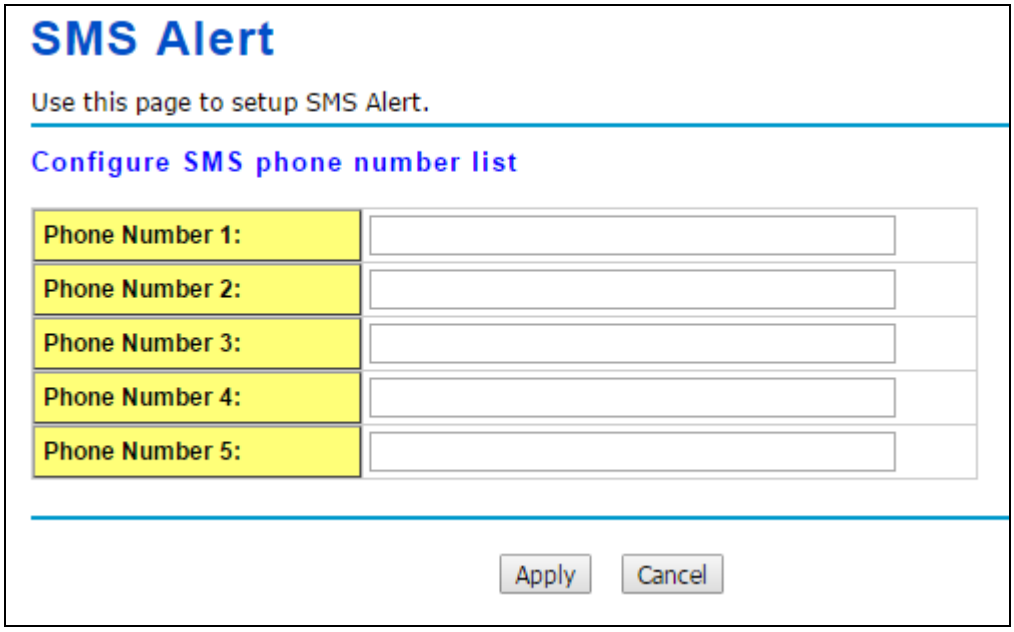
Confirm Password: Confirm the Password of the Sender Email account.

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.

4.6.3 SMS Configuration



Phone Number 1~5: Enter the SMS phone number: eg: +886912345678 or 0912345678

Press "**Apply**" to activate setting.

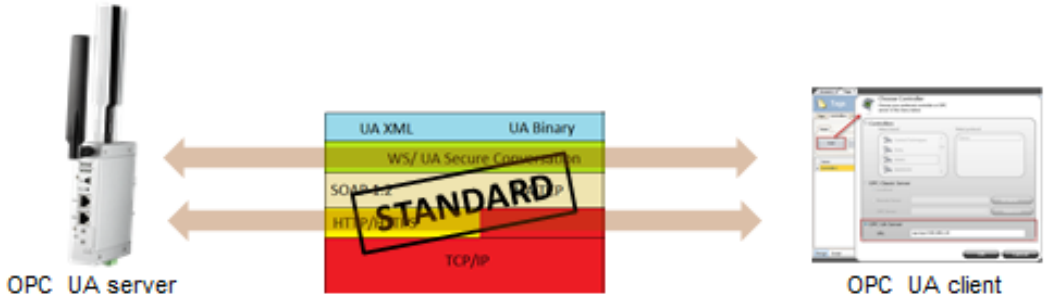
4.7 Management

The "**Management**" feature set pages allow users to configure the OPCUA Setting, Remote Setting, Login Setting, Firmware Upgrade, Configuration File, Certificate file and Remote IP scan.

