WI-OS-V2.0 User Manual

Version	Editor	Date	Approved
V2.0	Shirley	17/5/2018	John

OVERVIEW....1
1. CHAPTER 1: MAIN MENU....2
1.1 STATUS....2
1.2 STATISTICS....4
1.3 CONNECTIONS....5
2 CHAPTER 2:WIZARD....7
2.1 THE STEPS....7
3 SYSTEM....12
3.1 SYSTEM SETTINGS....12
3.2 PASSWORD SETTINGS....13
3.3 FIRMWARE UPGRADE....14
3.4 BACKUP/RESTORE....15
3.5 REBOOT DEVICE....16
3.6 USER CERTIFICATES....16
3.7 RADIUS SETTINGS....17
4 NETWORK....19
4.1 NETWORK SETTINGS....19
4.2 SNMP SETTINGS....23
4.3 VLAN SETTINGS....24
4.4 BRIDGE INFO....36
4.5 ARP INFO....37
5 WIRELESS....38
5.1 BASIC SETTINGS....38
5.2 VAP SETTINGS....50
5.3 ADVANCED SETTINGS....51
5.4 ACCESS CONTROL....54
5.5 THROUGHPUT CONTROL....56
6 TOOLS....57
6.1 SERVICES....57
6.2 SPEED TEST....58
6.3 SITE SURVEY....59
6.4 SYSTEM LOG....60
6.5 NETWORK PING....61
6.6 PING WATCHDOG....62

6.7 DEVICE DISCOVERY..... 64
6.8 ANTENNA ALIGNMENT.....64
6.9 NETWORK TRACEROUTE.....65

Overview

WI-OS V2.0 is the new generation of Wi-Tek's intuitive and versatile software technology. t he document details the method of the user to use WI-OS V2.0.

Following is WI-OS V2.0 support product list:

WI-CPE211, WI-CP214SMA, WI-CPE513,WI-CPE515, WI-CPE514SMA, WI-CPE517, WI-CP E518.

1. Chapter 1: Main Menu

1.1 Status

The page real-time display system "device info", "wireless parameters", wireless LAN and wired LAN throughput monitoring, and network status information.



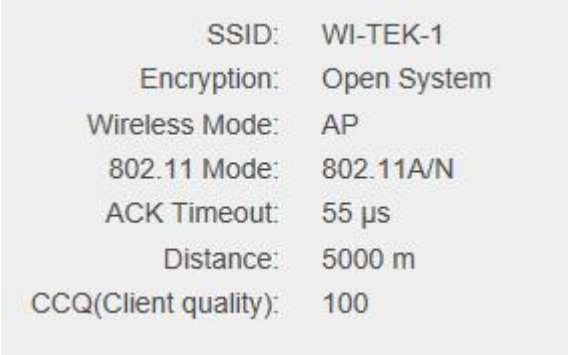
The device information area:



MAC Address	Display the device's MAC address.
Device Name	Display the device name or the definition of the device identifier.
Firmware Version	Display software version.
Country/Region	Displays the user locale or country defaults to the United States.
Working Time	Displays the total amount of time that the device is running, since the

	most recent reboot or software upgrades.
LAN IP Address	Displays the LAN IP address of the device.
LAN Subnet Mask	Displays the LAN Subnet Mask of the device.
LAN Default Gateway	Displays the LAN Default Gateway of the device.

Wireless information area



SSID — Displays the wireless network name (SSID). Wireless network name depends upon the wireless mode selected.

- In Access Point mode， this displays the SSID configured on the device using the Wireless page.
- In Station mode，this displays the SSID of the AP the device is associated with.

Encryption — Displays the encryption for your wireless network, WI-OS supported encryption modes: open system, shared key, Legacy 802.1x, WPA with Radius, WPA2 with Radius, and WPA-PSK, and WPA2-PSK. Default for open systems. If you need to modify the encryption method, please refer to the VAP settings.

Wireless Mode — Displays the working mode of the wireless interface, WI-OS supports 4 modes: AP、Wireless Client、Bridge、AP Repeater。 The system defaults to AP mode.

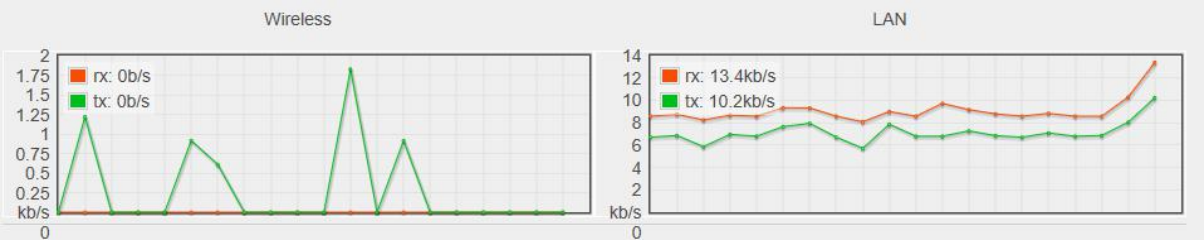
802.11 Mode — Displays the current system sets the wireless protocol, the default is 802.11A/N.

ACK Timeout — This represents the ACK frames received the maximum waiting time between wireless devices.

Distance — Displays the distance between the current one-to-one device (unit: m).

CCQ(Client quality) — The index is used to evaluate the quality of wireless clients to connect (CCQ), larger and if wireless link quality can reach 100, it's in a perfect link state.

Throughput monitoring



This graphic displays in real time the current wireless LAN and wired LAN data transmission, scale and throughput of the chart dimensions (b/s, KB/s, MB/s) depending on the variation of the average throughput. Auto update statistics. By default, displays only the throughput of the wireless LAN and the LAN1 graphic, open the LAN2 interface power supply, LAN2 port connected equipment after the LAN2 throughput graph is displayed. Disabling the wireless interface case, wireless LAN throughput graph will not be displayed.

Network interface status display area

Interface	Status	Channel	Rate
LAN	Up	N/A	100M/Full-Duplex
Wireless	Up	5745MHz (149)	Auto

This area displays real-time network connection status and the current network interface data transfer rate. Status of automatic updates. LAN2 interface not connected is displayed by default, because the LAN2 interface is turned off by default, if you need to open the LAN2 interface, you need to LAN2 interface power supply enabled in your network settings page.

1.2 Statistics

Traffic statistics page, you can display the number of wireless and wired networks to send and receive packets, and set the auto-refresh interval.

Interface methods: Main->Statistics.

Statistics

This page shows the packet counters for both transmission and reception over the respective wireless and Ethernet networks.

Poll Interval: 5 (0-65534) Sec Set Interval Stop

	Received	Transmitted
Wireless		
Total Packets	0	1065
Total Bytes	0	243.4KB
Ethernet		
Total Packets	36195	35065
Total Bytes	3.6MB	3.7MB

Refresh

Poll Interval Page auto-refresh interval to obtain statistical information, the default is 5 seconds. Click on modify the parameter <Set Interval> commit configuration.

Stop Stop automatic refresh of the page access statistics.

Statistical tables description:

Statistical information for the wireless network:

Wireless		
Total Packets	0	1075
Total Bytes	0	245.7KB

Statistics for the wired network port 1:

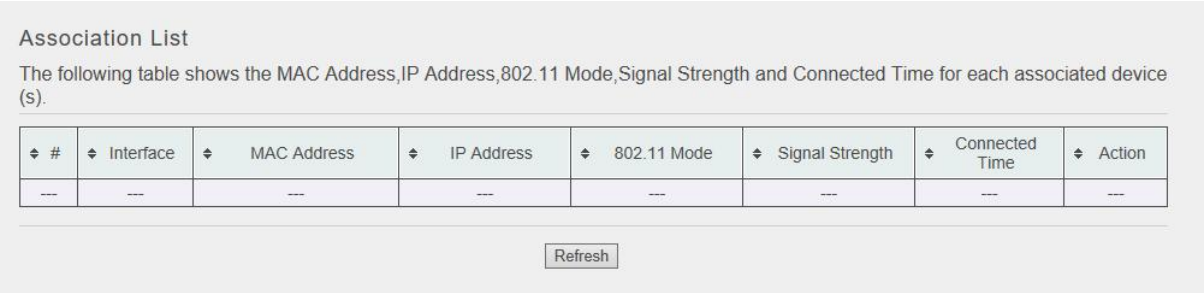
Ethernet		
Total Packets	36451	35337
Total Bytes	3.7MB	3.7MB

1.3 Connections

Shows the MAC Address, IP Address,802.11 Mode, Signal Strength and Connected Time for each associated device(s).

Interface methods: Main->Connections.

1) AP mode the association list description:



Interface VAP interface clients connect to the SSID.

MAC Address Client device's MAC address.

IP Address Client device's IP address.

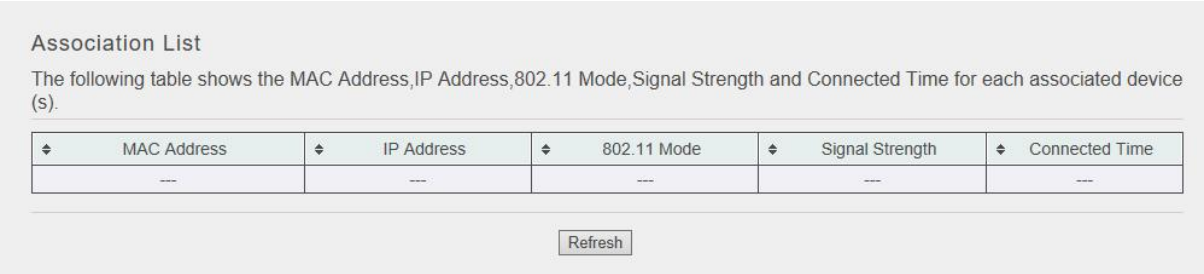
802.11 Mode Default to 802.11A/N mode (802.11A and 802.11A/N).

Signal Strength AP receives the signal strength from the client, the smaller the number indicates that the received signal strength is strong.

Connected Time Duration of the clients connected to the AP.

Action For clients that do not want to connect you can disconnect.

2) Station mode the association list description:

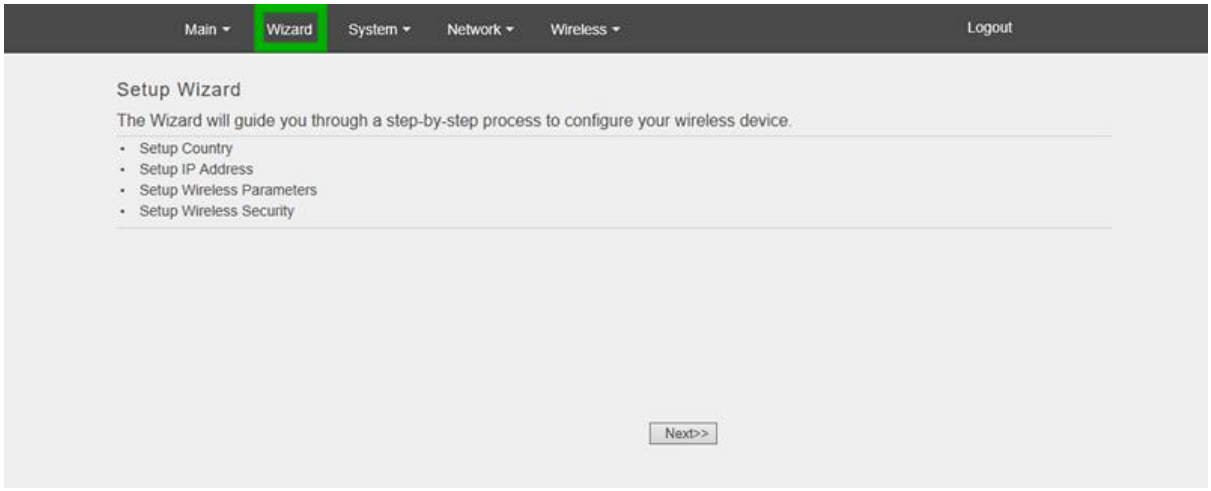


MAC Address	MAC address of sta.
IP Address	IP address of sta.
802.11 Mode	Default to 802.11A/N mode (802.11A and 802.11A/N).
Signal Strength	Clients receive AP signal strength, the smaller the number indicates that the received signal strength is strong.
Connected Time	Duration of the clients connected to the AP.

2 Chapter 2:Wizard

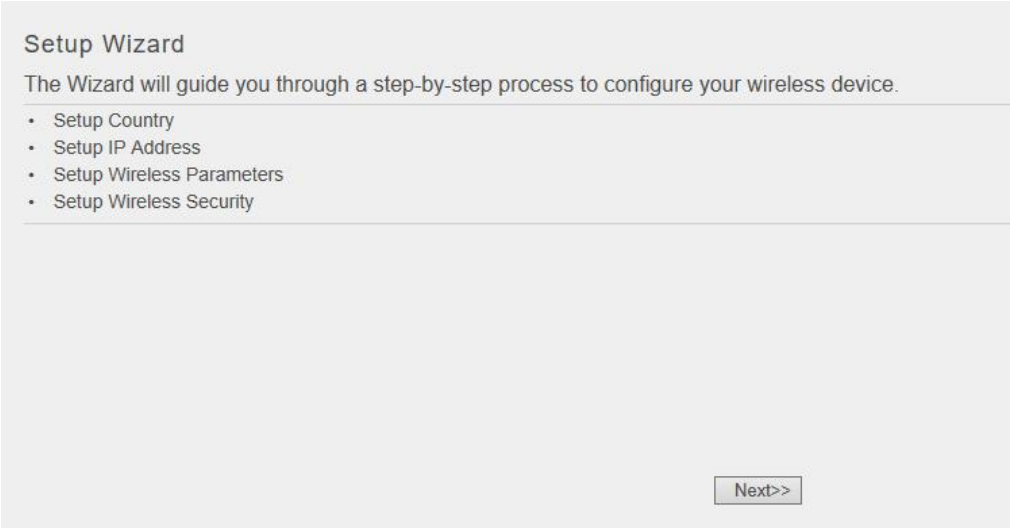
Use this wizard, you can set the basic network parameters.Even if the network you do not known, you can also set up it according to the wizard.

Interface methods:Wizard.



2.1 The Steps

1. It show the configuration for wizard.



Setup Country — You can select country what you want, Channel and power will be different in different countries

Setup IP Address Assignment — Get IP Address from the DHCP Server or you set up the IP Address;

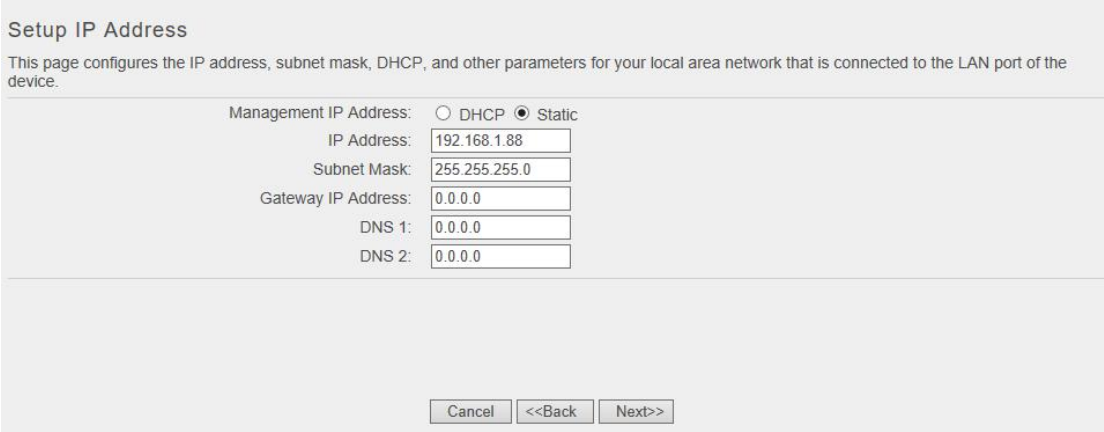
Setup Wireless LAN Interface — Setup the configuration about wireless;

Setup Wireless Security　　Setup Wireless security authentication;

2. Click ‘Next’,you will setup country



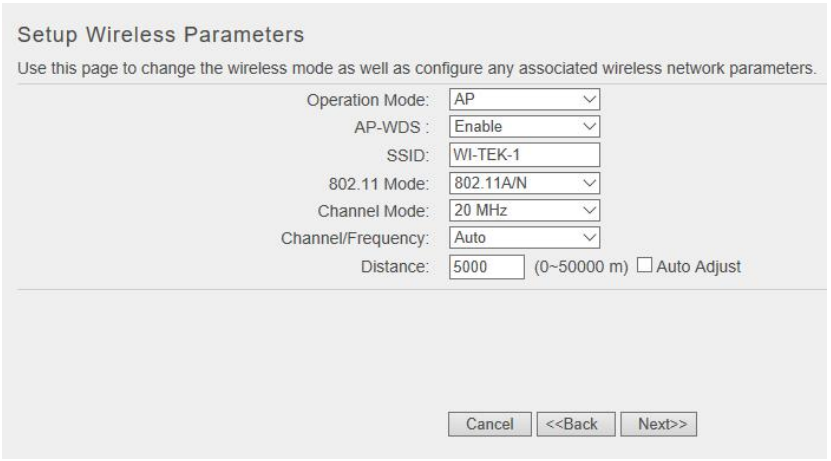
3. Click ‘Next’,you will setup the IP Address Assignment



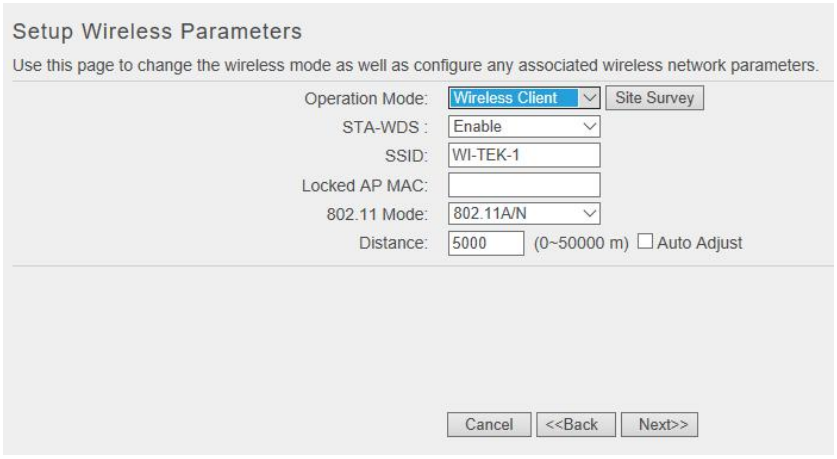
If you choose ‘DHCP’ device will get IP from DHCP Server,or you must setup IP address.

4. Click ‘Next’, setup the configuration about wireless

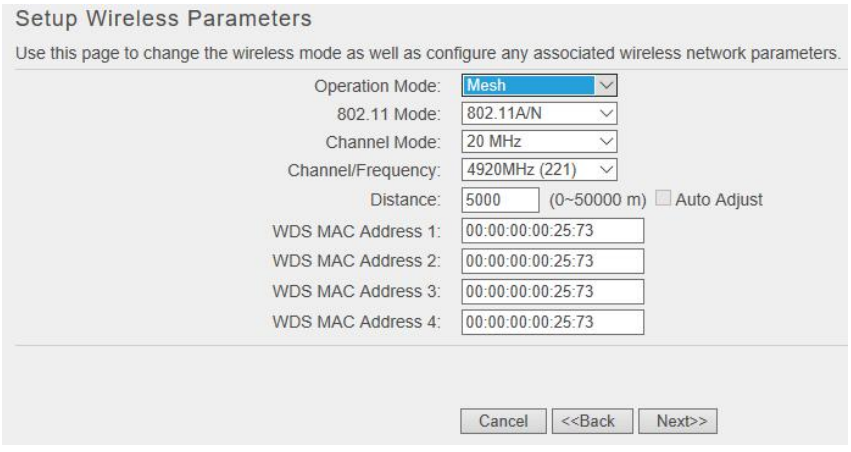
A、Operation Mode is AP



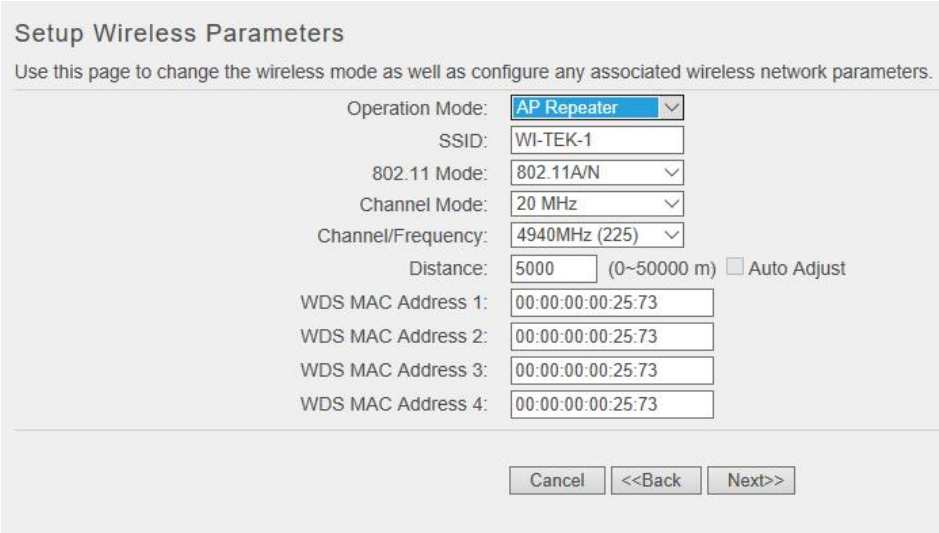
B、Operation Mode is Wireless Client



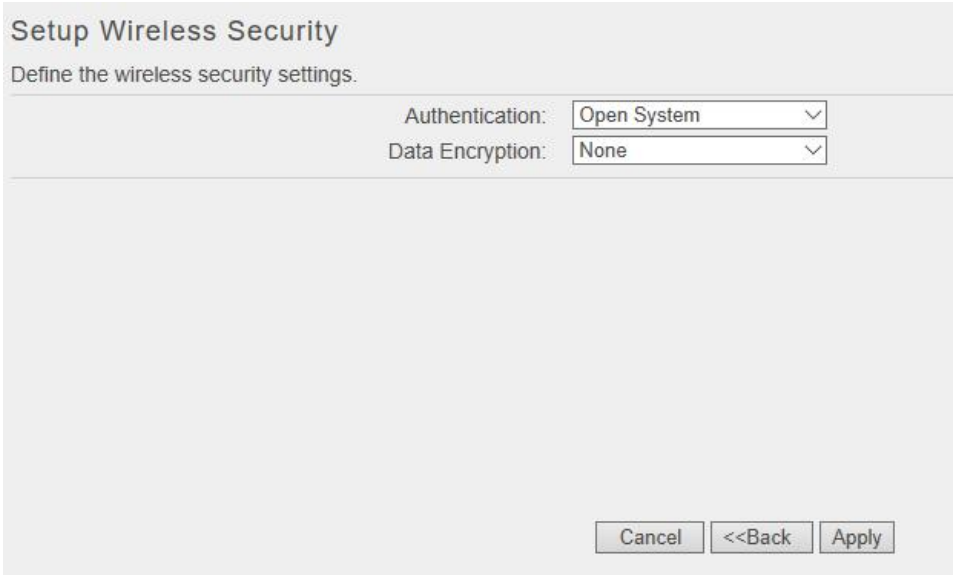
C、Operation Mode is Mesh



D、Operation Mode is AP Repeater



5. Click ‘Next’, setup the configuration about security.



Open System　It is open network, no security.

Shared Key　Shared key authentication（SKA）,both the wireless access points (AP) and all clients share the same key.

WPA with Radius/WPA2 with Radius　It work with Radius Server,and I suggest that user use this authentication;

WPA-PSK/WPA2-PSK/WPA-PSK&WPA2-PSK　I suggest that user use this authentication, Setup is easy and safe;

6. Click ‘Apply’, and enter wait page.

Change settings successfully! This device has been reboot, you have to login again.
Please wait for 58 seconds before attempting to access the device again...

