KWA-O6020-I

Outdoor Bridge

User’s Manual

Copyright

About This Manual

This user manual is intended to guide professional installer to install KWA-O6020-I and how to build the infrastructure centered on it. It includes procedures to assist you in avoiding unforeseen problems.

Conventions

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

*****Note:**

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

!!!Warning:

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

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

FCC Statement:

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.

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.

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.

This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

Index

Figure Index

Chapter 1 Introduction

Introduction

Designed for outdoor environment application, the KWA-O6020-I is a high-performance last-mile broadband solution that provides reliable wireless network coverage. As an IEEE 802.11a/n compliant wireless device, KWA-O6020-I is able to give stable and efficient wireless performance, while designed with IEEE 802.11n draft 2.0 standard and high output power makes it possible to deliver several times faster data rate then normal wireless device and higher bandwidth with longer range for outdoor applications.

KWA-O6020-I supports AP and Wireless Client dual wireless communication connectivity, allowing for various application requirements thus helping to find the key to the "last mile" with least effort.

With high output power and reliable performance, KWA-O6020-I is an ideal wireless broadband solution for wireless Internet service providers and system integrators!

Appearance

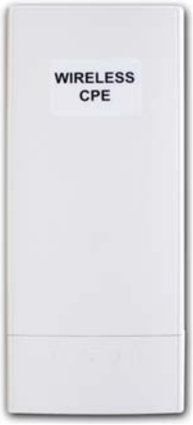


Figure 1 KWA-O6020-I

Key Features

- Compliant with IEEE 802.11a and IEEE 802.11n draft 2.0 as well.
- Support Power over Ethernet (PoE).
- IP65 waterproof housing endures almost any harsh environments.
- Dual operating modes including AP and Wireless Client
- Support 64/128-bit WEP and 802.1X, WPA, WPA2, WPA&WPA2,WPA-PSK, WPA2-PSK, and

WPA-PSK&WPA2-PSK etc

- Support WMM and Quality of service (QoS) for enhanced performance
- Advanced management tools like SNMP
- User-friendly Web and SNMP-based management interface
- Cost-effectively provide long distance backhaul for remote areas (e.g. village, oil well, island, mountain and etc.)
- Establish local backhaul for campus, farm and factory
- Provide and access for video streaming or surveillance for industrial and mining enterprises

Chapter 2 Hardware Installation

Installation Required

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

2. KWA-O6020-I is distributed through distributors and system installers with professional technicians.

Safety Precautions

1. To keep you safe and install the hardware properly, please read and follow these safety precautions.
2. If you are installing KWA-O6020-Ifor 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 KWA-O6020-I, 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.

Installation Precautions

To keep KWA-O6020-I well while you are installing it, please read and follow these installation precautions.

1. **Users MUST use a proper and well-installed surge arrestor and grounding kit with KWA-O6020-I; otherwise, a random lightening could easily cause fatal damage to KWA-O6020-I. EMD (Lightning) DAMAGE IS NOT COVERED UNDER WARRNTY.**
2. **Users MUS use the “Power cord & PoE Injector” shipped in the box with KWA-O6020-I . Use of other options will cause damage to KWA-O6020-I .**
3. **When you intend to use an external antenna with KWA-O6020-I, please power KWA-O6020-Ioff first, then install the external antenna, and finally power it on for further use. Please follow the steps as mentioned above; otherwise, damage might be caused to KWA-O6020-I 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.

●	KWA-O6020-I	×1
●	Mounting Kit	×1
●	Power Cord & PoE Injector	×1
●	Quick Installation Guide	×1
●	Product CD	×1

!!!Note

- Product CD contains Quick Installation Guide and User Manual.

Chapter 3 Basic Settings

Factory Default Settings

We'll elaborate KWA-O6020-I factory default settings. You can re-acquire these parameters by default. If necessary, please refer to the "Restore Factory Default Settings"

Table 1 KWA-O6020-I 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
Channel Number		149
SSID		Wireless
Broadcast SSID		Enable
HT Protect		Disable
Data Rate		Auto
Output Power		100% (Full)
Channel Mode		20MHz
WMM		Disable
RTS Threshold (byte)		2346
Fragmentation Length (byte)		2346
Beacon Interval		100
DTIM Interval		1
Space in Meter		0
Flow Control by AP		Disable
Uplink Speed Control(Tx)		1687
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

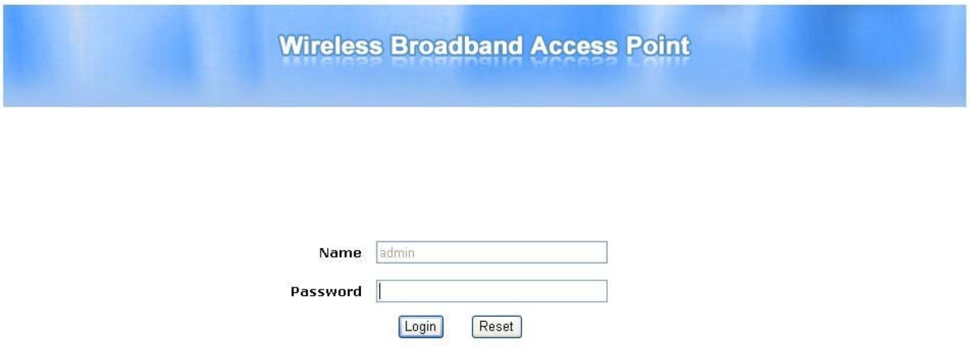
Before configuration, please make sure your system meets the following requirements :

- 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 KWA-O6020-I 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 or Firefox.

How to Login the Web-based Interface

KWA-O6020-I provides you with user-friendly Web-based management tool.

Open IE and enter the IP address (Default: **192.168.1.1**) of KWA-O6020-I into the address field. You will see the login page as below.



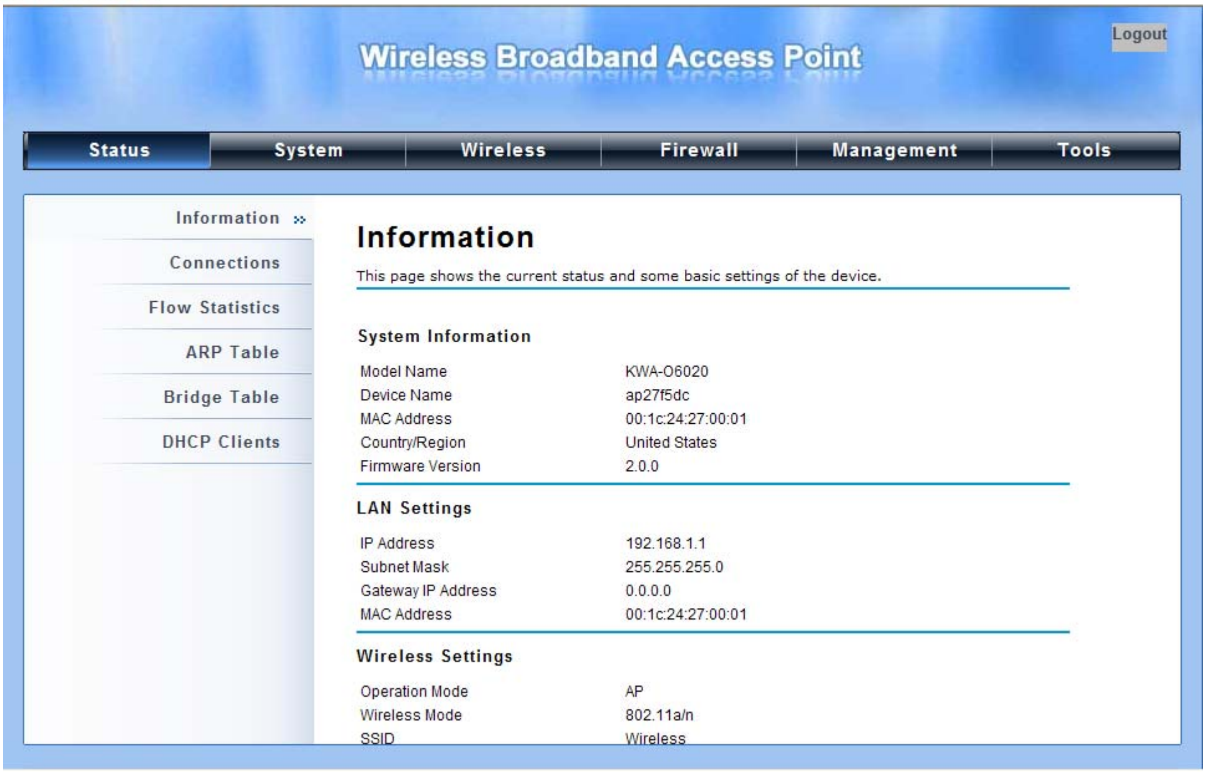
Wireless Broadband Access Point

Name admin

Password

Figure 2 Login Page

Enter the password (Default: **password**) and click “**Login**” to login the main page of KWA-O6020-I. As you can see, this management interface provides four main options in the black bar above, which are System, Wireless, Management and Statistics.



Information

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

System Information

Model Name	KWA-O6020
Device Name	ap27f5dc
MAC Address	00:1c:24:27:00:01
Country/Region	United States
Firmware Version	2.0.0

LAN Settings

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway IP Address	0.0.0.0
MAC Address	00:1c:24:27:00:01

Wireless Settings

Operation Mode	AP
Wireless Mode	802.11a/n
SSID	Wireless

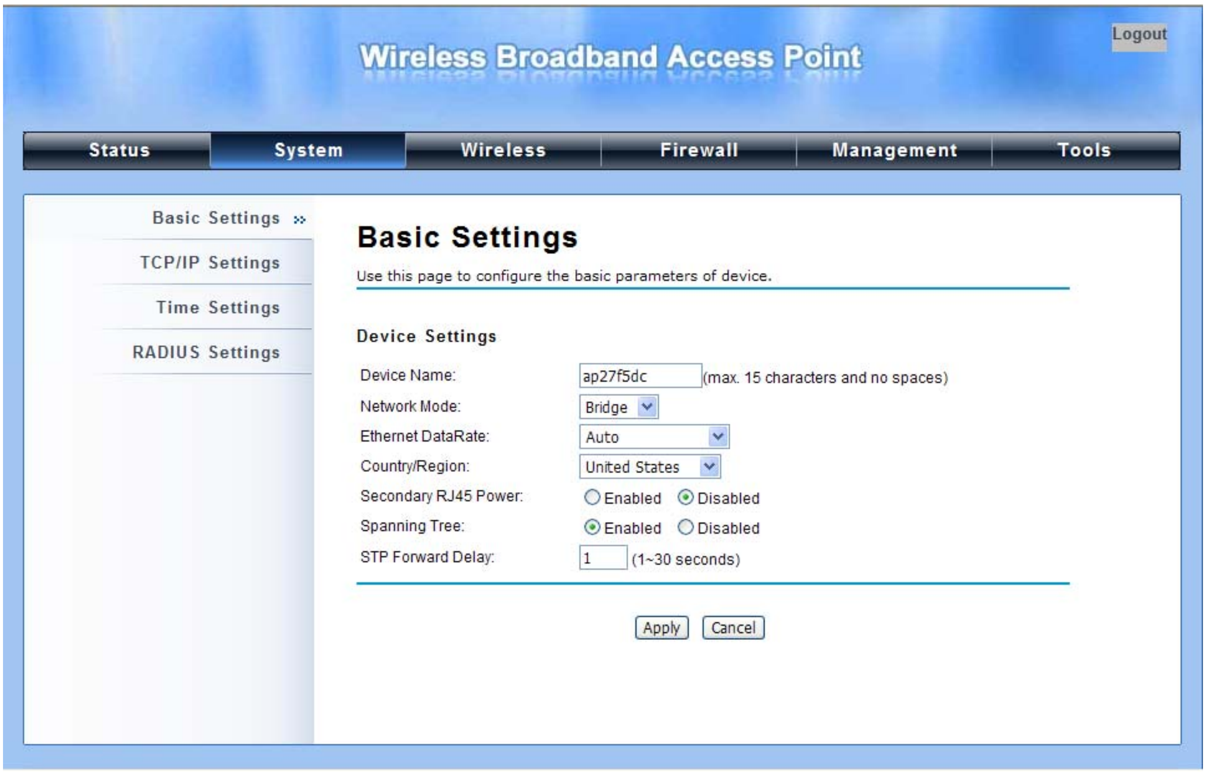
Figure 3 Main Page

!!!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 KWA-O6020-I 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: ap27f5dc (max. 15 characters and no spaces)

Network Mode: Bridge

Ethernet DataRate: Auto

Country/Region: United States

Secondary RJ45 Power: ○ Enabled ● Disabled

Spanning Tree: ● Enabled ○ Disabled

STP Forward Delay: 1 (1~30 seconds)

Figure 4 Basic System Settings

Basic Settings

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.

