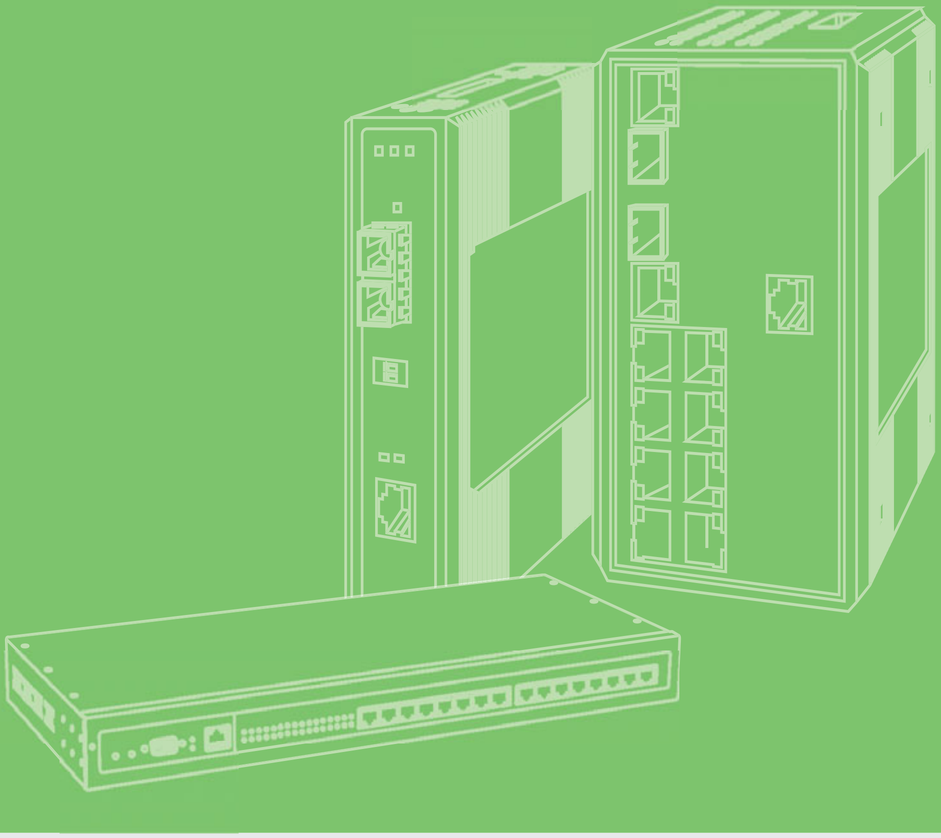


User Manual

EKI-6310GN

2.4GHz 802.11b/g/n Outdoor AP/ CPE

ADVANTECH

Enabling an Intelligent Planet

Copyright

Acknowledgements

Microsoft Windows and MS-DOS are registered trademarks of Microsoft Corp.

All other product names or trademarks are properties of their respective owners.

Product Warranty (5 years)

Advantech warrants to you, the original purchaser, that each of its products will be free from defects in materials and workmanship for five years from the date of purchase.

This warranty does not apply to any products which have been repaired or altered by persons other than repair personnel authorized by Advantech, or which have been subject to misuse, abuse, accident or improper installation. Advantech assumes no liability under the terms of this warranty as a consequence of such events.

Because of Advantech's high quality-control standards and rigorous testing, most of our customers never need to use our repair service. If an Advantech product is defective, it will be repaired or replaced at no charge during the warranty period. For out-of-warranty repairs, you will be billed according to the cost of replacement materials, service time and freight. Please consult your dealer for more details.

If you think you have a defective product, follow these steps:

1. Collect all the information about the problem encountered. (For example, CPU speed, Advantech products used, other hardware and software used, etc.) Note anything abnormal and list any onscreen messages you get when the problem occurs.
2. Call your dealer and describe the problem. Please have your manual, product, and any helpful information readily available.
3. If your product is diagnosed as defective, obtain an RMA (return merchandize authorization) number from your dealer. This allows us to process your return more quickly.
4. Carefully pack the defective product, a fully-completed Repair and Replacement Order Card and a photocopy proof of purchase date (such as your sales receipt) in a shippable container. A product returned without proof of the purchase date is not eligible for warranty service.
5. Write the RMA number visibly on the outside of the package and ship it prepaid to your dealer.

Part No. 2063634000 Edition 1
Printed in Taiwan May 2014

Declaration of Conformity

FCC Class A

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Class B

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 or more 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.

Technical Support and Assistance

1. Visit the Advantech web site at www.advantech.com/support where you can find the latest information about the product.
2. Contact your distributor, sales representative, or Advantech's customer service center for technical support if you need additional assistance. Please have the following information ready before you call:
   - Product name and serial number
   - Description of your peripheral attachments
   - Description of your software (operating system, version, application software, etc.)
   - A complete description of the problem
   - The exact wording of any error messages

Warnings, Cautions and Notes

Warning! *Warnings indicate conditions, which if not observed, can cause personal injury!*

Caution! *Cautions are included to help you avoid damaging hardware or losing data. e.g.*

There is a danger of a new battery exploding if it is incorrectly installed. Do not attempt to recharge, force open, or heat the battery. Replace the battery only with the same or equivalent type recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions.

Note! *Notes provide optional additional information.*

Document Feedback

To assist us in making improvements to this manual, we would welcome comments and constructive criticism. Please send all such - in writing to: support@advantech.com

Safety Instructions

1. Read these safety instructions carefully.
2. Keep this User Manual for later reference.
3. Disconnect this equipment from any AC outlet before cleaning. Use a damp cloth. Do not use liquid or spray detergents for cleaning.
4. For plug-in equipment, the power outlet socket must be located near the equipment and must be easily accessible.
5. Keep this equipment away from humidity.
6. Put this equipment on a reliable surface during installation. Dropping it or letting it fall may cause damage.
7. The openings on the enclosure are for air convection. Protect the equipment from overheating. DO NOT COVER THE OPENINGS.
8. Make sure the voltage of the power source is correct before connecting the equipment to the power outlet.
9. Position the power cord so that people cannot step on it. Do not place anything over the power cord.
10. All cautions and warnings on the equipment should be noted.
11. If the equipment is not used for a long time, disconnect it from the power source to avoid damage by transient overvoltage.
12. Never pour any liquid into an opening. This may cause fire or electrical shock.
13. Never open the equipment. For safety reasons, the equipment should be opened only by qualified service personnel.
14. If one of the following situations arises, get the equipment checked by service personnel:

- The power cord or plug is damaged.
- Liquid has penetrated into the equipment.
- The equipment has been exposed to moisture.
- The equipment does not work well, or you cannot get it to work according to the user's manual.
- The equipment has been dropped and damaged.
- The equipment has obvious signs of breakage.

15. DO NOT LEAVE THIS EQUIPMENT IN AN ENVIRONMENT WHERE THE STORAGE TEMPERATURE MAY GO BELOW -40° C (-4° F) OR ABOVE 85° C (185° F). THIS COULD DAMAGE THE EQUIPMENT. THE EQUIPMENT SHOULD BE IN A CONTROLLED ENVIRONMENT.
16. CAUTION: DANGER OF EXPLOSION IF BATTERY IS INCORRECTLY REPLACED. REPLACE ONLY WITH THE SAME OR EQUIVALENT TYPE RECOMMENDED BY THE MANUFACTURER, DISCARD USED BATTERIES ACCORDING TO THE MANUFACTURER'S INSTRUCTIONS.

The sound pressure level at the operator's position according to IEC 704-1:1982 is no more than 70 dB (A).

DISCLAIMER: This set of instructions is given according to IEC 704-1. Advantech disclaims all responsibility for the accuracy of any statements contained herein.

Safety Precaution - Static Electricity

Follow these simple precautions to protect yourself from harm and the products from damage.

- To avoid electrical shock, always disconnect the power from your PC chassis before you work on it. Don't touch any components on the CPU card or other cards while the PC is on.
- Disconnect power before making any configuration changes. The sudden rush of power as you connect a jumper or install a card may damage sensitive electronic components.

Professional Installation Required

Please seek assistance from a professional installer who is well trained in the RF installation and knowledgeable in the local regulations. Precautions

1. To keep you safe and install the hardware properly, please read and follow these safety precautions.
2. If you are installing EKI-6310GN for the first time, for your safety as well as others', please seek assistance from a professional installer who has received safety training on the hazards involved.
3. Keep safety as well as performance in mind when selecting your installation site, especially where there are electric power and phone lines.
4. When installing EKI-6310GN, please note the following things:
   – Do not use a metal ladder;
   – Do not work on a wet or windy day;
   – Wear shoes with rubber soles and heels, rubber gloves, long sleeved shirt or jacket.
5. When the system is operational, avoid standing directly in front of it. strong RF fields are present when the transmitter is on.

Contents

Chapter 8 Application Rules And Firewall........65

Appendix A Application Wizard 71

Chapter 1

Overview

1.1 Introduction

EKI-6310GN is a feature rich wireless AP/ CPE which provides a reliable wireless connectivity for industrial environments. The PoE helps to connect to PoE switch directly. As an 802.11n compliant device, EKI-6310GN provides 3 times higher data rates than legacy 802.11g devices. EKI-6310GN effectively improves the reliability of wireless connectivity, especially in applications that need high reliability and high throughput data transmission. To secure wireless connections, EKI-6310GN encrypts data through 64/128/152-bit WEP data encryption and also supports WPA2/WPA/ 802.1x for powerful security authentication.

1.2 Features

- Compliant with IEEE 802.11b/g and IEEE 802.11n
- Support Standard Power-over-Ethernet (PoE)
- IP66 waterproof certification
- Four operating modes including AP, Wireless Client, WDS and WDS AP Repeater
- Support 64/128/152-bit WEP and 802.1X, WPA, WPA2, WPA&WPA2,WPA-PSK, WPA2-PSK, and WPA-PSK&WPA2-PSK etc
- User-friendly Web and SNMP-based management interface
- With external N-type connector for optional antenna (default 5 dBi Omni antenna)
- Support distances up to 5Km

1.3 Specification

Standard Support

- Wireless: IEEE802.11b/g/n
- Ethernet: IEEE802.3u MDI / MDIX 10/100 Fast Ethernet
- LAN: IEEE802.11b/g/n wireless LAN interface
- Data Rates
  - 802.11b 11, 5.5, 2, 1 Mbps, auto-fallback
  - 802.11g 54, 48, 36, 24, 18, 12, 9, 6 Mbps, auto-fallback
  - 802.11n 6M, 6.5M, 13M, 13.5M, 19.5M, 26M, 27M, 39M,40.5M, 53M, 54M, 58.5M, 65M, 78M, 81M, 104M,108M, 117M, 121.5M, 130M, 135M, 150Mbps

Physical Specifications

- Power: 802.3af PoE
- Dimensions (L x W x H): 228 x 64 x 61 mm
- Weight: 500g

Antenna:

- Antenna Configuration 1x1 (1 Tx, 1 Rx)
- Reserve N-type Connector (Plug) with 5dBi dipole antenna for indoor AP application.

Modulation Techniques

- 802.11b DSSS (DBPSK, DQPSK, CCK)
- 802.11g OFDM, DSSS (BPSK, QPSK, 16-QAM, 64-QAM)
- 802.11n OFDM (BPSK, QPSK, 16-QAM, 64-QAM)

Channel Support

- 802.11b/g/n HT20
  FCC: CH1 ~ CH11; ETSI: CH1 ~ CH13
- 802.11gn HT40
  FCC: CH3 ~ CH9; ETSI: CH3 ~ CH11

Wireless Transmission Rates

- Transmitted Power
- 802.11b: 26dBm
- 802.11g: 26dBm @ 6Mbps, 24dBm @ 54Mbps
- 802.11gn HT20: 26dBm @ MCS0, 22dBm@ MCS7
- 802.11gn HT40: 26dBm @ MCS0, 21dBm@ MCS7

Receiver Sensitivity

- 802.11b: -93dBm @ 1Mbps; -88dBm @ 11Mbps
- 802.11g: -89dBm @ 6Mbps; -73dBm @ 54Mbps
- 802.11n HT20: -88dBm @ MCS0; -70dBm @ MCS7
- 802.11n HT40: -84dBm @ MCS0; -67dBm @ MCS7

1.4 Packing List

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.

EKI-6310GN	×1
Pole Mounting Ring	×1
PoE Adapter	×1
Start up manual	×1
User's manual CD	×1
RSMA Omni antenna	×1

Chapter 2

Installation

This chapter describes safety precautions and product information you have to know and check before installing EKI-6310GN.

2.1 Preparation before Installation

Professional Installation Required

Please seek assistance from a professional installer who is well trained in the RF installation and knowledgeable in the local regulations.

Safety Precautions

1. To keep you safe and install the hardware properly, please read and follow these safety precautions.
2. 2. If you are installing EKI-6310GN for the first time, for your safety as well as others', please seek assistance from a professional installer who has received safety training on the hazards involved.
3. Keep safety as well as performance in mind when selecting your installation site, especially where there are electric power and phone lines.
4. When installing EKI-6310GN, please note the following things:
   - Do not use a metal ladder;
   - Do not work on a wet or windy day;
   - Wear shoes with rubber soles and heels, rubber gloves, long sleeved shirt or jacket.
5. When the system is operational, avoid standing directly in front of it. Strong RF fields are present when the transmitter is on.

2.2 Installation Precautions

To keep the EKI-6310GN well while you are installing it, please read and follow these installation precautions.

1. Users MUST use a proper and well-installed surge arrestor with the EKI-6310GN; otherwise, a random lightening could easily cause fatal damage to EKI-6310GN.
   EMD (Lightning) DAMAGE IS NOT COVERED UNDER WARRNTY.
2. Users MUST use the "Power cord & PoE Injector" shipped in the box with the EKI-6310GN. Use of other options will cause damage to the EKI-6310GN.
3. Users MUST power off the EKI-6310GN first before connecting the external antenna to it. Do not switch from built-in antenna to the external antenna from WEB management without physically attaching the external antenna onto the EKI-6310GN; otherwise, damage might be caused to the EKI-6310GN itself.

2.3 Hardware Installation

Connect up

1. The bottom of the EKI-6310GN is a movable cover. Grab the cover and pull it back harder to take it out as the figure shown below.
2. Plug a standard Ethernet cable into the RJ45 port.
3. Slide the cover back to seal the bottom of the EKI-6310GN.

2.4 Pole Mounting

Connect up

1. Turn the EKI-6310GN over. Put the pole mounting ring through the middle hole of it. Note that you should unlock the pole mounting ring with a screw driver before putting it through EKI-6310GN as the following right picture shows.
2. Mount EKI-6310GN steadily to the pole by locking the pole mounting ring tightly.
3. Now you have completed the hardware installation of EKI-6310GN.

Using the External Antenna

- Grab the black rubber on the top of EKI-6310GN, and slightly pull it up. The metal N-type connector will appear.
- Connect your antenna on the top of EKI-6310GN. The following picture shows the full set of EKI-6310GN:

Chapter 3

Basic Settings

3.1 Factory Default Settings

We'll elaborate the EKI-6310GN factory default settings. You can re-acquire these parameters by default. If necessary, please refer to the "Restore Factory Default Settings".

Table 3.1: EKI-6310GN Factory Default Settings

Features		Factory Default Settings
Username		admin
Password		admin
Operation Mode		AP Bridge
LAN	IP Adress	192.168.2.1
	Subnet Mask	255.255.255.0
	Default Gateway	
	Primary DNS	
	Secondary DNS	
	MTU	1500
	Spanning Tree	Disable
WLAN	DHCP Server	Disable
	Country Code	United States
	Wireless mode	Access Point
	Network Name (SSID)	EKI-6310GN
	Frequency (Channel)	Channel 6
	Network Mode	WiFi 11gn HT20
	Encryption Setting	Disable (Open)
	Distance	0.6mi
	BG Protection Mode	Disable
Access Control		Disable
Advanced	Package Aggregate	Enable
	WMM	Enable
	TX Power	23 dBm
	Beacon Interval	100 ms
	DTIM	1
	RTS/CTS	Disable
	Fragmentation Threshold	Disable
	Station Control	127
	Wireless Isolation	Disable
Threshold	LED1	-94
	LED2	-80
	LED3	-73
	LED4	-65
SNMP	Enable/Disable	Disable
	Read Community Name	Public
	Write Community Name	Private
	IP Address	0.0.0.0
Telnet / SSH	Telnet	Enable
	SSH	Disable
	Username	root
	Password	Advantech

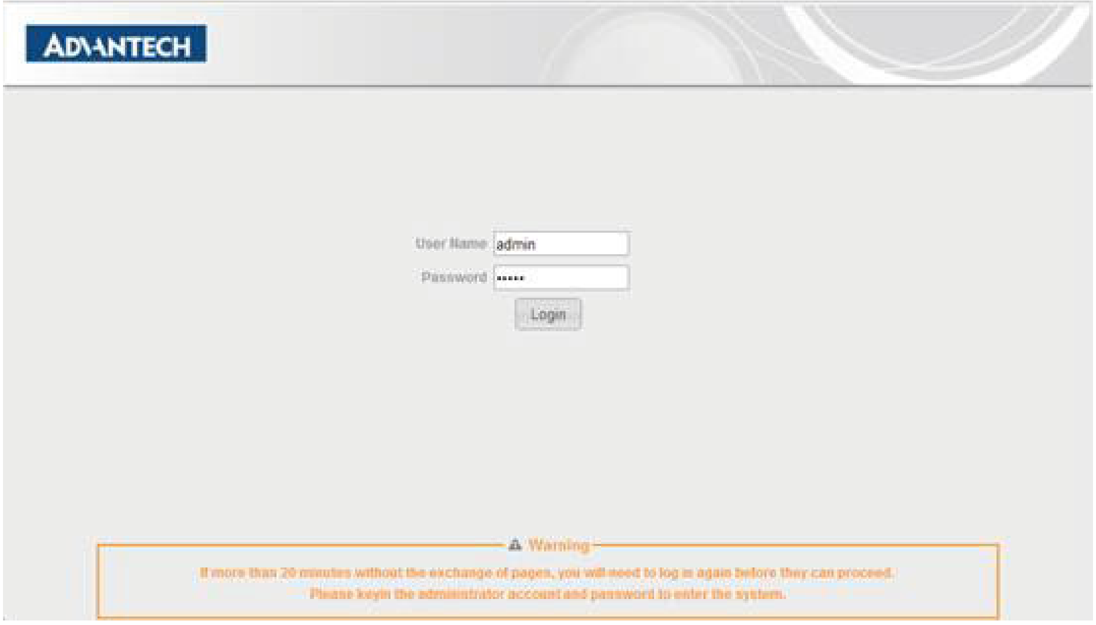
3.2 System Requirements

Before configuration, please make sure your system meets the following requirements:

- A computer coupled with 10/ 100 Base-TX adapter;
- Configure the computer with a static IP address of 192.168.2.x, as the default IP address of EKI-6310GN is 192.168.2.1. (X cannot be 0, 1, nor 255);
- A Web browser on PC for configuration such as Microsoft Internet Explorer 6.0 or above, Netscape, Firefox or Google Chrome.

3.3 How to Login the Web-based Interface

- Open Web browser and enter the IP address (Default: 192.168.2.1) of EKI-6310GN into the address field. You will see the login page as below.



User Name admin

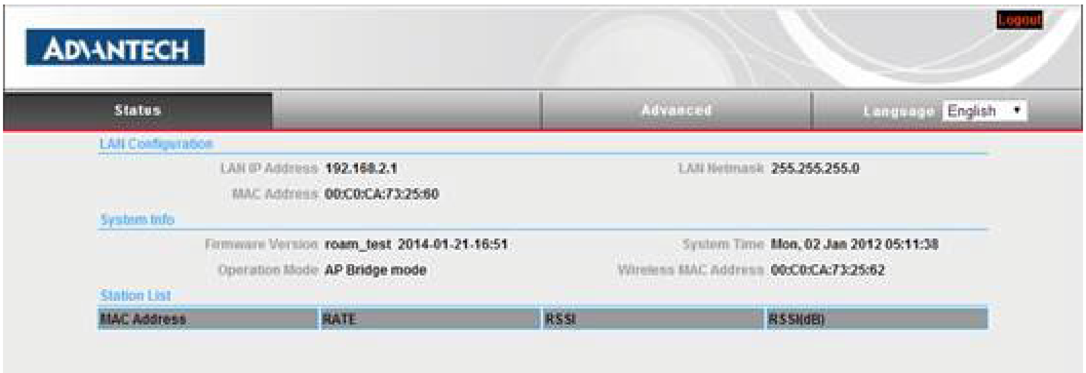
Password •••••

⚠ Warning

If more than 20 minutes without the exchange of pages, you will need to log in again before they can proceed.
Please keyin the administrator account and password to enter the system.

Figure 3.1 Login Page

- Enter the username (Default: admin) and password (Default: admin) respectively and click "Login" to login the main page of EKI-6310GN. As you can see, this management interface provides three main options in the gray bar above, which are Status, Advanced and Language. Most functions are configured in 'Advanced' option.



Language English

LAN Configuration

LAN IP Address 192.168.2.1 LAN Netmask 255.255.255.0

MAC Address 00:C0:CA:73:25:60

System Info

Firmware Version roam_test 2014-01-21-16:51 System Time Mon, 02 Jan 2012 05:11:38

Operation Mode AP Bridge mode Wireless MAC Address 00:C0:CA:73:25:62

Station List

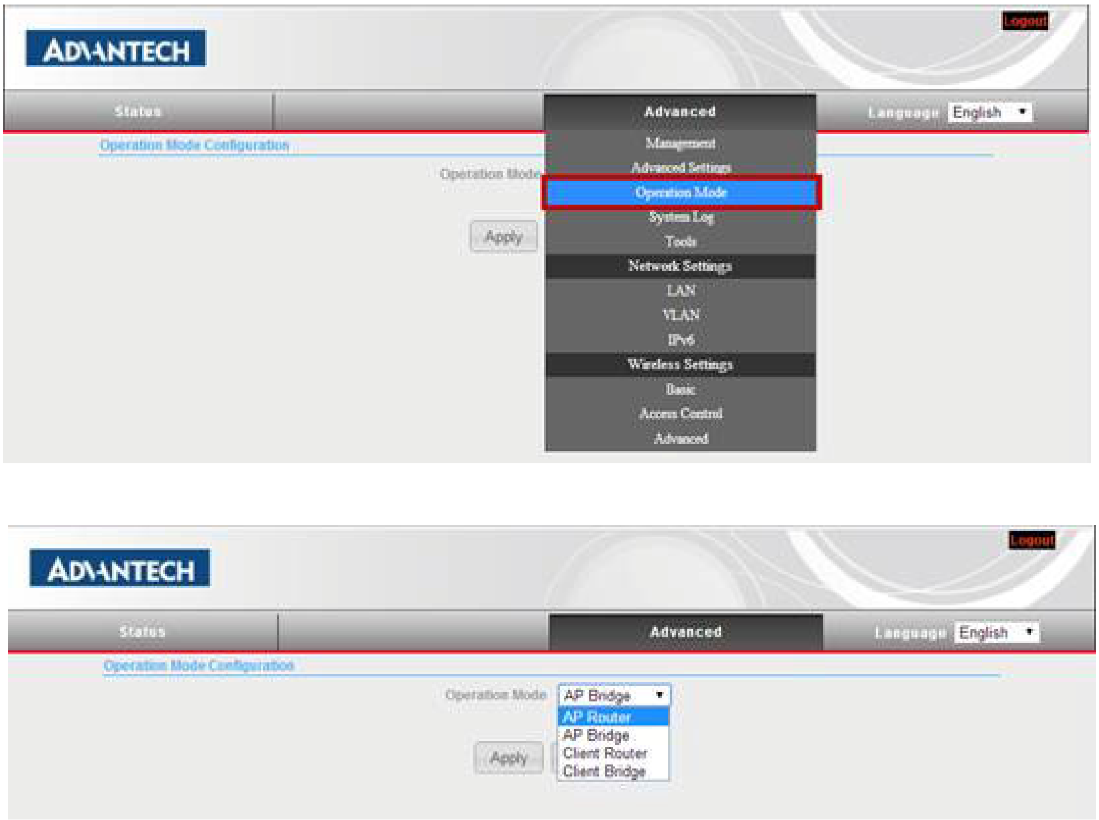
MAC Address	RATE	RSSI	RSSI(dB)

Figure 3.2 Main Page

3.4 Basic Setting Scenario

You can configure your devices to different roles in following scenario.

- Configure 'operation mode' of your device. You can configure EKI-6310GN as four different modes - AP Router (router connection), AP Bridge (access point), Client Router (WISP - wireless Internet Service Provider) and Client Bridge (WiFi client).



Operation Mode: AP Bridge

Figure 3.3 Operation mode

- Configure your network setting in 'WAN' and 'LAN' options. It will provide you the configuration of LAN or WAN based on bridge or router mode. The default IP of WAN and LAN is fixed IP '192.168.2.1' (WAN) & '192.168.1.1' (LAN) when you select router mode.

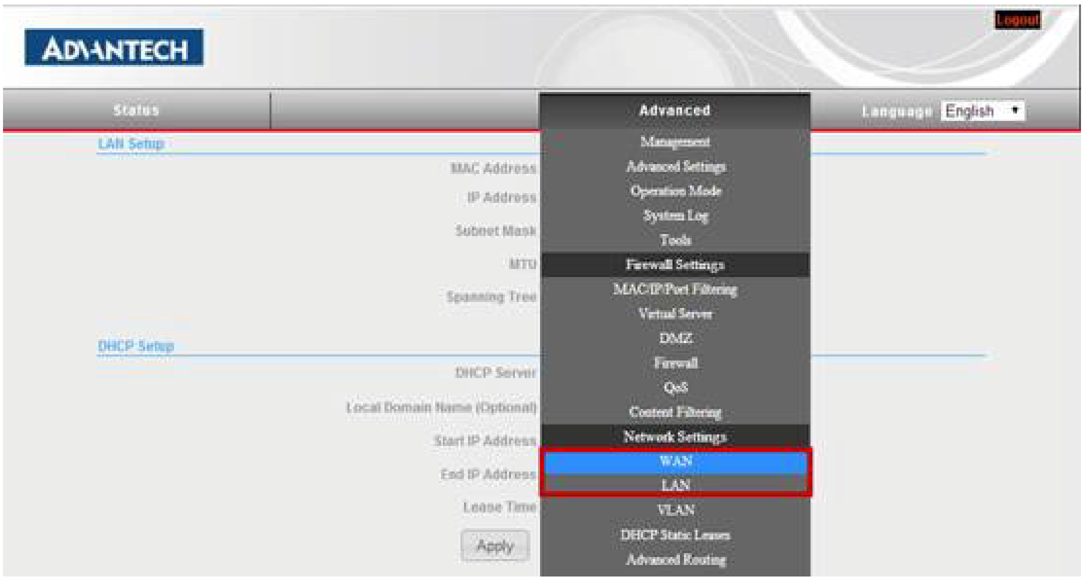
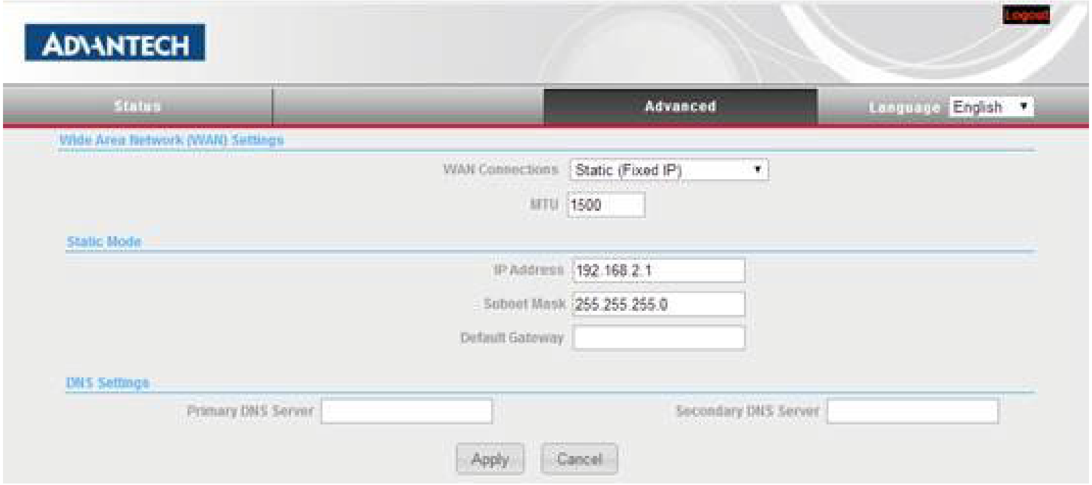


Figure 3.4 Network Settings



Wide Area Network (WAN) Settings

WAN Connections: Static (Fixed IP)

MTU: 1500

Static Mode

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

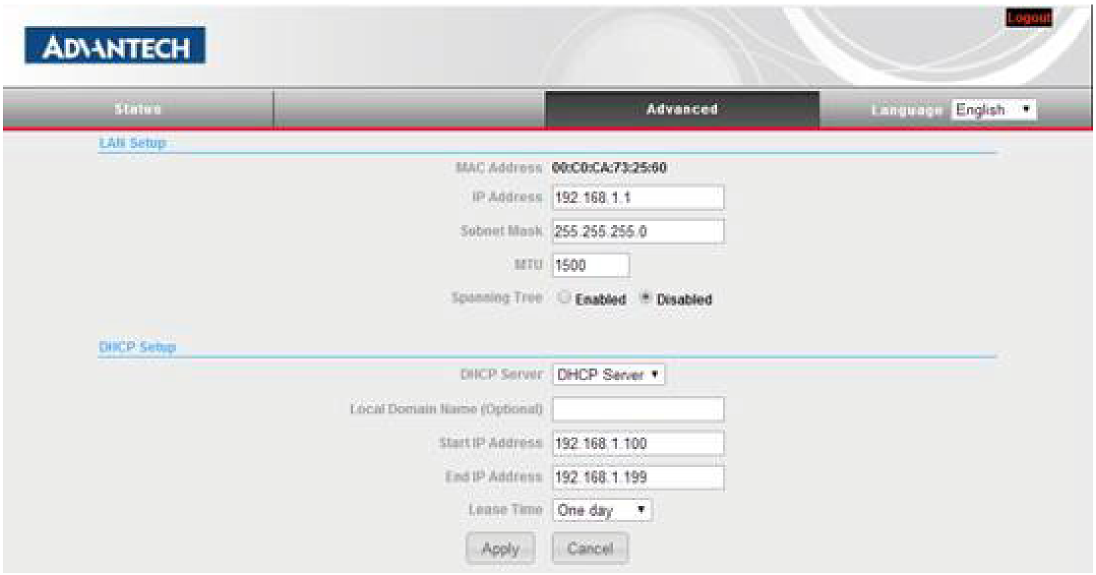
Default Gateway:

DNS Settings

Primary DNS Server:

Secondary DNS Server:

Figure 3.5 WAN Settings



LAN Setup

MAC Address: 00:C0:CA:73:25:60

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

MTU: 1500

Spanning Tree: ○ Enabled ● Disabled

DHCP Setup

DHCP Server: DHCP Server

Local Domain Name (Optional):

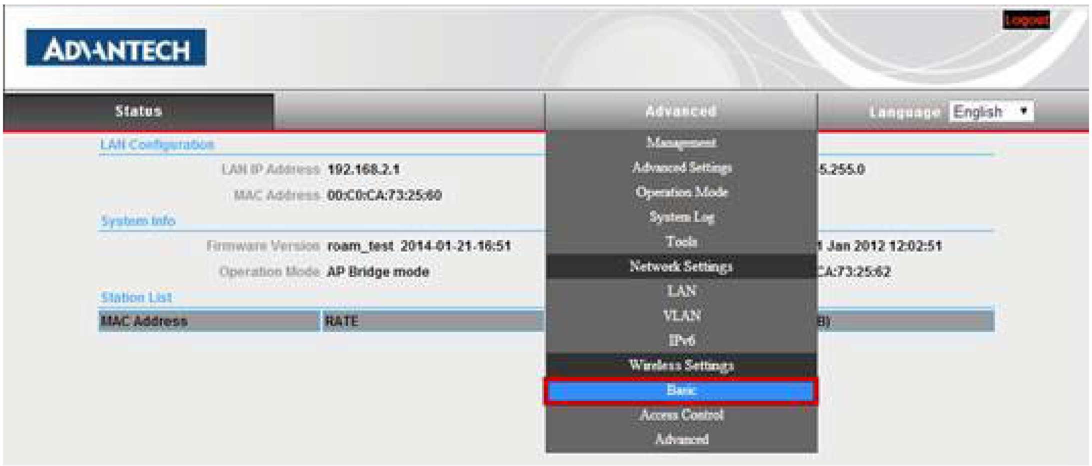
Start IP Address: 192.168.1.100

End IP Address: 192.168.1.199

Lease Time: One day

Figure 3.6 LAN Setting

- Please configure your wireless access point setting in 'Basic' options if you use as access point. Please configure your wireless client setting in 'Basic' options if you use as client.



LAN Configuration

LAN IP Address 192.168.2.1

MAC Address 00:C0:CA:73:25:60

5.255.0

System Info

Firmware Version roam_test 2014-01-21-16:51

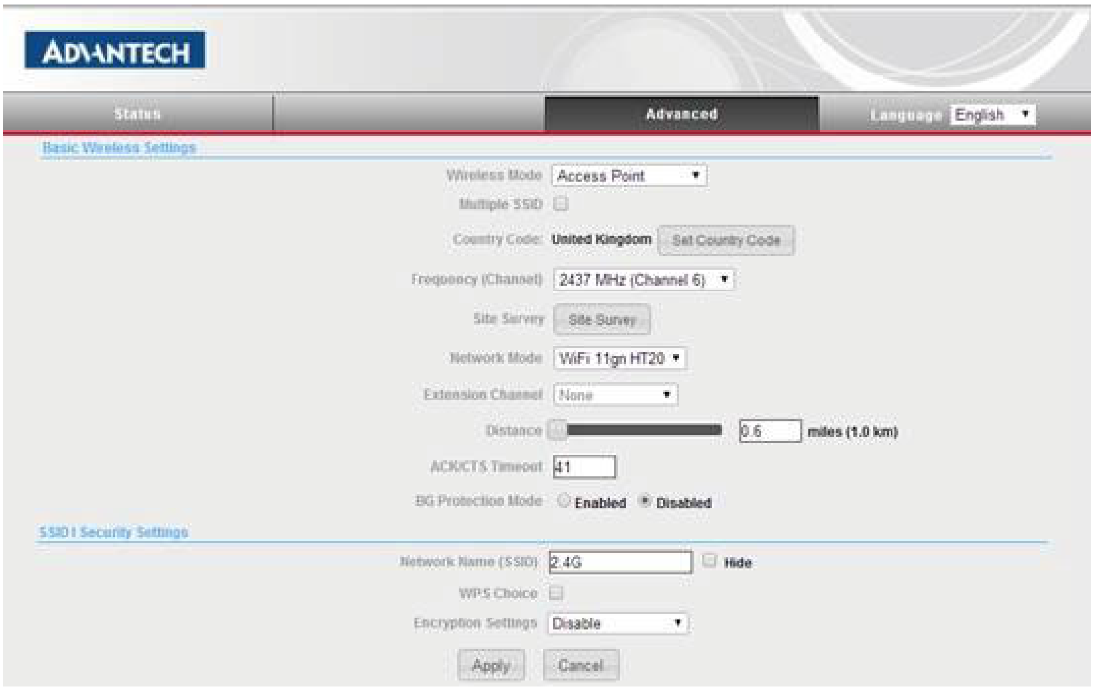
Operation Mode AP Bridge mode

1 Jan 2012 12:02:51

CA:73:25:62

Station List

MAC Address	RATE	B)



Basic Wireless Settings

Wireless Mode: Access Point

Multiple SSID: □

Country Code: United Kingdom

Frequency (Channel): 2437 MHz (Channel 6)

Network Mode: WiFi 11gn HT20

Extension Channel: None

Distance: 0.6 miles (1.0 km)

ACK/CTS Timeout: 41

BG Protection Mode: ○ Enabled ● Disabled

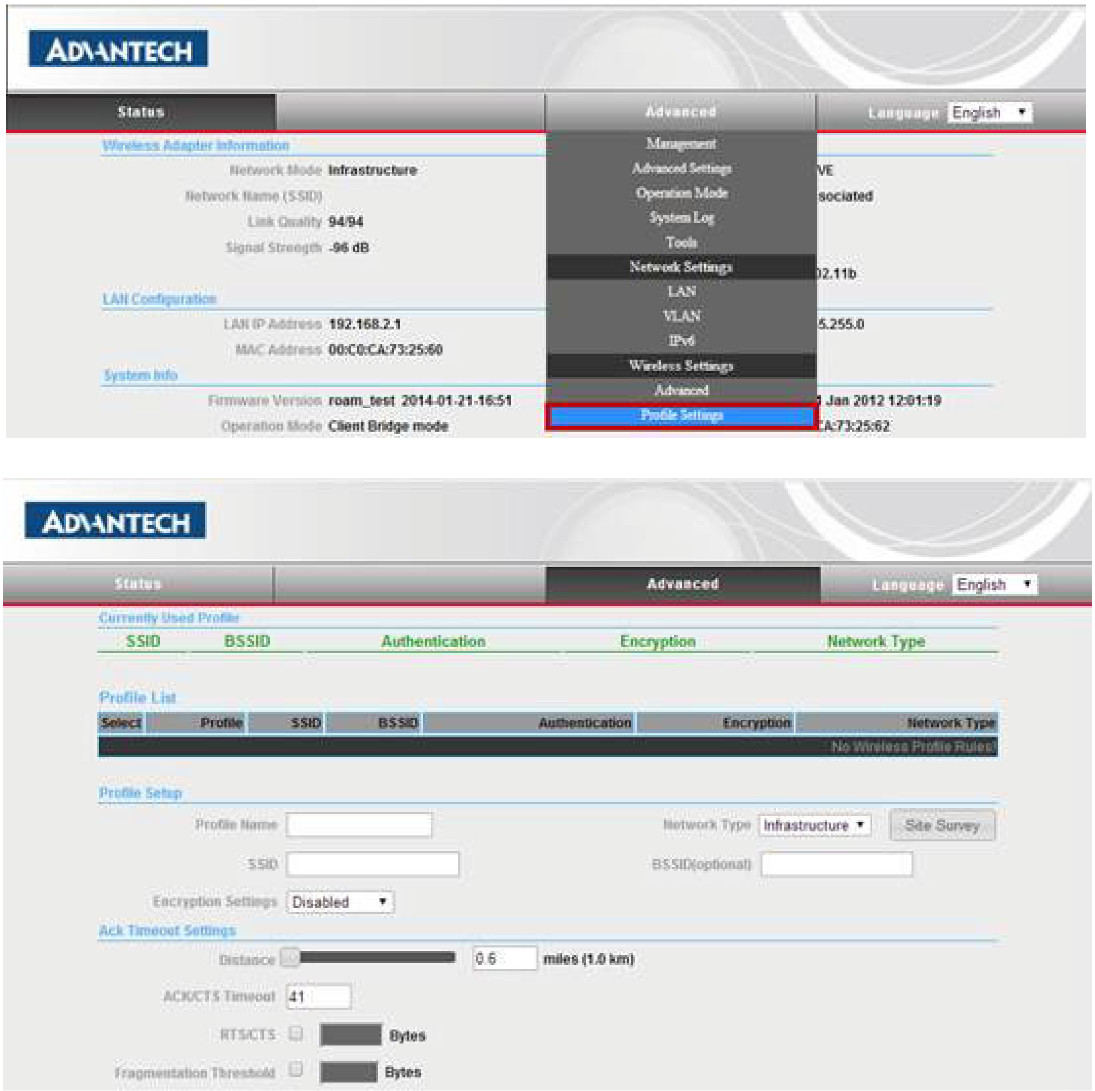
SSID1 Security Settings

Network Name (SSID): 2.4G □ Hide

WPS Choice: □

Encryption Settings: Disable

Figure 3.7 Basic Wireless Access Point Settings



Wireless Adapter Information

Network Mode Infrastructure

Network Name (SSID)

Link Quality 94/94

Signal Strength -96 dB

VE

sociated

02.11b

LAN Configuration

LAN IP Address 192.168.2.1

MAC Address 00:C0:CA:73:25:60

5.255.0

System Info

Firmware Version roam_test 2014-01-21-16:51

Operation Mode Client Bridge mode

1 Jan 2012 12:01:19

CA:73:25:62

Currently Used Profile

SSID	BSSID	Authentication	Encryption	Network Type

Profile List

Select	Profile	SSID	BSSID	Authentication	Encryption	Network Type
						No Wireless Profile Rules!

Profile Setup

Profile Name

Network Type Infrastructure

Site Survey

SSID

BSSID(optional)

Encryption Settings Disabled

Ack Timeout Settings

Distance 0.6 miles (1.0 km)

ACK/CTS Timeout 41

RTS/CTS □ Bytes

Fragmentation Threshold □ Bytes

Figure 3.8 Basic Wireless Client Settings

Chapter 4

Network Settings

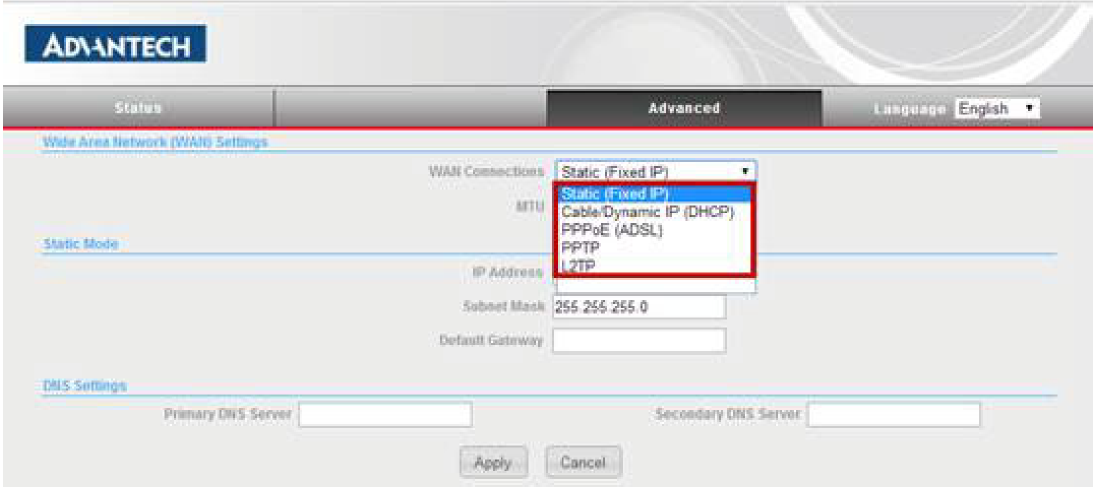
4.1 Router

You can configure the WAN and LAN in your network settings when you use EKI-6310GN as router. In router usage, the Ethernet LAN port will be your WAN interface and wireless LAN will be your LAN interface. EKI-6310GN supports IPv4 or IPv6 in WAN to access the internet. If you use IPv6 in Internet access, please follow the Chapter 4.1.3 to configure your WAN network setting. Otherwise, you can refer to Chapter 4.1.1 to configure your WAN.

