JetWave 3220v3/3420v3 Series

Industrial 802.11ac Multi-Radio

Wireless AP/ 4G Gateway / LTE Gateway

User Manual

V1.0 Jan, 2020

Copyright

About This Manual

This user manual is intended to guide professional installer to install the JetWave 3220v3/3420v3 and how to build the infrastructure centered on it. 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 wording 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

2.1.1Introduction

The user manual is applied to Korenix JetWave 3220v3 Series Industrial IEEE 802.11ac 2.4G/5G MIMO Wireless AP/Bridge, etWave 3420v3 Series Industrial Ethernet/802.11ac WIFI to LTE IP Gateway. The 2 product series equips with the same 802.11ac WIFI technology, the same hardware/software platform and the same installation consideration for indoor or outdoor field box.

The WIFI software configuration interface of the products is the same, for example the Web GUI, SNMP and CLI. If there are any specific features of JetWave 3420v3, they will be specially highlighted in the chapters.

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

2.1.2JetWave 3220v3 Series Appearance

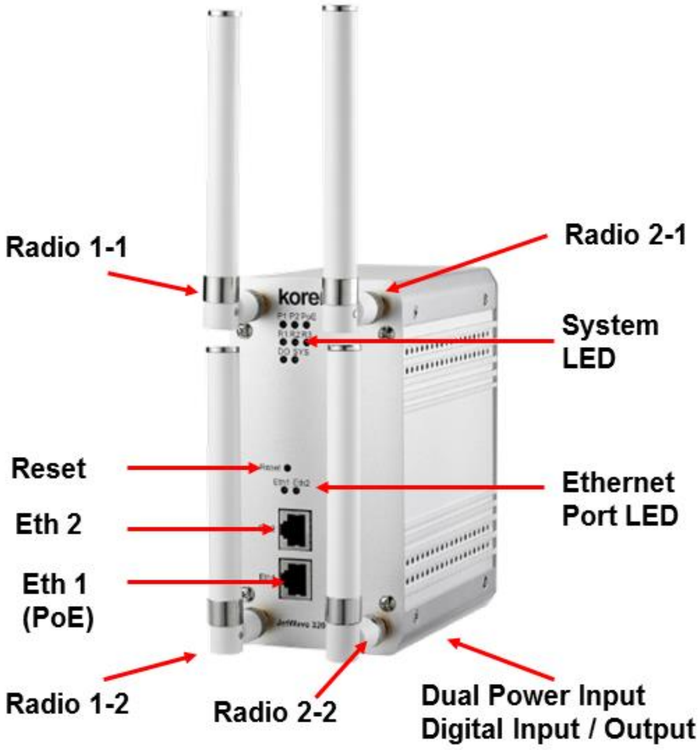


Figure - JetWave 3220v3 Appearance

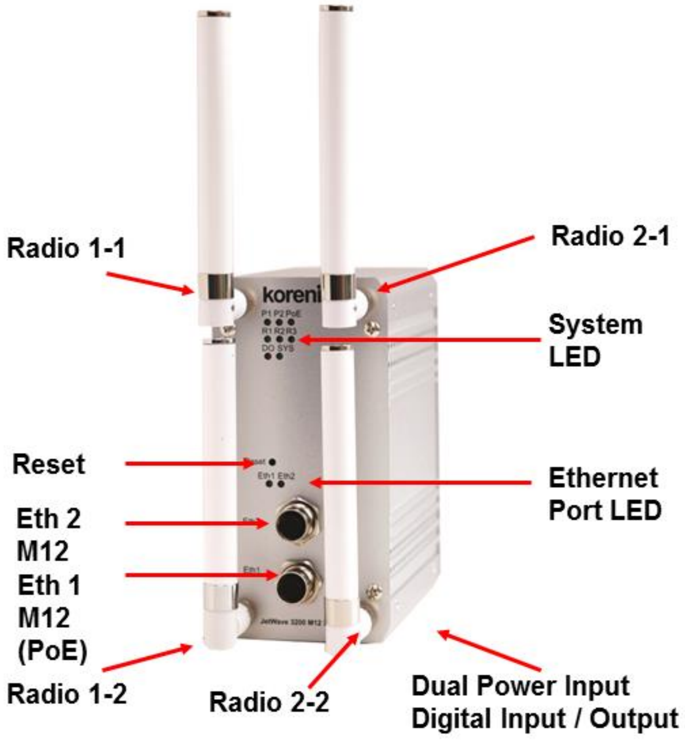


Figure - JetWave 3220v3-M12 Appearance

2.1.3JetWave 3220v3 Major Features

JetWave 3220v3: Industrial Dual 802.11ac 2T2R WIFI AP with 2x Gigabit LAN

JetWave 3220v3-M12: Industrial Dual 802.11ac 2T2R WIFI AP with 2x Gigabit LAN M12 Connector

802.11ac 2x2 MIMO doubles data rate, 300Mbps

Dual 802.11ac Radio Design

LAN/WIFI Bridge/Routing

Dual WIFI Redundancy

Link Fault Pass-Through

Clint Based Fast Roaming

Korenix View Utility for Wire & Wireless Management

M12 connector for vehicle installation (JetWave3220-M12)

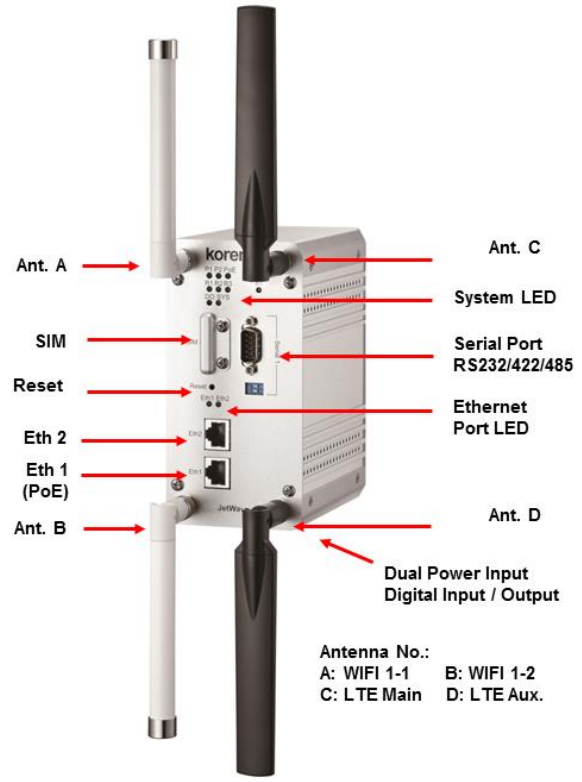
Gigabit PoE Input and DC 24V (12~48V) Redundant DC power input

Industrial IP31 Aluminum Housing

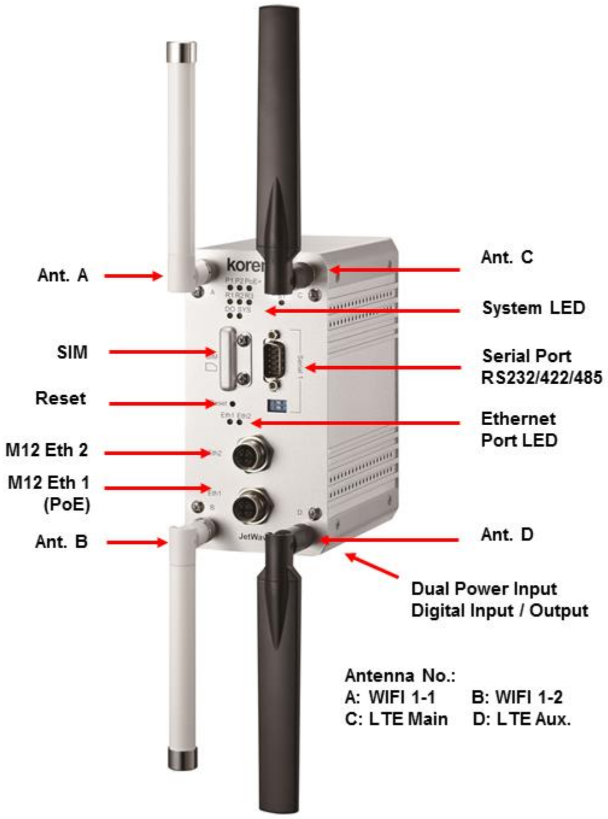
Digital Input, Relay Output

EN50121-4, -40~70℃ operating temp.

JetWave 3420v3 Appearance



JetWave 3420 Appearance



JetWave 3420-M12 Appearance

2.1.4JetWave 3420v3 Major Features

Models:

JetWave 3420v3-LTE-E: Industrial 4G LTE + 802.11ac WIFI IP Gateway, Band 20,8,3,7

JetWave 3420v3-LTE-U: Industrial 4G LTE + 802.11ac WIFI IP Gateway, Band 17,5,4,2

Features:

Connect Ethernet, WLAN & Serial device over 3G or LTE network

Next Generation Long Term Evolution (LTE) technology, 2x2 DL-MIMO, max. 100M DL /50M UL, backward compatible with UMTS/HSPA+ network to avoid connection lost (JetWave 3420 Series)

802.11ac 2x2 MIMO doubles data rate, 300Mbps

LAN to LTE Routing, WIFI to LTE Routing

LTE and WAN Redundant/Auto-offload

Korenix View Utility for Wire & Wireless Management

One RS-232/422/485 Serial interface, Serial mode includes TCP Server/Client and UDP

Gigabit PoE and DC24V(12~48V) Redundant DC power input

Industrial IP31 Aluminum Housing, Digital Input, Relay Output

M12 connector is available (JetWave 3220v3-M12/3420-M12)

EN50121-4, -40~70 ℃ Operating temp.

2.1.5Product Package

The product package you have received should contain the following items. If any of them are not included or damaged, please contact your local vendor for support.

Package:

JetWave 3220v3/3220v3-M12/JetWave 3420v3 Unit (depends on the model you purchase)

Pre-installed Embedded WIFI/LTE Module (depends on the model you purchase)

Default Antenna (JetWave 3220: 4, JetWave 3420: 4)

Din-Rail Mounting Kit

4-pin Power/DI+DO connector

Quick Installation Guide

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

Optional External Antenna Mounting Accessory:

4x Antenna Mounting L Plate

4x 90cm RG 316 Extended SMA Type Radio Cable

1x Celling-Mounting Plate

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 needs 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.

Chapter 2

Hardware Installation

Chapter 2 Hardware Installation

This chapter describes safety precautions and product information before installing JetWave 3200 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 setup and field plan.
2. The JetWave 3200 series is distributed through distributors and system installers with professional technicians and will not be sold directly through retail stores.

Safety Precautions

1. To keep you safe and install the hardware properly, please read and follow these safety precautions.
2. If you are installing JetWave 3200 series 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 JetWave 3200 series in the indoor office or factory, be aware of the power source and grounding must be well installed. The professional Wireless IT Engineer can provide service for AP location, channel and field plan to get better performance and coverage.
4. Users MUST use the safety certificated PoE switch/injector with the JetWave 3200 series. The Industrial PoE Switch/adapter is recommended.
5. When the system is operational with high gain antenna, avoid standing directly in front of it. Strong RF fields are present when the transmitter is on.
6. **Note that Field EMD (Lightning) DAMAGE IS NOT COVERED UNDER WARRANTY.**

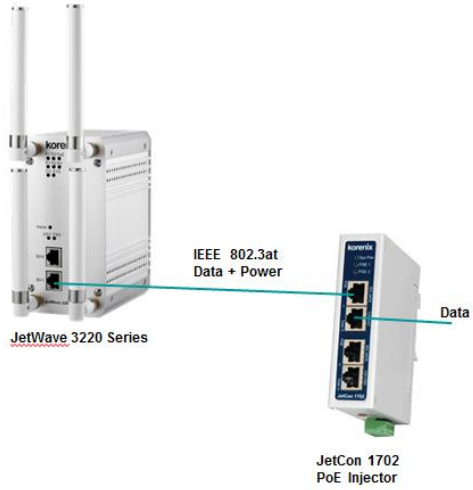
2.2 Power Installation

The system provides both DC power input and PoE power input.

DC Input

1. There is one 4-pin terminal block within the package for screwing the 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% (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. However, the DC power input can’t redundant with PoE. Please see the note at 2.2.3.

Powered by PoE



1. Connect the Ethernet cable to the Ethernet Port 1 in the front of the JetWave 3200 Series. The Ethernet port 1 is an IEEE 802.3at compliant PoE port.
2. If you are connecting the JetWave 3200 Series, the PoE function is applied to the Radio interface and the Eth 1. Eth 2 is only applied for data transmission.
3. While selecting power source by PoE, connect another end of the Ethernet cable to the PoE Switch or PoE Injector. Then the AP can be powered and user can access its management interface through the cable. The figure in right is an example of Connect AP to the PoE injector.

Note 1: Please choose Korenix Industrial IEEE 802.3at compliant PoE Injector or Switch as the power input source. Thus Korenix can provide better quality assurance for your network.

Note 2: Please select Industrial IEEE802.3at (PoE+) compliant PoE Injector or Switch as the power input source, it can deliver up to 30W power source. This is in case the system has more power once the power on inrush current is higher than 15W.

Connect both DC input and PoE

Note that the 2 power sources, DC input and PoE port are **NOT** redundant power design.

While you connect 2 power sources, for example you connect the DC Power 1 and PoE port. While you power on the DC power 1 as the 1st power source, the 2nd power source, the PoE chipset of the Eth 1 port detects the device is powered already. The PoE port will not request power from PSE switch. In this condition, while the DC power source failure, the PoE chipset of the Eth 1 port re-run PoE connection progress, the device will be reboot at this moment. The 2 power sources can NOT seamlessly redundant. This is current hardware restriction.

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. The 10/100Base-TX also support both full or half duplex mode. 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.

Eth 1: The Eth 1 is also an IEEE 802.3at compliant PoE – Power Device (PD) port. It can accept both power and data transmission from the PSE or PoE injector. Please refer to the 2.2.2 Powered by PoE for PoE installation.

Eth 2: The Eth 2 is an standard 10/100/1000Base-T RJ-45 port. It can transmit data only.

Available Cable Type: **(Refer to the appendix for M12 to RJ-45 cable assembly)**

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)

PoE Cable Request: CAT 5E/CAT 6 is preferred for PoE power + Data transmission.

Wiring STP Cable: STP (Shielded Twisted Pair) cable is preferred. The device is an EN50121-4 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 port or force reset the configuration to default. The function is depended on how much time you press the button.

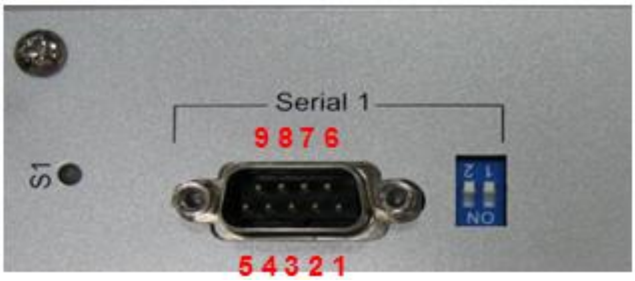
Press **3 seconds** to **reboot** the device.

Press **more than 7 seconds** can **reset the configuration to default.**

2.3.3 Serial Port

There is one RS232 serial port for serial communication on JetWave 3420v3. The serial port is designed for Serial over WIFI/Cellular communication. The port supports RS232/422/485 3-in-1, and up to 460.8kbps baud rate. The software supports TCP/UDP connection.

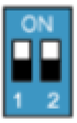
Below figure shows the pin assignment of the serial port.



Pin 1: DCD	**Pin 2: RXD**	**Pin 3: TXD**
Pin 4: DTR	**Pin 5: GND**	**Pin 6: DSR**
Pin 7: RTS	**Pin 8: CTS**	**Pin 9: RI**

Long Distance Termination:

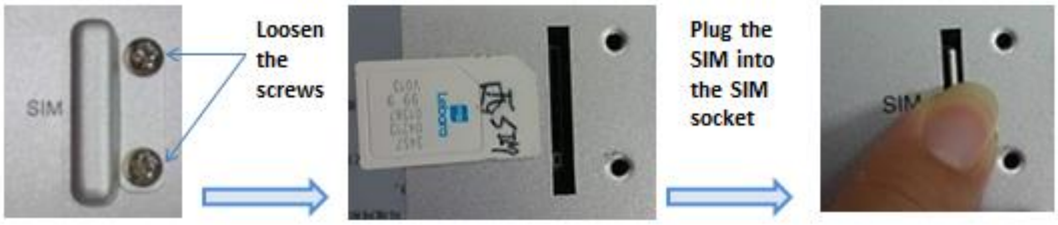
120ohm DIP



DIP 1	DIP 2	120ohm Termination Configuration
ON	ON	120ohm Terminator for long distance 4-wire RS485/422
ON	OFF	The setting may cause ERROR! Do Not use this.
OFF	ON	120ohm Terminator for long distance 2-wire RS485
OFF	OFF	No Terminator (short distance, Default value)

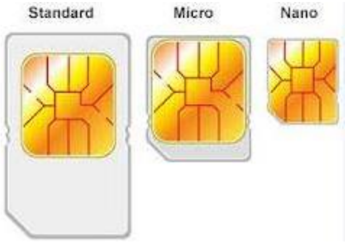
2.3.4 SIM Socket

The JetWave 3420v3 provides one external SIM (Subscriber Identity Module) socket to store the LTE SIM card. Loosen the screw and then you can plug in the SIM card.



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 JetWave 3420 standard SIM card.



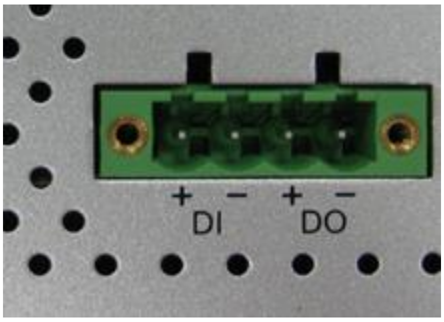
The Major type SIM card.

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 3420 system to detect the SIM card while booting up.

2.3.5 Digital Input

The system provides 1 digital input in the bottom side of the device.



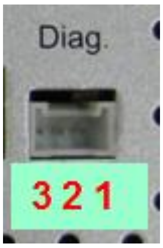
It allows users to connect the termination units' digital output and manage/monitor the status of the connected unit. The Digital Input pin can be pulled high or low; thus the connected equipment can actively drive these pins high or low. The embedded software UI allows you to read and set the value to the connected device. The power input voltage of logic low is DC 0~10V. Logic high is DC 11~30V. Wiring digital input is exactly the same as wiring power input.

2.3.6 Digital Output

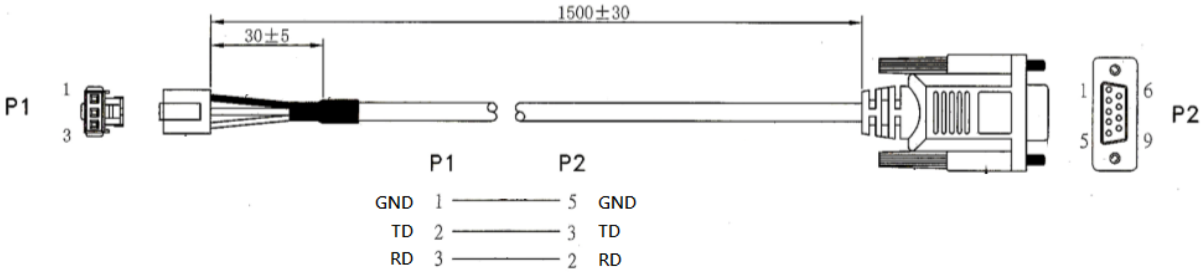
The system provides 1 digital output. It is also known as Relay Output. The relay contacts are energized (open) for normal operation and will close for fault conditions. The fault conditions include power failure, Ethernet port link break or other pre-defined events which can be configured in the management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

2.3.7 Diag. Console

There is one 3-pin console for diagnostic and command line on 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)



P1			P2
GND	1	5	GND
TD	2	3	TD
RD	3	2	RD

2.3.8 Ground

To ensure the system will not be damaged by noise or any electrical shock, we suggest you to 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 WIFI Antenna

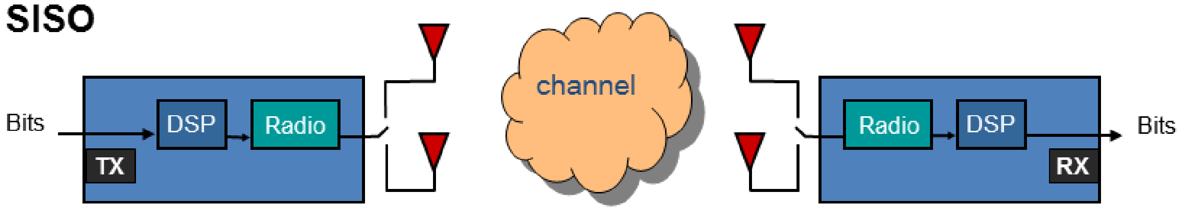
The JetWave 3220v3 series WIFI radio supports IEEE 802.11ac 2T2R (2 Transmit 2 Receive) Multiple-input Multiple-output (shot of MIMO) technology, is the use of dual polarization antenna to double the communication performance than traditional 1T1R SISO (Single-in Single-out).

MIMO & Dual Polarization

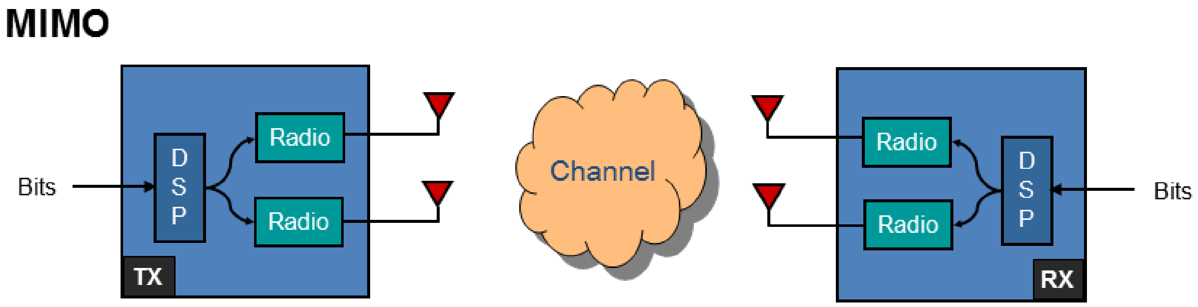
What is MIMO:

With the rising data rates and signal congestion, the MIMO is the proposed radio technology in IEEE 802.11ac 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.



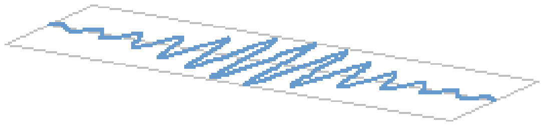
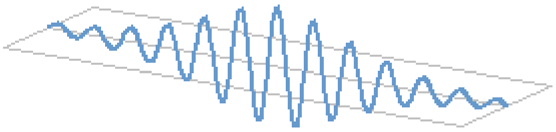
Polarization:

What is polarization

Polarization is a property of wireless antenna, the polarization determines the antennas that can pick up the signal, for example you can set up two antennas in close and pointing to the same direction, but with different polarization. The result is only antennas with the same polarization will be able to communicate with each other, this is important especially in point-to-pint wireless communication.

There are two major polarizations, Vertical and Horizontal. The antenna may support either one, you can choose Vertical or Horizontal polarization for the antenna installation. The result would be that antenna which is vertically polarized would only receive the signal from the vertically transmitting antenna, horizontally polarized antenna would only receive horizontally transmitting antenna.

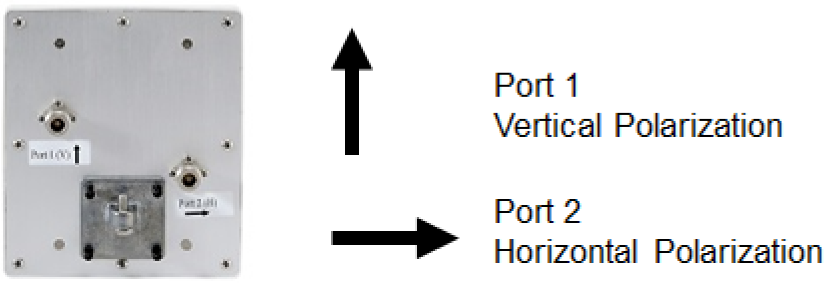
The below figures show the typical Horizontal / Vertical polarization:

Horizontal Polarization	Vertical Polarization
	

Dual Polarization:

There is also “Dual Polarization” antenna which provides two ports to plug in, one for the vertical and the other for the horizontal polarization. The dual polarization antenna can communicate with antennas of both types of polarities at the same time from one antenna.

The below figure is the example of Dual Polarization connectors. There are 2 ports, one is for Vertical polarization, the other is for Horizontal polarization. While installing the antenna, the 2 ports’ direction of the 2 end must be the same.

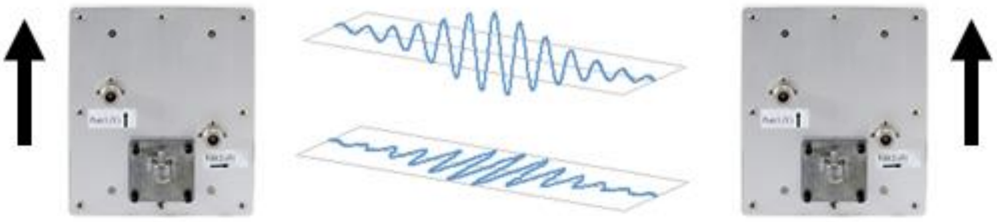


MIMO & Polarization:

To reach the 2T2R MIMO high performance, the antenna with dual polarization (also known as DP) which supports both Vertical and Horizontal Polarization is necessary. While you select the external antenna, check the Polarization specification of its datasheet or check with the supplier.

Normally, there are 2 connectors of the dual polarization antenna, this is also a way to identify whether this is Dual Polarization or not. Connect the 2 end of the antenna to the antenna socket of the Access Point.

The below figure shows the dual polarization transmitting between the 2 MIMO antennas:



Antenna Socket

The JetWave 3200 Series supports IEEE 802.11ac 2T2R MIMO technology. There are 2 SMA Type antenna sockets for one WIFI radio interface. You can connect 1 to 2 WIFI antenna based on your need.

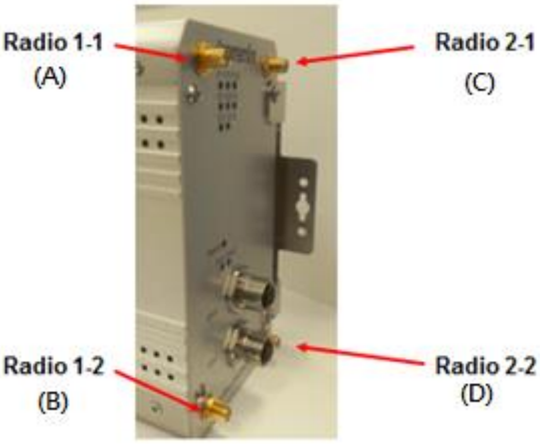
If you just need to connect one single polarization WIFI antenna, you must go to the Web GUI to change the antenna number to 1, and connect it to the 1st antenna socket, Radio 1-1 or Radio 2-1 of the JetWave 3220. Please remind that it is just 1T1R (150Mbps) in such installation.

If you would like to connect dual polarization antenna or 2 antennas for 2T2R, you must connect to the two antenna sockets, Radio 1-1 and Radio 1-2.

The figure indicates the WIFI Radio number.

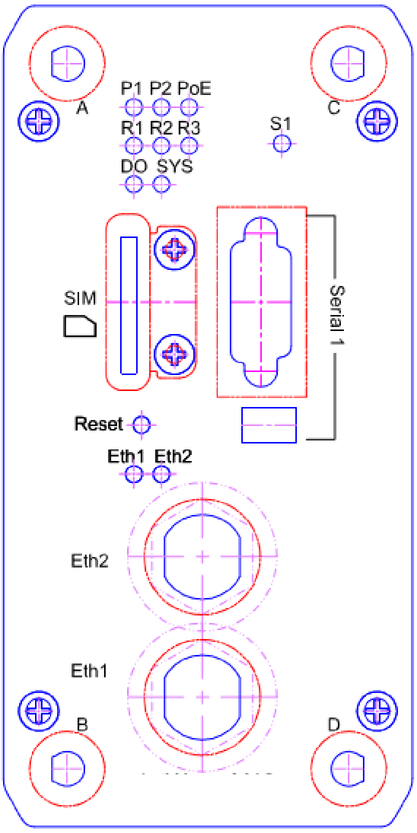
Radio 1-1(A) and 1-2(B) are applied to the 1st Radio of the JetWave 3220v3/3420v3.

Radio 2-1(C) and 2-1(D) are applied to the 2nd Radio of the JetWave 3220.



Added Number Table

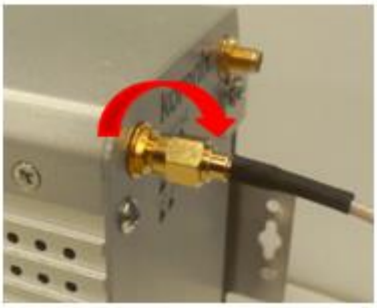
In new version print on front panel, Korenix remove the logo and print the antenna number A, B, C and D to represent for the Radio 1-1, 1-2, 2-1 and 2-2. Following figure shows the new print of the front panel and the antenna number table shows their functionality.



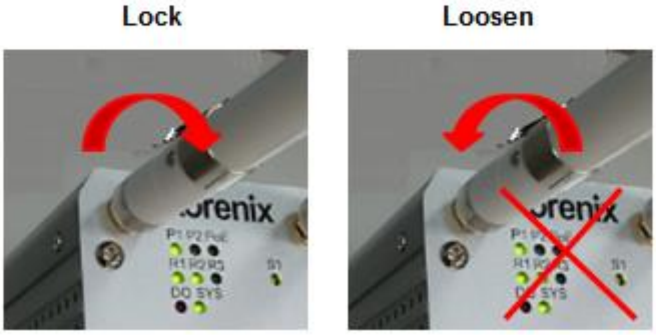
Antenna No.	JetWave 3220	JetWave 3420
A	WIFI 1-1	WIFI 1-1
B	WIFI 1-2	WIFI 1-2
C	WIFI 2-1	LTE Main
D	WIFI 2-2	LTE Aux

Antenna Installation

The figure shows the direction to lock the antenna, it is clockwise direction. There is Nylock pasted on the antenna to avoid antenna loosen in vibration environment, please don't often lock/un-lock the antenna, otherwise, the Nylock paste will be damaged.



Use the same way to lock the attached WIFI antennas, it is clockwise direction as well. **Note** that the counter-clockwise direction will loosen the antenna immediately.



For vibration environment, we don't recommend you connect the antenna directly to the device, no matter how heavy you lock it. It is 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, celling mounting kit as optional accessory. While you need it, you can purchase from Korenix.

For how to mounting the antenna plate and celling-mount plate, please refer to the chapter 2.6.

Default WIFI Antenna Specification:

The following information apply to the Default WIFI Antenna.

Material of the antenna: The body material is Brass, Insulator is Teflon.

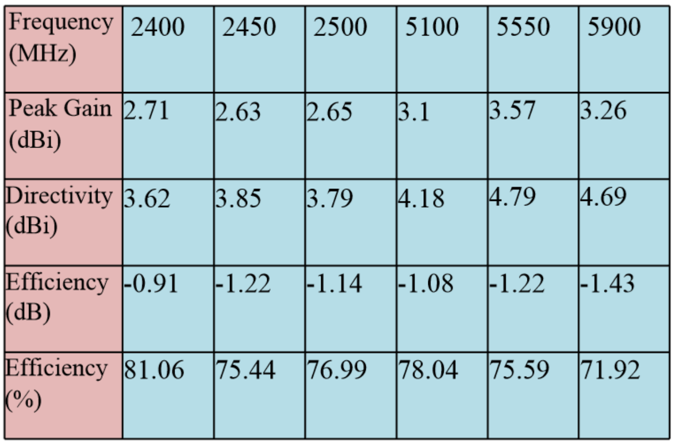
Frequency Range: 0~6GHz

Impedance: 50ohm

VSWR: ≦1.5

Gain: The default WIFI antenna support both 2.4G and 5G band, its gain value is 2.6dbi for 2.4G band, 3.5dBi for 5G band. This gain value is peak value of the antenna.

Antenna Efficiency for Reference:

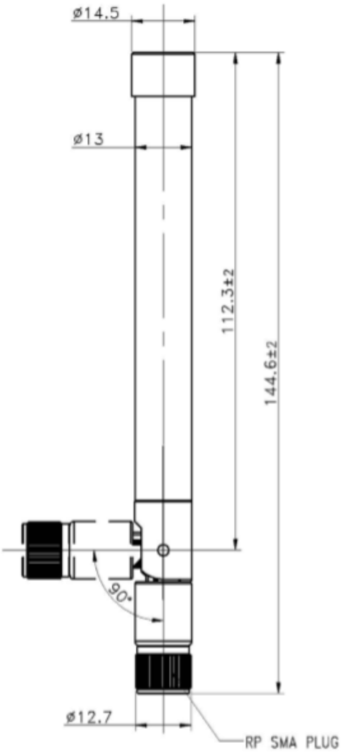


Frequency (MHz)	2400	2450	2500	5100	5550	5900
Peak Gain (dBi)	2.71	2.63	2.65	3.1	3.57	3.26
Directivity (dBi)	3.62	3.85	3.79	4.18	4.79	4.69
Efficiency (dB)	-0.91	-1.22	-1.14	-1.08	-1.22	-1.43
Efficiency (%)	81.06	75.44	76.99	78.04	75.59	71.92

Dimension: Length: 144.6mm

Directional: Omni-Direction

Operating Temperature: -65℃ ~ +165℃



Reference Distance:

The suggest distance of the default WIFI antenna is 100 meter wide, up to 200 meter in public space. (However, the free space lost may affect the transmitting distance, so that the device may have different performance in different environment.)

Note: Please install the antenna carefully due to the insulator material may be damaged after dropped to the ground. Once you find the insulator is broken, even very small hole or gap, please replace a new one.

2.5 LED Indicator

The following table indicates the LED of your device.

LED	Indication	LED	Indication
P1	**Power 1** Status Green ON = System ON	**R2**	Status of the **Radio Number 2** Green ON = Radio 2 is activated *Note
P2	**Power 2** Status Green ON = System ON		
PoE	**IEEE 802.3at PoE+ Status (Eth 1)** Green ON = Powered from the 802.3at PSE Switch. *Note 1 OFF: 802.3af or Not power by PoE	**DO**	**Digital Output** Status Red ON = The Relay is ON. It may indicate the alarm of specific events.
R1	**Radio 1** Status Green ON = Radio 1 is activated	**SYS**	**System Status** Green ON = The system is activated.
Eth 1	**Ethernet Port 1** Status. Green ON = Eth 1 is Link Up. Green Blinking = Eth 1 is Activating	**Eth 2**	**Ethernet Port 2** Status. Green ON = Eth 2 is Link Up. Green Blinking = Eth 2 is Activating
S1	**Serial Port 1** Status (JetWave 3420 Only) Green Blinking = Serial port is transmitting data Red Blinking = Serial port is receiving data		

Note 1: PoE LED is only applied to the IEEE 802.3at PoE+. Current PoE LED can't indicate IEEE802.3af PoE, this is known limitation of the LED display.

Note 2: R2 is the radio number. R1 is the first WIFI Radio, R2 is the 2nd WIFI Radio, LTE Radio.

In JetWave 3220v3, the R2 indicates the 2nd WIFI radio of the JetWave 3220v3.

In JetWave 3420v3, the R2 indicates the LTE radio of the JetWave 3420v3.

2.6 Mounting

2.6.1 Mounting the AP

The JetWave 3200 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 3200 series also provide celling-mount plate as optional accessory. The celling-mount plate is available for celling-mount or wall-mount installation, for example the vehicle, railway and warehouse.

