EKI-6311GN

IEEE 802.11 b/g/n Wireless
Access Point/Client Bridge

User Manual

Copyright

Acknowledgements

Product Warranty (2 years)

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

Federal Communication Commission Interference Statement

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

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

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

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

FCC Radiation Exposure Statement:

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

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

Technical Support and Assistance

Step 1. Visit the Advantech web site at **www.advantech.com/support** where you can find the latest information about the product.

Step 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

Safety Instructions

1. Read these safety instructions carefully.
2. Keep this User's 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 over voltage.
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:
    a. The power cord or plug is damaged.
    b. Liquid has penetrated into the equipment.
    c. The equipment has been exposed to moisture.
    d. The equipment does not work well, or you cannot get it to work according to the user's manual.
    e. The equipment has been dropped and damaged.
    f. The equipment has obvious signs of breakage.

15. DO NOT LEAVE THIS EQUIPMENT IN AN ENVIRONMENT WHERE THE STORAGE TEMPERATURE MAY GO BELOW -40℃ (-40℉) OR ABOVE 85℃ (185℉). THIS COULD DAMAGE THE EQUIPMENT. THE EQUIPMENT SHOULD BE IN A CONTROLLED ENVIRONMENT.

Safety Precaution - Static Electricity

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

1. 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.
2. 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.

Contents

CHAPTER 1

Overview

Chapter 1 Overview

1.1 Introduction

EKI-6311GN is a feature rich wireless AP/ CPE which provides a reliable wireless connectivity for industrial environments. The PoE injector enhances flexibility in deployment of this AP/ CPE even where the DC power supply is hard to fulfill. As an 802.11n compliant device, EKI-6311GN provides 3 times higher data rates than legacy 802.11g devices. With the support of STP, WMM and IGMP snooping protocols, EKI-6311GN effectively improves the reliability of wireless connectivity, especially in applications that need high reliability and high throughput data transmission. To secure wireless connections, EKI-6311GN 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 Power-through-Ethernet which is supplied with 12V.
- IP55 waterproof certification
- Four operating modes including AP, Wireless Client, WDS and 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
- Embedded 8dBi directional antenna with external N-type connector for optional antenna
- Support distances up to 5Km
- Spanning Tree and IGMP snooping protocol support

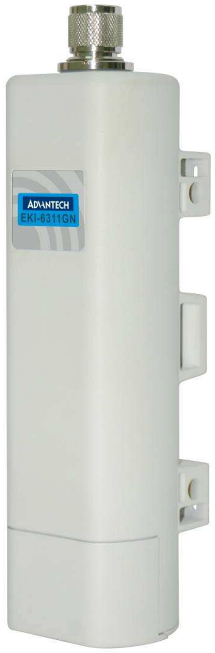


Figure 1 EKI-6311GN

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
  Passive 12V PoE, max. Distance: 20 meters
- **Certifications**
  US FCC Part 15 Class B & C & E
  Europe ETSI 300 328, ETSI 301 489-1&17
  EN 60950 compliant and CE Mark
- **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** DC 12Volt / 1.0A; AC Adapter 100V~240V
- **Dimensions (L x W x H)** 228 x 64 x 61 mm
- **Weight** 500g

Interface Operation Modes

- Access Point (AP)
- Customer Premise Equipment (CPE)

Antenna

- Antenna Configuration 1x1 (1 Tx, 1 Rx)
- Default embedded 8dBi directional antenna (Vertical-Polarity)
- Reserve N-type Connector (Plug) *Switchable by software
- Equipped N-to-RSMA adaptor and 5dBi dipole antenna for indoor AP application.

Other Features

- Telnet, FTP, SNMP, Password Changes, Firmware updates, Configuration Files
- Radio on/off, WMM/Regatta Mode, Output Power Control, Fragmentation Length, Beacon Interval
- RTS/CTS threshold, DTIM Interval

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/ gn** 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 Sensitivity** -93dBm @ 1Mbps; -88dBm @ 11Mbps
- **802.11g Sensitivity** -89dBm @ 6Mbps; -73dBm @ 54Mbps
- **802.11n HT20** -88dBm @ MCS0; -70dBm @ MCS7
- **802.11n HT40** -84dBm @ MCS0; -67dBm @ MCS7

1.4 Packing List

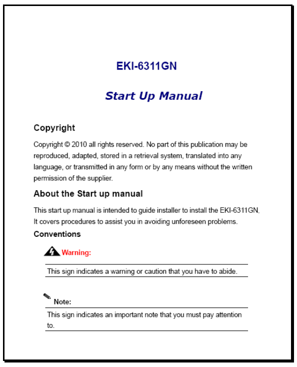
The product package you have received should contain the following items. If any of them are not included or damaged, please contact your local vendor for support.

EKI-6311GN	×1
Pole Mounting Ring	×1
Power Cord & PoE Injector	×1
Start up manual	×1
User’s manual CD	×1
N-to-RSMA adaptor	×1
RSMA Omni antenna	×1

Pole Mounting Ring

Power Cord & PoE Injector

Start up manual & User's manual CD



EKI-6311GN

Start Up Manual

Copyright

Copyright © 2010 all rights reserved. No part of this publication may be reproduced, adapted, stored in a retrieval system, translated into any language, or transmitted in any form or by any means without the written permission of the supplier.

About the Start up manual

This start up manual is intended to guide installer to install the EKI-6311GN. It covers procedures to assist you in avoiding unforeseen problems.

Conventions

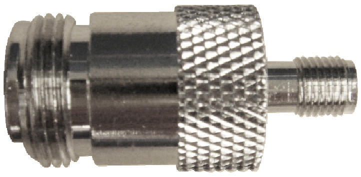
Warning:

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

Note:

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

N-to-RSMA adaptor



RSMA Omni Antenna

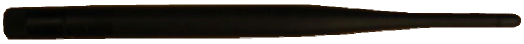


Figure 2 Accessories

Warning:

- Users MUST use the "Power cord & PoE Injector" shipped in the box with the EKI-6311GN. Use of other options will cause damage to the EKI-6311GN.

1.5 Safety Precaution

Attention *IF DC voltage is supplied by other power injector, please check the voltage and use a protection device on the power supply input.*

CHAPTER 2

Installation

Chapter 2 Installation

This chapter describes safety precautions and product information you have to know and check before installing EKI-6311GN.

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. If you are installing EKI-6311GN 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-6311GN, 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-6311GN 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-6311GN; otherwise, a random lightening could easily cause fatal damage to EKI-6311GN.

   EMD (Lightning) DAMAGE IS NOT COVERED UNDER WARRNTY.

2. **Users MUST use the "Power cord & PoE Injector" shipped in the box with the EKI-6311GN. Use of other options will cause damage to the EKI-6311GN.**
3. Users MUST power off the EKI-6311GN 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-6311GN; otherwise, damage might be caused to the EKI-6311GN itself.

2.3 Hardware Installation

Connect up

1. The bottom of the EKI-6311GN is a movable cover. Grab the cover and pull it back harder to take it out as the figure shown below.

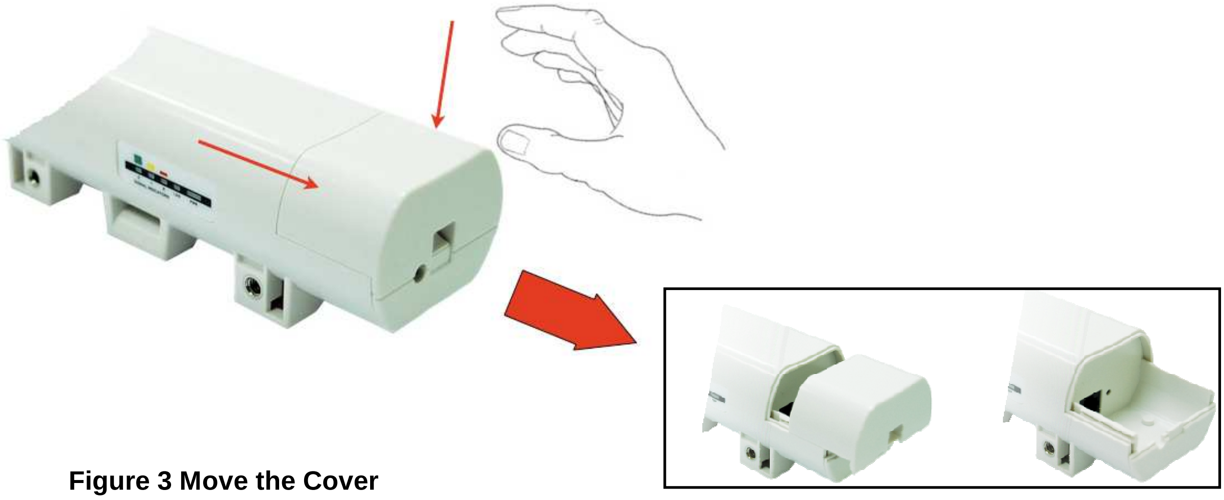


Figure 3 Move the Cover

2. Plug a standard Ethernet cable into the RJ45 port.

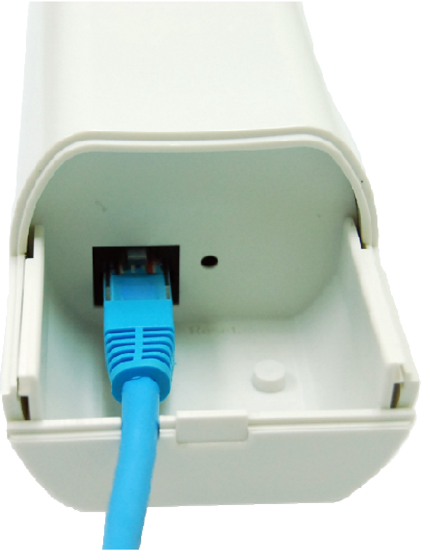


Figure 4 Cable Connection

3. Slide the cover back to seal the bottom of the EKI-6311GN.

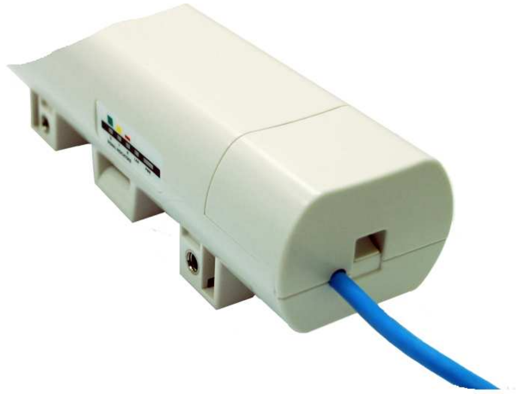


Figure 5 Seal the Bottom

4. Plug the power cord into the DC port of the PoE injector as the following right picture shows.

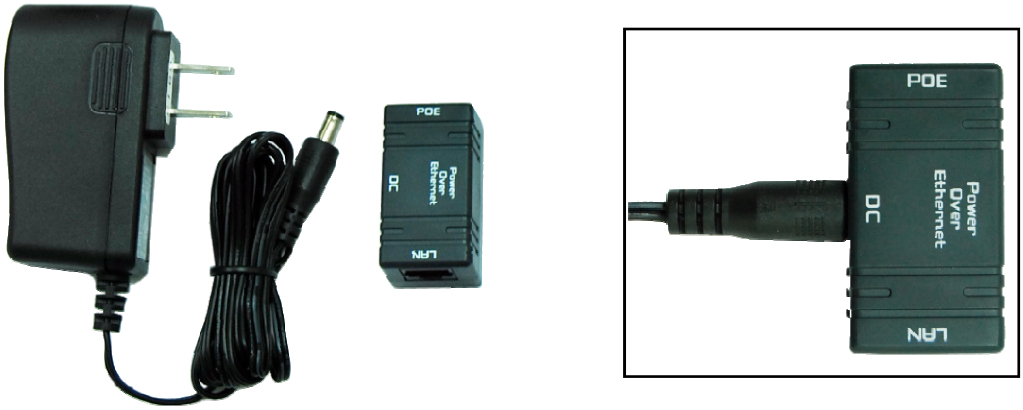


Figure 6 Connect to PoE Injector

5. Plug the other side of the Ethernet cable as shown in Step 3 into the PoE port of the PoE injector and get the complete set ready.

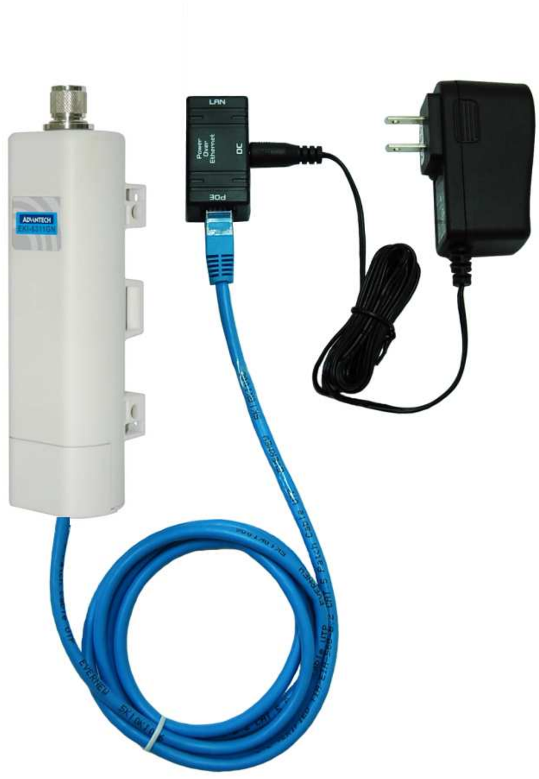


Figure 7 Complete Set

2.4 Pole Mounting

Pole Mounting

1. Turn the EKI-6311GN 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-6311GN as the following right picture shows.

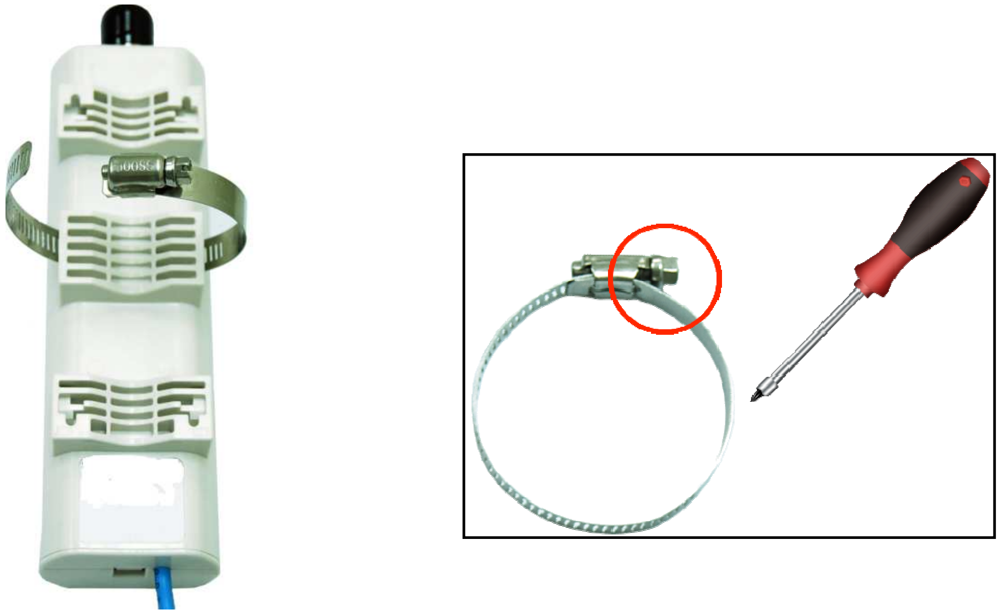


Figure 8 Pole Mounting – Step 1

2. Mount EKI-6311GN steadily to the pole by locking the pole mounting ring tightly.

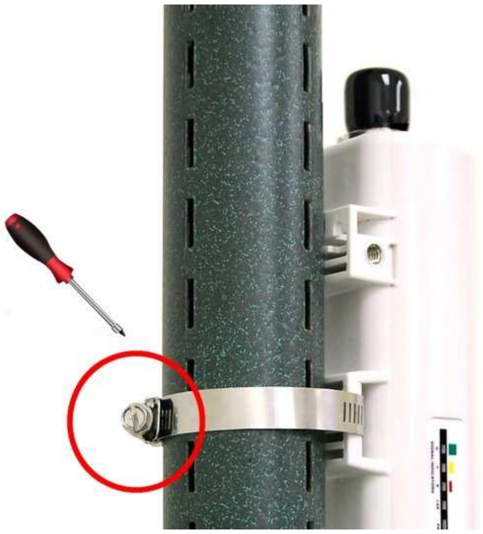


Figure 9 Pole Mounting – Step 2

3. Now you have completed the hardware installation of EKI-6311GN.

Using the External Antenna

If you prefer to use the external antenna for your application instead of the built-in directional antenna, please follow the steps below.

- Grab the black rubber on the top of EKI-6311GN, and slightly pull it up. The metal N-type connector will appear.

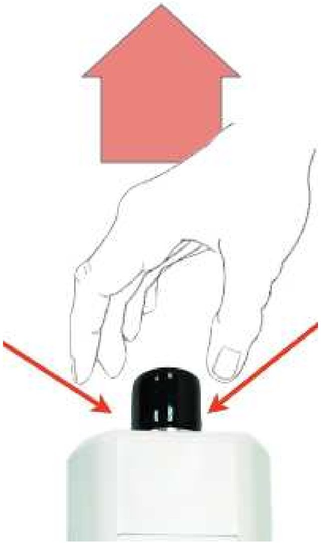


Figure 10 Move the Rubber

- Connect your antenna with the N-type to RSMA adaptor on the top of EKI-6311GN. The following picture shows the full set of EKI-6311GN:

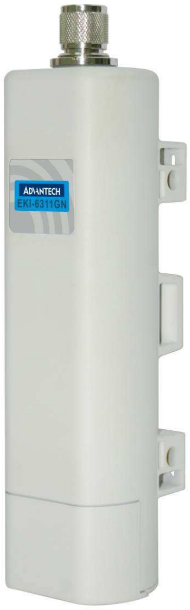


Figure 11 Removed the Rubber

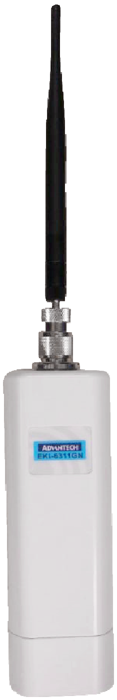


Figure 12 Full set with antenna

✎ **Note:**

- If you are going to use an external antenna on EKI-6311GN, get some cable in advance.
- Be aware of the force you use while connecting to the N-type connector, inappropriate force may damage the N-type connector!

⚠ **Warning:**

- Users MUST power off the EKI-6311GN 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-6311GN; otherwise, damage might be caused to the EKI-6311GN itself.

CHAPTER 3

Basic Settings

Chapter 3 Basic Settings

3.1 Factory Default Settings

We'll elaborate the EKI-6311GN factory default settings. You can re-acquire these parameters by default. If necessary, please refer to the "Restore Factory Default Settings".

Table 1 EKI-6311GN Factory Default Settings

Features		Factory Default Settings
Username		admin
Password		password
Wireless Device Name		apXXXXXX (X represents the last 6 digits of Ethernet MAC address)
Operating Mode		AP
Data Rate		Auto
LAN	IP Address	192.168.1.1
	Subnet Mask	255.255.255.0
	Gateway	0.0.0.0
	Primary DNS Server	0.0.0.0
	Secondary DNS Server	0.0.0.0
Spanning Tree		Enable
802.11 Mode		802.11b/g/n
Channel Number		6
SSID		Wireless
Broadcast SSID		Enable
HT Protect		Disable
Data Rate		Auto
Output Power		Full
Channel Mode		20MHz
WMM		Enabled
RTS Threshold (byte)		2346
Fragmentation Length (byte)		2346
Beacon Interval		100
DTIM Interval		1
Space in Meter		0
Flow Control by AP		Disable
Security		Open System
Encryption		None
Wireless Separation		Disable
Access Control		Disable
SNMP	Enable/Disable	Enable
	Read Community Name	Public
	Write Community Name	Private
	IP Address	0.0.0.0

3.2 System Requirements

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

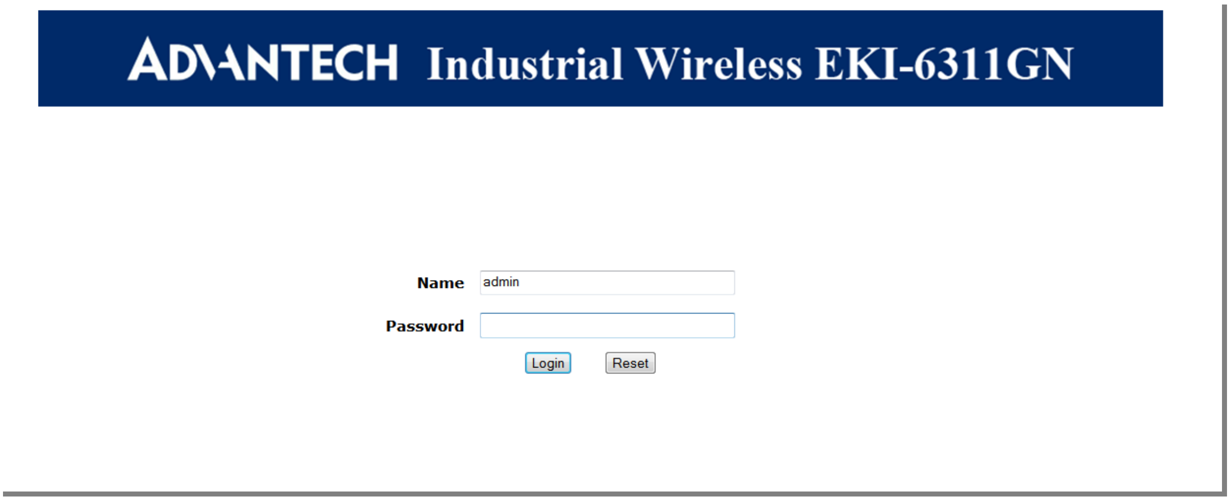
- A computer coupled with 10/ 100 Base-TX adapter;

- Configure the computer with a static IP address of 192.168.1.x, as the default IP address of EKI-6311GN is 192.168.1.1. (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

The EKI-6311GN provides you with user-friendly Web-based management tool.

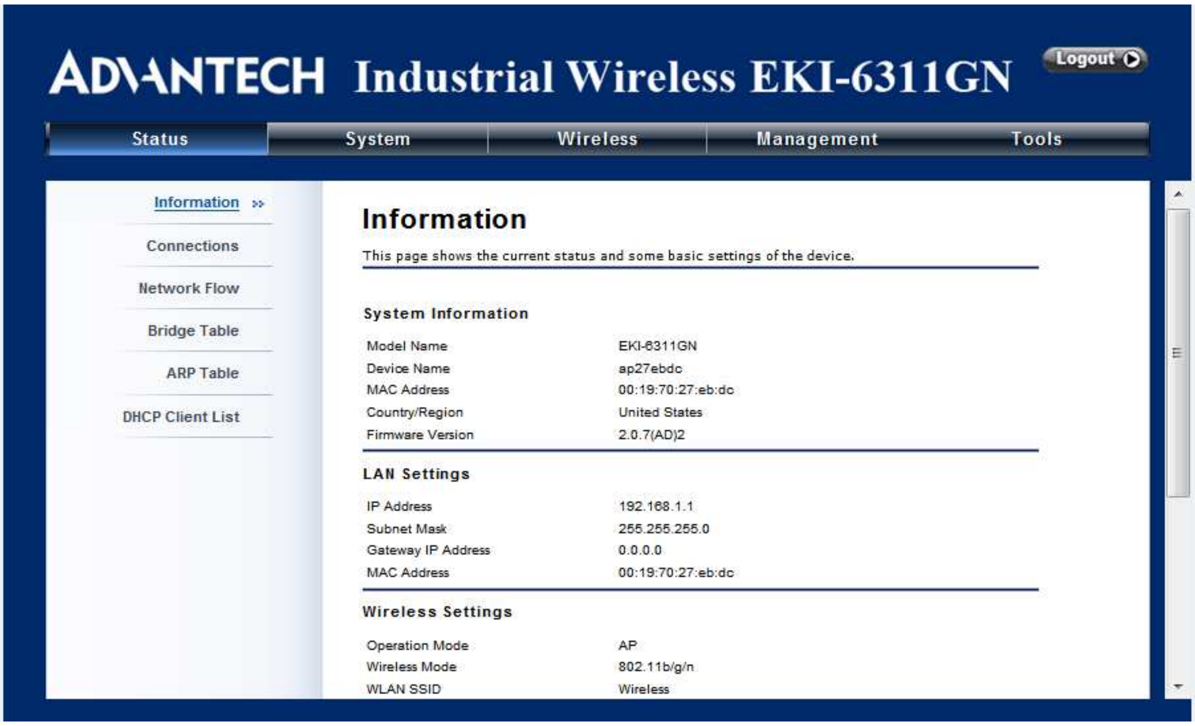
- Open Web browser and enter the IP address (Default: **192.168.1.1**) of EKI-6311GN into the address field. You will see the login page as below.



Name: admin

Figure 13 Login Page

- Enter the username (Default: **admin**) and password (Default: **password**) respectively and click “**Login**” to login the main page of EKI-6311GN. As you can see, this management interface provides five main options in the black bar above, which are Status, System, Wireless, Management and Tools.



