JetWave 2111L/2411L Series

Wireless LTE Gateway

User Manual

V1.0 Nov.22. 2019

Copyright

About This Manual

This user manual is intended to guide professional installer to install the JetWave 2111L/2411L and how to build the infrastructure centered on it. It includes procedures to assist you in avoiding unforeseen problems.

Conventions

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

Note:

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

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

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

Warning:

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

The Red wording is very important you must avoid.

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

Federal Communication Commission Interference Statement

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

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

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

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

FCC Radiation Exposure Statement:

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

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

Content

Chapter 1

Introduction

Chapter 1 Introduction

1.1 Introduction

The user manual is applied to Korenix JetWave 2111L/2411L LTE IP Gateway. The 2 product series equips with the same LTE technology, the same hardware/software platform and the same installation consideration for indoor or outdoor field box.

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

1.2 JetWave 2111L/2411L Series Appearance

Figure - JetWave 2111L Appearance

Figure - JetWave 2411L Appearance

1.3 JetWave 2111L/2411L Major Features

Model Name	LTE	Bandwidth	Ethernet	Serial	DI/DO	Cellular
JetWave2111L-EU	Cat 1	10M DL/5M UL	1 x FE	N/A	1DI,1DO	FDD-LTE - B1/ B3/ B5/ B7/ B8/ B20 TDD-LTE - B38/ B40 /B41 WCDA -B1/ B5/ B8
JetWave2111L-AU	Cat 1	10M DL/5M UL	1 x FE	N/A	1DI,1DO	FDD-LTE -B1/ B2/ B3/ B4/ B5/ B7/ B8/ B28 TDD-LTE - B40 WCDMA-B1/ B2/ B5/ B8
JetWave2411L-EU	Cat 4	150M DL/50M UL	1 x FE	N/A	1DI,1DO	FDD-LTE - B1/ B3/ B5/ B7/ B8/ B20 TDD-LTE - B38/ B40 /B41 WCDA -B1/ B5/ B8
JetWave2411L-AU	Cat 4	150M DL/50M UL	1 x FE	N/A	1DI,1DO	FDD-LTE -B1/ B2/ B3/ B4/ B5/ B7/ B8/ B28 TDD-LTE - B40 WCDMA-B1/ B2/ B5/ B8

- Industrial Slim Size Cellular Router/IP Gateway
- JetWave2411L (LTE Cat 4) max. 150M DL/50M UL
- JetWave2111L (LTE Cat 1) max. 10M DL/5M UL
- One MicroSD card slot support
- 1 DI + 1 DO
- 1 Fast Ethernet Port
- VPN/Firewall/DMZ and Secure VPN Connectivity
- LAN to 4G/LTE Routing
- Remote management by Web GUI, SNMP, Auto IP Report, Korenix View, Mobile Manager
- 24V(9~48V) DC power input
- Wide Temperature, Heavy Industrial Grade design

1.4 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 2111L/2411L Unit (depends on the model you purchase) Pre-installed Embedded LTE Module (depends on the model you purchase)

Default Antenna 2

Din-Rail Mounting Kit

6-pin Power/DI+DO connector

Quick Installation Guide

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

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

Note 2: Different model 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 2111L/2411L Series.

2.1 Professional Installation Required

1. Please seek assistance from a professional installer for field installation or professional IT Engineer for indoor installation.
2. The JetWave 2111L/2411L series is distributed through distributors and system installers with professional technicians and will not be sold directly through retail stores.

2.2 Power Installation

2.2.1 DC Input

1. There is one 6-pin terminal block within the package for screwing the DC wires. It is a good practice to turn off the system power, and to unplug power terminal block before making wire connections.
2. Insert the positive and negative wires into the V+ and V- contact on the terminal block connector. Tighten the wire-clamp screws to prevent DC wires from being loosened. The range of the suitable electric wire is from 9 to 48 AWG.
3. The typical and suggest power source is DC 24V, the acceptable range is range from 9~48V.
4. The single DC power can be redundant. You can connect one power to typical power source and the other to battery/UPS as backup.

2.3 I/O Configuration

2.3.1 Wiring your Ethernet Port

There are 1 Fast Ethernet port. The 1 port is standard RJ-45 form factor. They can support 10Base-TX, 100Base-TX. 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.

Available Cable Type:

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

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

Wiring STP Cable: STP (Shielded Twisted Pair) cable is preferred. The device is an EN50121-4 certificated product and usually install in harsh environment, part of the EMS protection are based on STP cable, for example the Surge protection of front Ethernet ports. STP cable can provide better field protection. It is MUST for the device installation in harsh environment.

2.3.2 Reset

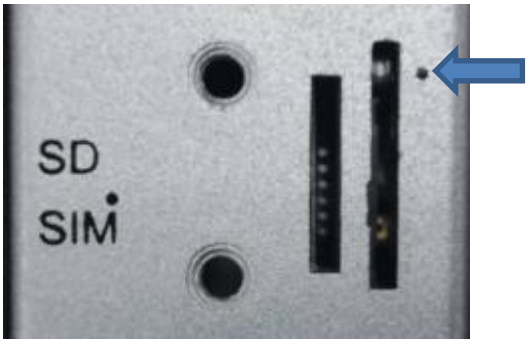
There is one Reset button located on the front of the device. This is design for user to reboot the system port or force reset the configuration to default. The function is depended on how much time you press the button.

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

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

2.3.3 SIM Socket

The JetWave 2111L/2411L provides one external SIM (Subscriber Identity Module) socket to store the LTE SIM card. Loosen the screw and then you can plug in the SIM card.



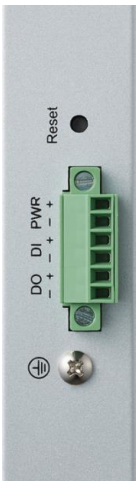
SIM connecter

The supported SIM card is Nano-SIM.

Note: While you prepare to plug in the SIM card, please remember to power off the system first. This is a **MUST** step, it allows the JetWave 2111L/2411L system to detect the SIM card while booting up.

2.3.4 Digital Input

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



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

2.3.5 Digital Output

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

2.3.6 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 LED Indicator

The following table indicates the LED of your device.

LED	Indication	LED	Indication
DO	**Digital Output** Status Red ON = The Relay is ON. It may indicate the alarm of specific events.	**R**	Status of the **Radio** Green ON = Radio is activated
PWR	**Power 1** Status Green ON = System ON		

2.5 Using the External Antenna

Consult your system integrator or our technical support engineer to choose the suitable external antenna with SMA-type or N-Type connector for your application. Different antenna supports different bands, polarization and different range of coverage.

Antenna Socket of the Gateway:
LTE2: SMA connector LTE antenna
LTE1: SMA connector LTE antenna

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.

Chapter 3

Prepare for Management

Chapter 3 Prepare for Management

The JetWave 2111L/2411L Series supports Web GUI Configuration, Simple Network Management Protocol (SNMP), Telnet and Diagnostic Command Line Interface for management and Window Utility helps you discover the device cross network, basic IP setting, firmware management…etc.

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

3.1 Basic Factory Default Settings

We'll elaborate the JetWave 2111L/2411L 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 2111L/2411L Basic Factory Default Settings

Features		Factory Default Settings
Username		admin
Password		admin
Model Name		JetWave2111L (2411L depends on which model you access)
Device Name		korenixXXXXXX (X represents the last 6 digits of Ethernet MAC address)
Default IP at Bridge Mode (JetWave 2111L/2411L Default)		
Access Type		Static IP
IP Address		192.168.10.1
Subnet Mask		255.255.255.0
Default Gateway		0.0.0.0
Primary DNS Server		0.0.0.0
Secondary DNS Server		0.0.0.0
Remote Settings	Remote Management Privacy	Telnet, SNMP, SNMP Trap, Email Alert
	Even Warning Type	WLAN association, Authentication fail, Configuration Changed
	Version	2/3
	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	
Diagnostic CLI	Baud Rate	115,200
	Parameter	N, 8, 1

Warning:

It is Important to change all the default settings of the Gateway, 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 10/100Base-T(X) adapter;

Configure the computer with a static IP address of 192.168.10.x (X cannot be 0, 1, nor 255) 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.

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

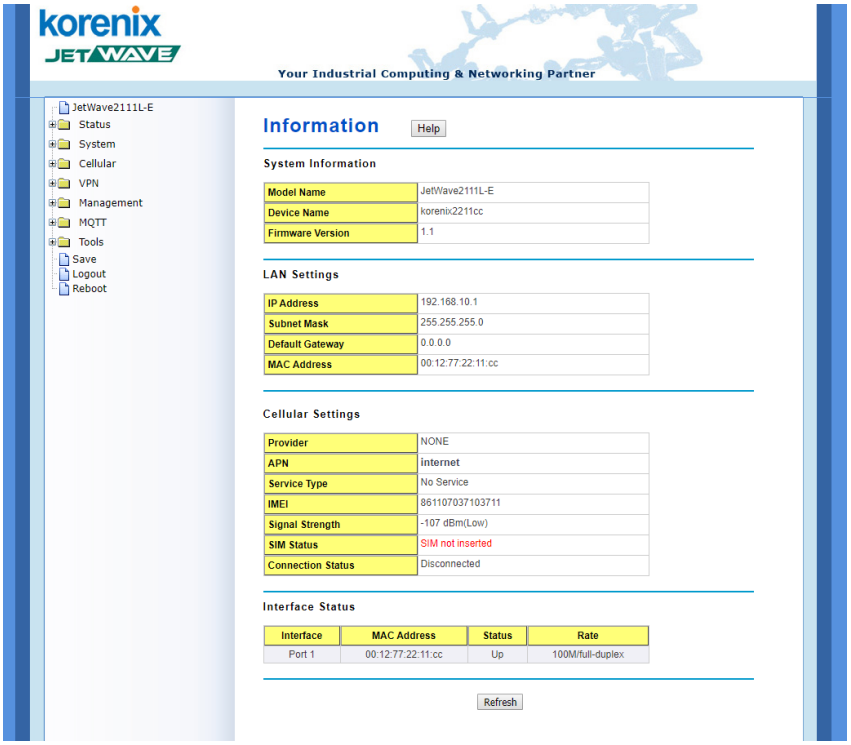


Figure - Main Page

Note:

The username and password are case-sensitive!

3.4 Fail to login the Web GUI

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

1. Please disable the firewall setting of your browser. The firewall setting may block the connection from your PC to the device. The firewall may stop the firmware upgrade, configuration backup and restore as well. Note that after finished the setting, re-enable your firewall to protect your PC.
2. Check the IP Setting, your PC and managed device must be located within the same subnet.
3. 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.

3.5 How to login the CLI

Telnet/SSH:

You can connect to the device by Telnet and the command lines. 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

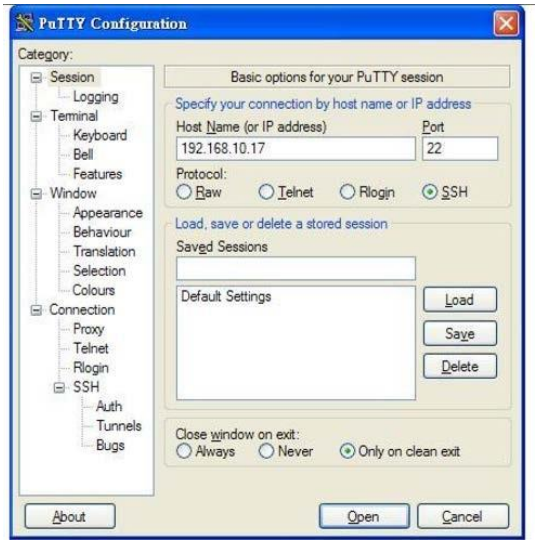
Note that the Telnet.exe file is not provided after Window 7. You can download it from Microsoft web site. Or you can use 3rd Party tool, for example the Putty.

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).



3.6 Discovery Utility – Korenix View Utility

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

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

The chapter 5.3 introduces how to use Korenix View Utility.

Chapter 4

Web GUI Configuration

Chapter 4 Web GUI Configuration

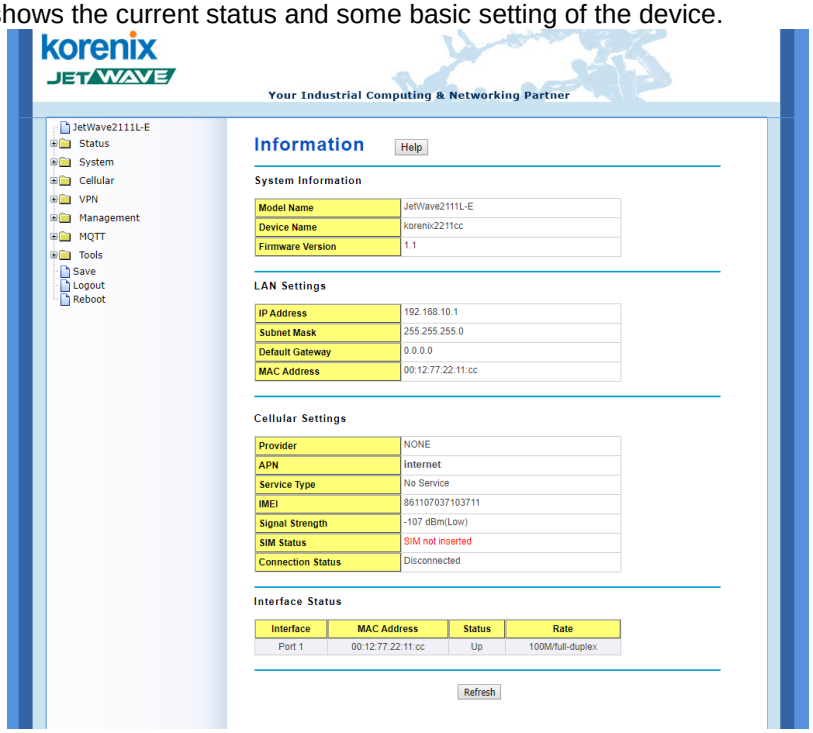
This chapter describes the Web GUI for Software Configuration.