Optional Accessory: JetWave 3400/3200 External SMA Antenna Mounting Kit

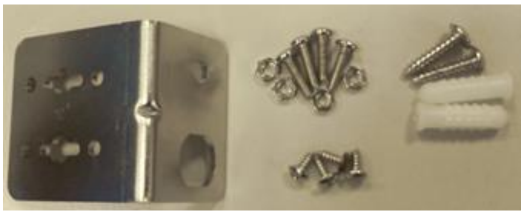
The package:

4x Antenna Mounting L Plate

4x 90cm RG316 Extended SMA Type Radio Cable

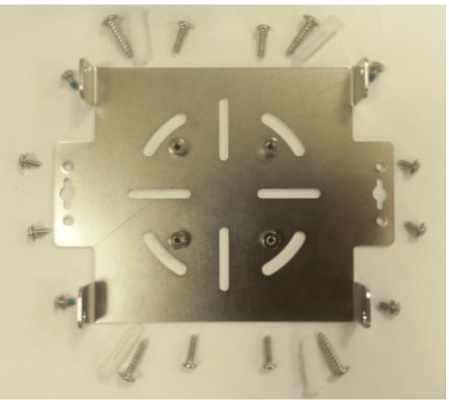
1x Celling-Mounting Plate

Antenna Mounting L Plate



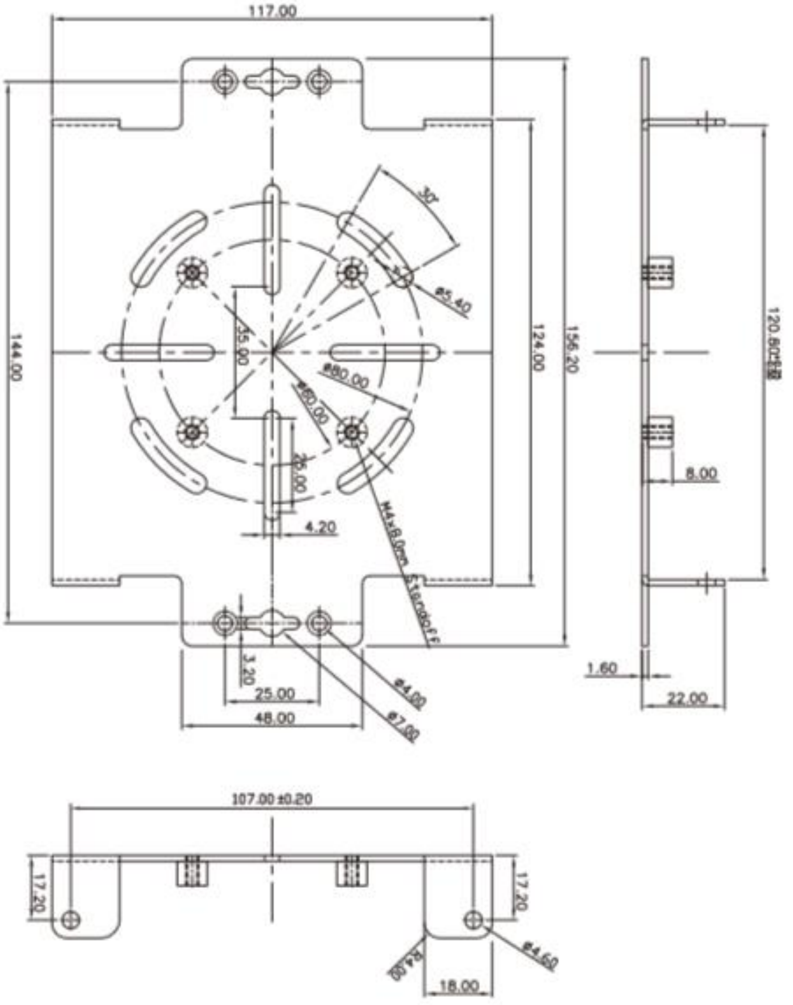
90cm RG316 Extended SMA type Radio cable

Celling-mounting Plate (include screws)



Dimension: 156x117x22mm

Celling-mounting Plate Dimension:

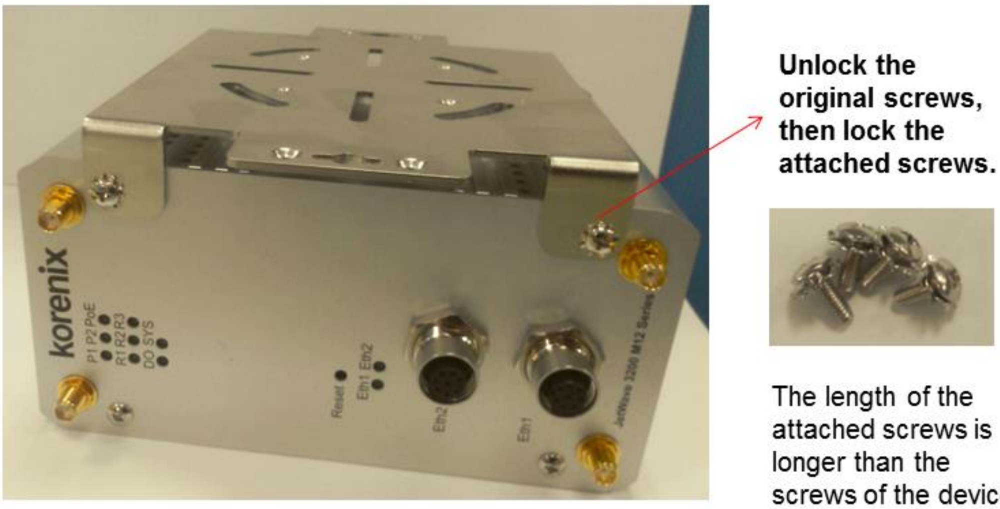


JetWave 3200/3300/3400 Series
Celling-mount Plate Dimension

2.6.2 Mounting the AP with Celling-mounting Kit

To mount the AP with celling-mounting plate, you must unlock 4 screws on the front/back of the unit first. Use the new attached screws to lock the device. Then you have some other optional screws for different kinds of celling-mounting.

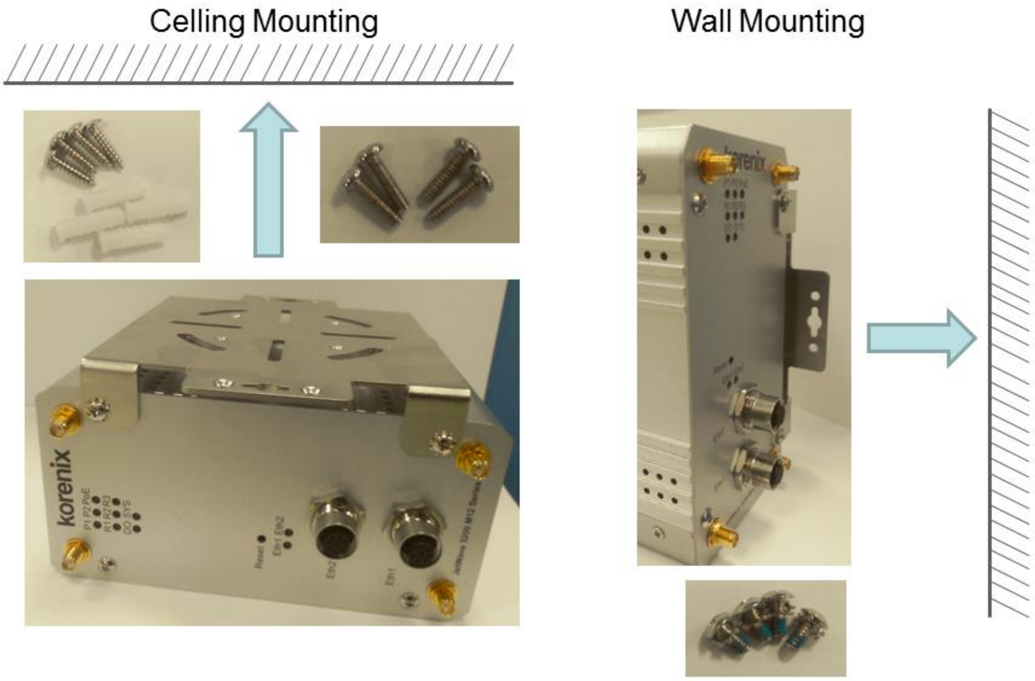
1. Unlock the original screws, lock the device with new attached screws.
2. The celling mount plate is available for both Celling and Wall mounting.



Unlock the original screws, then lock the attached screws.

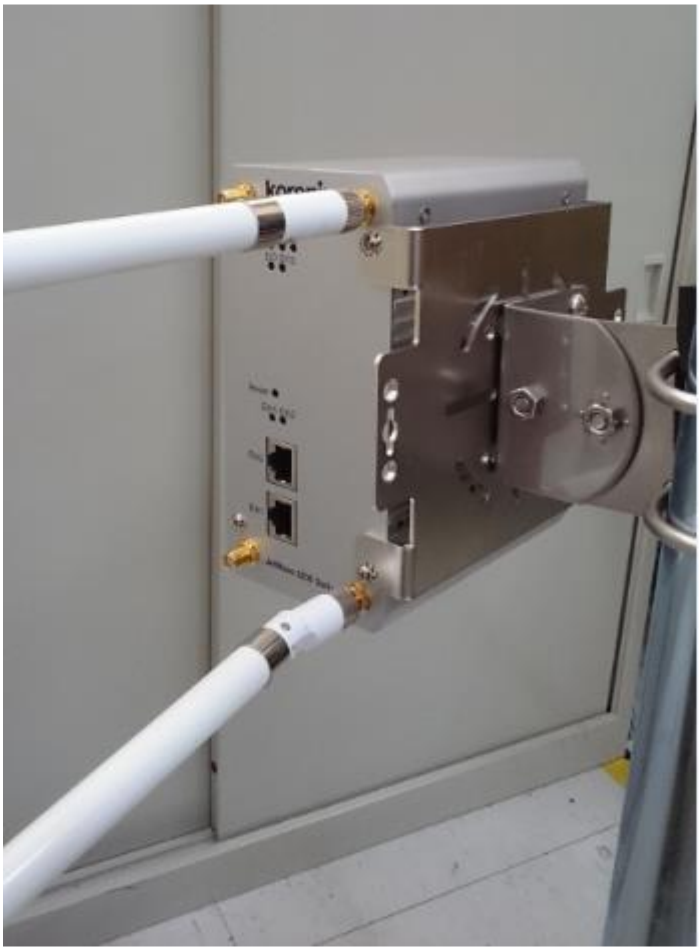
The length of the attached screws is longer than the screws of the device.

Note: Please notice that the screw hole on the front panel will be damaged after lock/unlock few times. DO NOT often change the celling mounting kit!



3. The celling mount plate is flexible for different installation. This figure shows the poll-mount

installation by using the celling mount kit. This is applied to the indoor environment.



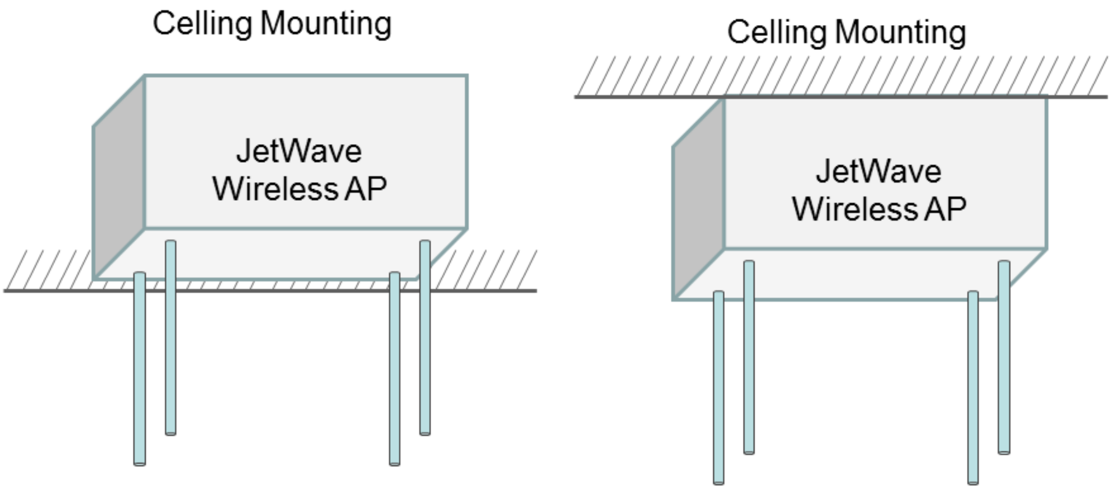
4. In some cases, you may need to install the celling mount plate first then lock the AP/Gateway to the celling-mount plate.

2.6.3 Mounting the default antenna on unit

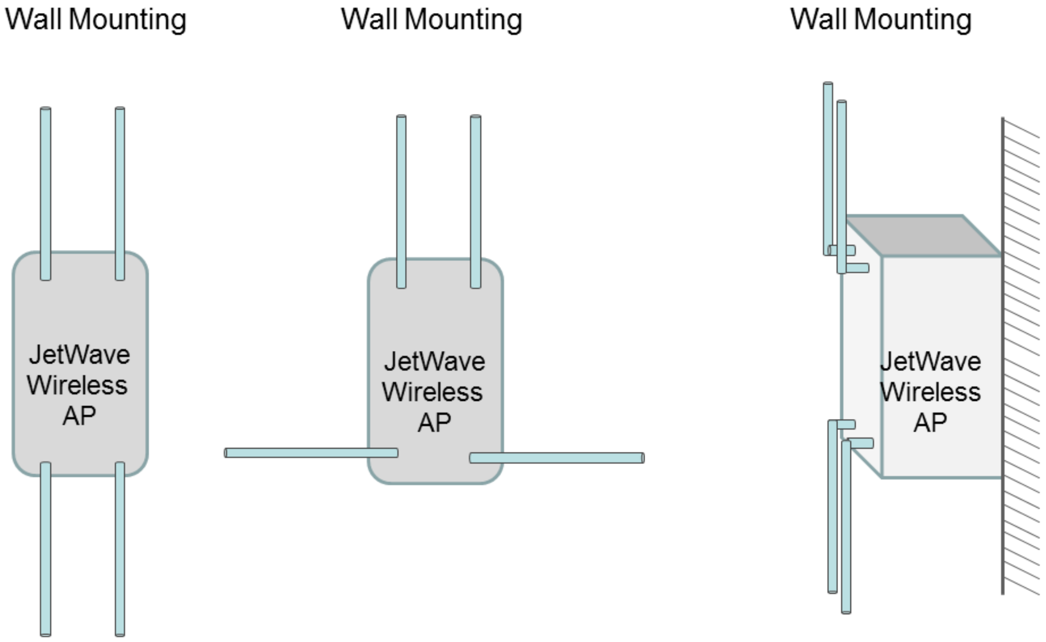
There are dual band antennas for the JetWave3200 Series in the product package. You can install the default antenna to the SMA socket on the front. Each radio supports 2T2R MIMO technology, you must install 2 antennas for one radio.

Since the AP housing material is Aluminum, the antenna zone may be affected if you install the antennas directly in front of the panel. The below figures introduces the suggestion for the default antenna installation. Or you can install the antennas by antenna mounting L plate in other better locations.

Celling-mount (or Desktop)



Din-Rail / Wall-mounting



2.6.4 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.

2.6.5 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 Dual Polarization for 2T2R MIMO radio transmission. You can choose SMA-type Dual Polarization antenna and follow the same steps as “Mounting the default antenna on unit” to install your antenna.

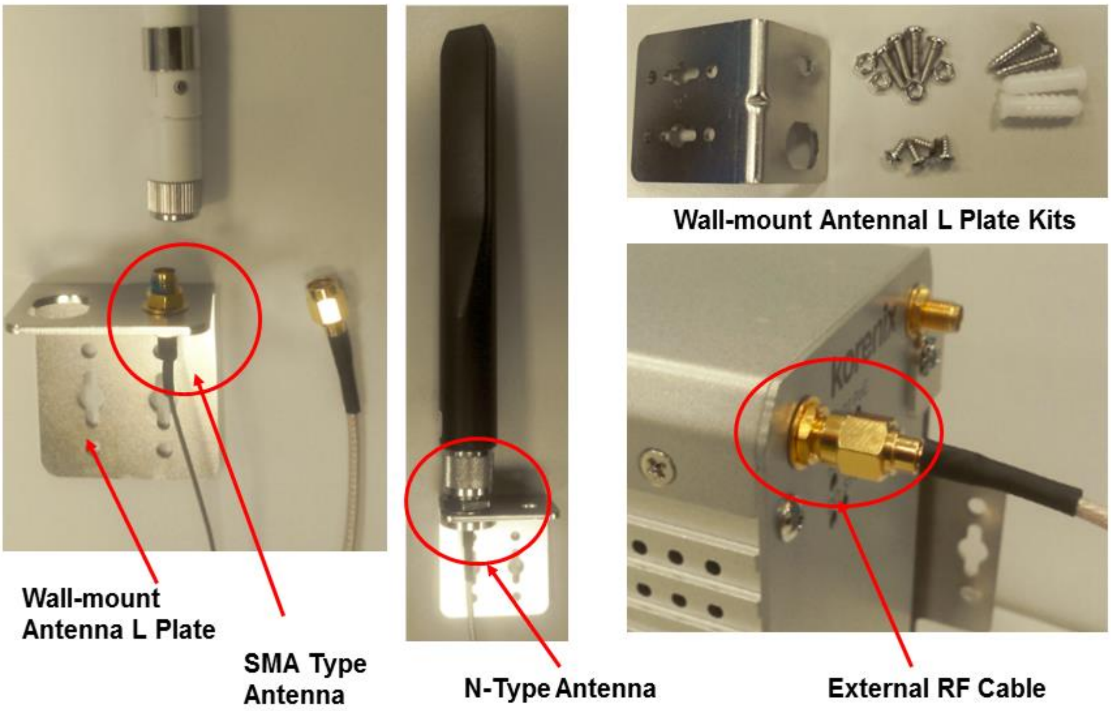
2.6.6 Mounting the N-Type external antenna:

While selecting the N-type external antenna, you must notice that the antenna should support Dual Polarization for 2T2R MIMO radio transmission. The JetWave 3200 series external antenna mounting L plate is available for both SMA and N-Type antenna, purchase the external N-type antenna mounting kit from your sales.

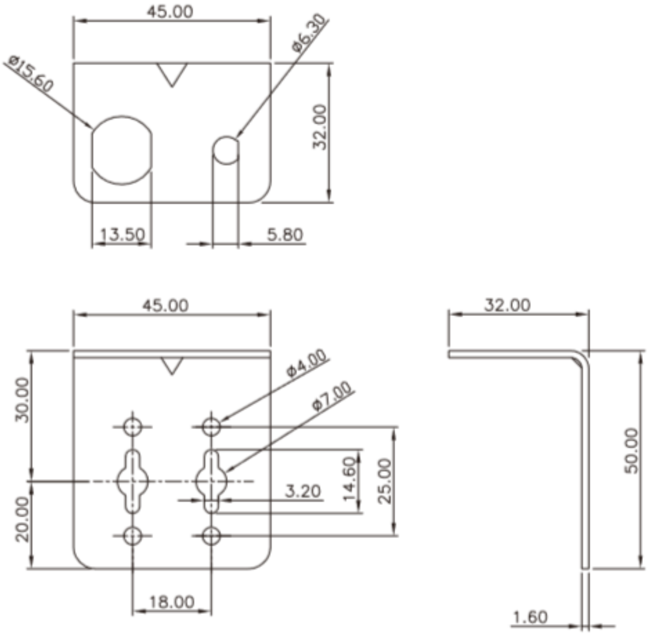
2.6.7 Below figure shows the optional External Antenna Mounting Kit

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

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



Wall-mount Antenna L Plate Dimension



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

2.7 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.

Antenna Socket of the AP/Gateway:

Front Left: Radio 1 (WLAN 1). There are 2 SMA connectors for 2T2R MIMO.

Front Right: Radio 2 (WLAN 2/3G/4G LTE). There are 1-2 SMA connectors. It may be WIFI MIMO, 3G or LTE antenna connector depends on the model you purchase.

Select the External Antenna:

Gain: It affects the system performance.

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

Polarization: Dual Polarization is MUST for this 2T2R MIMO product.

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.

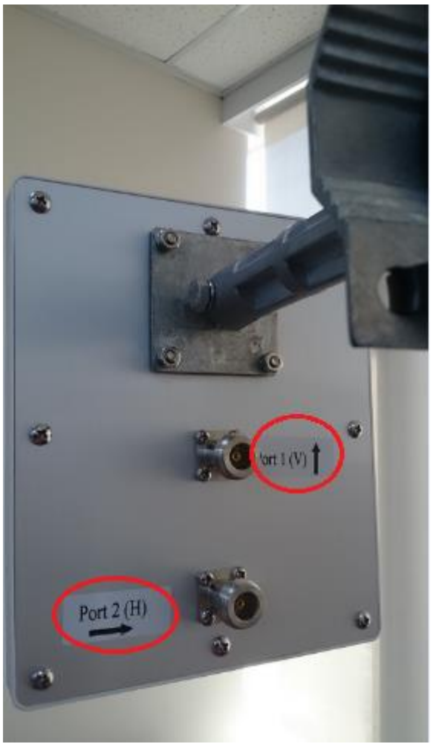
b. Find the remote location of the target AP. The Telescope, GPS positioning tool, Google Map are convenient tool.

c. The polarization of the two ends of the directional antenna MUST be the same. Refer to the label on the antenna, the direction of the "**Port 1(V)** ↑ "and "**Port 2(H)**→" must be the same in the 2 ends.

d. Connect the extended Radio Cable from the AP/Gateway to the antenna. The level

e. Go to Web GUI, use the **Antenna Alignment tool** (Refer to the 4.6.5) can help you find the target Antenna.

f. Run the **Data Rate Test** (4.6.4) can help you check the performance between the two ends.



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 Dual Polarization. Most of the high gain directional antenna supports Dual Polarization.

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

The JetWave 3220v3/3420v3 Series supports Web GUI Configuration, Simple Network Management Protocol (SNMP), Telnet and Diagnostic Command Line Interface for management and Window Utility helps you discover the device cross network, basic IP setting, firmware management…etc.

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 3200/4300 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 3200/3400 Basic Factory Default Settings

Features		Factory Default Settings
Username		admin
Password		admin
Model Name		JetWave3220 (3420 depends on which model you access)
Device Name		korenixXXXXXX (X represents the last 6 digits of Ethernet MAC address)
Network Mode		**Bridge Mode** (JetWave 3220) **Note:** In Bridge mode, only one IP Address (LAN) interface is available. **Router Mode** (JetWave 3420) **Note:** In Router mode, WAN (Eth 1) and LAN (Eth 2) interface has its own IP Address.
Default IP at Bridge Mode (JetWave 3220 Default)		
IP Address		192.168.10.1
Subnet Mask		255.255.255.0
Gateway		0.0.0.0
Default IP at Router Mode (JetWave 3420 Default)		
IP Setup – Eth 1 (WAN)	Access Type	Static IP
	IP Address	192.168.1.1

	Subnet Mask	255.255.255.0
	Gateway	0.0.0.0
	Primary DNS Server	0.0.0.0
	Secondary DNS Server	0.0.0.0
IP Setup – Eth 2 (LAN)	IP Address	192.168.10.1
	Subnet Mask	255.255.255.0
	DHCP Server	Enabled
	DHCP IP Range Start	192.168.10.101
	DHCP IP Range End	192.168.10.150
	DHCP Subnet Mask	255.255.255.0
	DHCP Gateway	192.168.10.1
	(Refer to the System – IP Setting for further info.)	
Wireless Basic Setting	Wireless Mode	AP
	Wireless Network Name (SSID)	JetWave3000_1 (WIFI 1) JetWave3000_2 (WIFI 2)
	Broadcast SSID	Enabled
	802.11 Mode	802.11G/N
	Data Rate	Auto
	(Refer to the Wireless – WLAN Settings – Basic Settings)	
Remote Settings	Remote Management Privacy	Telnet, SNMP, SNMP Trap, Email Alert
	Even Warning Type	WLAN association, Authentication fail, Configuration Changed
SNMP	Version	2
	Server Port:	161
	Get Community	Public
	Set Community	Private
	Trap Destination	0.0.0.0
	Trap Community	Public
Korenix View Utility	Device Search, IP Assign, Basic Tool, Wireless Panel	**Note:** While using Korenix View Utility to search the device, please connect to the Eth 2 (LAN).
Diagnostic CLI	Console Type	3-pin (Tx, Rx, GND) Refer to the appendix B, RS232 to 3-pin pin assignment.
	Baud Rate	115,200
	Parameter	N, 8, 1

⚠ **Warning:**

It is Important to change all the default settings of the Wireless AP, includes the User Name, Password, Default IP Address, Default SSID, SNMP Community Name and configure Wireless Security to secure your network.

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 3200/3400 Series is 192.168.10.1 (Eth 2 of JetWave 3420).

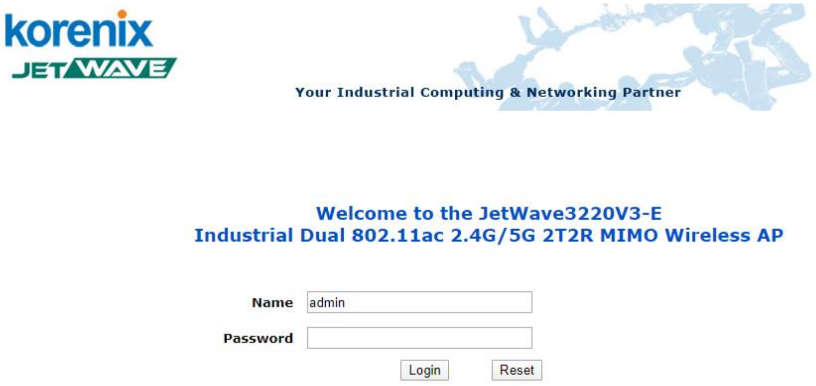
A Web browser on PC for configuration such as Microsoft Internet Explorer 6.0 or above, Google Chrome or Firefox.

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

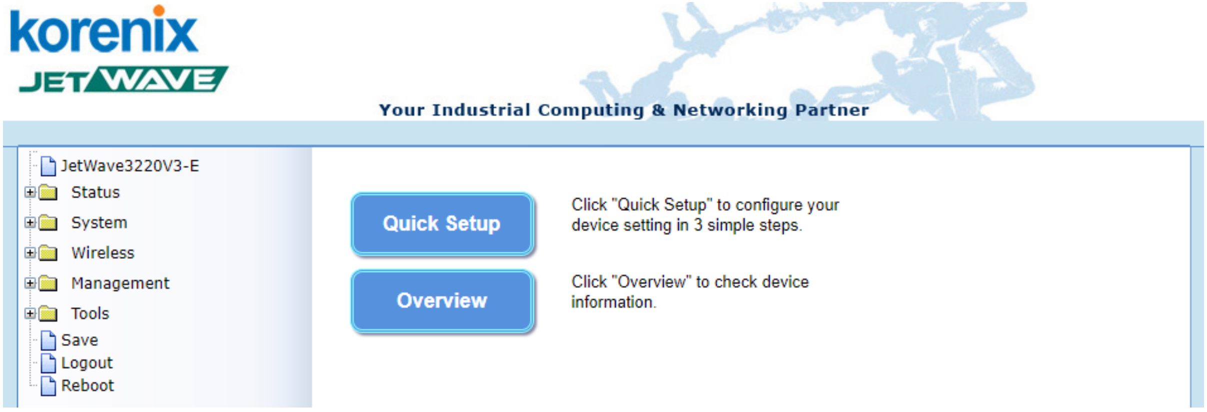


Welcome to the JetWave3220V3-E
Industrial Dual 802.11ac 2.4G/5G 2T2R MIMO Wireless AP

Name: admin
Password:

Figure – Web GUI 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**, **Wireless**, **Management**, **Tools**, **Device Front Panel, Save, Reboot** and **Logout**.



Click "Quick Setup" to configure your device setting in 3 simple steps.

Click "Overview" to check device information.

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. The firewall may stop the firmware upgrade, configuration backup and restore as well. 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 the connected port, the default Eth 1 and Eth 2 equipped with different IP Address.
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.

3.5 How to login the CLI

You can access the CLI (Command Line Interface) through 3-pin Diagnostic Console or Telnet.

3-pin Diagnostic Console:

There is one 3-pin Diagnostic console for out of band management. If you want to access the AP through the console, please assembly the console cable or purchase from our sales first.

Please attach RS-232 DB-9 connector to your PC COM port, connect another end to the 3-pin socket Console port located in the bottom side.

1. Go to Start -> Program -> Accessories -> Communication -> Hyper Terminal
2. Give a name to the new console connection.
3. Choose the COM name
4. Select correct serial settings. The serial settings of JetWave 3220v3/3420v3 series are as below:

   Baud Rate: 115,200 /

   Parity: None /

   Data Bit: 8 /

   Stop Bit: 1
5. After connected, you can see Switch login request.
6. Login the switch. The default username is “admin”, password, “admin”.

Telnet/SSH:

You can connect to the device by Telnet and the command lines are the same as what you see by RS232 console port. Below are the steps to open Telnet connection to the switch.

1. Go to Start -> Run -> cmd. And then press Enter
2. Type the Telnet 192.168.10.1 (or the IP address of the switch). And then press Enter

Note that the Telnet.exe file is not provided after Window 7. You can download it from Microsoft web site. Or you can use 3rd Party tool, for example the Putty.

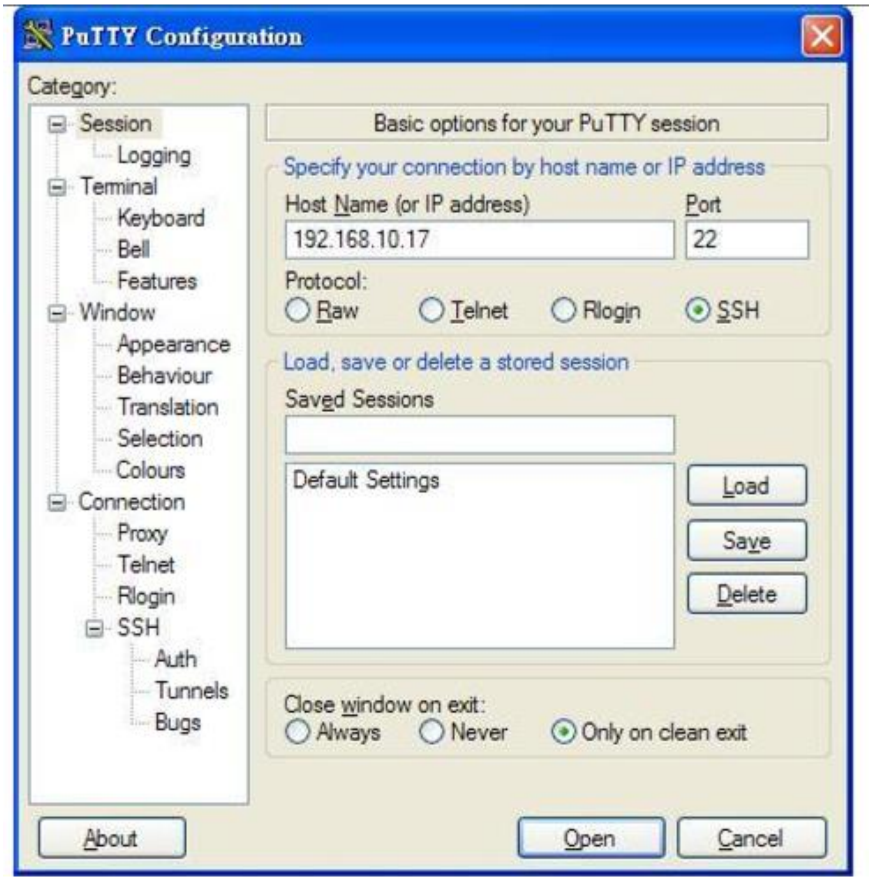
3rd Party tool:

Download PuTTY: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

The copyright of PuTTY is belonged to Putty. We don’t have any contract with them. Please follow the shareware policy of their company.

1. Open SSH Client/PuTTY In the Session configuration, enter the Host Name (IP Address of your device) and Port number (default = 22).

2. Choose the “Telnet” protocol. Then click on “Open” to start the Telnet session console.
3. If you want remote access the CLI securely, choose the “SSH” protocol. Then click on “Open” to start the SSH session console.
4. For SSH login: After click on Open, then you can see the cipher information in the popup screen. Press Yes to accept the Security Alert.
5. After few seconds, you can see the login screen of the device, the username/password is the same as the Web GUI (Default: admin/admin).



PuTTY Configuration

Basic options for your PuTTY session

Specify your connection by host name or IP address

Host Name (or IP address): 192.168.10.17

Port: 22

Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

Load, save or delete a stored session

Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

3.6 Discovery Utility – Korenix View Utility

Please download the latest Korenix View Utility from Korenix Web Support page.

The PC with Korenix View Utility can discover the AP/Gateway cross the IP subnet. But, if you want to do further configuration, the PC must be located in the same subnet with your AP/Gateway. Change the IP address of your PC or change the IP address of the AP/Gateway.

The chapter 5.3 introduces how to use Korenix View Utility.

Chapter 4

Web GUI Configuration

Chapter 4 Web GUI Configuration

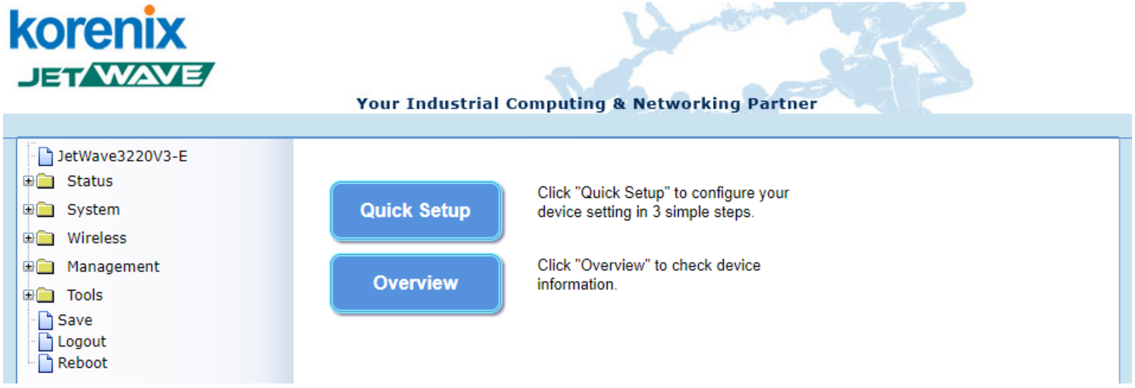
This chapter describes the Web GUI for Software Configuration.

4.1 Status

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

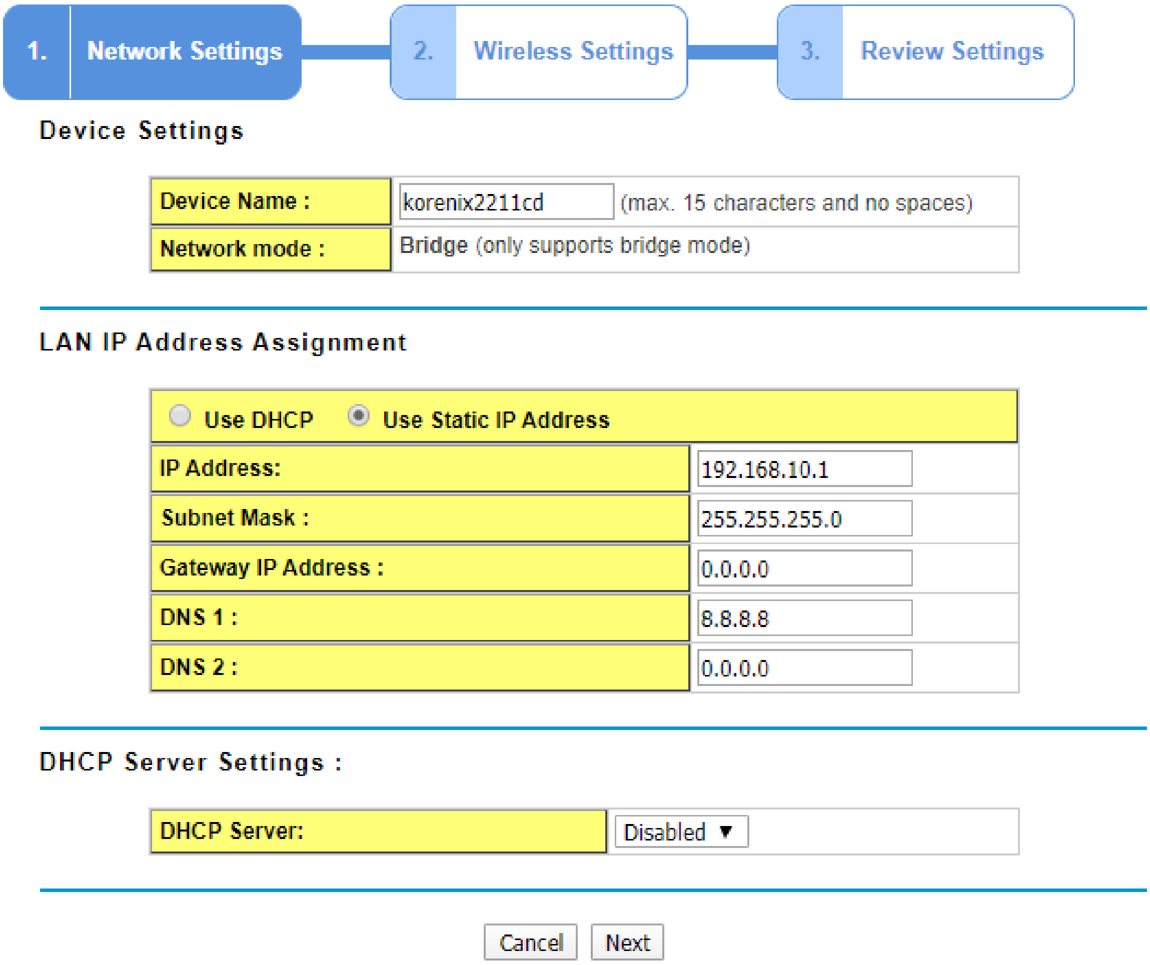
4.1.1 Quick Setup and Overview

Quick Setup page can is design for simple use case. User can complete WIFI setting without study complete user manual. Follow three steps below then can finish simple WIFI setting.



Click "Quick Setup" to configure your device setting in 3 simple steps.

Click "Overview" to check device information.