3 System

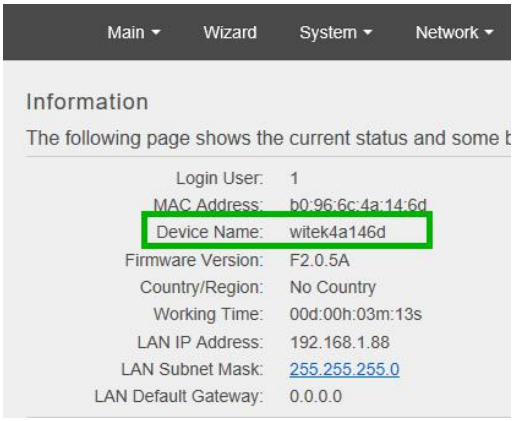
3.1 System Settings

Use this page to configure the Country、modify the device's name、Time Zone of device.

1. Device configuration:

A、Device name where we can set a name for our device, we can view the status page after you have finished configuring the configuration:





B、Country/region selection, user can choose according to their own country, which directly affects the 5G device support for 5G band:



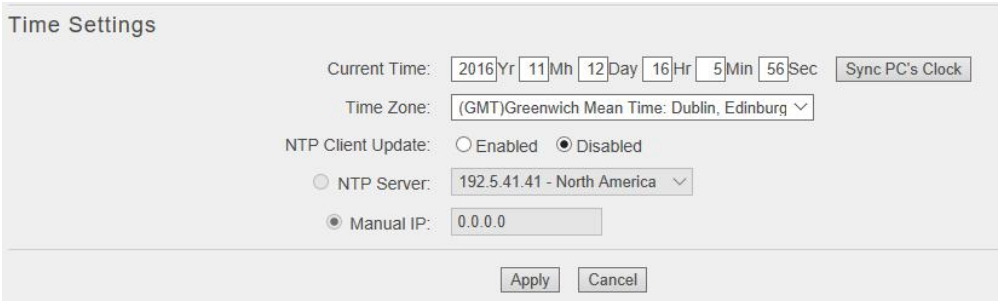
2. Time zone settings:

A、Users can set up an NTP server for your devices to keep the accuracy of the equipment time:

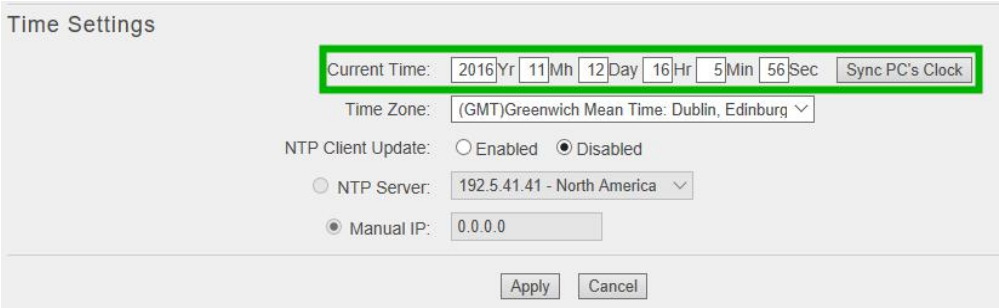
First select the time zone for your area and enable NTP client updates, real-time updates to keep time.

Second, we can choose whether to use the NTP server is manually configured IP.

Note that if you select a NTP server, devices must be able to connect with the NTP server, the same manually configured IP also must be able to connect and support the NTP service.



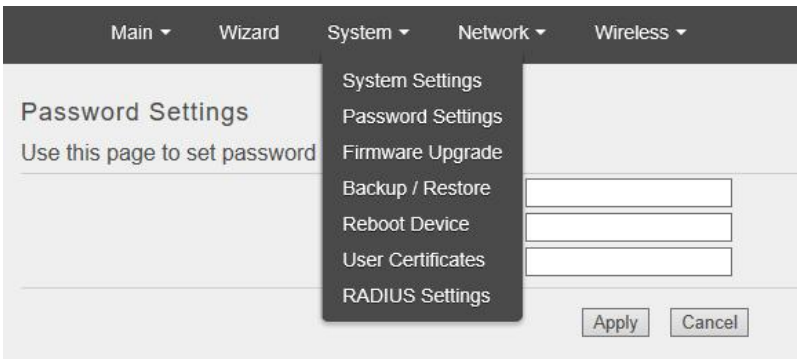
B、Click after the application is configured, you can see good time synchronization.



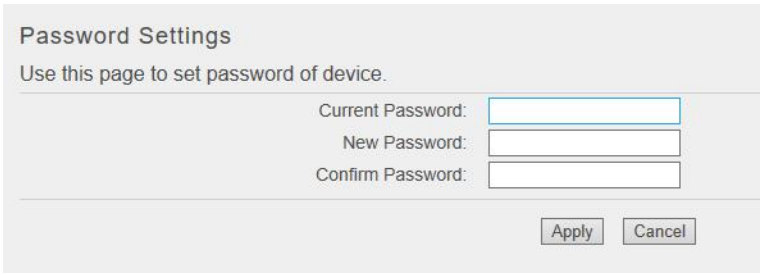
3.2 Password Settings

For the safety of equipment, users often need to be modified after the purchase of equipment and equipment for initial logon password.

1. Enter the password settings page:



2. New password for the configuration you want to modify, and click apply:



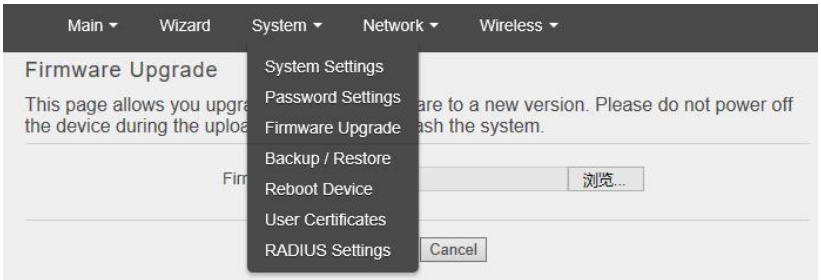
3. Re-enter the page, enter a new password to log in:



3.3 Firmware Upgrade

When a new version is released, when the device needs to be upgraded, can enter the operating firmware upgrade page.

1）Enter firmware upgrade page:



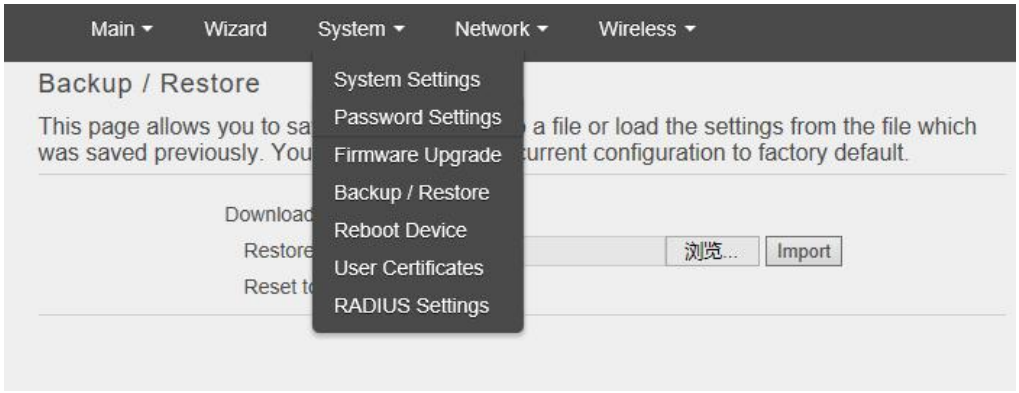
2）Select the version to upgrade, click upgrade and into waiting for the upgrade page. Attention, do not power off the upgrade process, so as to avoid damage to the system:



3.4 Backup/Restore

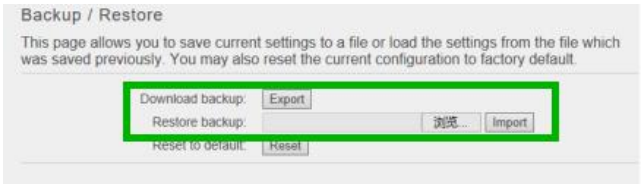
This page allows you to save current settings to a file or load the settings from the file which was saved previously. You may also reset the current configuration to factory default.

1. Enter the backup/restore factory setting page:

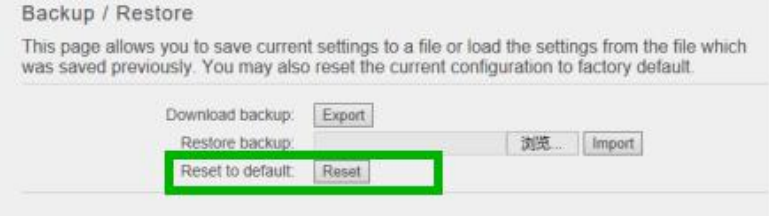


2. Download backup: back up the device saves all configuration download, which contains the wireless configuration, network configuration, system configuration, and so on all other configurations.

   Restore backup: save configuration before importing equipment, restore the previous configuration, eliminating the reconfiguration of the trouble again.



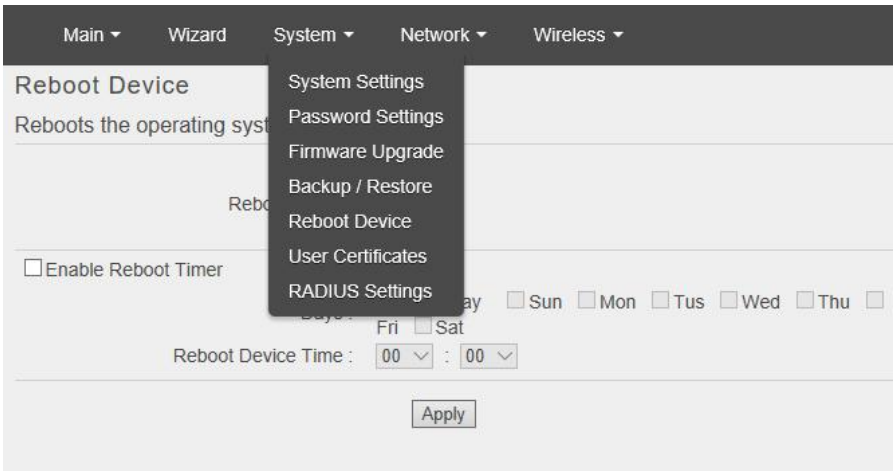
Restore factory settings: all configuration to clear and restore the system to factory default configuration.

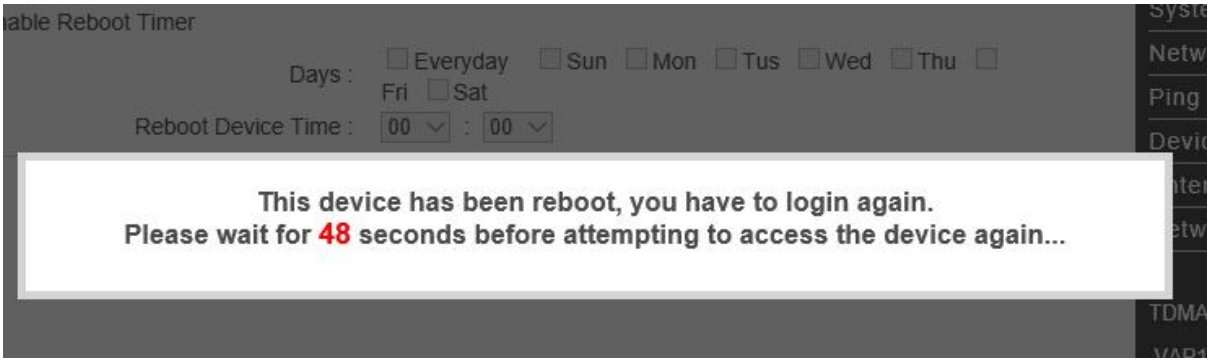


3.5 Reboot Device

Restart device: when users need to hot reset or through the remote restart device, can enter the reset device in action page to restart operations.

Click "reboot", the device will reboot and enter the wait page.

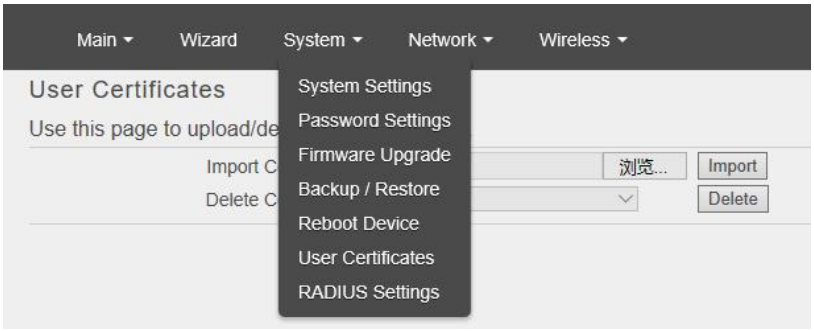




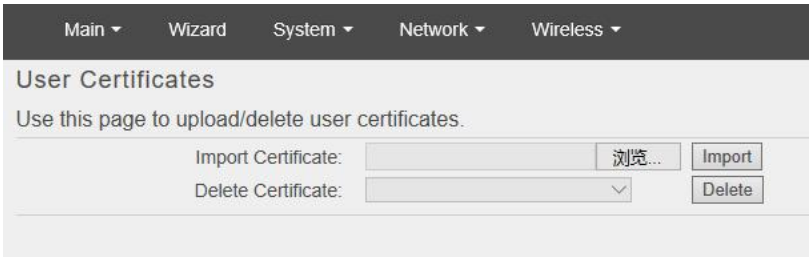
3.6 User Certificates

When the device requires WPA Radius when TLS authentication, user settings for the certificate is required, the user certificates generated by the Radius Server.

1. Enter the user certificate settings page.



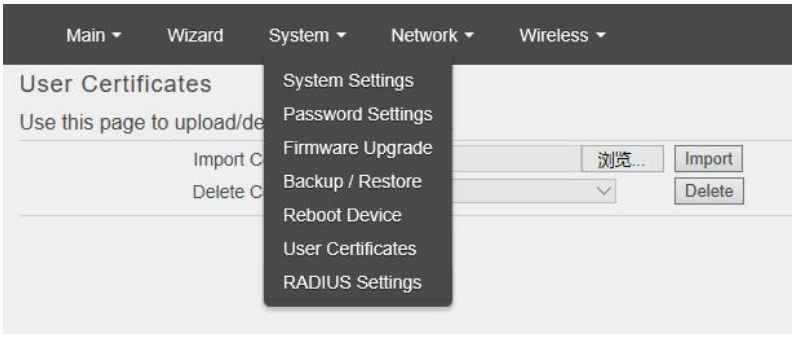
2. Certificate Import device can remove certificates.



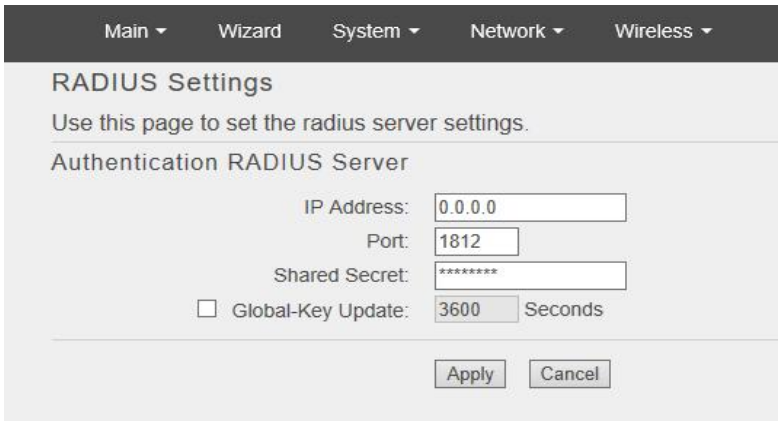
3.7 Radius Settings

When the device when Radius Authentication is required, some related to Radius server settings.

1. Enter the Radius settings page.



2. Radius settings:



IP address　　the IP address of the Radius server.

Port　　authenticated communication port number.

Shared key between the Radius client and the Radius Server for authentication key.

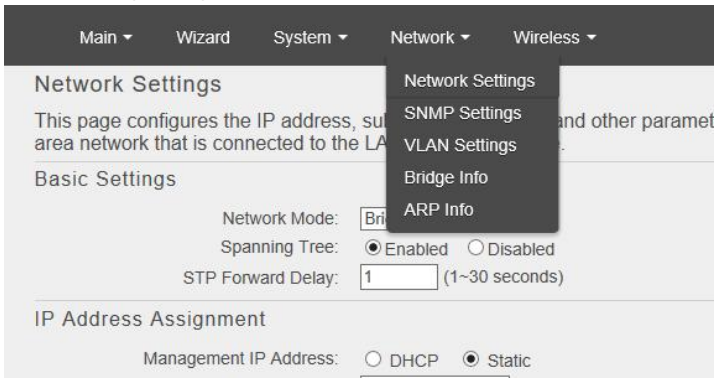
Global key updates password update key update is not what we say, but how you set the WIFI password, it is converted to 16 binary algorithm to encrypt the key update time is here said the 16 binary encryption algorithms change, but your password is unchanged, thus more difficult to crack passwords.

4 Network

4.1 Network Settings

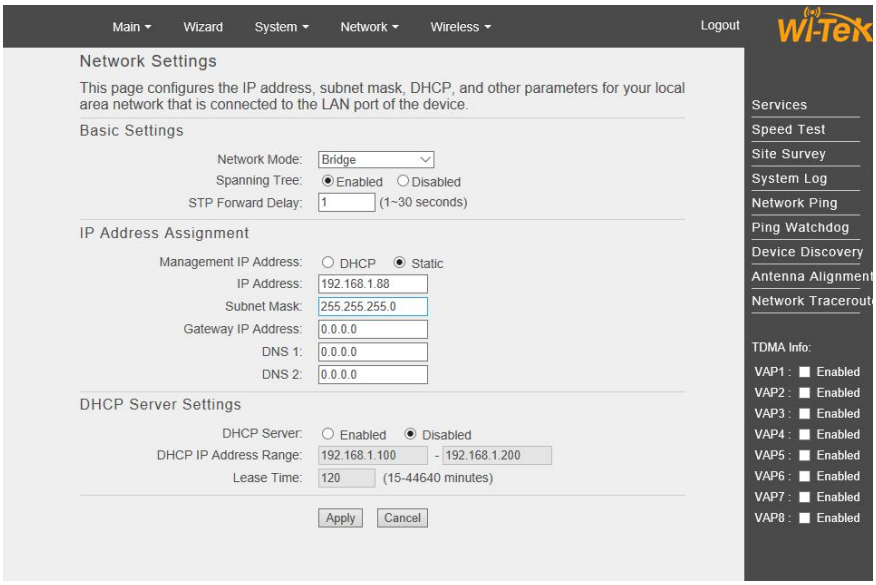
One new device, users often require basic network settings for network communication, this document provides instructions for some basic network configuration.

1. Enter the network settings page:

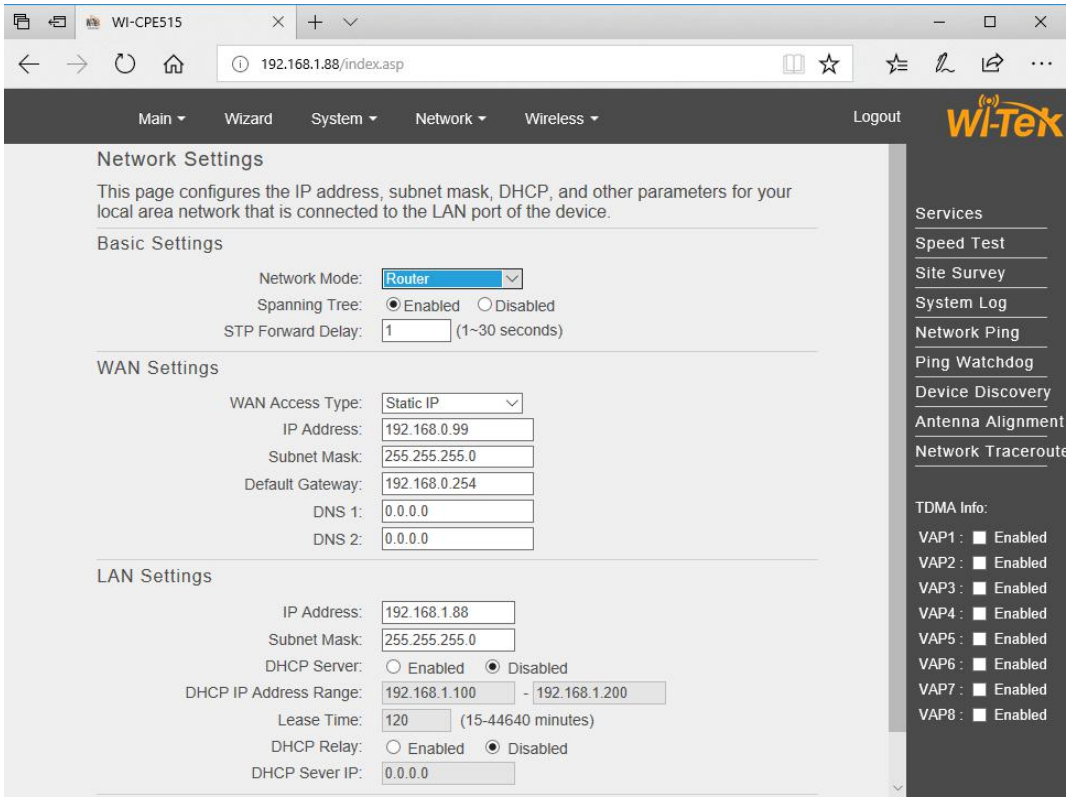


2. Basic settings network mode select: used to select the device model is routing or bridge mode.

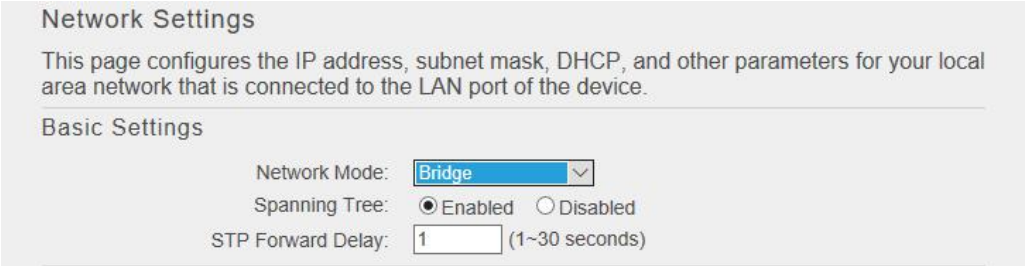
A、Bridge mode: device without routing capabilities, data transmission at the MAC layer, apply to local area network within the network.



B、Routing mode: If the device is required in the network as a foreign function with the routing address, which needs to access the superior operator's network (Internet), then the device is configured for routing mode.



C、Other basic settings:

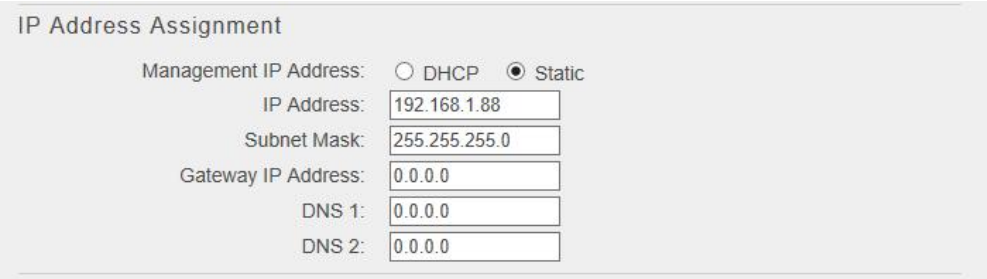


POE Passthrough :LAN2 interface power supply, to enable this feature LAN2 means devices can be powered through the network to other devices.

Spanning tree (STP): this Protocol can be used to build a tree topology in networks, eliminating loops in the network, and can be realized through certain path redundancy, but not be able to realize the path redundancy.

STP forward delay: spanning tree Protocol (STP) build a tree topology to listen or study time, this defaults to 1s.

D） IP address assignment: Select Device IP address access, DHCP automatically or manually set static.

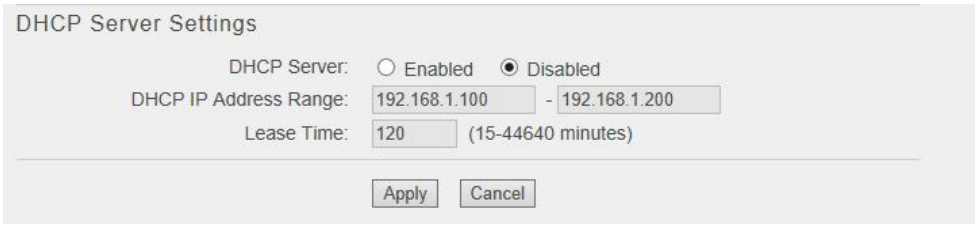


DHCP access: device to obtain an IP address automatically.