4.1 Status

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

4.1.1 Information

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



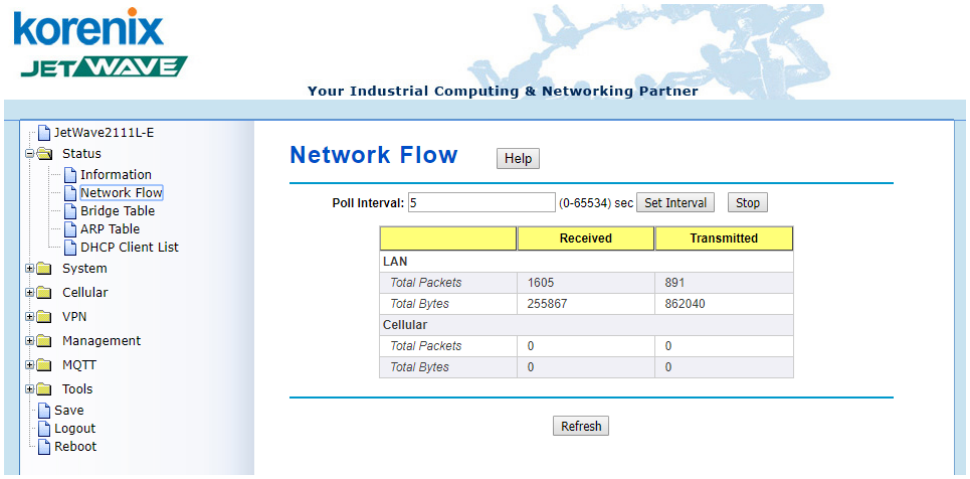
System Information: The Model Name, Device Name, Country/Region you selected and Firmware version number.

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

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

4.1.2 Network Flow (Statistics):

This page shows the packet counters for transmission and reception regarding to Cellular and Ethernet.



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 Bridge Table

This table shows bridge table.

MAC Address: The MAC address of the connected device.

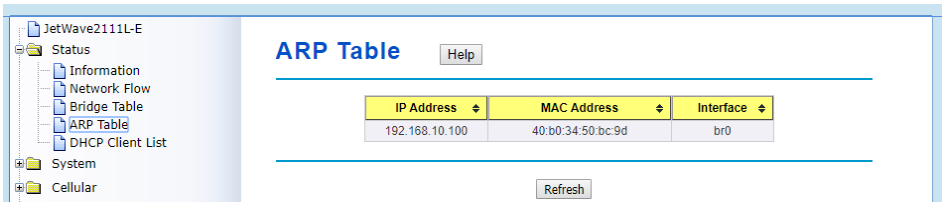
Interface: This field shows the interface which learnt the MAC Address.

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

Refresh: Refresh the table.

4.1.4 ARP Table

This table shows the ARP table.



IP Address: The IP Address leant from the interface.

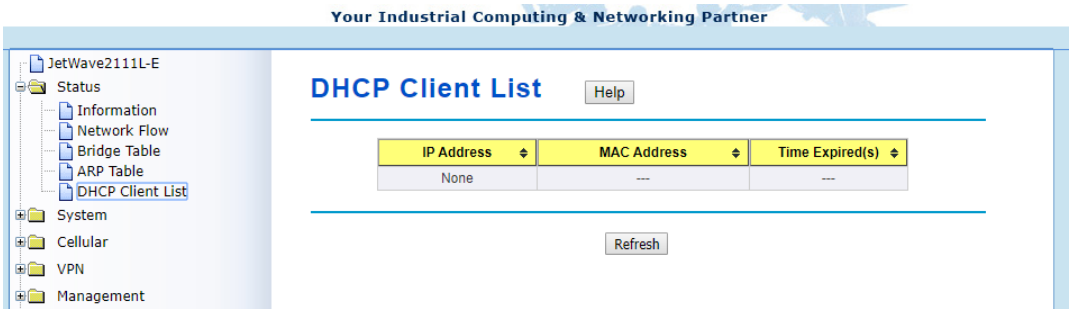
MAC Address: The MAC Address leant from the interface.

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

Refresh: Refresh the table.

4.1.5 DHCP Client List

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



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

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

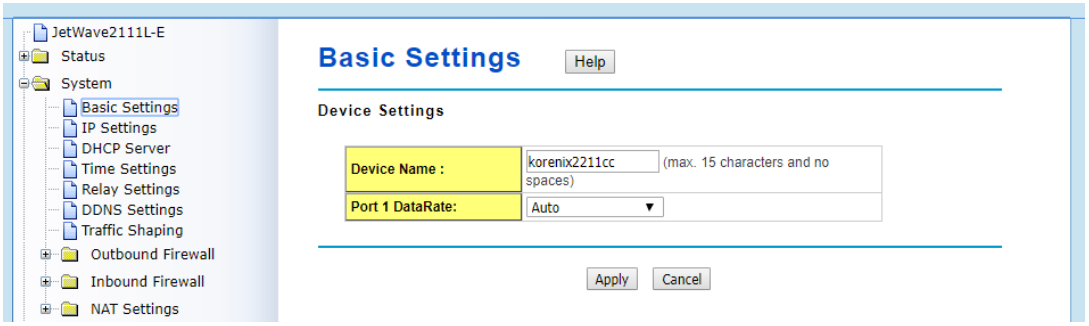
Time Expired(s): The DHCP expire timer connected DHCP client device. Time unit is second. The number can be changed in DHCP Server Lease Time setting.

Refresh: Refresh the table.

4.2 System

For users who use the JetWave 2111L/2411L series for the first time, it is recommended that you begin configuration from the "**System**" feature set pages shown below:

In **System** pages, there are some configuration pages for the system settings. These setups are introduced in below pages.



4.2.1 Basic Settings

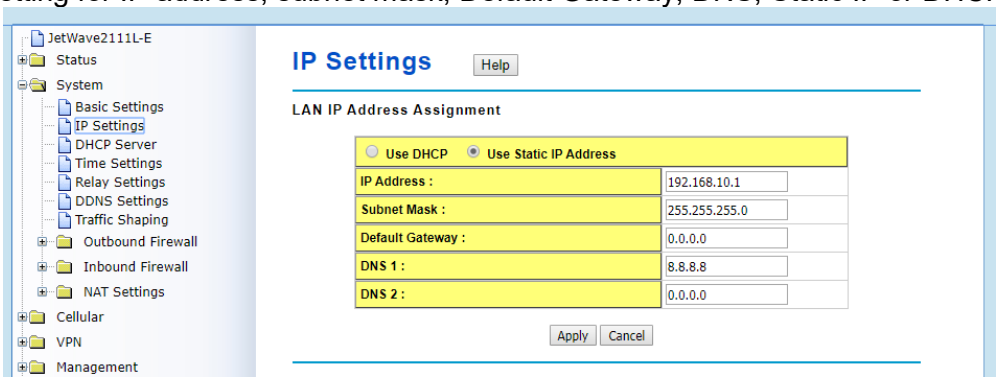
Use this page to configure the basic parameters of the device.

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

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

4.2.2 IP Settings

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



LAN Settings:

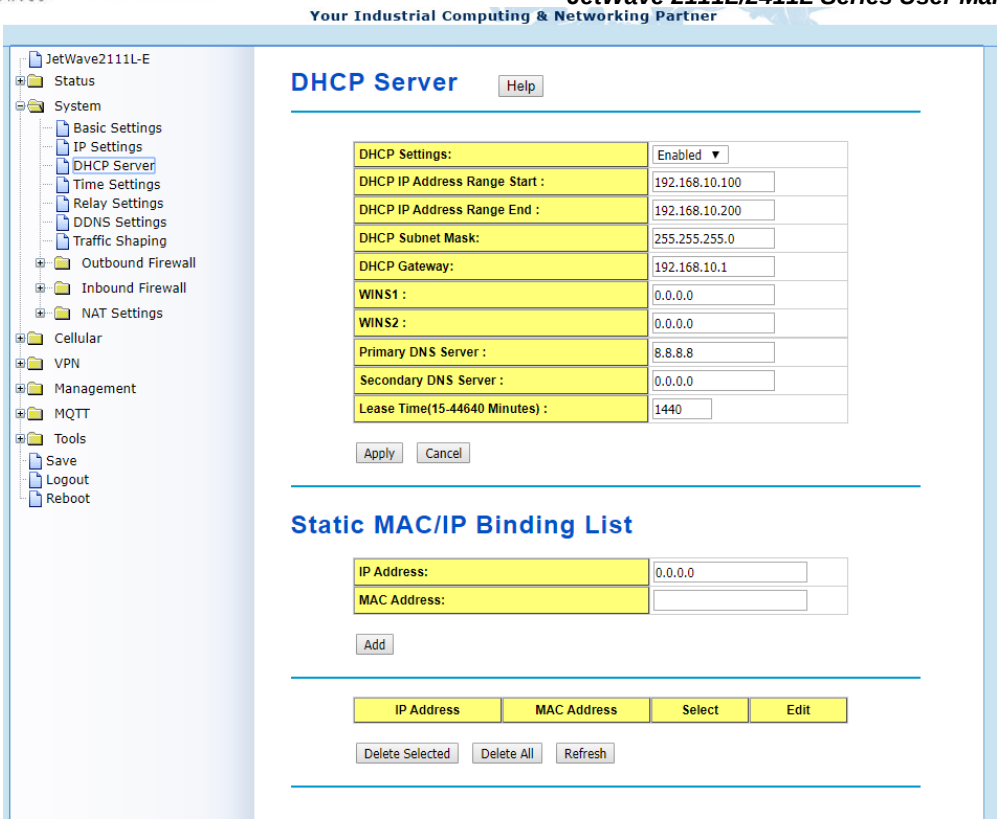
IP Address: The IP Address field allows you to set the device's WAN IP address manually.

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

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.

DHCP Server: Enabled / Disabled



DHCP Server Setting:

In Router mode, you can enable DHCP Server to assign IP address to DHCP clients. And you should define the address pool by configuring the Start IP and End IP. DHCP server will allocate IP address dynamically from the pool. The device allows you to assign up to one Class C, 255 IP Addresses. Since the maximum connection session is 64, configuring 64 IP addresses is enough for the need.

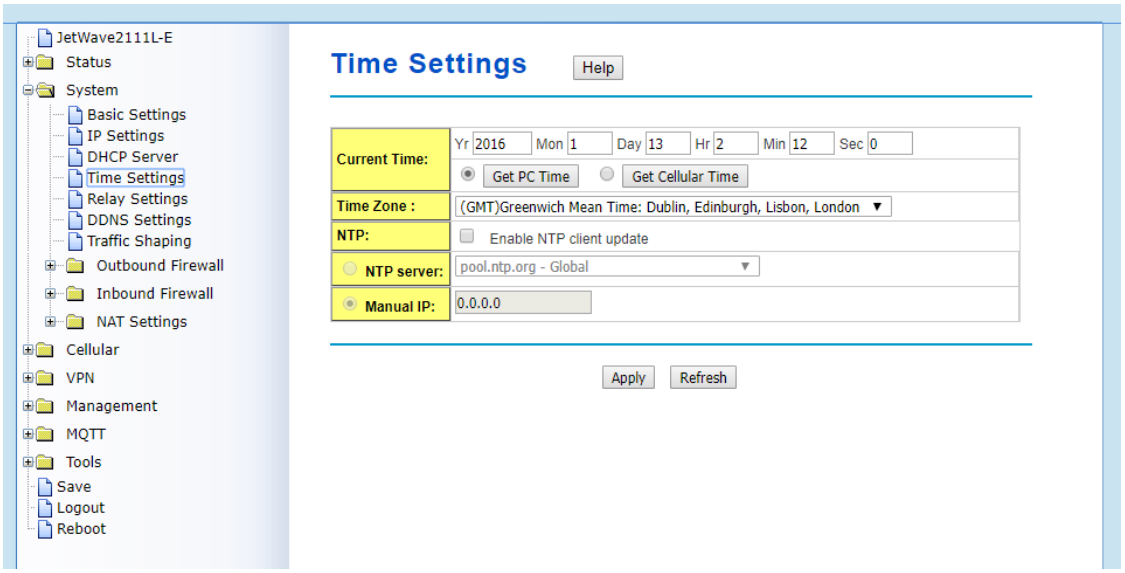
You can also configure the **Subnet Mask, DHCP Gateway, WIS, Primary/Secondary DNS Server**s' IP Address and **Least Time** of the assigned IP addresses.

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 Time Settings

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



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

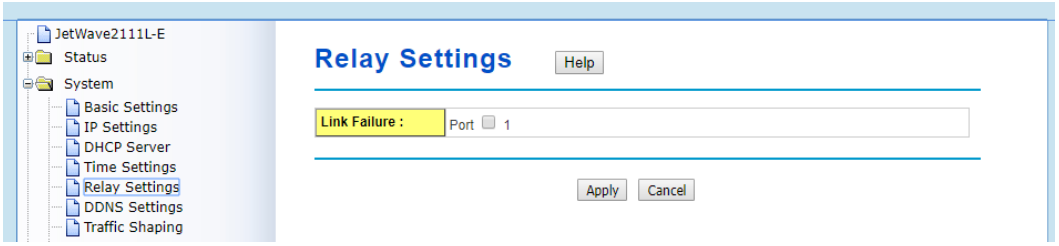
Time Zone Select: Select the time zone of your country from the dropdown list.

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

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

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

4.2.4 Relay Settings



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

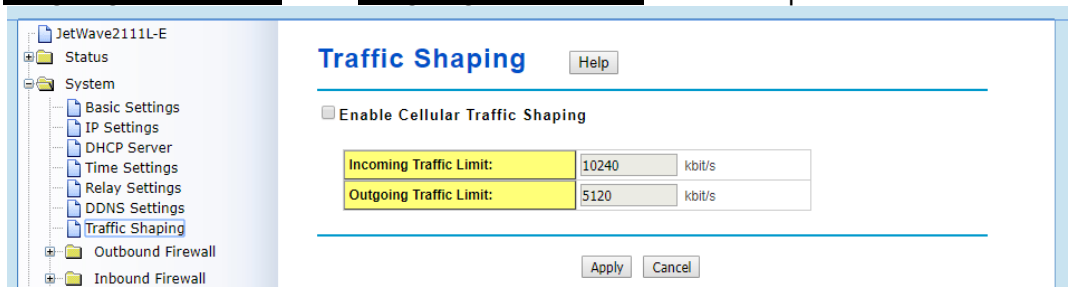
Link Failure: You can bind the Ethernet port failure event with Relay output.

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

4.2.5 Traffic Shaping

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

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



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

4.2.6 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.