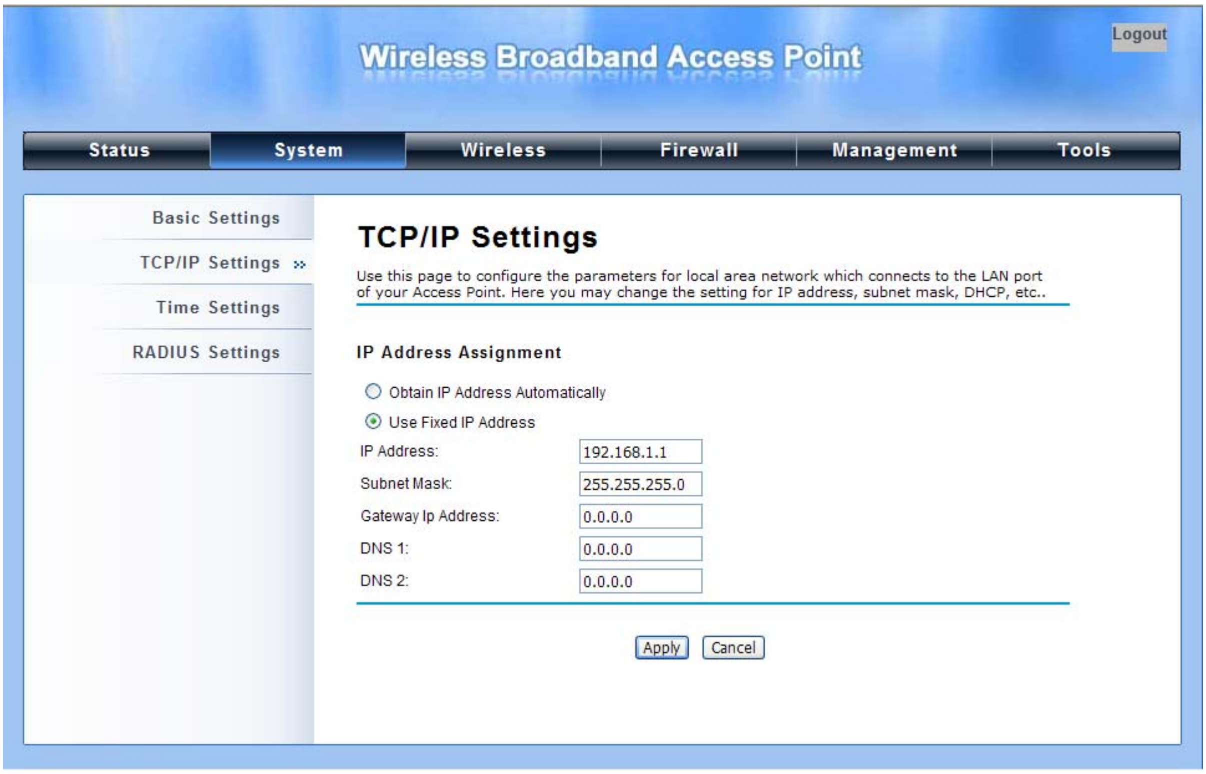
Device Name: Specify the device name for recognition, which is composed of no more than 15 characters with (0-9), (A-Z), (a-z) or (-). Device Name provides users with another option to view the login webpage; in other words, open IE, enter the Device Name (ex: ap243943) of KWA-O6020-I into the address field, click enter, and then login webpage will show up.

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.

IP Settings (Bridge)

This is available only under Bridge network mode. Open “**TCP/IP Settings**” in “**System**” as below to configure the parameters for LAN which connects to the LAN port of KWA-O6020-I . 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

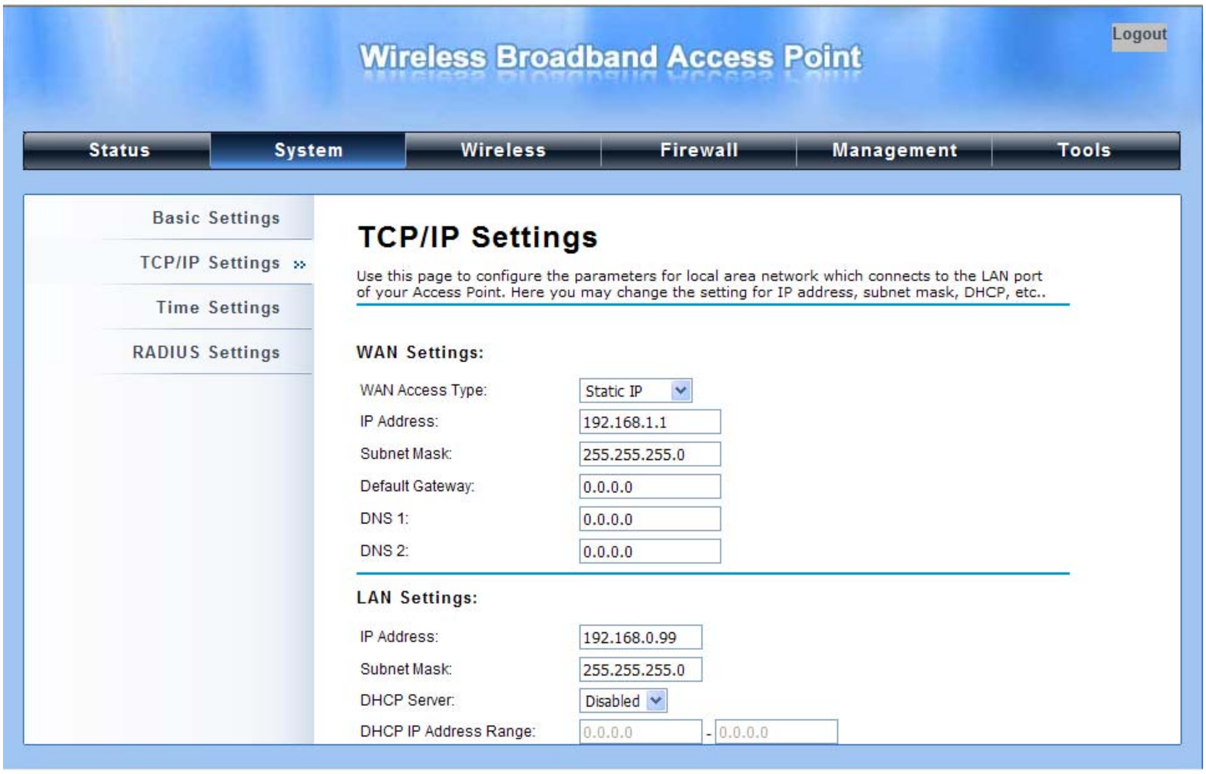
Figure 5 IP Settings (Bridge)

Obtain IP Address Automatically: If a DHCP server exists in your network, you can check this option, thus KWA-O6020-I is able to obtain IP settings automatically from that DHCP server.

Use Fixed IP Address: Check this option. You have to specify a static IP address, subnet mask, default gateway and DNS server for KWA-O6020-I manually. Make sure the specified IP address is unique on your network in order to prevent IP conflict.

IP Settings (Router)

This is available only under Router mode. Open “**TCP/IP Settings**” in “**System**” as below to configure the parameters of KWA-O6020-I 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

Figure 6 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.

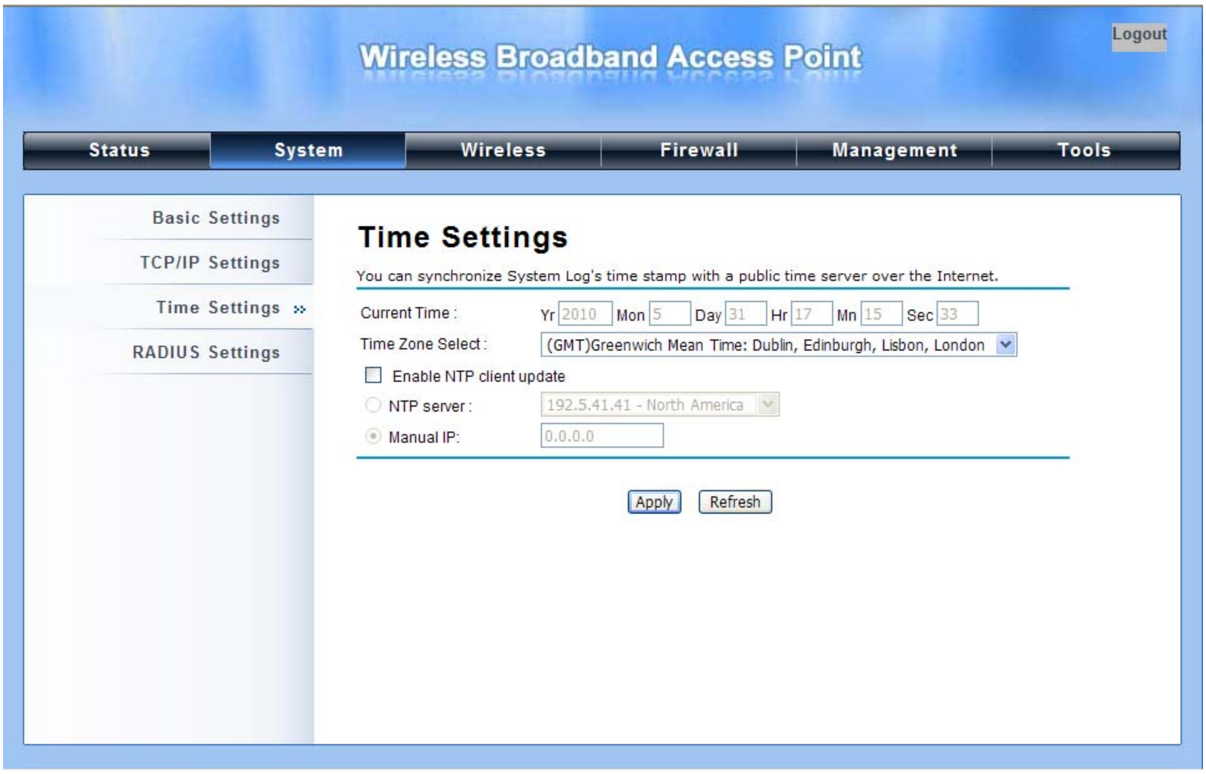
LAN Settings: When DHCP Server is disabled, users can specify IP address and subnet mask for KWA-O6020-I manually. Make sure the specified IP address is unique on your network in order to prevent IP conflict. When DHCP Server is enabled, users may specify DHCP IP Address Range, DHCP Subnet Mask, DHCP Gateway and Lease Time (15-44640 minutes).