Static access: user ourselves according to uplink the network address of the device on its own configuration.

E）DHCP server settings:

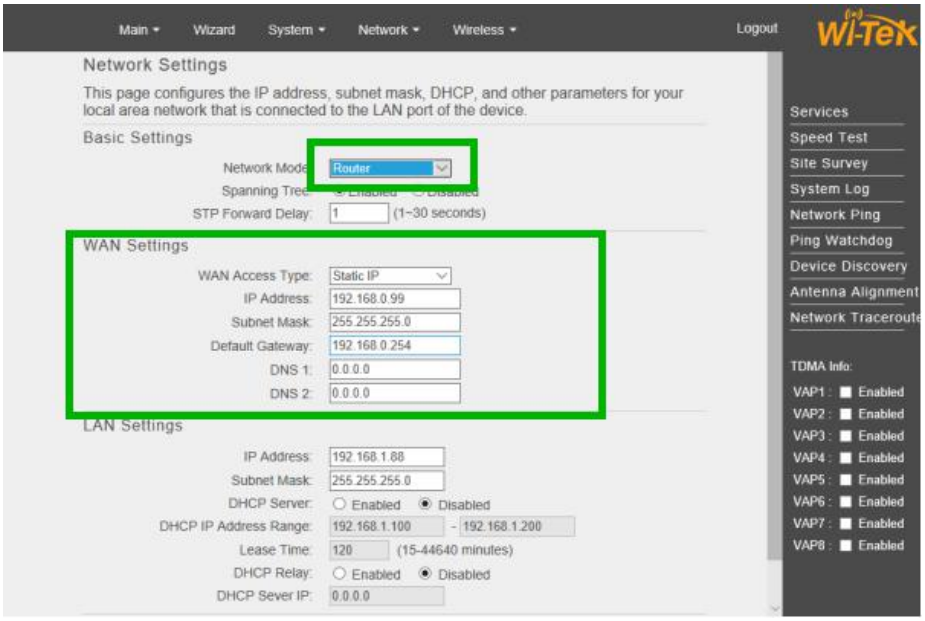
DHCP server: If you need the device to provide DHCP service, then enable this feature.

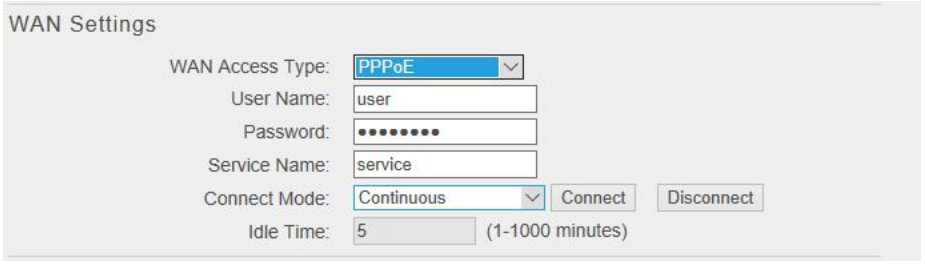


DHCP IP address range: used to set the DHCP server to assign IP address ranges. Note that this section must configure the management IP address on the same network segment.

Lease time: used to determine the user's IP address by the DHCP server to obtain valid, due to renew.

F、WAN port settings: device interface configured for routing mode, WAN communication between the interface and the next-hop routing, that is run with superior business network (Internet) communications interfaces. The interface can only connect to the cat, home cable, or by the network, cannot be used to connect a computer. The interface's IP address gets into a static configuration, DHCP access or PPOE dial-up access.





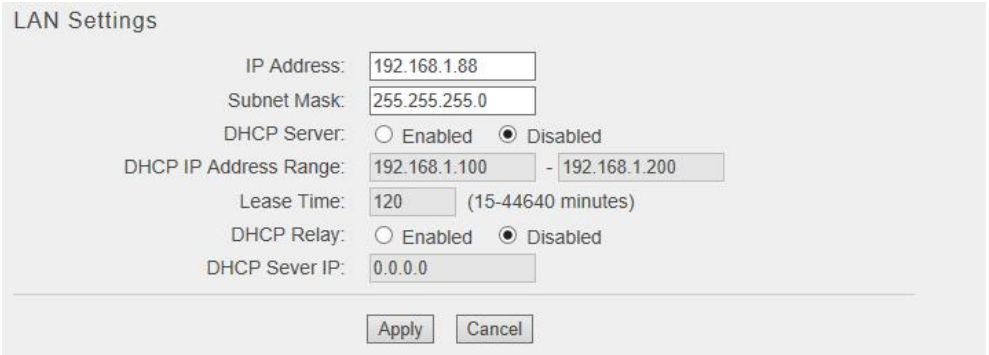
User name: dial-up account name.

Password: password for the dial-up.

Service name: If the server has set the server name, you will need to fill out, no, you do not need to fill in.

Connection modes: continuous, that is, continuous automatic dialing; on-demand, which flows only when dial-up connections; manual, user manual dial-up connection.

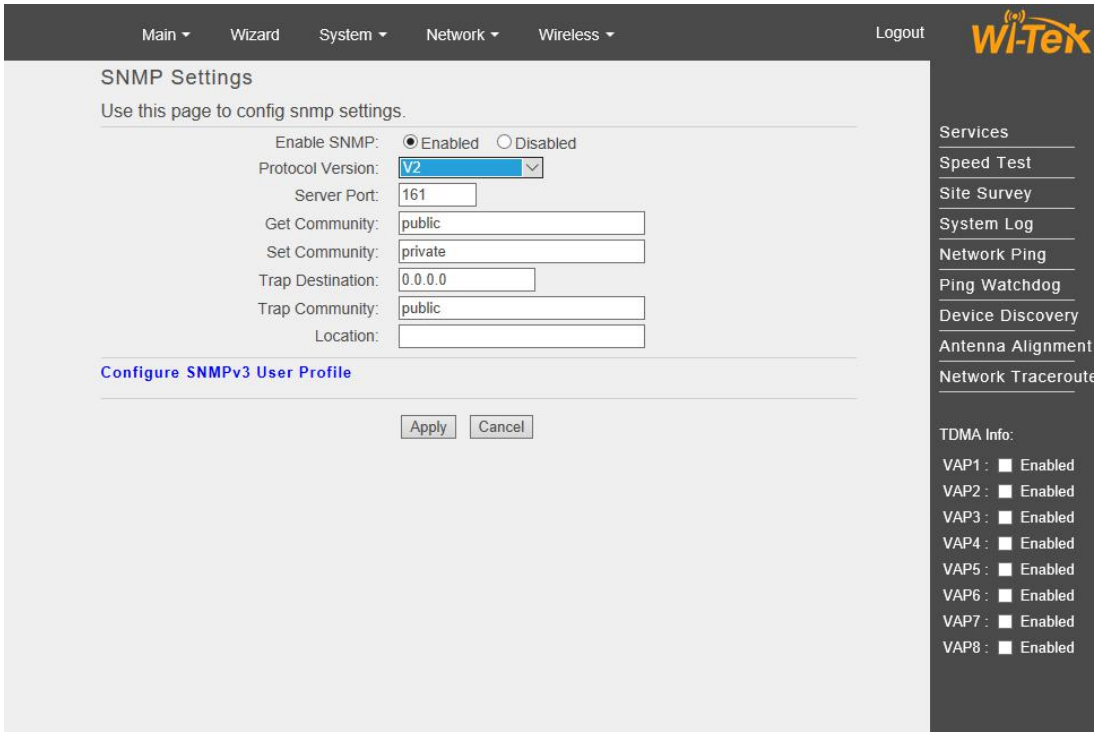
G、LAN setup and manage IP settings is bridge mode, which does not support the DHCP to obtain, only static manual settings. Also, if DHCP server is enabled, configuration of the DHCP server IP address range must also be manually configured IP address in the same network segment.



Note that in routing mode, LAN port can only be used to connect computer, can't connect to the cat, cat, home cable, otherwise it will cause the router to the Internet.

4.2 SNMP Settings

Simple Network Management Protocol（SNMP），Can support network management system, management many manufacturers of hardware and software platform on the Internet.



If use V2 protocol version only need to configure the following parameters:

Enable SNMP	Enable or disable SNMP;
Protocol Version	The SNMP protocol has three version,we support V2 and V3 protocol;The remote configuration and security in V3;
Server port	The port of SNMP server;
Get/Set Community	Use the default value;
Trap Destination	Trap will sent to the destination;
Trap Community	Use the default value;

If use the V3 protocol version also need to configure the following parameters (SNMPv3 users need to click on the configuration file will display the configuration options below)

Enable SNMPv3Admin	Enable or disable SNMPv3Admin;
Access Type	Access type has Read Only and Read/Write, Read/Write only used in Admin;
Privacy Protocol	Use the default value;

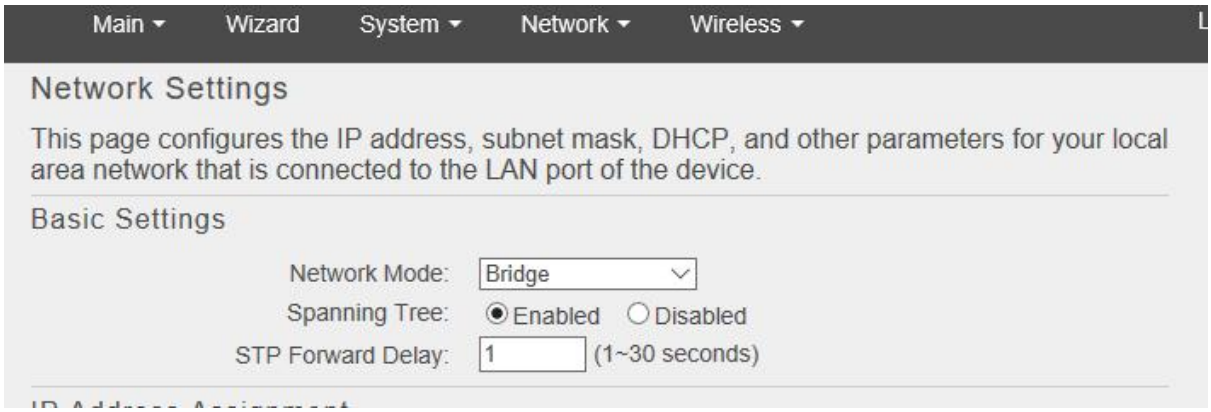
Enable SNMPv3Admin	Enable or disable SNMPv3Admin;
Access Type	Access type has Read Only and Read/Write, Read/Write only used in Admin;
Privacy Protocol	Use the default value;

4.3 VLAN Settings

VLAN Settings allow you to create Virtual Local Area Network (VLAN) on the device.

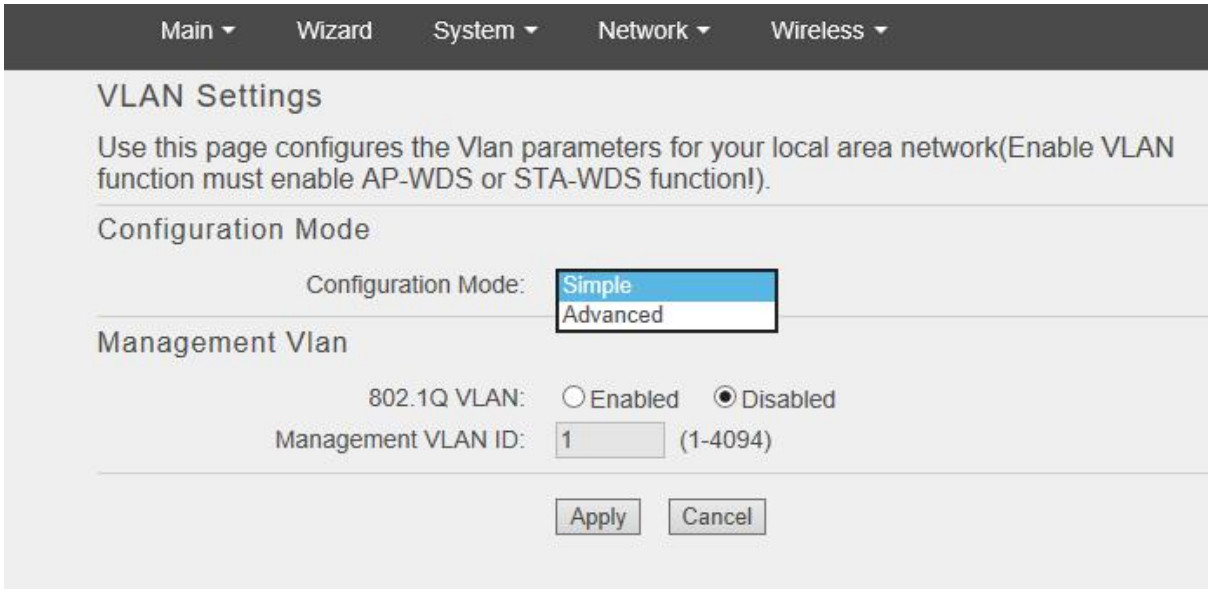
The VLAN technology is important for forwarding on Layer 2 networks. The VLAN technology is used to divide a physical LAN into multiple logical broadcast domains,each of which is called a VLAN. Each VLAN contains a group of devices that have the same requirements. If two devices are located on one LAN segment but belong to different VLANs, they do not send packets to each other. With VLAN, network is simplified，and network security is improved.

The VLAN Settings only exists in bridge mode, the Network Mode need to choose in the Network Settings: "Bridge":



VLAN MODE

The VLAN page has two views, Simple and Advanced.



Configuration Mode Select the appropriate mode for your application:

• **Simple** configures basic VLAN settings, If enabled, automatically creates a management Virtual Local Area Network (VLAN). The following basic configuration settings are available:

• **"Configuration Mode" on page 4**

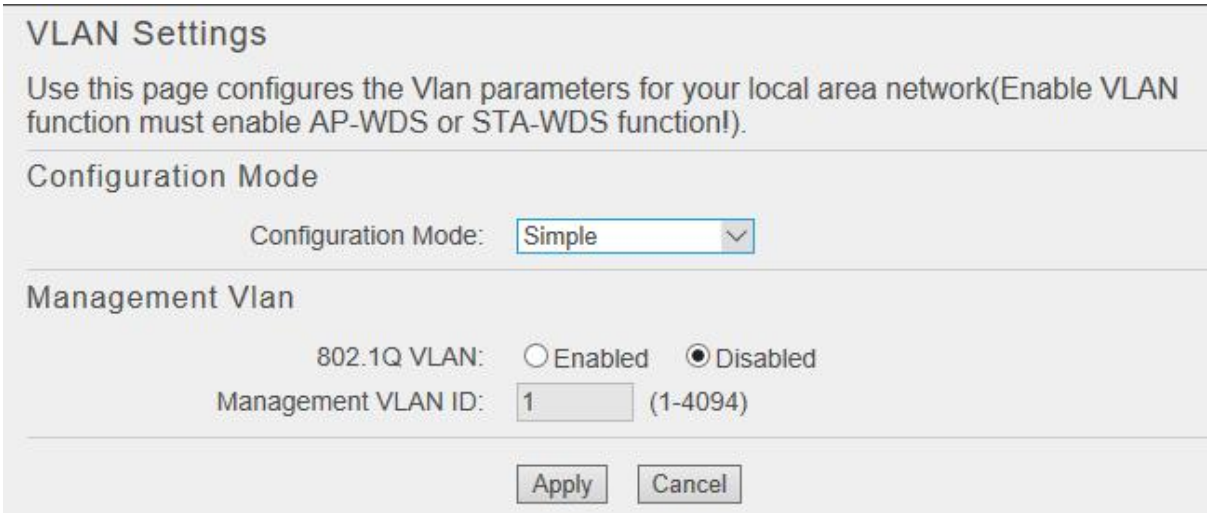
• **"Management Vlan" on page 5**

• **Advanced** Applies to scenarios where there are high requirements for VLAN settings. The network administrator can flexibly select which settings to use according to the requirements. Displays the advanced configuration settings, The following advanced configuration settings are available:

NOTE： Advanced mode configuration, the user is required to have some knowledge of VLAN network, if configured incorrectly, it is possible to cause the user can not access the device. If you have advanced VLAN configuration requirements, Please be configured according to the **configuration examples,** If there are other requirements, please contact: Wi-Tek.

Management Vlan

Available in Simple view . For the user to create a management VLAN automatically.



802.1Q VLAN： For setting the opening and closing VLAN. If enabled,automatically creates a management VLAN.

Management VLAN ID: For setting the management VLAN ID, Enter a unique VLAN ID from 1 to 4094.

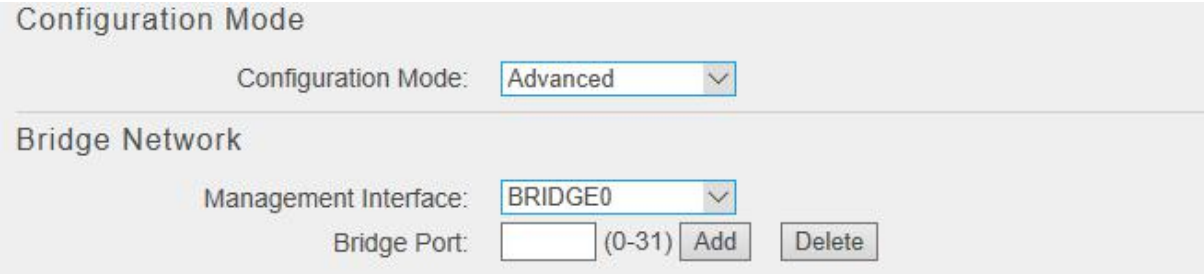
NOTE： If *Management VLAN* is enabled, then the device will not be accessible from other VLANs, including the untagged VLAN.

Apply: To save your changes, click **Apply**. If you do not change any configuration, then only refresh the page.

Cancel: Refresh the page to display the existing configuration of the device.

Bridge Network

Available in Advance view . You can set the management interface, and create or delete a bridge interface.



Management Interface: Select the bridge used for management.

Bridge Port: To add or delete the bridge interface. Enter a unique value from 0 to 31.

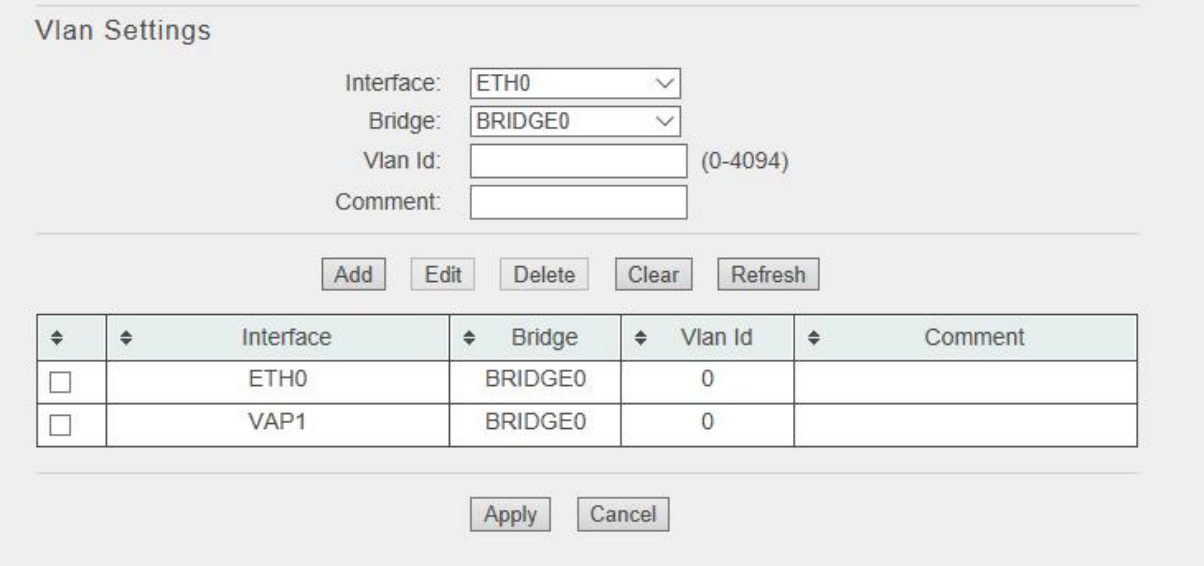
Add: Add a bridge interface.

Delete: Delete a bridge interface.

NOTE：A bridge interface cannot be deleted, if it is selected as the management interface ,or it contains other device ports.

Vlan Settings

Available in Advance view . Select the appropriate bridge interface and vlan id for your device interface.



Interface：Select the appropriate interface. If a interface of the device is disabled or not created does not appear in the drop-down list.

Bridge：Select the appropriate bridge. If a bridge interface of the device is disabled or not created does not appear in the drop-down list.

Vlan Id：The vlan id is a unique value assigned to each vlan at a single device; every vlan id represents a different vlan. The vlan id range is 0 to 4094. 0 represents the device interface without vlan.

Comment：You can enter a brief description of the purpose for the VLAN. Enter up to 32 characters.

Add：Add the above VLAN configuration.

Edit：Used with the following table. Modify vlan settings entries in the table. Only one entry in the table for editing.

Delete：Used with the following table. Delete VLAN Settings in the table, Every time you can delete multiple entries in the table.

Clear：Used with the following table. Clear the table for all configurations. But the configuration in the management interface will be saved, will not be cleared.

Refresh：To update the information, click **Refresh**.

Change: When the edit button is clicked, the change button appears. Save the current edit configuration.

Cancel: When the edit button is clicked, the cancel button appears. Discard the current edit configuration.

Table: Displays the bridge, vlan id, and comment information for the device's interfaces.

Only selected entry in the table, in order to edit or delete the entry operations.

	Interface	Bridge	Vlan Id	Comment
☐	ETH0	BRIDGE0	0	
☐	VAP1	BRIDGE0	0	

NOTE：If the device interface is disabled or deleted in other operations, The configuration of the interface does not display in the table. If the interface has been enabled in the subsequent operation, Follow before the interface configuration.

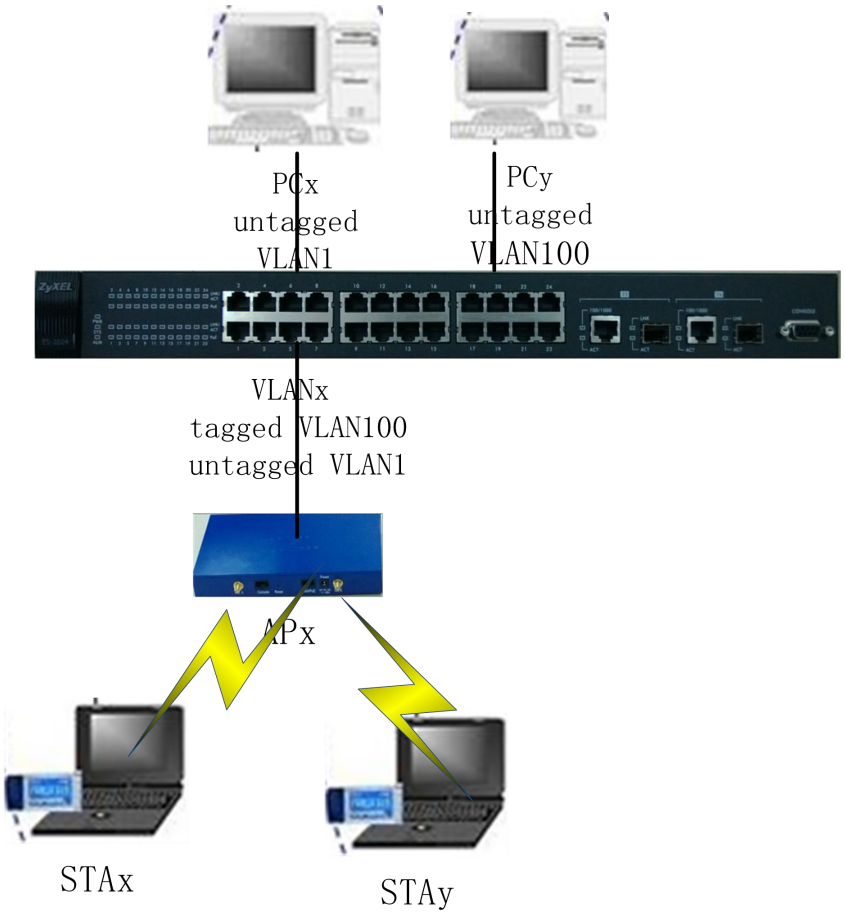
Chaper 2: Configuration Examples

This section provides several configuration examples of VLAN technology, including network requirements, network topology, and configuration procedure.