Information

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

System Information

Model Name	EKI-6311GN
Device Name	ap27ebdc
MAC Address	00:19:70:27:eb:dc
Country/Region	United States
Firmware Version	2.0.7(AD)2

LAN Settings

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway IP Address	0.0.0.0
MAC Address	00:19:70:27:eb:dc

Wireless Settings

Operation Mode	AP
Wireless Mode	802.11b/g/n
WLAN SSID	Wireless

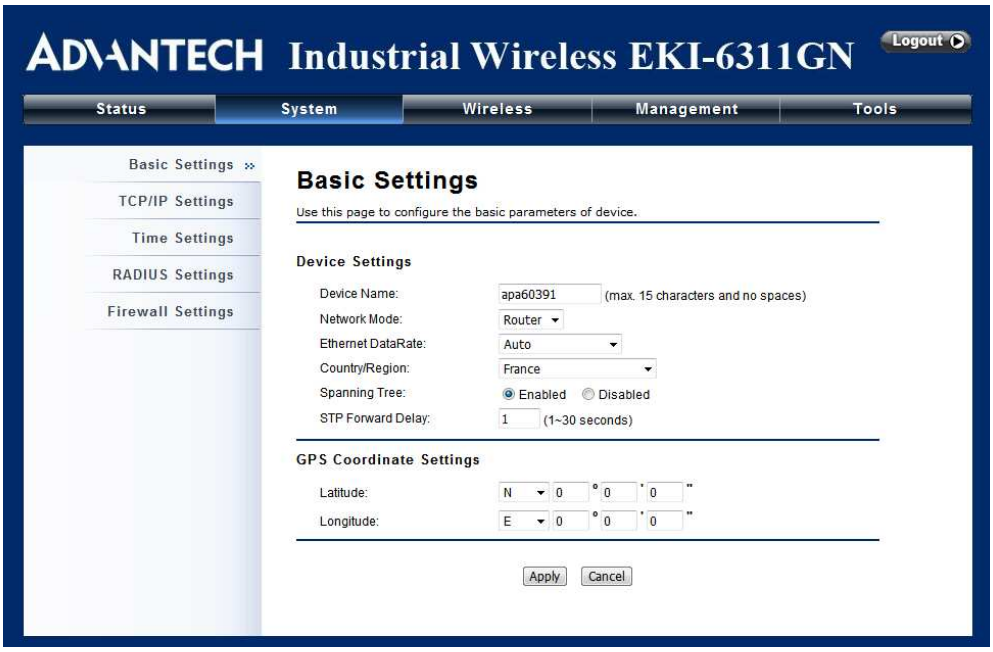
Figure 14 Main Page

Note:

- The username and password are case-sensitive, and the password should be no more than 19 characters!

3.4 Basic System Settings

For users who use the EKI-6311GN for the first time, it is recommended that you begin configuration from “**Basic Settings**” in “**System**” shown below:



Basic Settings

Use this page to configure the basic parameters of device.

Device Settings

Device Name:	apa60391 (max. 15 characters and no spaces)
Network Mode:	Router
Ethernet DataRate:	Auto
Country/Region:	France
Spanning Tree:	● Enabled ○ Disabled
STP Forward Delay:	1 (1~30 seconds)

GPS Coordinate Settings

Latitude:	N 0 ° 0 ' 0 "
Longitude:	E 0 ° 0 ' 0 "

Figure 15 Basic System Settings

- **Basic Settings**

Device Name: Specify the device name, which is composed of no more than 15 characters with (0-9), (A-Z), (a-z) or (-).

Network Mode: Specify the network mode, including Bridge and Router. It is easy to configure parameters in Bridge Mode; however, users must pay extra attention to the way they configure the device when it is set to Router Mode. For details, please refer to **TCP/IP Settings"**.

Ethernet Data Rate: Specify the transmission rate of data for Ethernet. Default is **Auto**.

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

Spanning Tree: Spanning Tree Protocol (STP) is a link management protocol for AP which provides path redundancy while preventing loops in a network. STP allows only one active path at a time between the access points but establish the redundant link as a backup if the initial link fails.

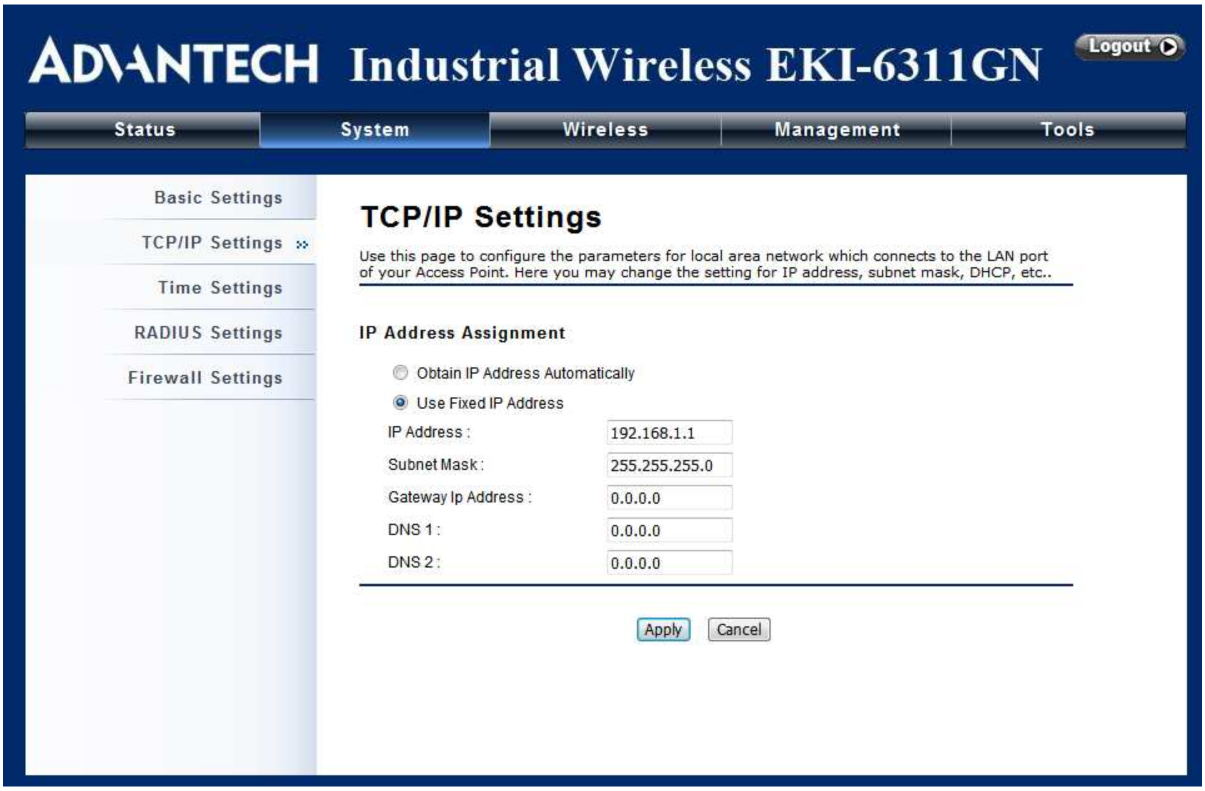
STP Forward Delay: STP Forward Delay is the time spent in detecting and learning network tree topology state before entering the forward state. Default time value is 1 sec.

GPS Coordinate Settings

The GPS Coordinate Setting helps you mark the latitude and longitude of EKI-6311GN. Just enter the coordinates and click the **Apply** button.

- **TCP/IP Settings**

Open "**TCP/IP Settings**" in "**System**" as below to configure the parameters for LAN which connects to the LAN port of the CPE. In this page, users may change the settings for IP Address, Subnet Mask, and DHCP Server.



TCP/IP Settings

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

IP Address Assignment

○ Obtain IP Address Automatically
● Use Fixed IP Address

IP Address : 192.168.1.1
Subnet Mask : 255.255.255.0
Gateway Ip Address : 0.0.0.0
DNS 1 : 0.0.0.0
DNS 2 : 0.0.0.0

Figure 16 IP Settings (Bridge)

Obtain IP Address Automatically: If a DHCP server exists in your network, you can check this option, thus the IEEE 802.11b/g/n Wireless Outdoor CPE is able to obtain IP settings automatically from that DHCP server.

Note:

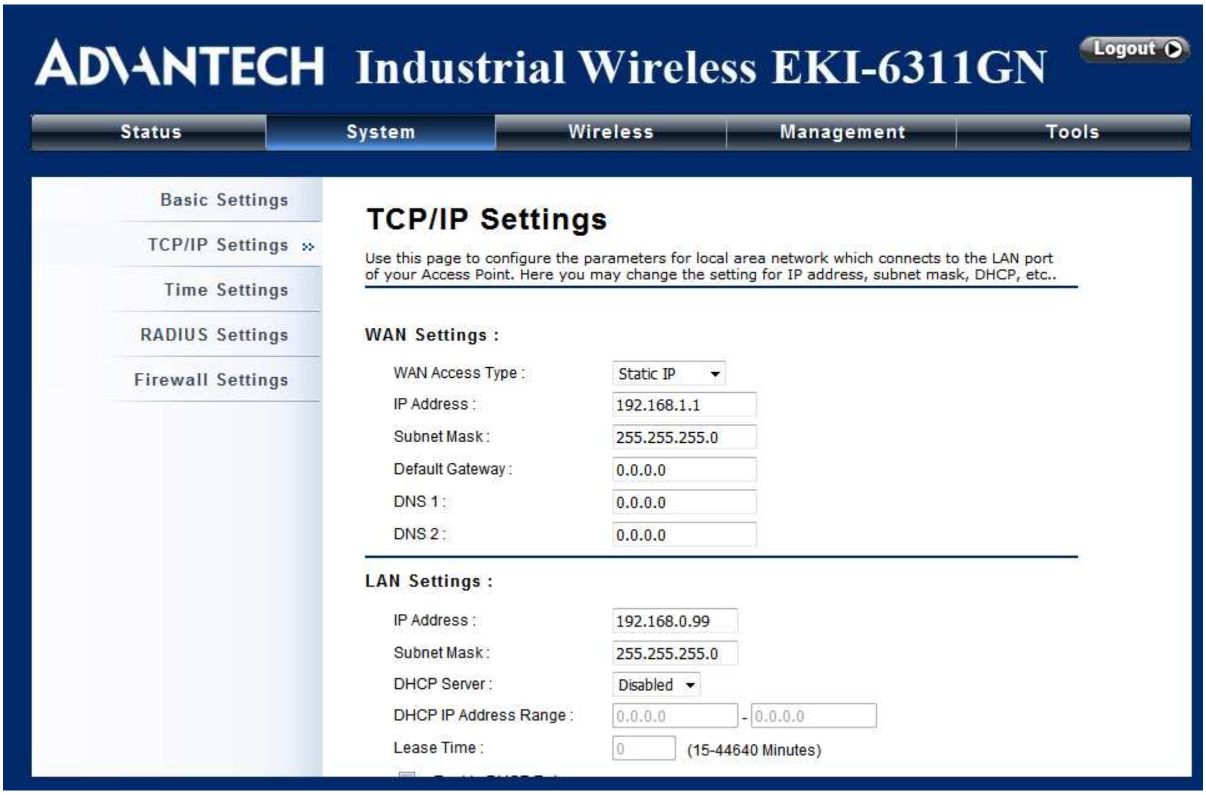
- When the IP address of the CPE is changed, the clients on the network often need to wait for a while or even reboot before they can access the new IP address. For an immediate access to the bridge, please flush the netbios cache on the client computer by running the “nbtstat –r” command before using the device name of the CPE to access its Web Management page.
- In case the IEEE 802.11b/g/n Wireless Outdoor CPE is unable to obtain an IP address from a valid DHCP server, it will fall back to default static IP address.

Use Fixed IP Address: Check this option. You have to specify a static IP address, subnet mask, default gateway and DNS server for the CPE manually. Make sure the specified IP address is unique on your network in order to prevent IP conflict.

If the IEEE 802.11b/g/n Wireless Outdoor CPE is configured as Router mode, you need to configure some additional TCP/IP parameters for accessing the Internet.

- **IP Settings (Router)**

This is available only under Router mode. Open “**IP Settings (Router)**” in “**System**” below to configure the parameters of EKI-6311GN for accessing the Internet.



TCP/IP Settings

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

WAN Settings :

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

LAN Settings :

IP Address : 192.168.0.99
Subnet Mask : 255.255.255.0
DHCP Server : Disabled
DHCP IP Address Range : 0.0.0.0 - 0.0.0.0
Lease Time : 0 (15-44640 Minutes)

Figure 17 IP Settings (Router)

WAN Settings: Specify the Internet access method to Static IP, DHCP or PPPoE. Users must enter WAN IP Address, Subnet Mask, Gateway settings provided by your ISPs.

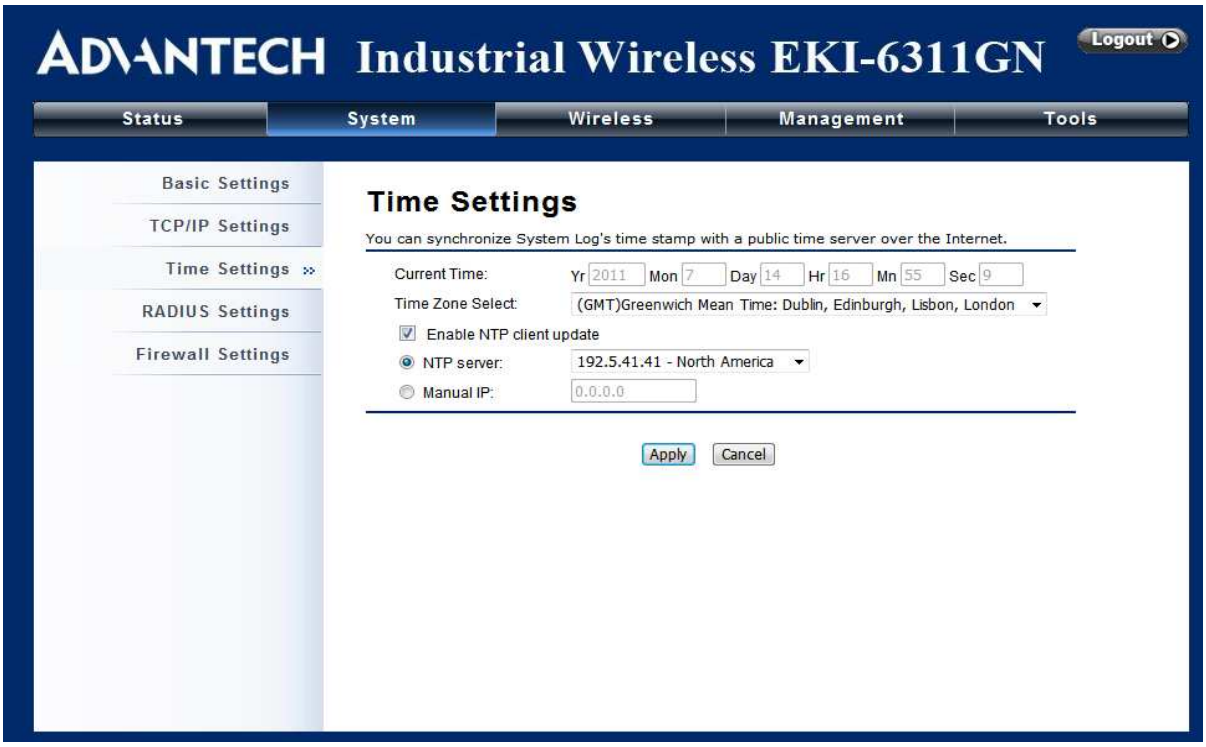
LAN Settings: When DHCP Server is disabled, users can specify IP address and subnet mask for the CPE manually. Make sure the specified IP address is unique on your network in order to prevent IP conflict. When DHCP Server is enabled, users may specify DHCP IP Address Range, DHCP Subnet Mask, DHCP Gateway and Lease Time (15-44640 minutes). A DHCP relay agents is used to forward DHCP requests and replies between clients and servers when they are not on the same physical subnet. To enable the DHCP relay agent, check the “**Enable DHCP Relay**” checkbox and enter the IP address of the DHCP server.

Warning:

- In AP mode, the IEEE 802.11b/g/n Wireless Outdoor CPE must establish connection with another wireless device before it is set to Router mode. To access the unit in Router mode via wired port, please type the WAN IP address to enter the web page for WAN is on wired port and LAN is on wireless port. Or, you can access device through the wireless device connected with the CPE.
- In wireless client mode, users can access the CPE via its wired port, for WAN is on wireless port and LAN is on wired port when device is set to Router mode.
- Bridge mode and AP Repeater mode are similar to AP mode when device is set to Router mode; WAN is on wired port and LAN is on wireless port. Thus users must also connect the CPE with another wireless device before it is set to Router mode and access the CPE via the connected wireless device.

Time Settings

Compliant with NTP, the IEEE 802.11b/g/n Wireless Outdoor CPE is capable of keeping its time in complete accord with the Internet time. Make configuration in “**Time Settings**” from “**System**”. To use this feature, check “**Enable NTP Client Update**” in advance.



Time Settings

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

Current Time: Yr 2011 Mon 7 Day 14 Hr 16 Mn 55 Sec 9

Time Zone Select: (GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

☑ Enable NTP client update

● NTP server: 192.5.41.41 - North America

○ Manual IP: 0.0.0.0

Figure 28 Time Settings

- **Current Time**

  Display the present time in Yr, Mon, Day, Hr, Min and Sec.

- **Time Zone Select**

  Select the time zone from the dropdown list.

- **NTP Server**

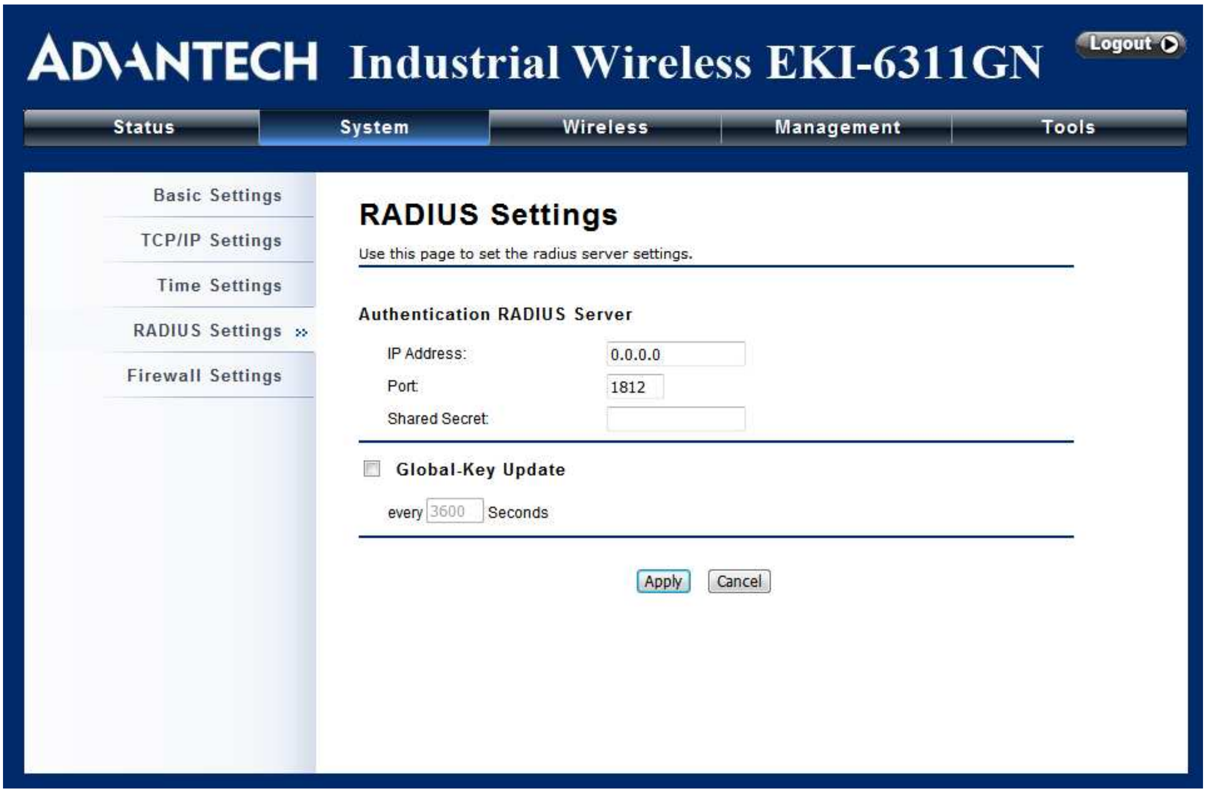
  Select the time server from the “**NTP Serve**r” dropdown list or manually input the IP address of available time server into “**Manual IP**”.

  Hit “**Apply**” to save settings.

3.5 RADIUS Settings

RADIUS (Remote Authentication Dial-In User Service) is a server for remote user authentication and accounting; playing a central role in the network in providing the capabilities of authenticating, authorizing, accounting, auditing, alarming and etc. It allows an organization to maintain user profiles in a central database that all remote servers can share.

Open “**RADIUS Settings**” in “**System**” to make RADIUS configuration.



RADIUS Settings

Use this page to set the radius server settings.

Authentication RADIUS Server

IP Address: 0.0.0.0

Port: 1812

Shared Secret:

□ Global-Key Update

every 3600 Seconds

Figure 39 RADIUS Settings

- **Authentication RADIUS Server**

  This is for RADIUS authentication. It can communicate with RADIUS through IP Address, Port and Shared Secret.

  IP Address: Enter the IP address of the Radius Server;

  Port: Enter the port number of the Radius Server;

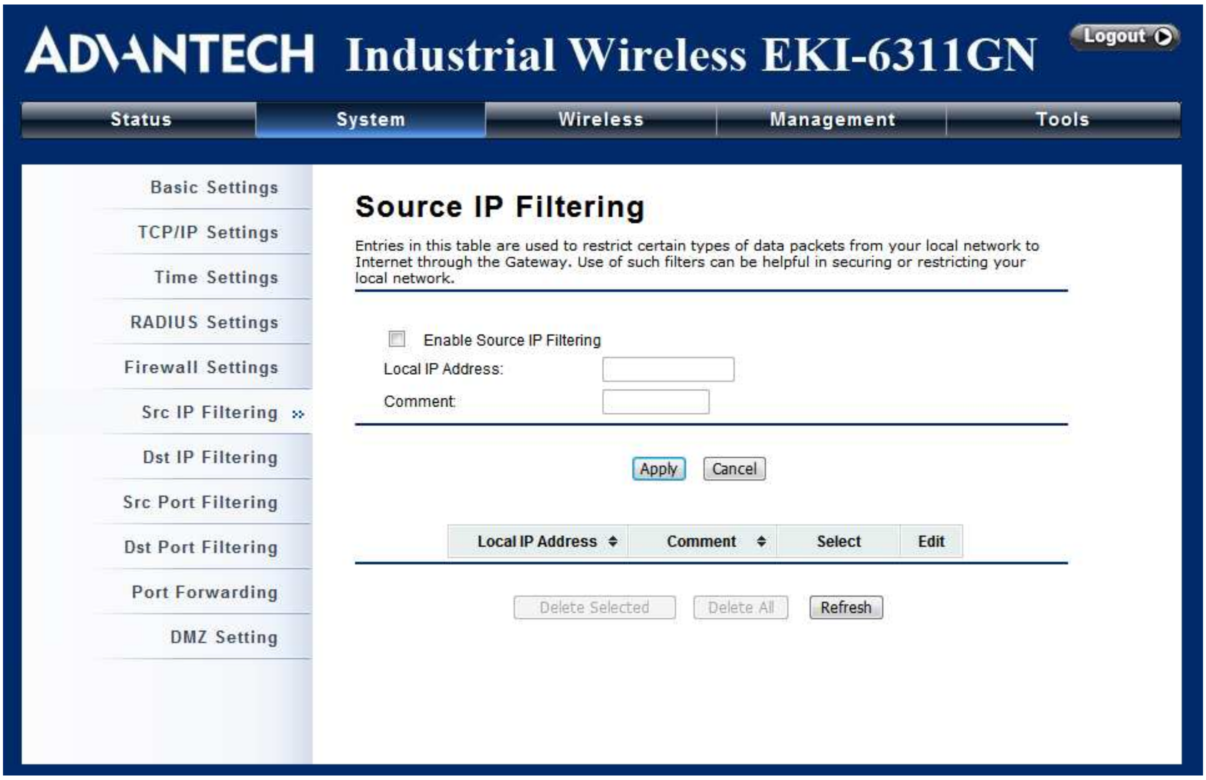
  Shared Secret: This secret, which is composed of no more than 31 characters, is shared by the EKI-6311GN and RADIUS during authentication.

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

3.6 Firewall Settings

The firewall is a system or group of systems that enforce an access control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an un-trusted network. EKI-6311GN has capabilities of Source IP Filtering, Destination IP Filtering, Source Port Filtering, Destination Port Filtering, Port Forwarding as well as DMZ. This is available only under Router Mode.

Source IP Filtering: The source IP filtering gives users the ability to restrict certain types of data packets from your local network to Internet through EKI-6311GN. Use of such filters can be helpful in securing or restricting your local network.



Source IP Filtering

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

□ Enable Source IP Filtering

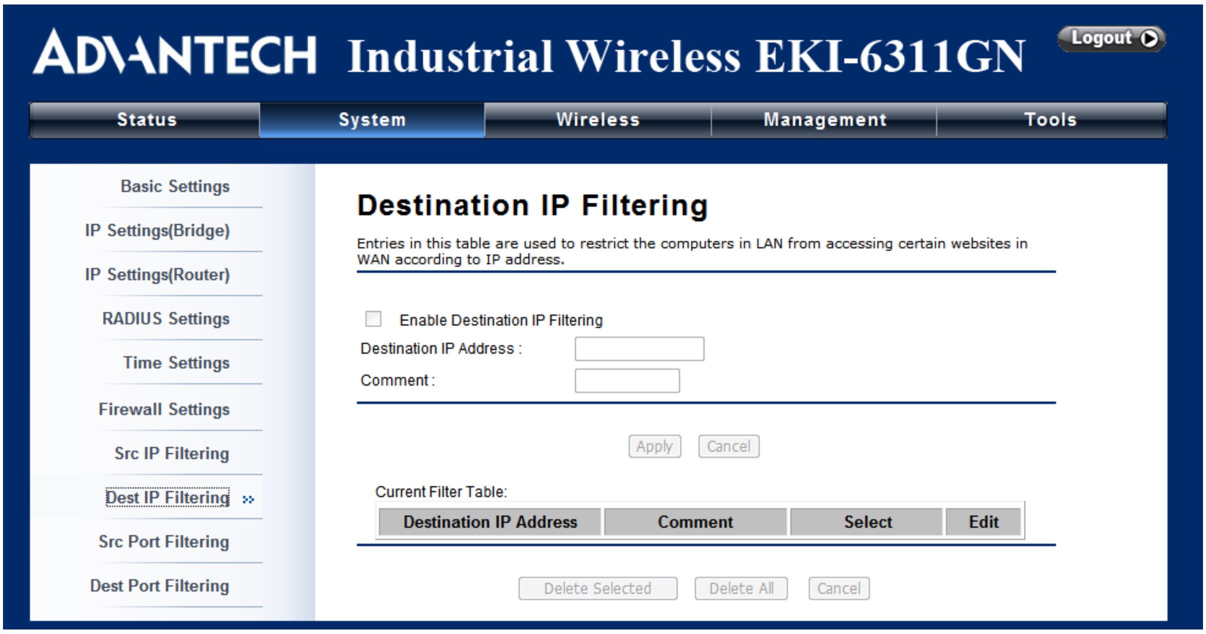
Local IP Address:

Comment:

Local IP Address	Comment	Select	Edit

Figure 20 Source IP Filtering

Destination IP Filtering: The destination IP filtering gives you the ability to restrict the computers in LAN from accessing certain websites in WAN according to specified IP addresses. Check the "**Enable Source IP Filtering**" checkbox and enter the IP address of the clients to be restricted. Hit **Apply** to make the setting take effect.