Note! *The Ethernet port will convert into WAN port requiring you to configure your CPE via WLAN if you configure EKI-6310GN through Ethernet port in the beginning.*

4.1.1 WAN

You can have five types of WAN connection, including of Static Fixed IP, Cable/ Dynamic IP(DHCP), PPPoE(ADSL), PPTP and L2TP.



Wide Area Network (WAN) Settings

WAN Connections: Static (Fixed IP)

MTU

Static Mode

IP Address

Subnet Mask: 255.255.255.0

Default Gateway

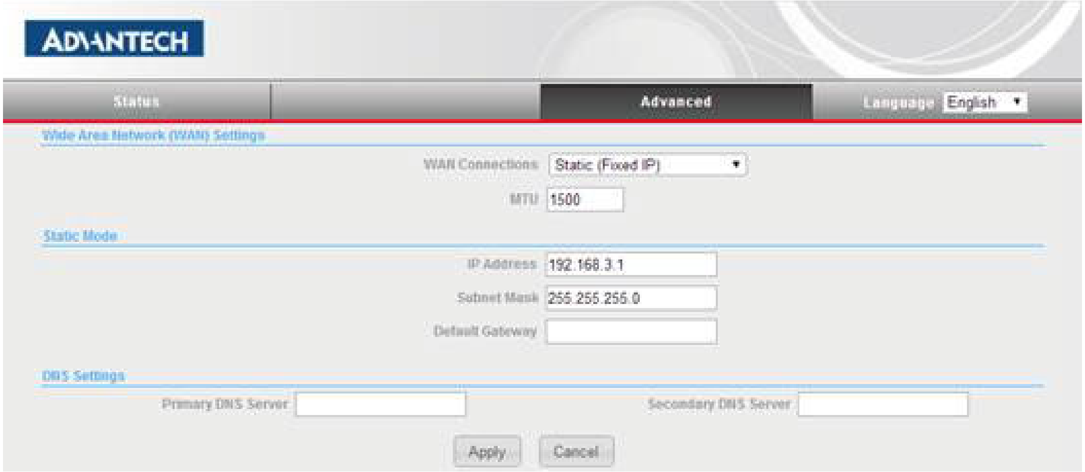
DNS Settings

Primary DNS Server

Secondary DNS Server

Figure 4.1 WAN Settings

- Static Fixed IP
  Select Static (Fixed IP), if your Internet service provider (ISP) to be permanent address on the Internet. A Static IP address is a number (in the form of a dotted quad). Users must enter WAN IP address, Subnet Mask, Gateway setting or DNS settings provided by your ISPs.



Language: English

Wide Area Network (WAN) Settings

WAN Connections: Static (Fixed IP)

MTU: 1500

Static Mode

IP Address: 192.168.3.1

Subnet Mask: 255.255.255.0

Default Gateway:

DNS Settings

Primary DNS Server:

Secondary DNS Server:

Figure 4.2 Static Fixed IP Settings

MTU: Maximum transmission unit (MTU) is the largest protocol data unit that the layer can pass onwards. You need to configure this parameter based on your networking.

IP Address: Sets the static IP address.

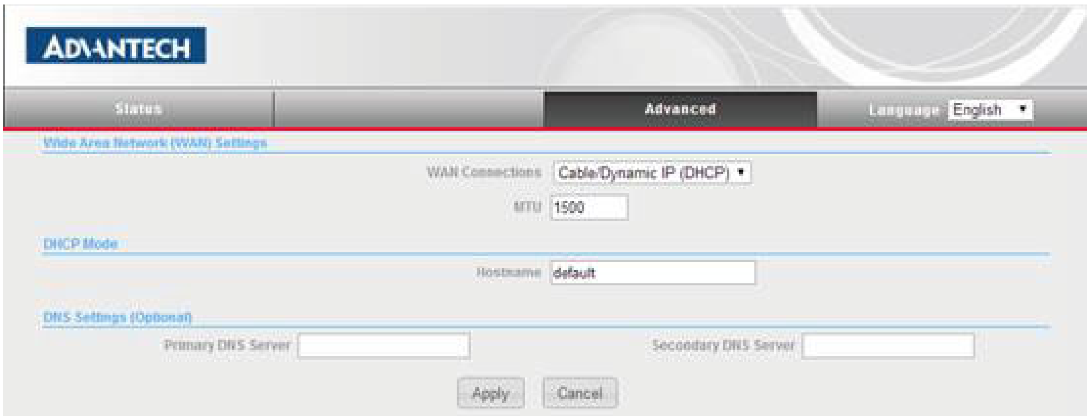
Subnet Mask: Sets the static IP subnet mask. (Default: 255.255.255.0)

Default Gateway: The IP address of a router that is used when the requested destination IP address is not on the local subnet.

Primary DNS Server: The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.

Secondary DNS Server: The IP address of the Secondary Domain Name Server.

- Cable/Dynamic IP
  Select Cable/Dynamic IP (DHCP), if your Internet service provider (ISP) uses a DHCP service to assign your Router an IP address when you connect to the Internet.



Language: English

Wide Area Network (WAN) Settings

WAN Connections: Cable/Dynamic IP (DHCP)

MTU: 1500

DHCP Mode

Hostname: default

DNS Settings (Optional)

Primary DNS Server:

Secondary DNS Server:

Figure 4.3 Cable/Dynamic IP Settings

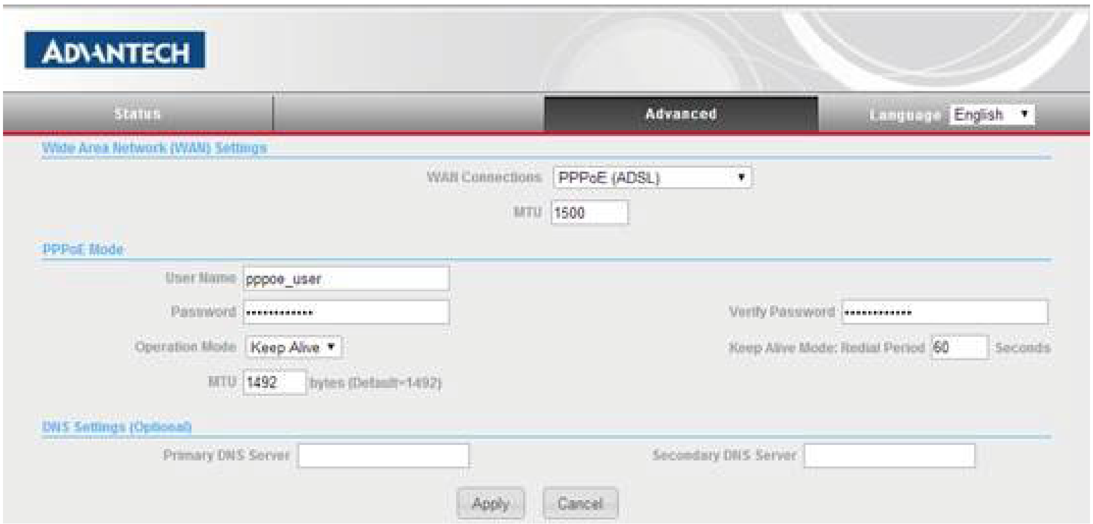
MTU: Maximum transmission unit (MTU) is the largest protocol data unit that the layer can pass onwards. You need to configure this parameter based on your networking.

<u>Hostname</u>: The name of the host on the network providing the IP address

<u>Primary DNS Server</u>: The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.

<u>Secondary DNS Server</u>: The IP address of the Secondary Domain Name Server.

- PPPoE
  Select PPPoE to be assigned automatically from an Internet service provider (ISP) through a DSL modem using Point-to-Point Protocol over Ethernet (PPPoE).



Language: English

Wide Area Network (WAN) Settings

WAN Connections: PPPoE (ADSL)

MTU: 1500

PPPoE Mode

User Name: pppoe_user

Password: •••••••••••••

Verify Password: •••••••••••••

Operation Mode: Keep Alive

Keep Alive Mode: Redial Period 60 Seconds

MTU: 1492 bytes (Default=1492)

DNS Settings (Optional)

Primary DNS Server:

Secondary DNS Server:

Figure 4.4 PPPoE Settings

<u>MTU</u>: Maximum transmission unit (MTU) is the largest protocol data unit that the layer can pass onwards. You need to configure this parameter based on your networking.

<u>Username</u>: Sets the PPPoE dial-in user name for the WAN port.

<u>Password</u>: Sets a PPPoE dial-in password for the WAN port.

<u>Verify Password</u>: Double-confirm the password you key-in in password field.

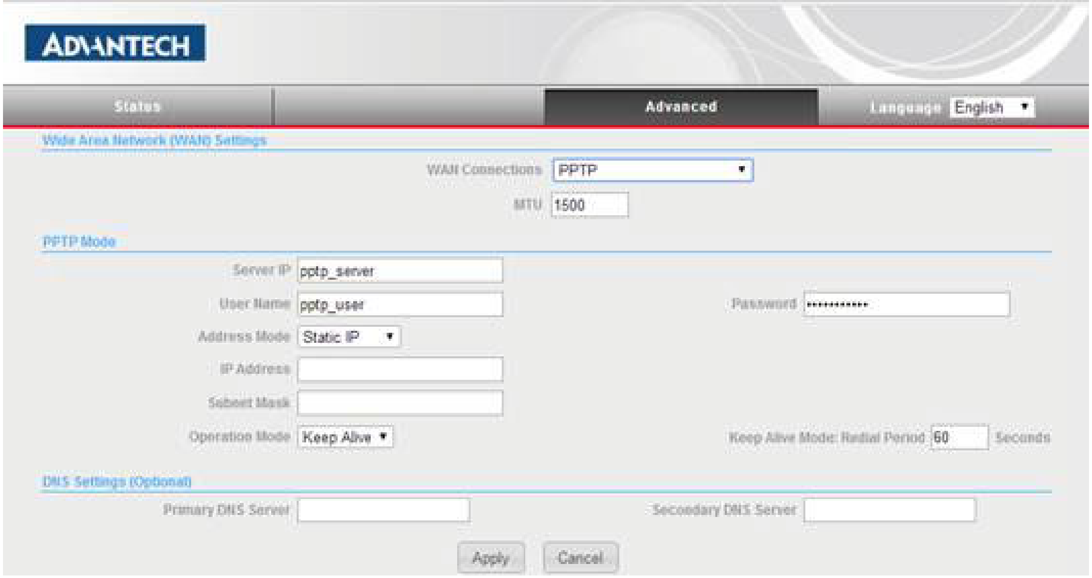
<u>Operation mode</u>: Enables and configures the keep alive time.

<u>Keep Alive Mode</u>: Setup the timer. After the timer, PPPoE will re-dial again.

<u>Primary DNS Server</u>: The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.

<u>Secondary DNS Server</u>: The IP address of the Secondary Domain Name Server.

- PPTP
  Select PPTP, if you are using PPTP service to gain connection to the Internet.



Wide Area Network (WAN) Settings

WAN Connections: PPTP

MTU: 1500

PPTP Mode

Server IP: pptp_server

User Name: pptp_user

Password: ••••••••••••

Address Mode: Static IP

IP Address:

Subnet Mask:

Operation Mode: Keep Alive

Keep Alive Mode: Redial Period 60 Seconds

DNS Settings (Optional)

Primary DNS Server:

Secondary DNS Server:

Figure 4.5 PPTP Settings

MTU: Maximum transmission unit (MTU) is the largest protocol data unit that the layer can pass onwards. You need to configure this parameter based on your networking.

Server IP: Sets the PPTP server IP Address. (Default: pptp_server)

Username: Sets the PPTP user name for the WAN port.

Password: Sets a PPTP password for the WAN port.

Address Mode: Sets a PPTP network mode. (Default: Static IP)

IP Address: Sets the static IP address.

Subnet Mask: Sets the static IP subnet mask. (Default: 255.255.255.0)

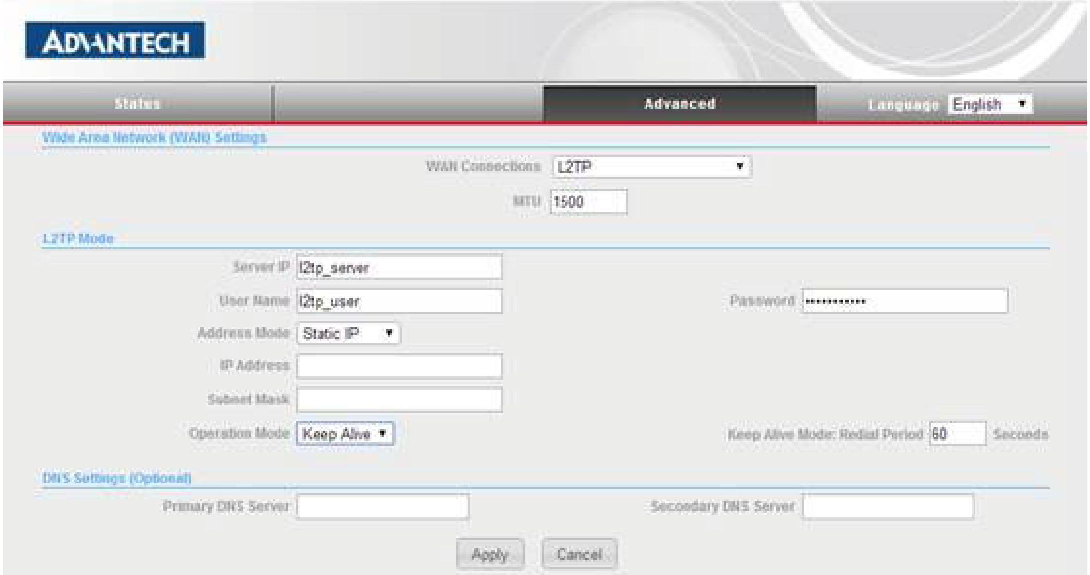
Operation mode: Enables and configures the keep alive time.

Keep Alive Mode: Setup the timer. After the timer, PPTP will re-connect again.

Primary DNS Server: The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.

Secondary DNS Server: The IP address of the Secondary Domain Name Server.

- L2TP
  Select L2TP, if you are using PPTP service to gain connection to the Internet.



Wide Area Network (WAN) Settings

WAN Connections: L2TP

MTU: 1500

L2TP Mode

Server IP: l2tp_server

User Name: l2tp_user

Password: ••••••••••••

Address Mode: Static IP

IP Address:

Subnet Mask:

Operation Mode: Keep Alive

Keep Alive Mode: Redial Period 60 Seconds

DNS Settings (Optional)

Primary DNS Server:

Secondary DNS Server:

Figure 4.6 L2TP Settings

MTU: Maximum transmission unit (MTU) is the largest protocol data unit that the layer can pass onwards. You need to configure this parameter based on your networking.

Server IP: Sets the L2TP server IP Address. (Default: l2tp_server)

Username: Sets the L2TP user name for the WAN port.

Password: Sets a L2TP password for the WAN port.

Address Mode: Sets a L2TP network mode. (Default: Static IP)

IP Address: Sets the static IP address.

Subnet Mask: Sets the static IP subnet mask. (Default: 255.255.255.0)

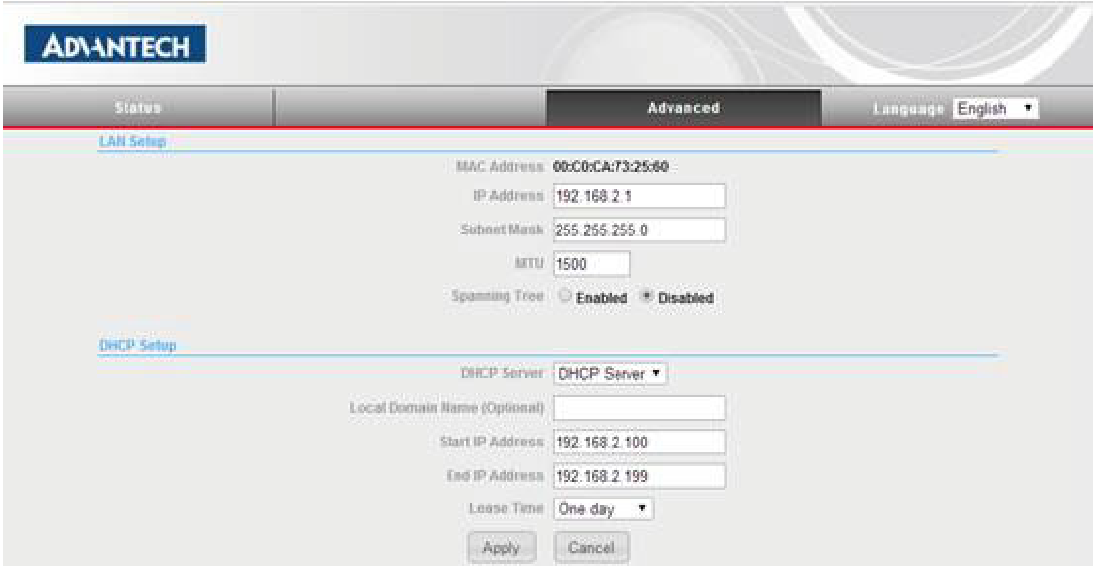
Operation mode: Enables and configures the keep alive time.

Keep Alive Mode: Setup the timer. After the timer, L2TP will re-connect again.

Primary DNS Server: The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.

Secondary DNS Server: The IP address of the Secondary Domain Name Server.

4.1.2 LAN



LAN Setup

MAC Address 00:C0:CA:73:25:60

IP Address 192.168.2.1

Subnet Mask 255.255.255.0

MTU 1500

Spanning Tree ○ Enabled ● Disabled

DHCP Setup

DHCP Server DHCP Server ▾

Local Domain Name (Optional)

Start IP Address 192.168.2.100

End IP Address 192.168.2.199

Lease Time One day ▾

Figure 4.7 LAN Settings in router

IP Address: Sets the static IP address for your LAN interface.

Subnet Mask: Sets the static IP subnet mask. (Default: 255.255.255.0)

MTU: Maximum transmission unit (MTU) is the largest protocol data unit that the layer can pass onwards. You need to configure this parameter based on your networking.

Spanning Tree: Enable or Disable STP (spanning-tree protocol). Spanning Tree Protocol (STP) is a link management protocol for AP which provides path redundancy while preventing loops in a network. STP allows only one active path at a time between the access points but establish the redundant link as a backup if the initial link fails. DHCP Server: You have three options for DHCP Server configuration, including of 'Disable', 'DHCP Relay' and 'DHCP Server'. When you disable DHCP Server service, you will don't need to configuration assigned IP range. If you configure to 'DHCP Relay', you will need to configure the DHCP Relay server and your device will relay the DHCP request to DHCP server.

DHCP Relay: Assign the IP of DHCP server in your network, and EKI-6310GN will forward DHCP request to DHCP server that you assign.

Local Domain Name: Optional, you can enter local domain name for your network

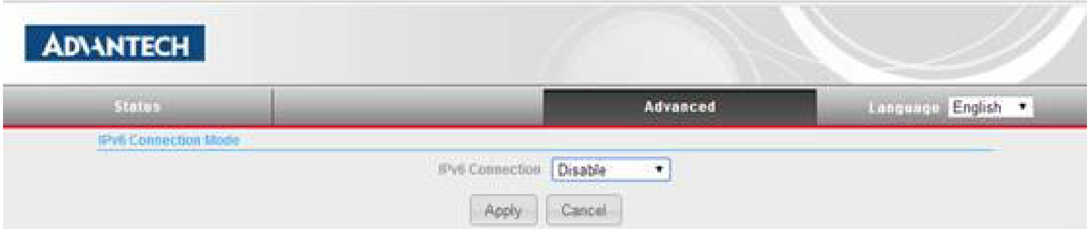
Start IP Address: Starting IP Address for the server's IP assignment

End IP Address: Ending IP Address for the server's IP assignment

Lease Time: The time period for the IP address lease

4.1.3 IPV6

You can have seven types of IPv6 Internet connection, including of Static Fixed IPv6, SLAAC, DHCPv6, 6in4 Tunnel, 6to4 Tunnel, IPV6 PPPoE and IPv6 pass through.

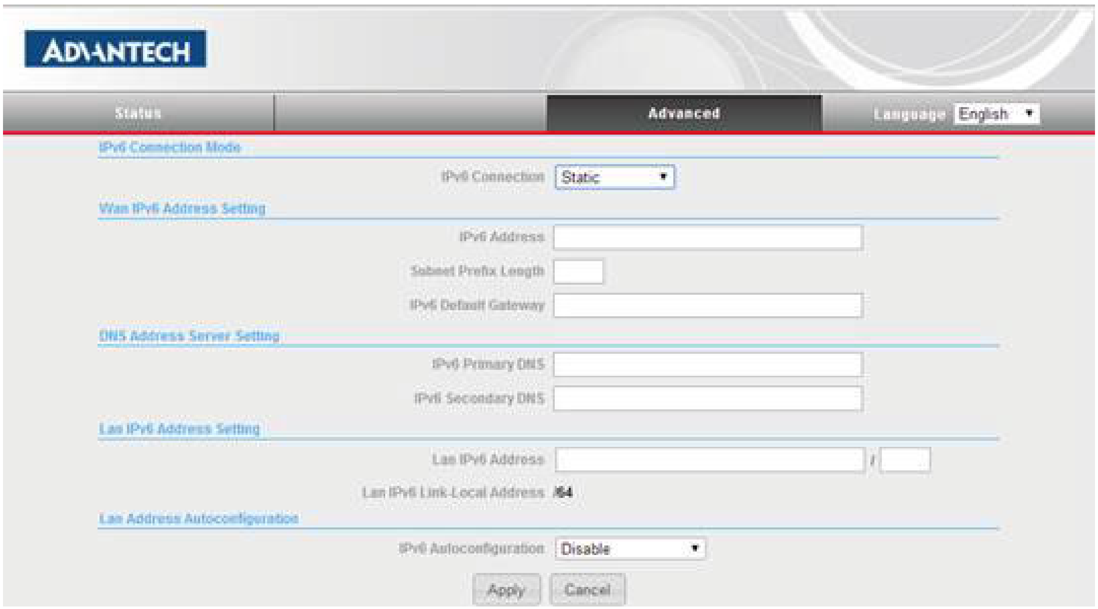


IPv6 Connection Mode

IPv6 Connection: Disable

Figure 4.8 IPv6 Settings

- Static Fixed IPv6
  Select Static (Fixed IP), if your ISP provides you with a set IPv6 addresses that does not change. The IPv6 information is manually entered in your IPv6 configuration settings.



IPv6 Connection Mode

IPv6 Connection: Static

Wan IPv6 Address Setting

IPv6 Address

Subnet Prefix Length

IPv6 Default Gateway

DNS Address Server Setting

IPv6 Primary DNS

IPv6 Secondary DNS

Lan IPv6 Address Setting

Lan IPv6 Address /

Lan IPv6 Link-Local Address /64

Lan Address Autoconfiguration

IPv6 Autoconfiguration: Disable

Figure 4.9 Static Fixed IPv6 Settings

IPv6 Address: Enter the WAN IPv6 address for the router here.

Subnet Prefix Length: Enter the WAN subnet prefix length value used here

IPv6 Default Gateway: Enter the WAN default gateway IPv6 address used here.

IPV6 Primary DNS Server: Enter the WAN primary DNS Server address used here.

IPV6 Secondary DNS Server: Enter the WAN secondary DNS Server address used here.

LAN IPv6 IP Address: These are the settings of the LAN (Local Area Network) IPv6 interface for the router. The router's LAN IPv6 Address configuration is based on the IPv6 Address and Subnet assigned by your ISP. (A subnet with prefix /64 is supported in LAN.)

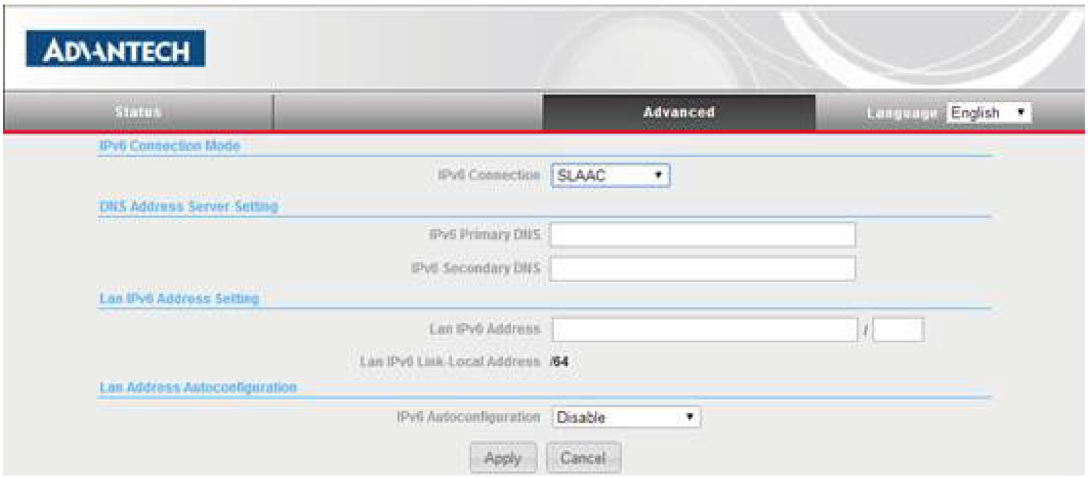
IPV6 AutoConfiguration: EKI-6310GN autonomously configures its own Link-Local address. Router solicitation is sent by booting nodes to request RAs for configuring the interfaces.

- SLAAC

  SLAAC is IPv6 Stateless Address Auto-configuration. EKI-6310GN will use this SLAAC technology to get prefix and generate Host ID (by EUI-64 algorithm). EKI-6310GN will use those two information as IPv6 address.

  Network ID (Prefix): 64bits   Host ID: 64bits

  IPv6 Address: ⟷ : ⟷



IPv6 Connection Mode

IPv6 Connection: SLAAC

DNS Address Server Setting

IPv6 Primary DNS:

IPv6 Secondary DNS:

Lan IPv6 Address Setting

Lan IPv6 Address: /

Lan IPv6 Link-Local Address: /64

Lan Address Autoconfiguration

IPv6 Autoconfiguration: Disable

Figure 4.10 SLAAC Settings

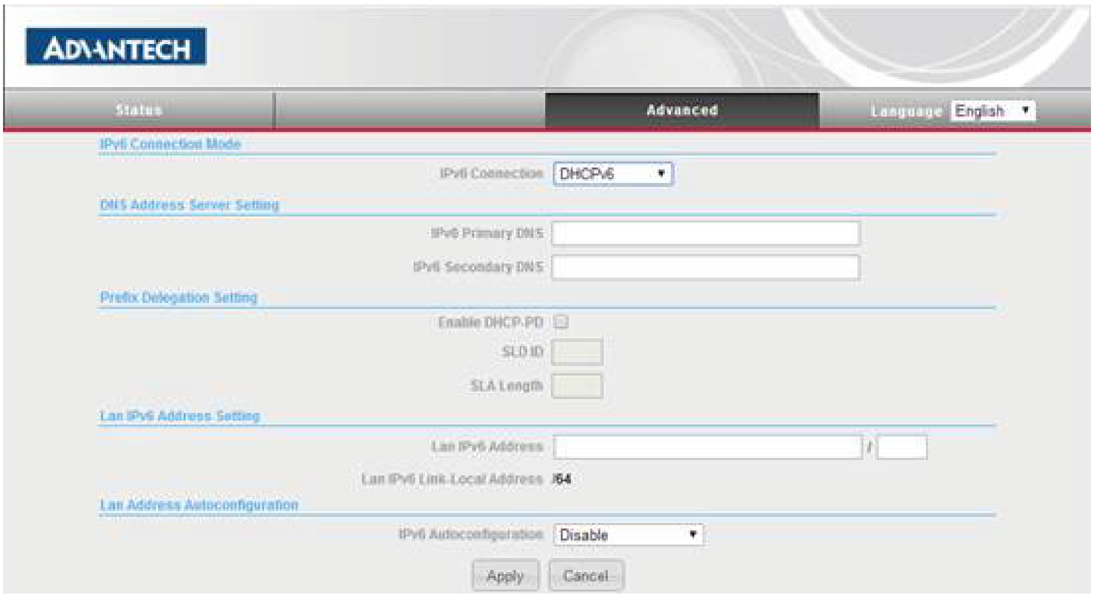
IPV6 Primary DNS Server: Enter the WAN primary DNS Server address used here.

IPV6 Secondary DNS Server: Enter the WAN secondary DNS Server address used here.

LAN IPv6 IP Address: These are the settings of the LAN (Local Area Network) IPv6 interface for the router. The router's LAN IPv6 Address configuration is based on the IPv6 Address and Subnet assigned by your ISP. (A subnet with prefix /64 is supported in LAN.)

IPV6 AutoConfiguration: EKI-6310GN autonomously configures its own Link-Local address. Router solicitation is sent by booting nodes to request RAs for configuring the interfaces.

- DHCPv6
  DHCPv6 provides a means of passing additional configuration options to nodes after they obtain their IPv6 addresses.



IPv6 Connection Mode

IPv6 Connection: DHCPv6

DNS Address Server Setting

IPv6 Primary DNS:

IPv6 Secondary DNS:

Prefix Delegation Setting

Enable DHCP-PD: □

SLD ID:

SLA Length:

Lan IPv6 Address Setting

Lan IPv6 Address: /

Lan IPv6 Link-Local Address: /64

Lan Address Autoconfiguration

IPv6 Autoconfiguration: Disable

Figure 4.11 DHCPv6 Settings

IPV6 Primary DNS Server: Enter the WAN primary DNS Server address used here.

IPV6 Secondary DNS Server: Enter the WAN secondary DNS Server address used here.

Ebable DHCP-PD: Enable DHCP-PD Support.

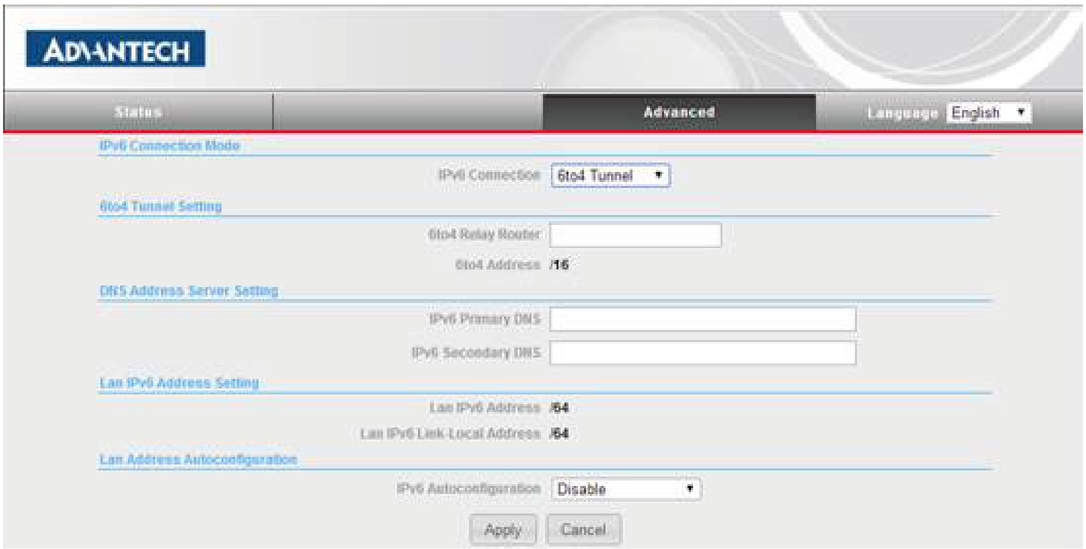
SLD ID: Site-Level Aggregation Identifier

SLA Length: Length of site-level aggregation identifier (SLA).

LAN IPv6 IP Address: These are the settings of the LAN (Local Area Network) IPv6 interface for the router. The router's LAN IPv6 Address configuration is based on the IPv6 Address and Subnet assigned by your ISP. (A subnet with prefix /64 is supported in LAN.)

IPV6 AutoConfiguration: EKI-6310GN autonomously configures its own Link-Local address. Router solicitation is sent by booting nodes to request RAs for configuring the interfaces.

- 6to4 Tunnel
  6to4 tunnel is an automatic tunnel method to tunnel IPv6 packets into IPv4 packets based on RFC3056. As time progressed, implementations came about allowing the tunnel to originate and terminate directly from personal computers using the same 6to4 protocol. This means that computers that are on IPv4-only networks can talk to computers on IPv6-only networks. It is the mode of 6to4 that we will focus on here. It gives a prefix to the attached IPv6 network in 6to4 tunnel mode.



IPv6 Connection Mode

IPv6 Connection: 6to4 Tunnel

6to4 Tunnel Setting

6to4 Relay Router:

6to4 Address: /16

DNS Address Server Setting

IPv6 Primary DNS:

IPv6 Secondary DNS:

Lan IPv6 Address Setting

Lan IPv6 Address: /64

Lan IPv6 Link-Local Address: /64

Lan Address Autoconfiguration

IPv6 Autoconfiguration: Disable

Figure 4.12 6to4 Tunnel Settings

IPV6 Primary DNS Server: Enter the WAN primary DNS Server address used here.

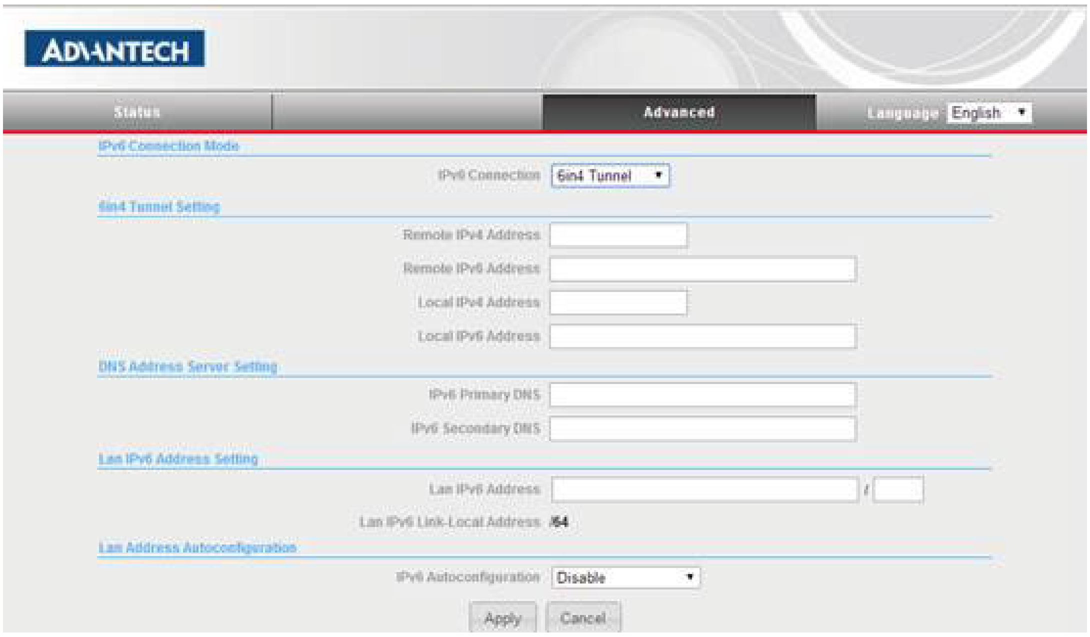
IPV6 Secondary DNS Server: Enter the WAN secondary DNS Server address used here.

6to4 Relay Router: The IPv6 address of 6to4 Relay Router

LAN IPv6 IP Address: These are the settings of the LAN (Local Area Network) IPv6 interface for the router. The router's LAN IPv6 Address configuration is based on the IPv6 Address and Subnet assigned by your ISP. (A subnet with prefix /64 is supported in LAN.)

IPV6 AutoConfiguration: EKI-6310GN autonomously configures its own Link-Local address. Router solicitation is sent by booting nodes to request RAs for configuring the interfaces.

- 6in4 Tunnel
  IPv6 in IPv4 tunneling is an Internet transition mechanism for migrating from IPv4 to IPv6. 6in4 uses tunneling to encapsulate IPv6 traffic over explicitly configured IPv4 lines as defined in RFC 4213.



IPv6 Connection Mode

IPv6 Connection: 6in4 Tunnel

6in4 Tunnel Setting

Remote IPv4 Address:

Remote IPv6 Address:

Local IPv4 Address:

Local IPv6 Address:

DNS Address Server Setting

IPv6 Primary DNS:

IPv6 Secondary DNS:

Lan IPv6 Address Setting

Lan IPv6 Address: /

Lan IPv6 Link-Local Address: /64

Lan Address Autoconfiguration

IPv6 Autoconfiguration: Disable

Figure 4.13 6in4 Tunnel Settings

Remote IPv4 Address: Remote IPv4 address for your ISP account.

Remote IPv6 Address: Remote IPv6 address for your ISP account.

Local IPv4 Address: Local IPv4 address for your ISP account

Local IPv6 Address: Local IPv6 address for your ISP account

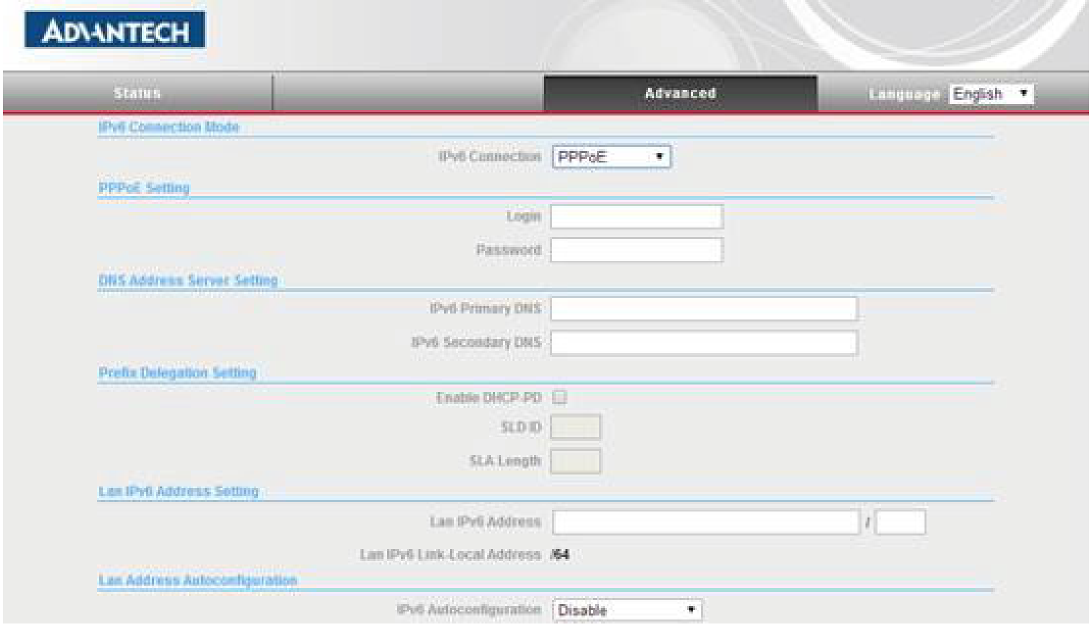
IPV6 Primary DNS Server: Enter the WAN primary DNS Server address used here.

IPV6 Secondary DNS Server: Enter the WAN secondary DNS Server address used here.

LAN IPv6 IP Address: These are the settings of the LAN (Local Area Network) IPv6 interface for the router. The router's LAN IPv6 Address configuration is based on the IPv6 Address and Subnet assigned by your ISP. (A subnet with prefix /64 is supported in LAN.)

IPV6 AutoConfiguration: EKI-6310GN autonomously configures its own Link-Local address. Router solicitation is sent by booting nodes to request RAs for configuring the interfaces.

- IPv6 PPPoE
  Use Point-to-Point Protocol over Ethernet (PPPoE) network protocol to dial-in ISP network.



IPv6 Connection Mode

IPv6 Connection: PPPoE

PPPoE Setting

Login

Password

DNS Address Server Setting

IPv6 Primary DNS

IPv6 Secondary DNS

Prefix Delegation Setting

Enable DHCP-PD ☐

SLD ID

SLA Length

Lan IPv6 Address Setting

Lan IPv6 Address /

Lan IPv6 Link-Local Address /64

Lan Address Autoconfiguration

IPv6 Autoconfiguration: Disable

Figure 4.14 IPv6 PPPoE Settings

Login: Enter your PPPoE user name.

Password: Enter your PPPoE password and then retype the password in the next box.

IPV6 Primary DNS Server: Enter the WAN primary DNS Server address used here.

IPV6 Secondary DNS Server: Enter the WAN secondary DNS Server address used here.

Ebable DHCP-PD: Enable DHCP-PD Support.

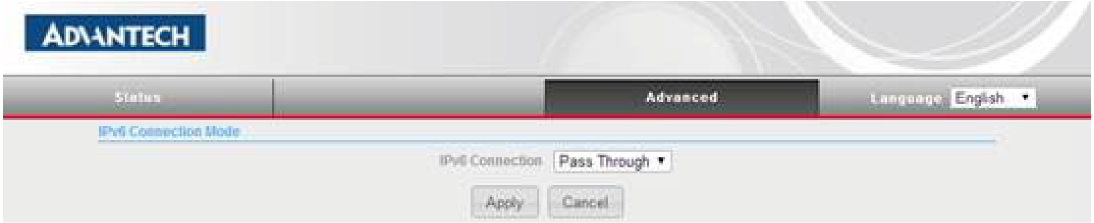
SLD ID: Site-Level Aggregation Identifier

SLA Length: Length of site-level aggregation identifier (SLA).

LAN IPv6 IP Address: These are the settings of the LAN (Local Area Network) IPv6 interface for the router. The router's LAN IPv6 Address configuration is based on the IPv6 Address and Subnet assigned by your ISP. (A subnet with prefix /64 is supported in LAN.)

IPV6 AutoConfiguration: EKI-6310GN autonomously configures its own Link-Local address. Router solicitation is sent by booting nodes to request RAs for configuring the interfaces.

