



User Guide For Gateway

www.wireless-tek.com

CONTENTS

1. Overview	4
2. Log in to the gateway	5
3. Dashboard	6
4. Network	7
4.1. Interface	7
4.2. DHCP Server	11
4.3. MWAN	11
4.4. VLAN	12
4.5. VPN Client	13
For PPTP Client	13
4.6. Static Route	19
4.7. ARP Binding	20
4.8. Static DHCP	21
4.9. Port Attributes	22
5. Status	23
5.1. Load Monitoring	23
5.2. User Info	24
5.3. WiFi Sta Info	25
5.4. DHCP Leases	25
5.5. Authorised Users	26
5.6. Line Monitoring	26
5.7. License	28
5.8. ARP List	28
5.9. System Route Table	30
6. Smart QoS	31
6.1. Qos Configuration	31
6.2. Flow Control	32
6.3. Port Route	34
6.4. Domain Route	36
6.5. Load Balance	37
6.6. ISP Segment	38
7. Firewall	39
7.1. Port Mapping	39
7.2. NAT	41

7.3. Host Mapping	42
7.4. Access Control List	43
7.5. LAN Forward	44
7.6. Share-Net Block	45
7.7. Connection Limit	46
7.8. DMZ Server	47
8. VPN Server	48
8.1. PPTP Service	48
8.2. L2TP Service	50
8.3. OpenVPN Service	52
9. Hotspot	55
9.1. Service Zone	55
9.2. Local Portal	56
9.3. Biling Plan	57
9.4. Local Users	58
9.5. Vouchers	60
9.6. PPPoE Server	61
9.7. RADIUS Server	63
9.8. SMS Gateway	64
9.9. White List	65
9.10. Black List	66
9.11. Expiration Notice	68
9.12. Local Notice	69
10. Wireless	70
10.1. Overview	70
10.2. AP Group	71
10.3. AP List	75
10.4. RF Planning	76
10.5. WhiteBlack List	77
10.6. Firmware	79
10.7. Network Topology	80
11. CPE Management	81
11.1. CPE Global Configuration	81
11.2. CPE List	82
11.3. Unified Cloud	82
11.4. SD-LAN	83
12. Application	85

12.1. UPnP Server	85
12.2. DDNS	85
12.3. Wake on LAN	86
12.4. Switch Linkage	88
12.5. Smart device	88
13. Security	89
13.1. Health Monitoring	89
13.2. Examination	89
13.3. Email Notice	89
13.4. Audit	90
14. System	92
14.1. System Maintenance	92
14.2. Remote Access	94
14.3. User Management	95
14.4. Diagnosis	96
14.5. Network Tools	98
14.6. Network Parameters	98
14.7. System Time	99
14.8. CA Configuration	100

1. Overview

Applicable product models are as follows:

WI-AC500 WI-AC150, WI-AC105P V1/V2, WI-AC108P V1/V2, WI-ER205

Note: The software interface is based on v5.0.build20230629-1419-c71c5a0 after.

Revision History:

Date	Doc Version	Description
June 2023	V1.0	Initial version
April 2024	V1.1	Correction of errors in section 14.1

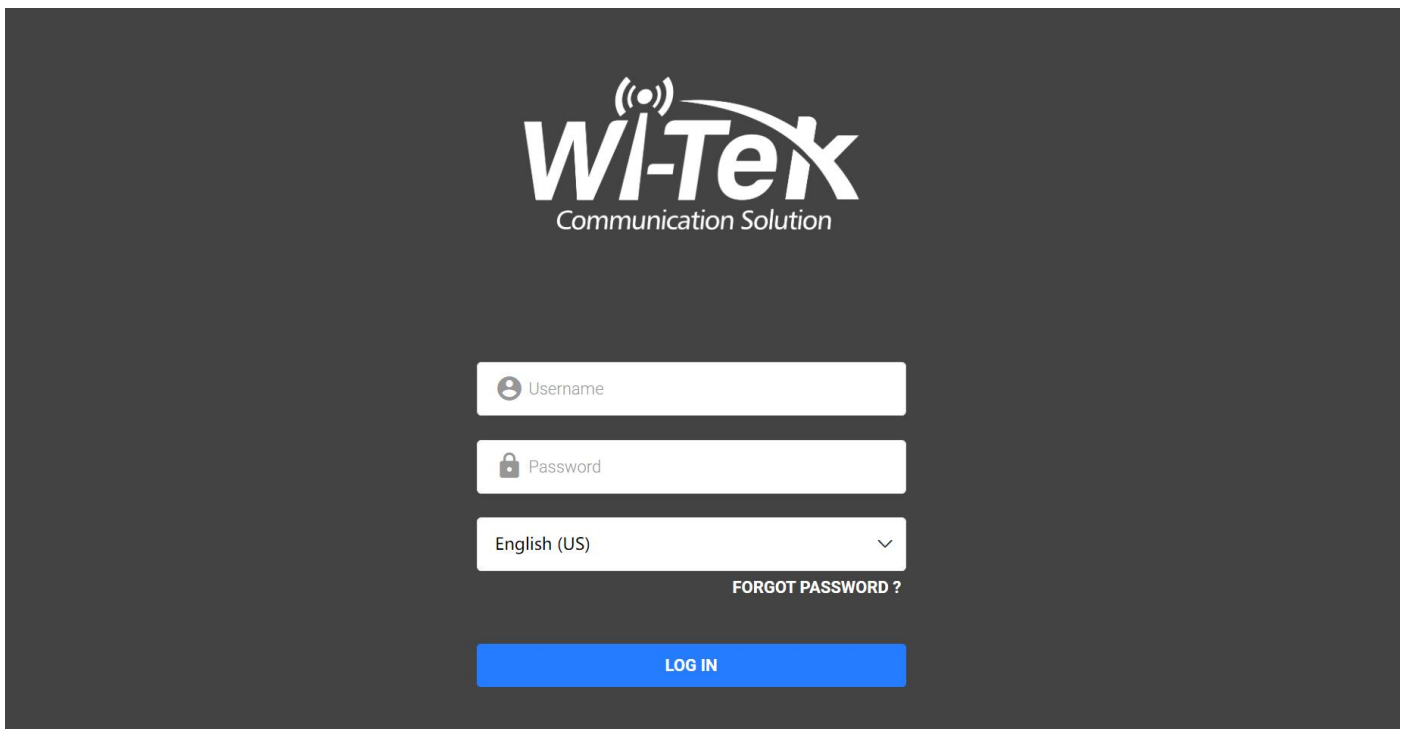
2. Log in to the gateway

1) Connect the computer to the LAN port of the gateway using a network cable. If your computer is configured with a fixed IP address, please change it to 'Automatically obtain IP address'.

2) Open a web browser and type the default management address **http://192.168.10.1** in the address field of the browser, then press the Enter key.



3) Enter the default username: **admin**, password: **admin**.



After a successful login, you can configure the function by clicking the setup menu on the left side of the screen.

3. Dashboard

The dashboard page displays basic system information (such as network status, WiFi information, and system time) and operational information (such as traffic statistics, interface status, memory utilization, and CPU utilization).

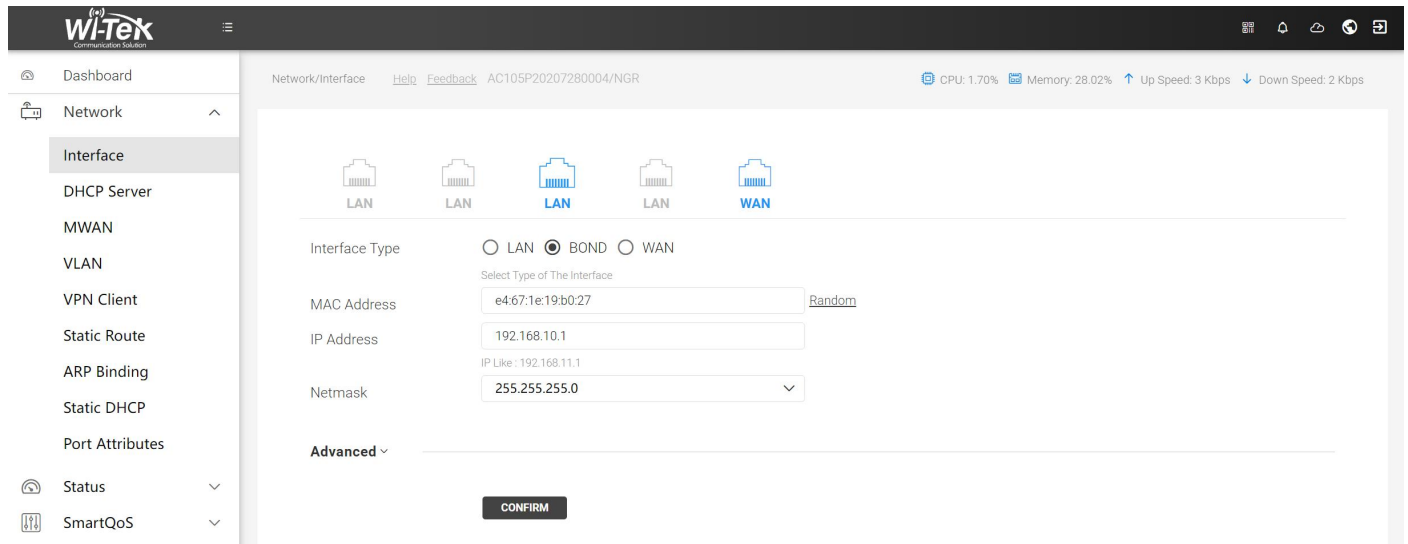
The screenshot shows the Wi-Tek dashboard interface. On the left is a navigation menu with options like Dashboard, Network, Status, SmartQoS, Firewall, VPN Server, HotSpot, Wireless, CPE Management, Unified Cloud, Application, Security, System, and Logging. The main content area displays system information at the top: CPU: 1.19%, Memory: 36.34%, Up Speed: 27 Kbps, Down Speed: 35 Kbps. Below this is a 'Network Status' section with icons for Network Capacity (0.0%), Users Online (3/147/150), Switch (Online 0/Total 0), Access Point (Online 1/Total 1), WiFi Users (1), and Authentication (0 Success/0 Failed/0 Total). A 'WiFi Allocation' bar shows 2.4G WiFi and 5G WiFi usage. Two line charts show 'Flow of recently 5 minutes' for Upload and Download flows. A 'Top10 User Flow' bar chart lists IP addresses and their data usage. A 'Top10 AP-Load' bar chart shows the load for AP ID CDUTD001217190003. At the bottom is a 'Network Monitoring' table with columns for Name, Type, Status, Protocol, IP Address, IPv6 Address, Gateway, DNS, MAC Address, and VLAN.

Name	Type	Status	Protocol	IP Address	IPv6 Address	Gateway	DNS	MAC Address	VLAN
lan	BOND	DOWN	static	192.168.10.1/255.255.255.0	-	-	-	e4:67:1e:19:b0:27	0
lan	BOND	UP	static	192.168.10.1/255.255.255.0	-	-	-	e4:67:1e:19:b0:27	0
lan	BOND	UP	static	192.168.10.1/255.255.255.0	-	-	-	e4:67:1e:19:b0:27	0
wan	WAN	UP	static	192.168.13.12/255.255.255.0	-	192.168.13.1	192.168.13.1	e4:67:1e:19:b0:28	0
wan2	WAN	DOWN	dhcp	-	-	-	-	00:db:b7:e9:46:1a	0

4. Network

4.1. Interface

Choose the menu **Network > Interface** to load the following page.




Parameter	Describe
Interface Type For LAN	<p>LAN:Each port is a separate physical interface and can be assigned to a separate network segment.</p> <p>Note: Supports up to 4 LAN ports.</p> <p>BOND:Combine multiple LAN ports into a switch group and and can be assigned to a separate network segment.</p> <p>Note: For AC108P, it cannot be split into multiple independent LAN ports.</p>

Then click on the **Advanced** option to load the following page.

Advanced ^

Secondary IP

Configure	IP Address	Netmask
 No data available		

IPv6 prefix length

Delegate a prefix of given length to this interface

IPv6 Address

Allowed values: "eui64", "random", fixed value like "::1"

DNS-Proxy Forced DNS-Proxy

DHCP Mode Disable Basic Mode Advance Mode

Parameter	Describe
Secondary IP	Add an IP or network segment to the specified LAN port.
IPv6 prefix length	Delegate a prefix of given length to this interface.
IPv6 Address	Specify an IPv6 address for the interface.
DNS-Proxy	Check it to force the use of local DNS for domain name resolution
DHCP Mode	Disable: Select it to disable the DHCP server under this interface. Basic Mode: Specify the range of IP address allocation, total number of IPs, and IP address lease term. Advance Mode: In addition to the basic mode, you can specify the subnet mask and gateway.



