Beijer ELECTRONICS korenix A Beijer Electronics Group Company

JetWave 4020/4020E Series

Industrial 802.11ac + 802.11n Multi-Radio Wireless AP

User Manual

V1.1 Aug., 2016

Copyright

About This Manual

This user manual provides the following notes:

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

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

Conventions

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

✎ **Note:**

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

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

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

⚠ **Warning:**

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

The Red wording is very important you must avoid.

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

Declaration of Conformity

R&TTE Directive 1999/5/EC

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

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

The declaration of R&TTE is authorized at the following company and address.

Korenix Technology Co., Ltd.

14F., No.213, Beixin Rd., Xindian Dist., New Taipei City 23143, Taiwan (R.O.C.)

TEL: +886-2-8911-1000

Safety Precautions – JetWave Wireless Product

General Notification

- Only operate the device according to the technical specification. You can find the information from the product datasheet, user manual…etc.
- Read the installation instructions before connecting the system to the power source.
- If you don’t get exact info you need, you can contact Korenix technical people, korecare@korenix.com. Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

- The devices are designed for operation with extra-low voltage (SELV). Connect the unit only to DC power source that complies with the safety extra-low voltage (SELV) requirements in IEC/EN 60950 based safety standards.

  (Not included 110V input model)

Solely connect the power supply that corresponds to the type of your device. For power connection, make sure the following requirement are met:

- The DC power circuit of the product is isolated design circuit. In practical, it is suggested to use isolated DC power design PSU for field installation. Besides the PSU selection, well digital/earth grounding is also important before power on the system.
- The Power Supply conforms to the overvoltage category I or II.
- The output voltage of the AC/DC to DC Power Supply conforms to the range of the input voltage of the equipment.
- The connection cables used are permitted for the specified electronic voltage, current, wire diameter and temperature range. (Wire Diameter of AC voltage is at least 0.75mm, AWG18. For DC voltage, it is at least 1.0mm, AWG16.)
- Follow the power installing instruction of the user manual, it indicates the input voltage, pin assignment, connection circuit and notice.
- The Power Supply must be well installed, includes grounded and other notices which are defined in its instruction guide.
- Only switch on the supply voltage to the device if the housing is closed, the terminal blocks are wired up correctly and the terminal blocks are connected.

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

PoE (Power over Ethernet) Input:

- If the product supports standard PoE Input, please make sure the voltage range of PSE comforts to the standard PoE request, maximum current and cable resistance of the Ethernet cable. Since the Ethernet cable may lead voltage drop, the CAT 5 or above standard cable is suggested, and the maximum Ethernet cable restriction is under 100 meter.
- Users MUST use the safety certificated PoE switch/injector with the PoE power input. The Industrial PoE Switch, attached PoE injector/adapter is recommended.

Environment & Housing

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

Installation

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

Please note the following things as well:

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

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

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

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

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

Content

Chapter 1

Introduction

Chapter 1 Introduction

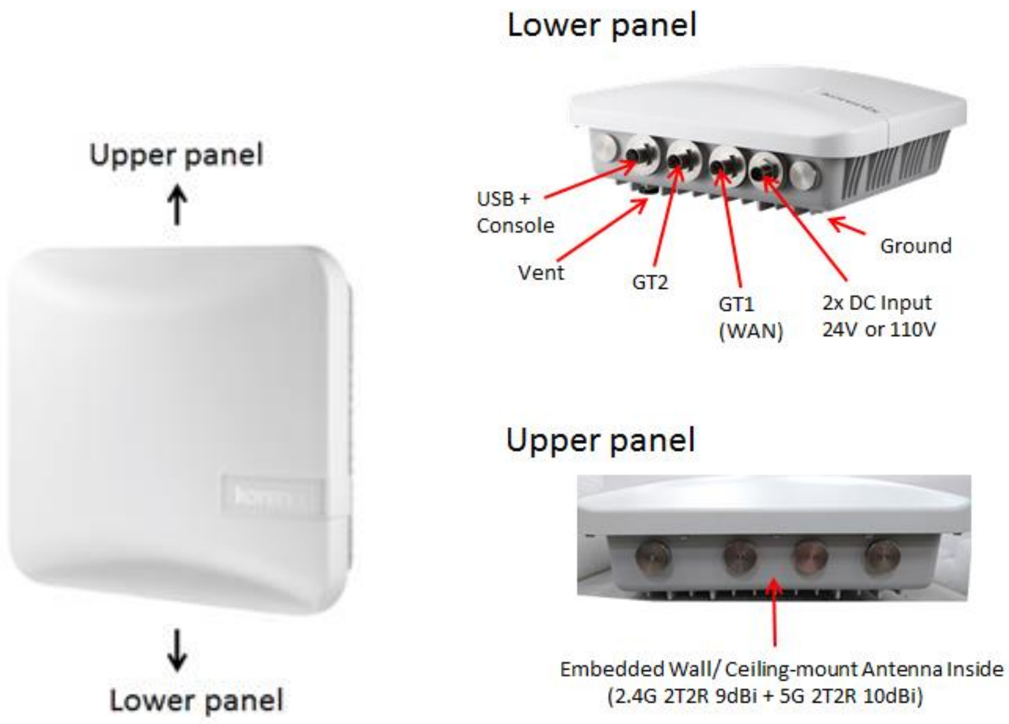
1.1 Introduction

The user manual is applied to Korenix JetWave 4020 Series Industrial Dual Band Dual Radio 802.11ac Wireless AP, Embedded Antenna and JetWave 4020E Industrial Dual Band Dual Radio 802.11ac Wireless AP, External N-Type Antenna. 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 environment.

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 4020 and JetWave 4020E, they will be specially highlighted in the chapters.

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

1.2 JetWave 4020 Series Appearance



1.3 JetWave 4020 Major Features

JetWave 4020: Industrial Dual Band Dual Radio 802.11ac Wireless AP with 2x Gigabit LAN M12 Connector, Embedded Antenna, 24V input

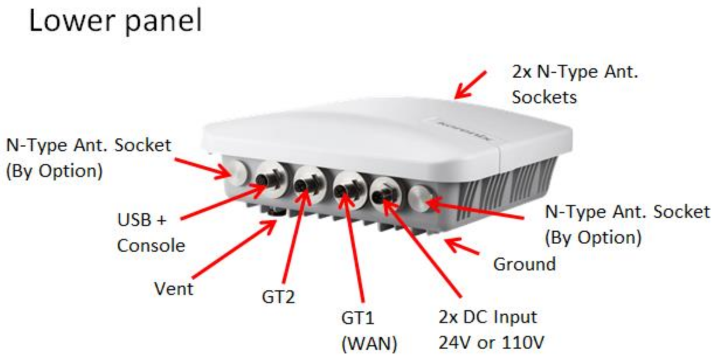
JetWave 4020-HV: Industrial Dual Band Dual Radio 802.11ac Wireless AP with 2x Gigabit LAN M12 Connector, Embedded Antenna, 110V input

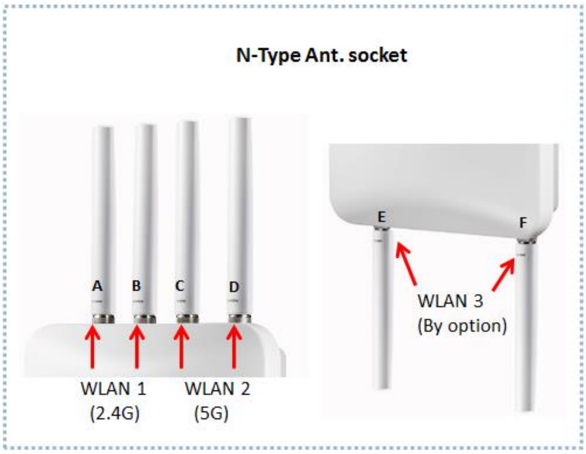
Features:

- Dual Band Dual Radios, 2.4G 802.11n + 5.8G 802.11ac Wave 1
- Up to 1.16Gbps concurrent performance and Beamforming technology
- Dual M12 Gigabit Ethernet Bridging or NAT Routing
- Controller-based AP management, 100ms Super Roaming,
- Link Fault Pass-Through
- Dual Radio Redundancy
- SNMP/ LLDP

- WPA/WPA2 Security & VPN Connectivity
- IP67 Water-proof, -40~70℃ operating temperature, EN50121-4 EMC protection
- M12 24V/110VDC Power Input
- M12 USB for configuration restoring

1.4 JetWave 4020E Series Appearance





1.5 JetWave 4020E Major Features

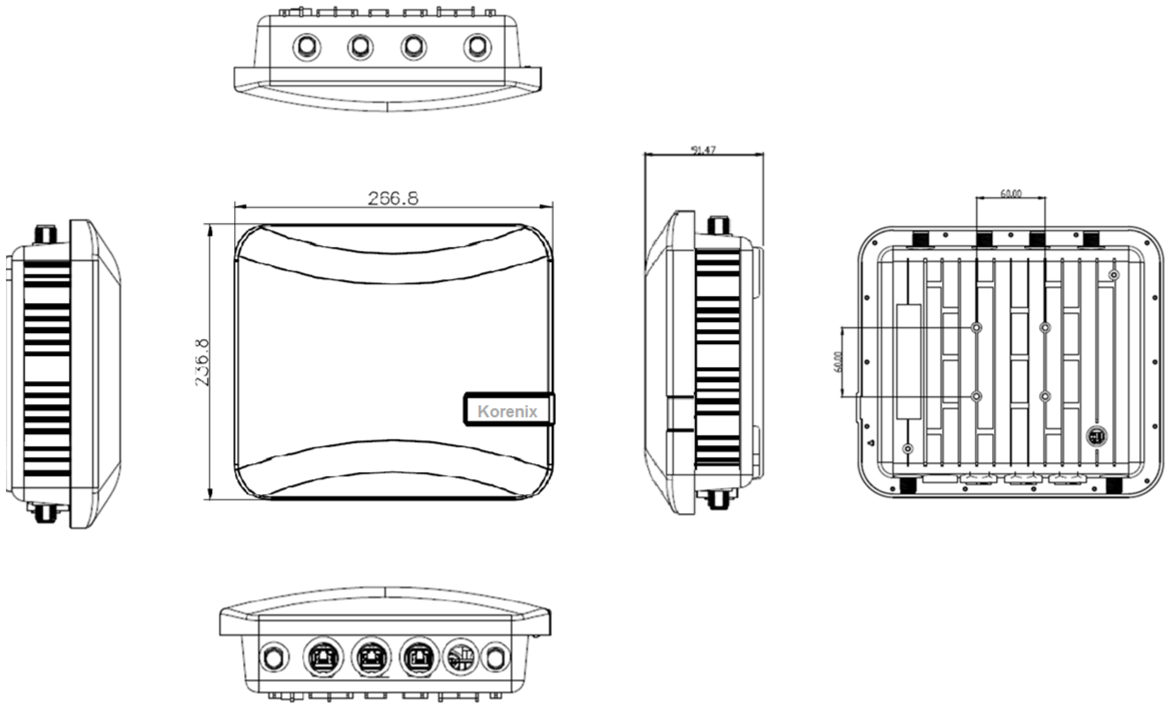
JetWave 4020E: Industrial Dual Band Dual Radio 802.11ac Wireless AP with 2x Gigabit LAN M12 Connector, External N-Type Ant., 24V input

JetWave 4020E-HV: Industrial Dual Band Dual Radio 802.11ac Wireless AP with 2x Gigabit LAN M12 Connector, External N-Type Ant., 110V input

Features:

- Industrial leading 802.11ac WIFI performance
- Dual Band Dual Radios, 2.4G 802.11n + 5.8G 802.11ac Wave 1, 3rd Radio by option
- Up to 1.16Gbps concurrent performance and Beamforming technology
- N-Type Connector for external antenna
- Dual M12 Gigabit Ethernet Bridging or NAT Routing
- Controller-based AP management, 100ms Super Roaming
- Link Fault Pass-Through, Dual Radio Redundancy
- SNMP/LLDP
- WPA/WPA2 Security & VPN Connectivity
- IP67 Water-proof, -40~70℃ operating temperature, EN50121-4 EMC protection
- M12 24V/110VDC Power Input
- M12 USB for configuration restoring

1.6 JetWave 4020/4020E Product Dimension



1.7 Product 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 4020/4020E product unit (Depends on the model you purchase)
- Quick Installation Guide
- Embedded 2.4G+5G 9dBi/10dBi Antennas inside the body (JetWave 4020)
- No Antenna (JetWave 4020E)
- JetWave 4020/4020E Mounting Kits

*Please download user manual from Korenix Web Site

Optional Accessory:

- JetWave 25m RJ-45 to X-code M12 Cable
- External Antenna

2.4GHz	
JWDA-2.4G-12dBi-NF	JetWave Directional Sector Antenna, Wi-Fi 2.4GHz, 12dBi, N-Type Female
JWA-2.4G-15dBi-NF	JetWave Omni Directional Antenna, Wi-Fi 2.4GHz, 15dBi, N-Type Female
5.8GHz	
JWA-5.8G-12dBi-NF	JetWave Omni Directional Antenna, Wi-Fi 5.8GHz, 12dBi, N-Type Female
JWDA-5.8G-15dBi-DP-2xNF	JetWave Directional Panel Antenna, Wi-Fi 5.8GHz, 15dBi, Dual Polarization, 2 x N-Type Female
JWDA-5.8G-23dBi-DP-2xNF	JetWave Directional Panel Antenna, Wi-Fi 5.8GHz, 23dBi, Dual Polarization, 2 x N-Type Female

- IEEE 802.11ac Wave 1 Module for 3rd Radio:
  - IEEE 802.11ac Wave 1, 5G Band, 2T2R MIMO
  - Optional 3rd Radio by Request, Please check with Korenix Sales

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 4020/4020E Series.

2.1 Professional Installation Required

- 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.
- The JetWave 4020/4020E series is distributed through distributors and system installers with professional technicians and will not be sold directly through retail stores.

2.1.1 Safety Precautions

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

Additional Notification for the product:

1. The DC power circuit of the product is isolated design circuit. In practical, it is suggested to use isolated DC power design PSU for field installation. Besides the PSU selection, well digital/earth grounding is also important before power on the system. Connect the Ethernet Cables, Antennas or Antenna RF Cables, Ground and Power Terminal Block well before powering on.

2. The USB port is only reserved for device maintenance. Please do NOT use it for other purpose. To charge the battery by the USB is restricted due to the safety concern. If the device is damaged due to the restricted behavior, this is not included in product warranty range.

3. If you are installing the product in the field box, for your safety as well as others', please seek assistance from a professional installer who has received safety training on the hazards involved.

Keep safety as well as performance in mind when selecting your installation site, especially where there are electric power and phone lines. Please note the following things as well:

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

4. If you are installing the product in the indoor office or factory, be aware of the power source and grounding must be well installed. The professional Wireless IT Engineer can provide service for location, antenna and field plan to get better performance and coverage.

5. When you exchange to high gain antenna on JetWave 4020E, please notice that the Radio Output power and antenna gain value must be allowed according to the regulations of the country. And avoid standing directly in front of high gain antenna. Strong RF fields are present when the transmitter is on.

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

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

7. The operating temperature of JetWave 4020 series is from -40 to 70℃, please MUST installed the device in a restricted access location to avoid the hot surface of housing, and make more aware of potential hazards and reduce the risk. ⚠

2.2 Power Installation

The system provides dual DC power input and passive PoE power input.

2.2.1 DC Input

1. There is one M12 A-code connector located at the right of lower panel with 2x DC power input, the system support power redundancy and it is isolated design. 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 M12 power input connector.

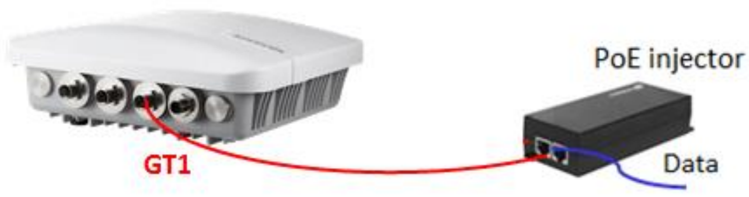
3. The typical and suggest power source is DC 24V or DC 110V (Depend on the model that you purchase), accepted Input Range: ±15%.

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 the chapter 2.2.3.

2.2.2 Powered by PoE

Connect the Ethernet cable to the GT1 Port and 24V PoE injector. The 4020/4020E support passive PoE input, DO NOT accept force mode from PSE switch.

While selecting power source by PoE, connect another end of the Ethernet cable to the PoE injector. Then the AP can be powered and user can access its management interface through the cable. The figure below is an example of connect AP to the PoE injector.



Note: Please choose Korenix Industrial AC to 24VDC PoE Injector for better quality.

2.2.3 Connect both DC input and PoE

The 2 power sources DC input and PoE port are **NOT** redundant power design.

When 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 PoE port will not powering from PoE injector. In this condition, while the DC power source failure, the other power source 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 M12 X-code connector. 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.

GT1: The GT1 Port support passive PoE input. It can accept both power and data transmission from the PoE injector.

Please refer to the chapter 2.2.2 Powered by PoE for PoE installation.

GT2: The GT2 Port is 10/100/1000Base-T M12 Ethernet port. It can transmit data only.

Available Cable Type: (Refer to the chapter 6.3.3 for M12 to RJ-45 cable assembly)

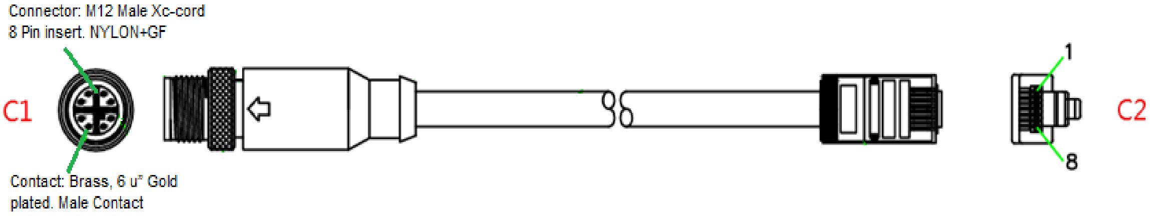
10Base-T: 2-pair UTP/STP Cat. 3, 4, 5 cable (100m)

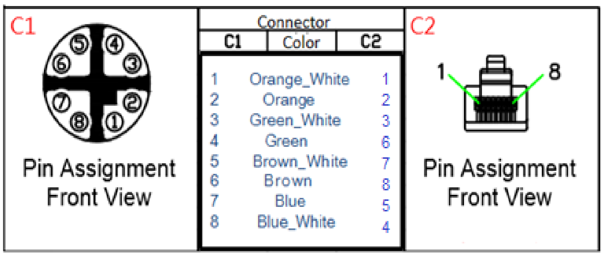
100 Base-TX: 2/4-pair UTP/STP Cat. 5 cable (100m)

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.

Please follow below figure to assembly your cable.

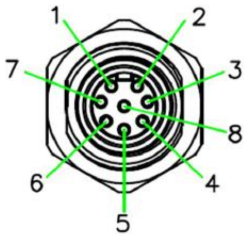




Connector		
C1	Color	C2
1	Orange_White	1
2	Orange	2
3	Green_White	3
4	Green	6
5	Brown_White	7
6	Brown	8
7	Blue	5
8	Blue_White	4

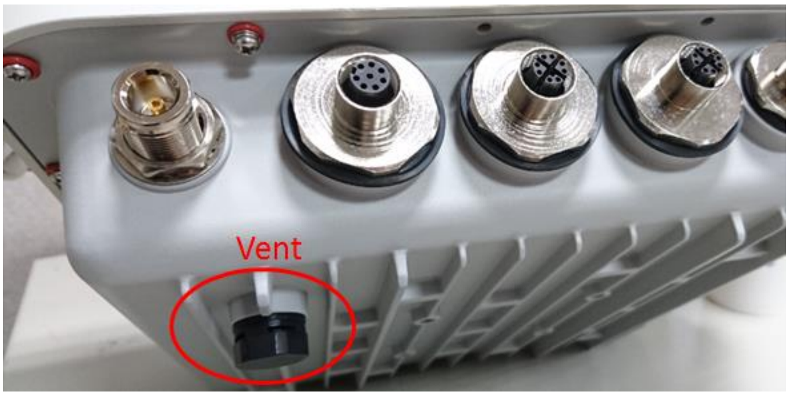
2.3.2 USB + RS-232 Console

The RS-232 console and USB are connected via the assembly type of one 8-pole M12 A-coding connector.

 Pin Assignment Front View	**M12 PIN**	**Functionality**	
	1	TX	Console
	2	RX	
	3	GND	
	4	GND	USB
	5	USB DP	
	6	USB DM	
	7	USB +5V	
	8	GND	

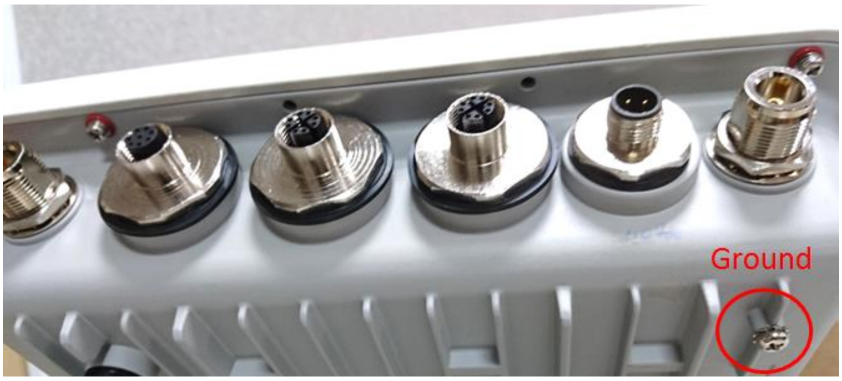
2.3.3 Vent

There is one Vent on the bottom of JetWave 4020/4020E. Vent hole is a small hole which is provided for liquid flow. When non-normal use that cause water into JetWave 4020/4020E, open the Vent hole to let the water flow out and evaporated can reduce the damage to the equipment.



2.3.4 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 4020/4020E series WIFI radio supports IEEE 802.11n and 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).

The Radio 1 (Top of front left) is designed for 802.11n 2.4G, the Radio 2 (Top of front right) is designed for 802.11ac 5G. See table below.

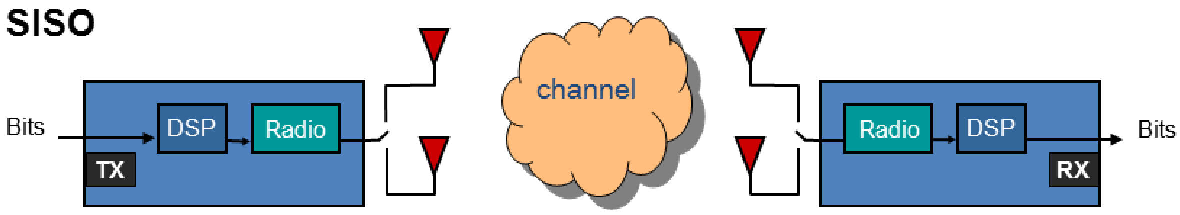
Model Name/ Type	JetWave 4020	JetWave 4020E
Radio 1	802.11n 2.4GHz	802.11n 2.4GHz
Radio 2	802.11ac 5GHz	802.11ac 5GHz
Antenna	Embedded 9/10dBi	External N-Type

2.4.1 MIMO & Dual Polarization

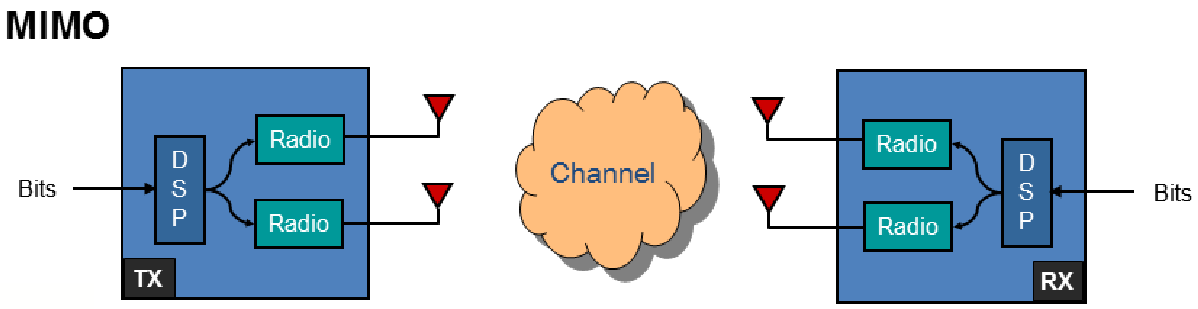
➢ **What is MIMO:**

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

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



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

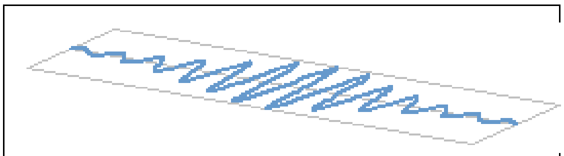
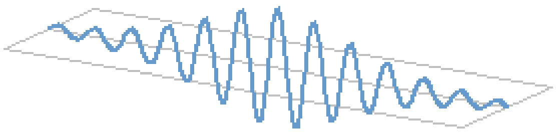


- **What is Polarization:**

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:

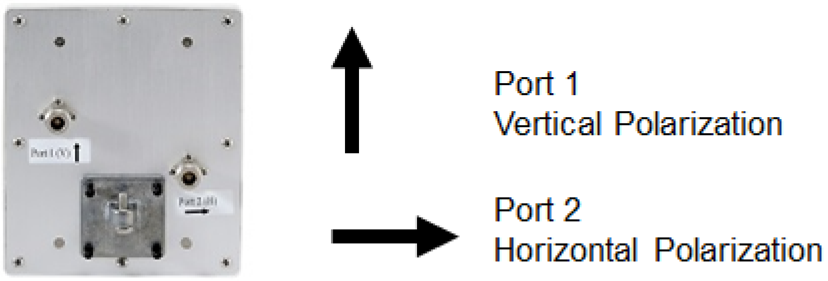
Horizontal Polarization	Vertical Polarization
	

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, and the other is for Horizontal polarization. While installing the antenna, the 2 ports' direction of the 2 end must be the same.

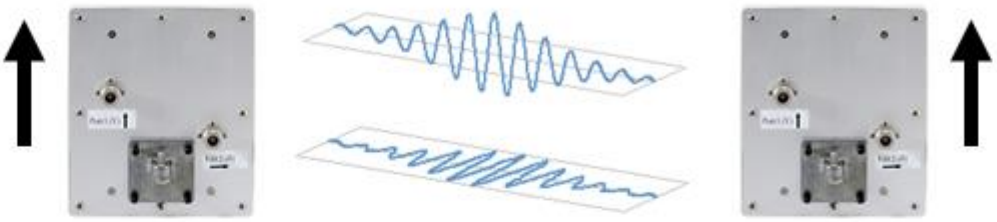


MIMO & Polarization:

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:



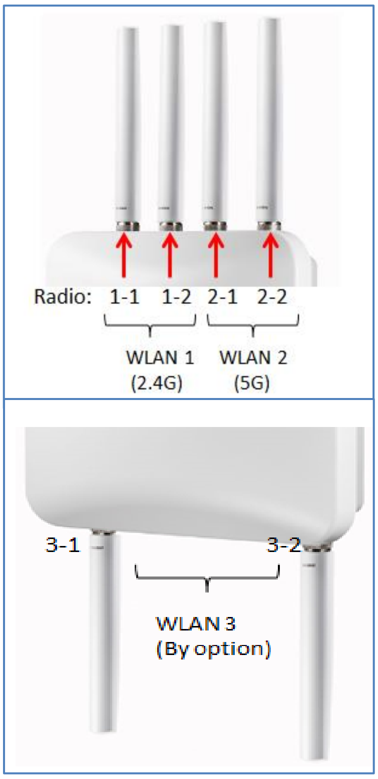
2.4.2 Antenna Socket

The JetWave 4020/4020E Series supports IEEE 802.11n and 802.11ac 2T2R MIMO technology. There are. JetWave 4020 series is embedded antenna that you don't need to mount external antennas. JetWave 4020E series is external antenna model, it equips 6x N-Type antenna sockets for two WIFI radio (2x sockets by option), you can connect 1 to 6 WIFI antennas based on your need.

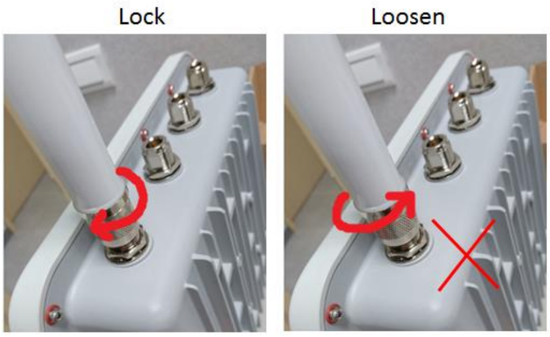
If you just need to connect one single polarization WIFI antenna on JetWave 4020E, you must go to the Web GUI to change the antenna number to 1 (The chapter 4.4.3 for reference), and connect it to the 1st antenna socket, Radio 1-1(A) or Radio 2-1(C) of the JetWave 4020E. Please remind that it is just 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 1-2(B) and Radio 2-2(D).

Antenna Number	JetWave 4020	JetWave 4020E
A	X	Radio 1-1
B	X	Radio 1-2
C	X	Radio 2-1
D	X	Radio 2-2
E	X	Radio 3-1
F	X	Radio 3-2



2.4.3 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 antenna, 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.

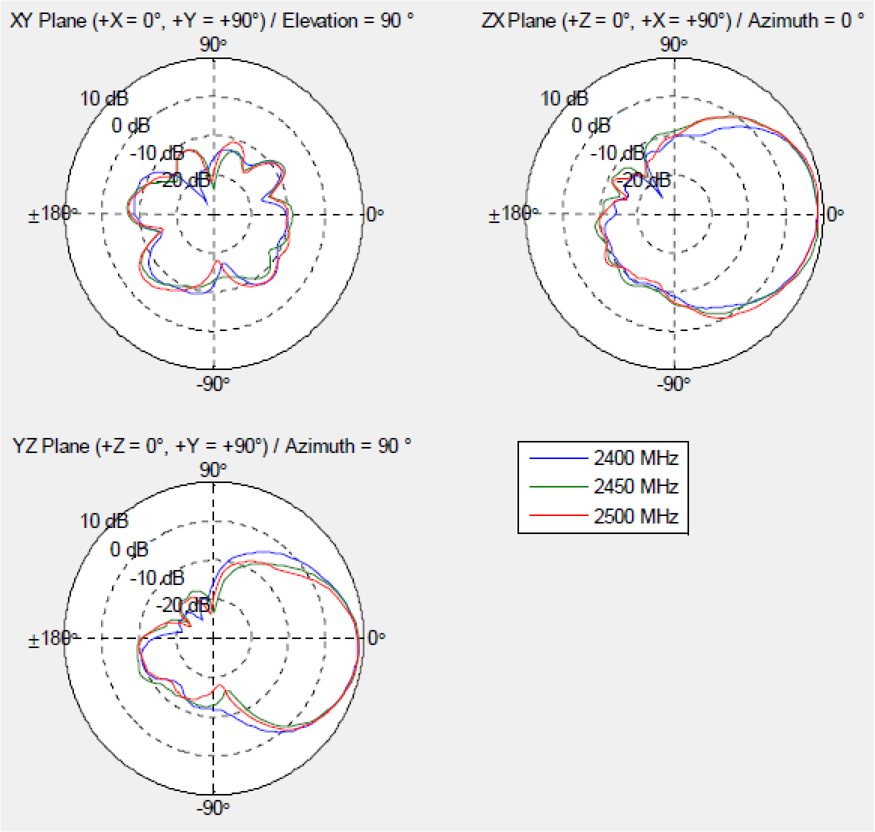
2.4.4 Default Embedded WIFI Antenna Specification:

The following information applied to the default WIFI antenna.

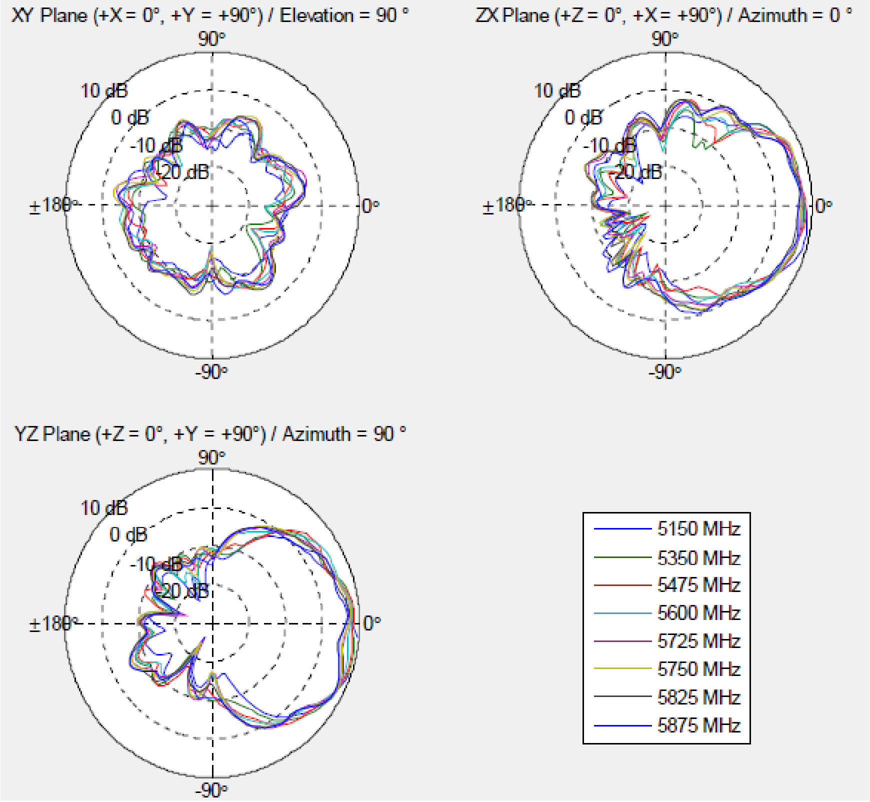
Embedded Wall/Ceiling-mount 180° 2.4G 2T2R + 5G 2T2R bands antenna			
Frequency (MHz)	2400-2500	5150-5350	5475-5875
Peak gain(dBi)	9	10	8
VSWR	2.5：1 Max.		
Polarization	Linear, vertical		
Impedance	50 Ω		

Reference Distance: The suggested distance of the embedded WIFI antenna is from 150 to 300 meters wide in public space. (However, the free space lost may affect the transmitting distance, so that the device may have different performance in different environment.)