- IPv6 Pass Through
  In pass-through mode, the router works as a Layer 2 Ethernet switch with two ports (LAN and WAN Ethernet ports) for IPv6 packets. The router does not process any IPv6 header packets.



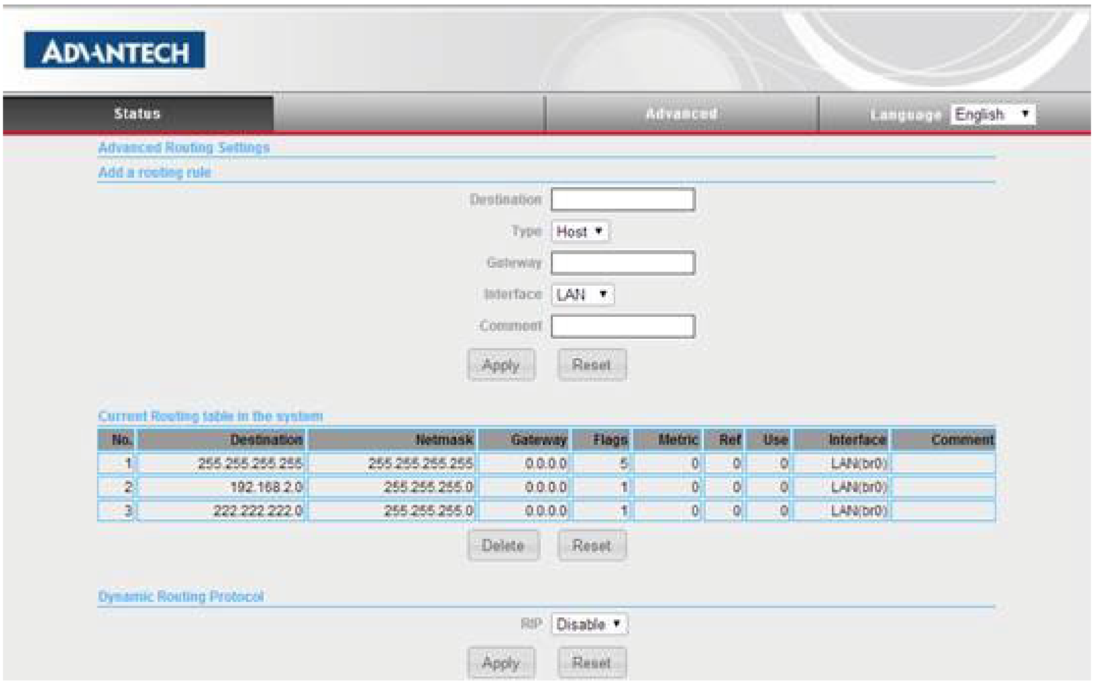
IPv6 Connection Mode

IPv6 Connection: Pass Through ▾

Figure 4.15 IPv6 Pass Through Settings

4.1.4 Advanced Routing

EKI-6310GN allows you to configure advanced routing feature.



Advanced Routing Settings

Add a routing rule

Destination:
Type: Host ▾
Gateway:
Interface: LAN ▾
Comment:

Current Routing table in the system

No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface	Comment
1	255.255.255.255	255.255.255.255	0.0.0.0	5	0	0	0	LAN(br0)	
2	192.168.2.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN(br0)	
3	222.222.222.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN(br0)	

Dynamic Routing Protocol

RIP: Disable ▾

Figure 4.16 Advanced Routing

Destination: The IP address of packets that can be routed.

Type: Defines the type of destination. (Host: Signal IP address / Net: Portion of Network)

Netmask: Displays the sub network associated with the destination.

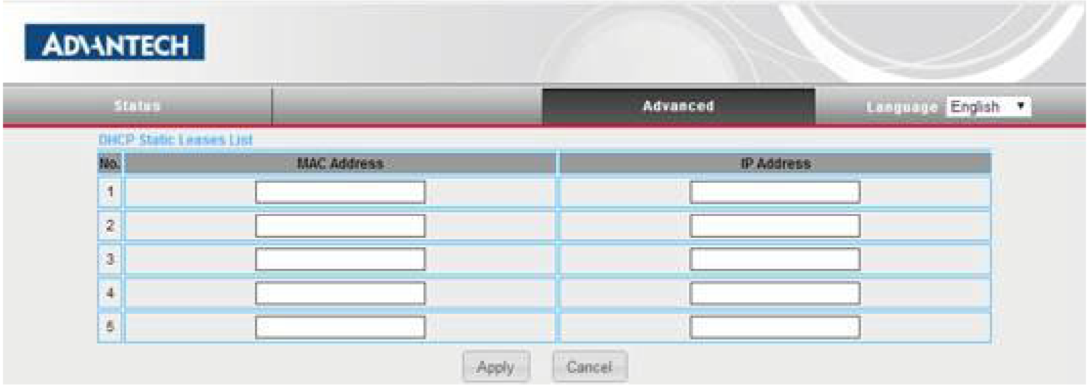
Gateway: Defines the packets destination next hop. Interface: Select interface to which a static routing subnet is to be applied.

Comment: Help identify the routing.

RIP: Enable or disable the RIP (Routing Information Protocol) for the WAN or LAN interface

4.1.5 DHCP STATIC LEASED (STATIC DHCP)

EKI-6310GN provides a solution to this mess: static DHCP, also known as DHCP reservation. While configuring your router for DHCP, you have the ability to enter the MAC addresses of Client and enter which IP address to assign them. EKI-6310GN will automatically take care of rest.



DHCP Static Leases List

No.	MAC Address	IP Address
1		
2		
3		
4		
5		

Figure 4.17 Static DHCP

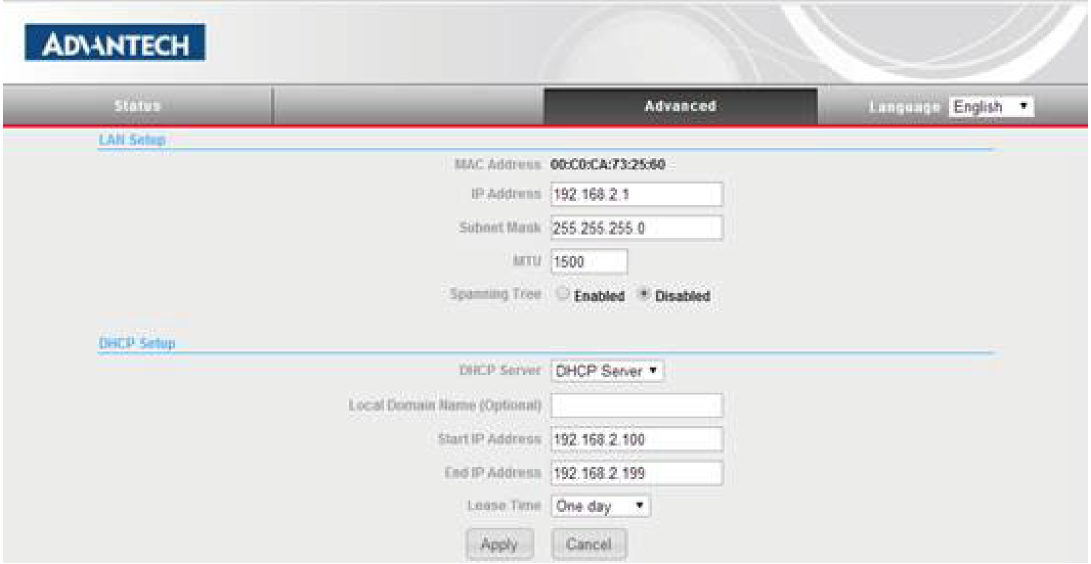
MAC Address: Enter the MAC address of client.

IP Address: Assign them an IP address. You won't be able to add the same IP address to two different MAC addresses, so make sure each MAC has a unique IP.

4.2 Bridge

You can configure the LAN in your network settings when you use EKI-6310GN as bridge.

4.2.1 LAN



LAN Setup

MAC Address 00:C0:CA:73:25:60
IP Address 192.168.2.1
Subnet Mask 255.255.255.0
MTU 1500
Spanning Tree ○ Enabled ● Disabled

DHCP Setup

DHCP Server DHCP Server
Local Domain Name (Optional)
Start IP Address 192.168.2.100
End IP Address 192.168.2.199
Lease Time One day

Figure 4.18 LAN Settings in router

IP Address: Sets the static IP address for your LAN interface.

Subnet Mask: Sets the static IP subnet mask. (Default: 255.255.255.0)

MTU: Maximum transmission unit (MTU) is the largest protocol data unit that the layer can pass onwards. You need to configure this parameter based on your networking.

Spanning Tree: Enable or Disable STP (spanning-tree protocol). The spanning-tree algorithm calculates the best loop-free path throughout a Layer 2 network. DHCP Server: You have three options for DHCP Server configuration, including of 'Disable', 'DHCP Relay' and 'DHCP Server'. When you disable DHCP Server service, you will don't need to configuration assigned IP range. If you configure to 'DHCP Relay', you will need to configure the DHCP Relay server and your device will relay the DHCP request to DHCP server.

DHCP Relay: Assign the IP of DHCP server in your network, and EKI-6310GN will forward DHCP request to DHCP server that you assign.

Local Domain Name: Optional, you can enter local domain name for your network

Start IP Address: Starting IP Address for the server's IP assignment

End IP Address: Ending IP Address for the server's IP assignment

Lease Time: The time period for the IP address lease

Chapter 5

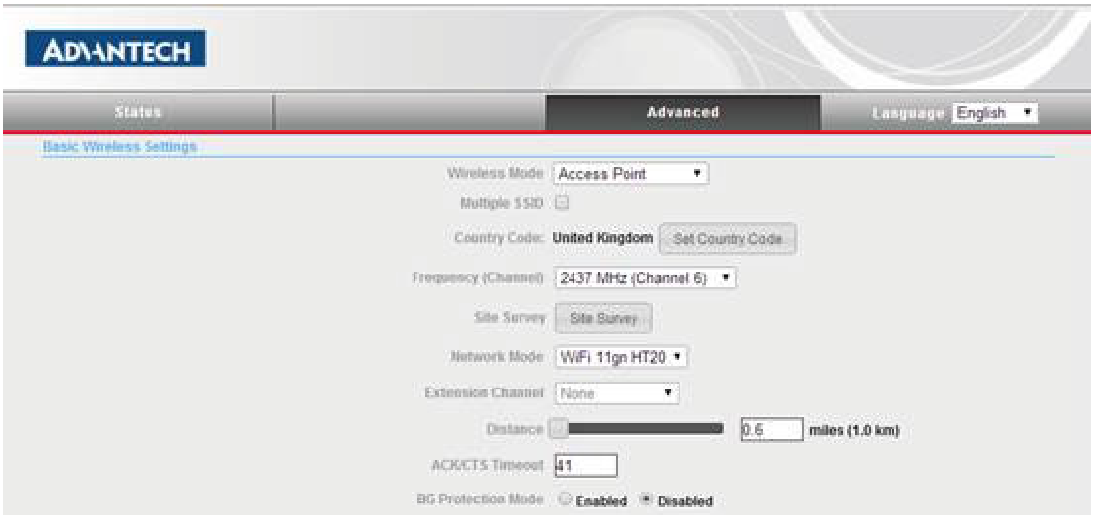
Wireless Access Point Settings

This chapter describes Access Point configuration, including of Access Point, WDS Access Point and WDS Repeater.

5.1 Access Point

In Access Point Mode, the EKI-6310GN connects your wireless devices together, and it also allows a connected wired device to connect to your other devices wirelessly. This can be useful if you already had an existing Internet router that does not have built-in wireless capabilities or used this to create a private wireless network without Internet access so that your devices can securely connect to one another without being exposed to the Internet or other computers.

5.1.1 Basic Wireless Settings



Basic Wireless Settings

Wireless Mode: Access Point

Multiple SSID: □

Country Code: United Kingdom

Frequency (Channel): 2437 MHz (Channel 6)

Network Mode: WiFi 11gn HT20

Extension Channel: None

Distance: 0.6 miles (1.0 km)

ACK/CTS Timeout: 41

BG Protection Mode: ○ Enabled ● Disabled

Figure 5.1 Basic Wireless Settings in AP mode

Wireless mode: You have three options (Access Point, WDS Access Point or WDS Repeater)

Multiple SSID: Enable or Disable multiple SSIDs support. When you enable this option, you will have maximum two SSIDs (Configure in 'SSID I' and 'SSID II').

Country Code: The availability of some specific channels and/or operational frequency bands is country dependent.

Frequency (Channel): Channel varies much as the available band differs from country to country. Select a proper operating channel in the drop-down list according to your situation. Site Survey: You can scan the available access point in site survey action.

Network Mode: Four levels are available: 5MHz, 10MHz, 20MHz and 40MHz. The last one can enhance data throughput, but it takes more bandwidth, thus it might cause potential interference.

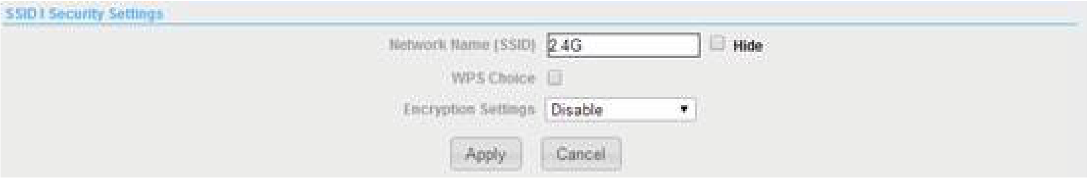
Extension Channel: This is to avoid conflict with other wireless network and boost the ability of your device to catch all 802.11g transmissions. However, it may decrease wireless network performance. Compared to CTS-Self; the transmission amount of CTS-RTS is much lower.

Distance: To decrease the chances of data retransmission at long distance, the EKI-6310GN can automatically adjust proper ACK timeout value by specifying distance of the two nodes.

ACK/CTS Timeout: ACK/CTS timeout will be adjusted by distance automatically

BG Protection Mode: The time period for the IP address lease

5.1.2 SSID Security Settings



SSID I Security Settings

Network Name (SSID) 2.4G □ Hide

WPS Choice □

Encryption Settings Disable

Figure 5.2 Security settings

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

Hide SSID: Under AP mode, hiding network name is necessary when you are in a wireless environment that may have potential risk. By hided broadcast SSID, the STA CAN NOT scan and find EKI-6310GN, so that malicious attack by some illegal STA could be avoided.

WPS Choice: Wi-Fi Protected Setup (WPS) System is a simplified way to set up the basic encryption of the EKI-6310GN. It can also be used to automatically create a secure wireless connection to a wireless client.

Encryption Setting: Select the wireless encryption used by the Access Point that you provide for connection. There are nine encryption modes including of no encryption, WEP-AUTO, WPA, WPA-PSK, WPA-AUTO, WPA-AUTO-PSK, WPA2, WPA2-PSK and 802.1x. WEP is the original wireless encryption standard. WPA provides a higher level of security and WPA-Personal does not require an authentication server. When 802.1x encryption is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.

- WEP-AUTO
  In WEP-AUTO option, it can support 64-bit or 128-bit encryption automatically. You can enter up to 4 different keys.

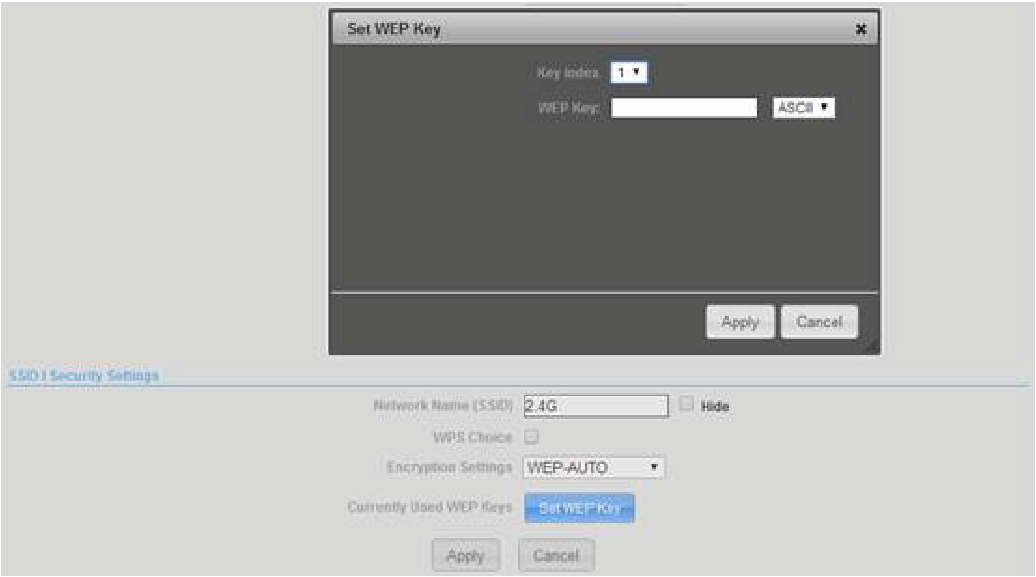
  Key Index: You can configure up to 4 different keys.

  WEP Key: encryption key you want to create.

  ASCII/Hex: Select key type either Hex or ASCII.

  Hex (recommended) - Letters A-F and numbers 0-9 are valid.

  ASCII - All numbers and letters are valid.



Set WEP Key ×

Key Index 1

WEP Key: ASCII

SSID I Security Settings

Network Name (SSID) 2.4G □ Hide

WPS Choice □

Encryption Settings WEP-AUTO

Currently Used WEP Keys Set WEP Key

Figure 5.3 WEP Encryption

- WPA
  WPA (Wi-Fi Protected Access), is a Wi-Fi standard that was designed to improve the security features of WEP (Wired Equivalent Privacy). WPA improved data encryption through the different cipher modes, including of Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES).

  WPA-PSK/WPA2-PSK uses a passphrase or key to authenticate your wireless connection. The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. This key must be the exact same key entered on your wireless router or access point.

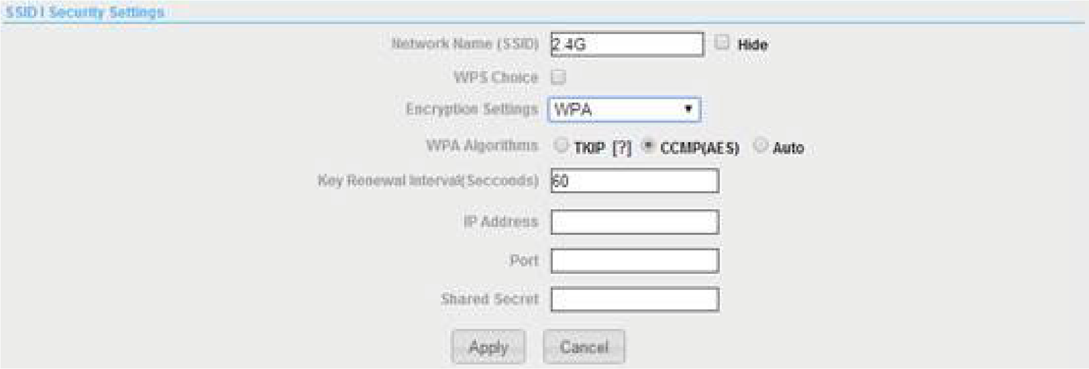
  WPA Algorithms: Select the cipher mode either TKIP, AES or Auto-selection

  Key Renewal Interval: The period of time that EKI-6310GN will use the same key before a new one is generated. The recommend value is 3600 seconds (1 hour).

  IP Address: Optional, the IP address of Radius Server. The configuration is required for accounting using a Radius Server.

  Port: Optional, the Port number of Radius Server. The configuration is required for accounting using a Radius Server.

  Shared Secret: Optional, that is shared between the EKI-6310GN and the Radius Server while authenticating the supplicant. The configuration is required for accounting using a Radius Server.



SSID I Security Settings

Network Name (SSID): 2.4G ☐ Hide

WPS Choice ☐

Encryption Settings: WPA ▾

WPA Algorithms: ○ TKIP [?] ● CCMP(AES) ○ Auto

Key Renewal Interval(Secconds): 60

IP Address:

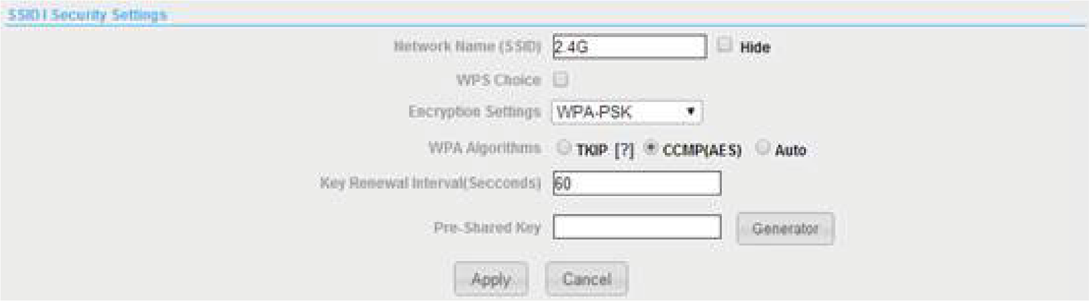
Port:

Shared Secret:

Figure 5.4 WPA Encryption

- WPA-PSK
  WPA-PSK (Pre-Shared Key) uses a passphrase or key to authenticate your wireless connection. The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. This key must be the exact same key entered on your wireless router or access point.
  WPA Algorithms: Select the cipher mode either TKIP, AES or Auto-selection
  Key Renewal Interval: The period of time that EKI-6310GN will use the same key before a new one is generated. The recommend value is 3600 seconds (1 hour).

  Pre-Shared Key: enter a key (passphrase). The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. Make sure you enter this key exactly the same on all other wireless clients.



SSID I Security Settings

Network Name (SSID): 2.4G □ Hide

WPS Choice: □

Encryption Settings: WPA-PSK

WPA Algorithms: ○ TKIP [?] ● CCMP(AES) ○ Auto

Key Renewal Interval(Secconds): 60

Pre-Shared Key: Generator

Figure 5.5 WPA-PSK Encryption

- WPA2

  WPA2 (Wi-Fi Protected Access 2), is a Wi-Fi standard that was designed to improve the security features of WEP and WPA. WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead of TKIP. In particular, it introduces CCMP, a new AES-based encryption mode with strong security.

  WPA2-PSK uses a passphrase or key to authenticate your wireless connection. The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. This key must be the exact same key entered on your wireless router or access point.

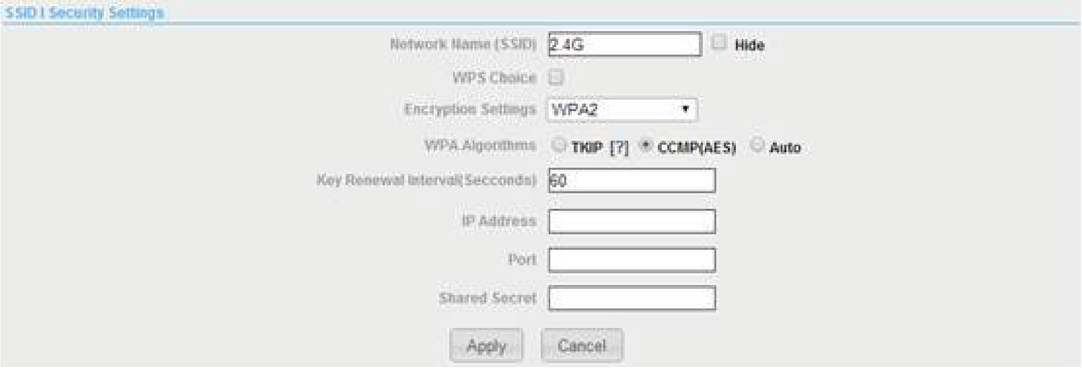
  WPA Algorithms: Select the cipher mode either TKIP, AES or Auto-selection

  Key Renewal Interval: The period of time that EKI-6310GN will use the same key before a new one is generated. The recommend value is 3600 seconds (1 hour).

  IP Address: Optional, the IP address of Radius Server. The configuration is required for accounting using a Radius Server.

  Port: Optional, the Port number of Radius Server. The configuration is required for accounting using a Radius Server.

  Shared Secret: Optional, that is shared between the EKI-6310GN and the Radius Server while authenticating the supplicant. The configuration is required for accounting using a Radius Server.



SSID I Security Settings

Network Name (SSID): 2.4G □ Hide

WPS Choice: □

Encryption Settings: WPA2

WPA Algorithms: ○ TKIP [?] ● CCMP(AES) ○ Auto

Key Renewal Interval(Secconds): 60

IP Address:

Port:

Shared Secret:

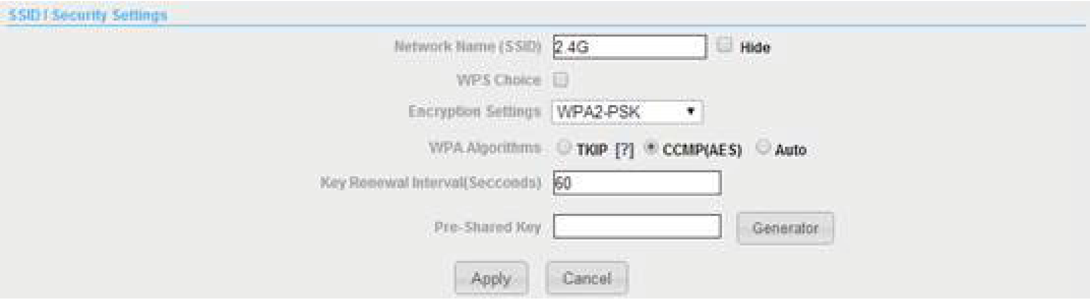
Figure 5.6 WPA2 Encryption

- WPA2-PSK
  WPA2-PSK (Pre-Shared Key) uses a passphrase or key to authenticate your wireless connection. The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. This key must be the exact same key entered on your wireless router or access point.

  WPA Algorithms: Select the cipher mode either TKIP, AES or Auto-selection

  Key Renewal Interval: The period of time that EKI-6310GN will use the same key before a new one is generated. The recommend value is 3600 seconds (1 hour).

  Pre-Shared Key: enter a key (passphrase). The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. Make sure you enter this key exactly the same on all other wireless clients.



SSID I Security Settings

Network Name (SSID) 2.4G □ Hide

WPS Choice □

Encryption Settings WPA2-PSK ▾

WPA Algorithms ○ TKIP [?] ● CCMP(AES) ○ Auto

Key Renewal Interval(Secconds) 60

Pre-Shared Key

Figure 5.7 WPA2-PSK Encryption

- WPA-AUTO
  WPA-AUTO supports stations configured as WPA or WPA2.

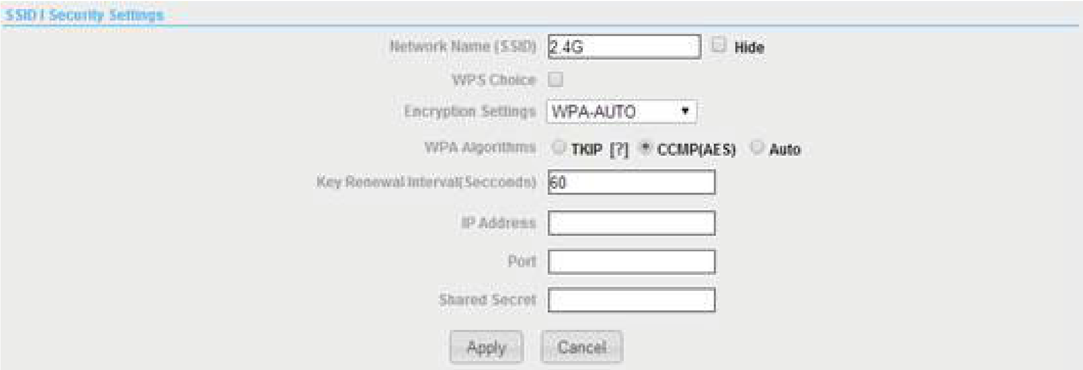
  WPA Algorithms: Select the cipher mode either TKIP, AES or Auto-selection

  Key Renewal Interval: The period of time that EKI-6310GN will use the same key before a new one is generated. The recommend value is 3600 seconds (1 hour).

  IP Address: Optional, the IP address of Radius Server. The configuration is required for accounting using a Radius Server.

  Port: Optional, the Port number of Radius Server. The configuration is required for accounting using a Radius Server.

  Shared Secret: Optional, that is shared between the EKI-6310GN and the Radius Server while authenticating the supplicant. The configuration is required for accounting using a Radius Server.



SSID I Security Settings

Network Name (SSID) 2.4G □ Hide

WPS Choice □

Encryption Settings WPA-AUTO ▾

WPA Algorithms ○ TKIP [?] ● CCMP(AES) ○ Auto

Key Renewal Interval(Secconds) 60

IP Address

Port

Shared Secret

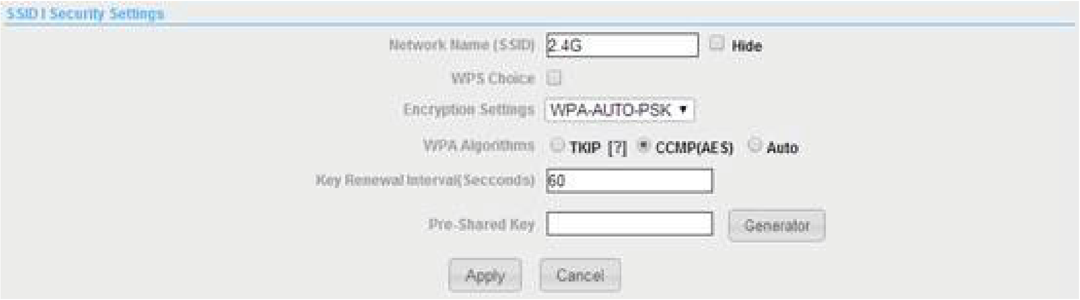
Figure 5.8 WPA-AUTO Encryption

- WPA-PSK-AUTO
  WPA-PSK-AUTO supports stations configured as WPA-PSK or WPA2-PSK.

  WPA Algorithms: Select the cipher mode either TKIP, AES or Auto-selection

  Key Renewal Interval: The period of time that EKI-6310GN will use the same key before a new one is generated. The recommend value is 3600 seconds (1 hour).

  Pre-Shared Key: enter a key (passphrase). The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. Make sure you enter this key exactly the same on all other wireless clients.



SSID I Security Settings

Network Name (SSID) 2.4G □ Hide

WPS Choice □

Encryption Settings WPA-AUTO-PSK

WPA Algorithms ○ TKIP [?] ● CCMP(AES) ○ Auto

Key Renewal Interval(Secconds) 60

Pre-Shared Key

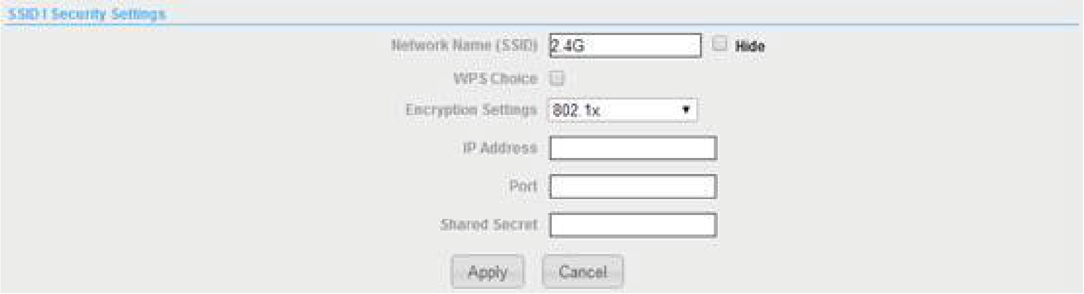
Figure 5.9 WPA-PSK-AUTO Encryption

- 802.1x
  EKI-6310GN uses Extension Authentication Protocol (EAP/802.1x) to authenticate client via a remote RADIUS server. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

  IP Address: Optional, the IP address of Radius Server. The configuration is required for accounting using a Radius Server.

  Port: Optional, the Port number of Radius Server. The configuration is required for accounting using a Radius Server.

  Shared Secret: Optional, that is shared between the EKI-6310GN and the Radius Server while authenticating the supplicant. The configuration is required for accounting using a Radius Server.



SSID I Security Settings

Network Name (SSID) 2.4G □ Hide

WPS Choice □

Encryption Settings 802.1x

IP Address

Port

Shared Secret

Figure 5.10 802.1x Encryption

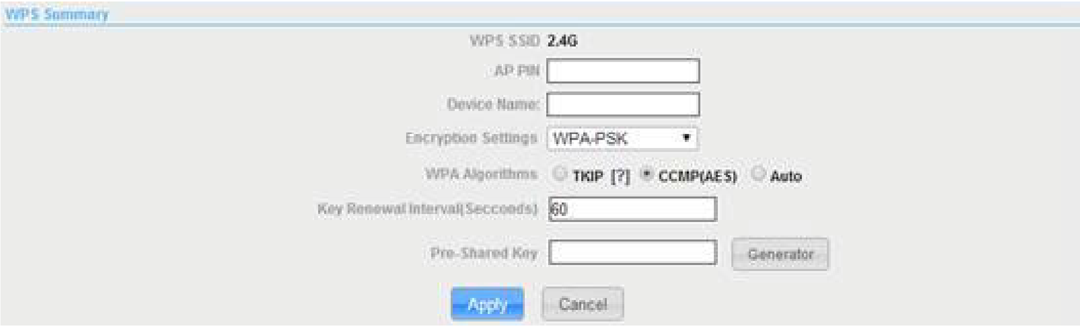
- WPS

  Wi-Fi Protected Setup (WPS) is designed to ease installation and activation of security features in wireless networks. WPS has two basic modes of operation, Push-button Configuration (PBC) and Personal Identification Number (PIN). The WPS PIN setup is optional to the PBC setup and provides more security. The WPS button on the Wireless Router can be pressed at any time to allow a single device to easily join the network.

  AP PIN: Displays the PIN Code for the Wireless Router.

  Device Name: WPS name for connecting to the device.

  Encryption Setting: Selects between methods of broadcasting the WPS beacon to network clients wanting to join the network.



WPS Summary

WPS SSID 2.4G

AP PIN

Device Name:

Encryption Settings WPA-PSK

WPA Algorithms ○ TKIP [?] ● CCMP(AES) ○ Auto

Key Renewal Interval(Secconds) 60

Pre-Shared Key

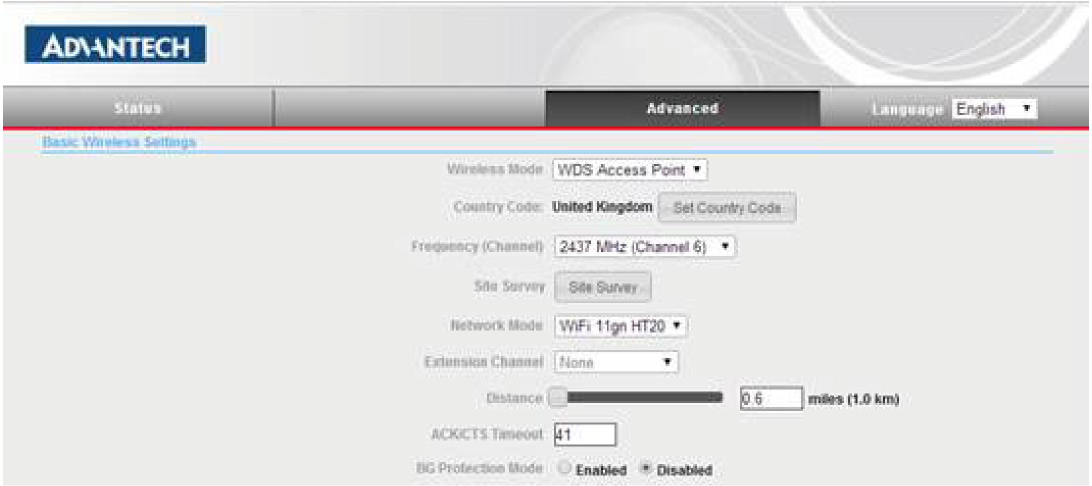
Figure 5.11 WPS Setting

5.2 WDS Access Point

In WDS Access Point Mode, the EKI-6310GN will work as Access Point Mode, but it supports Wireless Distribution System (WDS) function in this mode. (WDS) allows you to make a completely wireless infrastructure. There're three types of application of WDS: WDS AP, WDS Repeater and WDS Client in EKI-6310GN. WDS AP plays as access point function, and only WDS Repeater and WDS client can connect to WDS AP.

Note! *When you use WDS function, it will not be able to support multiple SSIDs.*

5.2.1 Basic Wireless Settings



Wireless Mode: WDS Access Point

Country Code: United Kingdom

Frequency (Channel): 2437 MHz (Channel 6)

Network Mode: WiFi 11gn HT20

Extension Channel: None

Distance: 0.6 miles (1.0 km)

ACK/CTS Timeout: 41

BG Protection Mode: ○ Enabled ● Disabled

Figure 5.12 Basic Wireless Settings in WDS AP mode

Wireless mode: You have three options (Access Point, WDS Access Point or WDS Repeater)

Country Code: The availability of some specific channels and/or operational frequency bands is country dependent.

Frequency (Channel): Channel varies much as the available band differs from country to country. Select a proper operating channel in the drop-down list according to your situation. Site Survey: You can scan the available access point in site survey action.

Network Mode: Four levels are available: 5MHz, 10MHz, 20MHz and 40MHz. The last one can enhance data throughput, but it takes more bandwidth, thus it might cause potential interference.

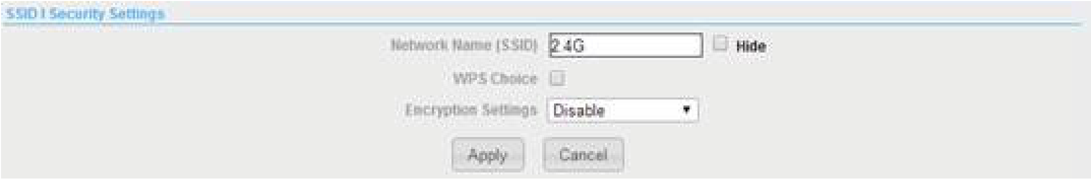
Extension Channel: This is to avoid conflict with other wireless network and boost the ability of your device to catch all 802.11g transmissions. However, it may decrease wireless network performance. Compared to CTS-Self; the transmission amount of CTS-RTS is much lower.

Distance: To decrease the chances of data retransmission at long distance, the EKI-6310GN can automatically adjust proper ACK timeout value by specifying distance of the two nodes.

ACK/CTS Timeout: ACK/CTS timeout will be adjusted by distance automatically

BG Protection Mode: The time period for the IP address lease

5.2.2 SSID SECURITY SETTINGS


SSID | Security Settings

Network Name (SSID) 2.4G □ Hide

WPS Choice □

Encryption Settings Disable

Figure 5.13 Security settings

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

Hide SSID: Under AP mode, hiding network name is necessary when you are in a wireless environment that may have potential risk. By hided broadcast SSID, the STA CAN NOT scan and find EKI-6310GN, so that malicious attack by some illegal STA could be avoided.

WPS Choice: Wi-Fi Protected Setup (WPS) System is a simplified way to set up the basic encryption of the EKI-6310GN. It can also be used to automatically create a secure wireless connection to a wireless client.

Encryption Setting: Select the wireless encryption used by the Access Point that you provide for connection. There are nine encryption modes including of no encryption, WEP-AUTO, WPA, WPA-PSK, WPA-AUTO, WPA-AUTO-PSK, WPA2, WPA2-PSK and 802.1x. WEP is the original wireless encryption standard. WPA provides a higher level of security and WPA-Personal does not require an authentication server. When 802.1x encryption is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.

- WEP-AUTO
  In WEP-AUTO option, it can support 64-bit or 128-bit encryption automatically. You can enter up to 4 different keys.

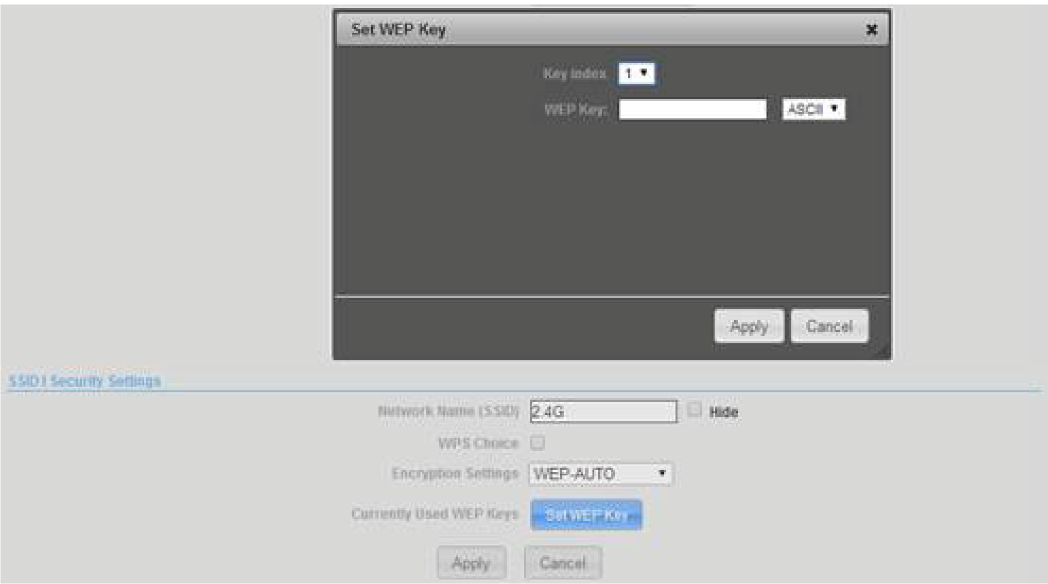
  Key Index: You can configure up to 4 different keys.

  WEP Key: encryption key you want to create.

  ASCII/Hex: Select key type either Hex or ASCII.

  Hex (recommended) - Letters A-F and numbers 0-9 are valid.

  ASCII - All numbers and letters are valid.


Set WEP Key

Key Index 1

WEP Key: ASCII

SSID | Security Settings

Network Name (SSID) 2.4G □ Hide

WPS Choice □

Encryption Settings WEP-AUTO

Currently Used WEP Keys

Figure 5.14 WEP Encryption

- WPA
  WPA (Wi-Fi Protected Access), is a Wi-Fi standard that was designed to improve the security features of WEP (Wired Equivalent Privacy). WPA improved data encryption through the different cipher modes, including of Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES).

  WPA-PSK/WPA2-PSK uses a passphrase or key to authenticate your wireless connection. The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. This key must be the exact same key entered on your wireless router or access point.