Simple Vlan Configuration Examples

Select Enable 802.1Q VLAN,it automatically creates a management VLAN.

Network Topology:



Network Requirements:

As shown in Network Topology：

PCx can communicate with STAx and STAy, But can not access and set APX.

PCy can not communicate with STAx and STAy, But can access and set APX.

Configuration Procedure:

Switch:

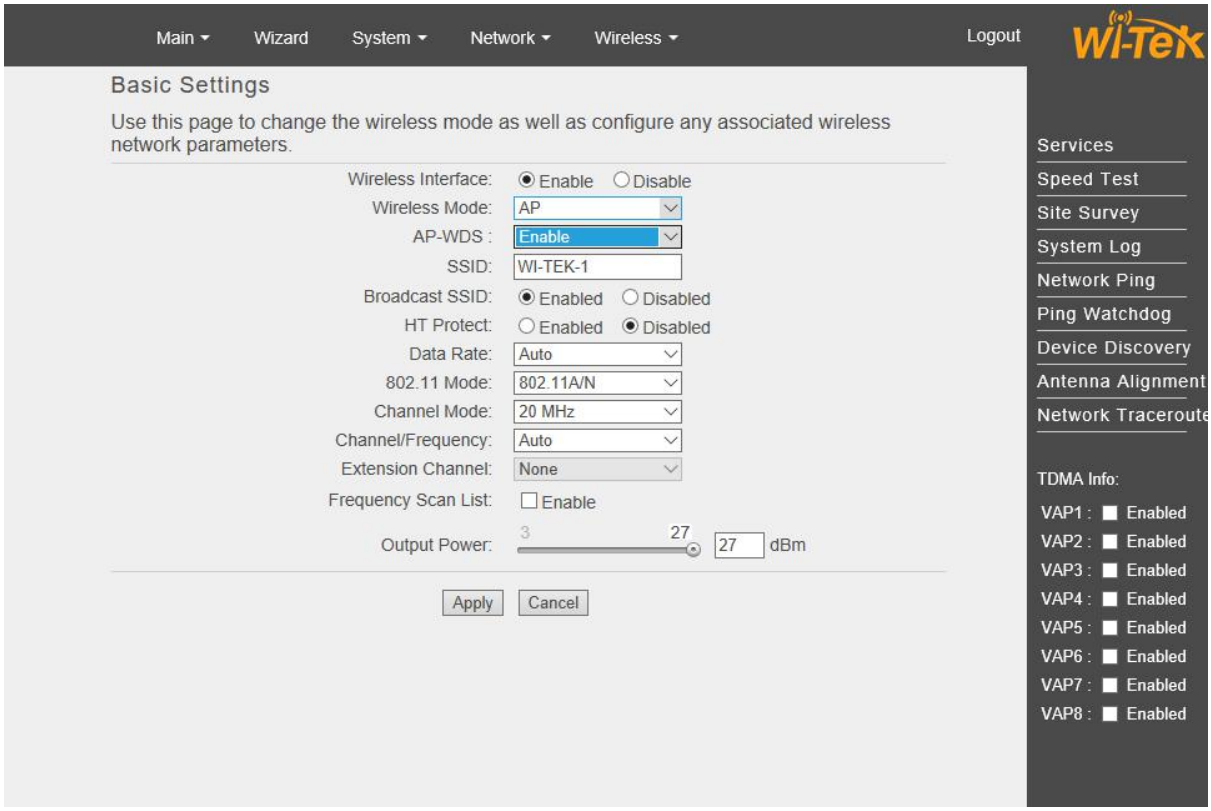
Mode in which interface of the Switch is connected to the PCx: untagged mode,The vlan id is not the management interface,for example 1,The PVID is 1.

Mode in which interface of the Switch is connected to the PCy: untagged mode,The vlan id is the management interface,for example 100,The PVID is 100.

Mode in which interface of the Switch is connected to the APx: untagged mode and tagged mode.The vlan id of tagged interface is the management interface,for example 100. The vlan id of untagged interface is not the management interface,for example 1. The PVID is 1.

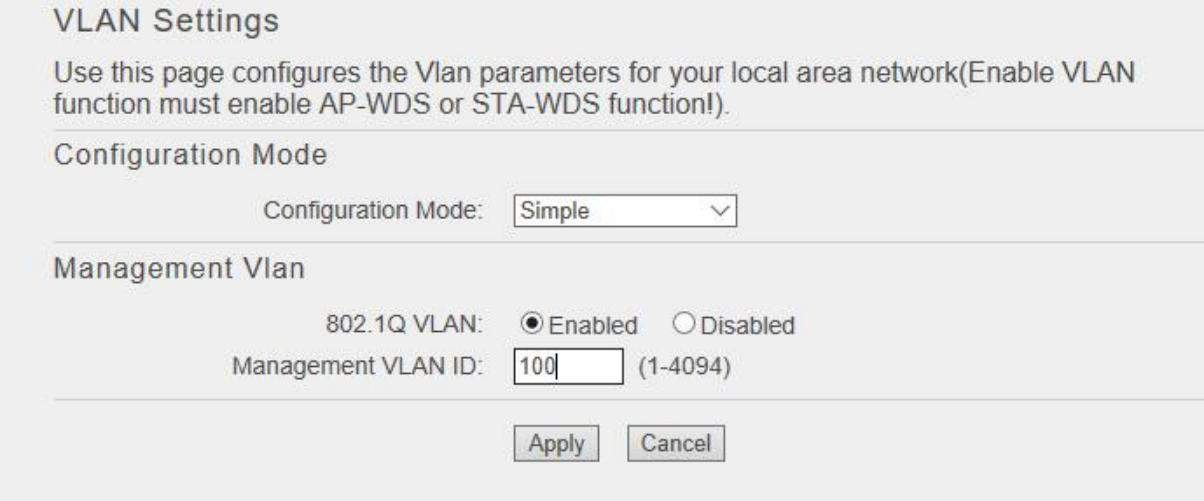
AP:

On the Wireless Mode tab, switch to AP. AP-WDS is Enabled. Now hit Apply at the bottom.



On the Configuration Mode tab, switch to Simple. 8021Q VLAN is Enabled.

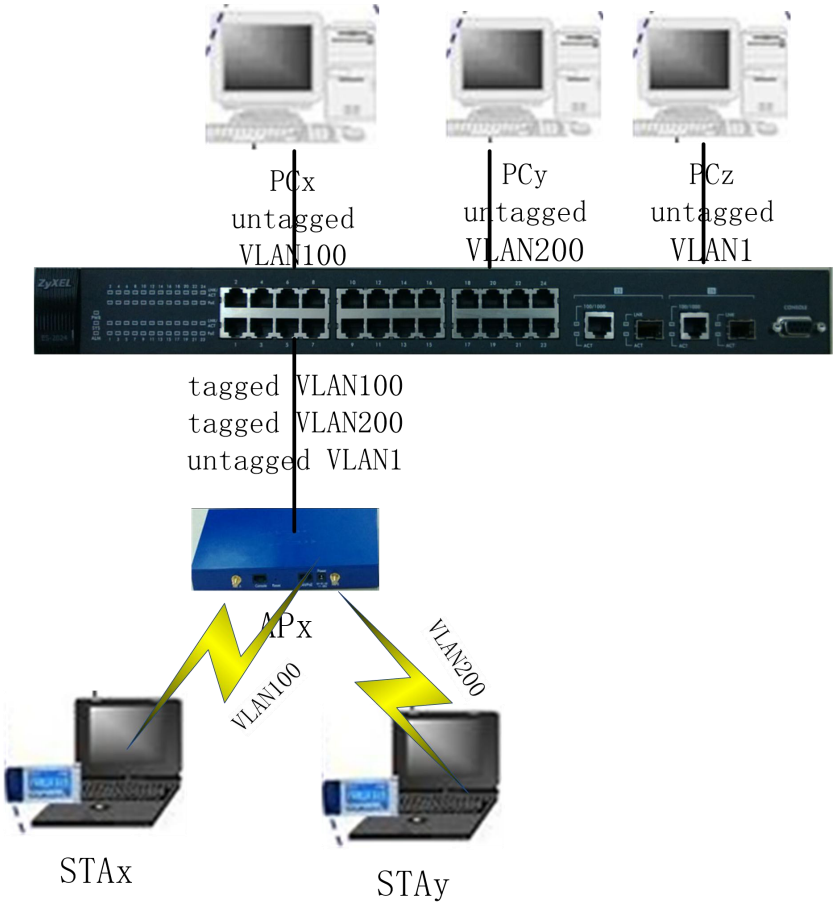
Management VLAN ID is 100.Now hit Apply at the bottom.



Advanced Vlan Configuration Examples

Advanced mode configuration is complex. if configured incorrectly, it is possible to cause the user can not access the device. Please be configured according to the example, If there are other requirements, please contact: www.WITEK.com.

Network Topology:



Network Requirements:

As shown in Network Topology：

PCx can communicate with STAx, But can not communicate with STAy,and can not access and set APX.

PCy can communicate with STAy, But can not communicate with STAx, and can not access and set APX.

PCz can access and set APX ,But can not communicate with STAx and STAy.

Configuration Procedure:

Switch:

Mode in which interface of the Switch is connected to the PCx: untagged mode,The vlan id is 100,The PVID is 100.

Mode in which interface of the Switch is connected to the PCy: untagged mode,The vlan id is 200,The PVID is 200.

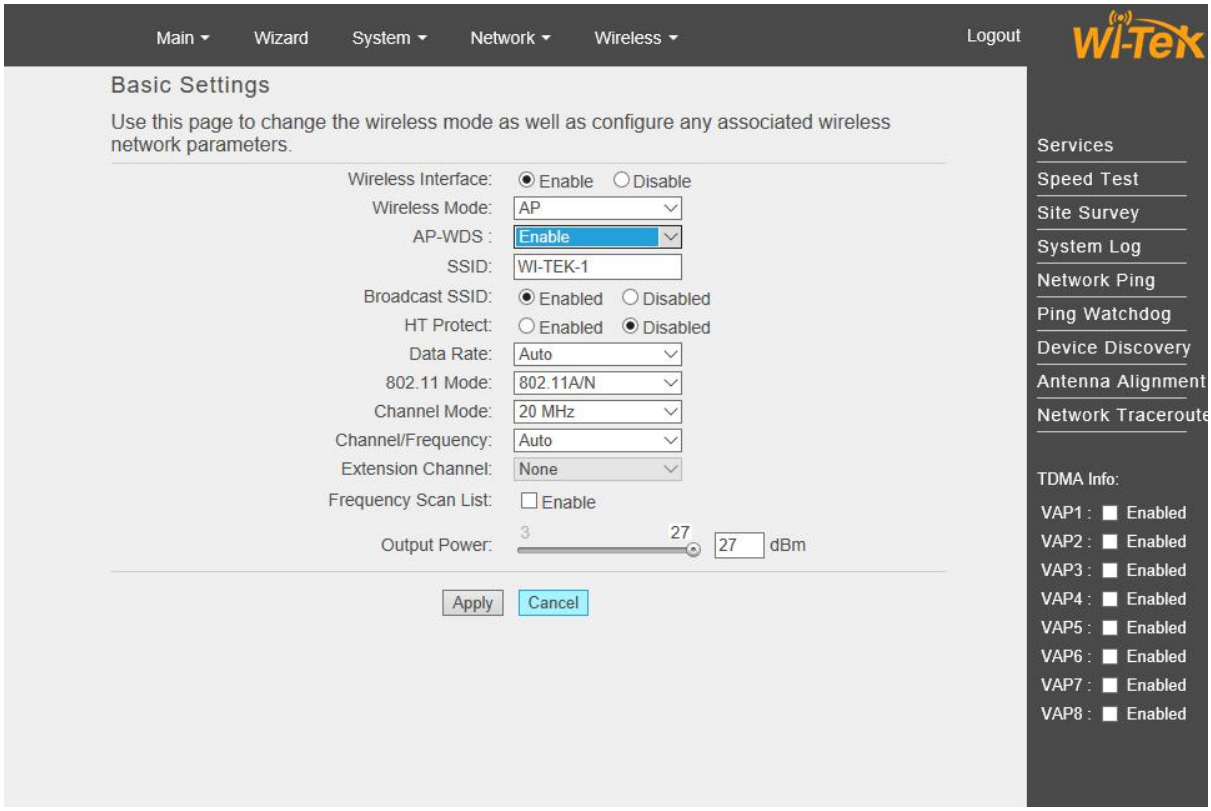
Mode in which interface of the Switch is connected to the PCz: untagged mode,The vlan id is 1,The PVID is 1.

Mode in which interface of the Switch is connected to the APx: untagged mode and tagged mode.The vlan id of tagged interface is 100 and 200. The vlan id of untagged interface is 1. The

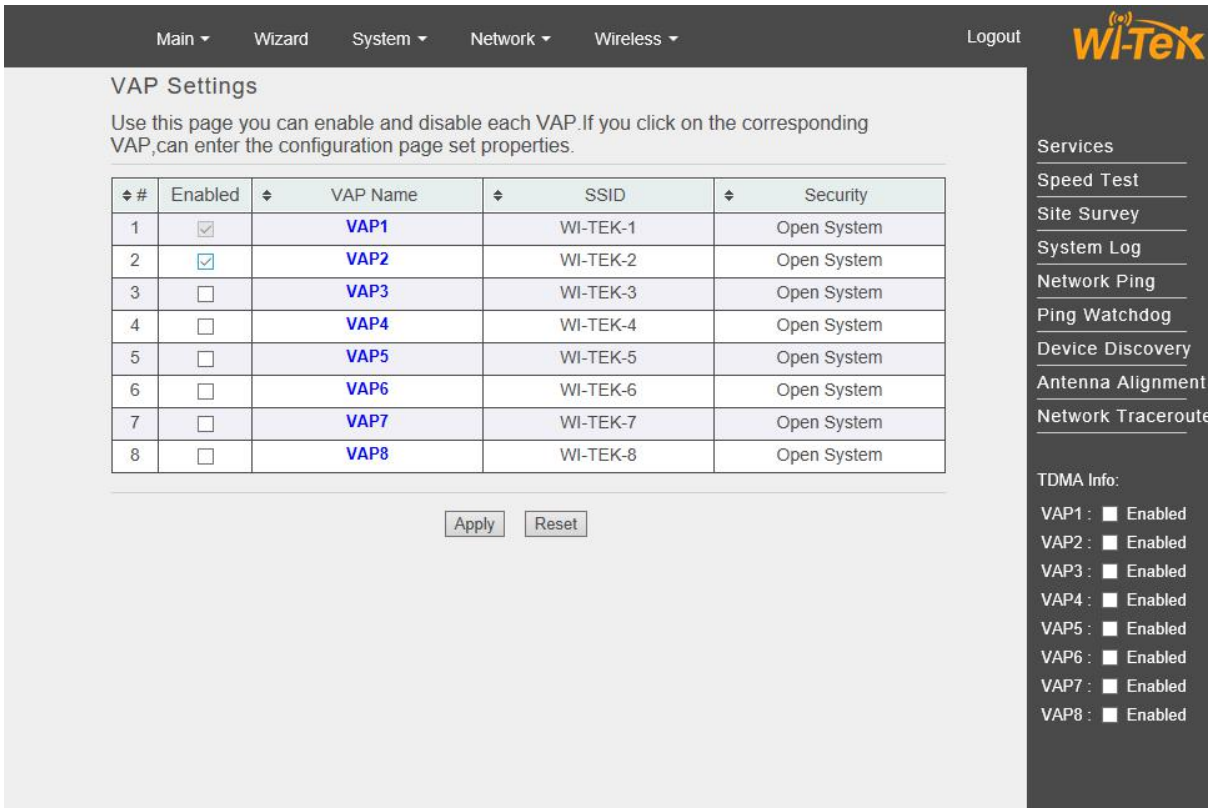
PVID is 1.

AP:

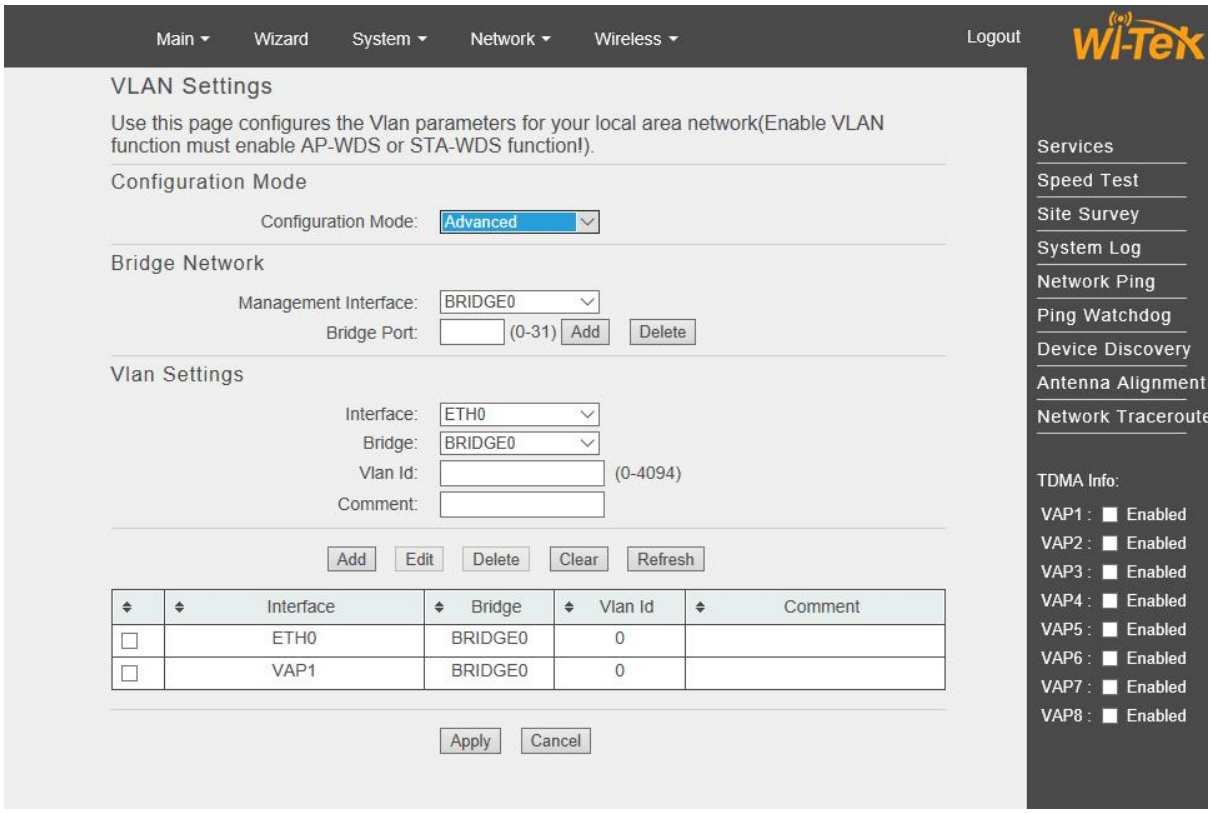
On the Wireless Mode tab, switch to AP. AP-WDS is Enabled. Now hit Apply at the bottom.



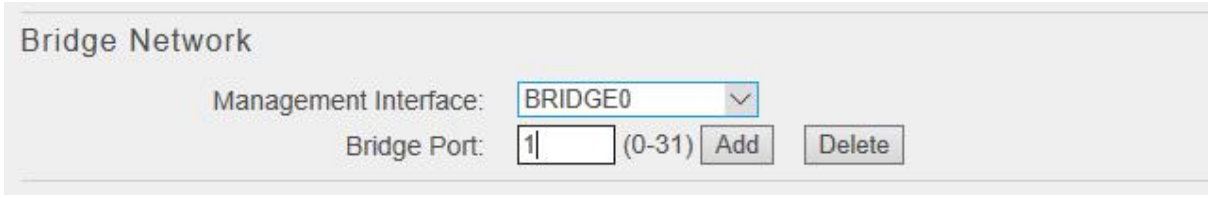
Select VAP2,and hit Apply at the bottom.



On the Configuration Mode tab, switch to Advanced,and hit Apply at the bottom.



Bridge Port fill 1, and hit Add.



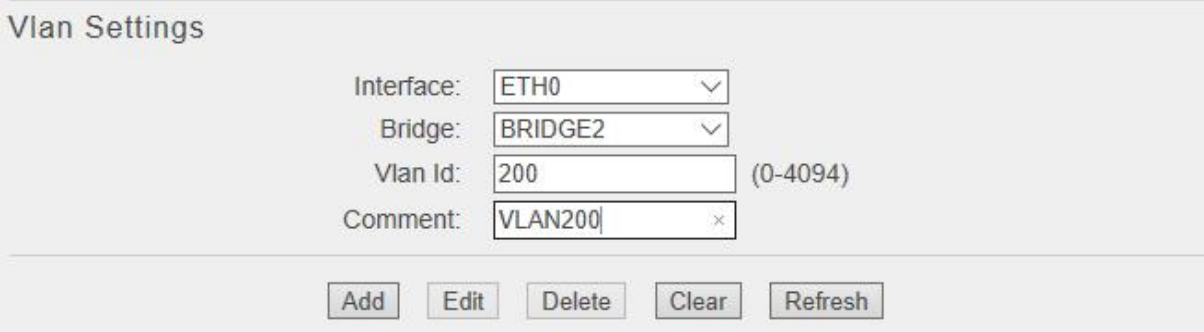
Bridge Port fill 2, and hit Add.



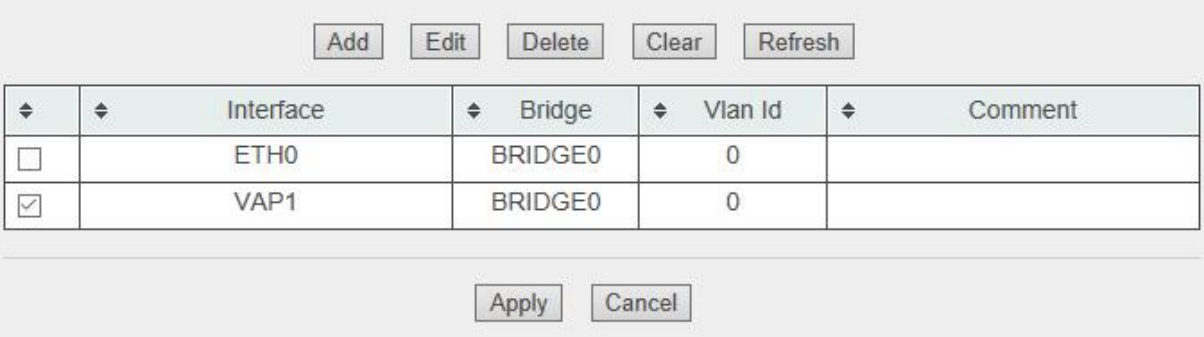
Interface is ETH0,Bridge is BRIDGE1,Vlan Id is 100,Comment is VLAN100, and hit Add.



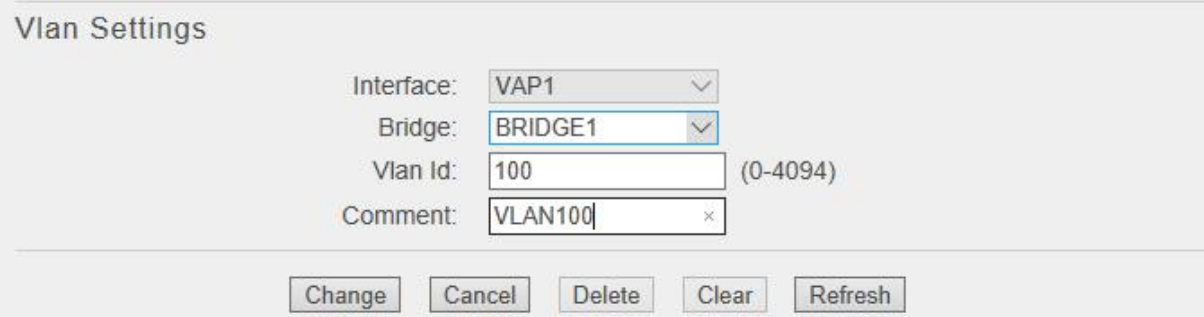
Interface is ETH0,Bridge is BRIDGE2,Vlan Id is 200,Comment is VLAN200, and hit Add.