➢ Embedded 2.4G Antenna Radiation Pattern



➢ Embedded 5G Antenna Radiation Pattern

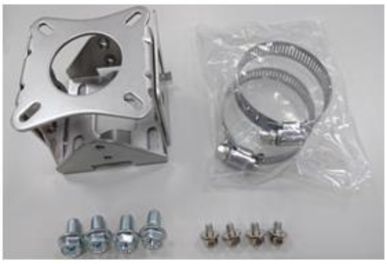


2.5 Mounting

2.5.1 Mounting the AP

The JetWave 4020/4020E series supports Pole-Mount, Wall-Mount, and Ceiling-Mount. The mounting package equipped with all the three mount types, and included in shipment.

Korenix provide two mounting brackets: Rectangular Mounting Bracket and Mounting Kit (Case plate), it's alternative when mount the bracket, you can based on your need to choose the suitable one. For convenient side, Rectangular Mounting Bracket is easier to assembly, but if you need to rotate the mounting angle, Mounting kit (Case plate) is appropriate than Rectangular Mounting Bracket.



The unassembled bracket consists as below. If there is any lost, please contact your sales.

1x Rectangular Mounting Bracket

1x Mounting Kit (Include Case plate and Wall plate)

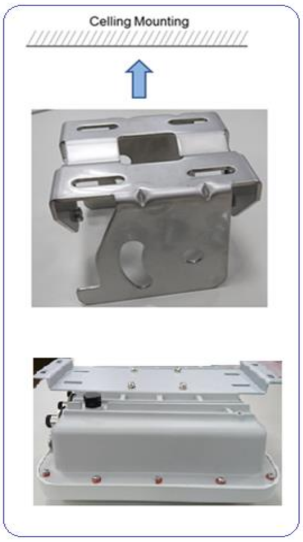
2x Pole Mount Clampers

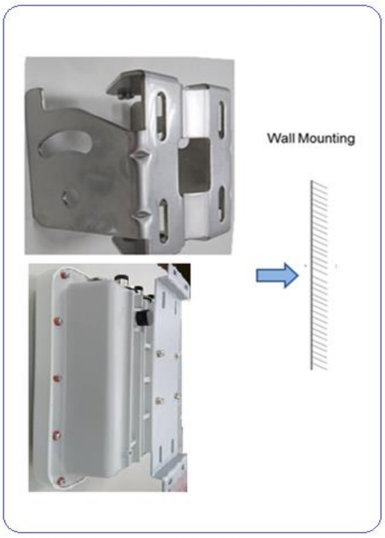
8x Screws (Include 4x M5 screw, 4x M8 screw)

The wall plate and mounting bracket are available for Ceiling, Wall or Pole mounting.

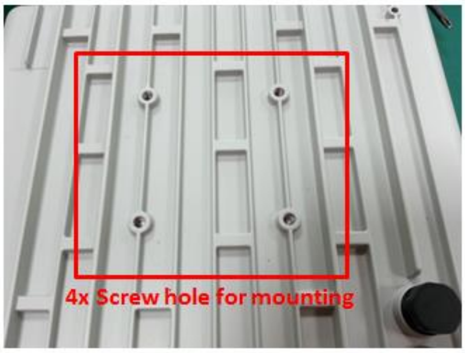
Following the steps to assemble Rectangular Mounting Bracket or Mounting Kit.

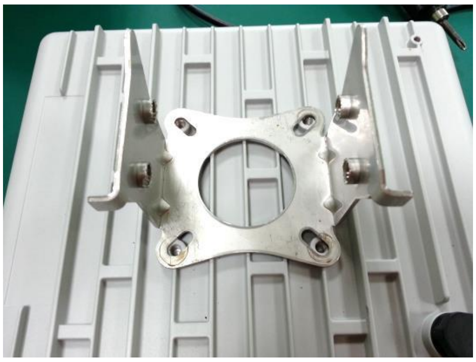
- **Mounting Kit**





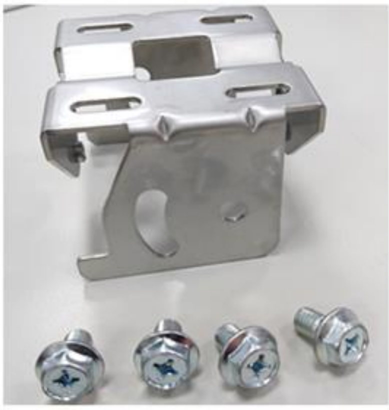
Step 1: Assemble the Mounting Kit (Case plate) with 4x M5 screws on the bottom of JetWave 4020/4020E.



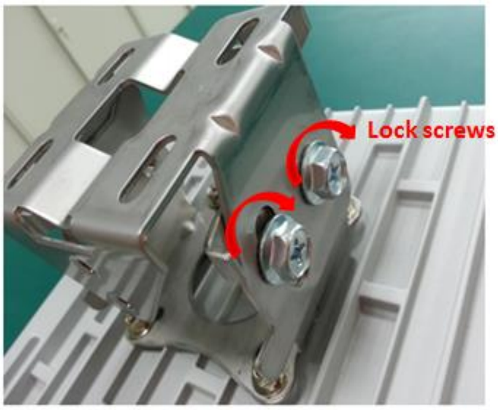


Step 2: Assemble Wall Plate and Case plate, and lock up with 4x M8 screws.

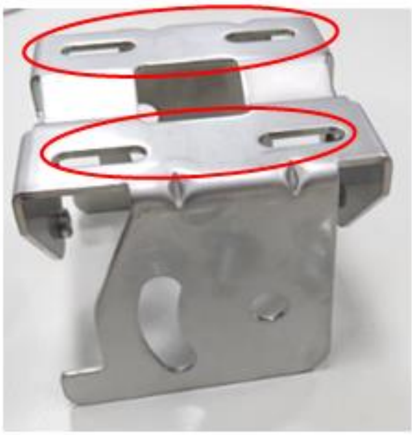
Wall Plate and screws



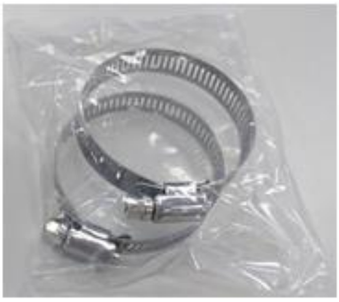
Assemble Wall Plate to bracket



Step 3: If you need to use pole mounting, assemble 2x clampers to Wall Plate

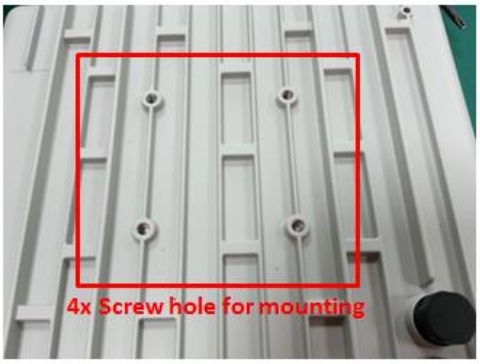


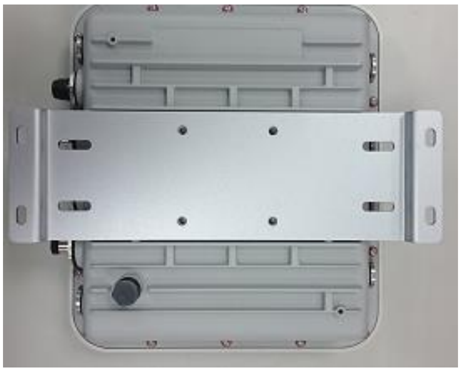
+



- **Rectangular Mounting Bracket:**

Step 1: Assemble the Rectangular Mounting Bracket with 4x M5 screws on the bottom of JetWave 4020/4020E.

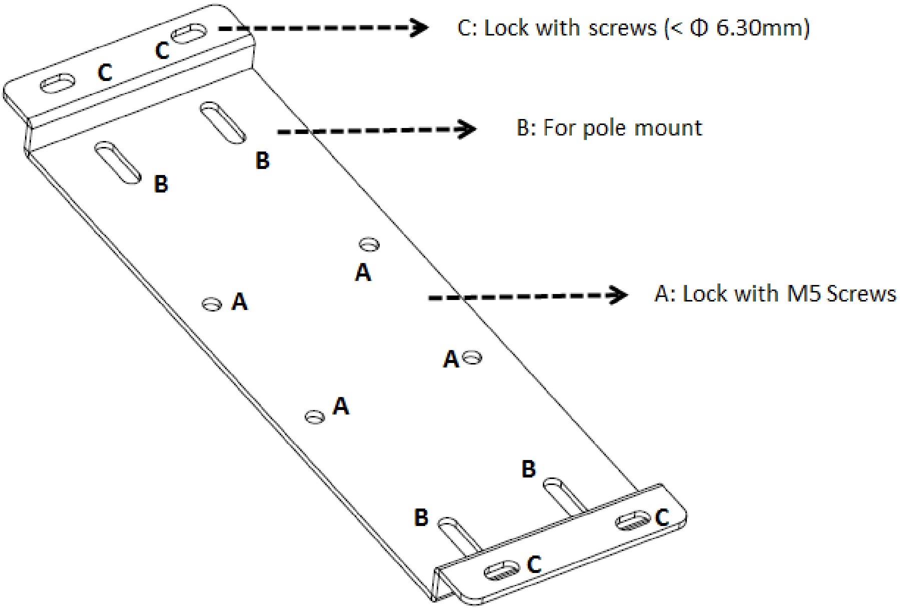




Step 2:

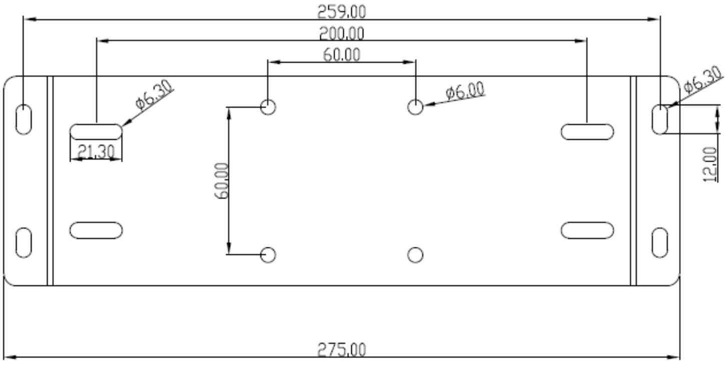
(1) Wall/Ceiling mount: Lock up with 4x screws (<Φ6.30mm) on C. (Picture below)

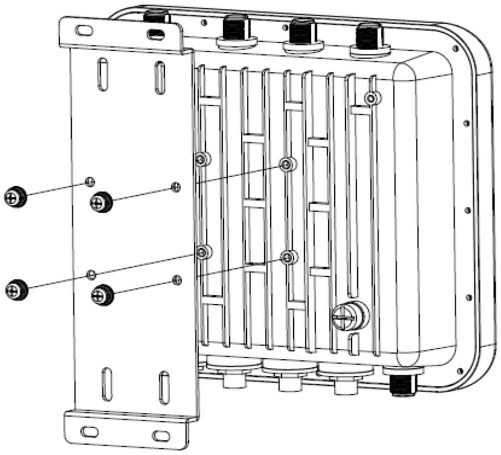
(2) Pole mount: Assemble Pole Mount Clampers or Cable Ties on B. (Picture below)



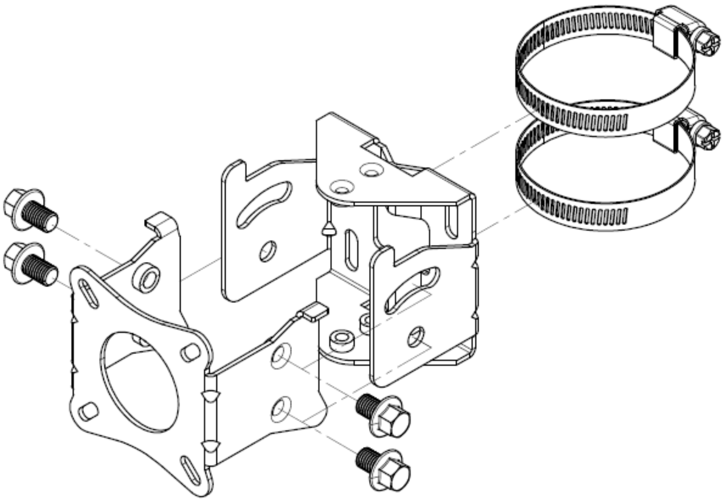
Schematic diagram:

- **Rectangular Mounting Bracket**





- **Mounting Kit (Case plate, Wall plate and pole mount)**



2.5.2 Mounting the N-Type external antenna

JetWave 4020E series need to mount external antennas for Wireless communication. N-Type antenna socket is the default type of JetWave 4020E. You must notice that the antenna should support Dual Polarization for 2T2R MIMO radio transmission. You can follow the same steps as “Antenna Installation” (The chapter 2.4.3) to install your antenna.

2.5.3 Mounting the SMA external antenna:

While selecting the SMA external antenna, you must use N-Type to SMA converter, and please notice that the antenna should support Dual Polarization for 2T2R MIMO radio transmission. You can follow the same steps as “Antenna Installation” (The chapter 2.4.3) to install your antenna.

2.6 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 Sockets of the AP:

Top of left side: Radio 1 (WLAN 1, 2.4G). There are 2 N-Type connectors for 2T2R MIMO.

Top of right side: Radio 2 (WLAN 2, 5G). There are 2 N-Type connectors for 2T2R MIMO.

Bottom of both sides: Radio 3 (Optional WLAN3). There are 2 N-Type connectors for 2T2R MIMO.

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.

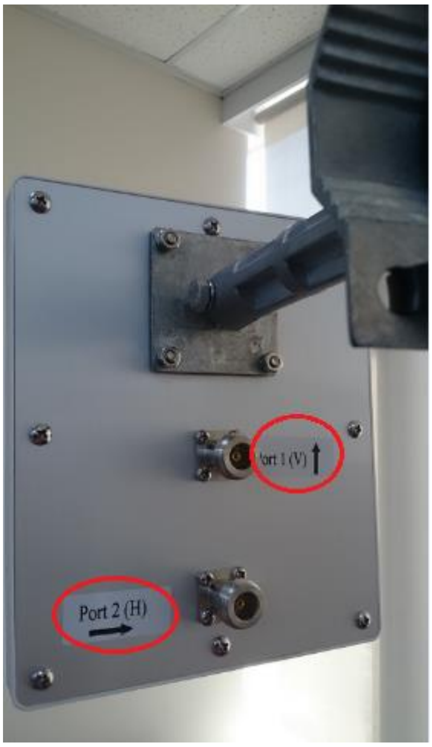
b. Find the remote location of the target AP. The Telescope, GPS positioning tool, Google Map are convenient tool.

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 to the antenna. The level

e. Go to Web GUI, use the **Antenna Alignment tool** (Refer to the 4.7.5) can help you find the target Antenna.

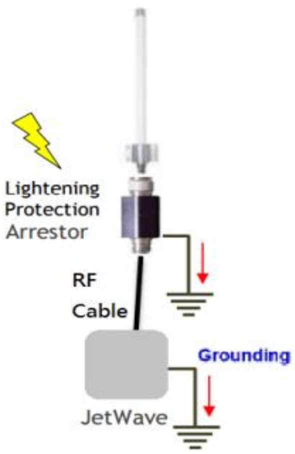
f. Run the **Data Rate Test** (4.7.4) can help you check



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 4020/4020E 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 to discover the devices' IP address and then access it.

3.1 Basic Factory Default Settings

We elaborated the JetWave 4020/4020E 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 4020/4020E Basic Factory Default Settings

Features	Factory Default Settings
Username	admin
Password	admin
Model Name	JetWave4020 (/4020E depends on which model you access)
Device Name	korenixXXXXXX (X represents the last 6 digits of Ethernet MAC address)
Network Mode	**Bridge Mode** **Note:** In Bridge mode, only one IP Address (LAN) interface is available. **Router Mode** **Note:** In Router mode, WAN (GT1) and LAN (GT2) interface has its own IP Address.

Default IP at Bridge Mode		
IP Address		192.168.10.1
Subnet Mask		255.255.255.0
Default Gateway		0.0.0.0
Default IP at Router Mode		
IP Setup – GT1 (WAN)	Access Type	Static IP
	IP Address	192.168.1.1
	Subnet Mask	255.255.255.0
	Default Gateway	0.0.0.0
	DNS1	8.8.8.8 (Google IP)
	DNS2	0.0.0.0
IP Setup – GT2 (LAN)	IP Address	192.168.10.1
	Subnet Mask	255.255.255.0
	DHCP Server	Enabled
	DHCP IP Range Start	192.168.10.100
	DHCP IP Range End	192.168.10.200
	DHCP Subnet Mask	255.255.255.0
	DHCP Gateway	192.168.10.1
	(Refer to the System – IP Settings for further information)	
Wireless Settings		
Wireless Basic Setting	Wireless Mode	AP
	Wireless Network Name (SSID)	JetWave_1 (WLAN 1) JetWave_2 (WLAN 2)
	Broadcast SSID	Enabled
	802.11 Mode	802.11G/N (WLAN 1) 802.11A/N (WLAN 2)

	Frequency/ Channel	2437MHz(6) (WLAN 1)
		5180MHz(36) (WLAN 2)

	Channel Mode	20 MHz
	Data Rate	Auto
	(Refer to the Wireless – WLAN – Basic Settings)	
Wireless Advanced Settings	Antenna Number	Two antenna
Other Settings		
Remote Settings	Remote Management Privacy	Telnet, SNMP
SNMP	Version	2
	Server Port:	161

SNMP	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 GT2 (LAN).
Diagnostic CLI	Console Type	M12 A-code: 3-pin (Tx, Rx, GND) Refer to the chapter 6.3 Appendix- M12 Connector 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:

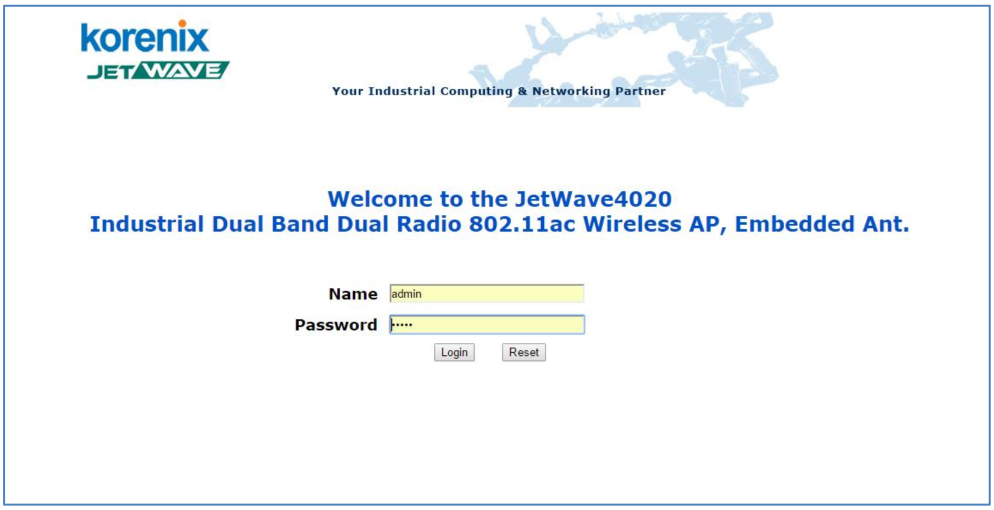
- A computer coupled with 10/100/1000 Base-T(X) adapter;
- Configure the computer with a static IP address of 192.168.10.X (X cannot be 0, 1, nor 255), as the default IP address of JetWave 4020/4020E Series is 192.168.10.1 (Both GT1 and GT2 in Bridge mode; GT2 only in Router mode).
- You can also connect your computer to the WAN port (In Router mode).
  - Please use 192.168.1.X (X cannot be 0, 1, nor 255) as the default IP address since the default IP Address of the JetWave 4020/4020E Series WAN port is 192.168.1.1.
  - Configure Inbound Filtering (The chapter 4.2.7 for reference), click on “Web” from Remote Management Exception List.
- 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.

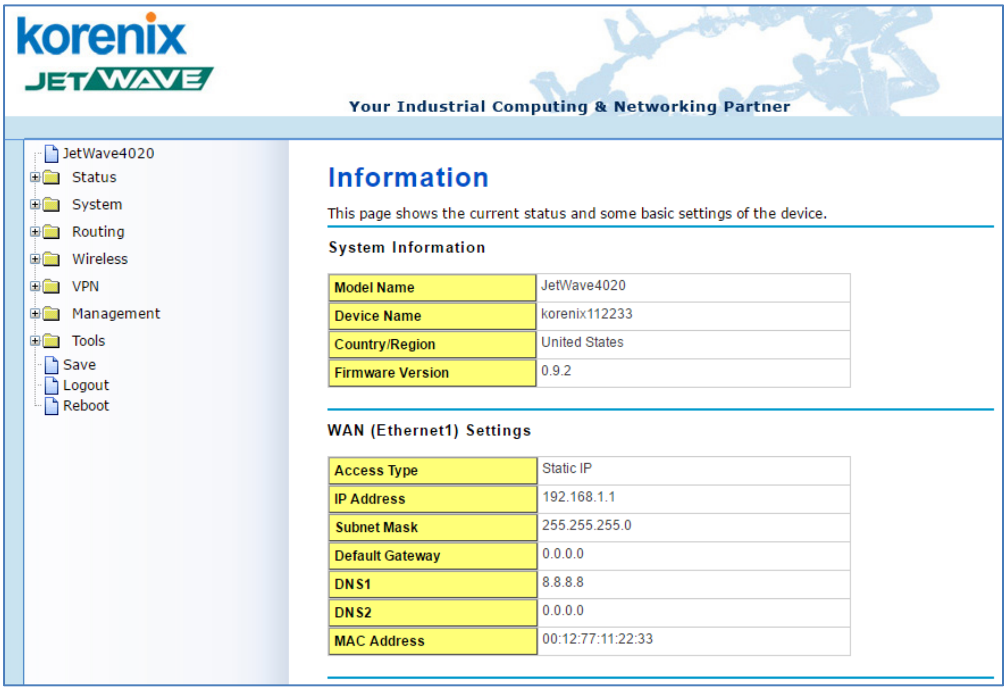


Welcome to the JetWave4020
Industrial Dual Band Dual Radio 802.11ac Wireless AP, Embedded Ant.

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**, **Routing, Wireless, VPN, Management, Tools, Save, Logout** and **Reboot.** (Note: Routing page appears when Network Mode set Route ETH WAN)



Information

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

System Information

Model Name	JetWave4020
Device Name	korenix112233
Country/Region	United States
Firmware Version	0.9.2

WAN (Ethernet1) Settings

Access Type	Static IP
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DNS1	8.8.8.8
DNS2	0.0.0.0
MAC Address	00:12:77:11:22:33

Figure - Main Page

3.4 Fail to login the Web GUI

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

1. Normally, you can access the device by using any kind of Window based Web browser, such as Microsoft Internet Explorer, Google Chrome, Firefox…, to configure and interrogate the product from anywhere on the network. If you failed access in either of the above Web browser, this might be the interoperability issue among your PC, OS version, Web browser and our product. You can try another Web browser as first self-aid, it usually works.
2. Please disable the firewall setting of your browser. The firewall setting may block the connection from your PC to the device. Note that after finished the setting, re-enable your firewall to protect your PC.
3. Check the IP Setting, your PC and managed device must be located within the same subnet.
4. Check the connected port, the default GT1 and GT2 equipped with different IP Address in Router mode.
5. The Web UI connection session of the device will be logged out automatically if you don't give any input after 30 seconds. After logged out, you should re-login and key in correct user name and password again.
6. Please contact 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 M12 USB/Console port or Telnet.

Diagnostic Console:

There is one 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 M12 A-code socket to USB/Console port.

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 4020/4020E 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

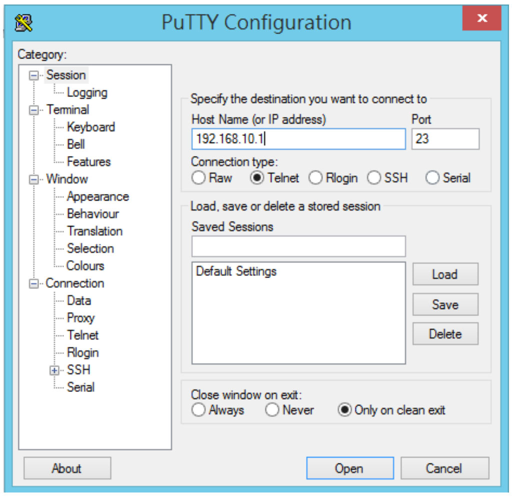
Note that the Telnet.exe file is not provided after Window 7. You can download it from Microsoft web site. Or you can use 3rd Party tool, for example the Putty.

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

Specify the destination you want to connect to

Host Name (or IP address): 192.168.10.1

Port: 23

Connection type: ○ Raw ● Telnet ○ Rlogin ○ SSH ○ Serial

Load, save or delete a stored session

Saved Sessions

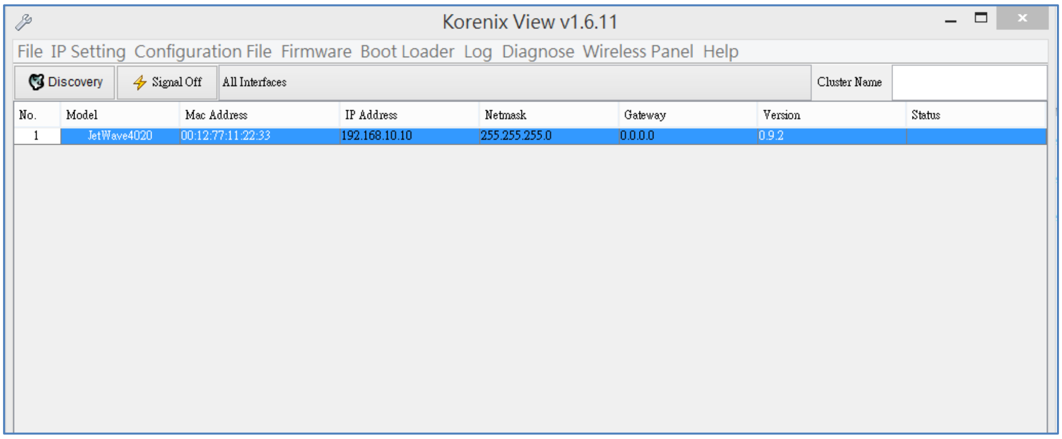
Default Settings

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

3.6 Discovery Utility – Korenix View Utility

Korenix View is client/server architecture. Users use the client application to issue the operations and there is a server on the device to do these operations. The major difference between the Korenix View and other management tools, ex. Web, CLI, and SNMP, is that the Korenix View can configure several devices at the same time.

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


Korenix View v1.6.11
File IP Setting Configuration File Firmware Boot Loader Log Diagnose Wireless Panel Help
Discovery
Signal Off
All Interfaces
Cluster Name

No.	Model	Mac Address	IP Address	Netmask	Gateway	Version	Status
1	JetWave4020	00:12:77:11:22:33	192.168.10.10	255.255.255.0	0.0.0.0	0.9.2	

- Please download the latest Korenix View Utility from Korenix Web Support page.
- The chapter 5.3 introduces how to use Korenix View Utility.

Chapter 4

Web GUI Configuration

Chapter 4 Web GUI Configuration

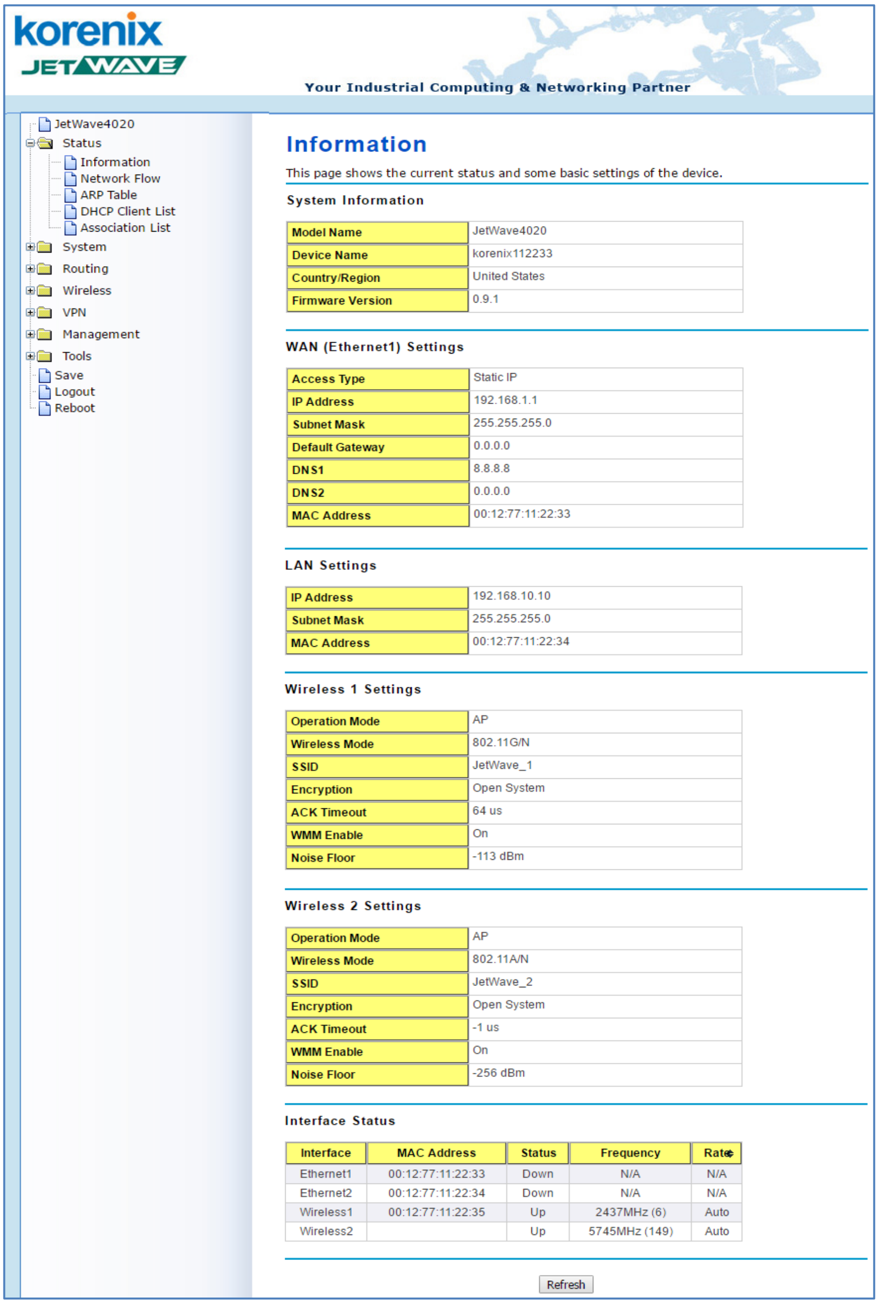
This chapter describes the Web GUI for Software Configuration.

4.1 Status

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

4.1.1 Information

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



Information

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

System Information

Model Name	JetWave4020
Device Name	korenix112233
Country/Region	United States
Firmware Version	0.9.1

WAN (Ethernet1) Settings

Access Type	Static IP
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DNS1	8.8.8.8
DNS2	0.0.0.0
MAC Address	00:12:77:11:22:33

LAN Settings

IP Address	192.168.10.10
Subnet Mask	255.255.255.0
MAC Address	00:12:77:11:22:34

Wireless 1 Settings

Operation Mode	AP
Wireless Mode	802.11G/N
SSID	JetWave_1
Encryption	Open System
ACK Timeout	64 us
WMM Enable	On
Noise Floor	-113 dBm

Wireless 2 Settings

Operation Mode	AP
Wireless Mode	802.11A/N
SSID	JetWave_2
Encryption	Open System
ACK Timeout	-1 us
WMM Enable	On
Noise Floor	-256 dBm

Interface Status

Interface	MAC Address	Status	Frequency	Rate
Ethernet1	00:12:77:11:22:33	Down	N/A	N/A
Ethernet2	00:12:77:11:22:34	Down	N/A	N/A
Wireless1	00:12:77:11:22:35	Up	2437MHz (6)	Auto
Wireless2		Up	5745MHz (149)	Auto

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

WAN (Ethernet1) Settings: It shows Access Type, IP Address, Subnet Mask, Default Gateway, DNS1, DNS2 and MAC address.

