IEEE 802.11a/n Wireless Access

Point/ Client Bridge

User Manual

Copyright

Acknowledgements

Intel and Pentium are trademarks of Intel Corporation.
Microsoft Windows and MS-DOS are registered trademarks of Microsoft Corp.
All other product names or trademarks are properties of their respective owners.

Product Warranty (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 Introduction

Introduction

EKI-6331AN is a feature rich wireless AP/ CPE which provides a reliable 5GHz 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-6331AN provides 3 times higher data rates than legacy 802.11a devices. With 2X2 MIMO technology, EKI-6331AN provides both robust wireless connectivity as well as high throughput rate in wireless transmission. With the support of WMM and IGMP snooping protocols, EKI-6331AN effectively improves the reliability of wireless connectivity, especially in applications that need high reliability and high throughput data transmission. To secure wireless connections, EKI-6331AN implements the latest encryption technologies including WPA2/WPA/802.1x for powerful security authentication.

Appearance

Figure 1 IEEE 802.11a/n Wireless Access Point/ Client Bridge

Key Features

- Compliant with IEEE802.11a/n
- IP55 waterproof certification
- MIMO 2 x 2 11n
- Embedded 16dBi dual-polarity directional antenna with external R-SMA connector for optional antenna
- Passive PoE
- WEP/WPA/WPA2/ IEEE 802.1 x authentication support
- IGMP snooping protocol support

Specification

Standard Support

- **Wireless** IEEE802.11a/n
- **Ethernet** IEEE802.3u MDI / MDIX 10/100 Fast Ethernet
- **LAN** IEEE802.11a/n wireless LAN interface
  Passive PoE, max. distance: 50 meters
- **Certifications**
  US FCC Part 15 Class B & C
  Europe ETSI 300 893, ETSI 301 489-1&17
  EN 60950 compliant and CE Mark
- **Data Rates**
  802.11a 54, 48, 36, 24, 18, 12, 9, 6 Mbps, auto-fallback
  802.11n:
  MCS0 - MCS15 (6.5 Mbps to 300 Mbps)

Physical Specifications

- **Power** AC Adapter 100V~240V
- **Dimensions (L x W x H)** 111 x 256 x 48 mm
- **Weight** 600g

Wireless Interface Operation Modes

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

- Bridge (WDS)
- AP repeater

Antenna

- Default embedded 2T2R 16dBi dual-polarity directional antenna
- Reverse SMA Connector x 2 for external antennas *Switchable by software

Modulation Techniques

- **802.11a** OFDM
- **802.11n** OFDM (BPSK, QPSK, 16-QAM, 64-QAM)

Support Frequency

- **FCC :** 5725-5850
- **CE:** 5470-5725 MHz (DFS band)

Wireless Tx power and Rx Sensitivity

- **Transmitted Power**
    - 802.11a: 24dBm @ 6Mbps, 21dBm @ 54Mbps
    - 802.11an HT20: 23dBm @ MCS0/8, 20dBm@ MCS7/15
    - 802.11an HT40: 20dBm @ MCS0/8, 19dBm@ MCS7/15

Receiver Sensitivity

- **802.11a Sensitivity** -89dBm @ 6Mbps; -73dBm @ 54Mbps
- **802.11n HT20** -89dBm @ MCS0; -71dBm @ MCS7; -65dBm @ MCS15
- **802.11n HT40** -85dBm @ MCS0; -67dBm @ MCS7; -61dBm @ MCS15

Typical Application

This section describes the typical applications of the IEEE 802.11a/n Wireless Access Point/ Client Bridge. By default, it is set to AP mode which allows it to establish a wireless coverage; besides, it is also able to join any available wireless network under wireless client mode. It is also able to deliver stable and efficient broadband connectivity for various applications.

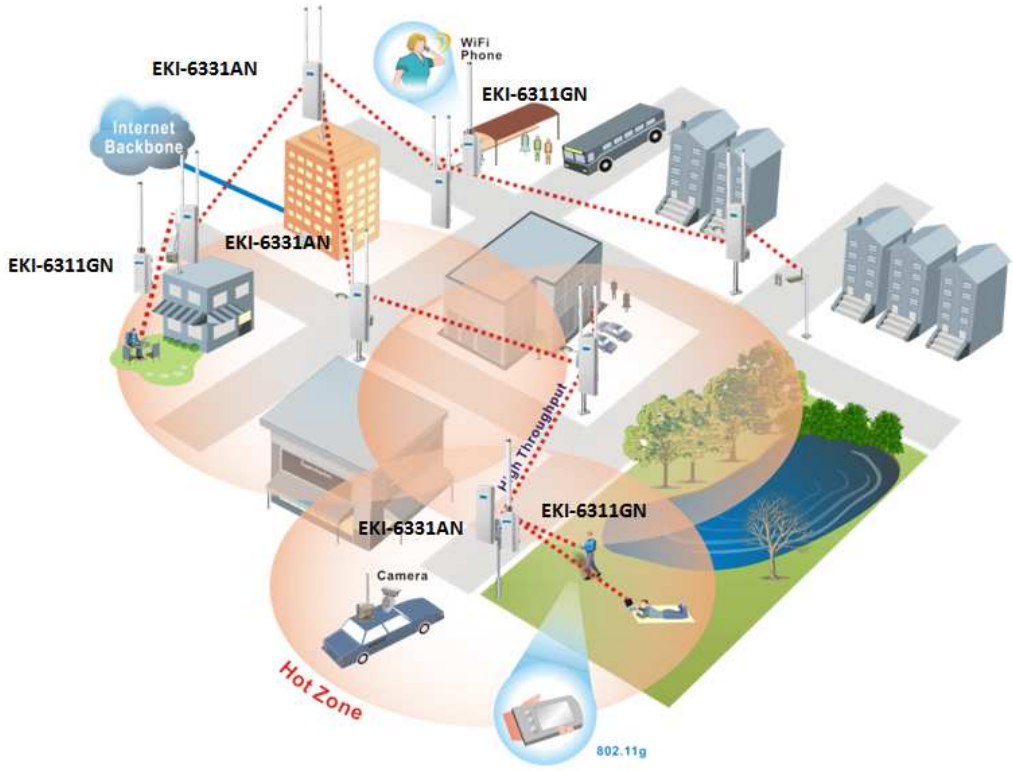


Figure 2 Typical Application

Chapter 2 Hardware Installation

This chapter describes safety precautions and product information you have to know and check before installing EKI-6331AN.

Preparation before Installation

Professional Installation Required

Please have EKI-6331AN installed by 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. When installing EKI-6331AN in outdoor environment, please note the following things:
   - Do not use a metal ladder;
   - Try to avoid the installation on a wet or windy day;
   - Wear shoes with rubber soles and heels, rubber gloves, long sleeved shirt or jacket.
3. When the system is operational, avoid standing directly in front of it. Strong RF fields are present when the transmitter is on.

Installation Precautions

To have EKI-6331AN functioning well in outdoor environment, please read and follow these installation precautions while you are installing.

1. Users MUST use a proper and well-installed grounding and surge arrestor with EKI-6331AN; otherwise, lightening could easily cause fatal damage to the unit. **EMD (Lightning) DAMAGE IS NOT COVERED UNDER WARRNTY.**
2. Users MUST use the “Power cord & POE Injector” shipped in the box with EKI-6331AN. Use of other options may cause damage to the unit.
3. Users MUST power off EKI-6331AN 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 EKI-6331AN; otherwise, damage might be caused to the device itself.

Product Package

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

- EKI-6331AN ×1
- Pole Mounting Ring ×2
- Power Cord & POE Injector ×1
- Start up manual ×1
- User’s manual CD ×1

Pole Mounting Ring

Power Cord & POE Injector

Start up manual & User's manual CD

Warning:

- Users MUST use the "Power cord & POE Injector" shipped in the box with EKI-6331AN. Use of other options will likely cause damage to the unit.

Hardware Installation

Connect up

1. The bottom of EKI-6331AN is a movable cover. Loosen the screw with a screwdriver. Grab the cover and pull it back harder to take it out as the figure shown below.

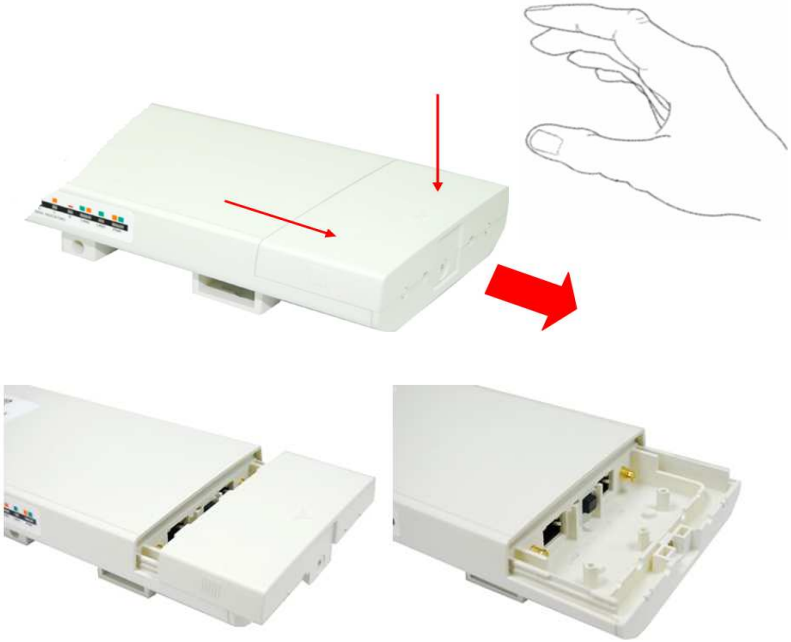
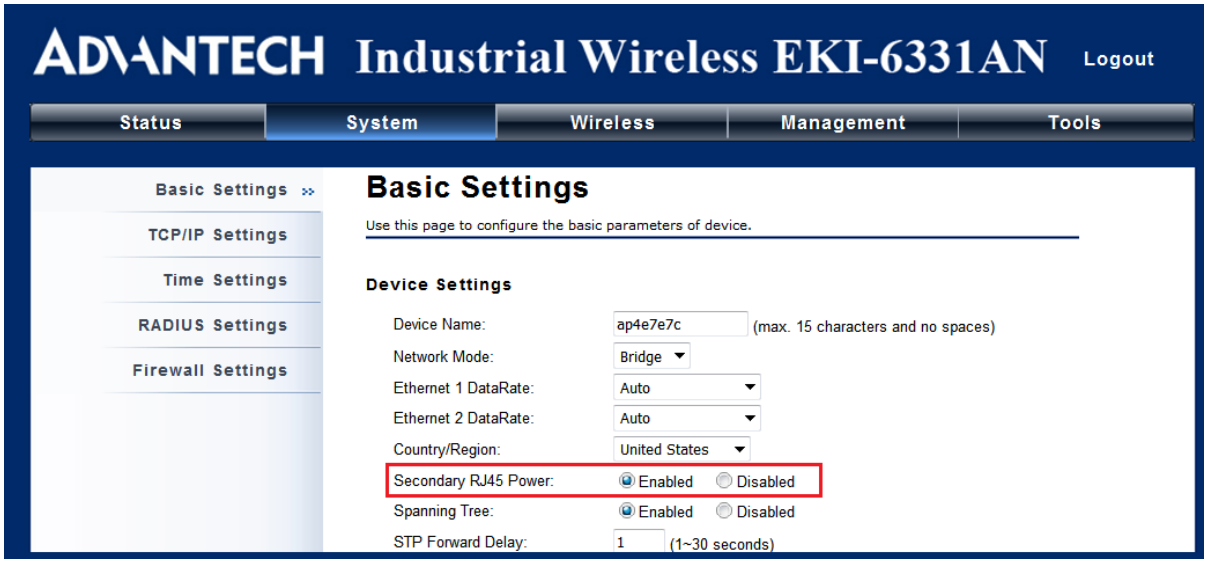