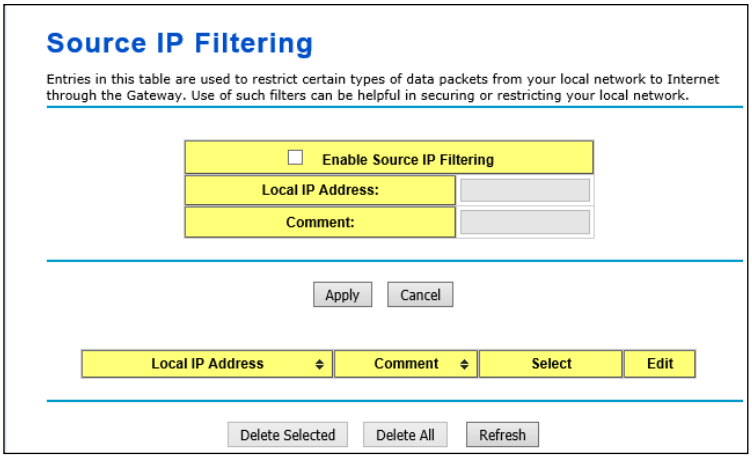
"**Src Port Filtering**": Source Ports Filtering from the LAN to Internet through the gateway.

"**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.

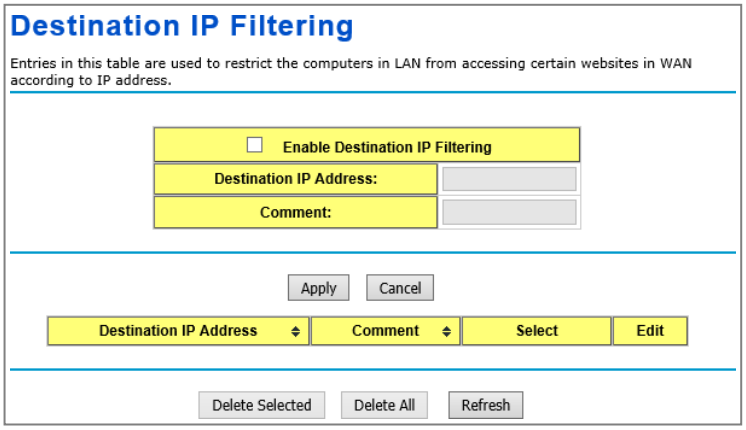


  After applied, the Web GUI will show "**Change settings successfully**". Click "**OK**" and then you can see the new entry shown in the below table.

- **Destination IP Filtering**

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

  Select "**Enable Destination IP Filtering**", type the "**Destination IP Address**" and "**Comment**"



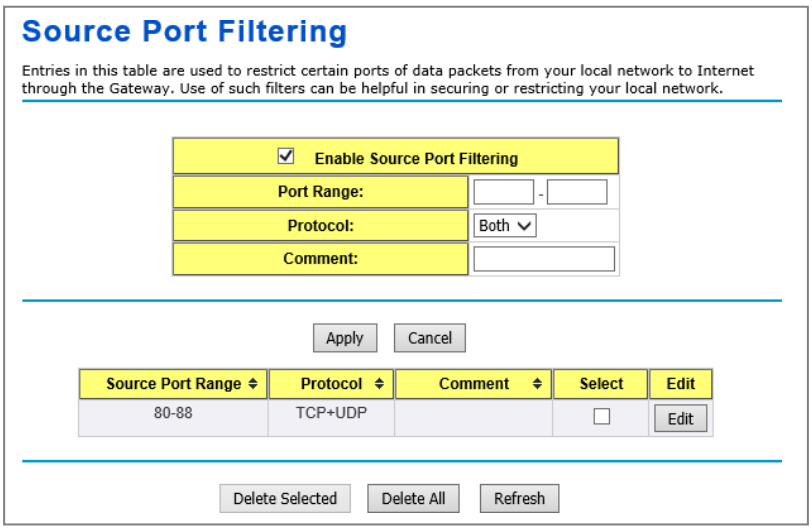
(note for the entry) and then press "**Apply**" to activate the settings.

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

- **Source Port Filtering**

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

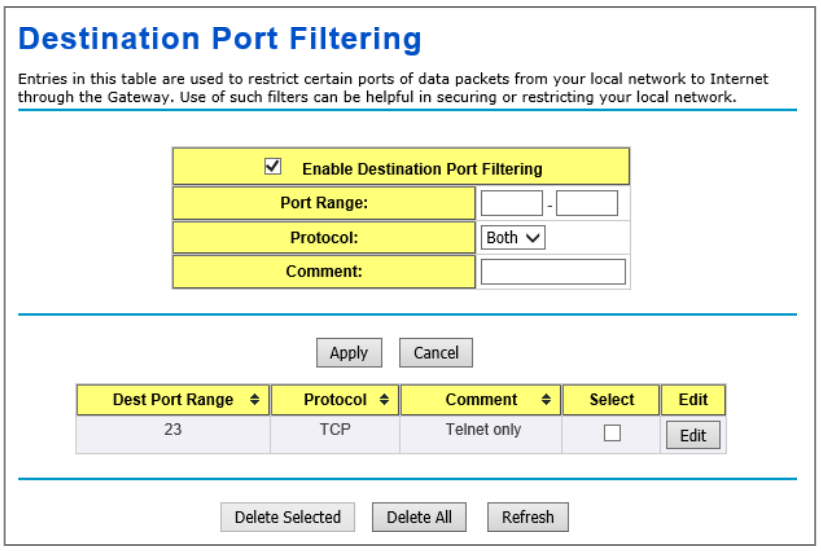
Select "**Enable Source Port Filtering**", type the "**Port Range**" of below "**Protocol**" type, the protocol type can be **UDP, TCP or Both**. Type the "**Comment**" (note for the entry) and then press "**Apply**" to activate the settings.



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

- **Destination Port Filtering**

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



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

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

4.2.7 Inbound Firewall

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

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

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

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

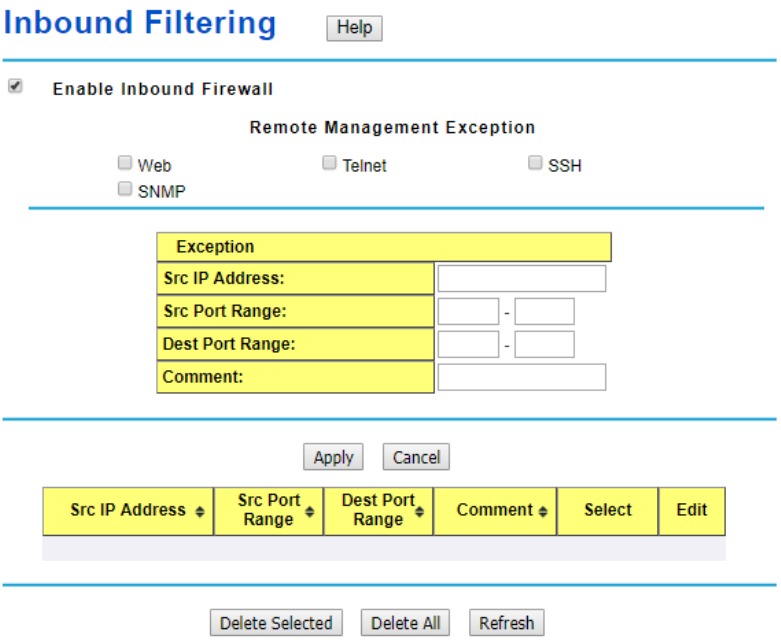
Src Port Range: The source port range of the above IP address.

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

Comment: Note for the entry.

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

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



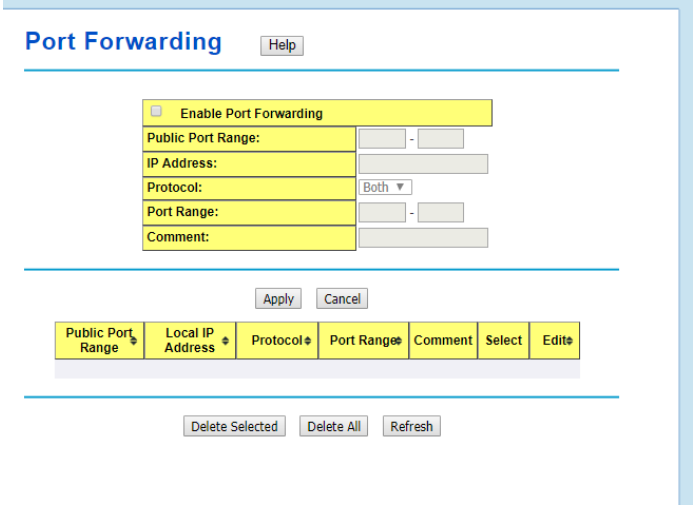
4.2.8 NAT Settings

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.



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.

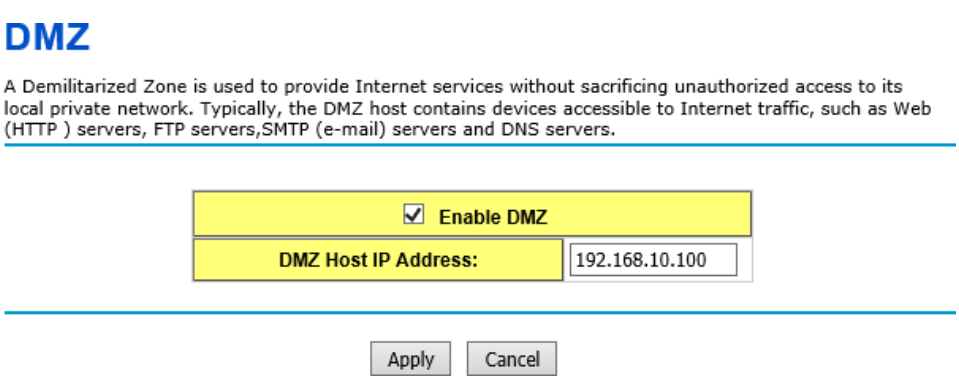
Port Range: Configure the port range of the LAN, the traffic from the public port will be redirected to these port.

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.



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.

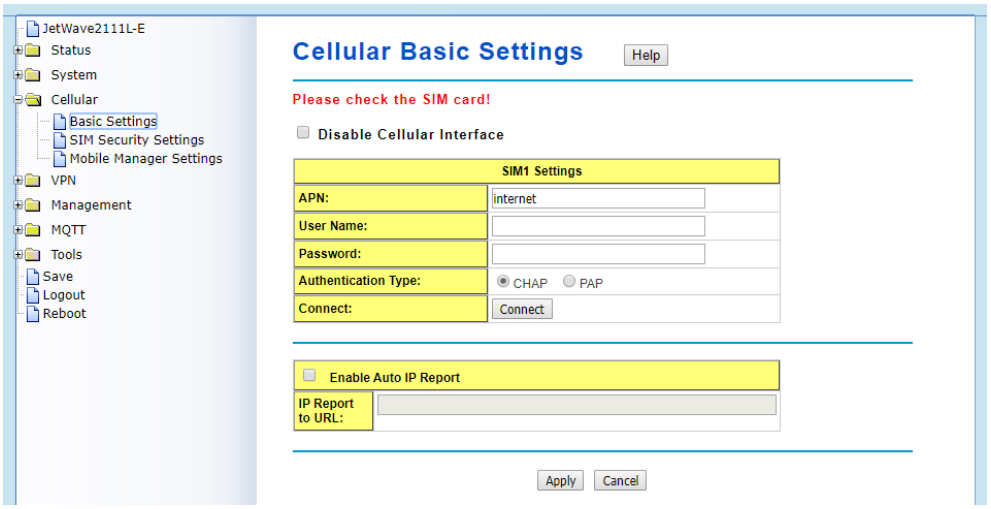
4.4 Cellular

The "**Cellular**" feature set pages allow users to see the LTE Status, configure the Basic LTE Setting, SIM Security and download the Debug message.

4.4.1 Status

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

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



Provider: The name of the ISP.

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

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

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

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

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

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

Below are the signal strength definitions in our system:

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

-113 dBm or less (Low)

-51 dBm or greater (Excellent)

Not known or not detectable

SIM Status:

SIM OK: The SIM card is okay to use.

SIM not inserted: The SIM card is not inserted.

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

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

Connection Status:

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

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

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

Refresh: You can press Refresh to refresh the table.

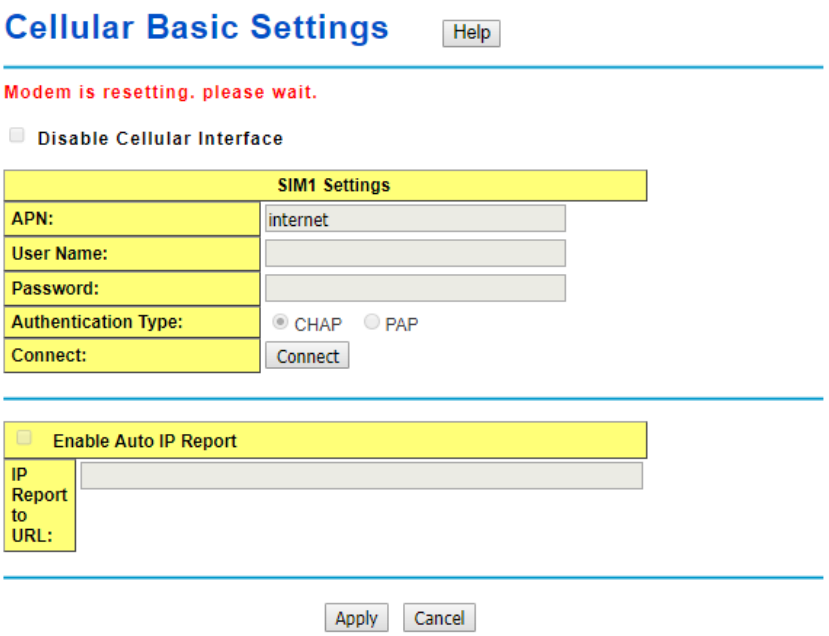
Below is the reference information after connected to UNICOM telecom in China. The service provider is China UNICOM, it provides the APN name, Service Type and assigns IP address for the JetWave 2111L/2411L.

System Information

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

4.4.2 Basic Settings

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



Disable 4G/Cellular Interface: You can disable the LTE interface manually.

APN: Every ISP has a specific APN (Access Point Name) assigned to its cellular network. The system can read this name from the SIM card. You can also find this setting by contacting your

ISP to know this. Once you failed to connect your LTE cellular network, this is the first way you can check. Please check with your ISP to know the APN and correctly input the setting through the page.