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

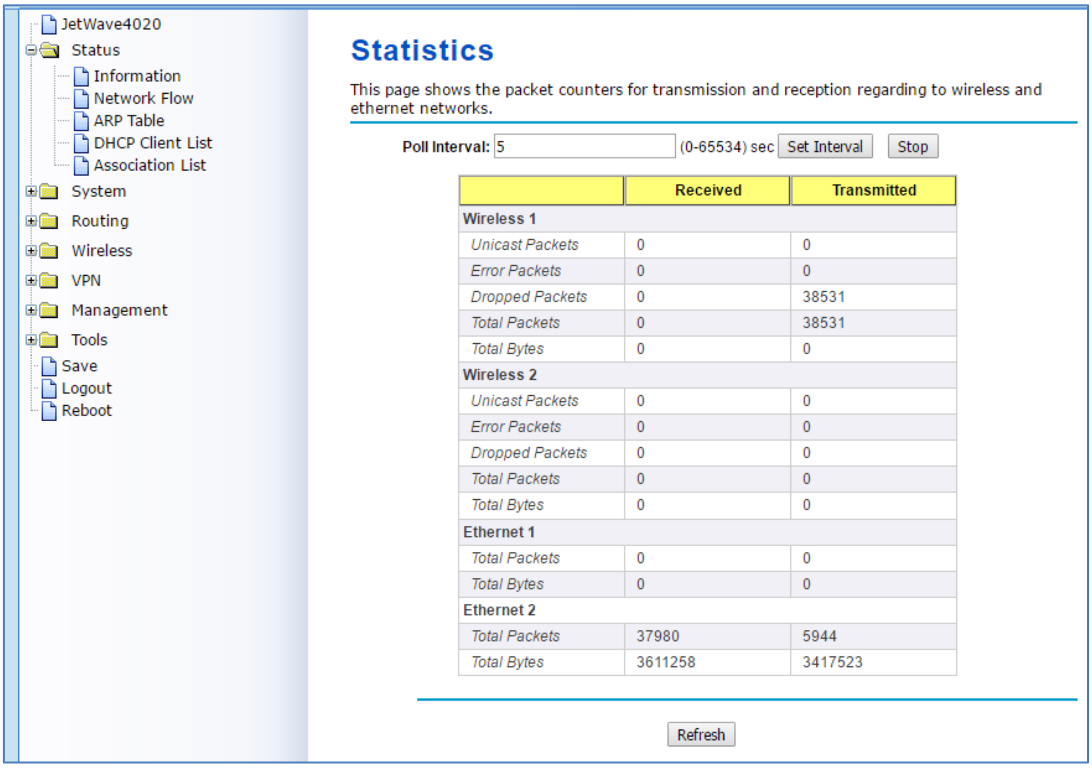
Wireless 1 Settings: It shows the Operation Mode, Wireless Mode, SSID, Encryption, ACK Timeout, WMM State, Noise Floor of the Wireless 1. There are 2 or 3 Wireless Settings for JetWave 4020/4020E Series multiple radio models.

Wireless 2 Settings: It shows the Operation Mode, Wireless Mode, SSID, Encryption, ACK Timeout, WMM State, Noise Floor of the Wireless 2.

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

4.1.2 Network Flow (Statistics)

This page shows the packet counters for transmission and reception regarding to Wireless 1, Wireless 2, Ethernet 1 (WAN) and Ethernet 2 (LAN).



Statistics

This page shows the packet counters for transmission and reception regarding to wireless and ethernet networks.

Poll Interval: 5 (0-65534) sec

	Received	Transmitted
Wireless 1		
Unicast Packets	0	0
Error Packets	0	0
Dropped Packets	0	38531
Total Packets	0	38531
Total Bytes	0	0
Wireless 2		
Unicast Packets	0	0
Error Packets	0	0
Dropped Packets	0	0
Total Packets	0	0
Total Bytes	0	0
Ethernet 1		
Total Packets	0	0
Total Bytes	0	0
Ethernet 2		
Total Packets	37980	5944
Total Bytes	3611258	3417523

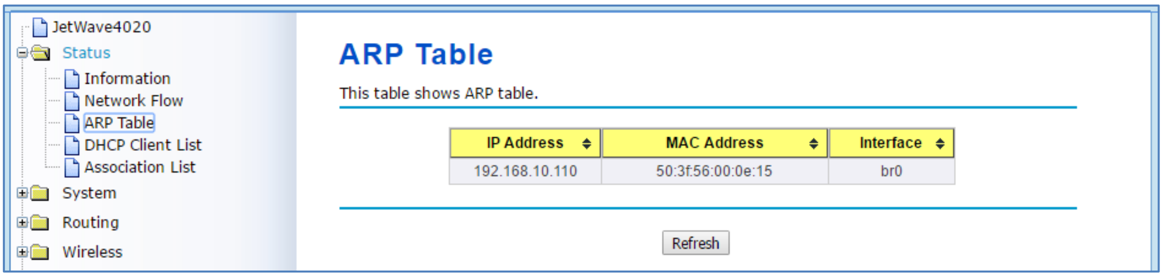
Poll Interval: The poll interval time setting, range from 0~65534 seconds. If you want to change the poll interval time, press “Stop” and then enter new value, press “Set Interval” to activate.

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

Stop: Stop polling the associated clients.

4.1.3 ARP Table

This table shows the ARP table.



ARP Table

This table shows ARP table.

IP Address	MAC Address	Interface
192.168.10.110	50:3f:56:00:0e:15	br0

IP Address: The IP Address leant from the interface.

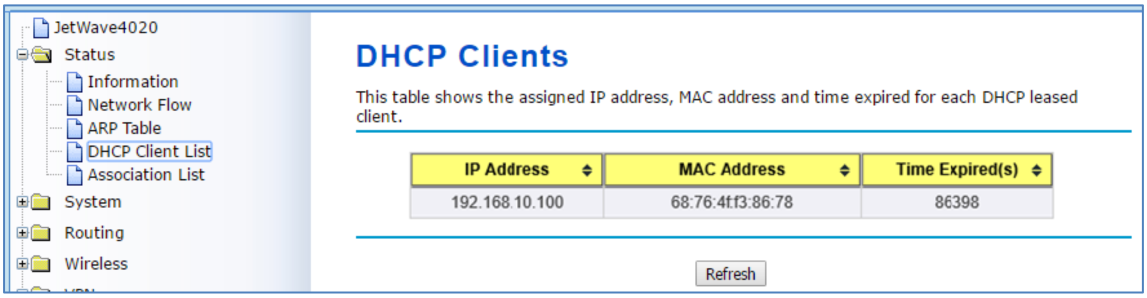
MAC Address: The MAC Address leant from the interface.

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

Refresh: Refresh the table.

4.1.4 DHCP Client List

This table shows the assigned IP address, MAC address and Time Expired of the connected DHCP client devices.



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.

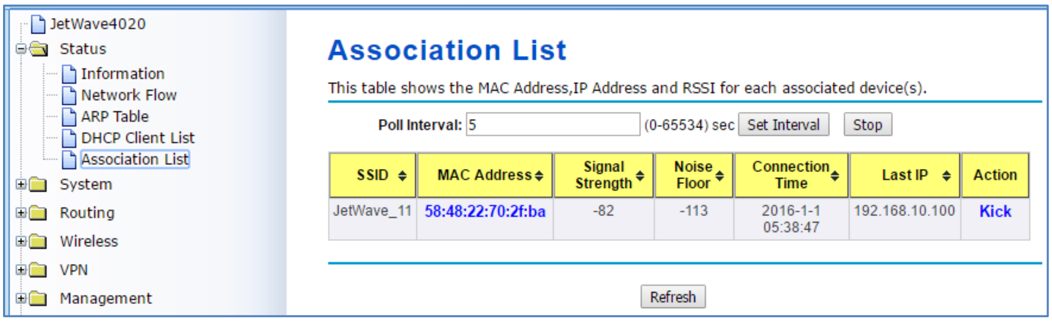
MAC Address: The MAC Address of the connected DHCP client device.

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.

4.1.5 Association List

This table shows the MAC Address, IP Address, RSSI and Connection Time 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 Set Interval Stop

SSID	MAC Address	Signal Strength	Noise Floor	Connection Time	Last IP	Action
JetWave_11	58:48:22:70:2f:ba	-82	-113	2016-1-1 05:38:47	192.168.10.100	Kick

Refresh

Poll Interval: The poll interval time setting, range from 0~65534 seconds. If you want to change the poll interval time, press “Stop” and then enter new value, press “Set Interval” to activate new setting.

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

Stop: Stop polling the associated clients.

====Entry Info===

SSID: The SSID of wireless interface that associated with wireless client device.

MAC Address: The MAC Address of the associated device.

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.

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

Last IP: The last IP address it had.

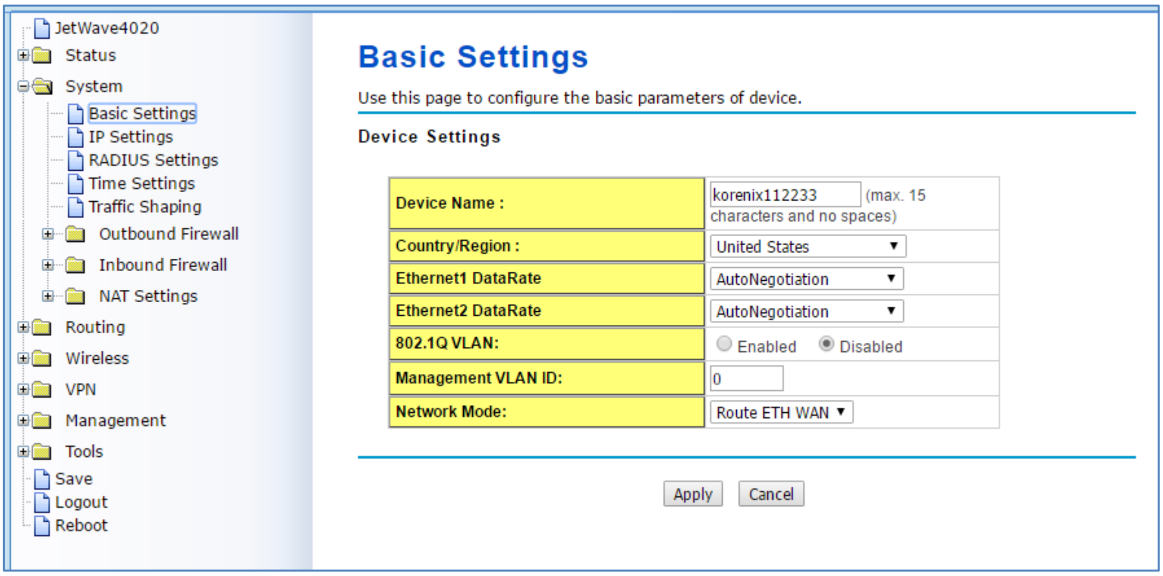
Action – Kick: This command allows you force kick the associated client.

Refresh: The item helps you refresh the table manually.

4.2 System

For users who use the JetWave 4020/4020E series for the first time, it is recommended that you begin configuration from the “**System**” feature set pages shown below:

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



Basic Settings

Use this page to configure the basic parameters of device.

Device Settings

Device Name :	korenix112233 (max. 15 characters and no spaces)
Country/Region :	United States ▼
Ethernet1 DataRate	AutoNegotiation ▼
Ethernet2 DataRate	AutoNegotiation ▼
802.1Q VLAN:	○ Enabled ● Disabled
Management VLAN ID:	0
Network Mode:	Route ETH WAN ▼

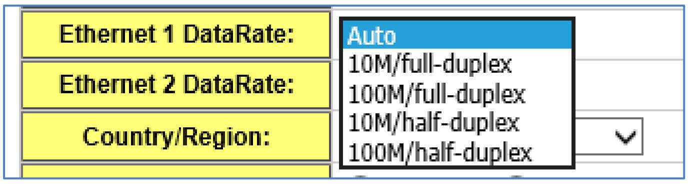
4.2.1 Basic Settings

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.

Country/Region: Select the country you are installed. The channel number may be different based on your country.

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



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

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. Select to enable or disable STP function.

STP Forward Delay: This is the Forward Delay value of the Spanning Tree protocol setting. The valid number is from 1~30 seconds, default value is 1.

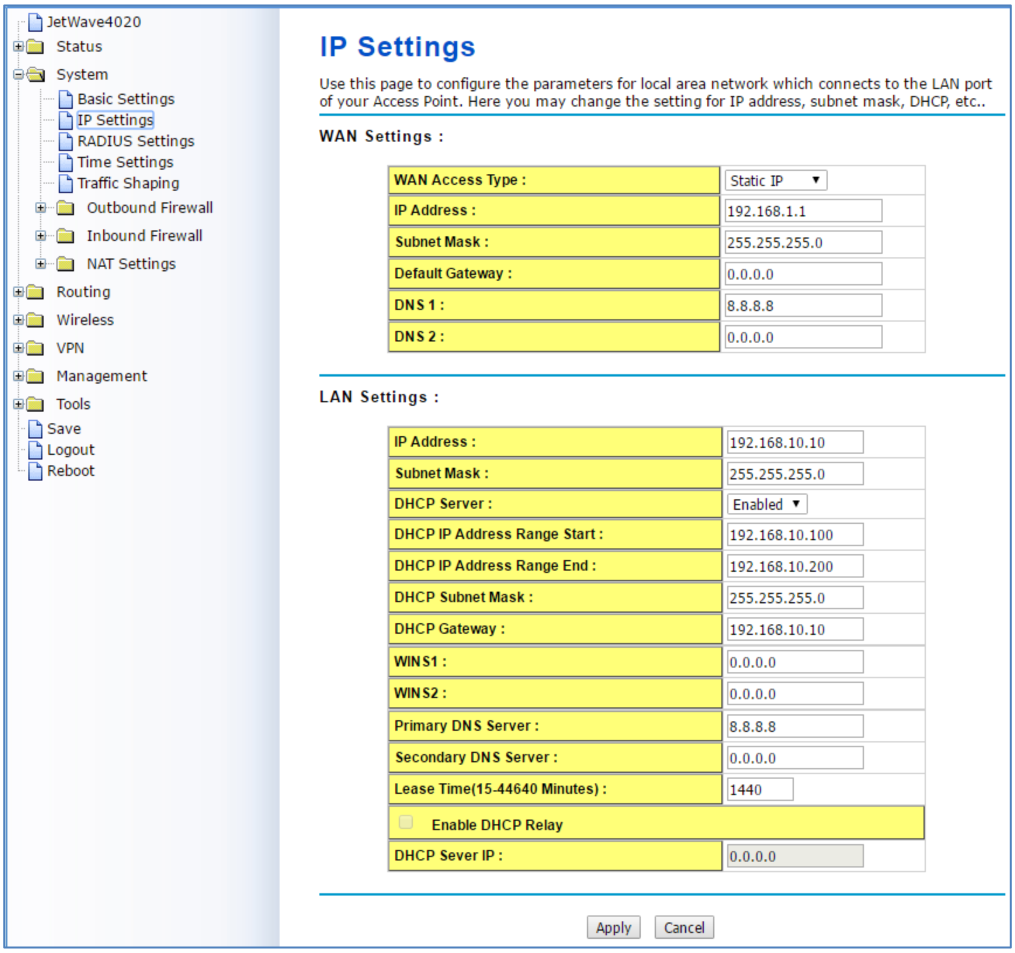
802.1Q VLAN: Enable or Disable 802.1Q VLAN. With 802.1Q enabled, the packet will attach the 1Q VLAN tag inside. To assign the VLAN ID for each AP profile, you should enable 802.1Q VLAN first. Here is the global VLAN Enable setup.

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.

Network Mode: There are **Bridge** and **Route ETH WAN** modes. The default setting is **Route ETH WAN,** it means GT1 (WAN) and GT2 has its own IP address.

4.2.2 IP Settings

Use this page to configure the IP related parameters for **WAN (GT1)** and **LAN (GT2)** interfaces. Here you may change the setting for IP address, subnet mask, Default Gateway, DNS, Static IP or DHCP…etc.



IP Settings

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

WAN Settings :

WAN Access Type :	Static IP ▼
IP Address :	192.168.1.1
Subnet Mask :	255.255.255.0
Default Gateway :	0.0.0.0
DNS 1 :	8.8.8.8
DNS 2 :	0.0.0.0

LAN Settings :

IP Address :	192.168.10.10
Subnet Mask :	255.255.255.0
DHCP Server :	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 :	192.168.10.10
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
□ Enable DHCP Relay	
DHCP Sever IP :	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.

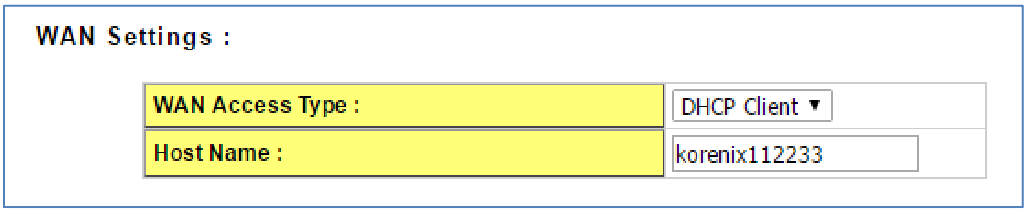
Subnet Mask: This is the subnet mask address for your WAN interface. Set the IP subnet mask manually.

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 :	korenix112233

- **LAN Settings:**

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

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

DHCP Server: Enabled / Disabled

DHCP Server Setting:

You can enable DHCP Server to assign IP address to DHCP clients. And you should define the address pool by configuring the DHCP IP Address Range Start/ End, 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**,** WIN S1/S2**,** Primary/Secondary DNS Servers’ IP Address and Least Time of the assigned IP addresses.

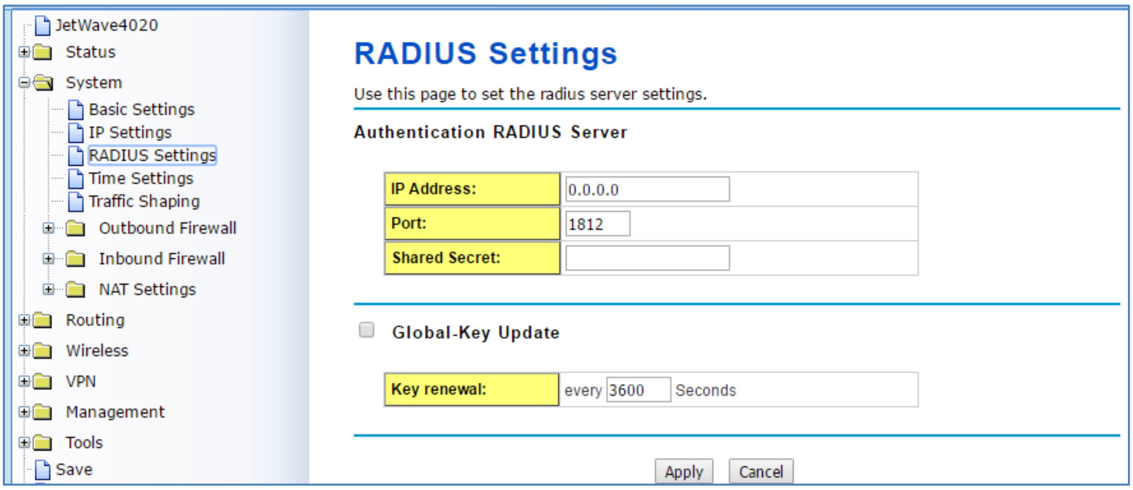
Enable DHCP Relay:

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

Use this page to set the radius server 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.

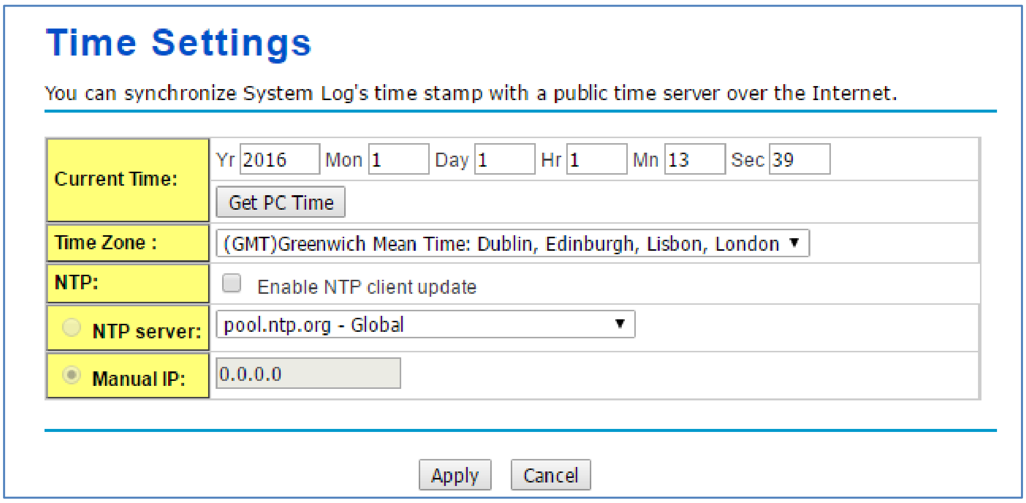
Global-Key Update: Check this option and specify the time interval between two global-key updates.

Key renewal: Set the time interval between two authentications.

For User Security, please go to Wireless Security Setting page (Refer to the chapter 4.4.2)

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

You can synchronize System Log's time stamp with a public time server over the Internet.

Current Time:	Yr 2016 Mon 1 Day 1 Hr 1 Mn 13 Sec 39
Time Zone :	(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
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.

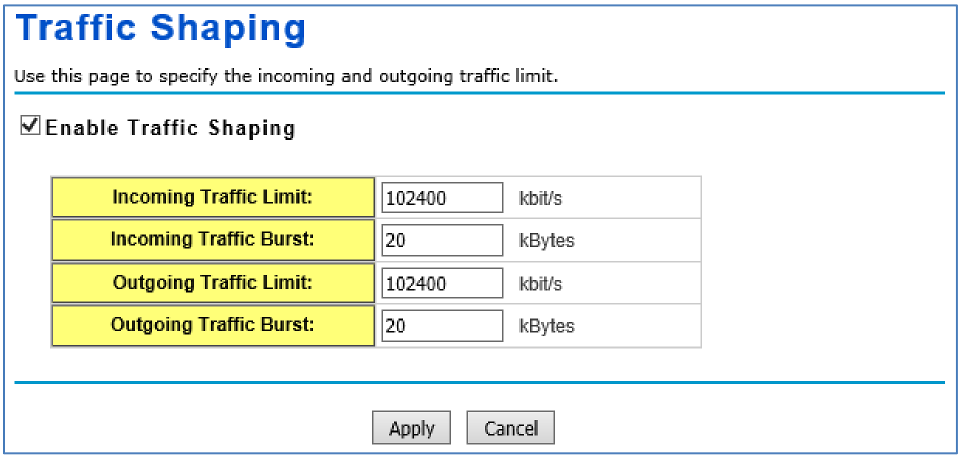
NTP: You can select **"Enable NTP client update"** in this page, then the NTP feature will be activated and synchronize from the remote time server.

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

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

4.2.5 Traffic Shaping

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



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

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

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

4.2.6 Outbound Firewall

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

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

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

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

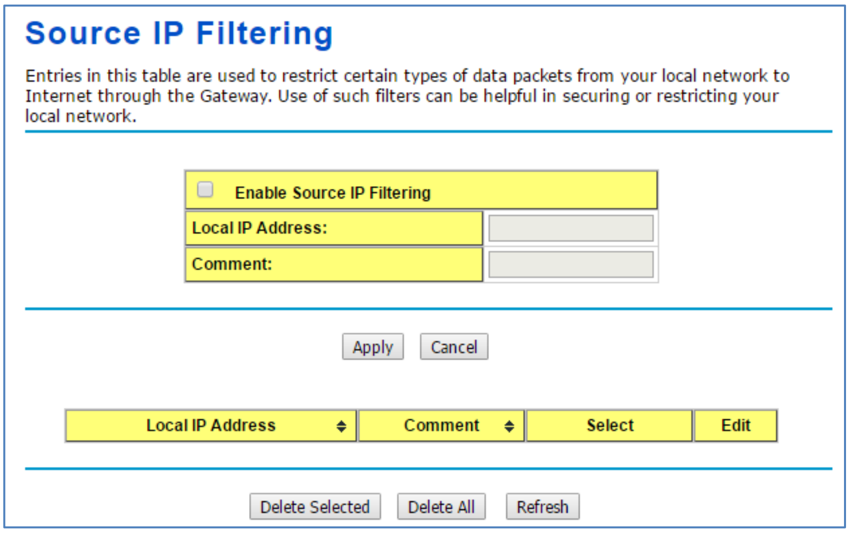
Dest Port Filtering: Destination ports filtering from the LAN to Internet through the gateway.

- **Source IP Filtering**

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

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

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



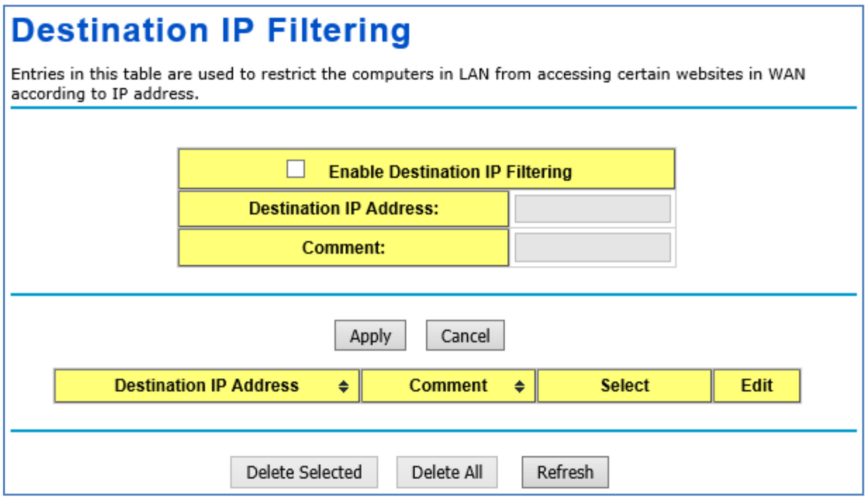
Source IP Filtering

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.

- **Destination IP Filtering**

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

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



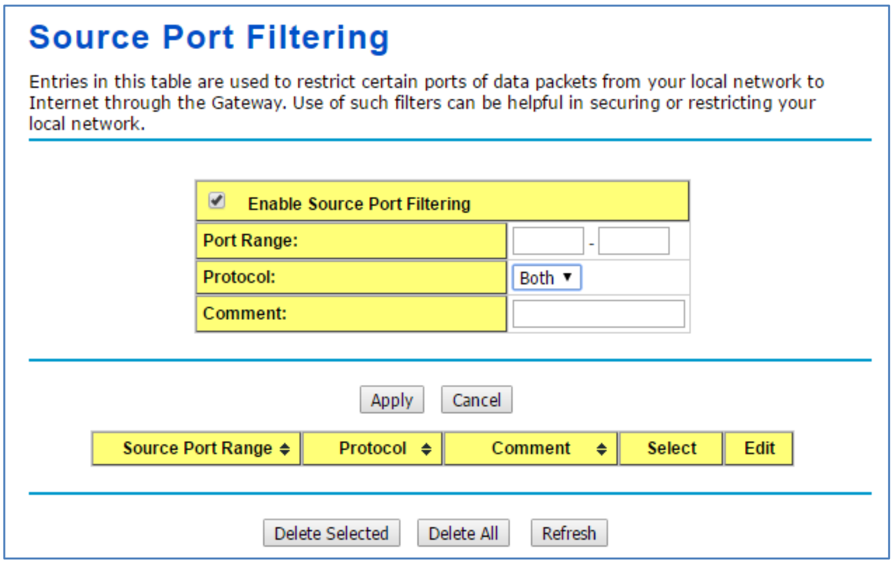
Destination IP Filtering

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

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

- **Source Port Filtering**

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



Source Port Filtering

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

☑ Enable Source Port Filtering	
Port Range:	-
Protocol:	Both ▾
Comment:	

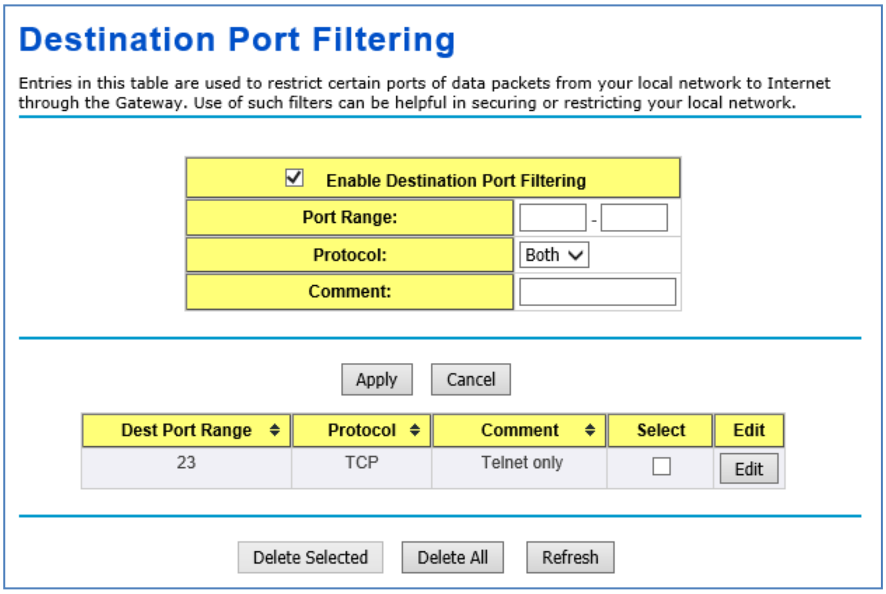
Source Port Range ⬍	Protocol ⬍	Comment ⬍	Select	Edit

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

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

- **Destination Port Filtering**

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



Destination Port Filtering

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

☑ Enable Destination Port Filtering	
Port Range:	[ ] - [ ]
Protocol:	Both
Comment:	[ ]

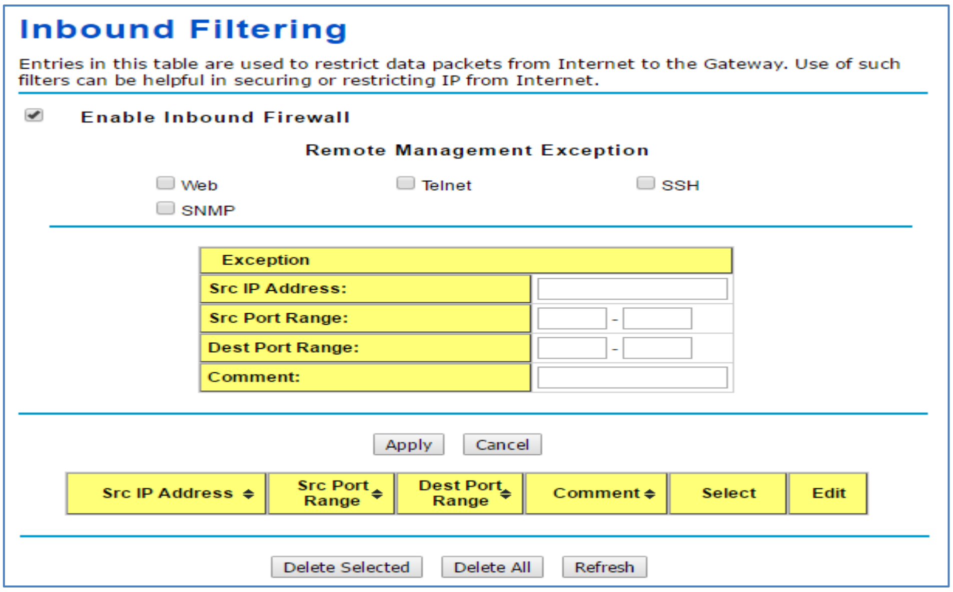
Dest Port Range	Protocol	Comment	Select	Edit
23	TCP	Telnet only	□	Edit

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

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

4.2.7 Inbound Firewall

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



Inbound Filtering

Entries in this table are used to restrict data packets from Internet to the Gateway. Use of such filters can be helpful in securing or restricting IP from Internet.

☑ 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

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

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

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

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

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

Comment: Note for the entry.