Destination IP Filtering

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

□ Enable Destination IP Filtering

Destination IP Address :

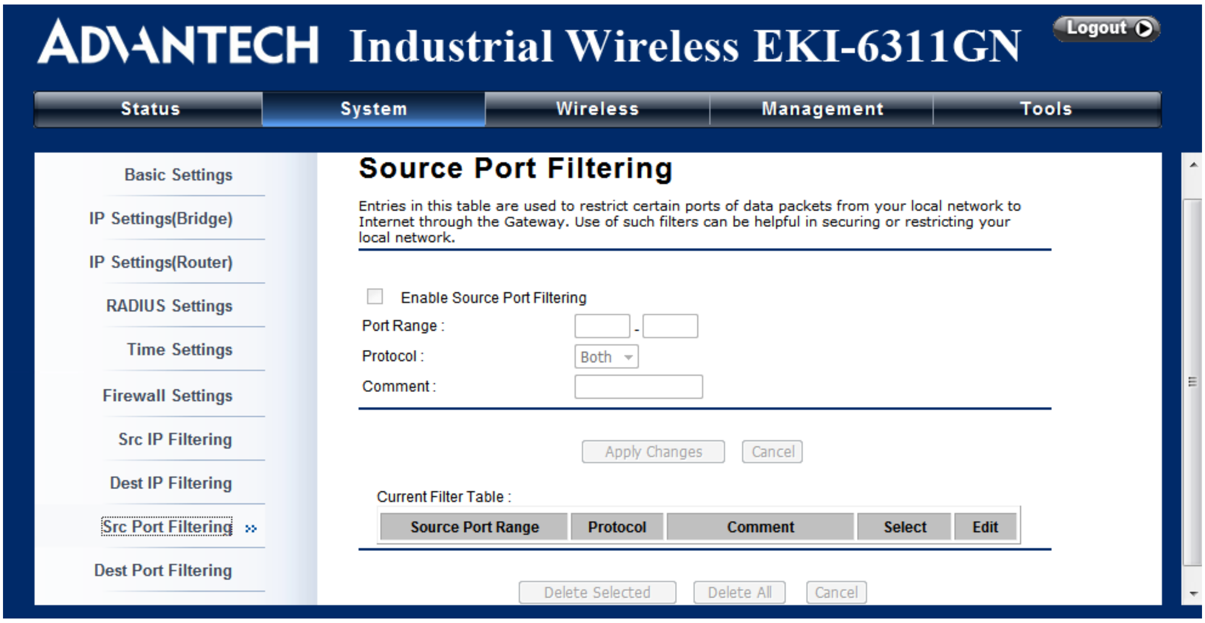
Comment :

Current Filter Table:

Destination IP Address	Comment	Select	Edit

Figure 21 Destination IP Filtering

Source Port Filtering: The source port filtering enable you to restrict certain ports of data packets from your local network to Internet through EKI-6311GN. Use of such filters can be helpful in securing or restricting your local network.



Source Port Filtering

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

□ Enable Source Port Filtering

Port Range : -

Protocol : Both

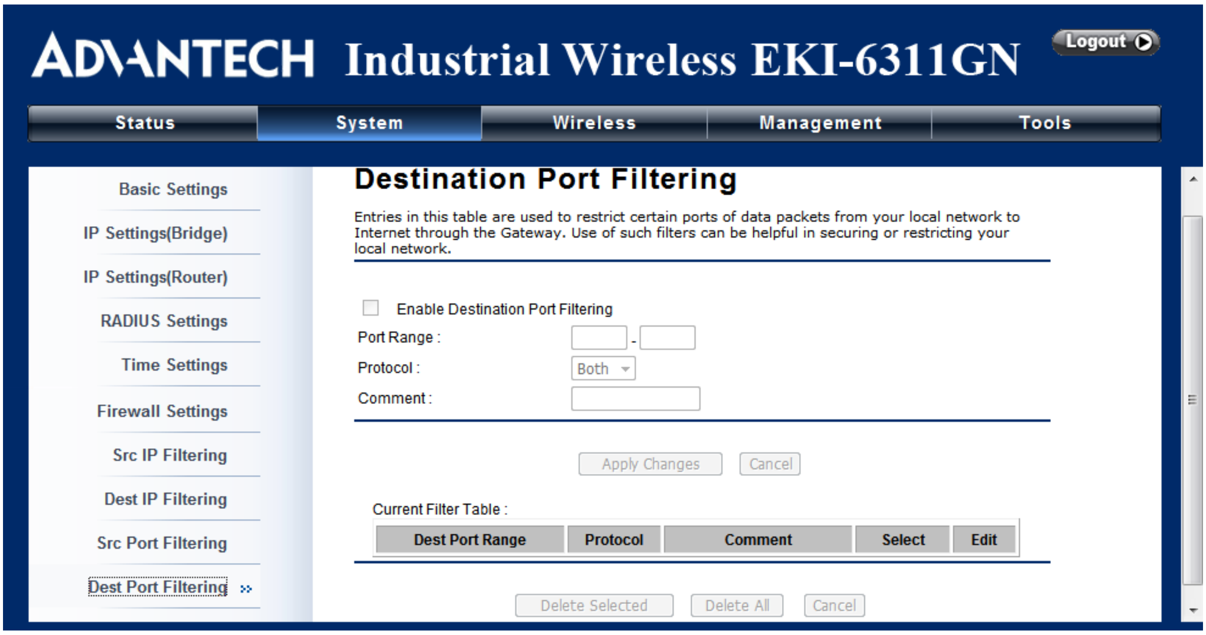
Comment :

Current Filter Table :

Source Port Range	Protocol	Comment	Select	Edit

Figure 22 Source Port Filtering

Destination Port Filtering: The destination port filtering enables you to restrict certain ports of data packets from your local network to Internet through EKI-6311GN. Use of such filters can be helpful in securing or restricting your local network.



Destination Port Filtering

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

☐ Enable Destination Port Filtering

Port Range : -

Protocol : Both

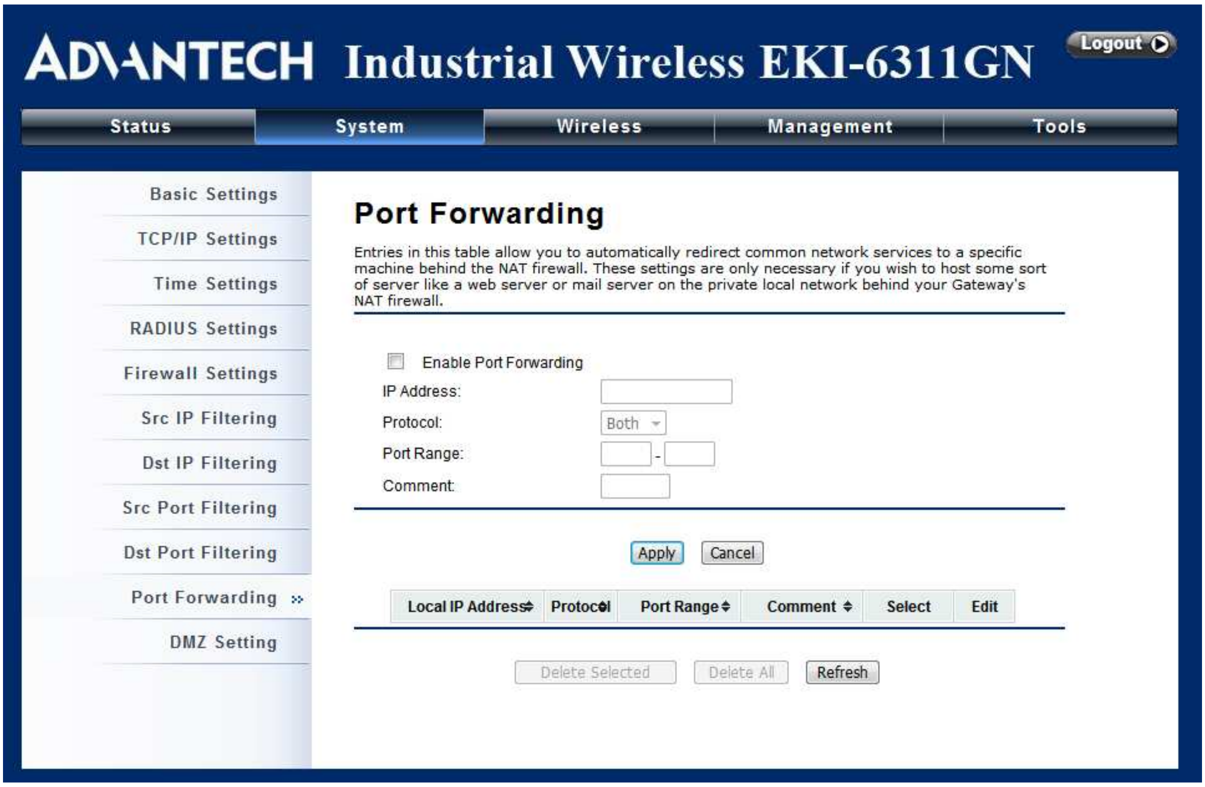
Comment :

Current Filter Table :

Dest Port Range	Protocol	Comment	Select	Edit

Figure 23 Destination Port Filtering

Port Forwarding: The port forwarding allows you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings ne are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind EKI-6311GN’s NAT firewall.



Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

☐ Enable Port Forwarding

IP Address:

Protocol: Both

Port Range: -

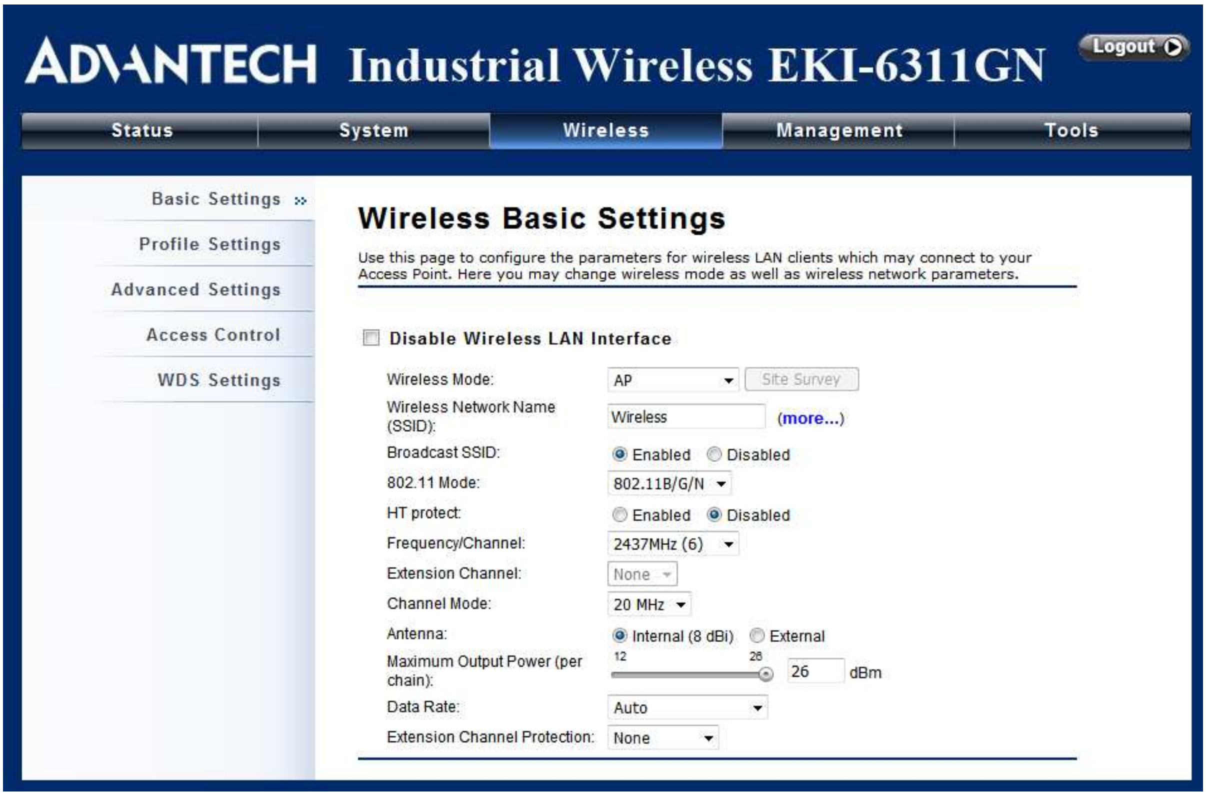
Comment:

Local IP Address	Protocol	Port Range	Comment	Select	Edit

Figure 24 Port Forwarding

3.7 Basic Wireless Settings

Open “**Basic Settings**” in “**Wireless**” as below to make basic wireless configuration.



Wireless Basic Settings

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

□ Disable Wireless LAN Interface

Wireless Mode:	AP
Wireless Network Name (SSID):	Wireless
Broadcast SSID:	● Enabled ○ Disabled
802.11 Mode:	802.11B/G/N
HT protect:	○ Enabled ● Disabled
Frequency/Channel:	2437MHz (6)
Extension Channel:	None
Channel Mode:	20 MHz
Antenna:	● Internal (8 dBi) ○ External
Maximum Output Power (per chain):	12 – 26: 26 dBm
Data Rate:	Auto
Extension Channel Protection:	None

Figure 25 Basic Wireless Settings

- **Disable Wireless LAN Interface**

  Check this option to disable WLAN interface, then the wireless module of EKI-6311GN will stop working and no wireless device can connect to it.

- **Wireless Mode**

  Four operating modes are available in EKI-6311GN.

  AP: The EKI-6311GN establishes a wireless coverage and receives connectivity from other wireless devices.

  Wireless Client: The EKI-6311GN is able to connect to the AP and thus join the wireless network around it.

  Bridge: The EKI-6311GN establishes wireless connectivity with other APs by keying in remote MAC address. Please refer to the “**WDS Setting**” for detailed configuration.

  AP Repeater: The EKI-6311GN servers as AP and Bridge concurrently. In other words, the EKI-6311GN can provide connectivity services for CPEs under Bridge mode.

- **Wireless Network Name (SSID)**

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

- **Broadcast SSID**

  Under AP mode, hiding network name is necessary when you are in a wireless environment that may have potential risk. By disabling broadcast SSID, the STA can not scan and find EKI-6311GN, so that malicious attack by some illegal STA could be avoided.

- **802.11 Mode**

  The EKI-6311GN can communicate with wireless devices of 802.11b/g or 802.11b/g/n.

- **HT Protect**

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

  ✎**Note:**

  - STA stands for Station which is referred to wireless clients connecting to Access Point.

- **Frequency/Channel**

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

- **Extension Channel**

  Only applicable to AP, AP Repeater, and 40MHz channel width indicates the use of channel bonding that allows the EKI-6311GN to use two channels at once. Two options are available: Upper Channel and Lower Channel.

- **Channel 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.

- **Antenna**

  By default, EKI-6311GN uses its built-in antenna for directional transmission; however, if you prefer to use an external antenna for your case-dependent applications, you can switch from “Internal (8 dBi)” to ”External (N-Type)”.

  When **External (N-Type)** is selected, an Antenna Gain bar will appear to allow you specify the gain of the external antenna. The antenna gain calculates the TX power back off needed to remain in compliance with regulations.

✎**Note:**

- You are able to choose “External (N-Type)” only when you have well done installing the external antenna; otherwise, it might damage EKI-6311GN itself.
- The maximum output power will vary depending on the country selected in order to comply with the local regulation.
- The output power here is counted from the RF single chain only not including the 8dBi internal antenna.

- **Maximum Output Power (per chain):**

  Specify the signal transmission power. The higher the output power is, the wider the signal can cover, but the power consumption will be greater accordingly.

- **Data Rate**

  Usually “**Auto**” is preferred. Under this rate, the EKI-6311GN will automatically select the highest available rate to transmit. In some cases, however, like where there is no great demand for speed, you can have a relatively-low transmit rate for compromise of a long distance.

- **Extension Channel Protection Mode**

  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.

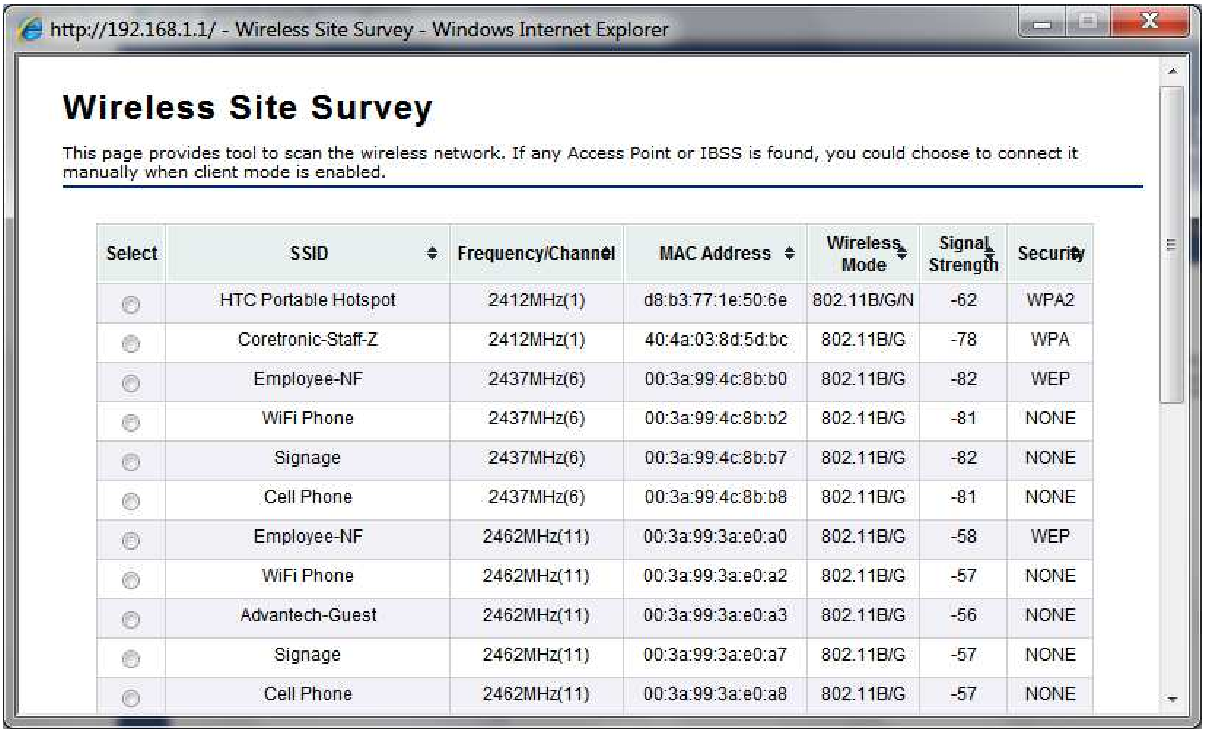
- **Enable MAC Clone**

  Available only under wireless client mode, it hides the MAC address of the AP while displays the one of associated wireless client or the MAC address designated manually.

3.8 Site Survey

Under wireless client mode, the EKI-6311GN is able to perform site survey, through which, information on the available access points will be detected.

Open "Basic Settings" in "Wireless", by clicking the "Site Survey" button beside "Wireless Mode" option, the wireless site survey window will pop up with a list of available AP in the vicinity. Select the AP you would like to connect and click "Selected" to establish connection.



http://192.168.1.1/ - Wireless Site Survey - Windows Internet Explorer

Wireless Site Survey

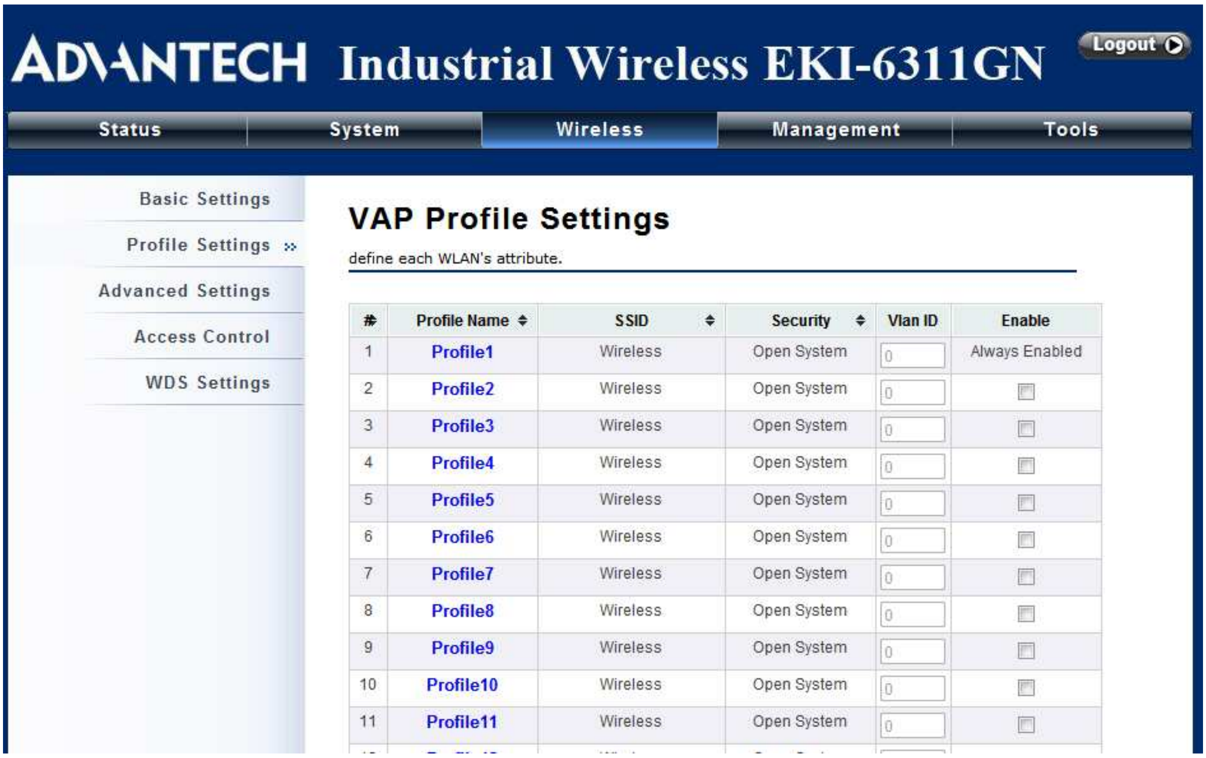
This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

Select	SSID	Frequency/Channel	MAC Address	Wireless Mode	Signal Strength	Security
○	HTC Portable Hotspot	2412MHz(1)	d8:b3:77:1e:50:6e	802.11B/G/N	-62	WPA2
○	Coretronic-Staff-Z	2412MHz(1)	40:4a:03:8d:5d:bc	802.11B/G	-78	WPA
○	Employee-NF	2437MHz(6)	00:3a:99:4c:8b:b0	802.11B/G	-82	WEP
○	WiFi Phone	2437MHz(6)	00:3a:99:4c:8b:b2	802.11B/G	-81	NONE
○	Signage	2437MHz(6)	00:3a:99:4c:8b:b7	802.11B/G	-82	NONE
○	Cell Phone	2437MHz(6)	00:3a:99:4c:8b:b8	802.11B/G	-81	NONE
○	Employee-NF	2462MHz(11)	00:3a:99:3a:e0:a0	802.11B/G	-58	WEP
○	WiFi Phone	2462MHz(11)	00:3a:99:3a:e0:a2	802.11B/G	-57	NONE
○	Advantech-Guest	2462MHz(11)	00:3a:99:3a:e0:a3	802.11B/G	-56	NONE
○	Signage	2462MHz(11)	00:3a:99:3a:e0:a7	802.11B/G	-57	NONE
○	Cell Phone	2462MHz(11)	00:3a:99:3a:e0:a8	802.11B/G	-57	NONE

Figure 26 Site Survey

VAP Profile Settings

Available in AP mode, the IEEE 802.11b/g/n Wireless Outdoor CPE allows up to 16 virtual SSIDs on a single BSSID and to configure different profile settings such as security and VLAN ID to each SSID. To create a virtual AP, you may check the **Enable** box of the profile and click on the profile (eg. Profile 2) to configure wireless and security settings. Hit **Apply** to active the profile.