Figure 3 Move the Cover

2. Plug a standard Ethernet cable into the RJ45 port labeled “LAN 1”. Do not plug the cable into the RJ45 port labeled “LAN 2”.

Figure 4 Cable Connection

The secondary Ethernet port (labeled LAN 2) is for EKI-6311GN or IP camera integration. To use it you need to enable the secondary port in advance before connecting with the EKI-6311GN or IP camera from EKI-6331AN Web Management as shown below.



3. Take out the power cord and POE injector from the gift box, and plug the power cord into the DC port of the POE injector as the below picture shows.

Figure 5 Connect to POE Injector

4. Put what in the Step.2 and Step.3 together by plugging the other side of the Ethernet cable in the Step.2 into the POE port of the POE injector in the Step.3. When you finish the Step.4, the set will be like the following picture:

Figure 6 Plug the Ethernet cable to the RJ-45 jack of the injector

5. Press the black PWR button beside the LAN 1 Ethernet port.

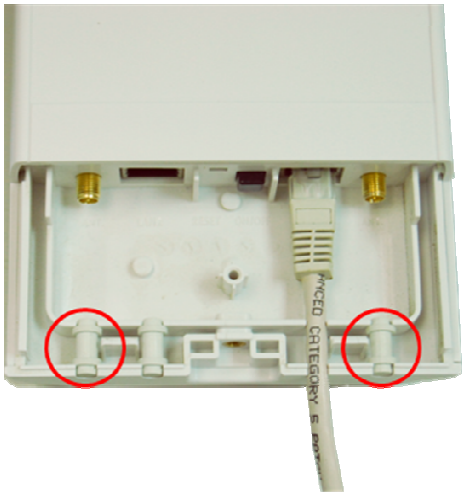
6. Attach and fasten the removable cover to the bottom of the unit with the screw.

7. Power on EKI-6331AN by plugging the power adapter to the power socket.

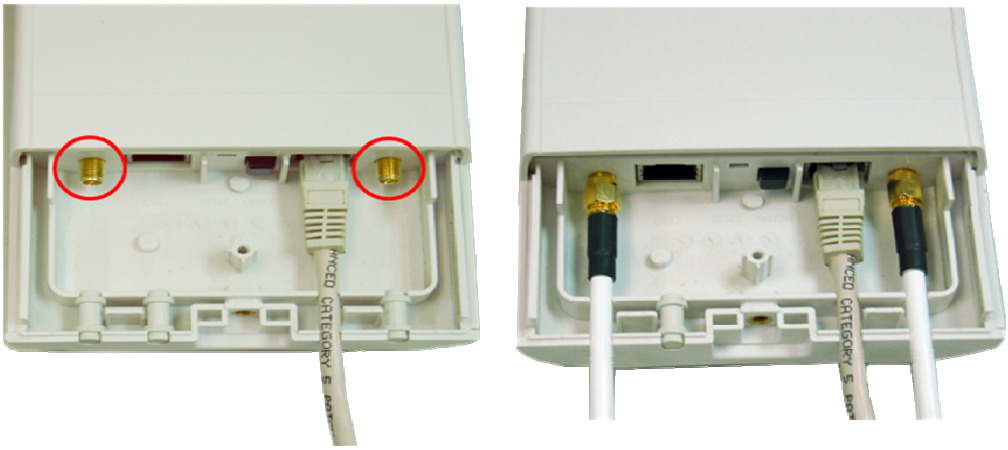
Using the External Antenna

EKI-6331AN provides two reverse SMA antenna connectors if you prefer to use the external antenna for your application instead of the built-in directional antenna, please follow the steps below.

1. Remove the two plugs as circled below:



2. Connect your external antenna to the SMA-type connectors at the bottom of the EKI-6331AN.



Warning:

- Users MUST power off the EKI-6331AN 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 EKI-6331AN; otherwise, damage might be caused to the unit itself.

Follow the steps described in **Connect Up** to finish the installation.

Pole Mounting

1. Turn EKI-6331AN over. Put the pole mounting rings through the middle hole of it. Note that you should unlock the pole mounting ring with a screw driver before putting it through EKI-6331AN as the following right picture shows.

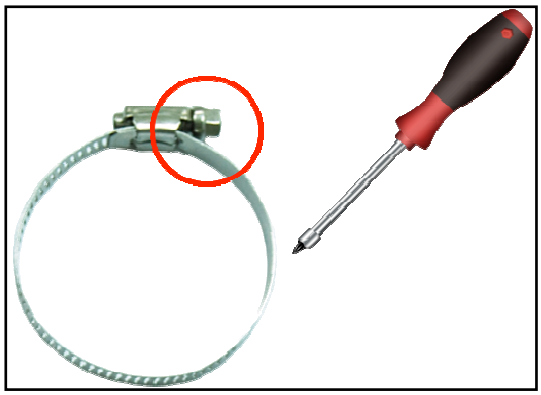


Figure 7 Pole Mounting – Step 1

2. Mount EKI-6331AN steadily to the pole by locking the pole mounting ring tightly. The mounting ring supports pole diameter 32mm to 70mm.

Figure 8 Pole Mounting – Step 2

3. Now you have completed the hardware installation of the EKI-6331AN.

Chapter 3 Basic Settings

Factory Default Settings

The following table shows EKI-6331AN factory default settings. You can re-acquire these parameters by default. If necessary, please refer to the "Restore Factory Default Settings".

Table 1 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		802.11a/n
Country/Region		United States
Channel Number		149
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

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-6331AN 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.

How to Login the Web-based Interface

EKI-6331AN provides you with user-friendly Web-based management tool.

- Open Web browser and enter the IP address (Default: **192.168.1.1**) of EKI-6331AN into the address field. You will see the login page as below.

Figure 9 Login Page

- Enter the username (Default: **admin**) and password (Default: **password**) respectively and click "**Login**" to login the main page of EKI-6331AN. As you can see, this management interface provides 5 main options in the black bar above, which are **Status**, **System**, **Wireless**, **Management** and **Tools**.

Figure 10 Main Page

Note:

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

Basic System Settings

For users who use EKI-6331AN for the first time, it is recommended that you begin configuration from "**Basic Settings**" in "**System**" shown below:

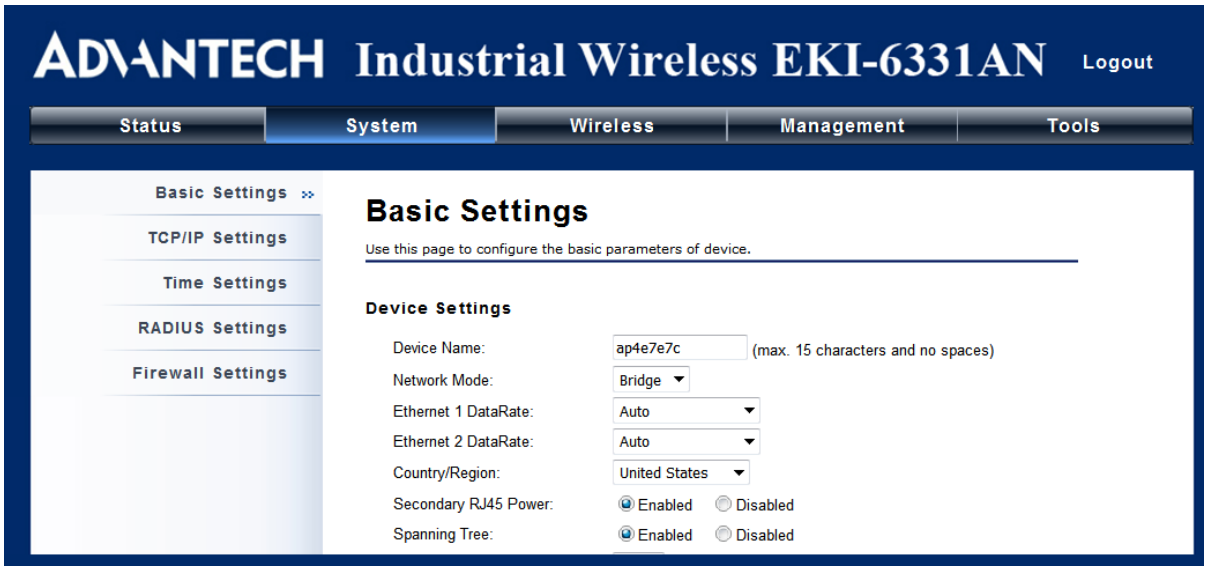


Figure 11 Basic System Settings

- **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.