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

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

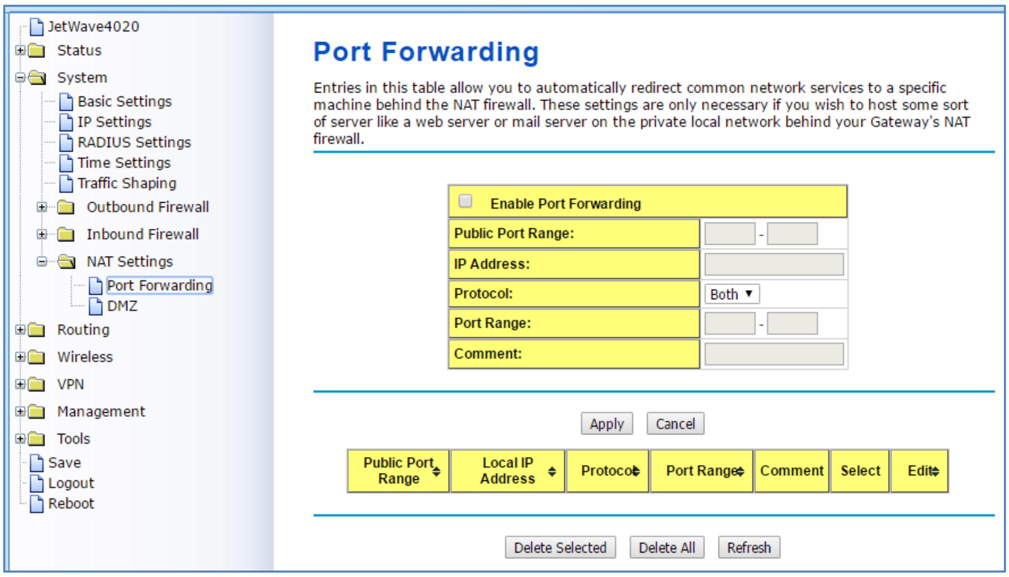
4.2.8 NAT Settings

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

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.

□ 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.

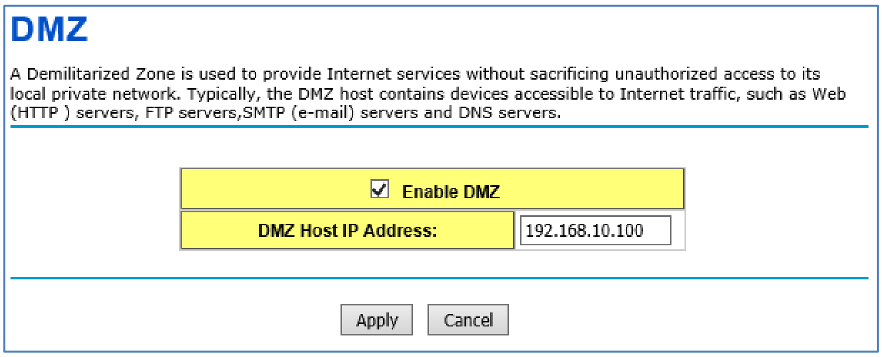
Port Range: Configure the port range of the LAN, the traffic from the public port will be redirected to these port.

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

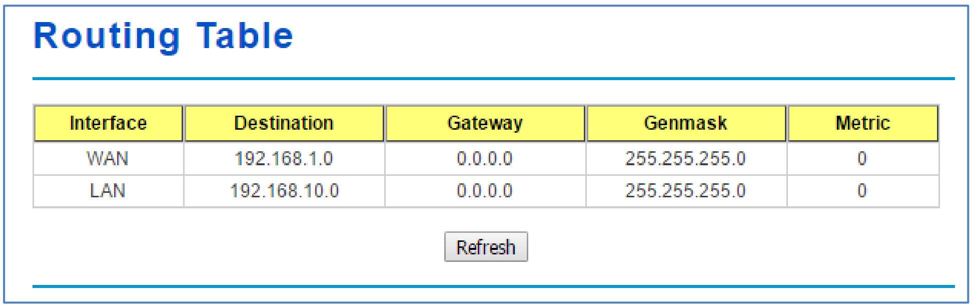
Select “**Enable DMZ**” and assign the IP address of the “**DMZ Host IP Address**”. This is the DMZ computer’s IP address. If you configure the DMZ function for your office network, please make sure this is agreed by the IT administrator.

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

4.3 Routing

4.3.1 Status

This page shows Routing Table. It includes Interface, Destination, Gateway, Genmask and Metric for all Route entries that already configured in “**Static Route**” page. Press “Refresh” to refresh the Routing Table.



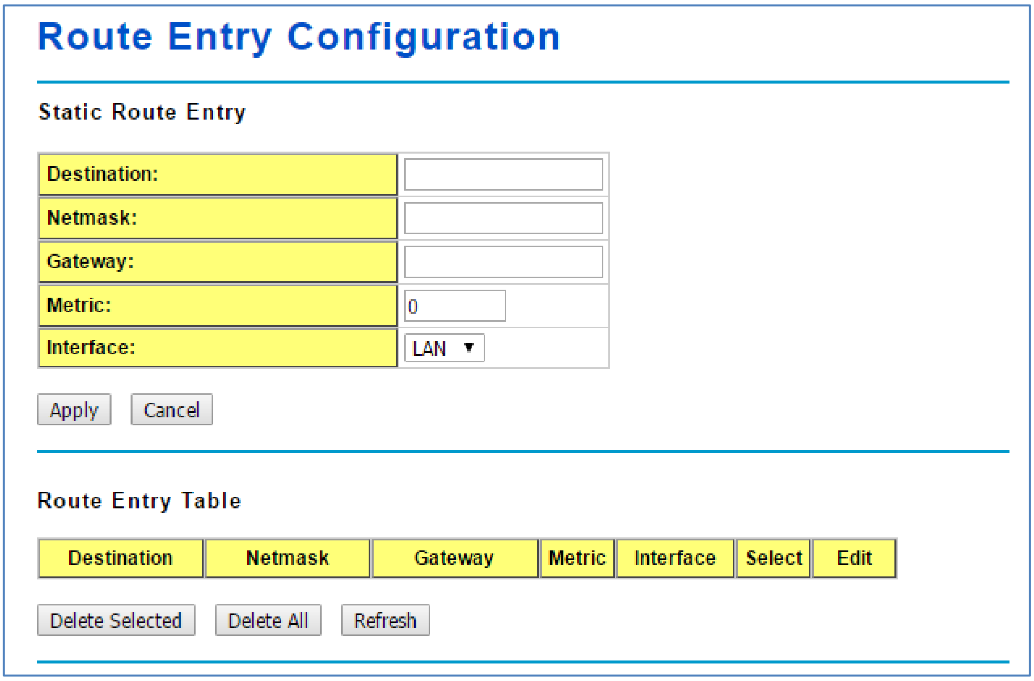
Routing Table

Interface	Destination	Gateway	Genmask	Metric
WAN	192.168.1.0	0.0.0.0	255.255.255.0	0
LAN	192.168.10.0	0.0.0.0	255.255.255.0	0

4.3.2 Static Route

This page shows “**Route Entry Configuration**”, it includes Static Route Entry and Route Entry Table.

Static Route Entry:



Route Entry Configuration

Static Route Entry

Destination:	
Netmask:	
Gateway:	
Metric:	0
Interface:	LAN ▼

Route Entry Table

Destination	Netmask	Gateway	Metric	Interface	Select	Edit

- **Static Route Entry**

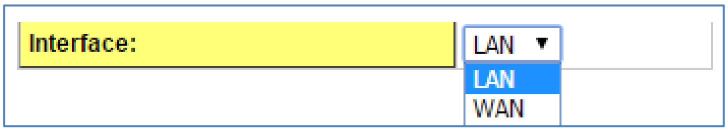
Destination: The IP address Network segment of packet’s final destination. For example, 192.168.10.0

Netmask: Enter Destination’s subnet mask

Gateway: Enter Gateway. Factory default is blank (0.0.0.0).

Metric: Assigns a cost to each available route so that the most cost-effective path can be chosen. Default value is Zero.

Interface: The outgoing network interface. LAN and WAN is available to setup here.

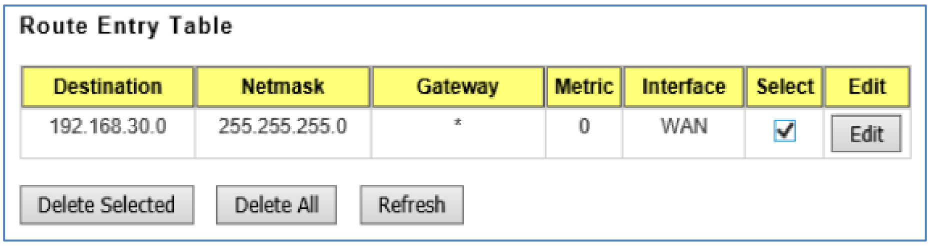


Interface: LAN ▼

Press "**Apply**" to activate the settings, or press "**Cancel**" to erase the non-apply setting value.

- **Route Entry Table**

After created entries in "**Static Route Entry**" table, it shows Destination, Netmask, Gateway, Metric, Interface for each Route Entry here.



Route Entry Table

Destination	Netmask	Gateway	Metric	Interface	Select	Edit
192.168.30.0	255.255.255.0	*	0	WAN	☑	Edit

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

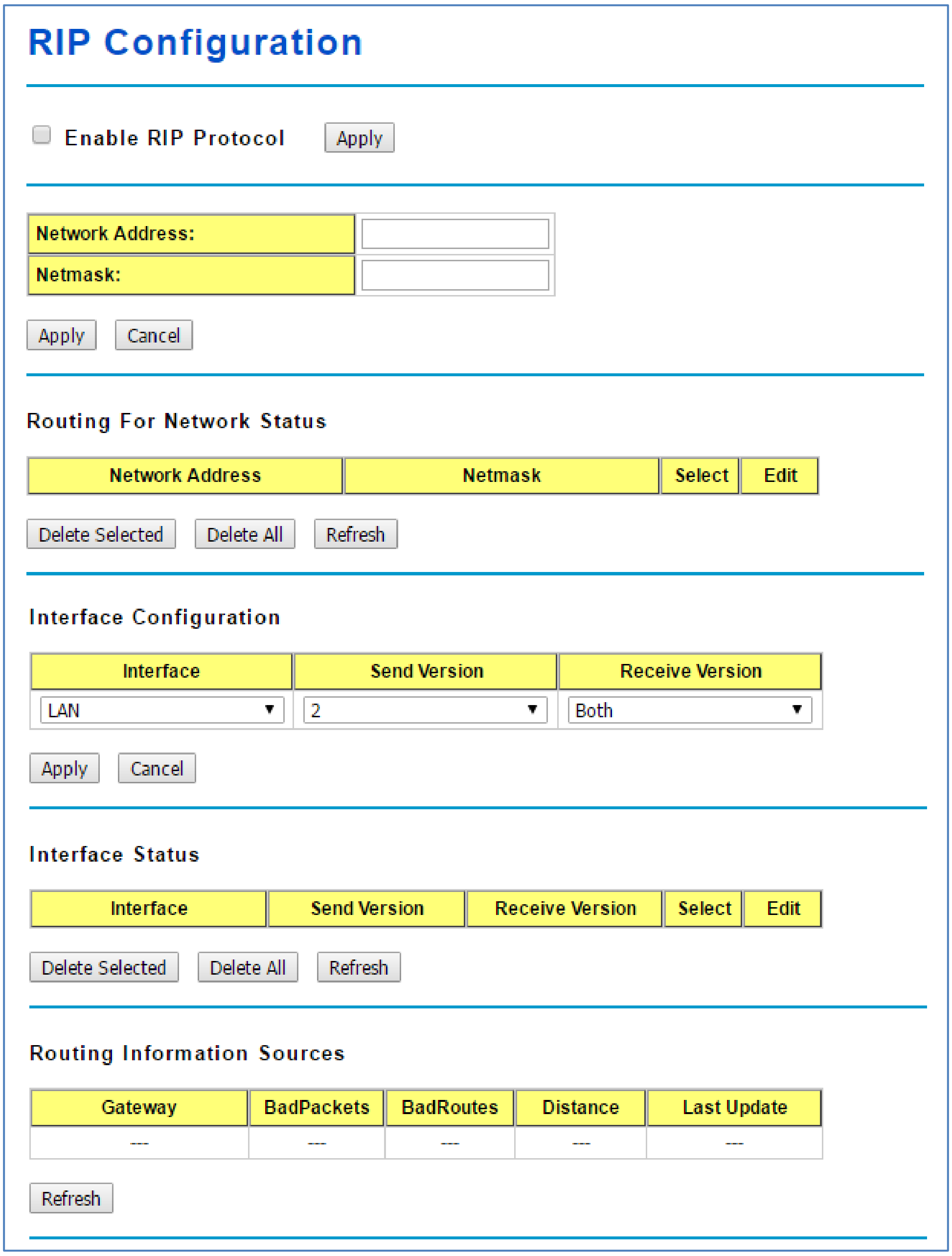
Edit: Edit entries for the Route Entry.

Delete all: Delete the all Route entries.

Refresh: Refresh Route Entry Table.

4.3.3 RIP

Use this page to configure RIP (Routing Information Protocol) Configuration.



RIP Configuration

□ Enable RIP Protocol [Apply]

Network Address:	
Netmask:	

[Apply] [Cancel]

Routing For Network Status

Network Address	Netmask	Select	Edit

[Delete Selected] [Delete All] [Refresh]

Interface Configuration

Interface	Send Version	Receive Version
LAN ▼	2 ▼	Both ▼

[Apply] [Cancel]

Interface Status

Interface	Send Version	Receive Version	Select	Edit

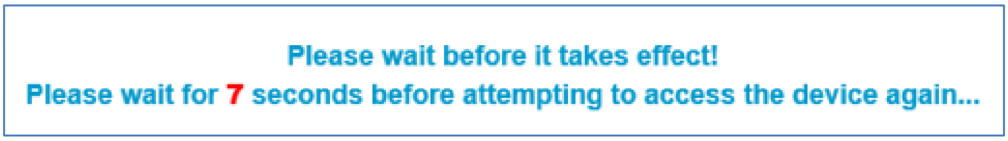
[Delete Selected] [Delete All] [Refresh]

Routing Information Sources

Gateway	BadPackets	BadRoutes	Distance	Last Update
---	---	---	---	---

[Refresh]

Enable RIP Protocol: Click to enable RIP Protocol, and then press "**Apply**" to activate the setting. Please wait for several seconds until the applied process finished.



Please wait before it takes effect!
Please wait for 7 seconds before attempting to access the device again...

Network Address: The IP address Network segment of packet's final destination. For example, 192.168.10.0

Netmask: Enter destination's subnet mask. Press "Apply" to activate the settings.

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

➢ Routing for Network Status

This table shows each configured Routing entry, it includes the Network Address and Netmask.

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

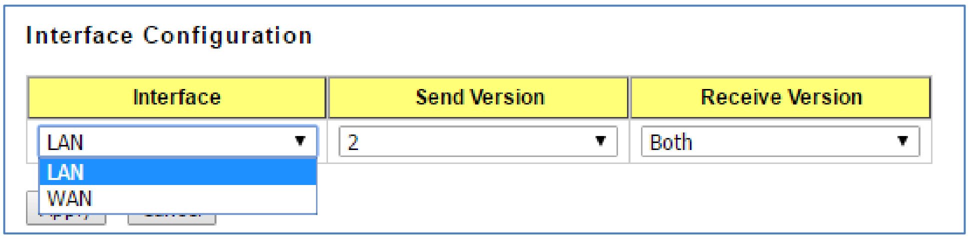
Edit: Edit entries for the Routing configuration.

Delete all: Delete the all Route entries.

Refresh: Refresh Route Entry Table.

➢ Interface Configuration

Configure RIP Version for each interface.



Interface Configuration

Interface	Send Version	Receive Version
LAN ▼	2 ▼	Both ▼

Interface: Select LAN or WAN.

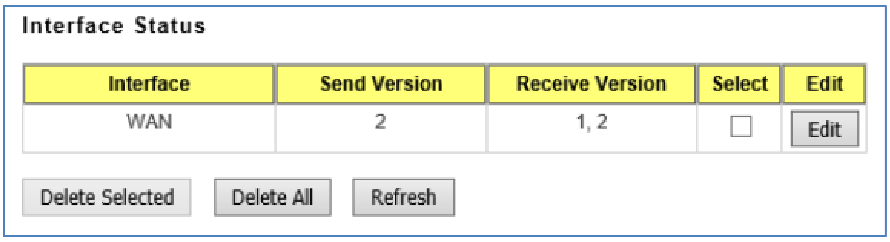
Send Version: Select 1, 2 or Both. Factory default is 2.

Receive Version: Select 1, 2 or Both. Factory default is Both.

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

➢ Interface Status

It shows configuration status for each interface. Version shows “1,2” means configure “**Both**” for RIP version.



Interface Status

Interface	Send Version	Receive Version	Select	Edit
WAN	2	1, 2	□	Edit

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

Edit: Edit entries for each interface.

Delete all: Delete the all Route entries.

Refresh: Refresh Route Entry Table.

➢ Routing Information Sources

The table shows Gateway, BadPackets, BadRoutes, Distance and Last Update for Routing information sources. Press “**Refresh**” to refresh the table.

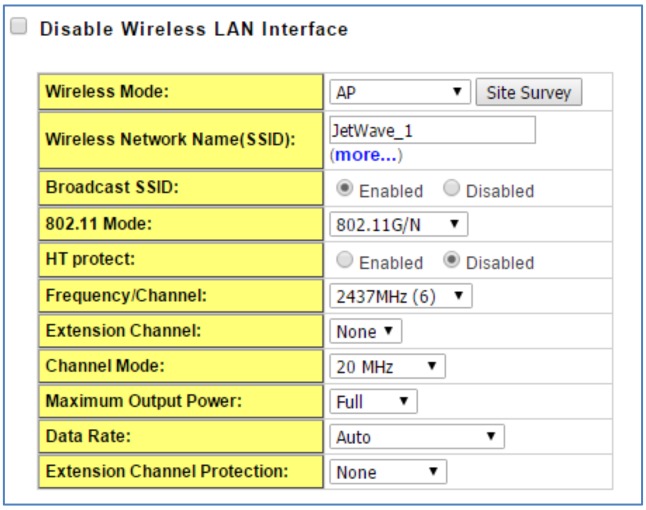
4.4 Wireless

The "**Wireless**" feature set pages allow users to configure the Wireless LAN configuration. The Wireless means the WIFI radio of the device. JetWave 4020/4020E series equip dual-radio interface, there are **WLAN 1** and **WLAN 2** for configuration, it includes Basic Settings, Security Settings, Advanced Settings and Access Control can be configured in the WLAN Settings.

4.4.1 Basic Settings

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

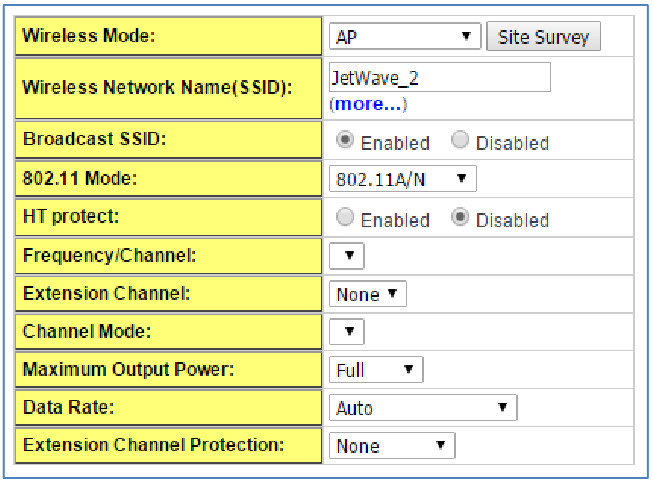
- **WLAN 1- Factory default setting**



□ Disable Wireless LAN Interface

Wireless Mode:	AP ▼ Site Survey
Wireless Network Name(SSID):	JetWave_1 (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:	Full ▼
Data Rate:	Auto ▼
Extension Channel Protection:	None ▼

- **WLAN 2- Factory default setting**



Wireless Mode:	AP ▼ Site Survey
Wireless Network Name(SSID):	JetWave_2 (more...)
Broadcast SSID:	● Enabled ○ Disabled
802.11 Mode:	802.11A/N ▼
HT protect:	○ Enabled ● Disabled
Frequency/Channel:	▼
Extension Channel:	None ▼
Channel Mode:	▼
Maximum Output Power:	Full ▼
Data Rate:	Auto ▼
Extension Channel Protection:	None ▼

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 JetWave 4020/4020E series.

AP: The AP works as the Access Point mode, it establishes a wireless coverage and receives connectivity from other wireless client 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, Extension Channel, Channel Mode, Maximum Output Power (per chain), Data Rate and Extension Channel Protection. When the Wireless Client connected to the AP, the client must follow AP settings for communicating. Factory default setting of WLAN 1 and WLAN 2 is AP mode.

Wireless Client: The JetWave 4020/4020E series 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. In Wireless Client mode, you can configure the Wireless Network Name (SSID) that you want to connect, 802.11 mode, Channel Mode, Maximum Output Power (per chain), Data Rate and Extension Channel Protection. While in wireless client, please note that all the rest of Wireless Client settings must be the same as your AP settings.

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

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

Factory default SSID on WLAN 1: JetWave_1

Factory default SSID on WLAN 2: JetWave_2

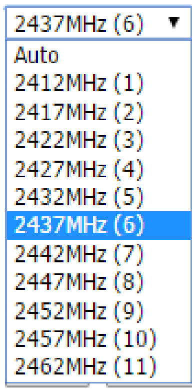
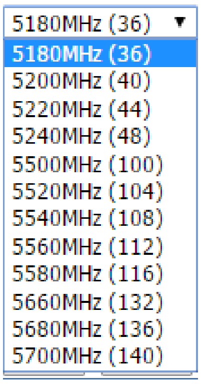
Broadcast SSID: Enable or disable Broadcast SSID. Under AP mode, hiding network name is necessary when you are in a wireless environment that may have potential risk. By disabling broadcast SSID, the clients can not scan and find the AP, so that malicious attack by some illegal clients could be avoided.

802.11 Mode: The AP can communicate with wireless devices of 802.11a/b/g/n/ac. You can select 802.11 Mode and it will work under an appropriate wireless mode automatically. WLAN 1 support 2.4G band, and WLAN 2 support 5G band. Different band has different settings.

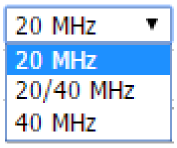
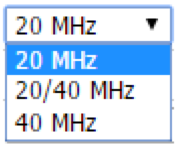
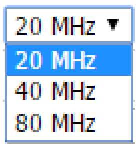
802.11 Supported Mode	
WLAN 1	**WLAN 2**
802.11B Only	802.11A Only
802.11G Only	802.11A/N
802.11 G/N	802.11AC

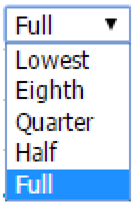
HT Protect: Enable HT (High Throughput) Protect to ensure HT transmission with MAC mechanism. Under 802.11n mode, wireless client can be divided into HT STA and Non-HT STA, among which the one with HT protect enabled gets higher throughput.

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. WLAN 1 support 2.4G band, which supports 12~13 channels. WLAN 2 support 5G band1 and band3, it includes 12 channels.

WLAN 1	**WLAN 2**
 2437MHz (6) Auto 2412MHz (1) 2417MHz (2) 2422MHz (3) 2427MHz (4) 2432MHz (5) 2437MHz (6) 2442MHz (7) 2447MHz (8) 2452MHz (9) 2457MHz (10) 2462MHz (11)	 5180MHz (36) 5180MHz (36) 5200MHz (40) 5220MHz (44) 5240MHz (48) 5500MHz (100) 5520MHz (104) 5540MHz (108) 5560MHz (112) 5580MHz (116) 5660MHz (132) 5680MHz (136) 5700MHz (140)

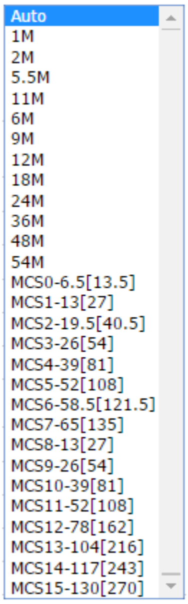
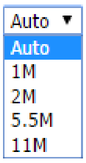
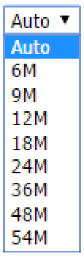
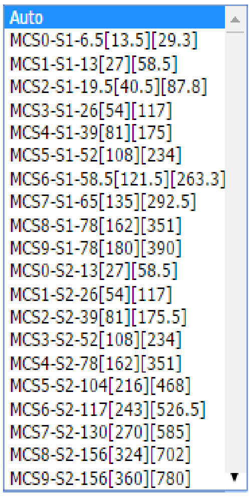
Channel Mode: Two levels are available: 20MHz and 20/40MHz. The latter one can enhance the data rate more effectively, but takes more bandwidth, thus cause potential interference.

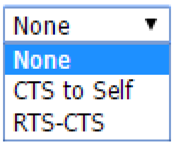
WLAN 1	**WLAN 2**	
802.11G/N	**802.11A/N**	**802.11AC**
 20 MHz 20 MHz 20/40 MHz 40 MHz	 20 MHz 20 MHz 20/40 MHz 40 MHz	 20 MHz 20 MHz 40 MHz 80 MHz



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. **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 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.

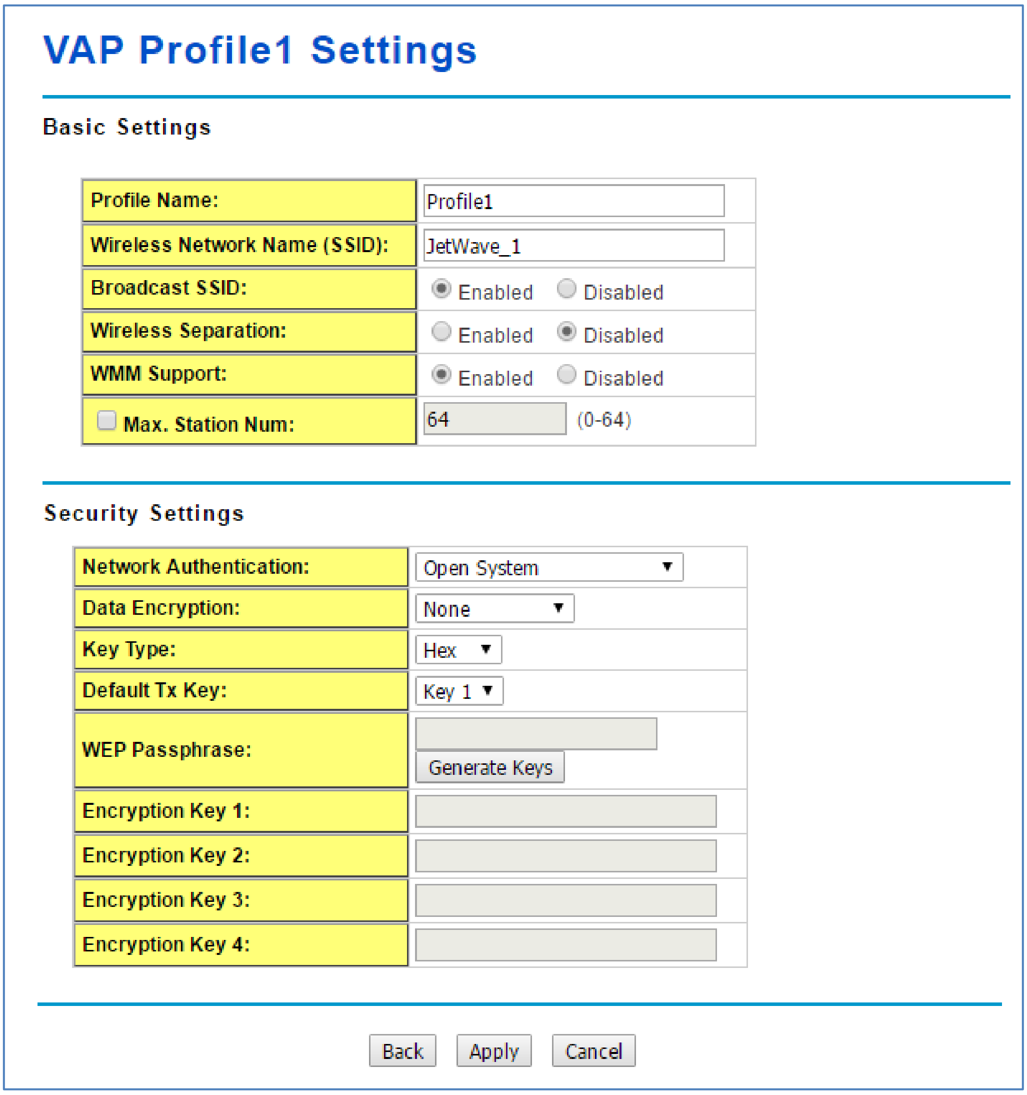
802.11G/N,	**802.11B Only**	**802.11G Only,**	**802.11AC**
802.11A/N		**802.11A Only**	
 Auto 1M 2M 5.5M 11M 6M 9M 12M 18M 24M 36M 48M 54M MCS0-6.5[13.5] MCS1-13[27] MCS2-19.5[40.5] MCS3-26[54] MCS4-39[81] MCS5-52[108] MCS6-58.5[121.5] MCS7-65[135] MCS8-13[27] MCS9-26[54] MCS10-39[81] MCS11-52[108] MCS12-78[162] MCS13-104[216] MCS14-117[243] MCS15-130[270]		 Auto Auto 6M 9M 12M 18M 24M 36M 48M 54M	 Auto MCS0-S1-6.5[13.5][29.3] MCS1-S1-13[27][58.5] MCS2-S1-19.5[40.5][87.8] MCS3-S1-26[54][117] MCS4-S1-39[81][175] MCS5-S1-52[108][234] MCS6-S1-58.5[121.5][263.3] MCS7-S1-65[135][292.5] MCS8-S1-78[162][351] MCS9-S1-78[180][390] MCS0-S2-13[27][58.5] MCS1-S2-26[54][117] MCS2-S2-39[81][175.5] MCS3-S2-52[108][234] MCS4-S2-78[162][351] MCS5-S2-104[216][468] MCS6-S2-117[243][526.5] MCS7-S2-130[270][585] MCS8-S2-156[324][702] MCS9-S2-156[360][780]



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 to Self**, the transmission amount of **RTS-CTS** is much lower. Press “**Apply**” to activate the settings.

4.4.2 Security Settings

The page allows you configure the 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 Settings**

Profile Name: The profile name of the settings.

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

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

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 Settings**

Network Authentication: Select Network Authentication type.

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.

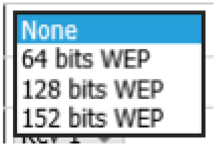
WPA & WPA2 with RADIUS: If it is selected, AES & TKIP encryption and RADIUS server is required.

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

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

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

<u>Data Encryption</u>: If data encryption is enabled, the key is required and only sharing the same key with other wireless devices can the communication be established.



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

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

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

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

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

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

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

Press "**Apply**" to activate the settings, and you can also press "Back" to check the **VAP Profile Settings** for each Profile.

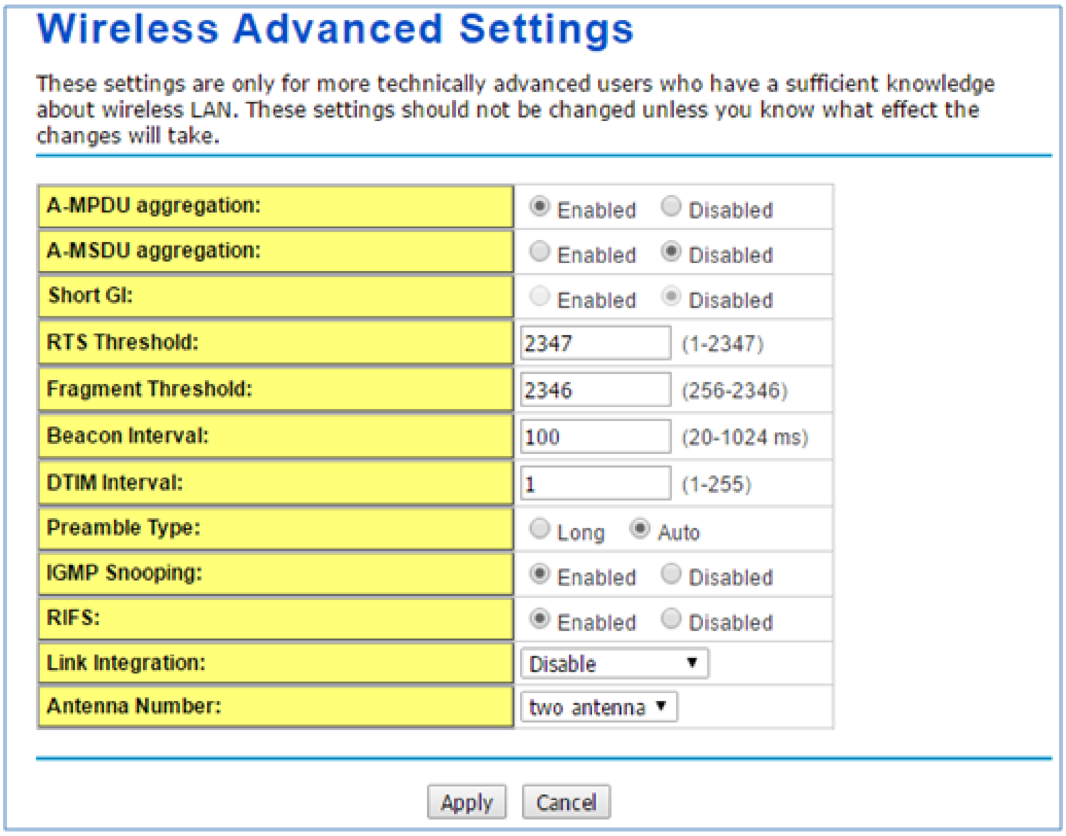
Note:

(1) We strongly recommend you enable wireless security on your network!