!!!Warning:

- In AP mode, KWA-O6020-I must establish connection with another wireless device before it is set to Router mode. In Router mode, it is impossible for users to access device via wired port, for WAN is on wired port and LAN is on wireless port. Users can access device through the wireless device connected with KWA-O6020-I .
- In CPE mode, users can access KWA-O6020-I via its wired port, for WAN is on wireless port and LAN is on wired port when device is set to Router mode.
- WDS 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 KWA-O6020-I with another wireless device before it is set to Router mode and access KWA-O6020-I via the connected wireless device.

Time Settings

Compliant with NTP, the KWA-O6020-I 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 2010 Mon 5 Day 31 Hr 17 Mn 15 Sec 33

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 7 Time Settings

- **Time Zone Select**

Select the time zone from the dropdown list.

- **Time Server**

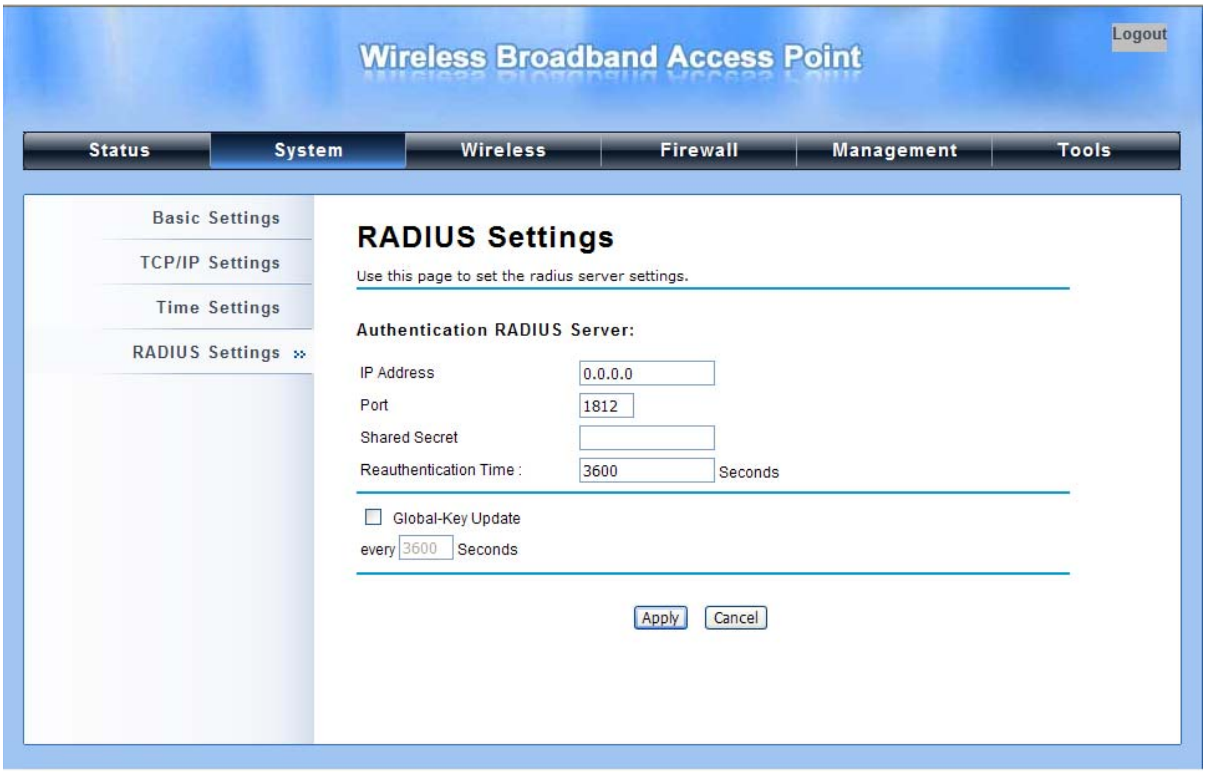
Select the time server from the “**NTP Server**” dropdown list or manually input the IP address of available time server into “**Manual IP**”.

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.



RADIUS Settings

Use this page to set the radius server settings.

Authentication RADIUS Server:

IP Address	0.0.0.0
Port	1812
Shared Secret	
Reauthentication Time :	3600 Seconds

□ Global-Key Update

every 3600 Seconds

Figure 8 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;

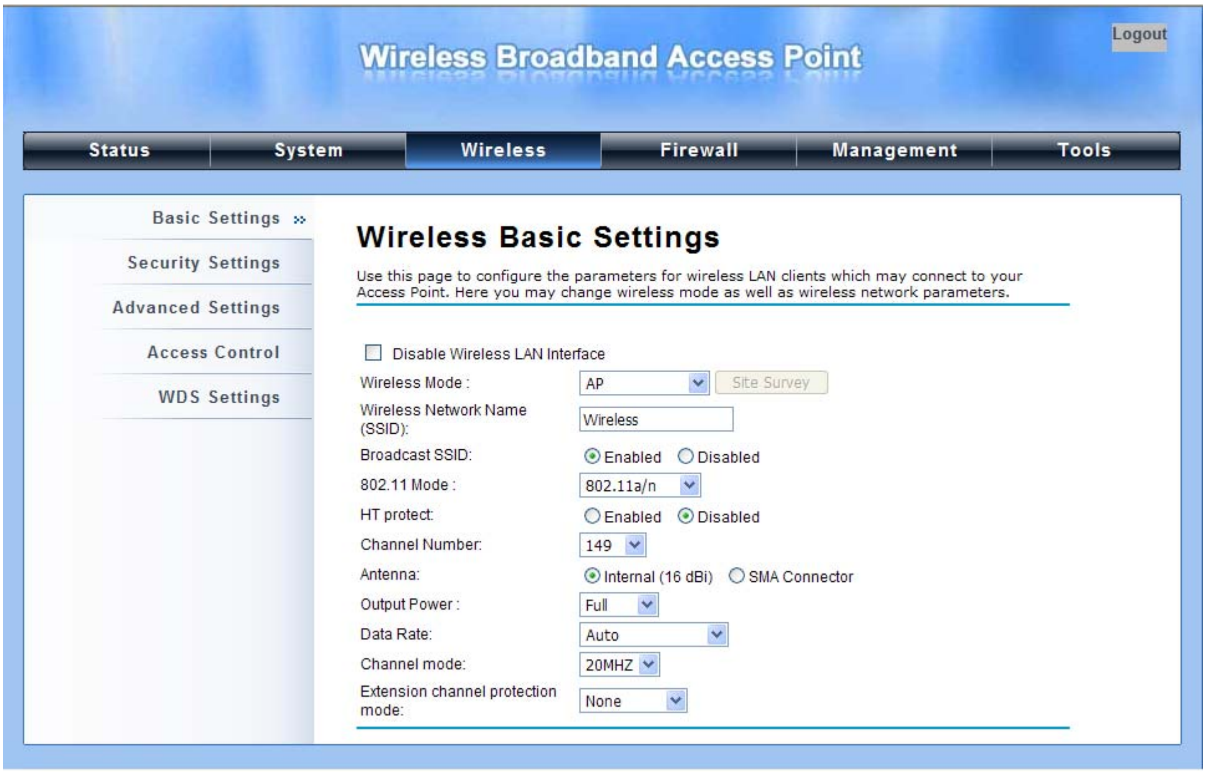
Shared Secret: This secret, which is composed of no more than 31 characters, is shared by the KWA-O6020-I and RADIUS during authentication.

Re-authentication Time: Set the time interval between two authentications.

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

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 (Site Survey)
Wireless Network Name (SSID):	Wireless
Broadcast SSID:	● Enabled ○ Disabled
802.11 Mode :	802.11a/n
HT protect:	○ Enabled ● Disabled
Channel Number:	149
Antenna:	● Internal (16 dBi) ○ SMA Connector
Output Power :	Full
Data Rate:	Auto
Channel mode:	20MHZ
Extension channel protection mode:	None

Figure 9 Basic Wireless Settings

Disable Wireless LAN Interface

Check this option to disable WLAN interface, then the wireless module of KWA-O6020-I will stop working and no wireless device can connect to it.

Wireless Mode

Four operating modes are available on KWA-O6020-I.

Wireless Client: The KWA-O6020-I is able to connect to the AP and thus join the wireless network around it.

AP: The KWA-O6020-I establishes a wireless coverage and receives connectivity from other wireless devices.

Bridge: The KWA-O6020-I establishes wireless connectivity with other APs.

AP Repeater: The KWA-O6020-I servers as AP and Bridge at the same time. In other words, the KWA-O6020-I can provide connectivity services for CPE’s under WDS 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 KWA-O6020-I, so that malicious attack by some illegal STA could be avoided.

802.11 Mode

KWA-O6020-I can communicate with wireless devices of 802.11a or 802.11a/n. You can also select Auto and make it work under an appropriate wireless mode automatically.

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.

Channel Number

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.

Antenna

By default, KWA-O6020-I 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 " to "External (RP SMA-Type)".

!!!Note

- You are able to choose "External (RP SMA-Type)" only when you have well done installing the external antenna; otherwise, it might hurt KWA-O6020-I itself.

Output Power

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. Usually "**Full**" is preferred.

Data Rate

Usually "**Auto**" is preferred. Under this rate, KWA-O6020-I 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.

Channel Mode

Two levels are available: 20MHz and 40MHz. The latter one can enhance the data rate more effectively, but takes more bandwidth, thus cause potential interference.

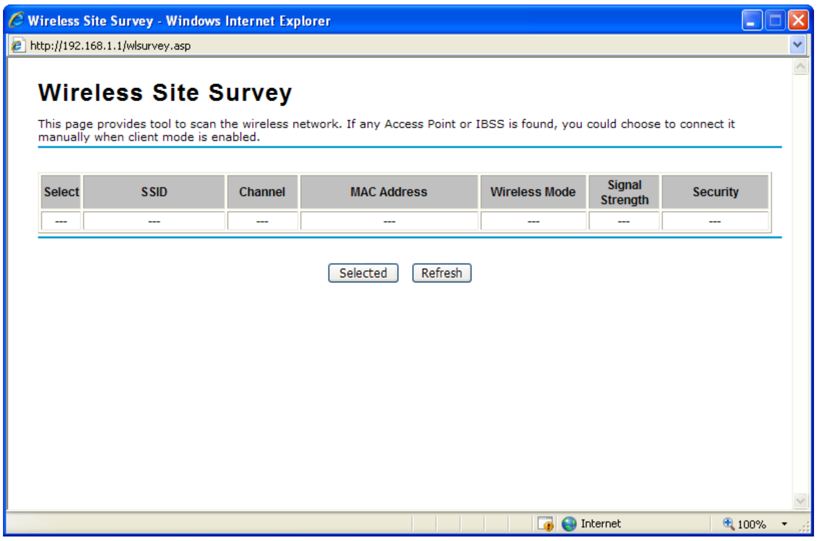
Extension Channel Protection Mode

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

Site Survey

Under wireless client mode, KWA-O6020-I 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 popup with a list of available wireless networks around. Select the AP you would like to connect and click “**Selected**” to establish connection.


Wireless Site Survey - Windows Internet Explorer
http://192.168.1.1/wlsurvey.asp
Selected
Refresh
Internet
100%

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.