  Ethernet 1 Data Rate: Specify the transmission rate of data of LAN1. Default is **Auto**.

  Ethernet 2 Data Rate: Specify the transmission rate of data of LAN2. Default is **Auto**.

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

  Secondary RJ45 Power: The secondary Ethernet port (labeled LAN 2) is for IP video integration. To use it you need to enable the secondary port via WEB UI in advance before connecting with the IP camera.

  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-6331AN. 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 EKI-6331AN. In this page, users may change the settings for IP Address, Subnet Mask, and DHCP Server.

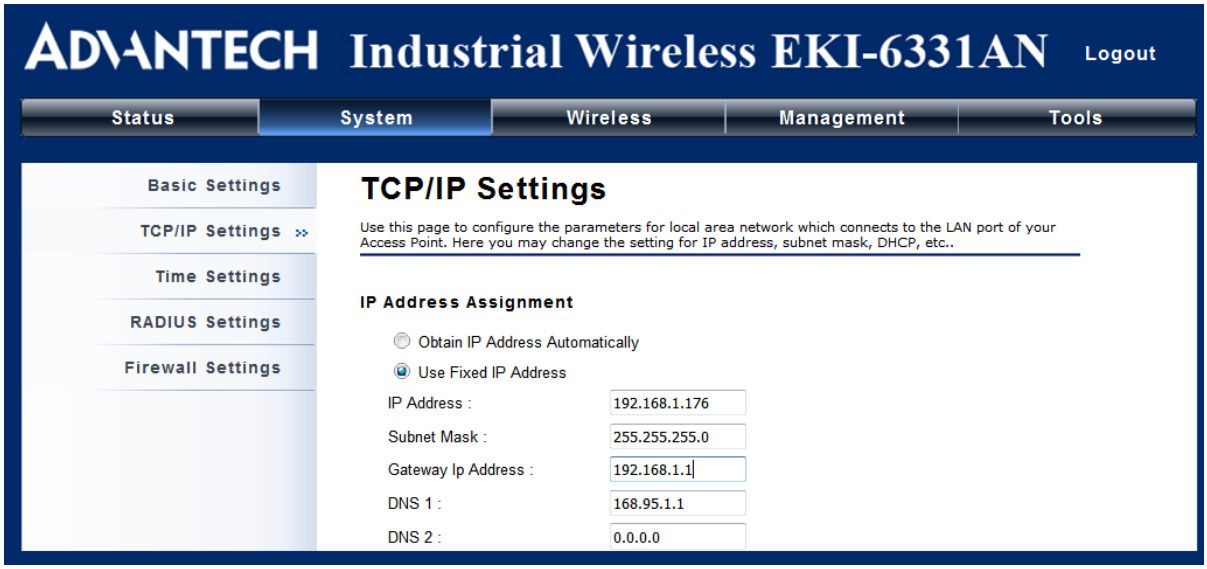


Figure 12 TCP/IP Settings (Bridge)

Obtain IP Address Automatically: If a DHCP server exists in your network, you can check this option, thus EKI-6331AN is able to obtain IP settings automatically from that DHCP server.

Note:

- When the IP address of EKI-6331AN 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 EKI-6331AN to access its Web Management page.
- In case the EKI-6331AN 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 EKI-6331AN manually. Make sure the specified IP address is unique on your network in order to prevent IP conflict.

If EKI-6331AN is configured as Router mode, you need to configure some additional TCP/IP parameters for accessing the Internet.

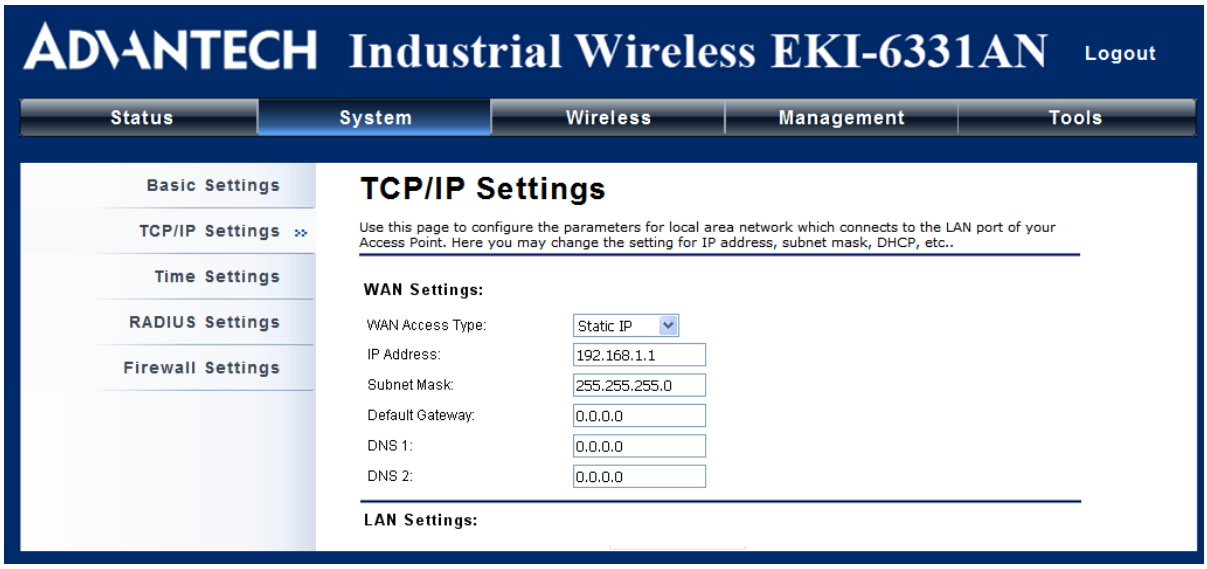


Figure 13 TCP/IP Settings (Router)

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 EKI-6331AN 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, EKI-6331AN 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 EKI-6331AN.

- In wireless client mode, users can access EKI-6331AN 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 EKI-6331AN with another wireless device before it is set to Router mode and access EKI-6331AN via the connected wireless device.

Time Settings

Compliant with NTP, EKI-6331AN 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.

Figure 14 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 Server**" dropdown list or manually input the IP address of available time server into "**Manual IP**". (For example, 192.43.244.18 for NIST server.)

  Hit "**Apply**" to save settings.

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.

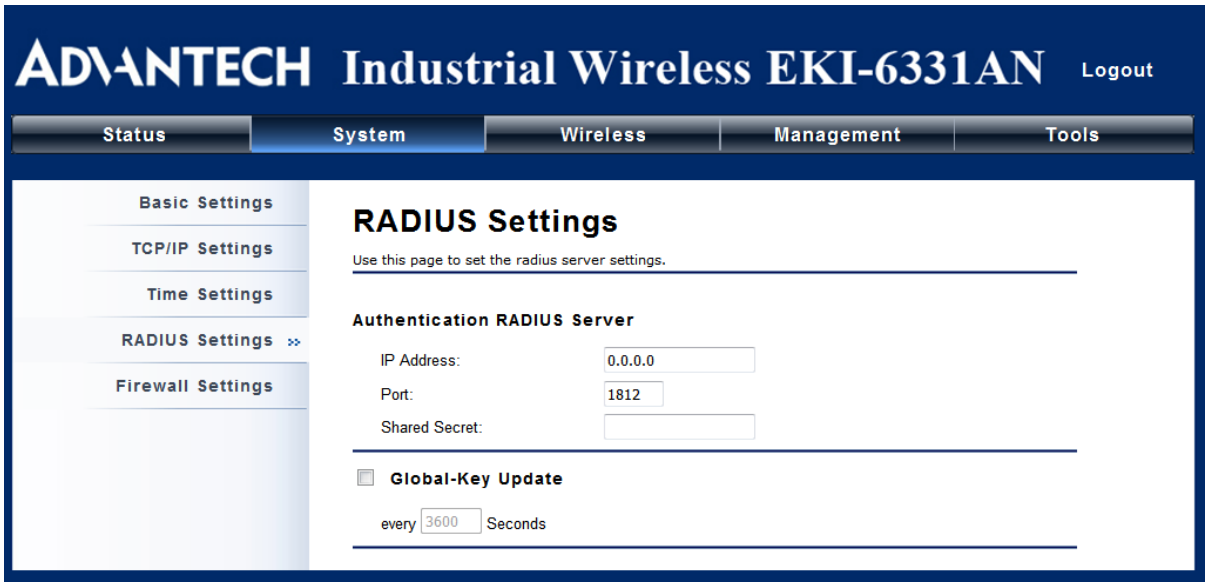


Figure 15 RADIUS Settings

- **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 AP and RADIUS during authentication.

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

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-6331AN 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-6331AN. Use of such filters can be helpful in securing or restricting your local network.

Figure 16 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 Destination IP Filtering**" checkbox and enter the IP address of the clients to be restricted. Hit **Apply** to make the setting take effect.

Figure 17 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-6331AN. Use of such filters can be helpful in securing or restricting your local network.