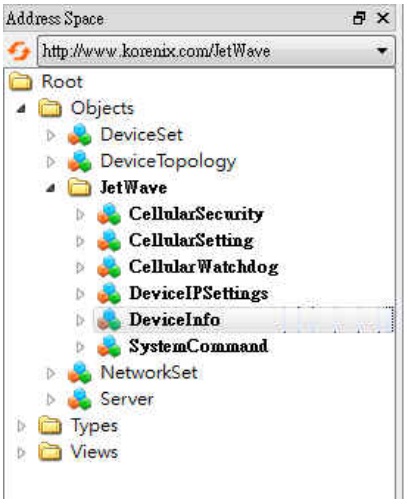
4.7.1 OPCUA Setting

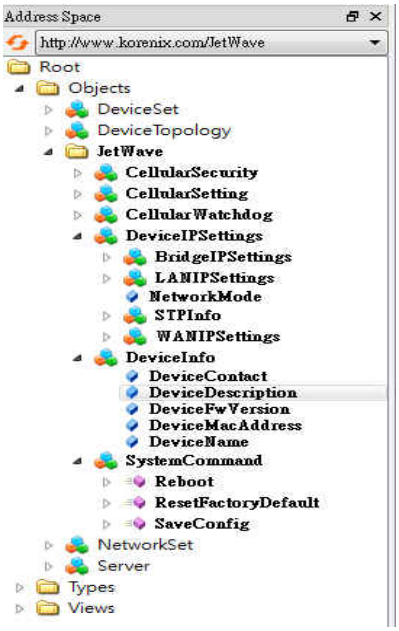
OPC UA (Unified Architecture) is the next generation of OPC technology. It is an industrial M2M communication protocol for interoperability developed, which integrates existing OPC specifications, providing a more secure, open, reliable mechanism for transferring information between servers and clients.

OPC UA communication is based on a client-server polling mechanism. OPC UA clients update data by polling OPCUA server and configure the parameters for OPCUA Server.

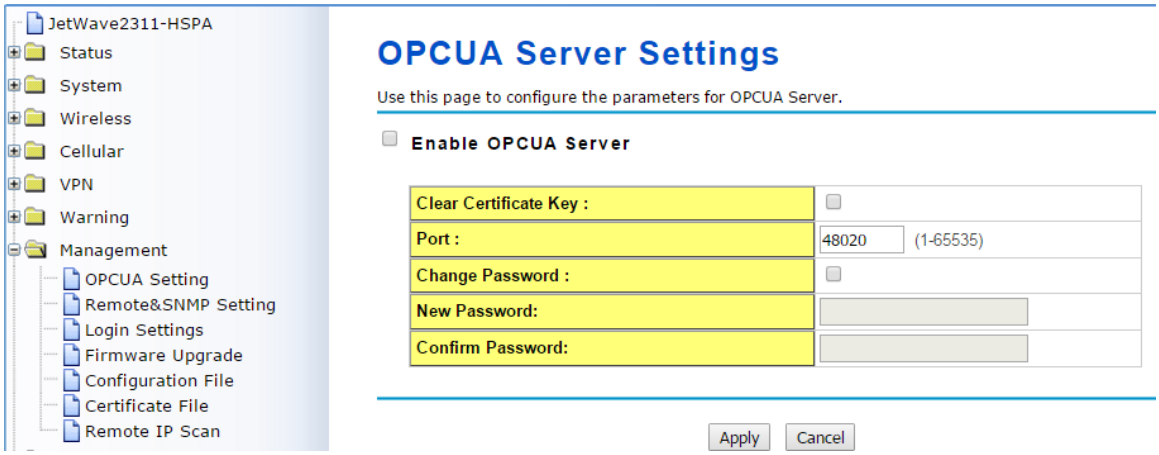


JetWave 2310 series support OPC UA server mode, which allow OPC UA clients (e.g. HMI) to get data and configure parameters, such as device information, cellular settings and Network settings on it.





This OPCUA Setting page allow user to configure the parameters for OPCUA Server.



Click on "**Enable OPCUA Server**" to enable the function.

Clear Certificate Key: Clear existing certificate keys.

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.