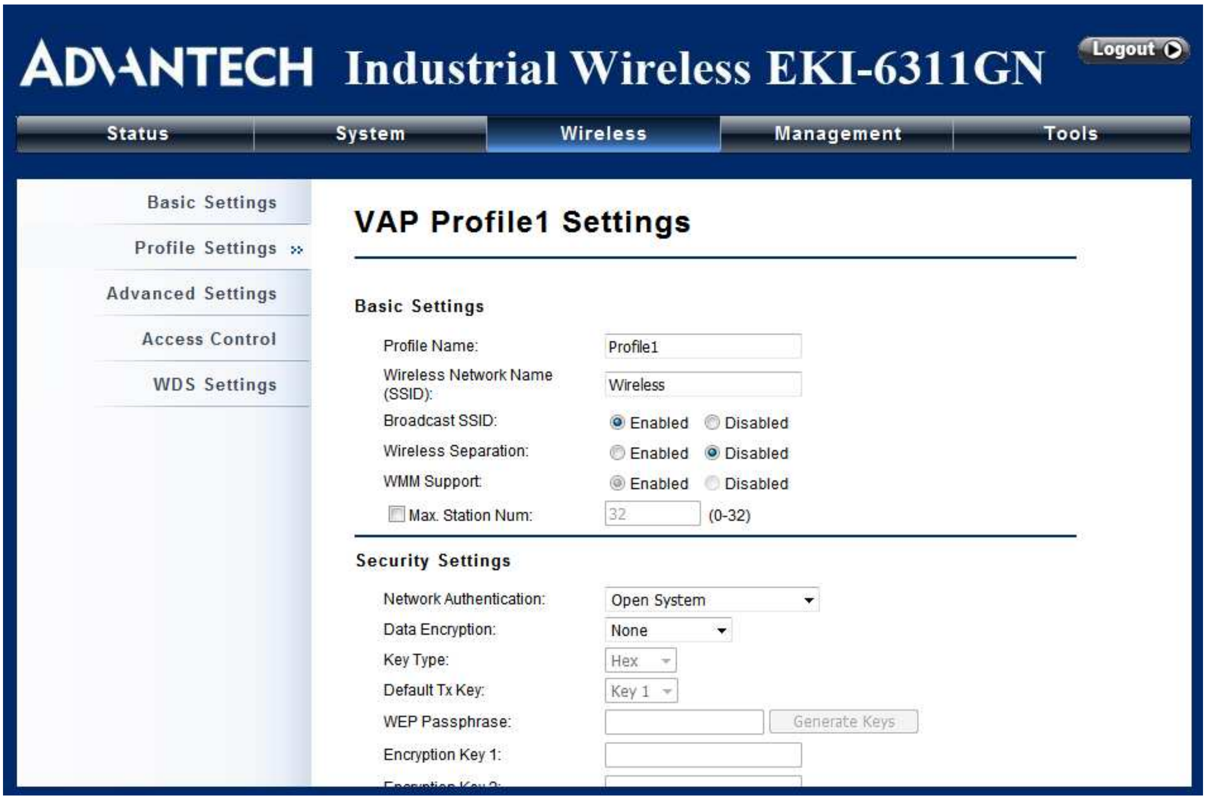


VAP Profile Settings

define each WLAN's attribute.

#	Profile Name	SSID	Security	Vlan ID	Enable
1	Profile1	Wireless	Open System	0	Always Enabled
2	Profile2	Wireless	Open System	0	☐
3	Profile3	Wireless	Open System	0	☐
4	Profile4	Wireless	Open System	0	☐
5	Profile5	Wireless	Open System	0	☐
6	Profile6	Wireless	Open System	0	☐
7	Profile7	Wireless	Open System	0	☐
8	Profile8	Wireless	Open System	0	☐
9	Profile9	Wireless	Open System	0	☐
10	Profile10	Wireless	Open System	0	☐
11	Profile11	Wireless	Open System	0	☐

Figure 4 VAP Profile Settings



VAP Profile1 Settings

Basic Settings

Profile Name: Profile1

Wireless Network Name (SSID): Wireless

Broadcast SSID: ● Enabled ○ Disabled

Wireless Separation: ○ Enabled ● Disabled

WMM Support: ● Enabled ○ Disabled

☐ Max. Station Num: 32 (0-32)

Security Settings

Network Authentication: Open System

Data Encryption: None

Key Type: Hex

Default Tx Key: Key 1

WEP Passphrase:

Encryption Key 1:

Figure 28 VAP Profile Settings

- **Basic Setting**

Profile Name: Name of the VAP profile

Wireless Network Name: Enter the virtual SSID for the VAP

Broadcast SSID: In AP mode, hiding network name is necessary when you are in a wireless environment that may have potential risk. By disabling broadcast SSID, the STA cannot scan and find the IEEE 802.11b/g/n Wireless Outdoor CPE, so that malicious attack by some illegal STA could be avoided.

Wireless Separation: Wireless separation is an ideal way to enhance the security of network transmission. Under the mode except wireless client mode, enable "**Wireless Separation**" can prevent the communication among associated wireless clients.

WMM Support: WMM (Wi-Fi Multimedia) is a subset of 802.11e. It allows wireless communication to define a priority limit on the basis of data type under AP mode only, thus those time-sensitive data, like video/audio data, may own a higher priority than common one. To enable WMM, the wireless client should also support it

Max. Station Number: By checking the "**Max. Station Num**" the CPE will only allow up to 32 wireless clients to associate with for better bandwidth for each client. By disabling the checkbox the CPE will allow up to 128 clients to connect, but it is likely to cause network congestion or poor performance.

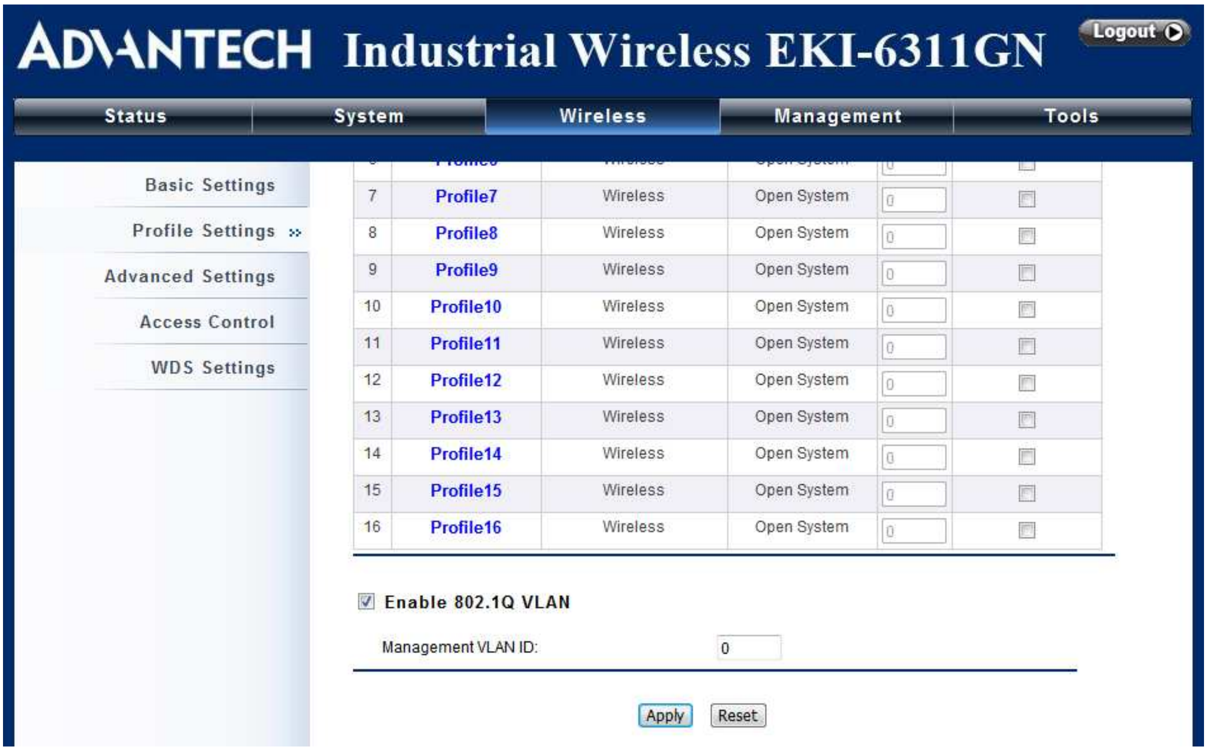
- **Security Setting:**

  To prevent unauthorized radios from accessing data transmitting over the connectivity, the IEEE 802.11a/n Wireless Outdoor CPE provides you with rock solid security settings.

VLAN Tab

If your network uses VLANs, you can assign one SSID to a VLAN, and client devices using the SSID are grouped in that VLAN.

To allow users on the VLAN to access the WEB page of the IEEE 802.11a/n Wireless Outdoor CPE, you need to enable "**Enable 802.1Q VLAN**" and assign a management VLAN ID for your device. Make sure the assigned management VLAN ID is identical to your network VLAN ID to avoid failures of accessing the Web page of the EKI-6311GN.



7	Profile7	Wireless	Open System	0	□
8	Profile8	Wireless	Open System	0	□
9	Profile9	Wireless	Open System	0	□
10	Profile10	Wireless	Open System	0	□
11	Profile11	Wireless	Open System	0	□
12	Profile12	Wireless	Open System	0	□
13	Profile13	Wireless	Open System	0	□
14	Profile14	Wireless	Open System	0	□
15	Profile15	Wireless	Open System	0	□
16	Profile16	Wireless	Open System	0	□

☑ Enable 802.1Q VLAN

Management VLAN ID: 0

Figure 5 Management VLAN ID

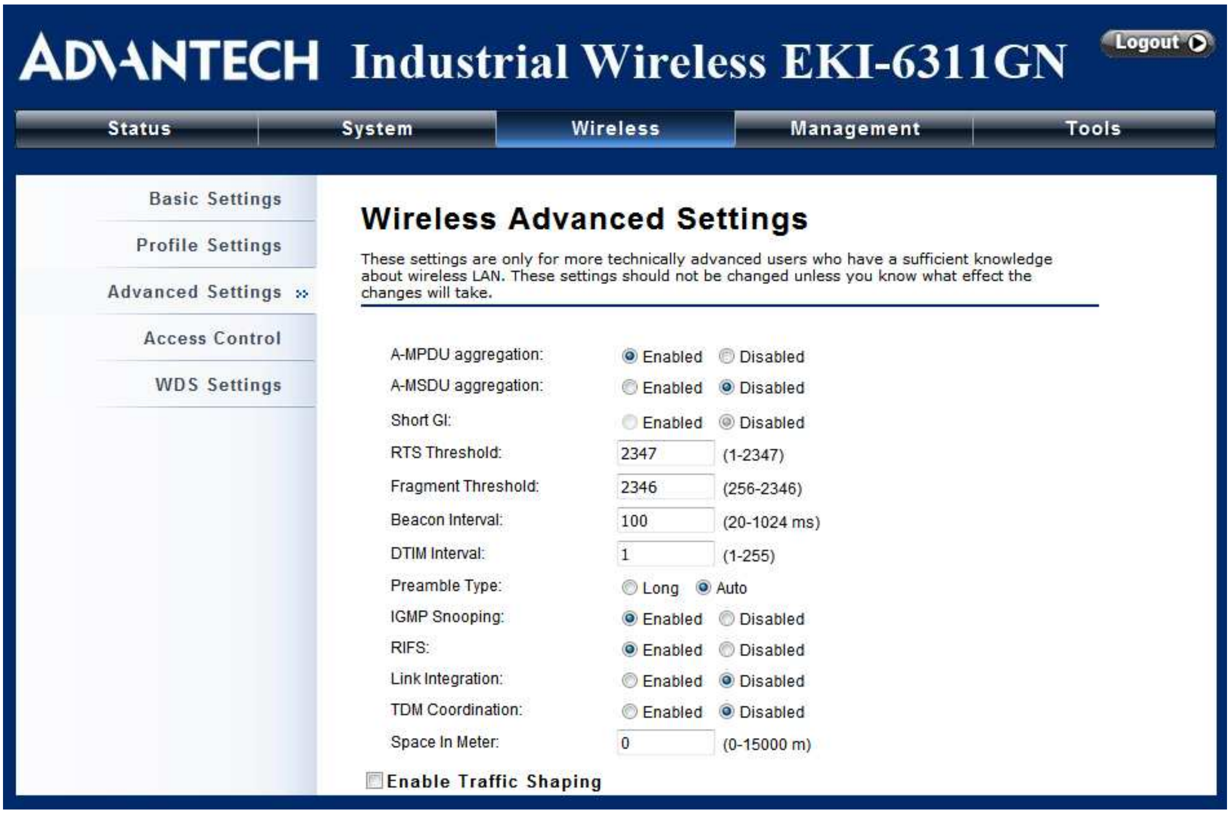
CHAPTER 4

Advanced Settings

Chapter 4   Advanced Settings

4.1   Advanced Wireless Settings

Open “**Advanced Settings**” in “**Wireless**” to make advanced wireless settings.



Wireless Advanced Settings

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

A-MPDU aggregation:	● Enabled	○ Disabled
A-MSDU aggregation:	○ Enabled	● Disabled
Short GI:	○ Enabled	● Disabled
RTS Threshold:	2347	(1-2347)
Fragment Threshold:	2346	(256-2346)
Beacon Interval:	100	(20-1024 ms)
DTIM Interval:	1	(1-255)
Preamble Type:	○ Long	● Auto
IGMP Snooping:	● Enabled	○ Disabled
RIFS:	● Enabled	○ Disabled
Link Integration:	○ Enabled	● Disabled
TDM Coordination:	○ Enabled	● Disabled
Space In Meter:	0	(0-15000 m)

□ Enable Traffic Shaping

Figure 6 Advanced Wireless Settings

- **A-MPDU/A-MSDU Aggregation**

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

- **Short GI**

  Under 802.11n mode, enable it to obtain better data rate if there is no negative compatibility issue.

- **RTS Threshold**

  The EKI-6311GN sends RTS (Request to Send) frames to certain receiving station and negotiates the sending of a data frame. After receiving an RTS, that STA responds with a CTS (Clear to Send) frame to acknowledge the right to start transmission. The setting range is 0 to 2346 in byte. Setting it too low may result in poor network performance. Leave it at its default of 2346 is recommended.

- **Fragmentation Length**

Specify the maximum size in byte for a packet before data is fragmented into multiple packets. Setting it too low may result in poor network performance. Leave it at its default of 2346 is recommended.

- **Beacon Interval**

  Specify the frequency interval to broadcast packets. Enter a value between 20 and 1024.

- **DTIM Interval**

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

- **Preamble Type**

  It defines some details on the 802.11 physical layer. "**Long**" and "**Auto**" are available.

- **IGMP Snooping**

  Available in AP/Router mode, IGMP snooping is the process of listening to IGMP network traffic. By enabling IGMP snooping, the AP will listen to IGMP membership reports, queries and leave messages to identify the ports that are members of multicast groups. Multicast traffic will only be forwarded to ports identified as members of the specific multicast group or groups.

- **RIFS**

  RIFS (Reduced Interframe Spacing) is a means of reducing overhead and thereby increasing network efficiency.

- **Link Integration**

  Available under AP/Bridge/AP repeater mode, it monitors the connection on the Ethernet port by checking "**Enabled**". It can inform the associating wireless clients as soon as the disconnection occurs.

- **TDM Coordination**

  Stands for "Time-Division Multiplexing Technique", this resource reservation control mechanisms can avoid packet collisions and send the packets much more efficiently allowing for higher effective throughput rates. This function is only available in AP/CPE mode. It is highly recommended to enable TDM coordination when there are multiple CPEs needed to connect to the AP in your application.

- **LAN2LAN CPE**

  LAN2LAN CPE mode enables packet forwarding at layer 2 level. It is fully transparent for all the Layer2 protocols.

- **Space in Meter**

  To decrease the chances of data retransmission at long distance, the EKI-6311GN can automatically adjust proper ACK timeout value by specifying distance of the two nodes.

- **Flow Control**

  It allows the administrator to specify the incoming and outgoing traffic limit by checking "**Enable Traffic Shaping**". This is only available in Router mode.

Note:

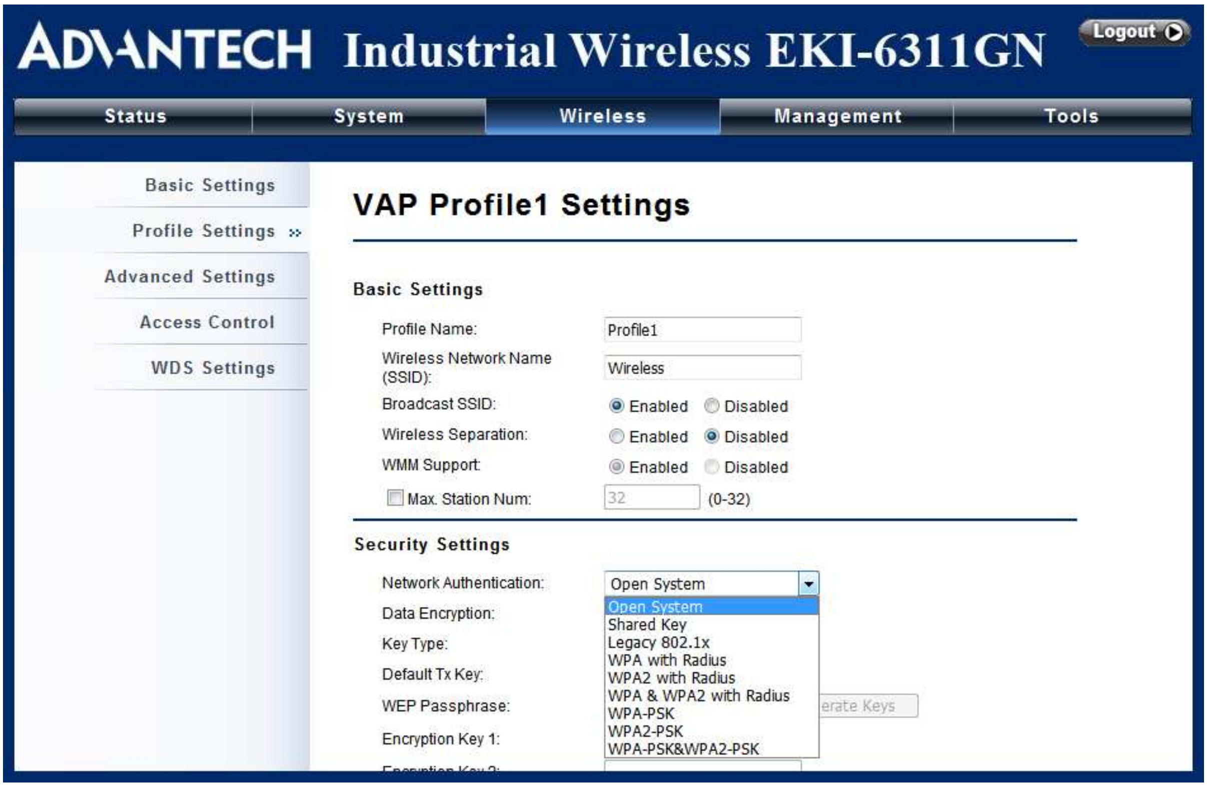
- We strongly recommend you leave most advanced settings at their defaults except "Distance in Meters" adjusted the parameter for real distance; any modification on them may negatively impact the performance of your wireless network.

4.2 Wireless Security Settings

To prevent unauthorized radios from accessing data transmitting over the connectivity, the EKI-6311GN provides you with rock solid security settings.

Data Encryption and Authentication Settings

Open "**Profile Setting**" in "**Wireless**" and enter "**VAP Profile 1 Settings**" as below.



VAP Profile1 Settings

Basic Settings

Profile Name: Profile1

Wireless Network Name (SSID): Wireless

Broadcast SSID: ● Enabled ○ Disabled

Wireless Separation: ○ Enabled ● Disabled

WMM Support: ● Enabled ○ Disabled

□ Max. Station Num: 32 (0-32)

Security Settings

Network Authentication: Open System

Data Encryption:

Key Type:

Default Tx Key:

WEP Passphrase:

Encryption Key 1:

Encryption Key 2:

Figure 7 Security Settings

- **Network Authentication**

Open System: It allows any device to join the network without performing any security check.
Shared Key: Data encryption and key are required for wireless authentication (Not available in Bridge/AP Repeater mode).
Legacy 802.1x: Available in AP/Wireless Client mode, it provides the rights to access the wireless network and wired Ethernet. With User and PC identity, centralized authentication as well as dynamic key management, it controls the security risk of wireless network to the lowest. To serve the 802.1x, at least one EAP type should be supported by the RADIUS Server, AP and wireless client.

Note:

- For first time users, if EAP type "TLS" is selected, you need to import valid user certificate given by CA in prior. To import user certificates, please refer to Chapter 5 Management/Certificate Settings for more details. .

WPA with RADIUS: Available in AP/Wireless Client mode, with warrant (username, password and etc.) offered by user, this kind of authentication can be realized with specific RADIUS server. This is the common way to be adopted in large enterprise network.
WPA2 with RADIUS: Available in AP/Wireless Client mode, as a new version of WPA, only all the clients support WPA2, can it be available. If it is selected, AES encryption and RADIUS server is required. It is only available in AP/Wireless Client mode.
WPA&WPA2 with RADIUS: Available in AP mode, it provides options of WPA (TKIP) or WPA2 (AES) for the client. If it is selected, the data encryption type must be TKIP + AES and the RADIUS server must be set.
WPA-PSK: It is a simplified WPA mode with no need for specific authentication server. In this so-called WPA Pre-Shared Key, all you have to do is just pre-enter a key in each WLAN node and this is the common way to be adopted in large and middle enterprise as well as residential network.
WPA2-PSK: As a new version of WPA, only all the clients support WPA2, can it be available. If it is selected, the data encryption can only be AES and the passphrase is required.
WPA-PSK&WPA2-PSK: Available in AP mode, it provides options of WPA (TKIP) or WPA2 (AES) encryption for the client. If it is selected, the data encryption can only be TKIP + AES and the passphrase is required.

- **Data Encryption**

If data encryption is enabled, the key is required and only sharing the same key with other wireless devices can the communication be established.
None: Available only when the authentication type is open system.
64 bits WEP: It is made up of 10 hexadecimal numbers.
128 bits WEP: It is made up of 26 hexadecimal numbers.
152 bits WEP: It is made up of 32 hexadecimal numbers.
TKIP: Temporal Key Integrity Protocol, which is a kind of dynamic encryption, is co-used with WPA-PSK, etc.
AES: Advanced Encryption Standard, it is usually co-used with WPA2-PSK, WPA, WPA2, etc.
TKIP + AES: It allows for backwards compatibility with devices using TKIP.

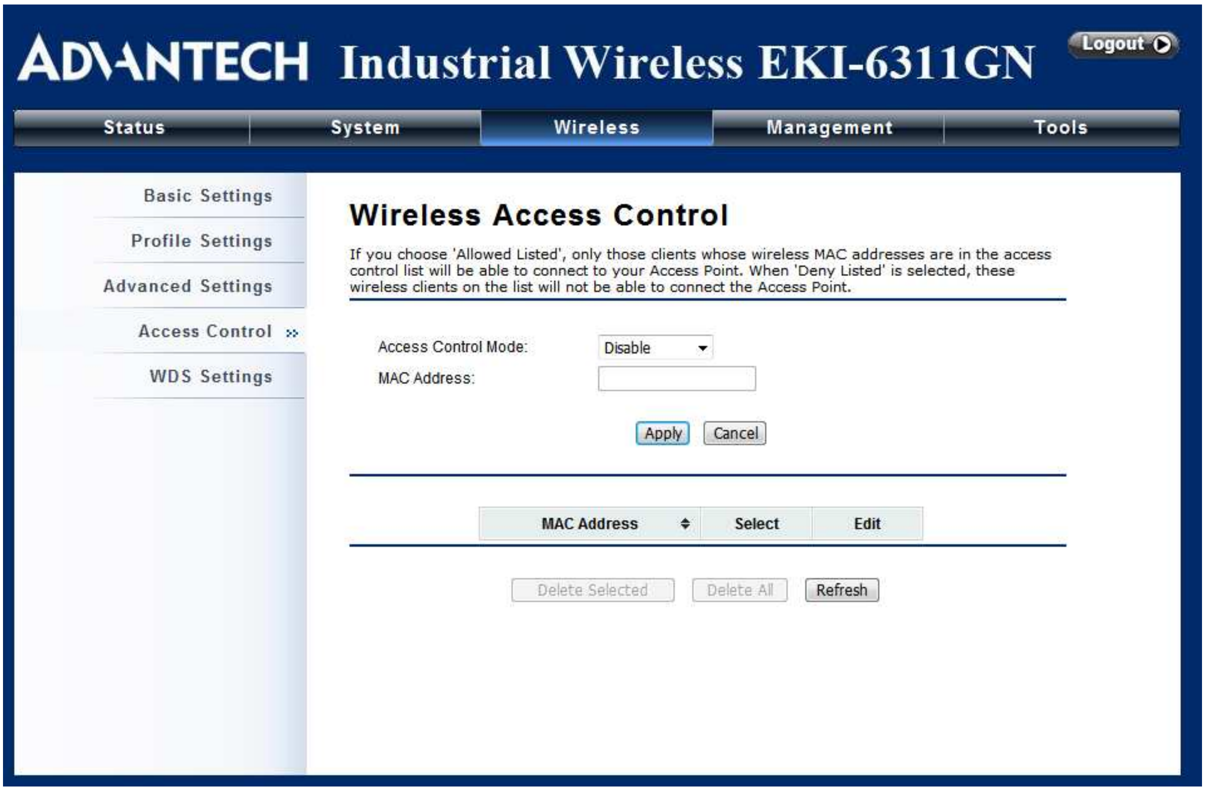
Note:

- We strongly recommend you enable wireless security on your network!
- Only setting the same Authentication, Data Encryption and Key in the EKI-6311GN and other associated wireless devices, can the communication be established!

Access Control

The Access Control appoints the authority to wireless client on accessing EKI-6311GN, thus a further security mechanism is provided. This function is available only under AP mode.

Open “**Access Control**” in “**Wireless**” as below.



Wireless Access Control

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

Access Control Mode: Disable

MAC Address:

Figure 8 Access Control

- **Access Control Mode**

  If you select “**Allow Listed**”, only those clients whose wireless MAC addresses are in the access control list will be able to connect to your AP. While when “**Deny Listed**” is selected, those wireless clients on the list will not be able to connect the AP.