(2) Only setting the same Authentication, Data Encryption and Key in the JetWave and other associated wireless devices, can the communication be established!

4.4.3 Advanced Settings

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

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will take.

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
IGMP Snooping:	● Enabled ○ Disabled
RIFS:	● Enabled ○ Disabled
Link Integration:	Disable ▾
Antenna Number:	two antenna ▾

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

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

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

Fragment 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.

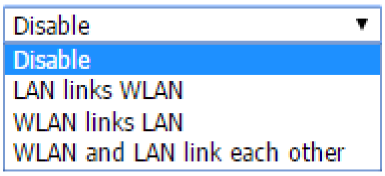
DTIM Interval: DTIM, which stands for Delivery Traffic Indication Message, is contained in the data packets. It is for enhancing the wireless transmission efficiency. The default is set to 1. Enter a value between 1 and 255.

Preamble Type: It defines some details on the 802.11 physical layer. "**Long**" and "**Short**" are available. (WLAN 1 supported only)

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 and Wireless LAN interface together. Once one of them fails, the other interface becomes down as well. The function appears when wireless mode set AP or Wireless Client.



Disable: Disable the Link Integration.

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

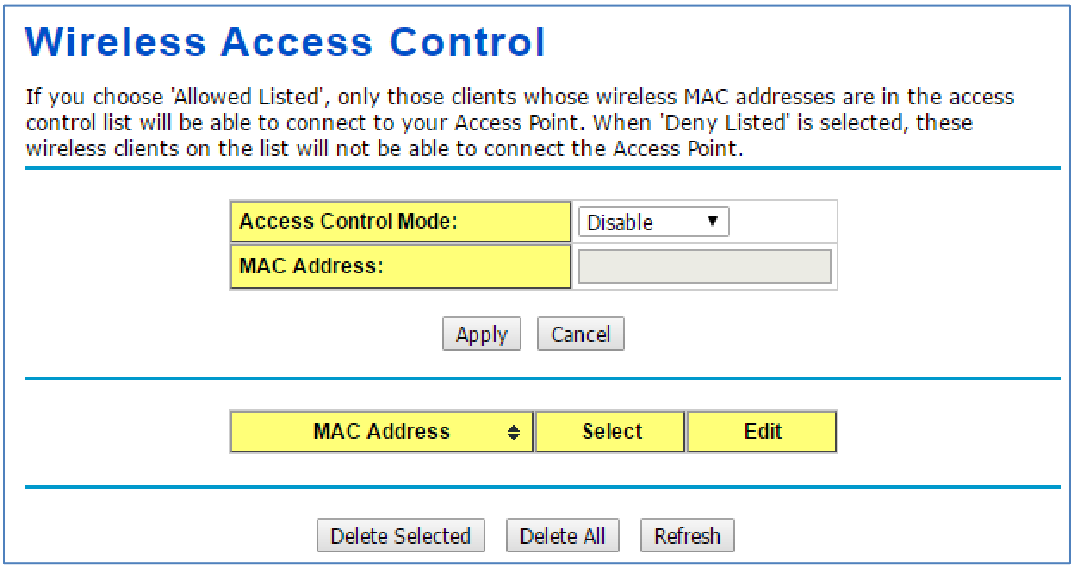
WLAN links LAN: Single direction only while the WLAN failure, the binding Ethernet port will become link down. (Wireless Client mode supported only)

WLAN and LAN link each other: This is Bi-directional integration no matter while LAN Ethernet port failure or WLAN radio failure. (Wireless Client mode supported only)

Antenna Number: The setting allows you configure **one antenna** for 1T1R SISO or **two antenna** for 2T2R MIMO. While you change the antenna number, please connect the antenna to the correct antenna sockets of the WIFI radio. Please refer to the chapter 2.4 for WIFI antenna information.

4.4.4 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 JetWave.



Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

Access Control Mode:	Disable ▼
MAC Address:	

MAC Address	Select	Edit

<u>Access Control Mode</u>: Allow Listed or Deny Listed.

<u>MAC Address</u>: 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.

4.5 VPN

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

The OpenVPN is a full-featured SSL VPN which implements OSI layer 2 or 3 secure network extension using the industry standard SSL/TLS protocol, supports flexible client authentication methods based on certificates, smart cards, and/or username/password credentials, and allows user or group-specific access control policies using firewall rules applied to the VPN virtual interface. The first step in building an OpenVPN 2.x configuration is to establish a PKI (public key infrastructure). PKI consists of a separate certificate (also known as a public key) and private key for the server and each client, and a master Certificate Authority (CA) certificate and key which is used to sign each of the server and client certificates. Please refer to Korenix JetBox 5630 user manual for example PKI key generation.

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

Filename	Needed By	Purpose	Secret
ca.crt	server + all clients	Root CA certificate	NO
ca.key	key signing machine only	Root CA key	YES
dh{n}.pem	server only	Diffie Hellman parameters	NO
server.crt	server only	Server Certificate	NO
server.key	server only	Server Key	YES
client.crt	client only	Client1 Certificate	NO
client.key	client only	Client key	YES

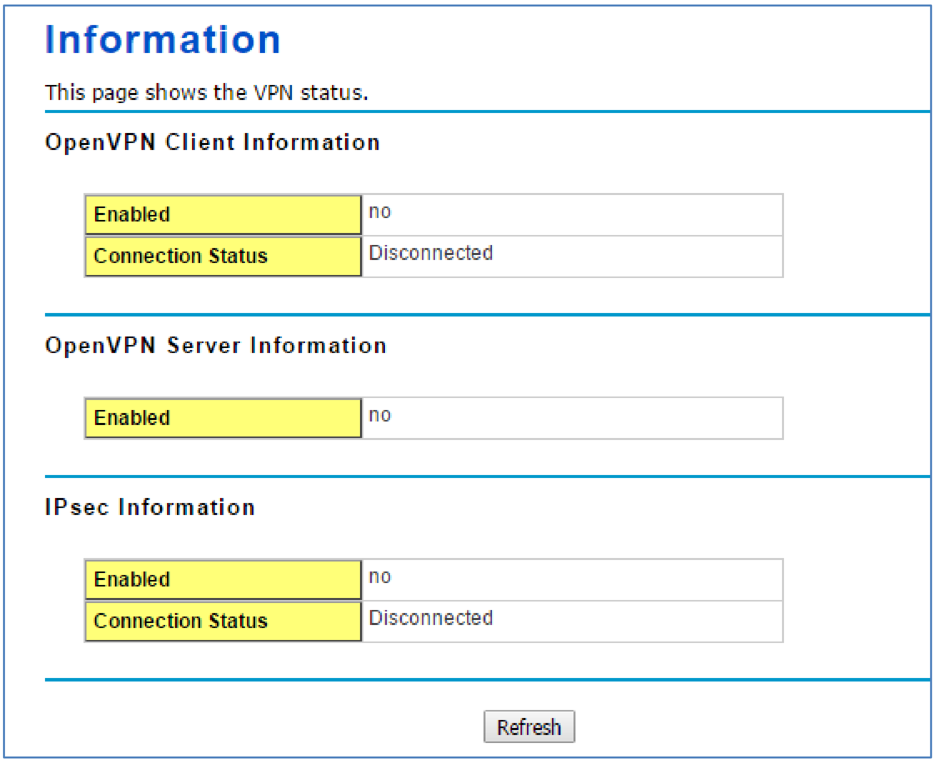
Note: The file names of these keys are pre-defined and can’t be changed.

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

Note: The settings should be consistent with OpenVPN server.

4.5.1 Status

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



Information

This page shows the VPN status.

OpenVPN Client Information

Enabled	no
Connection Status	Disconnected

OpenVPN Server Information

Enabled	no

IPsec Information

Enabled	no
Connection Status	Disconnected

Enabled:

yes: The VPN function already enabled.

no: The VPN function not enabled yet.

Connection Status:

Connected: The VPN connection already build successfully.

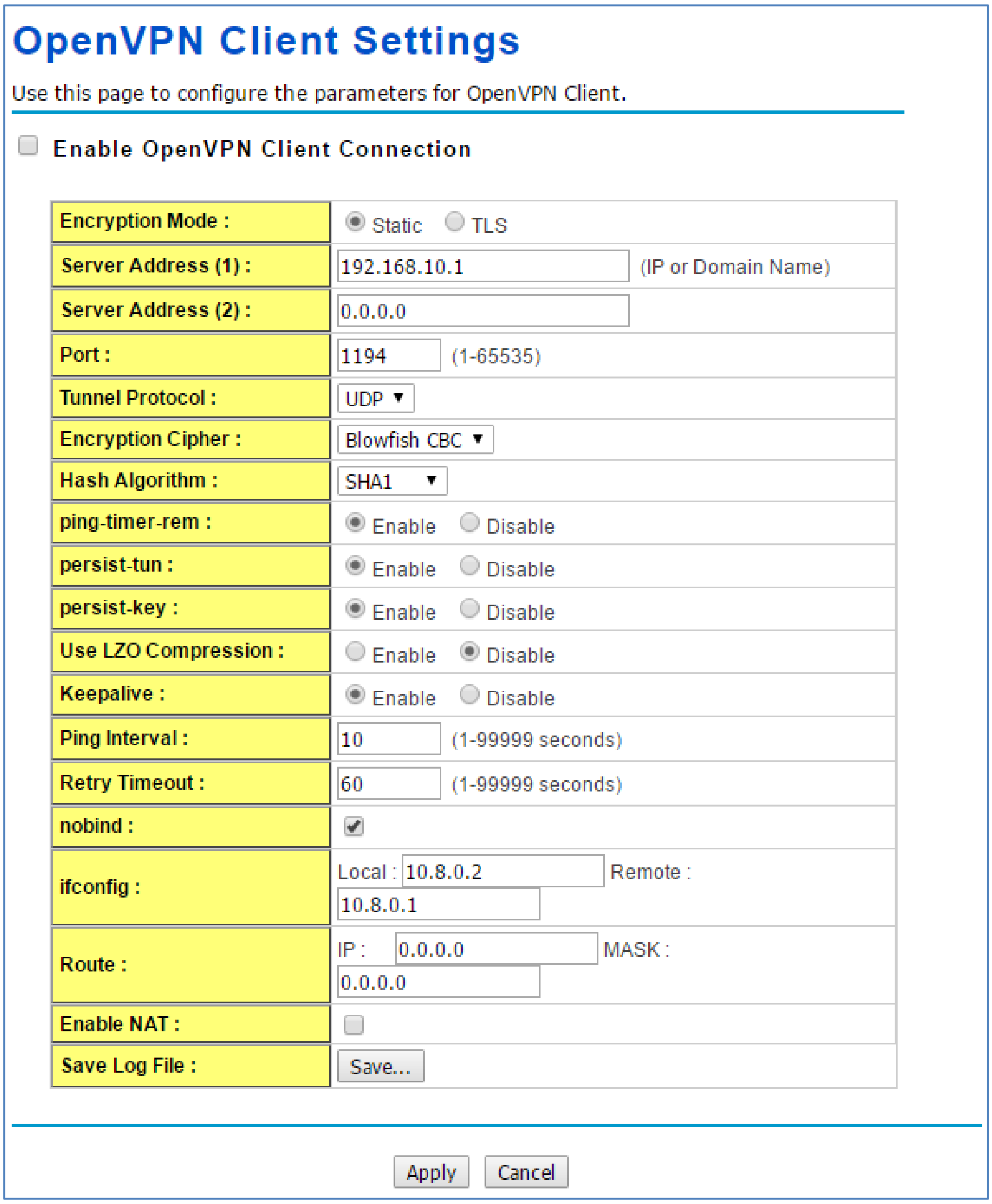
Disconnected: The VPN not connect.

Tx / Rx Bytes: You can see the transmission data volume in bytes after the VPN client is connected.

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

4.5.2 OpenVPN Client

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



OpenVPN Client Settings

Use this page to configure the parameters for OpenVPN Client.

☐ Enable OpenVPN Client Connection

Encryption Mode :	● 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...

Apply Cancel

Click on "**Enable OpenVPN Client Connection**" to enable OpenVPN Client mode.

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

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

Port: Input the port number that your VPN service used. Default value is 1194.

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.

Login: Certificated with Username and Password. Must go with login authenticated supported VPN server.

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.

Renegotiation Interval: Renegotiation interval for data channel key. (TLS mode only)

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

ifconfig: Input the tunnel IP address that VPN use.

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

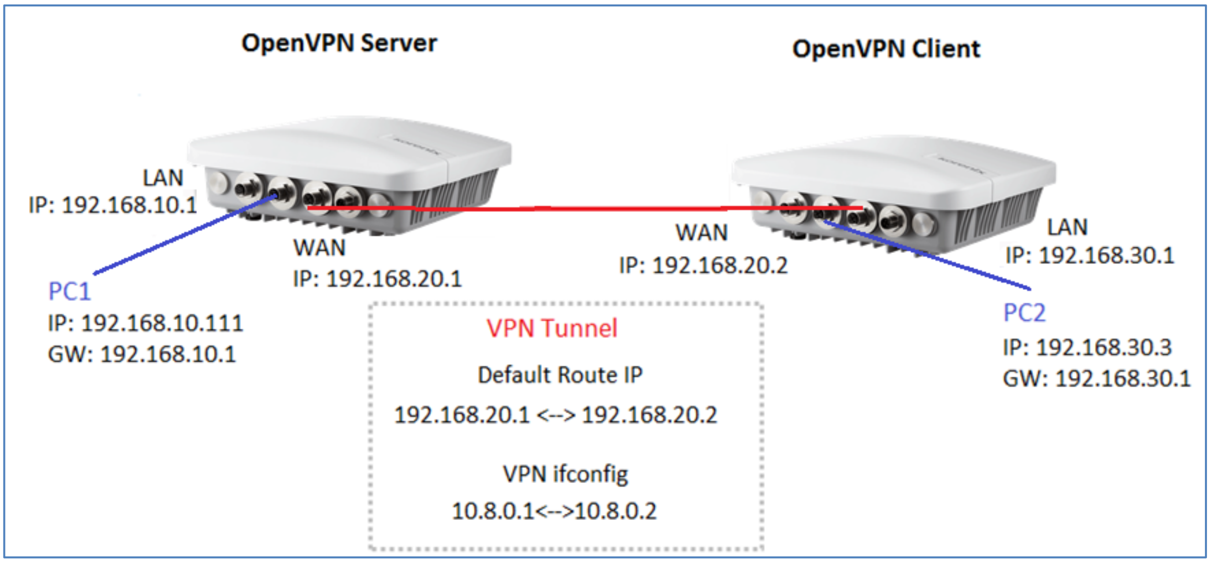
Enable NAT: Enable NAT(Network Address Translation).

Save Log File: Save OpenVPN Client log file.

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

4.5.3 OpenVPN Server

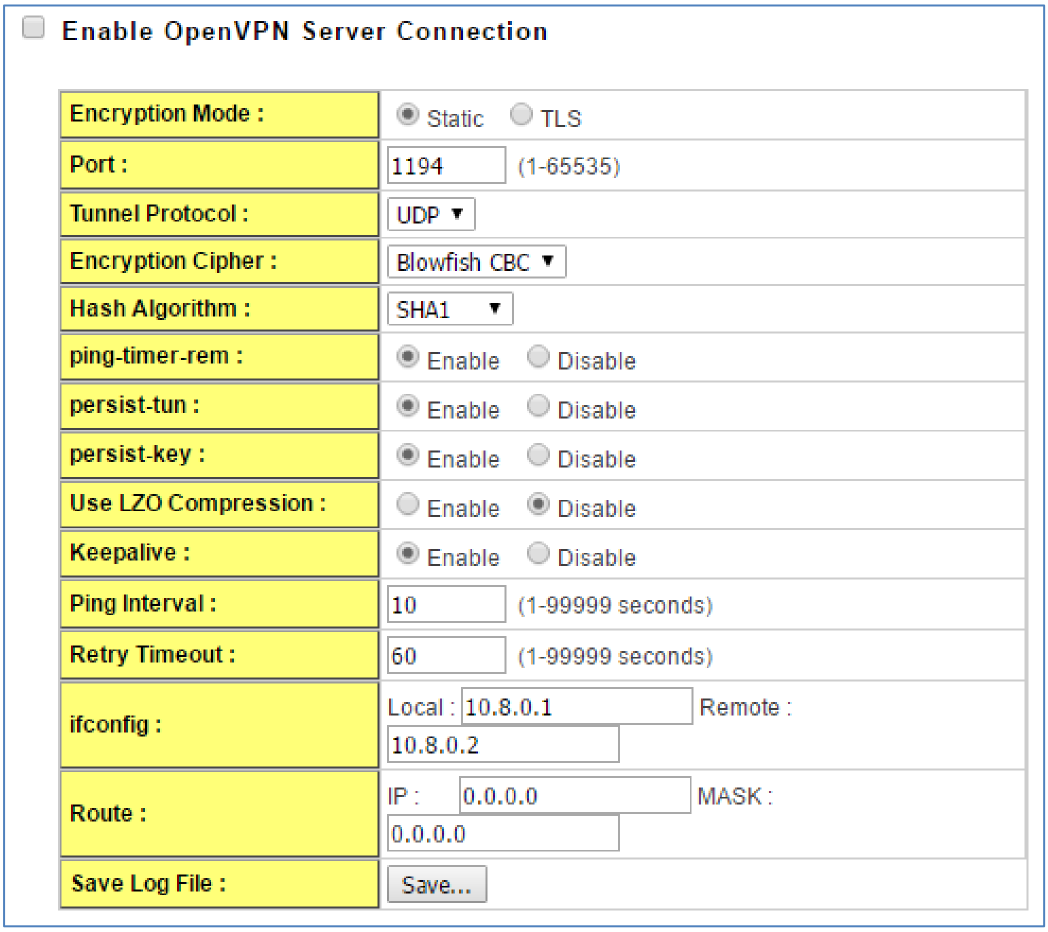
To help you easier create the One to One Secure M2M (machine to machine) connection for the remote devices. The device supports both OpenVPN Server and OpenVPN Client. This Server setting allows you to configure the Secure M2M connection for one remote client. Below is the simple test setup for your reference. The red color line becomes a VPN Tunnel and the transmission data are secured. To configure the settings, you need to have IP plan of the 2 sites and the routing/VPN path first. Configure the device as Router mode and give the Ethernet ports specific IP as the default gateway for the connected devices (ex: PCs). For VPN Tunnel, you can choose WAN port or WIFI interface. Type the connected IP in VPN ifconfig and apply/save the settings.



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

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

Please generate the key by VPN Server (ex: JetBox 5630) or 3rd party Key generation tool.



□ Enable OpenVPN Server Connection

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...

Click on "**Enable OpenVPN Server Connection**" to enable OpenVPN Server mode.

Encryption Mode: Select the encryption is Static or TLS.

Static Key: Use a pre-shared static key.

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

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

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

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

Hash Algorithm: Select the hash algorithm.

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

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

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

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

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

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

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

Renegotiation Interval: Renegotiation interval for data channel key. (TLS mode only)

Ifconfig: Input the tunnel IP address that VPN use.

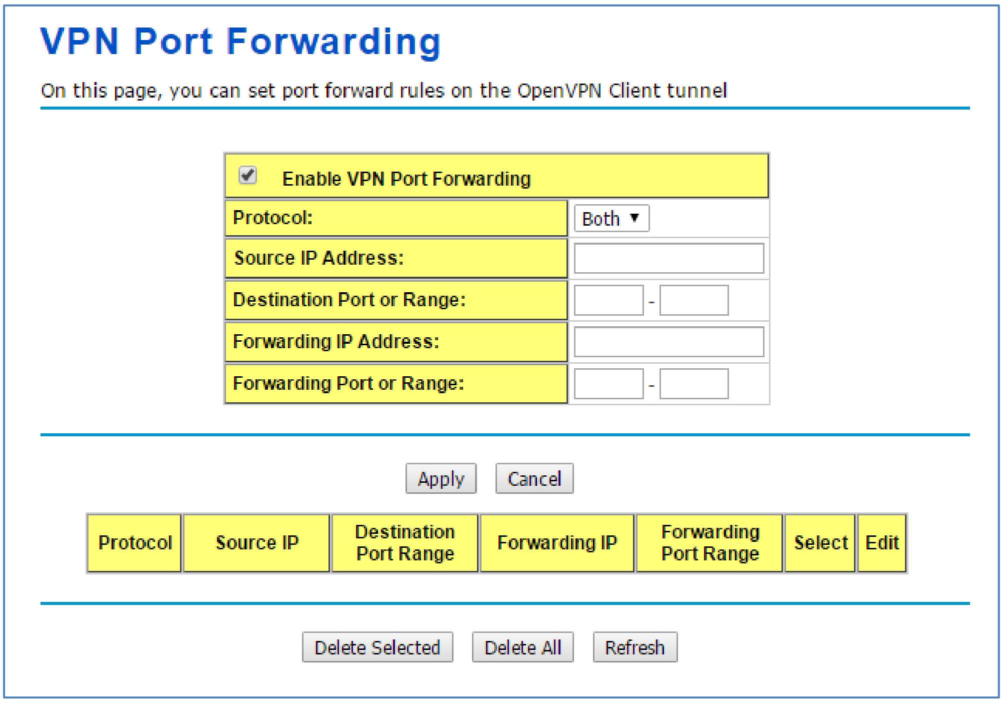
Route: Input the route IP and MASK. This is the target IP domain you can access through the VPN tunnel.

Save Log File: Save OpenVPN Server log file.

Press “Apply” to activate settings.

4.5.4 Port Forwarding

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



VPN Port Forwarding

On this page, you can set port forward rules on the OpenVPN Client tunnel

☑ 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

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

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

Source IP Address: Type specific source IP address.

Destination Port or Range: Configure the port range of destination.(Destination is JetWave

4020/4020E that you use)

Forwarding IP Address: Type the specific forwarding IP address.

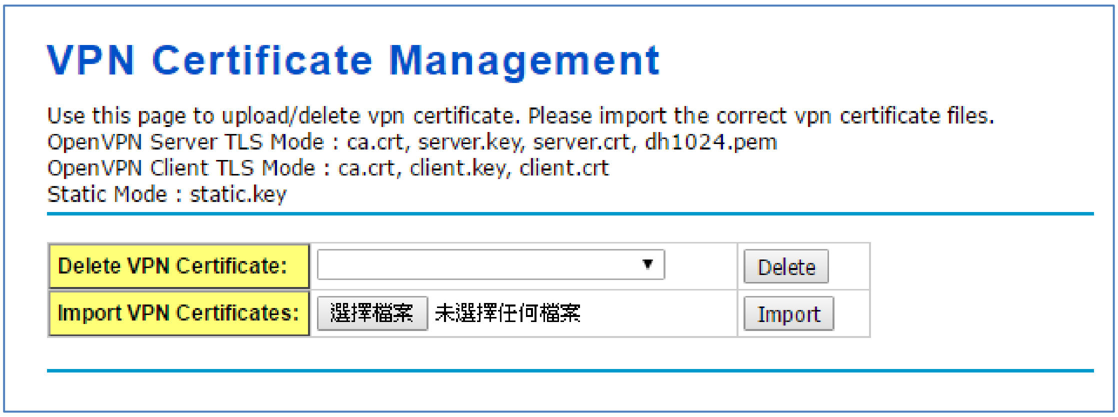
Forwarding Port or Range: Configure the port or range for forwarding device.

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

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

4.5.5 VPN Certificate

This page allow user to manage the user certificate file.



VPN Certificate Management

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

Delete VPN Certificate:	▼	Delete
Import VPN Certificates:	選擇檔案 未選擇任何檔案	Import

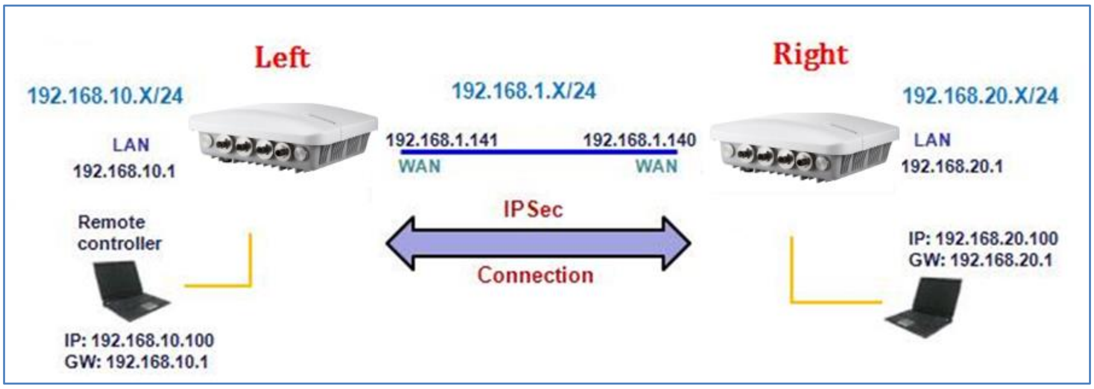
Import: Import the correct VPN Certificate.

Delete: Delete existing VPN Certificate.

4.5.6 IPSec

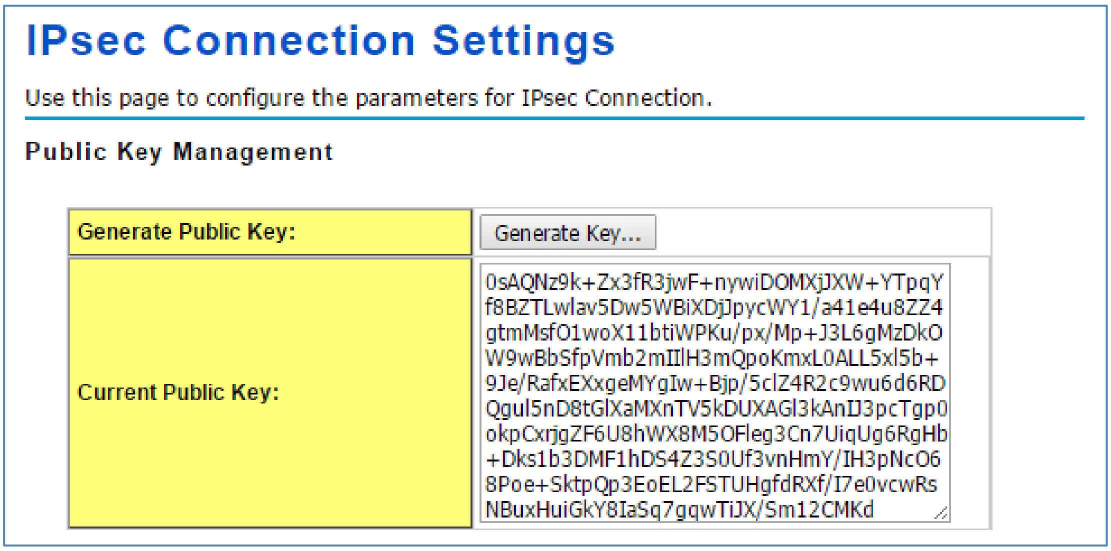
Use this page to configure the parameters for IPsec Connection. The VPN tunnel has two participants on its ends, called left and right, and which participant is considered left or right is arbitrary. You can configure various parameters for these two ends in this page.

Simple example about IPsec connection:



<u>Public Key Management</u>:

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



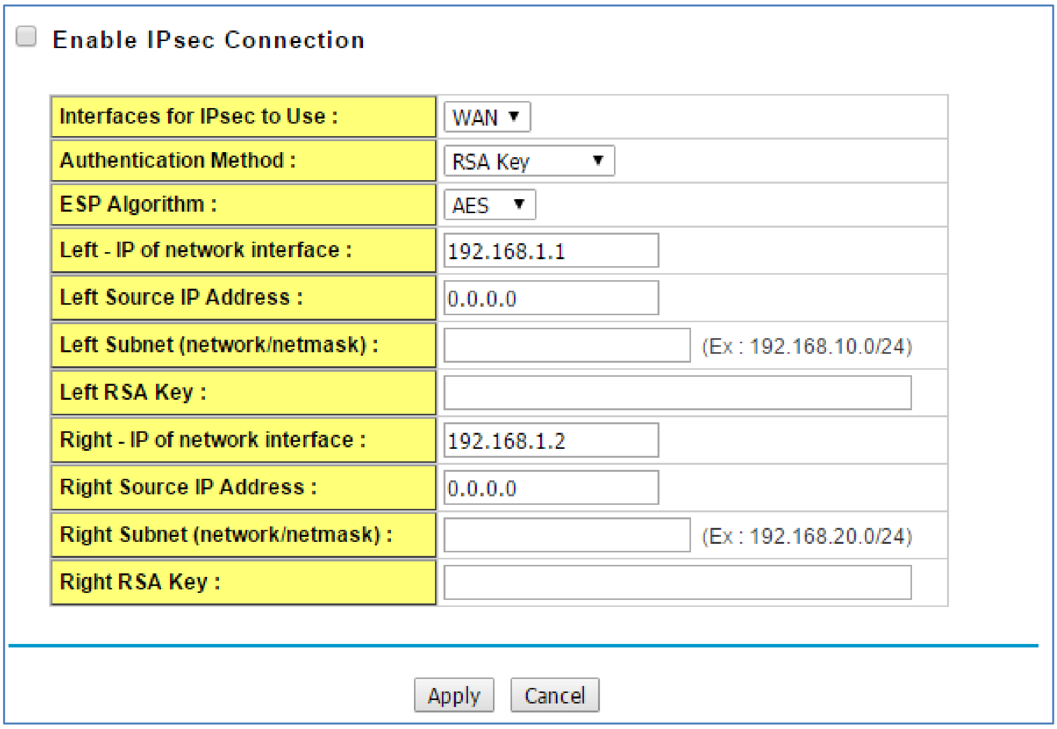
IPsec Connection Settings

Use this page to configure the parameters for IPsec Connection.

Public Key Management

Generate Public Key:	Generate Key...
Current Public Key:	0sAQNz9k+Zx3fR3jwF+nywiDOMXjJXW+YTpqY f8BZTLwlav5Dw5WBiXDjJpycWY1/a41e4u8ZZ4 gtmMsfO1woX11btiWPKu/px/Mp+J3L6gMzDkO W9wBbSfpVmb2mIIlH3mQpoKmxL0ALL5xl5b+ 9Je/RafxEXxgeMYgIw+Bjp/5clZ4R2c9wu6d6RD Qgul5nD8tGlXaMXnTV5kDUXAGl3kAnIJ3pcTgp0 okpCxrjgZF6U8hWX8M5OFleg3Cn7UiqUg6RgHb +Dks1b3DMF1hDS4Z3S0Uf3vnHmY/IH3pNcO6 8Poe+SktpQp3EoEL2FSTUHgfdRXf/I7e0vcwRs NBuxHuiGkY8IaSq7gqwTiJX/Sm12CMKd

Click on "**IPsec Connection**" to enable IPsec function.



□ Enable IPsec Connection

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.6 Management

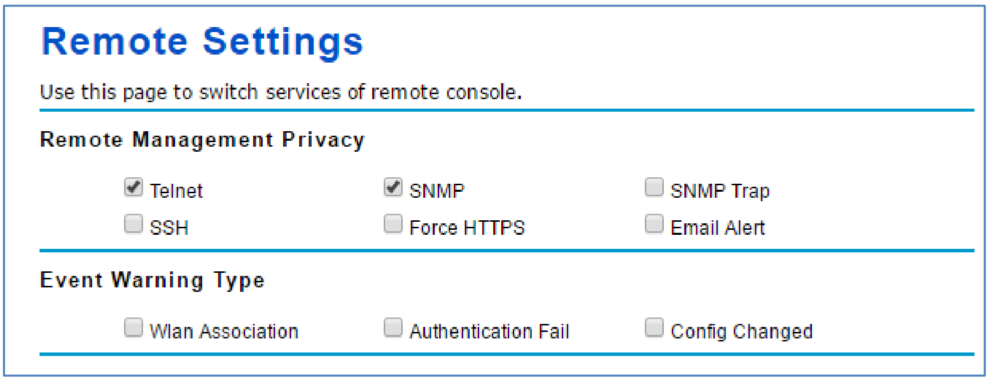
The "**Management**" feature set pages allow users to configure the Remote Setting, SMTP Configuration, Login Settings, Firmware Update, Configuration File, Certification File, Controller, Remote IP Scan and Topology Discovery.

4.6.1 Remote Setting

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

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

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



Remote Settings

Use this page to switch services of remote console.