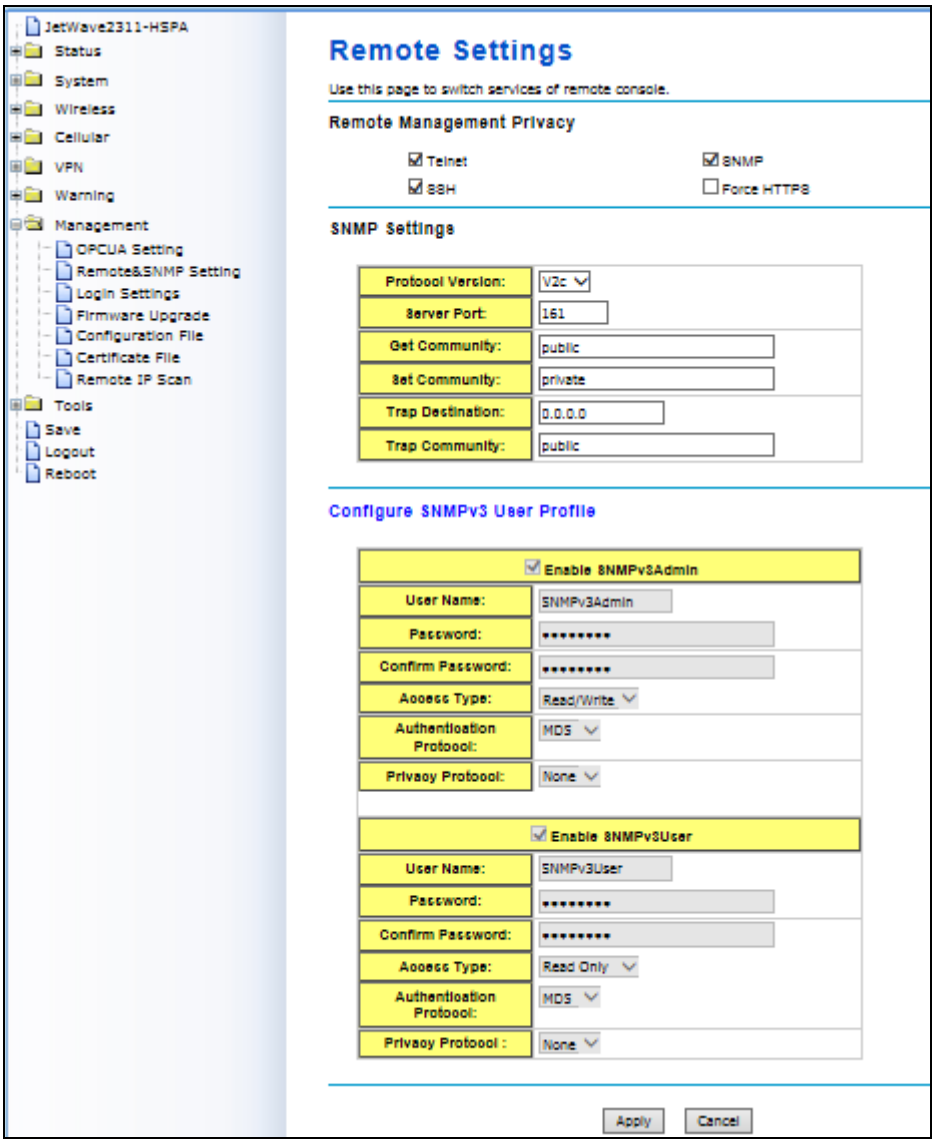
Press "Apply" to activate setting.

4.7.2 Remote Setting

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 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 warming type selection.

Wlan association: The client associated to the AP event.

Authentication Fail: The client failure of authentication event.

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

SNMP Settings:

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.

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.

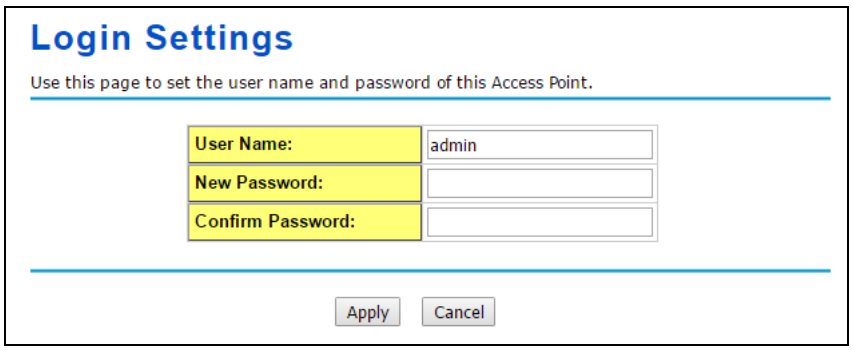
DES: Data Encryption Standard, it applies a 58-bit key to each 64-bit block of data.

Note: For security concern, it is recommended change the Community Name before you connect the AP/Gateway 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.*

4.7.3 Login Settings

Use this page to set the user name and password of the AP/Gateway.

Type the **User Name**, **New Password** and **Confirm Password** again. Press **"Apply"** to activate the new setting. The default user name is **admin**.

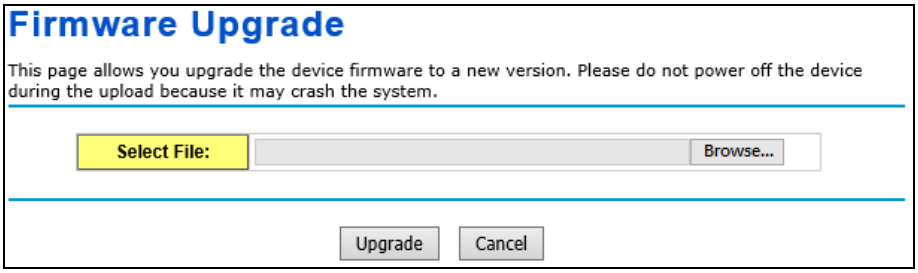


4.7.4 Firmware Upgrade

In this section, you can update the latest firmware for your AP/Gateway. Korenix provides the latest firmware in Korenix 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/Gateway to the customer site.