- **MAC Address**

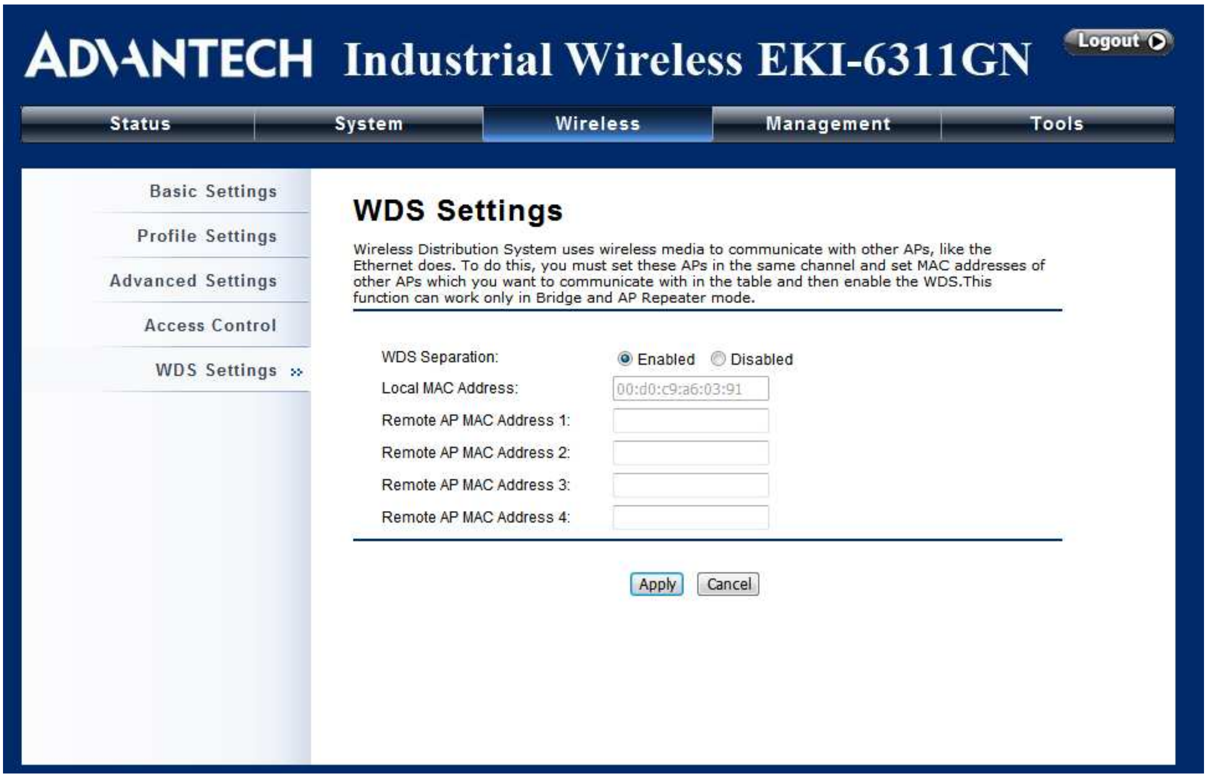
  Enter the MAC address of the wireless client that you would like to list into the access control list, click “**Apply**” then it will be added into the table at the bottom.

- **Delete Selected/All**

  Check the box before one or more MAC addresses of wireless client(s) that you would like to cancel, and click “**Delete Selected**” or “**Delete All**” to cancel that access control rule.

WDS Settings

Extend the range of your network without having to use cables to link the Access Points by using the Wireless Distribution System (WDS): Simply put, you can link the Access Points wirelessly. Open "**WDS Settings**" in "**Wireless**" as below:



WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC addresses of other APs which you want to communicate with in the table and then enable the WDS.This function can work only in Bridge and AP Repeater mode.

WDS Separation: ● Enabled ○ Disabled

Local MAC Address: 00:d0:c9:a6:03:91

Remote AP MAC Address 1:

Remote AP MAC Address 2:

Remote AP MAC Address 3:

Remote AP MAC Address 4:

Figure 33 WDS Settings

Enter the MAC address of another AP you wirelessly want to connect to into the appropriate field and click "**Apply**" to save settings.

Note:

- WDS Settings is available only under Bridge and AP Repeater Mode.
- Bridge uses the WDS protocol that is not defined as the standard thus compatibility issues between equipment from different vendors may arise. Moreover, Tree or Star shape network topology should be used in all WDS use-cases (i.e. if AP2 and AP3 are specified as the WDS peers of AP1, AP2 should not be specified as the WDS peer of AP3 and AP3 should not be specified as the WDS peer of AP2 in any case). Mesh and Ring network topologies are not supported by WDS and should be avoided in all the use cases.

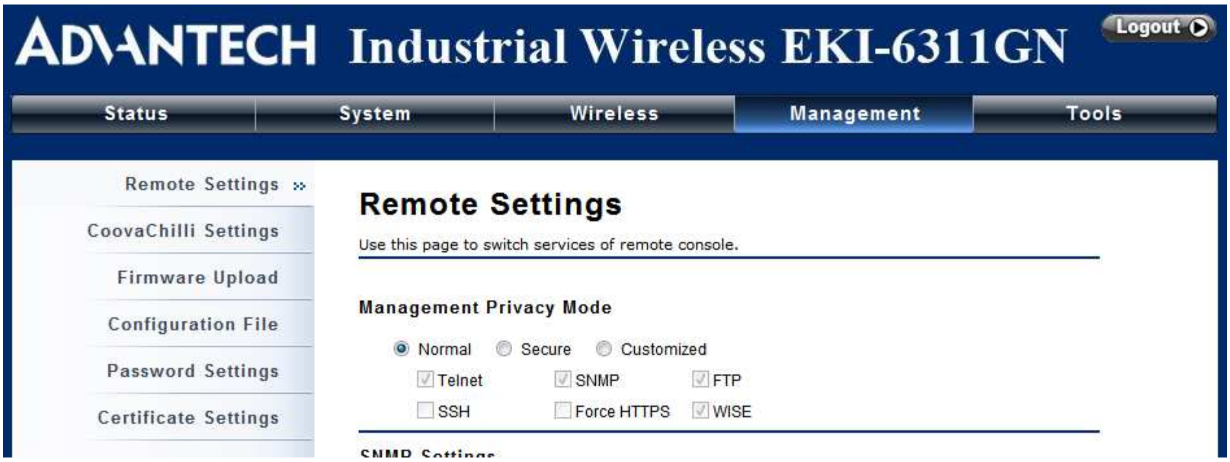
CHAPTER 5

Management

Chapter 5 Management

Remote Management

The IEEE 802.11b/g/n Wireless Outdoor CPE provides a variety of remotes managements including Telnet, SNMP, FTP, SSH, HTTPS and exclusive WISE tool, making configuration more convenient and secure.
With **Normal** selected, Telnet, SNMP and FTP are activated as default remote management options. To use secure management tools such as SSH, HTTPS and WISE, please select "**Secure**". You may also choose "**Customized**" to enable any methods as desired.



Remote Settings

Use this page to switch services of remote console.

Management Privacy Mode

● Normal ○ Secure ○ Customized

☑ Telnet ☑ SNMP ☑ FTP

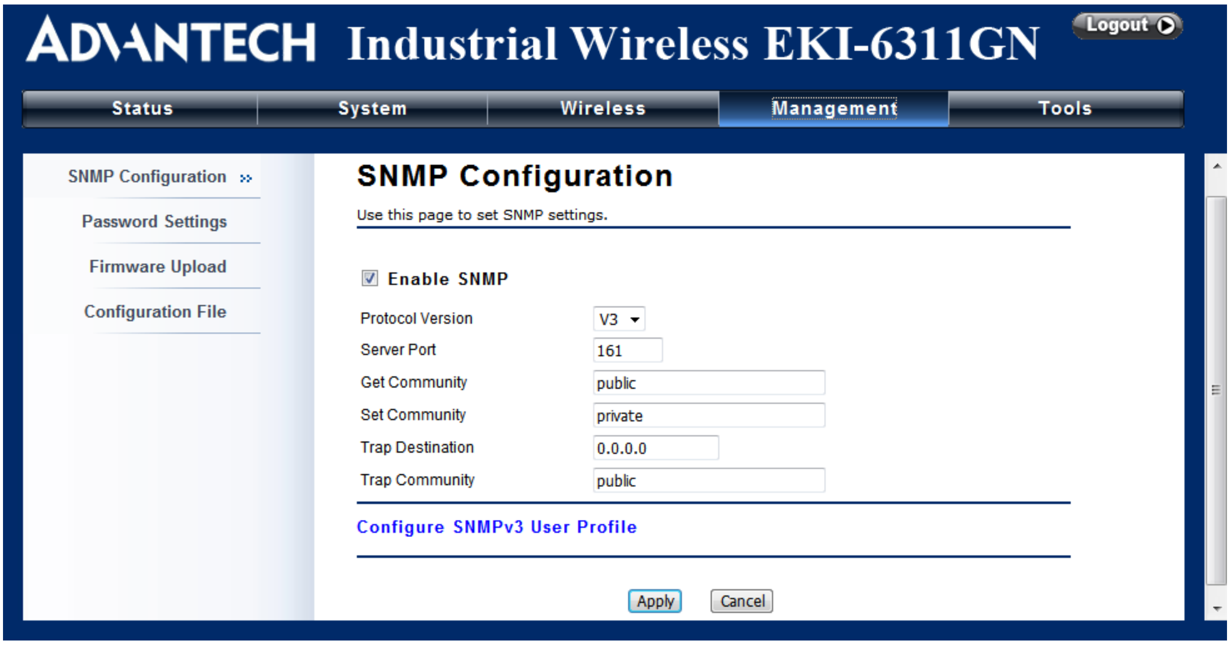
□ SSH □ Force HTTPS ☑ WISE

SNMP Settings

Figure 34 Remote Settings

5.1 SNMP Management

The EKI-6311GN supports SNMP for convenient remote management. Open "**SNMP Configuration**" in "**Management**" shown below. Set the SNMP parameters and obtain MIB file before remote management.



SNMP Configuration

Use this page to set SNMP settings.

☑ Enable SNMP

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

Figure 35 SNMP Configuration

- **Protocol Version**

  Select the SNMP version, and keep it identical on the EKI-6311GN and the SNMP manager. The EKI-6311GN supports SNMP v2/v3.

- **Server Port**

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

- **Get Community**

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

- **Set Community**

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

- **Trap Destination**

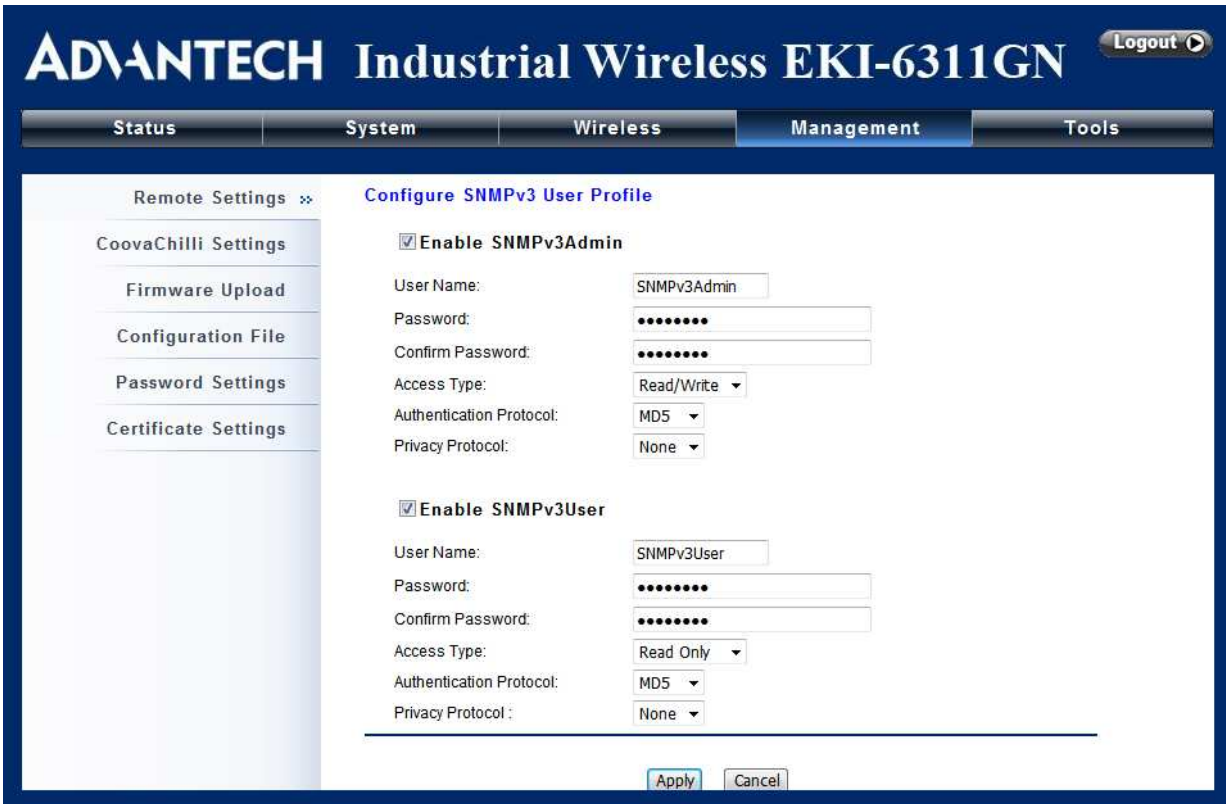
  Specify the IP address of the station to send the SNMP traps to.

- **Trap Community**

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

Configure SNMPv3 User Profile

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



Configure SNMPv3 User Profile

☑ Enable SNMPv3Admin

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

☑ Enable SNMPv3User

User Name: SNMPv3User
Password: ••••••••
Confirm Password: ••••••••
Access Type: Read Only
Authentication Protocol: MD5
Privacy Protocol : None

Figure 9 Configure SNMPv3 User Profile

- **User Name**

  Specify a user name for the SNMPv3 administrator or user. Only the SNMP commands carrying this user name are allowed to access the EKI-6311GN.

- **Password**

  Specify a password for the SNMPv3 administrator or user. Only the SNMP commands carrying this password are allowed to access the EKI-6311GN.

- **Confirm Password**

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

- **Access Type**

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

- **Authentication Protocol**

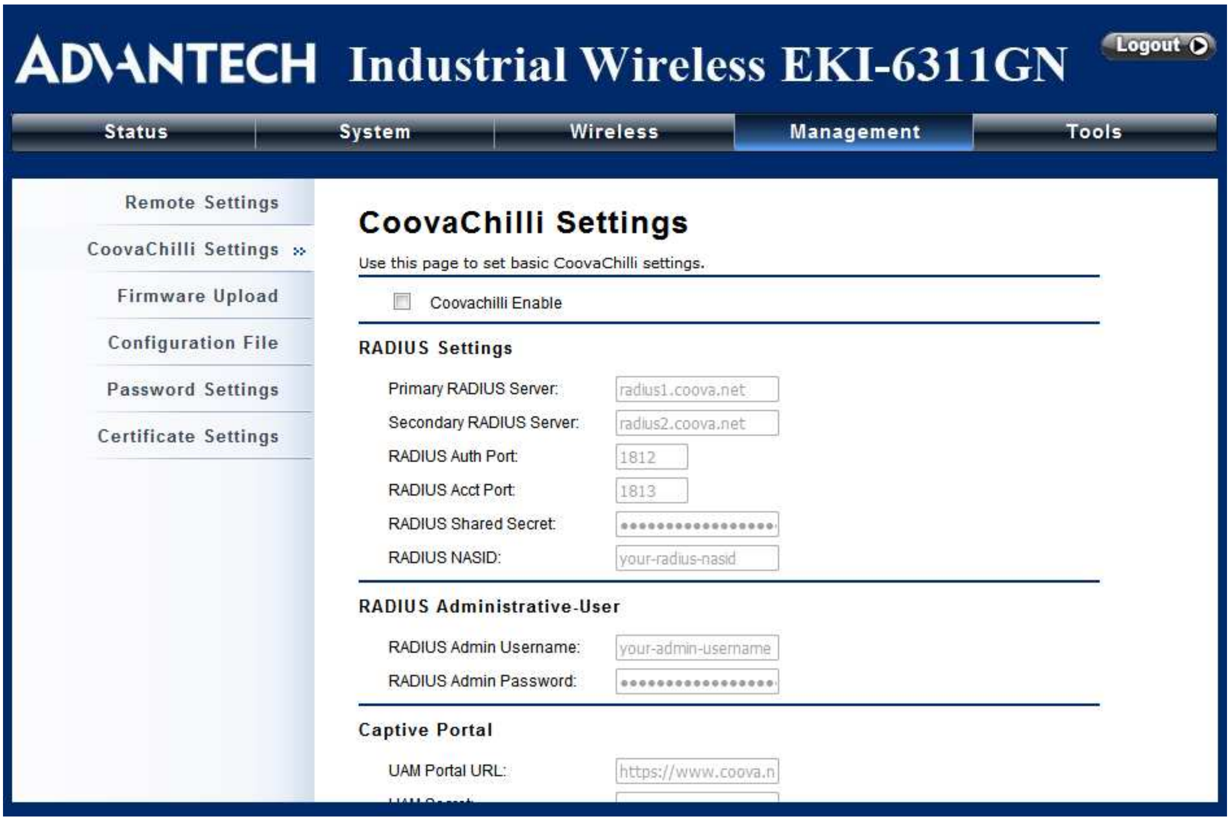
  Select an authentication algorithm. SHA authentication is stronger than MD5 but is slower.

- **Privacy Protocol**

  Specify the encryption method for SNMP communication. None and DES are available.
  None: No encryption is applied.
  DES: Data Encryption Standard, it applies a 58-bit key to each 64-bit block of data.

Coovachilli Settings

Coovachilli is a captive portal management which allows WLAN users to easily and securely access the Internet. Under Router mode, when Coovachilli is enabled, the IEEE 802.11b/g/n Wireless Access Point will force an HTTP client on a network to see a special web page (usually for authentication purposes) before using the Internet normally. At that time the browser is redirected to a web page which may require authentication. Captive portals are used at most Wi-Fi hotspots. Therefore, to use Coovachilli, you need to find Coovachilli service providers that have the additional services needed to make Coovahcilli work.



CoovaChilli Settings

Use this page to set basic CoovaChilli settings.

□ Coovachilli Enable

RADIUS Settings

Primary RADIUS Server: radius1.coova.net

Secondary RADIUS Server: radius2.coova.net

RADIUS Auth Port: 1812

RADIUS Acct Port: 1813

RADIUS Shared Secret: •••••••••••••••••

RADIUS NASID: your-radius-nasid

RADIUS Administrative-User

RADIUS Admin Username: your-admin-username

RADIUS Admin Password: •••••••••••••••••

Captive Portal

UAM Portal URL: https://www.coova.n

Figure 10 Coovachilli Settings

Radius Settings

- **Primary Radius Server**

  Enter the name or IP address of the primary radius server

- **Secondary Radius Server**

  Enter the name or IP address of the primary radius server if any.

- **Radius Auth Port:**

  Enter the port number for authentication

- **Radius Acct Port:**

  Enter the port number for billing

- **Radius Shared Secret:**

Enter the secret key of the radius server

- **Radius NAS ID:**

  Enter the name of the radius server if any

Radius Administrative-User

- **Radius Admin Username:**

  Enter the username of the Radius Administrator

- **Radius Admin Password:**

  Enter the password of the Radius Administrator

Captive Portal

- **UAM Portal URL:**

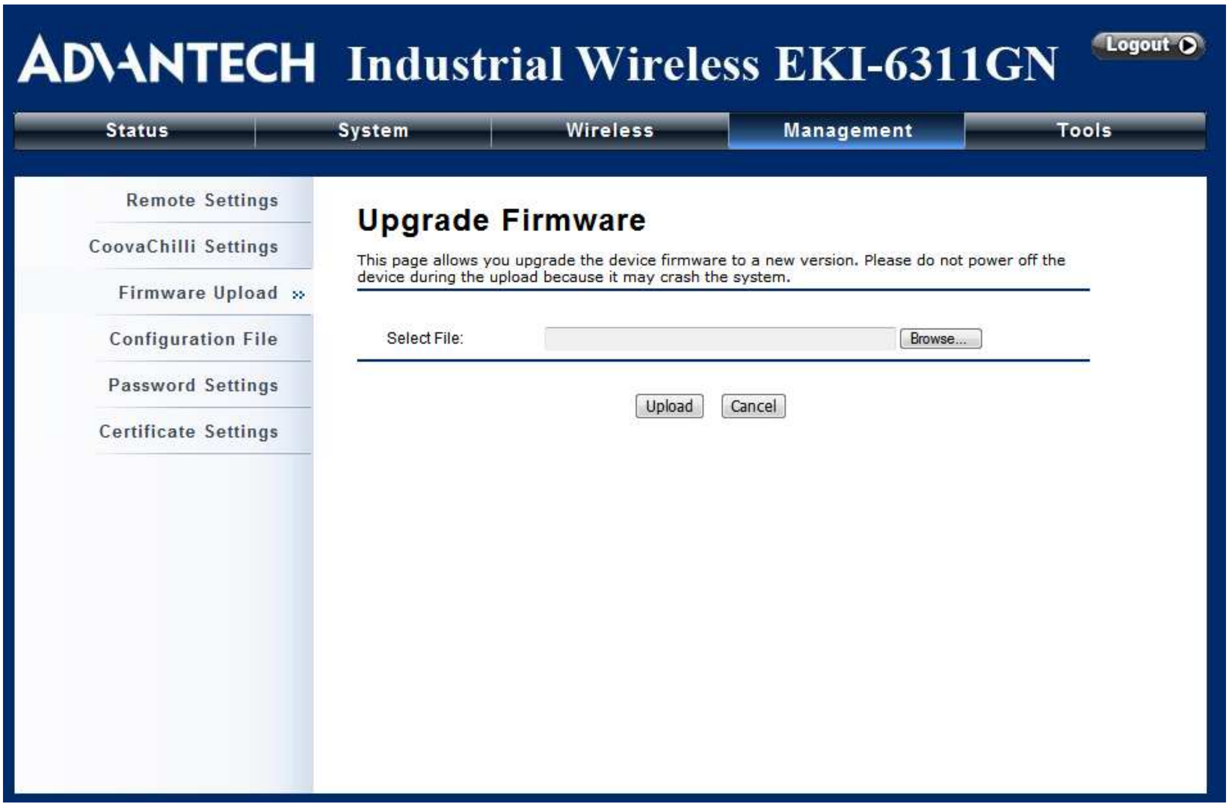
  Enter the address of the UAM portal server

- **UAM Secret:**

  Enter the secret password between the redirect URL and the Hotspot.

Upgrade Firmware

Open “**Firmware Upload**” in “**Management**” and follow the steps below to upgrade firmware locally or remotely through EKI-6311GN’s Web:



Upgrade Firmware

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

Select File:

Figure 11 Upgrade Firmware

- Click “**Browse**” to select the firmware file you would like to load;

- Click "**Upload**" to start the upload process;
- Wait a moment, the system will reboot after successful upgrade.

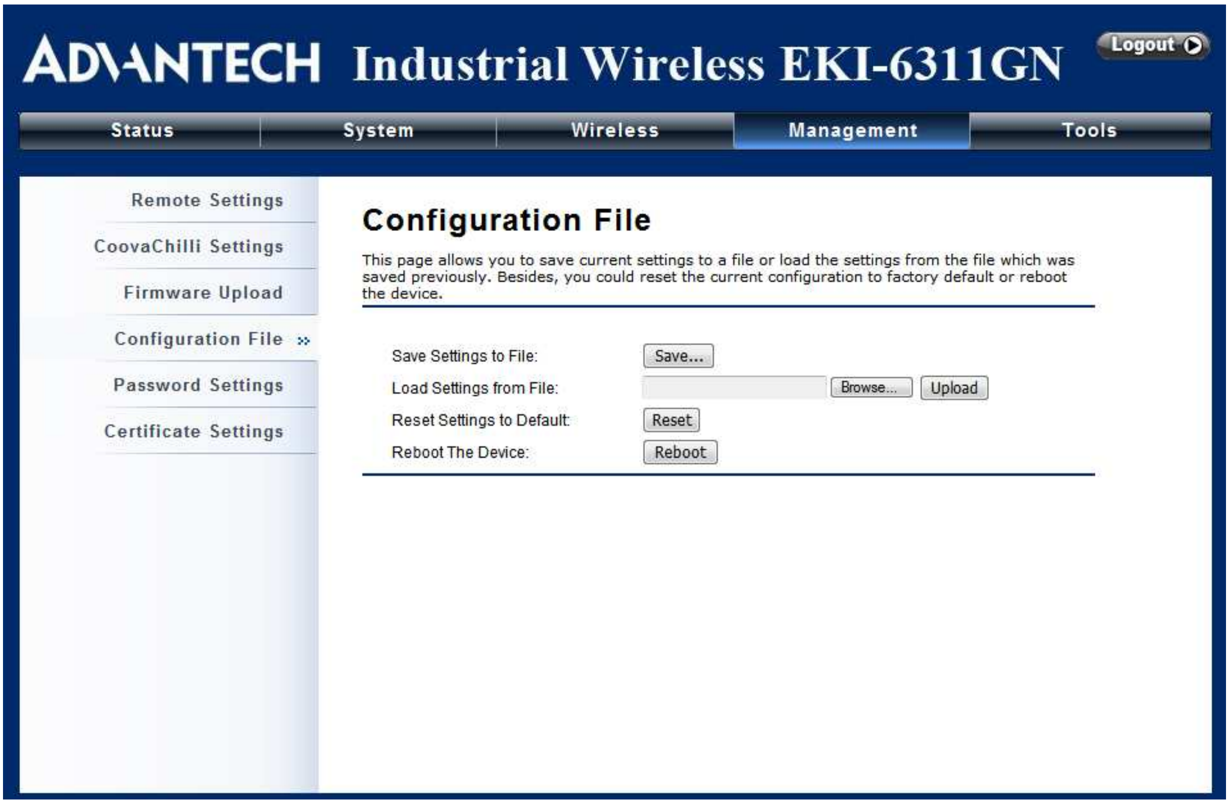
Note:

- Do NOT cut the power off during upgrade, otherwise the system may crash!