Remote Management Privacy

☑ Telnet ☑ SNMP □ SNMP Trap
□ SSH □ Force HTTPS □ Email Alert

Event Warning Type

□ Wlan Association □ Authentication Fail □ Config Changed

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

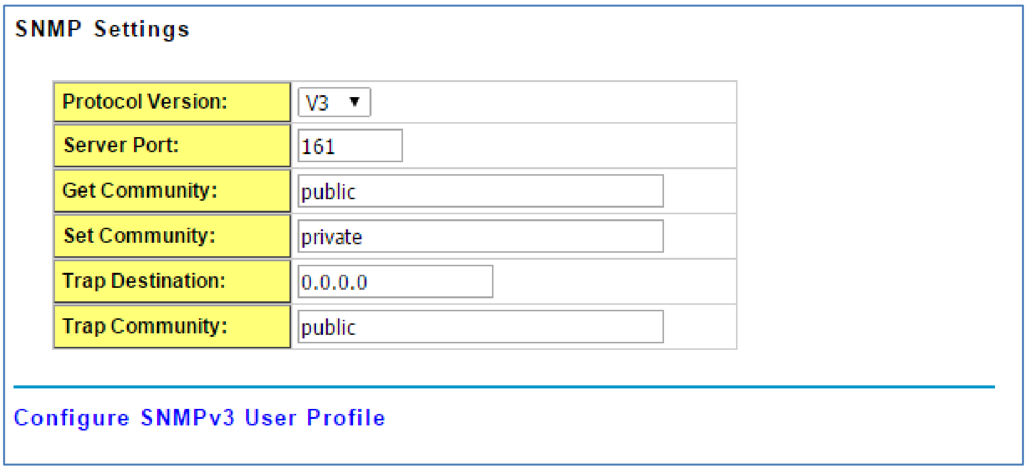
Event Warning Type: The event warning type selection.

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



SNMP Settings

Protocol Version:	V3
Server Port:	161
Get Community:	public
Set Community:	private
Trap Destination:	0.0.0.0
Trap Community:	public

Configure SNMPv3 User Profile

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

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

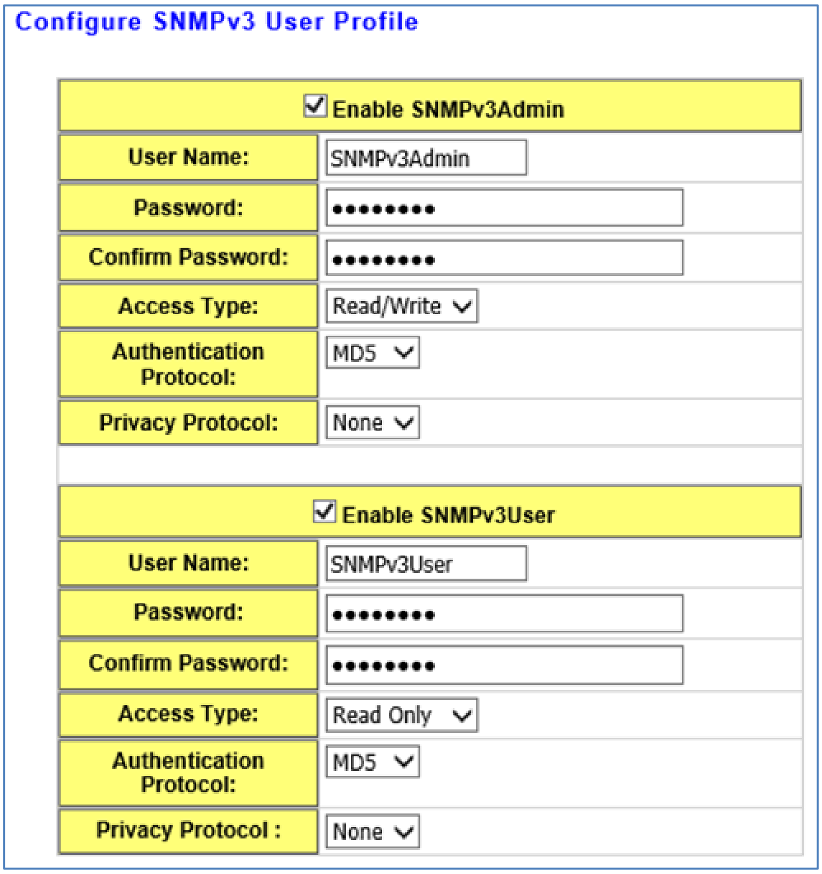
Get Community: Specify the password for the incoming Get and GetNext requests from the management station. By default, it is set to public and allows all requests.

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

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

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

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



Configure SNMPv3 User Profile

☑ Enable SNMPv3Admin	
User Name:	SNMPv3Admin
Password:	••••••••
Confirm Password:	••••••••
Access Type:	Read/Write
Authentication Protocol:	MD5
Privacy Protocol:	None
☑ Enable SNMPv3User	
User Name:	SNMPv3User
Password:	••••••••
Confirm Password:	••••••••
Access Type:	Read Only
Authentication Protocol:	MD5
Privacy Protocol :	None

User Name

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

Password

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

Confirm Password

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

Access Type

Select “**Read Only**” or “**Read and Write**” accordingly.

Authentication Protocol

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

Privacy Protocol

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

None: No encryption is applied.

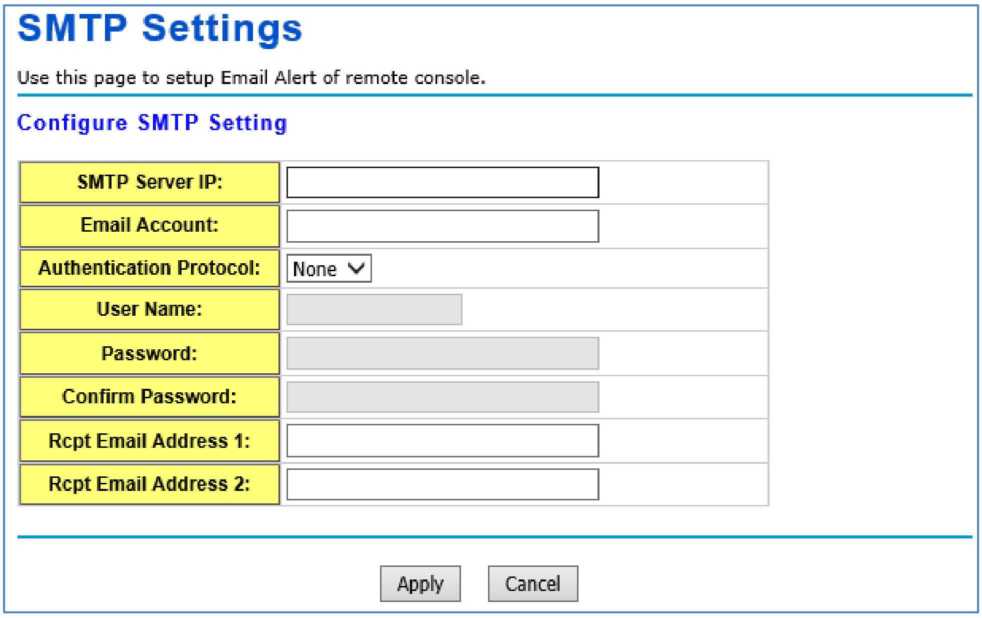
DES: Data Encryption Standard, it applies a 58-bit key to each 64-bit block of data.

Note:

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

4.6.2 SMTP Configuration

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



SMTP Settings

Use this page to setup Email Alert of remote console.

Configure SMTP Setting

SMTP Server IP:	
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.

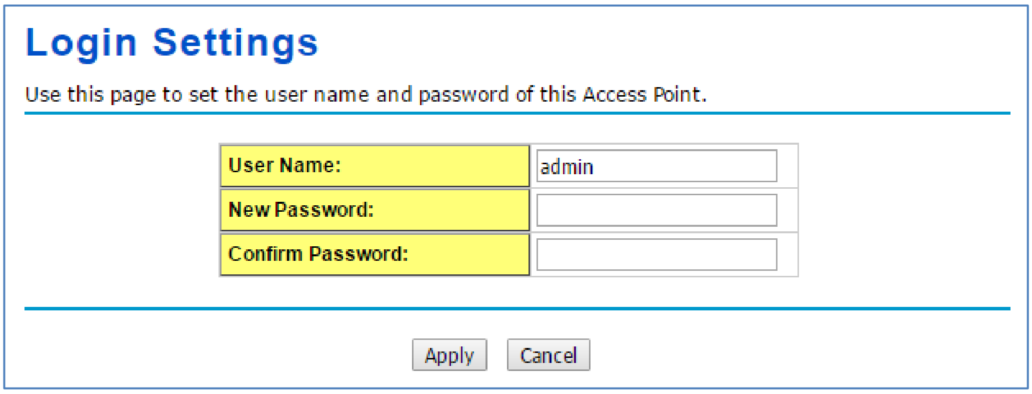
Rcpt Email Address 1: The first Receiver's email address.

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

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

4.6.3 Login Settings

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



Login Settings

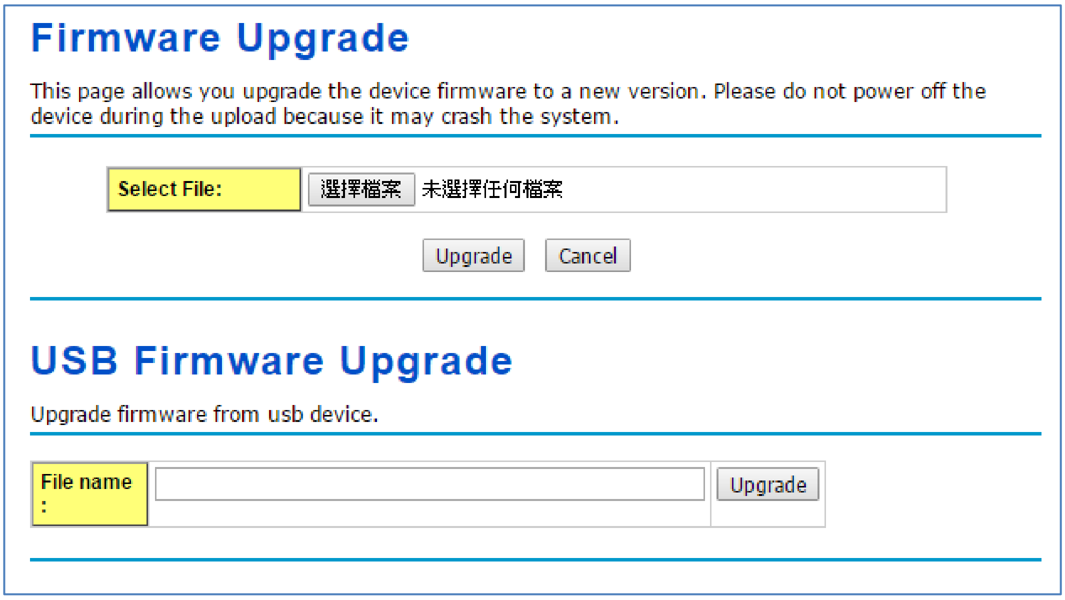
Use this page to set the user name and password of this Access Point.

User Name:	admin
New Password:	
Confirm Password:	

4.6.4 Firmware Upgrade

In this section, you can update the latest firmware for your AP. 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 to the customer site.

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



Firmware Upgrade

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

Select File: 選擇檔案 未選擇任何檔案

USB Firmware Upgrade

Upgrade firmware from usb device.

File name :

Firmware Upgrade:

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

USB Firmware Upgrade:

Plug the USB storage device into USB port (Must with firmware file stored). Type the same firmware file name at **File name** field, and then press "**Upgrade**" to upload the firmware file to the AP. After finish transmitting the firmware, the system will copy the firmware file and replace the firmware in the flash.

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

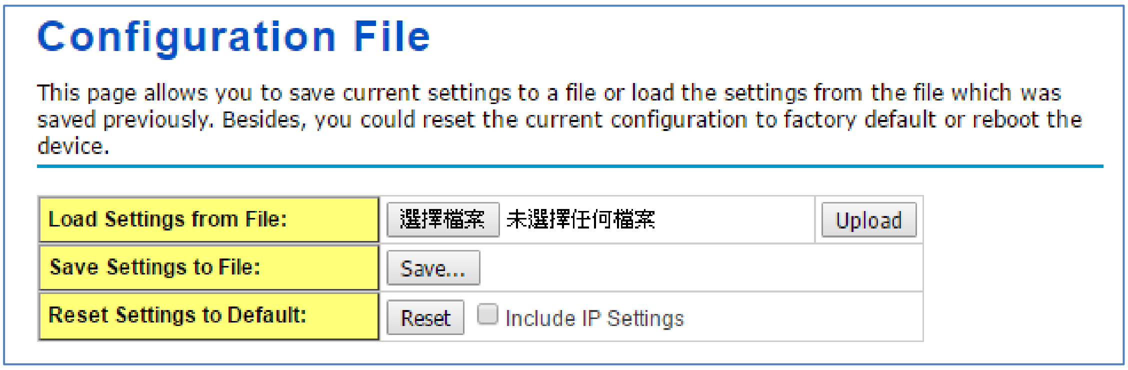
4.6.5 Configuration File

JetWave 4020/4020E provides configuration file **Backup (Save Settings to File), Restore (Load Settings from File)** and **Reset Settings to Default** features.

With Backup command, you can save current configuration file saved in the AP's flash to admin PC. This allowed you to go to restore command later to restore the configuration file back to the AP. 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 can download this file back to the flash.

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

Configuration File:



Configuration File

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

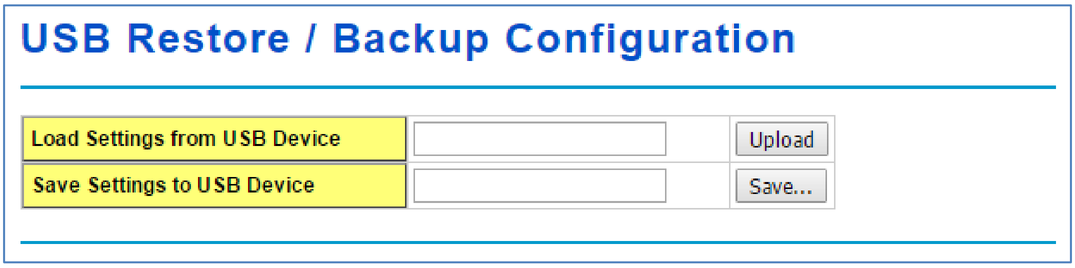
Load Settings from File:	選擇檔案 未選擇任何檔案	Upload
Save Settings to File:	Save...	
Reset Settings to Default:	Reset ☐ Include IP Settings	

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

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

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

USB Restore / Backup Configuration:



USB Restore / Backup Configuration

Load Settings from USB Device		
Save Settings to USB Device		

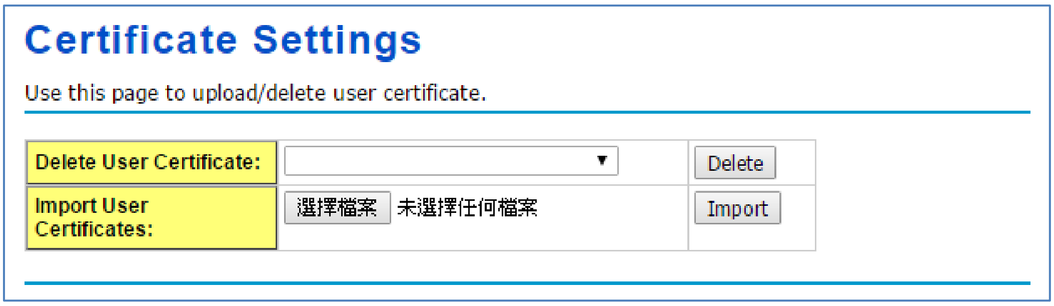
Need to plug a USB storage device into USB port. Please stored JetWave 4020/4020E configuration file into USB storage device if you need to implement USB restore function.

Restore (Load Settings from USB Device): Type the configuration file name and press "Upload" to load the settings.

Backup (Save Settings to USB device): Type the specific configuration file name and press "Save" to save the current configuration file to USB storage device.

4.6.6 Certificate File

Use this page to manage the user certificate file. You can import user certificate file, select "**Browse…**" to select the certificate file and press "**Import**". You can generate the file by 3rd party tool, web site or get from the IT administrator. Select the user certificate, and then use the **Delete** to remove it.



Certificate Settings

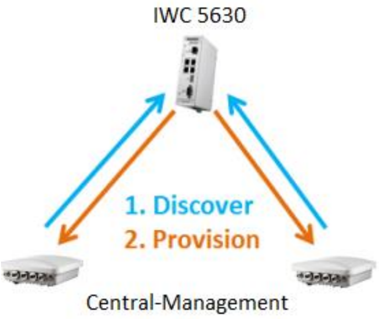
Use this page to upload/delete user certificate.

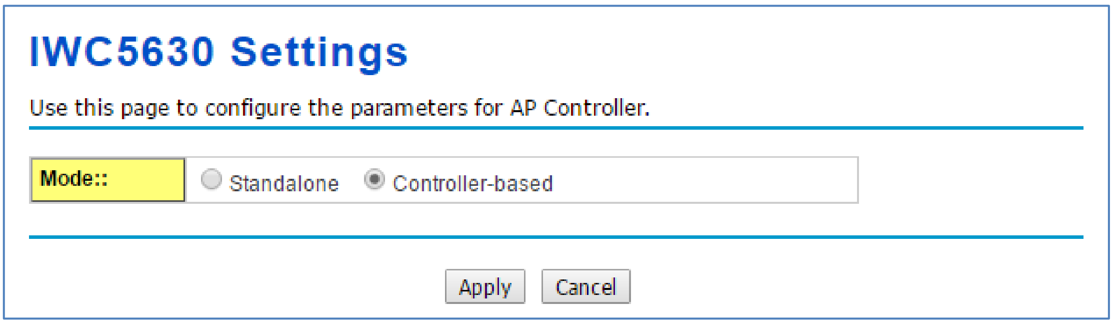
Delete User Certificate:	▼	Delete
Import User Certificates:	選擇檔案 未選擇任何檔案	Import

In **Wireless/Security Settings**, following is the security setting under "**WPA with Radius**" Authentication mode, the Eap type is **"TLS"**. You can see the "User Certificate file" is assigned. The AP must use the same certificate file as your Radius Server under this setting.

4.6.7 WLAN Controller

The JetWave 4020/4020E can be central-managed by Korenix IWC5630 series. The JetWave IWC 5630 is an industrial-grade WLAN controller supports up to 25 APs management. JetWave 4020/4020E series APs auto-discover JetWave IWC 5630 and AP configuration can be set on JetWave IWC 5630 provisioned to APs automatically.





IWC5630 Settings

Use this page to configure the parameters for AP Controller.

Mode::	○ Standalone ● Controller-based

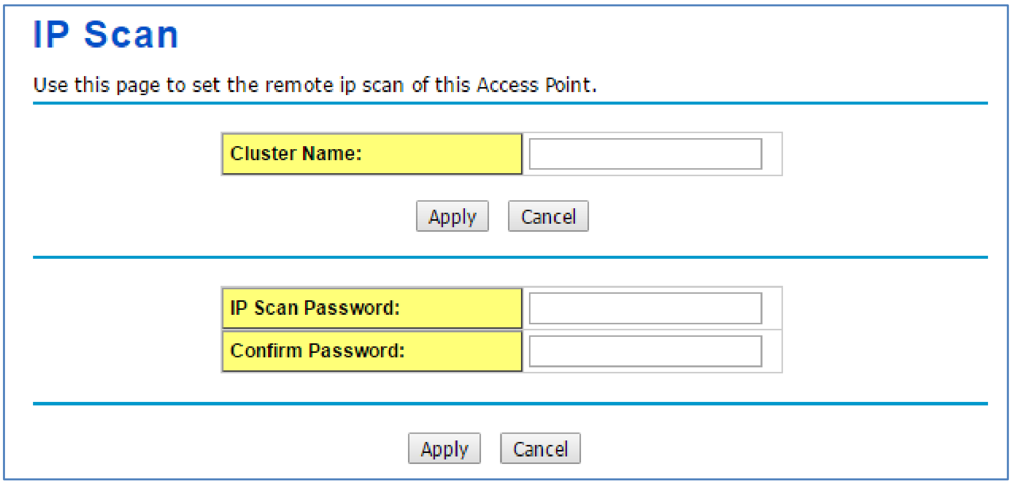
Apply Cancel

Standalone: The AP keep standalone mode, it means IWC 5630 can not configure and manage on JetWave 4020/4020E.

Controller-based: The AP can be configured and managed by IWC 5630.

4.6.8 Remote IP Scan

The page allow user to set remote IP Scan, it include **Cluster Name** and **IP Scan Password.** With **Remote IP Scan,** it provide higher wireless security when use Korenix View management tool. Note: Must use Korenix View V1.6.9 or higher version



IP Scan

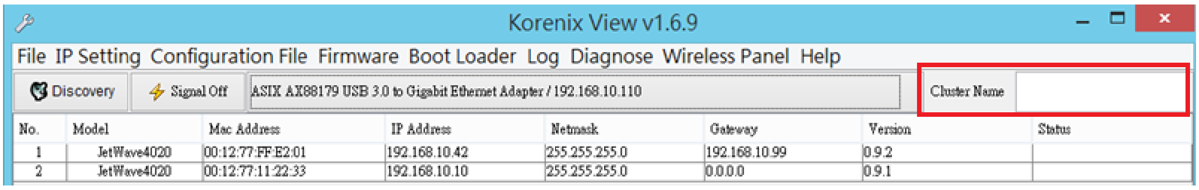
Use this page to set the remote ip scan of this Access Point.

Cluster Name:	

IP Scan Password:	
Confirm Password:	

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

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



Korenix View v1.6.9
File IP Setting Configuration File Firmware Boot Loader Log Diagnose Wireless Panel Help
Discovery
Signal Off
Cluster Name

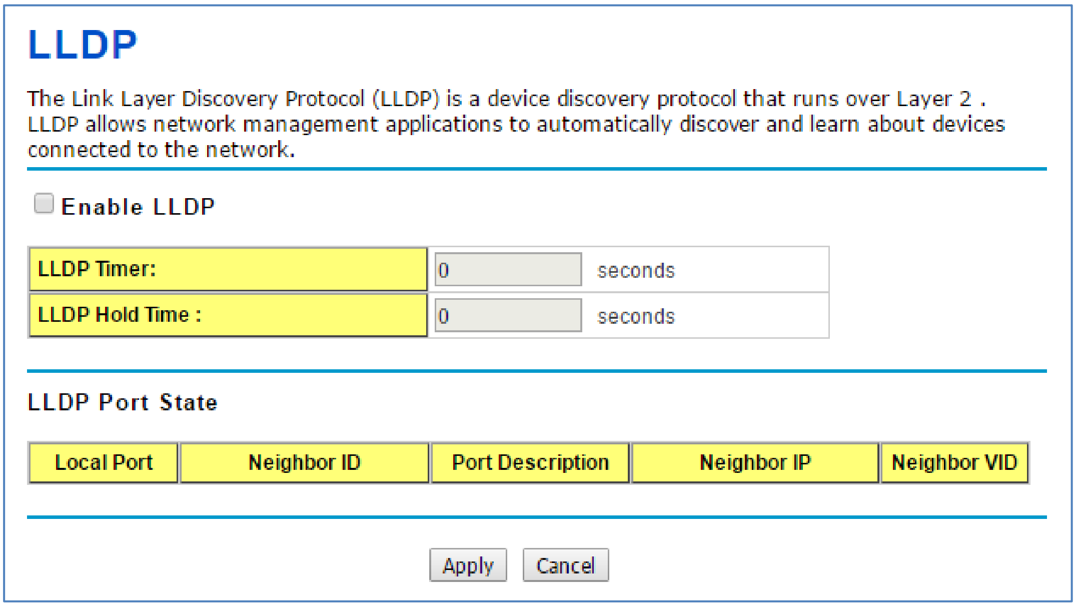
ASIX AX88179 USB 3.0 to Gigabit Ethernet Adapter / 192.168.10.110

No.	Model	Mac Address	IP Address	Netmask	Gateway	Version	Status
1	JetWave4020	00:12:77:FF:E2:01	192.168.10.42	255.255.255.0	192.168.10.99	0.9.2	
2	JetWave4020	00:12:77:11:22:33	192.168.10.10	255.255.255.0	0.0.0.0	0.9.1	

4.6.9 Topology Discovery (LLDP)

This page allow user to set the Topology Discovery (LLDP - IEEE 802.1AB Link Layer Discovery Protocol) function, it can helps user to discovery multi-vendor's network devices on same segment by Korenix NMS which supports LLDP function; With LLDP function, Korenix NMS can easier maintain the topology map, display port ID, port description, system description, VLAN ID. Once the link failure, the topology change events can be updated to the Korenix NMS as well.

The LLDP Port State can display the neighbor ID and IP leant from the connected devices. Once configured the management switch's LLDP setting, it will be auto discover by the Korenix NMS platform. The configuration and settings explain as following.



LLDP

The Link Layer Discovery Protocol (LLDP) is a device discovery protocol that runs over Layer 2 . LLDP allows network management applications to automatically discover and learn about devices connected to the network.

☐ Enable LLDP

LLDP Timer:	0	seconds
LLDP Hold Time :	0	seconds

LLDP Port State

Local Port	Neighbor ID	Port Description	Neighbor IP	Neighbor VID

Select **Enable LLDP** to enable or disable LLDP function.

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

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

LLDP Port State

Local port: The current port (eth1 or eth0) of JetWave 4020/4020E that linked with neighbor network device.

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

Port Description: The port number of neighbor device that linked to JetWave 4020/4020E.

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

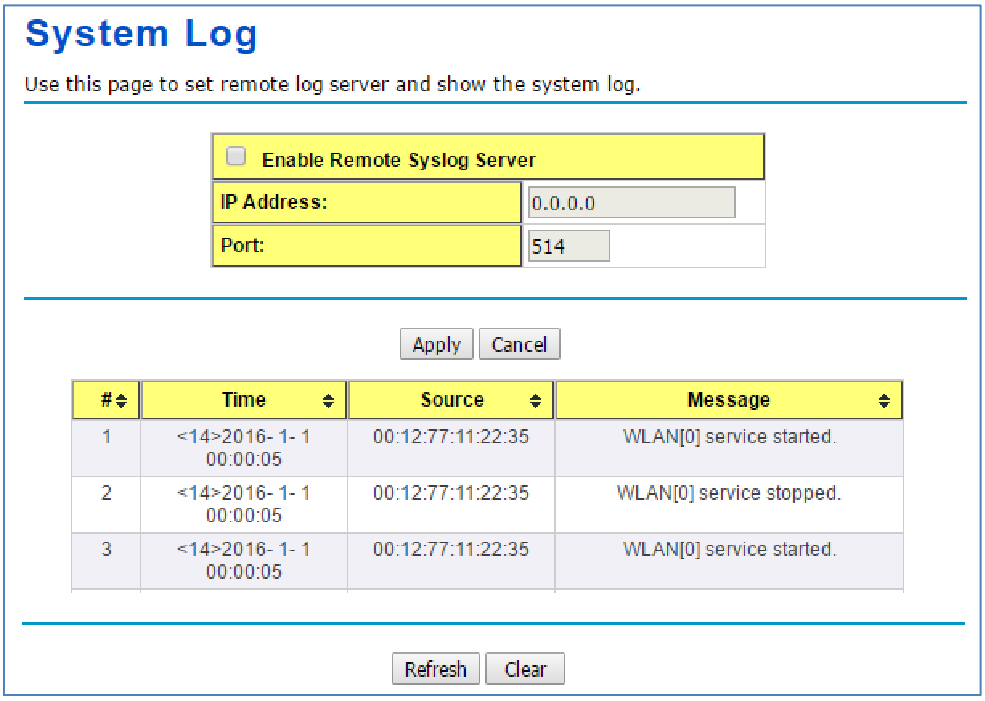
Neighbor VID: The VLAN ID of neighbor device on the same network segment

4.7 Tools

The "**Tools**" feature set pages provides some additional useful tools. It includes System Log, Site Survey, Ping Watchdog, Data Rate Test, Antenna Alignment and Ping.

4.7.1 System Log

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



System Log

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

☐ Enable Remote Syslog Server

IP Address:	0.0.0.0
Port:	514

#	Time	Source	Message
1	<14>2016- 1- 1 00:00:05	00:12:77:11:22:35	WLAN[0] service started.
2	<14>2016- 1- 1 00:00:05	00:12:77:11:22:35	WLAN[0] service stopped.
3	<14>2016- 1- 1 00:00:05	00:12:77:11:22:35	WLAN[0] service started.

Enable Remote Syslog Server: Enable System log or not.

IP Address: Specify the IP address of the server.

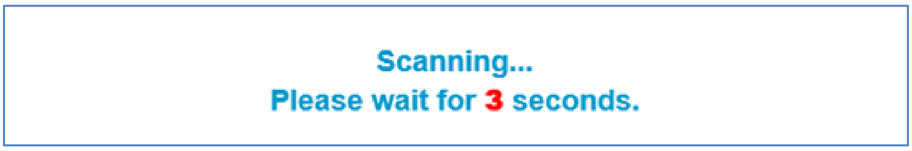
Port: Specify the port number of the server.

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

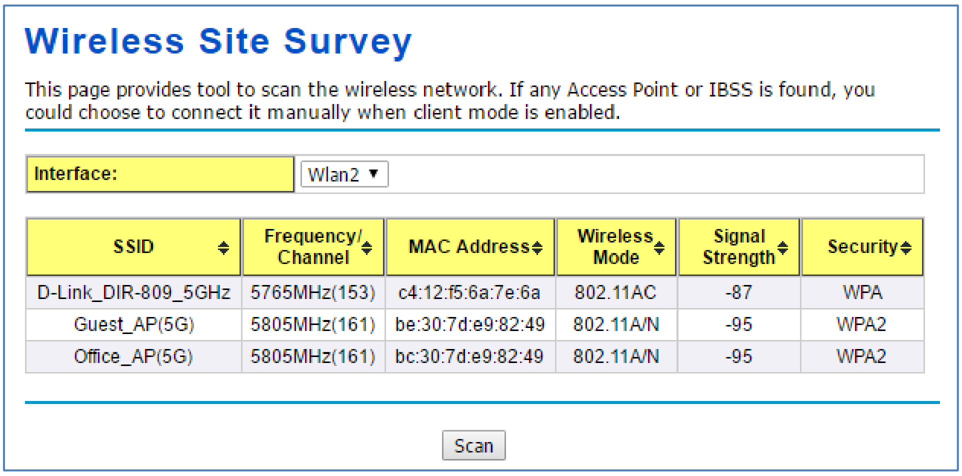
It shows system log information in the bottom half of the page. Press "**Refresh**" to reload the log table or press "**Clear**" to delete log information.

4.7.2 Site Survey

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



Scanning...
Please wait for 3 seconds.



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:	Wlan2 ▼

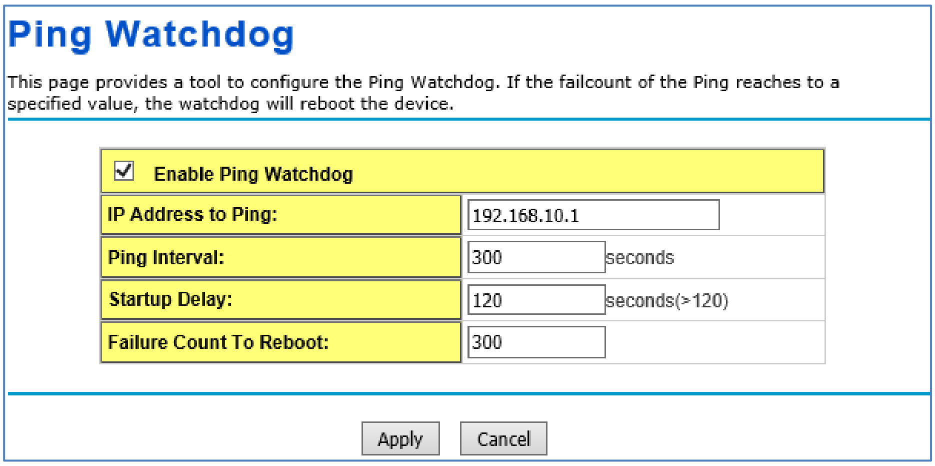
SSID	Frequency/ Channel	MAC Address	Wireless Mode	Signal Strength	Security
D-Link_DIR-809_5GHz	5765MHz(153)	c4:12:f5:6a:7e:6a	802.11AC	-87	WPA
Guest_AP(5G)	5805MHz(161)	be:30:7d:e9:82:49	802.11A/N	-95	WPA2
Office_AP(5G)	5805MHz(161)	bc:30:7d:e9:82:49	802.11A/N	-95	WPA2

Interface: Select the interface number, Wlan1 or Wlan2.

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

4.7.3 Ping Watchdog

This page provides a tool to 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.

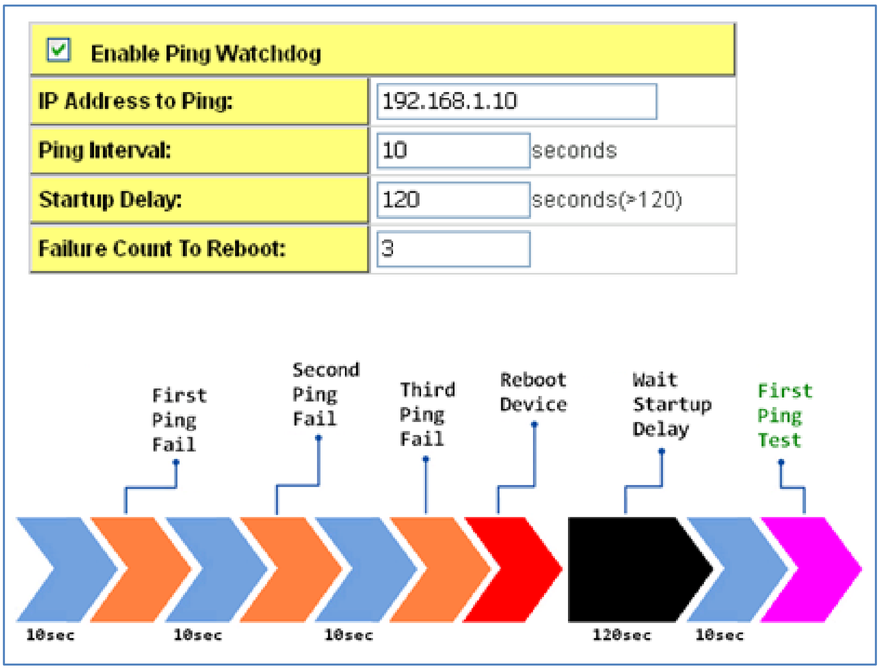
Ping Interval: The interval time between each Ping packet.