Interface Type WAN

Select Type of The Interface

MAC Address [Random](#)

IP Protocol DHCP DHCPv6 Static PPPoE

RECONNECT

DNS

Acquire IPv6 Addr

DHCPv6 related Disable Enable

Bandwidth /

REFERENCE BANDWIDTH

Load Balance

Link Detection Enable Detection

CONFIRM

Parameter	Describe
Interface Type For WAN	WAN:The port used for internet connectivity. Note:Supports up to 4 WAN
MAC Address	Randomly generate MAC addresses.
IP Protocol	DHCP: Automatically obtain the IP address of IPv4 DHCP v6: Automatically obtain the IP address of IPv6 Static: Enter normal IP address, mask, gateway,etc. PPPoE: Enter the broadband account and password provided by your ISP.
DNS	Optional. Enter the IP address of the DNS server provided by your ISP.
Acquire IPv6 Addr	The default is disabled. If auto is selected, it will detect whether the upper network has an IPv6 IP address.
DHCPv6 related	The default is disabled. Select Enable to set the corresponding mode.

Bandwidth	Select a value greater than or equal to the actual bandwidth.
Load Balance	The realization of load balancing requires multiple WAN to be in one group.
Link Detection	For the network topology with multiple WAN accesses, enable it, enter the corresponding parameters, and automatically kick off the offline WAN port from the load balancing group.

4.2. DHCP Server

Choose the menu **Network > DHCP Server** to load the following page. You can add or edit the parameters of the DHCP server.

Network/DHCP Server Help Feedback AC105P202072 CPU: 1.79% Memory: 26.39% Up Speed: 7 Kbps Down Speed: 6 Kbps

Input Content ADD RESTART SERVICE

Configure	LAN	Status	DHCPv4 Start IP	DHCPv4 Pool Size	IPv4 DNS	Gateway	DHCPv6 Status	DHCPv6-Mode
Edit Delete	lan	Enable	192.168.103.100	150	-	192.168.103.1	Disabled	Stateless
Edit Delete	lan2	Enable	192.168.11.100	150	-	192.168.11.1	Disabled	Stateless

Records per page: 20 1-2 of 2 < >

4.3. MWAN

In special scenarios where the number of WAN connections exceeds the available WAN ports on the gateway, the MWAN (Multi-WAN) feature can be used in conjunction with a managed switch that supports the 802.1q protocol. This allows for an expansion of the WAN port capacity beyond the physical limitations of the gateway.

Choose the menu **Network > MWAN** to load the following page.

Interface Type VLAN-Tag based WAN Port MAC based WAN Port

Select Type of The Interface

Main Interface

VLAN TAG

MAC Address [Random](#)

IP Protocol DHCP DHCPv6 Static PPPoE

RECONNECT

DNS

Acquire IPv6 Addr

DHCPv6 related Disable Enable

Bandwidth /

REFERENCE BANDWIDTH

Load Balance

Link Detection Enable Detection

CONFIRM

Parameter	Describe
Interface Type	<p>VLAN-Tag based WAN Port</p> <p>Select it, select the corresponding WAN port, and enter the VLAN ID of the corresponding port created on the managed switch.</p> <p>Interface Type <input checked="" type="radio"/> VLAN-Tag based WAN Port <input type="radio"/> MAC based WAN Port</p> <p>Select Type of The Interface</p> <p>Main Interface <input type="text"/></p> <p>VLAN TAG <input type="text" value="1 ~ 4094, Can not be repeated."/></p> <p>MAC based WAN Port</p> <p>Select it, select the corresponding WAN port, and enter any number in the Port Index without repeating it.</p> <p>Interface Type <input type="radio"/> VLAN-Tag based WAN Port <input checked="" type="radio"/> MAC based WAN Port</p> <p>Select Type of The Interface</p> <p>Main Interface <input type="text"/></p> <p>Port Index <input type="text" value="1 ~ 4094, Can not be repeated."/></p>

Follow the WAN settings described in section 3.1 for other functions.

4.4. VLAN

This feature allows the creation of VLANs based on physical interfaces, enabling a single physical interface to accommodate multiple subnets.

Choose the menu **Network > VLAN** to load the following page.

Main Interface

VLAN TAG

MAC Address [Random](#)

IP Address

Netmask

IP Like : 192.168.11.1

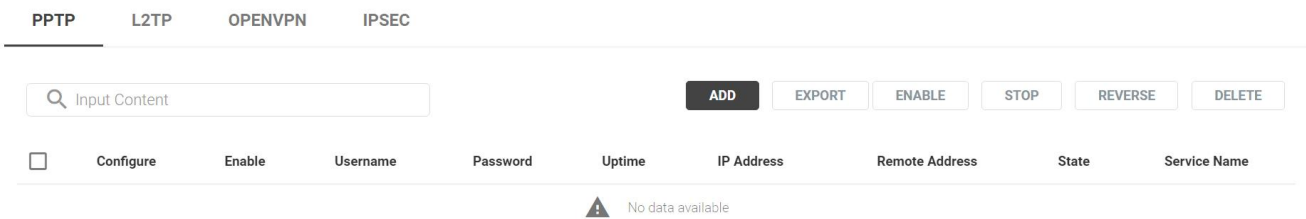
Advanced ▾

Parameter	Describe
Main interface	VLAN can only be created on non-BOND port. Please switch the certain Interface to role LAN first.
VLAN TAG	Enter VLAN ID, In actual networks, it will be used in conjunction with managed switches and APs.

Follow the LAN settings described in section 3.1 for other functions.

4.5. VPN Client

Choose the menu **Network > VPN Client** to load the following page.



For PPTP Client

Choose the menu **Network > VPN Client > PPTP** and click **ADD** to load the following page.

Name *

Enable

Server IP *

Username *

Password *

Working Mode Remote Access Site to Site

Peer subnet
Network subnet like 192.168.1.0/24, separate multiple items by space

Check Time
Disconnection reconnection detection time (unit: second), 0 indicates no detection

Parameter	Describe	
Name	Enter any name for easy recognition.	
Enable	Enable or disable PPTP Client.	
Server IP	Enter the IP or domain name provided by the VPN server.	
Username	Enter the account provided by the VPN server.	
Password	Enter the password provided by the VPN server.	
Working Mode	Remote Access (Client to Site)	It is a type of VPN that connects a single device, such as a laptop or smartphone, to a remote network, such as a corporate or cloud network.
	Site to Site	It is a type of VPN that connects two or more networks, such as branch offices or data centers, over the internet.
Peer subnet	Enter as the internal subnet of the VPN service gateway.	
Check Time	Disconnection reconnection detection time (unit: second). 0 indicates no detection.	

For L2TP Client

Choose the menu **Network > VPN Client > L2TP** and click **ADD** to load the following page.

Name *

Enable

Server IP *

Username *

Password *

Working Mode Remote Access Site to Site

Peer subnet
Network subnet like 192.168.1.0/24, separate multiple items by space

Check Time
Disconnection reconnection detection time (unit: second). 0 indicates no detection

Parameter	Describe	
Name	Enter any name for easy recognition.	
Enable	Enable or disable PPTP Client.	
Server IP	Enter the IP or domain name provided by the VPN server.	
Username	Enter the account provided by the VPN server.	
Password	Enter the password provided by the VPN server.	
Working Mode	Remote Access (Client to Site)	It is a type of VPN that connects a single device, such as a laptop or smartphone, to a remote network, such as a corporate or cloud network.
	Site to Site	It is a type of VPN that connects two or more networks, such as branch offices or data centers, over the internet.
Peer subnet	Enter as the internal subnet of the VPN service gateway.	
Check Time	Disconnection reconnection detection time (unit: second). 0 indicates no detection.	

For OPENVPN

Choose the menu **Network > VPN Client > OPENVPN** and click **ADD** to load the following page.

Client Name	<input type="text" value="Input Client Name"/>	*
	If it is our product, please enter the client name generated by certificate manager	
Enable	<input type="checkbox"/>	
Server IP	<input type="text" value="Input Server IP"/>	*
Server Port	<input type="text" value="1194"/>	*
Tunnel Proto	<input type="text" value="UDP"/>	▼
Tunnel Dev	<input type="text" value="TUN"/>	▼
Authentication Method	<input type="text" value="TLS-AUTH"/>	▼
Compress	<input type="text" value="LZO"/>	▼
Tunnel SSL	<input type="text" value="BF-CBC"/>	▼

Static Key

CA

Client Crt

Client Key

CONFIRM CANCEL

Parameter	Describe
Client Name	If the VPN service side is built by a Wi Tek gateway, please enter the client name generated by certificate management.
Enable	Enable or disable VPN client.
Server IP	Enter the public IP or domain name of the VPN server.

Server Port	Specify UDP port number.(Default :1194)
Tunnel Proto	Specify Tunnel protocol.
Tunel Dev	Support TAP and TUN mode, TAP is similar to bridge mode, TUN is similar to routing mode, and the selection of client and server should be consistent.
Authentication Method	TLS_AUTH and TLA_CRYPY are supported. Make sure the server and client choose the same.
Compress	A data compression algorithm that supports LZO and LZ4 modes.Make sure the server and client choose the same.
Tunnel SSL	Specify the encryption algorithm type.Make sure the server and client choose the same.
Static Key	Maintain consistency with the static key of the VPN server.
CA	Maintain consistency with the CA of the VPN server.
Client Crt	Create a client crt file from the VPN server side
Client Key	Create a client key from the VPN server side

For IPSEC

Choose the menu **Network > VPN Client > IPSEC** and click **ADD** to load the following page.

Name *

Enable

Remote IP

If the local host serves as the server, do not enter this parameter

Line

Local Net

eg:192.168.1.0/24 or 0.0.0.0/0. 0.0.0.0/0 indicates all lan

Remote Net

If there are multiple network segments, you can add them by wrapping lines

If there are multiple network segments, you can add them by wrapping lines

IKE Aggressive	<input type="text" value="Main Mode"/>
IKE Version	<input type="text" value="IKEv1"/>
IKE Auth	<input type="text" value="AUTO"/> , <input type="text" value="AUTO"/> , <input type="text" value="AUTO"/>
Authentication Method	<input type="text" value="Pre-Share Key"/>
Pre-Share Key	<input type="text" value="Input Pre-Share Key"/> *
Local ID	<input type="text" value="Input Local ID"/>
Remote ID	<input type="text" value="Input Remote ID"/>
ESP Encrypt	<input type="text" value="AUTO"/>
ESP Auth	<input type="text" value="AUTO"/>

Parameter	Describe
Name	Enter any name for easy recognition.
Enable	Enable or disable IPsec.
Server IP	Enter the public IP or domain name of the VPN server.
Line	Specify tunnel establishment at interface.
Local Net	Specify the local network.
Remote Net	Specify the remote network.
IKE Aggressive	Specify the IKE Exchange Mode as Main Mode or Aggressive Mode . By default, it is Main Mode. Main Mode: Main mode provides identity protection and exchanges more information, which applies to scenarios with higher requirements for identity protection. Aggressive Mode: Aggressive Mode establishes a faster connection but with lower security, which applies to scenarios with lower requirements for identity protection.
IKE Version	Specify the IKE version. Ensure that the local and remote selection versions are consistent.

IKE Auth	Specify the IKE authentication.Ensure that the local and remote IKE authentication are consistent.
Authentication Method	Pre-Share Key and Self-signed certificate are supported.
Pre-Share Key	Specify the unique pre-shared key for both peers' authentication.
Local ID	Specify the Local ID. Fill in local ID and remote ID each other.
Remote ID	Specify the remote ID. Fill in local ID and remote ID each other.
ESP Encrypt	Specify the ESP encryption algorithm used by the SA.Ensure that the local and remote ESP Encrypt are consistent.
ESP Auth	Specify the ESP authentication algorithm used by the SA.Ensure that the local and remote ESP authentication are consistent.

4.6. Static Route

Choose the menu **Network > Static Route** and click **ADD** to load the following page.

Line	<input type="text" value="wan"/>
Dest Addr	<input type="text" value="Input Dest Addr"/> *
Netmask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="Input Gateway Addrees(Optional)"/>
Priority	<input type="text" value="10"/>
Remarks	<input type="text" value="Input Remarks"/>

Parameter	Describe
Line	Specify the physical network interface through which this route is accessible.
Dest Addr	Specify the destination IP address the route leads to.
Netmask	Specify the subnet mask of the destination network.

Gateway	Specify the IP address to which the packet should be sent next
Priority	Define the priority of the route. A smaller value means a higher priority. The default value is 10. It is recommended to keep the default value.
Remarks	Give a remarks for identification.

4.7. ARP Binding

Choose the menu **Network > ARP Binding** and click ADD to load the following page.

IP	<input type="text" value="Input IP"/>
MAC	<input type="text" value="Input MAC"/>
Interface Associated	<input type="text" value=""/> ▼
Remarks	<input type="text" value="Input Remarks"/>

Parameter	Describe
IP	Enter an IP address to be bound.
MAC	Enter an MAC address to be bound.
Interface Associated	Select the specified interface.
Remarks	Give a remarks for identification.