Select VAP1,and hit Edit.



Bridge is BRIDGE1, Comment is VLAN100, and hit Change.



Select VAP2,and hit Edit.



Bridge is BRIDGE2, Comment is VLAN200, and hit Change.



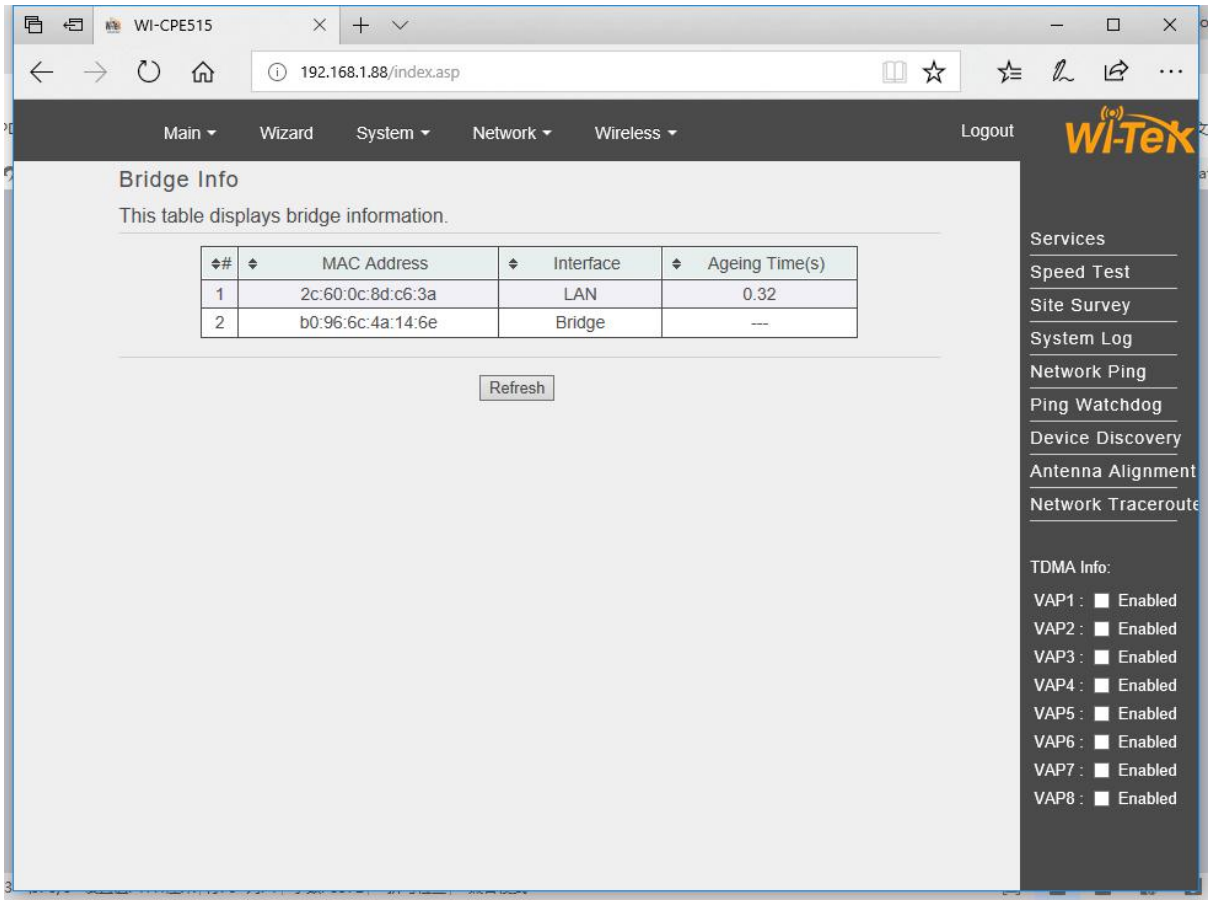
Final table as follows:

	Interface	Bridge	Vlan Id	Comment
	ETH0	BRIDGE0	0	
	ETH0	BRIDGE1	100	VLAN100
	ETH0	BRIDGE2	200	VLAN200
	ETH1	BRIDGE0	0	
	VAP1	BRIDGE1	0	VLAN100
	VAP2	BRIDGE2	0	VLAN200

STAx association VAP1, namely witek-1; STAy association VAP2, namely witek-2.

4.4 Bridge Info

View system bridge forwarding table, or MAC learning table. This table displays a learning system to correspond to the port associated with the MAC address.



MAC Address The identifier for the MAC address of the network device.

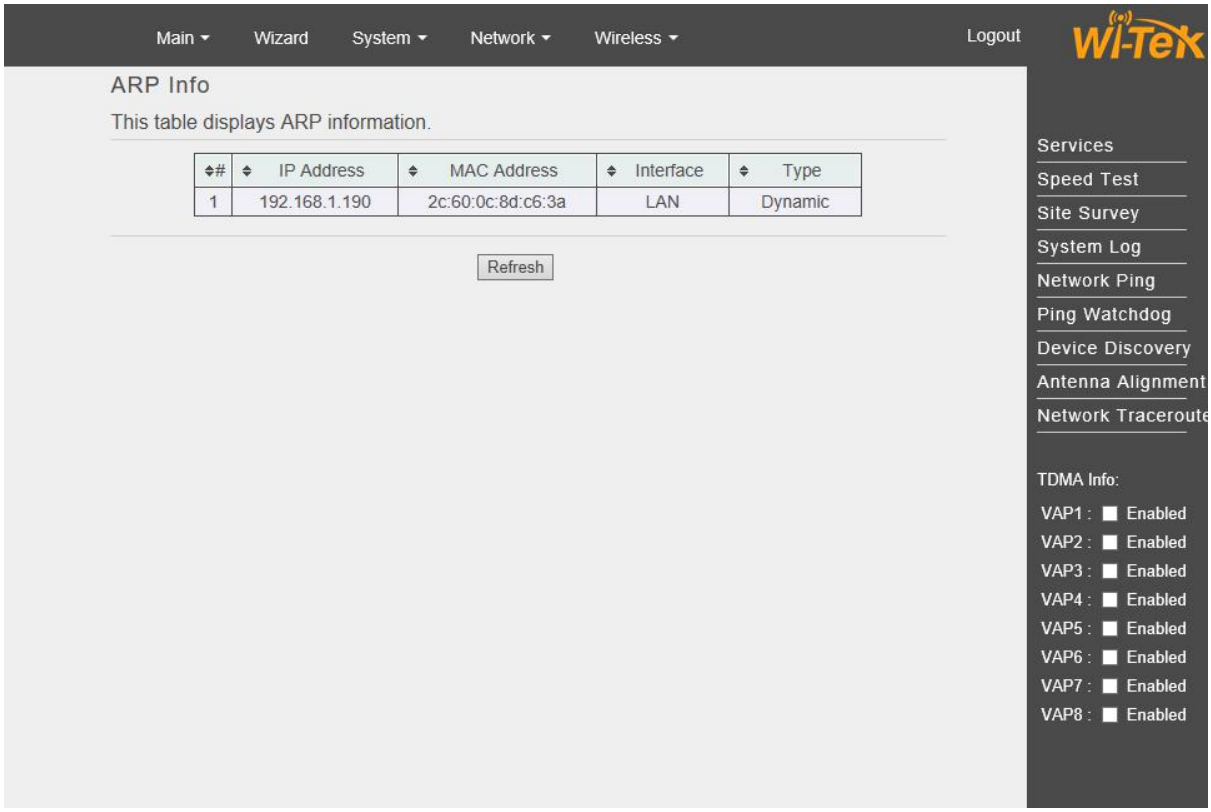
Interface The Bridge Table shows which bridge port or interface, LAN (Ethernet) or WLAN (Wireless), the specific network device is associated with.

Ageing Time(s) Display each address entry aging time (in seconds). After a certain timeout, if the device is not seen after a packet from the listed addresses, it will delete the address from the bridge table.

Refresh To update bridge table information, Click Refresh.

4.5 ARP Info

Display the current system the address resolution Protocol (ARP) all entries in the record corresponding to the static IP address and MAC address. System gets through the ARP protocol associated with this device to the network (data communications) of the neighbor device IP address and MAC address of correspondence are stored in this table to prepare for the next devices use to communicate with one's neighbors.

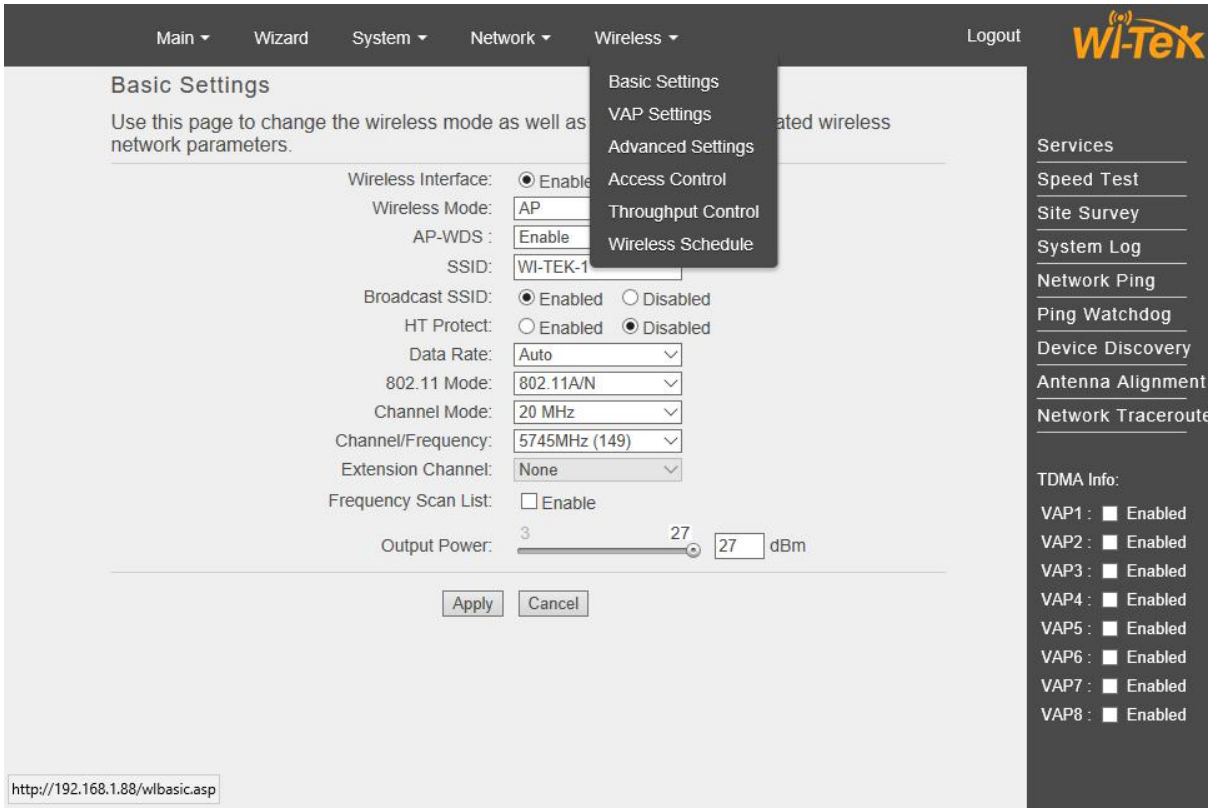


IP Address	Displays the associated (data communication) IP address of the network device.
MAC Address	Displays the associated (data communication) MAC address of the network device.
Interface	Display connected to the corresponding network device interfaces (LAN and the WAN).
Type	Display gets the type of the entry in the ARP table.
Refresh	To update the ARP table information, click Refresh.

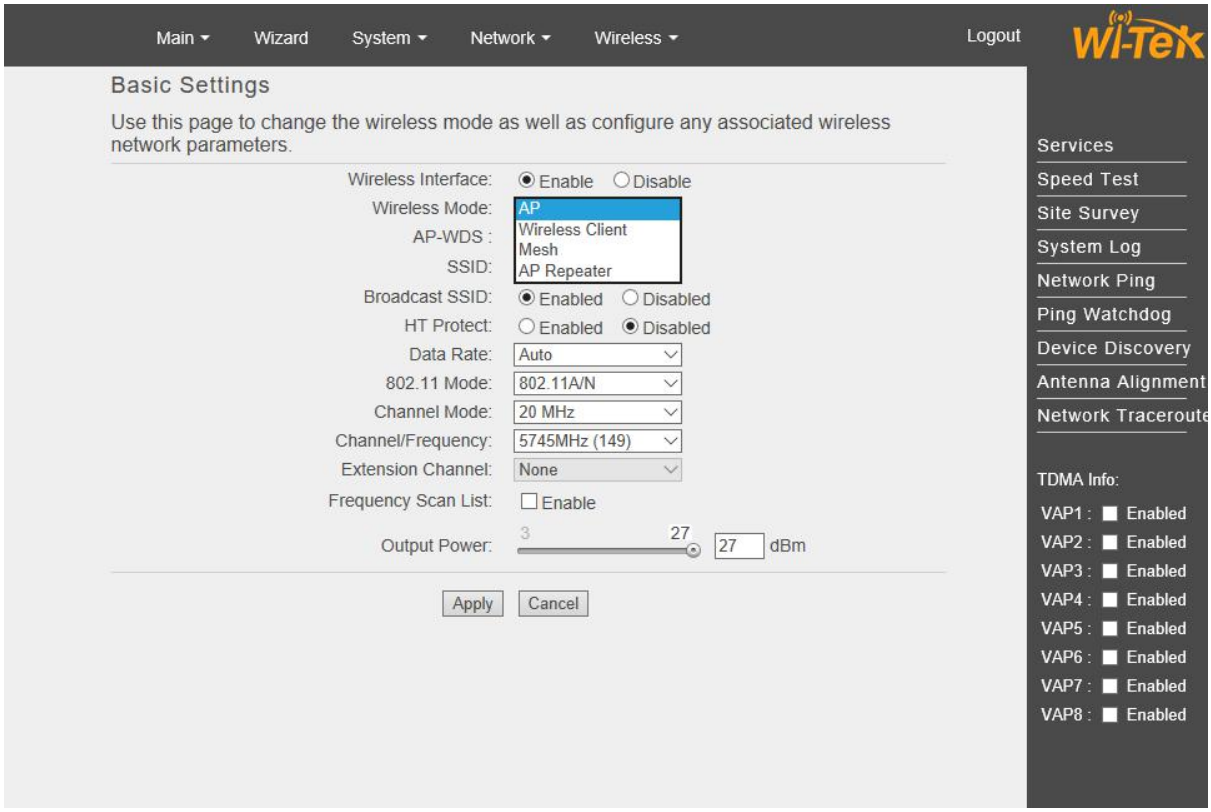
5 Wireless

5.1 Basic Settings

The wireless menu contains everything needed to set up the wireless part of the link. This includes Basic Settings, VAP Settings , Advanced Settings, Access Control, and Throughput Control.



Working in different Wireless mode (AP and Wireless Client, Mesh, AP Repater), display the configuration page will be different. Please selectively read the details according to the working mode of your device.



. AP Mode contains configuration page

Basic Settings	VAP Settings	Advanced Settings
Access Control	Throughput Control	

. Wireless Client Mode contains configuration page

Basic Settings	VAP Settings	Advanced Settings

.Mesh Mode contains configuration page

Basic Settings	VAP Settings	Advanced Settings

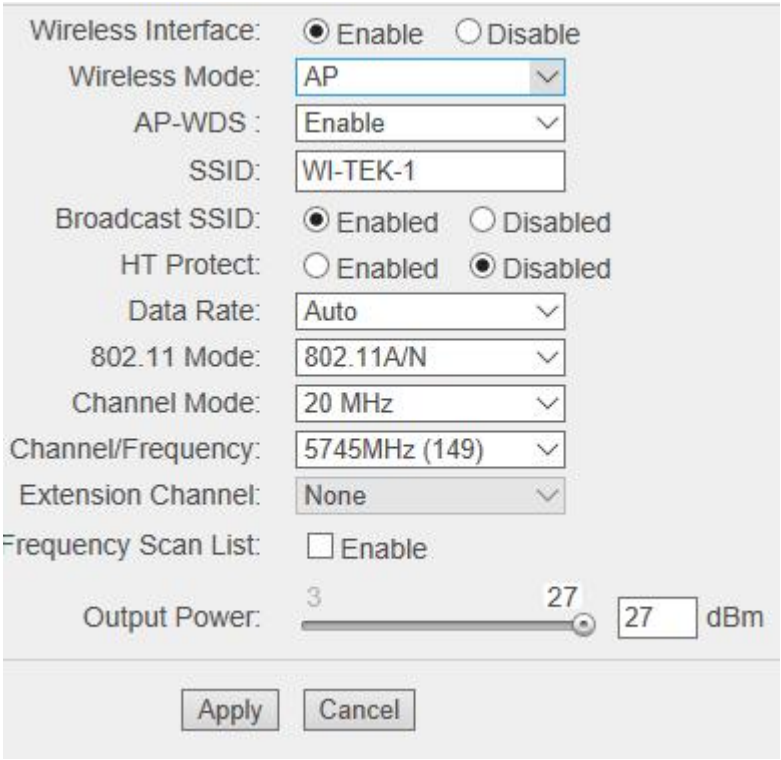
. AP Repater Mode contains configuration page

Basic Settings	VAP Settings	Advanced Settings
Access Control	Throughput Control	WDS Settings

1.1 Basic Settings

This section allows you to configure wireless basic settings, such as Wireless Mode, SSID, Data Rate, 802.11 Mode,and Output Power.

On Wireless Mode, you can configure the related wireless parameters in different modes. Working in different Wireless Mode, the configurable parameters will be different.



Wireless Interface： Check the wireless radio box to enable this device to send and receive the wireless signal.

Wireless Mode： Specify the *Wireless Mode* of the device. Including the AP , Wireless Client, Bridge and AP Repater four work modes. Select different Wireless Mode, the configurable parameters will be different.

. AP Access Point.If you have a single device to act as an AP, configure it as Access Point mode. The device functions as an AP that connects multiple client devices. Usage scenarios and sample, please refer to the section ().The following configuration settings are available:

	SSID	Broadcast SSID	HT Protect
Data Rate	802.11 Mode	Channel Mode	Channel/Frequency

Extension Channel	Center Frequency	Output Power	

.Wireless Client With client mode,the device can connent to a wired device and Works as a wireless adapter to receive wireless signal from your wireless network. Usage scenarios and sample, please refer to the section () 。 The following configuration settings are available:

STA-WDS	SSID	Locked AP MAC	Enable MAC Clone
Auto MAC Clone	Manual MAC Clone	Data Rate	802.11 Mode
Site Survey	Output Power		

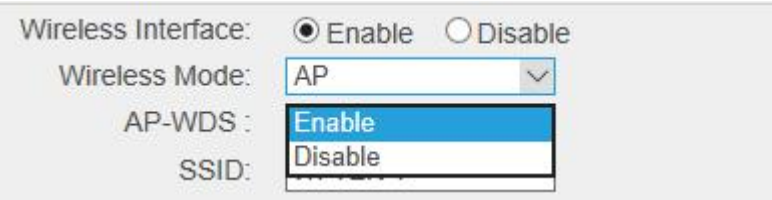
. Mesh Wireless bridge mode, wireless connection with each other through the MAC address equivalent to a second network of wireless switches. Usage scenarios and sample, please refer to the section .The following configuration settings are available:

Data Rate	802.11 Mode	Channel Mode	Channel/Frequency
Extension Channel	Center Frequency	Output Power	

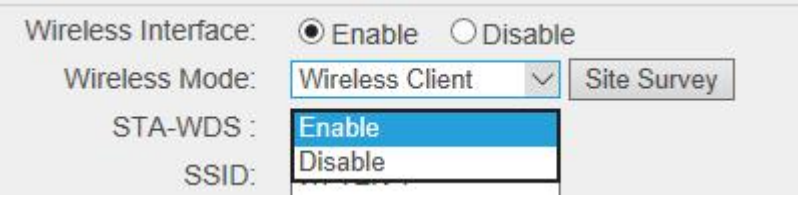
. AP Repeater In this mode, you setup a Wireless Bridge to connect with other Bridge and a Wireless AP for local wireless coverage.Usage scenarios and sample, please refer to the section ()。The following configuration settings are available:

AP-WDS	SSID	Broadcast SSID	HT Protect
Data Rate	802.11 Mode	Channel Mode	Channel/Frequency
Extension Channel	Center Frequency	Output Power	

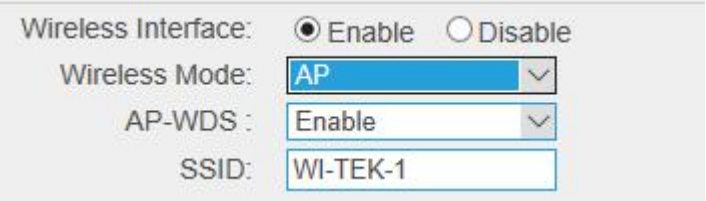
AP-WDS： Available in AP mode. Displays whether the Wireless Distribution System (WDS) is enabled or not . If you choose to enable the AP support four address data frame, will deal with forward four address data frames.And if you choose to disable, it will be received four address data frames dropped.



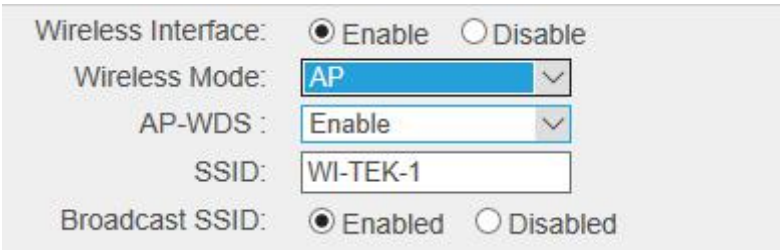
STA-WDS： Available in Wireless Client mode. Displays whether the Wireless Distribution System (WDS) is enabled or not . If you choose to enable the Wireless Clien support four address data frame, will deal with forward four address data frames.And if you choose to disable, it will be Used three address sending data frames.



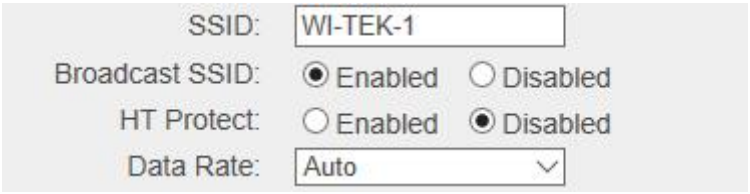
SSID： Service Set Identity.Enter a character string no more than 32 characters to name your wireless network. The default SSID is WITEK-1.



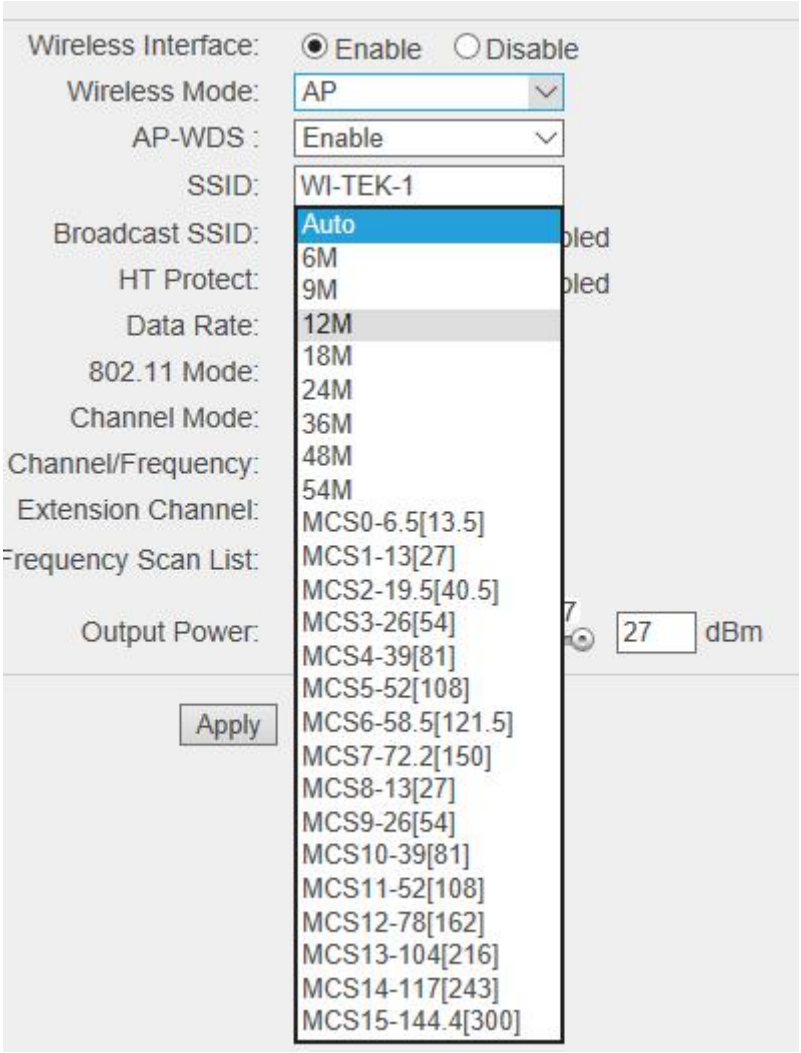
Broadcast SSID： Available in AP and AP Repater mode. Check this option, AP will broadcast its SSID to hosts in the surrounding environment, as thus hosts can find the wireless network identified by this SSID. If SSID Broadcast is not enabled, hosts must enter the AP's SSID manually to connect to this AP.