Device Settings

Device Name :	korenix2211cd (max. 15 characters and no spaces)
Network mode :	Bridge (only supports bridge mode)

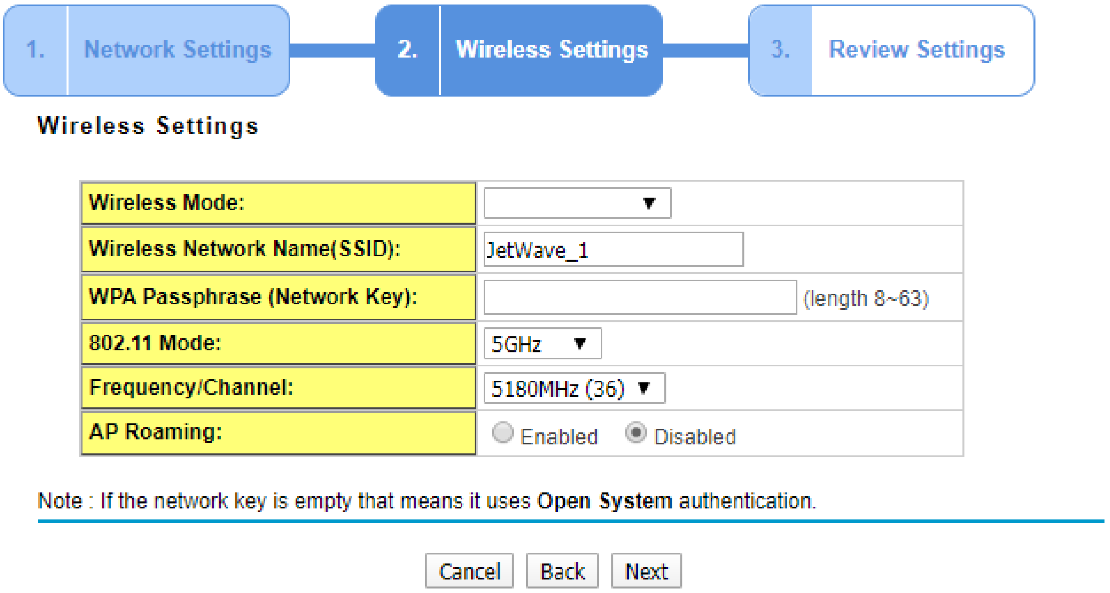
LAN IP Address Assignment

○ Use DHCP ● Use Static IP Address

IP Address:	192.168.10.1
Subnet Mask :	255.255.255.0
Gateway IP Address :	0.0.0.0
DNS 1 :	8.8.8.8
DNS 2 :	0.0.0.0

DHCP Server Settings :

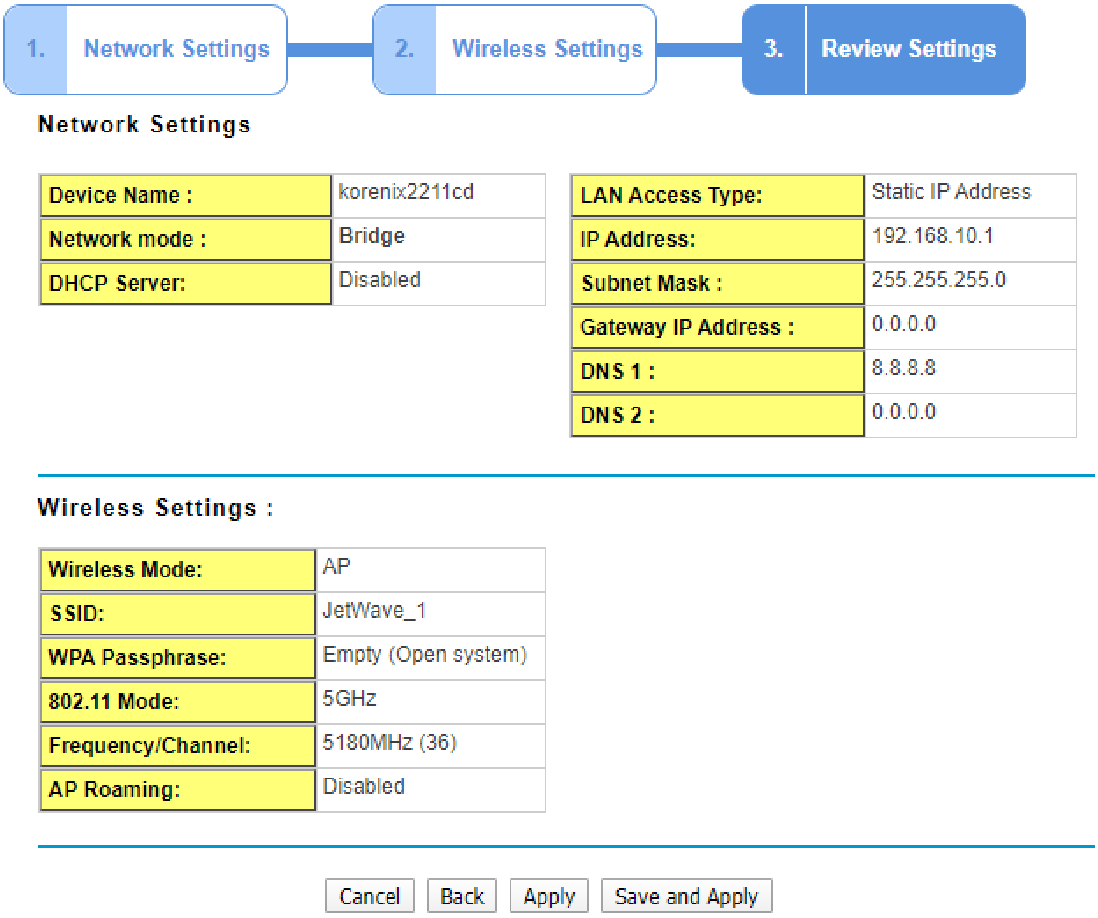
DHCP Server:	Disabled ▼



Wireless Settings

Wireless Mode:	▼
Wireless Network Name(SSID):	JetWave_1
WPA Passphrase (Network Key):	(length 8~63)
802.11 Mode:	5GHz ▼
Frequency/Channel:	5180MHz (36) ▼
AP Roaming:	○ Enabled ● Disabled

Note : If the network key is empty that means it uses **Open System** authentication.



Network Settings

Device Name :	korenix2211cd
Network mode :	Bridge
DHCP Server:	Disabled

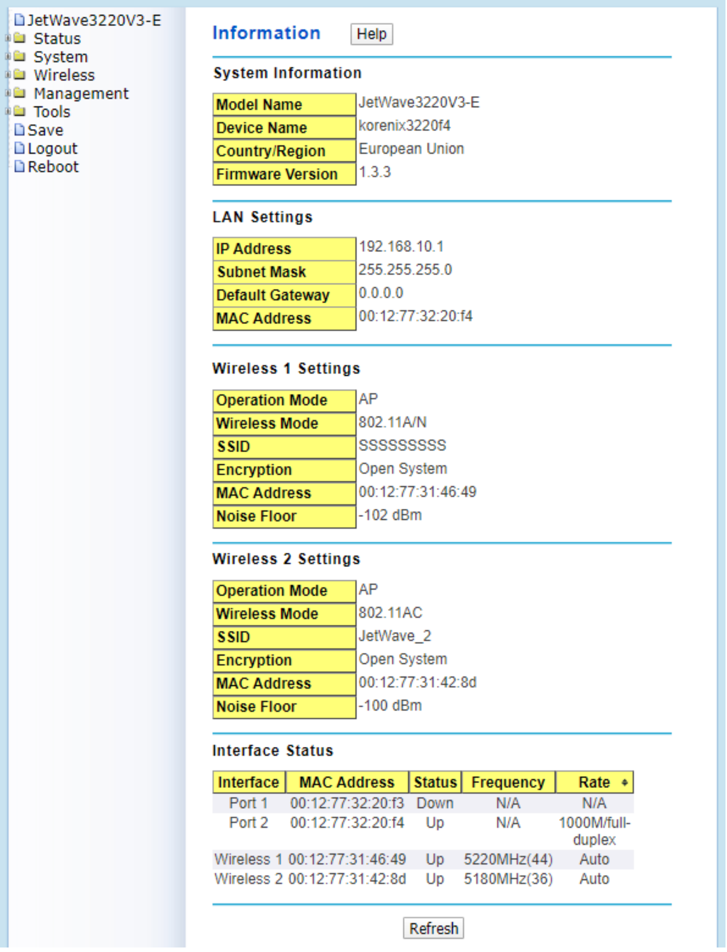
LAN Access Type:	Static IP Address
IP Address:	192.168.10.1
Subnet Mask :	255.255.255.0
Gateway IP Address :	0.0.0.0
DNS 1 :	8.8.8.8
DNS 2 :	0.0.0.0

Wireless Settings :

Wireless Mode:	AP
SSID:	JetWave_1
WPA Passphrase:	Empty (Open system)
802.11 Mode:	5GHz
Frequency/Channel:	5180MHz (36)
AP Roaming:	Disabled

Overview(Information)

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



System Information

Model Name	JetWave3220V3-E
Device Name	korenix3220f4
Country/Region	European Union
Firmware Version	1.3.3

LAN Settings

IP Address	192.168.10.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
MAC Address	00:12:77:32:20:f4

Wireless 1 Settings

Operation Mode	AP
Wireless Mode	802.11A/N
SSID	SSSSSSSSS
Encryption	Open System
MAC Address	00:12:77:31:46:49
Noise Floor	-102 dBm

Wireless 2 Settings

Operation Mode	AP
Wireless Mode	802.11AC
SSID	JetWave_2
Encryption	Open System
MAC Address	00:12:77:31:42:8d
Noise Floor	-100 dBm

Interface Status

Interface	MAC Address	Status	Frequency	Rate
Port 1	00:12:77:32:20:f3	Down	N/A	N/A
Port 2	00:12:77:32:20:f4	Up	N/A	1000M/full-duplex
Wireless 1	00:12:77:31:46:49	Up	5220MHz(44)	Auto
Wireless 2	00:12:77:31:42:8d	Up	5180MHz(36)	Auto

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.

Wireless 1 Settings: It shows the Operation Mode, Wireless Mode, SSID, Encryption, ACK Timeout, WMM State, Noise Floor of the Wireless 1. There are 2 Wireless Settings for JetWave 3220 dual radio models.

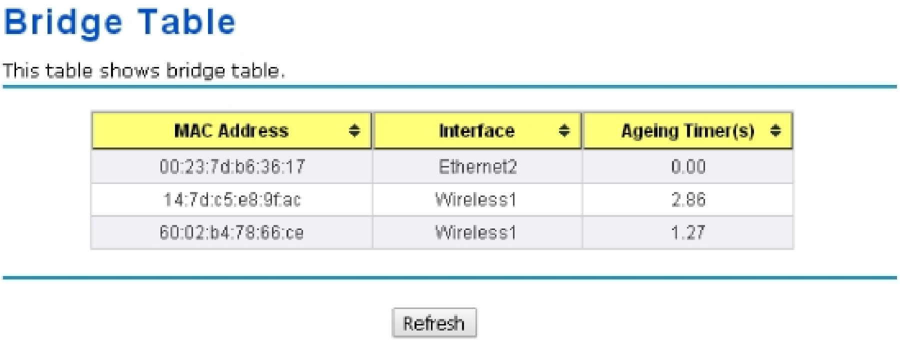
Interface Status: This table shows the Interface Name, MAC Address, Status, Frequency and Rate.

4.1.2 Network Flow

This page shows the packet counters for transmission and reception regarding the wireless interface(s).

4.1.3 Bridge Table

This table shows bridge table.



Bridge Table

This table shows bridge table.

MAC Address	Interface	Ageing Timer(s)
00:23:7d:b6:36:17	Ethernet2	0.00
14:7d:c5:e8:9f:ac	Wireless1	2.86
60:02:b4:78:66:ce	Wireless1	1.27

MAC Address: The MAC address of the connected device.

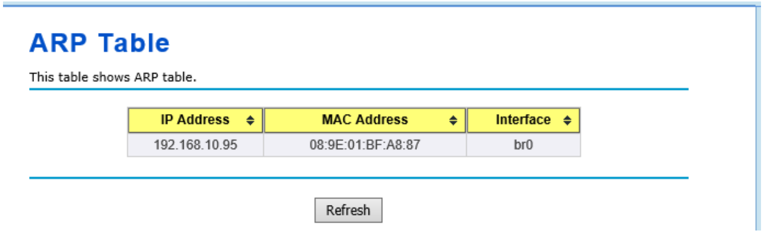
Interface: This field shows the interface which learnt the MAC Address.

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.



ARP Table

This table shows ARP table.

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

IP Address: The IP Address leant from the interface.

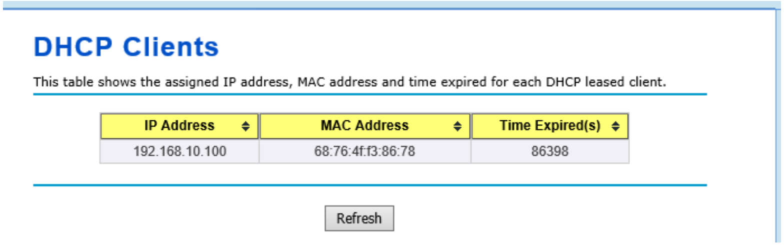
MAC Address: The MAC Address leant from the interface.

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.



DHCP Clients

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

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

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

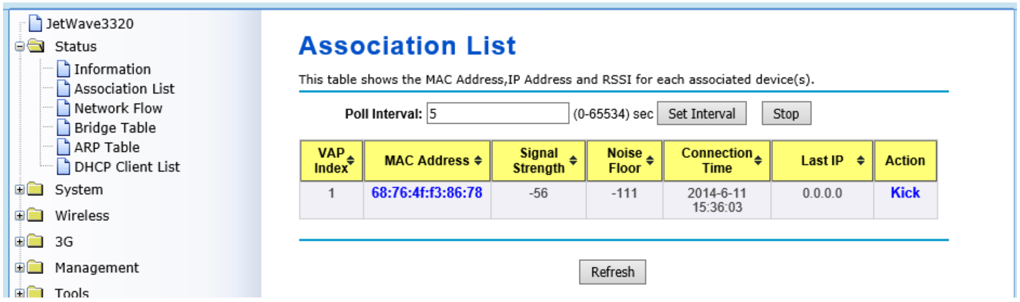
MAC Address: The MAC Address of the connected DHCP client device.

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.

4.1.6 Association List

This table shows the MAC Address, IP Address and RSSI for each associated devices.



Association List

This table shows the MAC Address,IP Address and RSSI for each associated device(s).

Poll Interval: 5 (0-65534) sec

VAP Index	MAC Address	Signal Strength	Noise Floor	Connection Time	Last IP	Action
1	68:76:4f:f3:86:78	-56	-111	2014-6-11 15:36:03	0.0.0.0	Kick

5 **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 new setting.

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

7 **Stop:** Stop polling the associated clients.

8 ====Entry Info===

9 **VAP Index:** Virtual AP Index number.

10 **MAC Address:** The MAC Address of the associated device.

11 **Signal Strength:** The signal strength of the associated device. The value can help you to see the connection quality of AP/WDS-AP and Client/WDS-Client.

12 **Noise Floor:** The Noise Floor of the associated device.

13 **Connection Time:** The time when the device connected to the AP.

14 **Last IP:** The last IP address it had.

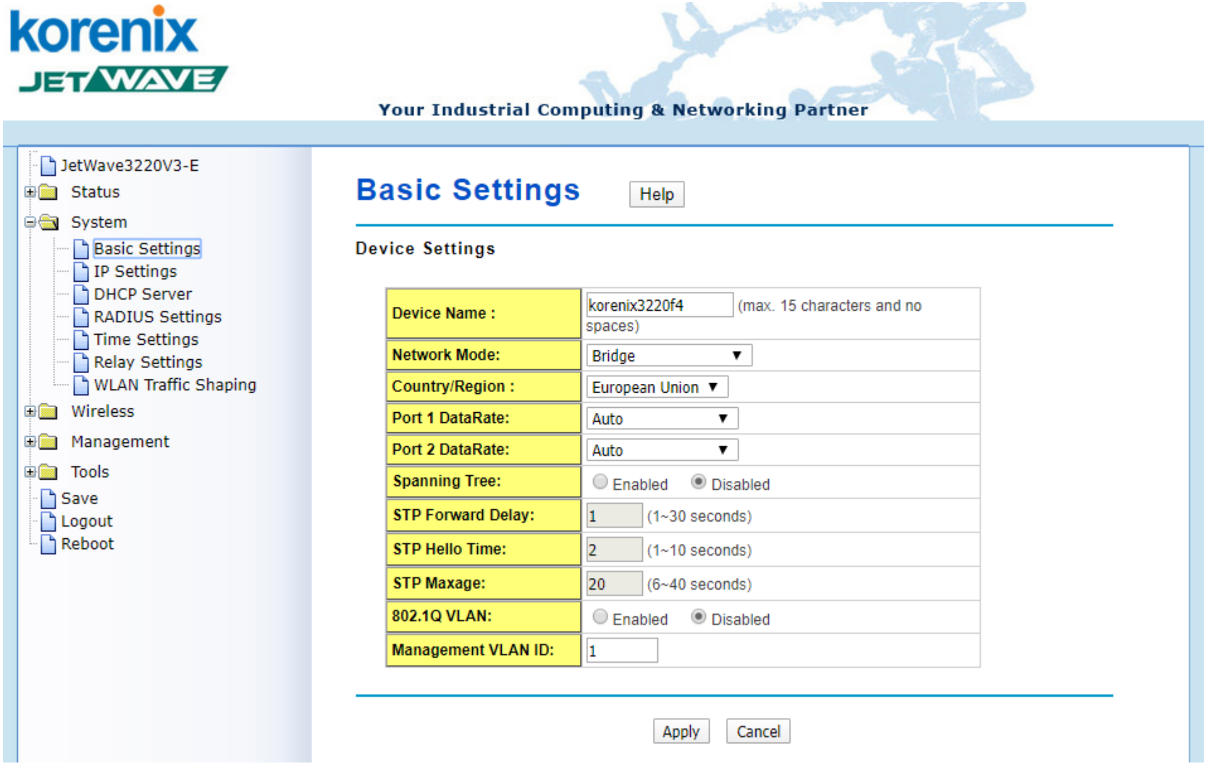
15 **Action – Kick:** This command allows you force Kick the associated client.

16 **Refresh:** The item helps you refresh the table manually.

4.2 System

For users who use the JetWave 3200 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 are introduced in below pages.



Basic Settings

Device Settings

Device Name :	korenix3220f4 (max. 15 characters and no spaces)
Network Mode:	Bridge ▼
Country/Region :	European Union ▼
Port 1 DataRate:	Auto ▼
Port 2 DataRate:	Auto ▼
Spanning Tree:	○ Enabled ● Disabled
STP Forward Delay:	1 (1~30 seconds)
STP Hello Time:	2 (1~10 seconds)
STP Maxage:	20 (6~40 seconds)
802.1Q VLAN:	○ Enabled ● Disabled
Management VLAN ID:	1

4.2.1 Basic Settings

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

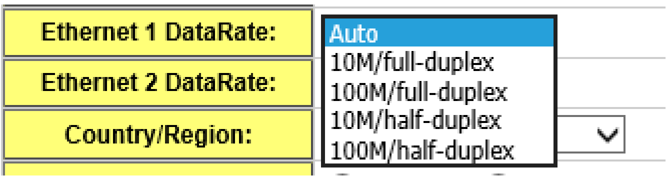
Device Name: User could give a name for identifying a particular access point here. It allows maximum 15 characters and no spaces.

Network Mode: There are 2 modes, Bridge and Router modes. The default setting of JetWave 3220 is Bridge mode. The default setting of JetWave 3420 is Router mode.

Bridge: When configured to Bridge mode, the AP acts as bridge to transmit/receive traffic between LAN (Eth 1 + Eth 2) to Wireless LAN. And there is only one IP address available for the system. **JetWave 3420 4G function do Not work under this mode.**

Router: When configured to Router mode, the AP acts as Router/IP Gateway, the Eth 1 and Eth 2 port will be separated to different network. The Wireless LAN and Eth 2 will be located within the same network. In JetWave 3420 default setting, the LAN/WLAN to 3G connection is working under Router mode as well.

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 1 DataRate: Auto

Ethernet 2 DataRate:

Country/Region:

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. The channel number may be different based on your country.

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.

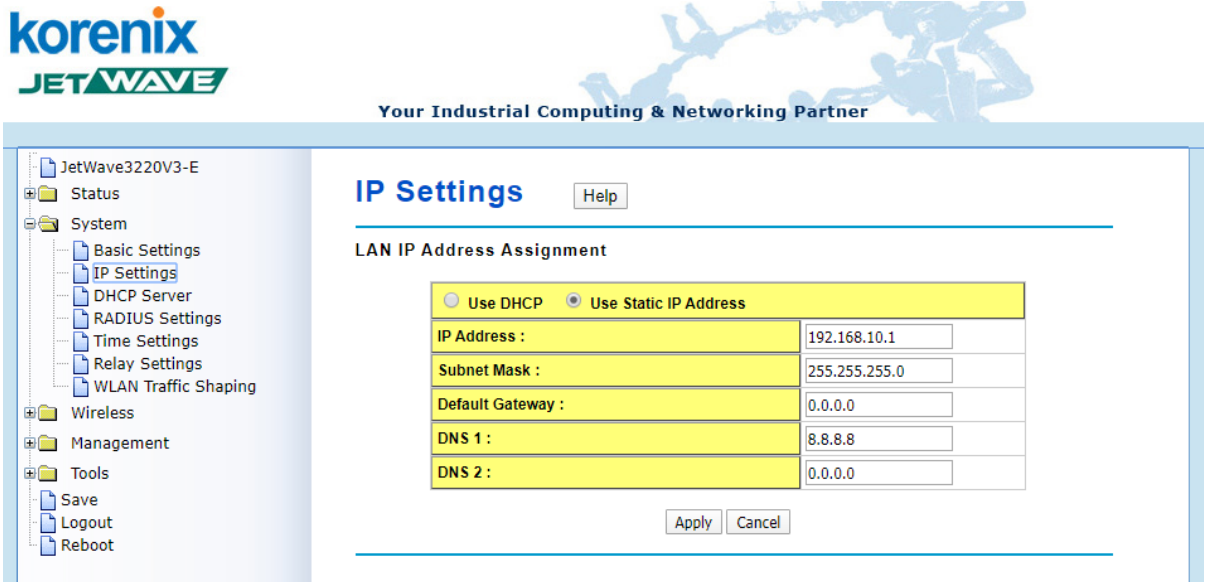
STP Forward Delay (1~30 Seconds): This is the Forward Delay value of the Spanning Tree protocol setting. The default value 1 is not comfort to 802.1D STP standard, however, it can shorten the topology change time. But, once you want to connect with other STP device, for example the management Ethernet switch, you must follow STP protocol value. The min. time is range from 4~30.

802.1Q VLAN: Enable or Disable 802.1Q VLAN. With 802.1Q enabled, the packet will attach the 1Q VLAN tag inside. To assign the VLAN ID for each AP profile, you should enable 802.1Q VLAN first. Here is the global VLAN Enable setup.

Management VLAN ID: This is the management VLAN ID of the device. Only the client within the same management VLAN can access the device's management interface. To enable Management VLAN ID, you must enable "802.1Q VLAN" and assign "VLAN ID" for each AP profile first.

4.2.2 IP Settings

Use this page to configure the IP related parameters for **WAN (Eth 1)** and **LAN (Eth 2)** interfaces. Here you may change the setting for IP address, subnet mask, Default Gateway, DNS, Static IP or DHCP…etc.



IP Settings

LAN IP Address Assignment

○ Use DHCP ● Use Static IP Address

IP Address :	192.168.10.1
Subnet Mask :	255.255.255.0
Default Gateway :	0.0.0.0
DNS 1 :	8.8.8.8
DNS 2 :	0.0.0.0

WAN Settings:

WAN Access Type: Static IP

IP Address: Once **Static IP** is selected, the IP Address field allows you to set the device's WAN IP address manually.

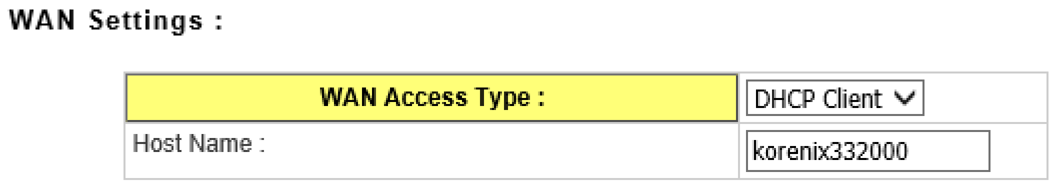
Subnet Mask: This is the subnet mask address for your WAN interface. Set the IP subnet mask manually.

Default Gateway: Set the default gateway IP address manually.

DNS 1 & 2: The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Your ISP will provide you with at least one DNS Server IP Address. If you wish to use another, enter that IP Address in **DNS 2** field.

WAN Access Type: DHCP Client.

Once **DHCP Client** is selected, the WAN interface acts as the DHCP Client and automatically search the DHCP



WAN Settings :

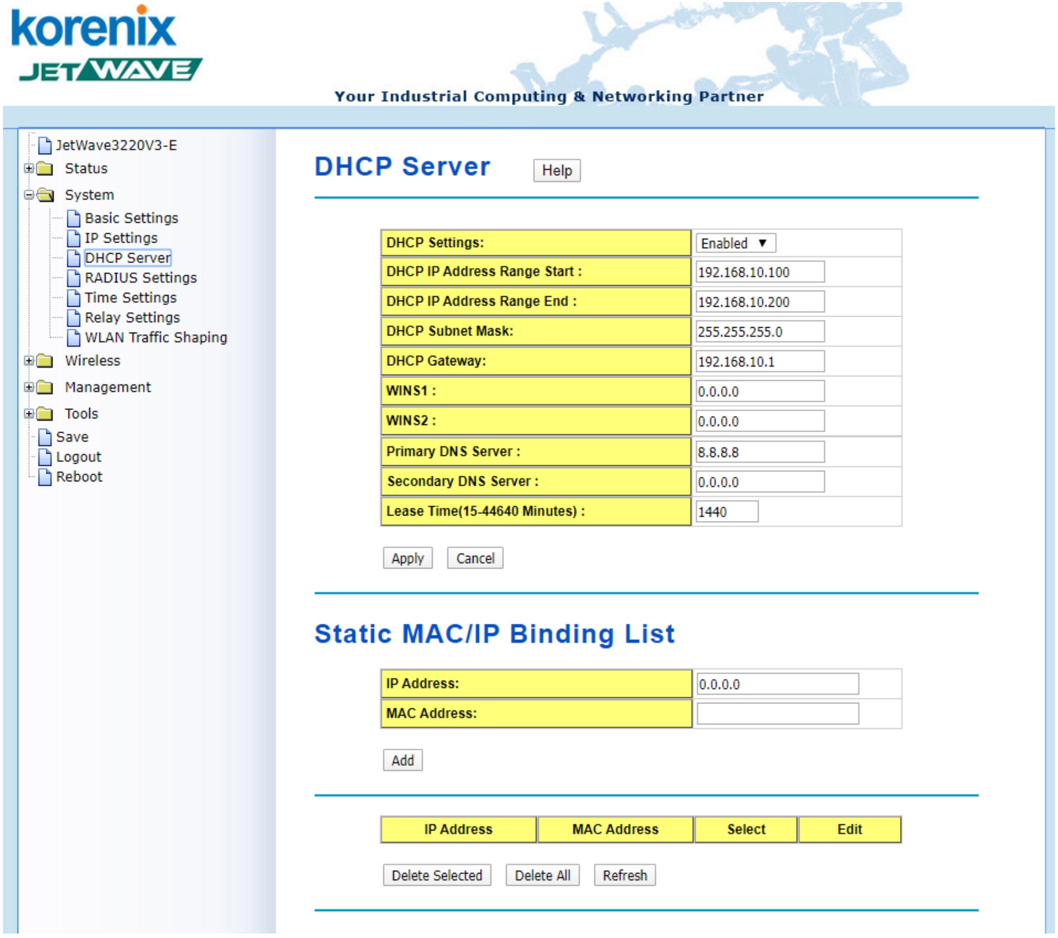
WAN Access Type :	DHCP Client
Host Name :	korenix332000

LAN Settings:

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

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

DHCP Server: Enabled / Disabled



DHCP Server

DHCP Settings:	Enabled ▼
DHCP IP Address Range Start :	192.168.10.100
DHCP IP Address Range End :	192.168.10.200
DHCP Subnet Mask:	255.255.255.0
DHCP Gateway:	192.168.10.1
WINS1 :	0.0.0.0
WINS2 :	0.0.0.0
Primary DNS Server :	8.8.8.8
Secondary DNS Server :	0.0.0.0
Lease Time(15-44640 Minutes) :	1440

Static MAC/IP Binding List

IP Address:	0.0.0.0
MAC Address:	

IP Address	MAC Address	Select	Edit

<u>DHCP Server Setting</u>:

In Router mode, you can enable DHCP Server to assign IP address to DHCP clients. And you should define the address pool by configuring the Start IP and End IP. DHCP server will allocate IP address dynamically from the pool. The device allows you to 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.

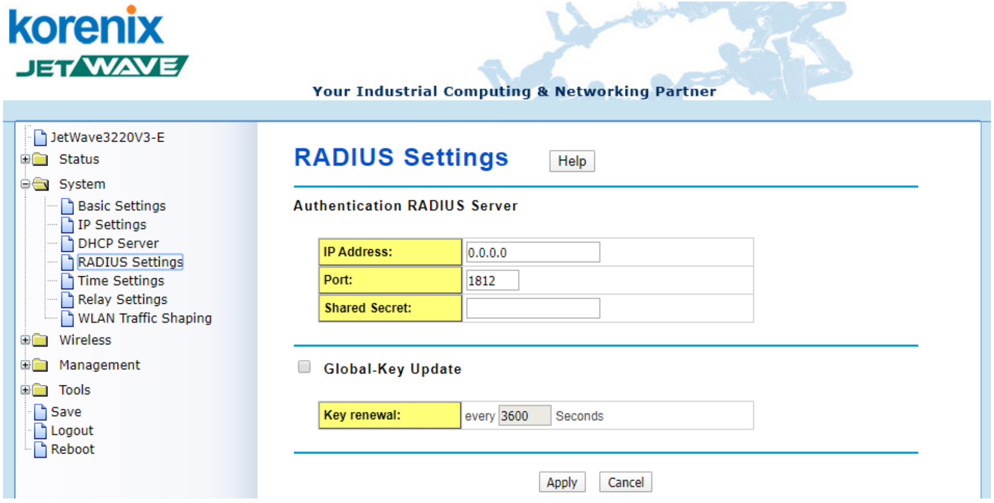
<u>Enable DHCP Relay</u>:

If you already have DHCP server in other subnet, you can "**Disable" DHCP Server** and then check "**Enable DHCP Relay**" to redirect the DHCP request to the DHCP Server. Assign the Server IP address in "**DHCP Server IP"** field 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.



RADIUS Settings

Authentication RADIUS Server

IP Address:	0.0.0.0
Port:	1812
Shared Secret:	

□ Global-Key Update

Key renewal:	every 3600 Seconds

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.

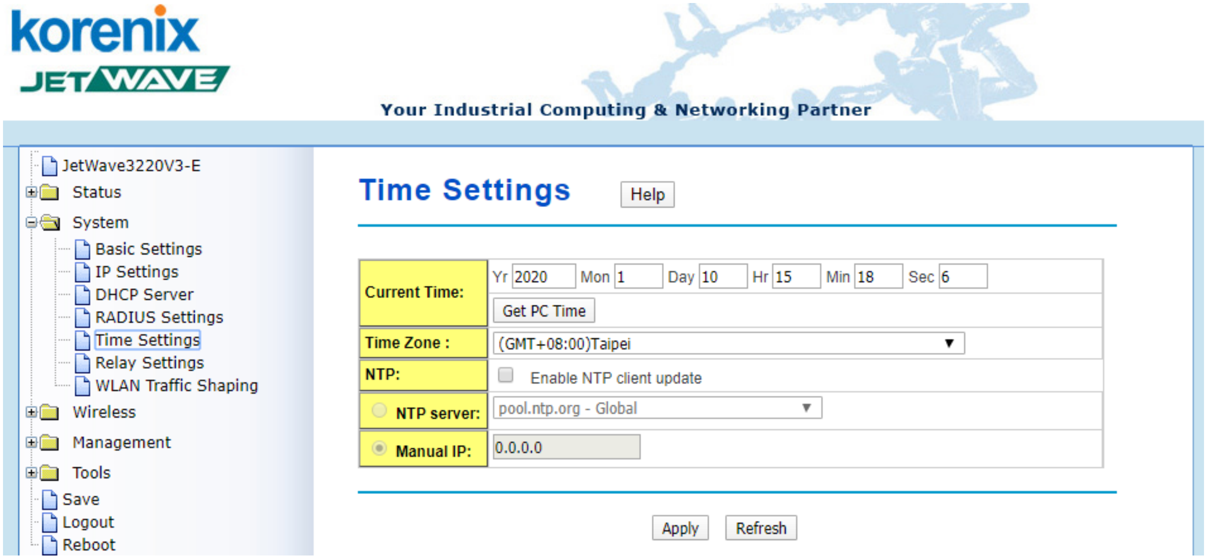
Global-Key Update: Check this option and specify the time interval between two global-key updates.

Re-authentication Time: 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.



Time Settings

Current Time:	Yr 2020 Mon 1 Day 10 Hr 15 Min 18 Sec 6
Time Zone :	(GMT+08:00)Taipei
NTP:	□ Enable NTP client update
○ NTP server:	pool.ntp.org - Global
● Manual IP:	0.0.0.0

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

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

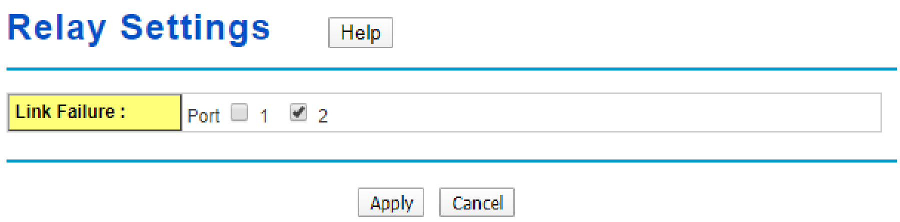
NTP: You can select **"Enable NTP client update"** in this page, then the NTP feature will be activated and synchronize from the remote time server.

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

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

4.2.5 Relay Settings

You can bind the selected events to Relay Output. While the event is activated, the Relay output is changed to "Open" status, the RO LED will turn on to alarm the administrators/technician.



Relay Settings

Link Failure :	Port □ 1 ☑ 2

Power Failure: You can bind the power failure event with Relay Output. There are 3 types power input, you can choose one/multiple events as the power failure event.

DI: The **DI** is presented to **Digital Input**. There is one DI design in the bottom of the device. You can bind the Relay Output event to the DI here.

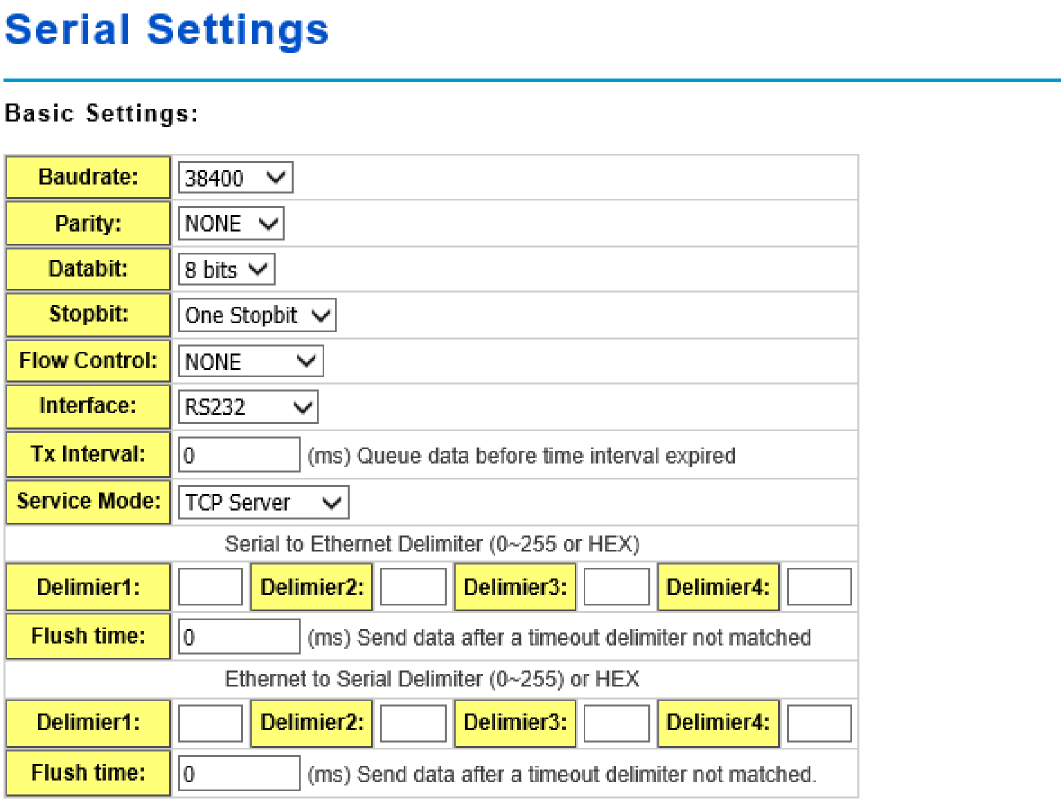
<u>Link Failure:</u> You can bind the Ethernet port failure event with Relay output. Select the Port 1, 2 or 1+2 as the power failure event.

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

4.2.6 Serial Settings

Use this page to configure the **Serial Settings**. The JetWave 3420 series is equipped with one RS-232/422/485 3-in-1 Serial port. It supports TCP Server/Client and UDP for remote connection. This page allows you to configure the Serial interface’s parameters.

Basic Settings: This page allows you configure basic settings of the Serial port.



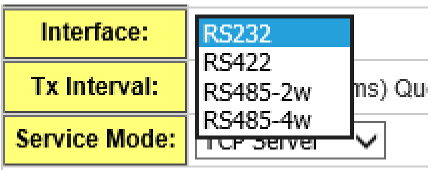
Serial Settings

Basic Settings:

Baudrate:	38400						
Parity:	NONE						
Databit:	8 bits						
Stopbit:	One Stopbit						
Flow Control:	NONE						
Interface:	RS232						
Tx Interval:	0	(ms) Queue data before time interval expired					
Service Mode:	TCP Server						
Serial to Ethernet Delimiter (0~255 or HEX)							
Delimier1:		Delimier2:		Delimier3:		Delimier4:	
Flush time:	0	(ms) Send data after a timeout delimiter not matched					
Ethernet to Serial Delimiter (0~255) or HEX							
Delimier1:		Delimier2:		Delimier3:		Delimier4:	
Flush time:	0	(ms) Send data after a timeout delimiter not matched.					

Serial port Settings: You can select the “**<u>Baudrate</u>**”, “**<u>Parity</u>**”, “**<u>Databit</u>**”, “**<u>Stopbit</u>**” and “**<u>Flow control</u>**” settings from the dropdown list.

<u>Interface:</u> Manually choose and change the interface type. The serial port supports the RS232, RS422, RS485-2w, RS485-4w, you can select either one from the dropdown list.



<u>Tx Interval:</u> Configure the Tx Interval time, the system will queue the transmit data before time interval expired. The time unit is millisecond.

Service mode: You can select TCP Server, TCP Client, and UDP listening.

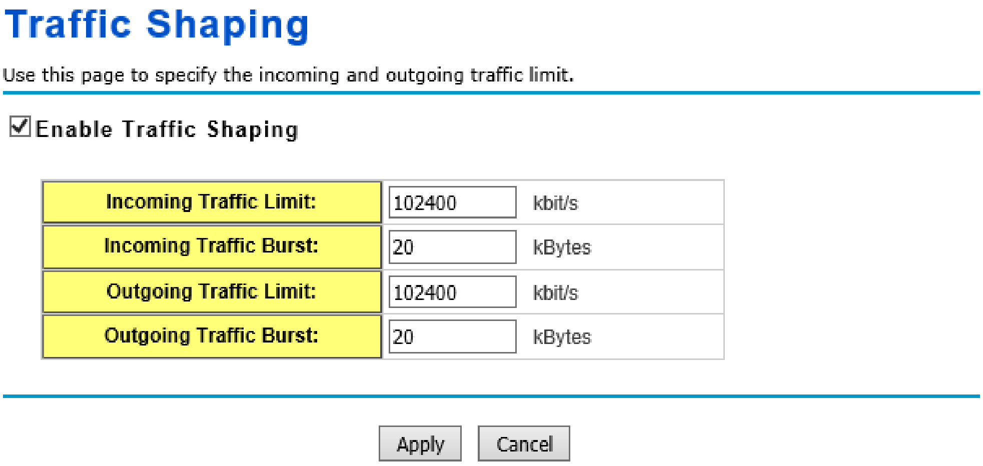
Serial to Ethernet/ Ethernet to Serial Delimiter: Configure the **Delimiter** and **Flush time** (a timeout that the delimiter not matched) setting for Serial to Ethernet or Ethernet to Serial transmission. There are up to 4 delimiters can be configured here. After the Delimiter is configured, the data will be stored in the buffer until hit the Delimiter or the Flush time timeout.