To complete Anti ARP Spoofing configuration, there are two steps. First, add IP-MAC Binding entries to the IP-MAC Binding List. Then enable **BINDING POLICY** for these entries.

Click the **BINDING POLICY** button to load the following image.

Force Binding

 Enable

Tip: Forced binding will lose or redirect packets that does not according to rules in binding table

CONFIRM

CANCEL

Tick the **enable** button, Forced binding will lose or redirect packets that does not according to rules in binding table.

4.8. Static DHCP

Static DHCP will be needed if you want an device to always have the same IP address. So metimes required for certain programs, this feature is useful if other people on your LAN know your IP and access your PC using this IP. Static DHCP should be used in conduction with Port Forwarding. If you forward an external WAN TCP/UDP port to a port on a server running inside your LAN, you have to give that server a static IP, and this can be achieved easily through Static DHCP.

Choose the menu **Network > Static DHCP** and click **ADD** to load the following page.

IP

Input IP

MAC

Input MAC

Remarks

Input Remarks

CONFIRM

CANCEL

Parameter	Describe
IP	Enter an IP address.
MAC	Enter an MAC address.
Remarks	Give a remarks for identification.

4.9. Port Attributes

Port attributes page displays the basic port information (like the link status, speed and in/out packets).

Choose the menu **Network > Port Attributes** to load the following page.

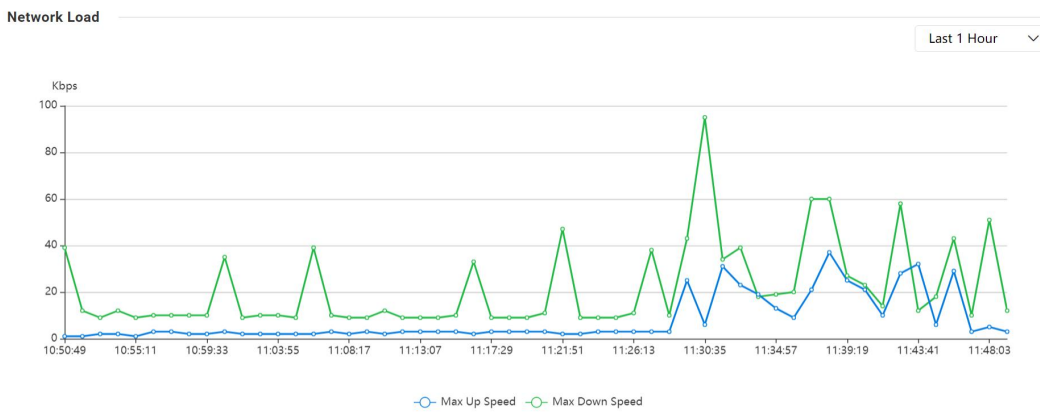
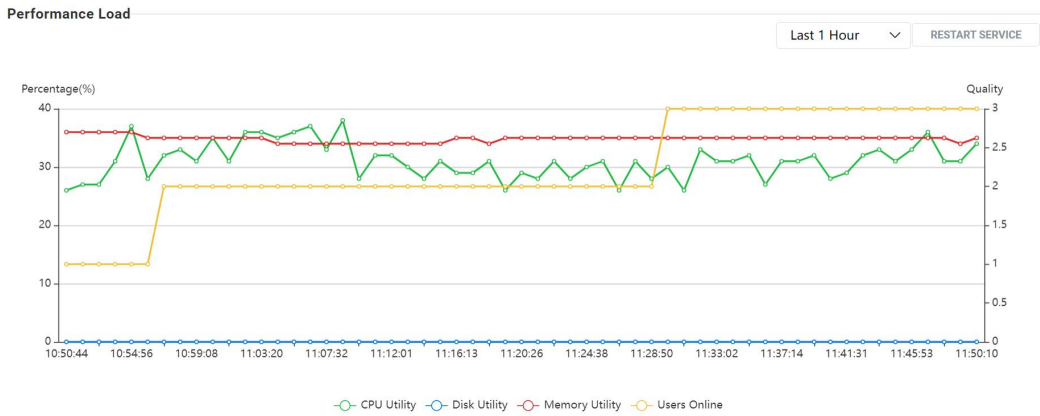
Port Name	Logic Ifname	Link Status	Auto-Negotiation	Speed	Duplex	In/Out Packets	In/Out Bytes
Port0	lan	up	Yes	1000baseT	full-duplex	145410/160621	21110888/16581521
Port1	lan2	down	Yes	NA	NA	362/1019	169626/36115
Port2	lan	up	Yes	1000baseT	full-duplex	208314/163586	31335765/159125547
Port3	wan2	down	Yes	NA	NA	0/0	0/0
Port4	wan	up	Yes	100baseT	full-duplex	245173/245397	150311911/33596704

Records per page: 20 ▾ 1-5 of 5 < >

5. Status

5.1. Load Monitoring

You can choose different time intervals to observe the device load situation. Choose the menu **Status > Load Monitoring** to load the following page.



5.2. User Info

You can observe the basic information of each user, such as IP address, MAC address, source area, online duration, etc.

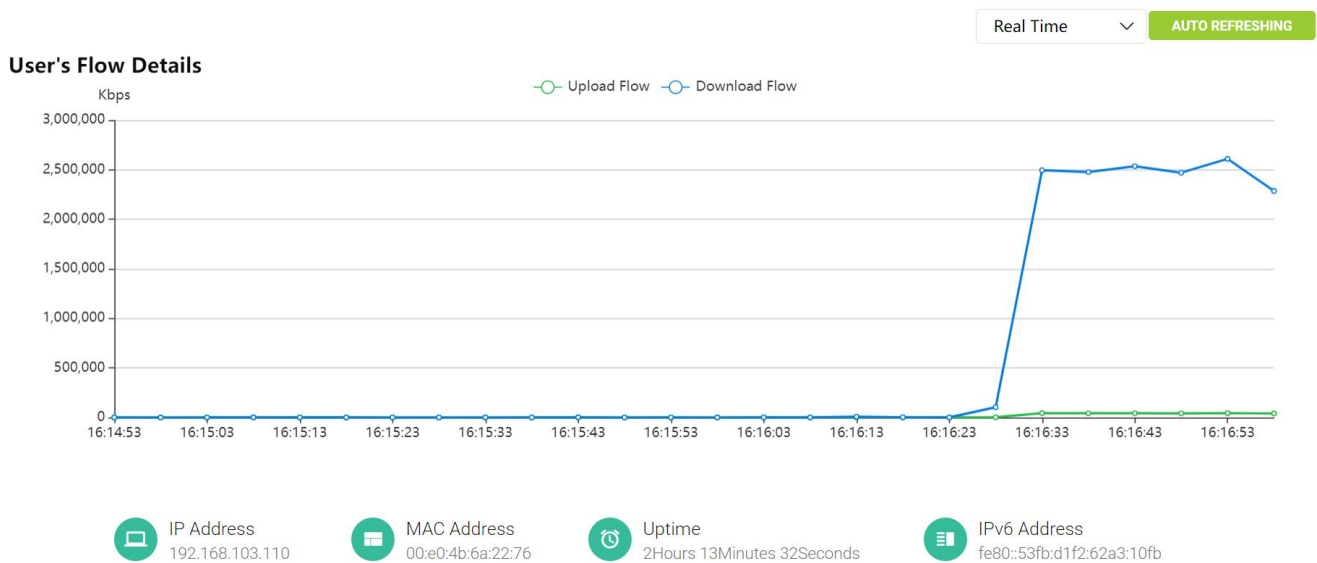
Choose the menu **Status > User Info** to load the following page.

Search: Input Content

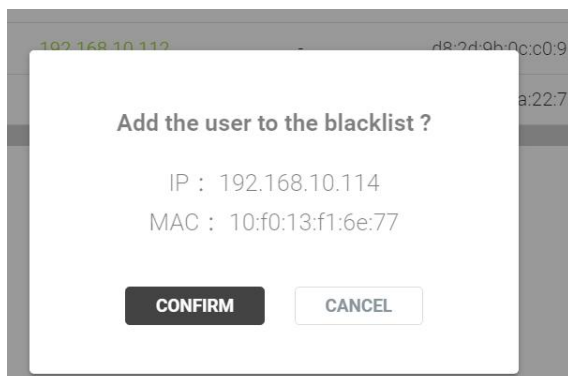
	Configure	Remarks	IP Address	IPv6 Address	MAC Address	Hostname	Src Zone	Uptime	Session Num
Details	Block	Rate Limit	192.168.10.114	fe80::12f0:13ff:fe71:6e77	10:f0:13:f1:6e:77	*	lan	1Days 3Hours 6Minutes 52Seconds	1
Details	Block	Rate Limit	192.168.10.117	fe80::2628:fdff:fe34:a382	24:28:fd:34:a3:82	*	lan	1Days 2Hours 33Minutes 5Seconds	1
Details	Block	Rate Limit	192.168.10.112	-	d8:2d:9b:0c:c0:9d	WI-TEK-CPE	lan	22Hours 27Minutes 36Seconds	6
Details	Block	Rate Limit	192.168.10.101	fe80::53fb:d1f2:62a3:10fb	00:e0:4b:6a:22:76	Aiden	lan	2Hours 26Minutes 32Seconds	37

Records per page: 20 | 1-4 of 4

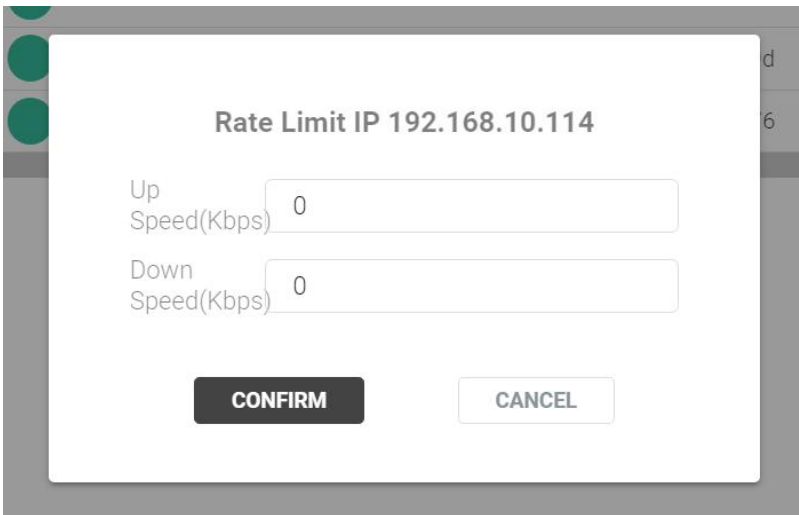
If you want to view the traffic of a specified user, please click the **Details** button to load the following image.



Clicking **Block** allows users to join the blacklist and block access to the network.



Clicking on **Rate limit** can limit users' upload and download speeds.

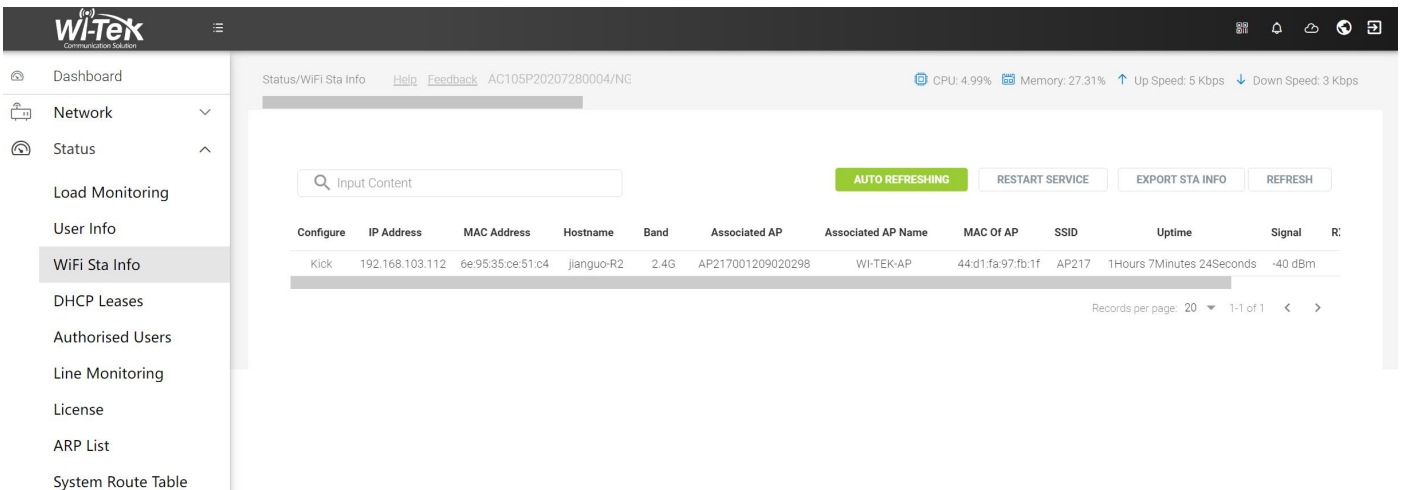


A dialog box titled "Rate Limit IP 192.168.10.114" is shown. It contains two input fields: "Up Speed(Kbps)" and "Down Speed(Kbps)", both with the value "0" entered. At the bottom, there are two buttons: "CONFIRM" and "CANCEL".