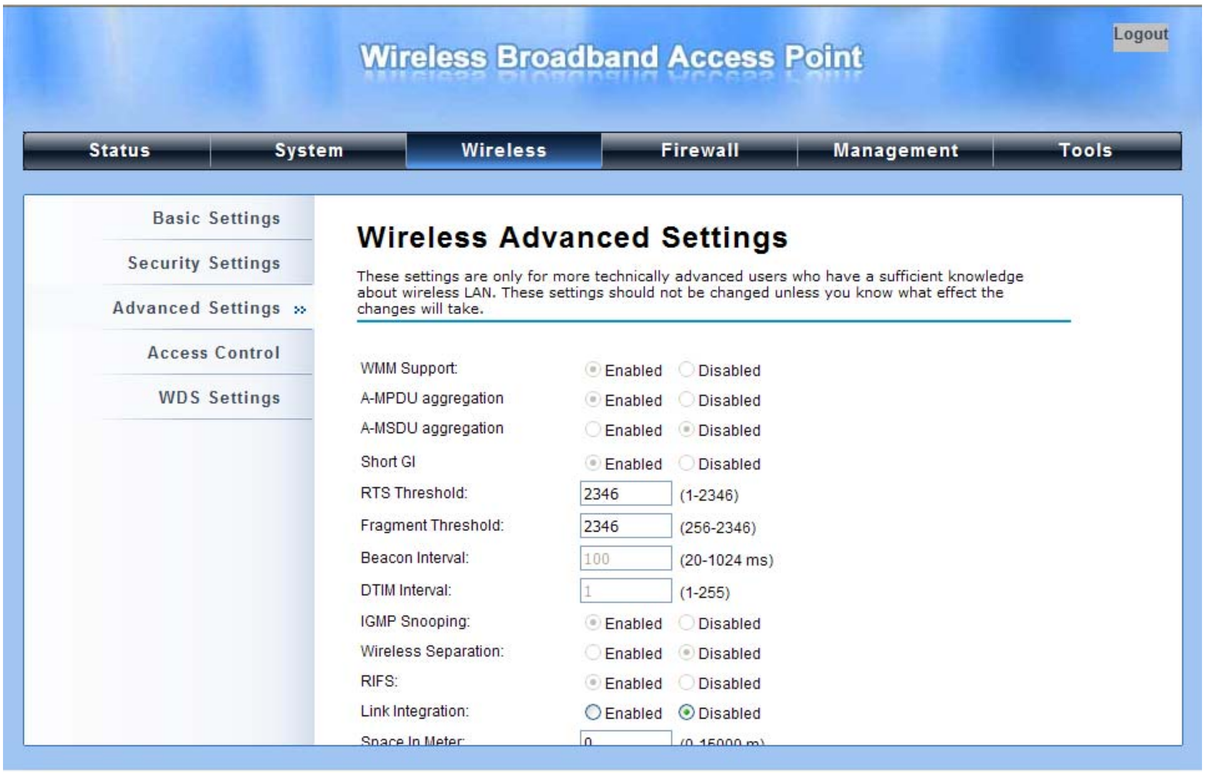
Select	SSID	Channel	MAC Address	Wireless Mode	Signal Strength	Security
---	---	---	---	---	---	---

Figure 10 Site Survey

Chapter 4 Advanced Settings

Advanced 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.

WMM Support:	● Enabled	○ Disabled
A-MPDU aggregation	● Enabled	○ Disabled
A-MSDU aggregation	○ Enabled	● Disabled
Short GI	● Enabled	○ Disabled
RTS Threshold:	2346	(1-2346)
Fragment Threshold:	2346	(256-2346)
Beacon Interval:	100	(20-1024 ms)
DTIM Interval:	1	(1-255)
IGMP Snooping:	● Enabled	○ Disabled
Wireless Separation:	○ Enabled	● Disabled
RIFS:	● Enabled	○ Disabled
Link Integration:	○ Enabled	● Disabled
Space In Meter:	0	(0-15000 m)

Figure 11 Advanced Wireless Settings

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, thus those time-sensitive data, like video/audio data, may own a higher priority than common one. To enable WMM, the wireless client should support it.

A-MPDU/A-MSDU Aggregation

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

KWA-O6020-I 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.

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 “**Short**” are available.

IGMP Snooping

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.

Wireless Separation

Wireless separation is an ideal way to enhance the security of network transmission. Under the AP mode, enable “**Wireless Separation**” can prevent the communication among associated wireless clients.

RIFS

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

Link Integration

Available only under AP 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.

Max. Station Num

Available only under AP mode, it defines the maximum amount of wireless clients allowed to be connected.

Space in Meter

To reduce the chances of data retransmission at long distance, the KWA-O6020-I can automatically adjust proper ACK timeout value by specifying distance of the two nodes. The distance to be entered here is calculated in terms of meters, so if the actual distance between two nodes is 5Km, please enter 5000 in the blank.

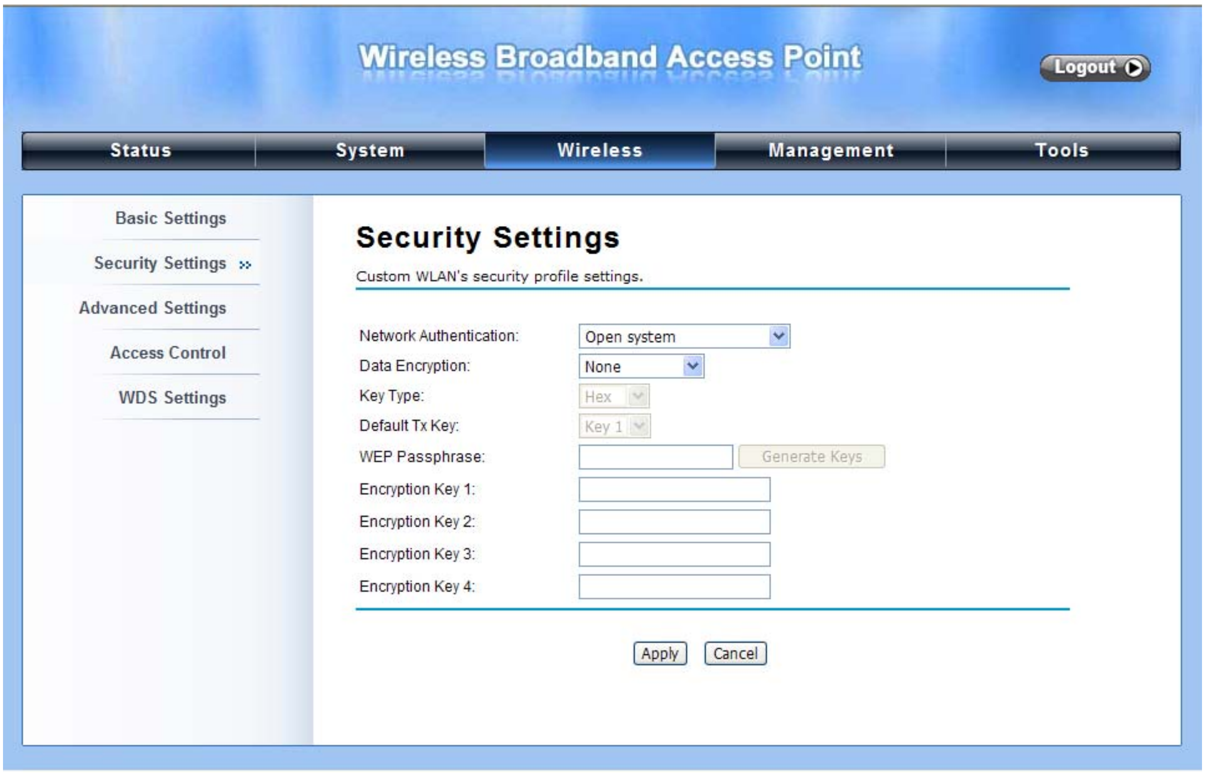
Flow Control

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

Security Settings

To prevent unauthorized radios from accessing data transmitting over the connectivity, the KWA-O6020-I provides you with rock solid security settings.

Open "**Security Settings**" in "**Wireless**" as below:



Security Settings

Custom WLAN's security profile settings.

Network Authentication: Open system

Data Encryption: None

Key Type: Hex

Default Tx Key: Key 1

WEP Passphrase:

Encryption Key 1:

Encryption Key 2:

Encryption Key 3:

Encryption Key 4:

Figure 12 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.

Legacy 802.1x: As an IEEE standard for port-based Network Access Control, 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.

WPA with RADIUS: 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: 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: 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: 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.

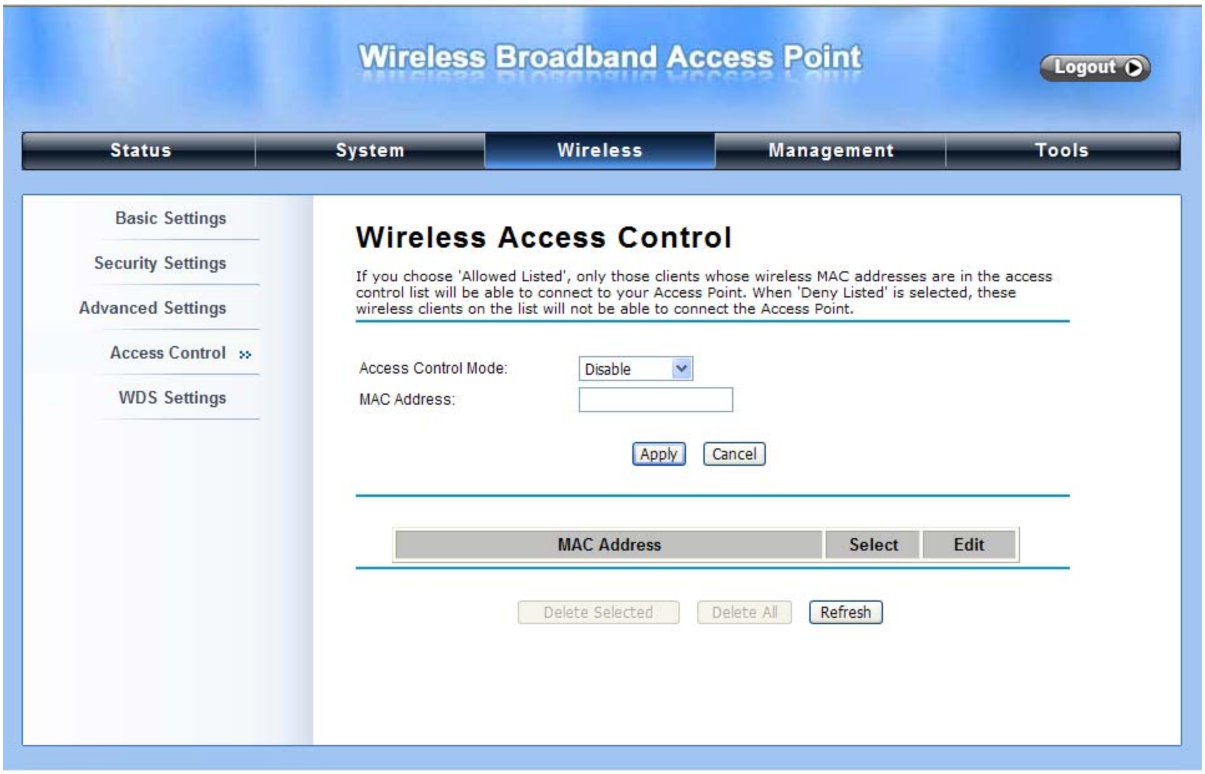
AES: Advanced Encryption Standard, it is usually co-used with WPA2-PSK, WPA, WPA2, etc.

TKIP + AES: It allows for backwards compatibility with devices using TKIP.

