EKI-6311G

IEEE 802.11 b/g Wireless Access Point/Client Bridge
User Manual

ADVANTECH
eAutomation

Contents

Chapter 1. *Introduction*

1.1 Introducing the EKI-6311G

The EKI-6311G is fully interoperable with IEEE 802.11b/g compliant Wireless Last-mile product. The EKI-6311G operates in AP mode or remote bridge mode, and connects to EKI-6311G AP/CB to construct point-to-point as well as point-to-multipoint topologies, for maximum flexibility in configuring building-to-building networks and WISP functions.

1.2 Product Features

- Outdoor enclosure in compliance with versatile industrial IP（Ingress Protection） level covering IP65.
- RF transmit power 802.11b mode @ 11Mbps data rate.
- RF transmit power 802.11g mode @ 54Mbps data rate.
- IEEE 802.3 af Power over Ethernet (PoE) support
- WEP/WPA/WPA2/ IEEE 802.1x authenticator support.
- WDS (Wireless Distribution System)
- Multi-SSID (up to 4 SSID) support
- MAC address based access control

Hint: IP（Ingress Protection）

1.3 Package Contents

The product package contains the following items.

1. One (1) EKI-6311G Outdoor Wireless Access Point / Client Bridge unit
2. One (1) 100~240VAC, 50~60Hz AC to 48V/0.375A DC switching adapter
3. One (1) 48VDC, 0.375A Inline Power Injector (PoE)
4. One (1) 1.8m grounding wire (Optional)
5. One (1) User manual CD-disc
6. One (1) wall/mast mounting kit
7. One (1) band clamp

1.4 System Requirements

Installation of the EKI-6311G Outdoor Wireless Access Point/Client Bridge requires the following:

1. A Windows-based PC/AT compatible computer（PC system requirement：better than PIII 800 or other 100% compatible equipment , OS：windows 2000/XP ） or Ethernet data device with an available RJ-45 Ethernet port to run the configuration program or with TCP/IP connection to the Ethernet network.
2. A 10/100Base-T Ethernet RJ-45 Ethernet cable is connected to Ethernet network.
3. An AC power outlet (100~240V, 50~60Hz) supplies the power.

1.5 Inline Power Injector (PoE)

The EKI-6311G is equipped with an Inline Power Injector module. The Inline Power Injector (PoE) delivers both data and power to EKI-6311G unit via a signal Ethernet cable, and gives the following benefits to improve the performance vs. installation cost ratio.

- This unit works great in areas where you may not have power , like house roof.
- This also allows you to place the EKI-6311G unit closer to the antenna, to make installation easier more thus reducing signal loss over antenna cabling.
- Ethernet signal travels well over CAT 5 cable but 2.4GHz signal doesn't do as well over antenna cabling.
- Ethernet cabling is much cheaper than Antenna cabling.

Chapter 2. *Installation and Basic Configuration*

This chapter describes the procedures of installing the EKI-6311G.

2.1 Before You Start

After unpacking the system, make sure the following items are present and in good condition. Refer to below pictures for product image.

1. EKI-6311G Outdoor Wireless Access Point/Client Bridge unit
2. 100~240VAC, 50~60Hz AC to 48V/0.375A DC switching adapter
3. Inline Power Injector (PoE) 48VDC, 0.375A
4. Grounding wire 1.8m
5. User manual CD-disc
6. Wall/mast mounting kit, including one (1) band clamp
7. Screws
8. 5dBi Oimi-type Antenna
9. RJ-45 cable waterproof cap

1. Unit	2. Adapter	3. PoE	4. Grounding wire
			
5. CD	6. Wall mount	7. Screws	8. Antenna(for AP)
			
9. RJ-45 cable waterproof cap			
			

2.2 Locate the EKI-6311G and Inline Power Injector Ports

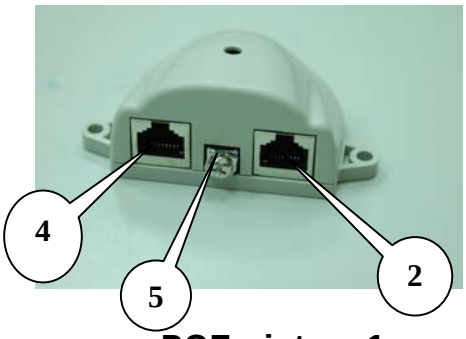
► **Interface on the EKI-6311G Unit**

- **Ethernet Port** 1 : for connecting the RJ-45 CAT-5 Ethernet cable.

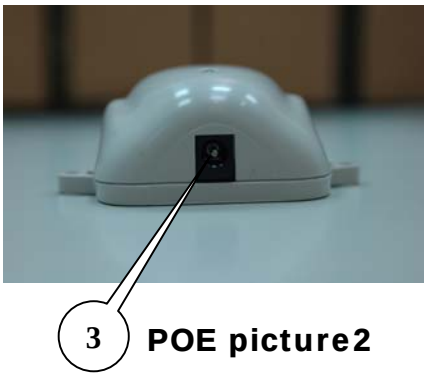
► **Interface on the Inline Power Injector**

- **Data Input Port** 2 : for connecting cross-over Ethernet Cable to PC or straight Ethernet cable to Hub Switch Router .
- **DC Input Port** 3 : power adapter 48V, 0.375A DC input.
- **Power & Data Output Port** 4 : for connecting the RJ-45 CAT-5 Ethernet Cable.
- **Grounding Port** 5 : for connecting grounding wire.

Device



POE picture1



POE picture2

Figure 2-1
Power and Data Interface location on the PoE denoted by numbers 1-6.

► Mount EKI-6311G on A Wall/Mast

The EKI-6311G can be mounted on the wall, you can use the Wall Mount kit to mount the EKI-6311G as shown in **Figure 2-2**.

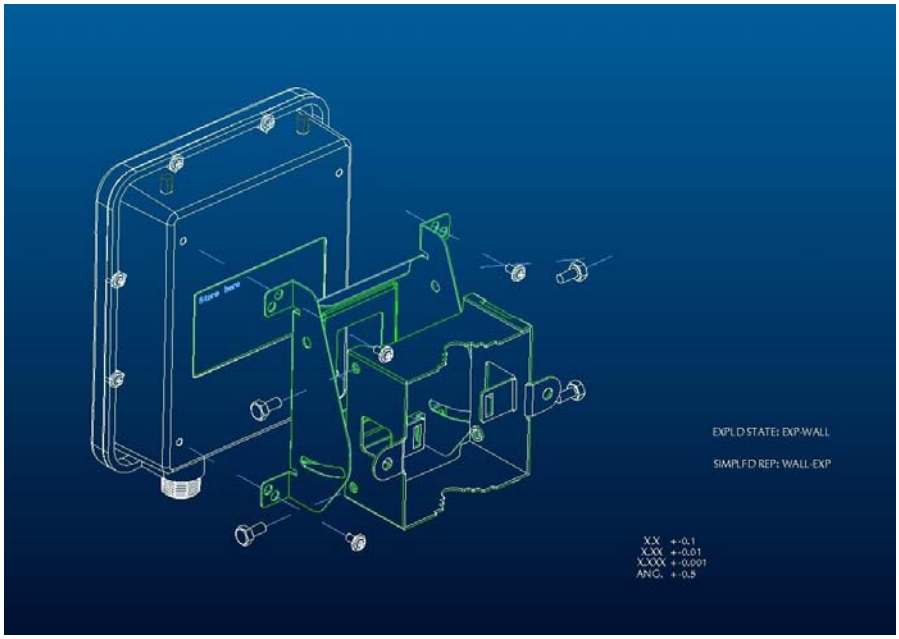


Figure 2-2

You can also mount the EKI-6311G to the mast as shown in **Figure 2-3**.

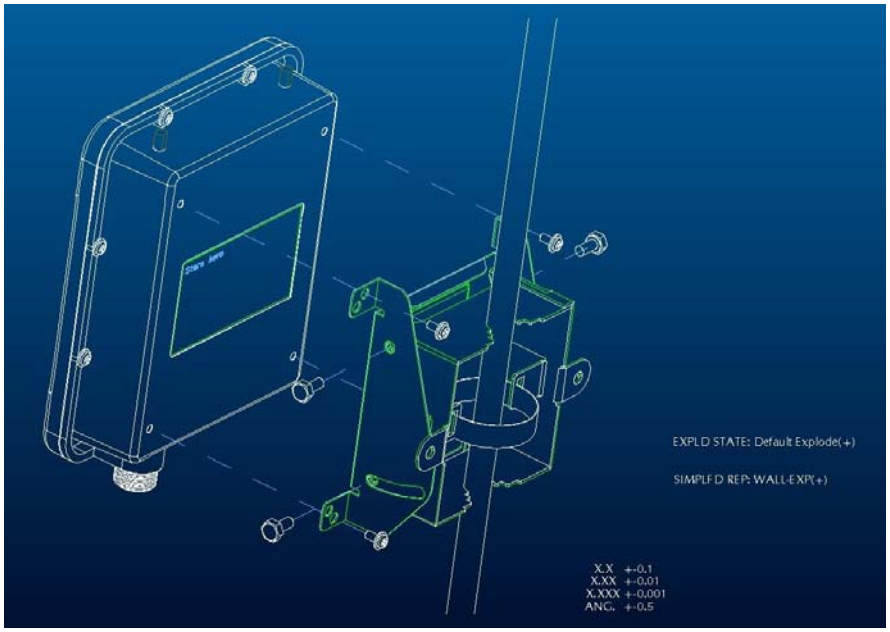


Figure 2-3

2.3 Preparing Installation

Before installing EKI-6311G for outdoor application or hard-to-reach location, we recommend configuring and test all the devices first.

For configuring the EKI-6311G, please follow the quick steps below to power up the EKI-6311G. Refer to **Figure 2-4** for steps 1 through 5.

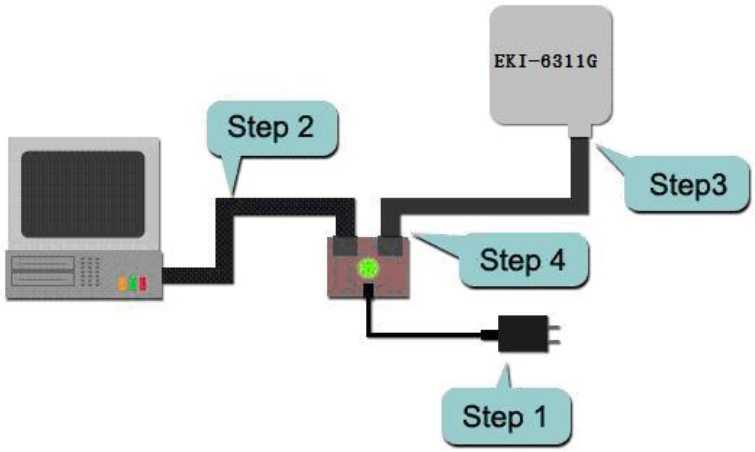


Figure 2-4

Step1 : Connect the DC plug of the AC/DC power adapter into the **DC Input Port** of Inline Power Injector and the wall-mount plug into a power outlet or power strip (refer to **page 6**). The Power LED on the Inline Power Injector will light up.