5.3. WiFi Sta Info

You can observe the basic information of wireless users and click **Kick** to kick off the wireless client.

Choose the menu **Status > WiFi Sta Info** to load the following page.



The screenshot shows the "WiFi Sta Info" page in the Wi-Tek management interface. The page displays system status (CPU: 4.99%, Memory: 27.31%, Up Speed: 5 Kbps, Down Speed: 3 Kbps) and a table of wireless stations. A search bar and several control buttons (AUTO REFRESHING, RESTART SERVICE, EXPORT STA INFO, REFRESH) are visible above the table.

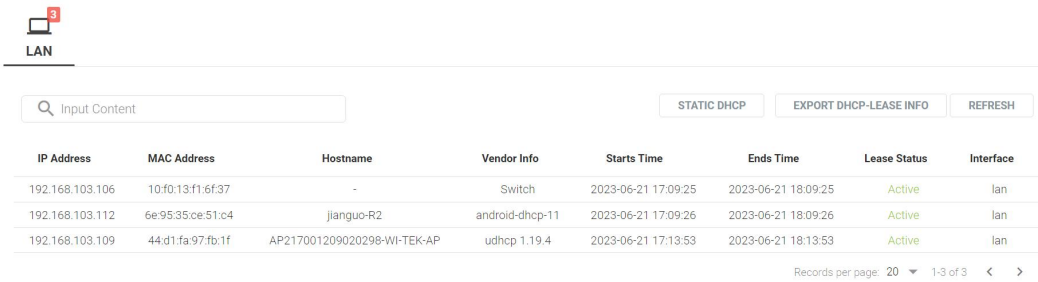
Configure	IP Address	MAC Address	Hostname	Band	Associated AP	Associated AP Name	MAC Of AP	SSID	Uptime	Signal	R
Kick	192.168.103.112	6e:95:35:ce:51:c4	jianguo-R2	2.4G	AP217001209020298	WI-TEK-AP	44:d1:fa:97:fb:1f	AP217	1Hours 7Minutes 24Seconds	-40 dBm	

Records per page: 20 1-1 of 1

5.4. DHCP Leases

You can view the DHCP client list. If you want to schedule an IP address for a specified client to use, you can click the **STATIC DHCP** button to go to the specified page and add a n IP address.

Choose the menu **Status > DHCP Leases** to load the following page.

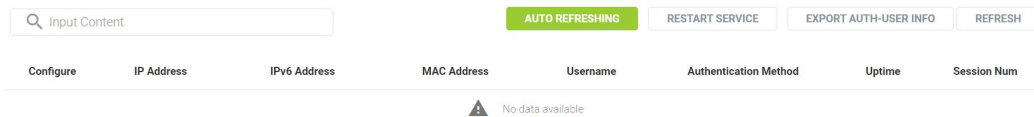


IP Address	MAC Address	Hostname	Vendor Info	Starts Time	Ends Time	Lease Status	Interface
192.168.103.106	10:fd:13:f1:f6:37	-	Switch	2023-06-21 17:09:25	2023-06-21 18:09:25	Active	lan
192.168.103.112	6e:95:35:ce:51:c4	jianguo-R2	android-dhcp-11	2023-06-21 17:09:26	2023-06-21 18:09:26	Active	lan
192.168.103.109	44:d1:fa:97:fb:1f	AP217001209020298-WI-TEK-AP	udhcp 1.19.4	2023-06-21 17:13:53	2023-06-21 18:13:53	Active	lan

Records per page: 20 1-3 of 3

5.5. Authorised Users

Choose the menu **Status > Authorised Users** to load the following page.



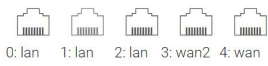
Configure	IP Address	IPv6 Address	MAC Address	Username	Authentication Method	Uptime	Session Num
⚠ No data available							

5.6. Line Monitoring

Line monitoring will collect statistics on line status and receive and transmit data packets, providing visual basis for IT administrators.

Choose the menu **Status > Line Monitoring** to load the following page.

Interface Status



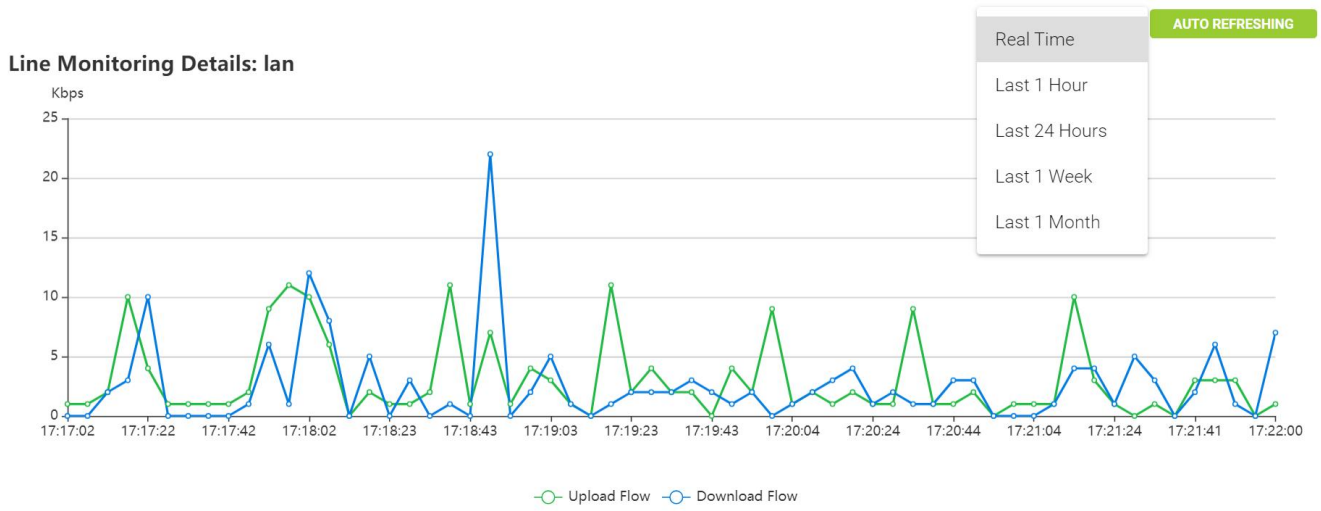
Line Monitoring

Input Content AUTO REFRESHING REFRESH

Details	Interface	Port Name	Status	IP Address	IPv6 Address	Sessions	RX rate	TX rate	TX bytes	RX bytes	TX packets(dropped/total)	RX packets(dropp
Details	lan	eth0.4090	Enable	192.168.103.1/255.255.255.0	-	84	10 Kbps	4 Kbps	845.689 MB	39.616 MB	0 / 668037	359 / 4074
Details	lan	eth0.4091	Stop	192.168.103.1/255.255.255.0	-	84	0 Kbps	12 Kbps	53.538 KB	0.000 B	0 / 363	0 / 0
Details	lan	eth0.4092	Enable	192.168.103.1/255.255.255.0	-	84	2 Kbps	17 Kbps	1.967 GB	566.810 MB	0 / 1611620	17 / 109050
Details	wan2	eth0.4093	Enable	10.10.89.254/255.255.255.0	-	186	2 Kbps	4 Kbps	2.768 MB	49.395 MB	0 / 29748	10 / 4183
Details	wan	eth0.4094	Enable	10.10.88.253/255.255.255.0	-	87	1 Kbps	1 Kbps	1.694 MB	8.546 MB	0 / 13812	19 / 14550

Records per page: 20 1-5 of 5 < >

Click the **Details** button to load the following image.



5.7. License

The device has been activated at the factory, and you can view information such as the device model, SN, and the number of manageable APs.

Choose the menu **Status > License** to load the following page.

License Status

Device has been Licensed

License Info

Model	WI-AC105P
Serial Number	AC105P20207280004
Product Vendor	
System Version	v5.0.build20230407-2049-c3a8d05

extrainfo

Max AP Num	64
Max CPE Num	64
Max MWAN Num	5
Max Account Num	400
Max PPPoE Client Num	200

EXTENDED LICENSE

5.8. ARP List

ARP List to view and bind the ARP Scanning entries. The ARP Scanning list displays all the historical scanned entries.

Choose the menu **Status > ARP List** to load the following page.

IPV4 **IPV6**

EXPORT
ADD TO DHCP STATIC ALLOCATION
ADD TO ARP BINDING TABLE
REVERSE

<input type="checkbox"/>	Interface Associated	Device IP	Device MAC	Type
<input type="checkbox"/>	eth0.4094	192.168.13.1	44:d1:fa:7b:4c:eb	REACHABLE
<input type="checkbox"/>	eth0.4094	192.168.13.15	e4:67:1e:09:90:60	STALE
<input type="checkbox"/>	br-lan	192.168.10.105	44:d1:fa:a6:d7:f8	REACHABLE
<input type="checkbox"/>	br-lan	192.168.10.101	00:e0:4b:6a:22:76	REACHABLE

Records per page: 20 1-4 of 4 < >

Parameter	Describe
-----------	----------

Interface Associated	Displays the network interface of an ARP entry.
Device IP	Displays the IP address of an ARP entry.
Device MAC	Displays the MAC address of an ARP entry.
Type	Displays the type of an ARP entry.

Select the entry and click the **ADD TO DHCP STATIC ALLOCATION** button to add static DHCP list.

The screenshot shows a web interface with a search bar and several buttons: EXPORT, ADD TO DHCP STATIC ALLOCATION, ADD TO ARP BINDING TABLE, and REVERSE. Below the buttons is a table with columns: Interface Associated, Device IP, Device MAC, and Type. The table contains four rows of data. The first row is selected, and a confirmation dialog is displayed over it. The dialog text is: "Confirm to Add the following to the Static DHCP List", "IP : 192.168.10.101", "MAC : 00:e0:4b:6a:22:76". There are CONFIRM and CANCEL buttons at the bottom of the dialog.

Interface Associated	Device IP	Device MAC	Type
eth0.4094	192.168.13.1	44:d1:fa:7b:4c:eb	REACHABLE
eth0		e4:67:1e:09:90:60	STALE
br-lan		44:d1:fa:a6:d7:f8	REACHABLE
br-lan		00:e0:4b:6a:22:76	REACHABLE

Select the entry and click the **ADD TO DHCP BINDING TABLE** button to add static DHCP list.

The screenshot shows a web interface with tabs for IPV4 and IPV6. Below the tabs is a search bar and several buttons: EXPORT, ADD TO DHCP STATIC ALLOCATION, ADD TO ARP BINDING TABLE, and REVERSE. Below the buttons is a table with columns: Interface Associated, Device IP, Device MAC, and Type. The table contains four rows of data. The first row is selected, and a confirmation dialog is displayed over it. The dialog text is: "Confirm to add the following to the ARP binding List?", "IP : 192.168.10.101", "MAC : 00:e0:4b:6a:22:76", "Interface : br-lan". There are CONFIRM and CANCEL buttons at the bottom of the dialog.

Interface Associated	Device IP	Device MAC	Type
eth0.4094	192.168.13.1	44:d1:fa:7b:4c:eb	REACHABLE
eth0		e4:67:1e:09:90:60	STALE
br-lan		44:d1:fa:a6:d7:f8	REACHABLE
br-lan		00:e0:4b:6a:22:76	REACHABLE

5.9. System Route Table

Choose the menu **Status > System Route Table** to load the following page.

Dest Addr	Gateway	Line	Priority
0.0.0.0/0	10.10.89.1	eth0.4093	-
0.0.0.0/0	10.10.88.1	eth0.4094	-
0.0.0.0/0	10.10.88.1	eth0.4094	1
0.0.0.0/0	10.10.89.1	eth0.4093	2
10.10.88.0/24	-	eth0.4094	1
10.10.89.0/24	-	eth0.4093	2
192.168.103.0/24	-	br-lan	-

Parameter	Describe
Dest Addr	Specify the destination IP address the route leads to.
Gateway	Specify the IP address to which the packet should be sent next.
Line	Specify the physical network interface through which this route is accessible.
Priority	Define the priority of the route. A smaller value means a higher priority.

6. Smart QoS

6.1. QoS Configuration

Enabling QoS functionality can improve service quality in situations where WAN bandwidth resources are small and there are a large number of users. Intelligent QoS is Automatically adjust usage priority based on traffic usage. The more forwarded traffic, the lower the priority.

Choose the menu **SmartQoS > QoS Configuration** to load the following page.