Access Control

The Access Control appoints the authority to wireless client on accessing KWA-O6020-I, 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:

MAC Address	Select	Edit

Figure 13 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

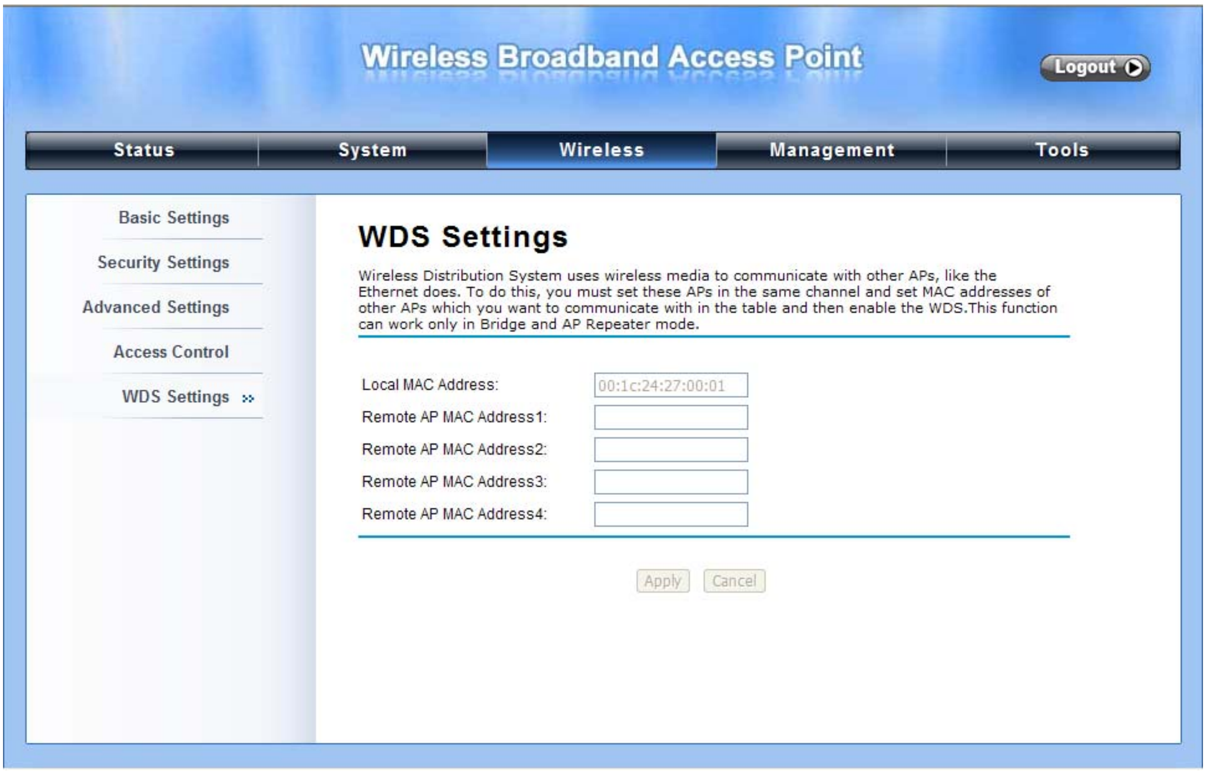
Enter the MAC address of the wireless client that you would like to list into the access control list, click “**Apply**” then it will be added into the table at the bottom.

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): Put simply, 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.

Local MAC Address:	00:1c:24:27:00:01
Remote AP MAC Address1:	
Remote AP MAC Address2:	
Remote AP MAC Address3:	
Remote AP MAC Address4:	

Figure 14 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.

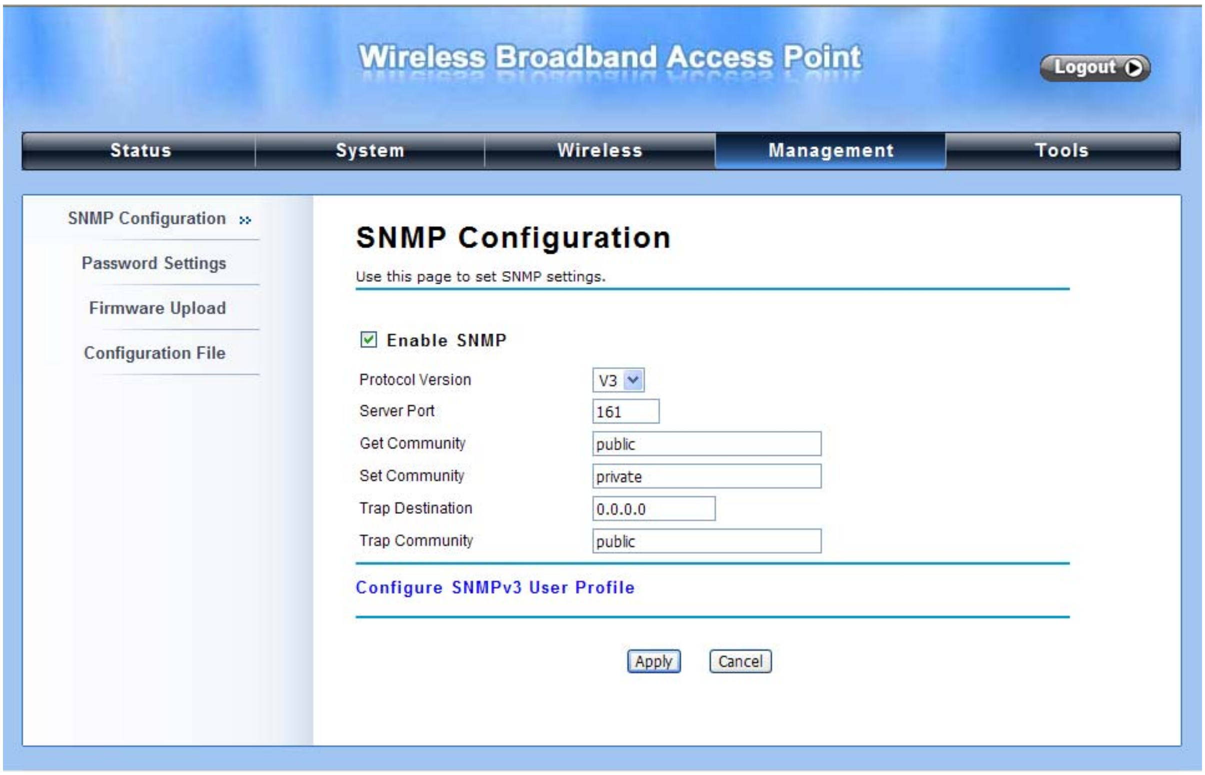
*****Note:**

- WDS Settings is available only under Bridge and AP Repeater Mode.

Chapter 5 Management

SNMP Management

KWA-O6020-I 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 15 SNMP Configuration

Enable SNMP

Check this box to enable SNMP settings.

Protocol Version

Select the SNMP version, and keep it identical on KWA-O6020-I and the SNMP manager.

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

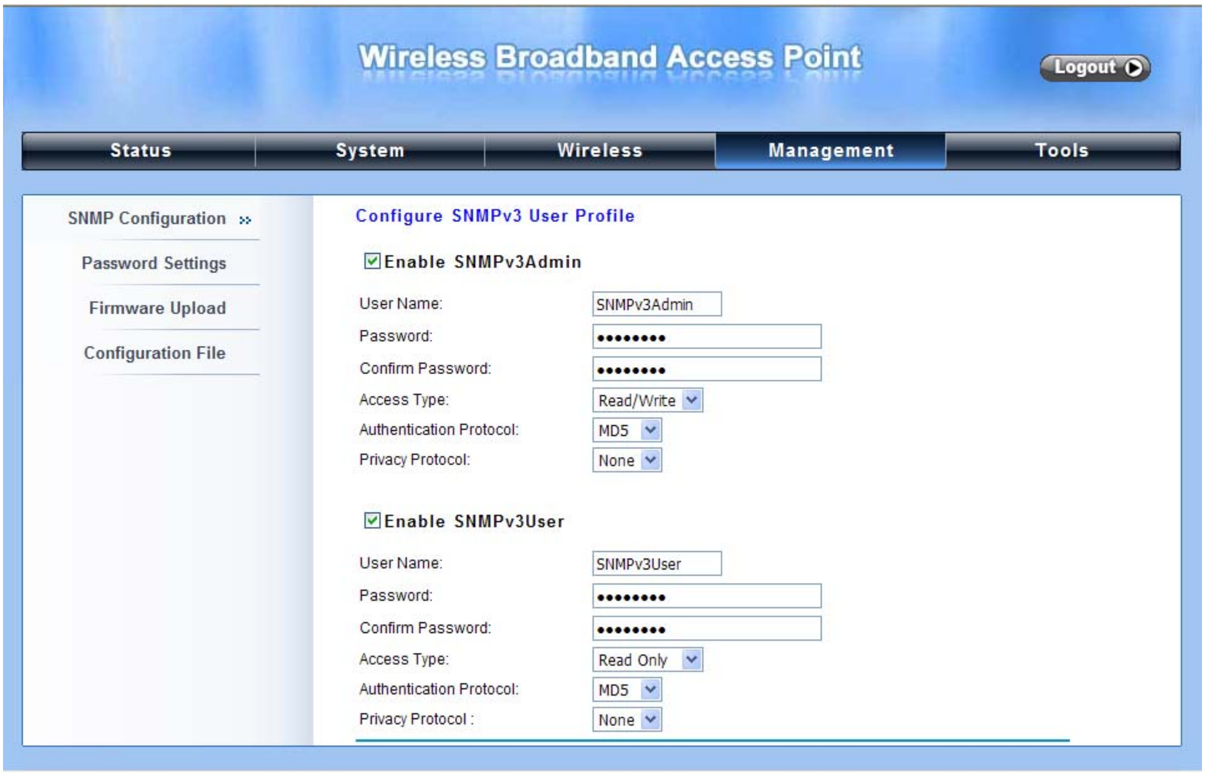
Specify the IP address of the station to send the SNMP traps to.

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 16 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 KWA-O6020-I.

Password

Specify a password for the SNMPv3 administrator or user. Only the SNMP commands carrying this password are allowed to access KWA-O6020-I. 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, DES and None are available.

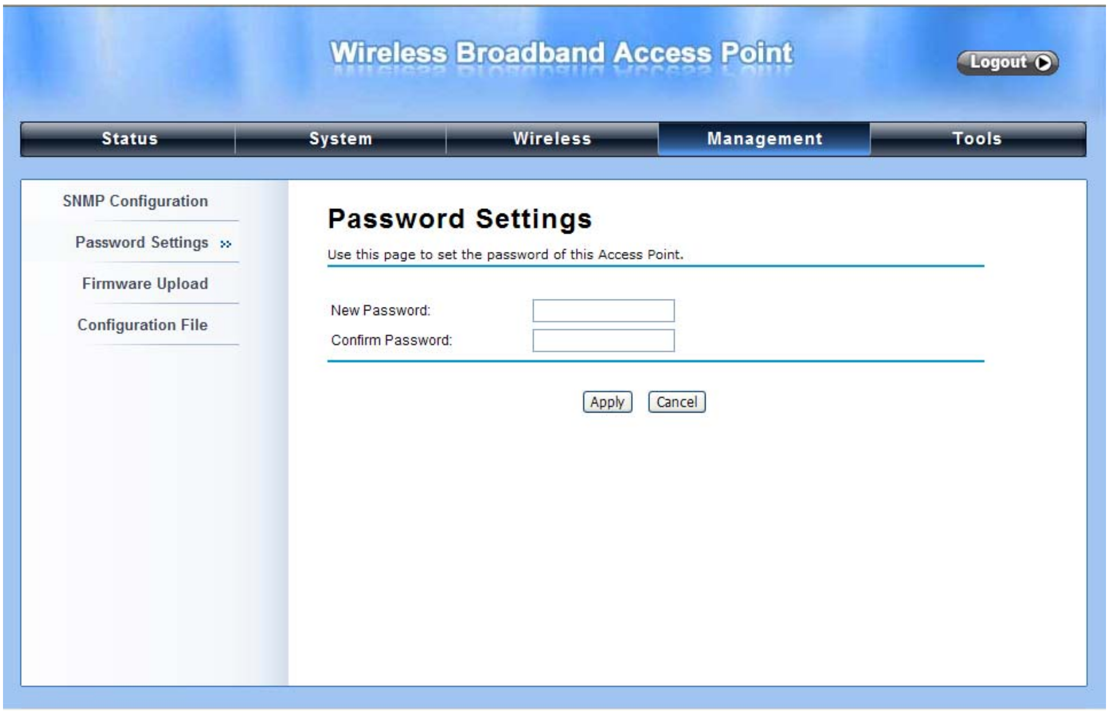
None: No encryption is applied.