Step2 : Run the cross-over type uplink Ethernet cable from **Data Input Port** (refer to**page 6**) to the Ethernet port on a PC.

Step3 : Connect the 30m CAT 5 Ethernet cable into the EKI-6311G unit. Hand tighten the connector.

Step4 : Connect the remaining end of the 30m CAT 5 cable into the PoE labeled AP/Bridge. This is the power side of the PoE that will power up the EKI-6311G.

When the EKI-6311G receives power over the Ethernet cable, the EKI-6311G will start its boot up sequence and the **Active** LED on the Inline Power Injector will light up.

You can configure the EKI-6311G via HTML browser, such as Microsoft Internet Explorer or Netscape Navigator from a remote host or PC.

2.4 Basic Configuration

2.4.1 Basic Configuration Steps

This section describes a two-step SYSTEM configuration procedure to setup EKI-6311G.

Step1 : Modify the factory-default parameters on the web page "**/Network/Network/**", and click **APPLY** to save the changes.

Step2 : Modify the factory-default parameters on the web page "**/WIRELESS/Wi-Fi 1**", and click **APPLY** to save the changes, than click "**/SYSTEM/Reboot/**"**Reboot** to take effect on the previous configuration changes.

2.4.2 Logging into the Web Interface

The EKI-6311G supports access to the configuration system through the use of an HTTP Interface.

► **Web Configuration**

Before configuring EKI-6311G, the user needs to know the IP Address assigned to the unit. When shipped from the factory, the IP Address **192.168.1.1** was assigned to the EKI-6311G by default. **To start a web connection, use http://192.168.1.1**

► **Web Access Procedures**

Once you identify the IP Address assigned to EKI-6311G, use web browser to configure EKI-6311G through the HTTP Interface. The following procedure explains how to configure each item.

Step1 : Open your browser and enter the IP Address

Step2 : Press <**ENTER**> key and the EKI-6311G **Login** screen appears as shown in **Figure 2-5**.

Figure 2-5

Step3 : Enter "**admin**" in the **Username** and **Password** fields, and click **LOGIN** to enter the web configuration user interface screen as shown below.

Figure 2-6

► Web Configuration Structure

The web configuration user interface shown above in **Figure 2-6** is grouped into a tree structure, and contains the following settings or information.

▽ SYSTEM

- Administrator
- Firmware
- Configuration
- Status

- Log
- System Time
- Reboot

▽ NETWORK
- Network
- HotSpot

▽ WIRELESS
- Wi-fi 1
- Wi-fi 2
- Wi-fi 3
- Wi-fi 4

▽ ACL
- ACL for Wi-fi 1
- ACL for Wi-fi 2
- ACL for Wi-fi 3
- ACL for Wi-fi 4

▽ SNMP
- Agent Settings

▽ EXIT

Move through the tree by clicking on an icon to expand or collapse the tree. The nodes on the tree represent web pages that allow viewing and modifying the parameters.

2.4.3 Set Operating Mode, IP Address, Subnet Mask, Default Route IP, DNS Server IP of EKI-6311G

► LAN Settings

These are the settings of the LAN (Local Area Network) interface for the Access Point. The Access Point's local network (LAN) settings are configured based on the IP Address and Subnet Mask assigned in this section. The IP address is also used to access this Web-based management interface. This option is available in the "/**NETWORK/ NETWORK /**" page as shown in **Figure 2-7**.

Figure 2-7

► Get LAN IP From

Choose "DHCP (Dynamic)" if your router supports DHCP and you want the router to assign an IP address to the AP. In this case, you do not need to fill in the following fields. Choose "Static IP (Manual)" if your router does not support DHCP or if for any other reason you need to assign a fixed address to the AP. In this case, you must also configure the following fields.

Note that you cannot choose "DHCP (Dynamic)" if you have enabled the "DHCP Server" option on the DHCP page; the AP cannot be both a DHCP client and a DHCP server.

► IP Address

The IP address of the AP on the local area network. Assign any unused IP address in the range of IP addresses available for the LAN. For example, 192.168.1.1.

► Subnet Mask

The subnet mask of the local area network.

► Gateway

The IP address of the router on the local area network.

► DNS Server

This entry is optional. Enter a DNS Server for the local network.

2.4.4 Set Wireless SSID for Wireless Interface

► Wireless Network Name （Also called the SSID）

When you are browsing for available wireless networks, this is the name that will appear in the list (unless Visibility Status is set to Invisible, see below). This name is also referred to as the SSID. For security purposes, it is highly recommended to change from the pre-configured network name. This option is available in the "**/WIRELESS/Wi-Fi 1/**" page as shown in **Figure 2-8**

****Default SSID: "Advantech/1" in wifi-1.**

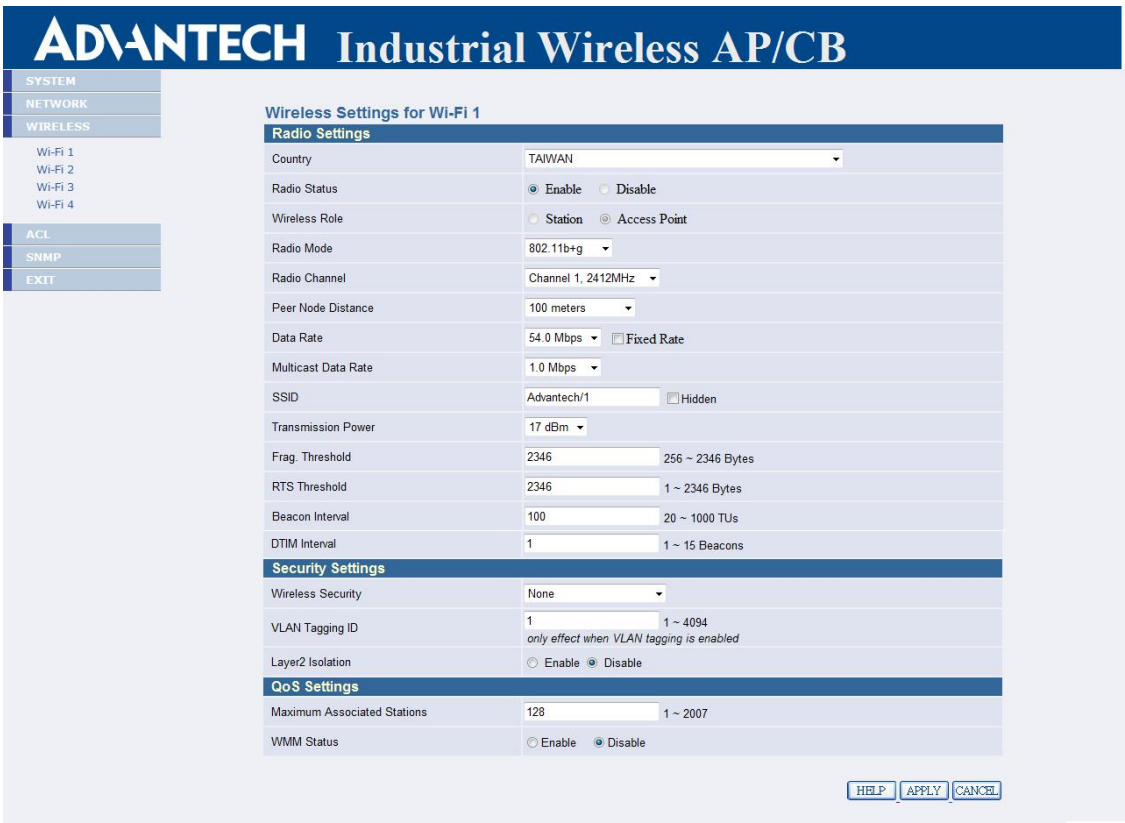


Figure 2-8

2.4.5 Set Wireless Encryption for Wireless Interface

The EKI-6311G supports 64-bit and 128-bit WEP encryption.

For **64-bit** WEP encryption, an encryption key is 10 hexadecimal characters (0-9 and A-F) or 5 ASCII characters.

For **128-bit** WEP encryption, an encryption key is 26 hexadecimal characters or 13 ASCII characters.

Modify the WEP encryption parameters on the web page "**/WIRELESS/Wi-Fi 1 SECURITY** ". Choice "WEP" Enter 1~15 characters into the **WEP Key** field, than click **Apply** , "**/SYSTEM/Reboot** "**Reboot**. page as shown in **Figure 2-9**

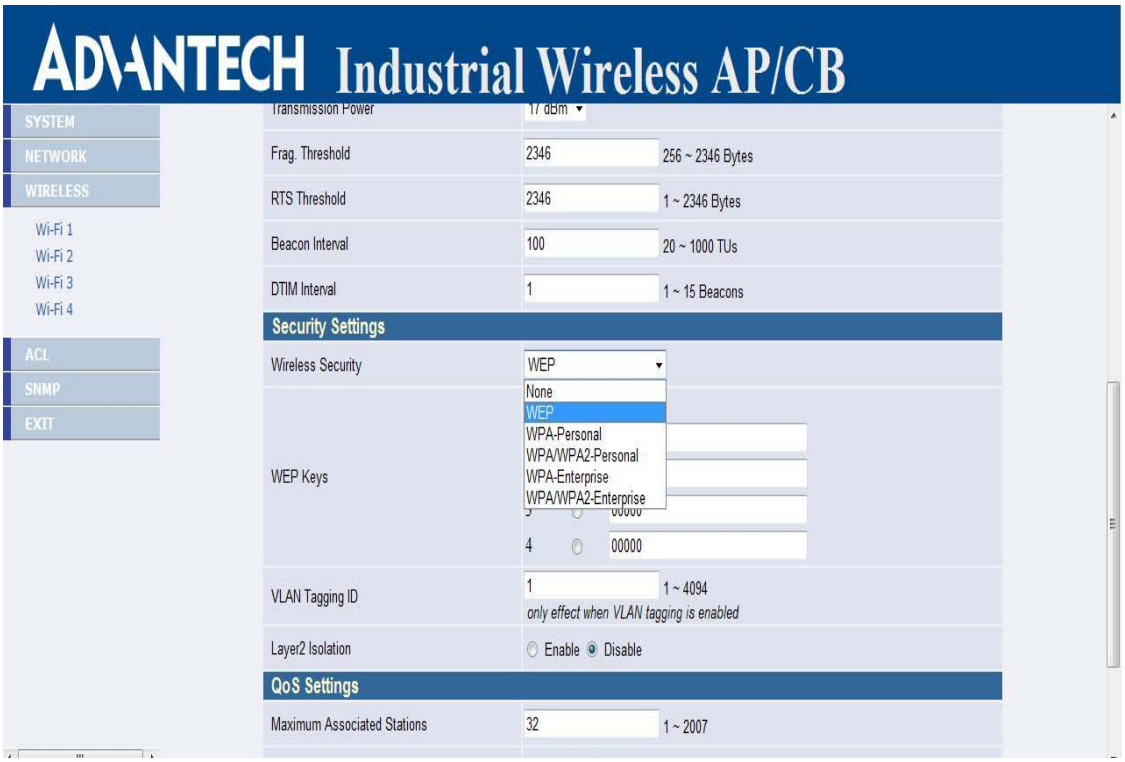


Figure 2-9

2.4.6 Change Supervisor Account & Password

Enter the **SYSTEM** > **Administrator** page. **Figure 2-10** below shows the **SYSTEM / Administrator** page.