HT Protect：Available in AP and AP Repater mode，High throughput protected mode。



Data Rate：Wireless data sending rate of frame, its value depends on the selection of 802.11 Mode. If you select 11n mode, its value depends on Channel Mode and Short GI.



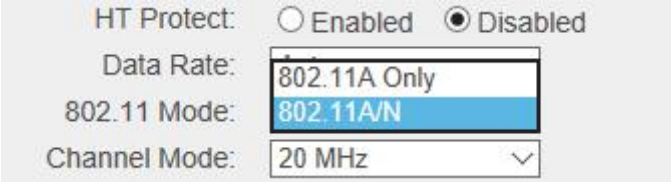
Mode Rate	1M	2M	5.5M	11 M	6M	9M	12 M	18 M	24 M	36 M	48 M	54 M	MCS0-15
11B	√	√	√	√	T	T	T	T	T	T	T	T	T
11G	√	√	√	√	√	√	√	√	√	√	√	√	T
11A	T	T	T	T	√	√	√	√	√	√	√	√	T
11N	√	√	√	√	√	√	√	√	√	√	√	√	√

MCS (Modulation and Coding Scheme) depends on Channel Mode and Short GI. Have the following relations :

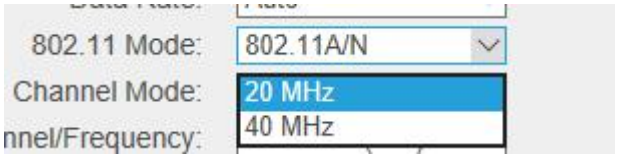
MCS	Short Gi Disable		Short Gi Enable	
	20MHz	40MHz	20MHz	40MHz
0	6.5	13.5	6.5	13.5
1	13	27	13	27
2	19.5	40.5	19.5	40.5
3	26	54	26	54
4	39	81	39	81
5	52	108	52[	108
6	58.5	121.5	58.5	121.5
7	65	135	72.2	150
8	13	27	13	27
9	26	54	26	54
10	39	81	39	81
11	52	108	52	108
12	78	162	78	162
13	104	216	104	216
14	117	243	117	243
15	130	270	144.4	300

802.11 Mode： This is the radio standard used for operation of your device.2G device and 5G device have different protocols supported:

5G device: ” 802.11A/N” ” 802.1 A only”

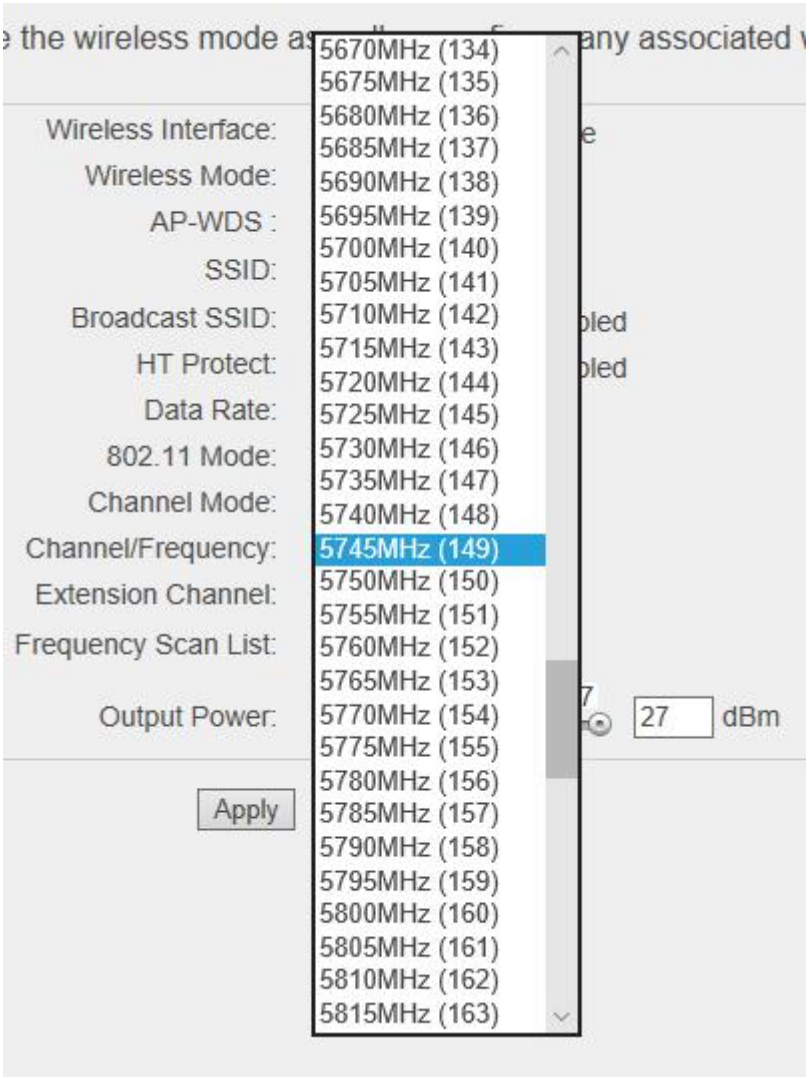


Channel Mode： Only Available when the model chosen as"802.11 A/N" (5 G equipment). Options include 20MHz, 40MHz. Users select corresponding channel width according to whether their devices support it. According to IEEE 802.11n standard, using a channel width of 40MHz can increase wireless throughput.

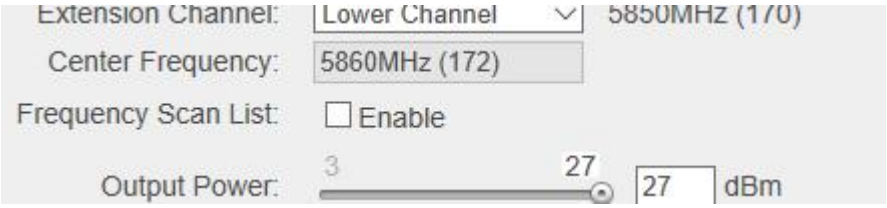


Channel/Frequency： Available in AP , Bridge and AP Repater mode. Select the channel used by this device to improve wireless performance. We highly recommend you use the Spectrum Analysis tool to select a proper channel.

The channel number varies in different regions. 5G channel device contains more, United States has 234.



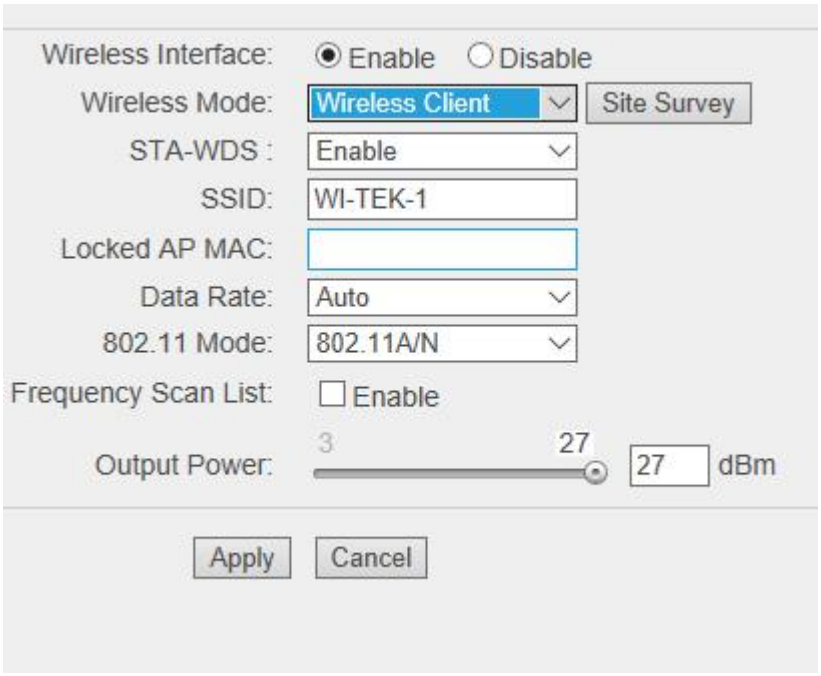
Center Frequency： Valid only when the channel mode is selected to 40M. When 40M bandwidth of the signal can be expanded, show the center channel frequency.



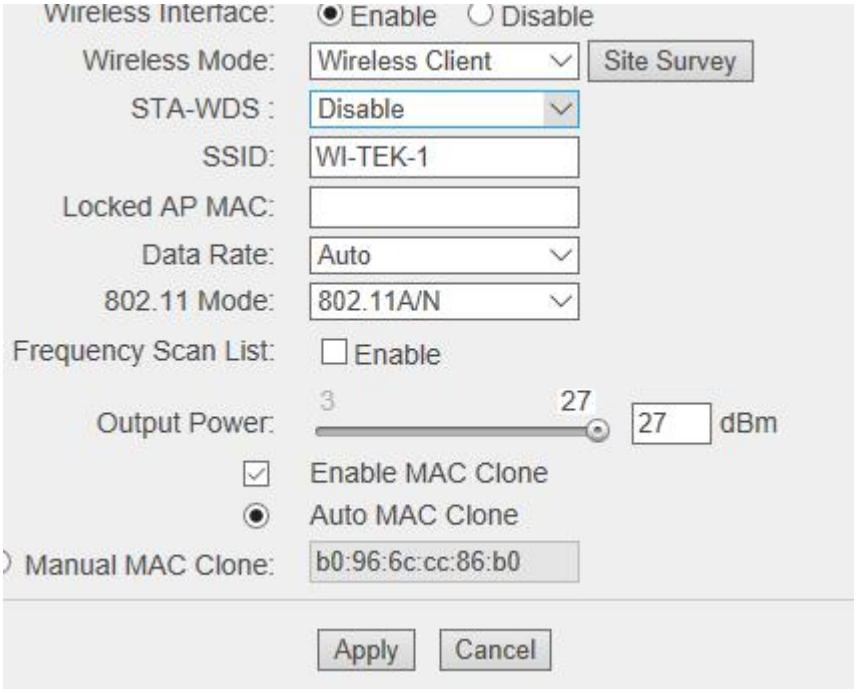
Output Power：You can use the slider or manually enter the transmit power value. The maximum transmit power may vary among different countries or regions.



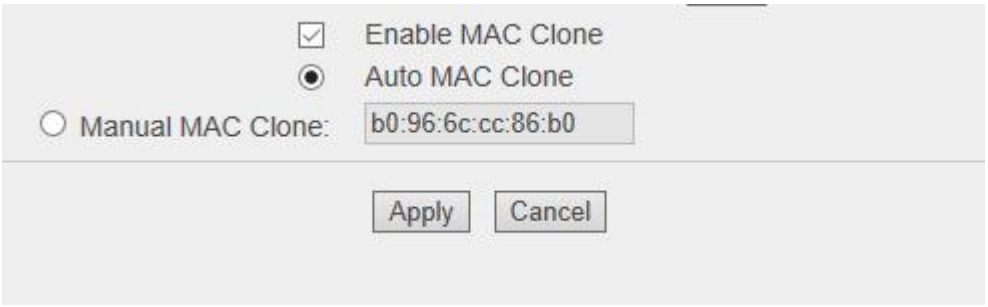
Locked AP MAC： Available in Wireless Client mode. Displays the MAC address of the root AP. It's possible that two or more networksuse the same SSID in the AP list. Lock to AP can make the device connect to thespecified AP you had connected before the next time.



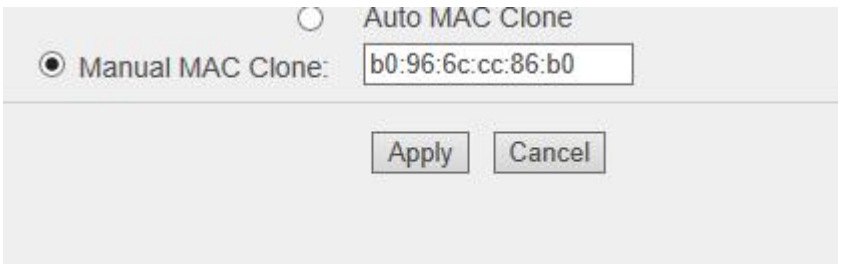
Enable MAC Clone： Available in Wireless Client mode. Effective when STA-WDS disabled. When enabled, MAC address of the device will user's MAC address or manually enter the MAC.



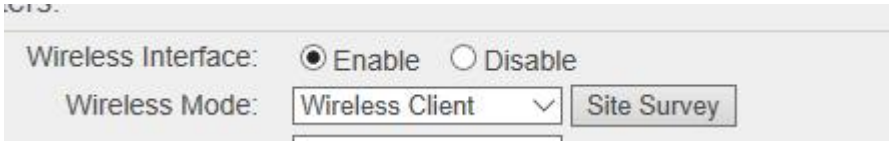
Auto MAC Clone：Available in Wireless Client mode. Effective when STA-WDS disabled. When enabled, MAC address of the device will user's MAC address.



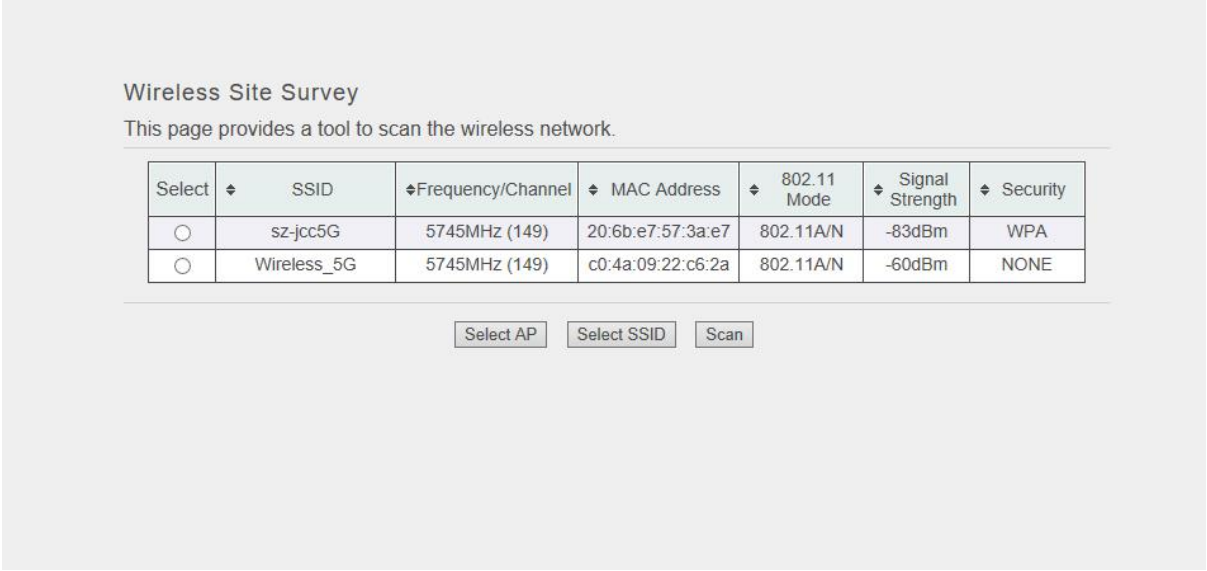
Manual MAC Clone：Available in Wireless Client mode. Effective when STA-WDS disabled. When enabled, MAC address of the device will manually enter the MAC.



Site Survey：Available in Wireless Client mode. Used to scan surrounding wireless AP.



Click on the site scan, shown below：

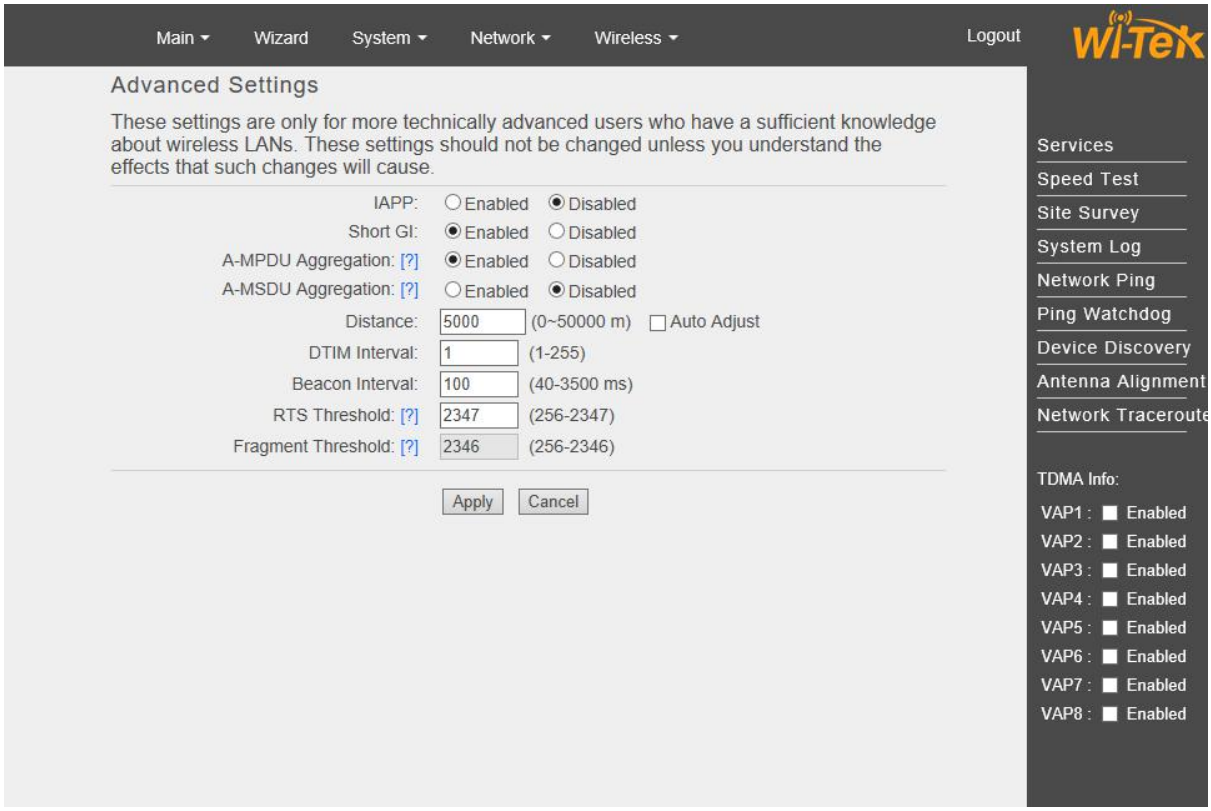


Select the desired wireless network and click Connect(Above Figure 1). It’s possible that two or more networks use the same SSID in the AP list(Above Figure 3). Select AP can make the device connect to the specified AP you had connected before the next time(Above Figure 2). Scanning (Above Figure 4) button will rescan.

5.2 VAP Settings

5.3 Advanced Settings

The Advanced page handles advanced wireless settings.Such as Short GI 、 A-MPDU Aggregation、A-MSDU Aggregation、RTS Threshold、Fragment Threshold。



AP and AP Repater Mode contains configuration parameters：

IAPP	Short GI	A-MPDU Aggregation	A-MSDU Aggregation
Distance	Auto Adjust	DTIM Interval	Beacon Interval
RTS Threshold	Channel Protection	Fragment Threshold	

Wireless Client Mode contains configuration parameters：

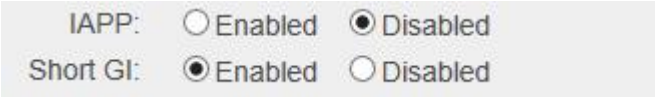
Short GI	WMM Support	A-MPDU Aggregation	A-MSDU Aggregation
Distance	Auto Adjust	TDMA Support	Signal LED Thresholds
RTS Threshold	Channel Protection	Fragment Threshold	Roaming threshold

Difference the two AP's RSSI			

Bridge Mode contains configuration parameters：

Short GI	WMM Support	A-MPDU Aggregation	A-MSDU Aggregation
Distance	Auto Adjust	TDMA Support	IGMP Snooping
RTS Threshold	Channel Protection	Fragment Threshold	

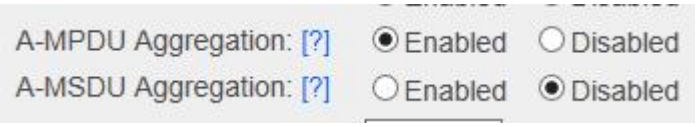
IAPP：Base station interconnection (IAPP,Inter-Access Point Protocol) is an upper layer protocol for communication between the AP and is mainly used for AP interactive STA STA access process information for fast roaming. To refresh the page.



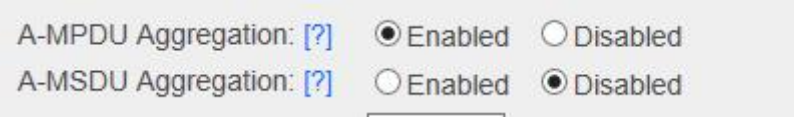
Short GI：Check "enable" This allows devices to receive and send short packet intervals to improve device transfer rate, recommend check.



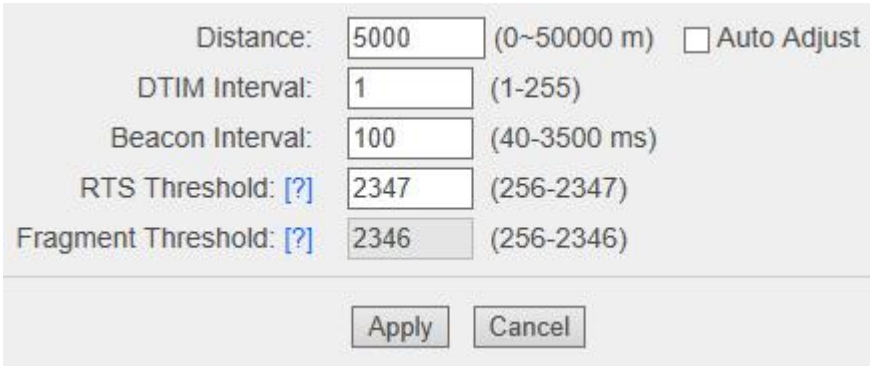
A-MPDU Aggregation：A-MPDU is the result of an aggregation of 802.11 packets after the MPDU package, and improve system throughput.



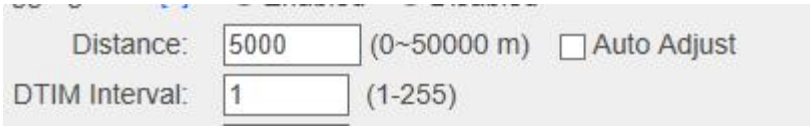
A-MSDU Aggregation：A-msdu technology refers to the aggregation of multiple MSDS into A larger load in A certain way to improve the rate of sending messages.



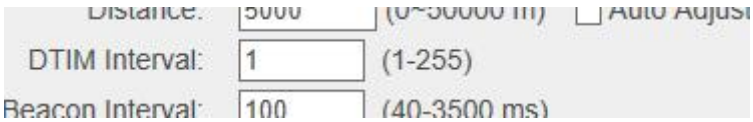
Distance：Enter the distance between the AP and Client, this setting will have a great effect on long distance wireless transmission performance. If the device as a Client device, enter the distance between devices and front-end AP; if the device as AP device, enter the farthest distance between the client and the device. If it is difficult to measure accurately, and in a one-to-one connection, can be checked automatically.