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

4.2.7 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.



Traffic Shaping

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

☑ Enable Traffic Shaping

Incoming Traffic Limit:	102400	kbit/s
Incoming Traffic Burst:	20	kBytes
Outgoing Traffic Limit:	102400	kbit/s
Outgoing Traffic Burst:	20	kBytes

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

4.2.8 Outbound Firewall

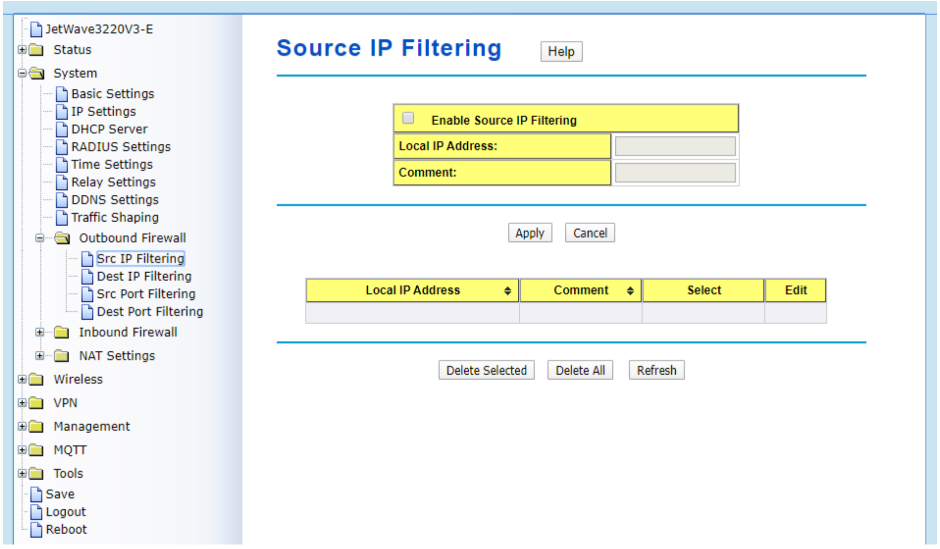
Use the "**Firewall Settings**" pages to configure the Firewall setting. There are different types firewall settings, you can enable the setting, configure the rules, check the table you configured and Delete Select/All rules.

"**Src IP Filtering**": Source IP addresses Filtering from your LAN to WAN through the gateway.

"**Dest IP Filtering**": Destination IP addresses Filtering from the LAN to WAN through the gateway.

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

“**Dest Port Filtering**”: Destination Ports Filtering from the LAN to WAN through the gateway.



Source IP Filtering

☐ Enable Source IP Filtering

Local IP Address:

Comment:

Local IP Address	Comment	Select	Edit

- **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.

- **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 “**Local IP Address**” and “**Comment**” (note for the entry) and then press “**Apply**” to activate the settings.

- **Source Port Filtering**

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

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

- **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 "**Local Port Number**" and "**Comment**" (note for the entry) and then press "**Apply**" to activate the settings.

4.2.9 Inbound Firewall

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

Enable Inbound Firewall: After enabling the inbound firewall, it means that all of the IP addresses from the Internet can NOT access the gateway.

Remote Management Exception: You can select which exceptions that you want to exclude from these: Web, Telnet, SSH and SNMP.

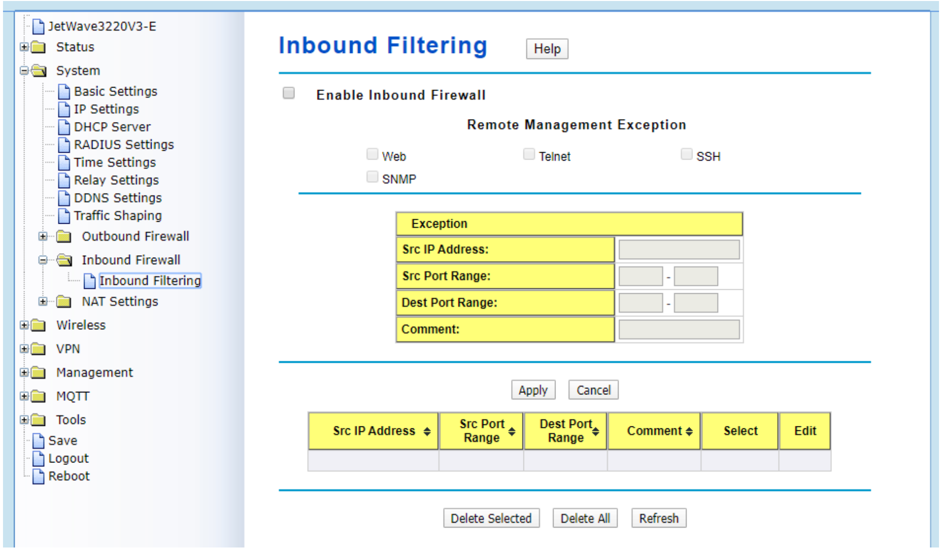
Src IP Address: This entry allows you to configure the source IP address from the Internet.

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

Dest Port Range: This is 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: Comment for this rule. Maximum of 64 characters.

Click the Apply button to apply the configuration changes.



Inbound Filtering

□ Enable Inbound Firewall

Remote Management Exception

□ Web □ Telnet □ SSH
□ SNMP

Exception	
Src IP Address:	
Src Port Range:	-
Dest Port Range:	-
Comment:	

Src IP Address	Src Port Range	Dest Port Range	Comment	Select	Edit

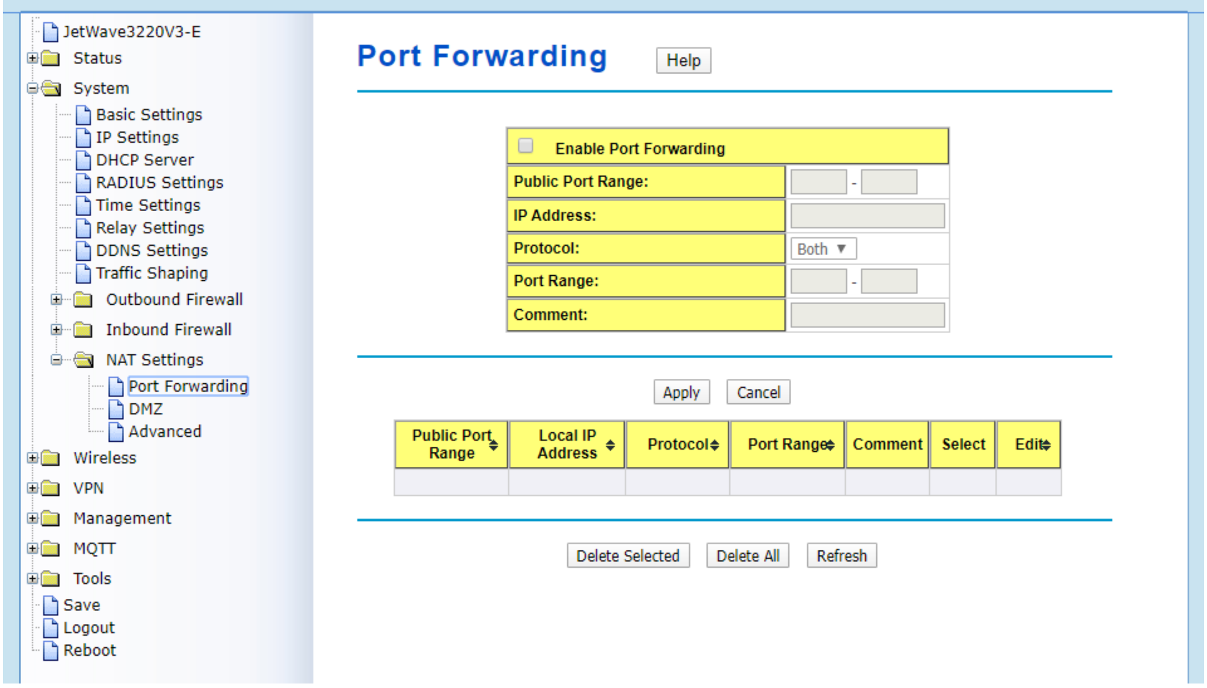
4.2.10 NAT Settings

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.



Port Forwarding

□ Enable Port Forwarding	
Public Port Range:	-
IP Address:	
Protocol:	Both ▼
Port Range:	-
Comment:	

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

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

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

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

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

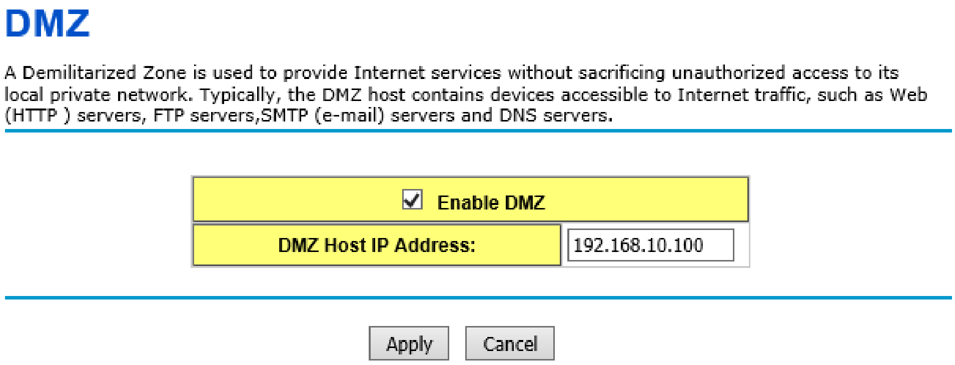
Port Range: Configure the port range of the LAN, the traffic from the public port will be redirected to these port.

Comment: Add information of the entry.

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

- **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.



DMZ

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

☑ Enable DMZ

DMZ Host IP Address: 192.168.10.100

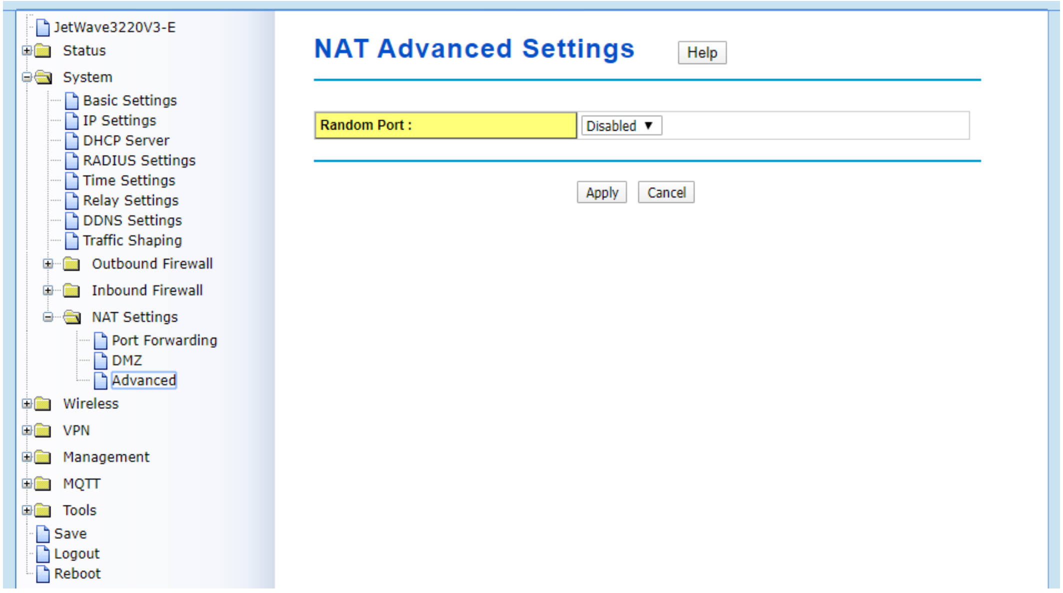
Select “**Enable DMZ**” and assign the IP address of the “**DMZ Host IP Address**”. This is the DMZ computer’s IP address. If you configure the DMZ function for your office network, please make sure this is agreed by the IT administrator.

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

Randomize NAT source port mapping. When enabled, port mapping is randomized.

Random Port: Enable/Disable NAT random port function.

Click the Apply button to apply the configuration changes.



NAT Advanced Settings

Random Port : Disabled

4.3 Wireless

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

JetWave 3220 supports dual WIFI radios, you must configure **Wireless 1** and **Wireless 2**.

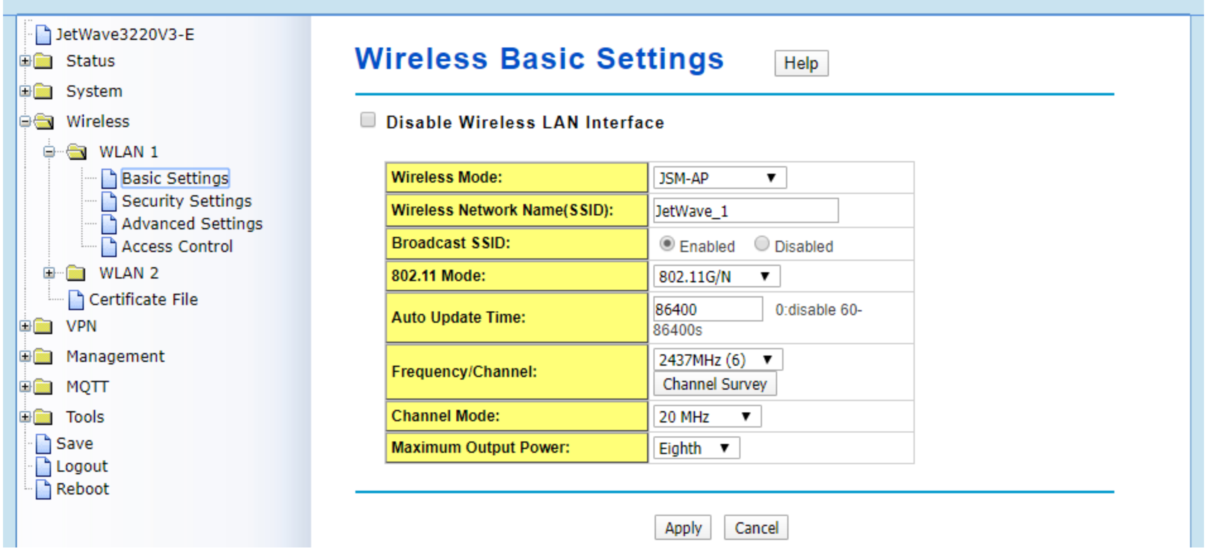
JetWave 3420 support one WIFI and one 4G radio, you must configure WIFI features here and go to 3G/4G LTE page to configure other settings.

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 3420. The Wireless and 4G settings are separated to different feature set.

4.2.1 Wireless Basic Setting (JetWave 3220v3)

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



Wireless Basic Settings

☐ Disable Wireless LAN Interface

Wireless Mode:	JSM-AP
Wireless Network Name(SSID):	JetWave_1
Broadcast SSID:	● Enabled ○ Disabled
802.11 Mode:	802.11G/N
Auto Update Time:	86400 0:disable 60-86400s
Frequency/Channel:	2437MHz (6)
Channel Mode:	20 MHz
Maximum Output Power:	Eighth

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.

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.

JSM-AP: In JSM-AP mode, the JSM-AP will sync settings with JSM-Client automatic when config changed. The sync range include SSID,802.11 Mode,BandWidth,Authentication(Open or WPA2PSK),Encryption,WPA Passphrase.

JSM-Client: In JSM-Client mode, the JSM-Client will connect a Best signal JSM-AP and sync configuration with same band automatically. When JSM-AP config changed, the JSM client will change configuration at same time.

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.

Brocadcast 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 several wireless starndards. You can select appropriate wireless mode. Different band has different settings as below:

802.11A Only

802.11B Only

802.11G Only

802.11A/N

802.11G/N

802.11AC

Auto Update Time: In JSM-AP mode, support the item to start Channel Survey automatically.

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.

Extension Channel: Specify extension (secondary) channel bonded to current operating channel of the AP.

Scan Mode: In JSM-Client mode,if the client can not search the JSM AP and the Scan Mode is All Band. The system will change 802.11mode and try to search JSM AP automatically.

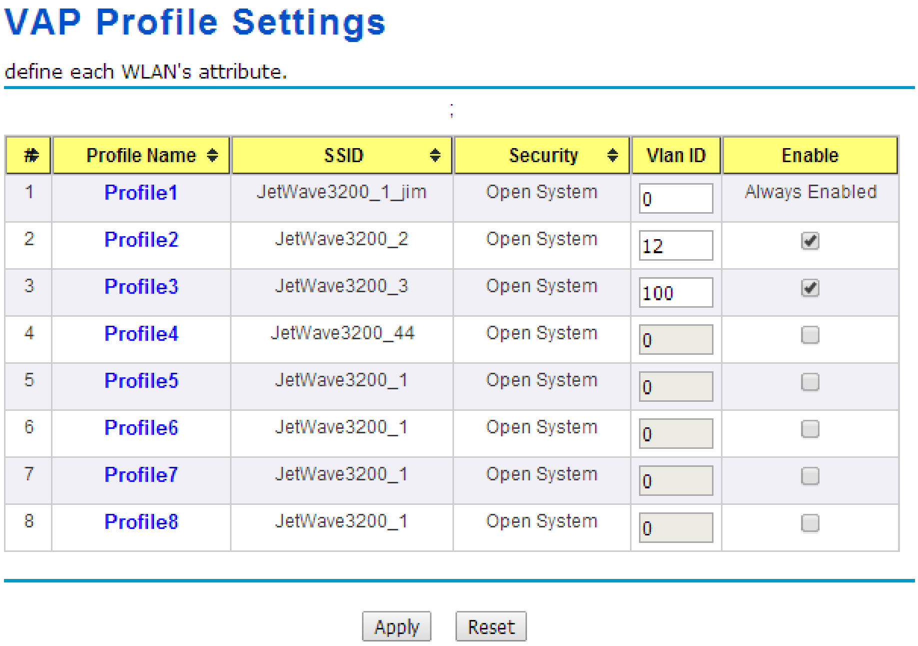
Channel Mode: Specify the bandwidth for wireless transmission.

Channel Survey: In AP mode,you can click the button to find the best channel and choice it automatically. *remind: The list will be cleared when the wireless mode or 802.11 mode setting changed.

Maximum Output Power: 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.

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.

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. Click the Apply button to apply the configuration changes.



VAP Profile Settings

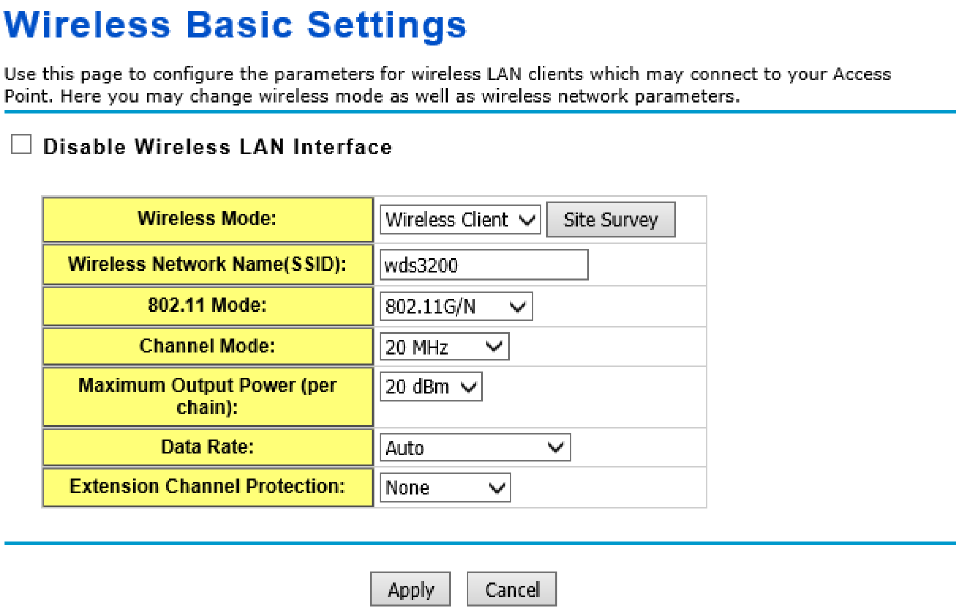
define each WLAN's attribute.

;

#	Profile Name ⬍	SSID ⬍	Security ⬍	Vlan ID	Enable
1	Profile1	JetWave3200_1_jim	Open System	0	Always Enabled
2	Profile2	JetWave3200_2	Open System	12	☑
3	Profile3	JetWave3200_3	Open System	100	☑
4	Profile4	JetWave3200_44	Open System	0	☐
5	Profile5	JetWave3200_1	Open System	0	☐
6	Profile6	JetWave3200_1	Open System	0	☐
7	Profile7	JetWave3200_1	Open System	0	☐
8	Profile8	JetWave3200_1	Open System	0	☐

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.



Wireless Basic Settings

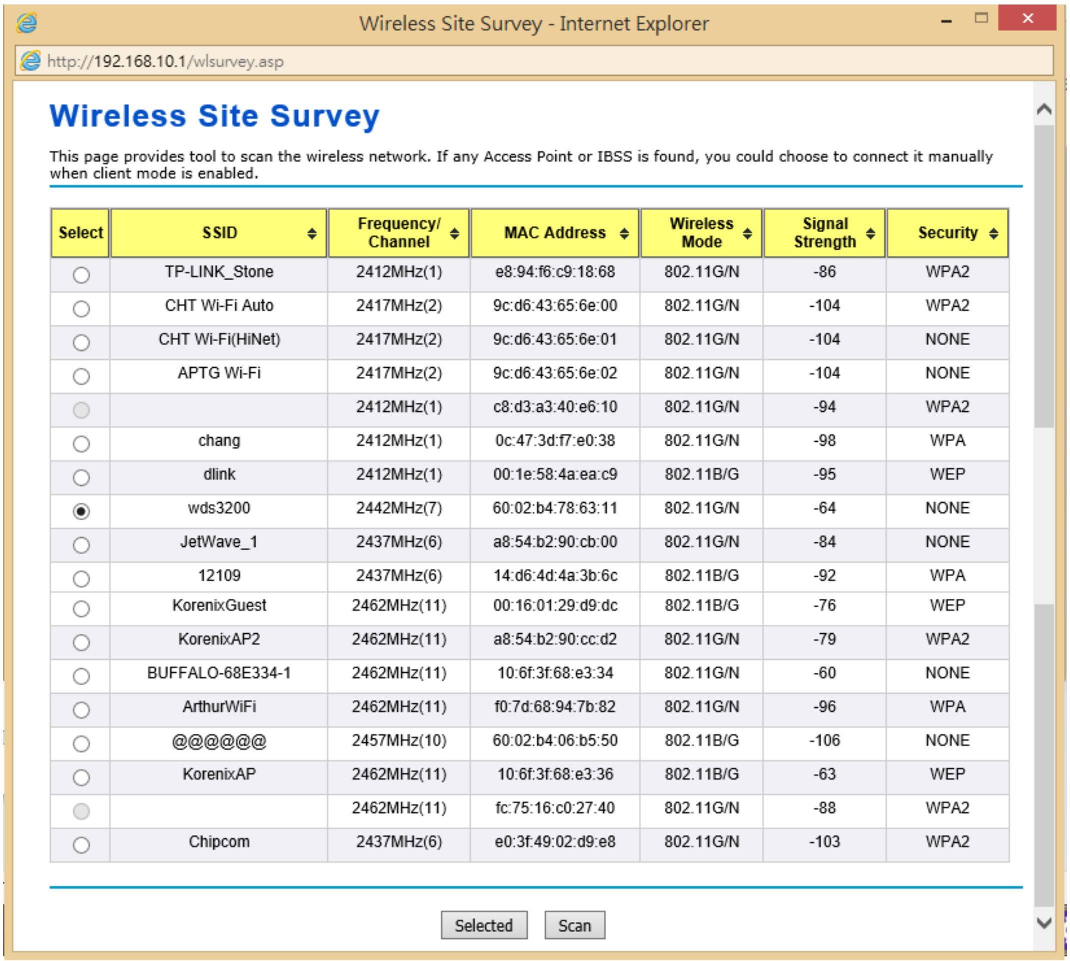
Use this page to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless mode as well as wireless network parameters.

☐ Disable Wireless LAN Interface

Wireless Mode:	Wireless Client ⌄
Wireless Network Name(SSID):	wds3200
802.11 Mode:	802.11G/N ⌄
Channel Mode:	20 MHz ⌄
Maximum Output Power (per chain):	20 dBm ⌄
Data Rate:	Auto ⌄
Extension Channel Protection:	None ⌄

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

In below figure, you can find the **SSID: wds3200** 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.



Wireless Site Survey - Internet Explorer
http://192.168.10.1/wlsurvey.asp

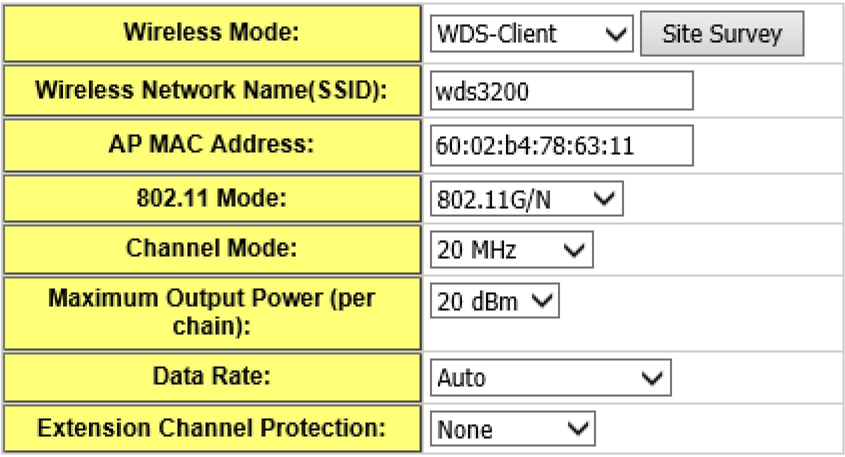
Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

Select	SSID	Frequency/ Channel	MAC Address	Wireless Mode	Signal Strength	Security
○	TP-LINK_Stone	2412MHz(1)	e8:94:f6:c9:18:68	802.11G/N	-86	WPA2
○	CHT Wi-Fi Auto	2417MHz(2)	9c:d6:43:65:6e:00	802.11G/N	-104	WPA2
○	CHT Wi-Fi(HiNet)	2417MHz(2)	9c:d6:43:65:6e:01	802.11G/N	-104	NONE
○	APTG Wi-Fi	2417MHz(2)	9c:d6:43:65:6e:02	802.11G/N	-104	NONE
○		2412MHz(1)	c8:d3:a3:40:e6:10	802.11G/N	-94	WPA2
○	chang	2412MHz(1)	0c:47:3d:f7:e0:38	802.11G/N	-98	WPA
○	dlink	2412MHz(1)	00:1e:58:4a:ea:c9	802.11B/G	-95	WEP
●	wds3200	2442MHz(7)	60:02:b4:78:63:11	802.11G/N	-64	NONE
○	JetWave_1	2437MHz(6)	a8:54:b2:90:cb:00	802.11G/N	-84	NONE
○	12109	2437MHz(6)	14:d6:4d:4a:3b:6c	802.11B/G	-92	WPA
○	KorenixGuest	2462MHz(11)	00:16:01:29:d9:dc	802.11B/G	-76	WEP
○	KorenixAP2	2462MHz(11)	a8:54:b2:90:cc:d2	802.11G/N	-79	WPA2
○	BUFFALO-68E334-1	2462MHz(11)	10:6f:3f:68:e3:34	802.11G/N	-60	NONE
○	ArthurWiFi	2462MHz(11)	f0:7d:68:94:7b:82	802.11G/N	-96	WPA
○	@@@@@@	2457MHz(10)	60:02:b4:06:b5:50	802.11B/G	-106	NONE
○	KorenixAP	2462MHz(11)	10:6f:3f:68:e3:36	802.11B/G	-63	WEP
○		2462MHz(11)	fc:75:16:c0:27:40	802.11G/N	-88	WPA2
○	Chipcom	2437MHz(6)	e0:3f:49:02:d9:e8	802.11G/N	-103	WPA2

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 Mode:	WDS-Client ▾ Site Survey
Wireless Network Name(SSID):	wds3200
AP MAC Address:	60:02:b4:78:63:11
802.11 Mode:	802.11G/N ▾
Channel Mode:	20 MHz ▾
Maximum Output Power (per chain):	20 dBm ▾
Data Rate:	Auto ▾
Extension Channel Protection:	None ▾

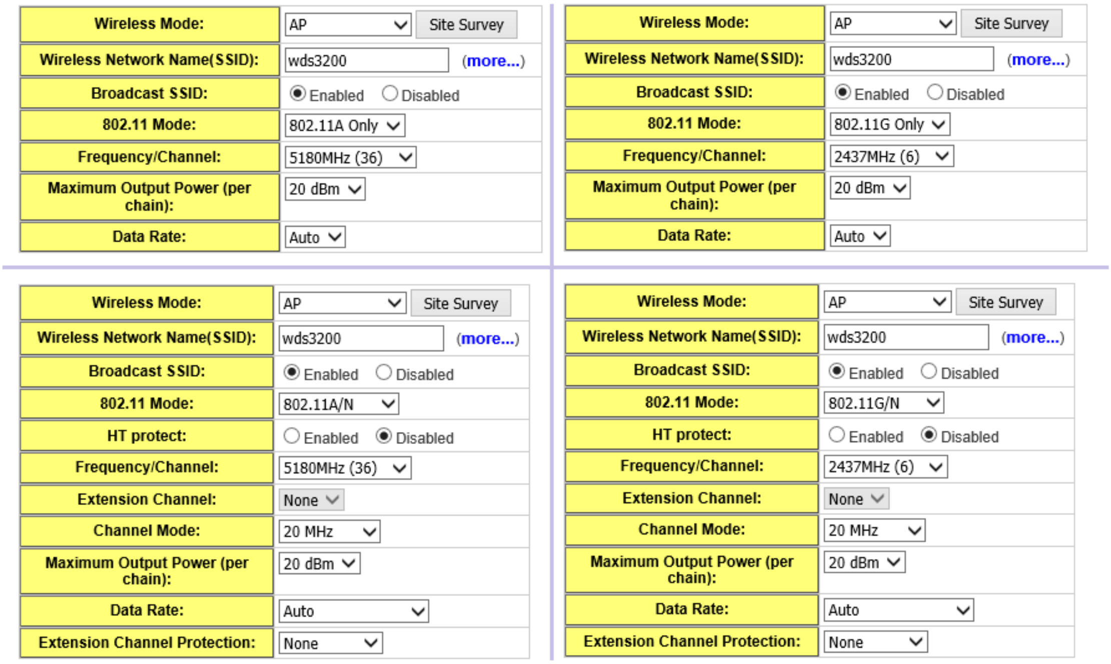
Primary Interface: You can select "Wlan 1" or "Wlan 2" as the primary interface. Wlan 1 is the default primary interface.

Signal Threshold(dbm): You can assign the signal threshold value, this value is the signal quality between the Redundant AP and Client. You can check the current value of the association list or configure it depends on the field test or experience. Once the signal threshold of primary interface is lower than the value you assigned, the backup interface will be activated. The default value is -60dbm, this is an medium signal quality.

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 802.11ac/a/g. You can also select 802.11A Only, 802.11G only, 801.11A/N and 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:	802.11A Only
Frequency/Channel:	5180MHz (36)
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 Only
Frequency/Channel:	2437MHz (6)
Maximum Output Power (per chain):	20 dBm
Data Rate:	Auto

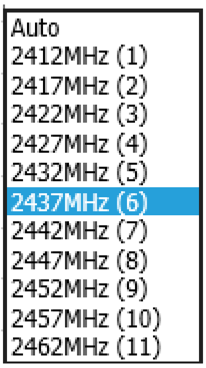
Wireless Mode:	AP Site Survey
Wireless Network Name(SSID):	wds3200 (more...)
Broadcast SSID:	● Enabled ○ Disabled
802.11 Mode:	802.11A/N
HT protect:	○ Enabled ● Disabled
Frequency/Channel:	5180MHz (36)
Extension Channel:	None
Channel Mode:	20 MHz
Maximum Output Power (per chain):	20 dBm
Data Rate:	Auto
Extension Channel Protection:	None

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 802.11ac mode, wireless client can be divided into HT STA and Non-HT STA, among which the one with HT protect enabled gets higher throughput.

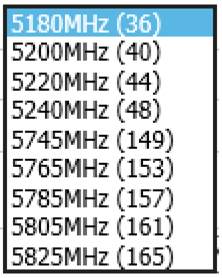
Frequency/Channel: Channel varies much as the available band differs from country to country. Select a proper operating channel in the drop-down list according to your situation.

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)

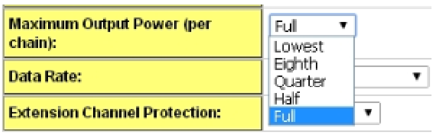
802.11A/N



5180MHz (36)
5200MHz (40)
5220MHz (44)
5240MHz (48)
5745MHz (149)
5765MHz (153)
5785MHz (157)
5805MHz (161)
5825MHz (165)

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

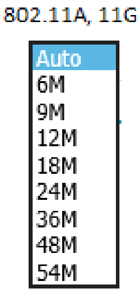
The 802.11A and 802.11A/N are 5.8G band, this product support Band 1 (36, 40, 44, 48) and Band 4 (149, 153, 157, 161, 167)

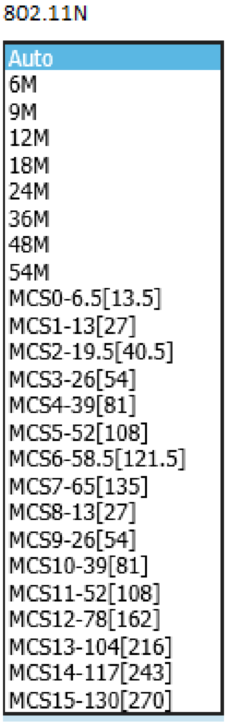


Maximum Output Power (per chain):	Full Lowest Eighth Quarter Half Full
Data Rate:	
Extension Channel Protection:	

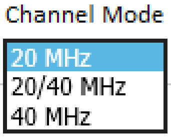
Maximum Output Power (per chain): Specify the signal transmission power. The higher the output power is, the wider the signal can cover, but the power consumption will be greater accordingly. Usually “**Full**” with proper antenna is preferred.

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.

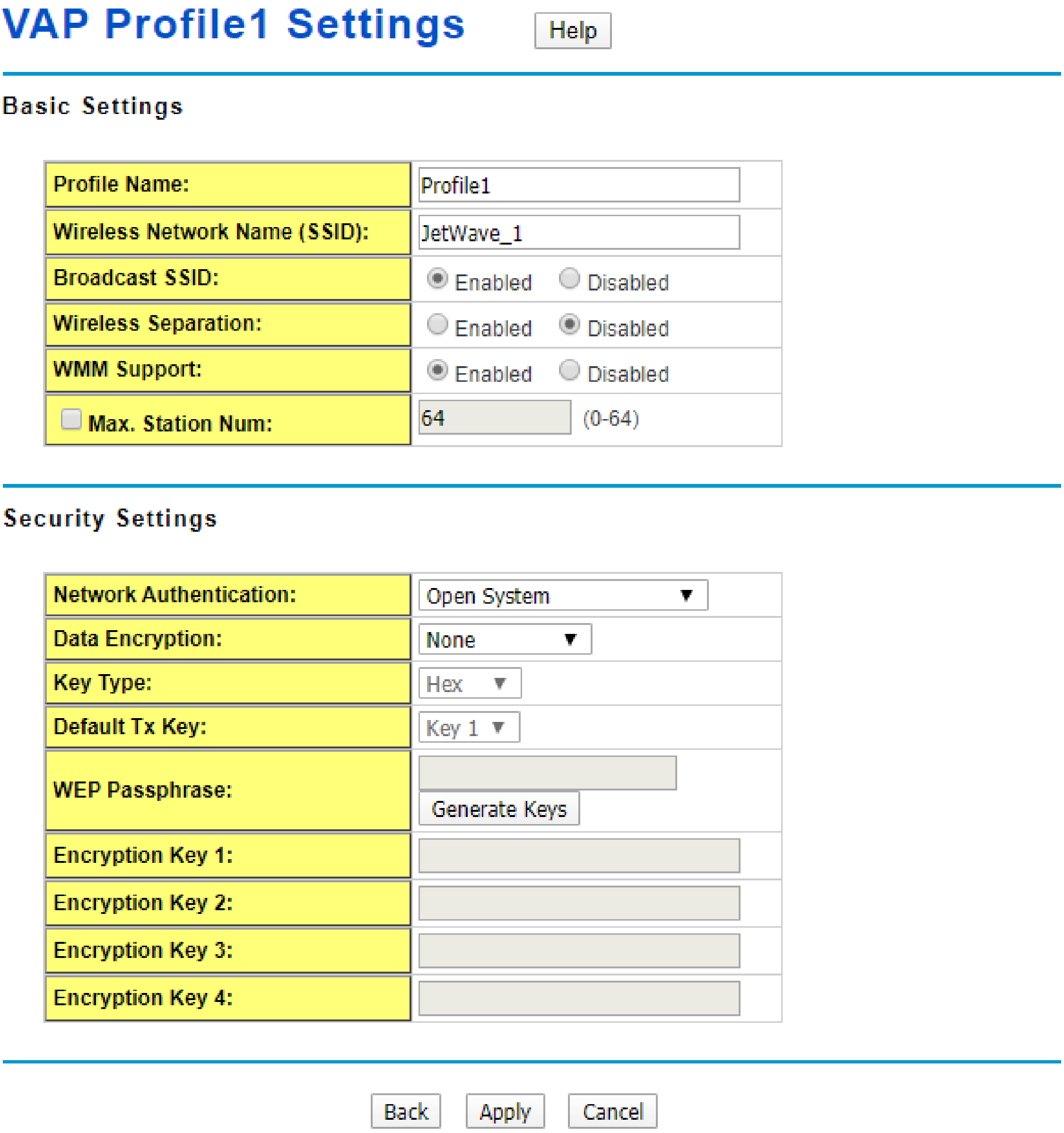


Channel Mode: Two levels are available: 20MHz and 20/40MHz. The latter one can enhance the data rate more effectively, but takes more bandwidth, thus cause potential interference.