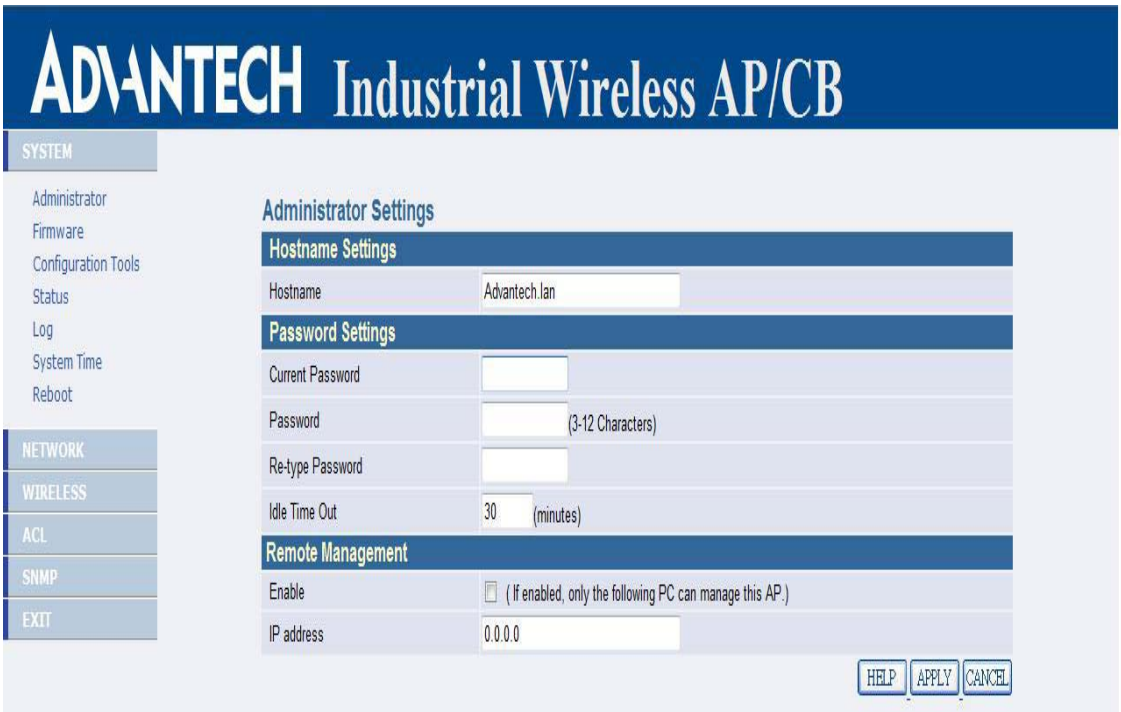


Figure 2-10

► **ADMIN PASSWORD**

Key in current password in the **SYSTEM / Administrator / Password Setting Current Password** field. Change the ADMIN PASSWORD's password in the **SYSTEM / Administrator Password Setting Password and Re-type Password** fields, and click **APPLY** ，than，"**/SYSTEM/Reboot** "**Reboot**.

2.4.7 Upgrade the Firmware

► Update the Firmware

Enter the **SYSTEM** > **FIRMWARE** page as shown in **Figure 2-11** to upgrade EKI-6311G. Here, user must select which file you want to upgrade it (**Program image**), then click **APPLY** button to start the upgrade process.

Hint: When choose "using web" for updating, choose the image file for updating directly. Do not unzip the image file.
i.e. Image file name: "Advantech-V 2.0.4.tgz"

Hint: It takes about 10 min, to complete the restart process.

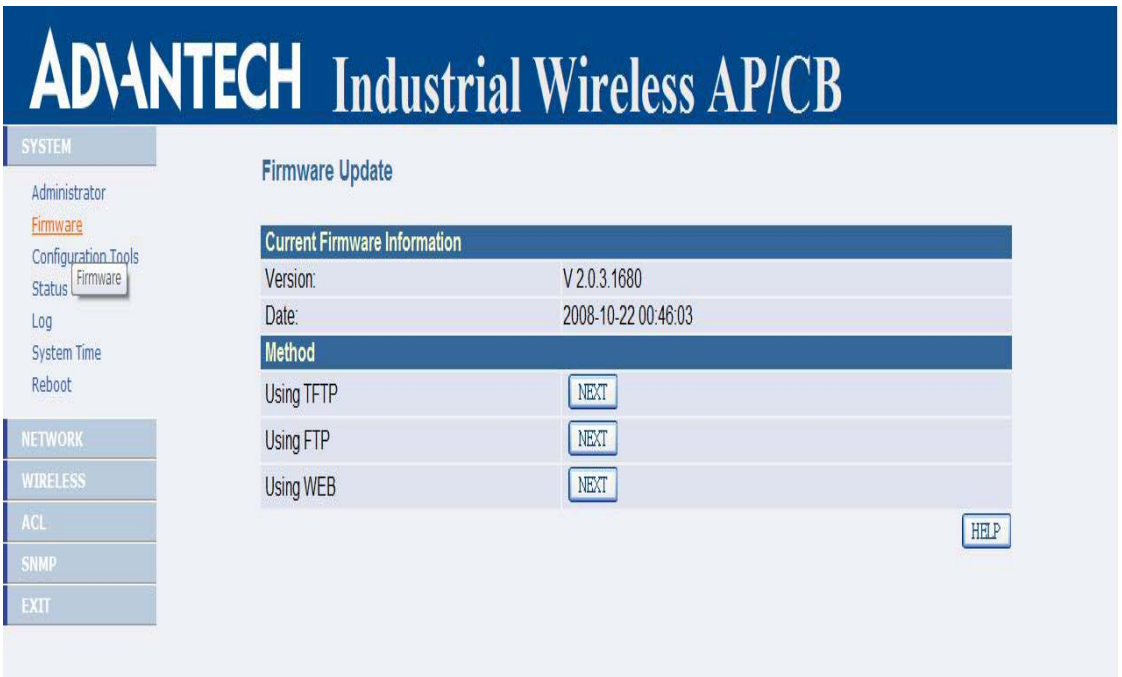


Figure 2-11

2.4.8 DHCP server

► DHCP server

Enter the **Network** > **Network** page as shown in **Figure 2-12** to **Enable** the DHCP server. Here, user can set **IP Pool Address range**, lease time and Local domain name. Then click **APPLY** button to set the parameter and click **Reboot** button for saving parameter.

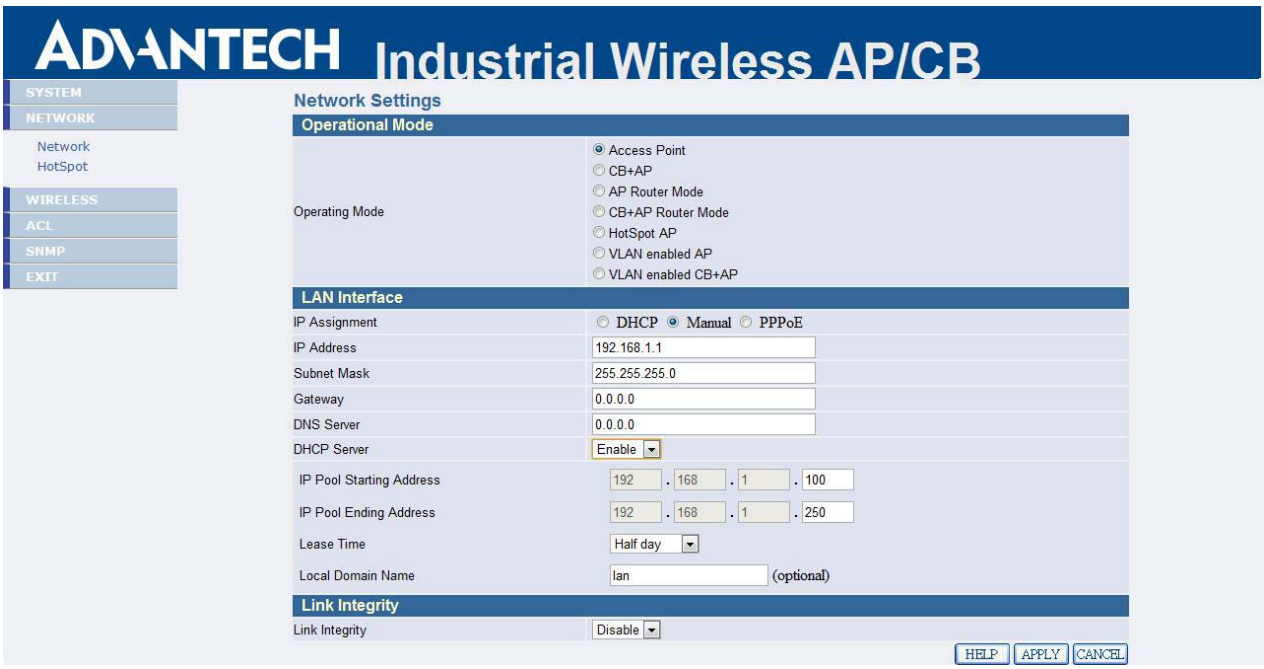


Figure 2-12

> ⚠ **Caution** The Part 15 radio device operates on a non-interference basis with other devices operating at this frequency when using integrated antennas. Any changes or modification to the product not expressly approved by Original Manufacture could void the user's authority to operate this device.