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

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

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

Auto IP Report:

Most of the ISP assigns the dynamic IP address to the LTE clients and change the IP address every period of time. While you need to remotely control the gateway, you may need additional information generated from the remote LTE client device. The Auto IP Report in JetWave 2111L/2114 can meet your need while you need to know the IP address from the product.

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

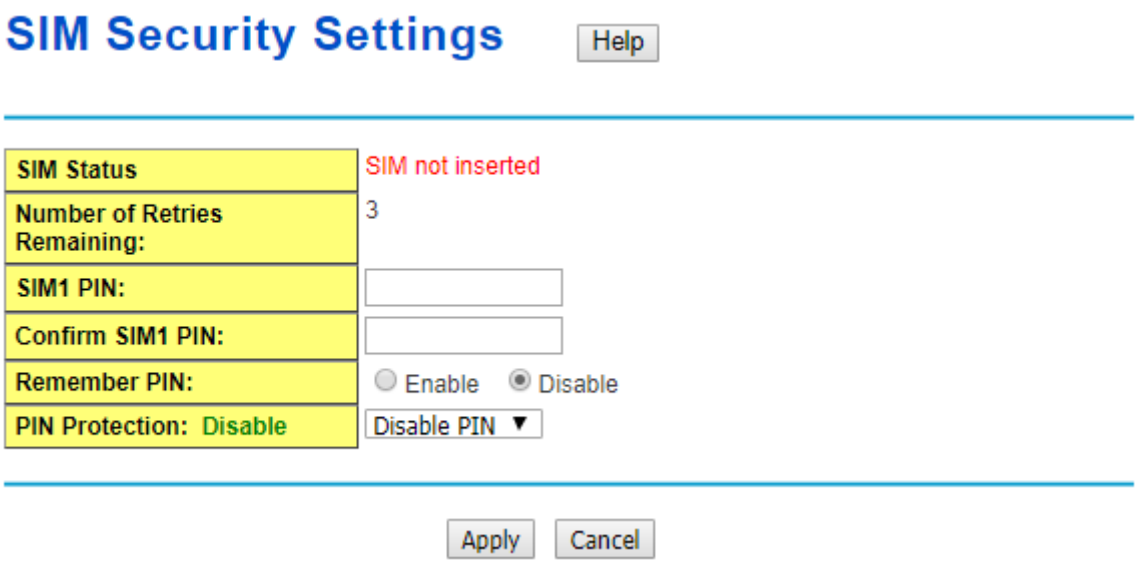
IP Report to URL: Type the correct URL here for your Gateway report to. You can build your own server, rent URL address from ISP or Google Cloud service also supports this functionality. Please check with your ISP or create through Google cloud.

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

4.4.3 SIM Security

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

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

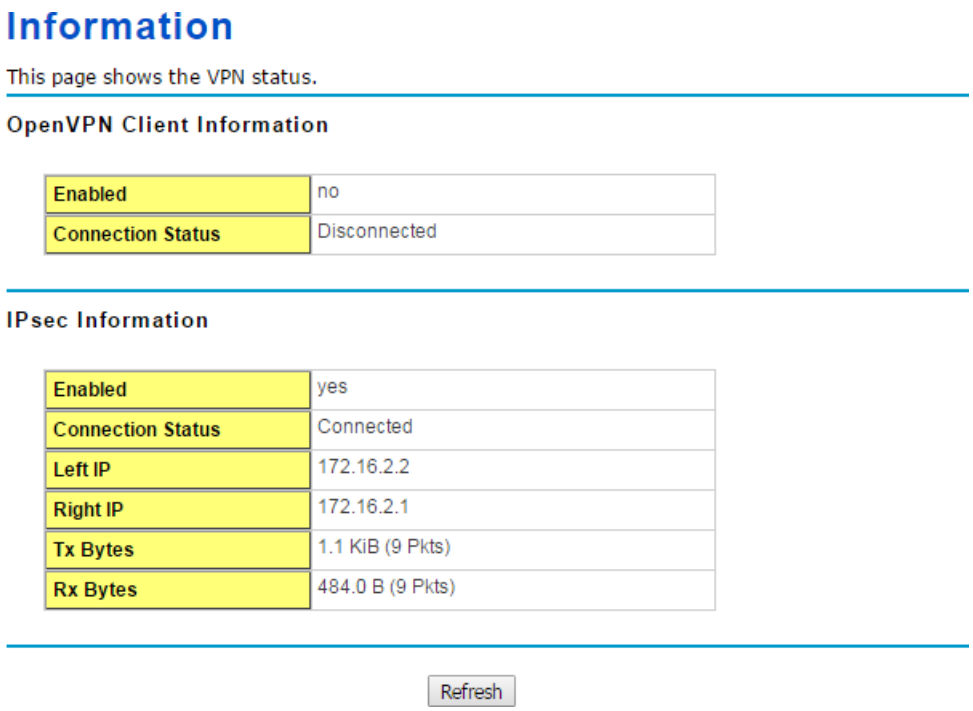


4.5 VPN

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

4.5.1 Status

This page shows the latest status of openVPN client and IPsec.



OpenVPN client:

Enabled:

yes: The VPN function already enabled.

no: The VPN function not enabled yet.

Connection Status:

Connected: The VPN connection already built successfully.

Disconnected: The VPN not connect.

IPsec:

Enabled:

yes: The IPsec function already enabled.

no: The IPsec function not enabled yet.

Connection Status:

Connected: The IPsec connection already built successfully.

Disconnected: The IPsec not connect.

Left IP: left IP corresponds to right IP. The two IPs should be conceptually connected between two JetWave. For example, bridge port IPs in LAN, or public IPs when using cellular network

Right IP: described as above.

Tx bytes: the amount of traffic transmitted in bytes from itself to another side. Number of packet also displayed.

Rx bytes: the amount of traffic received in bytes from itself to another side. Number of packet also displayed.

4.5.2 OpenVPN Client

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.

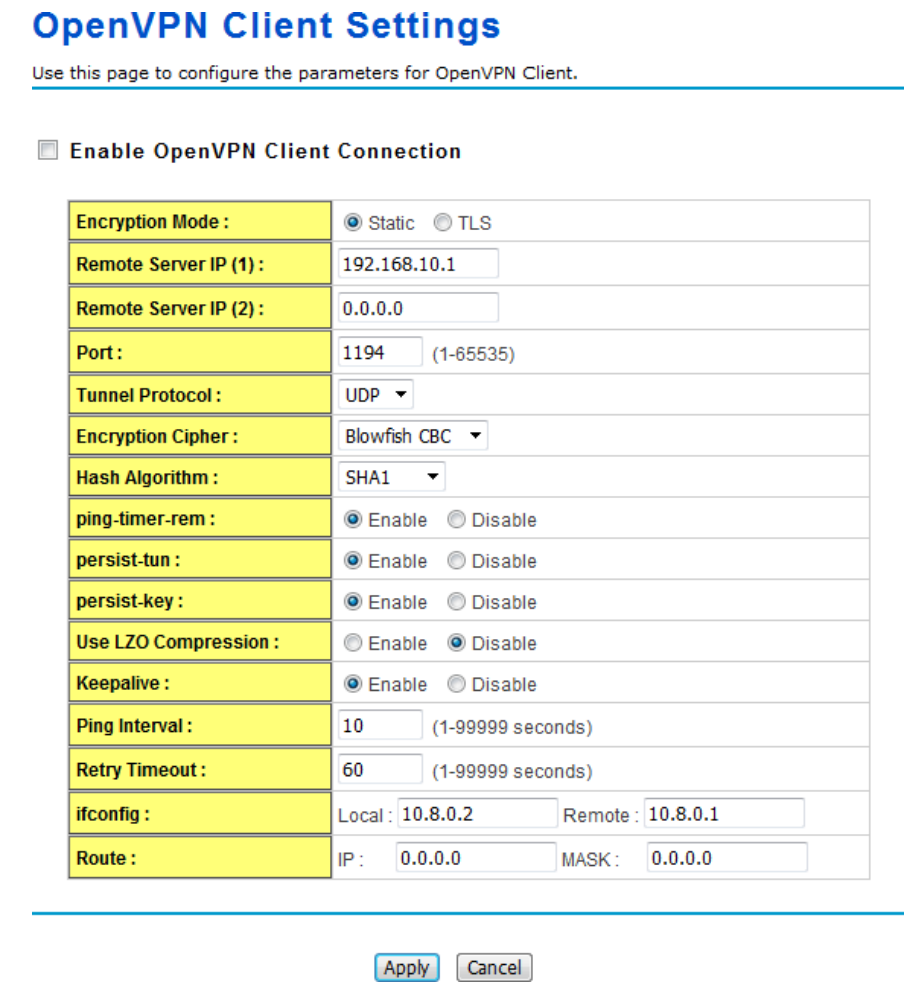
In TLS encryption mode, each VPN client needs 3 keys, while VPN server needs 4 keys. The description of the 7 keys listed below.

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

JetWave 2111L/2411L acts as OpenVPN client. ca.crt, client.crt and client.key are needed to establish OpenVPN tunnel as OpenVPN client. Notice that the file names of these keys are pre-defined and can't be changed.

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

The OpenVPN client configurations can be set in VPN->OpenVPN client Web configuration page. Check Enable OpenVPN client connection checkbox and configure OpenVPN client configurations. Note that the settings should be consistent with OpenVPN server.



Encryption Mode: Select the encryption is Static or TLS.

Static Key: Use a pre-shared static key.

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

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

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

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

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

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

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

Hash Algorithm: Select the hash algorithm.

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

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

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

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

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

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

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

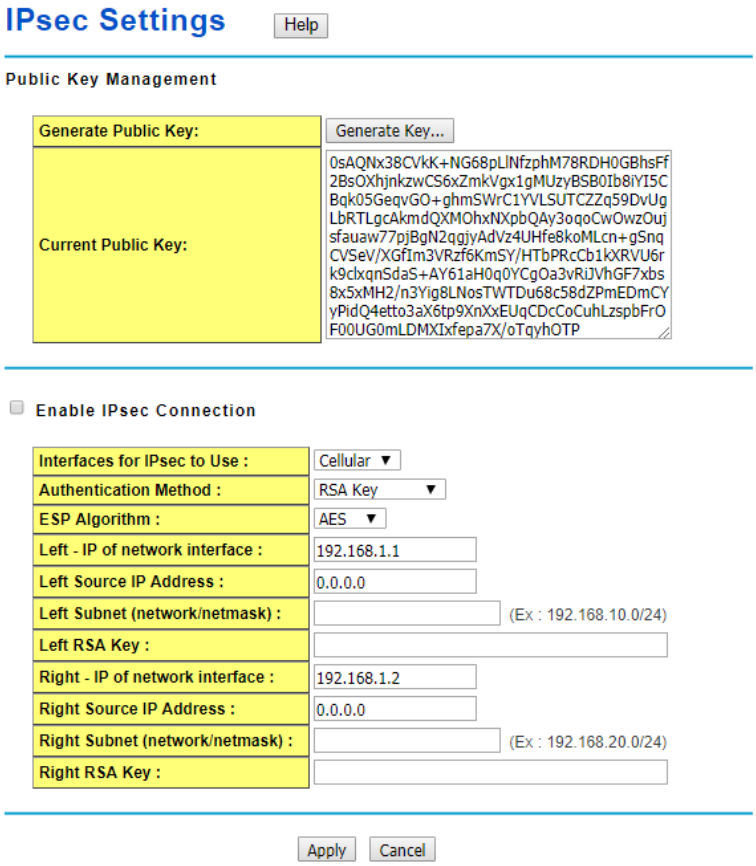
Ifconfig: Input the tunnel IP address that VPN use.

Route: Input the route IP and MASK.

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

4.5.3 IPsec

Point-to-point IPsec tunnel can be establish in VPN->IPsec Web configuration page. Check Enable IPSec connection checkbox and configure IPSec connection configurations.



The top-half page is a tool to generate public key. 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.

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

Authentication method: select authentication method, shared key or RSA key.

Static Key: Use a pre-shared static key.

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

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

ESP algorithm: select ESP (Encapsulating Security Payload) desired, AES/DES/3DES.

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

Left Source IP Address: 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 or cellular IP address when using cellular network.

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

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

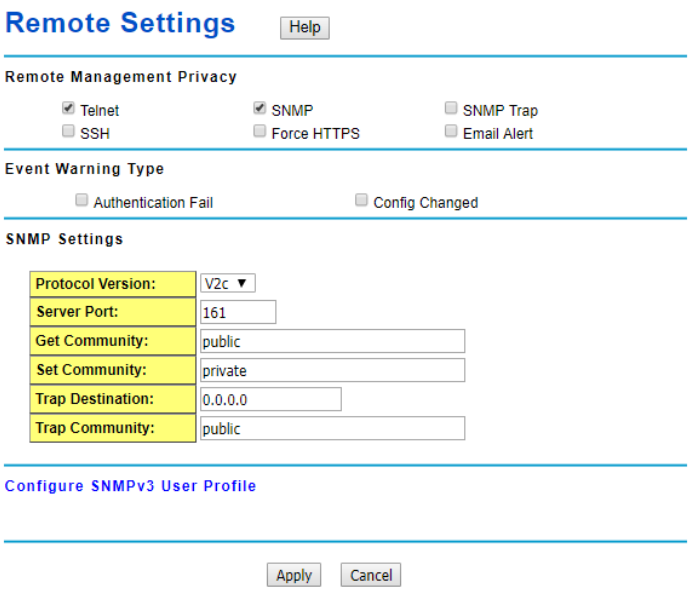
Right RSA key : the attribute is only required when using RSA key authentication method. Using public key generated from top-half page.

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

4.6 Management

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

4.6.1 Remote Setting



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

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

Event Warning Type: The event warming type selection.

Wlan association: The client associated to the AP event.

Authentication Fail: The client failure of authentication event.

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

SNMP Settings:

Protocol Version: Select the SNMP version, the product supports SNMP V1, V2c and V3. While selecting the SNMPv3, continue to configure the SNMPv3 User Name and Encryption in lower screen.

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

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

all requests.