Flow Control State Enable Disabled

Flow Control Mode Smart-Auto Mode Strict Priority Mode

P2P Block Enable Disabled

Balance Mode By Sessions By IP

CONFIRM

Parameter	Describe
Flow Control State	Enabling or disabling the Smart QoS feature.
Flow Control Mode	Smart-Auto Mode: For application scenarios with low bandwidth and high concurrency requirements. Strict Priority Mode: For application scenarios with low bandwidth, high concurrency, and low latency requirements.
P2P Block	Enable or disable P2P blocking.
Balance Mode	When the gateway is connected to multiple WANs, within the default balance group, select by session type will allocate sessions based on weight. Select by IP mode, and it will be assigned sequentially.

6.2. Flow Control

You can control uplink and downlink bandwidth for IP or IP range.

Choose the menu **Flow Control > Flow Control > IP-BASED** and click **ADD** to load the following page.

Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disabled	
Policy Name	<input type="text" value="rule"/>	
Use Interface IP	<input type="text" value=""/> ▼	
IPv4	<input type="text" value="192.168.100.1,192.168.100.2-192.168.100.100,192...."/>	Add
	<input type="text"/>	Remove
Up Speed	<input type="text" value="Guaranteed bandwidth(Kbps)"/>	<input type="text" value="Max bandwidth(Kbps)"/> *
Down Speed	<input type="text" value="Guaranteed bandwidth(Kbps)"/>	<input type="text" value="Max bandwidth(Kbps)"/> *
Long-term	<input checked="" type="radio"/> Yes <input type="radio"/> No	
	<input type="button" value="CONFIRM"/> <input type="button" value="CANCEL"/>	

Parameter	Describe
Status	Enable or disable rules.
Policy Name	Specify a name for easy identification.
Use Interface IP	Specify the Interface for the rule to define the controlled users.
IPv4	Specify the IP address for the rule to define the controlled users.
Up Speed	Specify the Upstream Bandwidth in Kbps for the rule.
Down Speed	Specify the Downstream Bandwidth in Kbps for the rule.
Long-term	Specify the time for the rule to take effect.

Choose the menu **Flow Control > Flow Control > MAC-BASED** and click **ADD** to load the following page.

Status Enable Disabled

Policy Name

MAC Address [Add](#)
 [Remove](#)

Up Speed / *

Down Speed / *

Long-term Yes No

CONFIRM

Parameter	Describe
Status	Specify the bandwidth control enable or disabled for rule.
Policy Name	Specify a name for easy identification.
Use Interface IP	Specify the Interface for the rule to define the controlled users.
IPv4	Specify the IP address for the rule to define the controlled users.
Up Speed	Specify the Upstream Bandwidth in Kbps for the rule.
Down Speed	Specify the Downstream Bandwidth in Kbps for the rule.
Long-term	Specify the time for the rule to take effect.

6.3. Port Route

You can create port based policy routing here.

Choose the menu **SmartQoS > Port Route** and click **ADD** to load the following page.

Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disabled
Description	<input type="text" value="New Rule"/>
Dest IP	<input type="text" value="192.168.100.1,192.168.100.2-192.168.100.100,192..."/> Add
	<input type="text"/> Remove
External Port	<input type="text" value="Single port or port range(e.g: 8080 or 8080:8090)"/> Add
	<input type="text"/> Remove
Protocol	<input type="text" value="TCP"/> <input type="button" value="v"/>
Flow Priority	<input type="text" value="Priority"/> <input type="button" value="v"/>
Interface	<input type="text"/> <input type="button" value="v"/>

Parameter	Describe
Status	Enable or disable this rule.
Description	Specify a name for easy identification.
Dest IP	Specify the destination IP or IP range for the rule.
External Port	Specify the destination port or port range for the rule.
Protocol	Specify the protocol for the rule.

6.4. Domain Route

You can create domain based policy routing here.

Choose the menu **SmartQos > Domain Route** and click **ADD** to load the following page.

Basic Config

Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disabled
Description	<input type="text" value="rule"/>
Domain	<input type="text" value="Input Domain"/> Add
	<div style="border: 1px solid #ccc; height: 100px; width: 100%;"></div> Remove
Policy Priority	<input type="text" value="Priority"/> ▼
Interface	<input type="text"/> ▼

Parameter	Describe
Status	Enable or disable this rule.
Description	Specify a name for easy identification.
Domain	Specify the destination domain for the rule. Note: Support domain format, for example: www.xxxx.com.
Policy Priority	Specify Priority for the rule.
Interface	Specify the effective port for the rule.

Then click on the **advanced** button to load the following page.

Advanced ^

Host IP [Add](#)

[Remove](#)

CONFIRM
CANCEL

Parameter	Describe
Host IP	Specify the source IP or IP range for the rule.

6.5. Load Balance

You can manually modify the balance ratio of WAN lines.

Choose the menu **SmartQos > Load Balance** to load the following page.


RESTART SERVICE

Configure	Interface	Line Status	Balance Weight	Balance Group	Link Detection
Edit	wan2	Online	200000	Default	Enable
Edit	wan	Online	100000	Default	Enable

Records per page: 20 ▾ 1-2 of 2 < >

6.6. ISP Segment

If you can collect IP addresses used by different ISPs, generate an IP file in a format and upload it, combined with the policy routing function.

CTCC	CUCC	CMCC	CERNET	CUSTOM ISP 1	CUSTOM ISP 2	CUSTOM ISP 3
				DOWNLOAD ISP IP FILE	0 (0.0 B)	+ 
				Upload ISP IP File		
<div style="border: 1px solid #ccc; height: 100px;"></div>						

7. Firewall

7.1. Port Mapping

Port mapping allows extranet access to a intranet server (such as to a WWW server or FTP server on an extranet). The private IP address and service port of an intranet server are mapped into a public IP address and port, so that users from the extranet can access the intranet server. With port mapping, the public IP address but not the private IP address is visible to the users.

Choose the menu **Firewall > Port Mapping** and click ADD to load the following page.

Basic Config

Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disabled
Description	<input type="text" value="WEB"/> *
Protocol	<input type="text" value="ANY"/> ▾
Protocol	<input type="text" value="TCP"/> ▾
External Port	<input type="text" value="Single port or port range(e.g: 8080 or 8080:8090)"/> *
	<small>Single port or port range(e.g: 8080 or 8080:8090)</small>
Internal Port	<input type="text" value="Single port or port range(e.g: 8080 or 8080:8090)"/> *
	<small>Single port or port range(e.g: 8080 or 8080:8090)</small>
Internal IP Address	<input type="text" value="Input Internal IP Address"/>

Parameter	Describe
Status	Enable or disable this rule.
Description	Specify a name for easy identification.
Protocol	Specify the trigger protocol for the trigger port.
External Port	Specify a port range used by extranet users to access the intranet server.
Internal Port	Specify the port or port range used by the Internal Services.
Internal IP Address	Specify the IP address of the intranet server.

Then click on the **advanced** button to load the following page.

Advanced ^

Source IP

Source port

WAN IP Address

Reflection Enable Disabled

SNAT Enable Disabled

Long-term Yes No

Parameter	Describe
Source IP	Specify the source IP input range.
Source port	Specify the source port input range.
WAN IP Address	If you specified the WAN IP, the outside can only Access through that address. If you do not specified the WAN IP, the outside can access through all WANs.
Reflecion	When use port mapping in lan, reflection should be enabled.
SNAT	Allows the source IP to be rewritten to a specific IP address, cannot be used at the same time with reflection.
Long-term	Specify the effective time of this rule.

7.2. NAT

Network Address Translation generally involves "re-writing the source and/or destination addresses of IP packets as they pass through a router or firewall".

Choose the menu **Firewall > NAT** and click **ADD** to load the following page.

Basic Config

Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disabled
Description	<input type="text" value="WEB"/> *
Protocol	<input type="text" value="ANY"/> ▼
Protocol	<input type="text" value="ANY"/> ▼
Source Zone	<input type="text" value="WAN"/> ▼
Dest Zone	<input type="text" value="LAN"/> ▼
Source IP	<input type="text" value="IP or IP range,like 172.16.3.2 or 172.16.3.0/24"/>
	<small>IP or IP range,like 172.16.3.2 or 172.16.3.0/24</small>
Dest Addr	<input type="text" value="IP or IP range,like 172.16.3.2 or 172.16.3.0/24"/>
	<small>IP or IP range,like 172.16.3.2 or 172.16.3.0/24</small>
NAT Addr	<input type="text" value="NAT Addr"/>
NAT Port	<input type="text" value="NAT Port"/>
Action	<input type="text" value="SNAT"/> ▼

Parameter	Describe
Status	Enable or disable this rule.
Description	Specify a name for easy identification.
Protocol	Specify the trigger protocol for the trigger port.
Source Zone	Specifies the traffic source zone(ROUTER, LAN or WAN).
Dest Zone	Specifies the traffic destination zone(ROUTER, LAN or WAN).
Source IP	Specifies the traffic source IP (IP or IP Range).

Dest Addr	Specifies the traffic Dest Addr (IP or IP Range).
NAT Addr	For SNAT rewrite the source address to the given address.For DNAT, match incoming traffic directed at the given destination ip address.
NAT Port	For SNAT, match traffic directed at the given ports.For DNAT, redirect matched incoming traffic to the given port on the internal host.
Action	NAT target (DNAT or SNAT) to use when generating the rule.

7.3. Host Mapping

Using IPv6 for internal networks,when the host IPv6 address changes, the host MAC address can be used as a condition for open internal services.

Choose the menu **Firewall > Host Mapping** and click **ADD** to load the following page.

Basic Config

Status Enable Disabled

Description *

Protocol ▾

Internal Port *

Single port or port range(e.g: 8080 or 8080:8090)

MAC Address [Add](#)

[Remove](#)

Sync To Cloud Enable Disabled

Server Type ▾

CONFIRM **CANCEL**

Parameter	Describe
-----------	----------

Status	Enable or disable this rule.
Description	Specify a name for easy identification.
Protocol	Specify the trigger protocol for the trigger port.
Internal Port	Matching and mapping internal port of internal network hosts
MAC Address	Matching and mapping MAC addresses of internal network hosts.
Sync To Cloud	the latest IPv6 address of servers can be seen through cloud platform or wx-app.
Server Type	Server Type (WWW, FTP, Email or SNAT) to use when generating the rule.

7.4. Access Control List

Access control lists (ACLs) can control the traffic entering a network. When you configure ACLs, you can selectively admit or reject inbound traffic, thereby controlling access to your network or to specific resources on your network.

Choose the menu **Firewall > Access Control List** and click **ADD** to load the following page.

Basic Config

Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disabled
Rule Description	<input type="text" value="Input Rule Description"/>
Protocol	<input type="text" value="ANY"/> <input type="button" value="v"/>
Source Zone	<input type="text" value="LAN"/> <input type="button" value="v"/>
Dest Zone	<input type="text" value="WAN"/> <input type="button" value="v"/>
Protocol	<input type="text" value="ANY"/> <input type="button" value="v"/>
Source IP Address	<input type="text" value="Input Source IP Address"/> <small>Single address or network (e.g. 172.16.3.2 or 172.16.3.0/24), separate multiple items by space</small>
Dest Addr	<input type="text" value="Input Dest Addr"/> <small>Single address or network (e.g. 172.16.3.2 or 172.16.3.0/24), separate multiple items by space</small>
Action	<input type="text" value="ACCEPT"/> <input type="button" value="v"/>
Long-term	<input checked="" type="radio"/> Yes <input type="radio"/> No

CONFIRM

CANCEL

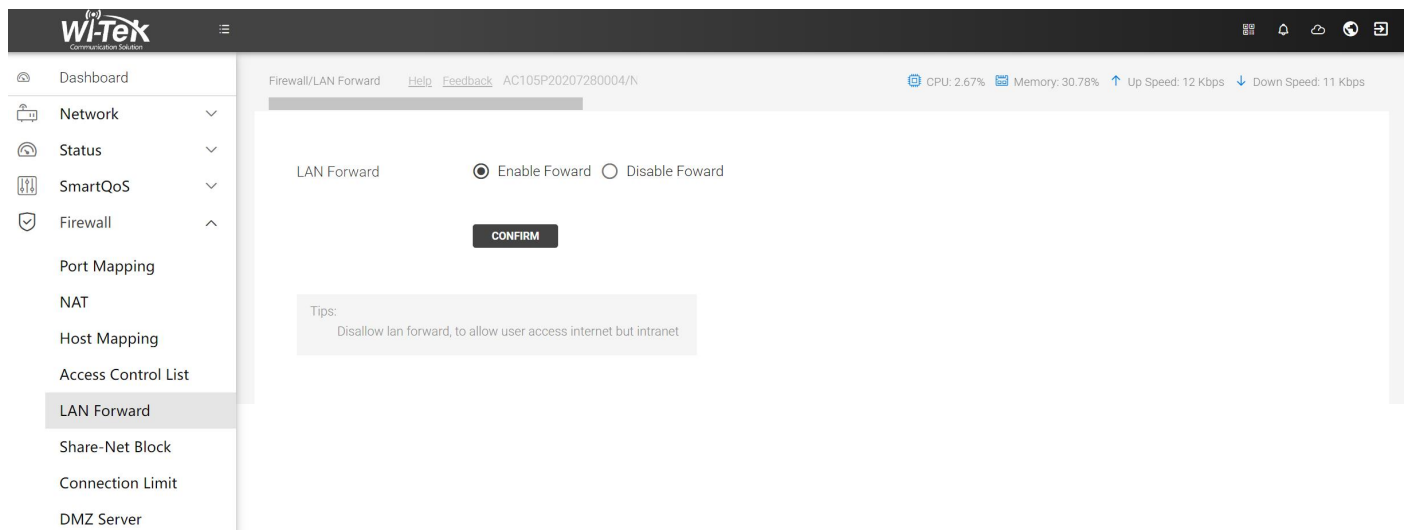
Parameter	Describe
-----------	----------

Status	Enable or disable this rule.
Rule Description	Specify a name for easy identification.
Protocol	Protocol family (ipv4, ipv6 or any) to generate ACL rules for.
Source Zone	Specifies the traffic source zone(ROUTER, LAN or WAN).
Dest Zone	Specifies the traffic destination zone(ROUTER, LAN or WAN).
Protocol	Protocol family (TCP, UDP, ICMP or any) to generate ACL rules for.
Source IP Address	Specifies the traffic source IP (IP or IP Range).
Dest Addr	Specifies the traffic Dest Addr (IP or IP Range).
Action	ACL target (ACCEPT, REJECT, DROP) to use when generating the rule.
Long-term	Specify the effective time of this rule.