> ⚠ **Caution** To meet regulatory restrictions and the safety of the installation, strongly recommends this product to be **professionally installed**.

Chapter 3. *Network Topologies*

This chapter describes several common types of installations implemented by using the EKI-6311G's line of Outdoor Wireless System. This is by no means intended to be an exhaustive list of all possible configurations, but rather shows examples of some of the more common implementations. The EKI-6311G CB can be configured to function as a Wireless Client Router or Bridge to a central access point like the EKI-6311G AP see Figure 3-1 below.

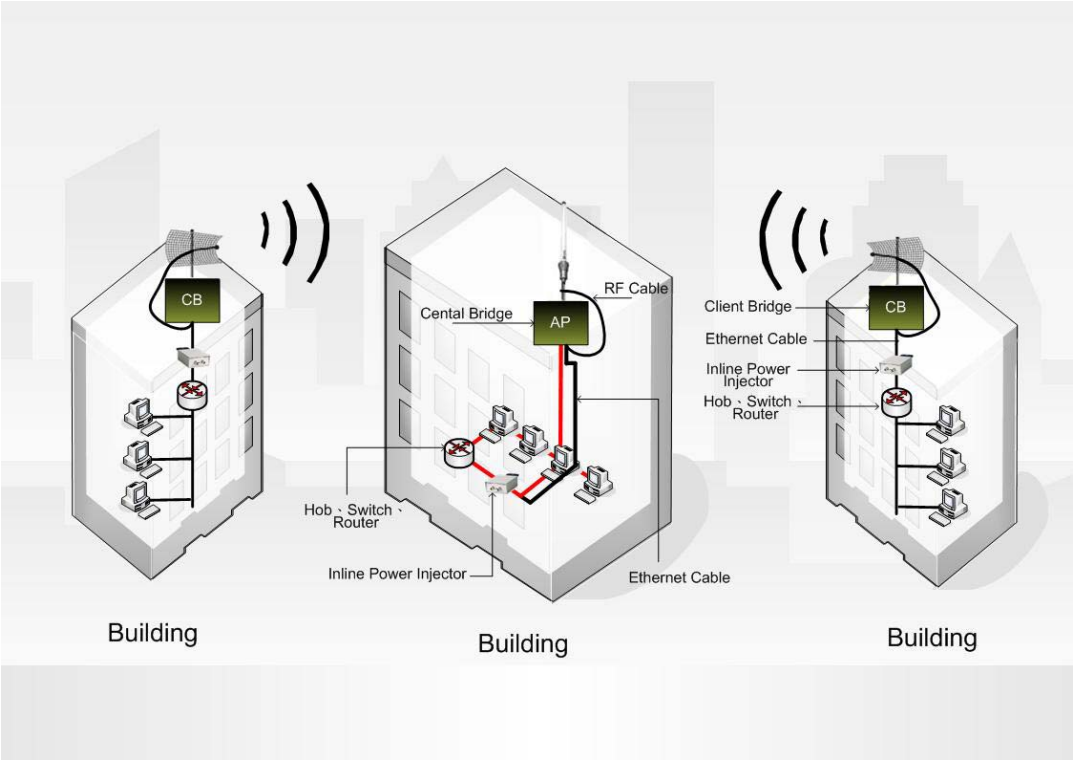


Figure 3-1

The EKI-6311G CB performs in either router or bridge mode. In a Point-to-Multipoint topology, all communication between network systems is done through a centralized agent. Among the EKI-6311G Outdoor Wireless Bridge products, the centralized agent is Central Bridge (EKI-6311G AP) and the individual network notes may be Bridge (EKI-6311G CB).

To show the available Point-to-Multipoint topologies, the following examples are provided.

Wireless Client Bridge-to-Central Wireless Bridge

3.1 Wireless Client Bridge-to-Central Wireless Bridge

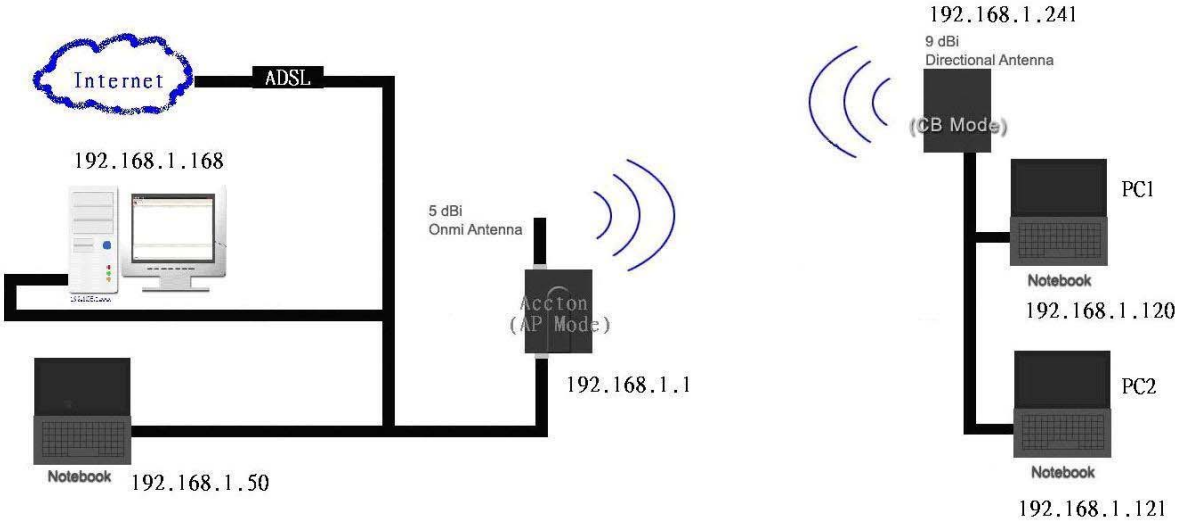


Figure 3-2

Refer to Figure 3-2 for the following setup.

Note: The EKI-6311G AP is the Central Wireless Bridge and EKI-6311G CB is the Wireless Client Bridge

Step 1 Set the EKI-6311G AP to perform a bridge (**bridge IP address: 192.168.1.1**).

Step 2 Set Wireless parameters on the AP to: **Channel (1)** and **SSID (wireless)**

Step 3 Set the EKI-6311G CB to function in the bridge mode (**bridge IP address: 192.168.1.241**).

Step 4 Set Wireless parameters on the EKI-6311G CB to: **Channel (1)** and **SSID (wireless)**, and these parameters must be the same with COU.

Step 5 Left side subnet is transparent to the right side.

Step 6 DHCP server assign IP address to PC1 and PC2

Chapter 4. *All function on Device*

4.1 SYSTEM

4.1.1 Administrator

Administrator Settings
Use this menu to restrict management access based on a specific password. The default password comes with the installation guide. Please change this password as soon as possible, and store it in a safe place. Passwords can contain from 3-12 alphanumeric characters,and are case sensitive.

Figure 4-1

Administrator Time-out
The amount of time of inactivity allowed before the user proceeds next action. The user needs to re-login if the idle time passes timeout.

Remote Management
By default, management access is only available to users on your local network. However, you can also manage the Wireless device from a remote host. Just check the **Enable** box and enter the IP address of an administrator to this screen.

4.1.2 Firmware

Figure 4-2

Firmware Update – WEB

You can use WEB to upgrade the firmware. The "firmware information" displays current firmware version and firmware date. On the managed computer, specify the folder in which the firmware file resides. Click **APPLY** to complete your change. At the end of the upgrade, the Wireless device may not respond to commands for as long as ten minute. This is normal behavior and do not turn off the Wireless device during the time.

Hint: When choose "using web" for updating, choose the image file for updating directly. Do not unzip the image file.
i.e. Image file name: "Advantech-V 2.0.4.tgz"

Hint: It takes about 10 min, to complete the restart process.

Firmware Update - TFTP

You can use TFTP to upgrade the firmware. The "firmware information" displays current firmware version and firmware date. On the managed computer, run the TFTP Server utility. And specify the folder in which the firmware file resides. After running the TFTP server, enter the TFTP server IP and the filename. Click **APPLY** to complete your change. At the end of the upgrade, the Wireless device may not

respond to commands for as long as ten minute. This is normal behavior and do not turn off the Wireless device during the time.

Firmware Update - FTP

You can use FTP to upgrade the firmware. The "firmware information" displays current firmware version and firmware date. Enter FTP Server IP , Type the correct firmware file path and file name on the File field. Keyin the current FTP Username and Password . Click on **APPLY** to complete your change. At the end of the upgrade, the Wireless device may not respond to commands for as long as ten minute. This is normal behavior and do not turn off the Wireless device during the time.

4.1.3 Configuration Tools

Figure 4-3

Restore Factory Defaults - Reset the device's configuration settings to the factory default values. Check the "Restore Factory Default Configuration" radio button then click on **APPLY** button.
Backup settings / Restore settings - Check the "Backup settings/Restore settings" radio button then click on **APPLY** button.
Backup Settings - Press the "Backup Settings" button to save the settings of this device to a file named "config.bin" on your PC.
Restore Settings - Restore the settings of this device to the backup settings. Enter the path and name of the backup file then press the "Restore Settings" button. You will be prompted to confirm the backup restoration.