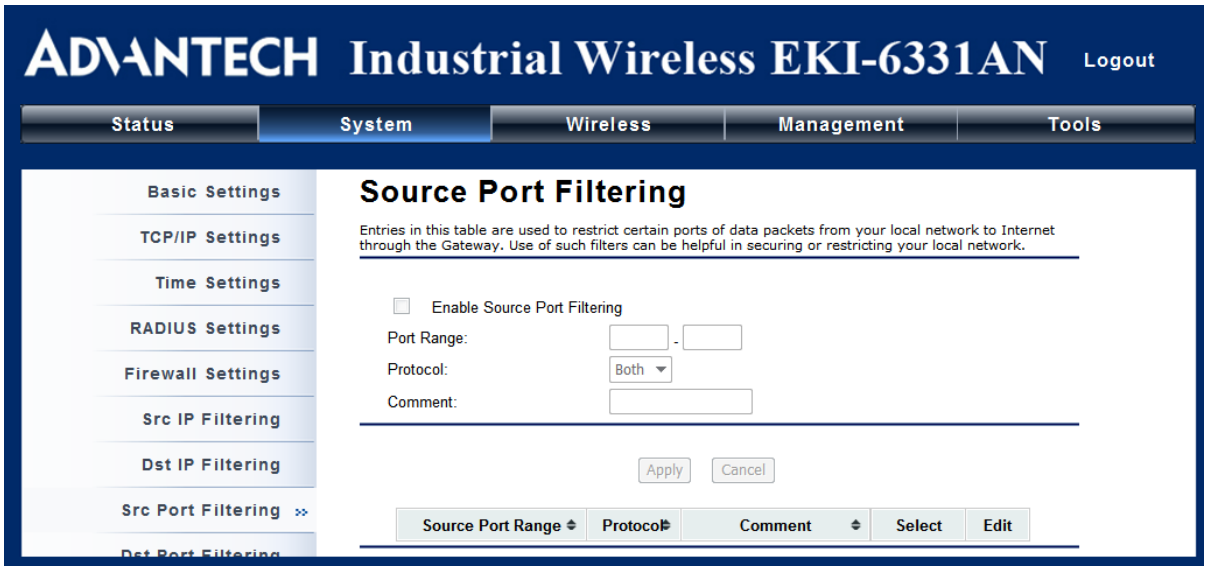


Figure 18 Source Port Filtering

Destination Port Filtering: The destination port filtering enables you to restrict certain ports of data packets from your local network to Internet through EKI-6331AN. Use of such filters can be helpful in securing or restricting your local network.

Figure 19 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 the router's NAT firewall.

Figure 20 Port Forwarding

DMZ: A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to the Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

Figure 21 DMZ Settings

Basic Wireless Settings

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

Figure 22 Basic Wireless Settings

- **Disable Wireless LAN Interface**

  Check this option to disable WLAN interface, then the wireless module of EKI-6331AN will stop working and no wireless device can connect to it.

- **Wireless Mode**

  Four operating modes are available on EKI-6331AN.

  AP: EKI-6331AN establishes a wireless coverage and receives connectivity from other wireless devices.

  Wireless Client: EKI-6331AN is able to connect to the AP and thus join the wireless network around it.

  Bridge: EKI-6331AN establishes wireless connectivity with other EKI-6331AN by keying in remote MAC address. Please refer to the "**WDS Setting**" for detailed configuration.

  AP Repeater: EKI-6331AN servers as AP and Bridge concurrently. In other words, it can provide connectivity services for EKI-6331AN 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 cannot exceed 32 characters.

- **802.11 Mode**

  EKI-6331AN can communicate with wireless devices of 802.11n or 802.11a/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 EKI-6331AN to use two channels at once. Two options are available: Upper Channel and Lower Channel.

- **Channel Mode**

  4 levels are available: 40MHz, 20MHz, 10MHz and 5MHz. 40MHz can enhance data throughput, but it takes more bandwidth, thus it might cause potential interference.

- **Antenna**

  By default, EKI-6331AN 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 (16 dBi)" to "SMA Connector".

  When **SMA Connector** 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.

Warning:

- You are able to choose "SMA Connector" only from the WEB UI after you have physically installed the external antenna; otherwise, it might damage the unit itself.

- **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.

Note:

- The output power here is counted from the RF single chain only not including the 16dBi internal antenna.
- The maximum output power will vary depending on the country selected in order to comply with the local regulation.
- You are able to choose "SMA Connector" only when you have well done installing the external antenna; otherwise, it might damage EKI-6331AN itself.

- **Data Rate**

  Usually "**Auto**" is preferred. Under this rate, EKI-6331AN 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 legacy devices 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 in wireless client mode, it hides the MAC address of EKI-6331AN while displays the one of associated wireless client or the MAC address designated manually.

Site Survey

Under wireless client mode, EKI-6331AN 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 wireless networks around. Select the AP you would like to connect and click "**Selected**" to establish connection.

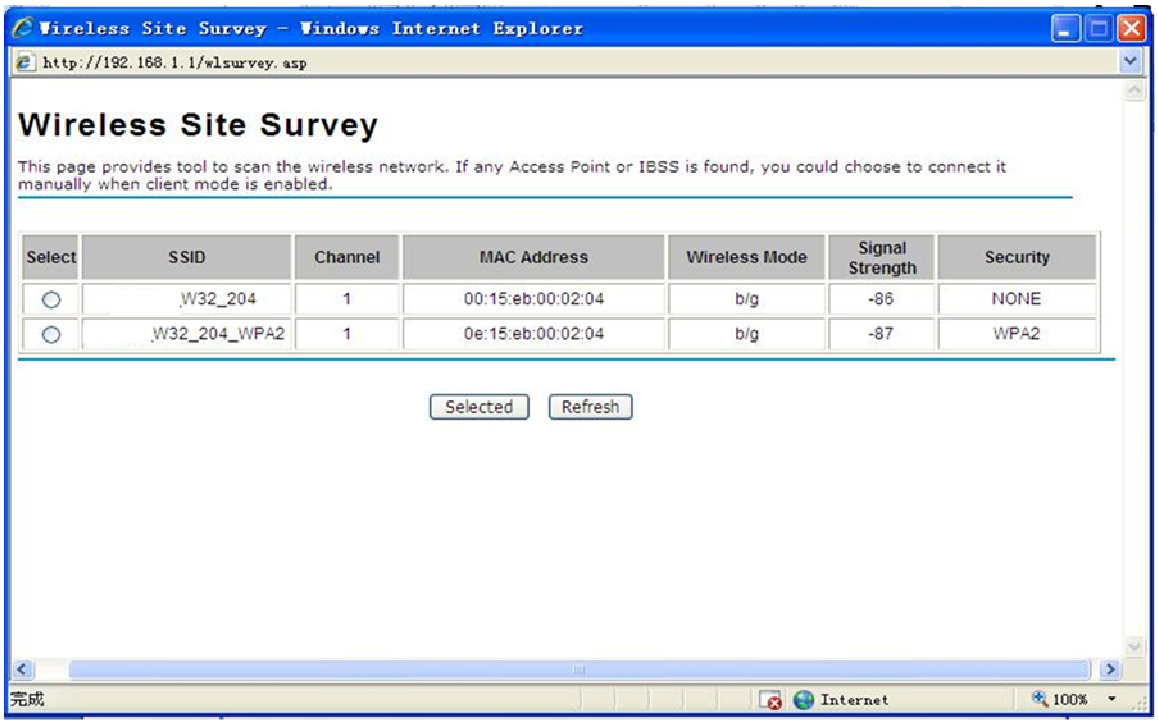


Figure 23 Site Survey

VAP Profile Settings

Available in AP mode, EKI-6331AN 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.

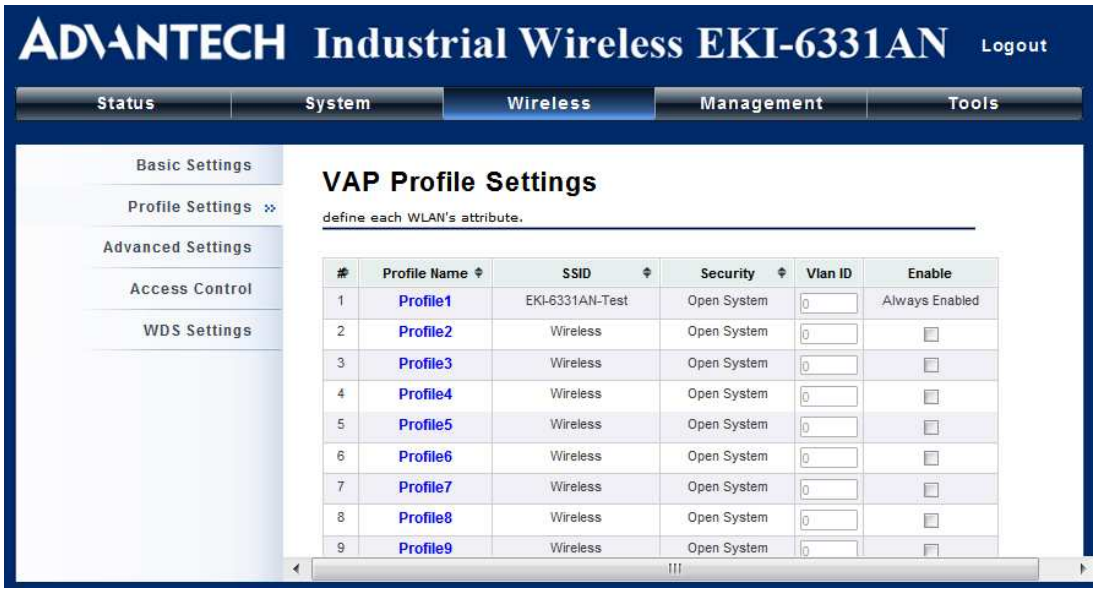


Figure 24 VAP Profile Settings

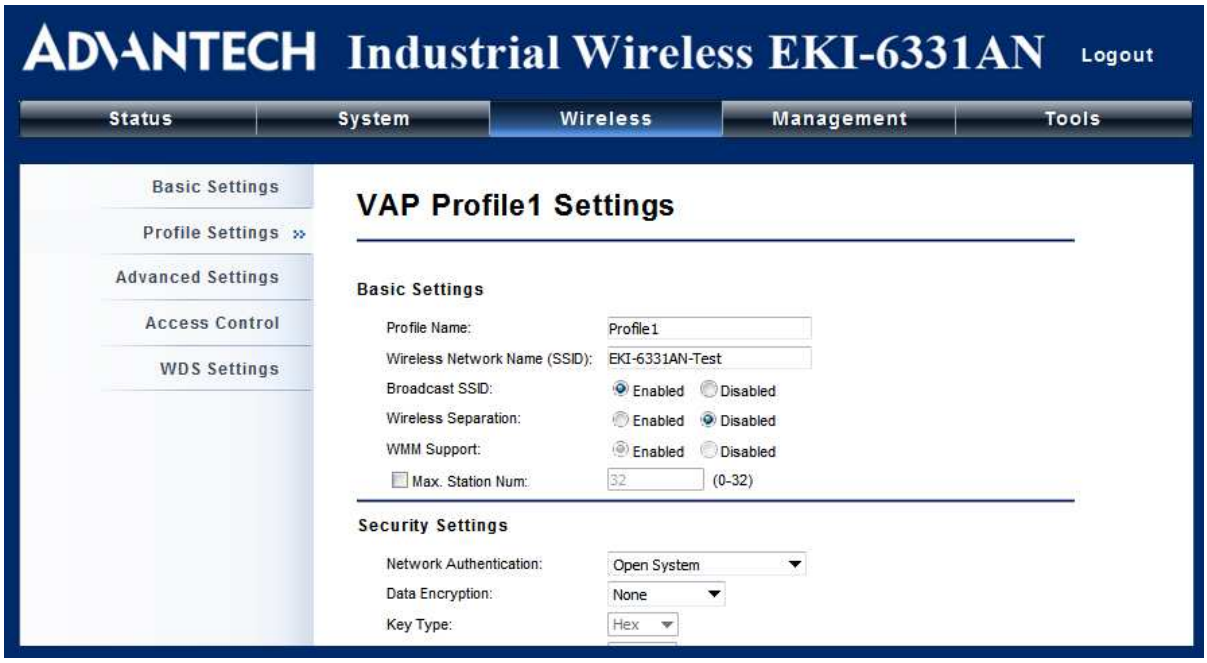


Figure 25 VAP Profile Settings

- **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 EKI-6331AN, 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**" EKI-6331AN will allow up to 32 wireless clients to associate with. By disabling the checkbox EKI-6331AN 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, EKI-6331AN 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 EKI-6331AN, 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 EKI-6331AN.