Backup/ Retrieve Settings

It is strongly recommended you back up configuration information in case of something unexpected. If tragedy hits your device, you may have an access to restore the important files by the backup. All these can be done by the local or remote computer.

Open "**Configuration File**" in "**Management**" as below:



Configuration File

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

Save Settings to File:

Load Settings from File:

Reset Settings to Default:

Reboot The Device:

Figure 12 Backup/Retrieve Settings

- **Save Setting to File**

  By clicking "**Save**", a dialog box will pop up. Save it, then the configuration file **ap.cfg** will be generated and saved to your local computer.

- **Load Settings from File**

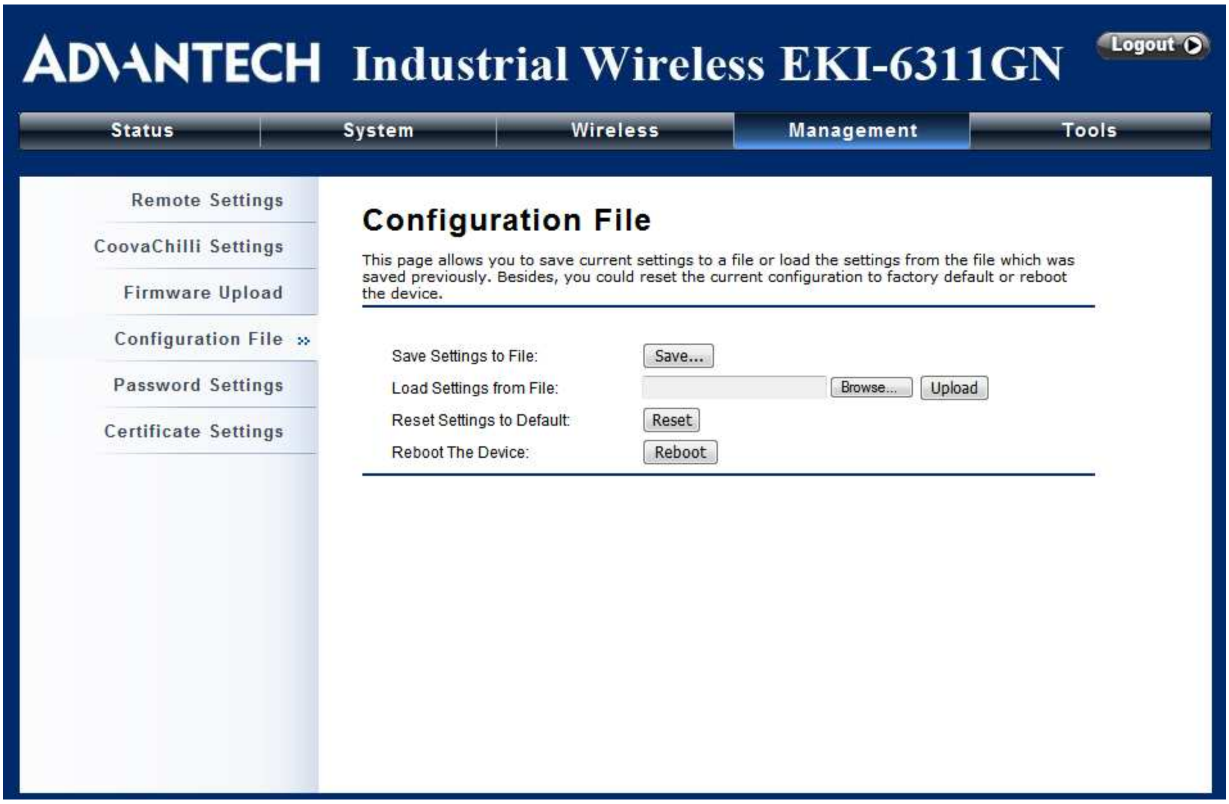
  By clicking "**Browse**", a file selection menu will appear, select the file you want to load, like **ap.cfg**; Click "**Upload**" to load the file. After automatically rebooting, new settings are applied.

Restore Factory Default Settings

The EKI-6311GN provides two ways to restore the factory default settings:

- **Restore factory default settings via Web**

  From “**Configuration File**”, clicking “**Reset**” will eliminate all current settings and reboot your device, then default settings are applied.



Configuration File

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

Save Settings to File:

Load Settings from File:

Reset Settings to Default:

Reboot The Device:

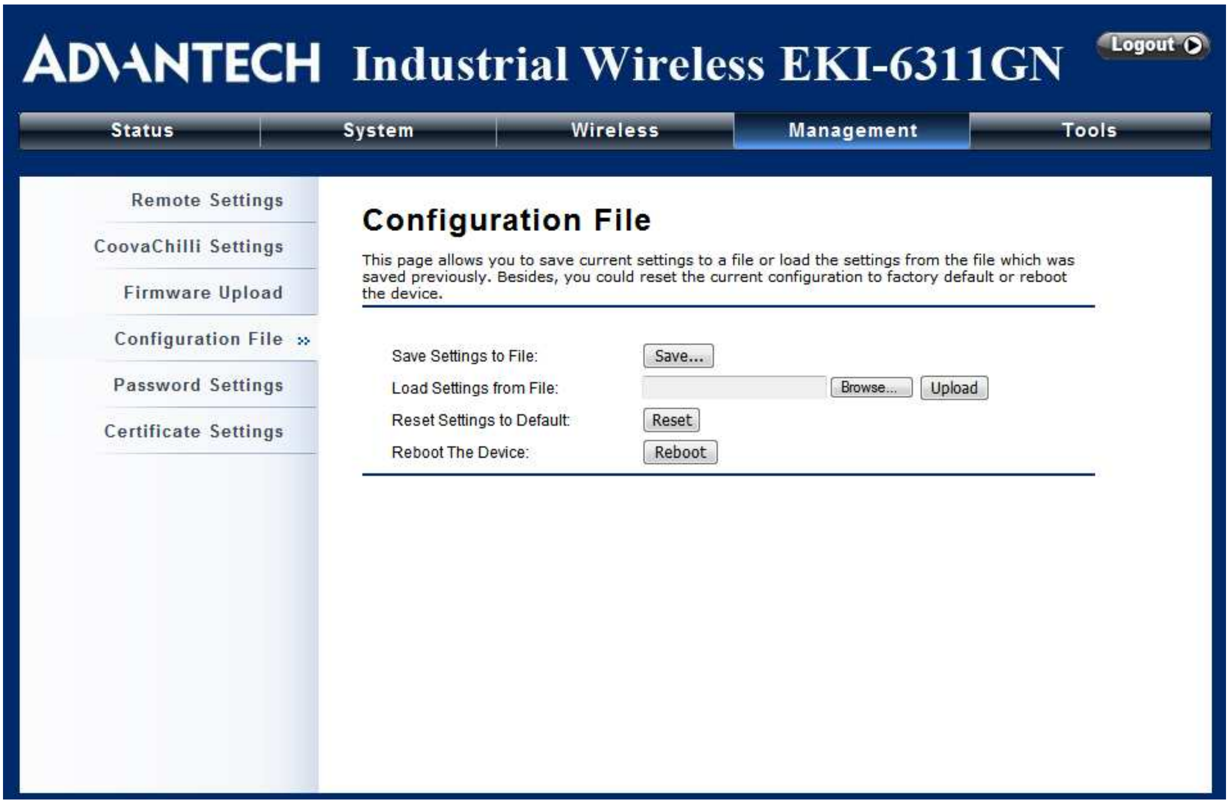
Figure 13 Restore Settings

- **Restore factory default settings via Reset Button**

  If software in EKI-6311GN is unexpectedly crashed and no longer reset the unit via Web, you may do hardware reset via the reset button. Press and hold the button for at least 5 seconds and then release it until the PWR LED gives a blink.

Reboot

You can reboot your EKI-6311GN from “**Configuration File**” in “**Management**” as below:
Click “**Reboot**” and hit “**Yes**” upon the appeared prompt to start reboot process. This takes a few minutes.



Configuration File

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

Save Settings to File:

Load Settings from File:

Reset Settings to Default:

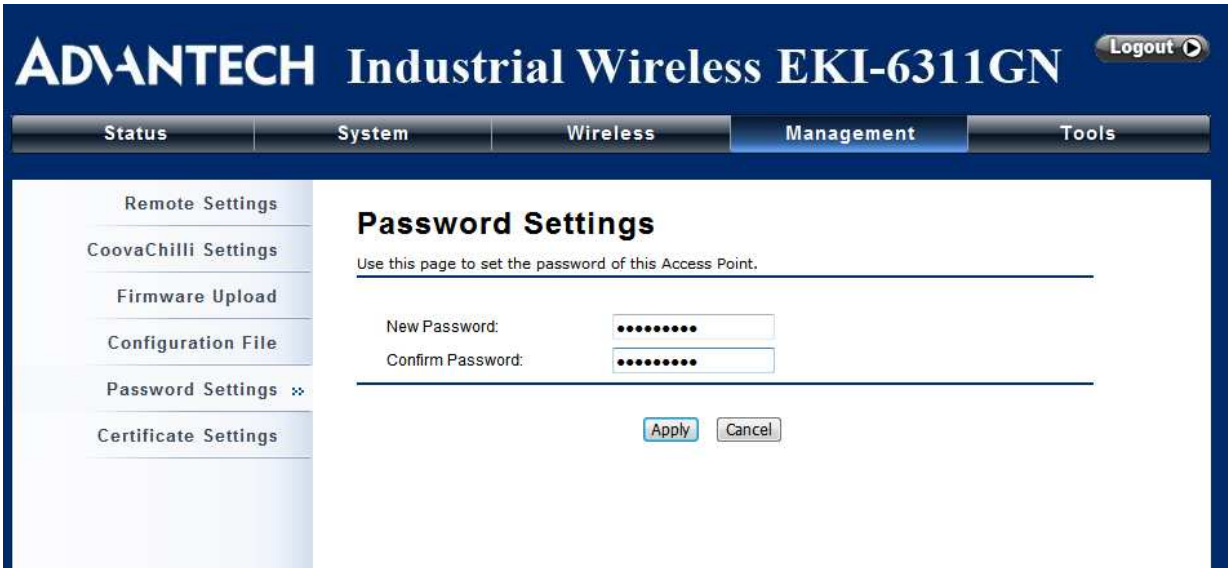
Reboot The Device:

Figure 14 Reboot

Password

From “**Password Settings**” in “**Management**”, you can change the password to manage your EKI-6311GN.

Enter the new password respectively in “**New Password**” and “**Confirm Password**” fields; click “**Apply**” to save settings.



Password Settings

Use this page to set the password of this Access Point.

New Password: •••••••••

Confirm Password: •••••••••

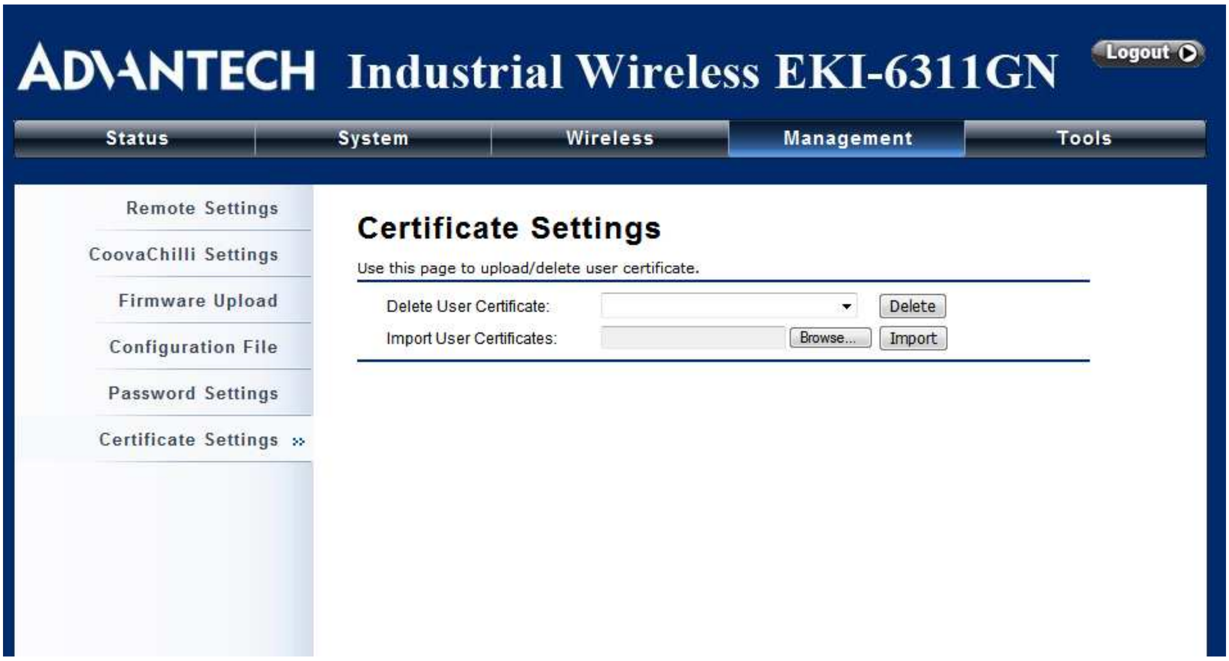
Figure 15 Password

Note:

- The password is case-sensitive and its length cannot exceed 19 characters!

Certificate Settings

Under Client mode, when EAP-TLS is used, the RADIUS server must know which user certificates to trust. The Server can trust all certificates issued by a given CA.
To import a user certificate, from Import User Certificates, click “**Browse**” and specify the location where the user certificate is placed. Click “**Import**”.



Certificate Settings

Use this page to upload/delete user certificate.

Delete User Certificate:

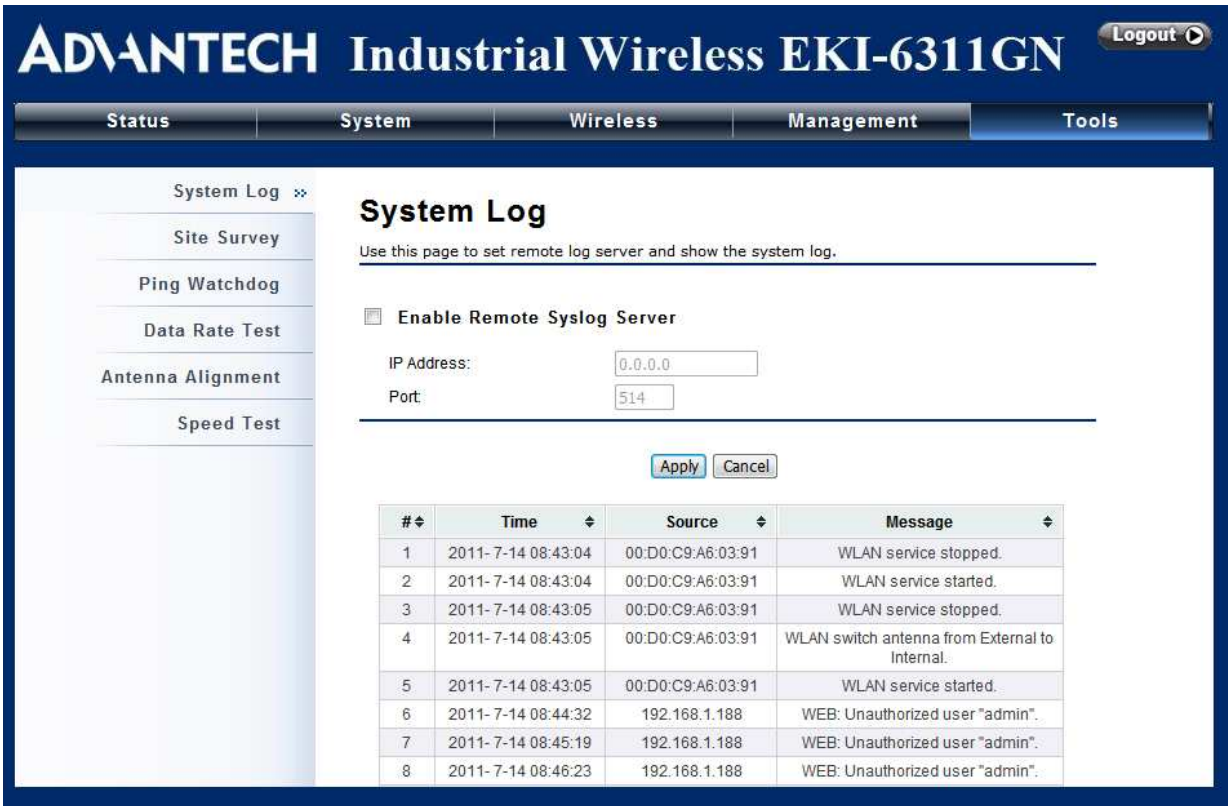
Import User Certificates:

Figure 16 Certificate Settings

Monitoring Tools

System Log

System log is used for recording events occurred on the EKI-6311GN, including station connection, disconnection, system reboot and etc.
Open “**System Log**” in “**Tools**” as below.



System Log

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

□ Enable Remote Syslog Server

IP Address: 0.0.0.0

Port: 514

#	Time	Source	Message
1	2011-7-14 08:43:04	00:D0:C9:A6:03:91	WLAN service stopped.
2	2011-7-14 08:43:04	00:D0:C9:A6:03:91	WLAN service started.
3	2011-7-14 08:43:05	00:D0:C9:A6:03:91	WLAN service stopped.
4	2011-7-14 08:43:05	00:D0:C9:A6:03:91	WLAN switch antenna from External to Internal.
5	2011-7-14 08:43:05	00:D0:C9:A6:03:91	WLAN service started.
6	2011-7-14 08:44:32	192.168.1.188	WEB: Unauthorized user "admin".
7	2011-7-14 08:45:19	192.168.1.188	WEB: Unauthorized user "admin".
8	2011-7-14 08:46:23	192.168.1.188	WEB: Unauthorized user "admin".

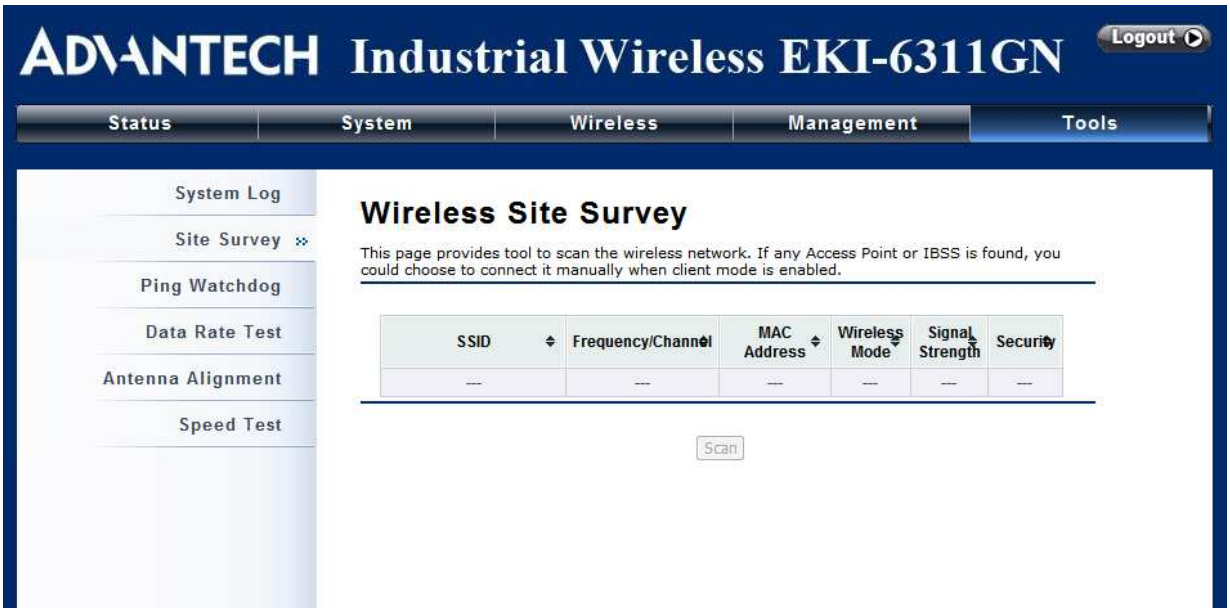
Figure 17 System Log

- **Remote Syslog Server**

  Enable Remote Syslog: Enable System log to alert remote server.
  IP Address: Specify the IP address of the remote server.
  Port: Specify the port number of the remote server.

Site Survey

Only available under Wireless Client mode, site survey allows you to scan all the APs within coverage. Open “**Site Survey**” in “**Tools**” as below and select the desired AP to connect.



Wireless Site Survey

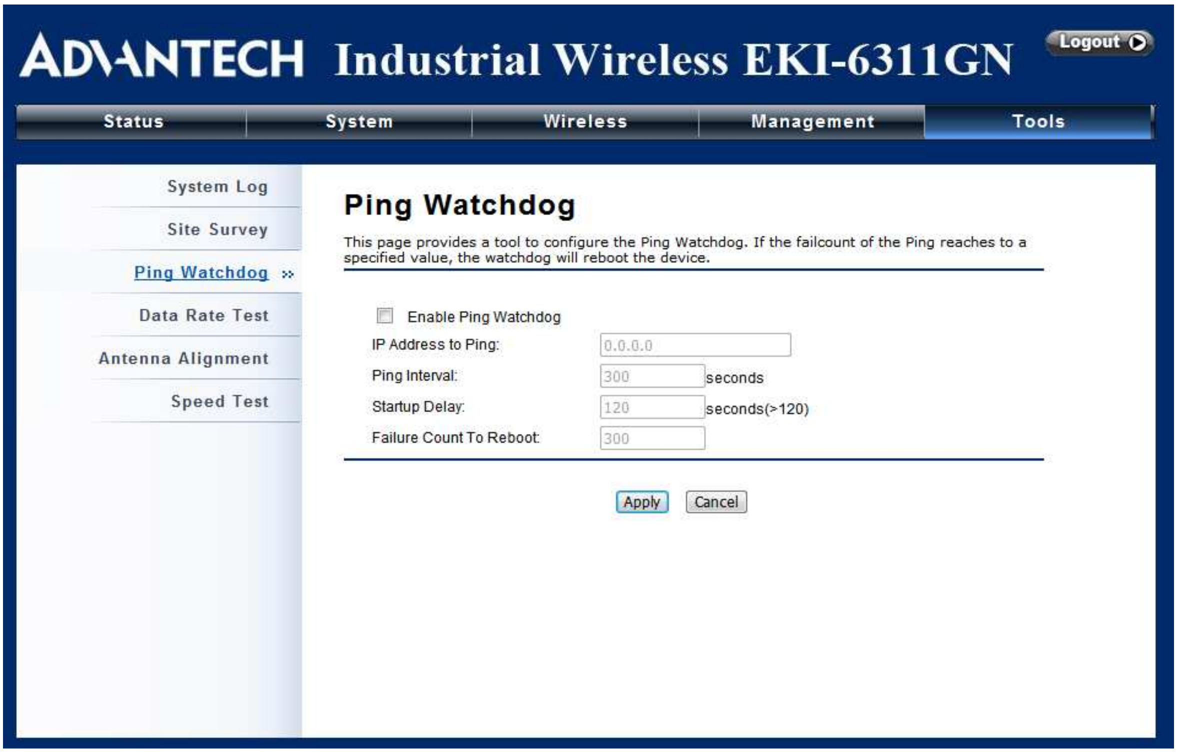
This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

SSID	Frequency/Channel	MAC Address	Wireless Mode	Signal Strength	Security
---	---	---	---	---	---

Figure 18 Site Survey

Ping Watch Dog

If you mess your connection up and cut off your ability the log in to the unit, the ping watchdog has a chance to reboot due to loss of connectivity.



Ping Watchdog

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

☐ Enable Ping Watchdog

IP Address to Ping: 0.0.0.0

Ping Interval: 300 seconds

Startup Delay: 120 seconds(>120)

Failure Count To Reboot: 300

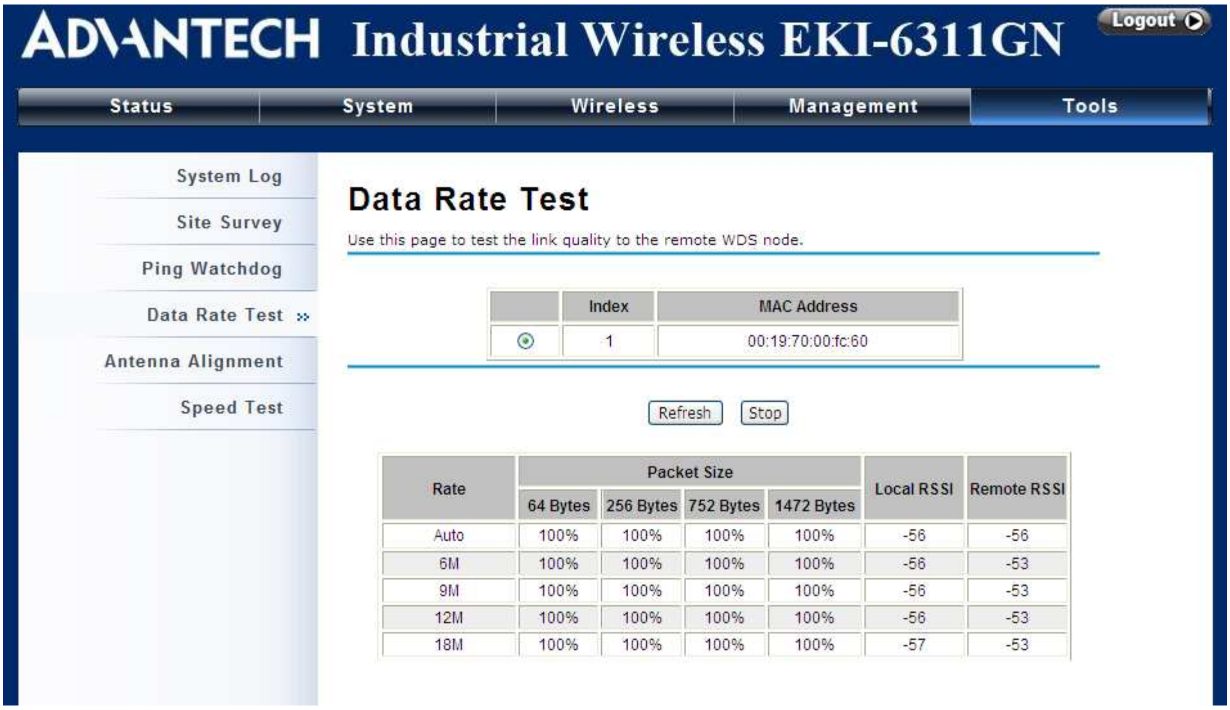
Figure 19 Ping Watchdog

- **Ping Watchdog**

Enable Ping Watchdog: To activate ping watchdog, check this checkbox.
IP Address to Ping: Specify the IP address of the remote unit to ping.
Ping Interval: Specify the interval time to ping the remote unit.
Startup Delay: Specify the startup delay time to prevent reboot before the EKI-6311GN is fully initialized.
Failure Count To Reboot: If the ping timeout packets reached the value, the EKI-6311GN will reboot automatically.