4.1.4 Status

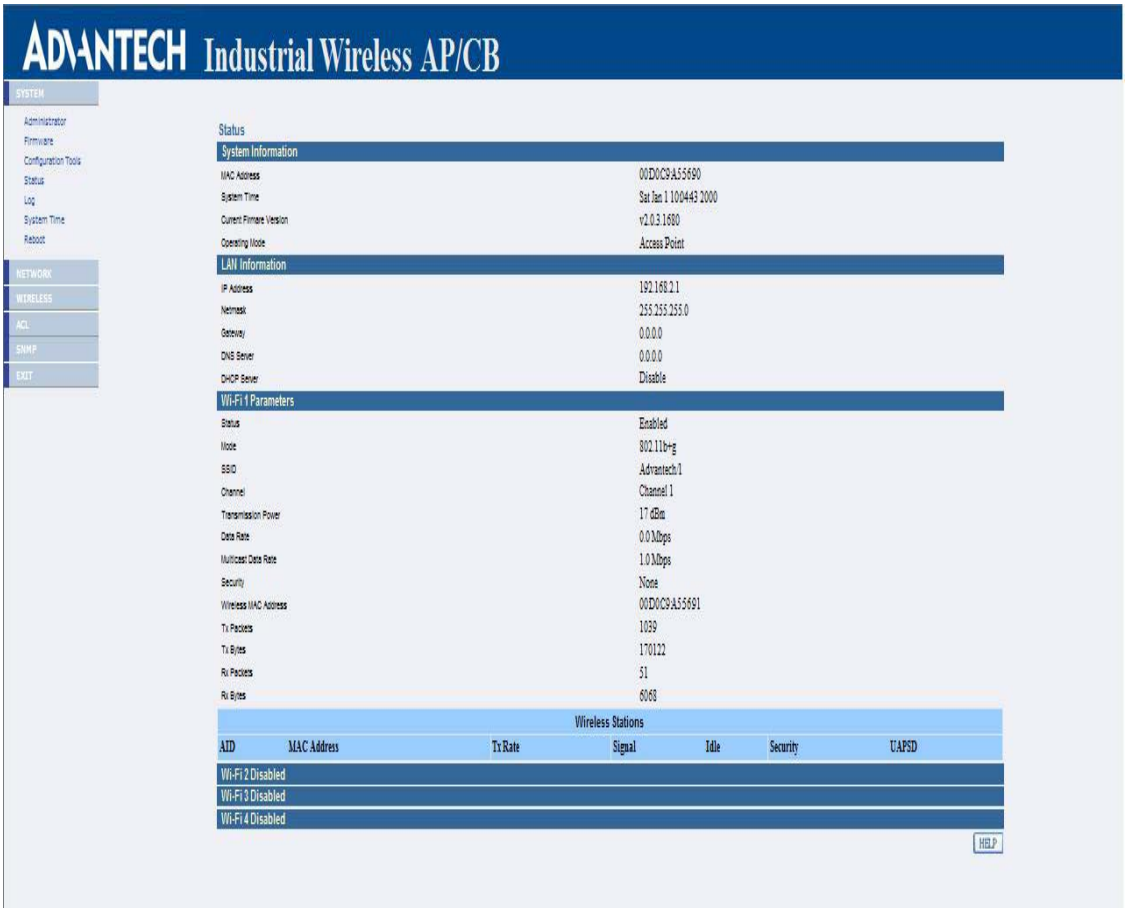


Figure 4-4

You can use the Status screen to see the connection status for the LAN and Wireless LAN interfaces. It also displays system up time and firmware version.

The following items are included in this screen:

WAN INFORMATION - Displays IP settings of WAN port, including IP Address, Subnet Mask, and Gateway.
LAN INFORMATION - Displays IP settings of LAN port, including IP Address and Subnet Mask.
WIRELESS INFORMATION - Displays wireless information, including SSID, channel, Security status, and MAC address.
SYSTEM INFORMATION - Displays the systemup time, the Wireless device's firmware version, and the serial number.

4.1.5 Log

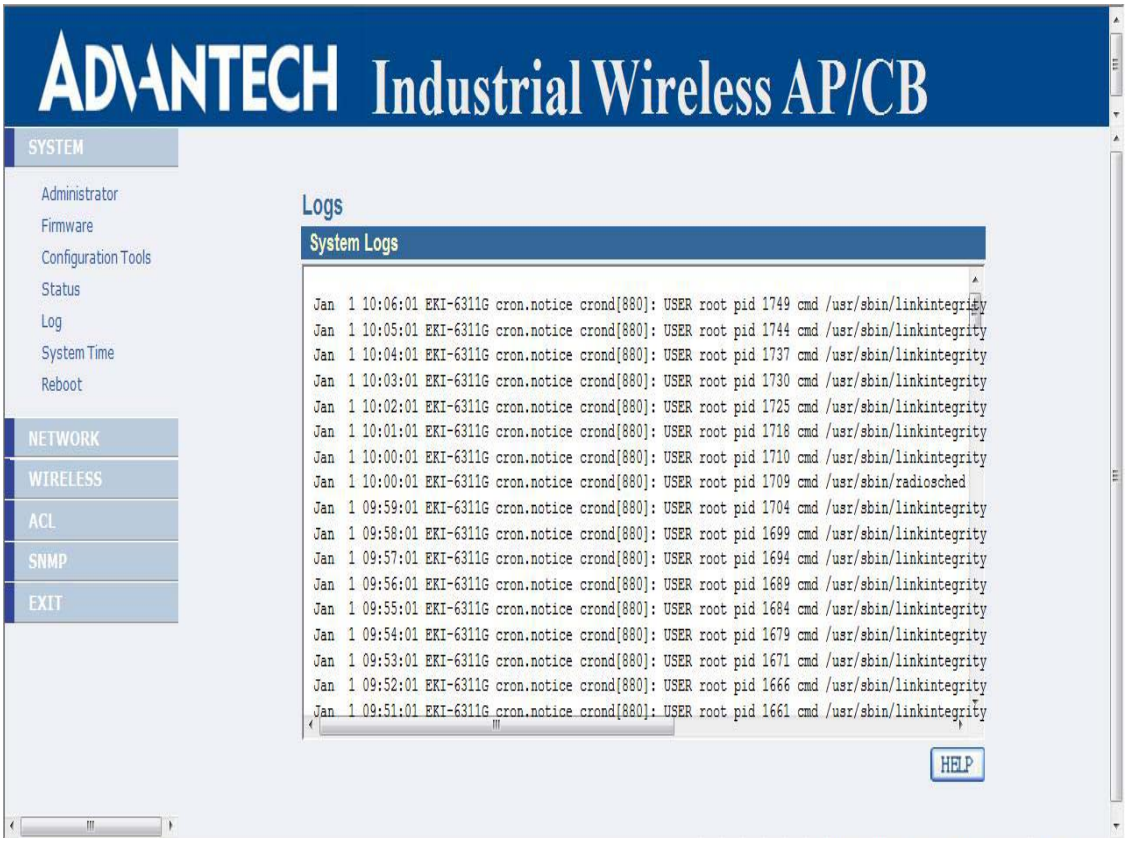


Figure 4-5

The Access Point automatically logs (records) events of possible interest in its internal memory. If there is not enough internal memory for all events, logs of older events are deleted, but logs of the latest events are retained. The Logs option allows you to view the Access Point logs.

4.1.6 System Time

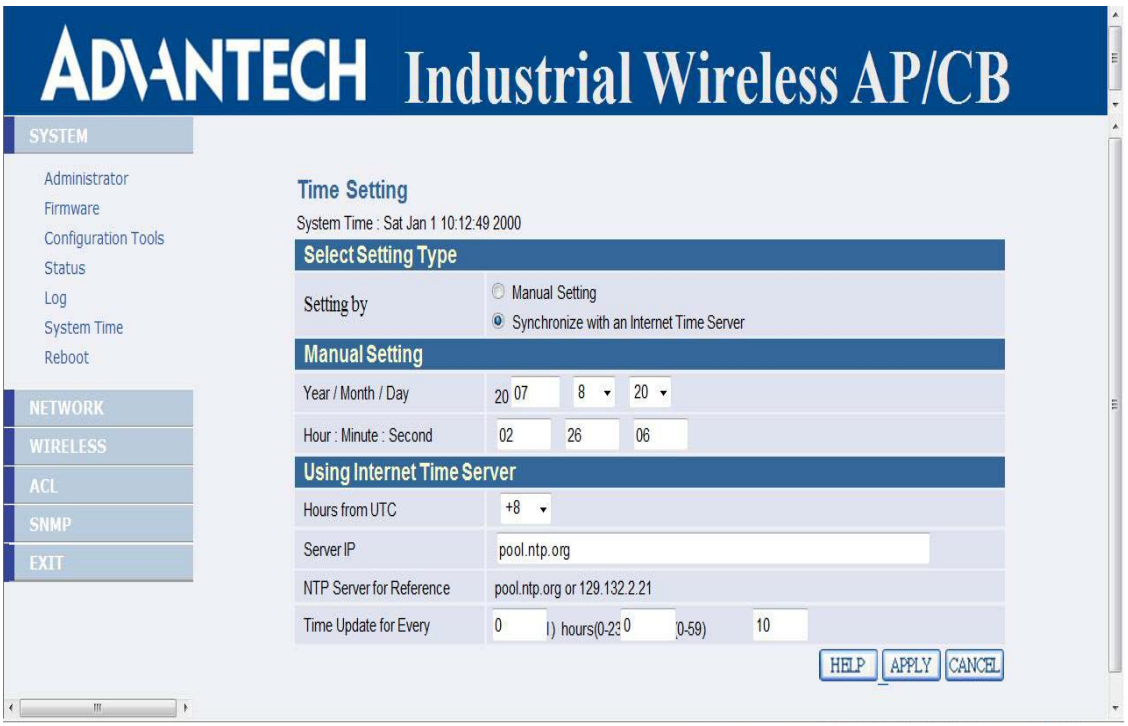


Figure 4-6

The Time Configuration option allows you to configure, update, and maintain the correct time on device's internal system clock. From this section you can set the time zone that you are in and set the Time Server.

Time Configuration- Set the Date and Time Manually. If you do not have the NTP Server option in effect, you can either manually set the time for your Access Point here.

Note: If the Access Point loses power for any reason, it cannot keep its clock running, and will not have the correct time when it is started again. To maintain correct time for schedules and logs, you must enter the correct time after you restart the Access Point.