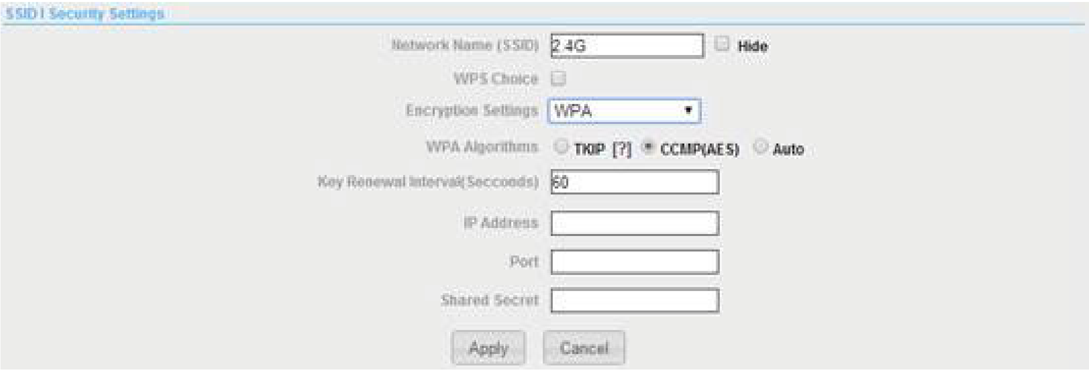
  WPA Algorithms: Select the cipher mode either TKIP, AES or Auto-selection

  Key Renewal Interval: The period of time that EKI-6310GN will use the same key before a new one is generated. The recommend value is 3600 seconds (1 hour).

  IP Address: Optional, the IP address of Radius Server. The configuration is required for accounting using a Radius Server.

  Port: Optional, the Port number of Radius Server. The configuration is required for accounting using a Radius Server.

  Shared Secret: Optional, that is shared between the EKI-6310GN and the Radius Server while authenticating the supplicant. The configuration is required for accounting using a Radius Server.



SSID I Security Settings

Network Name (SSID): 2.4G □ Hide

WPS Choice □

Encryption Settings: WPA ▾

WPA Algorithms: ○ TKIP [?] ● CCMP(AES) ○ Auto

Key Renewal Interval(Secconds): 60

IP Address:

Port:

Shared Secret:

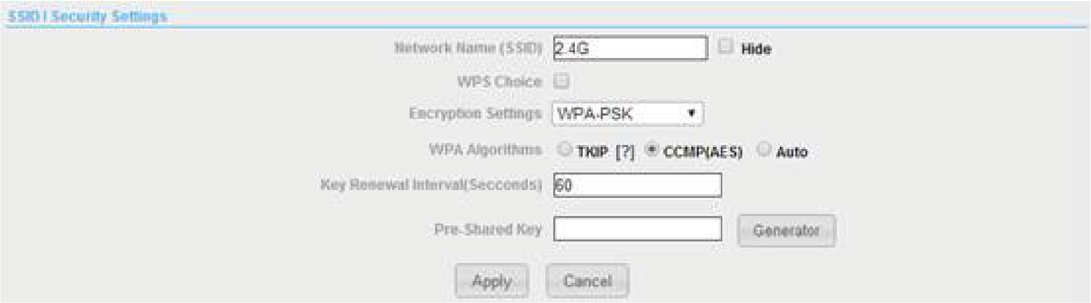
Figure 5.15 WPA Encryption

- WPA-PSK
  WPA-PSK (Pre-Shared Key) uses a passphrase or key to authenticate your wireless connection. The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. This key must be the exact same key entered on your wireless router or access point.

  WPA Algorithms: Select the cipher mode either TKIP, AES or Auto-selection

  Key Renewal Interval: The period of time that EKI-6310GN will use the same key before a new one is generated. The recommend value is 3600 seconds (1 hour).

  Pre-Shared Key: enter a key (passphrase). The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. Make sure you enter this key exactly the same on all other wireless clients.



SSID I Security Settings

Network Name (SSID): 2.4G ☐ Hide

WPS Choice: ☐

Encryption Settings: WPA-PSK

WPA Algorithms: ○ TKIP [?] ● CCMP(AES) ○ Auto

Key Renewal Interval(Secconds): 60

Pre-Shared Key:

Figure 5.16 WPA-PSK Encryption

- WPA2

  WPA2 (Wi-Fi Protected Access 2), is a Wi-Fi standard that was designed to improve the security features of WEP and WPA. WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead of TKIP. In particular, it introduces CCMP, a new AES-based encryption mode with strong security.

  WPA2-PSK uses a passphrase or key to authenticate your wireless connection. The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. This key must be the exact same key entered on your wireless router or access point.

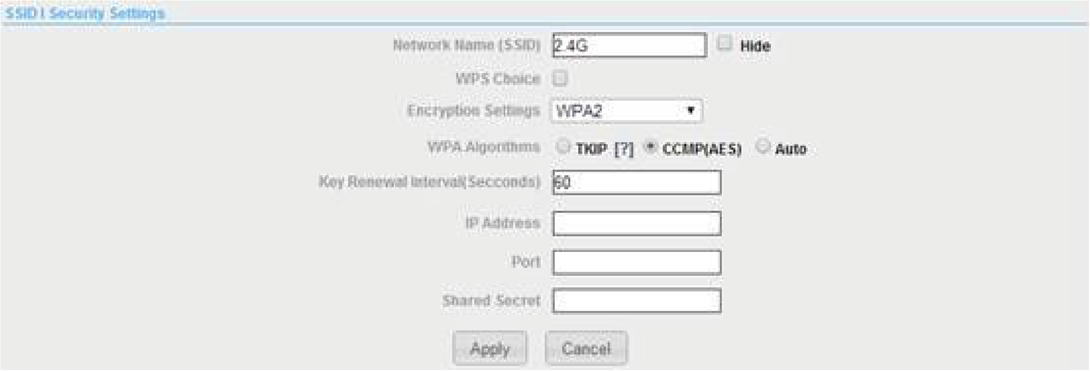
  WPA Algorithms: Select the cipher mode either TKIP, AES or Auto-selection

  Key Renewal Interval: The period of time that EKI-6310GN will use the same key before a new one is generated. The recommend value is 3600 seconds (1 hour).

  IP Address: Optional, the IP address of Radius Server. The configuration is required for accounting using a Radius Server.

  Port: Optional, the Port number of Radius Server. The configuration is required for accounting using a Radius Server.

  Shared Secret: Optional, that is shared between the EKI-6310GN and the Radius Server while authenticating the supplicant. The configuration is required for accounting using a Radius Server.



SSID I Security Settings

Network Name (SSID): 2.4G ☐ Hide

WPS Choice: ☐

Encryption Settings: WPA2

WPA Algorithms: ○ TKIP [?] ● CCMP(AES) ○ Auto

Key Renewal Interval(Secconds): 60

IP Address:

Port:

Shared Secret:

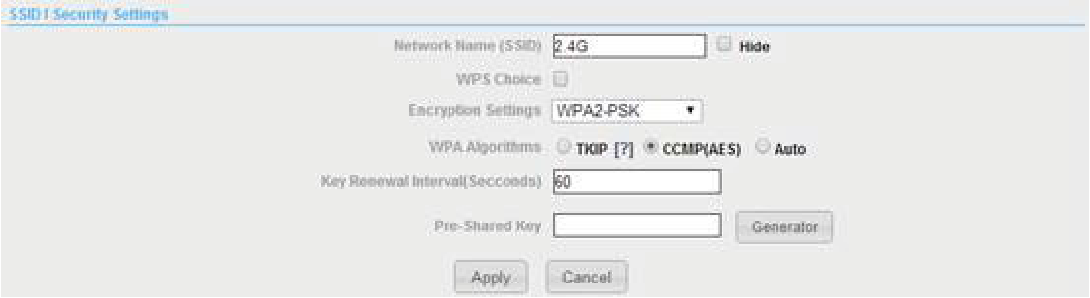
Figure 5.17 WPA2 Encryption

- WPA2-PSK
  WPA2-PSK (Pre-Shared Key) uses a passphrase or key to authenticate your wireless connection. The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. This key must be the exact same key entered on your wireless router or access point.

  WPA Algorithms: Select the cipher mode either TKIP, AES or Auto-selection

  Key Renewal Interval: The period of time that EKI-6310GN will use the same key before a new one is generated. The recommend value is 3600 seconds (1 hour).

  Pre-Shared Key: enter a key (passphrase). The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. Make sure you enter this key exactly the same on all other wireless clients.



SSID1 Security Settings

Network Name (SSID): 2.4G □ Hide

WPS Choice: □

Encryption Settings: WPA2-PSK

WPA Algorithms: ○ TKIP [?] ● CCMP(AES) ○ Auto

Key Renewal Interval(Secconds): 60

Pre-Shared Key:

Figure 5.18 WPA2-PSK Encryption

- WPA-AUTO
  WPA-AUTO supports stations configured as WPA or WPA2.

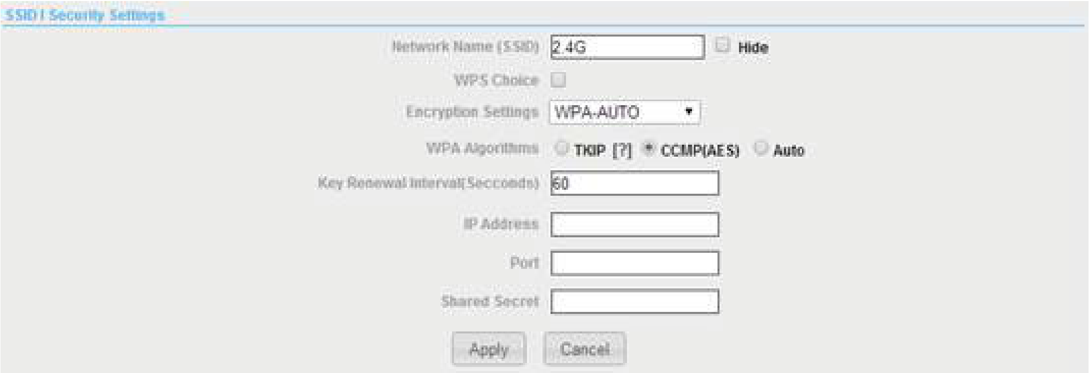
  WPA Algorithms: Select the cipher mode either TKIP, AES or Auto-selection

  Key Renewal Interval: The period of time that EKI-6310GN will use the same key before a new one is generated. The recommend value is 3600 seconds (1 hour).

  IP Address: Optional, the IP address of Radius Server. The configuration is required for accounting using a Radius Server.

  Port: Optional, the Port number of Radius Server. The configuration is required for accounting using a Radius Server.

  Shared Secret: Optional, that is shared between the EKI-6310GN and the Radius Server while authenticating the supplicant. The configuration is required for accounting using a Radius Server.



SSID1 Security Settings

Network Name (SSID): 2.4G □ Hide

WPS Choice: □

Encryption Settings: WPA-AUTO

WPA Algorithms: ○ TKIP [?] ● CCMP(AES) ○ Auto

Key Renewal Interval(Secconds): 60

IP Address:

Port:

Shared Secret:

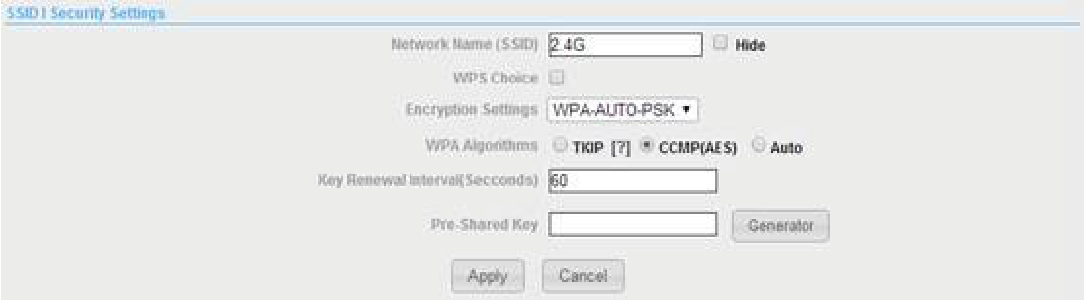
Figure 5.19 WPA-AUTO Encryption

- WPA-PSK-AUTO
  WPA-PSK-AUTO supports stations configured as WPA-PSK or WPA2-PSK.

  WPA Algorithms: Select the cipher mode either TKIP, AES or Auto-selection

  Key Renewal Interval: The period of time that EKI-6310GN will use the same key before a new one is generated. The recommend value is 3600 seconds (1 hour).

  Pre-Shared Key: enter a key (passphrase). The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. Make sure you enter this key exactly the same on all other wireless clients.



SSID I Security Settings

Network Name (SSID) 2.4G □ Hide

WPS Choice □

Encryption Settings WPA-AUTO-PSK

WPA Algorithms ○ TKIP [?] ● CCMP(AES) ○ Auto

Key Renewal Interval(Secconds) 60

Pre-Shared Key

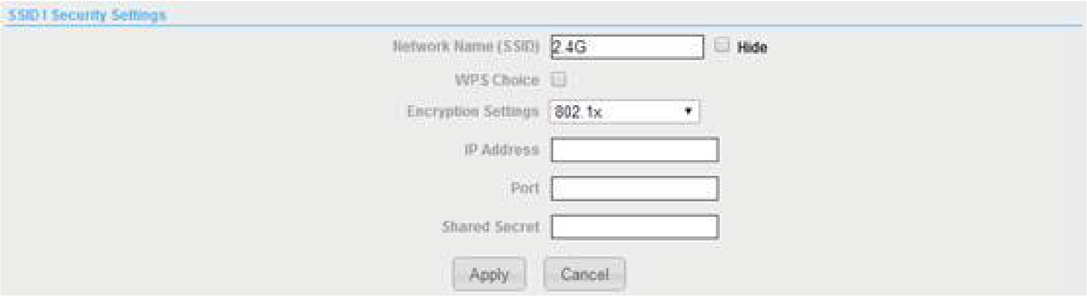
Figure 5.20 WPA-PSK-AUTO Encryption

- 802.1x
  EKI-6310GN uses Extension Authentication Protocol (EAP/802.1x) to authenticate client via a remote RADIUS server. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

  IP Address: Optional, the IP address of Radius Server. The configuration is required for accounting using a Radius Server.

  Port: Optional, the Port number of Radius Server. The configuration is required for accounting using a Radius Server.

  Shared Secret: Optional, that is shared between the EKI-6310GN and the Radius Server while authenticating the supplicant. The configuration is required for accounting using a Radius Server.



SSID I Security Settings

Network Name (SSID) 2.4G □ Hide

WPS Choice □

Encryption Settings 802.1x

IP Address

Port

Shared Secret

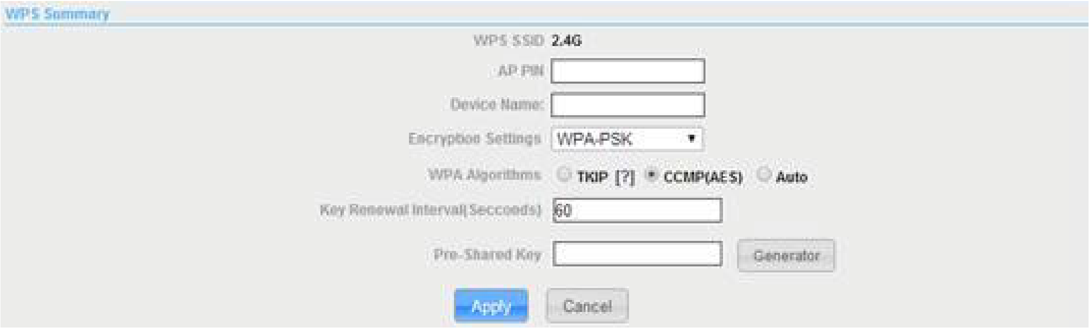
Figure 5.21 Figure 45 802.1x Encryption

- WPS
  Wi-Fi Protected Setup (WPS) is designed to ease installation and activation of security features in wireless networks. WPS has two basic modes of operation, Push-button Configuration (PBC) and Personal Identification Number (PIN). The WPS PIN setup is optional to the PBC setup and provides more security. The WPS button on the Wireless Router can be pressed at any time to allow a single device to easily join the network.

  AP PIN: Displays the PIN Code for the Wireless Router.

  Device Name: WPS name for connecting to the device.

  Encryption Setting: Selects between methods of broadcasting the WPS beacon to network clients wanting to join the network.



WPS Summary

WPS SSID 2.4G

AP PIN

Device Name:

Encryption Settings WPA-PSK

WPA Algorithms ○ TKIP [?] ● CCMP(AES) ○ Auto

Key Renewal Interval(Secconds) 60

Pre-Shared Key

Figure 5.22 WPS Setting

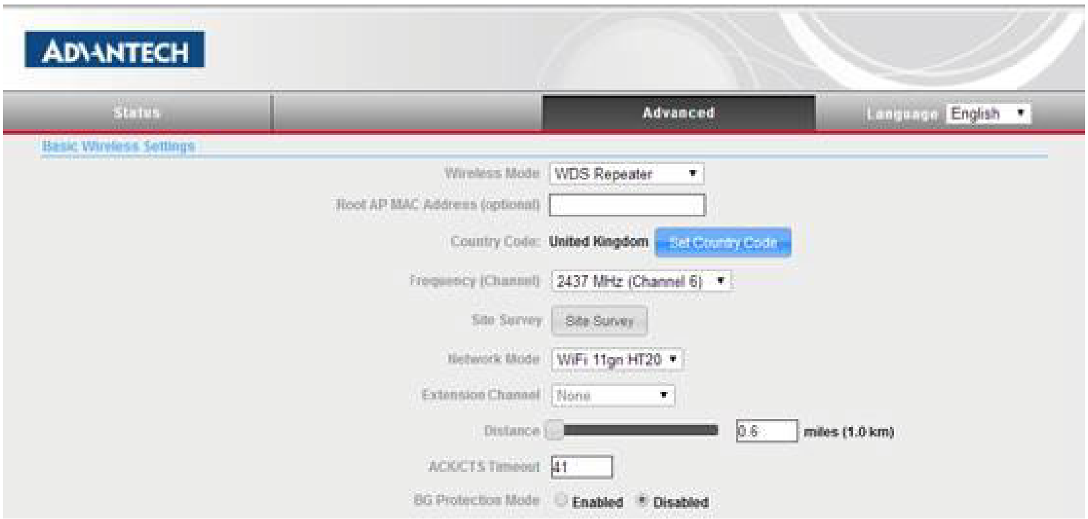
5.3 WDS Repeater

In WDS Repeater Mode, the EKI-6310GN will set to build communication with both wireless networks and other wireless equipment. WDS AP plays as access point function, and only WDS Repeater and WDS client can connect to WDS AP.

EKI-6310GN that plays as WDS Repeater extends the range of an existing wireless network. You can use this to extend the coverage of an existing wireless router to provide better signal for parts of your home or office that may have poor reception. Additionally, you can use this mode to connect a wired device to a wireless network.

Note! *When you use WDS function, it will not be able to support multiple SSIDs.*

5.3.1 BASIC WIRELESS SETTINGS



Wireless Mode: WDS Repeater

Root AP MAC Address (optional):

Country Code: United Kingdom

Frequency (Channel): 2437 MHz (Channel 6)

Network Mode: WiFi 11gn HT20

Extension Channel: None

Distance: 0.6 miles (1.0 km)

ACK/CTS Timeout: 41

BG Protection Mode: ○ Enabled ● Disabled

Figure 5.23 Basic Wireless Settings in WDS Repeater mode

Wireless mode: You have three options (Access Point, WDS Access Point or WDS Repeater)

Root AP MAC Address: It is optional for repeater mode. When you input the MAC address of previous WDS AP or WDS Repeater, you will only build-up the wireless backhaul connection to this specific WDS AP or WDS Repeater. If not, EKI-6310GN will search available WDS AP or WDS Repeater and build up the connection to the WDS AP or WDS Repeater with best signal automatically.

Country Code: The availability of some specific channels and/or operational frequency bands is country dependent.

Frequency (Channel): Channel varies much as the available band differs from country to country. Select a proper operating channel in the drop-down list according to your situation. Site Survey: You can scan the available access point in site survey action.

Network Mode: Four levels are available: 5MHz, 10MHz, 20MHz and 40MHz. The last one can enhance data throughput, but it takes more bandwidth, thus it might cause potential interference.

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

Distance: To decrease the chances of data retransmission at long distance, the EKI-6310GN can automatically adjust proper ACK timeout value by specifying distance of the two nodes.

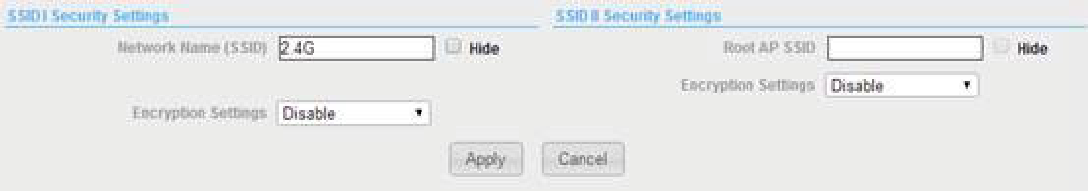
ACK/CTS Timeout: ACK/CTS timeout will be adjusted by distance automatically

BG Protection Mode: The time period for the IP address lease

5.3.2 SSID I / SSID II SECURITY SETTINGS

EKI-6310GN has two SSIDs selection in EKI-6310GN works as WDS Repeater mode. 'SSID I' is the wireless network name that EKI-6310GN shared among all associated devices in your wireless network. 'SSID II' is the wireless network name of other WDS AP or WDS Repeater that EKI-6310GN wants to associate.

Note! *When you use WDS function, it will not be able to support multiple SSIDs.*



SSID I Security Settings

Network Name (SSID) 2.4G □ Hide

Encryption Settings Disable

SSID II Security Settings

Root AP SSID □ Hide

Encryption Settings Disable

Figure 5.24 Security settings

SSID I Security Settings

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

Hide SSID: Under AP mode, hiding network name is necessary when you are in a wireless environment that may have potential risk. By hided broadcast SSID, the STA CAN NOT scan and find EKI-6310GN, so that malicious attack by some illegal STA could be avoided.

Encryption Setting: It is the same as the content of Chapter 5.2.2 SSID Security Settings.

- SSID II Security Settings

Network Name(SSID): This wireless network name of other WDS AP or WDS Repeater that EKI-6310GN wants to associate to build up the wireless backhaul.

Hide SSID: Under AP mode, hiding network name is necessary when you are in a wireless environment that may have potential risk. By hided broadcast SSID, the STA CAN NOT scan and find EKI-6310GN, so that malicious attack by some illegal STA could be avoided.

Encryption Setting: You need to configure the same encryption setting as other WDS AP or WDS Repeater that EKI-6310GN wants to associate.

Chapter 6

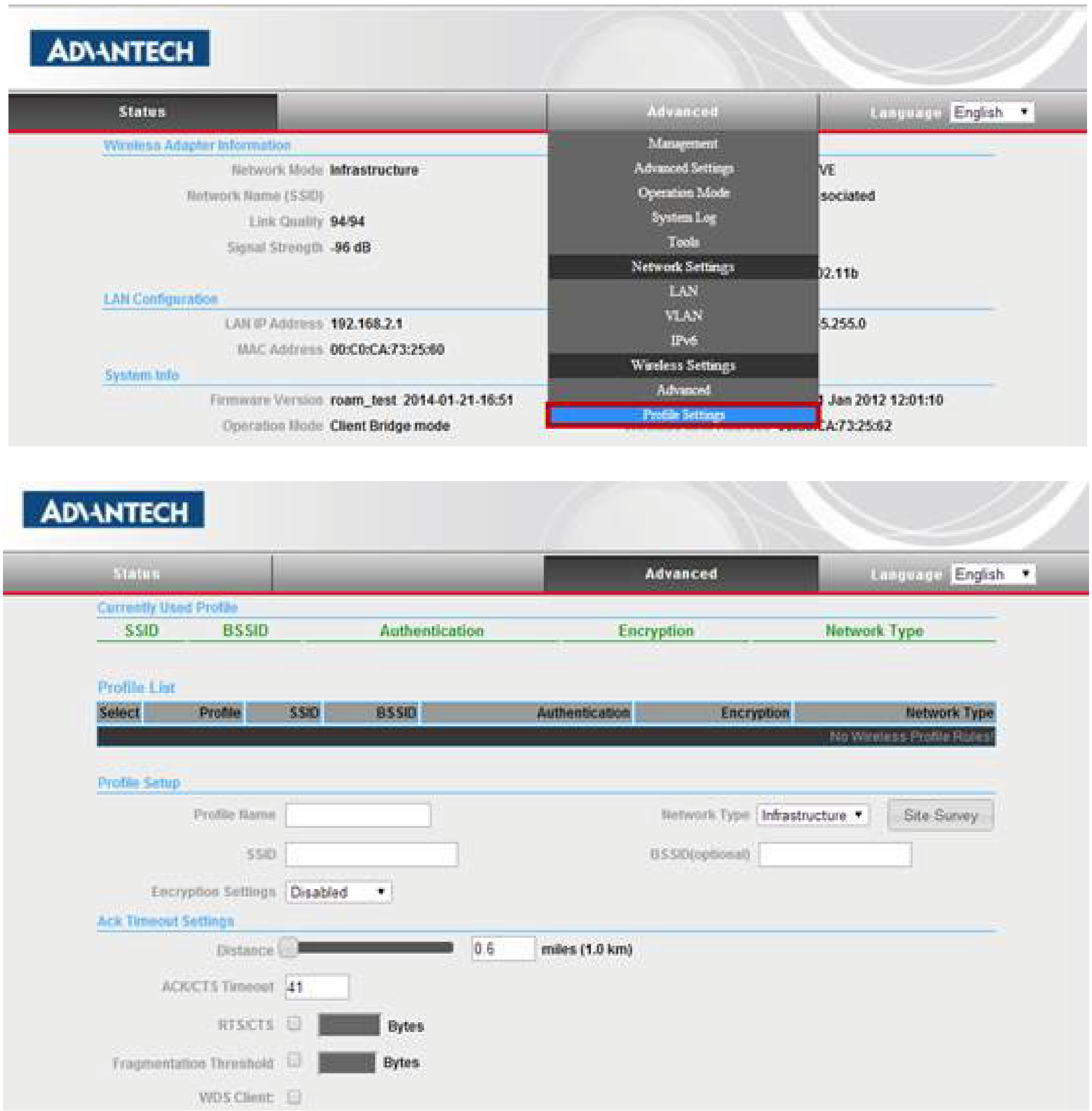
Wireless Client Settings

6.1 Client / WDS Client

This mode is for Dynamic LAN-to-LAN Bridging or Device-to-LAN scenarios. The AP Client automatically establishes bridge links with other APs. EKI-6310GN forwards packets between its Ethernet interface (LAN or WAN) and wireless interface (WLAN) to connect wired hosts on the Ethernet side with wireless host(s) on the wireless side. In Client Router mode, between the wireless and LAN is the IP sharing router function and the WAN is on the wireless side. There are two types of wireless links are specified by the IEEE802.11 standard:

- STA-AP
  This type of wireless link is established between an IEEE802.11 Station (STA) and an IEEE802.11 Access Point (AP). The Client mode is actually an STA.
- WDS
  This type of wireless link is established between two WDS Client and WDS AP. Wireless packets transmitted along the WDS link comply with WDS format at the link layer.

Note! *WPA/WPA2 CANNOT be supported in WDS.*



Wireless Adapter Information
Network Mode: Infrastructure
Network Name (SSID):
Link Quality: 94/94
Signal Strength: -96 dB

LAN Configuration
LAN IP Address: 192.168.2.1
MAC Address: 00:C0:CA:73:25:60

System Info
Firmware Version: roam_test 2014-01-21-16:51
Operation Mode: Client Bridge mode

Currently Used Profile

SSID	BSSID	Authentication	Encryption	Network Type

Profile List

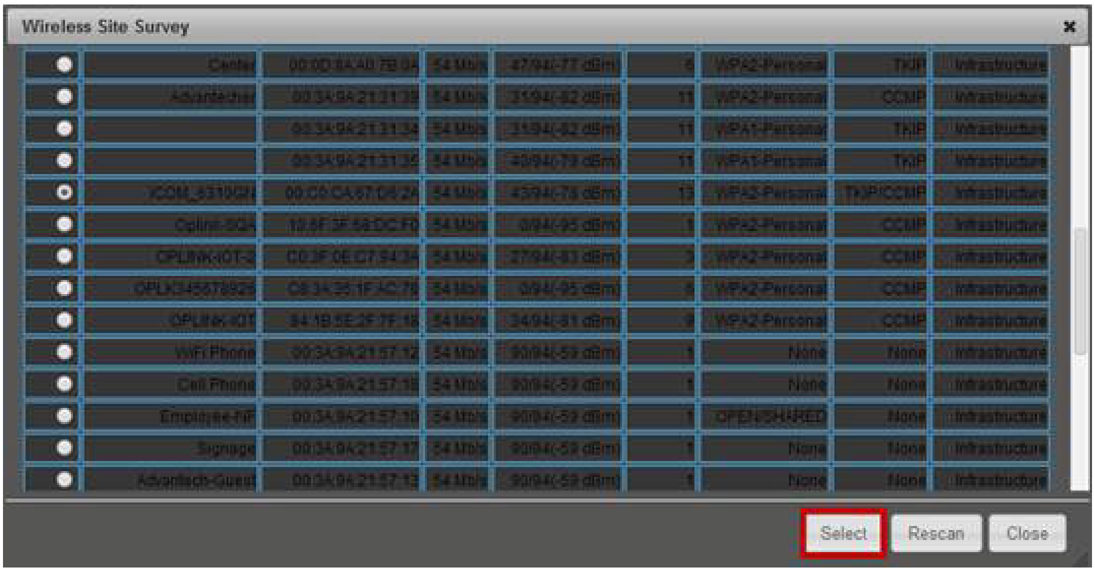
Select	Profile	SSID	BSSID	Authentication	Encryption	Network Type
						No Wireless Profile Rules!

Profile Setup
Profile Name:
Network Type: Infrastructure
SSID:
BSSID(optional):
Encryption Settings: Disabled

Ack Timeout Settings
Distance: 0.6 miles (1.0 km)
ACK/CTS Timeout: 41
RTS/CTS: □ Bytes
Fragmentation Threshold: □ Bytes
WDS Client: □

Figure 6.1 Client Profile settings

- Site Survey
  If you don't know which AP do you want to connect to, you need to do the site-survey first? And you can select the AP, it will help you fill in the AP SSID and encryption setting without key into profile setup automatically. After scanning, it will show the AP list EKI-6310GN can find.

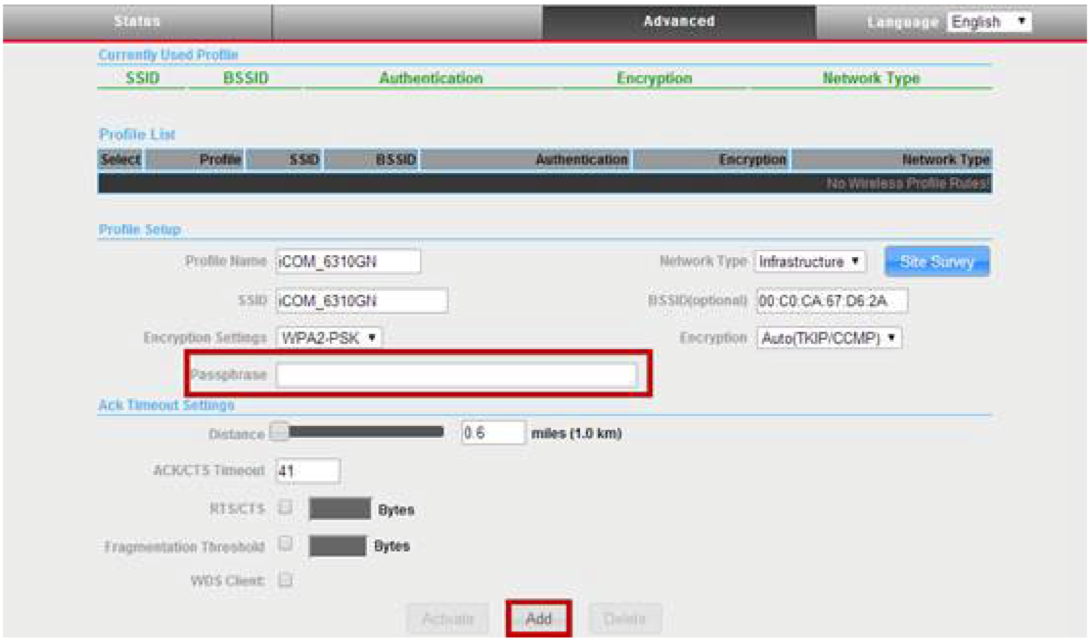


Wireless Site Survey

○	Center	00:0D:8A:A0:7B:04	54 Mb/s	47/94(-77 dBm)	6	WPA2-Personal	TKIP	Infrastructure
○	Advantechet	00:3A:9A:21:31:33	54 Mb/s	31/94(-82 dBm)	11	WPA2-Personal	CCMP	Infrastructure
○		00:3A:9A:21:31:34	54 Mb/s	31/94(-82 dBm)	11	WPA1-Personal	TKIP	Infrastructure
○		00:3A:9A:21:31:35	54 Mb/s	40/94(-79 dBm)	11	WPA1-Personal	TKIP	Infrastructure
●	iCOM_6310GN	00:C0:CA:67:D6:2A	54 Mb/s	45/94(-78 dBm)	13	WPA2-Personal	TKIP/CCMP	Infrastructure
○	Oplink-5G4	10:8F:3F:58:DC:F0	54 Mb/s	0/94(-95 dBm)	1	WPA2-Personal	CCMP	Infrastructure
○	OPLINK-IOT-2	C0:3F:0E:C7:94:34	54 Mb/s	27/94(-83 dBm)	3	WPA2-Personal	CCMP	Infrastructure
○	OPLK345678929	C8:3A:35:1F:AC:78	54 Mb/s	0/94(-95 dBm)	6	WPA2-Personal	CCMP	Infrastructure
○	OPLINK-IOT	94:1B:5E:2F:7F:18	54 Mb/s	34/94(-81 dBm)	9	WPA2-Personal	CCMP	Infrastructure
○	WiFi Phone	00:3A:9A:21:57:12	54 Mb/s	90/94(-59 dBm)	1	None	None	Infrastructure
○	Cell Phone	00:3A:9A:21:57:18	54 Mb/s	90/94(-59 dBm)	1	None	None	Infrastructure
○	Employee-NP	00:3A:9A:21:57:10	54 Mb/s	90/94(-59 dBm)	1	OPEN/SHARED	None	Infrastructure
○	Signage	00:3A:9A:21:57:17	54 Mb/s	90/94(-59 dBm)	1	None	None	Infrastructure
○	Advantech-Guest	00:3A:9A:21:57:13	54 Mb/s	90/94(-59 dBm)	1	None	None	Infrastructure

Figure 6.2 AP Selection in Site Survey

- Profile Setup
  You can store up to 32 profiles and select and activate the specific profile to connect to specific AP.



Currently Used Profile

SSID	BSSID	Authentication	Encryption	Network Type

Profile List

Select	Profile	SSID	BSSID	Authentication	Encryption	Network Type
						No Wireless Profile Rules!

Profile Setup

Profile Name: iCOM_6310GN

Network Type: Infrastructure ▾

SSID: iCOM_6310GN

BSSID(optional): 00:C0:CA:67:D6:2A

Encryption Settings: WPA2-PSK ▾

Encryption: Auto(TKIP/CCMP) ▾

Passphrase:

Ack Timeout Settings

Distance: 0.6 miles (1.0 km)

ACK/CTS Timeout: 41

RTS/CTS □ Bytes

Fragmentation Threshold □ Bytes

WDS Client: □

Figure 6.3 Profile Setup

Profile Name: The name to indicate the following AP configuration (SSID / Encryption)

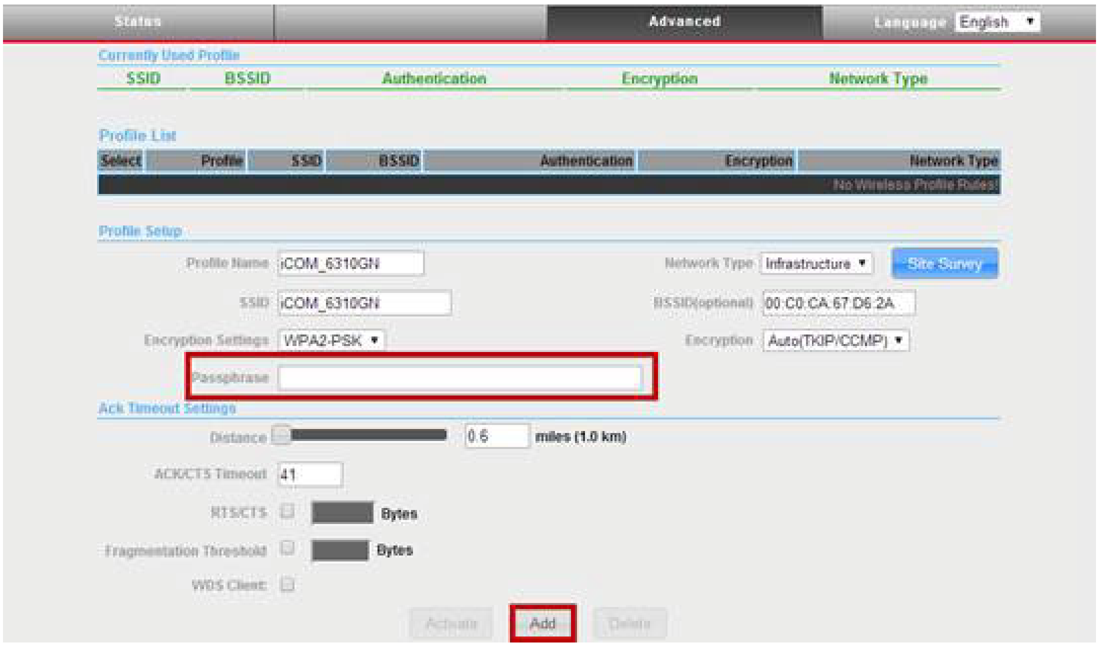
Network Type: There are two types of network modes. Infrastructure - All wireless clients will connect to an access point or wireless router. Ad-Hoc - Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer, such as two or more EKI-6310GN.

SSID: This wireless network name is shared among all associated devices in your wireless network. Keep it identical on all those devices. Note that the SSID is case-sensitive and CAN NOT exceed 32 characters.

BSSID: Each BSS is uniquely identified by a basic service set identification (BSSID). For infrastructure mode, the BSSID is the MAC address of the wireless AP. The BSSID is the formal name of the BSS and is always associated with only one BSS.

Encryption Setting: Select the wireless encryption used by the Access Point that you provide for connection. You can refer to the setting of Chapter 5.2.2.

- ACK Timeout Setting
  You can configure the ACK timeout clock based on the distance between AP and client.



Currently Used Profile

SSID	BSSID	Authentication	Encryption	Network Type

Profile List

Select	Profile	SSID	BSSID	Authentication	Encryption	Network Type
						No Wireless Profile Rules!

Profile Setup

Profile Name: iCOM_6310GN
Network Type: Infrastructure ▼
SSID: iCOM_6310GN
BSSID(optional): 00:C0:CA:67:D6:2A
Encryption Settings: WPA2-PSK ▼
Encryption: Auto(TKIP/CCMP) ▼
Passphrase:

Ack Timeout Settings

Distance: 0.6 miles (1.0 km)
ACK/CTS Timeout: 41
RTS/CTS: □ Bytes
Fragmentation Threshold: □ Bytes
WDS Client: □

Figure 6.4 ACK Timeout Setting

Distance: Specifies the transmission distance or maximum range between two EKI-6310GN devices. This parameter should be set properly, especially for long-distance communication.

ACK/CTS Timeout: System will calculate the ACK/CTS timeout according to the distance you setup in previous item.

RTS/CTS: Determines a packet size that can be before the Access Point coordinates transmission and reception to ensure efficient communication. The value is between 256 and 2346.

Fragmentation Threshold: Specifies the maximum size a data packet. When the transfer data is over the threshold, it will split the data and create another data package.

WDS Client: When you enable this option, it will work as WDS Client.

Chapter 7

Advanced Settings

7.1 Management

You can configure the system management in this chapter, including of web login interface, firmware upgrade, and configuration import/export, reset to default setting, reboot device and scheduling reset.

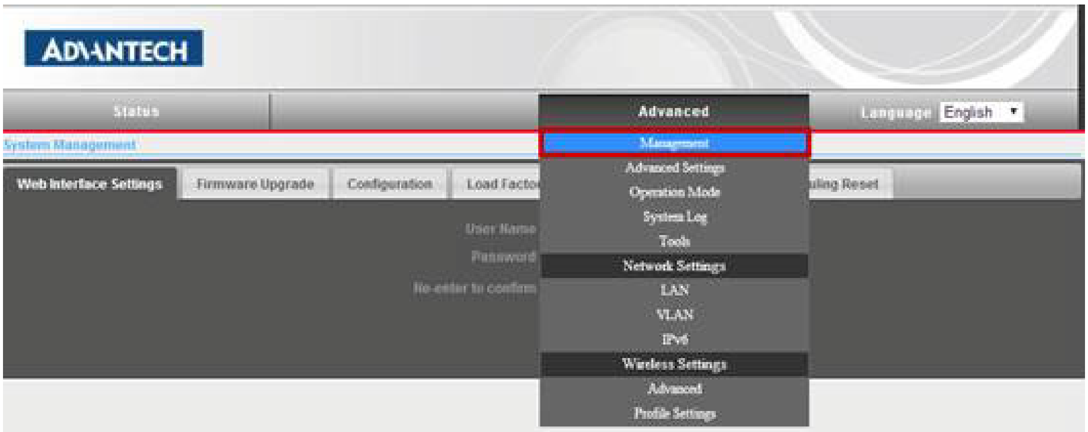
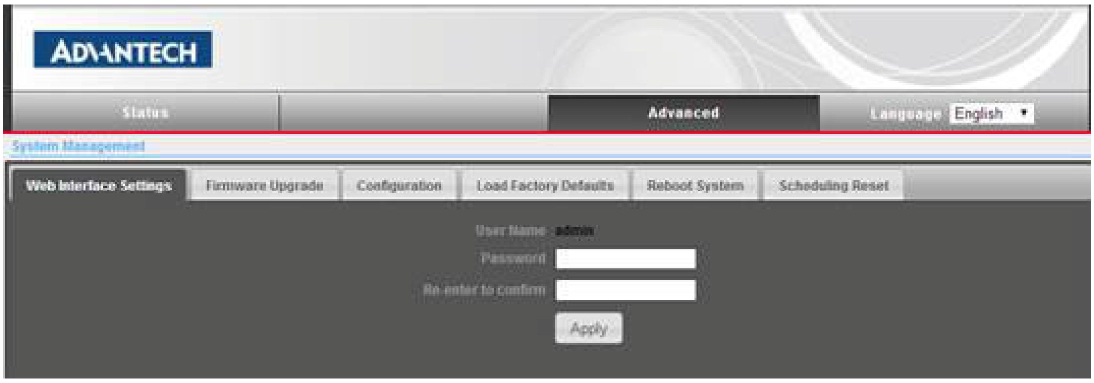


Figure 7.1 Management Setting

- Web Interface Settings
  Change the password when you log-in web service. The user name is fixed in 'admin' and password is 'admin' in default. The new password must NOT exceed 32 characters in length and must not include any spaces.