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.

4.2.2 Wireless Security Setting

The page allows you configure the Virtual AP’s basic setting and Security Settings.



VAP Profile1 Settings

Basic Settings

Profile Name:	Profile1
Wireless Network Name (SSID):	JetWave_1
Broadcast SSID:	● Enabled ○ Disabled
Wireless Separation:	○ Enabled ● Disabled
WMM Support:	● Enabled ○ Disabled
□ Max. Station Num:	64 (0-64)

Security Settings

Network Authentication:	Open System
Data Encryption:	None
Key Type:	Hex
Default Tx Key:	Key 1
WEP Passphrase:	Generate Keys
Encryption Key 1:	
Encryption Key 2:	
Encryption Key 3:	
Encryption Key 4:	

Basic Setting

Profile Name: The profile name of the settings.

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

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.

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.

Max. Station Num: In Wireless AP mode, you can define the maximum amount of wireless clients allowed to be connected. The maximum client of the system is 64. The most user access at the same time may cause system busy and the performance becomes lower. It is suggested to assign the value depends on how much bandwidth your client generally need, and totally bandwidth suggest is under 250Mbps for TCP based data transmission.

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-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.

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.

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.

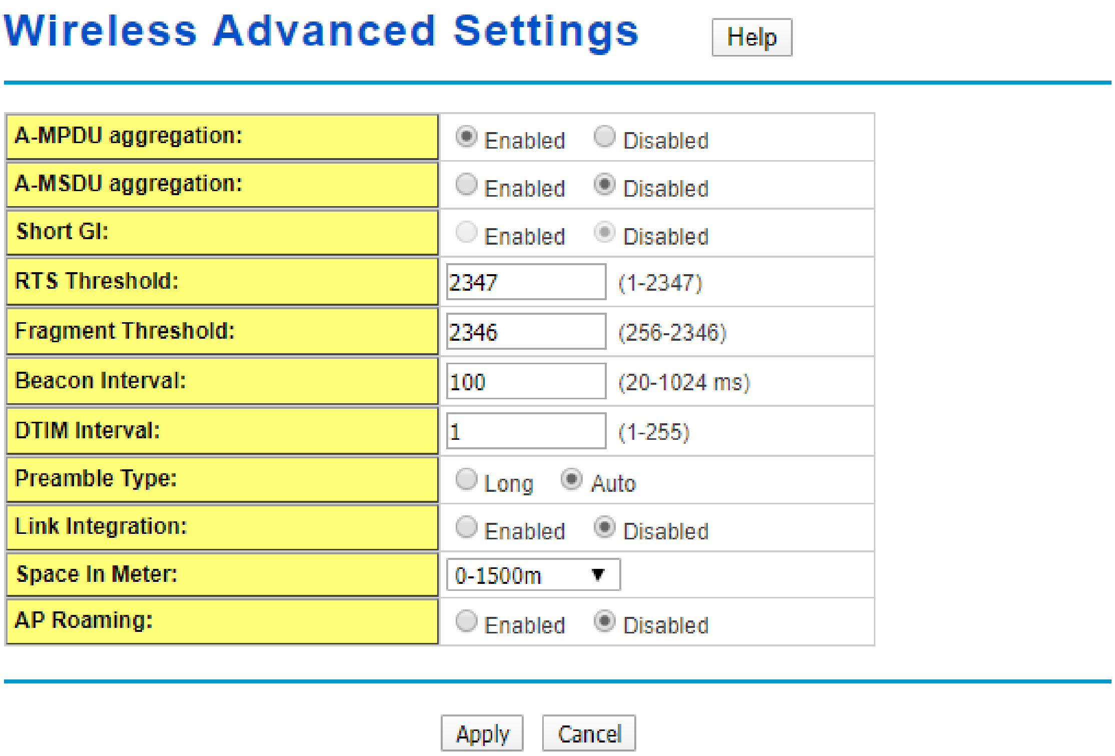
Press **"Apply"** to activate the setting.

✎**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!

4.2.3 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.



Wireless Advanced Settings

A-MPDU aggregation:	● Enabled ○ Disabled
A-MSDU aggregation:	○ Enabled ● Disabled
Short GI:	○ Enabled ● Disabled
RTS Threshold:	2347 (1-2347)
Fragment Threshold:	2346 (256-2346)
Beacon Interval:	100 (20-1024 ms)
DTIM Interval:	1 (1-255)
Preamble Type:	○ Long ● Auto
Link Integration:	○ Enabled ● Disabled
Space In Meter:	0-1500m ▼
AP Roaming:	○ Enabled ● Disabled

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 802.11ac 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.

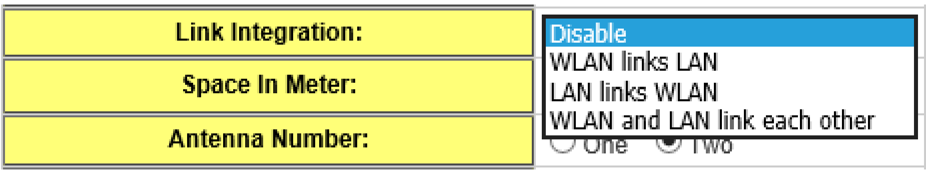
DTIM Interval: DTIM, which stands for Delivery Traffic Indication Message, is contained in the data packets. It is for enhancing the wireless transmission efficiency. The default is set to 1. Enter a value between 1 and 255.

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.



Link Integration:	Disable WLAN links LAN LAN links WLAN WLAN and LAN link each other
Space In Meter:	
Antenna Number:	○ One ● Two

Disable: Disable the Link Integration.

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

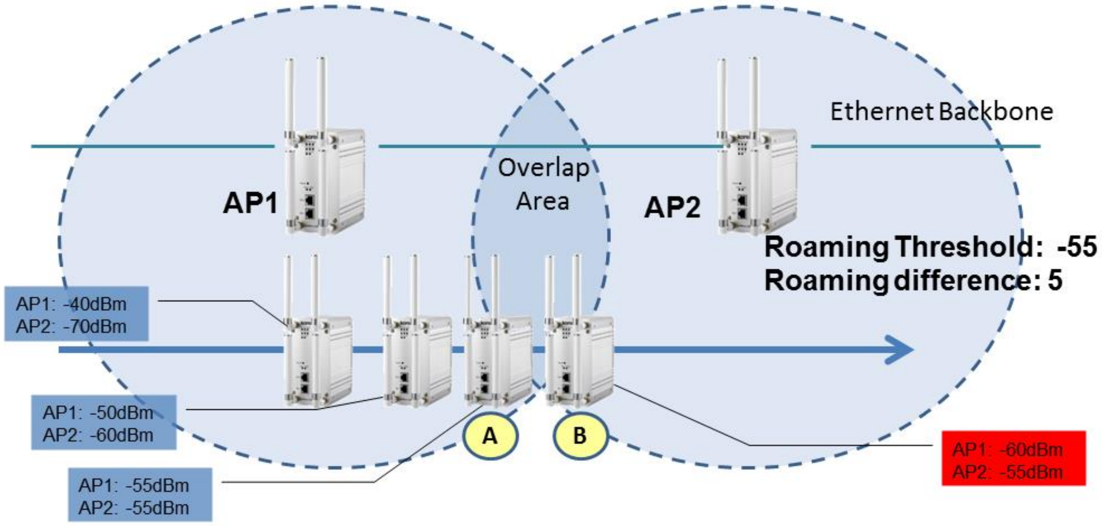
LAN links WLAN: Single direction only while the LAN Ethernet port failure, the binding WLAN radio will be shut down.

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

Space in Meter: To decrease the chances of data retransmission at long distance, the AP/Gateway can automatically adjust proper ACK timeout value by specifying distance of the two nodes. This is very important especially for long distance transmission. Correct Space in Meter helps to get better response time and performance.

Antenna Number: The setting allows you configure One for 1T1R SISO or Two for 2T2R MIMO. The default value is Two. While you change it to one, please connect the antenna to the first antenna of the radio, for example the Antenna 1-1 or 2-1.

Roaming: This is the setting to enable **Client Based Fast Roaming**. The Client Based Fast Roaming is a non-AP controller type fast roaming, it helps the wireless client (must Korenix Wireless Client) find the new AP with 100ms roaming time.



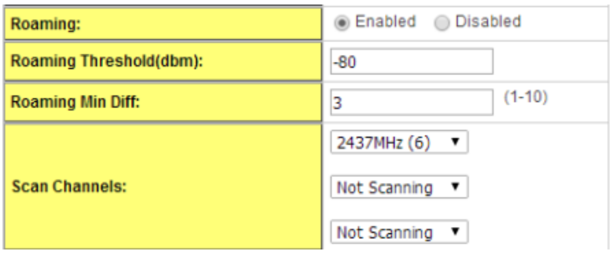
While the signal value in A = Roaming Threshold, the AP starts Fast Roaming Mechanism.

While the signal difference in B is higher than the roaming difference, the new AP will be selected.

After the roaming is enabled, some of the new setting will appear in below and you must enter the value.

Roaming: You can enable or disable the Fast Roaming feature here.

Roaming Threshold(dbm): While there are some Fast Roaming APs, the roaming threshold means when the client will start switch to new AP from the connected AP.



Roaming:	● Enabled ○ Disabled
Roaming Threshold(dbm):	-80
Roaming Min Diff:	3 (1-10)
Scan Channels:	2437MHz (6) ▼ Not Scanning ▼ Not Scanning ▼

Roaming Min Diff: In multiple APs overlapping area, the “Roaming Min Diff” is a value similar to the delay time. Only while the signal strength difference between the connected AP and New

AP is lower than the value, the AP will be switched.

Scan Channels:.This is the setting to configure what is the target scan channels.

Ping Watchdog: Under Wireless Client mode, the item support to create a ping connection with the specific ip address. If the connection lost. The system will restart wifi client to try restore the connection.

IP Address: The specific ip address for ping watchdog.

Failure CountThe Clinet will be restarted if the ping packets lost over the count

Mac Clone: Under Wireless Client or JSM-Client mode, this feature allows the client to clone and use the MAC address of the device connected to the LAN. Auto:Client will collect the mac address from LAN packets to replace wireless mac address. Static:Client shares the assigned MAC address with multiple devices connected to the LAN. This allows for multiple devices to connect to the AP via the LAN and only one of them needs to be assigned a MAC address.

Mac Clone Static Address:Specifies the static wireless MAC address for the device.

AP Roaming: Under AP mode, AP will kick out the wireless clients if the RSSI of client is lower than setting of AP Roaming Threshold.

AP Roaming Threshold: The RSSI value of AP Roaming. The default value is -80(dbm).

AP Roaming Time: The cycle scan time of AP Roaming. Enter a value between 1 and 30. The default value is 5(sec).

Roaming: Under Client mode, STA will roaming to better AP if the RSSI of client is lower than setting of Roaming Threshold.

Roaming Threshold: The RSSI value of roaming. The default value is -80(dbm).

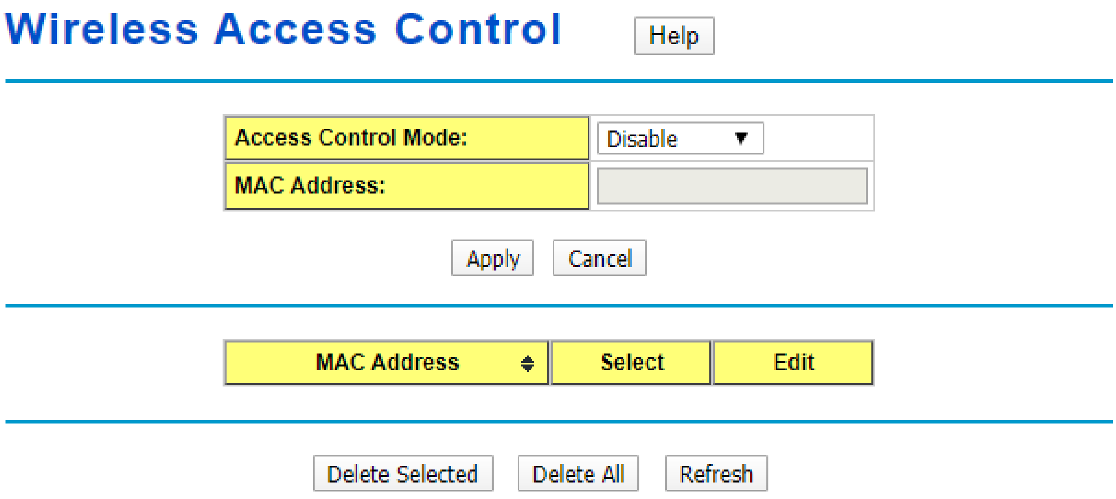
Roaming Min Diff: The Absolute value of roaming RSSI value. The default value is 3(dbm).

Roaming Sensitivity: The different level will decide the roaming scan period.

Scan Channels: When Roaming is enabled. The client will scan the APs on scan channels

4.2.4 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.



Wireless Access Control

Access Control Mode:	Disable ▼
MAC Address:	

MAC Address ⬍	Select	Edit

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.

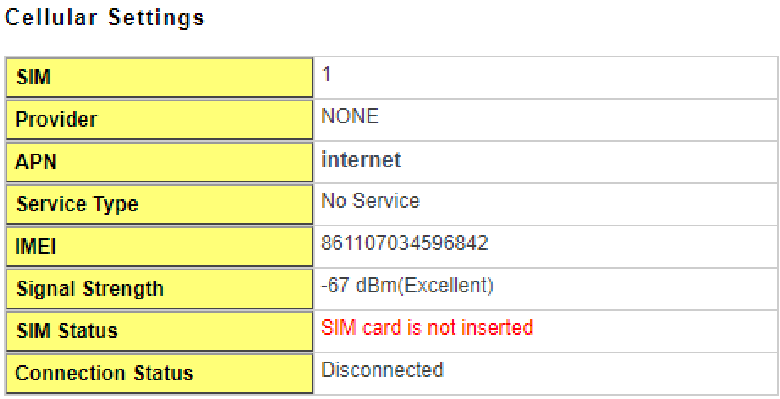
4.3 4G/Cellular

The "**4G/Cellular**" feature set pages allow users to see the 4G/LTE Status, configure the Basic LTE Setting, SIM Security and download the Debug message. The 4G means the 2nd radio of the JetWave 3420 device.

4.3.1 Status

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

After the 4G/LTE connected, some of the information will be updated per your ISP (Internet Service Provider).



Cellular Settings

SIM	1
Provider	NONE
APN	internet
Service Type	No Service
IMEI	861107034596842
Signal Strength	-67 dBm(Excellent)
SIM Status	SIM card is not inserted
Connection Status	Disconnected

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

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

IMEI: This item shows the International Mobile Equipment Identity (IMEI) of the LTE 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:

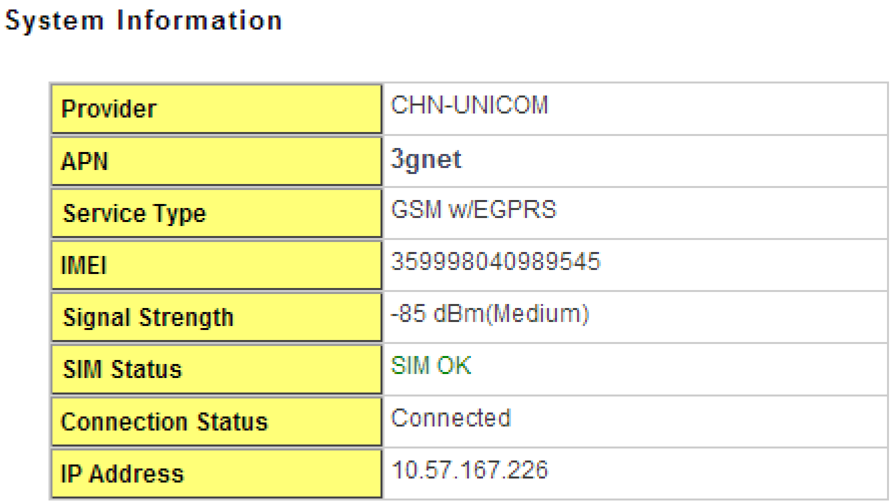
Connected: The LTE interface is connected to the base station.

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

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

Refresh: You can press Refresh to refresh the table.

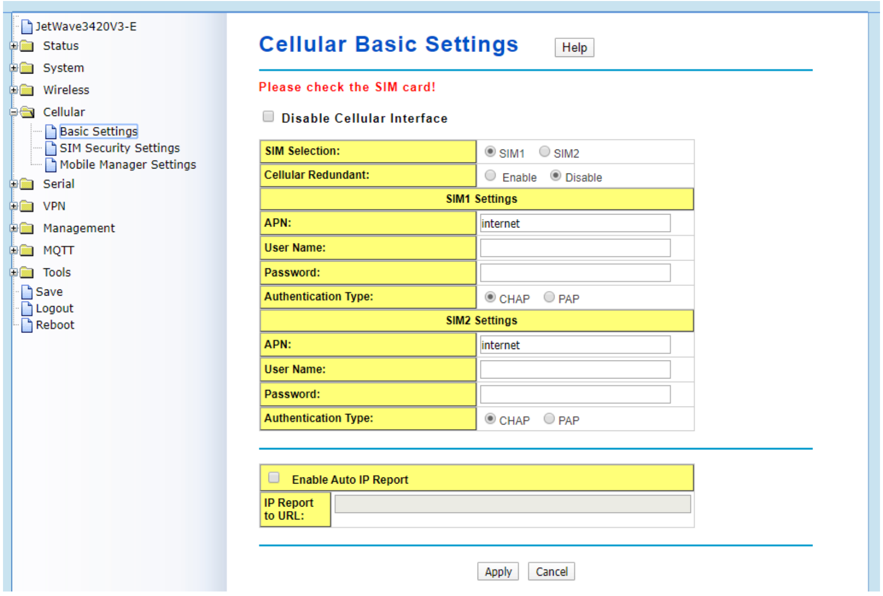
Below is the reference information after connected to UNICOM telecom in China. The service provider is China UNICOM, it provides the APN name, Service Type and assigns IP address for the JetWave 3420.



System Information

Provider	CHN-UNICOM
APN	3gnet
Service Type	GSM w/EGPRS
IMEI	359998040989545
Signal Strength	-85 dBm(Medium)
SIM Status	SIM OK
Connection Status	Connected
IP Address	10.57.167.226

4.3.2 Basic Settings



Cellular Basic Settings

Please check the SIM card!

□ Disable Cellular Interface

SIM Selection:	● SIM1 ○ SIM2
Cellular Redundant:	○ Enable ● Disable
SIM1 Settings	
APN:	internet
User Name:	
Password:	
Authentication Type:	● CHAP ○ PAP
SIM2 Settings	
APN:	internet
User Name:	
Password:	
Authentication Type:	● CHAP ○ PAP

□ Enable Auto IP Report

IP Report to URL:	

Normally, you can connect the LTE Gateway to the ISP cellular network without configuring LTE setting. However, in some countries, before the LTE 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/Cellular Interface: You can disable the LTE interface manually.

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 LTE 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 LTE connection. Normally, this is provided by your ISP.

Password: The password for the LTE 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.

Reconnection Delay: Reconnection Delay time is the delay time for each LTE Retry.

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

WAN Redundancy: The product can support WAN redundancy feature.

In default, the setting is **Fixed Cellular**, that means you can use LTE and Ethernet WAN port at the same time.

You can change the settings to **WAN First.** WAN first means the LTE feature is only activated when the Ethernet WAN port link down or failure.

Auto IP Report:

Most of the ISP assigns the dynamic IP address to the LTE 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 LTE client device. The Auto IP Report in JetWave 3420 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.

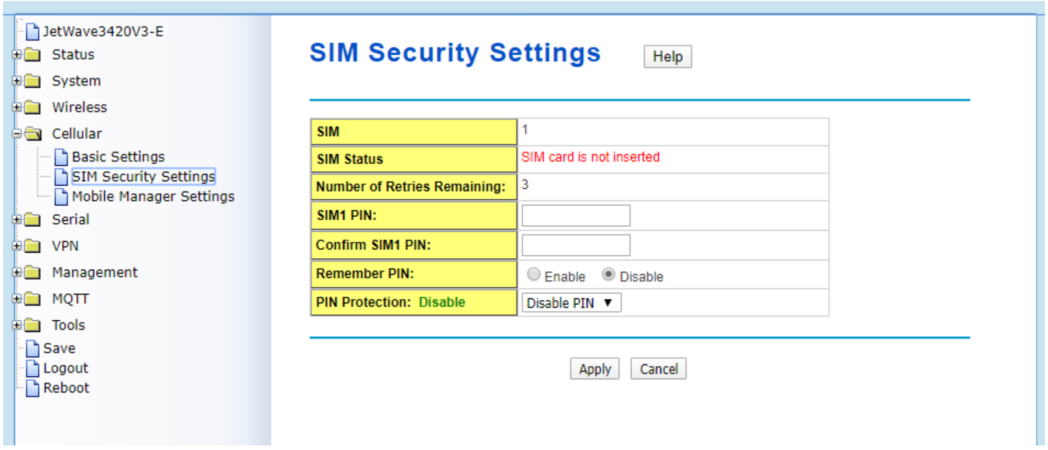
IP Report to URL: Type the correct URL here for your Gateway report to. You can build your own server, rent URL address from ISP or Google Cloud service also supports this functionality. Please check with your ISP or create through Google cloud.

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

4.3.3 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 LTE connection or change the new PIN settings.



SIM Security Settings

SIM	1
SIM Status	SIM card is not inserted
Number of Retries Remaining:	3
SIM1 PIN:	
Confirm SIM1 PIN:	
Remember PIN:	○ Enable ● Disable
PIN Protection: Disable	Disable PIN ▼

4.3.4 Debug Mode

You can use the Mobile Manager Utility to help you monitor the IP address of the cellular devices after you installed it in the remote field site.

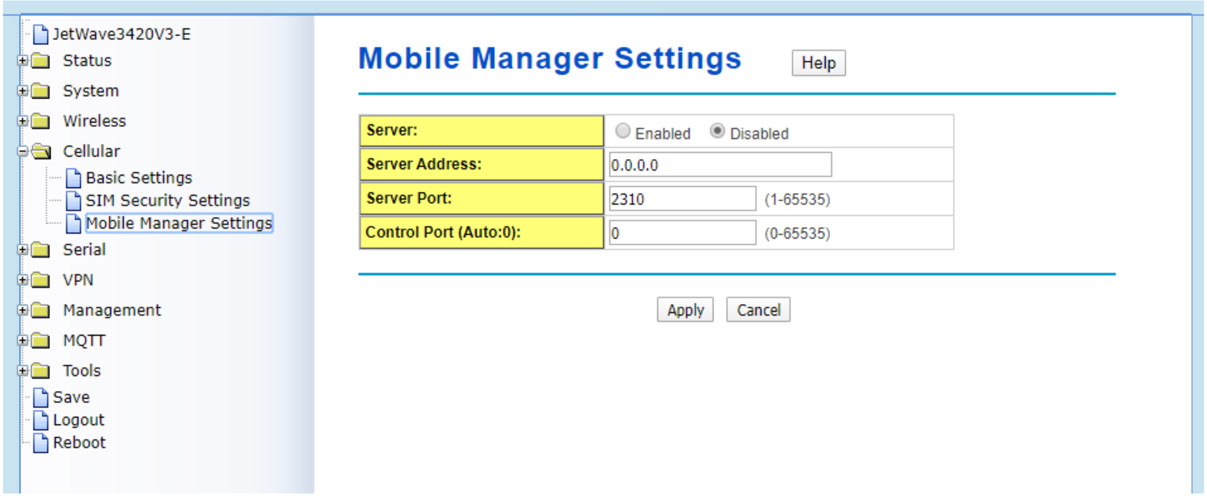
Server: You can Enable or Disable this function. The default value is disabled.

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

Server Port: Type the Mobile Manager Utility's Port in this field. The device updates information to the server through this port. The default is TCP port 2310.

Control Port: The Control Port (TCP port) allows you to connect to this device. Default value 0 means auto select.

Click the Apply button to apply the configuration changes.

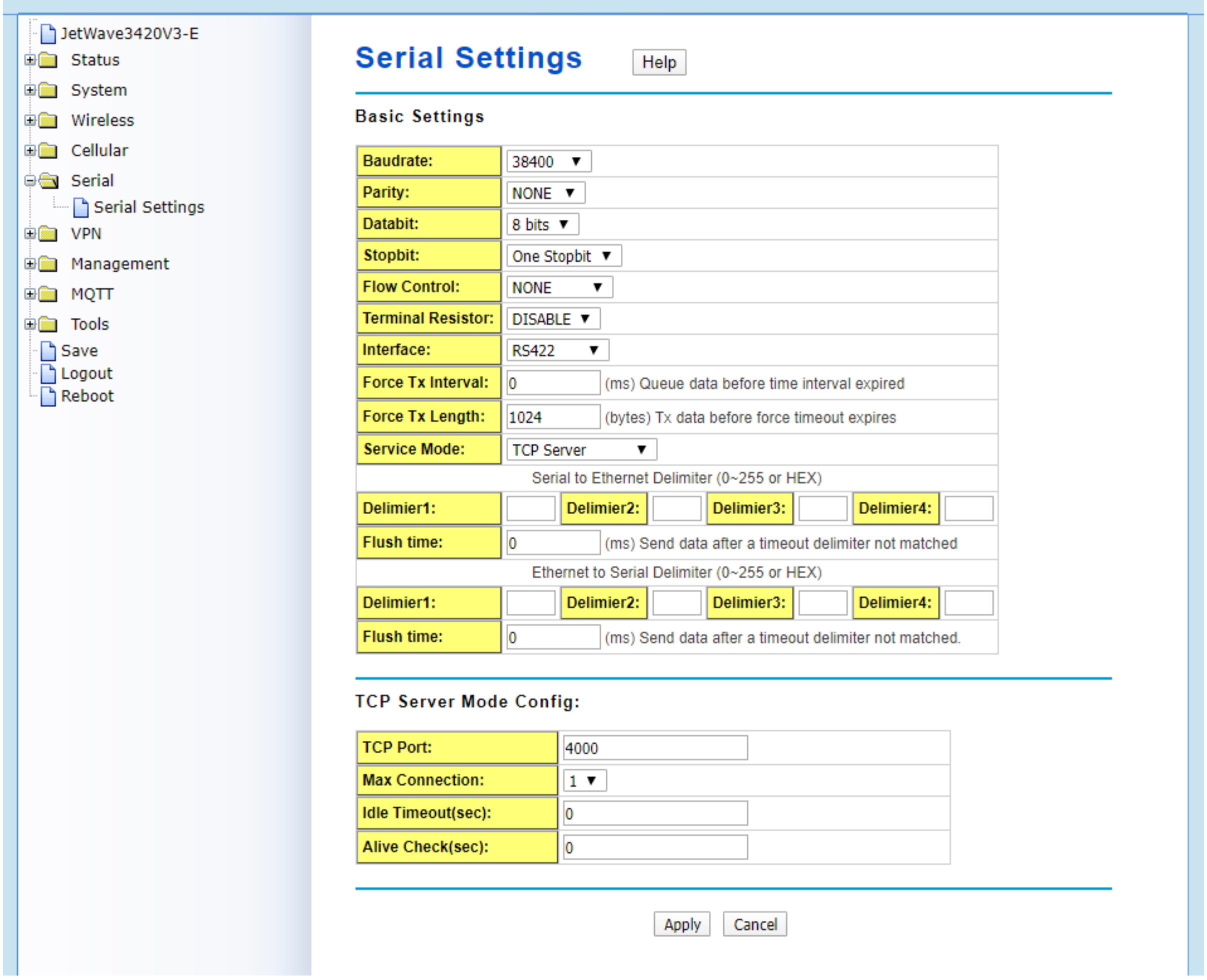


Mobile Manager Settings

Server:	○ Enabled ● Disabled	
Server Address:	0.0.0.0	
Server Port:	2310	(1-65535)
Control Port (Auto:0):	0	(0-65535)

4.4 Serial Setting

JetWave 3420v3 is equipped with RS-232/422/485 3-in-1 Serial port. It supports TCP Server/Client and UDP for remote connection. This page allows you to configure the Serial interface's parameters.



Serial Settings

Basic Settings

Baudrate:	38400 ▼						
Parity:	NONE ▼						
Databit:	8 bits ▼						
Stopbit:	One Stopbit ▼						
Flow Control:	NONE ▼						
Terminal Resistor:	DISABLE ▼						
Interface:	RS422 ▼						
Force Tx Interval:	0 (ms) Queue data before time interval expired						
Force Tx Length:	1024 (bytes) Tx data before force timeout expires						
Service Mode:	TCP Server ▼						
Serial to Ethernet Delimiter (0~255 or HEX)							
Delimier1:		Delimier2:		Delimier3:		Delimier4:	
Flush time:	0 (ms) Send data after a timeout delimiter not matched						
Ethernet to Serial Delimiter (0~255 or HEX)							
Delimier1:		Delimier2:		Delimier3:		Delimier4:	
Flush time:	0 (ms) Send data after a timeout delimiter not matched.						

TCP Server Mode Config:

TCP Port:	4000
Max Connection:	1 ▼
Idle Timeout(sec):	0
Alive Check(sec):	0

Basic Settings:

This page allows you to configure basic settings of the Serial port.

Serial port Settings: You can select the Baudrate, Parity, Databit, Stopbit and Flow control settings from the dropdown list.

Interface: Manually choose and change the interface type. The serial port supports the RS232, RS422, RS485-2w, RS485-4w, you can select either one from the dropdown list.

Force Tx Interval: Configure the Tx Interval time, the system will queue the transmit data before the time interval expired. The time unit is millisecond.

Force Tx Length: Configure the Tx data Length before force timeout expires. The data unit is byte.

Service mode: You can select TCP Server, TCP Client, and UDP listening.

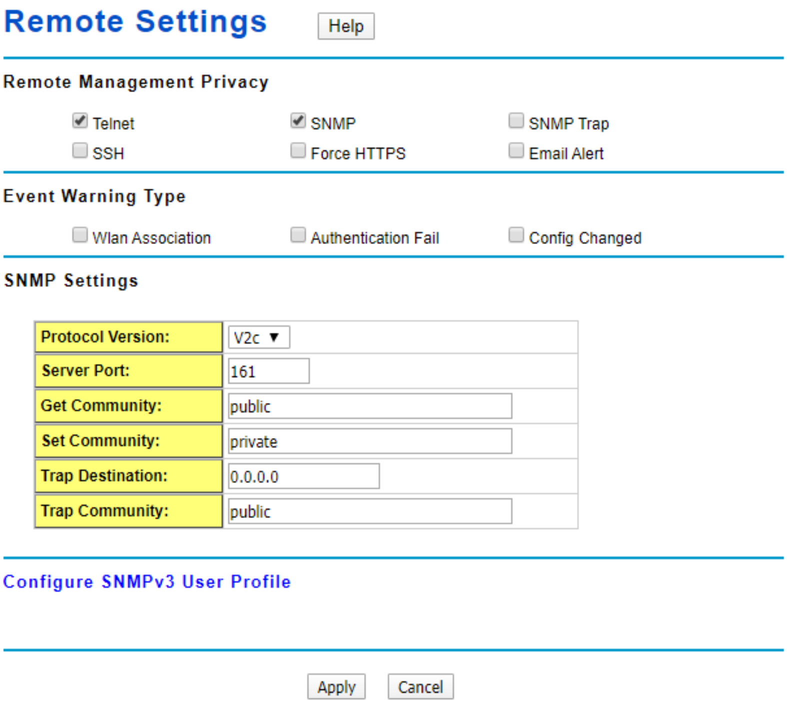
Serial to Ethernet/ Ethernet to Serial Delimiter: Configure the Delimiter and Flush time (a timeout that the delimiter not matched) setting for Serial to Ethernet or Ethernet to Serial transmission. There are up to 4 delimiters can be configured here. After the Delimiter is configured, the data will be stored in the buffer until hit the Delimiter or the Flush time timeout.

Click the Apply button to apply the configuration changes.

4.5 Management

The "**Management**" feature set pages allow users to configure the remote settings, event warming type, SNMP, SMTP, password and firmware update, configuration file, certification file upload.

4.5.1 Remote Setting



Remote Settings

Remote Management Privacy

☑ Telnet ☑ SNMP □ SNMP Trap

□ SSH □ Force HTTPS □ Email Alert

Event Warning Type

□ Wlan Association □ Authentication Fail □ Config Changed

SNMP Settings

Protocol Version:	V2c ▼
Server Port:	161
Get Community:	public
Set Community:	private
Trap Destination:	0.0.0.0
Trap Community:	public

Configure SNMPv3 User Profile

Use this page to configure the remote management privacy, select the event warming type and SNMP settings.

Remote Management Privacy: You can select which kinds of remote service should be opened in your environment. The services include **Telnet, SNMP, SMP 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, the product supports SNMP V1, V2c and V3. While selecting the SNMPv3, continue to configure the SNMPv3 User Name and Encryption in lower screen.

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 community name (password) for the incoming SNMP_Get and SNMP_GetNext requests from the management station. By default, it is set to public and allows all requests.

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

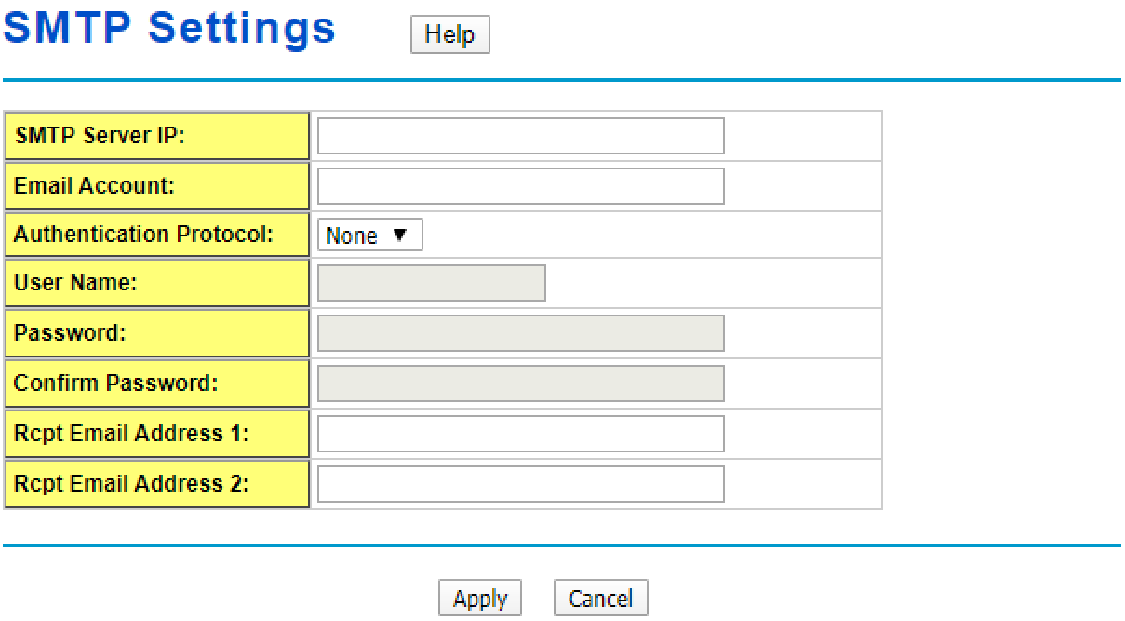
Trap Destination: Specify the IP address of the station to send the SNMP traps to.

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

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.*

4.5.2 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:	
Email Account:	
Authentication Protocol:	None ▼
User Name:	
Password:	
Confirm Password:	
Rcpt Email Address 1:	
Rcpt Email Address 2:	

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.

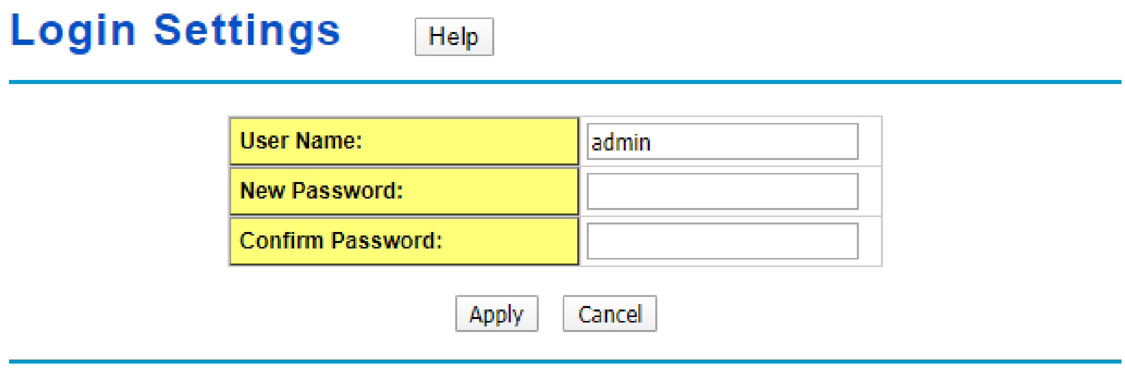
Rcpt Email Address 2: The second Receiver's email address.

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

4.5.3 Login Settings

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

Type the **New Password** and **Confirm Password** again. Press **"Apply"** to activate the new password.



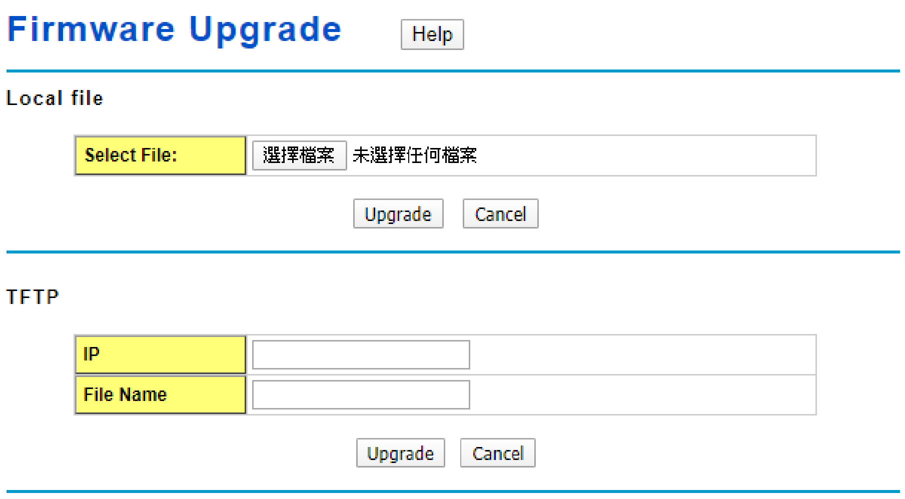
User Name:	admin
New Password:	
Confirm Password:	

4.5.4 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.