Note that the system will be automatically rebooted after you finished upgrading new firmware. Please remind the attached users before you do this. If you upgrade firmware 3G, the bandwidth may not enough (suggest 1Mbps) to upload firmware file correctly, this is not suggested.



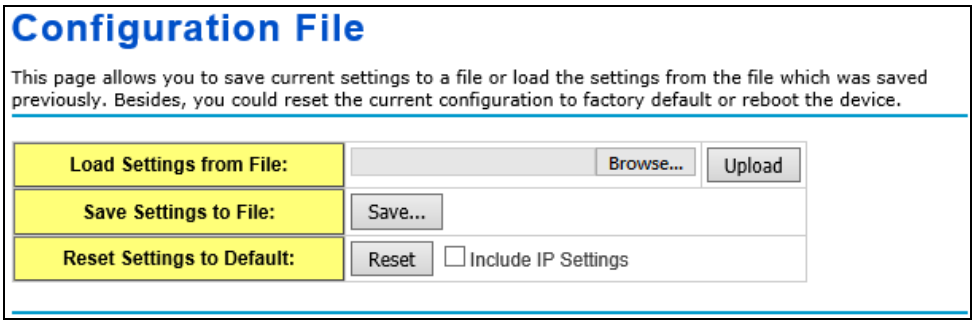
Type the path of the firmware in **Select File:** field. Or click "**Browse…**" to browse the firmware file. Press "**Upgrade**" to upload the firmware file to the AP/Gateway. After finishing transmitting the firmware, the system will copy the firmware file and replace the firmware in the flash. During the progress, please **DO NOT** power off your system.

4.7.5 Configuration File

The Gateway 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.



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

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.

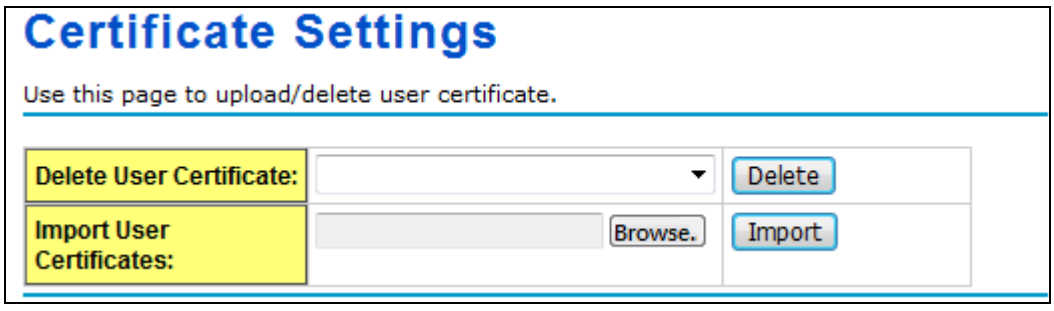
Reset Settings to Default: Press **"Reset"** can reset all the configurations, but not included default IP address to default settings. If you want to reset the IP address to default value, select "Include IP Settings".

4.7.6 Certificate File

Use this page to manage the user certificate file.

Use the **Import** to select the user certificates needs import.

Select the user certificate, then use the **Delete** to remove it.