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

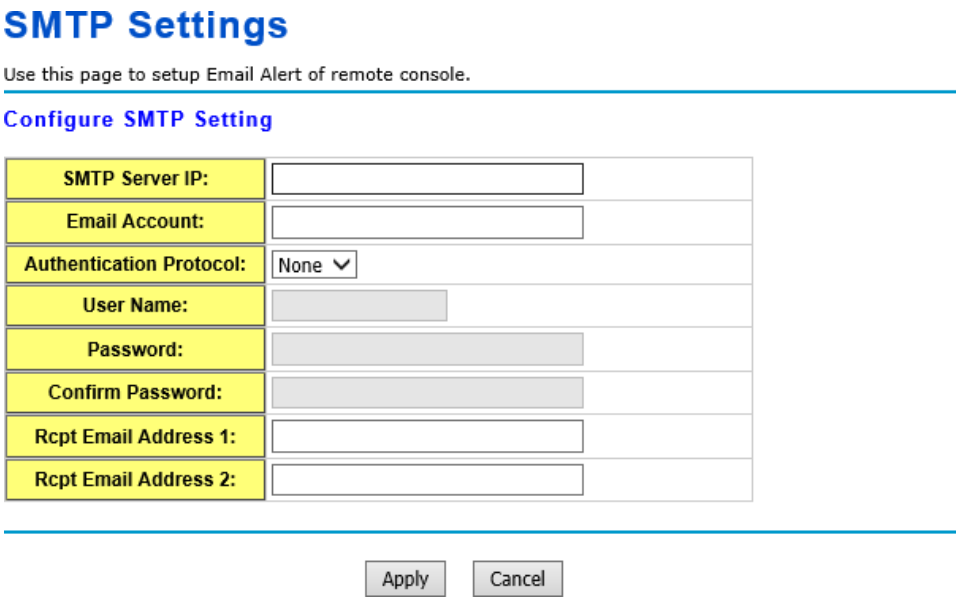
Trap Destination: Specify the IP address of the station to send the SNMP traps to.

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

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

4.6.2 SMTP Configuration

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



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

Email Account: The sender's Email Account.

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

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

Password: The Password of the Sender Email account.

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

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

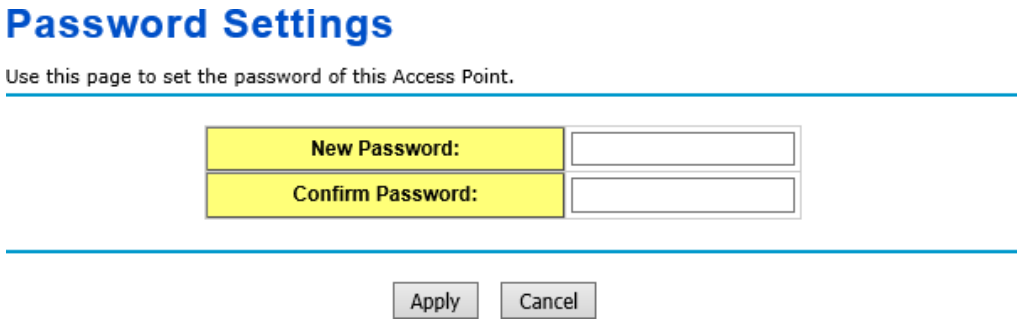
Rcpt Email Address 2: The second Receiver's email address.

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

4.6.3 Password Settings

Use this page to set the password of the Gateway.

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

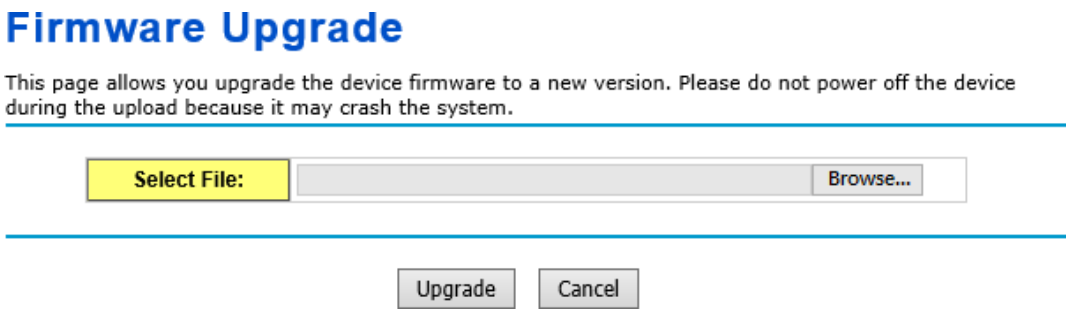


4.6.4 Firmware Upgrade

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

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

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



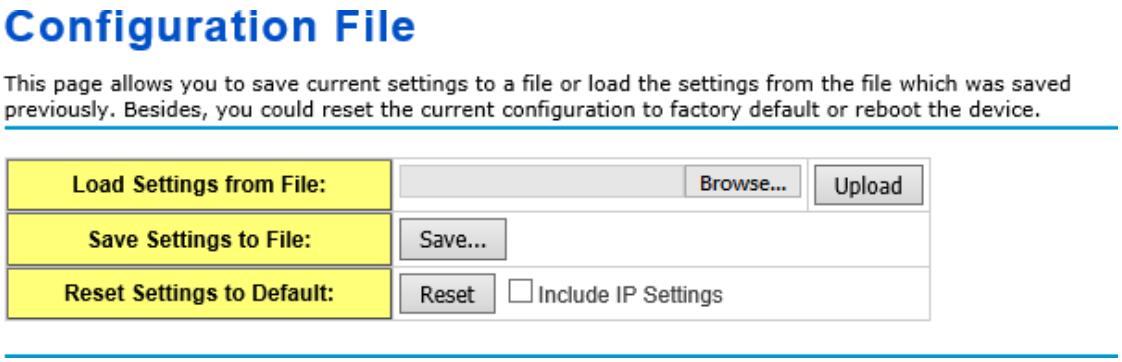
Type the path of the firmware in **Select File:** field. Or click "**Browse…**" to browse the firmware file. Press "**Upgrade**" to upload the firmware file to the Gateway. After finishing transmitting the firmware, the system will copy the firmware file and replace the firmware in the flash. During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

4.6.5 Configuration File

The Gateway provides Configuration File **Backup (Save Setting to File), Restore (Load Setting from File)** and **Reset Setting to Default** features.

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

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



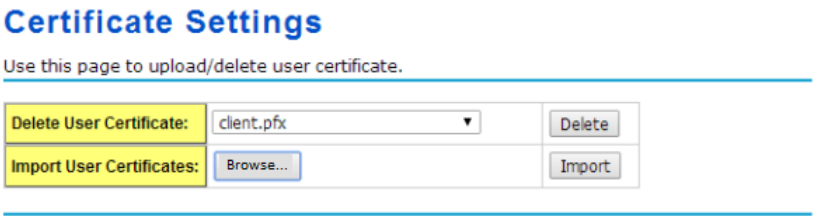
Backup (Save Setting to File): Press "Save…" to backup the configuration file to specific path/folder in your computer.

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

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

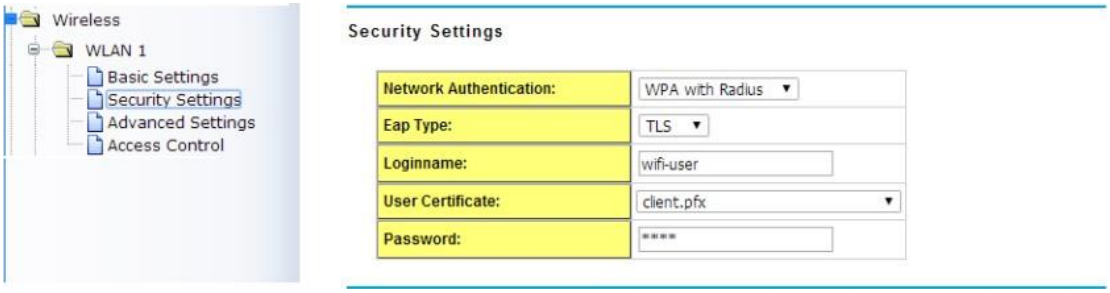
4.6.6 Certificate File

Use this page to import/delete 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 tool, web site or get from the IT administrator.

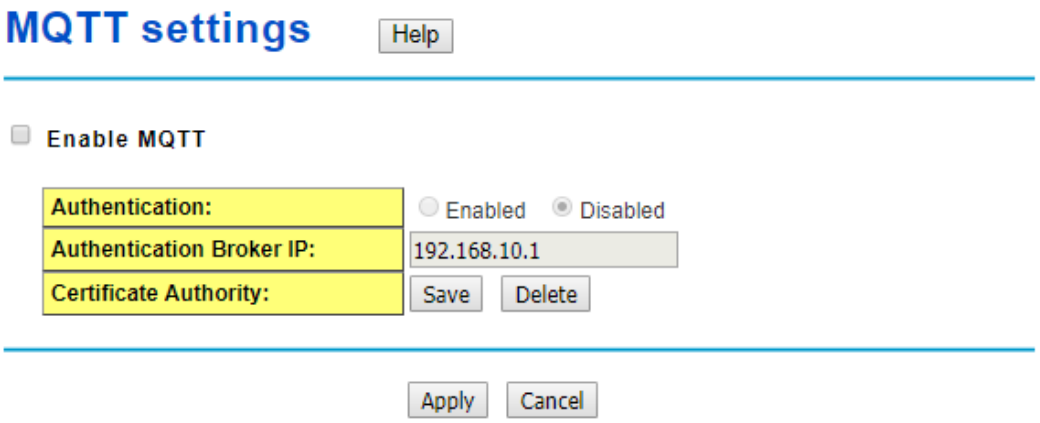
Following is the security setting under "WPA with Radius" Authentication mode, the Eap type is TLS. You can see the "User Certificate file" is assigned. The AP must use the same certificate file as your Radius Server under this setting.



4.6.7 MQTT

Authentication Broker IP: install Broker IP so our device can connect to the broker

Certificate Authority: choose certificate way

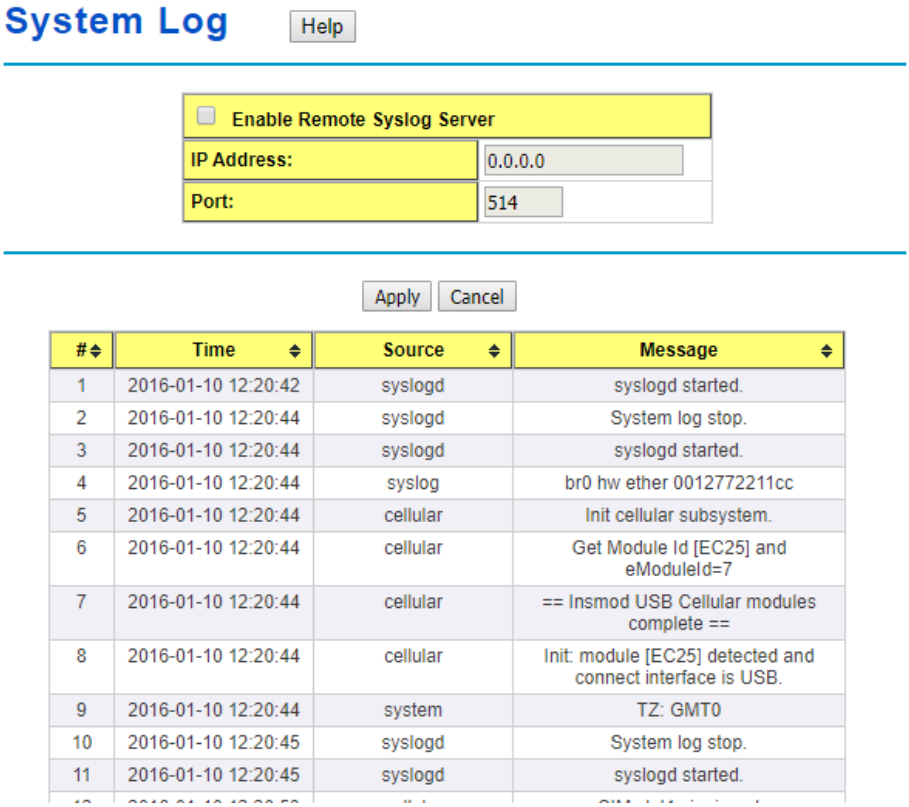


4.7 Tools

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

4.7.1 System Log

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



#	Time	Source	Message
1	2016-01-10 12:20:42	syslogd	syslogd started.
2	2016-01-10 12:20:44	syslogd	System log stop.
3	2016-01-10 12:20:44	syslogd	syslogd started.
4	2016-01-10 12:20:44	syslog	br0 hw ether 0012772211cc
5	2016-01-10 12:20:44	cellular	Init cellular subsystem.
6	2016-01-10 12:20:44	cellular	Get Module Id [EC25] and eModuleId=7
7	2016-01-10 12:20:44	cellular	== Insmod USB Cellular modules complete ==
8	2016-01-10 12:20:44	cellular	Init: module [EC25] detected and connect interface is USB.
9	2016-01-10 12:20:44	system	TZ: GMT0
10	2016-01-10 12:20:45	syslogd	System log stop.
11	2016-01-10 12:20:45	syslogd	syslogd started.

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

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

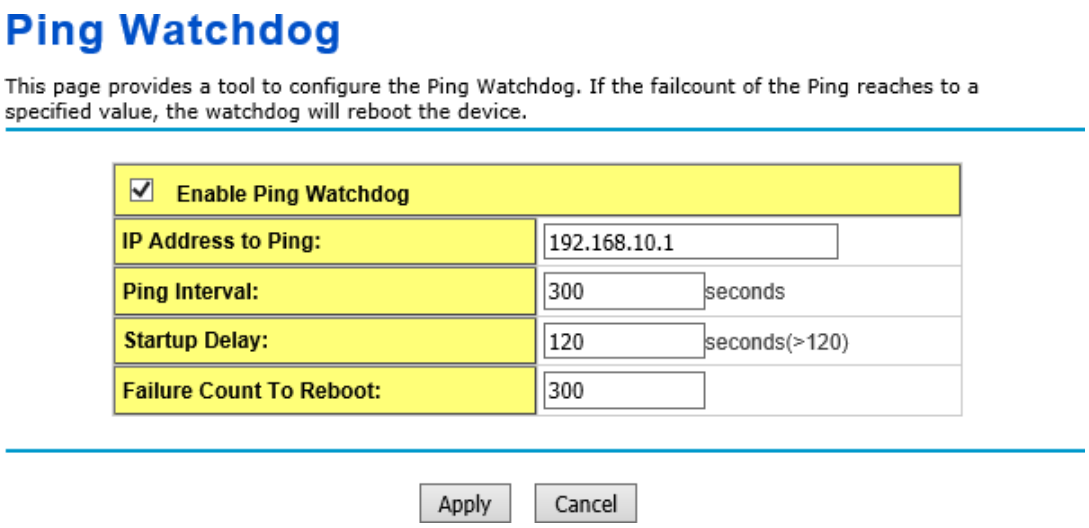
In the lower screen, it displays the occurred system logs. Each entry has the index, occurred time, source MAC address and the message. You can monitor the system by this screen, however, the logs will be removed after system reboot.