User Name admin

Password

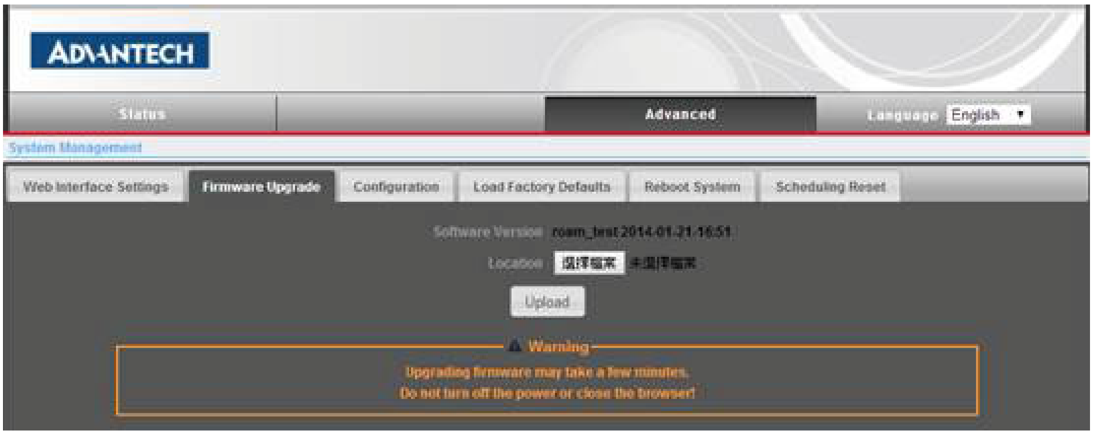
Re-enter to confirm

Figure 7.2 Web Interface Setting

- Firmware Upgrade
  Upgrade the firmware of EKI-6310GN that you select

Note!

1. *When you upgrade the EKI-6310GN firmware, you may lose some current configurations, so before upgrading the firmware please write down some of your customized settings to avoid losing important settings or export the configuration file in advance.*
2. *Do not turn off EKI-6310GN or press the Reset button while the firmware is being upgraded, otherwise, EKI-6310GN may be damaged.*
3. *The Router will reboot after the upgrading has been finished.*



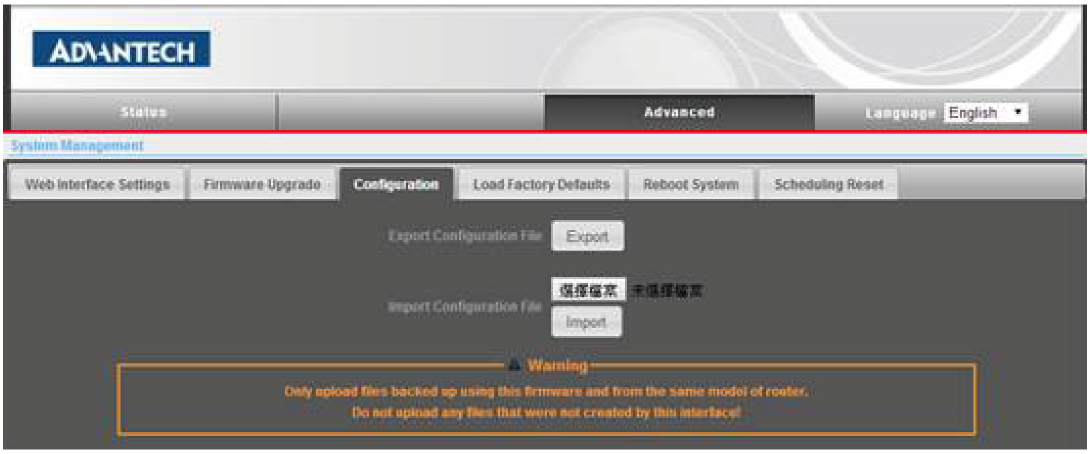
Software Version roam_test 2014-01-21 16:51

Location 選擇檔案 未選擇檔案

Upgrading firmware may take a few minutes.
Do not turn off the power or close the browser!

Figure 7.3 Firmware Upgrade Setting

- Configuration
  You can export current configuration to specific file to your laptop or import the configuration file that you already save to current EKI-6310GN.



Only upload files backed up using this firmware and from the same model of router.
Do not upload any files that were not created by this interface!

Figure 7.4 Configuration Setting

- Load Factory Defaults
  Return the configuration of current EKI-6310GN to factory default setting. You can refer to factory default parameters in Chapter 3.1.

Note! *When you return the configuration of EKI-6310GN to factory default parameters, the WAN and LAN information will also change to default parameters. You need to use default IP '192.168.2.1' to configure EKI-6310GN.*

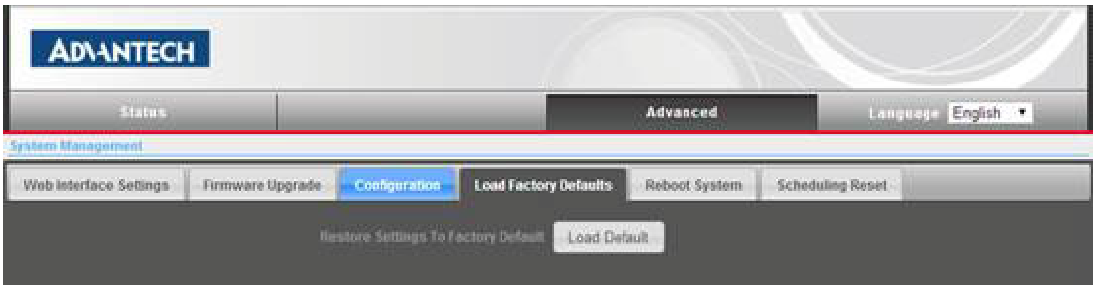


Figure 7.5 Load Factory Defaults Setting

- Reboot
  Reboot your EKI-6310GN.

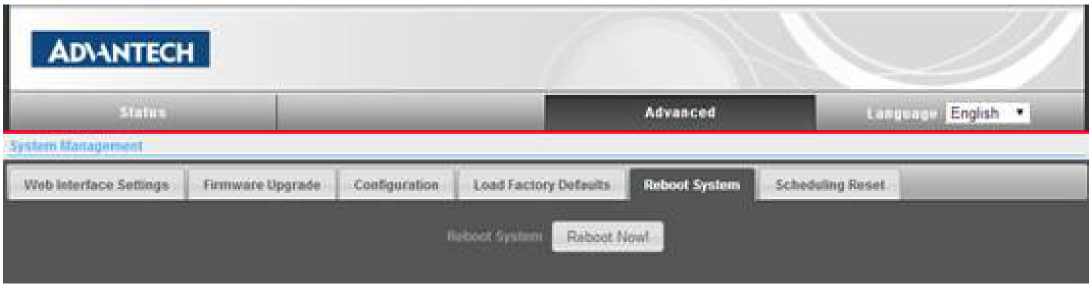
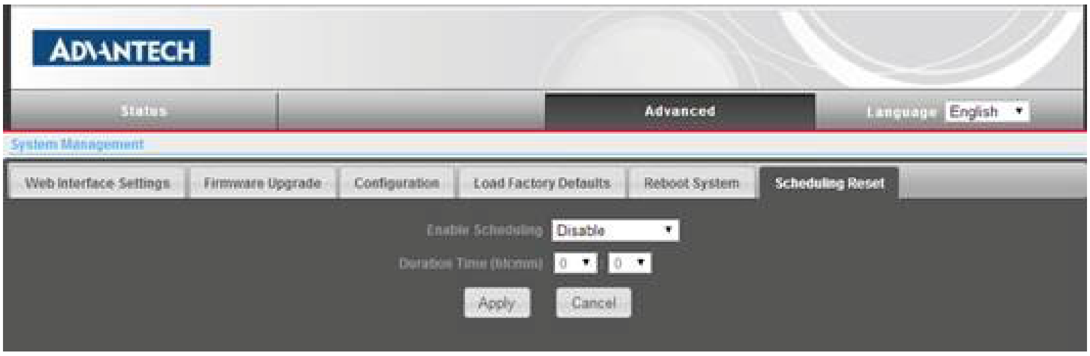


Figure 7.6 Reboot Setting

- Scheduling Reset
  System will arrange the reboot according your scheduling (Duration time: 24 hour time duration).



Enable Scheduling: Disable
Duration Time (hh:mm): 0 : 0

Figure 7.7 Scheduling Reset Setting

7.2 Advanced Setting

In this chapter, you can configure the system time and time zone, DDNS networking and remote management including of SNMP and Telnet/SSH.

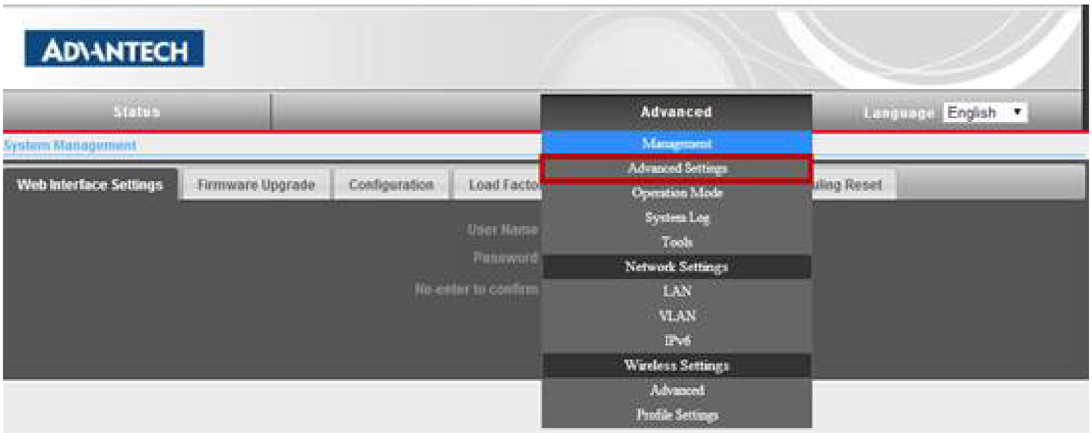


Figure 7.8 Advanced Setting

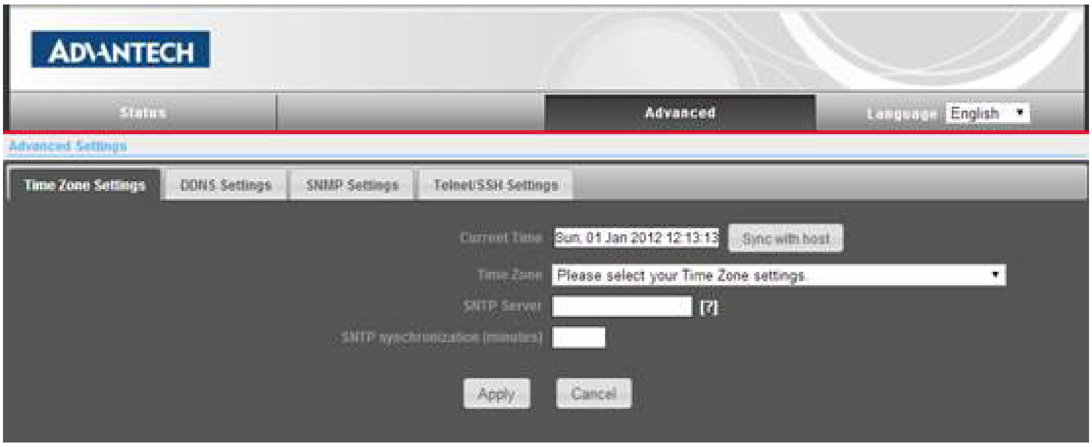
- System Time/Zone

  Current Time: current system time

  Time Zone: Select the appropriate Time Zone from your location

  SNTP Server: Choose the NTP Server used for synchronizing time and date. Daylight Saving can also be configured to adjust the time when you use NTP Server.

  SNTP Synchronization: These queries are performed at designated time intervals (generally about every 15 minutes) in order to maintain the required synchronization accuracy for the network.



Language: English

Current Time: Sun, 01 Jan 2012 12:13:13

Time Zone: Please select your Time Zone settings

SNTP Server:

SNTP synchronization (minutes):

Figure 7.9 System Time Setting

- DDNS

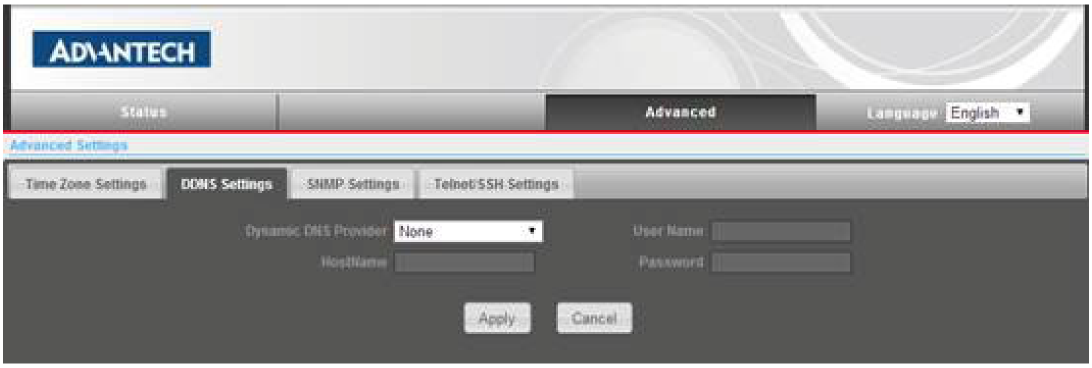
  The DDNS feature allows you to host a server (Web, FTP, Game Server, etc…) behind EKI-6310GN using a domain name that you have purchased with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter in your domain name to connect to your server no matter what your IP address is. It is useful when you are hosting your own website, FTP server, or other server behind it.

  Dynamic DNS Provider: Enter the DDNS server address, or select your DDNS service from the drop-down menu

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

  User Name: Enter the Username or key for your DDNS account.

  Password: Enter the Password or key for your DDNS account.



Language: English

Dynamic DNS Provider: None

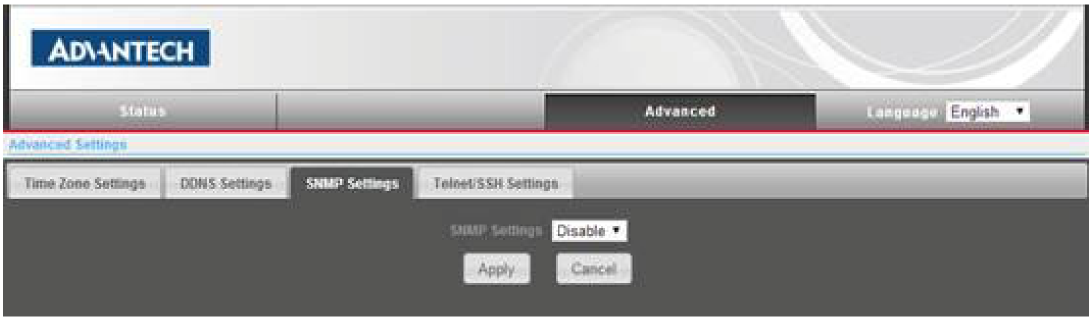
HostName:

User Name:

Password:

Figure 7.10 DDNS Setting

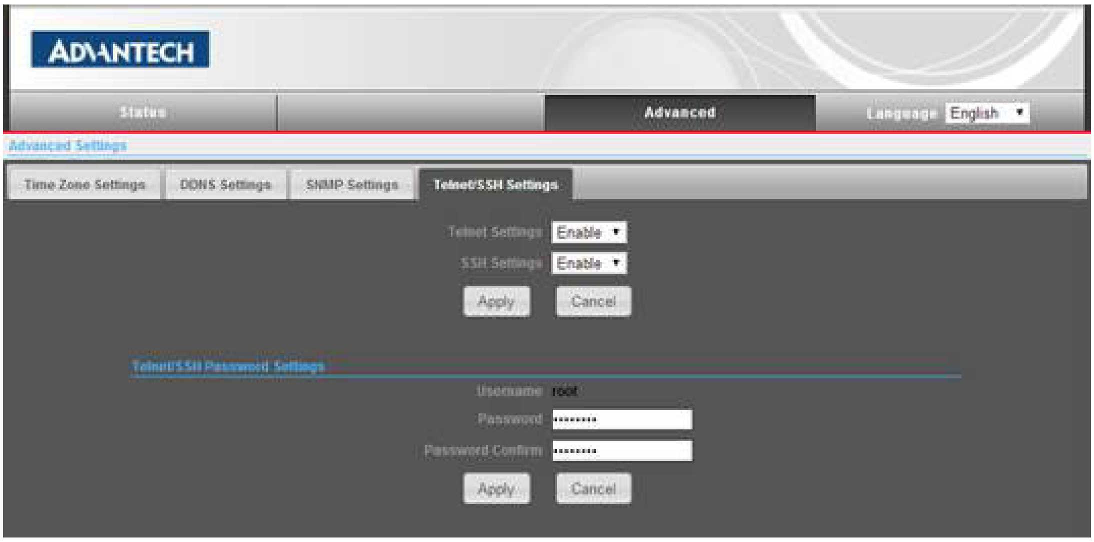
- SNMP
  SNMP (Simple Network Management Protocol) is a widely used network monitoring and control protocol that reports activity on each network device to the administrator of the network. SNMP can be used to manage your device in remote site and monitor traffic and statistics of EKI-6310GN. The EKI-6310GN supports SNMP v1 or v2c. Default setting is 'Disabled'.



SNMP Settings: Disable

Figure 7.11 SNMP Setting

- Telnet/SSH
  User can use CLI (Command-Line Interface) to access EKI-6310GN through Telnet (TCP Port #23) and secure shell SSH (TCP Port #22). Default setting of Telnet and SSH is enabled. The default password is 'Advantech'.



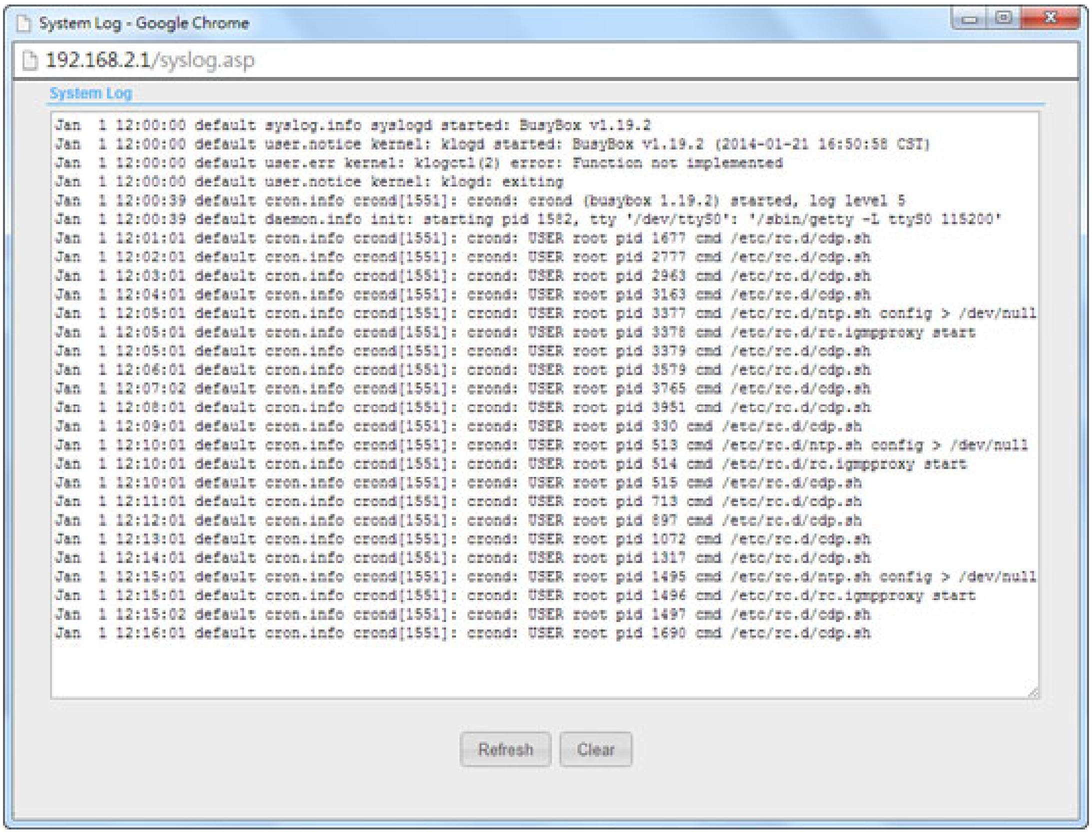
Telnet Settings: Enable
SSH Settings: Enable

Username: root
Password: ••••••••
Password Confirm: ••••••••

Figure 7.12 Telnet/SSH Setting

7.3 System Log

EKI-6310GN will keep the debugging message and system log in this page when system boots up.



```
Jan  1 12:00:00 default syslog.info syslogd started: BusyBox v1.19.2
Jan  1 12:00:00 default user.notice kernel: klogd started: BusyBox v1.19.2 (2014-01-21 16:50:58 CST)
Jan  1 12:00:00 default user.err kernel: klogctl(2) error: Function not implemented
Jan  1 12:00:00 default user.notice kernel: klogd: exiting
Jan  1 12:00:39 default cron.info crond[1551]: crond: crond (busybox 1.19.2) started, log level 5
Jan  1 12:00:39 default daemon.info init: starting pid 1582, tty '/dev/ttyS0': '/sbin/getty -L ttyS0 115200'
Jan  1 12:01:01 default cron.info crond[1551]: crond: USER root pid 1677 cmd /etc/rc.d/cdp.sh
Jan  1 12:02:01 default cron.info crond[1551]: crond: USER root pid 2777 cmd /etc/rc.d/cdp.sh
Jan  1 12:03:01 default cron.info crond[1551]: crond: USER root pid 2963 cmd /etc/rc.d/cdp.sh
Jan  1 12:04:01 default cron.info crond[1551]: crond: USER root pid 3163 cmd /etc/rc.d/cdp.sh
Jan  1 12:05:01 default cron.info crond[1551]: crond: USER root pid 3377 cmd /etc/rc.d/ntp.sh config > /dev/null
Jan  1 12:05:01 default cron.info crond[1551]: crond: USER root pid 3378 cmd /etc/rc.d/rc.igmpproxy start
Jan  1 12:05:01 default cron.info crond[1551]: crond: USER root pid 3379 cmd /etc/rc.d/cdp.sh
Jan  1 12:06:01 default cron.info crond[1551]: crond: USER root pid 3579 cmd /etc/rc.d/cdp.sh
Jan  1 12:07:02 default cron.info crond[1551]: crond: USER root pid 3765 cmd /etc/rc.d/cdp.sh
Jan  1 12:08:01 default cron.info crond[1551]: crond: USER root pid 3951 cmd /etc/rc.d/cdp.sh
Jan  1 12:09:01 default cron.info crond[1551]: crond: USER root pid 330 cmd /etc/rc.d/cdp.sh
Jan  1 12:10:01 default cron.info crond[1551]: crond: USER root pid 513 cmd /etc/rc.d/ntp.sh config > /dev/null
Jan  1 12:10:01 default cron.info crond[1551]: crond: USER root pid 514 cmd /etc/rc.d/rc.igmpproxy start
Jan  1 12:10:01 default cron.info crond[1551]: crond: USER root pid 515 cmd /etc/rc.d/cdp.sh
Jan  1 12:11:01 default cron.info crond[1551]: crond: USER root pid 713 cmd /etc/rc.d/cdp.sh
Jan  1 12:12:01 default cron.info crond[1551]: crond: USER root pid 897 cmd /etc/rc.d/cdp.sh
Jan  1 12:13:01 default cron.info crond[1551]: crond: USER root pid 1072 cmd /etc/rc.d/cdp.sh
Jan  1 12:14:01 default cron.info crond[1551]: crond: USER root pid 1317 cmd /etc/rc.d/cdp.sh
Jan  1 12:15:01 default cron.info crond[1551]: crond: USER root pid 1495 cmd /etc/rc.d/ntp.sh config > /dev/null
Jan  1 12:15:01 default cron.info crond[1551]: crond: USER root pid 1496 cmd /etc/rc.d/rc.igmpproxy start
Jan  1 12:15:02 default cron.info crond[1551]: crond: USER root pid 1497 cmd /etc/rc.d/cdp.sh
Jan  1 12:16:01 default cron.info crond[1551]: crond: USER root pid 1690 cmd /etc/rc.d/cdp.sh
```

Figure 7.13 System Log

7.4 Tools

This useful diagnostic utility can be used to check if a computer is connected to the network or customer can check the routing path and simple throughput.

- Ping Tool
  The Ping Test is used to send ping packets to test if your EKI-6310GN is connected to the Internet. Enter the IP address that you wish to ping and how many times do you want to ping.

  Ping IP Address: destination IP Address that you wish to ping

  Ping Count: the counter that you execute Ping function

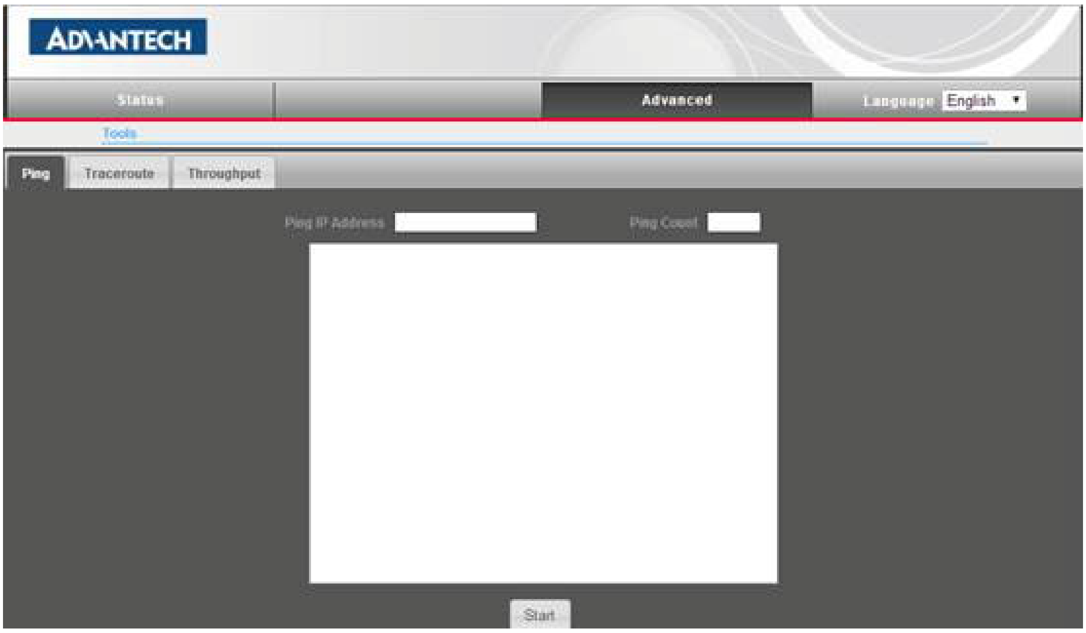


Figure 7.14 Ping Tool

- Trace route
  It is the diagnostic tool for displaying the route (path) to your destination and measuring transmit delays of packets across an IP network. It is the same command as 'tracert' in windows system.
  <u>**URL**</u>: destination URL that you wish to trace

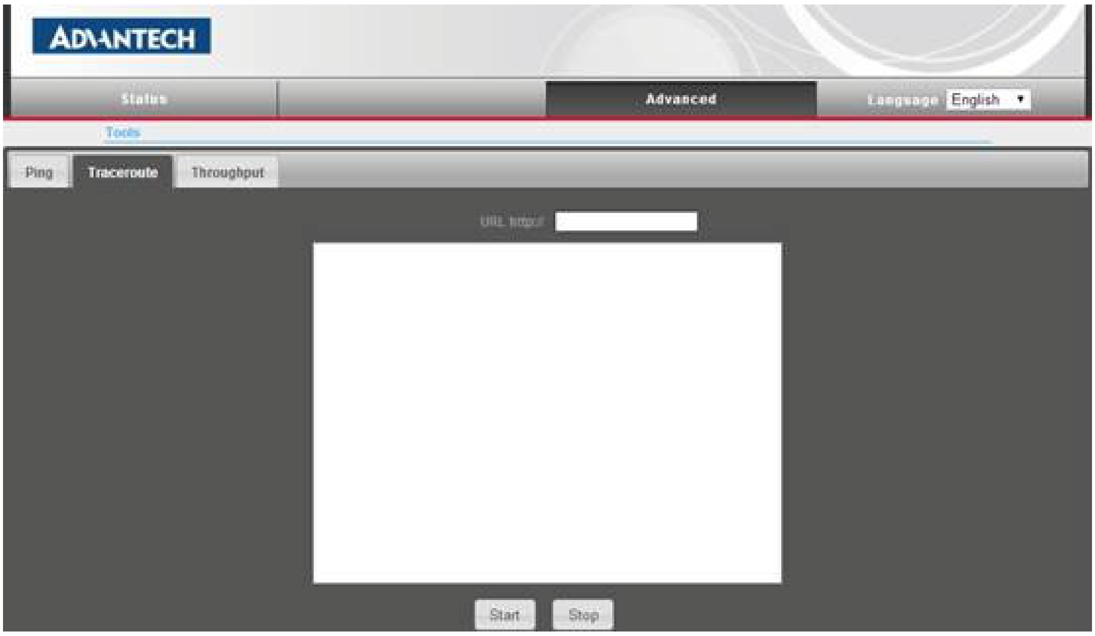
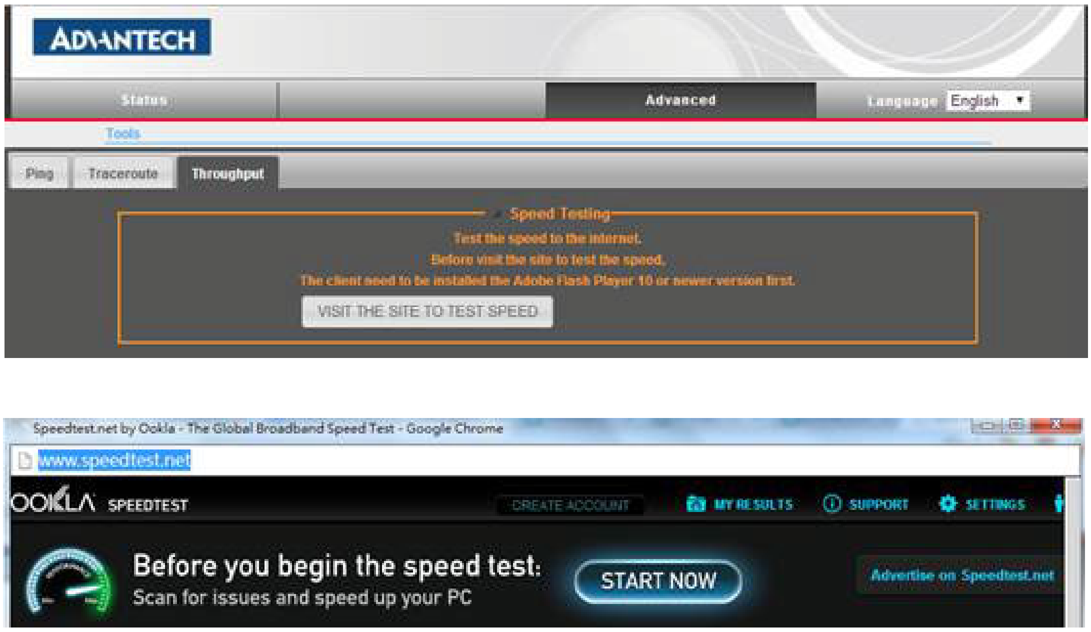


Figure 7.15 Trace Route tool

- Throughput
  It is the sample tool to measure the throughput that you access the Internet through your ISP vender. In EKI-6311GN, it will connect to 'www.speedtest.net' website to test the throughput.



ADVANTECH
Status
Advanced
Language English
Tools
Ping
Traceroute
Throughput
Speed Testing

Test the speed to the internet.
Before visit the site to test the speed.
The client need to be installed the Adobe Flash Player 10 or newer version first.

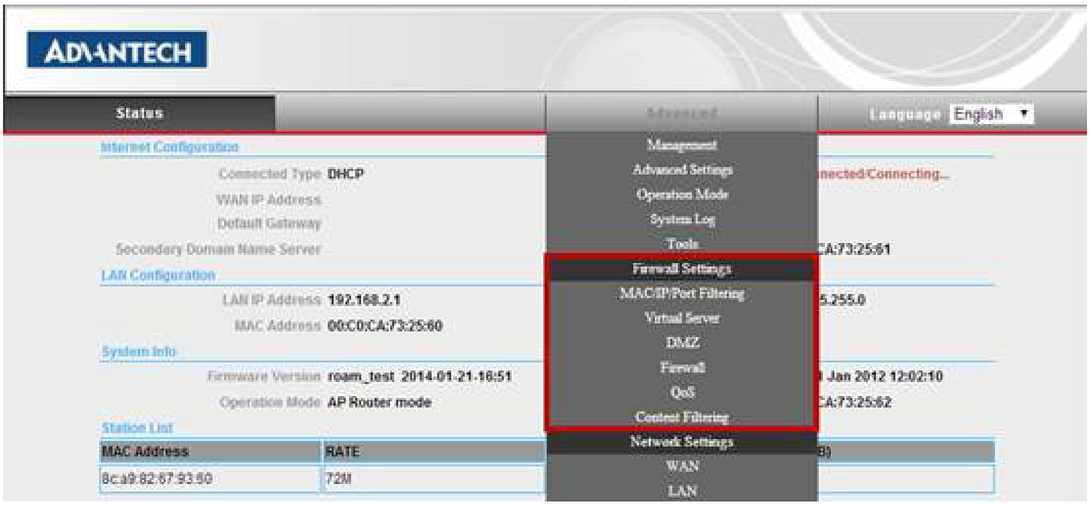
VISIT THE SITE TO TEST SPEED
Speedtest.net by Ookla - The Global Broadband Speed Test - Google Chrome
www.speedtest.net
OOKLA SPEEDTEST
CREATE ACCOUNT
MY RESULTS
SUPPORT
SETTINGS
Before you begin the speed test:
Scan for issues and speed up your PC
START NOW
Advertise on Speedtest.net

Figure 7.16 Throughput tool

Chapter 8

Application Rules And Firewall

Some applications may require multiple connections, such as Internet gaming, video conferencing, and VoIP calls over the Internet. Enabling the firewall and anti-spoof checking helps protect against attacks over the Internet in some cases.



Internet Configuration

Connected Type DHCP

WAN IP Address

Default Gateway

Secondary Domain Name Server

nected/Connecting...

CA:73:25:61

LAN Configuration

LAN IP Address 192.168.2.1

MAC Address 00:C0:CA:73:25:60

5.255.0

System Info

Firmware Version roam_test 2014-01-21-16:51

Operation Mode AP Router mode

Jan 2012 12:02:10

CA:73:25:62

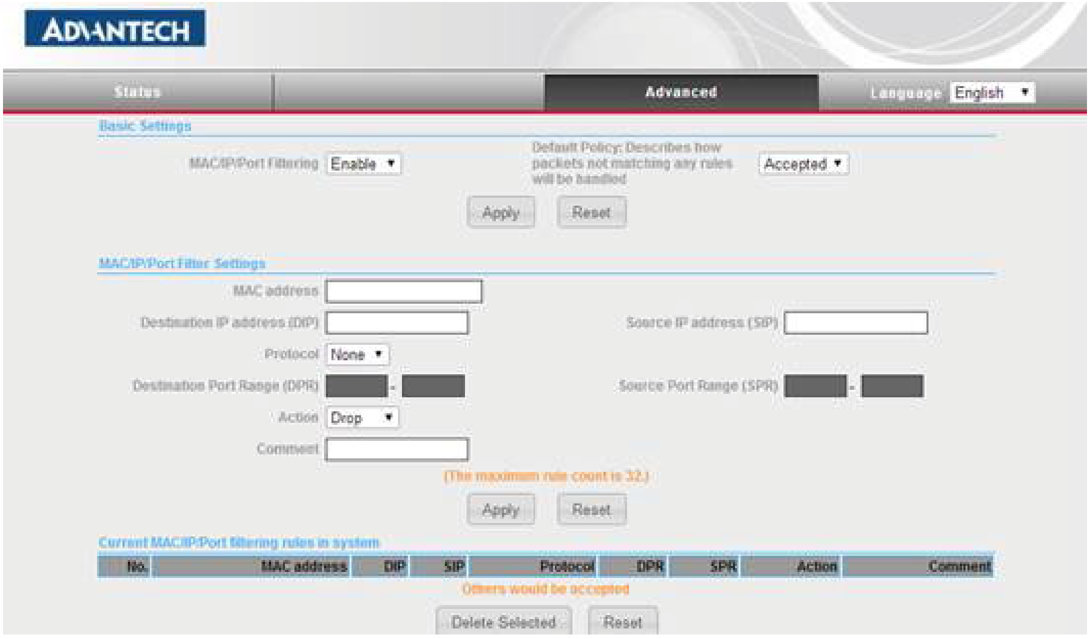
Station List

MAC Address	RATE
8c:a9:82:67:93:60	72M

Figure 8.1 Rules & Firewall

8.1 MAC/Port/IP Filtering

MAC/IP/Port filtering restricts connection parameters to limit the risk of intrusion and defends against a wide array of common hacker attacks. MAC/IP/Port filtering allows the unit to permit, deny or proxy traffic through its MAC addresses, IP addresses and ports. EKI-6310GN allows you define a sequential list of permit or deny filtering rules. This device tests ingress packets against the filter rules one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the packet is either accepted or dropped depending on the default policy setting.



Basic Settings

MAC/IP/Port Filtering Enable

Default Policy: Describes how packets not matching any rules will be handled Accepted

MAC/IP/Port Filter Settings

MAC address

Destination IP address (DIP)

Source IP address (SIP)

Protocol None

Destination Port Range (DPR) -

Source Port Range (SPR) -

Action Drop

Comment

(The maximum rule count is 32.)

Current MAC/IP/Port filtering rules in system

No.	MAC address	DIP	SIP	Protocol	DPR	SPR	Action	Comment

Others would be accepted

Figure 8.2 MAC/IP/Port Filter

MAC/IP/Port Filtering: Enables or disables MAC/IP/Port Filtering. (Default: Disable)

Default Policy: When MAC/IP/Port Filtering is enabled, the default policy will be enabled. If you set the default policy to "Dropped", all incoming packets that don't match the rules will be dropped. If the policy is set to "Accepted," all incoming packets that don't match the rules are accepted. (Default: Dropped)

MAC Address: Specifies the MAC address to block or allow traffic from.

DIP: Specifies the destination IP address to block or allow traffic from.

Protocol: Specifies the destination port type, TCP, UDP or ICMP.

Destination Port Range: Specifies the range of destination port to block traffic from the specified LAN IP address from reaching.

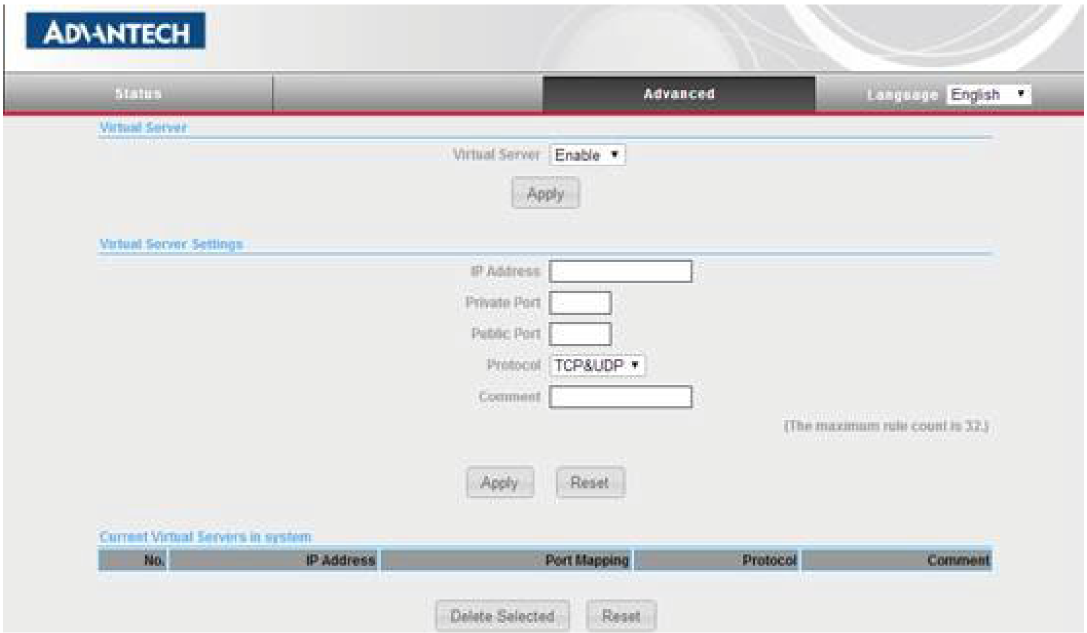
Source Port Range: Specifies the range of source port to block traffic from the specified LAN IP address from reaching.

Action: Specifies if traffic should be accepted or dropped. (Default: Accept)

Comment: Displays a useful comment to identify the filter rules

8.2 Virtual Server

Virtual Server (sometimes referred to as Port Forwarding) is the act of forwarding traffic from one network node to another based on received protocol port number. This technique can allow an external user to reach a port on a private IP address (inside a LAN) from the outside through a NAT enabled router.



Language: English

Virtual Server: Enable

Protocol: TCP&UDP

(The maximum rule count is 32.)