Figure 26 Management VLAN ID

Chapter 4 Advanced Settings

Advanced Wireless Settings

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

Figure 27 Advanced Wireless Settings

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

  The data rate of your EKI-6331AN 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**

  EKI-6331AN 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.

- **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, EKI-6331AN 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.

Wireless Security Settings

To prevent unauthorized radios from accessing data transmitting over the connectivity, EKI-6331AN 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.

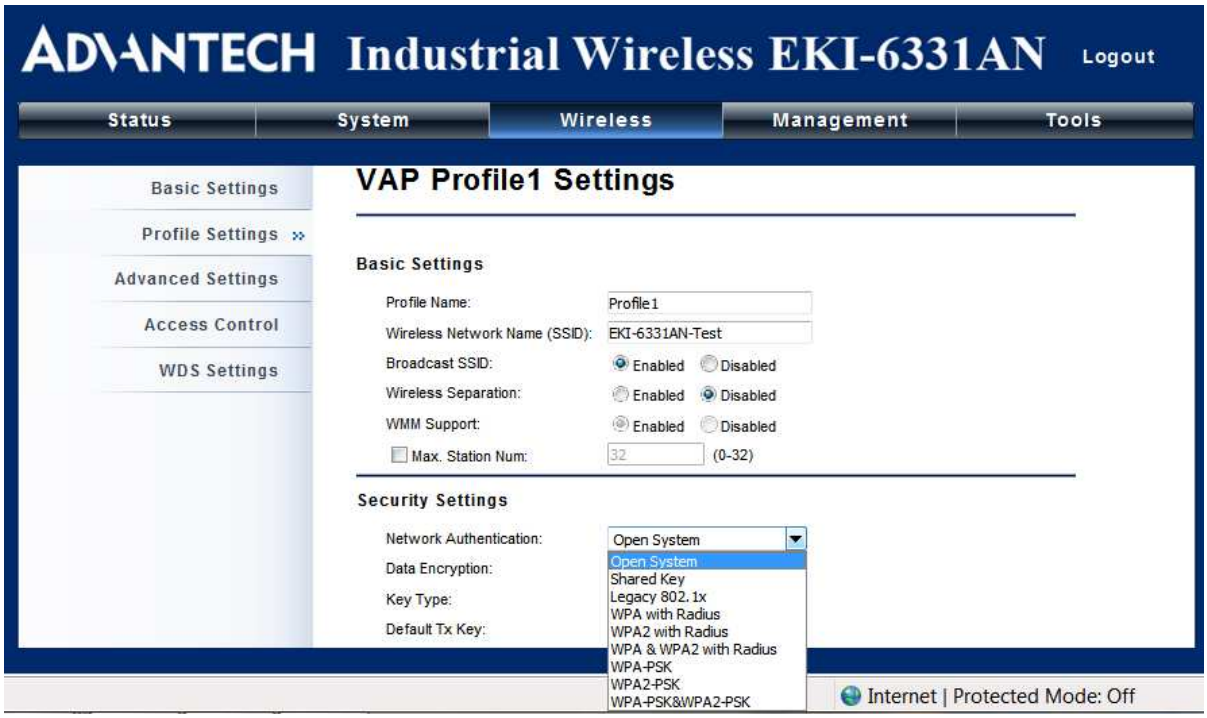


Figure 28 Security Settings

- **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.

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 EKI-6331AN and other associated wireless devices, can the communication be established!

Access Control

The Access Control appoints the authority to wireless client on accessing EKI-6331AN, thus a further security mechanism is provided. This function is available only under AP mode.

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

Figure 29 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 bridges by using the Wireless Distribution System (WDS): Simply put, you can link the bridges wirelessly. Open "**WDS Settings**" in "**Wireless**" as below:

Figure 30 WDS Settings

Enter the MAC address of another EKI-6331AN 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

Remote Management

EKI-6331AN 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.

Figure 31 Remote Management

SNMP Management

EKI-6331AN supports SNMP for convenient remote management. Open "**Remote Settings**" in "**Management**" shown below. Set the SNMP parameters and obtain MIB file before remote management.

Figure 32 SNMP Configuration

- **Protocol Version**

  Select the SNMP version, and keep it identical on EKI-6331AN and the SNMP manager. EKI-63331AN 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.

Figure 33 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 EKI-6331AN.

- **Password**

  Specify a password for the SNMPv3 administrator or user. Only the SNMP commands carrying this password are allowed to access EKI-6331AN.

- **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.

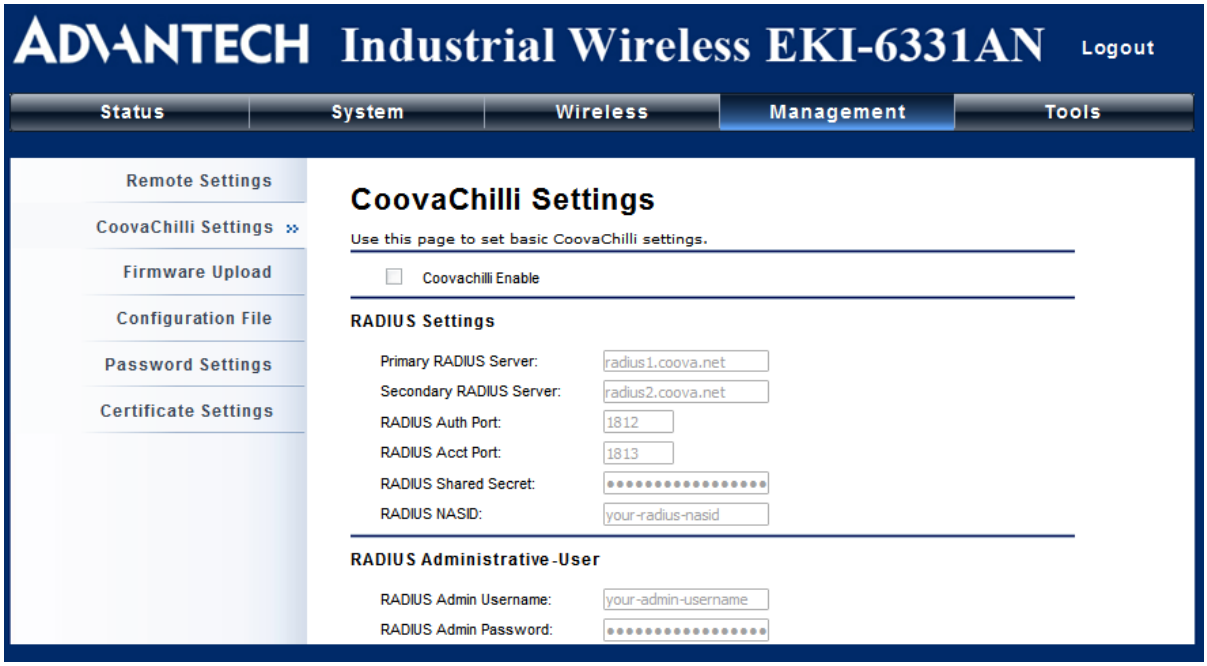


Figure 34 Coovachilli Settings

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-6331AN's Web:

Figure 35 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:

Figure 36 Backup/Retrieve Settings

- **Save Settings 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 Setting 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

EKI-6331AN provides two ways to restore the factory default settings:

- **Restore factory default settings via Web**

  From "**Configuration File**", clicking "**Reset Settings to Default**" will eliminate all current settings and reboot your device, then default settings are applied.

Figure 37 Restore Settings

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

  If software in EKI-6331AN 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-6331AN 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.

Figure 38 Reboot

Password

From "**Password Settings**" in "**Management**", you can change the password to manage your EKI-6331AN.

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

Figure 39 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**".

Figure 40 Certificate Settings

Monitoring Tools

System Log

System log is used for recording events occurred on EKI-6331AN, including station connection, disconnection, system reboot and etc.

Open “**System Log**” in “**Tools**” as below.

Figure 41 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 so that you may select a clean channel for your device based on the scan result. Open “**Site Survey**” in “**Tools**” as below.

Figure 42 Site Survey Tool

Ping Watch Dog

If the link is somehow broken and cut off your ability the log in to the unit, the ping watchdog has a chance to reboot due to loss of connectivity.

Figure 43 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 EKI-6331AN is fully initialized.

Failure Count To Reboot: If the ping timeout packets reached the value, EKI-6331AN will reboot automatically.

Date Rate Test

The Data Rate Test allows you test the current RSSI at each data rate between EKI-6331AN.