Auto Adjust：For one-on-one connections, a AP a Client connection. When you are in a one-to-one connection, and check the automatically adjusted equipment according to ACK frames return time, to automatically calculate the distance, which estimated the distance between the two devices.



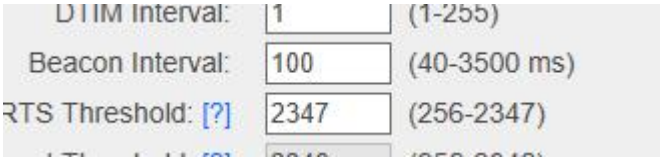
DTIM Interval：Specifies the transmission message (DTIM, Delivery Traffic Indication Message) interval, DTIM is a countdown timer job, to inform the next to receive the broadcast and multicast client window. When the system has an associated client-side caching the broadcast or multicast messages, it will carry the next DTIM interval in the Beacon message when clients hear the Beacon signal, you will receive the broadcast and multicast messages. DTIM in Beacon interval, the default value is 1, DTIM field is identical to the Beacon interval.



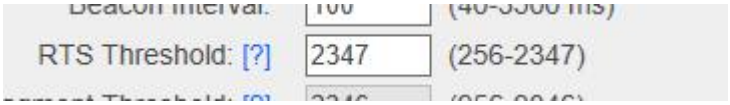
Beacon Interval： Beacon frames are devices broadcast packets for the release of the SSID wireless network device support. STA (Station) by Beacon frame was received to determine the SSID also exists if the SSID Beacon frame has not been received for a long time, the SSID is STA can be considered no longer exists, STA will automatically disconnect the connection with the

SSID, enabling Wi-Fi synchronization.

Beacon interval that sent AP Beacon broadcasting frequencies. The default value is 100 milliseconds, values is 40-3500 Ms.



RTS Threshold：Packet to specify RTS (Request to Send) threshold, when packet length exceeds the RTS threshold, the system sends the RTS to the destination site to consult, the default value is 2347.

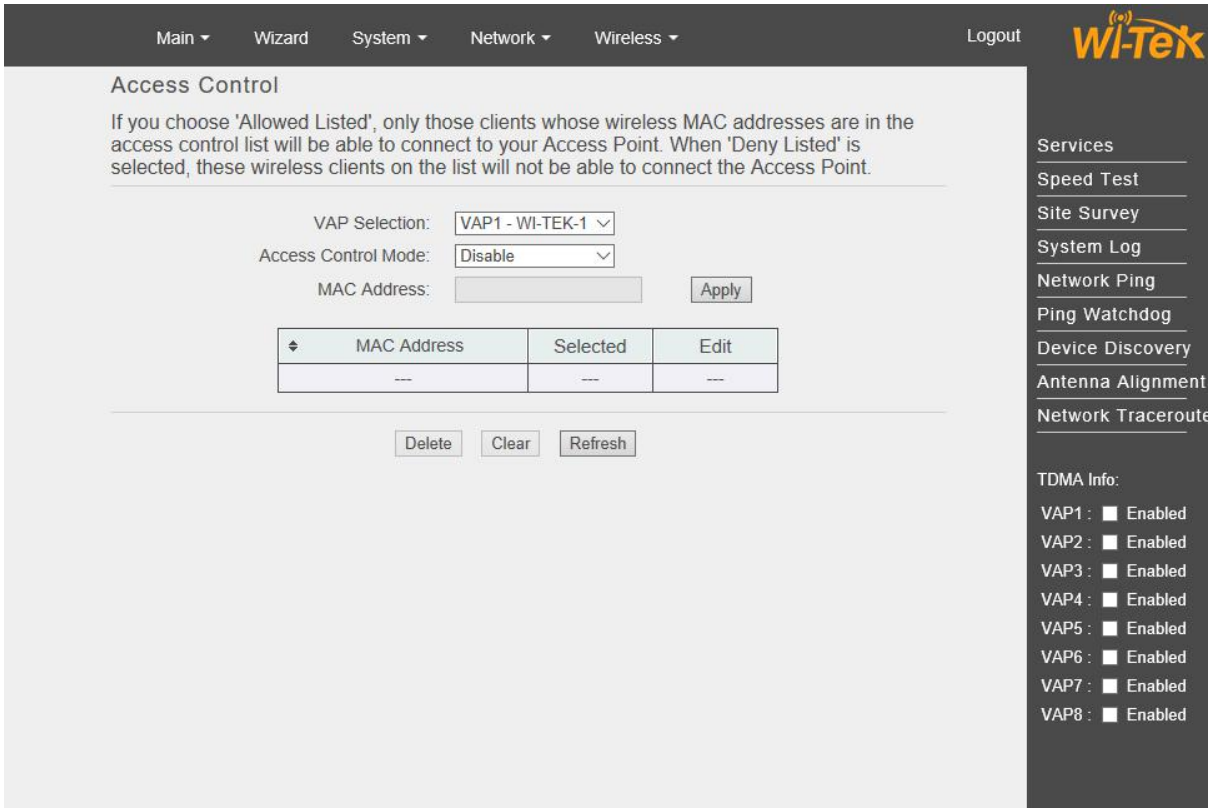


5.4 Access Control

Here you can specify the MAC address filter on some wireless devices within a network. Users can according to the actual situation, select an access rule. Each SSID can independently configure the wireless MAC address filtering rules, you can "select a template" drop down menu, select the SSID you have set, select a SSID will enter the wireless MAC address filtering rules configuration page.

Note:

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.



Profile Selection When you select a SSID will enter the wireless MAC address filtering for access rule configuration page.

Access Control Mode There are three modes: Disable, Allow Listed, Deny Listed.

- Disable：Disable access control rules.
- Allow Listed：Allow list has been added to allow the MAC address of the device connected to the AP to establish and access.
- Deny Listed： Not allowed to deny list has been added the MAC address of the device with the AP to establish a connection and access.

MAC Address Enter the managed device's MAC address.

Selected Select the access control list entries have been added.

Edit Can edit entries corresponding to the MAC address of the access rule.

Clear you can clear all of the MAC address of the access rule entries for this SSID.

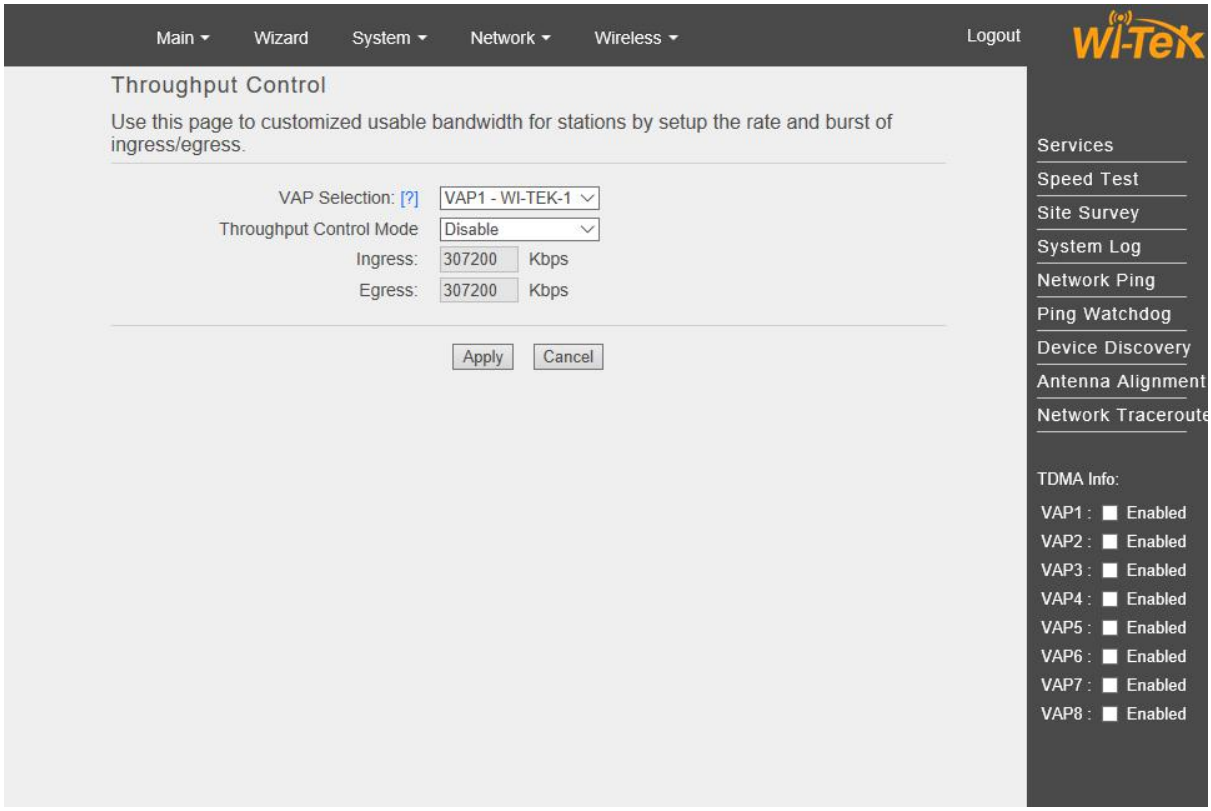
5.5 Date Rate Control

5.6 Throughput Control

You can control each of the wireless client is connected to the user's available bandwidth speed upward flow velocity, downstream flow speeds. Use throughput control to prevent network because of the instant shock of a large amount of data on the network to ensure user high performance and stable operation of the network.

Note：

Each SSID can independently configure your wireless traffic control rules, you can "Profile Selection" drop down menu, select the SSID you have set, select a SSID will enter the corresponding flow control rules configuration page.



Profile Selection	When you select a SSID will enter the wireless throughput control rule configuration page.
Throughput Control Mode	There are three modes：Disable、VAP(SSID)User、VAP(SSID)Total. ● Disable：Disable throughput control rules. ● VAP(SSID)User： Each connected client's available bandwidth speed on the AP side. ● VAP(SSID)Total：Sets all client devices that are connected to the AP shared bandwidth speed.
Ingress	Maximum available upload bandwidth of wireless clients traffic speed.

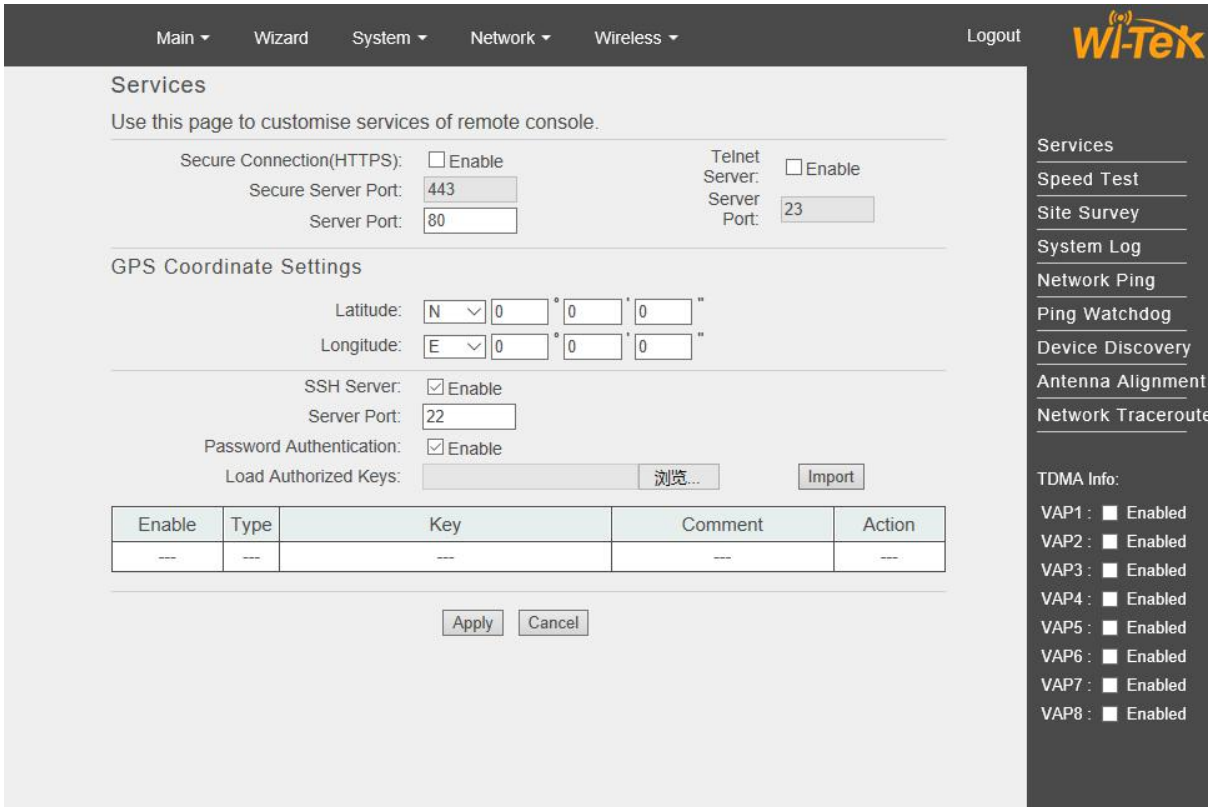
Egress	The maximum available bandwidth to download the flow speed of the wireless clients.

6 Tools

6.1 Services

For the safety of equipment, this device provides remote services configuration, users can be configured according to the actual situation.

1. Select the service configuration tool on the right:



2. HTTPS connection: click HTTPS enable connections, indicating that the user needs to use the https security protocol to connect to the Web page. Secure Server Port represents a safe port for HTTPS connection agreement settings and Server Port port port is the HTTP protocol connections. The connection timeout for Session Timeout on behalf of, more than the time to disconnect.

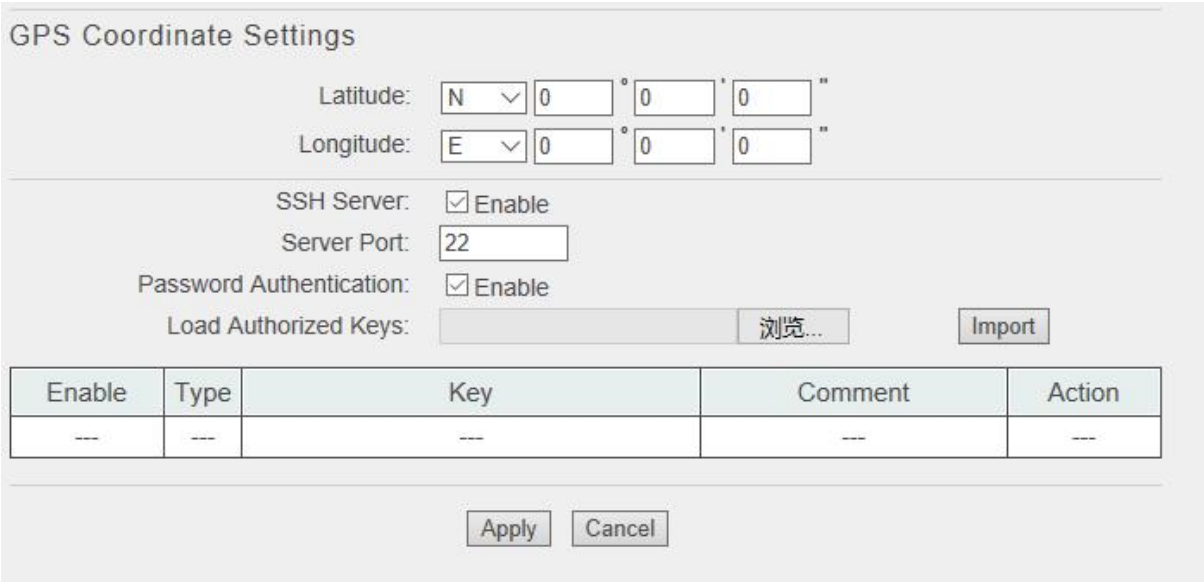


3. Telnet service: check enable to start Telnet service, it means users log on through Telnet device, but does not allow remote users to log on through Telnet device, but can also

modify login port.



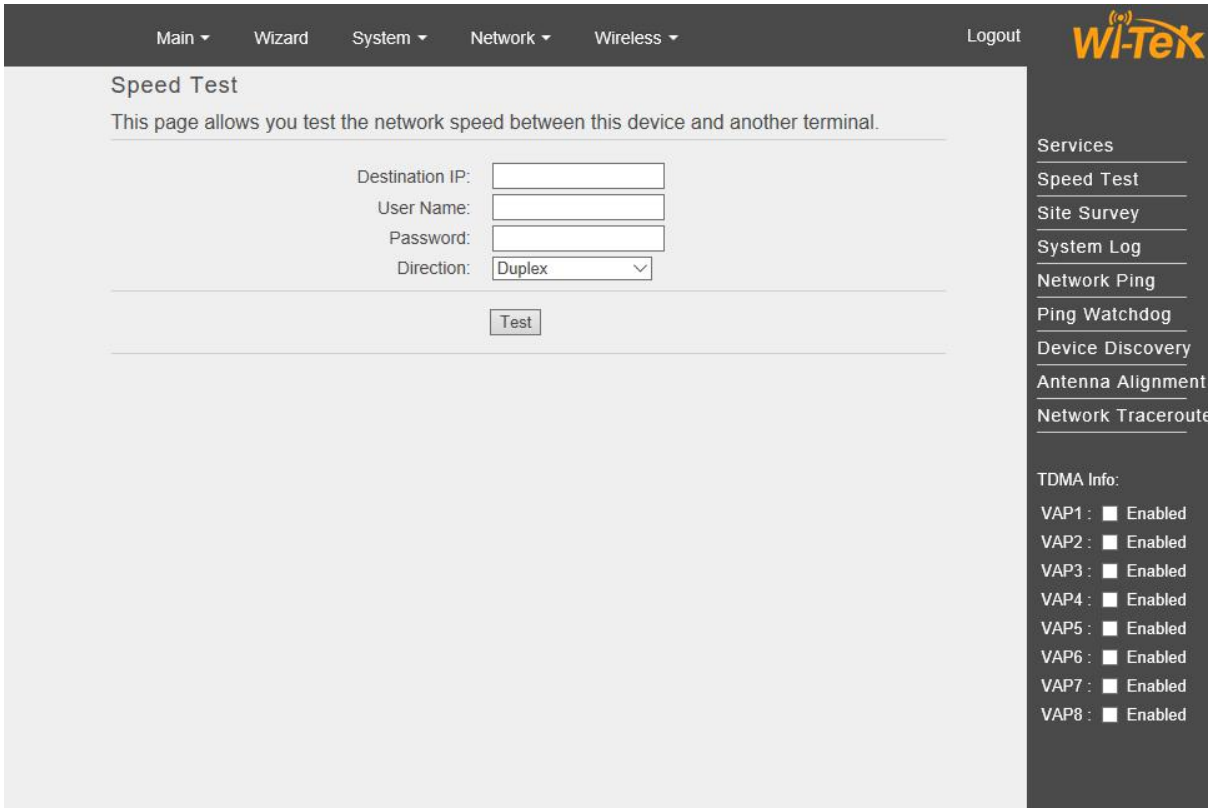
4. SSH services: If you consider security issues, Telnet service is not allowed, the user can select the SSH service. Similarly, port SSH login can be modified. Password authentication is representative of whether or not to allow SSH password, log on to the appliance, do not allow password (free password login), you will need to import in the following RSI of SSH keys, used for certificate login, RSI is Linux platform using the secret key: SSH-DSA, can also be obtained by SecureCRT, specific use please refer to the relevant information.



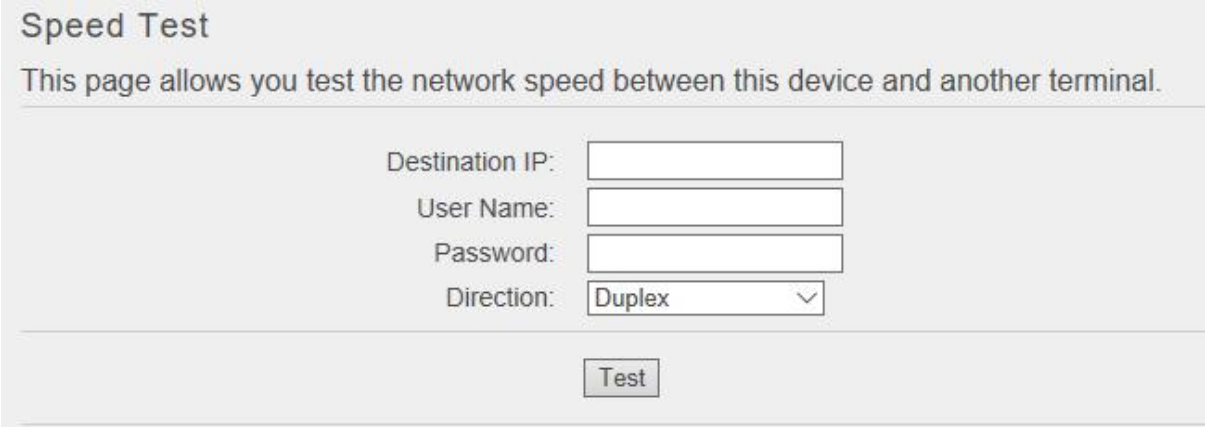
6.2 Speed Test

When you set up a one-to-one devices, unable to accurately determine whether the device antenna on each other on time or when the network is good, you can use the function of network speed, and observe whether the measured rate movements

1. Select the network speed on the right tools:



2. Fill the end device IP address and Web page login account name, password, and select the speed directions, click on the test:



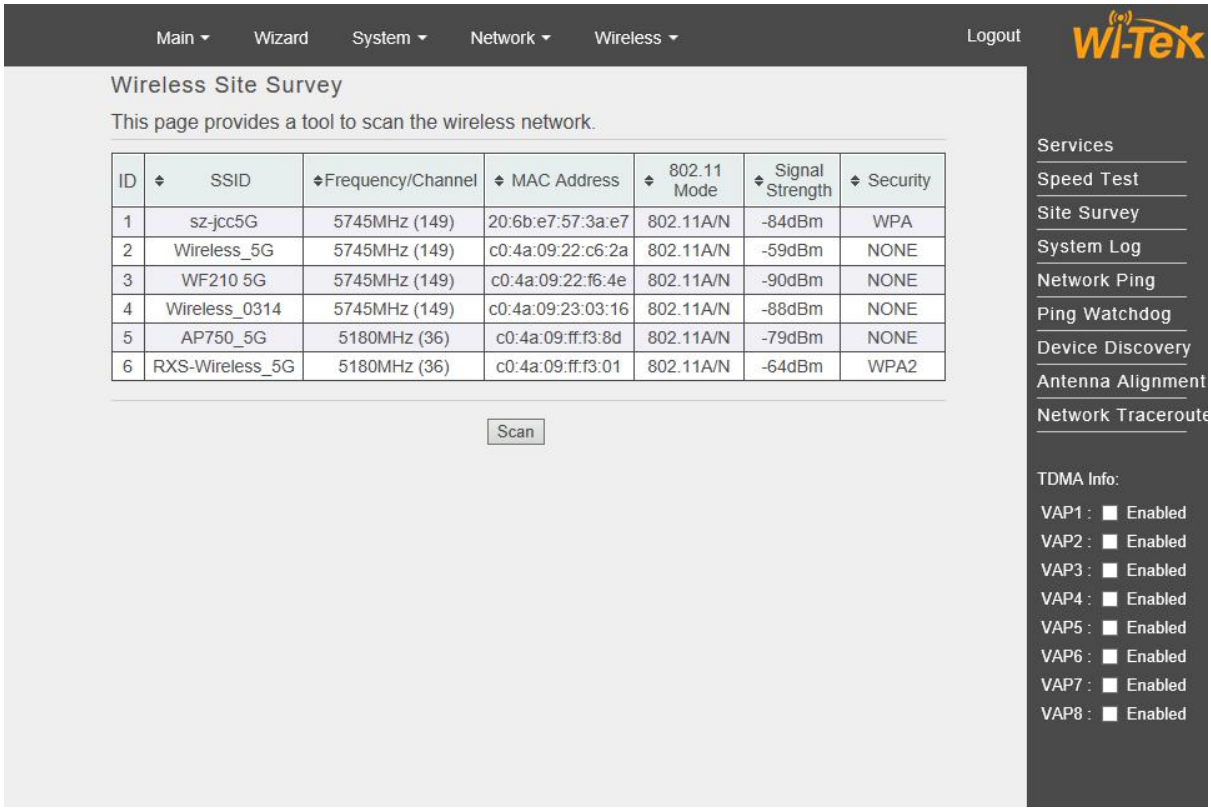
3. When you use the network speed, the equipment must be supported by the version of network speed function and ways to use HTTP login page.