Select File:	未選擇任何檔案

IP	
File Name	

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.

TFTP

This section allows you to upload a firmware image that is stored on a TFTP server.

IP: This is the IP address of the TFTP server where the firmware image resides.

File Name: This is the file name of the firmware image.

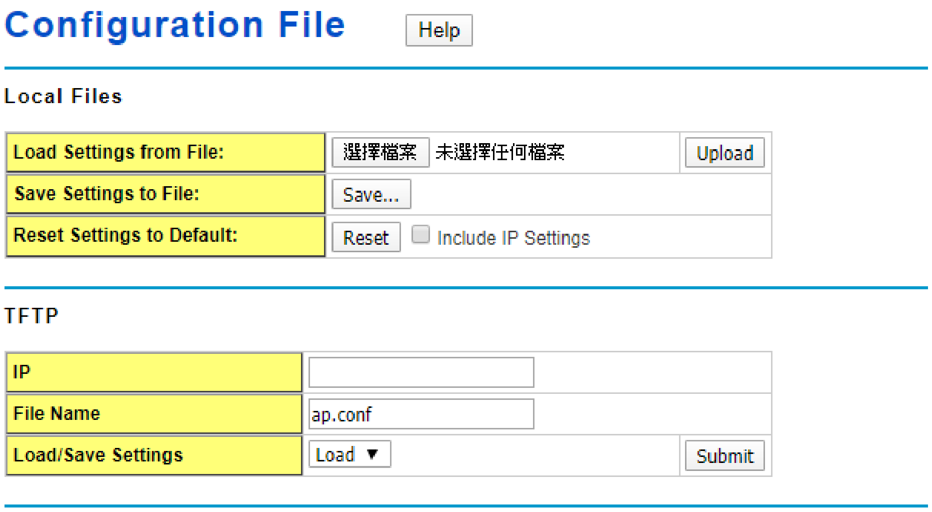
Click the Upgrade button to begin upgrading the firmware or click the Cancel button to clear the entered IP address and firmware file name. After the firmware has upgraded, the device reboots automatically.

4.5.5 Configuration File

The AP/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.


Configuration File

Local Files

Load Settings from File:	選擇檔案 未選擇任何檔案	Upload
Save Settings to File:	Save...	
Reset Settings to Default:	Reset □ Include IP Settings	

TFTP

IP		
File Name	ap.conf	
Load/Save Settings	Load ▼	Submit

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".

4.5.6 Remote IP Scan

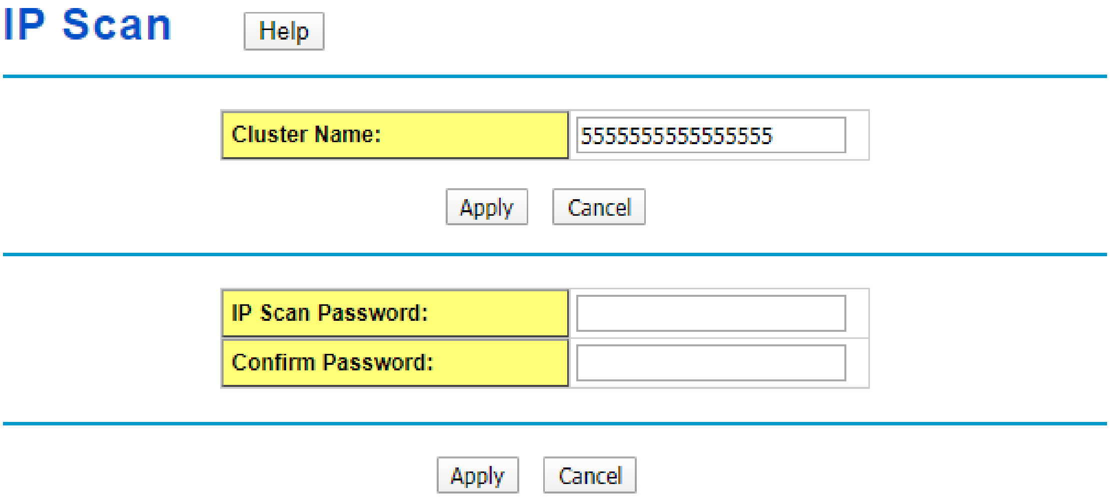
The page allows user to set remote IP Scan, it include Cluster Name and IP Scan Password. With Remote IP Scan, it provides higher wireless security when uses management tool.

Cluster Name: Set Cluster Name, management tool will not list this device in Model filed unless user type the same Cluster name at Korenix View interface.

Click the Apply button to apply the configuration changes or click the Cancel button to discard any changes.

IP Scan Password: Once the password is set, the user needs to key in password if the user wants to modify configuration, such as Reboot, Load factory default, Change Cluster Name and Wireless panel settings through management tool.

Click the Apply button to apply the configuration changes or click the Cancel button to discard any changes.



Cluster Name:	5555555555555555

IP Scan Password:	
Confirm Password:	

4.5.7 LLDP Configuration

The Link Layer Discovery Protocol (LLDP) allows devices to discover the other devices which are connected to them. This page allows you to configure LLDP settings.

Enable LLDP: Set this to Enable to enable LLDP on the router or to Disable to disable the LLDP function.

LLDP Timer: This setting determines how frequently (in seconds) it sends out LLDP discovery packets.

Valid values are 5 to 254 and default is 30.

LLDP Holdtime: This setting determines how long in seconds it will retain LLDP neighbor information.

Valid values are 10 to 255 and the default is 120.

Click the Apply button to apply the configuration changes or click the Cancel button to discard any changes.

LLDP Port State

This table shows the LLDP neighbors the switch is currently aware of.

Local Port: The router port to which the neighbor is connected.

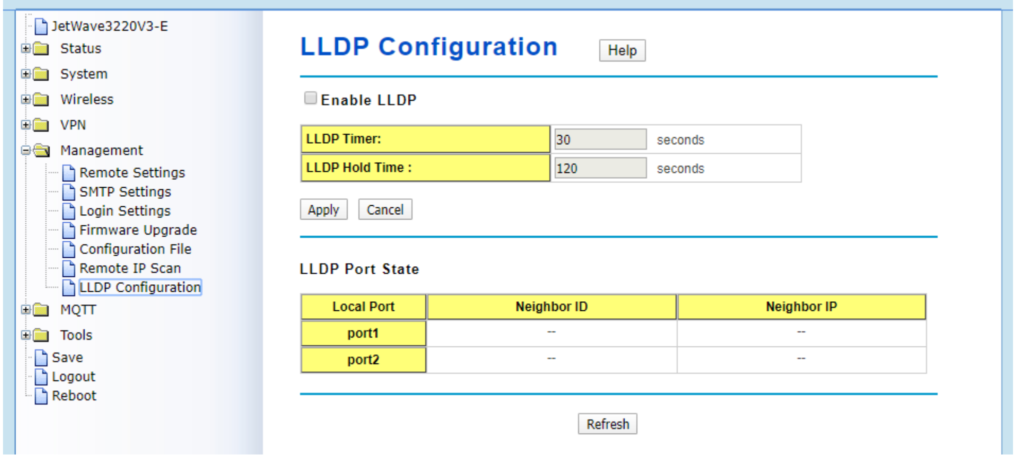
Neighbor ID: The MAC address of the LLDP neighbor.

Port Description: The description shows which port is connected on the neighbor device.

Neighbor IP: The IP address of the LLDP neighbor

Neighbor VID: The VLAN the LLDP neighbor is connected to.

Click the Refresh button to update the information in the table.



LLDP Configuration

□ Enable LLDP

LLDP Timer:	30	seconds
LLDP Hold Time :	120	seconds

LLDP Port State

Local Port	Neighbor ID	Neighbor IP
port1	--	--
port2	--	--

4.6 MQTT

4.6.1 Broker

The page allows user to set MQTT, it include Authentication, save and delete Certificate Authority.

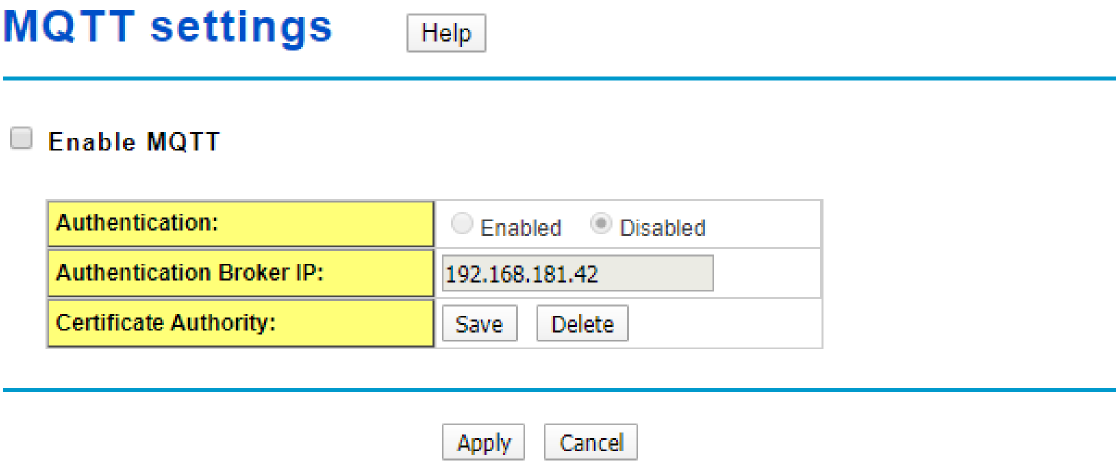
Enable MQTT: Check "Enable MQTT" to enable MQTT broker, uncheck means disable.

Authentication: Check "Enabled" to use Authentication for MQTT protocol.

Authentication Broker IP: The Authentication Broker IP field allows you to set the MQTT Broker IP address manually to create Certificate Authority file.

Certificate Authority: Check "Save" button to save Certificate Authority file or click the "Delete" button to delete current Certificate Authority file.

Click the Apply button to apply the configuration changes or click the Cancel button to discard any changes.


MQTT settings

☐ Enable MQTT

Authentication:	○ Enabled ● Disabled
Authentication Broker IP:	192.168.181.42
Certificate Authority:	Save Delete

4.6.2 Publisher

The page allows user to set MQTT Publisher, it include to upload or delete certificates.

Enable MQTT Publisher: Check "Enable MQTT Publisher" to enable MQTT Publisher, uncheck means disable.

Broker IP Address: The IP Address field allows you to set the Broker IP address manually.

Topic: The Topic field allows you to set MQTT topic infomation.

Message: The Message field allows you to set the message content.

Event: Select the event to detect device.

Certificate Authority: Select you saved certificate file.

Detect Time: The Detect Time field allows you to set time to detect device.

Click the Apply button to apply the configuration changes.

MQTT Publisher List

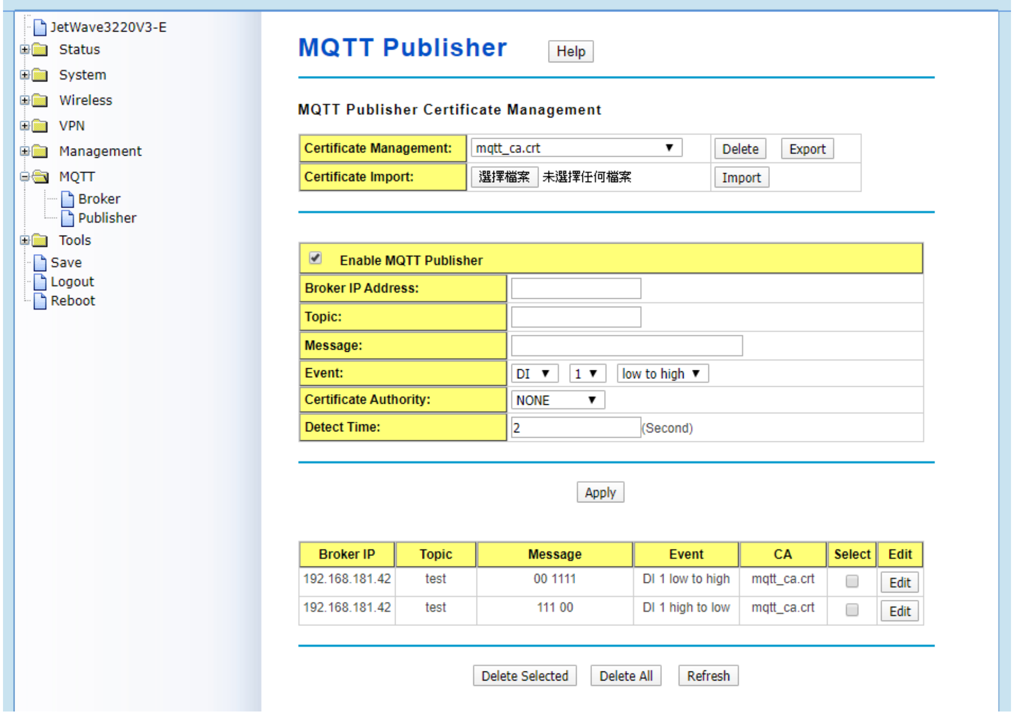
This section allows you to modify and shows all of the MQTT Publisher content.

Select: Click the Select checkbox to delete the selected entries.

Edit: Click the Edit button to modify saved entries.

Click the Delete Selected button to delete the selected entries.

Click the Delete ALL button to delete all entries.



MQTT Publisher Certificate Management

Certificate Management:	mqtt_ca.crt ▼
Certificate Import:	選擇檔案 未選擇任何檔案

☑ Enable MQTT Publisher

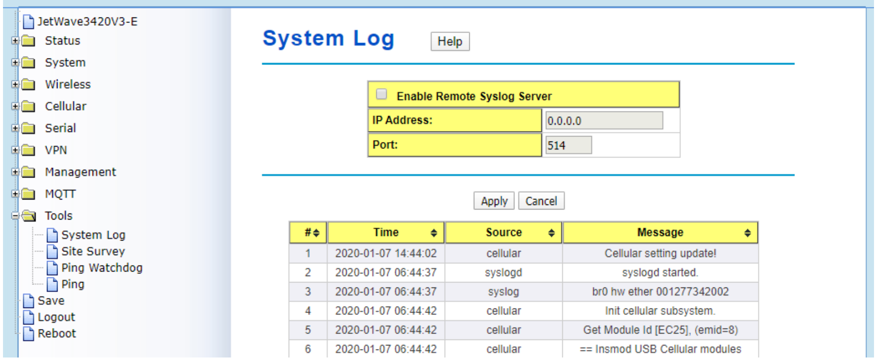
Broker IP Address:	
Topic:	
Message:	
Event:	DI ▼ 1 ▼ low to high ▼
Certificate Authority:	NONE ▼
Detect Time:	2 (Second)

Broker IP	Topic	Message	Event	CA	Select	Edit
192.168.181.42	test	00 1111	DI 1 low to high	mqtt_ca.crt	□	Edit
192.168.181.42	test	111 00	DI 1 high to low	mqtt_ca.crt	□	Edit

4.7 Tools

The “**Tools**” feature set pages provides some additional useful tools. The System Log help you see the occurred event logs, wireless AP site survey, Ping Watchdog, Data Rate Test, Antenna Alignment and Ping tool.

4.7.1 System Log



□ Enable Remote Syslog Server

IP Address:	0.0.0.0
Port:	514

#	Time	Source	Message
1	2020-01-07 14:44:02	cellular	Cellular setting update!
2	2020-01-07 06:44:37	syslogd	syslogd started.
3	2020-01-07 06:44:37	syslog	br0 hw ether 001277342002
4	2020-01-07 06:44:42	cellular	Init cellular subsystem.
5	2020-01-07 06:44:42	cellular	Get Module Id [EC25], (emid=8)
6	2020-01-07 06:44:42	cellular	== Insmod USB Cellular modules

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

Select "**Enable Remote Syslog Server**", type the **IP Address** and **Port** number of your syslog server. The default port number is 514.

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

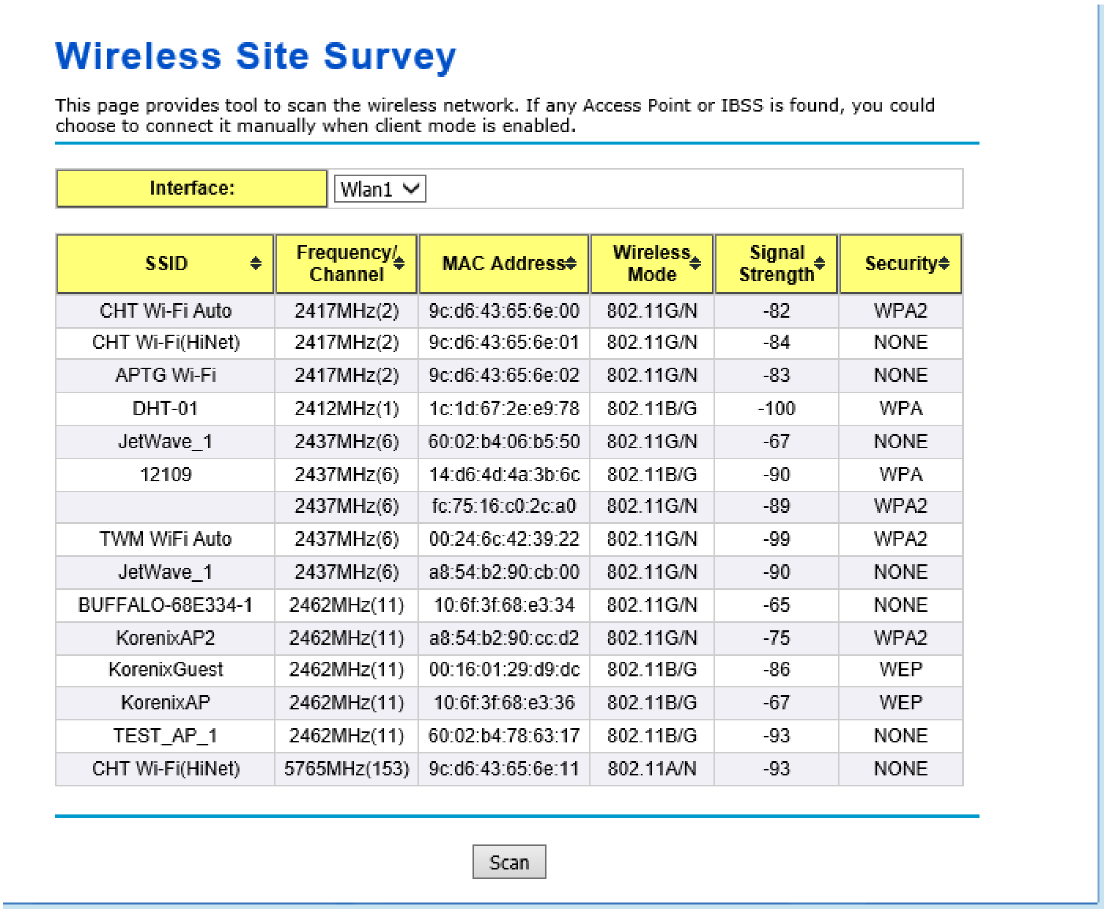
In the lower screen, it displays the occurred system logs. Each entry has the index, occurred time, source MAC address and the message. You can monitor the system by this screen, however, the logs will be removed after system reboot.

Press "**Clear**" allows you to remove all of entries.

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

4.7.2 Site Survey

While your AP/Gateway 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.



Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

Interface: Wlan1

SSID	Frequency/Channel	MAC Address	Wireless Mode	Signal Strength	Security
CHT Wi-Fi Auto	2417MHz(2)	9c:d6:43:65:6e:00	802.11G/N	-82	WPA2
CHT Wi-Fi(HiNet)	2417MHz(2)	9c:d6:43:65:6e:01	802.11G/N	-84	NONE
APTG Wi-Fi	2417MHz(2)	9c:d6:43:65:6e:02	802.11G/N	-83	NONE
DHT-01	2412MHz(1)	1c:1d:67:2e:e9:78	802.11B/G	-100	WPA
JetWave_1	2437MHz(6)	60:02:b4:06:b5:50	802.11G/N	-67	NONE
12109	2437MHz(6)	14:d6:4d:4a:3b:6c	802.11B/G	-90	WPA
	2437MHz(6)	fc:75:16:c0:2c:a0	802.11G/N	-89	WPA2
TWM WiFi Auto	2437MHz(6)	00:24:6c:42:39:22	802.11G/N	-99	WPA2
JetWave_1	2437MHz(6)	a8:54:b2:90:cb:00	802.11G/N	-90	NONE
BUFFALO-68E334-1	2462MHz(11)	10:6f:3f:68:e3:34	802.11G/N	-65	NONE
KorenixAP2	2462MHz(11)	a8:54:b2:90:cc:d2	802.11G/N	-75	WPA2
KorenixGuest	2462MHz(11)	00:16:01:29:d9:dc	802.11B/G	-86	WEP
KorenixAP	2462MHz(11)	10:6f:3f:68:e3:36	802.11B/G	-67	WEP
TEST_AP_1	2462MHz(11)	60:02:b4:78:63:17	802.11B/G	-93	NONE
CHT Wi-Fi(HiNet)	5765MHz(153)	9c:d6:43:65:6e:11	802.11A/N	-93	NONE

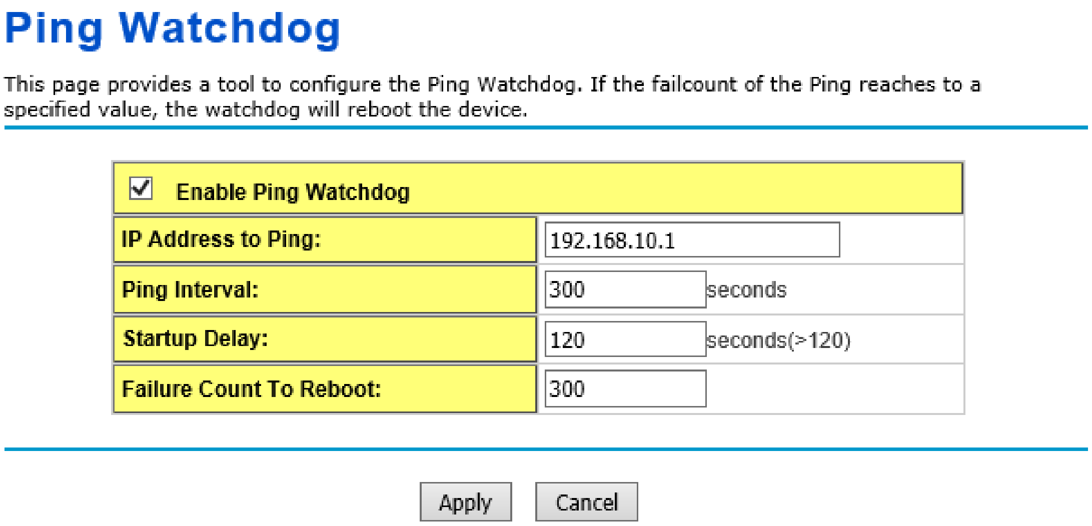
Interface: Select the interface number.

Scan: Press Scan to scan the network again. This progress takes around 3 seconds and you will see the below info.

Scanning...
Please wait for 1 seconds.

4.7.3 Ping Watchdog

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



Ping Watchdog

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

☑ Enable Ping Watchdog

IP Address to Ping:	192.168.10.1
Ping Interval:	300 seconds
Startup Delay:	120 seconds(>120)
Failure Count To Reboot:	300

Select "**Enable Ping Watchdog**" to enable the function.

IP Address to Ping: This is the target IP address of the Ping Watchdog. Please notice that this IP address MUST be a correct and existed IP address, otherwise, the ping watchdog will reboot your system after couple time.

Ping Interval: The interval time between each Ping packet.

Startup Delay: This is the startup delay time of the ping watchdog. After the time timeout, the system starts to do Ping watchdog checking.

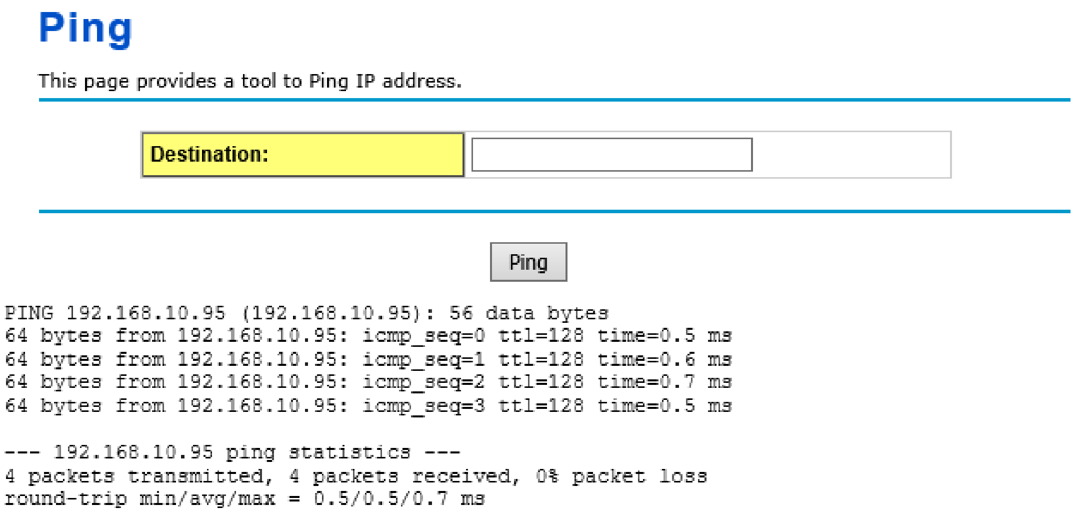
Failure Count to Reboot: After Ping failure count to the volume you assigned here, the system will reboot automatically.

4.7.4 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.



Ping

This page provides a tool to Ping IP address.

Destination:	