Startup Delay: This is the startup delay time of the ping watchdog. After the 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.

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

Below is the ping watchdog example:



☑ Enable Ping Watchdog

IP Address to Ping:	192.168.1.10
Ping Interval:	10 seconds
Startup Delay:	120 seconds(>120)
Failure Count To Reboot:	3

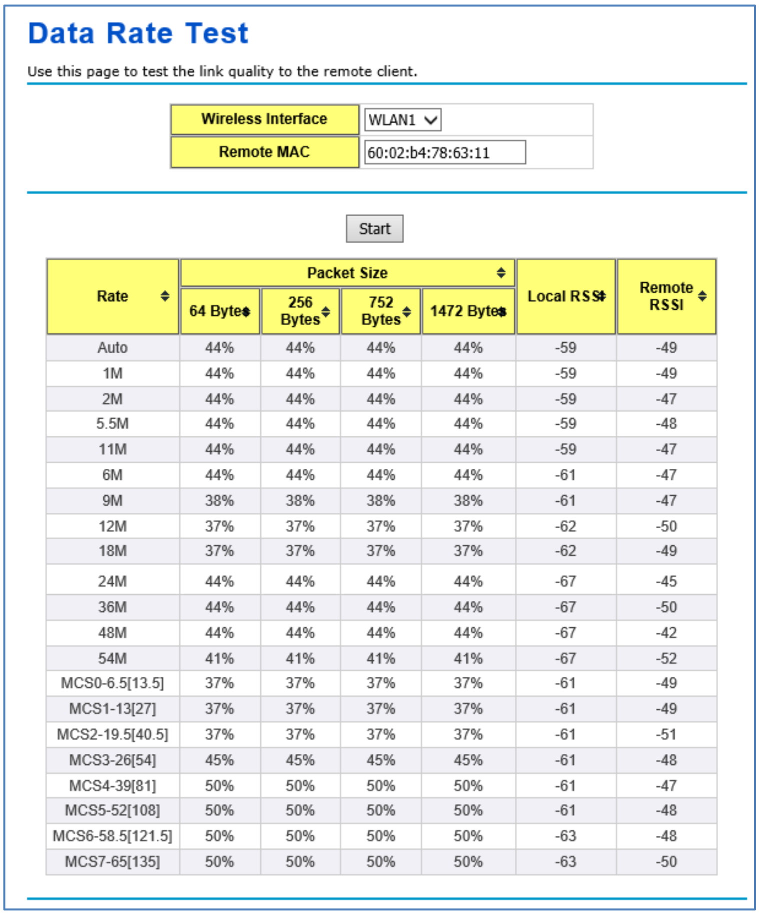
4.7.4 Data Rate Test

This page allows you to do Data Rate test to check the connection performance. This is a reference data for field test. The system will generate packet from one end to the other end.

Wireless Interface: Select the WLAN 1 or WLAN 2. The system will generate the data rate test packet from the interface you select.

Remote MAC: The MAC Address of the target AP you want to check. You must confirm your AP already connects to the remote AP first. You can find remote AP’s MAC address from the Site Survey or write the MAC Address print in the target AP’s label. The MAC Address format is “60:02:b4:78:63:11”.

Press “**Start”** to start the test. This may take couple seconds. Please wait and you will see the below test result. Note: Stop the test after finished the test, it can save the system resource.



Data Rate Test

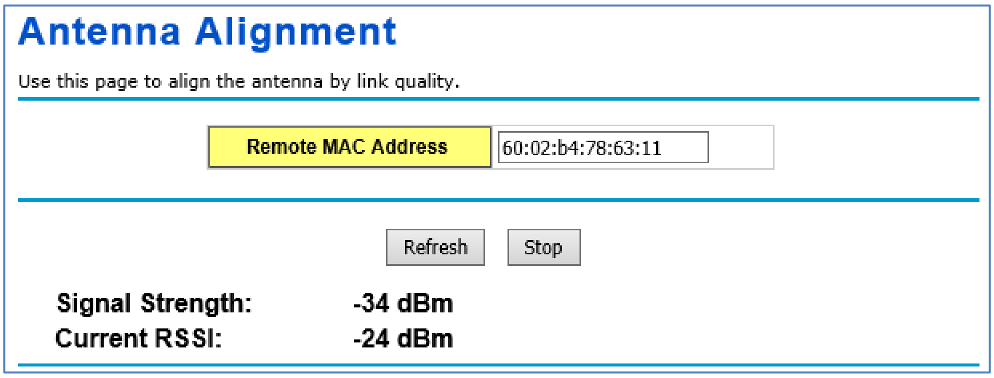
Use this page to test the link quality to the remote client.

Wireless Interface	WLAN1
Remote MAC	60:02:b4:78:63:11

Rate	Packet Size				Local RSSI	Remote RSSI
	64 Bytes	256 Bytes	752 Bytes	1472 Bytes		
Auto	44%	44%	44%	44%	-59	-49
1M	44%	44%	44%	44%	-59	-49
2M	44%	44%	44%	44%	-59	-47
5.5M	44%	44%	44%	44%	-59	-48
11M	44%	44%	44%	44%	-59	-47
6M	44%	44%	44%	44%	-61	-47
9M	38%	38%	38%	38%	-61	-47
12M	37%	37%	37%	37%	-62	-50
18M	37%	37%	37%	37%	-62	-49
24M	44%	44%	44%	44%	-67	-45
36M	44%	44%	44%	44%	-67	-50
48M	44%	44%	44%	44%	-67	-42
54M	41%	41%	41%	41%	-67	-52
MCS0-6.5[13.5]	37%	37%	37%	37%	-61	-49
MCS1-13[27]	37%	37%	37%	37%	-61	-49
MCS2-19.5[40.5]	37%	37%	37%	37%	-61	-51
MCS3-26[54]	45%	45%	45%	45%	-61	-48
MCS4-39[81]	50%	50%	50%	50%	-61	-47
MCS5-52[108]	50%	50%	50%	50%	-61	-48
MCS6-58.5[121.5]	50%	50%	50%	50%	-63	-48
MCS7-65[135]	50%	50%	50%	50%	-63	-50

4.7.5 Antenna Alignment

The Antenna Alignment tool is a convenient tool to find the target AP while you install the AP for long distance connection. In long distance transmission, it is not easy to see the remote AP clearly, with this tool, you can adjust the direction of the antenna and find out the best direction according to the result.



Antenna Alignment

Use this page to align the antenna by link quality.

Remote MAC Address	60:02:b4:78:63:11

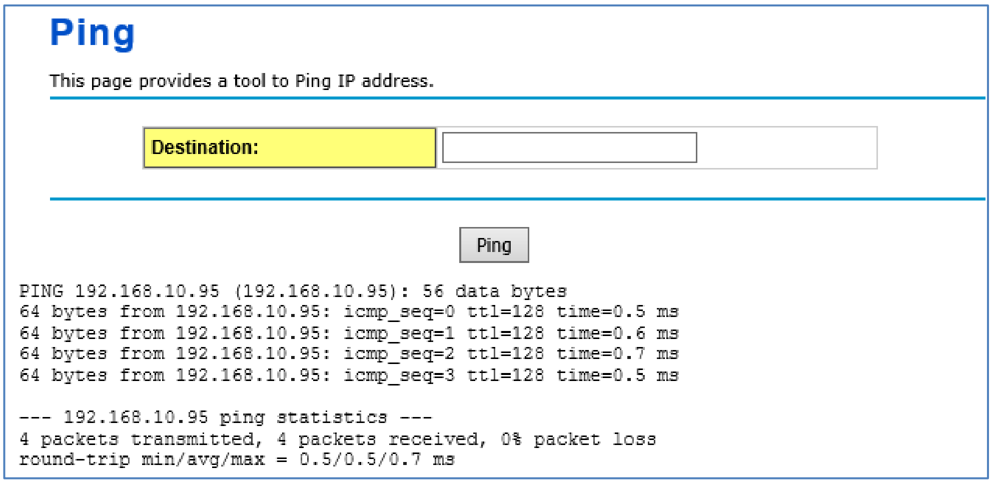
Signal Strength: -34 dBm
Current RSSI: -24 dBm

Type the Remote MAC Address (format: xx:xx:xx:xx:xx:xx) in this page and press “**Start”** to start the antenna alignment. Press “**Stop**” after you find the correct target AP. You can start the tool from one end or both ends of connection to find the target antenna.

In practical, we often install the same specification antennas for both ends of point to point connection and start the antenna alignment tool from both ends. It can easier helps you find the target AP by checking the signal strength changing.

4.7.6 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:

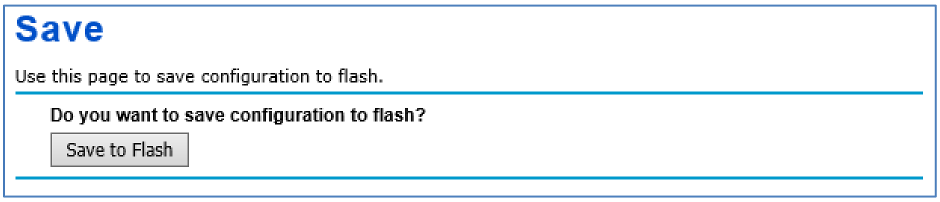
```
PING 192.168.10.95 (192.168.10.95): 56 data bytes
64 bytes from 192.168.10.95: icmp_seq=0 ttl=128 time=0.5 ms
64 bytes from 192.168.10.95: icmp_seq=1 ttl=128 time=0.6 ms
64 bytes from 192.168.10.95: icmp_seq=2 ttl=128 time=0.7 ms
64 bytes from 192.168.10.95: icmp_seq=3 ttl=128 time=0.5 ms

--- 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: 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

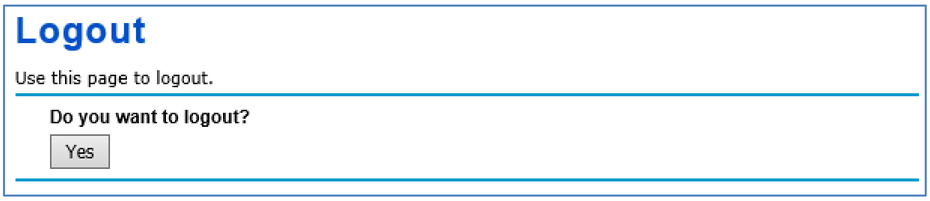
Use this page to save configuration to flash.

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.



Logout

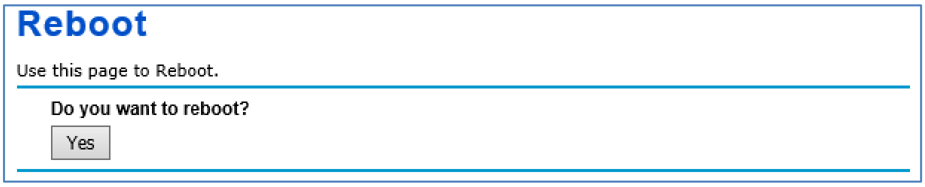
Use this page to logout.

Do you want to logout?

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

4.8.3 Reboot

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

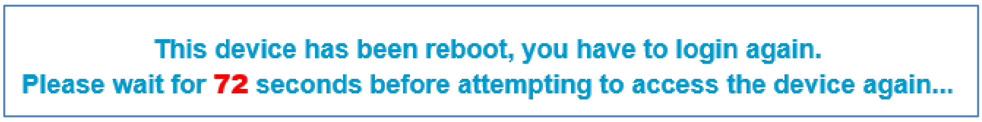


Reboot

Use this page to Reboot.

Do you want to reboot?

The below 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...

Chapter 5

Configuration – SNMP, CLI, View Utility

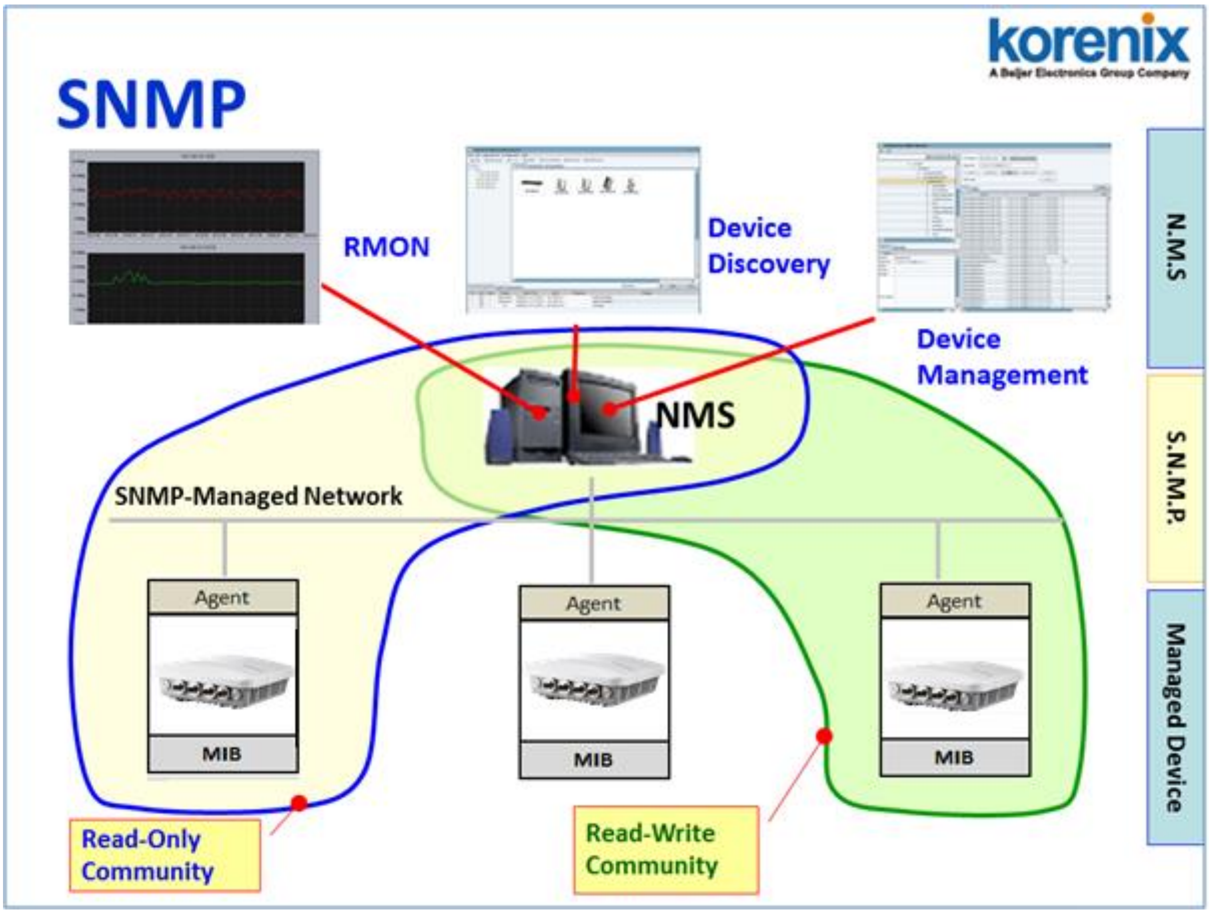
Chapter 5 Configuration – SNMP, CLI, View Utility

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. 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 **4.6.1 Remote Setting.**

5.1.2 Management Information Base (MIB):

Before you want to manage the JetWave 4020/4020E series AP through SNMP, please go to download the MIB files from Korenix web site and compile all of them to the NMS. The AP 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-ACL-MIB.my: This is the JetWave ACL object MIB.

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

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

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

e. JETWAVE-STATISTICS-MIB.my: This is the JetWave Serial Port object MIB.

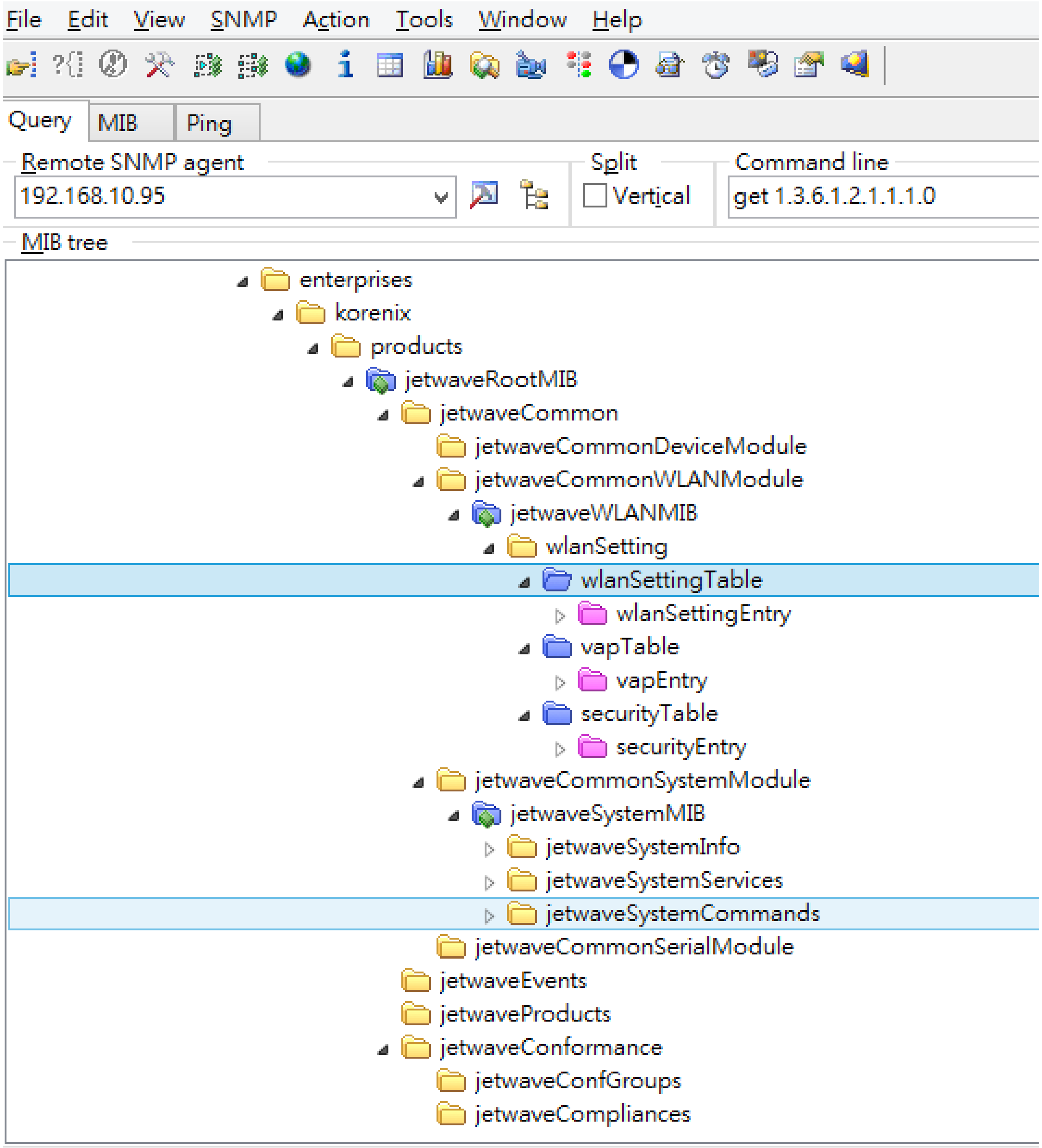
f. JETWAVE-SYSTEM-MIB.my: This is the JetWave System objects MIB.

g. JETWAVE-WLAN-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.



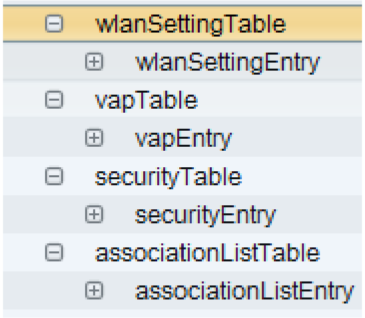
Remote SNMP agent: 192.168.10.95

□ Vertical

Command line: get 1.3.6.1.2.1.1.1.0

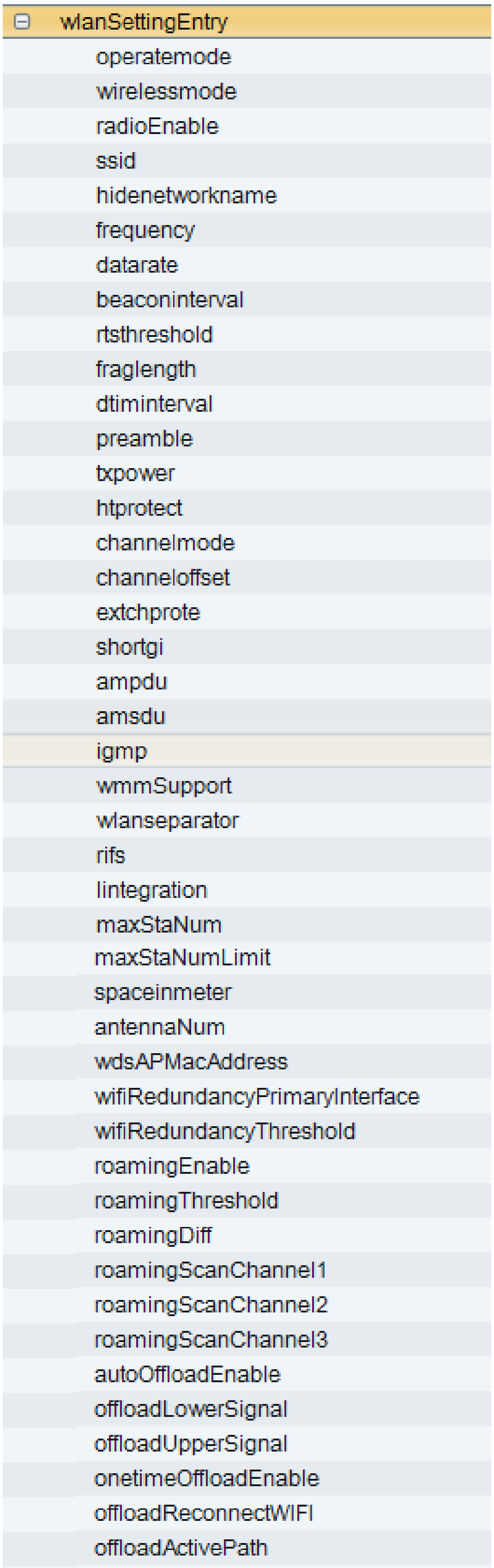
```
◢ enterprises
   ◢ korenix
      ◢ products
         ◢ jetwaveRootMIB
            ◢ jetwaveCommon
                  jetwaveCommonDeviceModule
               ◢ jetwaveCommonWLANModule
                  ◢ jetwaveWLANMIB
                     ◢ wlanSetting
                        ◢ wlanSettingTable
                           ▷ wlanSettingEntry
                        ◢ vapTable
                           ▷ vapEntry
                        ◢ securityTable
                           ▷ securityEntry
               ◢ jetwaveCommonSystemModule
                  ◢ jetwaveSystemMIB
                     ▷ jetwaveSystemInfo
                     ▷ jetwaveSystemServices
                     ▷ jetwaveSystemCommands
                  jetwaveCommonSerialModule
               jetwaveEvents
               jetwaveProducts
            ◢ jetwaveConformance
                  jetwaveConfGroups
                  jetwaveCompliances
```

Example: wlanSetting



- ⊟ wlanSettingTable
  - ⊞ wlanSettingEntry
- ⊟ vapTable
  - ⊞ vapEntry
- ⊟ securityTable
  - ⊞ securityEntry
- ⊟ associationListTable
  - ⊞ associationListEntry

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
  - wifiRedundancyPrimaryInterface
  - wifiRedundancyThreshold
  - roamingEnable
  - roamingThreshold
  - roamingDiff
  - roamingScanChannel1
  - roamingScanChannel2
  - roamingScanChannel3
  - autoOffloadEnable
  - offloadLowerSignal
  - offloadUpperSignal
  - onetimeOffloadEnable
  - offloadReconnectWIFI
  - offloadActivePath

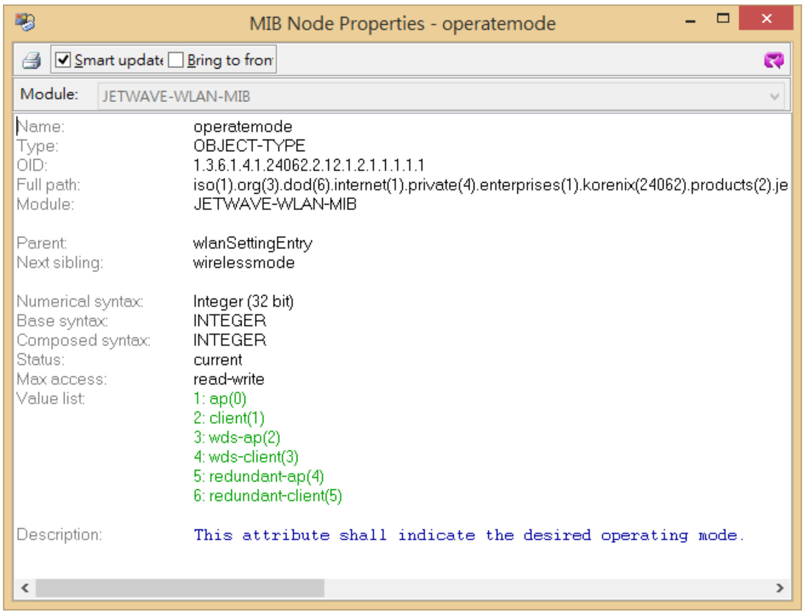
Example of Object in wlanSettingEntry

Operatemode: (Operation Mode)

The OID: .1.3.6.1.4.1.24062.2.12.1.2.1.1.1.1.1.

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.



MIB Node Properties - operatemode

☑ Smart updat ☐ Bring to fron

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.

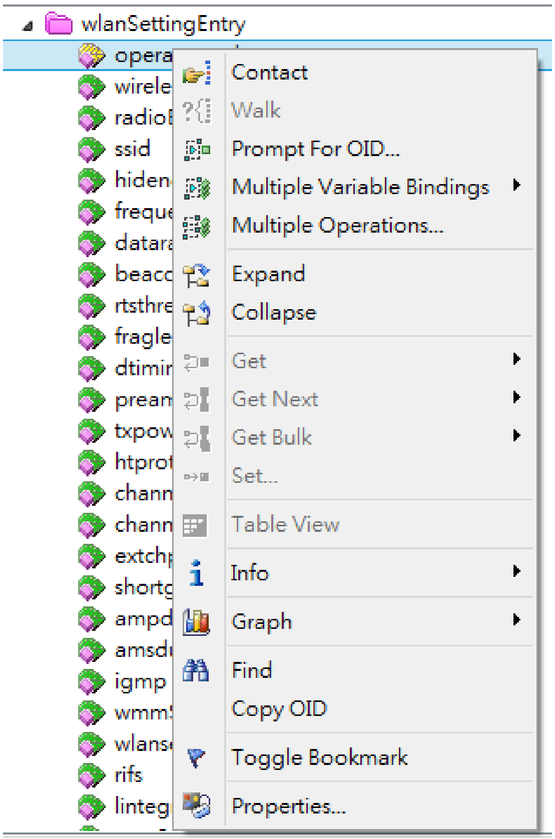
Get: Read the value of the selected OID.

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.

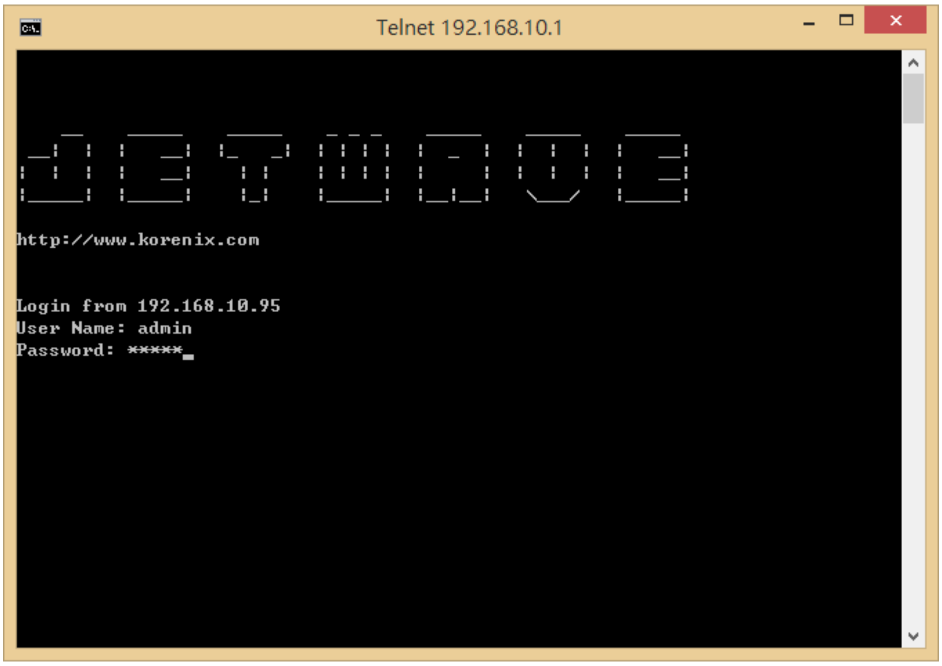
Property: See the MIB Node information.



5.2 Command Line Interface (CLI)

The AP provides the Command Line Interface (CLI), you can access it through the Telnet or Console. The Command Line Interface (CLI) is the user interface to the AP'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. 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.

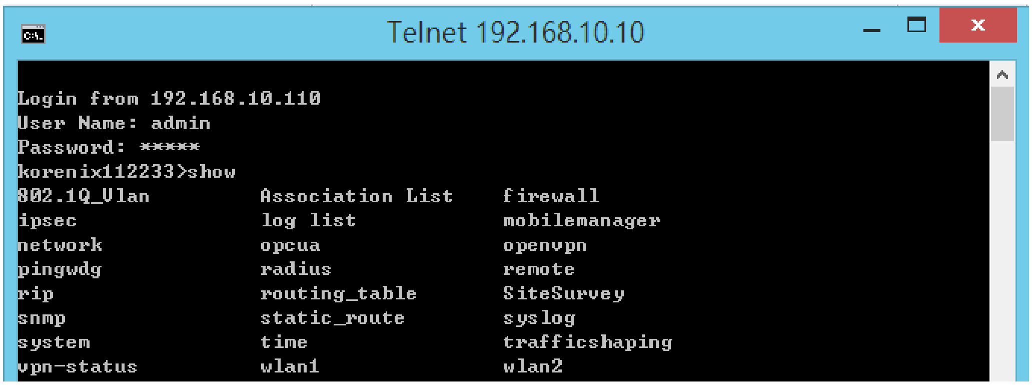
Del: This is Delete command to delete the applied settings.

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.

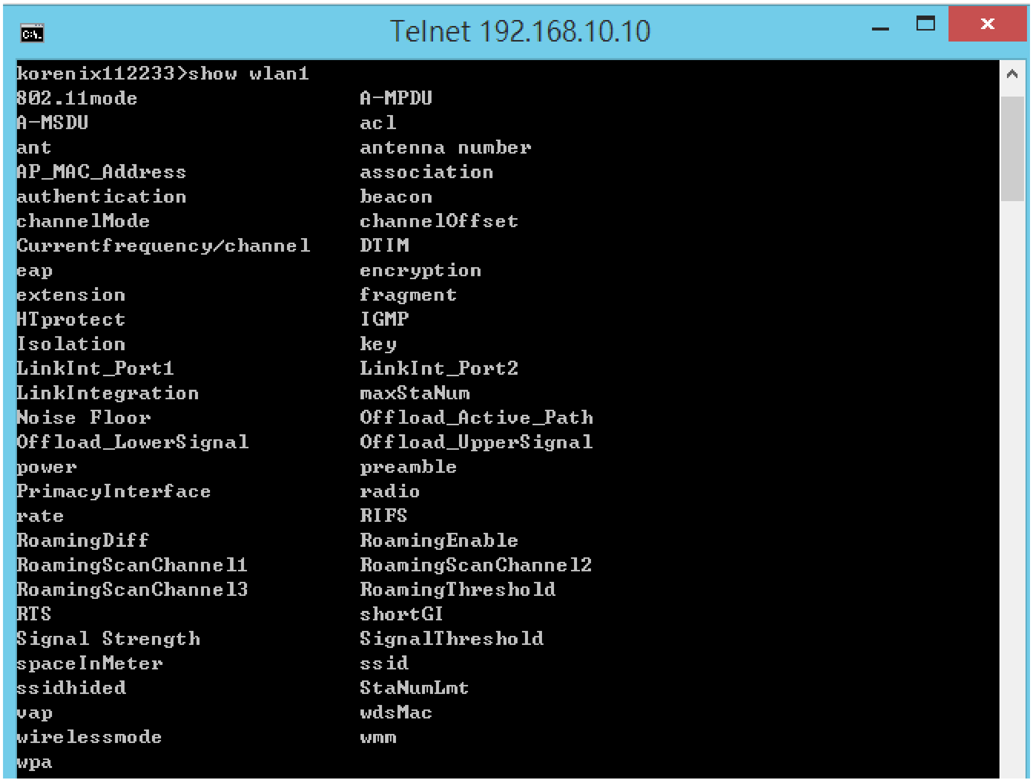
5.2.1 SHOW Command Set:

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



```
Login from 192.168.10.110
User Name: admin
Password: *****
korenix112233>show
802.1Q_Vlan         Association List    firewall
ipsec               log list            mobilemanager
network             opcua               openvpn
pingwdg             radius              remote
rip                 routing_table       SiteSurvey
snmp                static_route        syslog
system              time                trafficshaping
vpn-status          wlan1               wlan2
```

Type **show wlan1+ "Tab↹"** **or** **show wlan2+ "Tab↹"** to see all the wlan command lines.