Date Rate Test

The Data Rate Test allows you test the current RSSI at each data rate between your EKI-6311GNs.



Data Rate Test

Use this page to test the link quality to the remote WDS node.

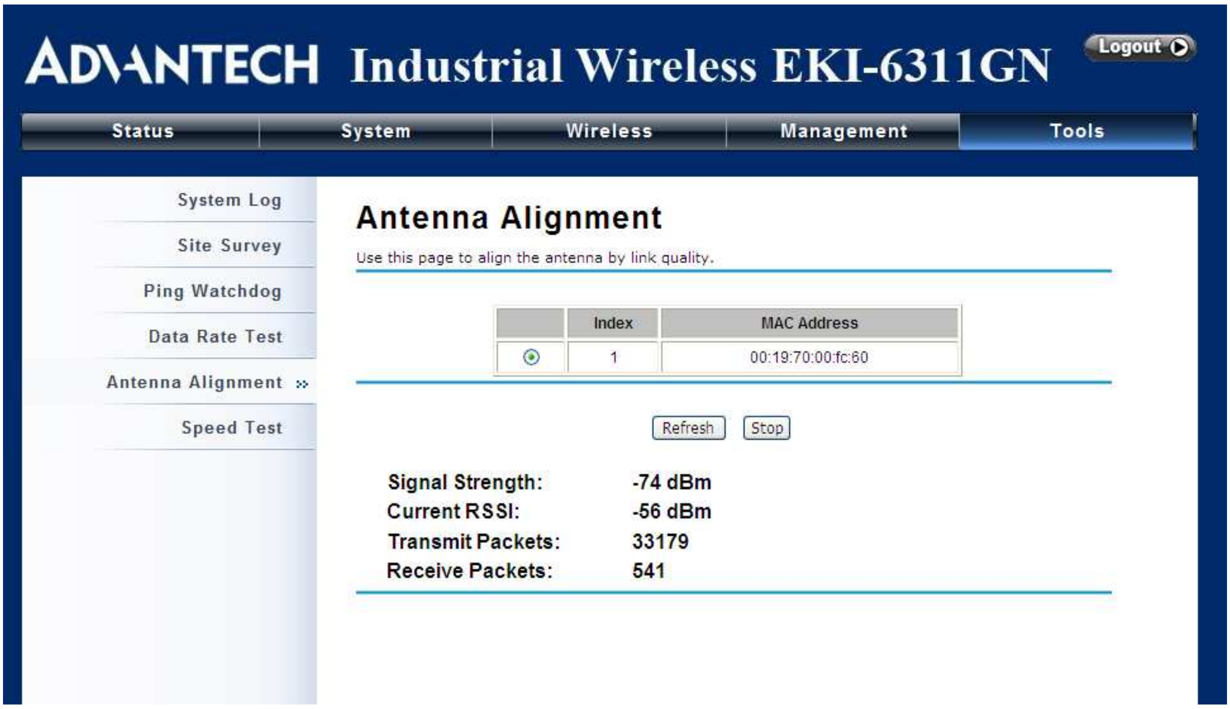
	Index	MAC Address
◉	1	00:19:70:00:fc:60

Rate	Packet Size				Local RSSI	Remote RSSI
	64 Bytes	256 Bytes	752 Bytes	1472 Bytes		
Auto	100%	100%	100%	100%	-56	-56
6M	100%	100%	100%	100%	-56	-53
9M	100%	100%	100%	100%	-56	-53
12M	100%	100%	100%	100%	-56	-53
18M	100%	100%	100%	100%	-57	-53

Figure 20 Data Rate Test

Antenna Alignment

Under Bridge mode, when the bridges are not easily visible from the location where the dish will be installed, the antenna alignment tool can help you evaluate the position of the unit and adjust the angle of the antenna more precisely. Keep it that in real circumstances a lot of additional factors should be taken into account when your unit is installed. These factors include various obstacles (buildings, trees), the landscape, the altitude, transponder orientation, polarization, etc.
To use the tool, select the desired remote WDS bridge and click “Start”, the web page will display the measured signal strength, RSSI and transmit/receive packets. If the signal quality is not quite good, try to adjust the antenna and see if the quality improves or not.



Antenna Alignment

Use this page to align the antenna by link quality.

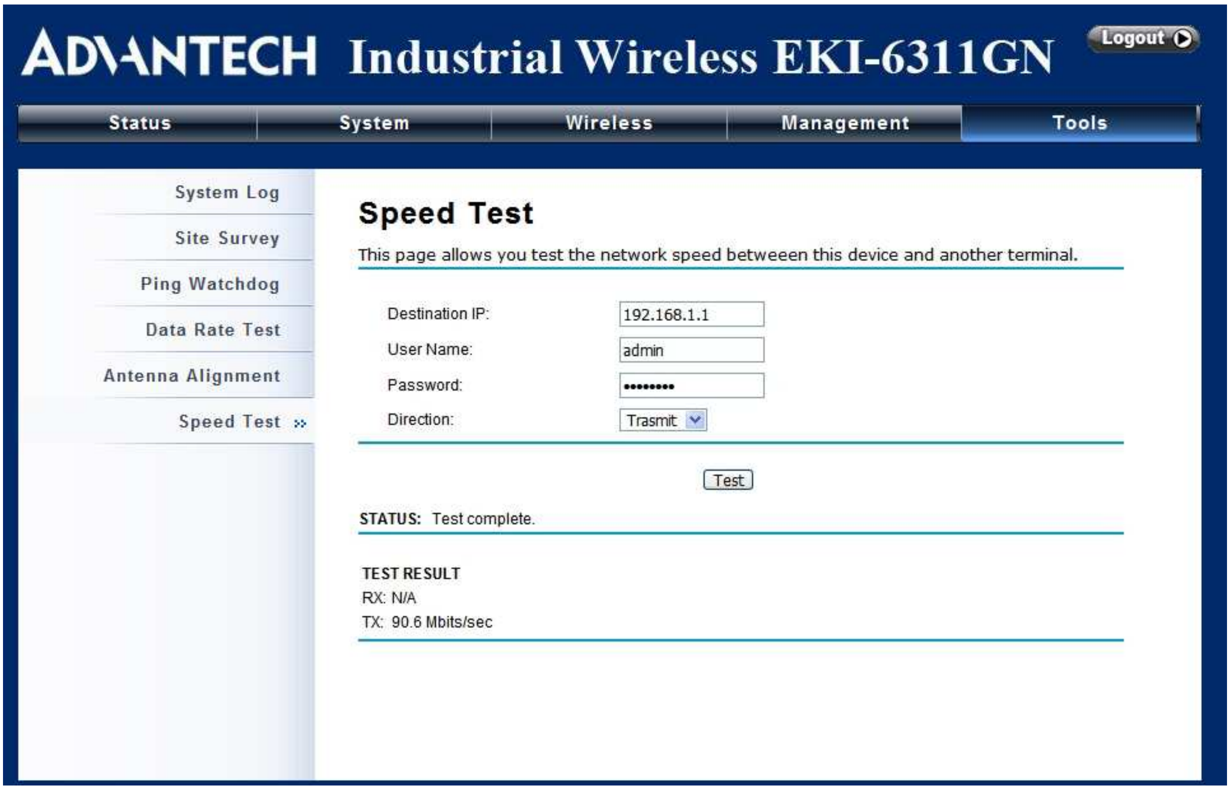
	Index	MAC Address
●	1	00:19:70:00:fc:60

Signal Strength:	-74 dBm
Current RSSI:	-56 dBm
Transmit Packets:	33179
Receive Packets:	541

Figure 21 Antenna Alignment

Speed Test

The speed test is to monitor the current data transmission (TX) and data reception (RX) rate with the remote 802.11an Wireless Outdoor CPE. Enter the IP address of the remote CPE, type in the user name/password and click "**Test**". The result will display in the bottom **STATUS**. You may test single TX/RX or bi-direction.



Speed Test

This page allows you test the network speed betweeen this device and another terminal.

Destination IP:	192.168.1.1
User Name:	admin
Password:	••••••••
Direction:	Trasmit

STATUS: Test complete.

TEST RESULT
RX: N/A
TX: 90.6 Mbits/sec

Figure 22 Speed Test

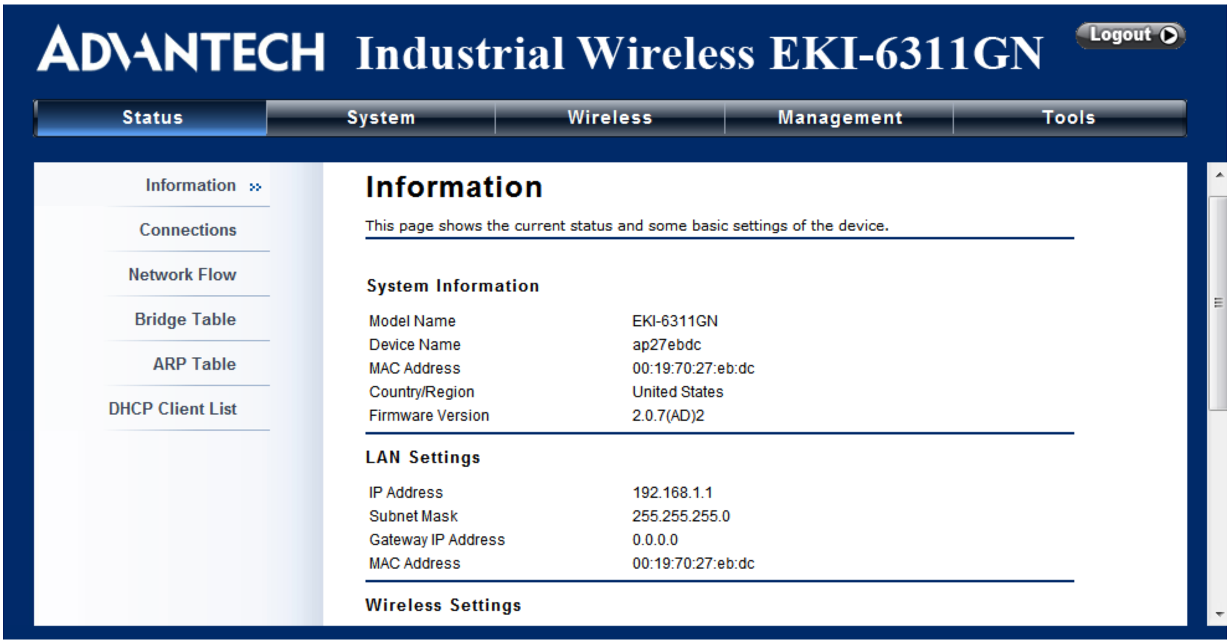
CHAPTER 6

Status

Chapter 6 Status

6.1 View EKI-6311GN Basic Information

Open “**Information**” in “**Status**” to check the basic information of EKI-6311GN, which is read only. Click “**Refresh**” at the bottom to have the real-time information.



Information

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

System Information

Model Name	EKI-6311GN
Device Name	ap27ebdc
MAC Address	00:19:70:27:eb:dc
Country/Region	United States
Firmware Version	2.0.7(AD)2

LAN Settings

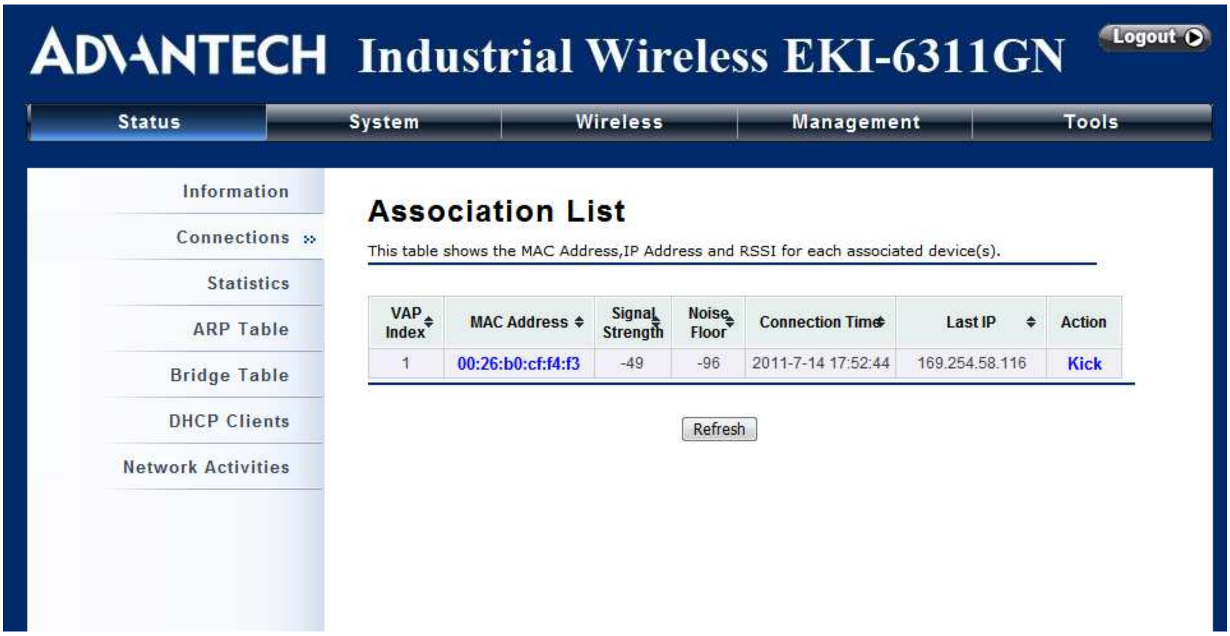
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway IP Address	0.0.0.0
MAC Address	00:19:70:27:eb:dc

Wireless Settings

Figure 50 Basic Information

6.2 View Association List

Open “**Association List**” in “**Connection**” from “**Status**” to check the information of associated wireless clients. All is read only. Click “**Refresh**” at the bottom to view the current association list.



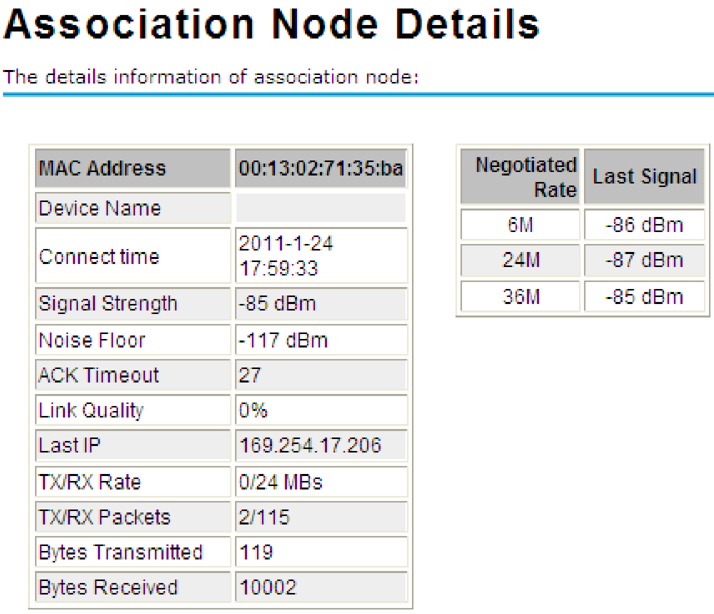
Association List

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

VAP Index	MAC Address	Signal Strength	Noise Floor	Connection Time	Last IP	Action
1	00:26:b0:cf:f4:f3	-49	-96	2011-7-14 17:52:44	169.254.58.116	Kick

Figure 51 Connection

By clicking on the MAC address of the selected device on the web you may see more details including device name, connection time, signal strength, noise floor, ACK timeout, link quality, IP information, current data rate, current TX/RX packets.



Association Node Details

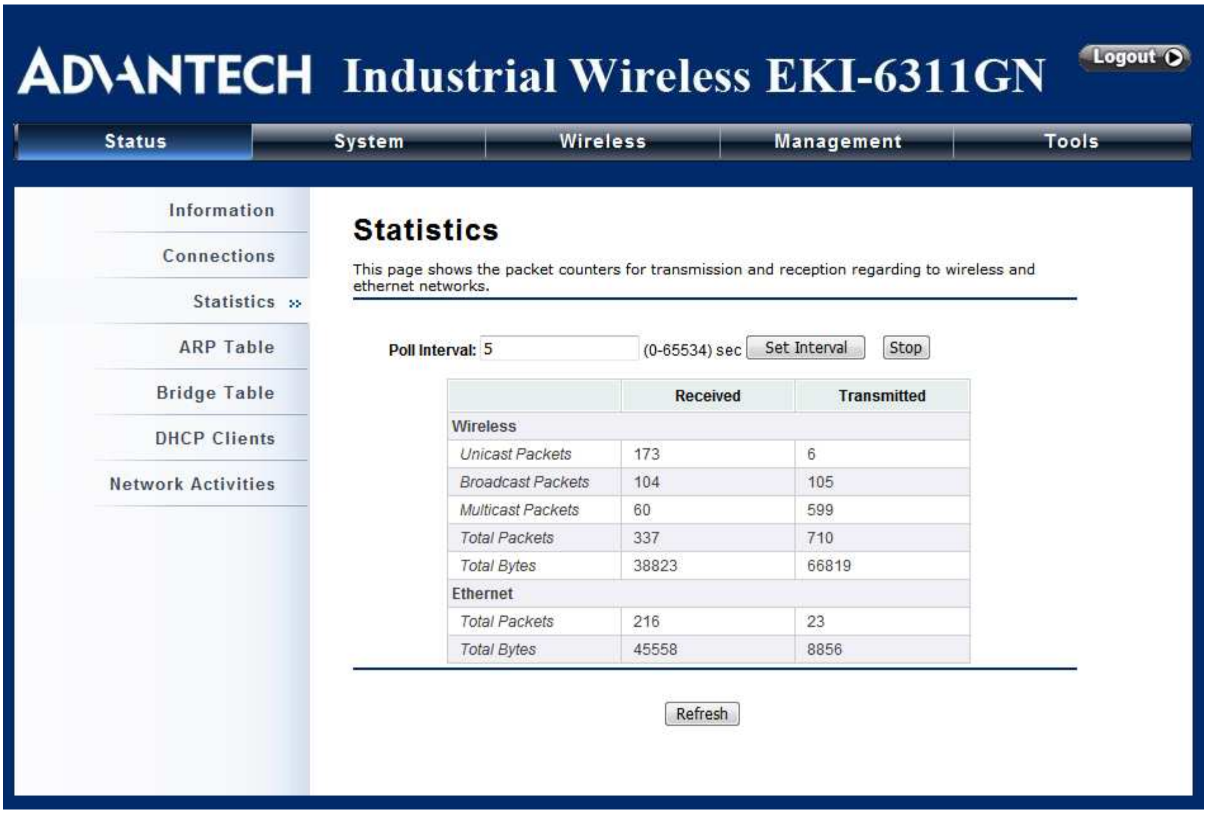
The details information of association node:

MAC Address	00:13:02:71:35:ba
Device Name	
Connect time	2011-1-24 17:59:33
Signal Strength	-85 dBm
Noise Floor	-117 dBm
ACK Timeout	27
Link Quality	0%
Last IP	169.254.17.206
TX/RX Rate	0/24 MBs
TX/RX Packets	2/115
Bytes Transmitted	119
Bytes Received	10002

Negotiated Rate	Last Signal
6M	-86 dBm
24M	-87 dBm
36M	-85 dBm

View Network Flow Statistics

Open “**Statistics**” in “**Status**” to check the data packets received on and transmitted from the wireless and Ethernet ports. Click “**Refresh**” to view current statistics.



Statistics

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

Poll Interval: 5 (0-65534) sec

	Received	Transmitted
Wireless		
Unicast Packets	173	6
Broadcast Packets	104	105
Multicast Packets	60	599
Total Packets	337	710
Total Bytes	38823	66819
Ethernet		
Total Packets	216	23
Total Bytes	45558	8856

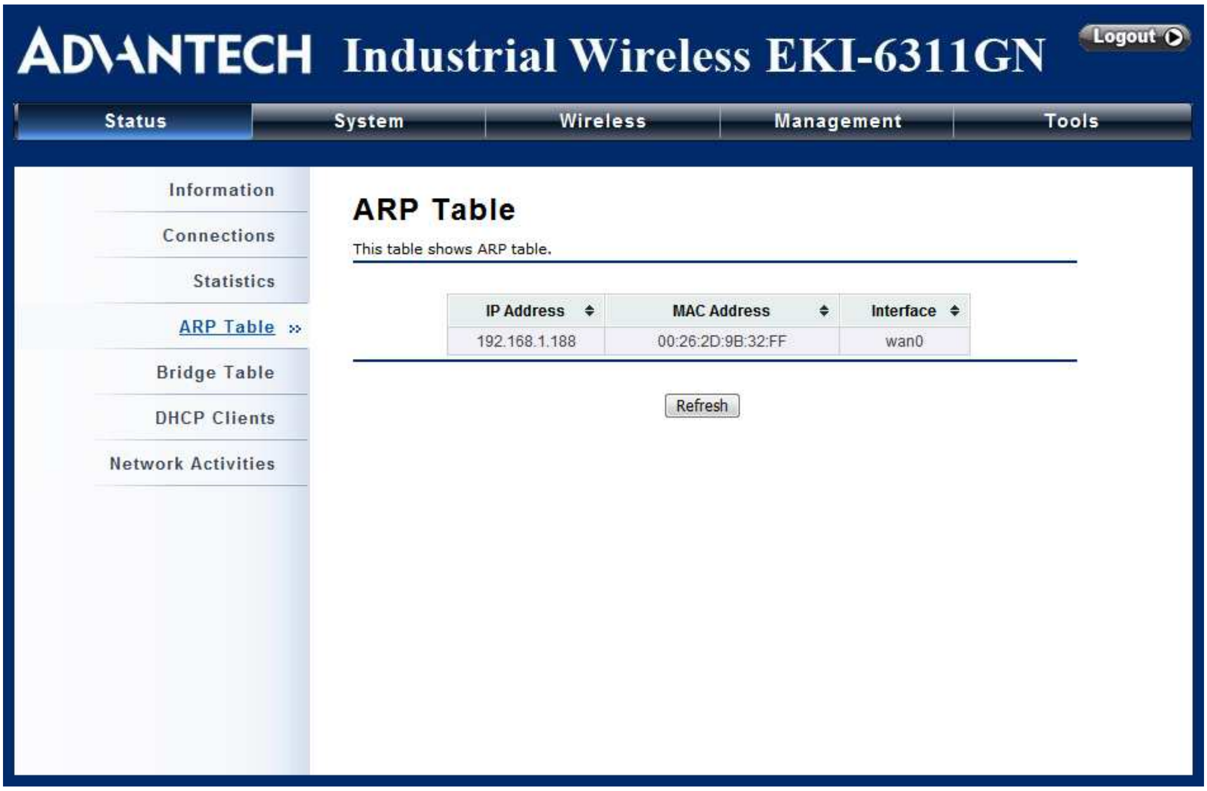
Figure 23 Network Flow Statistics

- **Poll Interval**

  Specify the refresh time interval in the box beside "**Poll Interval**" and click "**Set Interval**" to save settings. "**Stop**" helps to stop the auto refresh of network flow statistics.

View ARP Table

Open "**ARP Table**" in "**Status**" as below. Click "**Refresh**" to view current table.