7.5. LAN Forward

You can block inter LAN access with just one click, and the default is to allow forwarding between LANs.

Choose the menu **Firewall > LAN Forward** to load the following page.



If you set up multiple subnets in the gateway and select the Disable Forward option, the following page will be loaded.

Select the **Disallow Forward** button and check the blocked subnet.

LAN Forward Allow Foward Disallow Foward
 Disabled interface lan lan3

CONFIRM

Tips:
 Disallow lan forward, to allow user access internet but intranet

7.6. Share-Net Block

You can prevent the secondary router from accessing the internet.
 Choose the menu **Firewall > Share-Net Block** to load the following page.

Share-Net Block Configure

Subnet Blocked lan
 Unblock IP List [Add](#)
 [Remove](#)

CONFIRM

Parameter	Describe
Subnet Blocked	Select it, the secondary router under this subnet cannot access the internet.
Unblock IP List	Unblock IP or IP range.

7.7. Connection Limit

Session Limit feature allows Network Administrator to limit the number of sessions that a LAN client can use. This feature will prevent the router's resources from being occupied by a single host, especially who are downloading using P2P software.

Choose the menu **Firewall > Connection Limit** and click **ADD** to load the following page.

Status Enable Disabled

Internal IP Address [Add](#)
 [Remove](#)

Protocol ALL TCP UDP ICMP

External Port
Single port or port range(e.g: 8080 or 8080:8090)

Sessions *

Remarks *

Parameter	Describe
Status	Enable or disable this rule.
Internal IP Address	Restrict sessions for IP
Protocol	Select protocol type for the rules.
External Port	Restrict sessions for external port,
Sessions	Specify the max sessions for the IP
Remarks	Specify a name for easy identification.

7.8. DMZ Server

Choose the menu **Firewall > DMZ Server** and click **ADD** to load the following page.

Status Enable Disabled

Interface

External IP Address

Internal IP Address *

Advanced ^

Exclude Protocol

Exclude Port
Single port or port range(e.g: 8080 or 8080:8090)

Remarks

CONFIRM

CANCEL

Parameter	Describe
Status	Enable or disable this rule.
Interface	Specify the effective interface for the rule.
External IP Address	If you choose Any, you need to specify the WAN port public IP address.
Internal IP Address	Enter the IP address of the host specified as DMZ server.
Exclude Protocol	Exclude protocol not participating in DMZ services
Exclude Port	Exclude ports from participating in DMZ services
Remarks	Specify a name for easy identification.

8. VPN Server

8.1. PPTP Service

Choose the menu **VPN Server > PPTP Service** to load the following page.

Basic Config

PPTP Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Internal IP	<input type="text" value="172.16.3.1"/>
Start Address	<input type="text" value="172.16.3.2-200"/> <small>IP Range,like:172.16.3.2-200 or 172.16.3.1-255.254</small>
DNS	<input type="text" value="172.16.3.1"/>
Working Mode	<input checked="" type="radio"/> NAT <input type="radio"/> ROUTE
Service Binding Interface	<input type="checkbox"/> lan <input checked="" type="checkbox"/> wan <input type="checkbox"/> wan2
State	Stopped

Parameter	Describe
PPTP Server	Enable or disable this rule.
Internal IP	Local IP of VPN tunnel (Cannot conflict with other subnets)
Start Address	IP pool assigned for VPN clients.
DNS	Provide DNS resolution for PPTP clients.
Working Mode	Traffic forwarding mode.
Service Binding Interface	Specify the WAN port used for PPTP tunnel.

Then click on the **advanced** button to load the following page.

Advanced ^

Authentication Method Local User Auth RADIUS Auth

Auth Protocol pap chap mschap mschap-v2

MTU

MRU

Detection Interval Minutes

Detection Times time

Encrypted Enable Disable

Encryption Method Refuse 40bit-mppe Refuse 56bit-mppe Stateless

Compression Enable Disable

Compression Method Refuse BSD Compression Refuse Deflate Compression

Parameter	Describe
Authentication Method	Authentication method that server will accept.
Auth Protocol	Authentication protocol that server will accept.
MTU	Maximum Transmission Unit.You can keep the default value for this setting.
MRU	Maximum Receive Unit.You can keep the default value for this setting.
Detection Interval	Detect VPN tunnel "heartbeat "time interval.The default value is 600 seconds.
Detection Times	Detect VPN tunnel "heartbeat "count. The default value is 3.
Encrypted	Provide encryption for VPN tunnels.The default is enabled.
Encryption Method	Specify tunnel encryption type.
Compression	Provide compression types for data.
Compression Method	Specify compression method.

8.2. L2TP Service

Choose the menu **VPN Server > L2TP Service** to load the following page.

Basic Config

L2TP Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Internal IP	<input type="text" value="172.16.4.1"/>
Start Address	<input type="text" value="172.16.4.2-200"/> <small>IP Range,like:172.16.3.2-200 or 172.16.3.1-255.254</small>
DNS	<input type="text" value="172.16.4.1"/>
Working Mode	<input checked="" type="radio"/> NAT <input type="radio"/> ROUTE
Service Binding Interface	<input type="checkbox"/> lan <input checked="" type="checkbox"/> wan <input type="checkbox"/> wan2
State	Stopped

Parameter	Describe
L2TP Server	Enable or disable this rule.
Internal IP	Local IP of VPN tunnel (Cannot conflict with other subnets)
Start Address	IP pool assigned for VPN clients.
DNS	Provide DNS resolution for PPTP clients.
Working Mode	Traffic forwarding mode.
Service Binding Interface	Specify the WAN port used for L2TP tunnel.

Then click on the **advanced** button to load the following page.

Advanced ^

Authentication Method Local User Auth RADIUS Auth

Auth Protocol pap chap mschap mschap-v2

MTU

MRU

Detection Interval Minutes

Detection Times time

Encrypted Enable Disable

Encryption Method Refuse 40bit-mppe Refuse 56bit-mppe Stateless

Compression Enable Disable

Compression Method Refuse BSD Compression Refuse Deflate Compression

CONFIRM

Parameter	Describe
Authentication Method	Authentication method that server will accept.
Auth Protocol	Authentication protocol that server will accept.
MTU	Maximum Transmission Unit.You can keep the default value for this setting.
MRU	Maximum Receive Unit.You can keep the default value for this setting.
Detection Interval	Detect VPN tunnel "heartbeat "time interval.The default value is 600 seconds.
Detection Times	Detect VPN tunnel "heartbeat "count. The default value is 3.
Encrypted	Provide encryption for VPN tunnels.The default is enabled.
Encryption Method	Specify tunnel encryption type.
Compression	Provide compression types for data.
Compression Method	Specify compression method.

8.3. OpenVPN Service

Choose the menu **VPN Server > OpenVPN Service** to load the following page.

Basic Config

OpenVPN Service Enable Disable

IP Pool

Netmask ▼

State **Stopped**
To start the service, you need to create a certificate first in advance configuration

Parameter	Describe
OpenVPN Server	Enable or disable this rule.
IP Pool	IP pool assigned for VPN clients.
Netmask	Specify IP subnet range.

Then click on the **advanced** button to load the following page.

Server Port

Tunnel Proto

Tunnel Dev

Authentication Method

Compress

Tunnel SSL

Static Key

CA

Server Crt

Server Key

Push Route

<input type="checkbox"/>	IP Address	Netmask
No data available		

Client Subnet

<input type="checkbox"/>	Client Name	IP Address	Netmask
No data available			

Parameter	Describe
Server Port	Specify UDP port number.
Tunnel Proto	Specify Tunnel protocol.
Tunnel Dev	Support TAP and TUN mode, TAP is similar to bridge mode, TUN is similar to routing mode, and the selection of client and server should be consistent.

Authentication Method	TLS_AUTH and TLA_CRYPY are supported. Make sure the server and client choose the same.
Compress	A data compression algorithm that supports LZO and LZ4 modes. Make sure the server and client choose the same.
Tunnel SSL	Specify the encryption algorithm type. Make sure the server and client choose the same.
Static Key	Gateway-generated or third-party certificate source. You can jump to the following page to generate a certificate System>CA Configuration Page
CA	
Server Crt	
Server Key	
Push Route	Allow the server-side to push routes to the client-side, enabling the client side subnet to access the service side subnet.
Client Subnet	Add a client-side subnet to the server-side, enabling server-side subnet access to the client-side subnet.
EXPORT CLIENT CONFIG	If the computer is running Open VPN software, download the configuration with one click and directly import the file, then achieve remote connection.

9. Hotspot

9.1. Service Zone

Choose the menu **HotSpot > Service Zone** to load the following page.

Global Configure of Authentication

HTTPS Redirect Enable Disable
 Global Configure of Authentication MAC-Based Auth IP-Based Auth IP+MAC-Based Auth

CONFIRM

Auth Service Zone

Interface	NO AUTH	Local Portal
lan	<input checked="" type="radio"/>	<input type="radio"/>

Records per page: 5 ▾ 1-1 of 1 < >

Parameter	Describe
HTTPS Redirect	Enable or disable HTTPS redirect.
Global Configure of Authentication	Select HTTPS redirect trigger condition.

In the **Auth Service Zone**, you will be able to select subnets that participate in authentication.

9.2. Local Portal

Choose the menu **HotSpot > Local Portal** to load the following page.

In the **Display configuration** area, follow the prompts to set the text and image for the log in page.

Display configuration

Welcome	<input type="text" value="Welcome, Guest"/>
Contact information	<input type="text" value="Contact Phone:13800010001"/>
Copyright information	<input type="text" value="All Right Reserved"/>
Login Button Prompt	<input type="text" value="Login"/>
Help Button Prompt	<input type="text" value="Recharge"/>
Images	<input type="text" value="0 (0.0 B)"/> + <small>Picture size not exceeding 200K, names should not contain special characters such as spaces Size: 960*640 px</small>

In the **Authentication Configuration** area, you will be able to set the authentication type.

Authentication Configuration

Authentication Method	<input type="text" value="Local User Auth"/> ▾
Custom Portal	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Self Service Portal	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Self Service Portal Tips:	<input type="text" value="Self-Service"/> <small>Tip: The local self-service Portal path is /user</small>
Redirect Url after Athh success	<input type="text" value="http://www.example.com"/> <small>Url, for example: http://www.example.com/</small>
Auth Validity Time	<input type="radio"/> Minutes <input checked="" type="radio"/> Hours <input type="radio"/> Days <input type="text" value="2"/> <small>No more than 30 days</small>
Flow detection Interval	<input type="text" value="30 Minutes"/> ▾ <small>Users will be offline automatically if there is no traffic in the set time</small>

Parameter	Describe
Authentication Method	Select the authentication type from the dropdown option.
Custom Portal	Upload the designed login page file.
Self Service Portal	Enable it and the recharge button will appear on the login page.
Self Service Portal Tips	Enter a prompt and it will display the self-service login page.
Redirect Url after Auth success	Redirected address after successful authentication.
Auth Validity Time	Authentication is required after the preset time.
Flow detection Interval	Users will be offline automatically if there is no traffic in the set tim

9.3. Biling Plan

The billing plan prepares for user authentication and implements batch restrictions on the traffic of locally authenticated users.

Choose the menu **HotSpot** > **Billing Plan** and click **ADD** to load the following page.