Press “**Clear**” allows you to remove all of entries.

Press “**Refresh**” allows you to refresh the table.

4.7.2 Ping Watchdog

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



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

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

Ping Interval: The interval time between each Ping packet.

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

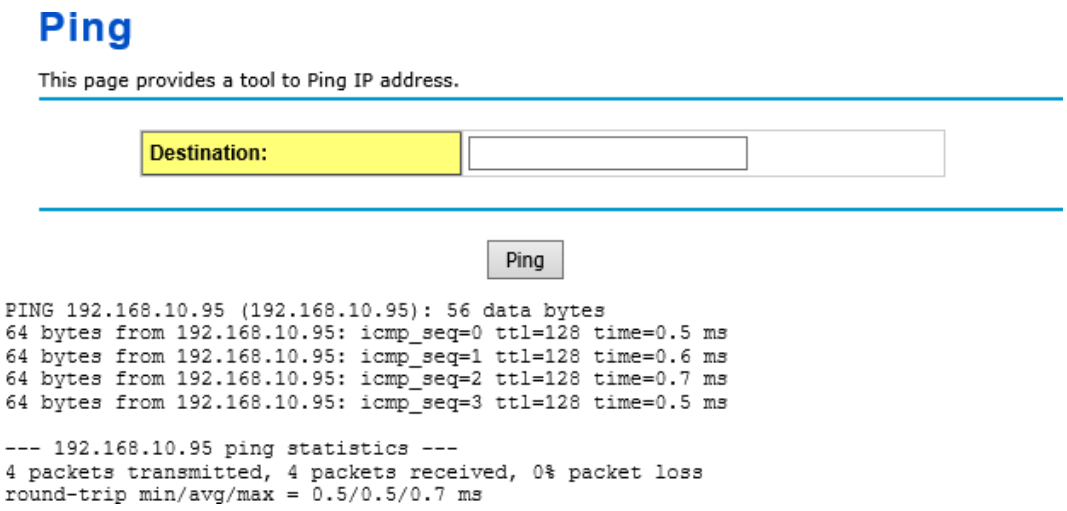
Failure Count to Reboot: After Ping failure count to the volume you assigned here, the system will reboot automatically

4.7.3 Ping

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

Type the target IP address in the "**Destination:_____**" field then press "**Ping**".

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

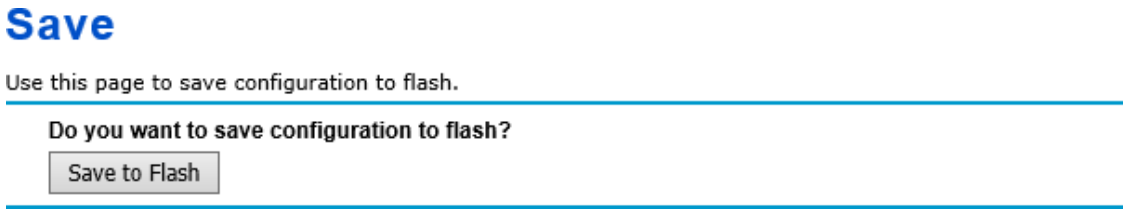


4.8 Main Entry

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.



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

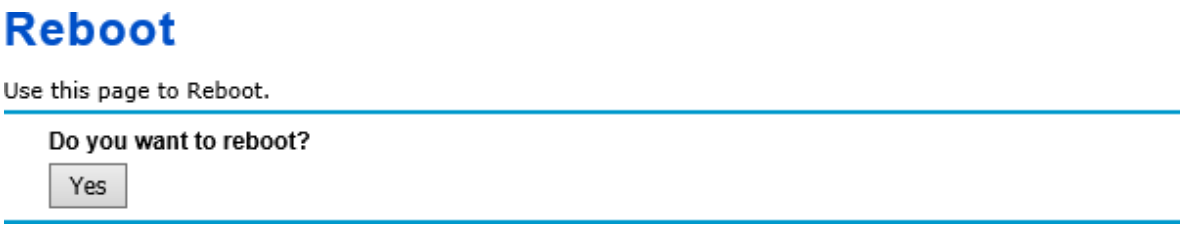
4.8.2 Logout

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

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

4.8.3 Reboot

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



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

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

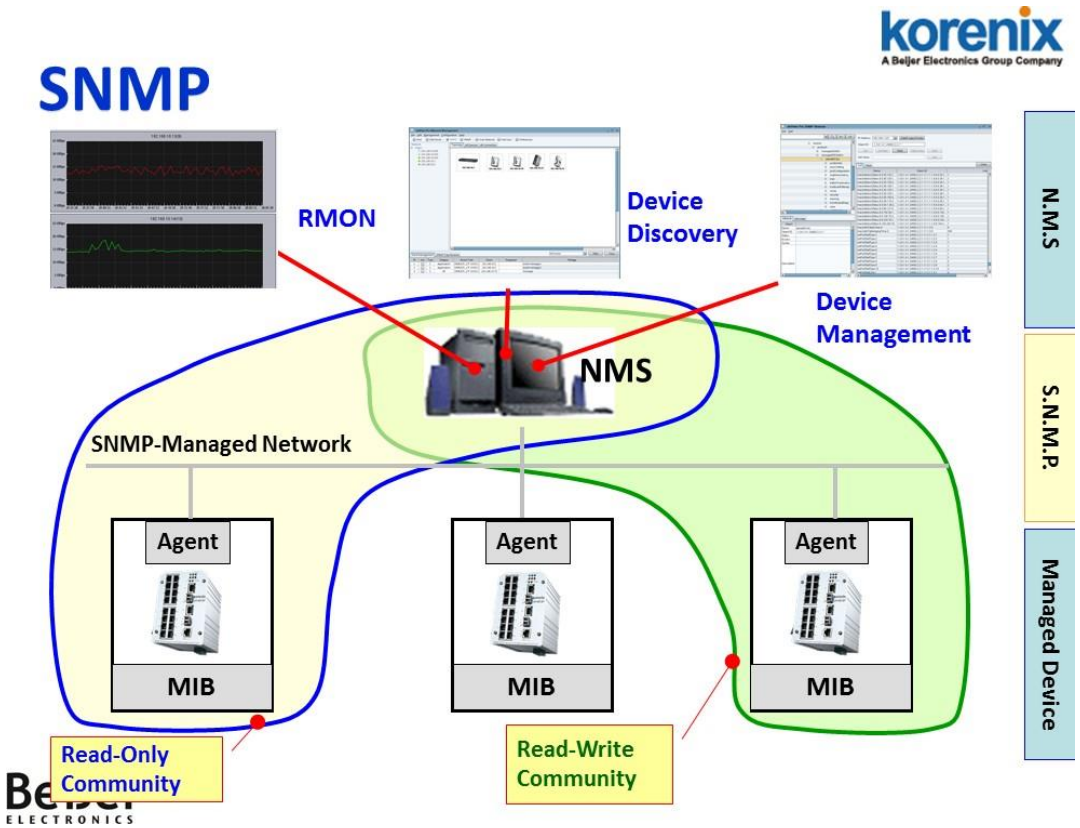
5.1 SNMP

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 Gateway. An agent translates the local management information (Management Information Base, MIB) from the managed device into a SNMP compatible format. In MIB, all the status and settings of the Gateway has its own specific object ID (OID), the manager can read or write the value of the OID.

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

Community:

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

SNMP Setup:

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

5.1.2 Management Information Base (MIB):

Before you want to manage the JetWave 2111L/2411L series Gateway through SNMP, please go to download the MIB files from Korenix web site and compile all of them to the NMS. The Gateway supports function based MIB, the same function/parameters in all the models have the same object ID (OID). The benefit is you just need to compile the MIB file one time even you purchase different models. While you purchase our new released models in the future, the MIB file can be applied as well. Once we provide new features for the MIB, you just need one time effort to update the MIB table for all the models.

There are some MIB files which are:

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

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

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

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

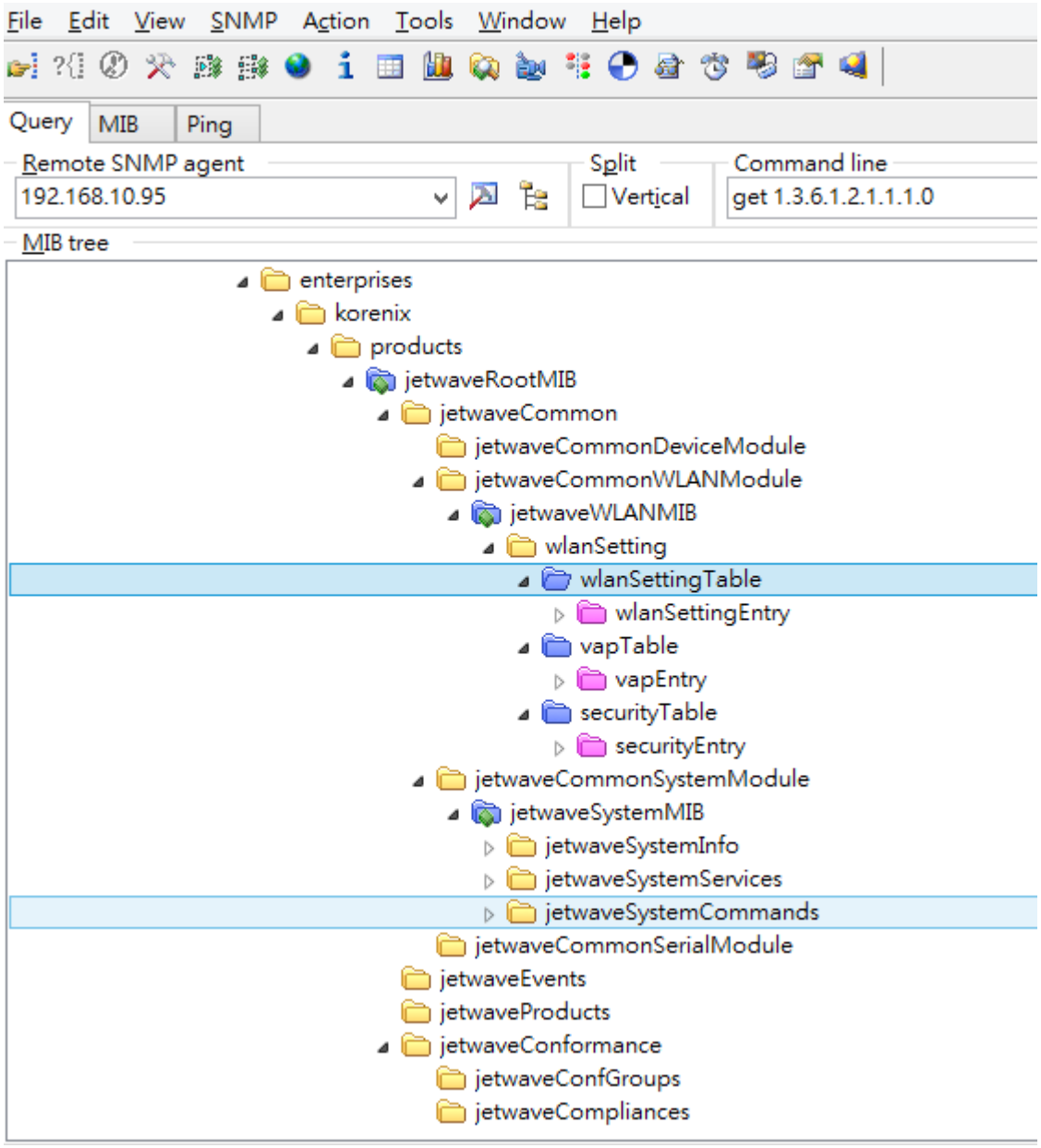
e. JETWAVE-SYSTEM-MIB.my: This is the JetWave System objects MIB.

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

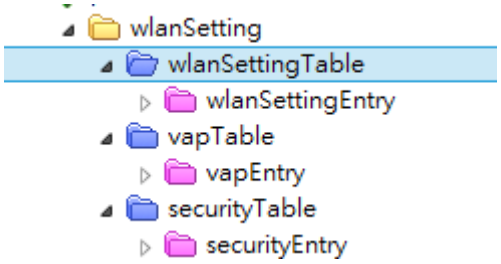
(Please download the latest MIB file from Korenix web site.)

5.1.3 MIB Tree in NMS

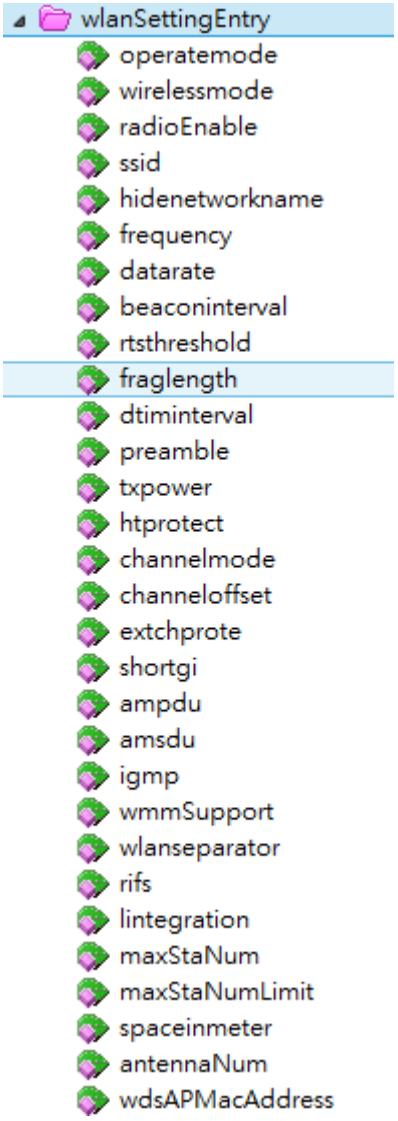
.The below figure shows the MIB tree after compiled in the NMS.