ARP Table

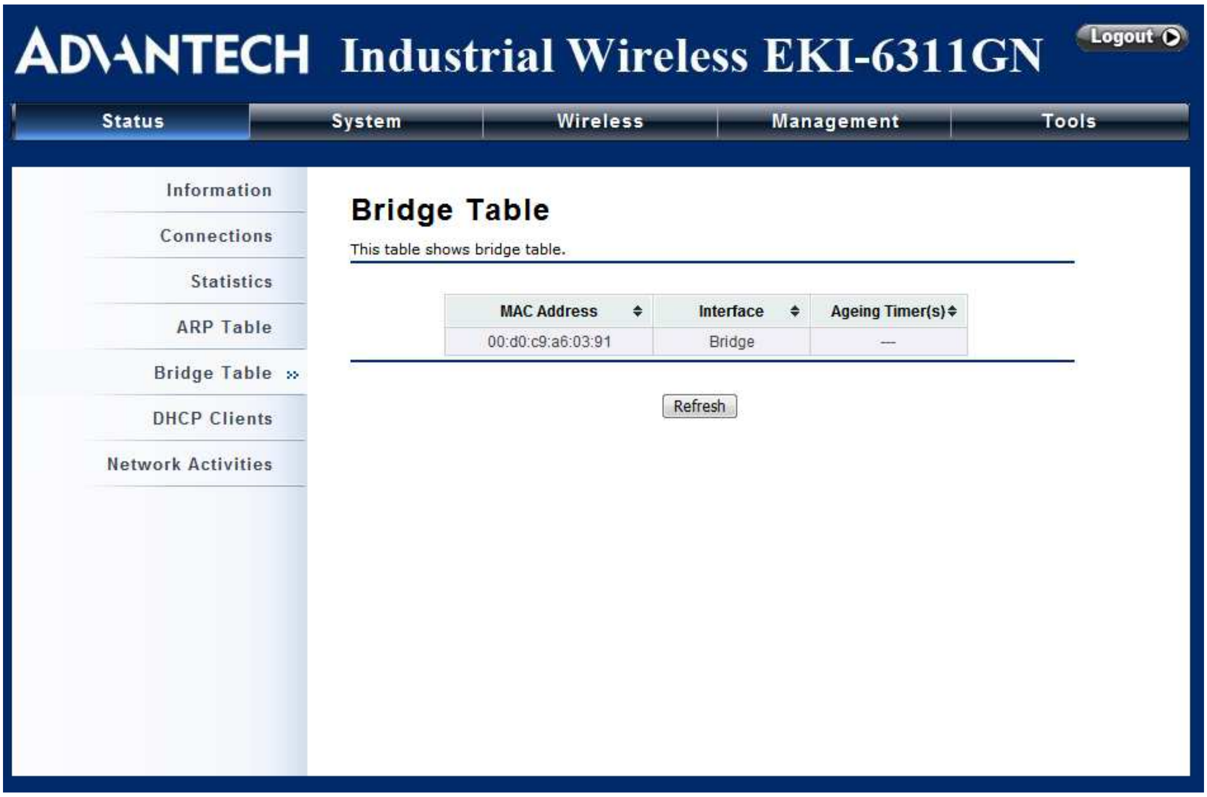
This table shows ARP table.

IP Address	MAC Address	Interface
192.168.1.188	00:26:2D:9B:32:FF	wan0

Figure 24 ARP Table

View Bridge Table

Open “**Bridge Table**” in “**Status**” as below. Click “**Refresh**” to view current connected status..



Bridge Table

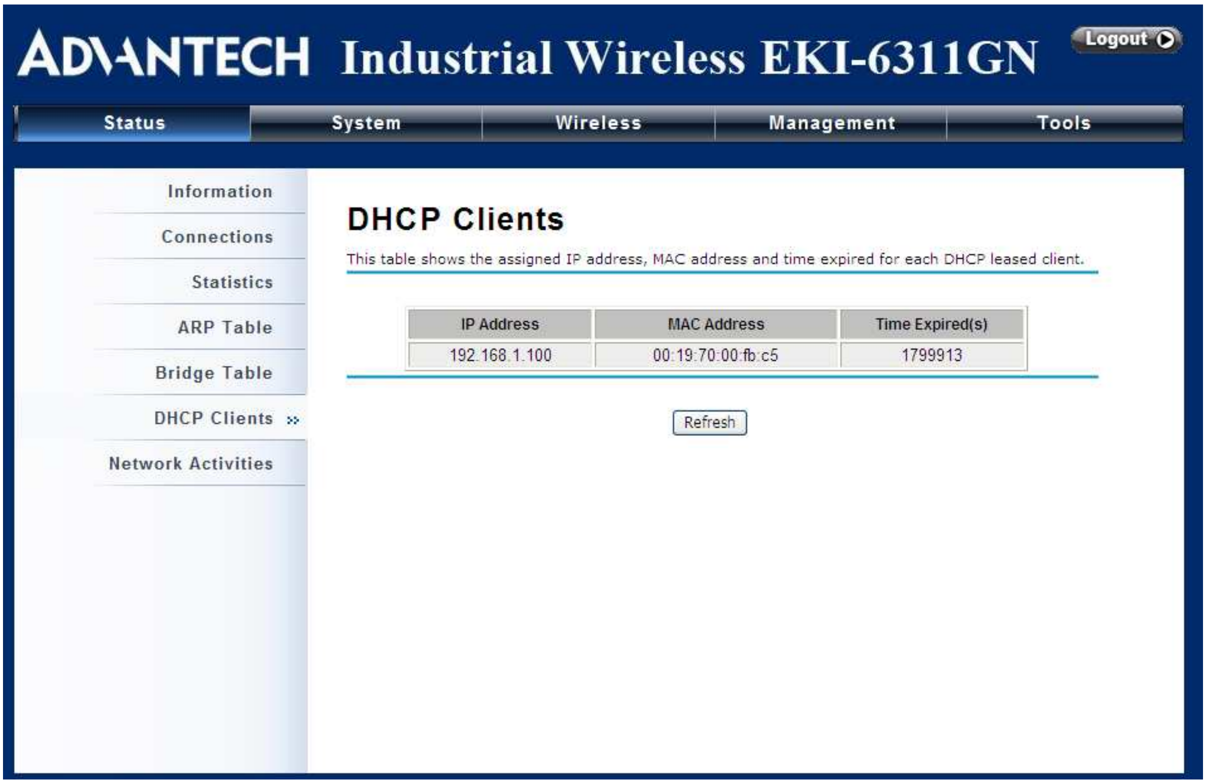
This table shows bridge table.

MAC Address	Interface	Ageing Timer(s)
00:d0:c9:a6:03:91	Bridge	---

Figure 25 Bridge Table

View Active DHCP Client Table

Open “**DHCP Clients**” in “**Status**” as below to check the assigned IP address, MAC address and time expired for each DHCP leased client. Click “**Refresh**” to view current table.



DHCP Clients

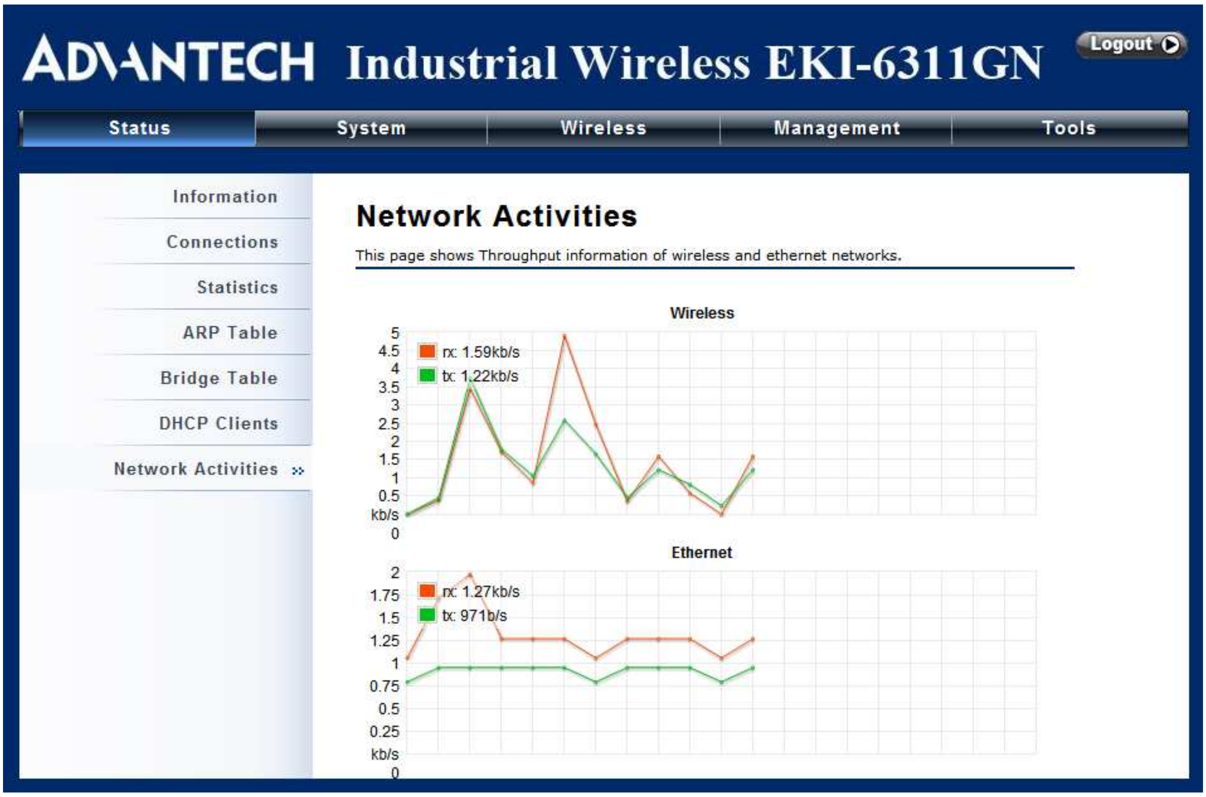
This table shows the assigned IP address, MAC address and time expired for each DHCP leased client.

IP Address	MAC Address	Time Expired(s)
192.168.1.100	00:19:70:00:fb:c5	1799913

Figure 26 DHCP Client Table

View Network Activities

The network activities allows you to monitor the current Wireless and Ethernet TX/RX data traffic in graphical and numerical form on the Web of the Skyport. The chart scale and throughput dimension (Bps, Kbps, Mbps) changes dynamically according to the mean throughput value. Throughput statistics can be updated manually using the “**Refresh***”* button.



Network Activities

This page shows Throughput information of wireless and ethernet networks.

Figure 27 Network Activities

CHAPTER 7

Trouble Shooting

Chapter 7 Trouble shooting

This chapter provides trouble shooting procedures for basic problems with the EKI-6311GN. For warranty assistance, contact your service provider or distributor for the process.

Q 1. How to know the MAC address of EKI-6311GN?

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

- Each device has a label posted with the MAC address. Please refer below.

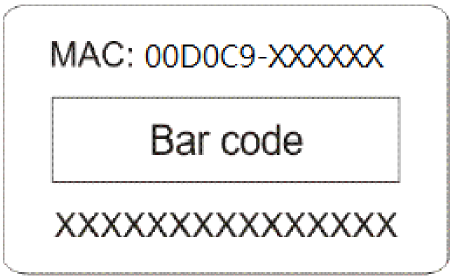


Figure 47 MAC Address

Q 2. What if I would like to reset the unit to default settings?

You may restore factory default settings in “**Configuration File**” from “**Management**”.

Q 3. What if I would like to backup and retrieve my configuration settings?

You may do the backup by generating a configuration file or retrieve the settings you have backed up previously in “**Configuration File**” from “**Management**”.

Q 4. What if I cannot access the Web-based management interface?

Please check the followings:

- Check whether the power supply is OK; Try to power on the unit again.
- Check whether the IP address of PC is correct (in the same network segment as the unit);
- Login the unit via other browsers such as Firefox.
- Hardware reset the unit.

Q 5. What if the wireless connection is not stable after associating with an AP under wireless client mode?

- Since the EKI-6311GN comes with a built-in directional antenna, it is recommended make the

EKI-6311GN face to the direction where the AP is to get the best connection quality.

- In addition, you can start “**Site Survey**” in “**Wireless Basic Settings**” to check the signal strength. If it is weak or unstable (The smaller the number is, the weaker the signal strength is.), please join other available AP for better connection.

Appendix A. ASCII

WEP can be configured with a 64-bit, 128-bit or 152-bit Shared Key (hexadecimal number or ACSII). As defined, hexadecimal number is represented by 0-9, A-F or a-f; ACSII is represented by 0-9, A-F, a-f or punctuation. Each one consists of two-digit hexadecimal.

Table 2 ACSII

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

Appendix B. SSH Settings

Table 3 CLI Commands

get	set	del	Keyword				Descriptions
√	√		time				--time setting
√				-now			--current system time
√	√			-zone			--time zone
√	√			-NTPUpdate			-- NTP Update
√	√			-servertype			--server type
√	√			-IP			-IP
√	√			-Manual IP			-Manual IP
√	√		system				--system setting
√				-swversion			--system firmware version
√	√			-systemmac			--system MAC address
√	√			-devname			--system name
√	√			-country			--country/region
	√			-ethernet1DataRate			--ether port 1 data rate
√	√			-ethernet2DataRate			--ether port 2 data rate
√	√			-macclone			--mac clone enable
√	√			-clonedmac			--cloned mac address
√	√			-poepower			--secondary RJ45 power
√	√			-stp			--Spanning Tree
√	√			-stpForwardDelay			--STP forward delay
√	√			-gpslatitude			--gps latitude
√	√			-gpslongitude			--gps longitude
√	√		ipset				
√	√			-networkmode			--network mode select (bridge or router)
√	√			-bridge			--bridge mode ip settings
√	√				-iptype		--fixed/dynamical ip(dhcp client)
√	√				-ipaddr		--ip address
√	√				-netmask		--subnet mask
√	√				-gateway		--gateway ip address
√	√				-dns1		--dns1
√	√				-dns2		--dns2
√	√			-router			--router mode ip settings
√	√				-wan		--wan ip settings
√	√					-accesstype	--router mode access type
√	√					-staticipaddr	--static ip address
√	√					-staticnetmask	--static subnet mask
√	√					-staticgateway	--static gateway ip address
√	√					-staticdns1	--static dns1
√	√					-staticdns2	--static dns2

√	√					-dhcpclienthostname	--dhcp client hostname
√						-pppoeconnectstatus	--pppoe connect status
√						-pppoelocalip	--obtains IP from pppoe server
√	√					-pppoestaticipaddr	--pppoe static ip address
√	√					-pppoeusername	--pppoe username
√	√					-pppoepassword	--pppoe password
√	√					-pppoeservername	--pppoe server name
√	√					-pppoeconnectmode	--pppoe connect mode
√	√					-pppoeidletime	--pppoe idle time
√	√				-lan		--lan ip settings
√	√					-ipaddr	--lan ip address
√	√					-netmask	--lan subnet mask
√	√					-dhcpserverenable	--dhcp server enable
√	√					-dhcpserveripstart	--dhcp server ip start
√	√					-dhcpserveripend	--dhcp server ip end
√	√					-dhcpserverleasetime	--dhcp server leasetime
√	√					-dhcprelayenable	--dhcp relay enable
√	√					-dhcpserverip	--dhcp server ip
√	√		wlan				--wlan setting
√	√			-operationmode			--operation mode
√	√			-ssid			--wireless network name
√	√			-ssidhided			--wireless SSID broadcast
√	√			-radio			--radio switch
√	√			-wirelessmode			--wireless mode
√	√						
√	√			-HTprotect			--HT protect
√	√			-frequency/channel			-wireless frequency/channel (depends on country and wireless mode)

√	√			-power			--power
√	√			-rate			--rate
√	√			-antenna			--antenna type
√	√			-antennaGain			--antenna gain setings
√	√			-wmm			--wmm settings
√	√			-Isolation			--wireless isolate communication between clients
√	√			-maxStaNum			--max sta connection number
√	√			-StaNumLmt			--Whether manually limit the number o f station
√	√			-spaceInMeter			--wireless bwa space in meter setting
√	√			-LinkIntegration			--wireless bwa coverage class setting
√	√			-channelMode			--channel mode
√	√			-channelOffset			--channel offset of 40MHz
√	√			-extension			--extension
√	√			-A-MPDU			--A-MPDU
√	√			-A-MSDU			--A-MSDU
√	√			-shortGI			--short GI
√	√			-RIFS			--rifs
√	√			-RTS			--RTS
√	√			-fragment			--fragment
√	√			-beacon			--beacon
√	√			-DTIM			--DTIM
√	√			-preamble			--preamble
√	√			-IGMP			--IGMP
√	√			-stdm			--stdm setting
√	√			-cpeType			--CPE Type
√	√			-authentication			--wireless authentication type
√	√			-encryption			--wireless data encryption
√	√	√		-key			--wireless wep key setting
√	√				-type		--wireless wep key type
√	√				-default		--wireless wep default key index
√	√	√			-1		--wireless wep key 1
√	√	√			-2		--wireless wep key 2
√	√	√			-3		--wireless wep key 3
√	√	√			-4		--wireless wep key 4
√	√	√		-wpa			--wireless WPA setting
√	√	√			-psk		--wireless pre-shared key (PSK) for WPA-PSK
√	√				-reauthtime		--wireless WPA re-auth period (in seconds)
√	√				-keyupdate		--enable wireless WPA global key update
√	√	√		-eap			--WPA EAP setting
√	√	√			-eaptype		--WPA EAP Type
√	√	√			-innereapty		--WPA inner EAP Type

					pe		
√	√				-username		--WPA user name
√	√				-loginname		--WPA login name
√	√				-password		--WPA password
√	√				-usercert		--WPA cert file
√	√				-privatekeyp assword		--WPA private key password
√	√			-trafficshaping			--traffic shaping
√	√				-enable		--enable Traffic Shaping
√	√				-downlimit		--Incoming Traffic Limit
√	√				-downburst		--Incoming Traffic Burst
√	√				-uplimit		--Outgoing Traffic Limit
√	√				-upburst		--Outgoing Traffic Burst
√	√			-wdsMac			--WDS Remote Mac
√					-local		--local macAddr
√	√				-remote1		--remote macAddr1
√	√				-remote2		--remote macAddr2
√	√				-remote3		--remote macAddr3
√	√				-remote4		--remote macAddr4
√	√			-wdsSeparation			--WDS Separation
√				-association			--list of associated wireless clients
√	√		vapprofile 1(2, 3,etc)				--VAP setting
√	√			-active			--on/off this vap
√	√			-profileName			--Name of profile
√	√			-ssid			--ssid of this vap
√	√			-ssidhided			--Broadcast SSID Enable or Disable
√	√			-vlanID			--vlanID of this vap
√	√			-Isolation			--wireless separation
√	√			-wmm			--WMM Support
√	√			-MaxStaNum			--Max Station Number
√	√			-StaNumLmt			--Whether manually limit the number o f station
√	√			-authentication			--wireless authentication type
√	√			-encryption			--wireless data encryption
√	√			-default			--wireless wep default key index
√	√			-wpa			--wireless WPA setting
√				-association			--list of associated wireless clients
√	√		vlan				--vlan setting
√	√			-active			--enable 802.1Q VLAN
√	√			-manageID			--Management VLAN ID
√	√		radius				--radius setting
√	√			-IPaddr			--IP address
√	√			-port			--port
	√			-shared secret			--Shared Secret
√	√		firewall				--firewall setting
√	√			-srcipfilter			--source ip filter settings

√	√				-enable		--source ip filter enable
√	√				-addrule		--add a source ip filter rule
	√				-delerule		--delete source ip filter rule
√					-rulelist		--show source ip filter rule lists
√	√			-destipfilter			--destination ip filter settings
√	√				-enable		--destination ip filter enable
√	√				-addrule		--add a destination ip filter rule
	√				-delerule		--delete destination ip filter rule
√					-rulelist		--show destination ip filter rule lists
√	√			-srcportfilter			--source port filter settings
√	√				-enable		--source port filter enable
√	√				-addrule		--add a source port filter rule
	√				-delerule		--delete source port filter rule
√					-rulelist		--show source port filter rule lists
√	√			-destportfilter			--destination port filter settings
√	√				-enable		--destination port filter enable
√	√				-addrule		--add a destination port filter rule
	√				-delerule		--delete destination port filter rule
√					-rulelist		--show destination port filter rule lists
√	√			-portforward			--port forward settings
√	√				-enable		--port forward enable
√	√				-addrule		--add a port forward rule
	√				-delerule		--delete port forward rule
√					-rulelist		--show port forward rule lists
√	√			-dmzenable			--dmz enable
√	√			-dmzipaddr			--dmz ip address
√	√		remote				--remote management setting
√	√			-privacy			--radius IP address
√	√			-telnet			--enable telnet
√	√			-snmp			--enable snmp
√	√			-ftp			--enable ftp
√	√			-ssh			--enable ssh
√	√			-forcehttps			--force https
√	√			-wise			--enable wise tools
√	√		snmp				--SNMP setting
√	√			-version			--Protocol Version
√	√			-port			--Server Port
√	√			-getCommunity			--SNMP Read Community
√	√			-setCommunity			--SNMP Write Community

√	√			-trapdestination			--Trap Destination
√	√			-trapcommunity			--Trap Community
√	√			-v3Admin			--v3Admin
√	√				-on		--Enable SNMPv3Admin
√	√				-name		--name
	√				-password		--password
√	√				-accessType		--access type
√	√				-authentication		--Authentication Protocol
√	√				-Privacy		--privacy protocol
√	√			-v3User			-v3User
√	√				-on		--Enable SNMPv3User
√	√				-name		--name
	√				-password		--password
√	√				-accessType		--access type
√	√				-authentication		--Authentication Protocol
√	√				-Privacy		--privacy protocol
√	√		coovachilli				--CoovaChilli setting
√	√			-coovaChilliEnable			--Coovachilli Enable
√	√			-primaryRadiusServer			--Primary RADIUS Server
√	√			-secondaryRadiusServer			--Secondary RADIUS Server
√	√			-radiusAuthPort			--RADIUS Authentication Port
√	√			-radiusAcctPort			--RADIUS Accounting Port
√	√			-radiusSharedSecret			--RADIUS Shared Secret
√	√			-radiusNasid			--RADIUS Nasid
√	√			-radiusAdminUsername			--RADIUS Admin Username
√	√			-radiusAdminPassword			--RADIUS Admin Password
√	√			-uamPortalUrl			--UAM Portal URL
√	√			-uamSecret			--UAM Secret
√	√		syslog				--syslog
√	√			-client			--enable syslog client
√	√			-ipaddr			--syslog server IP address
√	√			-port			--syslog server port number
	√			-clear			--syslog clear
√	√		pingwdg				--ping watchdog
√	√			-enable			--enable
√	√			-interval			--interval
√	√			-startdelay			--startup delay
√	√			-failcount			--failure count

√	√			-ip			--ip address
√	√	√	acl				--access control
√	√			-mode			--enable wireless access control (ACL)
		√		-delete			--delete a local ACL address
√		√		-list			--delete or display all local ACL address
	√			-MacAddr			--add mac address to Current Access Control List
√			statistics				--statistics
√				-Wireless			--Wireless LAN
√				-Ethernet			--Ethernet LAN
√		√	log list				--syslog list
	√		password				--system password
	√		reset				--restore factory
	√		reboot				--reboot system
	√		exit				--logout from CLI

Appendix C. GPL Declamation

PUBLIC SOFTWARE DECLAMATION

In the software we delivered, there may contains some public software, if it is, please read below carefully:

1. Definition

"**Public Software**", when applicable, shall mean that portion of the Licensed Software, in source code form, set forth in the below Table, and provided under the terms set forth in the Section 5, the indicated website, the complete license terms can be found.

"Public Software" shall mean each of:

(a) any computer code that contains, or is derived in any manner (in whole or in part) from, any computer code that is distributed as open source software (e.g. Linux) or similar licensing or distribution models; and

(b) any software that requires as a condition of use, modification and/or distribution of such software that such software or other software incorporated into, derived from or distributed with such software (i) be disclosed or distributed in source code form, (ii) be licensed for the purpose of making derivative works, or (iii) be redistributable at no charge.

Public Software includes, without limitation, software licensed or distributed under any of the following licenses or distribution models, or licenses or distribution models similar to any of the following: (1) GNU's General Public License (GPL) or Lesser/Library GPL (LGPL); (2) the Artistic License (e.g., PERL); (3) the Mozilla Public License; (4) the Netscape Public License; (5) the Sun Community Source License (SCSL); (6) the Sun Industry Source License (SISL); and (7) the Apache Software license.

2. Limited Use

Any Public Software provided under the agreement shall be subject to the licenses, terms and conditions of its model. Licensee hereby agrees to comply with the terms and conditions applicable to any such Public Software, as set forth in its presentation on website.

3. Limited Liability

The supplier hereby express that the supplier shall have no liability for any costs, loss or damages resulting from Licensee's breach of the terms and conditions applicable to use, conversion or combination of the licensed software with or into Public Software.

4. NO WARRANTY

This program or licensed software is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY. THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH LICENSEE.

5. Public Software Name and Description

Table 4 Public Software Name and Description

Program Name	Copy Right Description	Origin Sour Code	Licenses or Distribution Models or its special license terms	License Terms Website Reference
Redboot	Copyright (C) 1998, 1999, 2000, 2001, 2002, 2003 Red Hat, Inc.	ftp://ftp.ges.redhat.com/private/gnupro-xscale-030422/redboot-intel-xscale-030630.tar.Z	eCos License	http://sources.redhat.com/ecos/ecos-license/
Busybox		http://www.busybox.net/downloads/busybox-1.01.tar.bz2	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
brctl	Copyright (C) 2000 Lennert Buytenhek	http://nchc.dl.sourceforge.net/sourceforge/bridge/bridge-utils-1.0.6.tar.gz	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
dropbear	Copyright (c) 2002-2006 Matt Johnston Portions copyright (c) 2004 Mihnea Stoenescu	http://matt.ucc.asn.au/dropbear/dropbear-0.51.tar.bz2	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
hostapd	Copyright (c) 2002-2006, Jouni Malinen <jkmaline@cc.hut.fi> and contributors	http://hostap.epitest.fi/releases/hostapd-0.4.8.tar.gz	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
wpa_supplicant	Copyright (c) 2003-2005, Jouni Malinen <jkmaline@cc.hut.fi> and contributors	http://hostap.epitest.fi/releases/wpa_supplicant-0.4.7.tar.gz	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
mtdutil		ftp://ftp.uk.linux.org/pub/people/dwmw2/mtd/cvs/mtd/util/	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
ntpclient	Copyright 1997, 1999, 2000, 2003 Larry Doolittle	http://doolittle.icarus.com/ntpclient/ntpclient_2003_1	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html

		94.tar.gz		
procps	Author: Albert Cahalan, Michael K. Johnson, Jim Warner, etc.	http://procps.sourceforge.net/procps-3.2.7.tar.gz	GNU GENERAL PUBLIC LICENSE Version 2 GNU LIBRARY GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html http://www.gnu.org/licenses/old-licenses/library.html
vsftpd	Author: Chris Evans	ftp://vsftpd.beasts.org/users/cevans/vsftpd-1.1.2.tar.gz	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
linux		ftp://ftp.kernel.org/pub/linux/kernel/v2.6/linux-2.6.20.3.tar.bz2	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html