Plan Name	<input type="text" value="Default"/>
Total Flow(MB)	<input type="text" value="0"/>
	<small>0 mean No Limit</small>
Unit	<input type="radio"/> Minute <input type="radio"/> Hour <input checked="" type="radio"/> Day <input type="radio"/> Month
Available Time	<input type="text" value="0"/>
	<small>0 means No Limit</small>
Upload Speed(Kbps)	<input type="text" value="2000"/>
Download Speed(Kbps)	<input type="text" value="2000"/>
Self Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<input type="button" value="CONFIRM"/> <input type="button" value="CANCEL"/>	

Parameter	Describe
Plan Name	Specify a name for easy identification.
Total Flow(MB)	Specify the total traffic of the plan. If used up within the designated time, authenticated users will be taken offline.
Unit	Limit the usage time of traffic for this plan.
Available Time	Enter time value.
Upload Speed(Kbps)	Specify upload speed for this plan.
Download Speed(Kbps)	Specify the download speed for this plan.
Self Service	Used in conjunction with the Self Service Portal function, users can choose a billing plan on the page.

9.4. Local Users

You can create users and passwords in advance to provide user and password services for local authentication.

Choose the menu **HotSpot** > **Local Users** and click **ADD** to load the following page.

Username

Password

Amount of Concurrency
Note: At the same time, how many users using same account can login, default to 1, 0 means no

SMS Notification Enable Disable
Note: When selected, the account information will be sent to the user

Remarks

Available Authentication Method PPTP L2TP PPPoE Webportal

Peer subnet
Network subnet like 192.168.1.0/24, separate multiple items by space

Plan Select

Total Flow(MB)

Used Flow(MB)

Upload Speed(Kbps)

Download Speed(Kbps)

Due Time Long-term

Parameter	Describe
Username	Specify a user name.
Password	Specify password for user name.
Amount of Concurrency	Limit the number of times an account can be used.
SMS Notification	After docking with the SMS authentication service, enable it to accept SMS verification codes.
Remarks	Enter a name for easy identification.
Available Authentication Method	Specify the type of authentication.
Peer subnet	Combined with VPN authentication, input the remote intranet IP or subnet.

Plan Select	Select an account to create a billing plan.
Total Flow(MB)	Specify the total traffic of the account.
Used Flow(MB)	The amount of traffic used by the account.
Upload Speed(Kbps)	Specify upload speed for the account.
Download Speed(Kbps)	Specify download speed for the account.
Due Time	Specify the validity period of the account

9.5. Vouchers

With Voucher configured, you can distribute the vouchers automatically generated by the AC to the clients. Clients can use the vouchers to access the network.

Choose the menu **HotSpot > Vouchers** and click **BATCHADD** to load the following page.

Code length	<input type="text" value="6"/>
Amount	<input type="text" value="10"/>
Amount of Concurrency	<input type="text" value="1"/>
	<small>Note: At the same time, how many users using same account can login, default to 1, 0 means no limit</small>
Remarks	<input type="text" value="Input Remarks"/>
Upload Speed(Kbps)	<input type="text" value="10000"/>
Download Speed(Kbps)	<input type="text" value="100000"/>
Available Time	<input type="text" value="1 Day"/>
Unit	<input type="radio"/> Minutes <input type="radio"/> Hours <input checked="" type="radio"/> Day <input type="radio"/> Month
	<input type="button" value="CONFIRM"/> <input type="button" value="CANCEL"/>

Parameter	Describe
Code length	Select Code Length.
Amount	Enter the number of Vouchers.
Amount of Concurrency	Enter the number of concurrent users using Vouchers.

Remarks	Specify a name for easy identification.
Upload Speed(Kbps)	Specify upload speed for the vouchers.
Download Speed(Kbps)	Specify download speed for the vouchers.
Available Time	Specify the validity period of the vouchers.
Unit	Valid Unit of time for Vouchers.

9.6. PPPoE Server

Choose the menu **HotSpot** > **PPPoE Server** and click BATCHADD to load the following page.

Basic Config

PPPoE Server Enable Disable

PPPoE Server IP

PPPoE Server Subnet Mask

Peer DNS

Secondary DNS

PPPoE Service Name

Allow Any Service Name Enable Disable

PPPoE Only Enable Disable

Service Binding Interface lan

State Stopped

Parameter	Describe
PPPoE Server	Enable or disable PPPoE Server.
PPPoE Server IP	Specify the IP address for the PPPoE server.
PPPoE Server Subnet Mask	Specify subnet mask for PPPoE Server.

Peer DNS	Specify Peer DNS for PPPoE Server.
Secondary DNS	Specify Secondary DNS for PPPoE Server.
PPPoE Service Name	Customize the name for the PPPoE server.Run multiple PPPoE servers in the internal network and distinguish different PPPoE servers by name.
Allow Any Service Name	If you select Enable, do not check the PPPoE server name for the PPPoE client identification.
PPPoE Only	This subnet can only be used for PPPoE servers.
Service Binding Interface	Specify the line on which the PPPoE server runs.

Then click on the **advanced** button to load the following page.

Advanced ^

Auth Required Enable Disable
if disabled, user can dial ok using any username and password

Authentication Method Local User Auth RADIUS Auth

Auth Protocol pap chap mschap mschap-v2

MTU

MRU

Detection Interval Minutes

Detection Times time

Encrypted Enable Disable

Encryption Method Refuse 40bit-mppe Refuse 56bit-mppe Stateless

Compression Enable Disable

CONFIRM

Parameter	Describe
Auth Required	if disabled, user can dial ok using any username and password.
Authentication	Local User Auth: Create an account locally.

Method	RADIUS Auth: Create an account on radius.
Auth Protocol	Specify authentication protocol.
MTU	Maximum Transmission Unit.You can keep the default value for this setting.
MRU	Maximum Receive Unit.You can keep the default value for this setting.
Detection Interval	Detect PPP link "heartbeat "time interval.The default value is 600 seconds.
Detection Times	Detect PPP link "heartbeat "count. The default value is 3.
Encrypted	Provide encryption for PPP link.The default is enabled.
Encryption Method	Specify tunnel encryption type.
Compression	Provide compression types for data.
Compression Method	Specify compression method.

9.7. RADIUS Server

Choose the menu **HotSpot > RADIUS Server** to load the following page.

RADIUS Server Domain
e.g, 192.168.9.250 or www.example.com

Pre-Shared Key
Pre-Shared Key used to communicate with RADIUS server

Account Port
e.g, 1813

Auth Port
e.g, 1812

NAS Identifier
IP or NAS Token

Bind IP
IP used to communicate with RADIUS Server

Flow detection Interval
Users will be offline automatically if there is no traffic in the set time

Connection Status Connection Failed

Parameter	Describe
RADIUS Server Domain	Enter the domain name or IP address of the RADIUS server.
Pre-Shared Key	Enter the password you have set on the RADIUS server.
Account Port	Enter the port number you have set on the RADIUS server.
Auth Port	Enter the port number of the accounting server. The default port number is 1812.
NAS Identifier	Enter NAS Identifier. (IP or NAS Token)
Bind IP	Enter Bind IP (optional) * IP used to communicate with RADIUS Server.
Connection Status	Show connection status.

9.8. SMS Gateway

Clients can get verification codes using their mobile phones and enter the received codes to pass the authentication

Choose the menu **HotSpot > PPPoE Server** to load the following page.

SMS-Gateway Clickatell AliDaYu ihuyi

AppKey(Access Key ID)

Password(Access Key Secret)

SMS Signature

SMS Template CODE for Account Creating

SMS Template CODE for Notice

SMS Template CODE for Verification

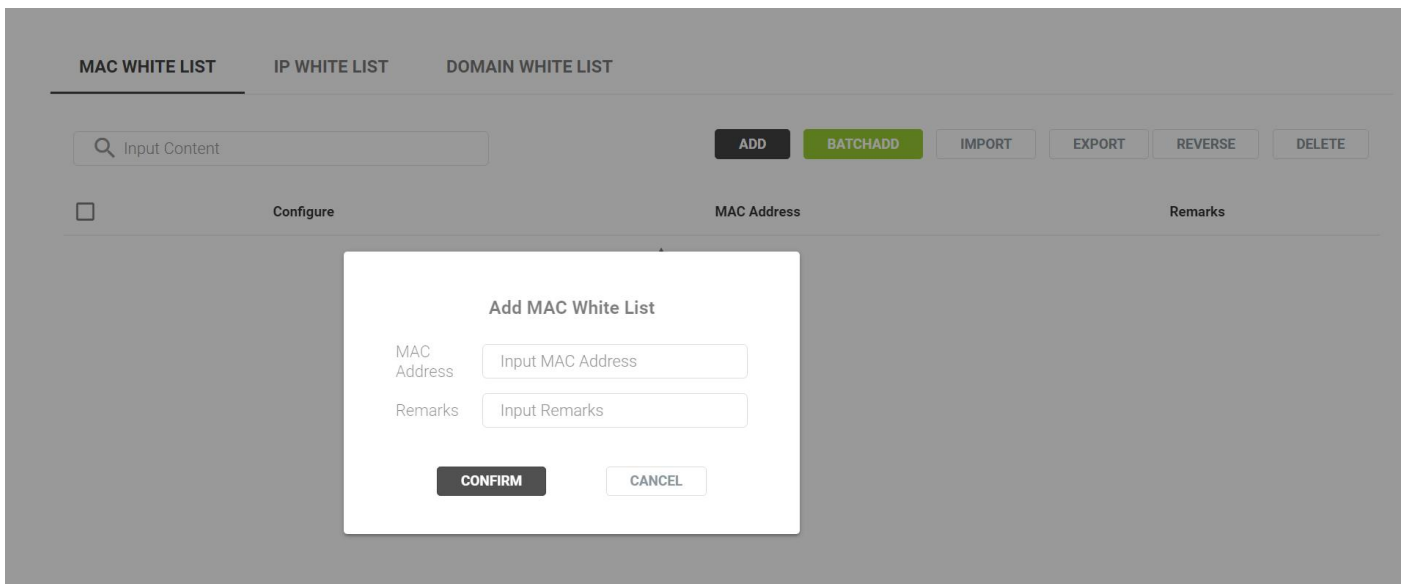
CONFIRM

Parameter	Describe
SMS -Gateway	Select the specified SMS gateway.
App Key	The specified Access Key ID obtained from the SMS gateway.
Password	Get the specified password from the SMS gateway.
SMS Signature	Input SMS Signature.
SMS Template CODE for Account Creating	Input SMS Template CODE for Account Creating.
SMS Template CODE for Notice	Input SMS Template CODE for Notice.
SMS Template CODE for Verification	Input SMS Template CODE for Verification.

9.9. White List

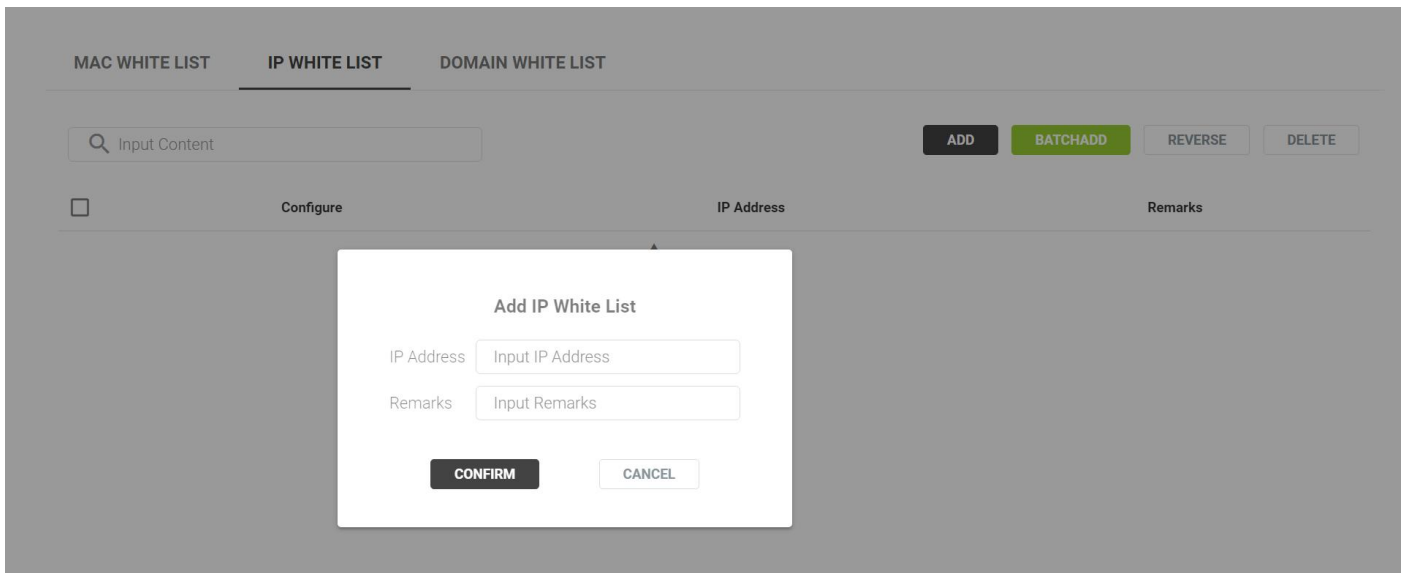
MAC whitelist allows only MAC in the list to access the network.