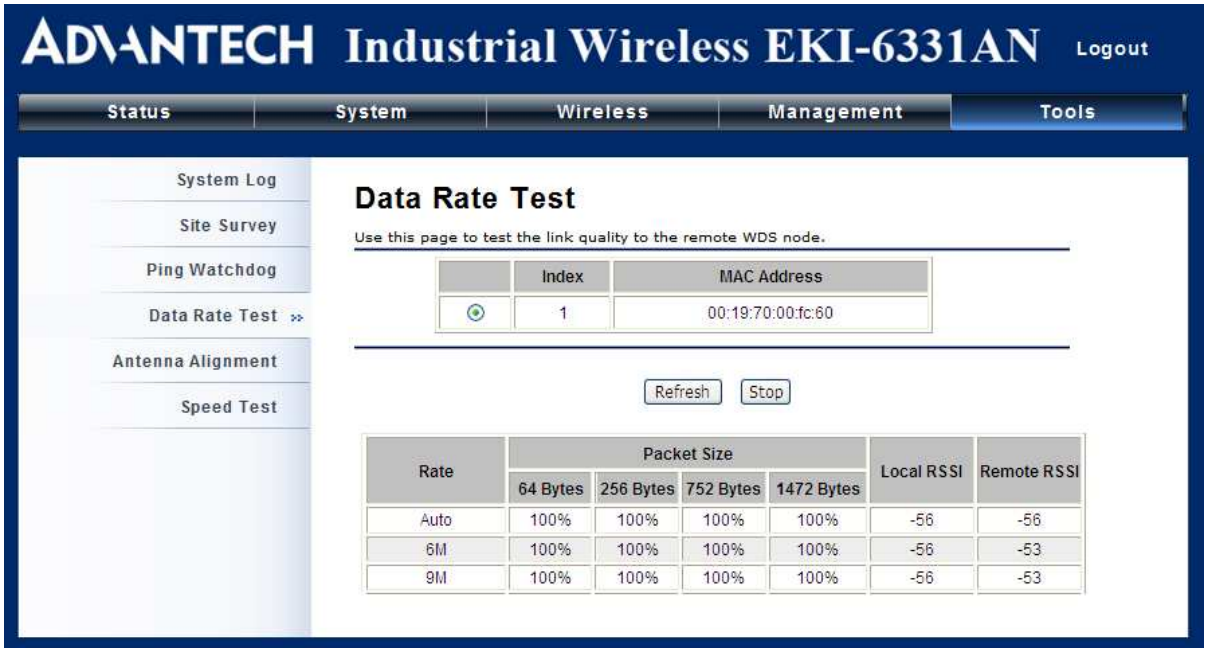


Figure 44 Data Rate Test

Antenna Alignment

Under WDS 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.

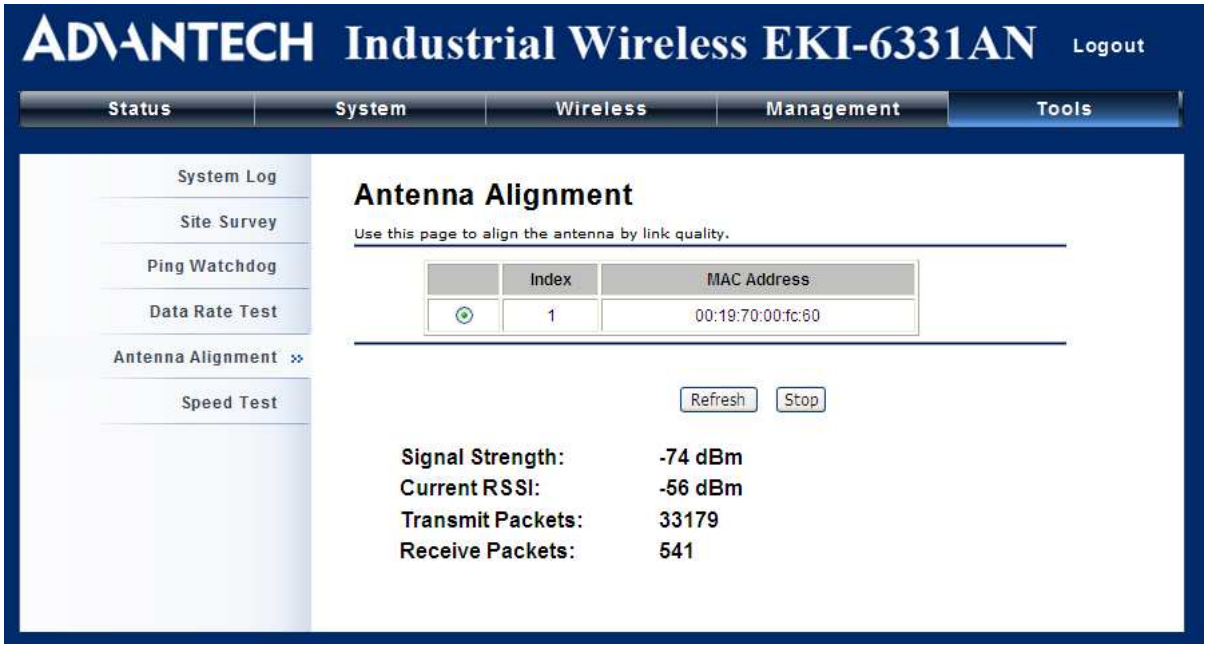


Figure 45 Antenna Alignment

Speed Test

The speed test is to monitor the current data transmission (TX) and data reception (RX) rate with the remote EKI-6331AN. Enter the IP address of the remote EKI-6331AN, 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.

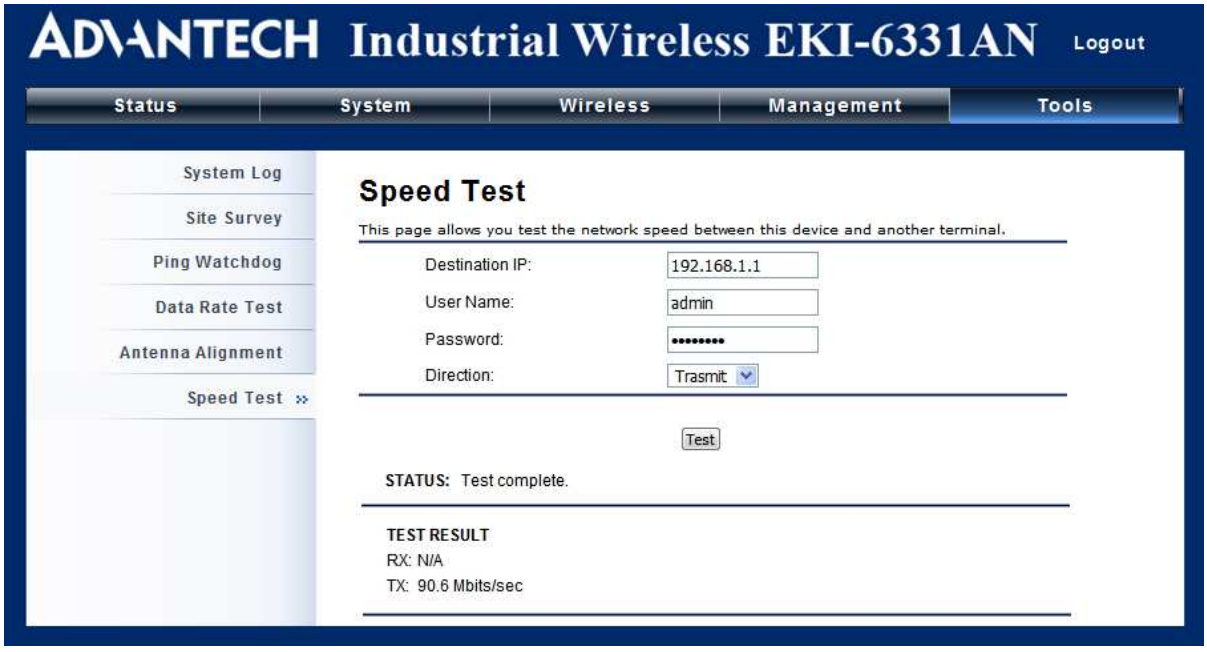


Figure 46 Speed Test

Chapter 6 Status

View Basic Information

Open “**Information**” in “**Status**” to check the basic information of EKI-6331AN, which is read only. Information includes system information, LAN settings, wireless setting and interface status. Click “**Refresh**” at the bottom to have the real-time information.