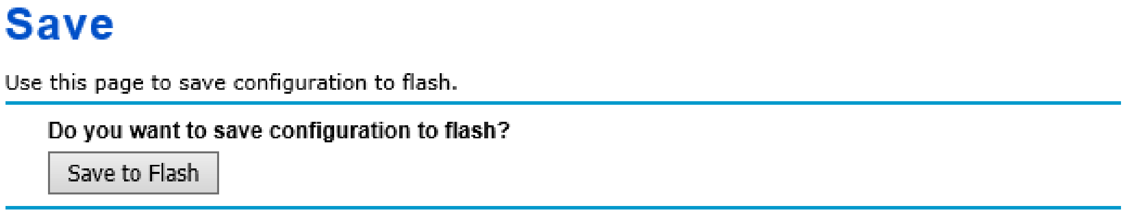
```
PING 192.168.10.95 (192.168.10.95): 56 data bytes
64 bytes from 192.168.10.95: icmp_seq=0 ttl=128 time=0.5 ms
64 bytes from 192.168.10.95: icmp_seq=1 ttl=128 time=0.6 ms
64 bytes from 192.168.10.95: icmp_seq=2 ttl=128 time=0.7 ms
64 bytes from 192.168.10.95: icmp_seq=3 ttl=128 time=0.5 ms

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

4.8 Main Entry

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

4.8.1 Save

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



Save

Use this page to save configuration to flash.

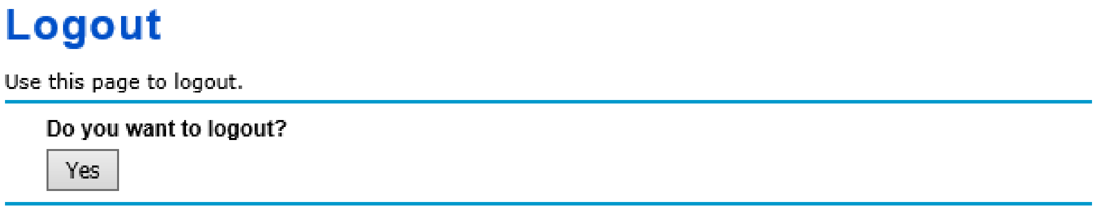
Do you want to save configuration to flash?

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

4.8.2 Logout

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

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



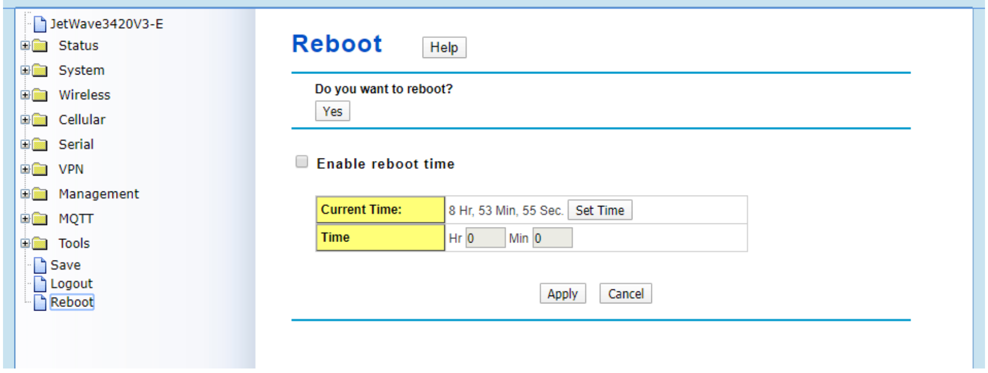
Logout

Use this page to logout.

Do you want to logout?

4.8.3 Reboot

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



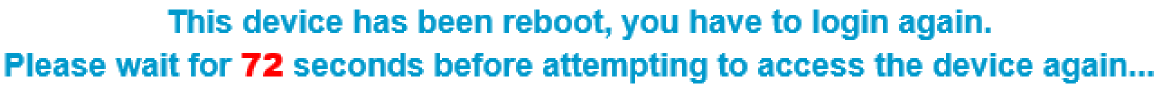
Reboot

Do you want to reboot?

□ Enable reboot time

Current Time:	8 Hr, 53 Min, 55 Sec.
Time	Hr 0 Min 0

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



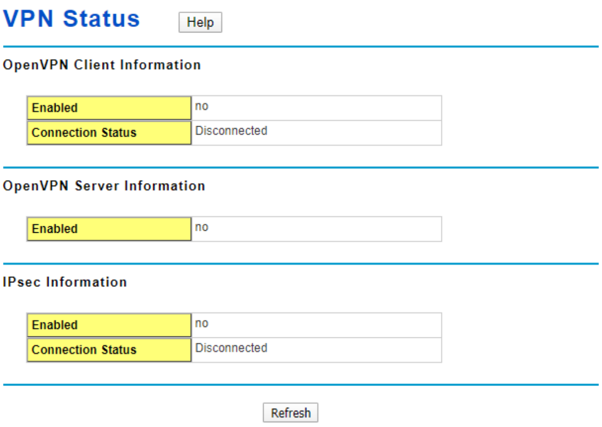
This device has been reboot, you have to login again.
Please wait for 72 seconds before attempting to access the device again...

4.9 VPN

The VPN is the new feature released from JetWave 3420v3 V1.1 firmware. In V1.1, the first VPN type supported is OPEN VPN Client. This page shows how to configure VPN settings and monitor its status.

The “**VPN**” feature set pages allow users to configure the device as VPN client to connect to VPN server.

4.9.1 Status



VPN Status

OpenVPN Client Information

Enabled	no
Connection Status	Disconnected

OpenVPN Server Information

Enabled	no

IPsec Information

Enabled	no
Connection Status	Disconnected

OpenVPN Client Information

Enabled:

yes: The VPN function is enabled.

no: The VPN function not enabled.

Connection Status:

Connected: The VPN connection is successfully connected.

Disconnected: The VPN has not connected.

Remote Server IP: The remote server IP displays after the VPN client connection is successful.

Tx / Rx Bytes: The transmission data volume in bytes displays after the VPN client connects.

OpenVPN Server Information

Enabled:

yes: The VPN function is enabled.

no: The VPN function is not enabled.

Connection Status:

Connected: The VPN connection is successfully connected.

Disconnected: The VPN has not connected.

Tx / Rx Bytes: The transmission data volume in bytes displays after the VPN interface connects.

IPsec Information

Enabled:

yes: The VPN function is enabled.

no: The VPN function is not enabled.

Connection Status:

Connected: The VPN connection is successfully connected.

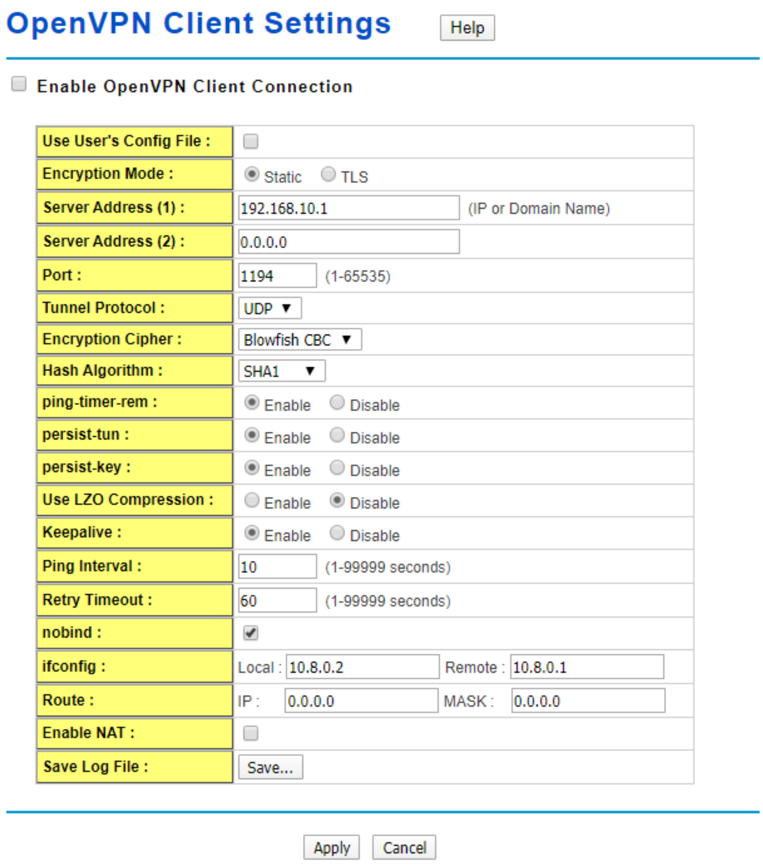
Disconnected: The VPN has not connected.

Left IP/ Right IP: The IP address of IPSec's left and right endpoint displays after the VPN connects.

Tx / Rx Bytes: You can see the transmission data volume in bytes on VPN interface.

Click the Refresh button to refresh the VPN status information.

4.9.2 OpenVPN Client



OpenVPN Client Settings

☐ Enable OpenVPN Client Connection

Use User's Config File :	☐
Encryption Mode :	● Static ○ TLS
Server Address (1) :	192.168.10.1 (IP or Domain Name)
Server Address (2) :	0.0.0.0
Port :	1194 (1-65535)
Tunnel Protocol :	UDP ▼
Encryption Cipher :	Blowfish CBC ▼
Hash Algorithm :	SHA1 ▼
ping-timer-rem :	● Enable ○ Disable
persist-tun :	● Enable ○ Disable
persist-key :	● Enable ○ Disable
Use LZO Compression :	○ Enable ● Disable
Keepalive :	● Enable ○ Disable
Ping Interval :	10 (1-99999 seconds)
Retry Timeout :	60 (1-99999 seconds)
nobind :	☑
ifconfig :	Local : 10.8.0.2 Remote : 10.8.0.1
Route :	IP : 0.0.0.0 MASK : 0.0.0.0
Enable NAT :	☐
Save Log File :	Save...

Encryption Mode: Select the encryption is Static or TLS.

Static Key: Use a pre-shared static key.

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

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

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

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

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

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

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

Hash Algorithm: Select the hash algorithm.

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

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

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

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

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

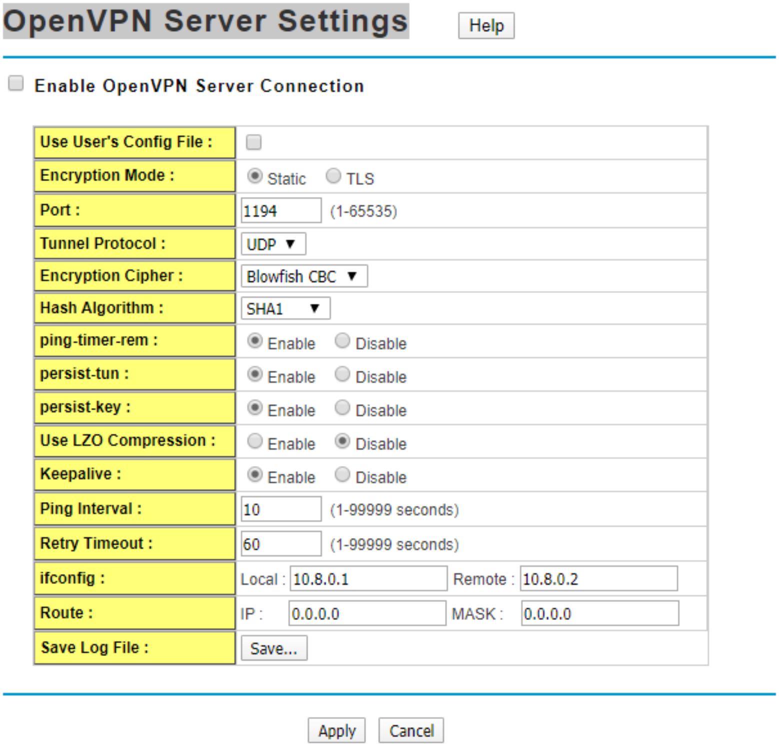
Ping Interval: Input the ping interval, the range can from 1~99999 seconds.

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

Ifconfig: Input the tunnel IP address that VPN use.

Route: Input the route IP and MASK.

4.9.3 OpenVPN Server



OpenVPN Server Settings

□ Enable OpenVPN Server Connection

Use User's Config File :	□
Encryption Mode :	● Static ○ TLS
Port :	1194 (1-65535)
Tunnel Protocol :	UDP ▼
Encryption Cipher :	Blowfish CBC ▼
Hash Algorithm :	SHA1 ▼
ping-timer-rem :	● Enable ○ Disable
persist-tun :	● Enable ○ Disable
persist-key :	● Enable ○ Disable
Use LZO Compression :	○ Enable ● Disable
Keepalive :	● Enable ○ Disable
Ping Interval :	10 (1-99999 seconds)
Retry Timeout :	60 (1-99999 seconds)
ifconfig :	Local : 10.8.0.1 Remote : 10.8.0.2
Route :	IP : 0.0.0.0 MASK : 0.0.0.0
Save Log File :	Save...

4.9.4 VPN Port Forwarding

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

Enable VPN Port Forwarding: Select Enable VPN Port Forwarding and then enter the parameters to create the port forwarding entries.

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

Source IP Address: Enter the specific incoming packet's source IP address for the VPN interface. This field can be left empty.

Destination Port or Range: Enter the specific incoming packet's destination port range for the VPN interface.

Forwarding IP Address: Enter the specific forwarding IP address of the LAN device.

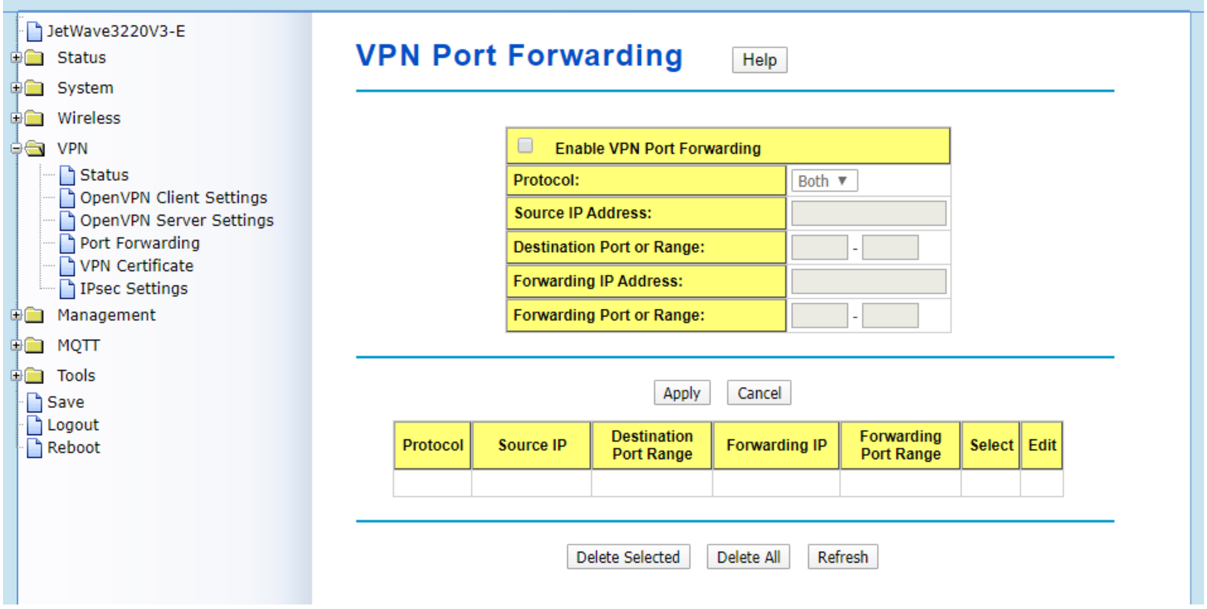
Forwarding Port or Range: Configure the port or the range of ports for the device in the LAN.

Click the Apply button to apply the configuration changes.

Click the Delete Selected button to delete selected entries.

Click the Delete All button to delete all entries.

Click the Refresh button to refresh the port forwarding entries.



☐ Enable VPN Port Forwarding	
Protocol:	Both ▼
Source IP Address:	
Destination Port or Range:	-
Forwarding IP Address:	
Forwarding Port or Range:	-

Protocol	Source IP	Destination Port Range	Forwarding IP	Forwarding Port Range	Select	Edit

4.9.5 VPN Certificate Management

Use this page to upload or delete VPN certificates.

The filename of the VPN certificate files MUST uploaded using the following file names.

OpenVPN Server TLS Mode: ca.crt, server.key, server.crt, dh1024.pem

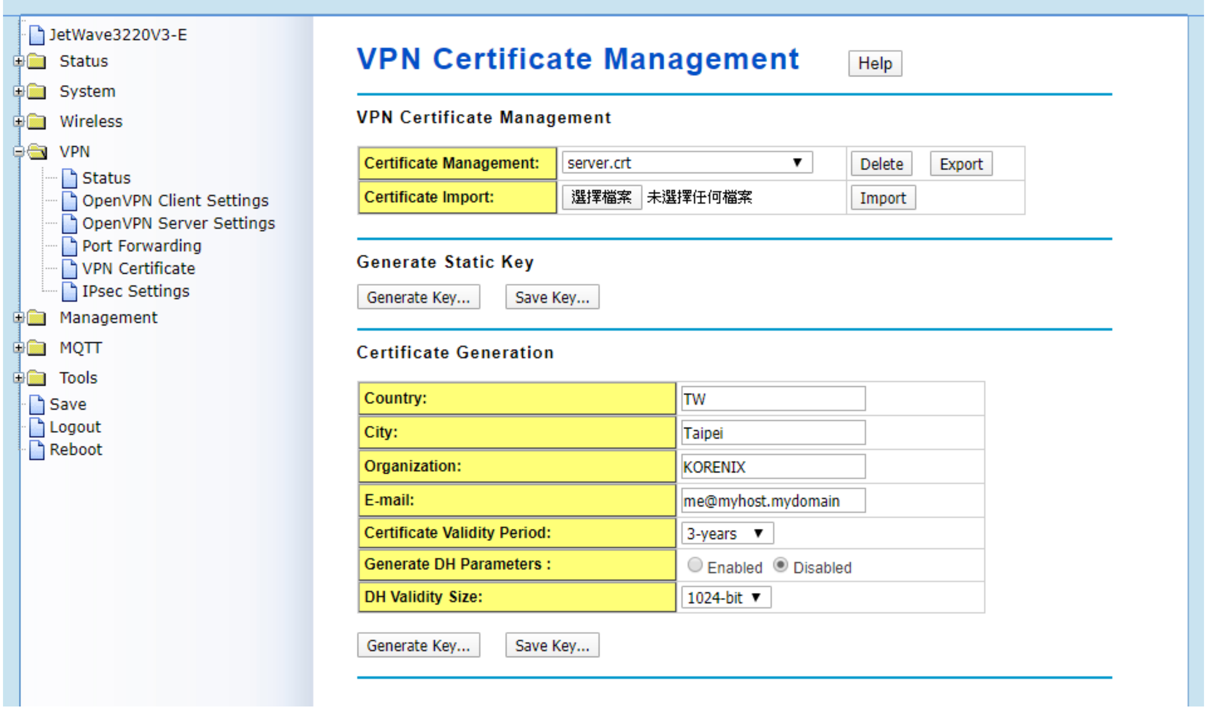
OpenVPN Client TLS Mode: ca.crt, client.key, client.crt

Static Mode: static.key

Delete VPN Certificate: Press the Delete to delete the selected certificate file.

Import VPN Certificates: Click the Browse button to select the certificate file. After locating the file, click the Import button.

Save Static Key to File: Press the Save to Generate the static.key and download the file.



VPN Certificate Management

VPN Certificate Management

Certificate Management:	server.crt ▼
Certificate Import:	選擇檔案 未選擇任何檔案

Generate Static Key

Certificate Generation

Country:	TW
City:	Taipei
Organization:	KORENIX
E-mail:	me@myhost.mydomain
Certificate Validity Period:	3-years ▼
Generate DH Parameters :	○ Enabled ● Disabled
DH Validity Size:	1024-bit ▼

4.9.6 IP Sec Setting

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

Public Key Management

Generate Public Key: Generate a new public key by pressing the Generate key... button. The Public key is used when the authentication method set to RSA key in the configuration (below).

Current Public Key: The content of the current public key is displayed.

Use the Enable IPsec Connection check box to enable or disable the IPSec function. Configure the appropriate fields below.

Interfaces for IPsec to Use: Select the interface that you want to use communicate with the VPN peer.

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

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

RSA key: Use an RSA digital signature authentication. The public key for RSA authentication can be generated on the top-half of this page.

ESP Algorithm: Select the algorithm (AES, DES, or 3DES) to encrypt an ESP (Encapsulating Security Payload) payload.

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

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

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

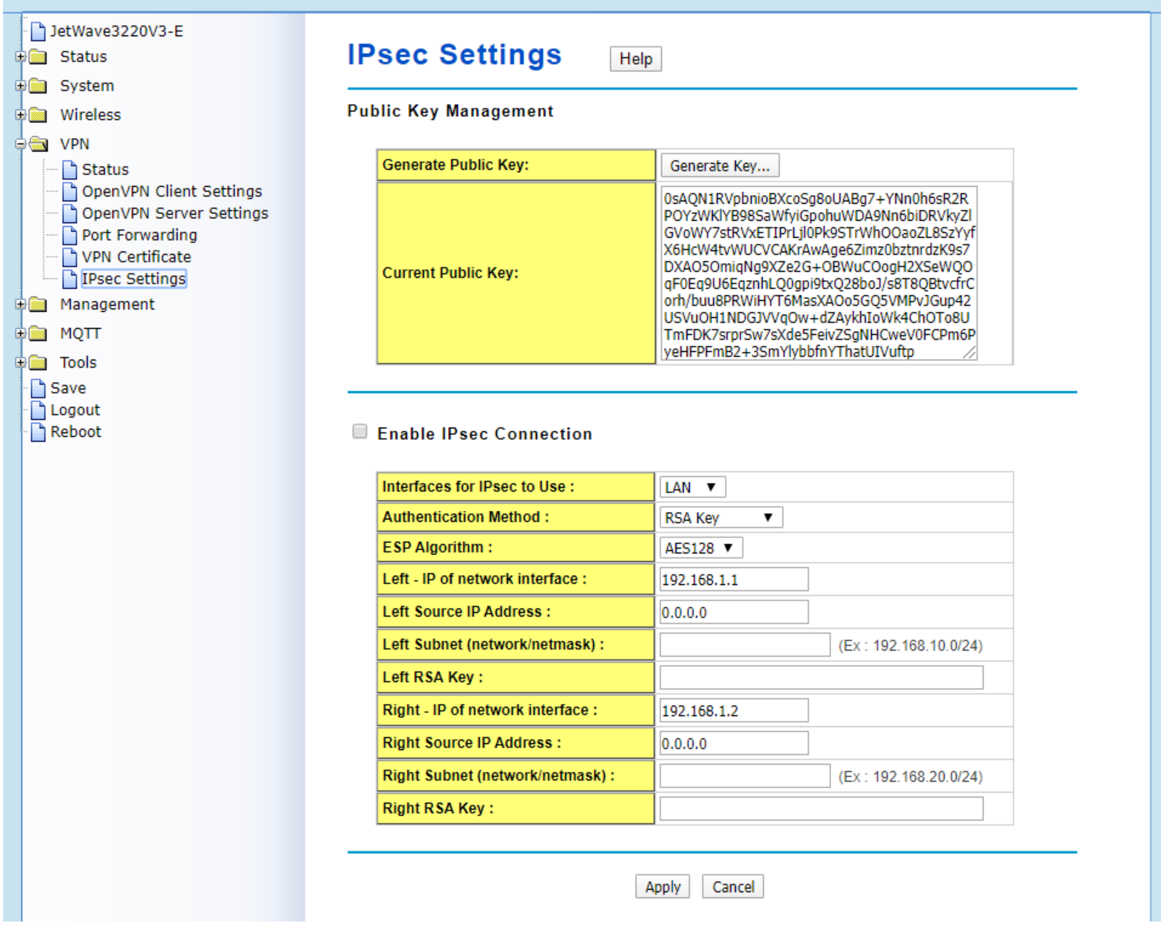
Left RSA Key: The attribute is only required when using the RSA key authentication method using the public key which was generated from the top-half of this page.

Right - IP of network interface: Right corresponds to the left in an IPsec point-to-point connection. The right IP settings should be the same in both IPsec endpoints. Enter the interface IP address of the right endpoint that can directly connected to the left endpoint. For example, a WAN port IP address or cellular IP address.

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

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

Right RSA Key: The attribute is only required when using the RSA key authentication method using the public key which was generated from the top-half of this page.



IPsec Settings

Public Key Management

Generate Public Key:	Generate Key...
Current Public Key:	0sAQN1RVpbnioBXcoSg8oUABg7+YNn0h6sR2R POYzWKlYB98SaWfyiGpohuWDA9Nn6biDRVkyZl GVoWY7stRVxETIPrLjl0Pk9STrWhOOaoZL8SzYyf X6HcW4tvWUCVCAKrAwAge6Zimz0bztnrdzK9s7 DXAO5OmiqNg9XZe2G+OBWuCOogH2XSeWQO qF0Eq9U6EqznhLQ0gpi9txQ28boJ/s8T8QBtvcfrC orh/buu8PRWiHYT6MasXAOo5GQ5VMPvJGup42 USVuOH1NDGJVVqOw+dZAykhIoWk4ChOTo8U TmFDK7srprSw7sXde5FeivZSgNHCweV0FCPm6P yeHFPFmB2+3SmYlybbfnYThatUIVuftp

☐ Enable IPsec Connection

Interfaces for IPsec to Use :	LAN ▼
Authentication Method :	RSA Key ▼
ESP Algorithm :	AES128 ▼
Left - IP of network interface :	192.168.1.1
Left Source IP Address :	0.0.0.0
Left Subnet (network/netmask) :	(Ex : 192.168.10.0/24)
Left RSA Key :	
Right - IP of network interface :	192.168.1.2
Right Source IP Address :	0.0.0.0
Right Subnet (network/netmask) :	(Ex : 192.168.20.0/24)
Right RSA Key :	

Apply Cancel

Chapter 5

Configuration – SNMP, CLI, View Utility

Chapter 5 Configuration – SNMP, CLI, View Utility

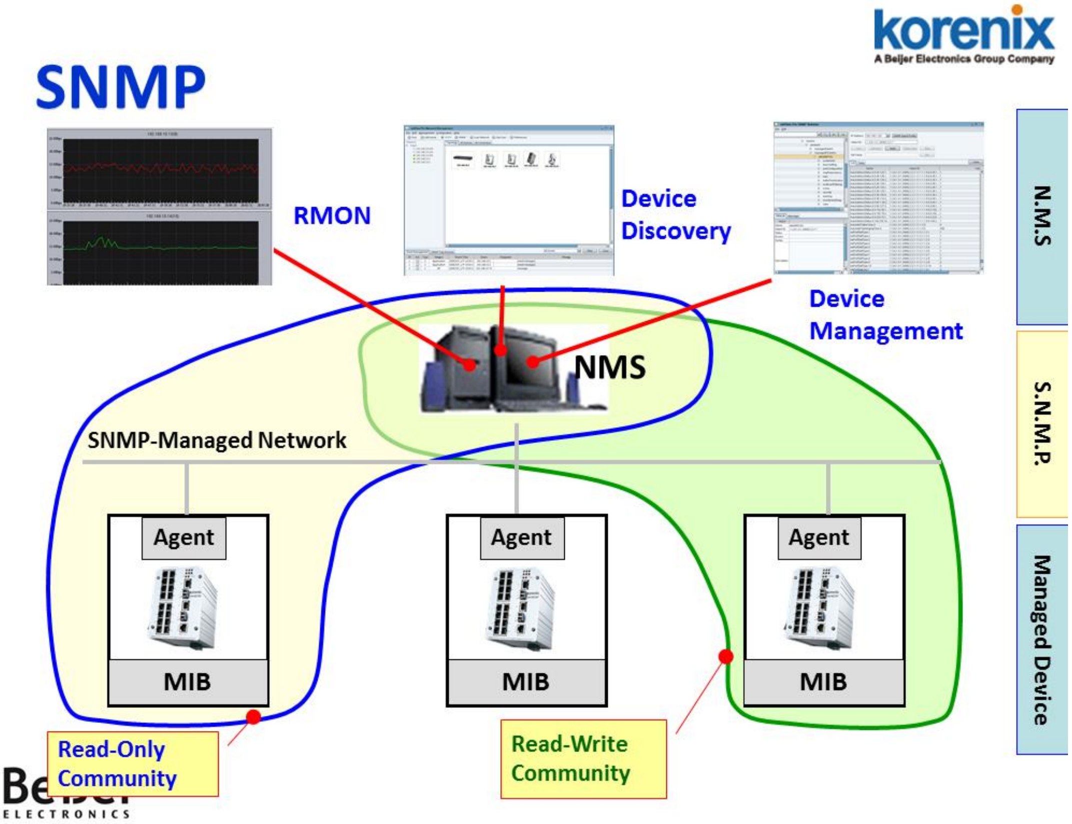
5.1 SNMP

5.1.1 What is SNMP?

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

Typical SNMP Architecture:

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



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

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

Community:

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

SNMP Setup:

Please refer to the **4.5.1 Remote Setting.**

5.1.2 Management Information Base (MIB):

Before you want to manage the JetWave 3200 series AP/Gateway through SNMP, please go to download the MIB files from Korenix web site and compile all of them to the NMS. The AP/Gateway supports function based MIB, the same function/parameters in all the models have the same object ID (OID). The benefit is you just need to compile the MIB file one time even you purchase different models. While you purchase our new released models in the future, the MIB file can be applied as well. Once we provide new features for the MIB, you just need one time effort to update the MIB table for all the models.

There are some MIB files which are:

a. JETWAVE-DEVICE-MIB.my: This is the JetWave Device Management object MIB.

b. JETWAVE-EVENT-MIB.my: This is the JetWave Event/Trap MIB.

c. JETWAVE-ROOT-MIB.my: This is the JetWave top level object MIB.

d. JETWAVE-SERIAL-MIB.my: This is the JetWave Serial Port object MIB.

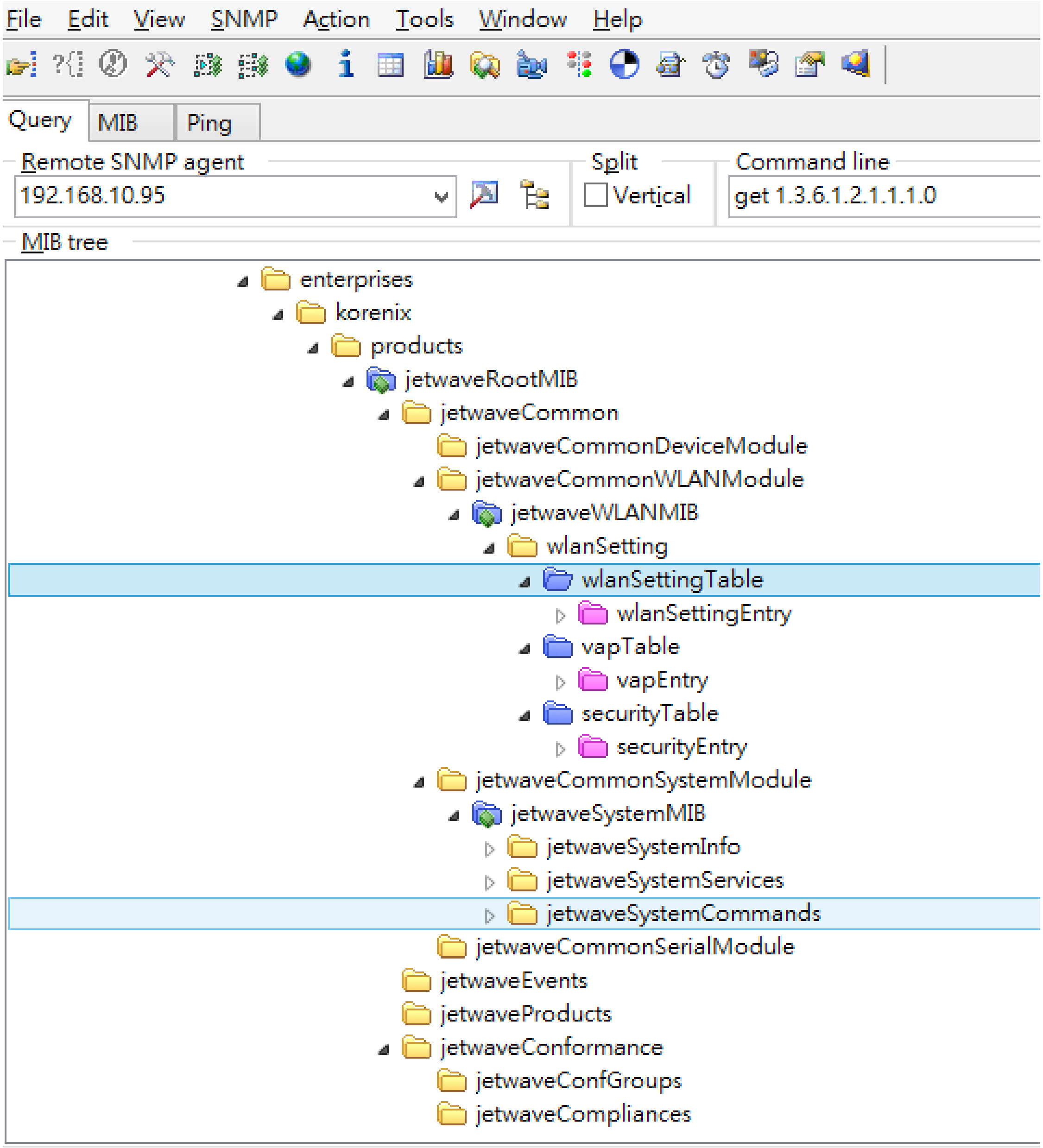
e. JETWAVE-SYSTEM-MIB.my: This is the JetWave System objects MIB.

f. JETWAVE-WALN-MIB.my: This is the JetWave Wireless LAN Setting object MIB.

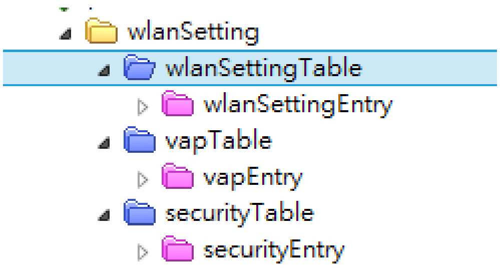
(Please download the latest MIB file from Korenix web site.)

5.1.3 MIB Tree in NMS

.The below figure shows the MIB tree after compiled in the NMS.

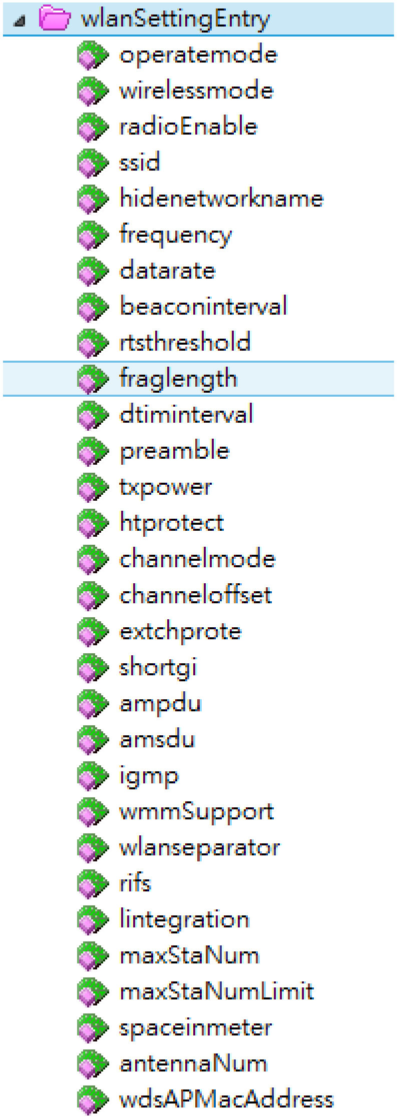


Example: wlanSetting



- wlanSetting
  - wlanSettingTable
    - wlanSettingEntry
  - vapTable
    - vapEntry
  - securityTable
    - securityEntry

wlanSettingEntry:



- wlanSettingEntry
  - operatemode
  - wirelessmode
  - radioEnable
  - ssid
  - hidenetworkname
  - frequency
  - datarate
  - beaconinterval
  - rtsthreshold
  - fraglength
  - dtiminterval
  - preamble
  - txpower
  - htprotect
  - channelmode
  - channeloffset
  - extchprote
  - shortgi
  - ampdu
  - amsdu
  - igmp
  - wmmSupport
  - wlanseparator
  - rifs
  - lintegration
  - maxStaNum
  - maxStaNumLimit
  - spaceinmeter
  - antennaNum
  - wdsAPMacAddress

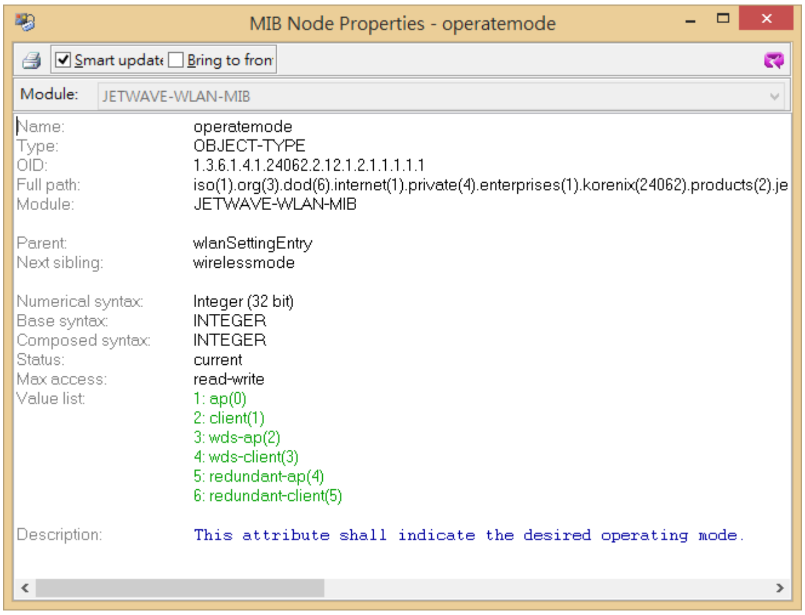
Example of Object in wlanSettingEntry

Operatemode: (Operation Mode)

The OID: 1.3.6.1.4.1.24062.2.12.1.1.1.1.1

Max Access: read-write (Read and Write)

Value list: you can read the value or set a new value according to the value list. This is the same as web GUI and CLI.



Module: JETWAVE-WLAN-MIB

```
Name:                operatemode
Type:                OBJECT-TYPE
OID:                 1.3.6.1.4.1.24062.2.12.1.2.1.1.1.1.1
Full path:           iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).korenix(24062).products(2).je
Module:              JETWAVE-WLAN-MIB

Parent:              wlanSettingEntry
Next sibling:        wirelessmode

Numerical syntax:    Integer (32 bit)
Base syntax:         INTEGER
Composed syntax:     INTEGER
Status:              current
Max access:          read-write
Value list:          1: ap(0)
                     2: client(1)
                     3: wds-ap(2)
                     4: wds-client(3)
                     5: redundant-ap(4)
                     6: redundant-client(5)

Description:         This attribute shall indicate the desired operating mode.
```

Select the OID and press the Right key of the mouse. You can see the tool set to read or write new value.

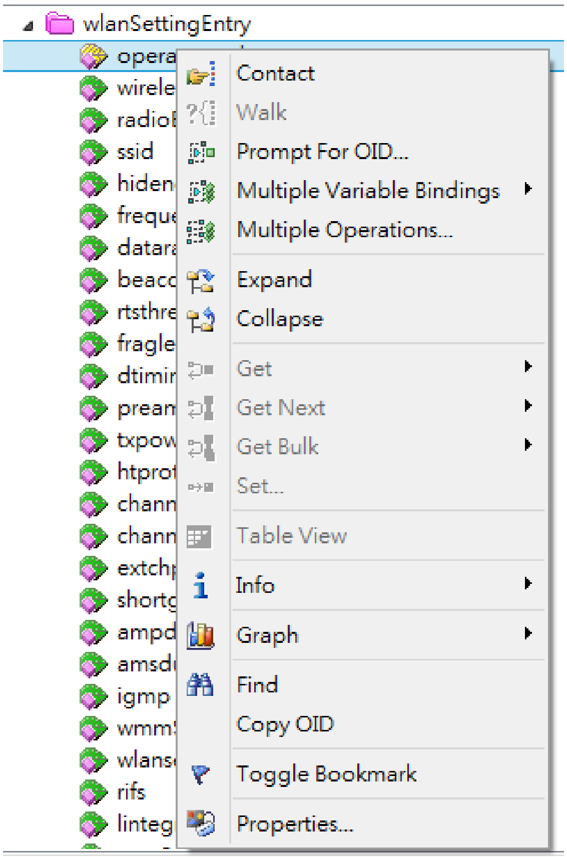
Get: Read the value of the selected OID.

GetNext: Read the value of the next OID.

GetBulk: Read the value of the next 10 OID.

Set: Set new value for the selected OID.

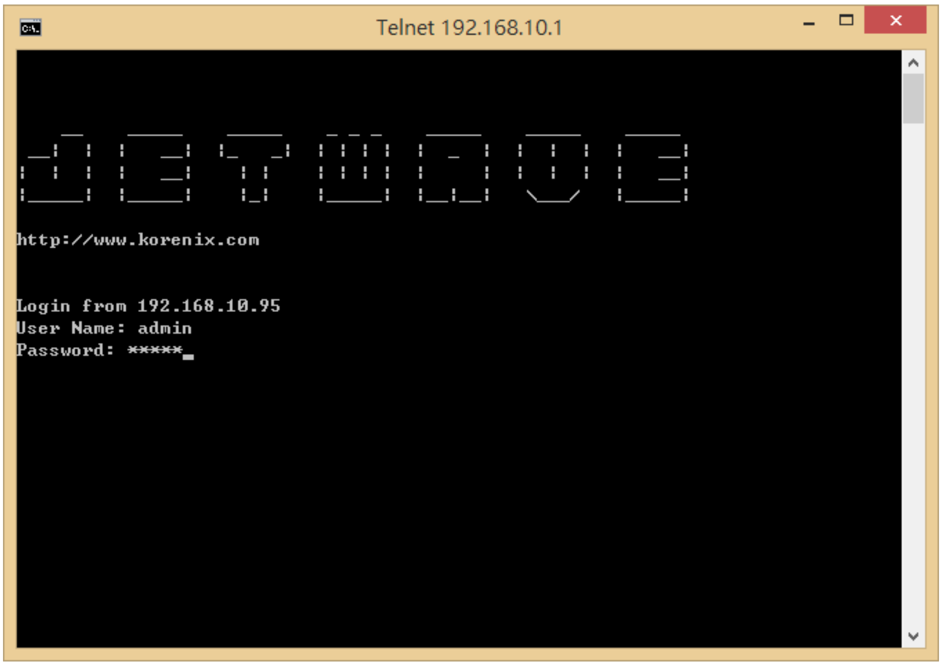
Property: See the MIB Node information.



5.2 Command Line Interface (CLI)

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

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



```
http://www.korenix.com


Login from 192.168.10.95
User Name: admin
Password: *****_
```

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

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

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

LIST: This is Help command to show the usage information of the command.

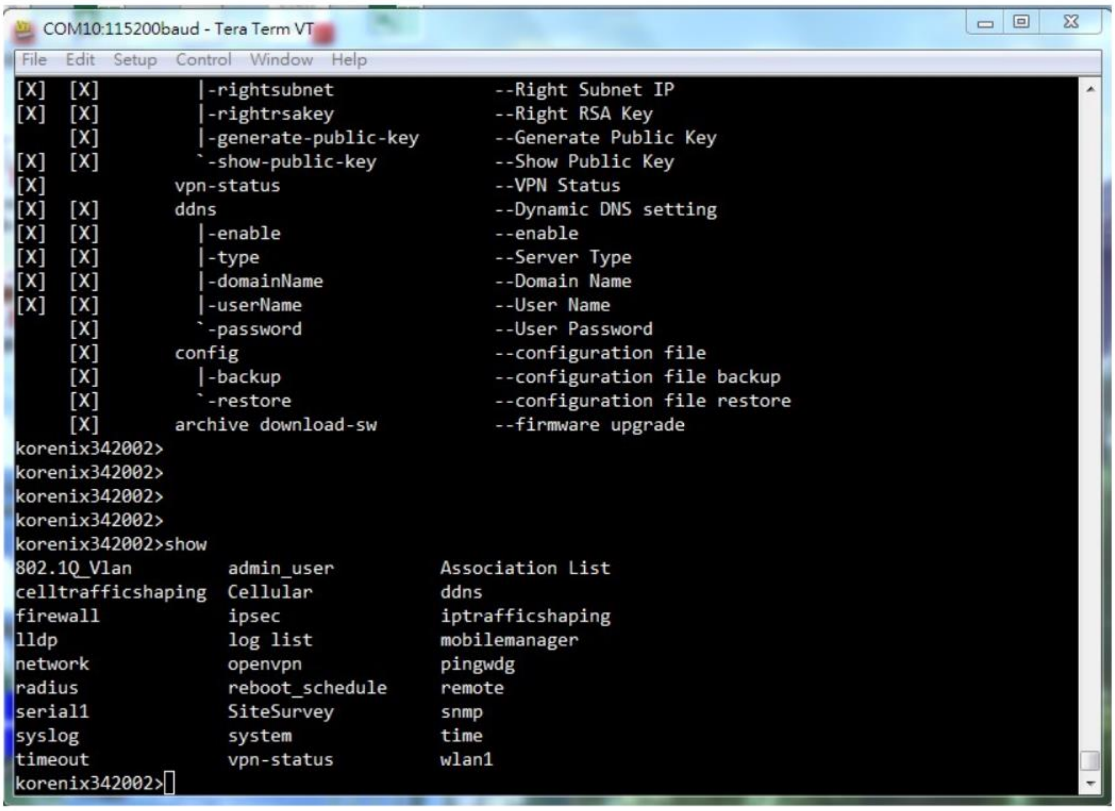
Del: This is Delete command to delete the applied settings.

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

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

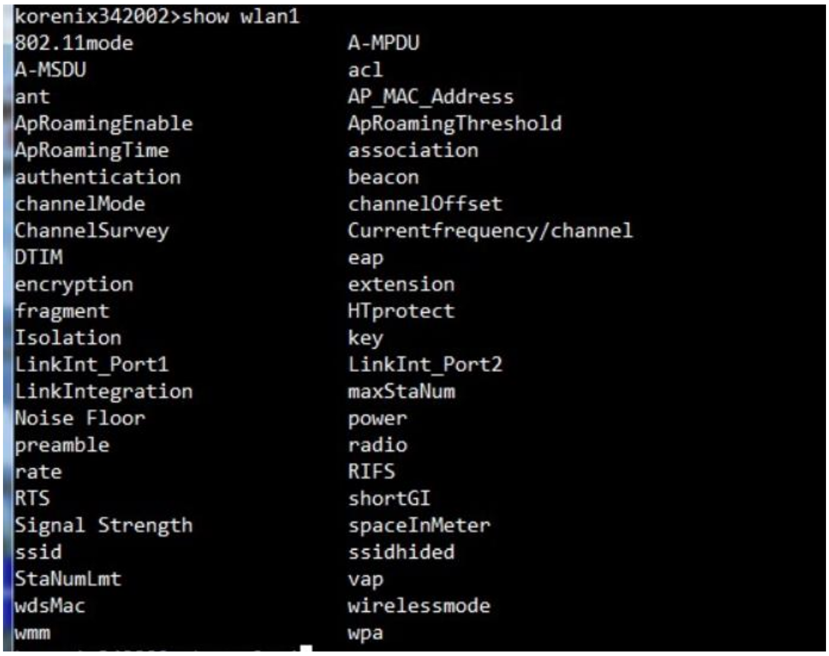
5.2.1 SHOW Command Set:

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


COM10:115200baud - Tera Term VT
File Edit Setup Control Window Help

```
[X]  [X]        |-rightsubnet            --Right Subnet IP
[X]  [X]        |-rightrsakey            --Right RSA Key
     [X]        |-generate-public-key    --Generate Public Key
[X]  [X]        `-show-public-key        --Show Public Key
[X]           vpn-status                 --VPN Status
[X]  [X]      ddns                       --Dynamic DNS setting
[X]  [X]        |-enable                 --enable
[X]  [X]        |-type                   --Server Type
[X]  [X]        |-domainName             --Domain Name
[X]  [X]        |-userName               --User Name
     [X]        `-password               --User Password
     [X]      config                     --configuration file
     [X]        |-backup                 --configuration file backup
     [X]        `-restore                --configuration file restore
     [X]      archive download-sw        --firmware upgrade
korenix342002>
korenix342002>
korenix342002>
korenix342002>
korenix342002>show
802.1Q_Vlan          admin_user          Association List
celltrafficshaping   Cellular            ddns
firewall             ipsec               iptrafficshaping
lldp                 log list            mobilemanager
network              openvpn             pingwdg
radius               reboot_schedule     remote
serial1              SiteSurvey          snmp
syslog               system              time
timeout              vpn-status          wlan1
korenix342002>
```

Type **Show wlan** + **“Tab↹”** to see all the show wlan command lines.