```
korenix112233>show wlan1
802.11mode                  A-MPDU
A-MSDU                      acl
ant                         antenna number
AP_MAC_Address              association
authentication              beacon
channelMode                 channelOffset
Currentfrequency/channel    DTIM
eap                         encryption
extension                   fragment
HTprotect                   IGMP
Isolation                   key
LinkInt_Port1               LinkInt_Port2
LinkIntegration             maxStaNum
Noise Floor                 Offload_Active_Path
Offload_LowerSignal         Offload_UpperSignal
power                       preamble
PrimacyInterface            radio
rate                        RIFS
RoamingDiff                 RoamingEnable
RoamingScanChannel1         RoamingScanChannel2
RoamingScanChannel3         RoamingThreshold
RTS                         shortGI
Signal Strength             SignalThreshold
spaceInMeter                ssid
ssidhided                   StaNumLmt
vap                         wdsMac
wirelessmode                wmm
wpa
```

Type **show wlan1 + "Enter"** **or** **show wlan2 + "Enter"** to see all the wlan information. The console print all the information for reference.

Type show **wlan1 ra + "Tab"** to complete the commands, and then you can see the result.

korenixffffff>show wlan1 ra (+Tab)

radio rate

korenixffffff>show wlan1 rad (+Tab)

radio rate

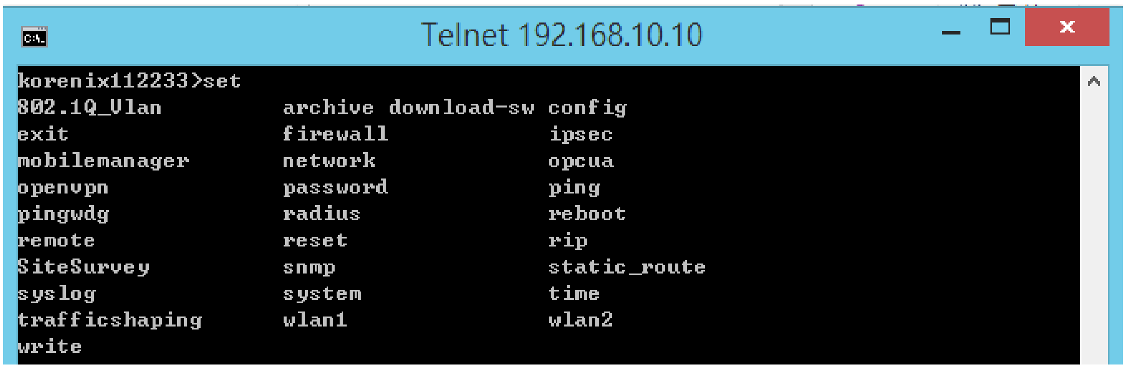
korenixffffff>show wlan1 radio (+ Enter)

wlan1 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.

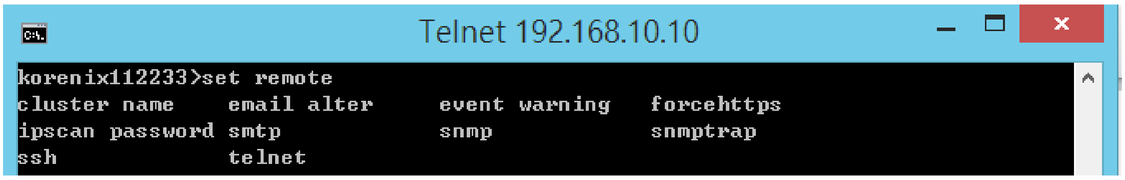


```
korenix112233>set
802.1Q_Vlan         archive download-sw config
exit                firewall            ipsec
mobilemanager       network             opcua
openvpn             password            ping
pingwdg             radius              reboot
remote              reset               rip
SiteSurvey          snmp                static_route
syslog              system              time
trafficshaping      wlan1               wlan2
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 supported. And the CLI is a different way for you to complete the setting.

Example: Set the remote configuration (Refer to the 4.6.1 – Remote Setting)

Type **set remote + “Tab↹”** to see all the remote settings.



```
korenix112233>set remote
cluster name    email alter     event warning   forcehttps
ipscan password 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=========

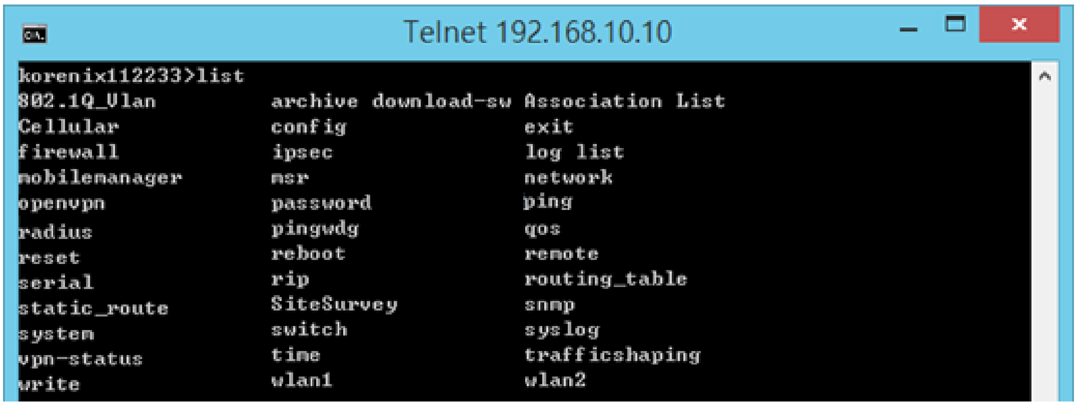
The SNMP command lines and how to set SNMP version, community name, trap server.

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
```

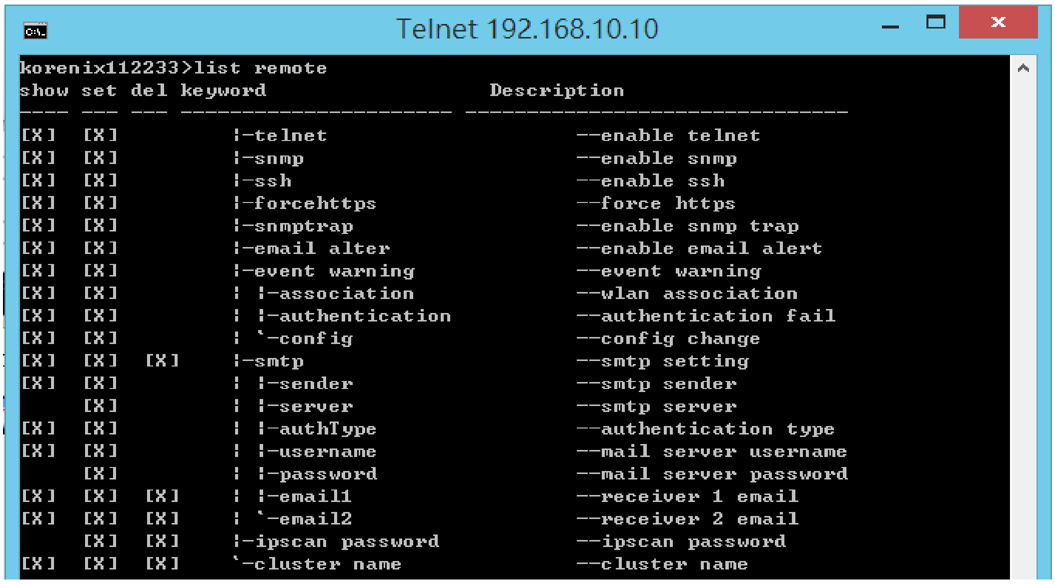
5.2.3 List Command Set:

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



```
korenix112233>list
802.1Q_Vlan         archive download-sw Association List
Cellular            config              exit
firewall            ipsec               log list
mobilemanager       msr                 network
openvpn             password            ping
radius              pingwdg             qos
reset               reboot              remote
serial              rip                 routing_table
static_route        SiteSurvey          snmp
system              switch              syslog
vpn-status          time                trafficshaping
write               wlan1               wlan2
```

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



```
korenix112233>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
     [X]  [X]     |-ipscan password          --ipscan password
[X]  [X]  [X]     `-cluster name             --cluster name
```

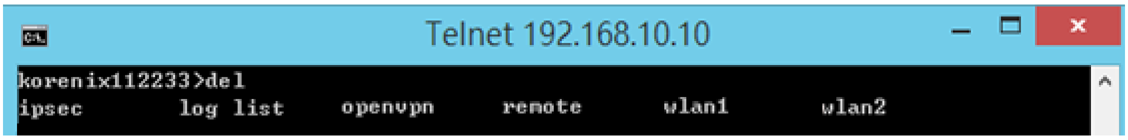
show, set and del: Which privilege the command has? [X] means Yes.

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.



```
korenix112233>del
ipsec          log list      openvpn       remote        wlan1         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 4020/4020E 1st Radio)

korenixffffff>del wlan1

acl eap key wpa

The below wlan 2 settings can be delete through CLI. (JetWave 4020/4020E 2nd Radio)

korenixffffff>del wlan2

acl eap key wpa

5.3 Korenix View Utility

The Korenix View Utility (Rename from the JetView) provides you convenient tool to scan the network and configure the AP. Please connect your PC to JetWave 4020/4020E Ethernet port and start below steps to scan and configure.

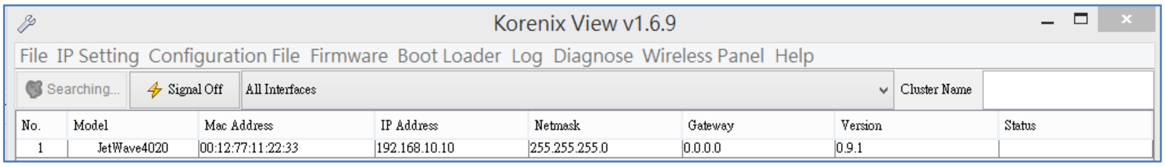
5.3.1 Device Discovery:

Step 1: Open the Korenix View Utility. (Must later than V1.7)

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

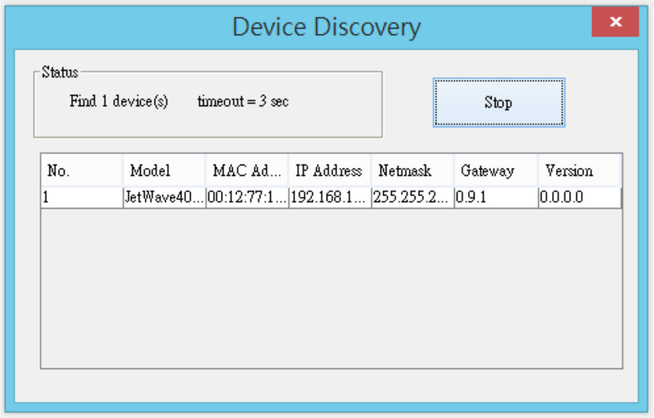
Step 3: Click **"Discovery"**, and then the Nodes and its IP address can be found and listed in Node list.

➢ Figure: The main screen of the Korenix View Utility



No.	Model	Mac Address	IP Address	Netmask	Gateway	Version	Status
1	JetWave4020	00:12:77:11:22:33	192.168.10.10	255.255.255.0	0.0.0.0	0.9.1	

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

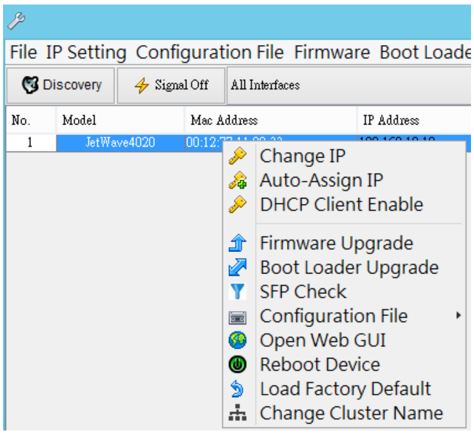


Find 1 device(s) timeout = 3 sec

No.	Model	MAC Ad...	IP Address	Netmask	Gateway	Version
1	JetWave40...	00:12:77:1...	192.168.1...	255.255.2...	0.9.1	0.0.0.0

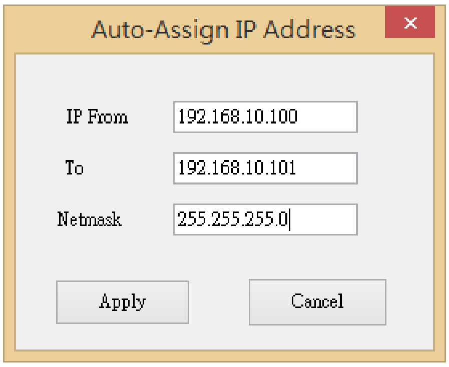
5.3.2 Basic Tools Shortcut:

After you scan the network, select the AP 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

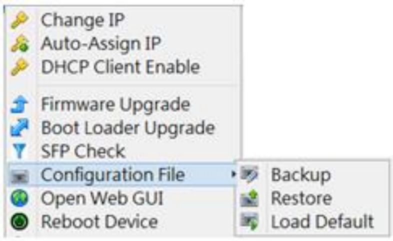
To 192.168.10.101

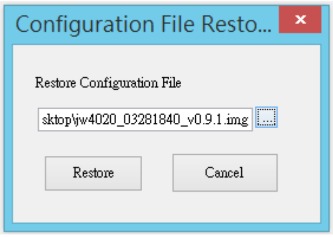
Netmask 255.255.255.0

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.

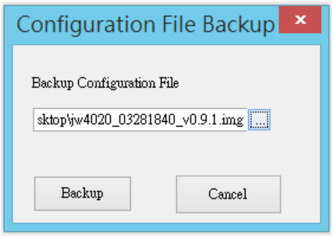
e. You can Backup/Restore the configuration file by “**Configuration File -> Backup/Restore”**. A popup screen will ask you select target configuration/target folder you’d like to backup or restore.





Restore Configuration File

sktop\jw4020_03281840_v0.9.1.img

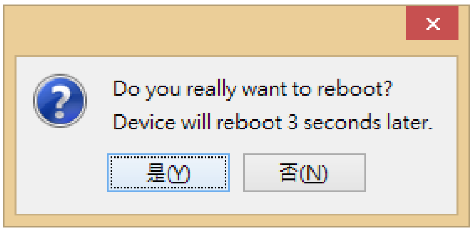


Backup Configuration File

sktop\jw4020_03281840_v0.9.1.img

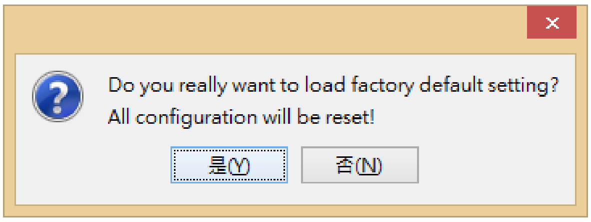
f. Click “**Open Web GUI**” to access the web management interface.

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.

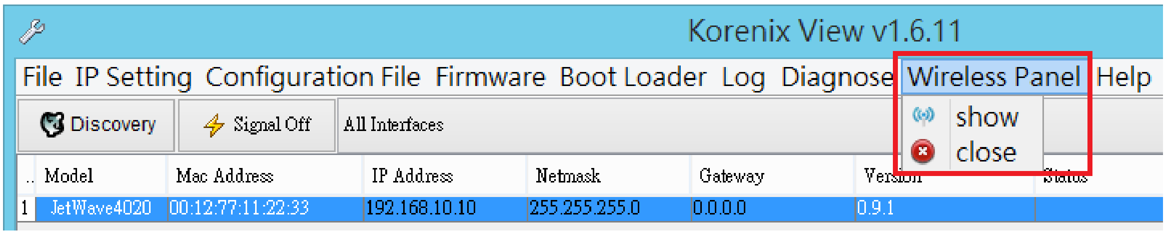


Do you really want to load factory default setting?
All configuration will be reset!

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

5.3.3 Wireless Panel

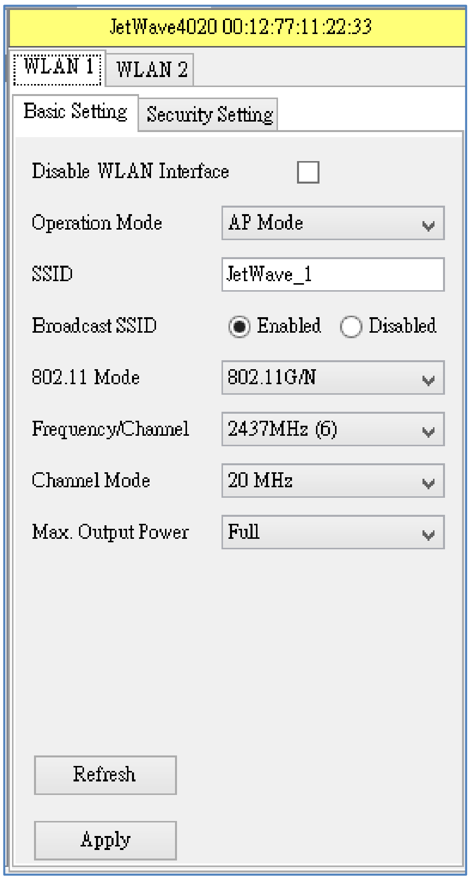
Korenix View Utility provides Wireless panel to configure some **Basic Setting** and **Security setting** for Wireless LAN Interfaces. You can use the tool to configure settings for single device or a group of devices. Select the target device/devices for further configuration.



..	Model	Mac Address	IP Address	Netmask	Gateway	Version	Status
1	JetWave4020	00:12:77:11:22:33	192.168.10.10	255.255.255.0	0.0.0.0	0.9.1	

Basic Setting

Security Setting



JetWave4020 00:12:77:11:22:33

Disable WLAN Interface □

Operation Mode: AP Mode

SSID: JetWave_1

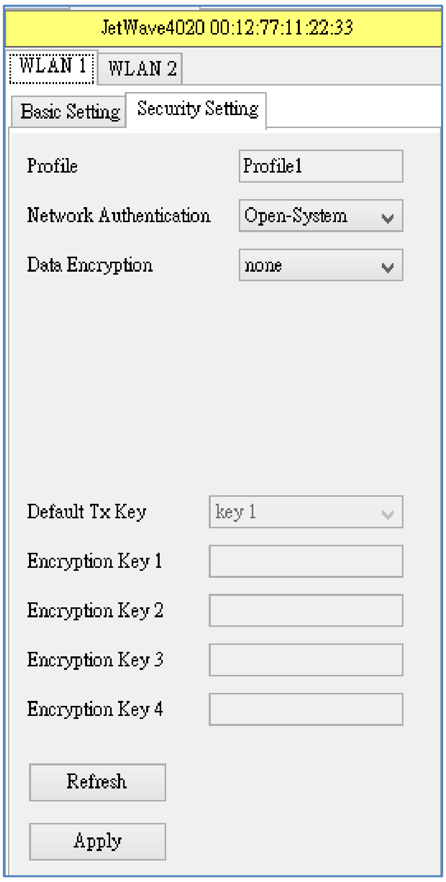
Broadcast SSID: ● Enabled ○ Disabled

802.11 Mode: 802.11G/N

Frequency/Channel: 2437MHz (6)

Channel Mode: 20 MHz

Max. Output Power: Full



JetWave4020 00:12:77:11:22:33

Profile: Profile1

Network Authentication: Open-System

Data Encryption: none

Default Tx Key: key 1

Encryption Key 1:

Encryption Key 2:

Encryption Key 3:

Encryption Key 4:

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.

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.

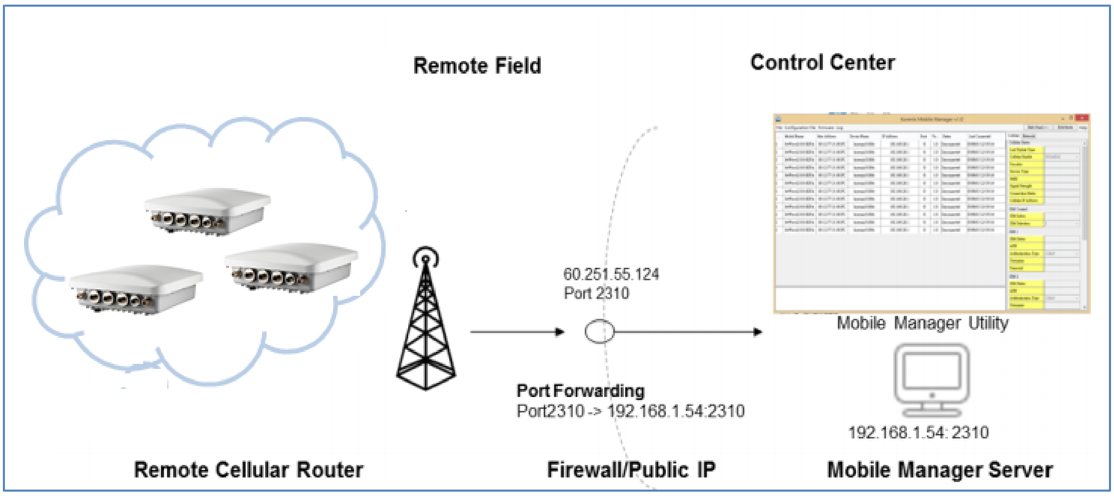
✎ **Note:**

Must click **"Refresh"** to load the current configuration of the selected AP

5.4 Korenix Mobile Manager

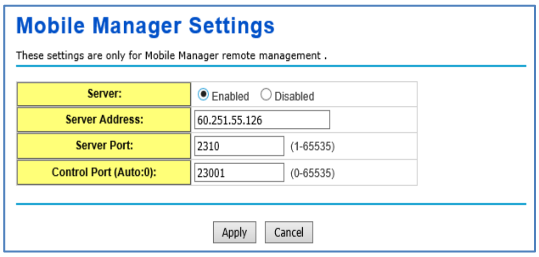
After the mobile devices are applied to the field, the issue of mobile devices' access is an important topic of administrators. Due to the limited number of public address, most carrier provider may offer you the private IP for the cellular router. The carrier provider may have different IP policy, for example, the IP address may be changed every a period of time, may get the different IP address while you reboot the device…etc.

The Korenix Mobile Manager (KMM) is a simple utility to resolve the issue of mobile devices' inabilities to be accessed from the internet. **Please Note that the Korenix Mobile Manager is used when the 3rd Radio of JetWave 4020/4020E applies to Cellular module.** With a PC and a public IP, the PC can be the Mobile Manager Server. Configuring the Mobile Manager Server's IP address on your mobile device, then the up-to-date IP address, cellular type, Ethernet port type…, Network status can be reported to the server. The utility also provides you device management and maintenance features.



(Figure- Remote cellular device management)

Configure Mobile Manager setting at JetWave 4020/4020E Web GUI or Console interface, you can assign the target Server IP Address and specific port (TCP port), then the device will automatically update the current IP address and device information to the server.



Mobile Manager Settings

These settings are only for Mobile Manager remote management .

Server:	● Enabled ○ Disabled	
Server Address:	60.251.55.126	
Server Port:	2310	(1-65535)
Control Port (Auto:0):	23001	(0-65535)

Note: You can download KMM program and user manual at Korenix website

Chapter 6

Troubleshooting

Chapter 6 Troubleshooting

This chapter provides troubleshooting procedures for basic problems with the JetWave 4020/4020E. 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?

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

6.1.3 Why 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

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.
- 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.

6.3 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.

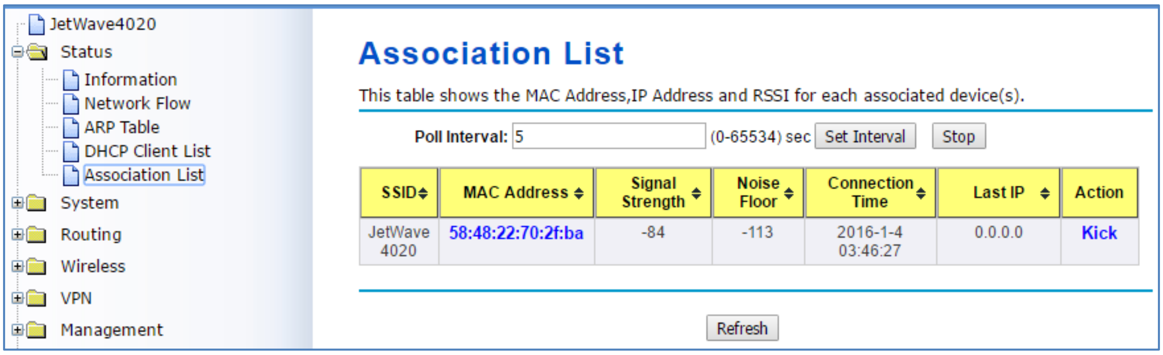
ASCII Table

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 4020/4020E 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 Set Interval Stop

SSID	MAC Address	Signal Strength	Noise Floor	Connection Time	Last IP	Action
JetWave 4020	58:48:22:70:2f:ba	-84	-113	2016-1-4 03:46:27	0.0.0.0	Kick

Refresh

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 4020/4020E 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

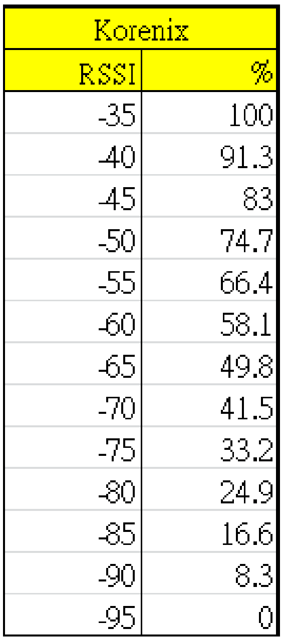
JetWave 4020/4020E series RSSI Conversion:

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.



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

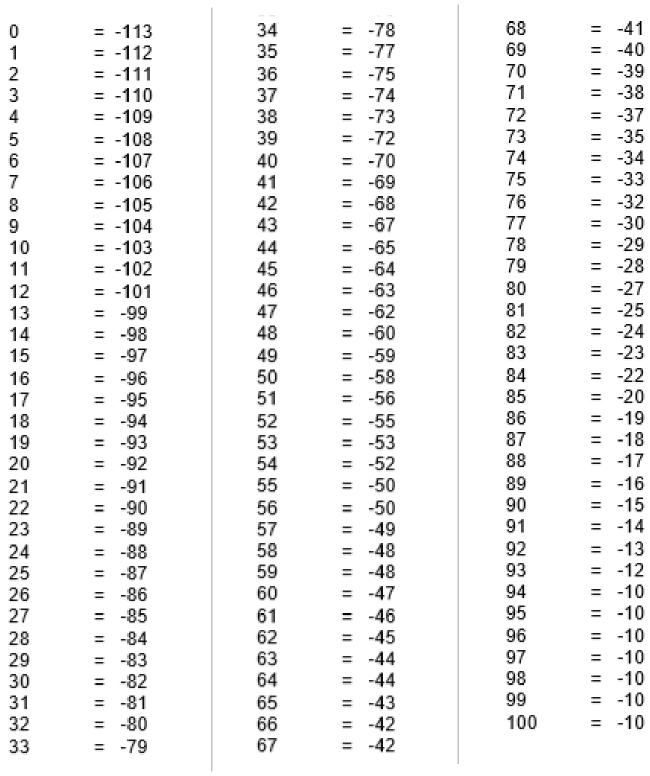
While comparing Korenix product with other competitors, you can follow the way to convert Korenix RSSI to % of the maximum RF Tx Power of other products.

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.

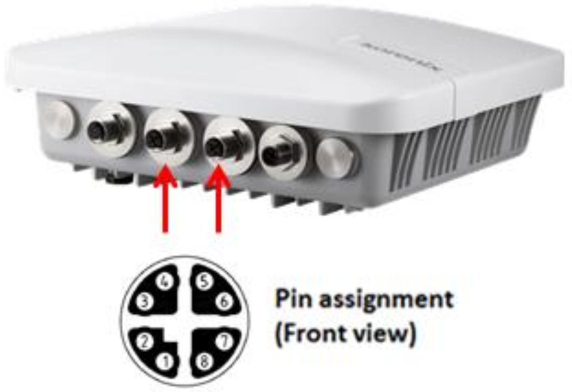


0	=	-113	34	=	-78	68	=	-41
1	=	-112	35	=	-77	69	=	-40
2	=	-111	36	=	-75	70	=	-39
3	=	-110	37	=	-74	71	=	-38
4	=	-109	38	=	-73	72	=	-37
5	=	-108	39	=	-72	73	=	-35
6	=	-107	40	=	-70	74	=	-34
7	=	-106	41	=	-69	75	=	-33
8	=	-105	42	=	-68	76	=	-32
9	=	-104	43	=	-67	77	=	-30
10	=	-103	44	=	-65	78	=	-29
11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

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

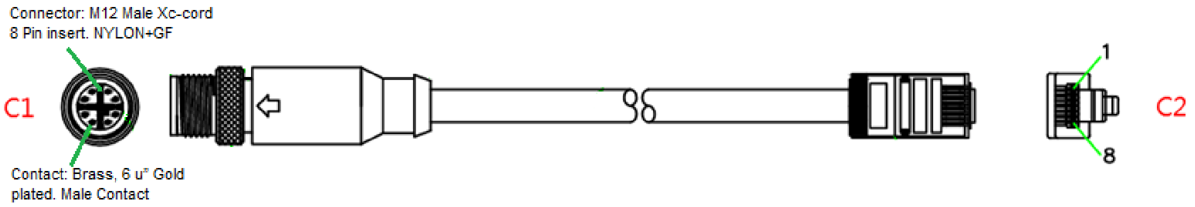
6.3.3 M12 Connector Pin Assignment

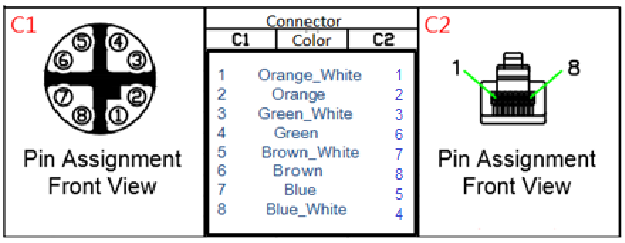
- **X-code Connector** **(Ethernet 1, 2 port)**



M12 X-code 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

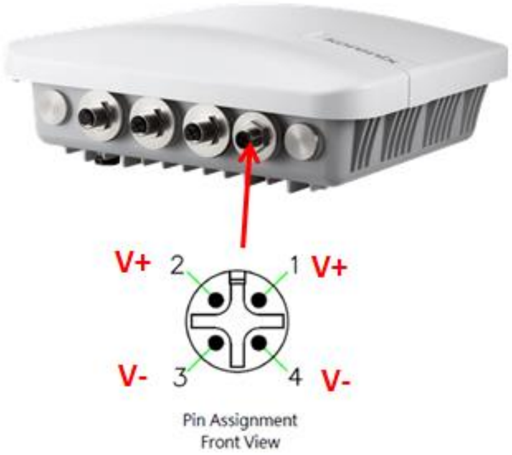
M12 Connector: M12 Male X-code 8 Pin insert. NYLON-GF

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-

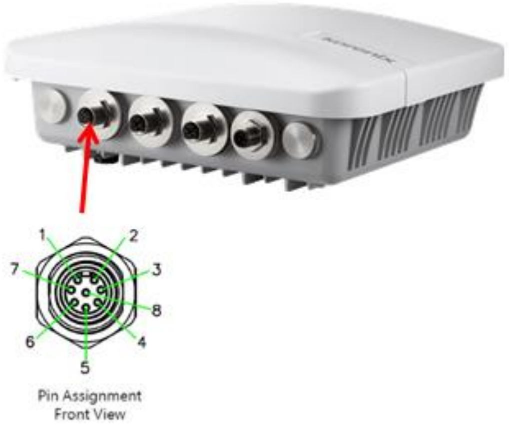
8	Blue_White	4	MDX 2+

- **A-code Connector (2x DC Power input)**



M12	Functionality
1	+
2	+
3	-
4	-

- **A-code Connector (USB + Console)**



M12	Functionality
1	TX
2	RX
3	GND
4	GND
5	USB DP
6	USB DM
7	USB +5V
8	GND

Revision History

Version	Description	Date	Editor
V1.0	1st release for JetWave 4020/4020E Series	May. 2016	Orwell Hsieh Queena Guan
V1.1	1. Revise mounting description and add RAL description 2. Change product photo	Aug. 2016	Queena Guan