6.3 Site Survey

When you cannot determine which channels with less interference, we can use the frequency scan function scans the surrounding interference so you can select the channels for wireless transmission of less interference

1. On the right side of the Web page select spectrum analysis tools, where y represents the

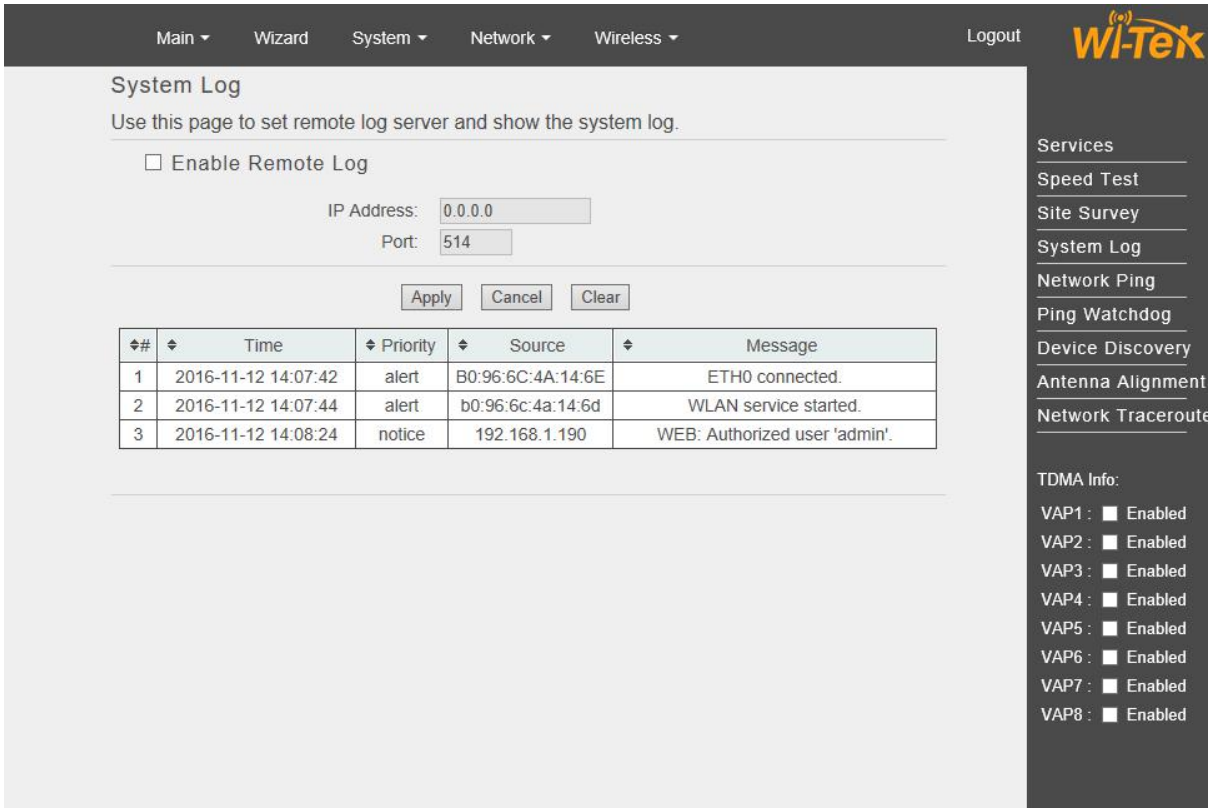
disturbing energy intensity, abscissa represent the count on the starting channel one channel per interval calculation plus one, as shown in Figure: +0 represents the start channel 147,+1 represents the next channel 148:



2. results show the recommended channels, less interference of the channel. From scanning interface to analyze, print more energy-intensive, more color on behalf of disturbing energy is strong, indicating serious disturbance of the channel.

6.4 System Log

In the system log page, you can set the remote syslog server, as well as in the list view wireless device in the system event log records.



If they need a host view device log in information, please first install the logging server on this host, and then check the device logs on the page "Enable Remote Log" option, and enter the host's IP address and port. After settings are applied you will be sent to the specified address to the system log.

Cancel To refresh the page.

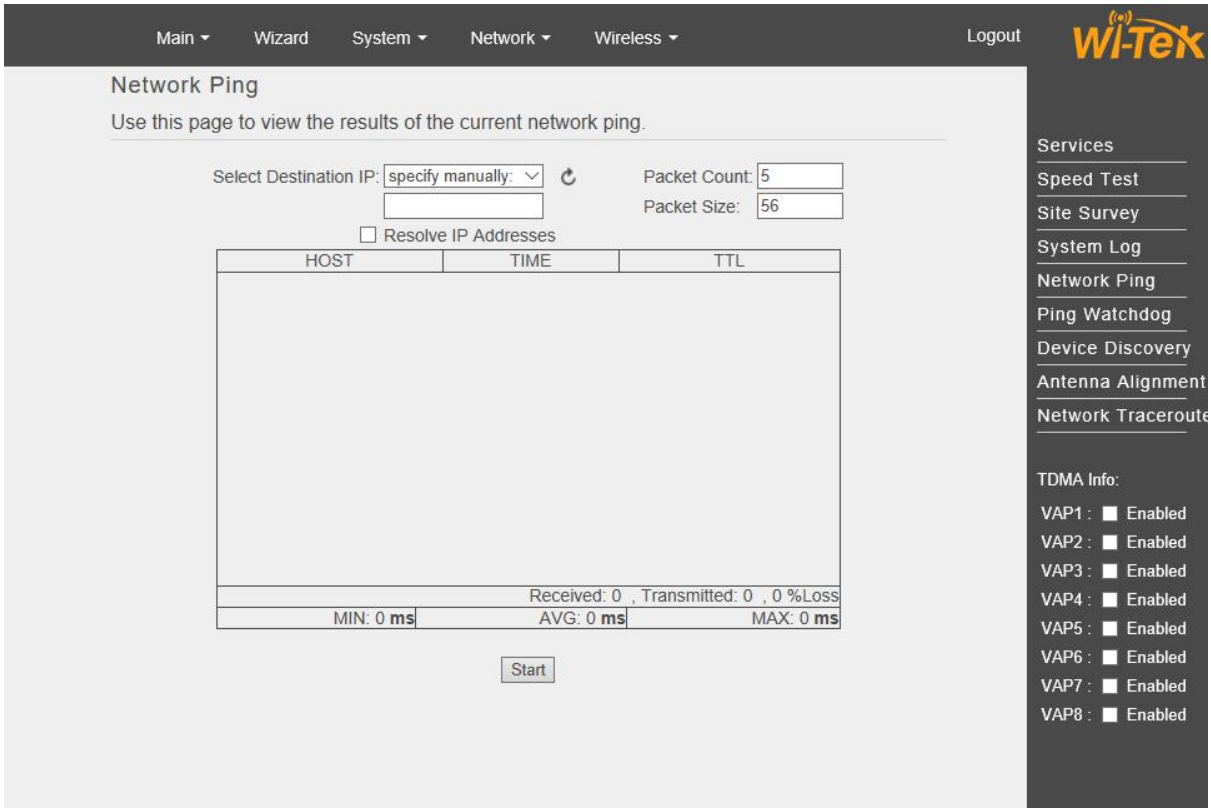
Clear Clear the system log list below.

A log in the log table can be divided into four parts:

#	Time	Priority	Source	Message
1	2016-11-12 14:07:42	alert	B0:96:6C:4A:14:6E	ETH0 connected.
2	2016-11-12 14:07:44	alert	b0:96:6c:4a:14:6d	WLAN service started.
3	2016-11-12 14:08:24	notice	192.168.1.190	WEB: Authorized user 'admin'.

6.5 Network Ping

In the network ping page, users can specify destination IP or domain name, the total number of messages, message size, by sending a ping packet inspection users wireless device network connectivity with the destination IP address.



Select Destination IP There are two options:

1)Specify manually From the drop-down list, select the remote IP address is generated automatically.

2)Manually enter Enter the destination IP address or domain name can be entered manually (such as www.Google.com), enter incorrect address you will be prompted to re-enter.

Packet Count To a destination IP address or domain name of the total number of Ping packets, default is 5.

Packet Size To a destination IP address or domain name of the Ping packet size, the default is 56.

Start Clicking < started > button to begin the test, the device will send ping packets to test whether destination address can be reached, and displays the results in the box above.

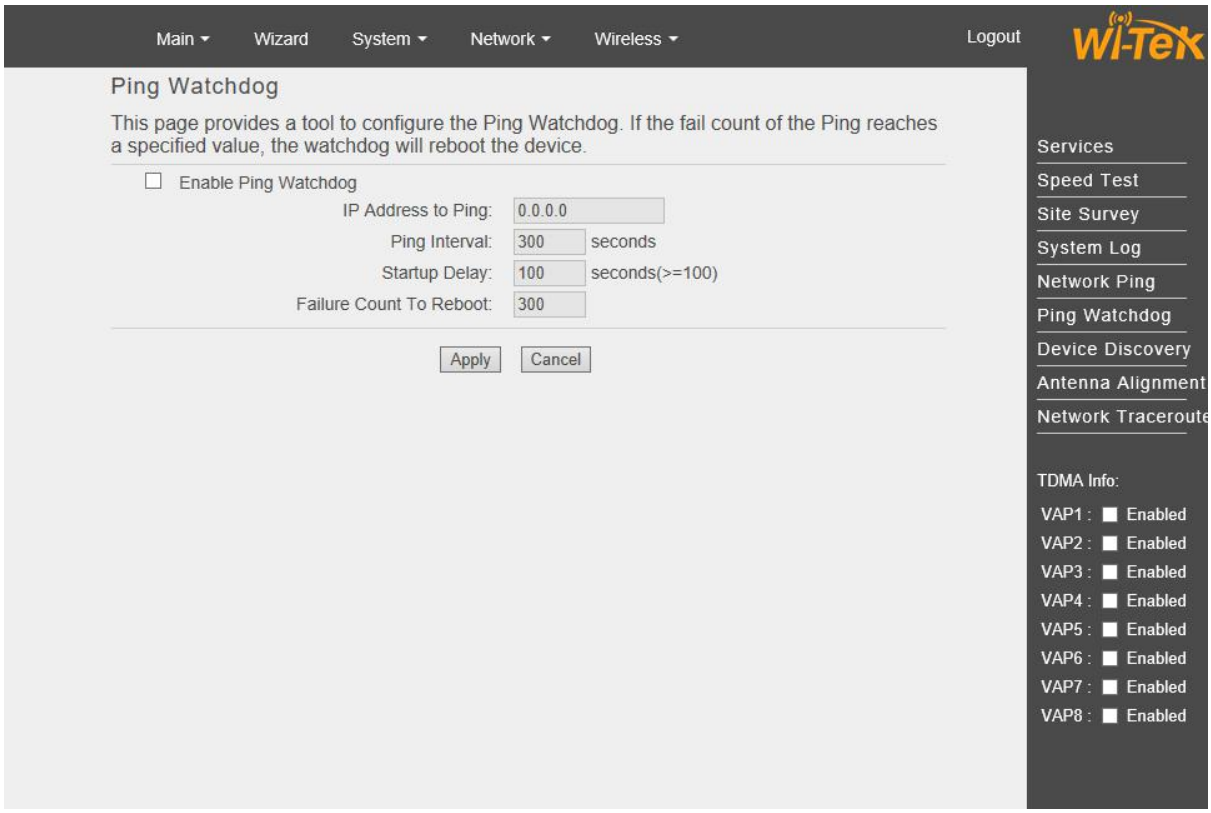
Network Ping tool results display box:

Displays the response the host name, response delay results, a record number Ping sent, received, number of Ping packets, packet loss rate, minimum Ping response delay, on average, the maximum Ping Ping response delay response delay.

6.6 Ping Watchdog

In the Ping watchdog page, you can set the destination IP address, Ping Inerval, etc. by

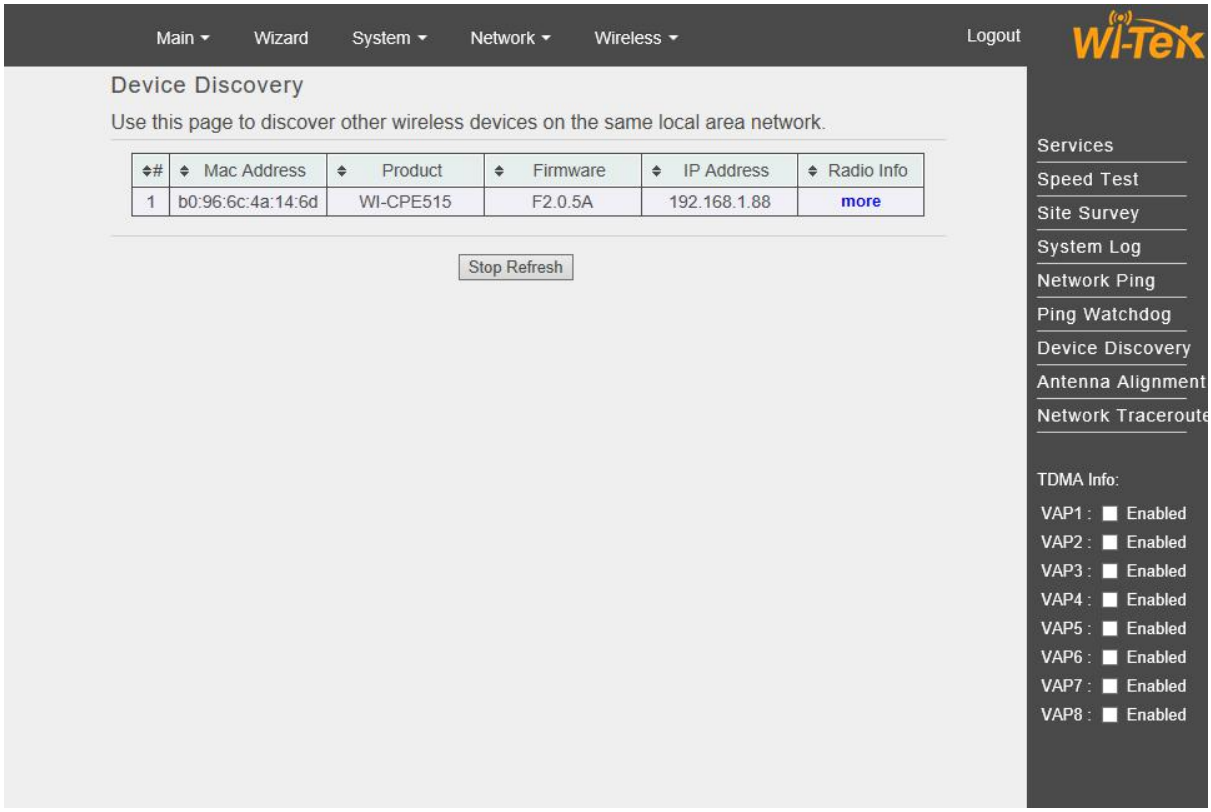
sending a Ping packet inspection device connectivity with the destination IP address of the network, in order to determine whether the current network has failed



Enable Ping Watchdog	To enable this, device will from time to time sends a ping packet to the destination address, if no answer is received in a row, after you set the number of times when the ping fails, the device will automatically reboot.
IP Address to Ping	Destination IP address of the device to send ping packets.
Ping Interval	Sending ping interval.
Start up Delay	Starting the Ping watchdog is enabled when you enable this item, after the system has booted, delaying the time to ping watchdog is enabled, set this parameter, you can avoid the ping watchdog function is triggered during system startup, and the user is unable to access the device management page to modify configuration and cause the device to continuously restart.
Failure Count To Reboot	Set device send ping packets to the destination IP address of the maximum number of Ping failed when the device failed to send ping packets to the destination IP address when setting a maximum number, the device will automatically reboot.

6.7 Device Discovery

In the device discovery tools page, you can view in other WITEK within the same local area network device information such as Mac address, wireless mode, SSID, product, firmware version, IP address, user views device information and managing devices.

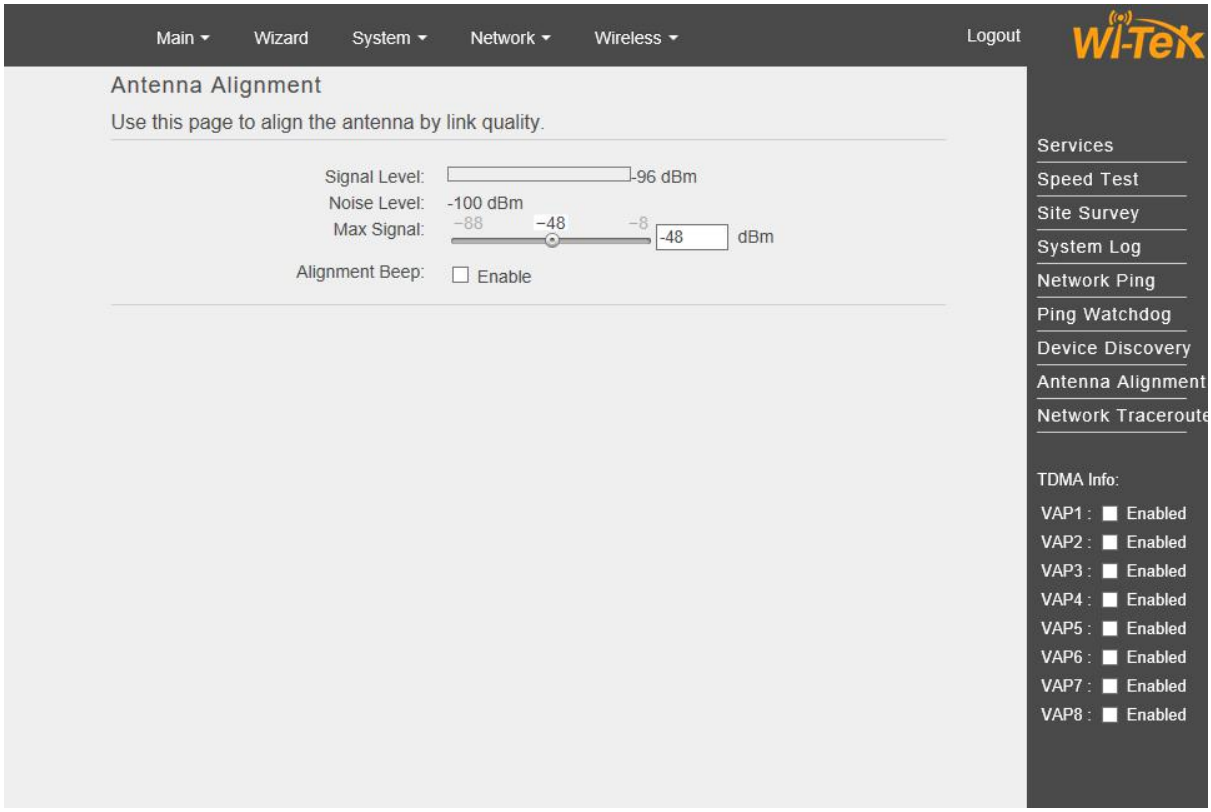


The device discovery tools in the table, No. 0 line displays the current device information for users of wireless devices, then the following are other WITEK device information for wireless devices in the LAN.

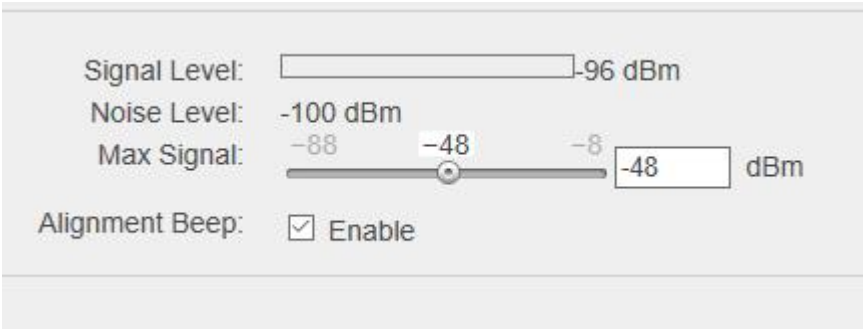
6.8 Antenna Alignment

When you set up a one-to-one devices, unable to accurately determine whether the device antenna alignment to each other, you can use the antenna proofreading function.

1. When the device antenna for more accurate with each other, showing signal strength is strong, the color blue. Among them, the strongest signal as the signal sensitivity, adjust its value, change color and beeps allows channel intensity more clearly:

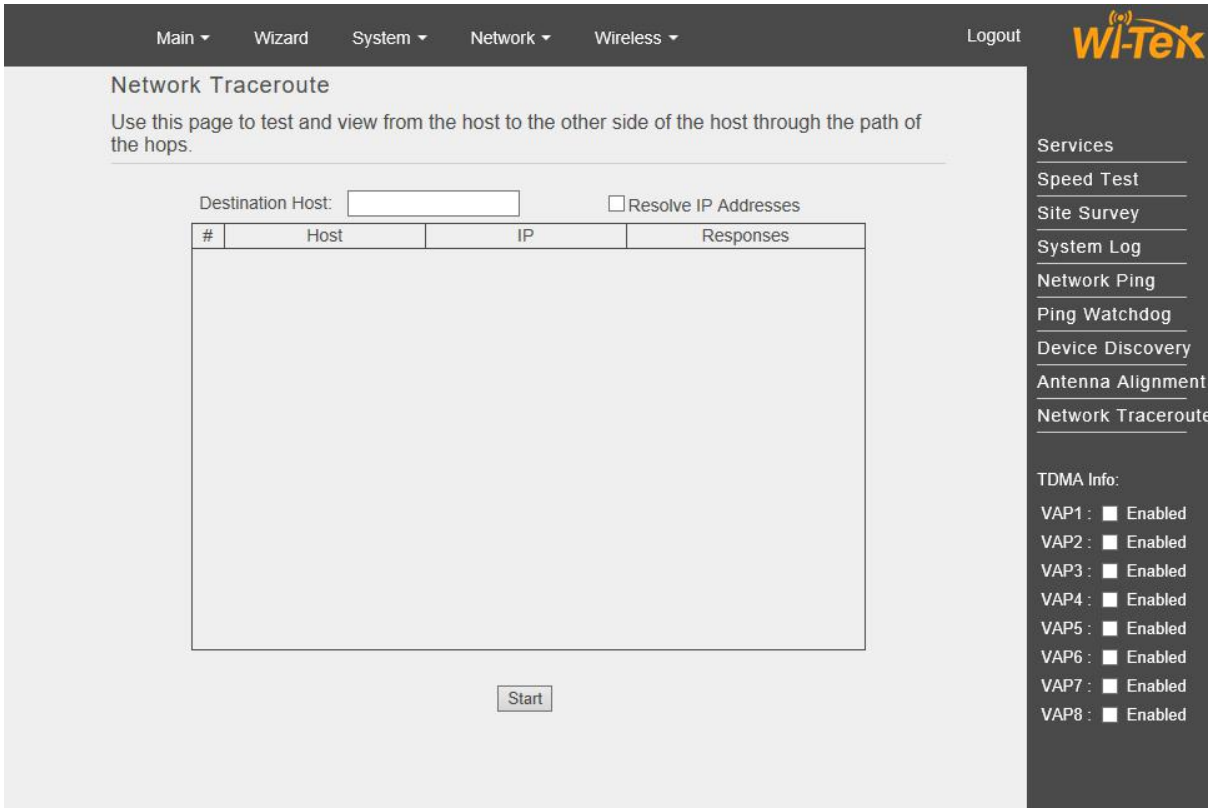


2. Which can enable beep switch, based on sound to determine if the device is on, more accurate, more beeping loudly and the more rapid:



6.9 Network Traceroute

In the network trceroute page, the user can test and view paths from the device to the specified destination host hops and delay, the network connection status and diagnostic equipment.



Destination Host	Enter the IP address or domain name of the target host (Note: on entering the domain name must be selected Resolve IP Addresses), if you enter an invalid address you will be prompted to reenter.
Resolve IP Addresses	Select this option to resolve the IP address of the target host name.
Start	Clicking < started > button to begin the test, the device will send a traceroute packet inspection on which the routing to the destination address, and displays the results in the box above.

Network Traceroute tool results display box:

Host	Display routing hop host name or IP address.
IP	Display routing hops IP addresses.
Responses	Response time display routing hop, if there is no response appears as "*".