4.1.7 Reboot

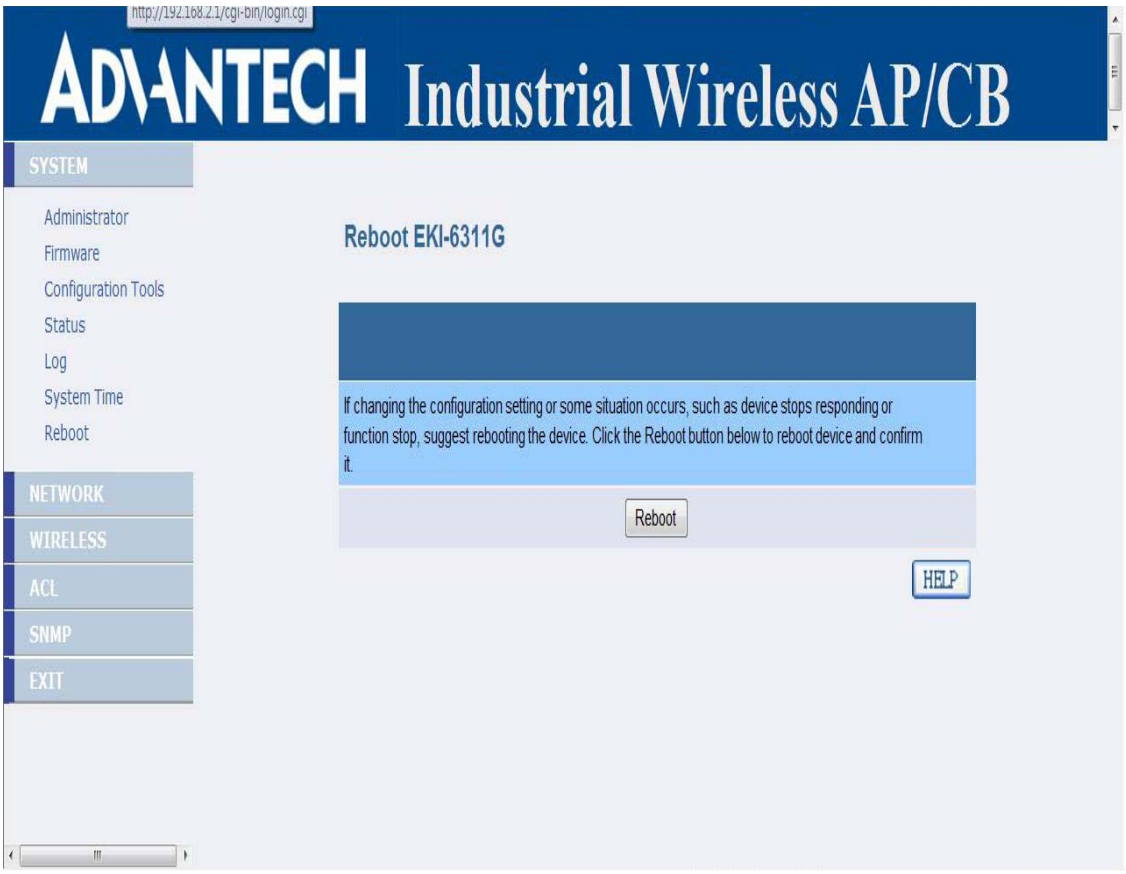


Figure 4-7

Reset Wireless device. In the event that the Wireless device stops responding correctly or in some way stops functioning, you can perform a reboot. Your existing settings will not be changed. To perform the reset, click on the **Reboot** button. You will be asked to confirm your decision.

4.2 NETWORK

4.2.1 Network

4.2.1.1 Operating Mode-Access Point

IP Assignment

DHCP

Choose "DHCP (Dynamic)" if your router supports DHCP and you want the router to assign an IP address to the AP. In this case, you do not need to fill in the following fields.

Figure 4-8

Manual

Choose "Manual" if your router does not support DHCP or if for any other reason you need to assign a fixed address to the AP. In this case, you must also configure the following fields.

IP Address

The IP address of the AP on the local area network. Assign any unused IP address in the range of IP addresses available for the LAN. For example, 192.168.1.101.

Subnet Mask

The subnet mask of the local area network.

Gateway

The IP address of the router on the local area network.

DNS Server

DNS （Domain Name System）, Penetrates the DNS system, We may look up its IP by machine domain name, Also may instead look up its domain name by machine IP

This entry is optional. Enter a DNS Server for the local network.

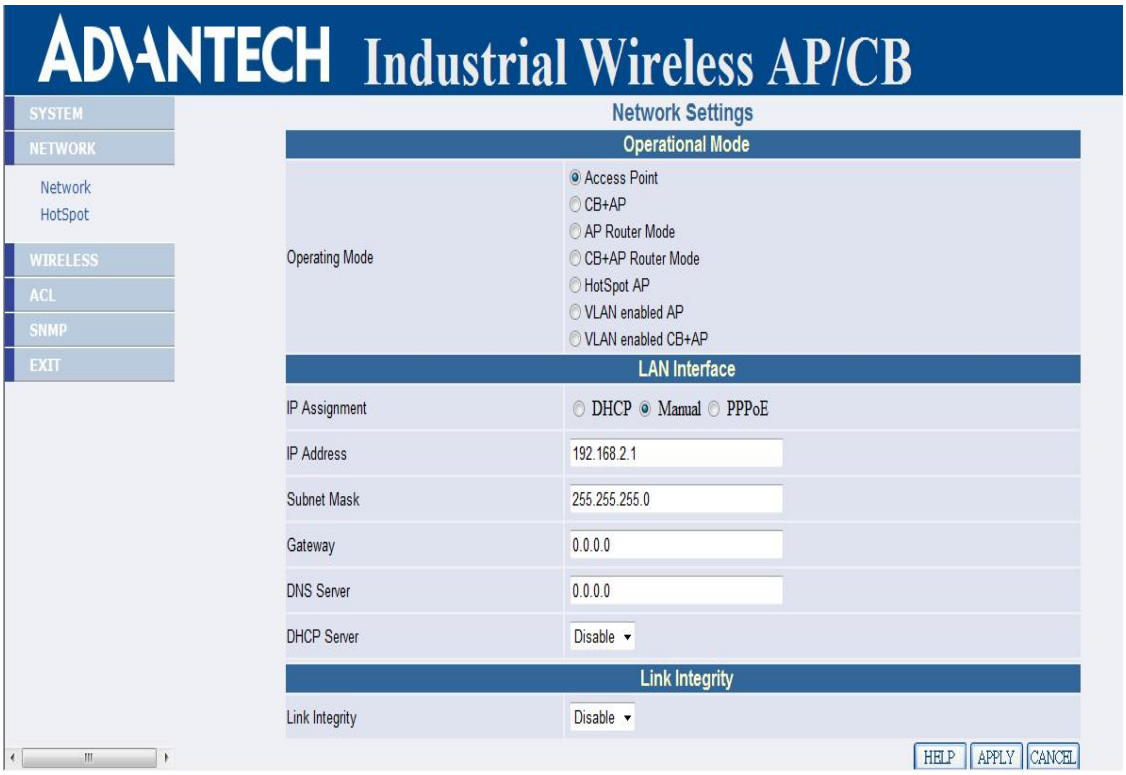


Figure 4-9

PPPoE

Choose "PPPoE" if your Internet support PPPoE Server .You need keyin **Username** and **Password** to login PPPoE Server.

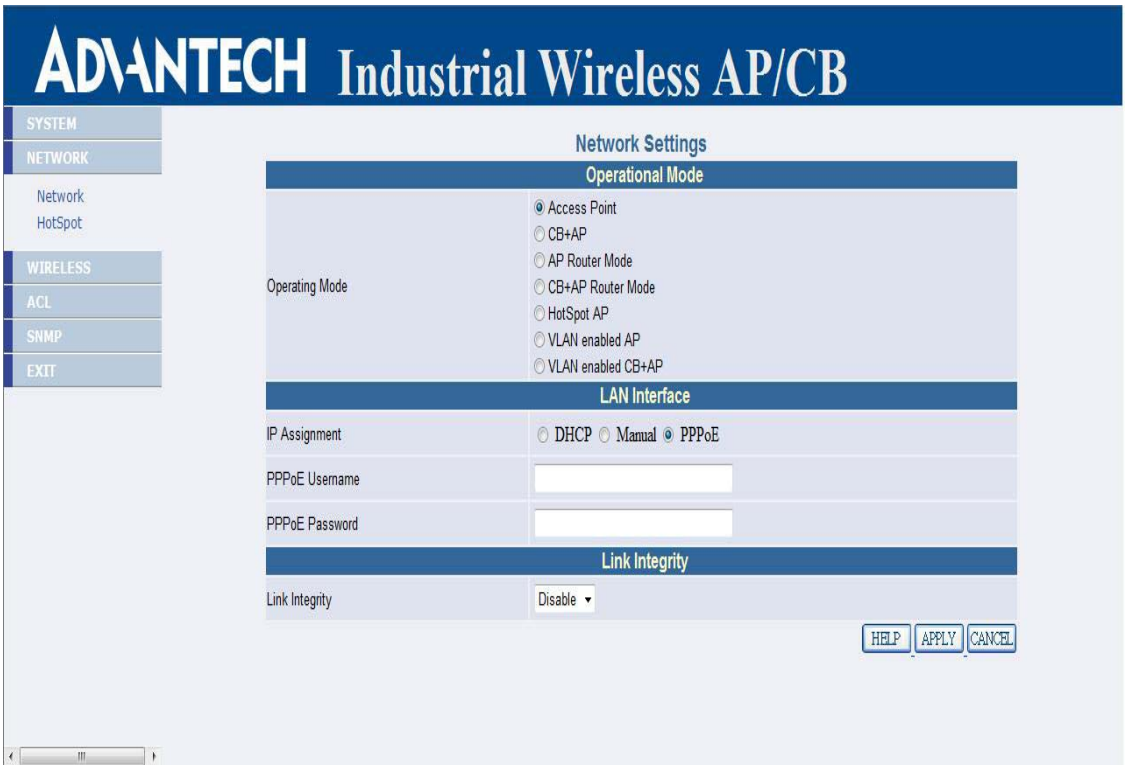


Figure 4-10

4.2.1.2 Operating Mode-Access Point

4.2.1.3 Operating Mode-CB+AP

4.2.1.4 Operating Mode-AP Router

4.2.1.5 Operating Mode-Access Point

4.2.1.6 Operating Mode-CB+AP Router

4.2.1.7 Operating Mode-Hot Spot

4.2.2 HotSpot（Captive Portal）

HotSpot: Enable/Disable captive portal function. Note, the device will become router mode and ALL SSID in Access Point role after HotSpot enabled.
Domain: Set domain name for hotspot.
Primary Radius: Set primary radius server for hotspot user authentication.
Secondary Radius: Set backup radius server for hotspot user authentication.
NAS ID: Set device's NAS ID in RADIUS frames.
Called Station Name: Set device's station name in RADIUS frames.
NAS Location: Set device's location name in RADIUS frames.
NAS Location ID: Set device's location ID in RADIUS frames.
UAM Server: The URL for hotspot user login.
UAM Secret: The encryption key between UAM server and device.
UAM Allowed List: IPs/Hostnames that hotspot can visit before login.