```
korenix342002>show wlan1
802.11mode                 A-MPDU
A-MSDU                     acl
ant                        AP_MAC_Address
ApRoamingEnable            ApRoamingThreshold
ApRoamingTime              association
authentication             beacon
channelMode                channelOffset
ChannelSurvey              Currentfrequency/channel
DTIM                       eap
encryption                 extension
fragment                   HTprotect
Isolation                  key
LinkInt_Port1              LinkInt_Port2
LinkIntegration            maxStaNum
Noise Floor                power
preamble                   radio
rate                       RIFS
RTS                        shortGI
Signal Strength            spaceInMeter
ssid                       ssidhided
StaNumLmt                  vap
wdsMac                     wirelessmode
wmm                        wpa
```

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

```
korenixffffff>show wlan

wlan wirelessmode           : AP
wlan ssid                 : 3200
wlan ssidhided             : Disabled
wlan radio                : Enabled
wlan 802.11mode             : 802.11G/N
wlan HTprotect             : Disabled
wlan Currentfrequency/channel: 2442MHz (7)
wlan Noise Floor          : -106 dBm
wlan AP_MAC_Address           : 60:02:b4:78:63:11
wlan power                 : 7
wlan rate                 : Auto
wlan antenna number         : two antenna
wlan wmm                     : Enabled
wlan Isolation            : Disabled
wlan maxStaNum               : 64
wlan StaNumLmt               : Disabled
wlan spaceInMeter          : 0
wlan LinkIntegration      : disabled
wlan channelMode            : 20 MHz
wlan channelOffset         : None
wlan extension             : No Protection
wlan A-MPDU                 : Enabled
wlan A-MSDU                 : Disabled
wlan shortGI               : Disabled
wlan RIFS                  : Enabled
wlan RTS                   : 2347
wlan fragment              : 2346
wlan beacon                : 100
wlan DTIM                  : 1
wlan preamble              : Auto
wlan IGMP                   : Enabled
wlan authentication       : WPA with Radius
wlan encryption            : TKIP
wlan key type             : None
wlan key default          : 4
wlan wpa psk               : 12345678
wlan wpa keyupdate mode      : Never
wlan wpa keyupdate sec      : 3600
wlan wdsMac remote          : 00:00:00:00:00:00
wlan acl mode              : disabled
wlan acl entry                : NULL
wlan acl list:
              index              MAC address
         ========== ====================
               NULL                    NULL

wlan RoamingEnable           : Disabled
wlan RoamingThreshold        : -80
wlan RoamingDiff           : 3
wlan RoamingScanChannel1      : 2437MHz (6)
wlan RoamingScanChannel2      : Not scanning
wlan RoamingScanChannel3      : Not scanning
wlan full11a              : Disabled
```

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

korenixffffff>show wlan ra (+Tab)

radio rate

korenixffffff>show wlan rad (+Tab)

radio rate

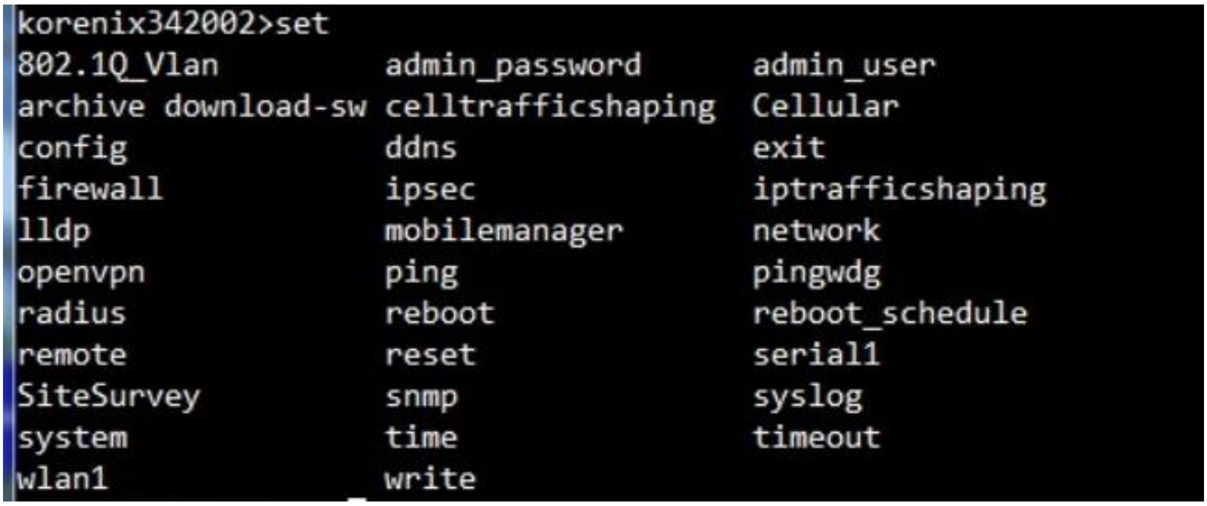
korenixffffff>show wlan radio (+ Enter)

wlan radio : Enabled (This is the result.)

Please check the List command set to know the usage of all commands.

5.2.2 Set Command Set:

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



```
korenix342002>set
802.1Q_Vlan          admin_password       admin_user
archive download-sw  celltrafficshaping   Cellular
config               ddns                 exit
firewall             ipsec                iptrafficshaping
lldp                 mobilemanager        network
openvpn              ping                 pingwdg
radius               reboot               reboot_schedule
remote               reset                serial1
SiteSurvey           snmp                 syslog
system               time                 timeout
wlan1                write
```

The most Set comment lines have the same functionality as the the Web GUI configuration we introduce in chapter 4. Please read chapter 4 to know all the features our AP/Gateway supported. And the CLI is a different way for you to complete the setting.

Example: Set the remote configuration (Refer to the 4.5.1 – Remote Configuration)

korenixffffff>set remote (+Tab)

email alter event warning forcehttps smtp
snmp snmptrap ssh telnet

Example: SNMP Enable/Disable:
korenixffffff>set remote snmp
Disabled Enabled
korenixffffff>set remote snmp Disabled
remote snmp : Disabled

```
    korenixffffff>set remote snmp Enabled
    remote snmp                          : Enabled
    korenixffffff>
```

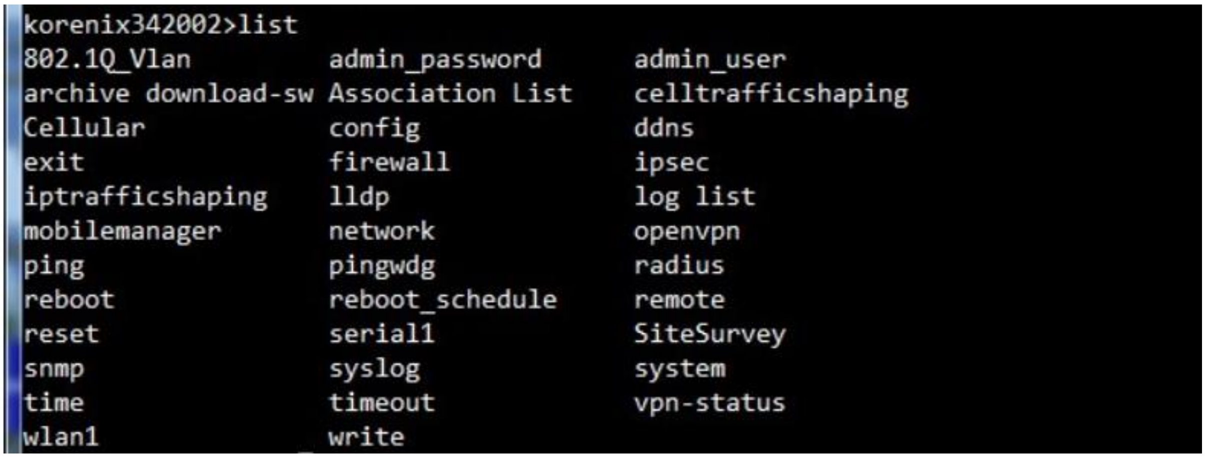
====SNMP Setting=========

The SNMP command lines and how to set SNMP version, community name, trap server.

```
korenixffffff>set snmp (+Tab)
getCommunity      port               setCommunity      trapcommunity
trapdestination v3Admin              v3User            version

korenixffffff>set snmp version V2
snmp version                         : V2

korenixffffff>set snmp getCommunity orwell
snmp getCommunity                    : orwell

korenixffffff>set snmp setCommunity orwell
snmp setCommunity                    : orwell

korenixffffff>set snmp trapdestination 192.168.10.95
snmp trapdestination                 : 192.168.10.95

korenixffffff>set snmp trapcommunity orwell
snmp trapcommunity                   : orwell
```

5.2.3 List Command Set:

Type **List** + **"Tab↹"** to see all the command usage. This is similar to the Help command.



```
korenix342002>list
802.1Q_Vlan             admin_password         admin_user
archive download-sw     Association List       celltrafficshaping
Cellular                config                 ddns
exit                    firewall               ipsec
iptrafficshaping        lldp                   log list
mobilemanager           network                openvpn
ping                    pingwdg                radius
reboot                  reboot_schedule        remote
reset                   serial1                SiteSurvey
snmp                    syslog                 system
time                    timeout                vpn-status
wlan1                   write
```

Below command is to list the remote configuration command line and its description.

```
korenixffffff>list remote
show set del    keyword                    Description
---- --- ---    ---------------------      ------------------------------
[X]  [X]          |-telnet                   --enable telnet
[X]  [X]          |-snmp                     --enable snmp
[X]  [X]          |-ssh                      --enable ssh
[X]  [X]          |-forcehttps                --force https
[X]  [X]          |-snmptrap                 --enable snmp trap
[X]  [X]          |-email alter              --enable email alert
[X]  [X]          |-event warning             --event warning
[X]  [X]          | |-association            --wlan association
[X]  [X]          | |-authentication         --authentication fail
[X]  [X]          | `-config                  --config change
[X]  [X]  [X]     `-smtp                      --smtp setting
[X]  [X]             |-sender                 --smtp sender
     [X]             |-server                 --smtp server
[X]  [X]             |-authType                --authentication type
[X]  [X]             |-username               --mail server username
     [X]             |-password                --mail server password
[X]  [X]  [X]        |-email1                  --receiver 1 email
[X]  [X]  [X]        `-email2                  --receiver 2 email
```

show, set and del: Which privilege the command has? [X] means Yes.

Keyword: The command you should enter in the CLI.

Description: Short description of the usage of the command.

5.2.4 Delete Command Set:

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

```
korenixffffff>del
log list      remote         wlan            wlan2
```

The log list can be delete through CLI.

```
korenixffffff>del log list
```

The configured smtp email addresses can be delete through CLI.

```
korenixffffff>del remote smtp
email1    email2
```

The below wlan 1 settings can be delete through CLI. (JetWave 3220/3420 1st Radio)

```
korenixffffff>del wlan
acl eap key wpa
```

The below wlan 2 settings can be delete through CLI. (JetWave 3220 2nd Radio)

```
korenixffffff>del wlan2
acl eap key wpa
```

5.3 Korenix View Utility

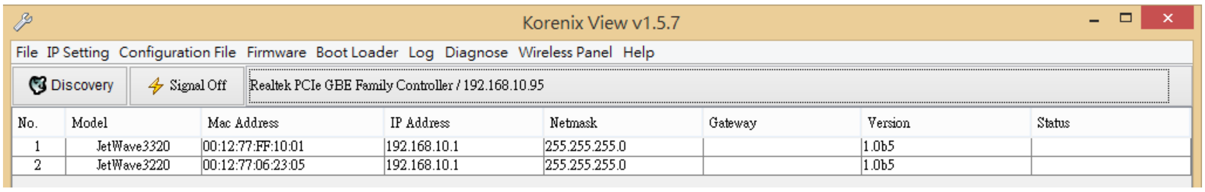
The Korenix View Utility (rename from the JetView V1.5.7) provides you convenient tool to scan the network and configure the AP. Please connect your PC to port Eth 2 (LAN) and start below steps to scan and configure.

5.3.1 Device Discovery:

Step 1: Open the Korenix View Utility. (Must later than V1.5.7)

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

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


Korenix View v1.5.7
File IP Setting Configuration File Firmware Boot Loader Log Diagnose Wireless Panel Help
Discovery
Signal Off

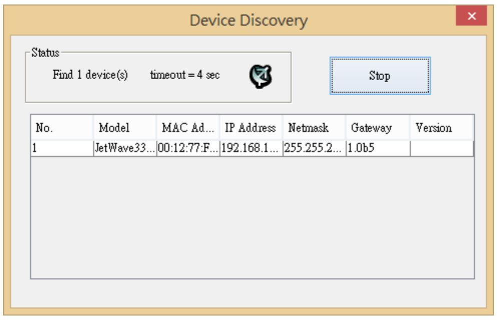
Realtek PCIe GBE Family Controller / 192.168.10.95

No.	Model	Mac Address	IP Address	Netmask	Gateway	Version	Status
1	JetWave3320	00:12:77:FF:10:01	192.168.10.1	255.255.255.0		1.0b5	
2	JetWave3220	00:12:77:06:23:05	192.168.10.1	255.255.255.0		1.0b5	

Figure: The main screen of the Korenix View Utility

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

5.3.2 Basic Tools Shortcut:



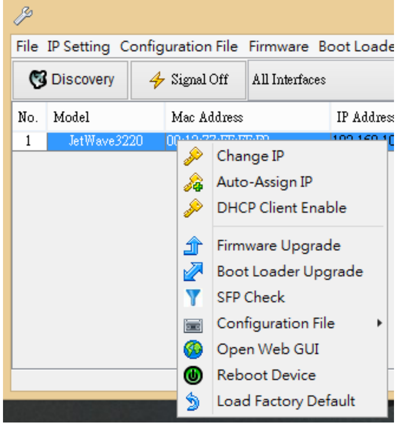
Find 1 device(s) timeout = 4 sec

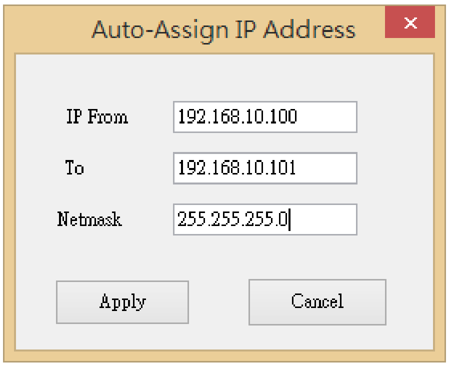
No.	Model	MAC Ad...	IP Address	Netmask	Gateway	Version
1	JetWave33...	00:12:77:F...	192.168.1...	255.255.2...	1.0b5	

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

a. You can modify the IP address/Netmask directly on the field and then click “**Change IP“** to change the IP settings.

b. Select multiple devices and click “**Auto-Assign IP**”, the popup screen will ask you type the IP Address range. You can assign new IP address for the selected devices.





IP From 192.168.10.100

To 192.168.10.101

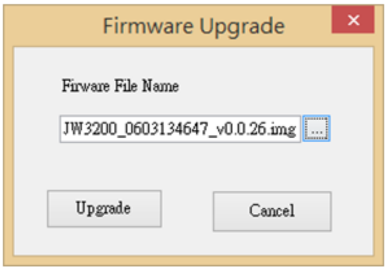
Netmask 255.255.255.0

Figure: Assign the Auto-Assign IP Range.

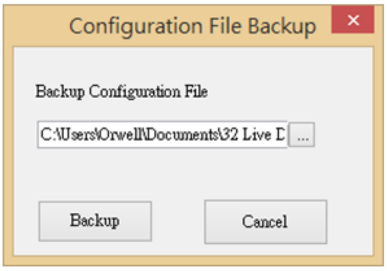
c. You can enable DHCP client by “DHCP Client Enable”.

d. You can upgrade firmware for single or multiple units by **“Firmware Upgrade”**. A popup screen will ask you select the target firmware file you’d like to upgrade.

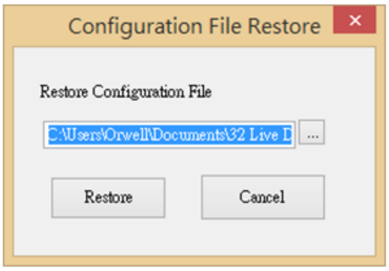
e. You can Backup/Restore the configuration file by “**Configuration File -> Backup/Restore”**. A popup screen will ask you select target configuration/target folder you’d like to backup or restore.



Firware File Name JW3200_0603134647_v0.0.26.img



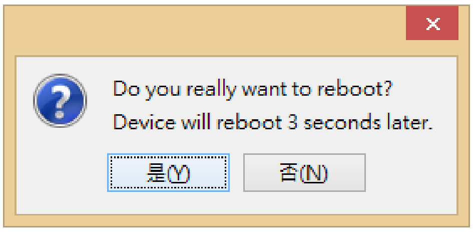
Backup Configuration File C:\Users\Orwell\Documents\32 Live D



Restore Configuration File C:\Users\Orwell\Documents\32 Live D

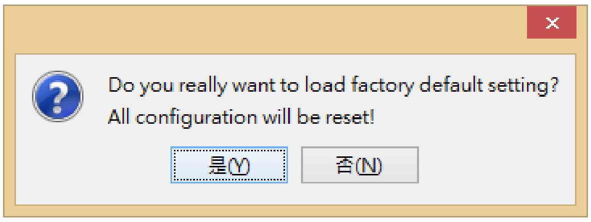
f. Click “**Open Web GUI**” to access the web management interface.

g. You can reboot the device by “**Reboot Device**”. A popup screen will ask you confirm again.



Do you really want to reboot?
Device will reboot 3 seconds later.

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

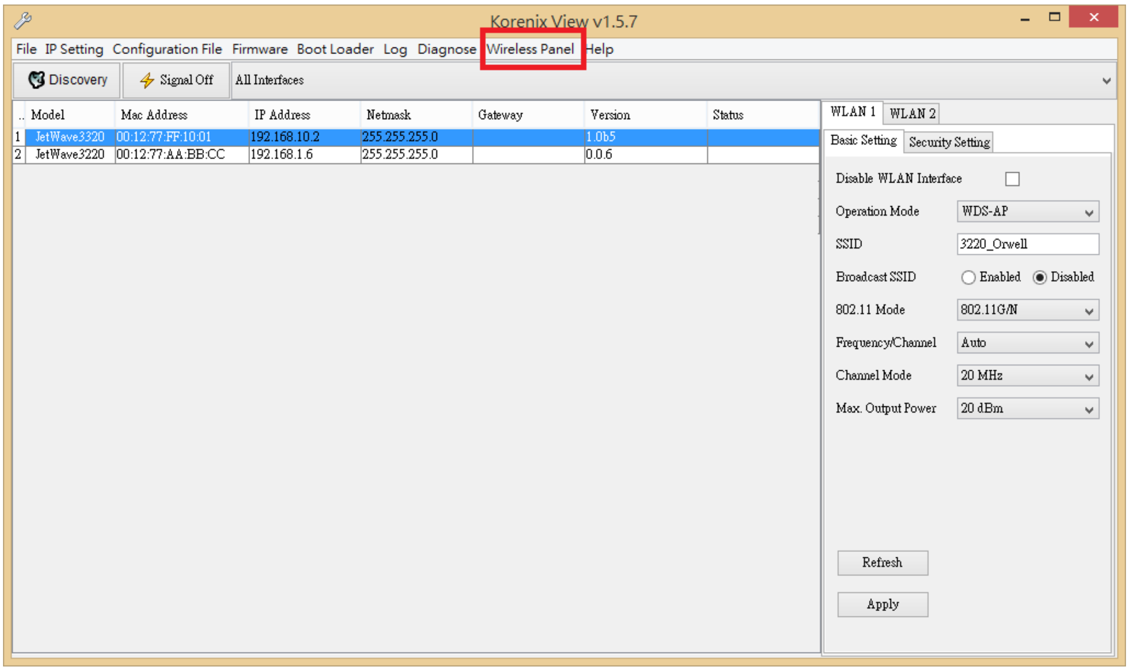


Do you really want to load factory default setting?
All configuration will be reset!

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

5.3.3 Wireless Panel

New version Korenix View Utility provides Wireless panel to configure some **Basic Setting** and **Security setting** for Wireless LAN Interfaces. You can use the tool to configure settings for single device or a group of devices. Select the target device/devices for further configuration.


Korenix View v1.5.7
File IP Setting Configuration File Firmware Boot Loader Log Diagnose Wireless Panel Help
Discovery
Signal Off
All Interfaces

..	Model	Mac Address	IP Address	Netmask	Gateway	Version	Status
1	JetWave3320	00:12:77:FF:10:01	192.168.10.2	255.255.255.0		1.0b5	
2	JetWave3220	00:12:77:AA:BB:CC	192.168.1.6	255.255.255.0		0.0.6	

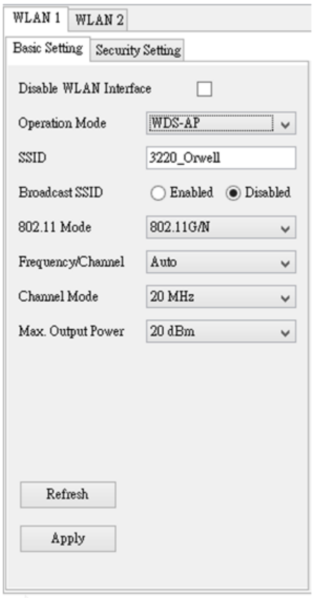
Disable WLAN Interface □
Operation Mode: WDS-AP
SSID: 3220_Orwell
Broadcast SSID: ○ Enabled ● Disabled
802.11 Mode: 802.11G/N
Frequency/Channel: Auto
Channel Mode: 20 MHz
Max. Output Power: 20 dBm

Click **"Refresh"** to load the current configuration of the selected AP/Gateway.

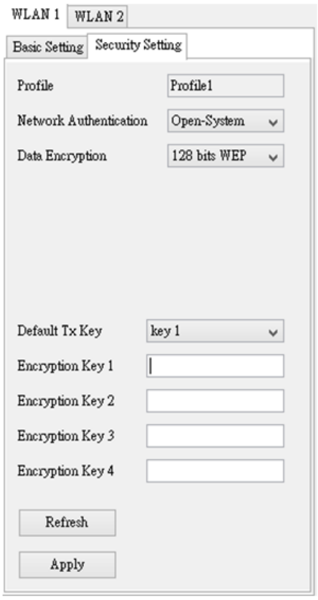
Basic Setting:

The Basic Setting panel allows you Disable WLAN Interface, configure the Operating Mode, SSID, Broadcast SSID Enable/Disable, 802.11 Mode, Frequency/Channel, Channel Mode and Max. output power.

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



Disable WLAN Interface □
Operation Mode: WDS-AP
SSID: 3220_Orwell
Broadcast SSID: ○ Enabled ● Disabled
802.11 Mode: 802.11G/N
Frequency/Channel: Auto
Channel Mode: 20 MHz
Max. Output Power: 20 dBm



Profile: Profile1
Network Authentication: Open-System
Data Encryption: 128 bits WEP
Default Tx Key: key 1
Encryption Key 1:
Encryption Key 2:
Encryption Key 3:
Encryption Key 4:

Security Setting:

The Security Setting panel allows you to configure the Network Authentication type and the encryption keys for the AP profile.

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

Chapter 6

Troubleshooting

Chapter 6 Troubleshooting

This chapter provides troubleshooting procedures for basic problems with the JetWave 3220v3/3420v3. For warranty assistance, contact your service provider or distributor for the process.

6.1 General Question

6.1.1 How to know the MAC address of the 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.

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

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

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

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

Please check the followings:

- Check whether the IP address of PC is correct (in the same network segment as the unit)
- Login the unit via other browsers such as Firefox, Google Chrome.
- Use 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.

6.2 Wireless/Cellular

6.2.1 What if the wireless connection is not stable after associating with an AP under wireless client mode?

- In addition, you can start "**Site Survey**" to check the signal strength. If it is weak or unstable (The smaller the number is, the weaker the signal strength is.), please join other available AP for better connection.
- If you install the directional antenna for point to point/multi-point connection, adjust the antenna and tune the signal strength/performance by Antenna Alignment Tool again. After antenna alignment, the data rate test can help you check the current performance.
- In Wireless client mode, type the connected AP' MAC address to fix the AP for your client. It avoid your wireless client not to connect other AP.

6.2.2 What if the wireless connection performance is not good, how to improve it?

- Once the signal strength RSSI is always under **-65dbm** in long distance transmission, it is suggest you to change antenna's direction or replace antenna with higher gain.
- Check the "**Space in meter**" setting in **"Wireless Advance Setting"**. Correct the distance can help improve the transmission quality.
- If the distance between the wireless client and target AP is short, but, the antenna gain is very high. Reduce the RF power is also an option.

6.2.3 What if the LTE connection is not stable or 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 LTE band or not? Normally, the outlook of the LTE

antenna is the same.

- Check with the ISP and ask them check LTE 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 LTE 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 LTE connection for a while, once the ping is often timeout, check the status before leave the device on site.

6.2.4 What if the LTE connection is always disconnected, how to resolve it?

- Make sure the SIM card is not damaged and you insert the SIM card before power on the device. Note: If the device supports LTE 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 LTE 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 LTE band or not? Normally, the outlook of the LTE antenna is the same.
- Download the screen message and debug message to our service engineer.

6.3 Appendix

6.3.1 ASCII

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

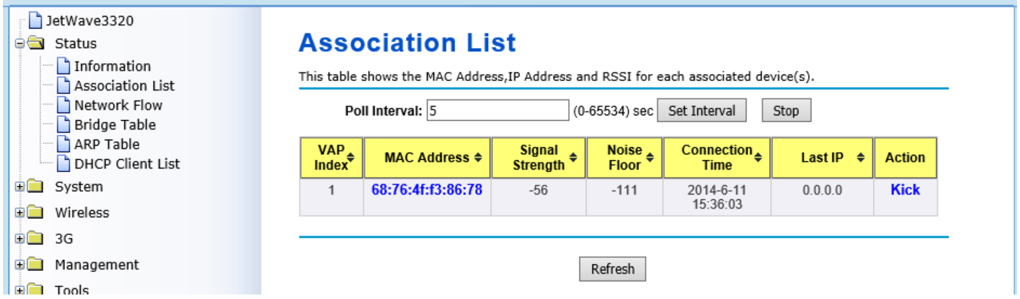
ASCII Table

ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent
!	21	9	39	Q	51	i	69
"	22	:	3A	R	52	j	6A
#	23	;	3B	S	53	k	6B
$	24	<	3C	T	54	l	6C
%	25	=	3D	U	55	m	6D
&	26	>	3E	V	56	n	6E
‘	27	?	3F	W	57	o	6F
(	28	@	40	X	58	p	70
)	29	A	41	Y	59	q	71
*	2A	B	42	Z	5A	r	72
+	2B	C	43	[	5B	s	73
,	2C	D	44	\	5C	t	74
-	2D	E	45	]	5D	u	75
.	2E	F	46	^	5E	v	76
/	2F	G	47	_	5F	w	77
0	30	H	48	`	60	x	78
1	31	I	49	a	61	y	79
2	32	J	4A	b	62	z	7A
3	33	K	4B	c	63	{	7B
4	34	L	4C	d	64	|	7C
5	35	M	4D	e	65	}	7D
6	36	N	4E	f	66	~	7E
7	37	O	4F	g	67		
8	38	P	50	h	68		

6.3.2 RSSI Conversion

RSSI Conversion in JetWave 3220/3420 Series WIFI:

RSSI is short of the **Received Signal Strength Indicator,** is a measurement of the power present in a received radio signal. In Korenix web GUI, you can see the two related values:



Association List

This table shows the MAC Address,IP Address and RSSI for each associated device(s).

Poll Interval: 5 (0-65534) sec

VAP Index	MAC Address	Signal Strength	Noise Floor	Connection Time	Last IP	Action
1	68:76:4f:f3:86:78	-56	-111	2014-6-11 15:36:03	0.0.0.0	Kick

Signal Strength: The signal strength of the associated device. The value can help you to see the connection quality of AP/WDS-AP and Client/WDS-Client.

Noise Floor: The Noise Floor of the associated device.

Different suppliers may use different way to display the signal strength. In korenix JetWave 3200/3400 series, the RSSI = Signal Strength – Noise Floor – 95 (defined by chipset provider).

The RSSI example of above figure is -56 – (-111) -95 = 55 -95 = -40

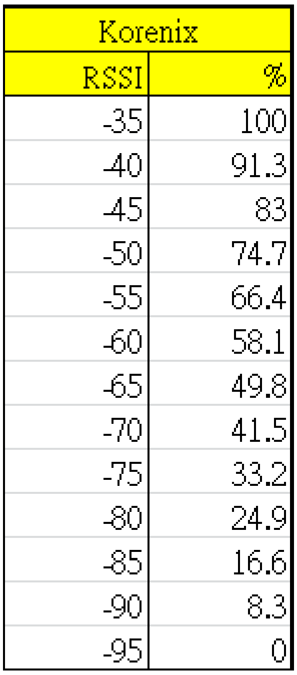
JetWave 3200/3400 series RSSI Conversion:

RSSI_Max = 60

The RSSI of is range from -35dBm (100%) ~ -95dBm (0%).

Ex: From the value in above example, you can convert -40dBm to around 91.3% of maximum radio power. The link quality is very good. The figure in the right is the lookup table for your reference.

While comparing Korenix product with other competitors, you can follow the way to convert Korenix RSSI to % of the maximum RF Tx Power of other products.



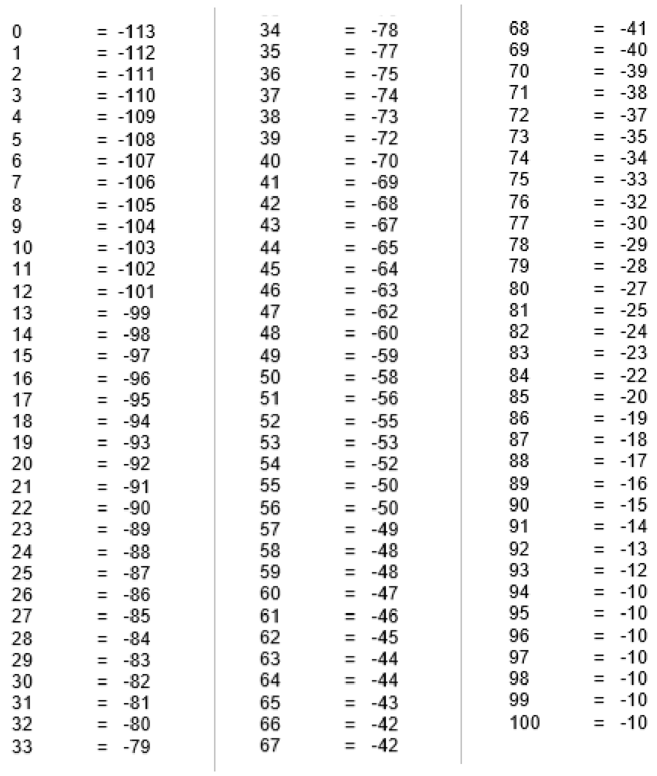
Korenix	
RSSI	%
-35	100
-40	91.3
-45	83
-50	74.7
-55	66.4
-60	58.1
-65	49.8
-70	41.5
-75	33.2
-80	24.9
-85	16.6
-90	8.3
-95	0

RSSI Conversion in Cisco for reference:

Cisco has the most granular dBm lookup table.

RSSI_Max = 100, Range from -10~-113dBm

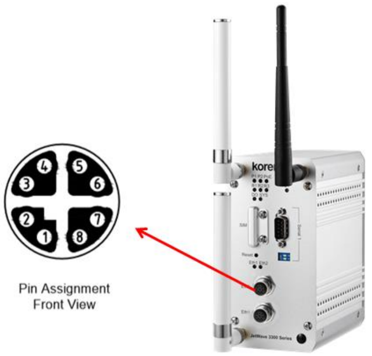
Convert % to RSSI in the following table. The RSSI is on the left, and the corresponding dBm value (a negative number) is on the right.



0	=	-113
1	=	-112
2	=	-111
3	=	-110
4	=	-109
5	=	-108
6	=	-107
7	=	-106
8	=	-105
9	=	-104
10	=	-103
11	=	-102
12	=	-101
13	=	-99
14	=	-98
15	=	-97
16	=	-96
17	=	-95
18	=	-94
19	=	-93
20	=	-92
21	=	-91
22	=	-90
23	=	-89
24	=	-88
25	=	-87
26	=	-86
27	=	-85
28	=	-84
29	=	-83
30	=	-82
31	=	-81
32	=	-80
33	=	-79
34	=	-78
35	=	-77
36	=	-75
37	=	-74
38	=	-73
39	=	-72
40	=	-70
41	=	-69
42	=	-68
43	=	-67
44	=	-65
45	=	-64
46	=	-63
47	=	-62
48	=	-60
49	=	-59
50	=	-58
51	=	-56
52	=	-55
53	=	-53
54	=	-52
55	=	-50
56	=	-50
57	=	-49
58	=	-48
59	=	-48
60	=	-47
61	=	-46
62	=	-45
63	=	-44
64	=	-44
65	=	-43
66	=	-42
67	=	-42
68	=	-41
69	=	-40
70	=	-39
71	=	-38
72	=	-37
73	=	-35
74	=	-34
75	=	-33
76	=	-32
77	=	-30
78	=	-29
79	=	-28
80	=	-27
81	=	-25
82	=	-24
83	=	-23
84	=	-22
85	=	-20
86	=	-19
87	=	-18
88	=	-17
89	=	-16
90	=	-15
91	=	-14
92	=	-13
93	=	-12
94	=	-10
95	=	-10
96	=	-10
97	=	-10
98	=	-10
99	=	-10
100	=	-10

(The figure is captured from Internet, it is just for reference only.)

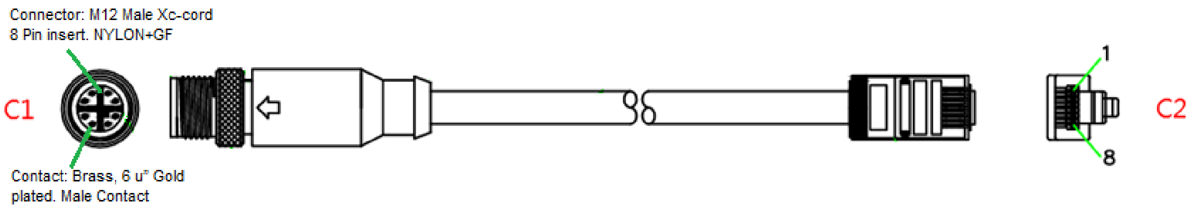
6.3.3 M12 Connector Pin Assignment

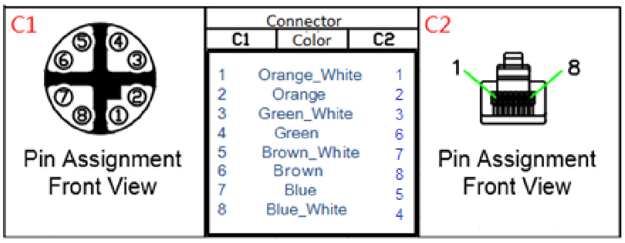


X-cord M12 Connector

M12X to RJ-45 (Shielding) Cable Pin Assignment:

Please follow below figure to assembly your cable.





Connector		
C1	Color	C2
1	Orange_White	1
2	Orange	2
3	Green_White	3
4	Green	6
5	Brown_White	7
6	Brown	8
7	Blue	5
8	Blue_White	4

M12 Connector: M12 Male Xc-cord 8 Pin insert. NYLON-GF

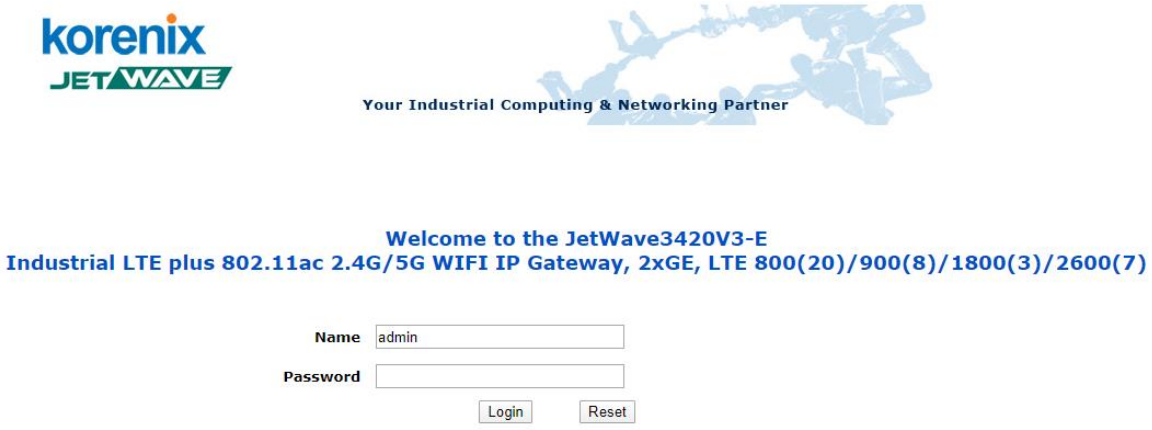
Contact: Brass, 6u" Gold plated. Male Contact

M12 (C1)	Color	RJ-45 (C2)	Functionality
1	Orange_White	1	MDX 0+
2	Orange	2	MDX 0-
3	Green_White	3	MDX 1+
4	Green	6	MDX 1-
5	Brown_White	7	MDX 3+
6	Brown	8	MDX 3-
7	Blue	5	MDX 2-
8	Blue_White	4	MDX 2+

6.3.4 JetWave 3420 Web GUI Pages

The firmware V1.1 released by Jan. 9, 2015 starts to support JetWave 3420 Series. This appendix shows the JetWave 3420 login page, Information and Main GUI.

The JetWave 3420 Login Page

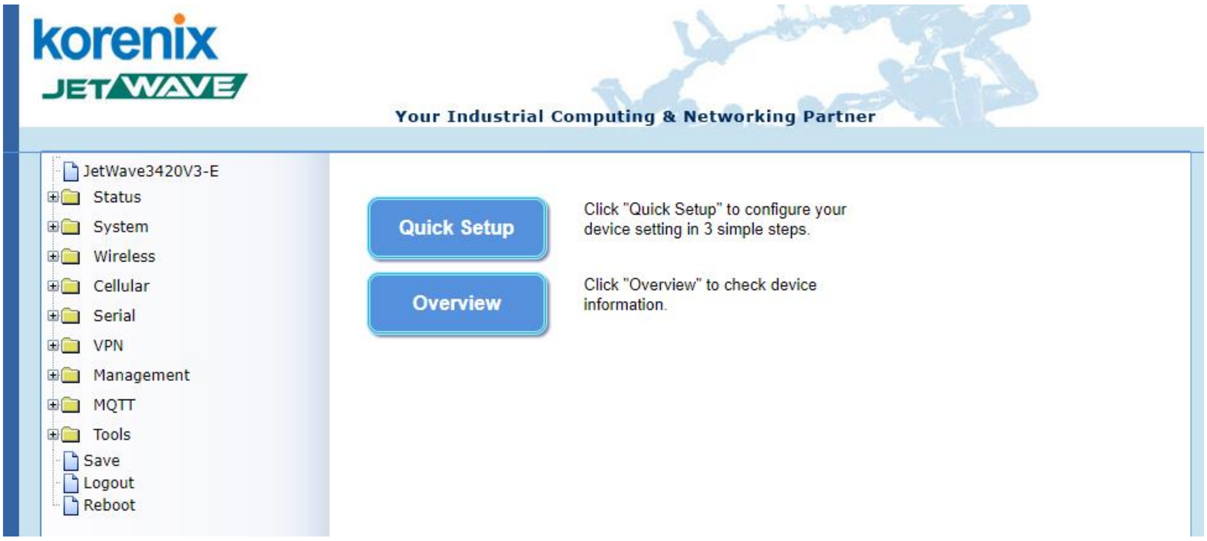


Welcome to the JetWave3420V3-E
Industrial LTE plus 802.11ac 2.4G/5G WIFI IP Gateway, 2xGE, LTE 800(20)/900(8)/1800(3)/2600(7)

Name admin

Password

The JetWave 3420 Main Entries



Click "Quick Setup" to configure your device setting in 3 simple steps.

Click "Overview" to check device information.

Revision History

Version	**Description**	**Date**	**Editor**
V1.0	1st release for JetWave 3220v3 and JetWave 3420v3.	Jan, 2020	Andrew Chen