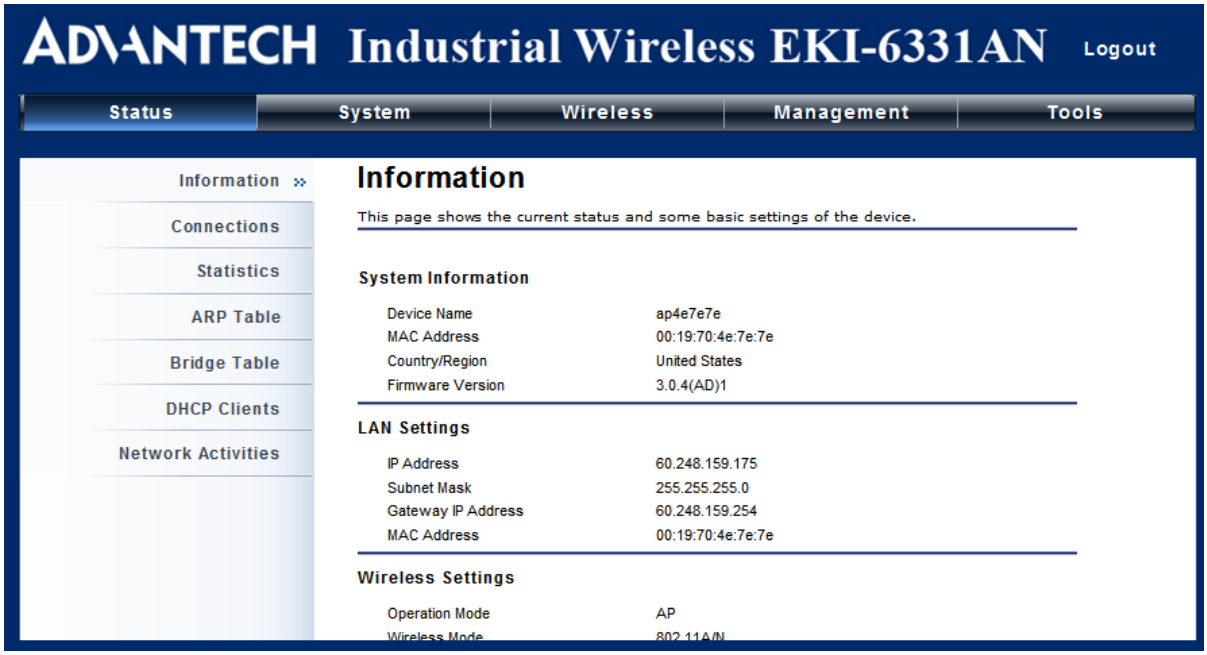


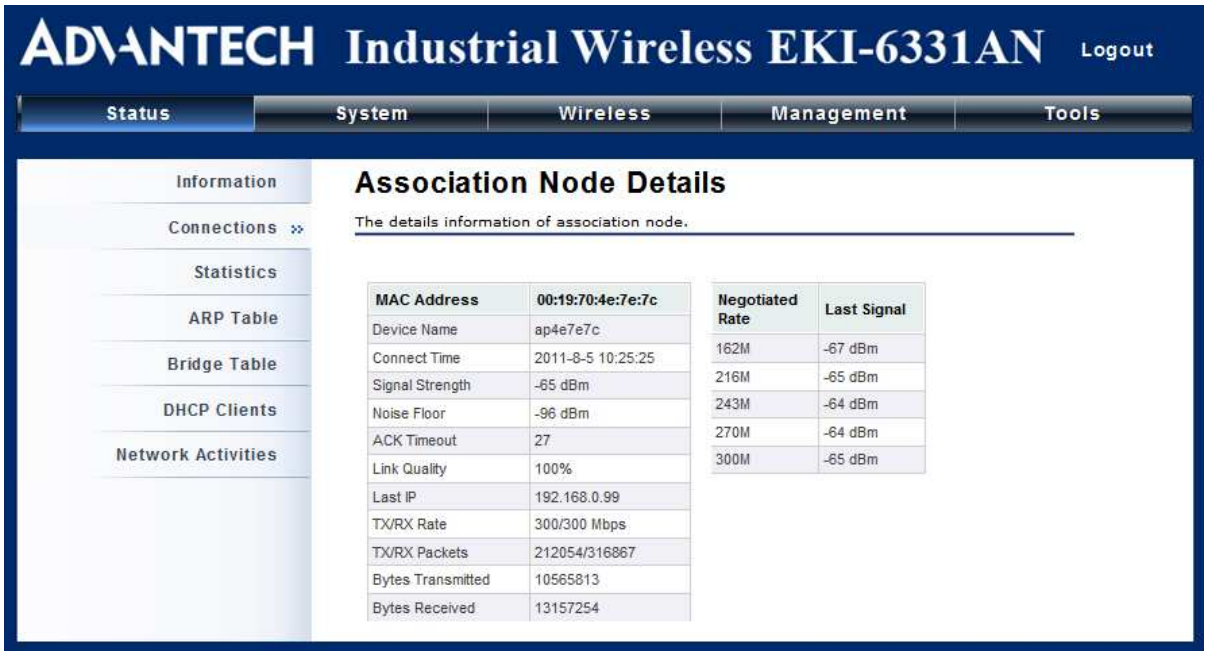
Figure 47 Basic Information

View Association List

Open “**Connections**” in “**Status**” to check the information of associated wireless devices such as MAC address, signal strength, connection time, IP address, etc. All is read only. Click “**Refresh**” at the bottom to update the current association list.

Figure 48 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.



View Network Flow Statistics

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

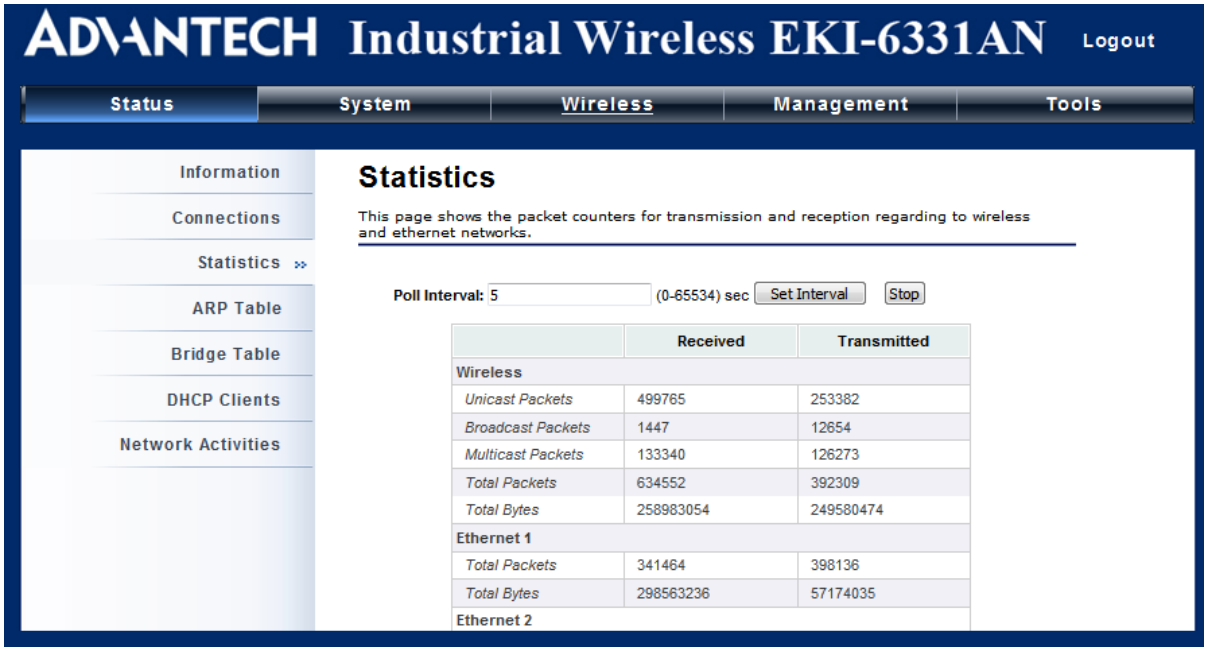


Figure 49 Network Flow Statistics

- **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.

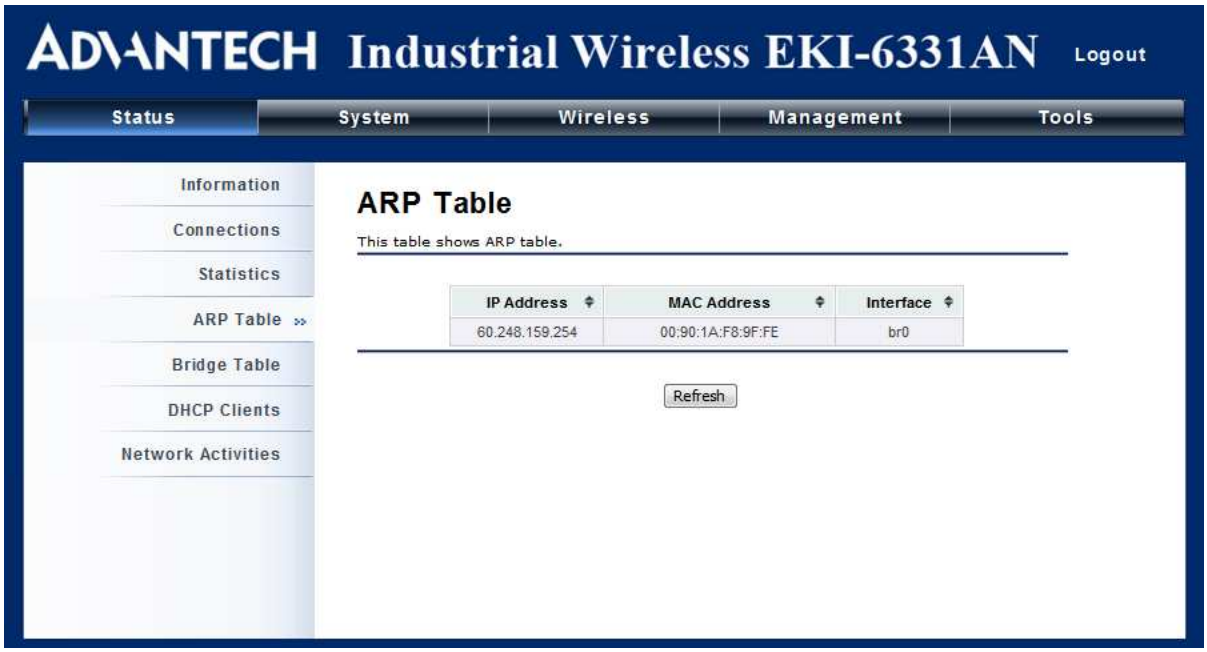


Figure 50 ARP Table

View Bridge Table

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

Figure 51 Bridge Table

View Active DHCP Client Table

Open "**DHCP Client**" 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.

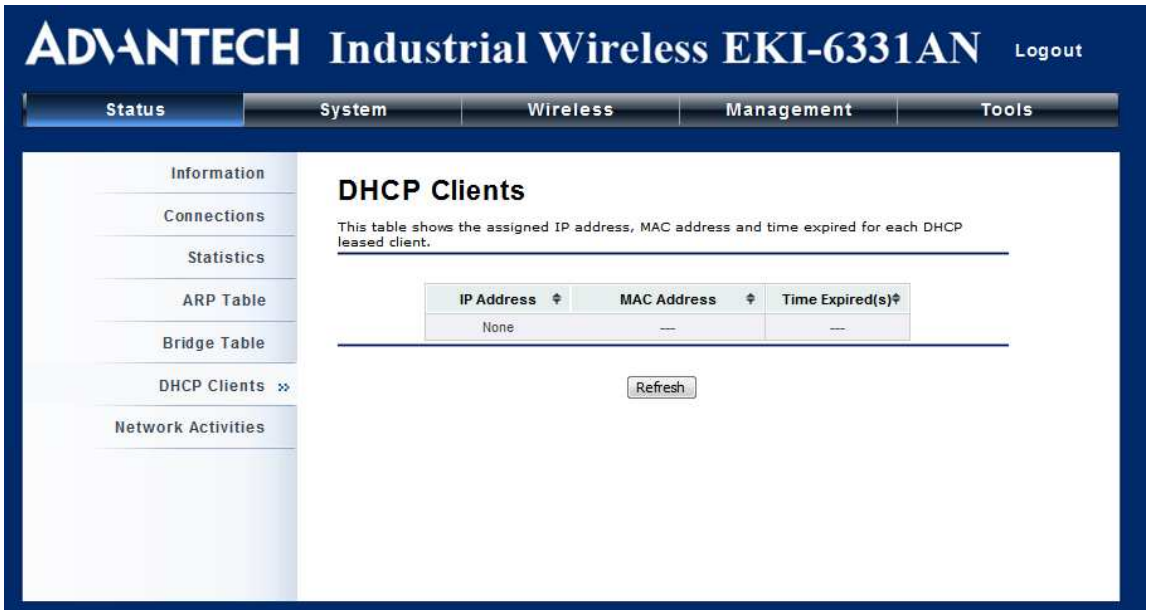


Figure 52 DHCP Client Table

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.