DES: Data Encryption Standard, it applies a 58-bit key to each 64-bit block of data.

Password Settings

From "**Password Settings**" in "**Management**", you can change the password to manage your KWA-O6020-I.

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:

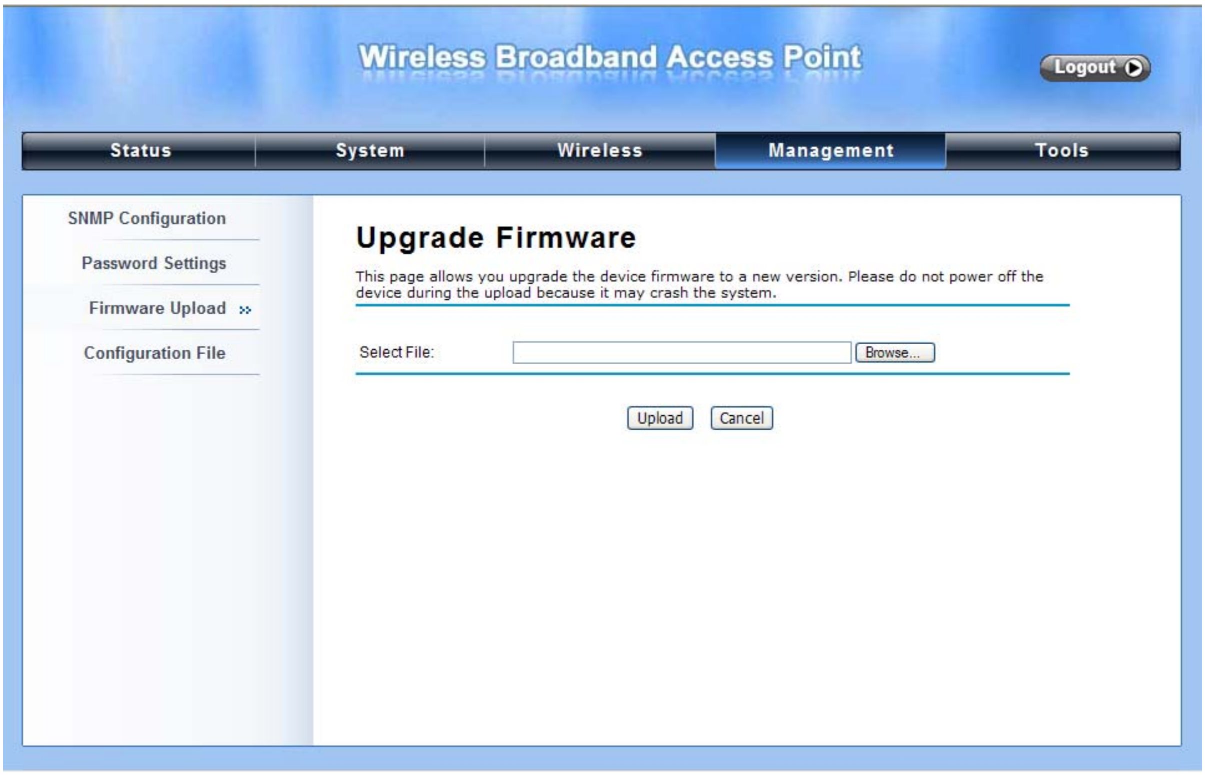
Figure 17 Password

!!!Note

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

Upgrade Firmware

Open “**Firmware Upload**” in “**Management**” and follow the steps below to upgrade firmware locally or remotely through KWA-O6020-I’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 18 Upgrade Firmware

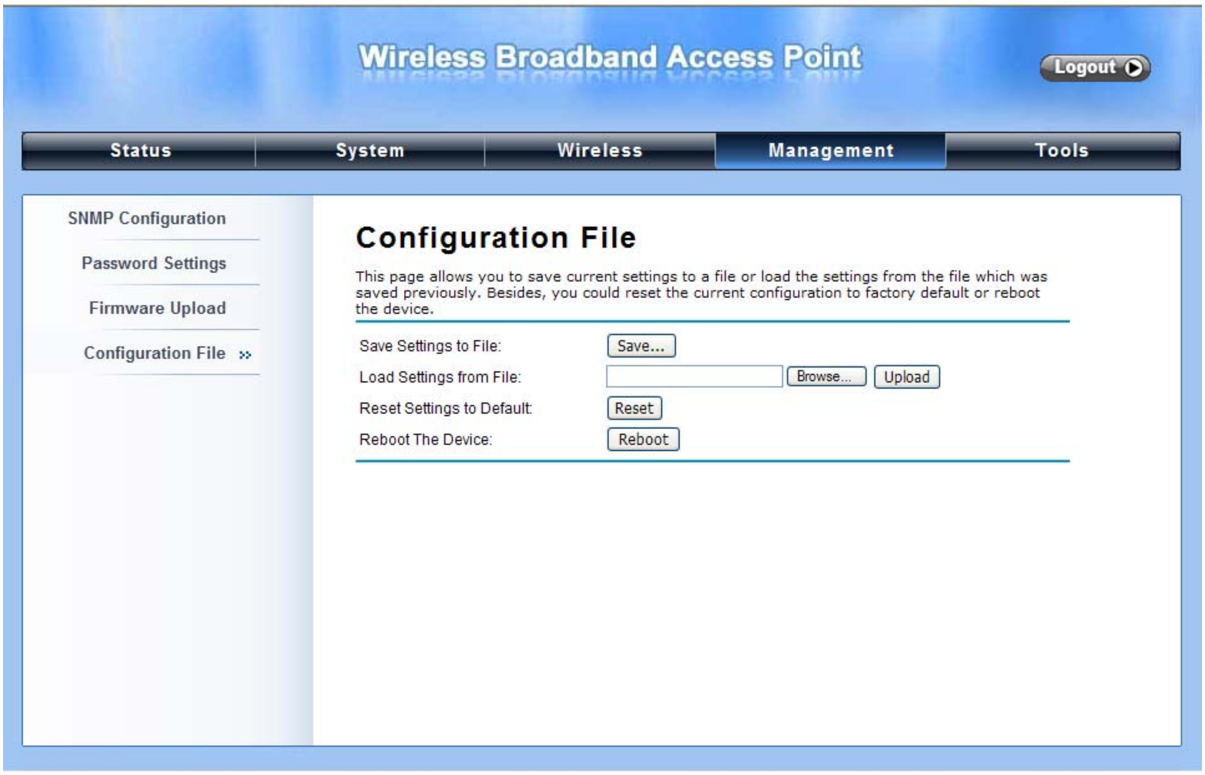
- Click “**Browse**” to select the firmware file you would like to load;
- Click “**Upload**” to start the upload process;
- Wait a moment, the system will reboot after successful upgrade.

!!!Note

- Do NOT cut the power off during upgrading; otherwise the system may severely crash !

Configuration File

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 19 Backup/Retrieve Setting

Save Settings to File

By clicking “**Save**”, a dialog box will popup. Save it, then the configuration file like ap.cfg will be 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.

Reset Settings to Default

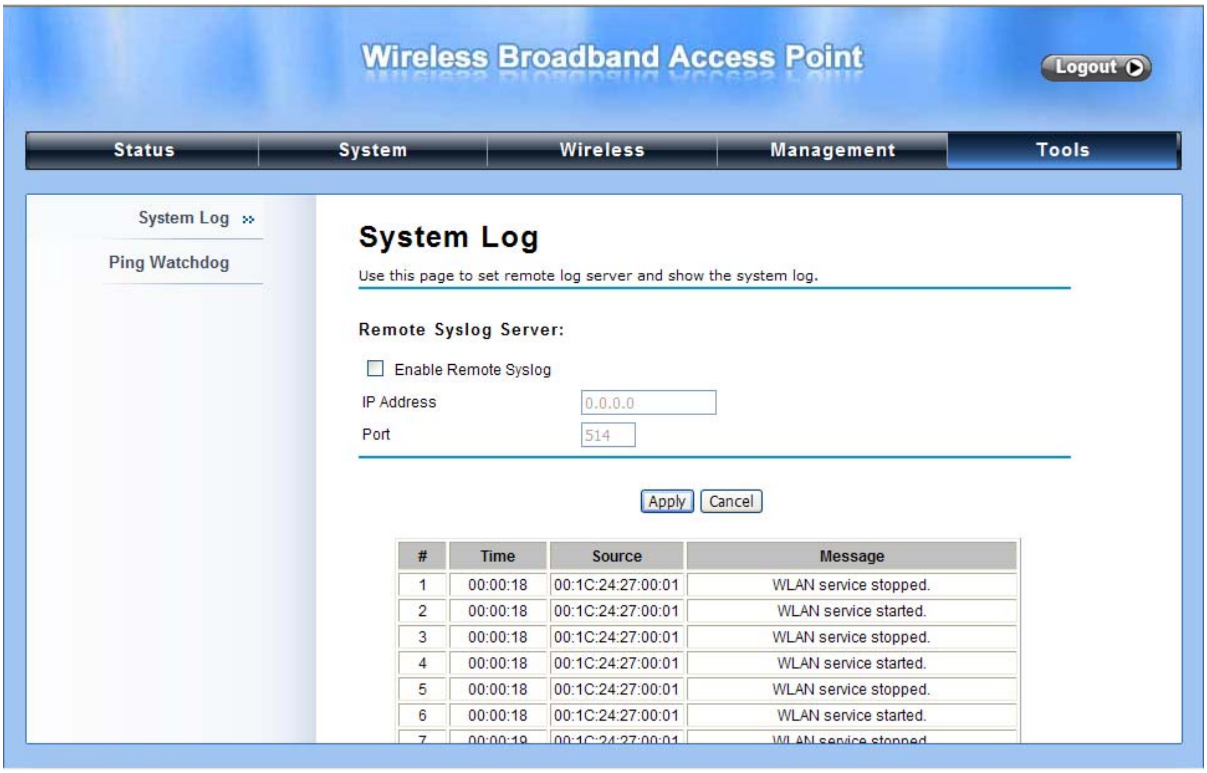
From “**Configuration File**”, clicking “**Reset**” will eliminate all current settings and reboot your device, then default settings are applied. In addition, KWA-O6020-I provides another way to restore the factory default settings: If software in KWA-O6020-I is unexpectedly crashed and no longer reset the unit via Web, you may do hardware reset via the reset button.

Reboot The Device

Click “**Reboot**” and hit “**Yes**” upon the appeared prompt to start reboot process. This takes a few minutes.

System Log

System log is used for recording events occurred on KWA-O6020-I, including station connection, disconnection, system reboot and etc. Open “**System Log**” in “**Tool**” as below.



System Log

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

Remote Syslog Server:

□ Enable Remote Syslog

IP Address: 0.0.0.0

Port: 514

#	Time	Source	Message
1	00:00:18	00:1C:24:27:00:01	WLAN service stopped.
2	00:00:18	00:1C:24:27:00:01	WLAN service started.
3	00:00:18	00:1C:24:27:00:01	WLAN service stopped.
4	00:00:18	00:1C:24:27:00:01	WLAN service started.
5	00:00:18	00:1C:24:27:00:01	WLAN service stopped.
6	00:00:18	00:1C:24:27:00:01	WLAN service started.
7	00:00:19	00:1C:24:27:00:01	WLAN service stopped.