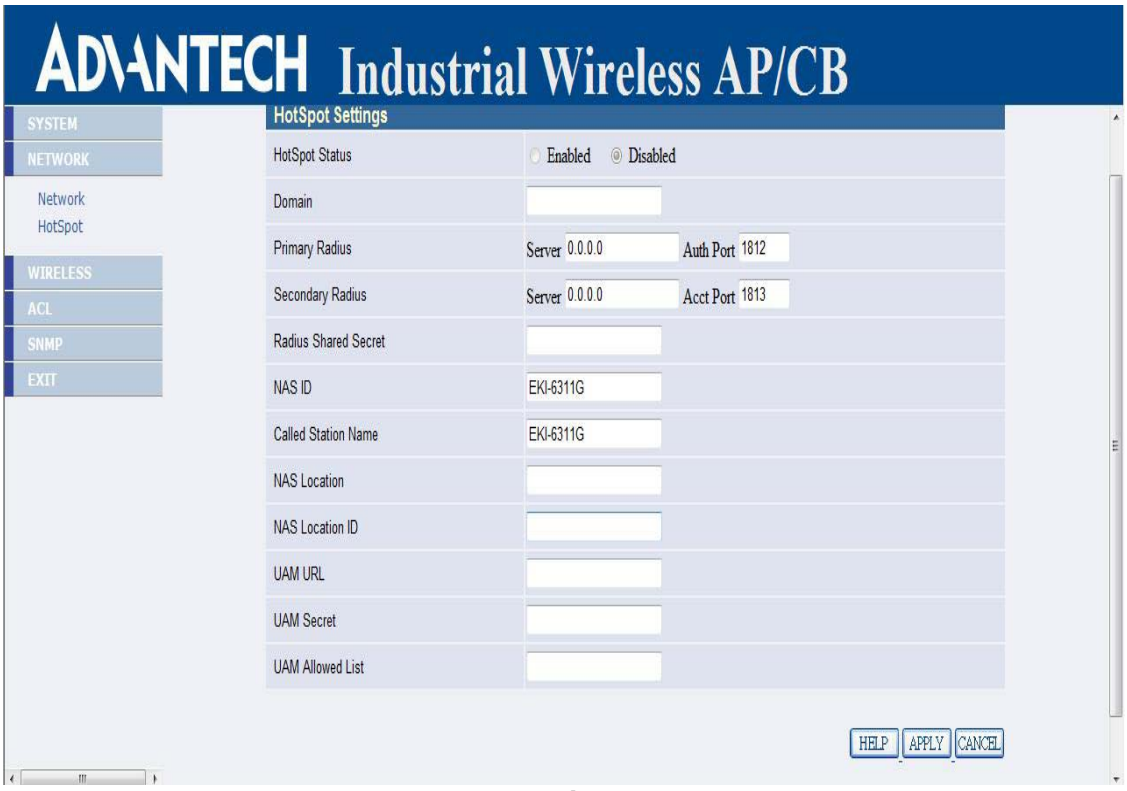


Figure 4-11

4.3 WIRELESS

You can set the wireless releated setting here

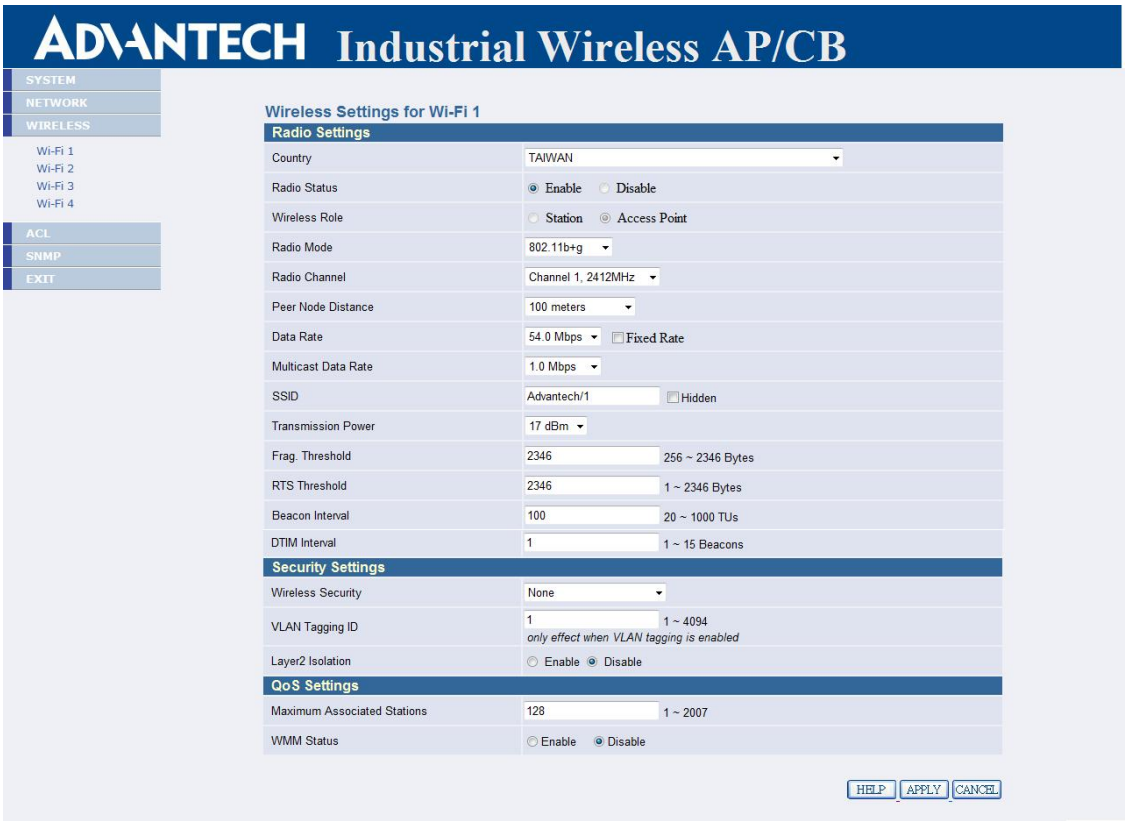


Figure 4-12

4.3.1 Wi-Fi 1

Wireless Settings

Radio Status: Enable/Disable SSID.
Wireless Role: This SSID will act as Station or Access Point. Note: only first SSID can act as station.
Radio Mode: Set 11g, 11b or 11b+g mode.
Radio Channel: Select radio channel or use auto.
Peer Node Distance: Set distance between this device and it's adjacent.
SSID: Set (extended) service set ID, a.k.a. netwrok name.
Transmission Power: Set transmission power in dBm, Note: H/W may not xmit power as high as you set, depends on H/W faculty.
VLAN Tagging ID: Set this SSID's VLAN tag when VLAN tagging enabled.
Maximum Associated Stations: Restrict maximu number of associated stations.
Layer 2 Isolation: Prevent packets exchange between associated stations.
Frag. Threshold: Fragmentation threshold.
RTS Threshold: RTS threshold.
Beacon Interval: Beacon interval in TUs.
WMM Tx: Set WMM parameters for packet transmission.
WMM Station: Set WMM parameters that provide for station.
Security:

WEP: Set WEP key in hexdecimal
WPA-Personal: WPA with pre-shared key.
WPA/WPA2-Personal: WPA and WPA2 co-existance with pre-shared key.
WPA-Enterprise: WPA, key provided by RADIUS server.
WPA/WPA2-Enterprise: WPA and WPA2 co-existance, key provided by RADIUS server.

4.3.2 Wi-Fi 2

4.3.3 Wi-Fi 3

4.3.4 Wi-Fi 4

4.4 ACL

You can set the access control releated setting here

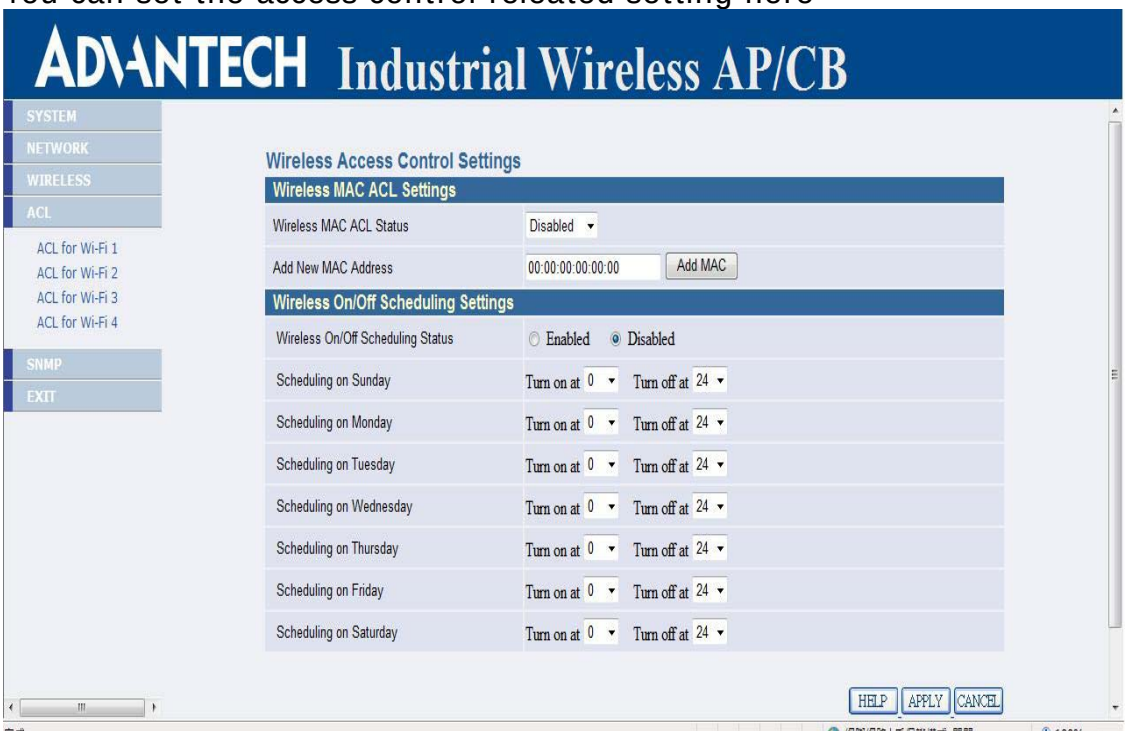


Figure 4-13

4.4.1 ACL for Wi-Fi 1

Wireless MAC ACL

Wireless MAC ACL Status: Enable/Disable ACL by MAC address.

Add New MAC Address: Add a new MAC address to MAC table and in active status.

MAC Table: Active, this MAC will be checked. Inactive, this MAC will ignore for checking. Remove, remove this MAC from MAC table.