Example: wlanSetting



wlanSettingEntry:



Example of Object in wlanSettingEntry

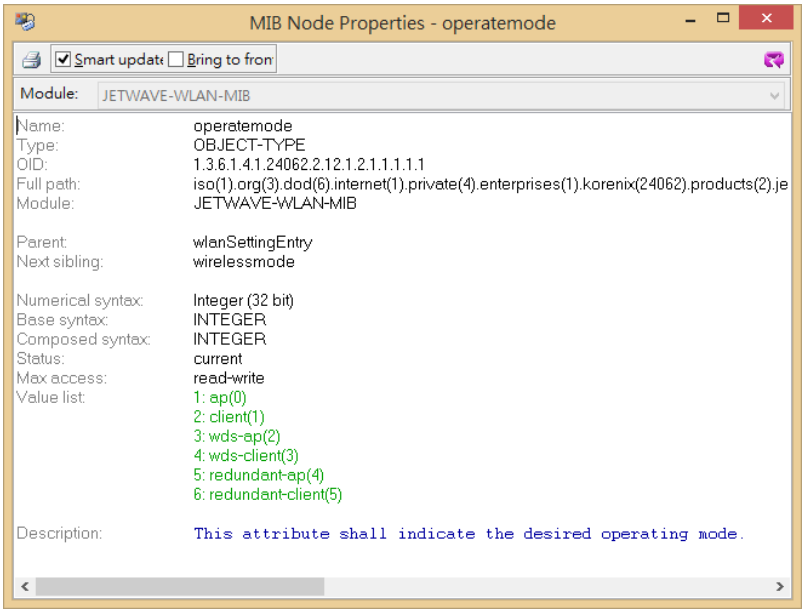
Operatemode: (Operation Mode)

The OID: 1.3.6.1.4.1.24062.2.12.1.1.1.1.1

Max Access: read-write

(Read and Write)

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



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

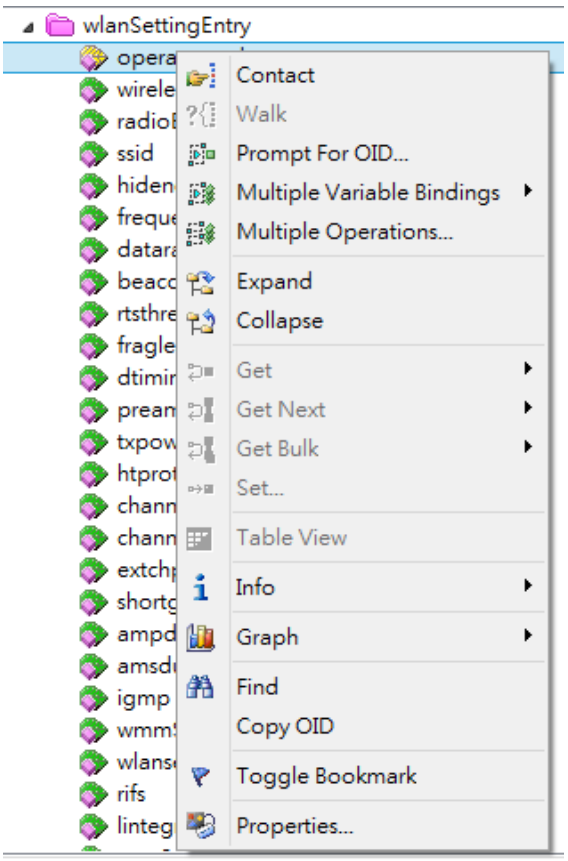
Get: Read the value of the selected OID.

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.

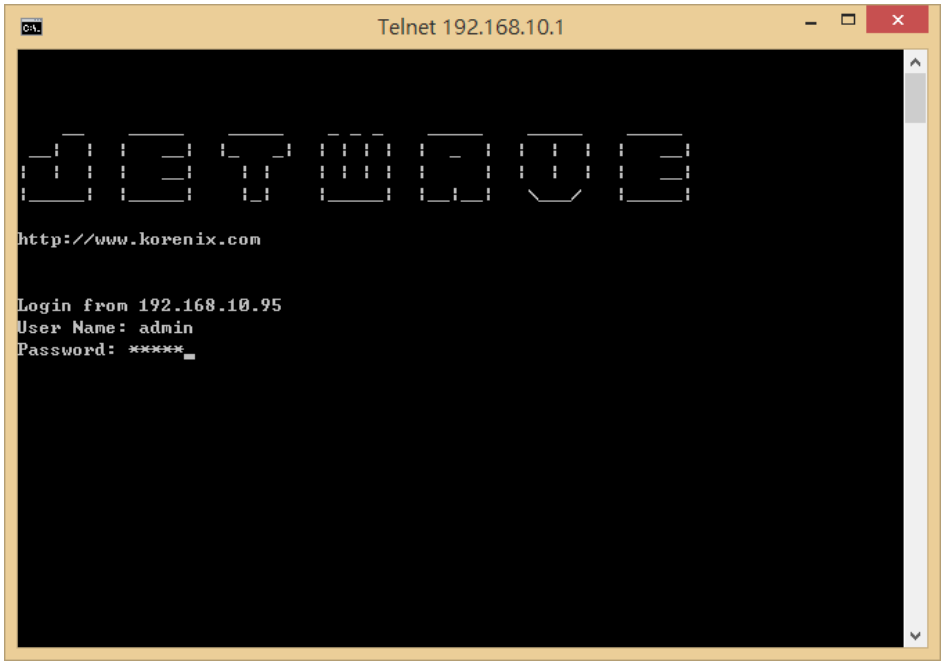
Property: See the MIB Node information.



5.2 Command Line Interface (CLI)

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

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



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 Gateway.

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

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

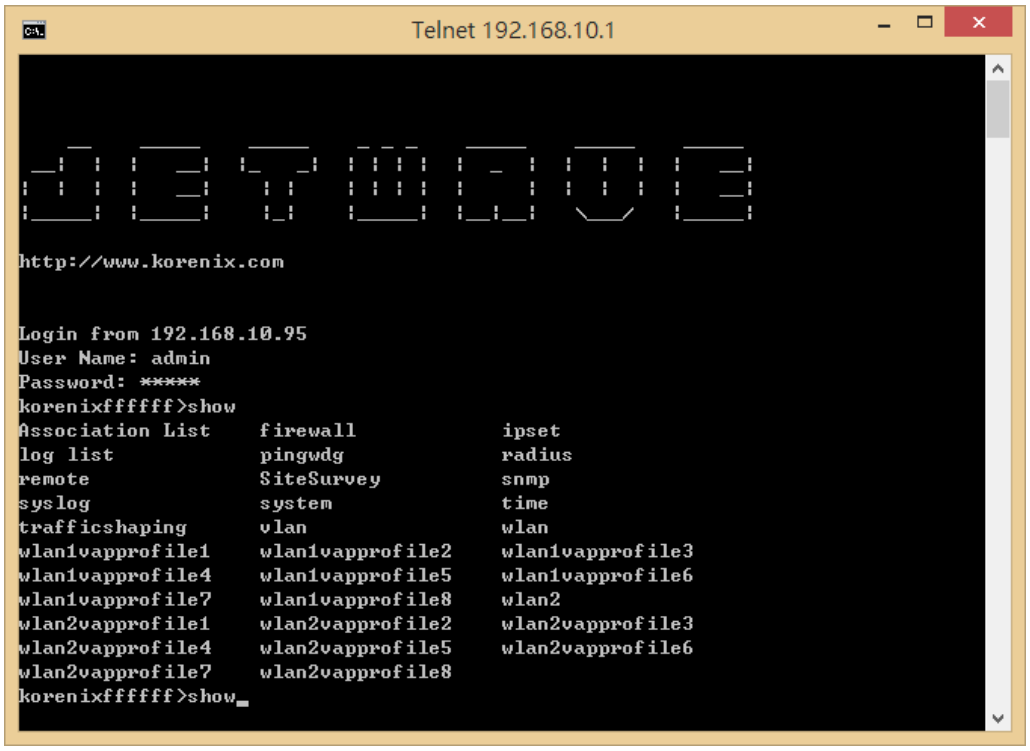
Del: This is Delete command to delete the applied settings.

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

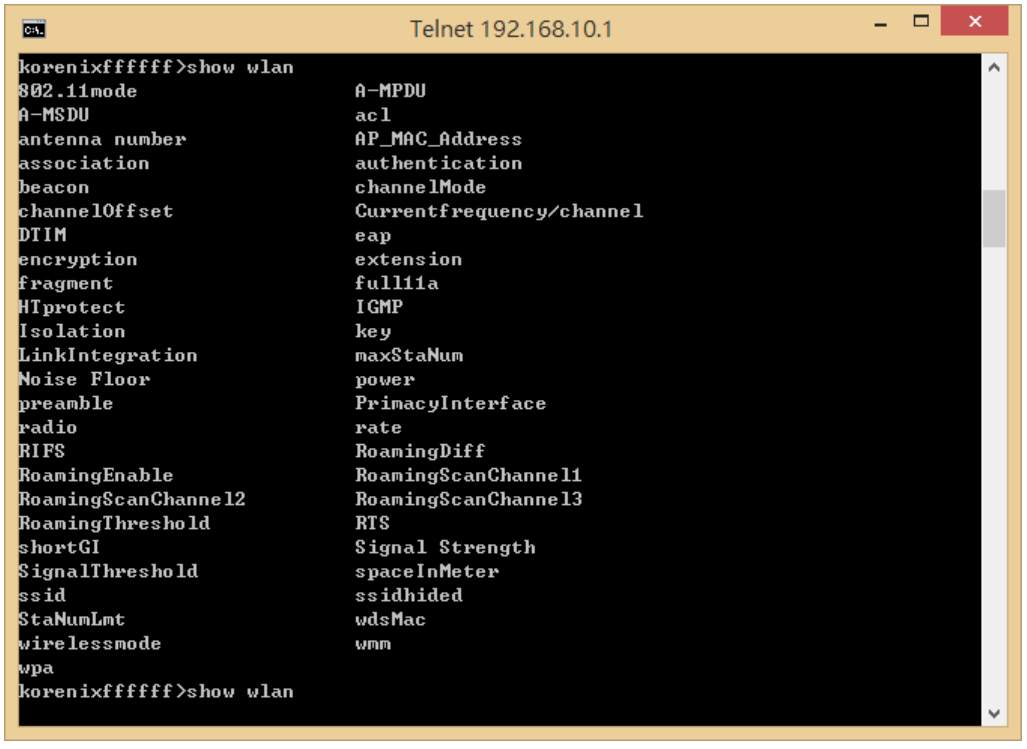
Note: Use **"Tab⇆"** key can help you find the correct command and complete the command no matter you want to Read or Write easier.

5.2.1 SHOW Command Set:

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



Type **Show wlan** + **"Tab⇆"** to see all the show wlan command lines.



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

```
korenixffffff>show wlan

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

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

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

korenixffffff>show wlan ra (+Tab)

radio rate

korenixffffff>show wlan rad (+Tab)

radio rate

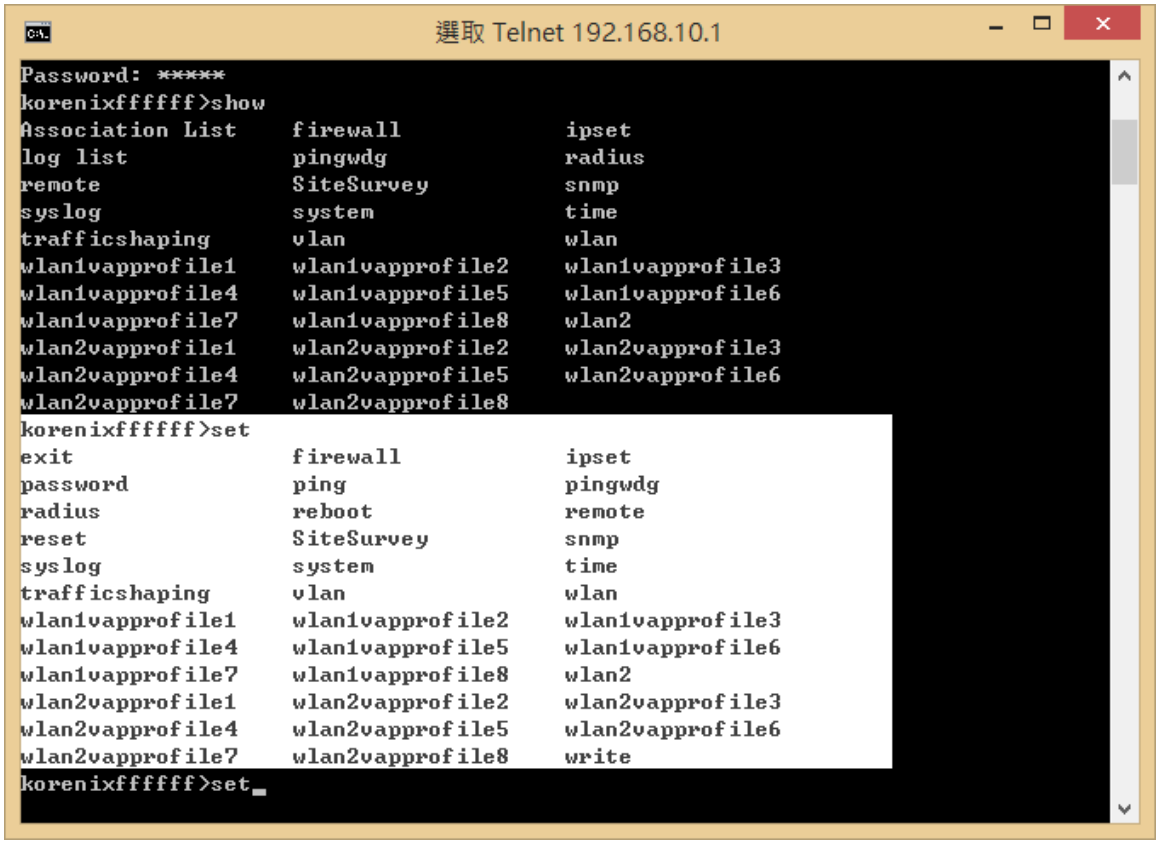
korenixffffff>show wlan radio (+ Enter)

wlan radio : Enabled (This is the result.)

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

5.2.2 Set Command Set:

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



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 Gateway supported. And the CLI is a different way for you to complete the setting.

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