No.	IP Address	Port Mapping	Protocol	Comment

Figure 8.3 Virtual Server

Virtual Server: Selects between enabling or disabling port forwarding the virtual server. (Default: Disable)

IP Address: Specifies the IP address of a server on the local network to allow external access.

Private Port: The protocol port number on the local server.

Public Port: The protocol port number on the router's WAN interface.

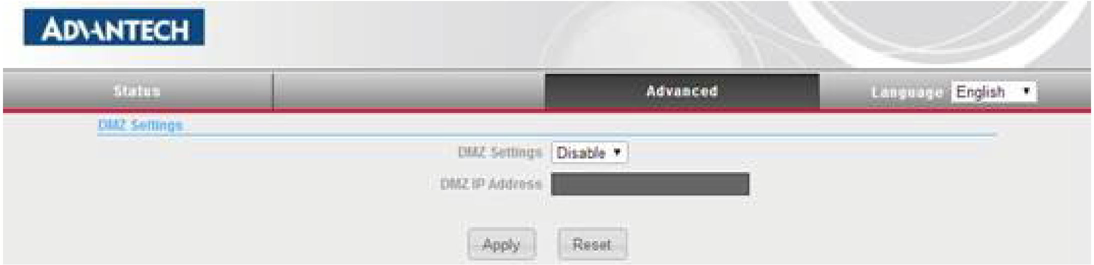
Protocol: Specifies the protocol to forward, either TCP, UDP, or TCP&UDP.

Comment: Enter a useful comment to help identify the port forwarding service on the network.

Current Virtual Servers in System: The Current Port Forwarding Table displays the entries that are allowed to forward packets through EKI-6310GN's firewall.

8.3 DMZ

DMZ is to specified host PC on the local network to access the Internet without any firewall protection. Some Internet applications, such as interactive games or video conferencing, may not function properly behind the firewall. By specifying a Demilitarized Zone (DMZ) host, the PC's TCP ports are completely exposed to the Internet, allowing open two-way communication. The host PC should be assigned a static IP address (which is mapped to its MAC address) and this must be configured as the DMZ IP address.



DMZ Settings

DMZ Settings: Disable

DMZ IP Address:

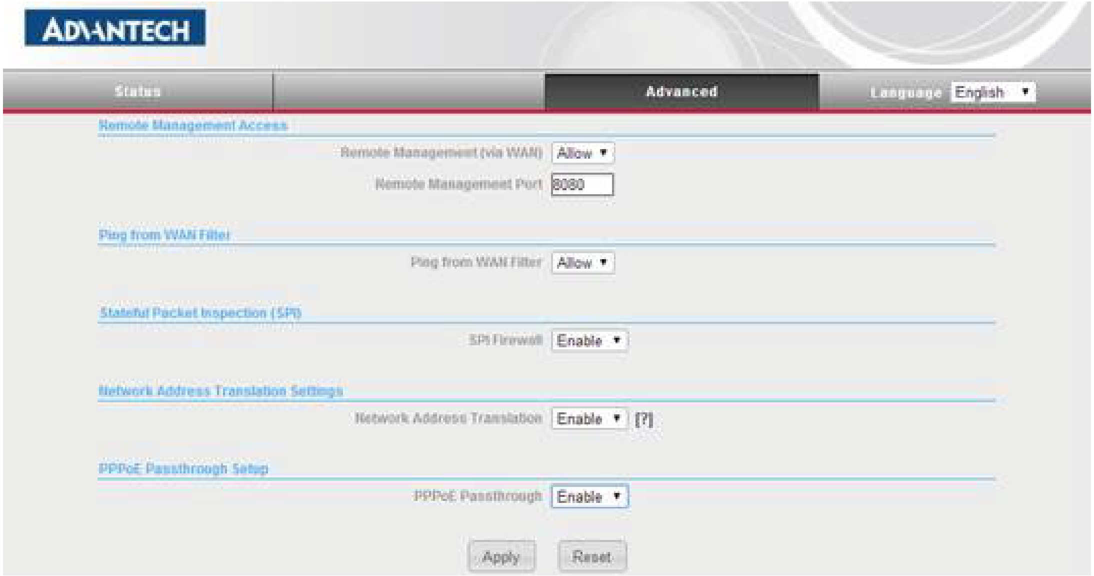
Figure 8.4 DMZ

DMZ Settings: Sets the DMZ status. (Default: Disable)

DMZ IP Address: Specifies an IP address on the local network allowed unblocked access to the WAN.

8.4 Firewall

Firewall functions which will help to protect your network and computer. You can utilize firmware functions to protect your network from hackers and malicious intruders.



Remote Management Access

Remote Management (via WAN): Allow

Remote Management Port: 8080

Ping from WAN Filter

Ping from WAN Filter: Allow

Stateful Packet Inspection (SPI)

SPI Firewall: Enable

Network Address Translation Settings

Network Address Translation: Enable

PPPoE Passthrough Setup

PPPoE Passthrough: Enable

Figure 8.5 Firewall

Remote Management (via WAN): allow or deny to manage the router from anywhere on the Internet.

Remote Management Port: The port that you will use to address the management from the Internet. For example, if you specify port 8080, then to access the EKI-

6310GN from Internet, you would use a URL of the form: http://xxx.xxx.xxx.xxx:8080/ EKI-6310GN will enable port 8080 when you configure to router mode.

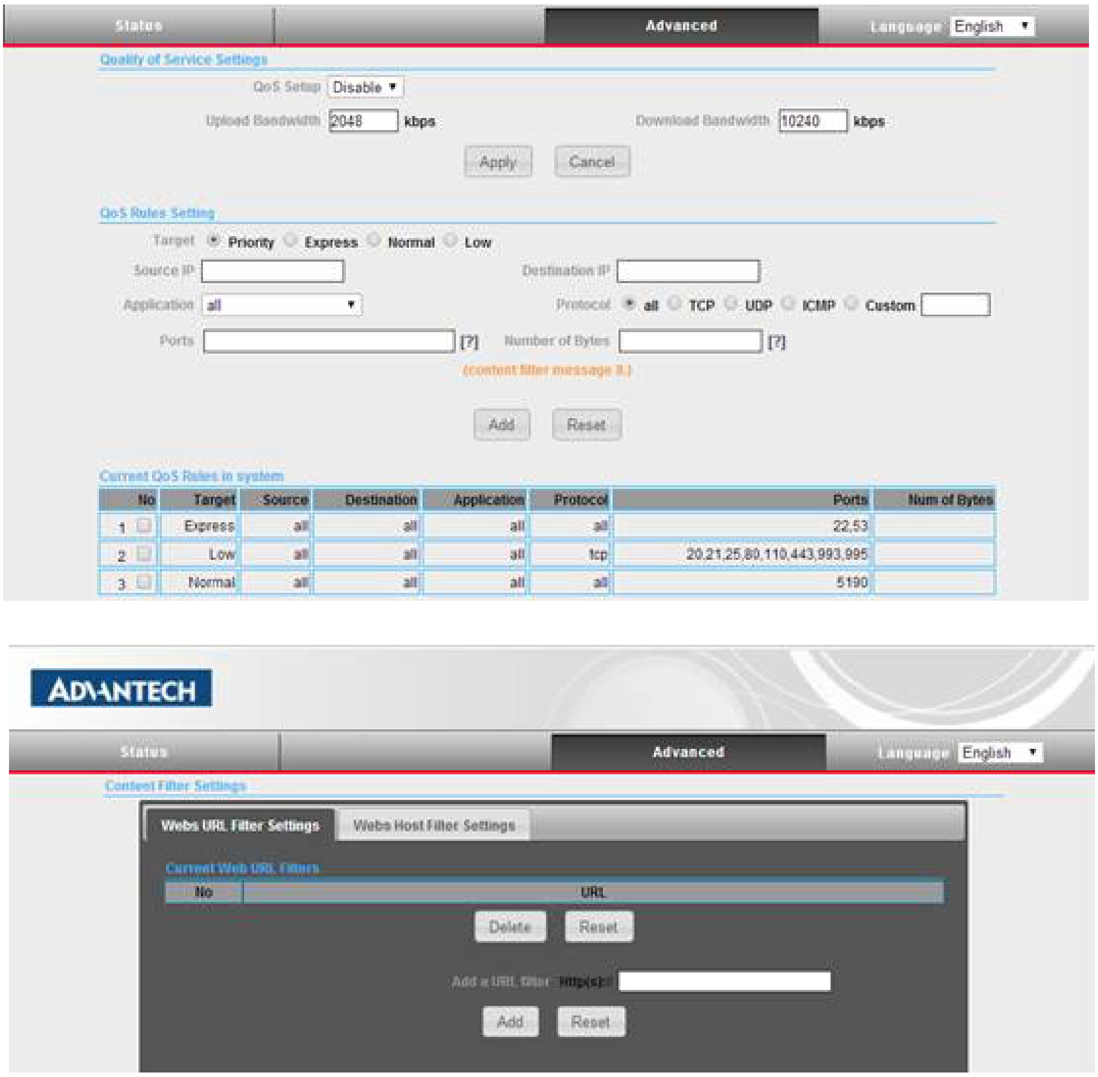
Ping from WAN Filter: When Allow, this outdoor AP/CPE does not respond to ping packets received on the WAN port.

SPI Firewall: SIP firewall help to keep track of the state of network connections (such as TCP streams, UDP communication) traveling across it. It is programmed to distinguish legitimate packets for different types of connections. Only packets matching a known active connection will be allowed by the firewall; others will be rejected.

Network Address Translation: NAT is the process of modifying IP address information in IP packet headers while in transit across a traffic routing device.

8.5 Content Filter

EKI-6310GN provides a variety of options for blocking Internet access based on content, URL and host name.



Language: English

Quality of Service Settings

QoS Setup: Disable

Upload Bandwidth: 2048 kbps

Download Bandwidth: 10240 kbps

QoS Rules Setting

Target: ● Priority ○ Express ○ Normal ○ Low

Source IP:

Destination IP:

Application: all

Protocol: ● all ○ TCP ○ UDP ○ ICMP ○ Custom

Ports: [?]

Number of Bytes: [?]

(content filter message 8.)

Current QoS Rules in system

No	Target	Source	Destination	Application	Protocol	Ports	Num of Bytes
1 □	Express	all	all	all	all	22,53	
2 □	Low	all	all	all	tcp	20,21,25,80,110,443,993,995	
3 □	Normal	all	all	all	all	5190	

Language: English

Content Filter Settings

Current Web URL Filters

No	URL

Add a URL filter: http(s)://

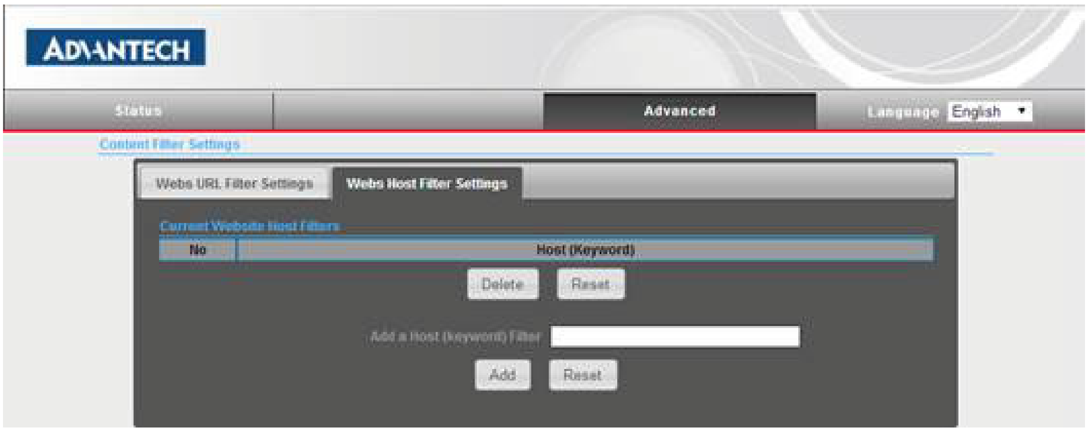
Figure 8.6 URL filter

Web URL Filter Settings: By filtering inbound Uniform Resource Locators (URLs) the risk of compromising the network can be reduced. URLs are commonly used to point to websites. By specifying a URL or a keyword contained in a URL traffic from that site may be blocked.

Current URL Filters: Displays current URL filter.

Add a URL Filter: Add a URL filter to the settings.

Delete a URL Filter: Deletes a URL filter entry from the list.



Language English

Figure 8.7 Host filter

Web Host Filter Settings: Allows Internet content access to be restricted based on web address keywords and web domains. A domain name is the name of a particular web site. For example, for the address www.HOST.com, the domain name is HOST.com. Enter the Keyword then click "Add."

Current Host Filters: Displays current Host filter.

Add a Host Filter: Enters the keyword for a host filtering.

Delete a Host Filter: Deletes a Host filter entry from the list.

Appendix A

Application Wizard

Some applications may require multiple connections, such as Internet gaming, video conferencing, and VoIP calls over the Internet. Enabling the firewall and anti-spoof checking helps protect against attacks over the Internet in some cases.

A.1 Hotspot

In Hotspot application, there are various customers who need to access the Internet. EKI-6310GN can effectively control the access to the Internet.

- Application Architecture
  Here is the architecture example when you want to use EKI-6310GN for WiFi hotspot application.

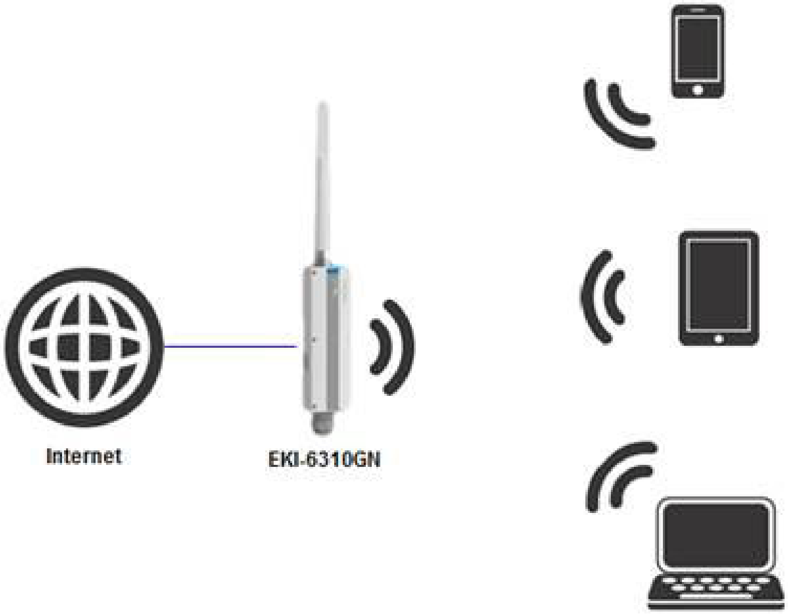
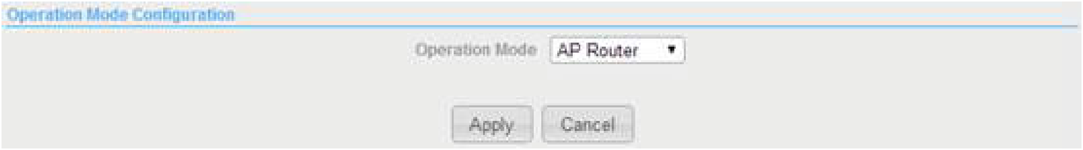


Figure A.1 WiFi Hotspot

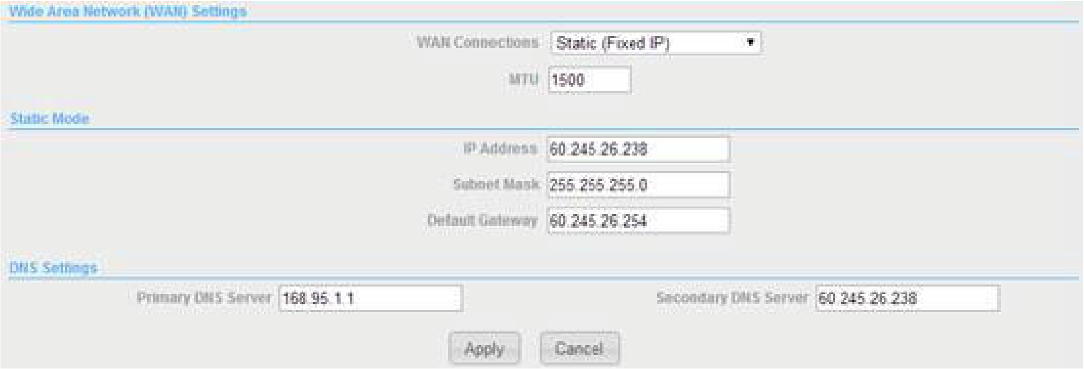
- Configuration Guideline
  Device: EKI-6310GN

1. Configure EKI-6310GN as “AP Router” mode in “Advanced” ? “Operation Mode” page.


Operation Mode Configuration

Operation Mode: AP Router

2. Configure WAN network according your ISP provider, such as static fixed IP, DHCP or PPPoE method in “Advanced” ? “Network Setting” ? “WAN” option. Here is the sample that we get the static fixed IP from our ISP Hinet in Taiwan. We need to enter the fixed IP address, subnet mask, default gateway, primary DNS server or secondary DNS server if we have.



Wide Area Network (WAN) Settings

WAN Connections: Static (Fixed IP)

MTU: 1500

Static Mode

IP Address: 60.245.26.238

Subnet Mask: 255.255.255.0

Default Gateway: 60.245.26.254

DNS Settings

Primary DNS Server: 168.95.1.1

Secondary DNS Server: 60.245.26.238

3. Configure SSID and wireless information that your end device can find, such notebook, pad or cellular phone. You need to configure the information in the page of “Advanced” ? “Wireless Settings” ? “Basic” option

   Here is the sample that I want to provide the wireless network with WPA2-PSK encryption. You need to configure the parameters as following.

   Wireless Mode: Access Point

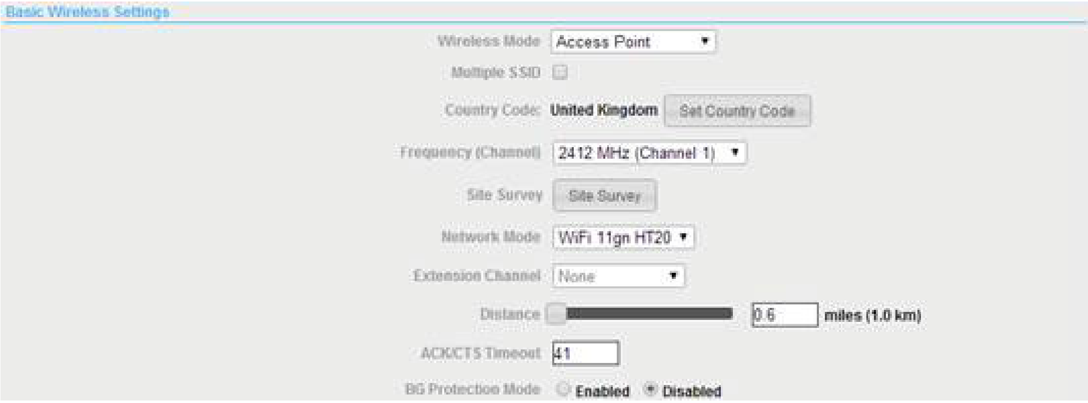
   Frequency (Channel): Channel 1

   Network Mode: WiFi 11gn HT20 (It can support 802.11b / 802.11g / 802.11n end devices)

   Network Name: EKI-6310GN (You can define your own network name)

   Encryption Settings: WPA2-PSK (Suggest that you need use WPA/WPA2, not WEP for security consideration)

   Pre-Shared Key: 1234567890 (The specific key)



Basic Wireless Settings

Wireless Mode: Access Point

Multiple SSID: □

Country Code: United Kingdom

Frequency (Channel): 2412 MHz (Channel 1)

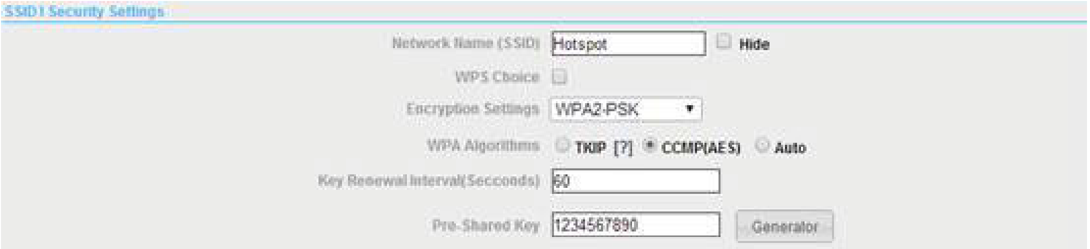
Network Mode: WiFi 11gn HT20

Extension Channel: None

Distance: 0.6 miles (1.0 km)

ACK/CTS Timeout: 41

BG Protection Mode: ○ Enabled ● Disabled



SSID1 Security Settings

Network Name (SSID): Hotspot □ Hide

WPS Choice: □

Encryption Settings: WPA2-PSK

WPA Algorithms: ○ TKIP [?] ● CCMP(AES) ○ Auto

Key Renewal Interval(Secconds): 60

Pre-Shared Key: 1234567890

A.2 Intranet Coverage

In Intranet coverage application, such as that you wish to provide the Wireless coverage to your factory, your client or wireless station wants to access the management server in your factory. In this application, your clients or wireless stations don't access the Internet, and it just needs to access the Intranet server.

- Application Architecture
  Here is the architecture example when you want to use EKI-6310GN for Intranet coverage.

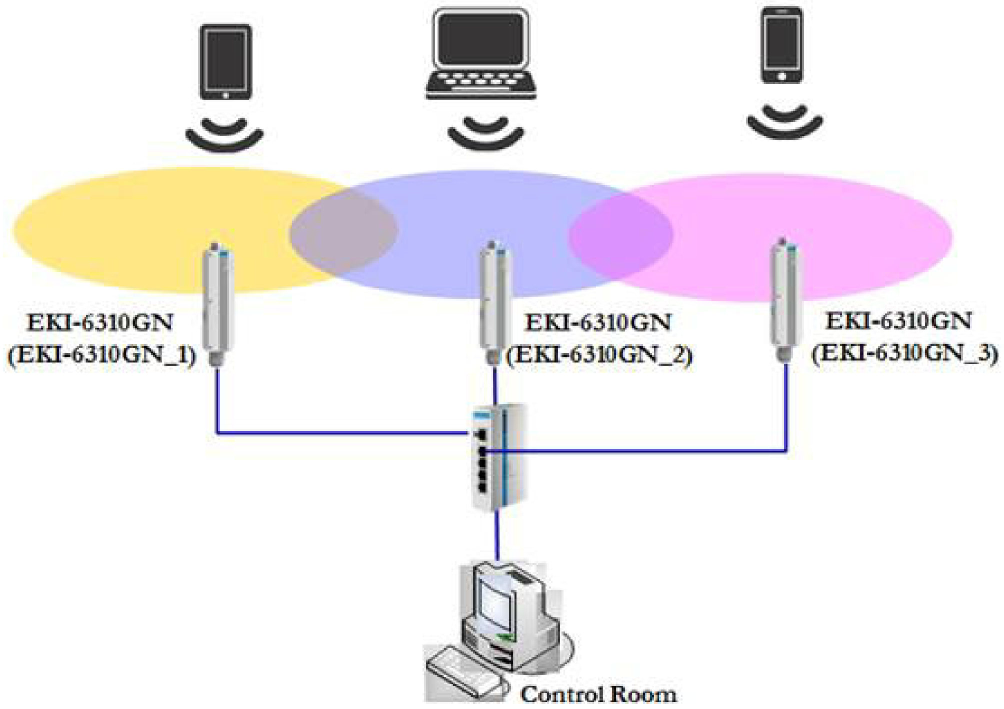
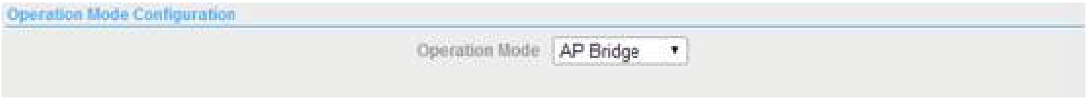


Figure A.2 Intranet coverage

- Configuration Guideline

Device: EKI-6310GN_1

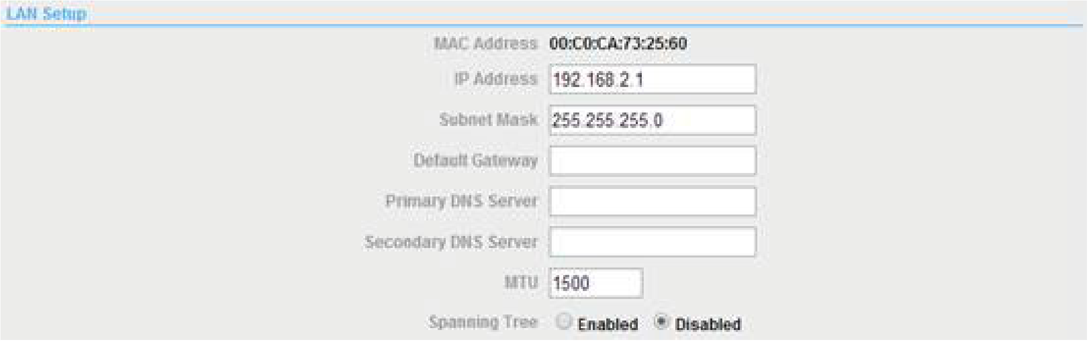
1. Configure EKI-6310GN as "AP Bridge" mode in "Advanced" ' "Operation Mode" page.



Operation Mode Configuration

Operation Mode: AP Bridge ▾

2. Configure Ethernet IP Address for your LAN network in "Advanced" ' "Network Setting" ' "LAN". We assume that all devices will locate in 192.168.2.xx network. You need to assign each AP with specific IP Address '192.168.2.1'.



LAN Setup

MAC Address	00:C0:CA:73:25:60
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Default Gateway	
Primary DNS Server	
Secondary DNS Server	
MTU	1500
Spanning Tree	○ Enabled ● Disabled

3. Configure SSID and wireless information that your end device can find, such notebook, pad or cellular phone. You need to configure the information in the page of "Advanced" ' "Wireless Settings" ' "Basic" option. Here is the sample that I want to provide the wireless network with WPA2-PSK encryption. You need to configure 3 APs with network name (SSID), different channels to avoid interference and same encryption setting and key. Hence, end devices can connect to 3 APs automatically without manual configuration.

   Wireless Mode: Access Point

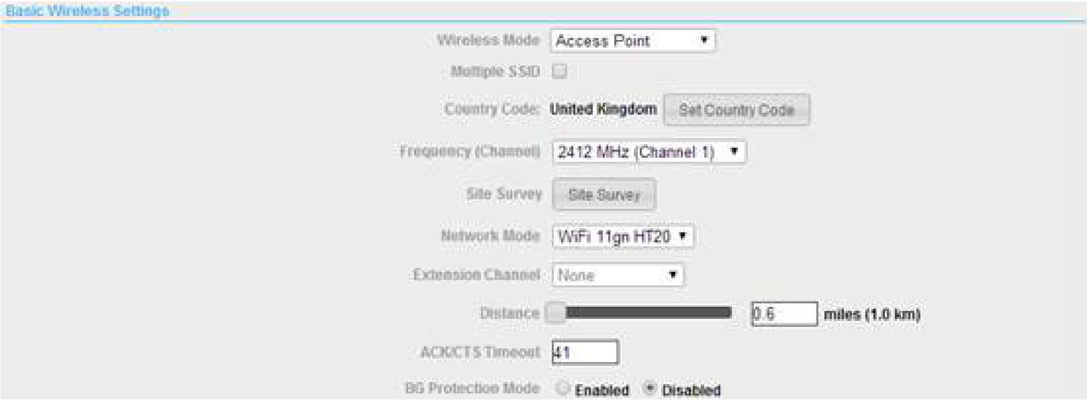
   Frequency (Channel): Channel 1

   Network Mode: WiFi 11gn HT20 (It can support 802.11b / 802.11g / 802.11n end devices)

   Network Name: EKI-6310GN (3 APs shall have same Network name SSID)

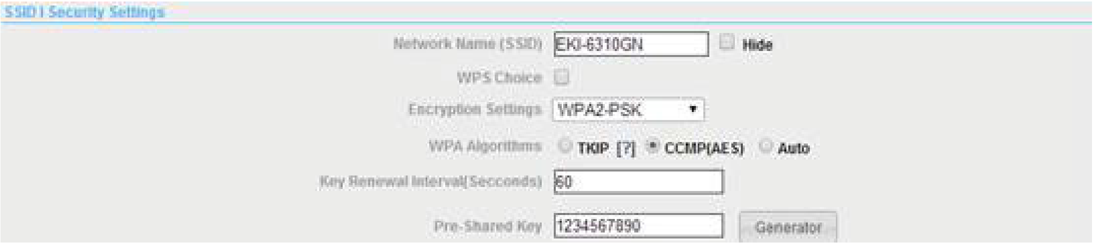
   Encryption Settings: WPA2-PSK (Suggest that you need use WPA/WPA2, not WEP for security consideration)

   Pre-Shared Key: 1234567890 (The specific key)



Basic Wireless Settings

Wireless Mode	Access Point ▾
Multiple SSID	□
Country Code	United Kingdom [Set Country Code]
Frequency (Channel)	2412 MHz (Channel 1) ▾
Site Survey	[Site Survey]
Network Mode	WiFi 11gn HT20 ▾
Extension Channel	None ▾
Distance	0.6 miles (1.0 km)
ACK/CTS Timeout	41
BG Protection Mode	○ Enabled ● Disabled

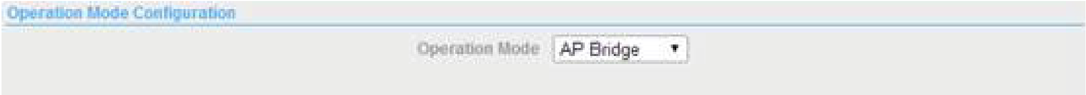


SSID I Security Settings

Network Name (SSID)	EKI-6310GN □ Hide
WPS Choice	□
Encryption Settings	WPA2-PSK ▾
WPA Algorithms	○ TKIP [?] ● CCMP(AES) ○ Auto
Key Renewal Interval(Secconds)	60
Pre-Shared Key	1234567890 [Generator]

Device: EKI-6310GN_2

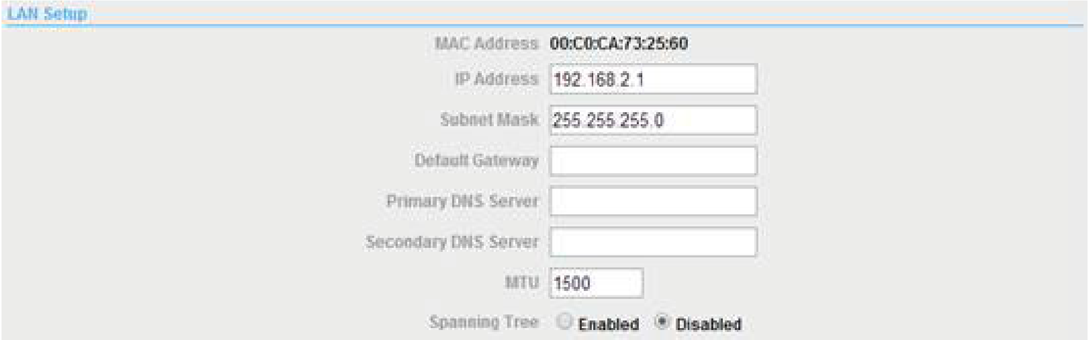
1. Configure EKI-6310GN as "AP Bridge" mode in "Advanced" ' "Operation Mode" page.



Operation Mode Configuration

Operation Mode: AP Bridge ▾

2. Configure Ethernet IP Address for your LAN network in "Advanced" ' "Network Setting" ' "LAN". We assume that all devices will locate in 192.168.2.xx network. You need to assign each AP with specific IP Address '192.168.2.2'.



LAN Setup

MAC Address	00:C0:CA:73:25:60
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Default Gateway	
Primary DNS Server	
Secondary DNS Server	
MTU	1500
Spanning Tree	○ Enabled ● Disabled

3. Configure SSID and wireless information that your end device can find, such notebook, pad or cellular phone. You need to configure the information in the page of "Advanced" ' "Wireless Settings" ' "Basic" option. Here is the sample that I want to provide the wireless network with WPA2-PSK encryption. You need to configure 3 APs with network name (SSID), different channels to avoid interference and same encryption setting and key. Hence, end devices can connect to 3 APs automatically without manual configuration.

Wireless Mode: Access Point

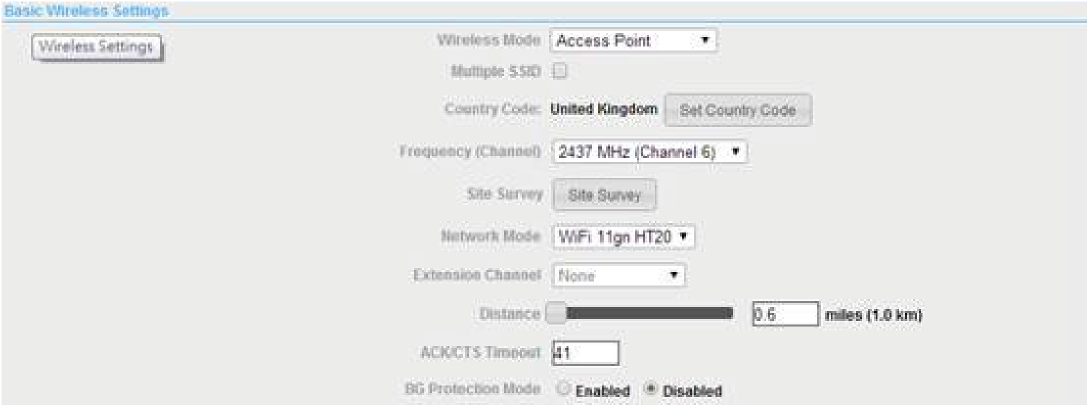
Frequency (Channel): Channel 6

Network Mode: WiFi 11gn HT20 (It can support 802.11b / 802.11g / 802.11n end devices)

Network Name: EKI-6310GN (3 APs shall have same Network name SSID)

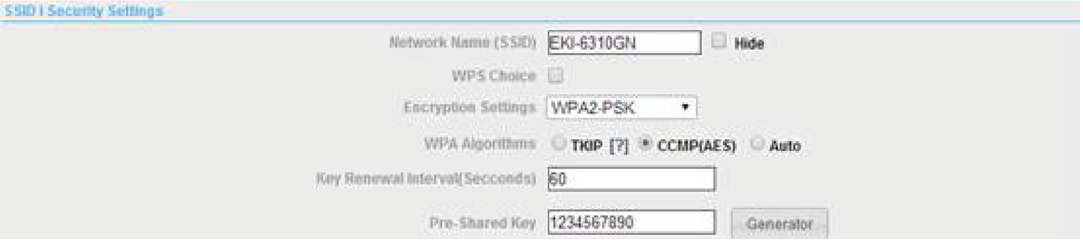
Encryption Settings: WPA2-PSK (Suggest that you need use WPA/WPA2, not WEP for security consideration)

Pre-Shared Key: 1234567890 (The specific key)



Basic Wireless Settings

Wireless Mode	Access Point ▾
Multiple SSID	□
Country Code	United Kingdom [Set Country Code]
Frequency (Channel)	2437 MHz (Channel 6) ▾
Site Survey	[Site Survey]
Network Mode	WiFi 11gn HT20 ▾
Extension Channel	None ▾
Distance	0.6 miles (1.0 km)
ACK/CTS Timeout	41
BG Protection Mode	○ Enabled ● Disabled



SSID1 Security Settings

Network Name (SSID): EKI-6310GN □ Hide

WPS Choice: □

Encryption Settings: WPA2-PSK

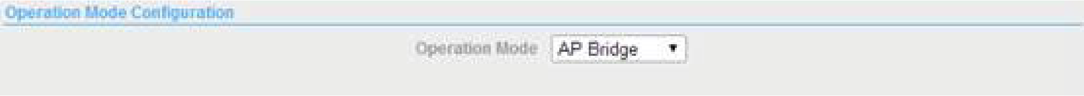
WPA Algorithms: ○ TKIP [?] ● CCMP(AES) ○ Auto

Key Renewal Interval(Secconds): 60

Pre-Shared Key: 1234567890 Generator

Device: EKI-6310GN_3

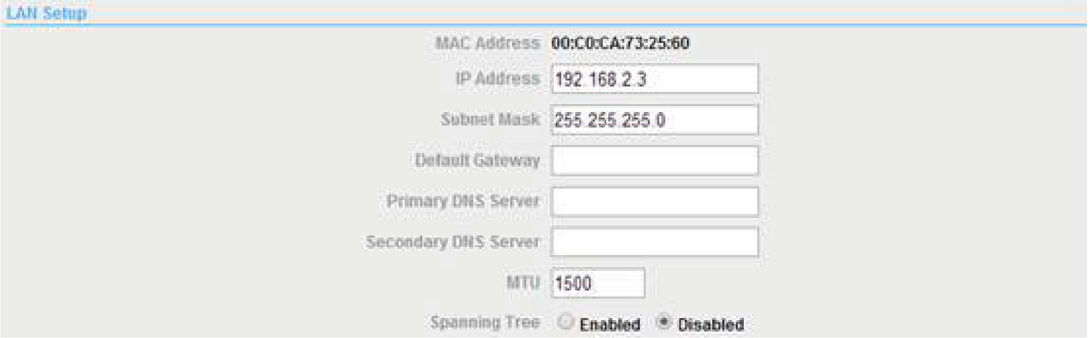
1. Configure EKI-6310GN as "AP Bridge" mode in "Advanced" ' "Operation Mode" page.



Operation Mode Configuration

Operation Mode: AP Bridge

2. Configure Ethernet IP Address for your LAN network in "Advanced" ' "Network Setting" ' "LAN". We assume that all devices will locate in 192.168.2.xx network. You need to assign each AP with specific IP Address '192.168.2.3'.



LAN Setup

MAC Address: 00:C0:CA:73:25:60

IP Address: 192.168.2.3

Subnet Mask: 255.255.255.0

Default Gateway:

Primary DNS Server:

Secondary DNS Server:

MTU: 1500

Spanning Tree: ○ Enabled ● Disabled

3. Configure SSID and wireless information that your end device can find, such notebook, pad or cellular phone. You need to configure the information in the page of "Advanced" ' "Wireless Settings" ' "Basic" option. Here is the sample that I want to provide the wireless network with WPA2-PSK encryption. You need to configure 3 APs with network name (SSID), different channels to avoid interference and same encryption setting and key. Hence, end devices can connect to 3 APs automatically without manual configuration.

   Wireless Mode: Access Point

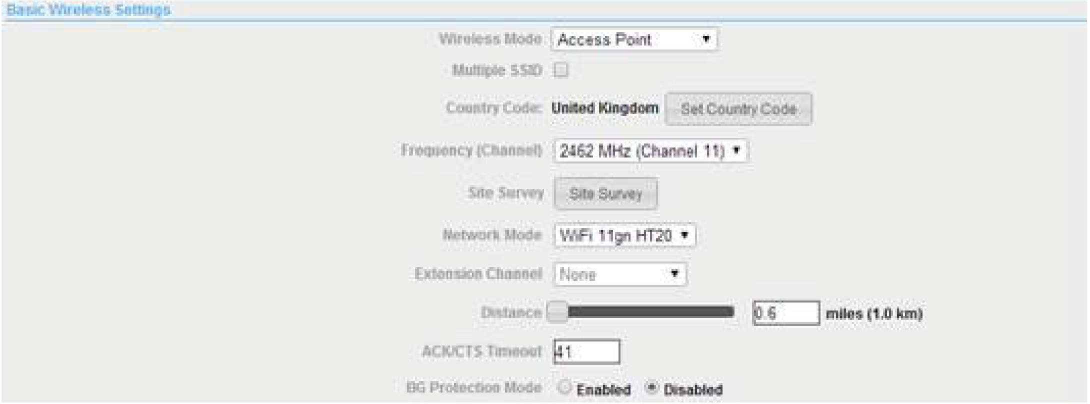
   Frequency (Channel): Channel 11

   Network Mode: WiFi 11gn HT20 (It can support 802.11b / 802.11g / 802.11n end devices)

   Network Name: EKI-6310GN (3 APs shall have same Network name SSID)

   Encryption Settings: WPA2-PSK (Suggest that you need use WPA/WPA2, not WEP for security consideration)

   Pre-Shared Key: 1234567890 (The specific key)



Basic Wireless Settings

Wireless Mode: Access Point ▾

Multiple SSID: □

Country Code: United Kingdom [Set Country Code]

Frequency (Channel): 2462 MHz (Channel 11) ▾

Site Survey: [Site Survey]

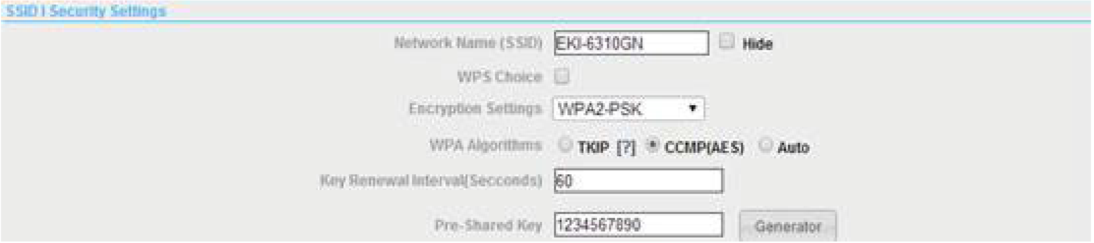
Network Mode: WiFi 11gn HT20 ▾

Extension Channel: None ▾

Distance: 0.6 miles (1.0 km)

ACK/CTS Timeout: 41

BG Protection Mode: ○ Enabled ● Disabled



SSID I Security Settings

Network Name (SSID): EKI-6310GN □ Hide

WPS Choice: □

Encryption Settings: WPA2-PSK ▾

WPA Algorithms: ○ TKIP [?] ● CCMP(AES) ○ Auto

Key Renewal Interval(Secconds): 60

Pre-Shared Key: 1234567890 [Generator]

A.3 Repeater

In some application scenario, you are hard to deployment wired cable between control room and your APs or you want to extend the coverage the coverage of existed Wireless WiFi network. EKI-6310GN that can work as Repeater mode is the best solution.

- Application Architecture
  Here is the architecture example when you want to use EKI-6310GN for wireless extension and repeater application.