Figure 20 System Log

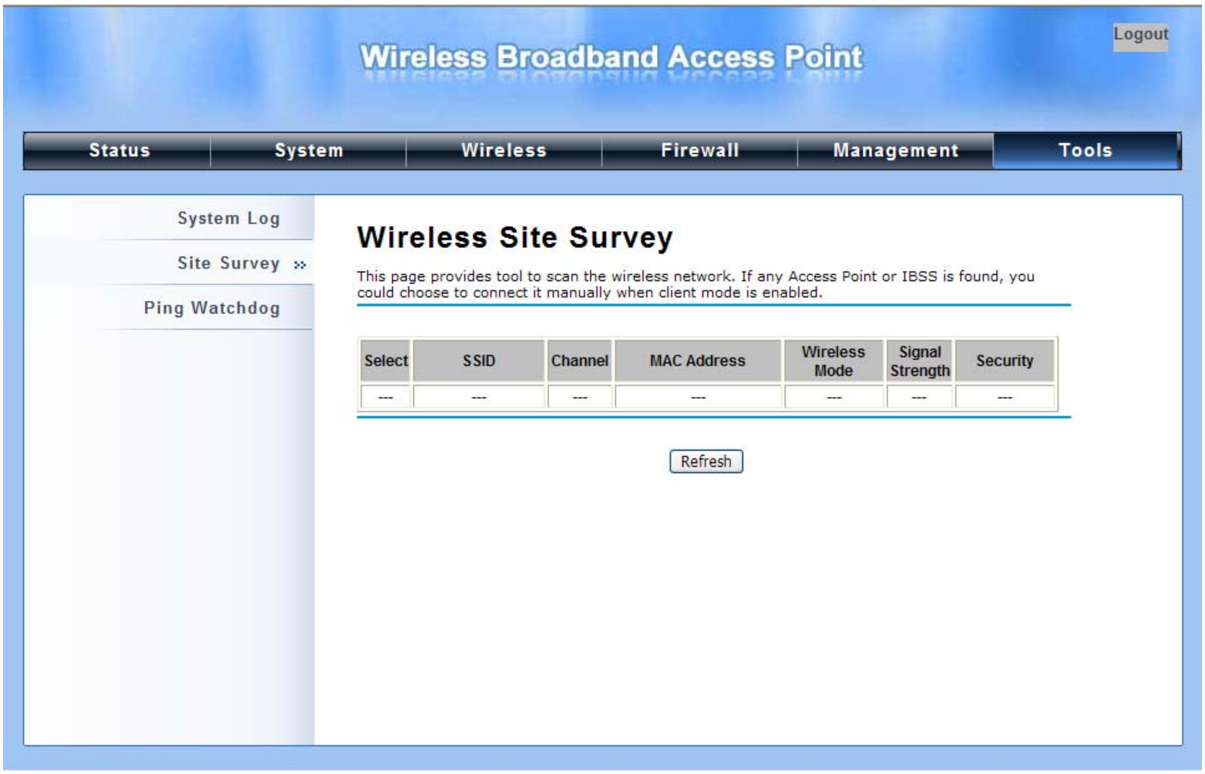
Remote Syslog Server

Enable Remote Syslog: Enable System log or not.

IP Address: Specify the IP address of the server.

Port: Specify the port number of the server.

Site Survey



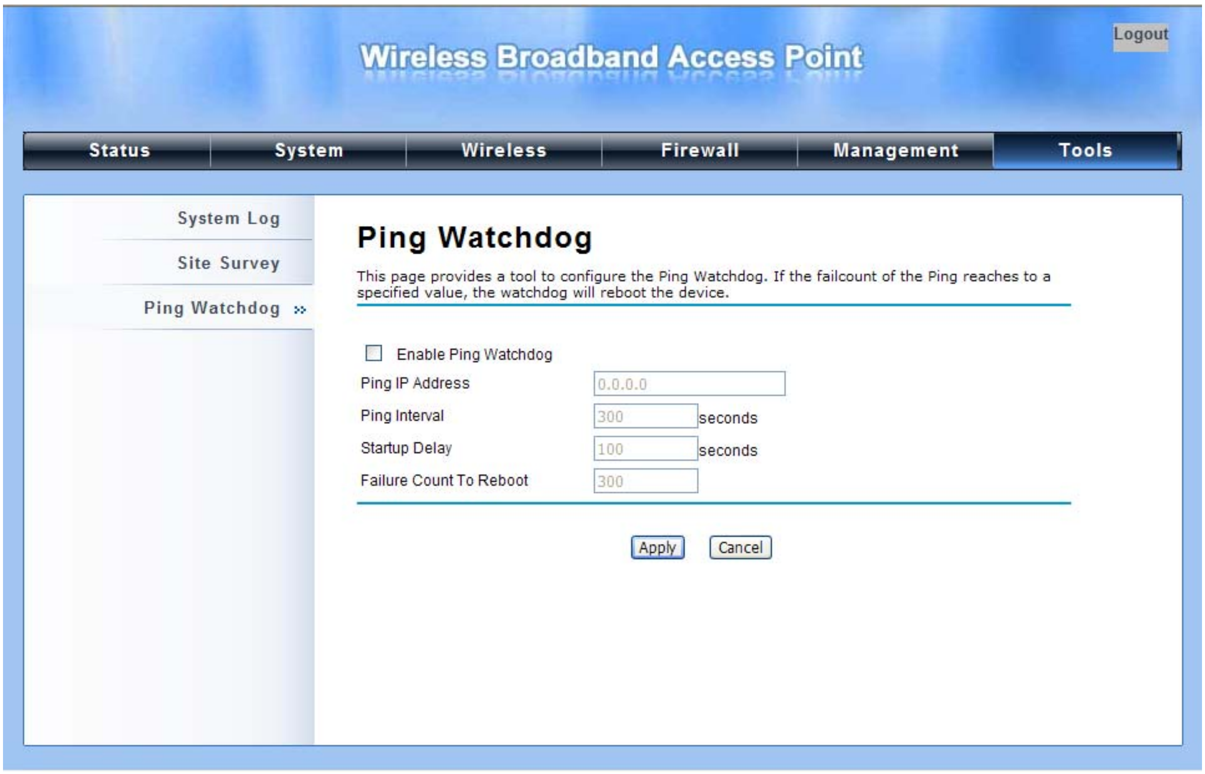
Wireless Site Survey

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	Channel	MAC Address	Wireless Mode	Signal Strength	Security
---	---	---	---	---	---	---

Figure 21 Site Survey

Ping Watchdog



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

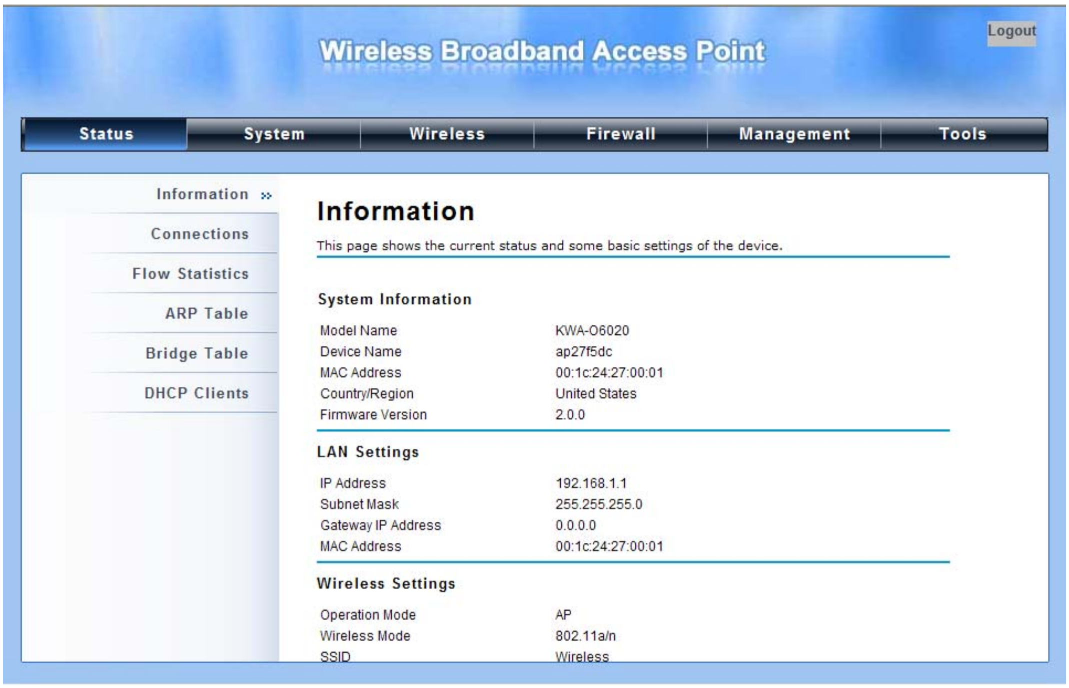
Ping IP Address	0.0.0.0
Ping Interval	300 seconds
Startup Delay	100 seconds
Failure Count To Reboot	300

Figure 22 Ping Watchdog

Chapter 6 Status

View KWA-O6020-I Basic Information

Open “**Information**” in “**Status**” to check the basic information of KWA-O6020, 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	KWA-O6020
Device Name	ap27f5dc
MAC Address	00:1c:24:27:00:01
Country/Region	United States
Firmware Version	2.0.0

LAN Settings

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway IP Address	0.0.0.0
MAC Address	00:1c:24:27:00:01

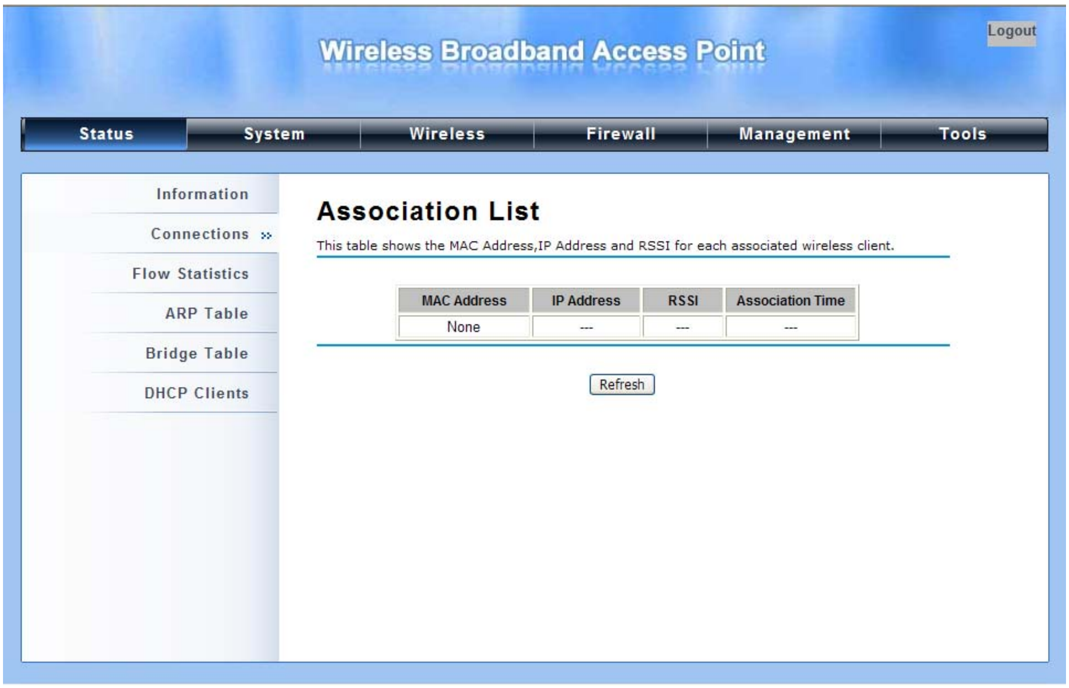
Wireless Settings

Operation Mode	AP
Wireless Mode	802.11a/n
SSID	Wireless

Figure 23 Basic Information

Association List

Open “**Association List**” in “**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