```
korenixffffff>set remote (+Tab)
email alter      event warning    forcehttps       smtp
snmp             snmptrap         ssh              telnet
```

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

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

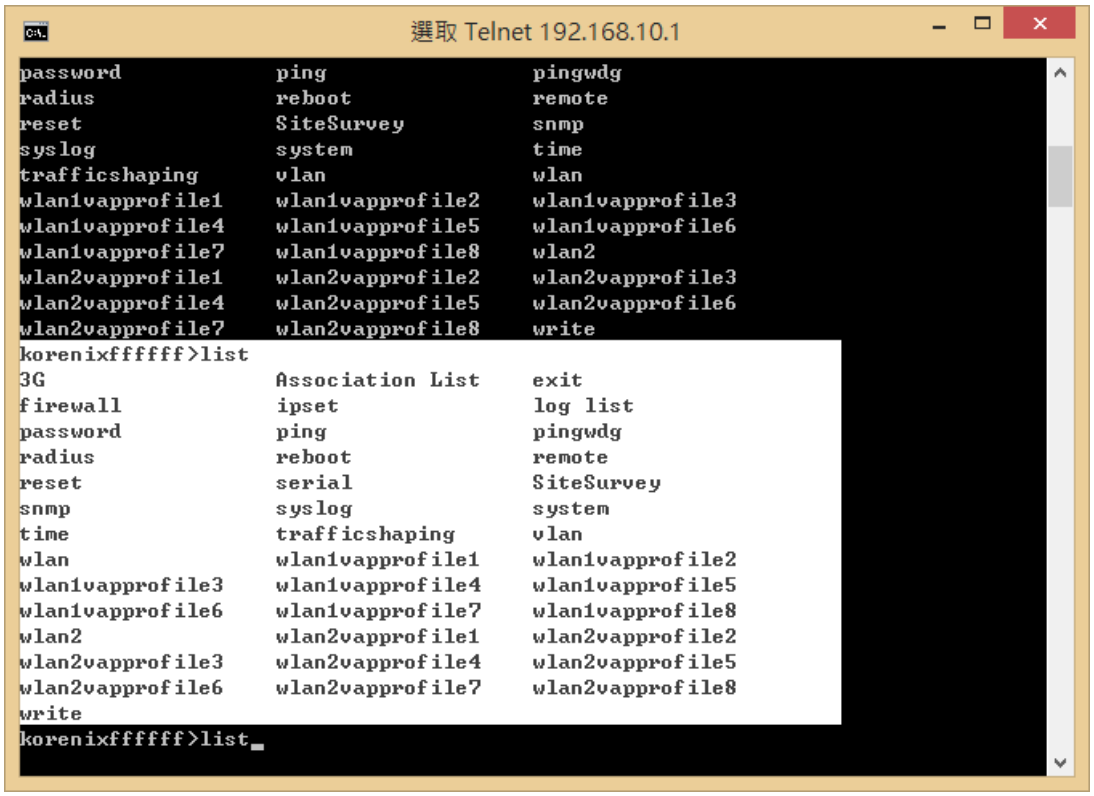
The SNMP command lines and how to set SNMP version, community name, trap server.

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

```
korenixffffff>set snmp version V2
snmp version                   : V2

korenixffffff>set snmp getCommunity orwell
snmp getCommunity              : orwell

korenixffffff>set snmp setCommunity orwell
snmp setCommunity              : orwell

korenixffffff>set snmp trapdestination 192.168.10.95
snmp trapdestination           : 192.168.10.95

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

5.2.3 List Command Set:

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



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

korenixffffff>list remote

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

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

Keyword: The command you should enter in the CLI.

Description: Short description of the usage of the command.

5.2.4 Delete Command Set:

Type **del** + **"Tab⇆"** to see all the delete command sets. The following command lines are available.

korenixffffff>del
log list remote wlan wlan2

The log list can be delete through CLI.
korenixffffff>del log list

The configured smtp email addresses can be delete through CLI.
korenixffffff>del remote smtp
email1 email2

The below wlan 1 settings can be delete through CLI. (JetWave 2111L/2411L)
korenixffffff>del wlan
acl eap key wpa

The below wlan 2 settings can be delete through CLI. (JetWave2111L/2411L)
korenixffffff>del wlan2
acl eap key wpa

5.3 Korenix View Utility

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

5.3.1 Device Discovery:

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

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

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

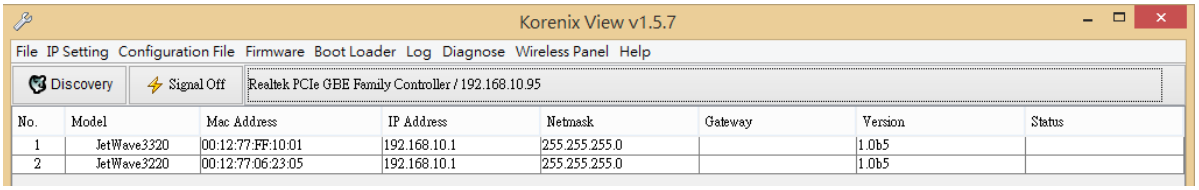
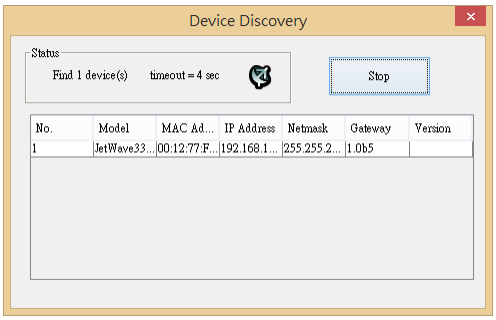


Figure: The main screen of the Korenix View Utility

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

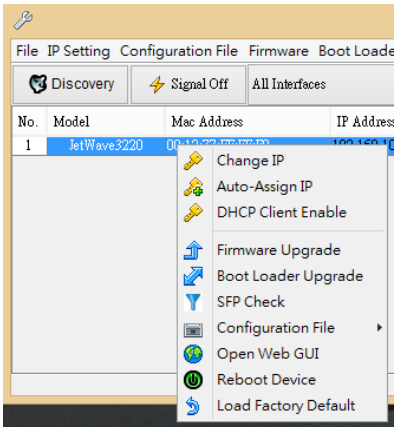


5.3.2 Basic Tools Shortcut:

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

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

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



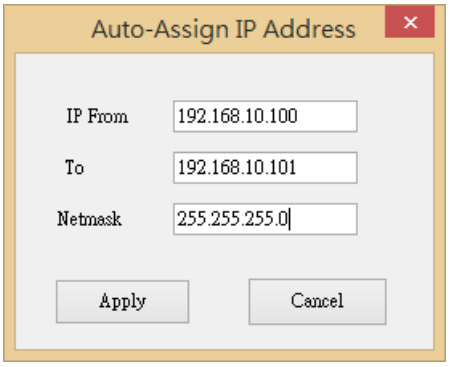
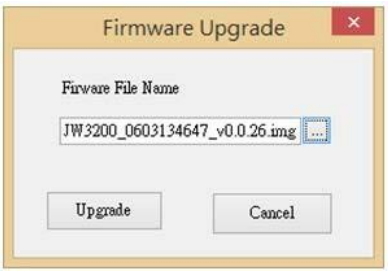


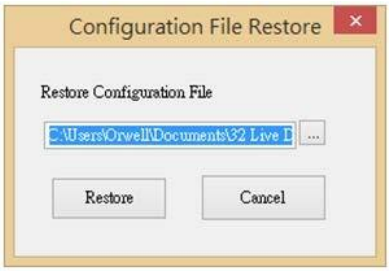
Figure: Assign the Auto-Assign IP Range.

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

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

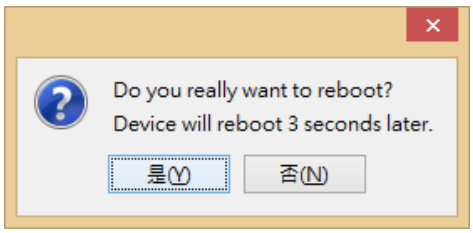
e. You can Backup/Restore the configuration file by “**Configuration File -> Backup/Restore”**. A popup screen will ask you select target configuration/target folder you’d like to backup or restore.



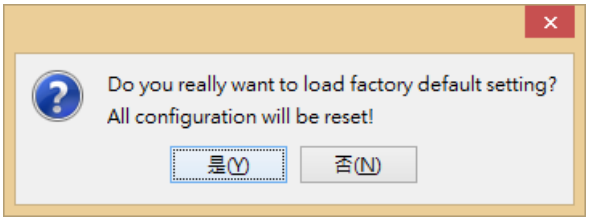


f. Click “**Open Web GUI**” to access the web management interface.

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



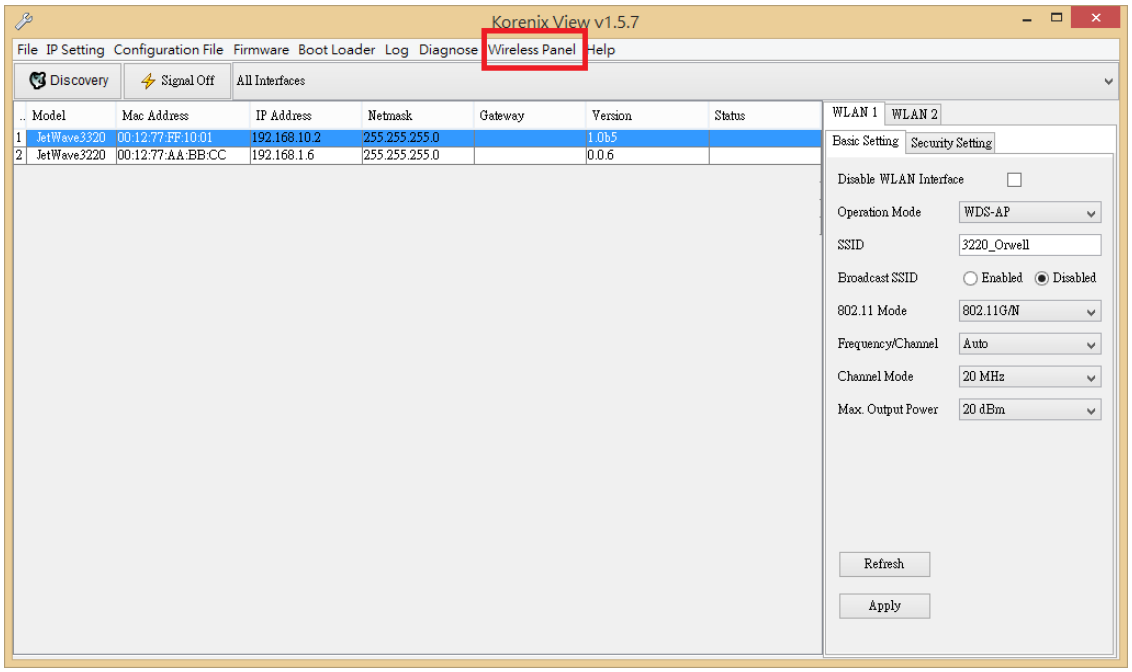
h. You can restore to default configuration by “**Load Factory Default**”. A popup screen will ask you confirm again.



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

5.3.3 Wireless Panel

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

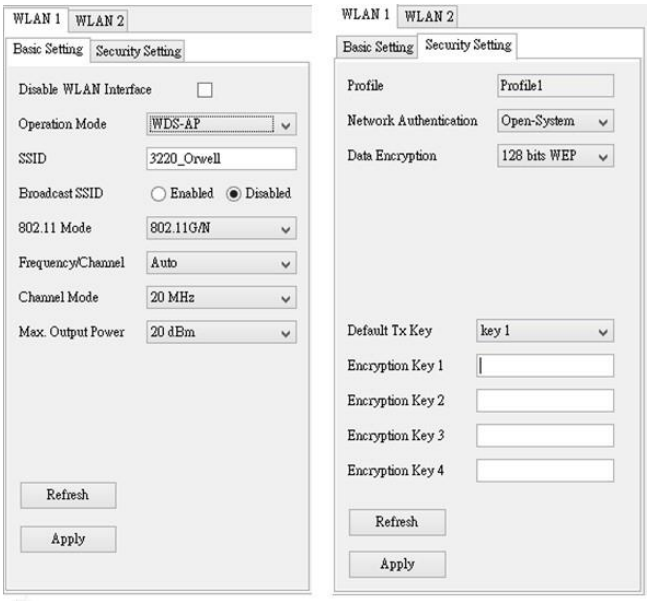


Click **"Refresh"** to load the current configuration of the selected Gateway.

5.3.4 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.



5.3.5 Security Setting:

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

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

Chapter 6

Troubleshooting

Chapter 6 Troubleshooting

This chapter provides troubleshooting procedures for basic problems with the JetWave 2111L/2411L.

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 Gateway?

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

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

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

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

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

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

Please check the followings:

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

6.2 Wireless/Cellular

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

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

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

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

6.2.3 What if the LTE connection is not stable or poor performance after associating with the base station?

- Please check the signal strength first. Once the signal strength is poor, the connection may be unstable. Even the connection is established, the performance is poor as well.
- You can move the device closed to the window or install external antenna outside the box/room/factory.
- If the distance between the Gateway and base station is far, the high gain antenna is an option to improve the transmission quality.

- Check whether the antenna supports LTE band or not? Normally, the outlook of the LTE antenna is the same.
- Check with the ISP and ask them check LTE connection condition of your site.
- Mark sure the SIM card has enough quota/budget for both data upload and download. Some out-of-quota/budget card is only available for Download stream only.
- Make sure the maximum LTE speed you applied from ISP. The remote connection will also reduce the performance. Make sure you have enough bandwidth from ISP.
- Download the screen message and debug message to our service engineer.
- Continuously ping one remote IP address through LTE connection for a while, once the ping is often timeout, check the status before leave the device on site.

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

- Make sure the SIM card is not damaged and you insert the SIM card before power on the device. Note: If the device supports LTE redundant, you MUST insert two SIM before power on the device.
- Make sure you insert the SIM card well, check the SIM status on Web GUI.
- Make sure the SIM card is available to support LTE connection. It is a simple way to insert it to smart phone for trail test.
- Mark sure the SIM card has enough quota/budget for both data upload and download. Some out-of-quota/budget card is only available for voice only.
- Make sure the SIM settings. For example the APN number, SIM security…etc. In some countries, the carrier service provider asks customer input the correct APN name first. The APN name may be different than its original setting. Please check the with your carrier service provider and type them correctly.
- Check whether the antenna supports LTE band or not? Normally, the outlook of the LTE antenna is the same.
- Download the screen message and debug message to our service engineer.

6.3 Appendix

6.3.1 ASCII

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

ASCII Table

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

Revision History

Version	Description	Date	Editor
V1.0	1st release for JetWave2111L/2411L 1.0	Nov, 2019	Andrew Chen