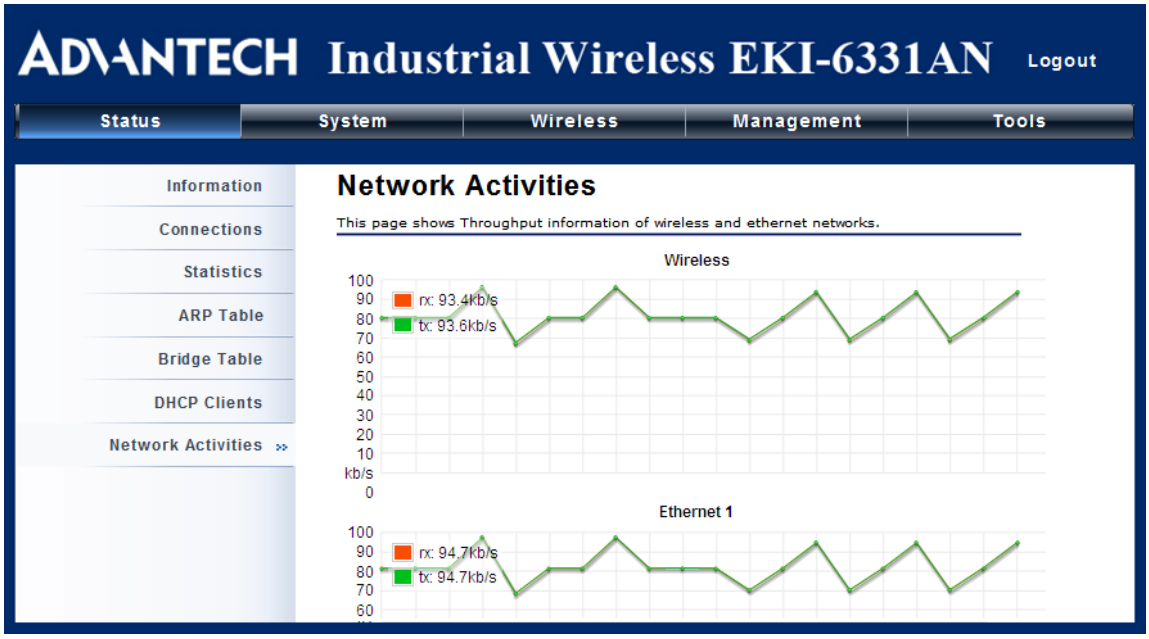


Figure 53 Network Activities

Chapter 7 Troubleshooting

This chapter provides troubleshooting procedures for basic problems with EKI-6331AN. For warranty assistance, contact your service provider or distributor for the process.

Q 1. How to know the MAC address of EKI-6331AN?

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.

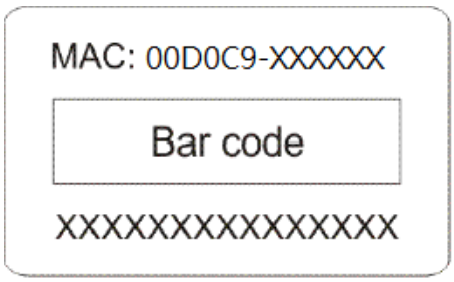


Figure 54 MAC Address

- On EKI-6331AN's Web-based management interface, you can view the MAC Address from "View Basic Information".

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. In wireless client mode, what if the wireless connection is not stable after associating with an AP?

- Since EKI-6331AN comes with a built-in directional antenna, it is recommended make it 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 SSH Settings

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
√	√	√			-innereaptype		--WPA inner EAP Type
√	√				-username		--WPA user name
√	√				-loginname		--WPA login name
√	√				-password		--WPA password
√	√				-usercert		--WPA cert file
√	√				-privatekey password		--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 3 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**
U-boot	Wolfgang Denk, DENX Software Engineering, wd@denx.de	ftp://ftp.denx.de/pub/u-boot/	GNU GENERAL PUBLIC LICENSE Version 2	GNU GENERAL PUBLIC LICENSE Version 2
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
Goahead	Copyright (c) GoAhead	http://data.goahead.com/Software		

	Software Inc., 1992-2000.	/Webserver/2.1.8/webs218.tar.gz		
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
ntpclient	Copyright 1997, 1999, 2000, 2003 Larry Doolittle	http://doolittle.icarus.com/ntpclient/ntpclient_2003_194.tar.gz	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
net-snmp	Copyright(c) 2001-2003, Networks Associates Technology, Inc All rights reserved.	http://prdownloads.sourceforge.net/net-snmp/net-snmp-5.4.1.tar.gz	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
vsftpd	Author: Chris Evans	ftp://vsftpd.beasts.org/users/ceva	GNU GENERAL PUBLIC LICENSE	http://www.gnu.org/licenses/old-lice

		ns/vsftpd-1.1.2.tar.gz	Version 2	nses/gpl-2.0.html
linux		ftp://ftp.kernel.org/pub/linux/kernel/v2.6/linux-2.6.15.tar.bz2	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
iptables	Copyright 2000-2004 netfilter project http://www.netfilter.org/	ftp://ftp.netfilter.org/pub/iptables/iptables-1.3.6.tar.bz2	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
openssl	Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.	http://www.openssl.org/source/openssl-0.9.8k.tar.gz	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
Igmpproxy	Copyright (C) 2005 Johnny Egeland <johnny@rlo.org>	http://sourceforge.net/projects/igmpproxy/files/igmpproxy/0.1/igmpproxy-0.1.tar.gz/download	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
Dnrd	Copyright (C) 1998 Brad M. Garcia <garsh@home.com>	http://sourceforge.net/projects/dnrd/files/dnrd/2.12/dnrd-2.12.tar.gz/download	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
iproute	Stephen Hemminger	http://developer.osdl.org/dev/ipro	GNU GENERAL PUBLIC LICENSE	http://www.gnu.org/licenses/old-lice

	shemminger@osdl.org Alexey Kuznetsov kuznet@ms2.inr.ac.ru	ute2	Version 2	nses/gpl-2.0.html
Pppd	Paul Mackerras <paulus@linuxcare.com>	ftp://ftp.samba.org/pub/ppp/		

Appendix D. Country Channel List

EKI-6331AN supports country selection. Channels may vary upon each country's regulation. The following tables list the channel with country code in each bandwidth.

Table 4 FCC Countries

Country	**Mode**	**Channel list**			
		40MHz	20MHz	10MHz	5MHz
United States Chile China Columbia Mexico Panama Pilippines Taiwan Uruguay Venezuela	(5725～5850)	149/153/157/161	149/153/157/161/165	149/151/153/155/157/159/161/163/165	149/150/151/152/153/154/155/156/157/158/159/160/161/162/163/164/165

Table 5 CE Countries

Country	**Mode**	**Channel list**			
		40MHz	20MHz	10MHz	5MHz
Albania Algeria Australia Austria Belgium Bulgaria Cyprus Czech Republic Denmark Estonia	11a (5470～5725) Excluded CH120~CH131 Meteorology Radars	100/104/108/112/116/132/136	100/104/108/112/116/132/136/140	100/102/104/106/108/110/112/114/116/118/132/134/136/138/140	100/101/102/103/104/105/106107/108/109/110/111/112/113/114/115/116/117/118/119/131/132/133/134/135/136/137/138/139/140/141

Finland					
France					
Germany					
Greece					
Hungary					
Iceland					
Ireland					
Italy					
Latvia					
Liechtenstein					
Lithuania					
Luxembourg					
Macedonia					
Malta					
Netherlands					
Norway					
Poland					
Portugal					
Romania					
Slovakia					
Slovenia					
Spain					
Sweden					
United Kingdom					

Table 6 Other Countries

Country	**Mode**	**Channel list**			
		40MHz	20MHz	10MHz	5MHz
India	11a 5725-5875MHz	149/153/157/161	149/153/157/161/165/169/173	149/151/153/155/157/159/161/163/165/167/169/171/173	149/150/151/152/153/154/155/156/157/158/159/160/161/162/163/164/165/166/167/168/169/170/171/172/173

Korea Russia	11a 5470-5650MHz 5725-5825MHz	100/104/108/ 112/149/153/ 157/161 *Russia: Does not support HT40.	100/104/108/112/ 116/149/153/157/ 161	100/102/104/106/ 108/110/112/114/ 116/149/151/153/1 55/157/159/161/	100/101/102/103/ 104/105/106107/ 108/109/110/111/ 112/113/114/115/ 116/149/150/151/ 152/153/154/155/ 156/157/158/159/ 160/161/
South Africa	11a 5470-5725MHz 5725-5875MHz	100/104/108/ 112/116/132/ 136/140/149/ 153/157/161/	100/104/108/112/ 116/132/136/140/ 149/153/157/161/ 165	100/102/104/106/ 108/110/112/114/ 116/118//132/134/1 36/138/140//151/15 3/155/157/159/161/ 165	100/101/102/103/ 104/105/106107/ 108/109/110/111/ 112/113/114/115/ 116/117/118/119/ 131/132/133/134/ 135/136/137/138/ 139/140/149/150/ 151/152/153/154/ 155/156/157/158/ 159/160/161/162/ 163/164/165