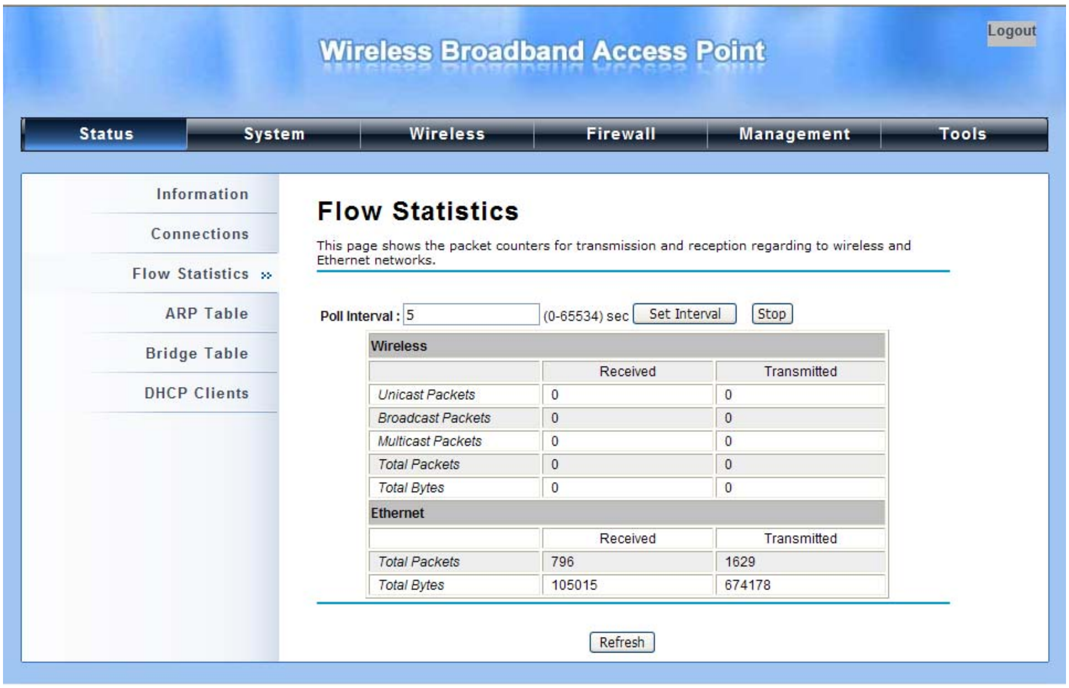
This table shows the MAC Address,IP Address and RSSI for each associated wireless client.

MAC Address	IP Address	RSSI	Association Time
None	---	---	---

Figure 24 Connection

View Network Flow Statistics

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



Flow Statistics

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

Poll Interval : 5 (0-65534) sec

Wireless		
	Received	Transmitted
Unicast Packets	0	0
Broadcast Packets	0	0
Multicast Packets	0	0
Total Packets	0	0
Total Bytes	0	0
Ethernet		
	Received	Transmitted
Total Packets	796	1629
Total Bytes	105015	674178

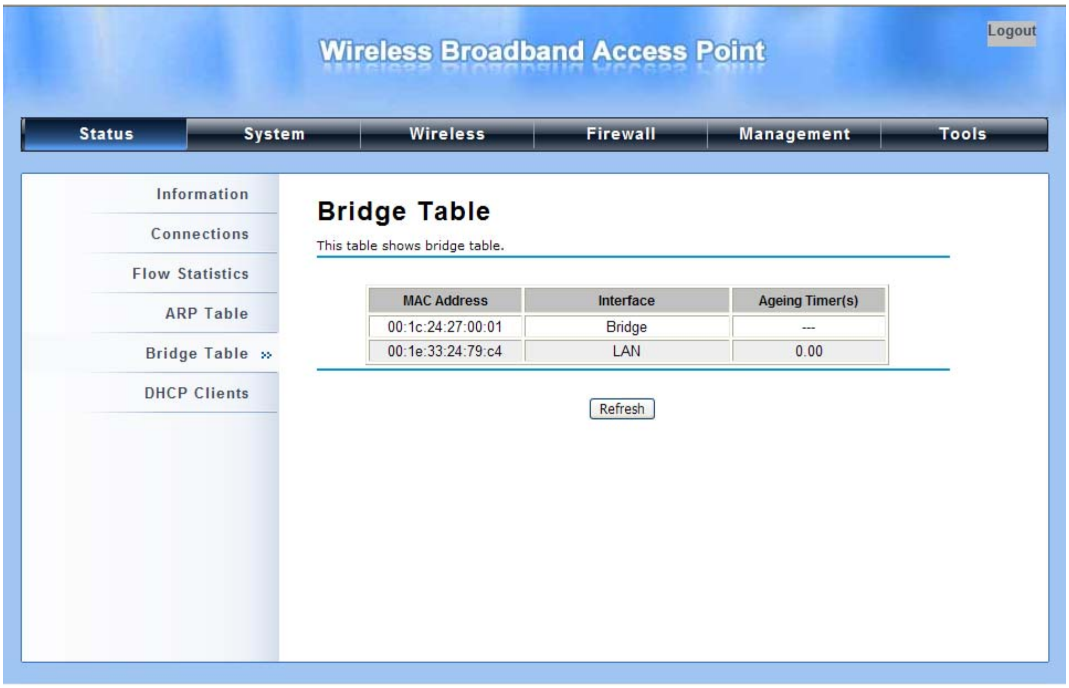
Figure 25 Network Flow Statistics

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 Bridge Table

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



Bridge Table

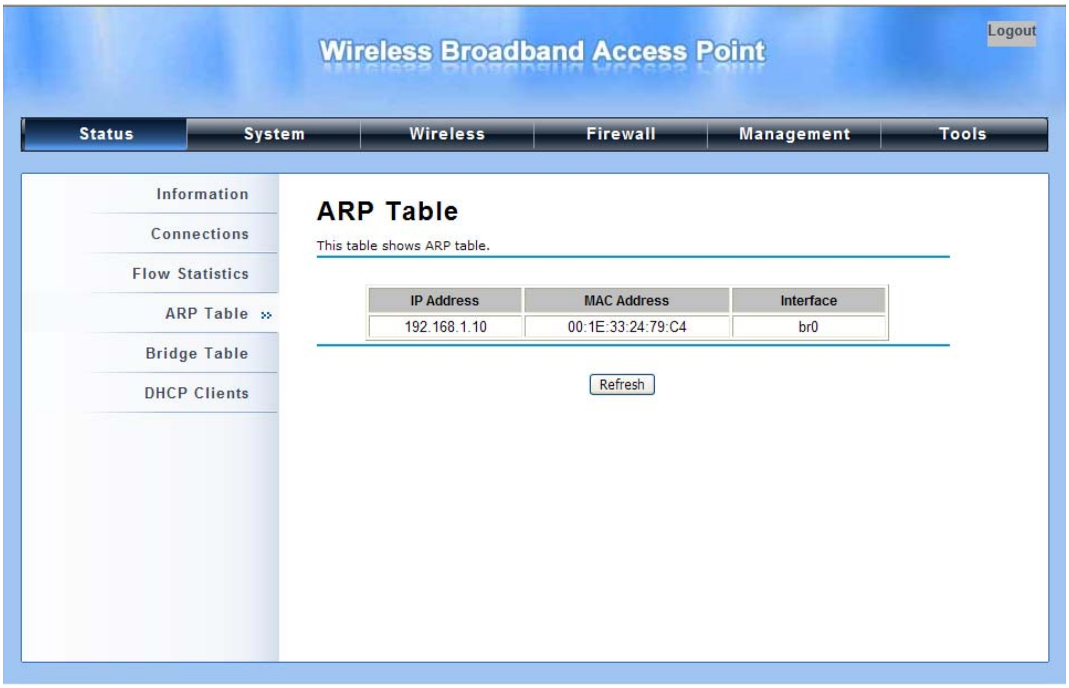
This table shows bridge table.

MAC Address	Interface	Ageing Timer(s)
00:1c:24:27:00:01	Bridge	---
00:1e:33:24:79:c4	LAN	0.00

Figure 26 Bridge Table

View ARP Table

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



ARP Table

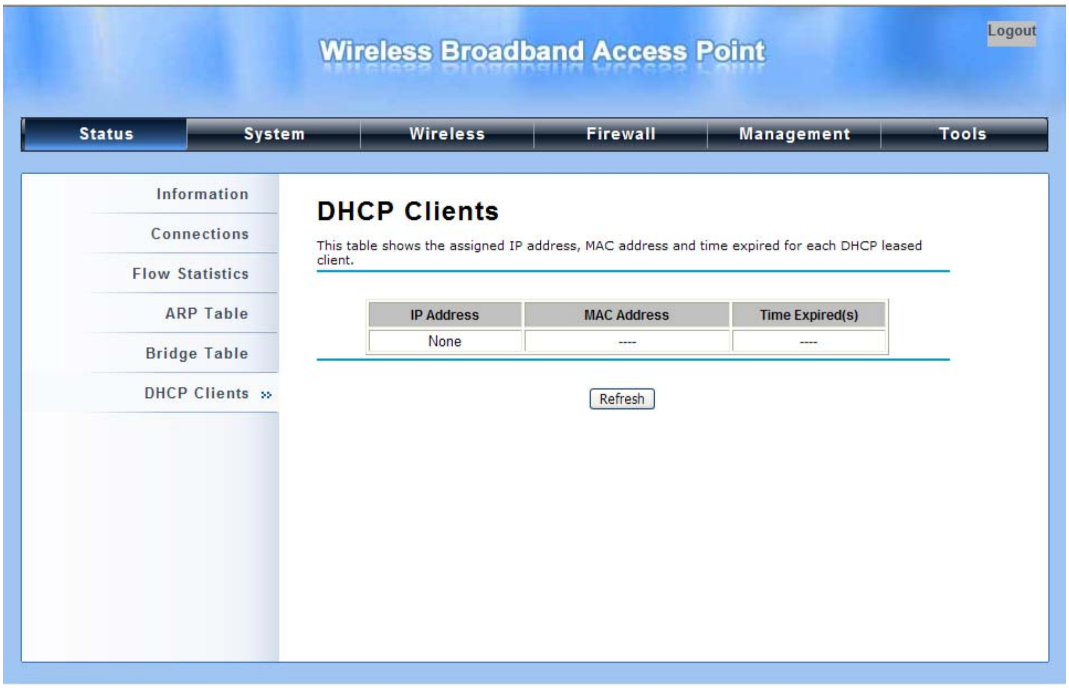
This table shows ARP table.

IP Address	MAC Address	Interface
192.168.1.10	00:1E:33:24:79:C4	br0

Figure 27 ARP Table

View DHCP Table

Open “**DHCP Client List**” 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)
None	----	----

Figure 28 DHCP Table

Chapter 7 Troubleshooting

This chapter provides troubleshooting procedures for basic problems with the KWA-O6020-I. For warranty assistance, contact your service provider or distributor for the process.

Q 1. How to know the MAC address of KWA-O6020-I?

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

1. Each device has a label posted with the MAC address.
2. On KWA-O6020-I Web-based status interface, you can view the MAC Address from "View KWA-O6020-IBasic 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**" or by doing hardware reset via the reset button.

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 can not access the Web-based management interface?

Please check the followings:

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

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

- Since KWA-O6020-I comes with a built-in directional antenna, it is recommended make KWA-O6020-I 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.