4.4.2 ACL for Wi-Fi 2

4.4.3 ACL for Wi-Fi 3

4.4.4 ACL for Wi-Fi 4

4.5 SNMP

You can set the SNMP Community and SNMP Trap setting here

4.5.1 Agent Settings

SNMP Agent provides a simple protection. Access to the SNMP device is controlled through community names. The community name can be thought of as a password. If you don't have the correct community name, you can't retrieve any data (get) or make any change (set). Multiple SNMP managers may be organized in a specified community. You can change your SNMP community settings on this screen. Check the “Enable” check box to turn on SNMP daemon. Click APPLY to complete your change.

Read Only Community : Specify the name of community for read only access.

Read Write Community : Specify the name of community for read and write access.

Figure 4-14

4.6 EXIT

Chapter 5. *Specifications*

The EKI-6311G Outdoor Wireless Access Point/Multi-Client Bridge/ WDS (wireless distribution system) operates seamlessly in the 2.4 GHz frequency supporting the IEEE 802.11b/802.11g wireless standards. It's the best way to add wireless capability to your existing wired network, or to add bandwidth to your existing wireless installation.

To secure your wireless connectivity, it can encrypt all wireless transmissions through 64/128-bit WEP data encryption and also supports WPA/WPA2 （Personal/Enterprise）. A MAC address filter lets you select exactly which stations should have access to your network. With the Wireless Multi-Client Bridge/Access Point, you'll experience the best wireless connectivity available today.

Features

- High Speed Data Rate Up to 54Mbps
- Power-over-Ethernet (IEEE802.3af Compliant)
- Output Power up to 19dBm
- IEEE 802.11b/g Compliant
- WEP/WPA/WPA2/ IEEE 802.1x Authenticator support
- Dust tight and Watertight and Weatherproof (IP65)
- Wide temperature range and robust mechanical design
- Multi-SSID (up to 4 SSID) support

Data Rates	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
Standards	IEEE802.11b/g, IEEE802.1x, IEEE802.3, IEEE802.3u
Compatibility	IEEE 802.11g/ IEEE 802.11b
Power Requirements	Active Ethernet (802.3af) – 48 VDC/0.35A
Regulation Certifications	FCC Part 15, ETSI 300/328/CE
RF Information	Atheros BB/MAC/RF
Frequency Band	2.400～2.484 GHz
Media Access Protocol	Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
Modulation Technology	Orthogonal Frequency Division Multiplexing (OFDM), DBPSK @ 1Mbps, DQPSK @2Mbps, CCK @ 5.5 & 11Mbps, BPSK @ 6 and 9 Mbps, QPSK @ 12 and 18 Mbps, 16-QAM @ 24 and 36 Mbps, 64-QAM @ 48 and 54 Mbps
Operating Channels	11 for North America, 14 for Japan, 13 for Europe
Receive Sensitivity (Typical)	-72dBm @ 54Mbps
Available transmit power(Typical)	17dBm±2dBm @1, 2, 5.5 and 11Mbps, 17dBm±2dBm @6Mbps, 14dBm±2dBm @54Mbps
Antenna	5dBi External
RF Connector	SMA Type

Networking Topology	Ad-Hoc, Infrastructure
Operation Mode	Access Point / CB+AP / AP Router / CB+AP Router / HotSpot AP / VLAN AP / VLAN CB+AP
Interface	One 10/100Mbps RJ-45 LAN Port , RS-232 Console
Security	IEEE802.1x authenticator /RADIUS client (EAPMD5/TLS/TTLS) support in AP mode WPA / Pre Share KEY (PSK)/TKIP MAC address filtering Hide SSID in beacons Layer 2 Isolation
IP Auto-configuration	DHCP client/server/PPPoE
Management Configuration	Web-based configuration (HTTP)
Firmware Upgrade	Upgrade firmware via web browser
Physical Dimensions	209.1(L)mm * 165.4(W)mm * 61.5(H)mm
Weight	500g (1.1 lbs);
Environmental Temperature Range	-Operating: -10°C to 60°C (14°F to 140°F) -Storage: -20°Cto 70°C (-4°F to 158°F)
Humidity (non-condensing)	5%~95% Typical
Package Contents	• Water tight Outdoor Wireless Client Bridge unit • 48V, 0.38A AC/DC adapter with wall-plug power code • Inline Power Injector (PoE) • User's manual CD-ROM • Wall mounting kit • Mast mounting kit

Chapter 6. *Default Settings*

6.1 SYSTEM

6.1.1 Administrator

Parameter	Description	Default Value
Hostname		Advantech.lan
Current Password		
Password		
Re-type Password		
Idle Time Out		30
Enable		
IP address		0.0.0.0

6.1.2 Firmware

Parameter	Description	Default Value
Using TFTP		
Using FTP		
Using WEB		

6.1.3 Configuration Tools

Parameter	Description	Default Value
Restore Factory Default Configuration		
Backup Settings / Restore Settings		

6.1.4 Status

6.1.5 Log

6.1.6 System Time

Parameter	Description	Default Value
Setting by		Synchronize with an Internet Time Server
Year / Month / Day		07/8/20
Hour : Minute : Second		02:26:06
Hours from UTC		+8
Server IP		pool.ntp.org
NTP Server for Reference		pool.ntp.org or 129.132.2.21
Time Update for Every		0/0/0

6.1.7 Reboot

6.2 NETWORK

6.2.1 Network

Parameter	Description	Default Value
Operating		Access Point
IP Assignment		Manual
IP Address		192.168.1.1
Subnet Mask		255.255.255.0
Gateway		0.0.0.0
DNS Server		0.0.0.0
Link Integrity		Disable
PPPoE Username		
PPPoE Password		

6.2.2 Hotspot

Parameter	Description	Default Value	
HotSpot Status		Disable	
Domain			
Primary Radius		0.0.0.0	1812
Secondary Radius		0.0.0.0	1813
Radius Shared Secret			
NAS ID		EKI-6311G	
Called Station Name		EKI-6311G	
NAS Location			
NAS Location ID			
UAM URL			
UAM Secret			
UAM Allowed List			

6.3 WIRELESS

6.3.1 Wi-Fi 1

Parameter	Description	Default Value
Country		TAIWAN
Radio Status		Enable
Wireless Role		Access Point
Radio Mode		802.11b+g
Radio Channel		Channel 1, 2412MHz
Peer Node Distance		100 meters
SSID		Advantech/1
Transmission Power		17dBm
Frag. Threshold		2346
RTS Threshold		2346
Beacon Interval		100
DTIM Interval		1
Wireless Security		None
VLAN Tagging ID		1
Layer2 Isolation		Disable
Maximum Associated Stations		32
WMM Status		Disable

6.3.2 Wi-Fi 2

Parameter	Description	Default Value
Country		TAIWAN
Radio Status		Disable
Wireless Role		Access Point
Radio Mode		802.11b+g
Radio Channel		Channel 1, 2412MHz
Peer Node Distance		100 meters
SSID		Advantech/2
Transmission Power		17dBm
Frag. Threshold		2346
RTS Threshold		2346
Beacon Interval		100
DTIM Interval		1
Wireless Security		None
VLAN Tagging ID		2
Layer2 Isolation		Disable
Maximum Associated Stations		32
WMM Status		Disable

6.3.3 Wi-Fi 3

Parameter	Description	Default Value
Country		TAIWAN
Radio Status		Disable
Wireless Role		Access Point
Radio Mode		802.11b+g
Radio Channel		Channel 1, 2412MHz
Peer Node Distance		100 meters
SSID		Advantech/3
Transmission Power		17dBm
Frag. Threshold		2346
RTS Threshold		2346
Beacon Interval		100
DTIM Interval		1
Wireless Security		None
VLAN Tagging ID		2
Layer2 Isolation		Disable
Maximum Associated Stations		32
WMM Status		Disable

6.3.4 Wi-Fi 4

Parameter	Description	Default Value
Country		TAIWAN
Radio Status		Disable
Wireless Role		Access Point
Radio Mode		802.11b+g
Radio Channel		Channel 1, 2412MHz
Peer Node Distance		100 meters
SSID		Advantech/4
Transmission Power		17dBm
Frag. Threshold		2346
RTS Threshold		2346
Beacon Interval		100
DTIM Interval		1
Wireless Security		None
VLAN Tagging ID		2
Layer2 Isolation		Disable
Maximum Associated Stations		32
WMM Status		Disable

6.4 ACL

6.4.1 ACL for Wi-Fi

Parameter	Description	Default Value	
Wireless MAC ACL Status		Disable	
Add New MAC Address		00:00:00:00:00:00	
Wireless On / Off Scheduling Status		Disabled	
Scheduling on Sunday		0	24
Scheduling on Monday		0	24
Scheduling on Tuesday		0	24
Scheduling on Wednesday		0	24
Scheduling on Thursday		0	24
Scheduling on Friday		0	24
Scheduling on Saturday		0	24

6.4.2 ACL for Wi-Fi 2

Parameter	Description	Default Value	
Wireless MAC ACL Status		Disable	
Add New MAC Address		00:00:00:00:00:00	
Wireless On / Off Scheduling Status		Disabled	
Scheduling on Sunday		0	24
Scheduling on Monday		0	24
Scheduling on Tuesday		0	24
Scheduling on Wednesday		0	24
Scheduling on Thursday		0	24
Scheduling on Friday		0	24
Scheduling on Saturday		0	24

6.4.3 ACL for Wi-Fi 3

Parameter	Description	Default Value	
Wireless MAC ACL Status		Disable	
Add New MAC Address		00:00:00:00:00:00	
Wireless On / Off Scheduling Status		Disabled	
Scheduling on Sunday		0	24
Scheduling on Monday		0	24
Scheduling on Tuesday		0	24
Scheduling on Wednesday		0	24
Scheduling on Thursday		0	24
Scheduling on Friday		0	24
Scheduling on Saturday		0	24

6.4.4 ACL for Wi-Fi 4

Parameter	Description	Default Value	
Wireless MAC ACL Status		Disable	
Add New MAC Address		00:00:00:00:00:00	
Wireless On / Off Scheduling Status		Disabled	
Scheduling on Sunday		0	24
Scheduling on Monday		0	24
Scheduling on Tuesday		0	24
Scheduling on Wednesday		0	24
Scheduling on Thursday		0	24
Scheduling on Friday		0	24
Scheduling on Saturday		0	24

6.5 SNMP

Parameter	Description	Default Value
Agent Status		Enable
System Location		
System Contact		
System Name		Advantech
System Description		Advantech Wireless AP/CB
Read Only Community		public
Read Write Community		Private

6.6 EXIT

Chapter 7. *Regulatory Compliance Information*

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.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna

⚠ **Caution** To meet regulatory restrictions and the safety of the installation, strongly recommends this product to be **professionally installed**.

Antenna type	Antenna Gain
Omni	5dBi