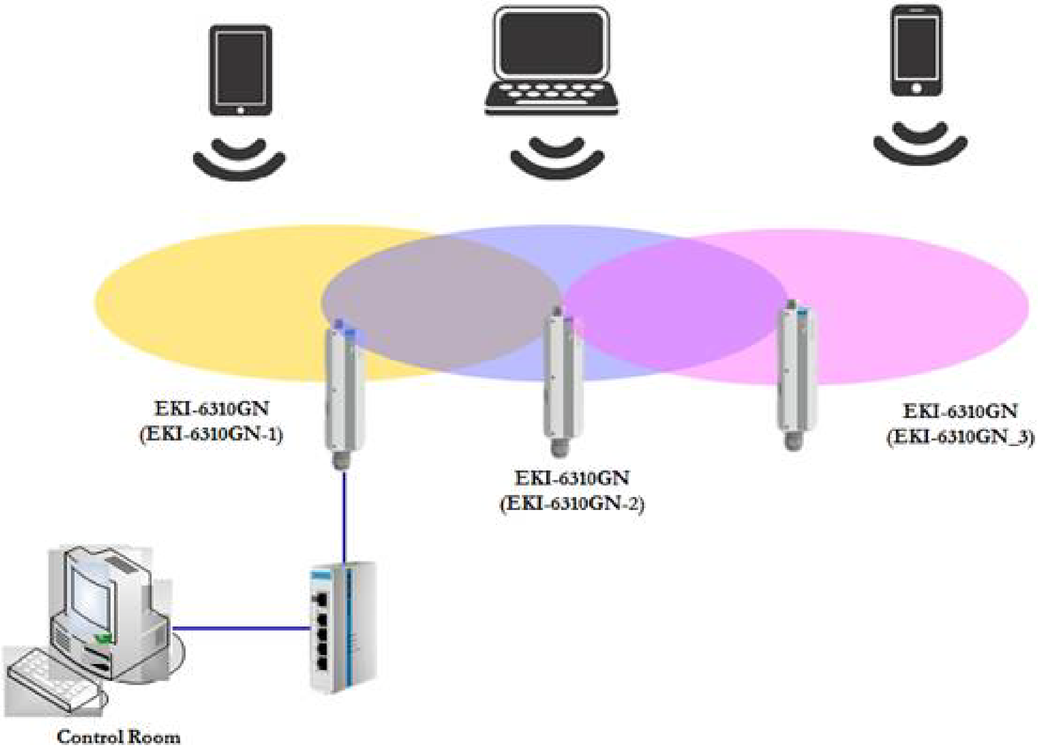
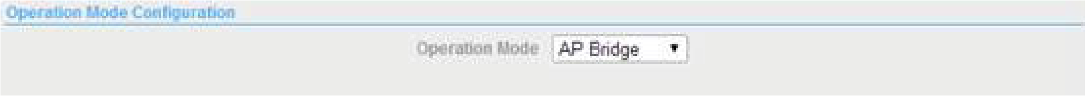


Figure A.3 Repeater usage

- Configuration Guideline

Device: EKI-6310GN_1

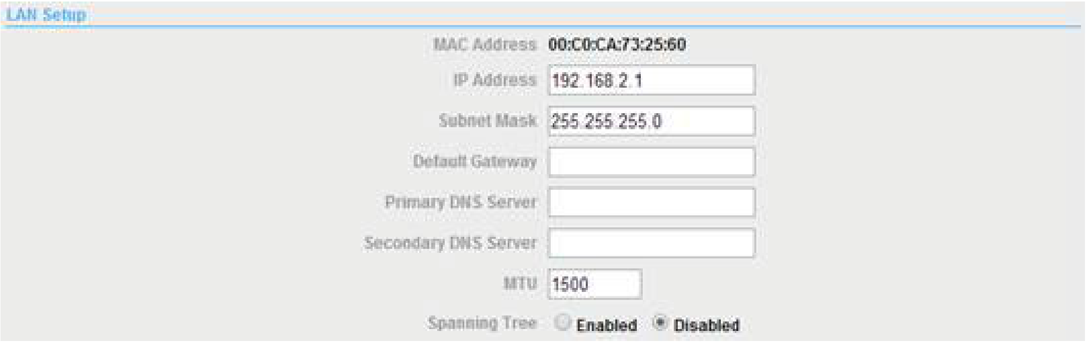
1. Configure EKI-6310GN as "AP Bridge" mode in "Advanced" ' "Operation Mode" page.



Operation Mode Configuration

Operation Mode: AP Bridge ▾

2. Configure Ethernet IP Address '192.168.2.1' for your LAN network in "Advanced" ' "Network Setting" ' "LAN".



LAN Setup

MAC Address: 00:C0:CA:73:25:60

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

Default Gateway:

Primary DNS Server:

Secondary DNS Server:

MTU: 1500

Spanning Tree: ○ Enabled ● Disabled

3. Configure SSID and wireless information that another EKI-6310GN can find. You need to configure the information in the page of "Advanced" ' "Wireless Settings" ' "Basic" option. Here is the sample that I want to provide the wireless network with WPA2-PSK encryption.

   Wireless Mode: WDS Access Point

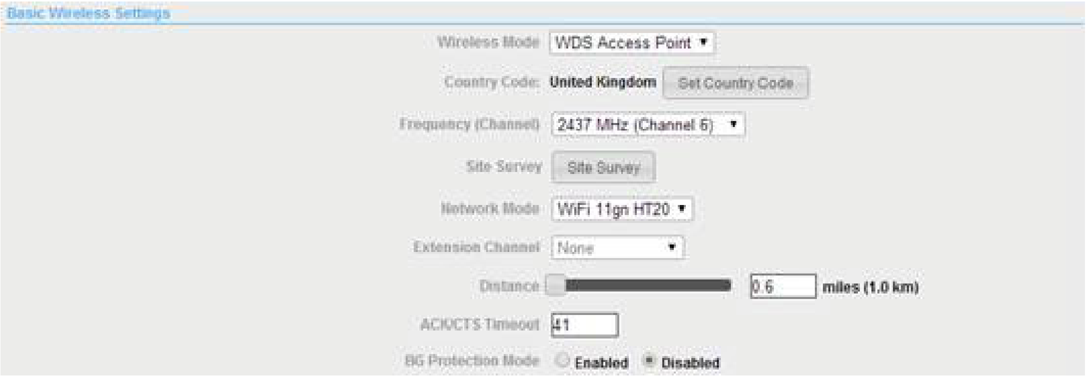
   Frequency (Channel): Channel 1

   Network Mode: WiFi 11gn HT20 (It can support 802.11b / 802.11g / 802.11n end devices)

   Network Name: EKI-6310GN

   Encryption Settings: WPA2-PSK (Suggest that you need use WPA/WPA2, not WEP for security consideration)

   Pre-Shared Key: 1234567890 (The specific key)



Basic Wireless Settings

Wireless Mode: WDS Access Point ▾

Country Code: United Kingdom [Set Country Code]

Frequency (Channel): 2437 MHz (Channel 6) ▾

Site Survey: [Site Survey]

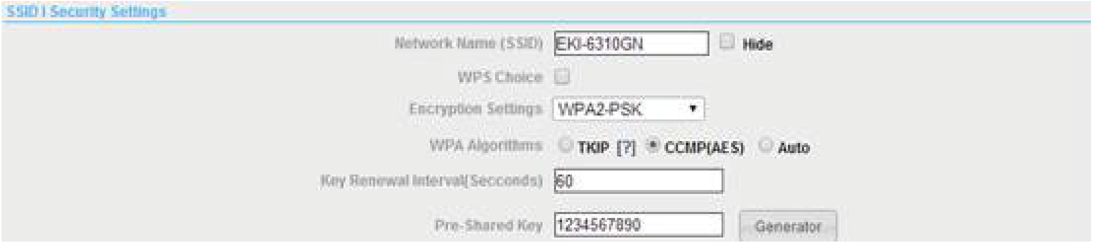
Network Mode: WiFi 11gn HT20 ▾

Extension Channel: None ▾

Distance: 0.6 miles (1.0 km)

ACK/CTS Timeout: 41

BG Protection Mode: ○ Enabled ● Disabled



SSID I Security Settings

Network Name (SSID): EKI-6310GN □ Hide

WPS Choice: □

Encryption Settings: WPA2-PSK ▾

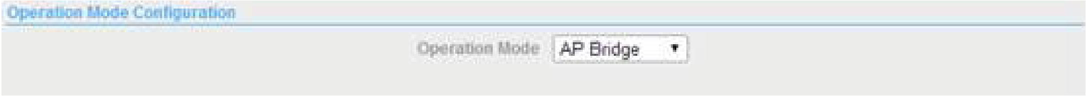
WPA Algorithms: ○ TKIP [?] ● CCMP(AES) ○ Auto

Key Renewal Interval(Secconds): 60

Pre-Shared Key: 1234567890 Generator

Device: EKI-6310GN_2

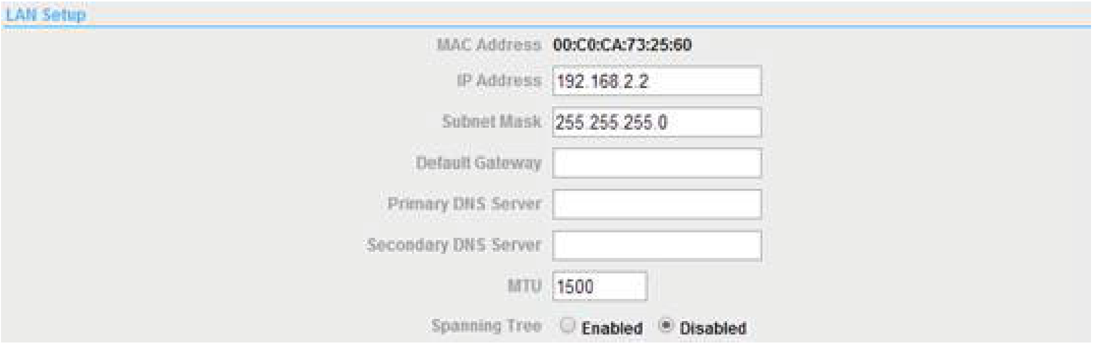
1. Configure EKI-6310GN as "AP Bridge" mode in "Advanced" ' "Operation Mode" page.



Operation Mode Configuration

Operation Mode: AP Bridge ▾

2. Configure Ethernet IP Address '192.168.2.2' for your LAN network in "Advanced" ' "Network Setting" ' "LAN".



LAN Setup

MAC Address: 00:C0:CA:73:25:60

IP Address: 192.168.2.2

Subnet Mask: 255.255.255.0

Default Gateway:

Primary DNS Server:

Secondary DNS Server:

MTU: 1500

Spanning Tree: ○ Enabled ● Disabled

3. Configure SSID and wireless information that another EKI-6310GN can find. You need to configure the information in the page of "Advanced" ' "Wireless Settings" ' "Basic" option. Here is the sample that I want to provide the wireless network with WPA2-PSK encryption.

   Wireless Mode: WDS Repeater

   Root AP MAC Address: keep this field as empty; otherwise you want this Repeater can always connect to specific WDS AP or Repeater

   Frequency (Channel): Channel 6 (To avoid the interference)

   Network Mode: WiFi 11gn HT20 (It can support 802.11b / 802.11g / 802.11n end devices)

   Root AP SSID (SSID II): EKI-6310GN (Shall be same as the SSID of WDS Access Point (Device: EKI-6310GN_1))

   Encryption Settings (SSID II): WPA2-PSK (Shall be same as the encryption setting of WDS Access Point (Device: EKI-6310GN_1))

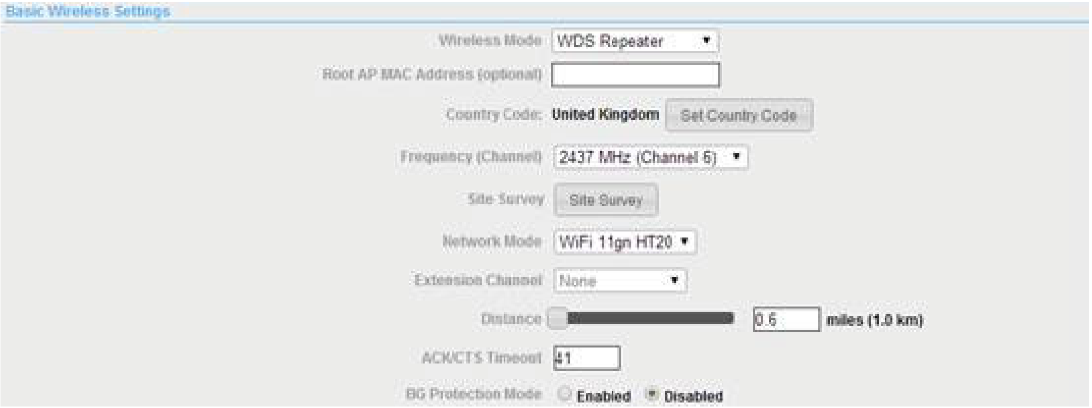
   Pre-Shared Key (SSID II): 1234567890 (Shall be same as the key of WDS Access Point (Device: EKI-6310GN_1))

   Network Name (SSID I): EKI-6310GN (network name that Device: EKI-6310GN_2 want to provides. It can be different of network name of Device: EKI-6310GN_1. It means that Device: EKI-6310GN_2 will connect to Device: EKI-

6310GN_1 in wireless backhaul and provide another different network coverage)

Encryption Settings: WPA2-PSK (encryption that Device: EKI-6310GN_2 want to provides. It can be different of network name of Device: EKI-6310GN_1. It means that Device: EKI-6310GN_2 will connect to Device: EKI-6310GN_1 in wireless backhaul and provide different network coverage)

Pre-Shared Key: 1234567890 (key that Device: EKI-6310GN_2 wants to provide. It can be different of network name of Device: EKI-6310GN_1. It means that Device: EKI-6310GN_2 will connect to Device: EKI-6310GN_1 in wireless backhaul and provide different network coverage)



Basic Wireless Settings

Wireless Mode: WDS Repeater

Root AP MAC Address (optional):

Country Code: United Kingdom

Frequency (Channel): 2437 MHz (Channel 6)

Site Survey

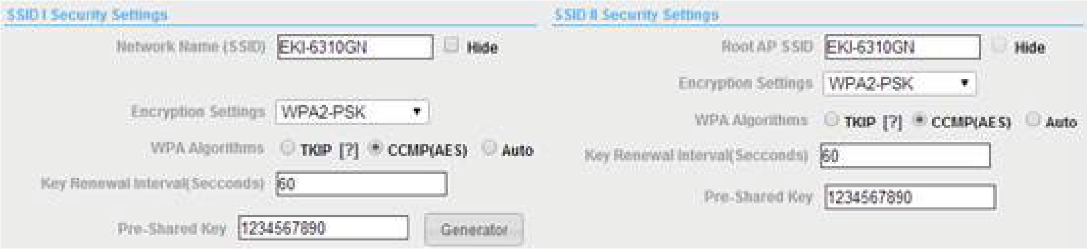
Network Mode: WiFi 11gn HT20

Extension Channel: None

Distance: 0.6 miles (1.0 km)

ACK/CTS Timeout: 41

BG Protection Mode: ○ Enabled ● Disabled



SSID I Security Settings

Network Name (SSID): EKI-6310GN □ Hide

Encryption Settings: WPA2-PSK

WPA Algorithms: ○ TKIP [?] ● CCMP(AES) ○ Auto

Key Renewal Interval(Secconds): 60

Pre-Shared Key: 1234567890

SSID 8 Security Settings

Root AP SSID: EKI-6310GN □ Hide

Encryption Settings: WPA2-PSK

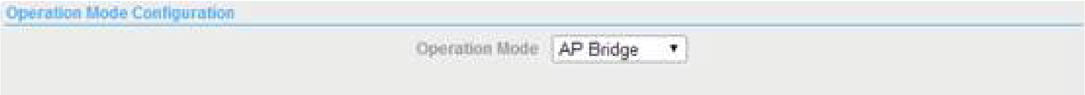
WPA Algorithms: ○ TKIP [?] ● CCMP(AES) ○ Auto

Key Renewal Interval(Secconds): 60

Pre-Shared Key: 1234567890

Device: EKI-6310GN_3

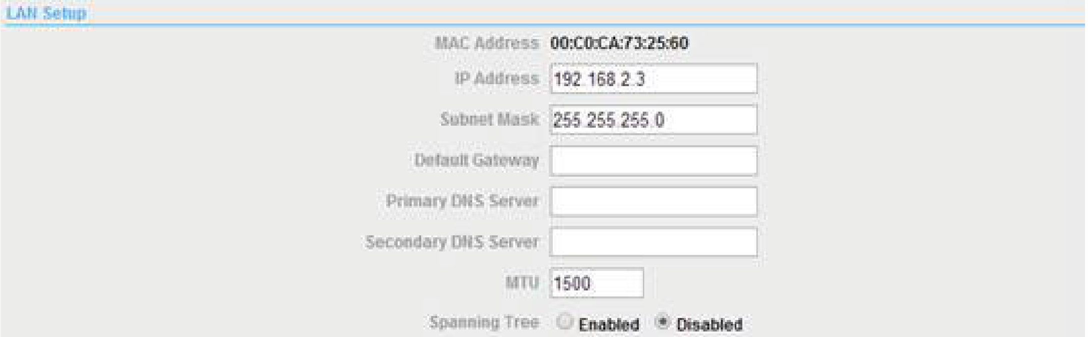
1. Configure EKI-6310GN as "AP Bridge" mode in "Advanced" ' "Operation Mode" page.



Operation Mode Configuration

Operation Mode: AP Bridge

2. Configure Ethernet IP Address '192.168.2.3' for your LAN network in "Advanced" ' "Network Setting" ' "LAN".



LAN Setup

MAC Address	00:C0:CA:73:25:60
IP Address	192.168.2.3
Subnet Mask	255.255.255.0
Default Gateway	
Primary DNS Server	
Secondary DNS Server	
MTU	1500
Spanning Tree	○ Enabled ● Disabled

3. Configure SSID and wireless information that another EKI-6310GN can find. You need to configure the information in the page of "Advanced" ' "Wireless Settings" ' "Basic" option. Here is the sample that I want to provide the wireless network with WPA2-PSK encryption.

   Wireless Mode: WDS Repeater

   Root AP MAC Address: keep this field as empty; otherwise you want this Repeater can always connect to specific WDS AP or Repeater

   Frequency (Channel): Channel 6 (To avoid the interference)

   Network Mode: WiFi 11gn HT20 (It can support 802.11b / 802.11g / 802.11n end devices)

   Root AP SSID (SSID II): EKI-6310GN (Shall be same as the SSID of WDS Repeater (Device: EKI-6310GN_2))

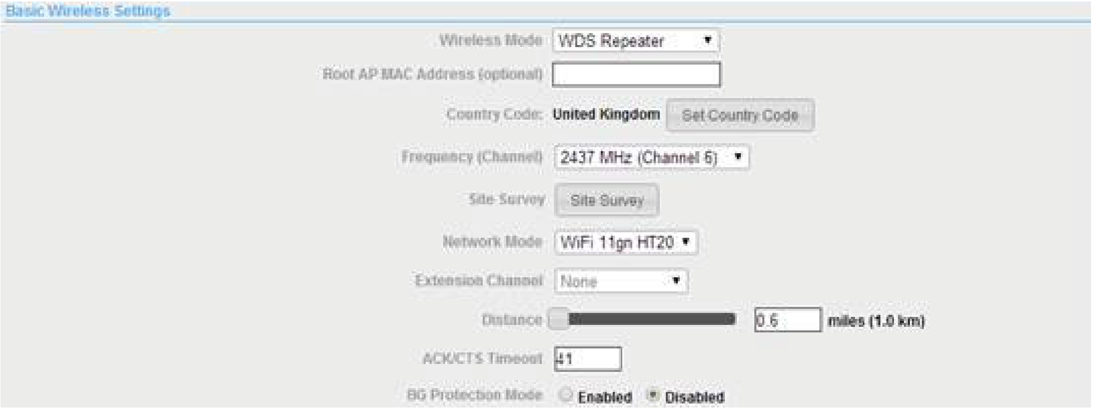
   Encryption Settings (SSID II): WPA2-PSK (Shall be same as the encryption setting of WDS Repeater (Device: EKI-6310GN_2))

   Pre-Shared Key (SSID II): 1234567890 (Shall be same as the key of WDS Repeater (Device: EKI-6310GN_2))

   Network Name (SSID I): EKI-6310GN (network name that Device: EKI-6310GN_2 want to provides. It can be different of network name of Device: EKI-6310GN_2. It means that Device: EKI-6310GN_3 will connect to Device: EKI-6310GN_2 in wireless backhaul and provide different network coverage)

   Encryption Settings: WPA2-PSK (encryption that Device: EKI-6310GN_3 wants to provide. It can be different of network name of Device: EKI-6310GN_2. It means that Device: EKI-6310GN_3 will connect to Device: EKI-6310GN_2 in wireless backhaul and provide different network coverage)

   Pre-Shared Key: 1234567890 (key that Device: EKI-6310GN_3 want to provides. It can be different of network name of Device: EKI-6310GN_2. It means that Device: EKI-6310GN_3 will connect to Device: EKI-6310GN_2 in wireless backhaul and provide different network coverage)



Basic Wireless Settings

Wireless Mode: WDS Repeater

Root AP MAC Address (optional):

Country Code: United Kingdom [Set Country Code]

Frequency (Channel): 2437 MHz (Channel 6)

Site Survey: [Site Survey]

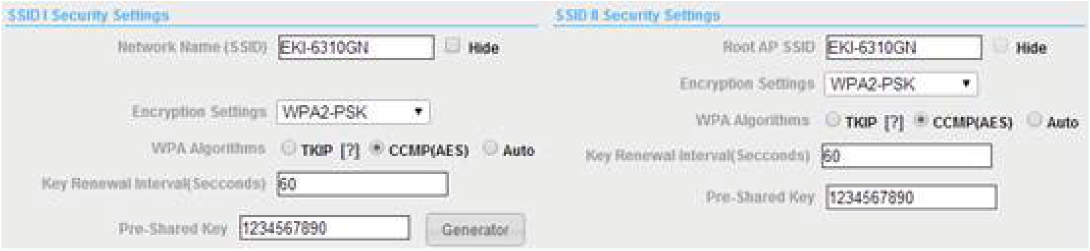
Network Mode: WiFi 11gn HT20

Extension Channel: None

Distance: 0.6 miles (1.0 km)

ACK/CTS Timeout: 41

BG Protection Mode: ○ Enabled ● Disabled



SSID I Security Settings

Network Name (SSID): EKI-6310GN □ Hide

Encryption Settings: WPA2-PSK

WPA Algorithms: ○ TKIP [?] ● CCMP(AES) ○ Auto

Key Renewal Interval(Secconds): 60

Pre-Shared Key: 1234567890 [Generator]

SSID II Security Settings

Root AP SSID: EKI-6310GN □ Hide

Encryption Settings: WPA2-PSK

WPA Algorithms: ○ TKIP [?] ● CCMP(AES) ○ Auto

Key Renewal Interval(Secconds): 60

Pre-Shared Key: 1234567890

A.4 Long Distance Point-to-point

If you want to exchange the data between two sites and the distance between two sites is 6 miles far away, EKI-6310GN can help you to reach the target.

- Application Architecture
  Here is the architecture example when you want to use EKI-6310GN for Long-Distance application.

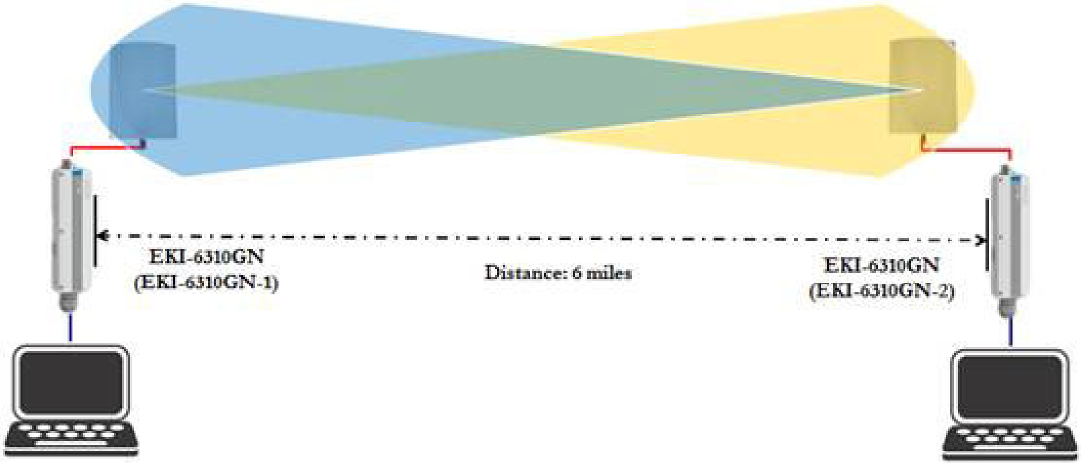
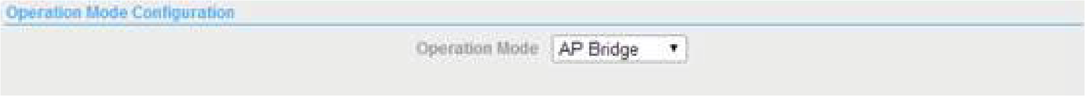


Figure A.4 Long distance Transition

- Configuration Guideline

Device: EKI-6310GN_1

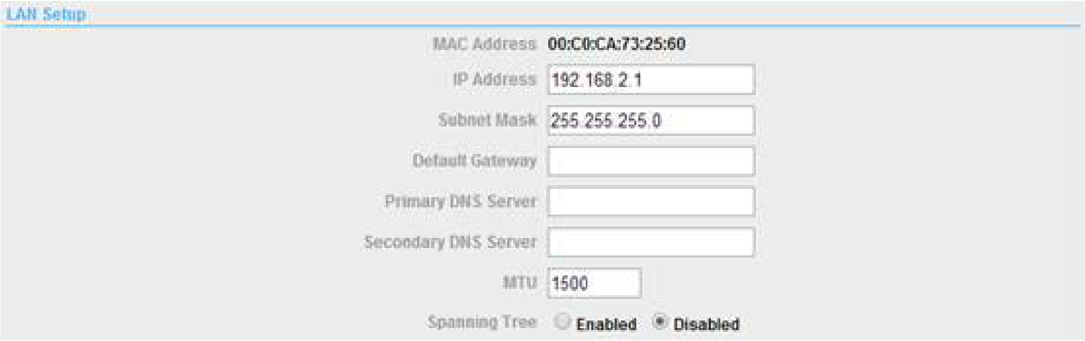
1. Configure EKI-6310GN as "AP Bridge" mode in "Advanced" ' "Operation Mode" page.



Operation Mode Configuration

Operation Mode: AP Bridge

2. Configure Ethernet IP Address '192.168.2.1' for your LAN network in "Advanced" ' "Network Setting" ' "LAN".



LAN Setup

MAC Address	00:C0:CA:73:25:60
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Default Gateway	
Primary DNS Server	
Secondary DNS Server	
MTU	1500
Spanning Tree	○ Enabled ● Disabled

3. Configure SSID and wireless information that another EKI-6310GN can find. You need to configure the information in the page of "Advanced" ' "Wireless Settings" ' "Basic" option. Here is the sample that I want to provide the wireless network with WPA2-PSK encryption.

   Wireless Mode: Access Point

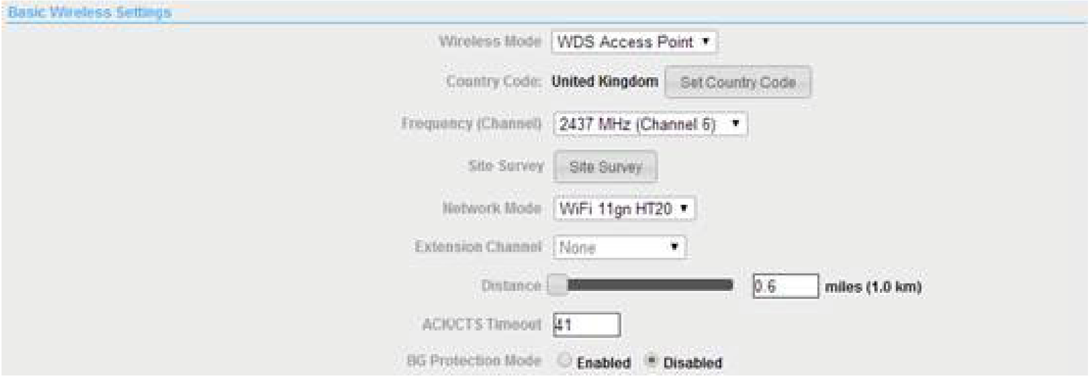
   Frequency (Channel): Channel 1

   Network Mode: WiFi 11gn HT20 (It can support 802.11b / 802.11g / 802.11n end devices)

   Network Name: EKI-6310GN

   Encryption Settings: WPA2-PSK (Suggest that you need use WPA/WPA2, not WEP for security consideration)

   Pre-Shared Key: 1234567890 (The specific key)



Basic Wireless Settings

Wireless Mode: WDS Access Point ▾

Country Code: United Kingdom [Set Country Code]

Frequency (Channel): 2437 MHz (Channel 6) ▾

Site Survey: [Site Survey]

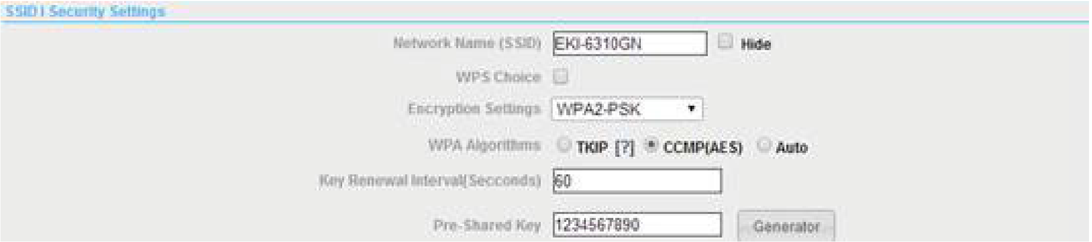
Network Mode: WiFi 11gn HT20 ▾

Extension Channel: None ▾

Distance: 0.6 miles (1.0 km)

ACK/CTS Timeout: 41

BG Protection Mode: ○ Enabled ● Disabled



SSID I Security Settings

Network Name (SSID): EKI-6310GN □ Hide

WPS Choice: □

Encryption Settings: WPA2-PSK ▾

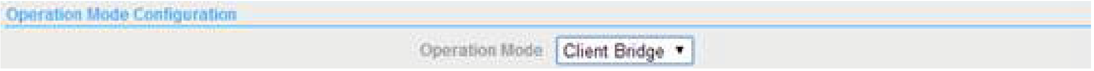
WPA Algorithms: ○ TKIP [?] ● CCMP(AES) ○ Auto

Key Renewal Interval(Secconds): 60

Pre-Shared Key: 1234567890 [Generator]

Device: EKI-6310GN_2

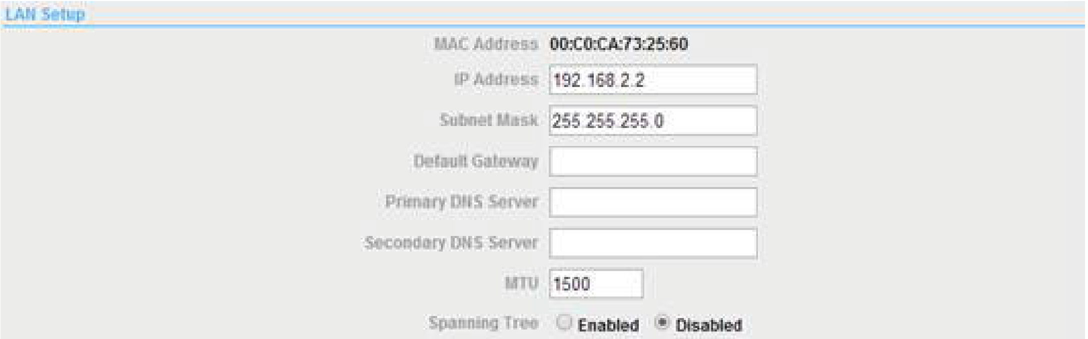
1. Configure EKI-6310GN as "Client Bridge" mode in "Advanced" ' "Operation Mode" page.



Operation Mode Configuration

Operation Mode: Client Bridge ▾

2. Configure Ethernet IP Address '192.168.2.2' for your LAN network in "Advanced" ' "Network Setting" ' "LAN".



LAN Setup

MAC Address: 00:C0:CA:73:25:60

IP Address: 192.168.2.2

Subnet Mask: 255.255.255.0

Default Gateway:

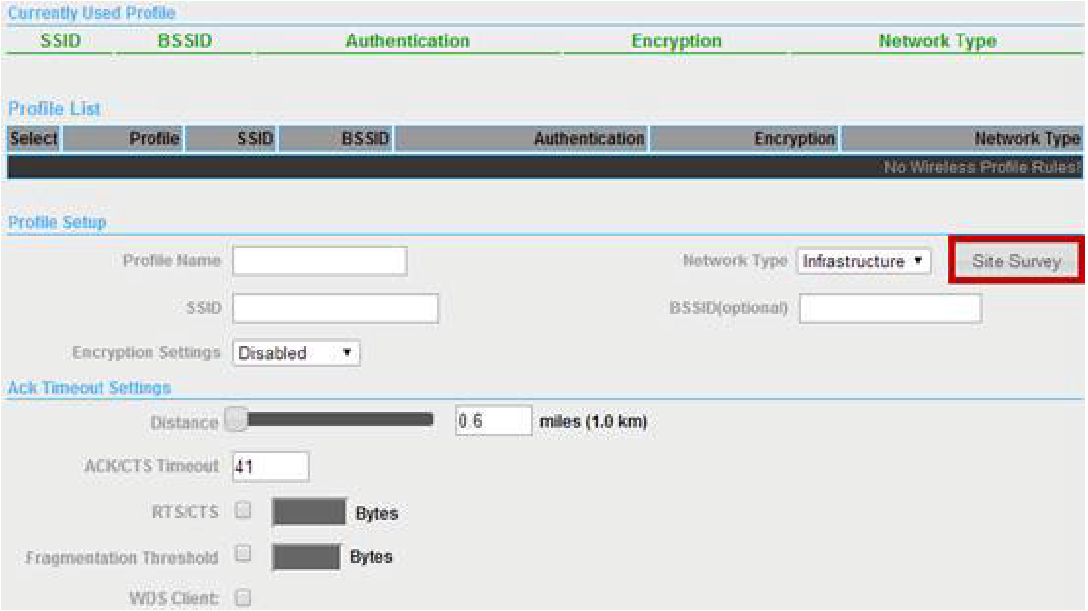
Primary DNS Server:

Secondary DNS Server:

MTU: 1500

Spanning Tree: ○ Enabled ● Disabled

3. Configure client profile to connect with Access Point in "Advanced" ' "Wireless settings" ' "Profile Settings". You can do the Site Survey to find the SSID of matched Access Point on the click of "Site Survey" button if you already had installed the EKI-6310GN in right location.



Currently Used Profile

SSID	BSSID	Authentication	Encryption	Network Type

Profile List

Select	Profile	SSID	BSSID	Authentication	Encryption	Network Type
						No Wireless Profile Rules!

Profile Setup

Profile Name:

Network Type: Infrastructure ▾

SSID:

BSSID(optional):

Encryption Settings: Disabled ▾

Ack Timeout Settings

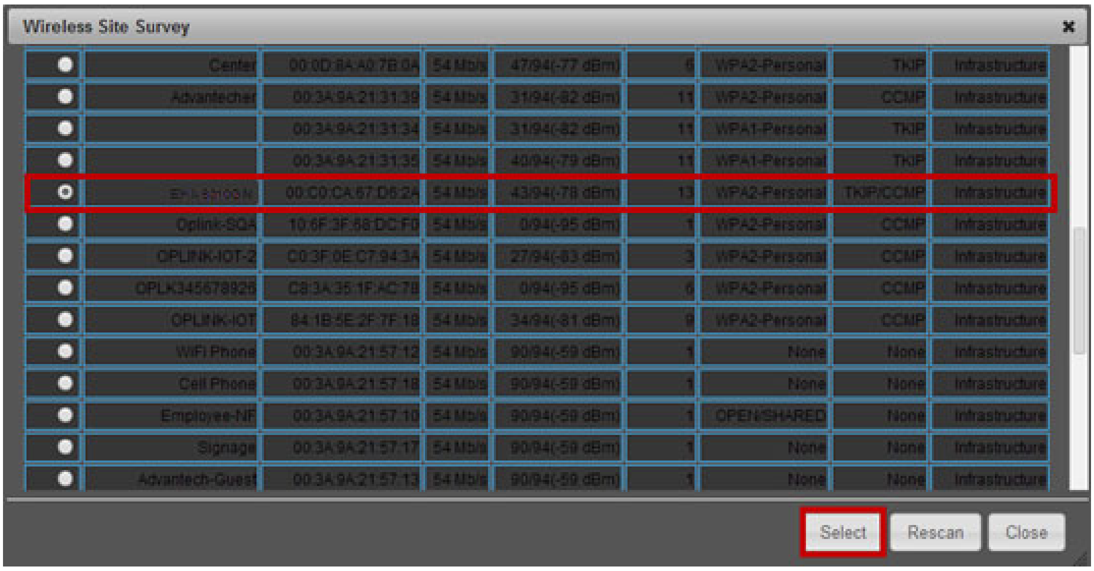
Distance: 0.6 miles (1.0 km)

ACK/CTS Timeout: 41

RTS/CTS □ Bytes

Fragmentation Threshold □ Bytes

WDS Client: □



Wireless Site Survey

○	Center	00:0D:8A:A0:7B:0A	54 Mb/s	47/94(-77 dBm)	6	WPA2-Personal	TKIP	Infrastructure
○	Advantecher	00:3A:9A:21:31:39	54 Mb/s	31/94(-82 dBm)	11	WPA2-Personal	CCMP	Infrastructure
○		00:3A:9A:21:31:34	54 Mb/s	31/94(-82 dBm)	11	WPA1-Personal	TKIP	Infrastructure
○		00:3A:9A:21:31:35	54 Mb/s	40/94(-79 dBm)	11	WPA1-Personal	TKIP	Infrastructure
●	EKI-6310GN	00:C0:CA:67:D6:2A	54 Mb/s	43/94(-78 dBm)	13	WPA2-Personal	TKIP/CCMP	Infrastructure
○	Oplink-SQA	10:6F:3F:68:DC:F0	54 Mb/s	0/94(-95 dBm)	1	WPA2-Personal	CCMP	Infrastructure
○	OPLINK-IOT-2	C0:3F:0E:C7:94:3A	54 Mb/s	27/94(-83 dBm)	3	WPA2-Personal	CCMP	Infrastructure
○	OPLK345678926	C8:3A:35:1F:AC:78	54 Mb/s	0/94(-95 dBm)	6	WPA2-Personal	CCMP	Infrastructure
○	OPLINK-IOT	84:1B:5E:2F:7F:18	54 Mb/s	34/94(-81 dBm)	9	WPA2-Personal	CCMP	Infrastructure
○	WiFi Phone	00:3A:9A:21:57:12	54 Mb/s	90/94(-59 dBm)	1	None	None	Infrastructure
○	Cell Phone	00:3A:9A:21:57:18	54 Mb/s	90/94(-59 dBm)	1	None	None	Infrastructure
○	Employee-NF	00:3A:9A:21:57:10	54 Mb/s	90/94(-59 dBm)	1	OPEN/SHARED	None	Infrastructure
○	Signage	00:3A:9A:21:57:17	54 Mb/s	90/94(-59 dBm)	1	None	None	Infrastructure
○	Advantech-Guest	00:3A:9A:21:57:13	54 Mb/s	90/94(-59 dBm)	1	None	None	Infrastructure

4. Enter the encryption information.

   Profile Name: EKI-6310GN (EKI-6310GN will fill-in the profile name same as SSID when you select access point through site survey)

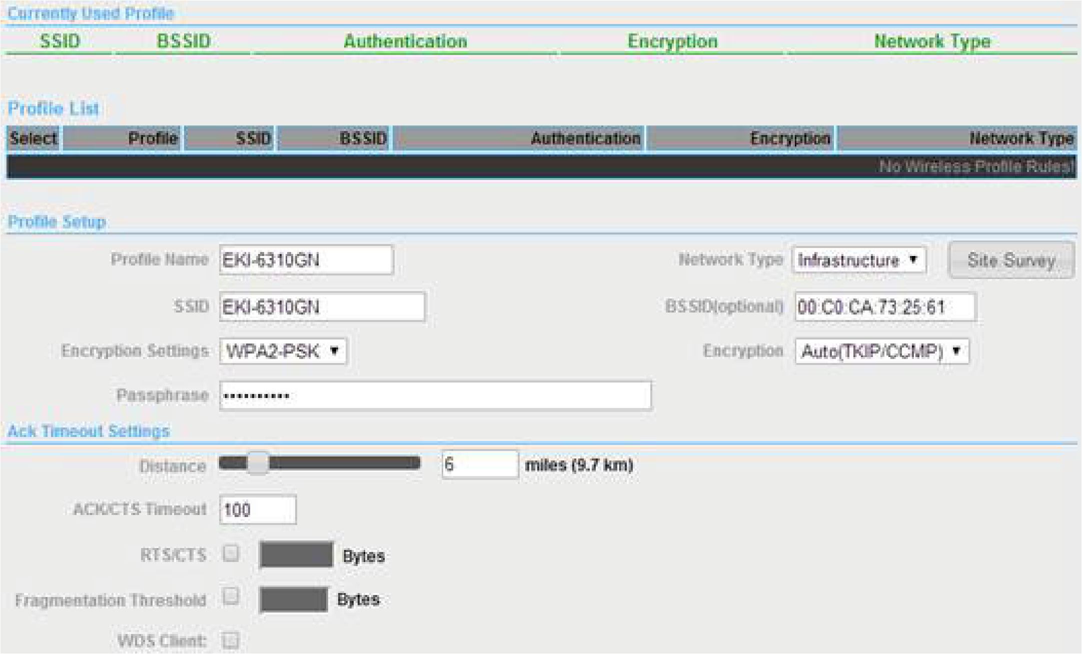
   SSID: EKI-6310GN (EKI-6310GN will fill-in the SSID when you select access point through site survey)

   BSSID: Fill-in the MAC address of Access Point (It will help to have stable connection, because client will only be able to specific AP with same BSSID.)

   Encryption Settings: WPA2-PSK (EKI-6310GN will select the matched encryption setting automatically if you select the access point through site survey.)