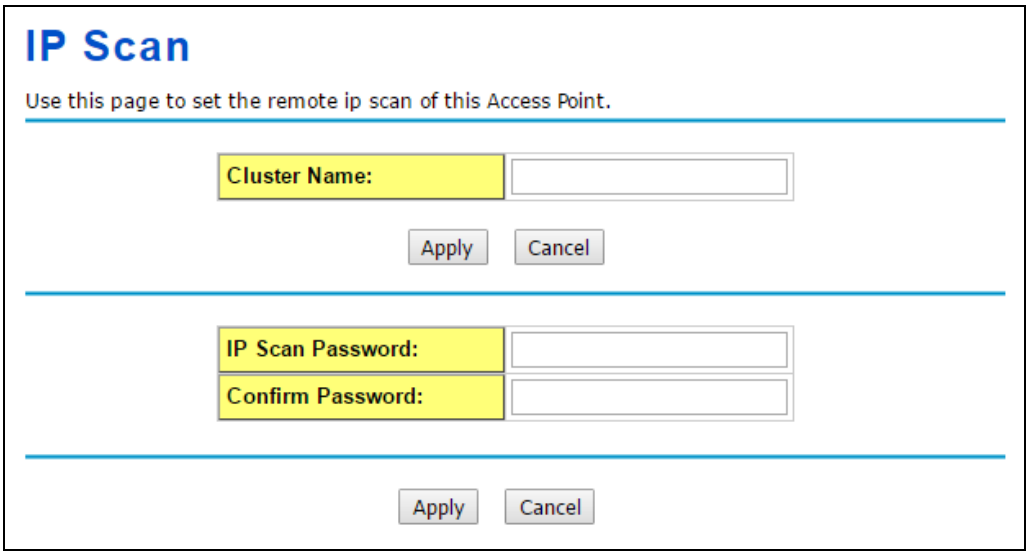


4.7.7 Remote IP Scan/ Cluster

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

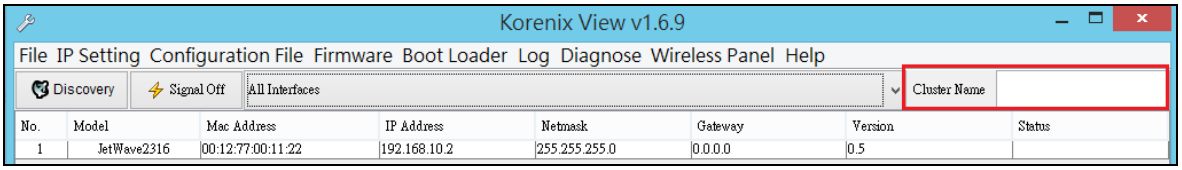
With **Remote IP Scan/ Cluster,** it provide higher wireless security when use Korenix View management tool.

Note: Must use Korenix View V1.6.9 or higher version



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

If set **Cluster Name** with **Password**, Korenix View will not list JetWave device in Model filed unless user type the same Cluster name at Korenix View interface, if user already type the same Cluster Name at Korenix View, it will list JetWave device 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.



4.8 Tools

The "**Tools**" feature set pages provides the additional useful tools.

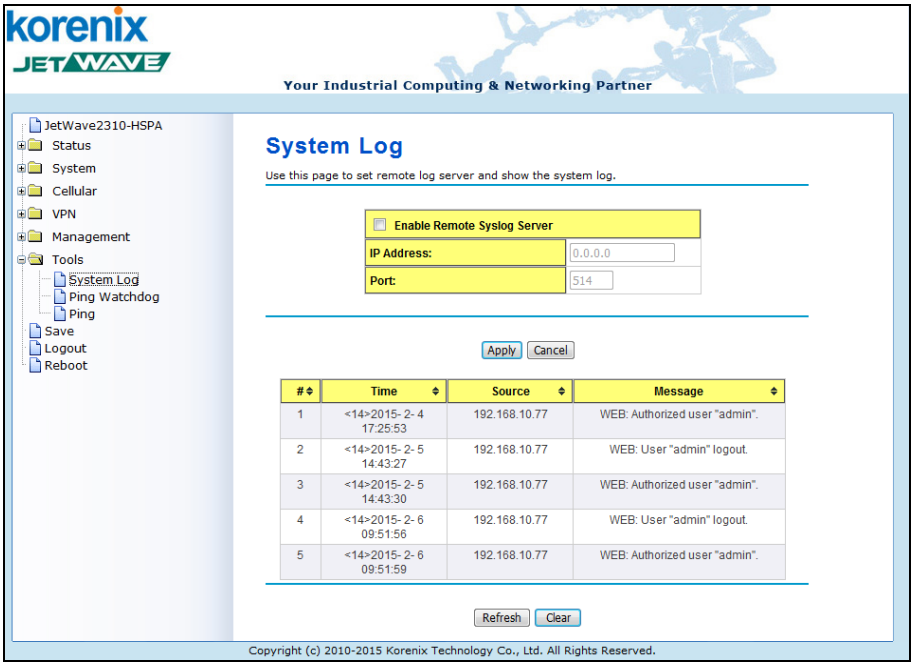
4.8.1 System Log

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

Enable Remote Syslog: Enable System log or not.

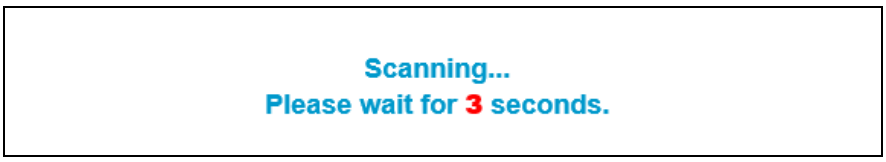
IP Address: Specify the IP address of the server.

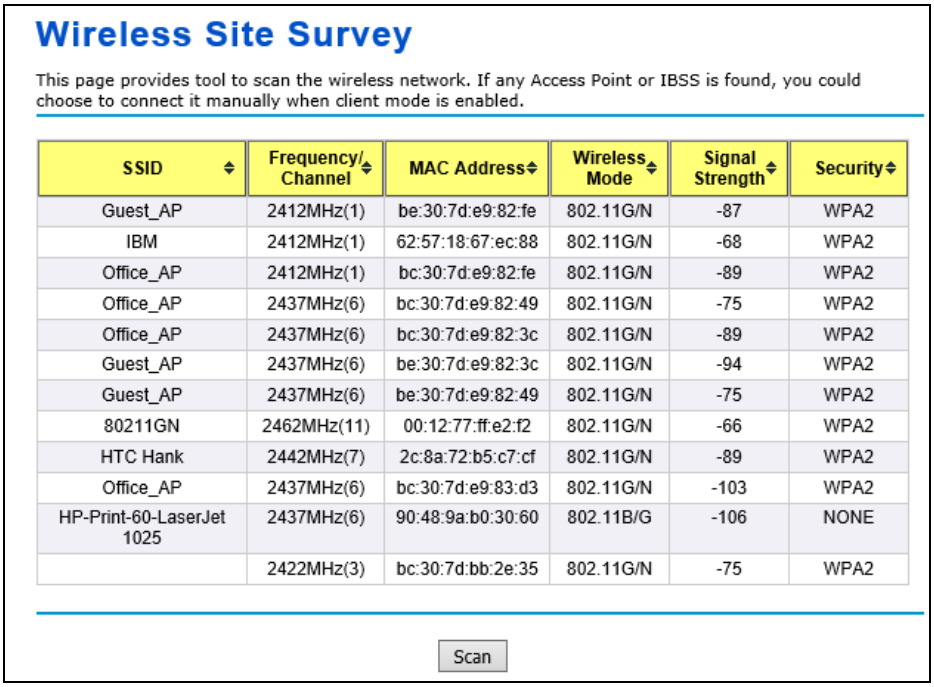
Port: Specify the port number of the server.



4.8.2 Site Survey

While your JetWave 2311 is in **Wireless Client** mode, this page provides tool to scan the wireless network. You can monitor current existed wireless network, connect to the SSID with better signal strength…etc. You need to wait for 3 seconds when you access to Site Survey page.



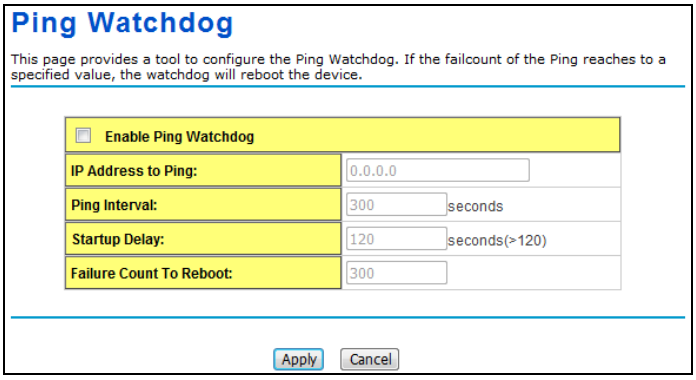


Press "**Scan**" if you want to scan the Wireless Network again. This progress takes around 3 seconds.

4.8.3 Ping Watchdog

This is a simple tool great to reduce maintain cost for JetWave.

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



Enable Ping Watchdog: Check means enable ping watchdog function.

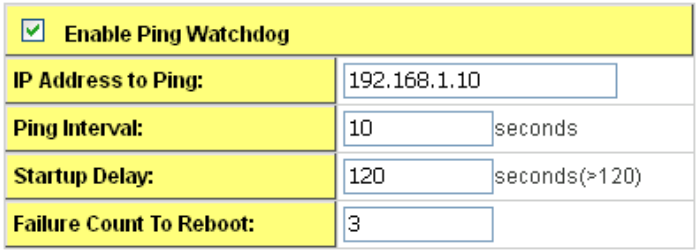
IP Address to Ping: input the IP address, JetWave will ping this IP.