   Passphrase: 1234567890 (key that Device: EKI-6310GN_1 Provides)

   Distance: 6 miles (Please select the accuracy distance between access point and client. Because the RTT will be longer, you transmit in longer distance. If you don't enlarge the distance, some packets will be dropped when the RTT is longer than ACK timeout.)



Currently Used Profile

SSID	BSSID	Authentication	Encryption	Network Type

Profile List

Select	Profile	SSID	BSSID	Authentication	Encryption	Network Type
No Wireless Profile Rules!						

Profile Setup

Profile Name: EKI-6310GN
Network Type: Infrastructure ▾
Site Survey
SSID: EKI-6310GN
BSSID(optional): 00:C0:CA:73:25:61
Encryption Settings: WPA2-PSK ▾
Encryption: Auto(TKIP/CCMP) ▾
Passphrase: ••••••••••

Ack Timeout Settings

Distance: 6 miles (9.7 km)
ACK/CTS Timeout: 100
RTS/CTS ☐ Bytes
Fragmentation Threshold ☐ Bytes
WDS Client: ☐

A.5 Fast Roaming

In some application, clients are in moving stage, such as AGV application.

- Application Architecture
  Here is the architecture example when you want to use EKI-6310GN for AGV application.

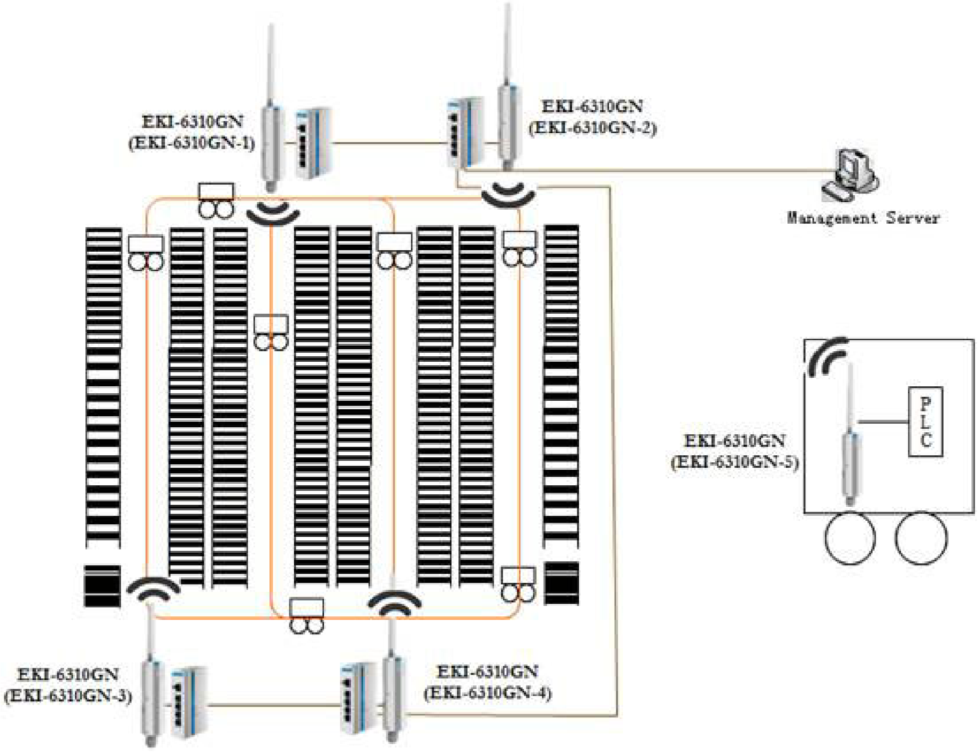
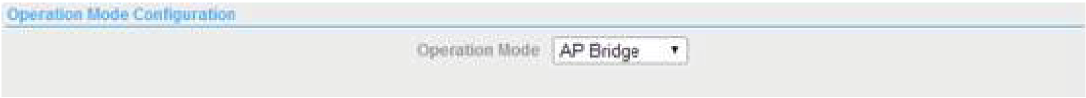


Figure A.5 AGV - Fast Roaming

- Configuration Guideline

Device: EKI-6310GN_1

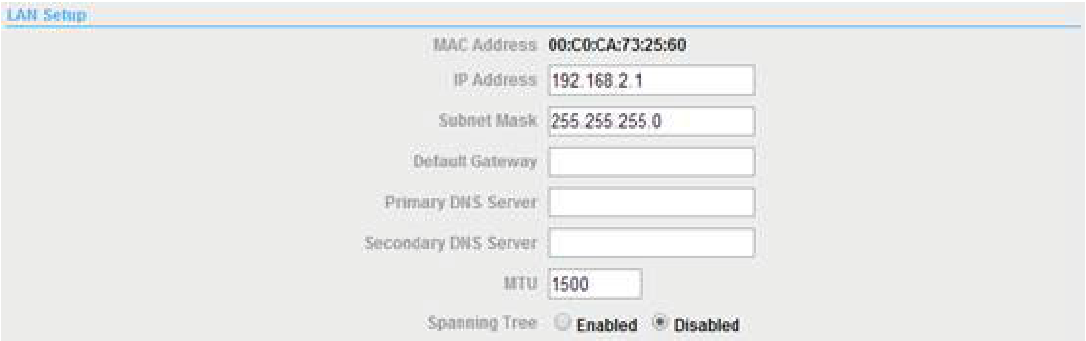
1. Configure EKI-6310GN as "AP Bridge" mode in "Advanced" ' "Operation Mode" page.



Operation Mode Configuration

Operation Mode: AP Bridge

2. Configure Ethernet IP Address for your LAN network in "Advanced" ' "Network Setting" ' "LAN". We assume that all devices will locate in 192.168.2.xx network. You need to assign each AP with specific IP Address '192.168.2.1'.



LAN Setup

MAC Address 00:C0:CA:73:25:60

IP Address 192.168.2.1

Subnet Mask 255.255.255.0

Default Gateway

Primary DNS Server

Secondary DNS Server

MTU 1500

Spanning Tree ○ Enabled ● Disabled

3. Configure SSID and wireless information that your end device can find, such notebook, pad or cellular phone. You need to configure the information in the page of "Advanced" ' "Wireless Settings" ' "Basic" option. If you want EKI-6310GN to be able to have fast roaming function when it roams between EKI-6310GN APs, EKI-6310GN CAN NOT have encryption.

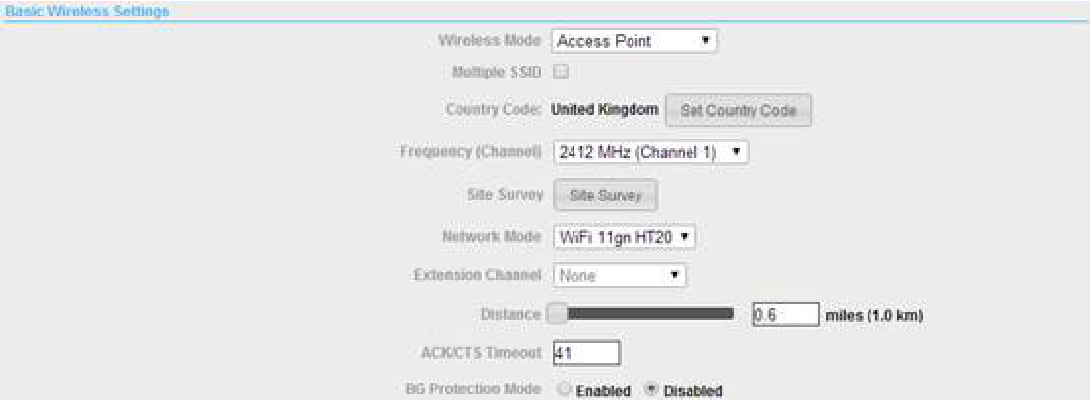
Wireless Mode: Access Point

Frequency (Channel): Channel 1

Network Mode: WiFi 11gn HT20 (It can support 802.11b / 802.11g / 802.11n end devices)

Network Name: EKI-6310GN (4 APs shall have same Network name SSID)

Encryption Settings: Disable



Basic Wireless Settings

Wireless Mode Access Point

Multiple SSID □

Country Code United Kingdom

Frequency (Channel) 2412 MHz (Channel 1)

Site Survey

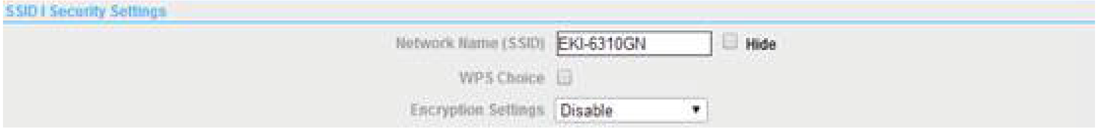
Network Mode WiFi 11gn HT20

Extension Channel None

Distance 0.6 miles (1.0 km)

ACK/CTS Timeout 41

BG Protection Mode ○ Enabled ● Disabled



SSID I Security Settings

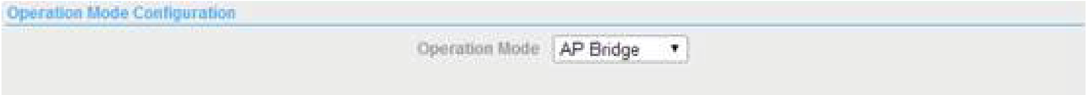
Network Name (SSID) EKI-6310GN □ Hide

WPS Choice □

Encryption Settings Disable

Device: EKI-6310GN_2

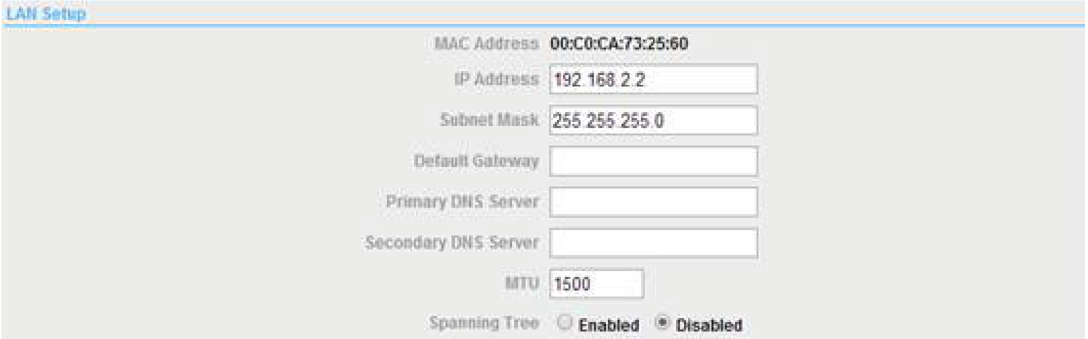
1. Configure EKI-6310GN as "AP Bridge" mode in "Advanced" ' "Operation Mode" page.



Operation Mode Configuration

Operation Mode: AP Bridge ▾

2. Configure Ethernet IP Address for your LAN network in "Advanced" ' "Network Setting" ' "LAN". We assume that all devices will locate in 192.168.2.xx network. You need to assign each AP with specific IP Address '192.168.2.2'.



LAN Setup

MAC Address: 00:C0:CA:73:25:60
IP Address: 192.168.2.2
Subnet Mask: 255.255.255.0
Default Gateway:
Primary DNS Server:
Secondary DNS Server:
MTU: 1500
Spanning Tree: ○ Enabled ● Disabled

3. Configure SSID and wireless information that your end device can find, such notebook, pad or cellular phone. You need to configure the information in the page of "Advanced" ' "Wireless Settings" ' "Basic" option. If you want EKI-6310GN to be able to have fast roaming function when it roams between EKI-6310GN APs, EKI-6310GN CAN NOT have encryption.

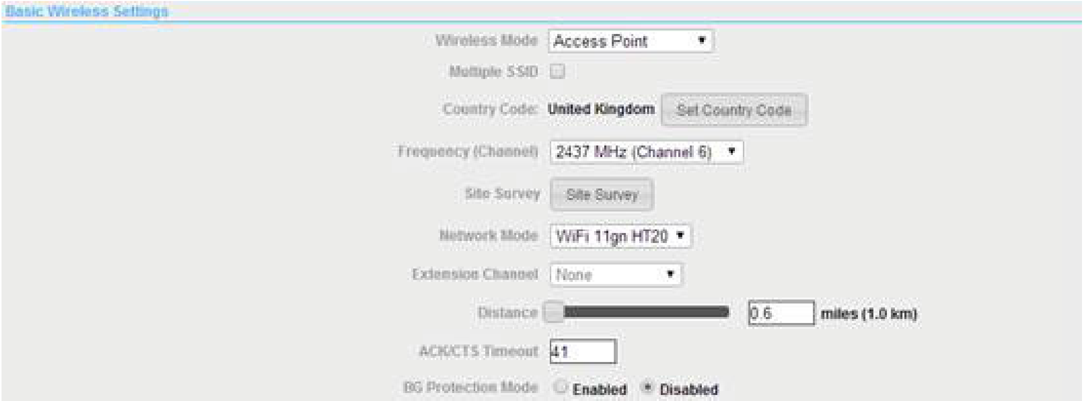
   Wireless Mode: Access Point

   Frequency (Channel): Channel 6

   Network Mode: WiFi 11gn HT20 (It can support 802.11b / 802.11g / 802.11n end devices)

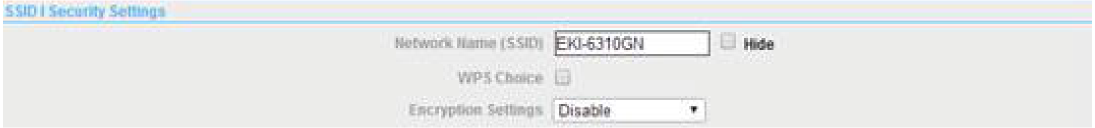
   Network Name: EKI-6310GN (4 APs shall have same Network name SSID)

   Encryption Settings: Disable



Basic Wireless Settings

Wireless Mode: Access Point ▾
Multiple SSID: □
Country Code: United Kingdom [Set Country Code]
Frequency (Channel): 2437 MHz (Channel 6) ▾
Site Survey: [Site Survey]
Network Mode: WiFi 11gn HT20 ▾
Extension Channel: None ▾
Distance: 0.6 miles (1.0 km)
ACK/CTS Timeout: 41
BG Protection Mode: ○ Enabled ● Disabled

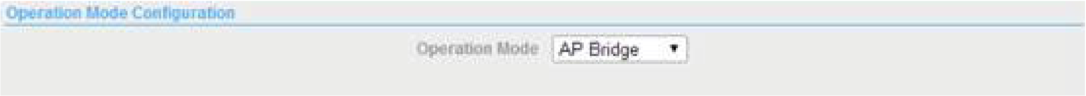


SSID I Security Settings

Network Name (SSID): EKI-6310GN □ Hide
WPS Choice: □
Encryption Settings: Disable ▾

Device: EKI-6310GN_3

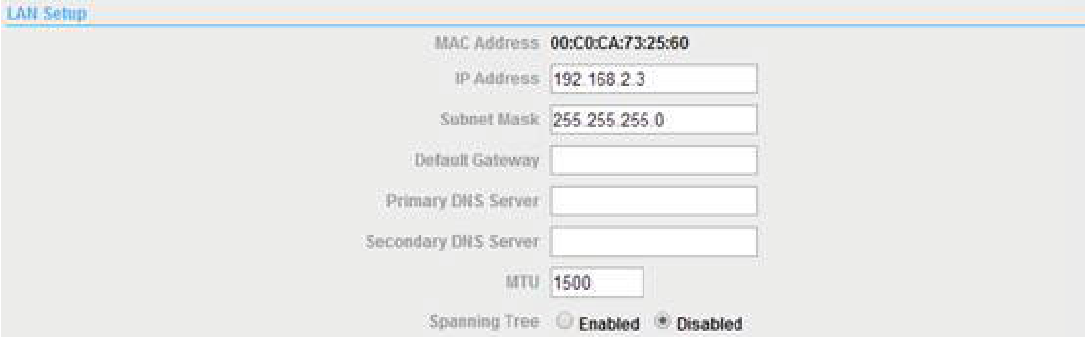
1. Configure EKI-6310GN as "AP Bridge" mode in "Advanced" ' "Operation Mode" page.



Operation Mode Configuration

Operation Mode: AP Bridge ▾

2. Configure Ethernet IP Address for your LAN network in "Advanced" ' "Network Setting" ' "LAN". We assume that all devices will locate in 192.168.2.xx network. You need to assign each AP with specific IP Address '192.168.2.3'.



LAN Setup

MAC Address: 00:C0:CA:73:25:60

IP Address: 192.168.2.3

Subnet Mask: 255.255.255.0

Default Gateway:

Primary DNS Server:

Secondary DNS Server:

MTU: 1500

Spanning Tree: ○ Enabled ● Disabled

3. Configure SSID and wireless information that your end device can find, such notebook, pad or cellular phone. You need to configure the information in the page of "Advanced" ' "Wireless Settings" ' "Basic" option. If you want EKI-6310GN to be able to have fast roaming function when it roams between EKI-6310GN APs, EKI-6310GN CAN NOT have encryption.

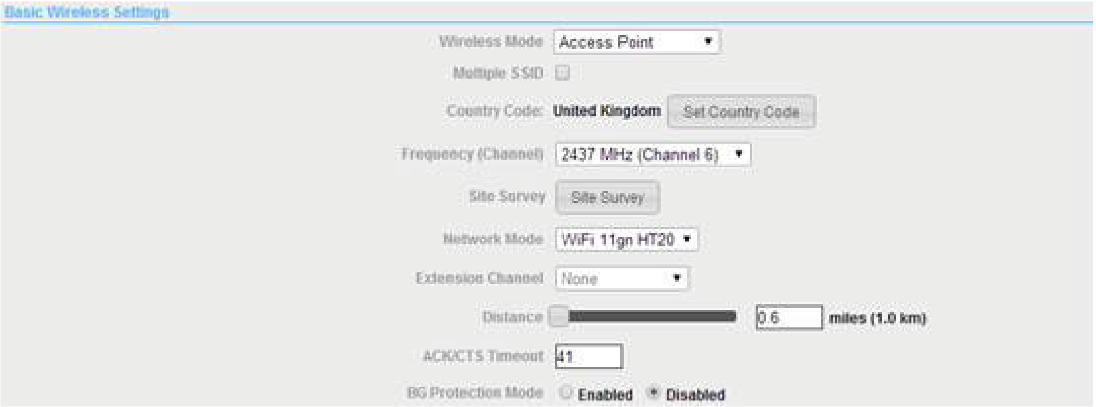
Wireless Mode: Access Point

Frequency (Channel): Channel 6

Network Mode: WiFi 11gn HT20 (It can support 802.11b / 802.11g / 802.11n end devices)

Network Name: EKI-6310GN (4 APs shall have same Network name SSID)

Encryption Settings: Disable



Basic Wireless Settings

Wireless Mode: Access Point ▾

Multiple SSID: □

Country Code: United Kingdom [Set Country Code]

Frequency (Channel): 2437 MHz (Channel 6) ▾

Site Survey: [Site Survey]

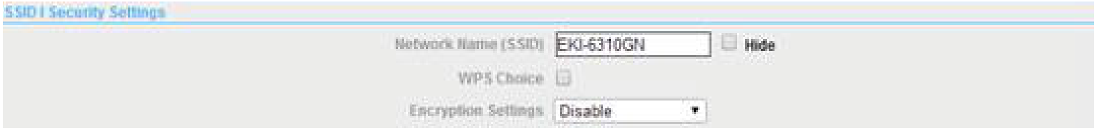
Network Mode: WiFi 11gn HT20 ▾

Extension Channel: None ▾

Distance: 0.6 miles (1.0 km)

ACK/CTS Timeout: 41

BG Protection Mode: ○ Enabled ● Disabled



SSID I Security Settings

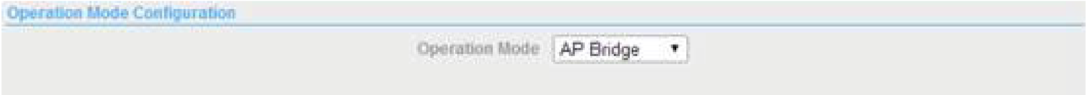
Network Name (SSID): EKI-6310GN □ Hide

WPS Choice: □

Encryption Settings: Disable ▾

Device: EKI-6310GN_2

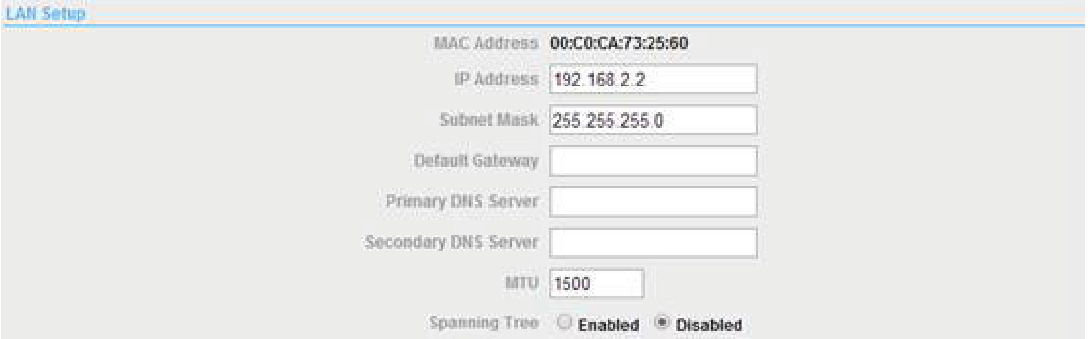
1. Configure EKI-6310GN as "AP Bridge" mode in "Advanced" ' "Operation Mode" page.



Operation Mode Configuration

Operation Mode: AP Bridge

2. Configure Ethernet IP Address for your LAN network in "Advanced" ' "Network Setting" ' "LAN". We assume that all devices will locate in 192.168.2.xx network. You need to assign each AP with specific IP Address '192.168.2.2'.



LAN Setup

MAC Address: 00:C0:CA:73:25:60
IP Address: 192.168.2.2
Subnet Mask: 255.255.255.0
Default Gateway:
Primary DNS Server:
Secondary DNS Server:
MTU: 1500
Spanning Tree: ○ Enabled ● Disabled

3. Configure SSID and wireless information that your end device can find, such notebook, pad or cellular phone. You need to configure the information in the page of "Advanced" ' "Wireless Settings" ' "Basic" option. If you want EKI-6310GN to be able to have fast roaming function when it roams between EKI-6310GN APs, EKI-6310GN CAN NOT have encryption.

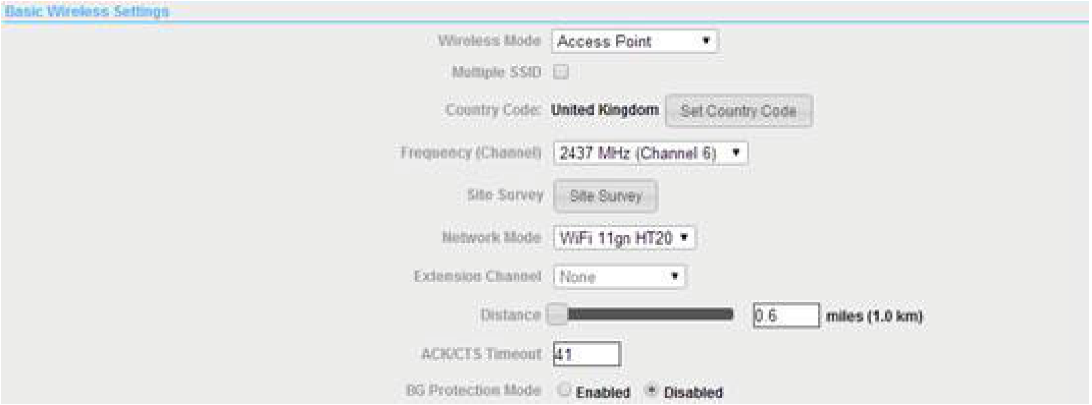
   Wireless Mode: Access Point

   Frequency (Channel): Channel 6

   Network Mode: WiFi 11gn HT20 (It can support 802.11b / 802.11g / 802.11n end devices)

   Network Name: EKI-6310GN (4 APs shall have same Network name SSID)

   Encryption Settings: Disable

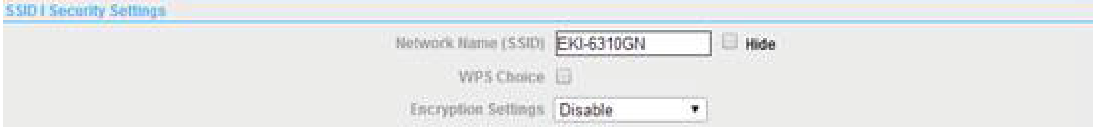


Basic Wireless Settings

Wireless Mode: Access Point
Multiple SSID: □
Country Code: United Kingdom

Frequency (Channel): 2437 MHz (Channel 6)
Site Survey

Network Mode: WiFi 11gn HT20
Extension Channel: None
Distance: 0.6 miles (1.0 km)
ACK/CTS Timeout: 41
BG Protection Mode: ○ Enabled ● Disabled

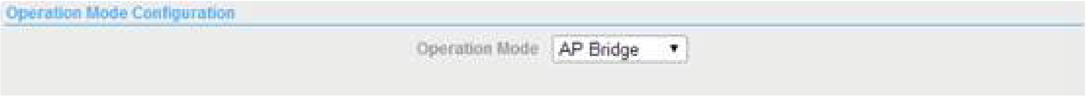


SSID I Security Settings

Network Name (SSID): EKI-6310GN □ Hide
WPS Choice: □
Encryption Settings: Disable

Device: EKI-6310GN_4

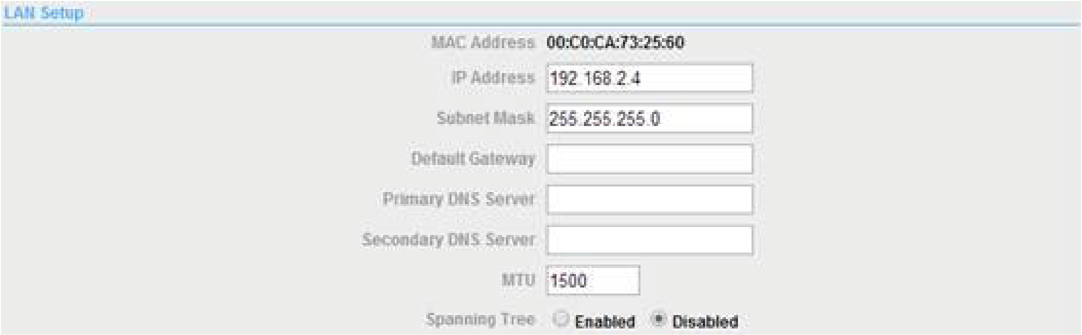
1. Configure EKI-6310GN as "AP Bridge" mode in "Advanced" ' "Operation Mode" page.



Operation Mode Configuration

Operation Mode: AP Bridge ▾

2. Configure Ethernet IP Address for your LAN network in "Advanced" ' "Network Setting" ' "LAN". We assume that all devices will locate in 192.168.2.xx network. You need to assign each AP with specific IP Address '192.168.2.4'.



LAN Setup

MAC Address: 00:C0:CA:73:25:60
IP Address: 192.168.2.4
Subnet Mask: 255.255.255.0
Default Gateway:
Primary DNS Server:
Secondary DNS Server:
MTU: 1500
Spanning Tree: ○ Enabled ● Disabled

3. Configure SSID and wireless information that your end device can find, such notebook, pad or cellular phone. You need to configure the information in the page of "Advanced" ' "Wireless Settings" ' "Basic" option. If you want EKI-6310GN to be able to have fast roaming function when it roams between EKI-6310GN APs, EKI-6310GN CAN NOT have encryption.

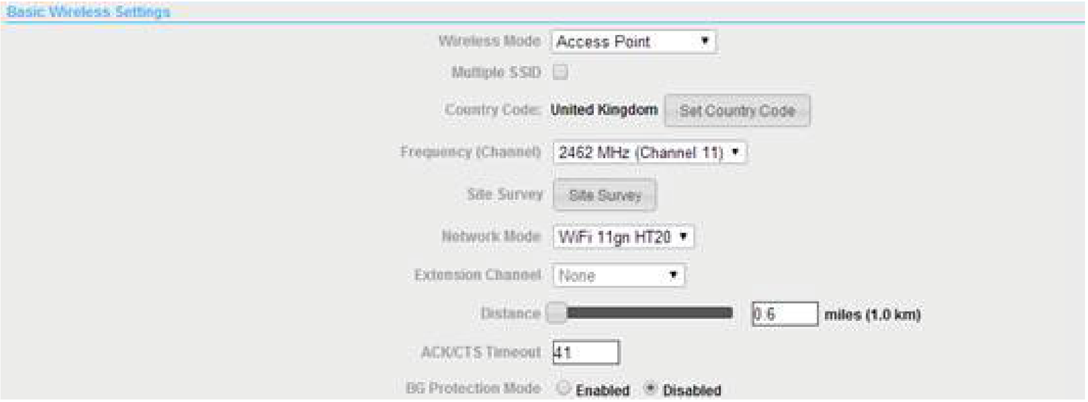
   Wireless Mode: Access Point

   Frequency (Channel): Channel 11

   Network Mode: WiFi 11gn HT20 (It can support 802.11b / 802.11g / 802.11n end devices)

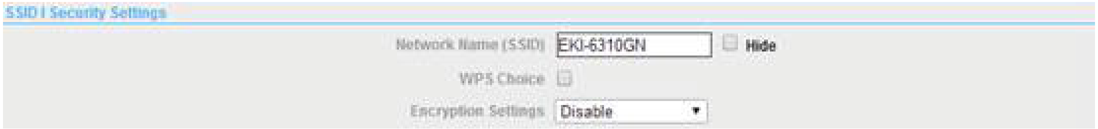
   Network Name: EKI-6310GN (4 APs shall have same Network name SSID)

   Encryption Settings: Disable



Basic Wireless Settings

Wireless Mode: Access Point ▾
Multiple SSID: □
Country Code: United Kingdom [Set Country Code]
Frequency (Channel): 2462 MHz (Channel 11) ▾
Site Survey: [Site Survey]
Network Mode: WiFi 11gn HT20 ▾
Extension Channel: None ▾
Distance: 0.6 miles (1.0 km)
ACK/CTS Timeout: 41
BG Protection Mode: ○ Enabled ● Disabled

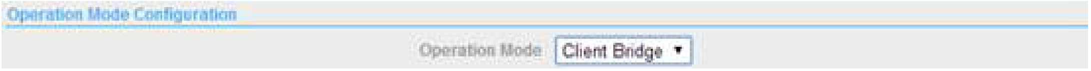


SSID I Security Settings

Network Name (SSID): EKI-6310GN □ Hide
WPS Choice: □
Encryption Settings: Disable ▾

Device: EKI-6310GN_5

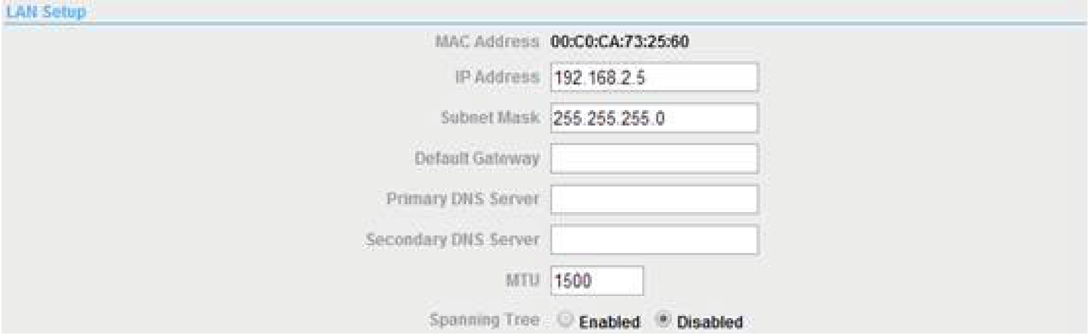
1. Configure EKI-6310GN as "Client Bridge" mode in "Advanced" ' "Operation Mode" page.



Operation Mode Configuration

Operation Mode: Client Bridge ▾

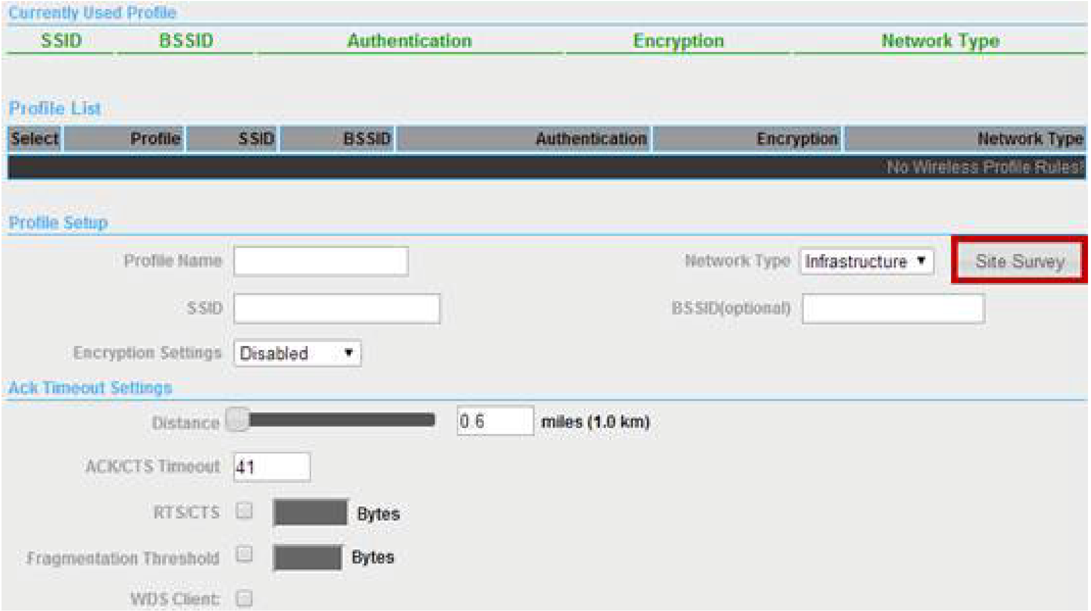
2. Configure Ethernet IP Address '192.168.2.5' for your LAN network in "Advanced" ' "Network Setting" ' "LAN".



LAN Setup

MAC Address	00:C0:CA:73:25:60
IP Address	192.168.2.5
Subnet Mask	255.255.255.0
Default Gateway	
Primary DNS Server	
Secondary DNS Server	
MTU	1500
Spanning Tree	○ Enabled ● Disabled

3. Configure client profile to connect with Access Point in "Advanced" ' "Wireless settings" ' "Profile Settings". You can do the Site Survey to find the SSID of matched Access Point.



Currently Used Profile

SSID	BSSID	Authentication	Encryption	Network Type

Profile List

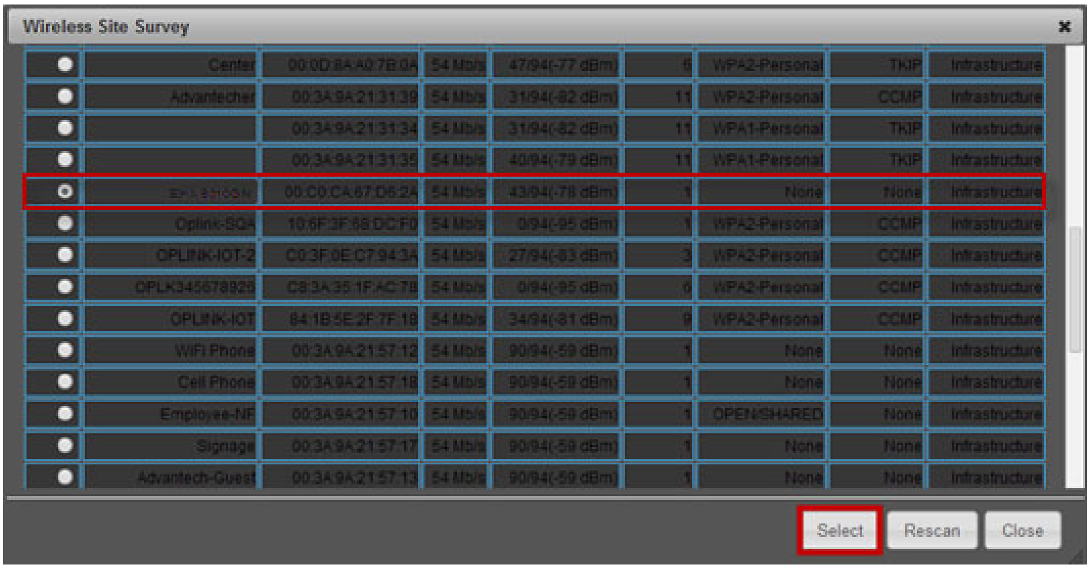
Select	Profile	SSID	BSSID	Authentication	Encryption	Network Type
No Wireless Profile Rules!						

Profile Setup

Profile Name		Network Type	Infrastructure ▾
SSID		BSSID(optional)	
Encryption Settings	Disabled ▾		

Ack Timeout Settings

Distance	0.6 miles (1.0 km)
ACK/CTS Timeout	41
RTS/CTS	□ Bytes
Fragmentation Threshold	□ Bytes
WDS Client	□



Wireless Site Survey

○	Center	00:0D:8A:A0:7B:0A	54 Mb/s	47/94(-77 dBm)	6	WPA2-Personal	TKIP	Infrastructure
○	Advantecher	00:3A:9A:21:31:39	54 Mb/s	31/94(-82 dBm)	11	WPA2-Personal	CCMP	Infrastructure
○		00:3A:9A:21:31:34	54 Mb/s	31/94(-82 dBm)	11	WPA1-Personal	TKIP	Infrastructure
○		00:3A:9A:21:31:35	54 Mb/s	40/94(-79 dBm)	11	WPA1-Personal	TKIP	Infrastructure
●	EKI-6310GN	00:C0:CA:67:D6:2A	54 Mb/s	43/94(-78 dBm)	1	None	None	Infrastructure
○	Oplink-SQA	10:6F:3F:68:DC:F0	54 Mb/s	0/94(-95 dBm)	1	WPA2-Personal	CCMP	Infrastructure
○	OPLINK-IOT-2	C0:3F:0E:C7:94:3A	54 Mb/s	27/94(-83 dBm)	3	WPA2-Personal	CCMP	Infrastructure
○	OPLK345678926	C8:3A:35:1F:AC:78	54 Mb/s	0/94(-95 dBm)	6	WPA2-Personal	CCMP	Infrastructure
○	OPLINK-IOT	84:1B:5E:2F:7F:18	54 Mb/s	34/94(-81 dBm)	9	WPA2-Personal	CCMP	Infrastructure
○	WiFi Phone	00:3A:9A:21:57:12	54 Mb/s	90/94(-59 dBm)	1	None	None	Infrastructure
○	Cell Phone	00:3A:9A:21:57:18	54 Mb/s	90/94(-59 dBm)	1	None	None	Infrastructure
○	Employee-NF	00:3A:9A:21:57:10	54 Mb/s	90/94(-59 dBm)	1	OPEN/SHARED	None	Infrastructure
○	Signage	00:3A:9A:21:57:17	54 Mb/s	90/94(-59 dBm)	1	None	None	Infrastructure
○	Advantech-Guest	00:3A:9A:21:57:13	54 Mb/s	90/94(-59 dBm)	1	None	None	Infrastructure

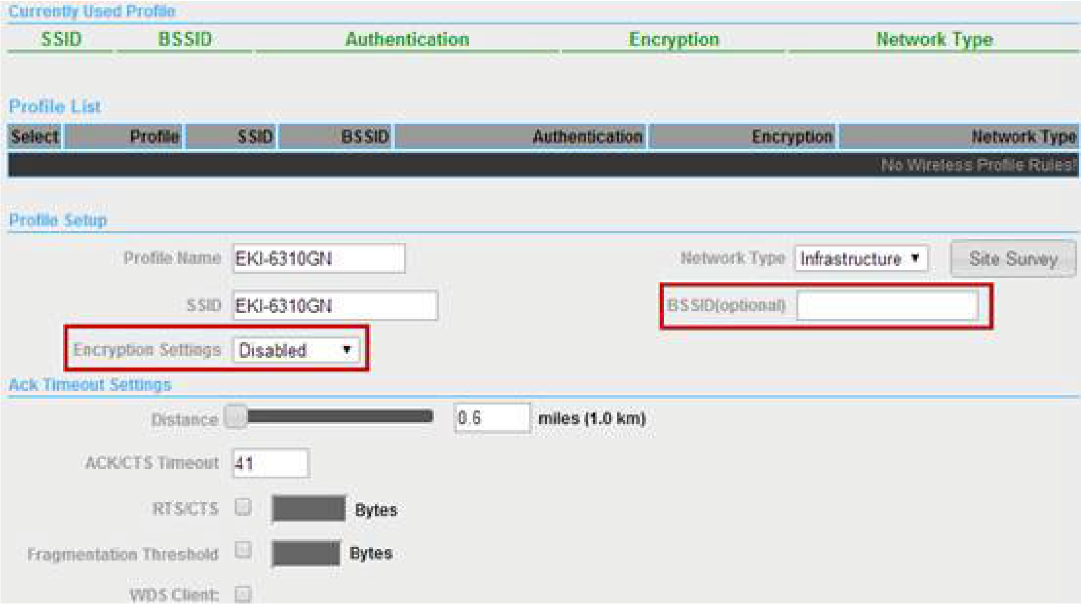
4. Enter the encryption information.

   Profile Name: EKI-6310GN (EKI-6310GN will fill-in the profile name same as SSID when you select access point through site survey)

   SSID: EKI-6310GN (EKI-6310GN will fill-in the SSID when you select access point through site survey)

   BSSID: Please keep this field as EMPTY. Once you enter the BSSID, it will only connect to specific Access Point. It won't roam between those APs, even those APs have same SSID and encryption setting.

   Encryption Settings: None



Currently Used Profile

SSID	BSSID	Authentication	Encryption	Network Type

Profile List

Select	Profile	SSID	BSSID	Authentication	Encryption	Network Type
						No Wireless Profile Rules!

Profile Setup

Profile Name: EKI-6310GN

SSID: EKI-6310GN

Encryption Settings: Disabled

Network Type: Infrastructure

BSSID(optional):

Ack Timeout Settings

Distance: 0.6 miles (1.0 km)

ACK/CTS Timeout: 41

RTS/CTS □ Bytes

Fragmentation Threshold □ Bytes

WDS Client: □

ADVANTECH

Enabling an Intelligent Planet

www.advantech.com