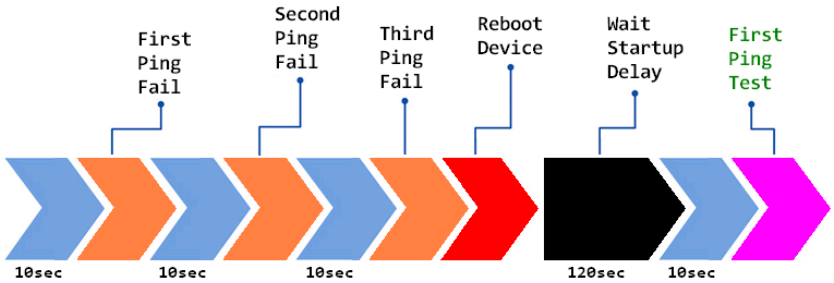
Ping Interval: JetWave will ping this IP every ping interval.

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

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

Below is the ping watchdog example:



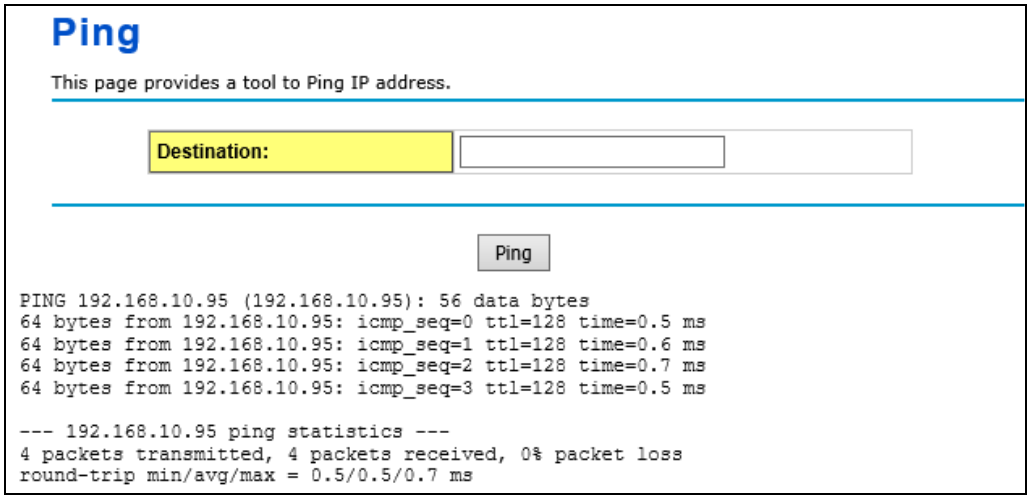


4.8.4 Ping

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.

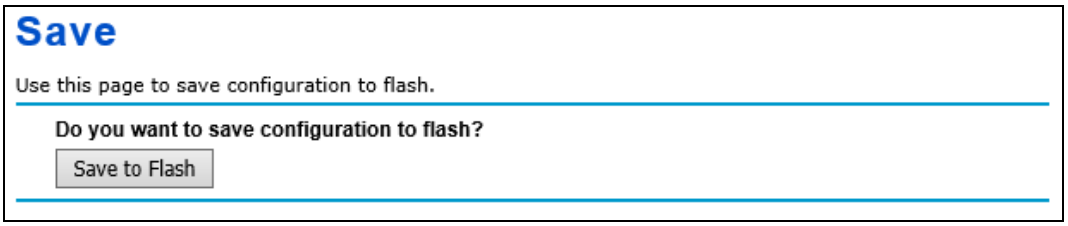


4.9 Main Entry

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

4.9.1 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.

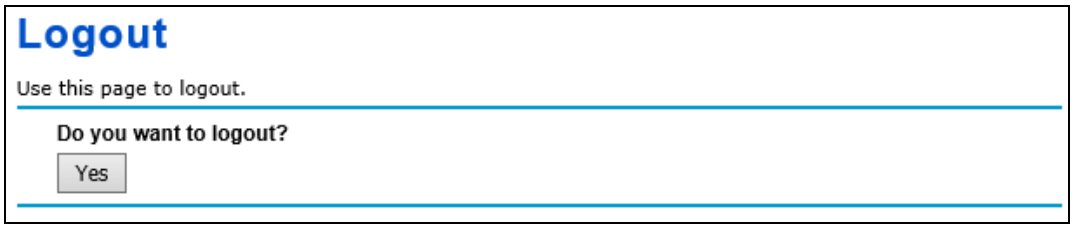


Press "**Save to Flash**" to save the configuration to flash.

4.9.2 Logout

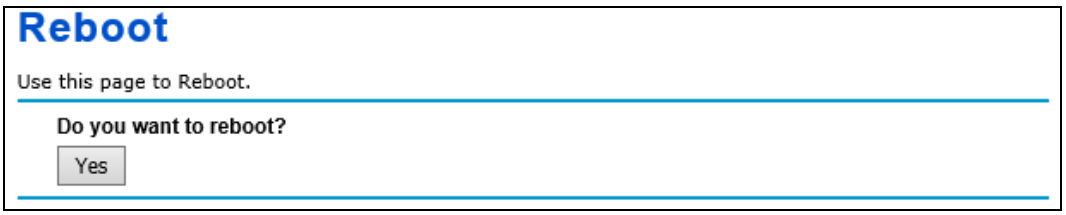
After finished configuring and leave, please remember to Logout the system. Without Logout the system, the login session will not timeout for couple minutes, it is a risk that other user may login your system without password checking before timeout. Another affect is that the user can NOT access at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

Use this page to logout. Press "**Yes**" to logout.

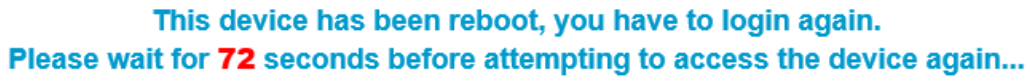


4.9.3 Reboot

Use this page to reboot the system. Press "**Yes**" to reboot system.



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



Chapter 5

Troubleshooting

Chapter 5 Troubleshooting

This chapter provides troubleshooting procedures for basic problems with the JetWave 2700/2800. For warranty assistance, contact your service provider or distributor for the process.

5.1 General Question

5.1.1 How to know the MAC address of the AP/Gateway?

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 AP. 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.

5.1.2 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 192.168.10.1.

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

5.1.3 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 Korenix 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.

5.2 Cellular

5.2.1 What if the 3G 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 3G band or not? Normally, the outlook of the 3G and WIFI antennas are the same.
- Check with the ISP and ask them check 3G connection condition of your site.
- Mark 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 3G speed you applied from ISP. The remote connection will also reduce the performance. Make sure you have enough bandwidth from ISP.
- Download the screen message and debug message to our service engineer.
- Continuously ping one remote IP address through 3G connection for a while, once the ping is often timeout, check the status before leave the device on site.

5.2.2 What if the 3G 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.
- Mark 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.

5.2.3 Why the backup 3G connection is not active?

- 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 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.

5.3 Appendix

5.3.1 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	1st release for JetWave 2310.	July, 2014	Orwell Hsieh
V1.0a	Correct model name error (3200/3300 -> 2310). Correct external antenna info. Add info in 3G Debug mode.	Apr. 1, 2014	Orwell Hsieh
V1.0b	Change appearance photo. Update the dimension depth from 30 to 33mm. Update 2.3.2 Reset functionality. Update 2.3.4 SIM description and wordings. Update 2.3.5 Digital Output description. Update 2.5 LED description. Update 4.2.5 Firewall Setting functionality and GUI. The device supports both Outbound and Inbound firewall from firmware version 0.8. Update 4.3.2 3G Redundant descriptions.	Nov., 2014	Orwell Hsieh
V1.1	Add JetWave 2310-LTE series and JetWave 2311-HSPA/LTE series product description, appearance, dimension, antenna placement, cellular and WIFI antenna spec…information. Add JetWave 2310-LTE/2311 series Web GUI: -Wireless (WIFI) Web GUI Setting -Cellular Connection Watchdog Setting Add OpenVPN Client Web GUI Setting	Feb., 2015	Patrick Teng, Orwell Hsieh
V1.1a	Add Mobile Manager Setting pages. Add OpenVPN Server Setting pages.	May. 2015	Orwell Hsieh
V1.1b	Change R1 led behavior Add “RADIUS Settings” page Add “get Cellular time” item Add “OPCuA Setting” page Add “Remote IP Scan/ Cluster” page Add Tools->Site Survey page Add “VPN Port forwarding” page Add “VPN Certificate” page	Mar. 2016	Queena Guan
V1.2	Update “System/Basic Settings” pages Move “System/Wireless Auto Offload Settings” from “System/Wireless Auto Offload Settings” Add “DDNS” pages Update “VPN/Status” pages Add “VPN/L2TP client” pages Add “VPN/IPsec” pages Add “Warning/Basic Setting” pages Add “Warning/SMS Configuration” pages Move “Warning/SMTP Configuration” from “Management/SMTP Configuration”	Jan. 2017	Nobby Shen