Choose the menu **HotSpot** > **White List** > **MAC WHITE LIST** and click **ADD** to load the following page.



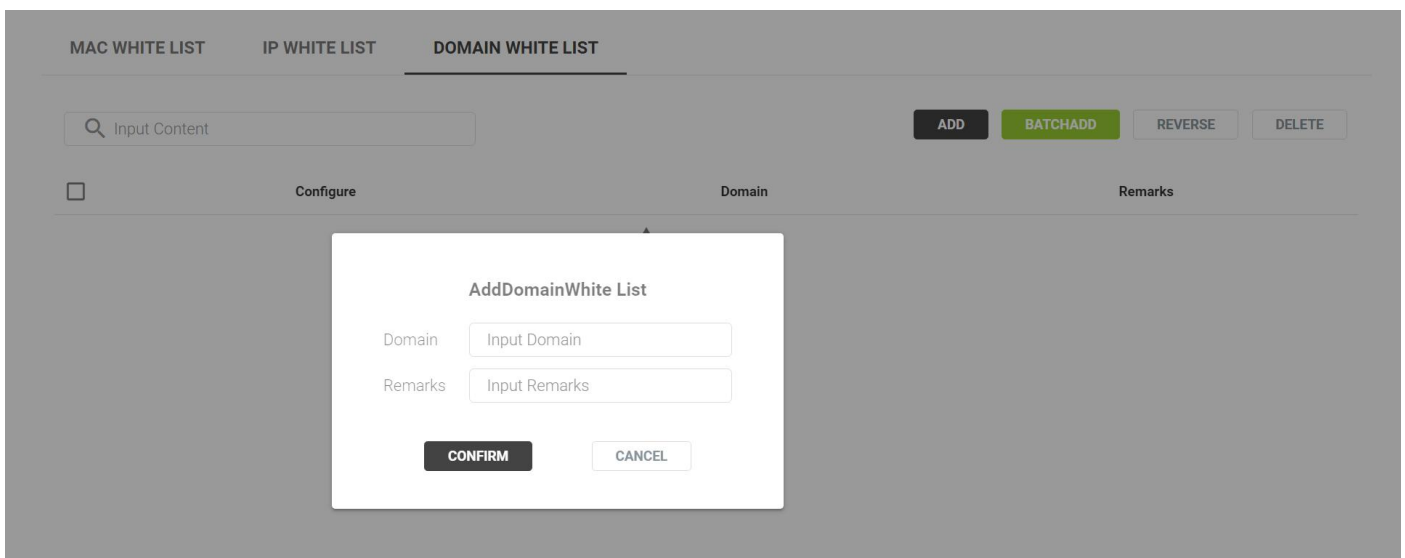
IP whitelist allows only IP in the list to access the network.

Choose the menu **HotSpot** > **White List** > **IP WHITE LIST** and click **ADD** to load the following page.



Domain whitelist Only allow access to domain names within the list.

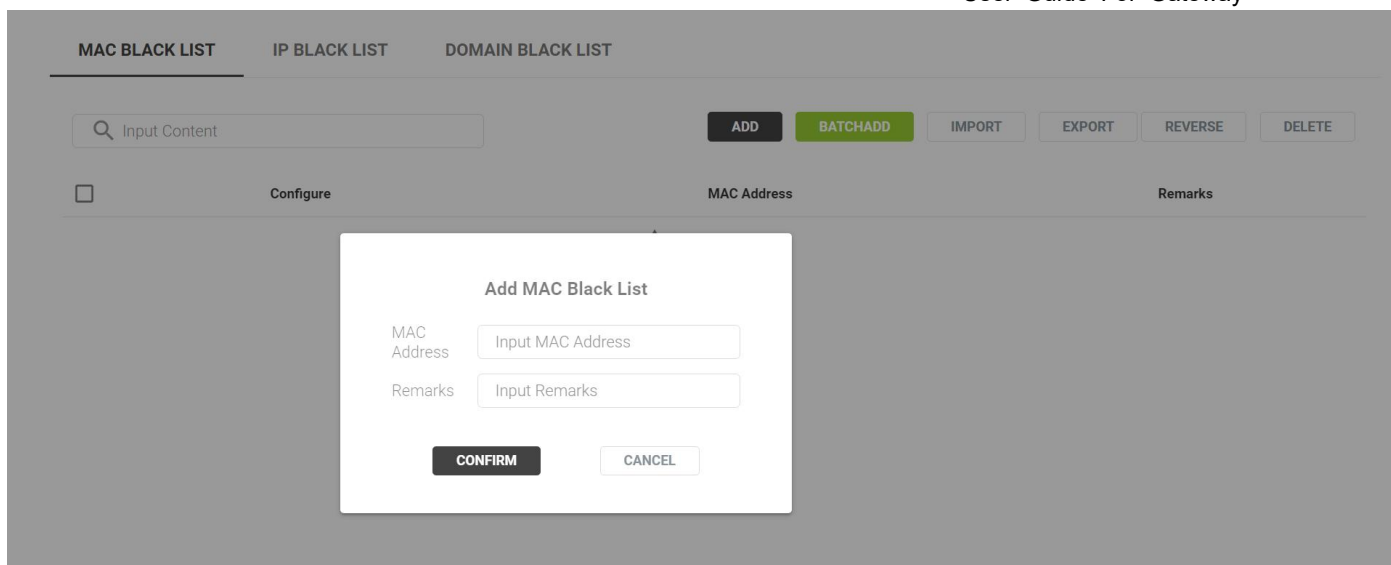
Choose the menu **HotSpot > White List > DAMAIN WHITE LIST** and click **ADD** to load the following page.



9.10. Black List

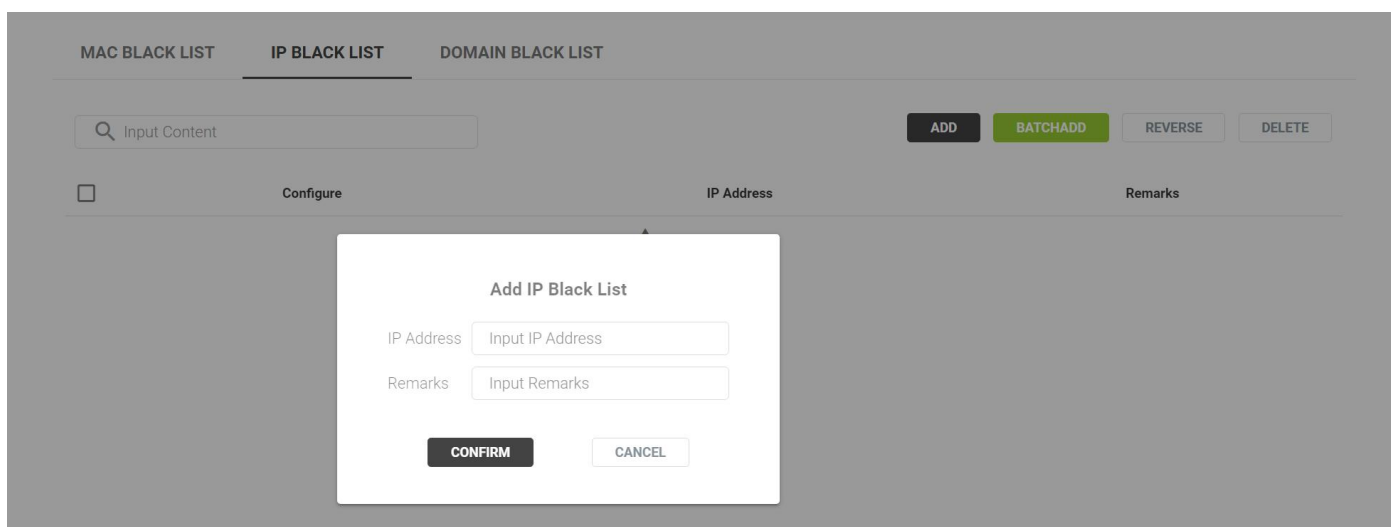
Based on the MAC blacklist, except for the MAC addresses in the list, other MAC addresses can access the network.

Choose the menu **HotSpot > Black List > MAC BLACK LIST** and click **ADD** to load the following page.



Based on the IP blacklist, except for the IP addresses in the list, other IP addresses can access the network.

Choose the menu **HotSpot** > **Black List** > **IP BLACK LIST** and click **ADD** to load the following page.



Block intranet devices from accessing domain names in the list.

Choose the menu **HotSpot** > **Black List** > **DOMAIN BLACK LIST** and click **ADD** to load the following page.

Auto Rest Time	If the Portal notification is unsuccessful within the specified time, the expiration notification of the corresponding user will automatically stop.
Notice Port	Specify the port number for this service.
Notice Content	Specify oneself to edit the notification content.

9.12. Local Notice

When the computer dials up and connects to the PPPoE server, the user opens a browser to access the internet, and a notification page will pop up. If the user does not take any action to access the browser, there will be no pop-up notification when accessing the browser after 10 minutes. The reset time can be manually set.

Local Announcement Enable Disable

Enabled Interface lan

Announcement Content

B *I* ~~S~~ U ↓ ↑ —
¶ Paragraph ▾
¶ 字体大小 ▾
A Default Font ▾
✕
”
≡
≡
≡
≡

CONFIRM

Parameter	Describe
Local Announcement	Enable or disable this feature.
Enabled Interface	Choose which subnet to apply notifications to.
Announcement Content	Edit announcement text.

10. Wireless

10.1. Overview

Choose the menu **Wireless** > **Overview** to load the following page.

Global Config

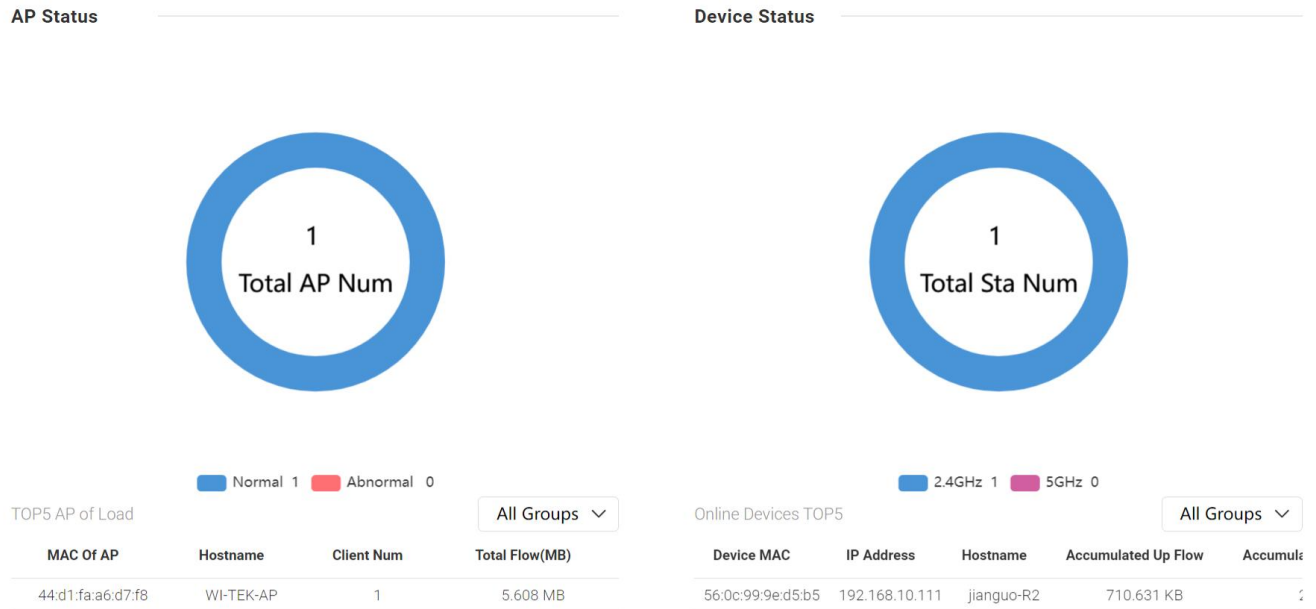
Access Controller Enable Disable
 Distribute AC Address Disabled Using LAN IP Custom AC Address
When Enable, use DHCP option 43 to distribute the AC address
 AC-AP Time Sync Enable Disable
 AP Auto Upgrade Enable Disable
 AP Scheduled Reboot Enable Disable
The device will not restart again if it runs for less than one hour
 AC Scheduled Reboot Enable Disable
The device will not restart again if it runs for less than one hour
 Wireless Optimization Enable Disable
 AP Watchdog Enable Disable
 Country For All AP

Parameter	Describe
Access Controller	Enabled by default, If this option is disabled, the Access Controller function will be turned off.
AC-AP Time Sync	Select time type.
AP Scheduled Reboot	Disabled by default, If this option is enabled, you can periodically reboot all APs in the network as needed.
AC Scheduled Reboot	Disabled by default, If this option is enabled, you can periodically reboot AC in the network as needed.
Wireless Optimization	Disabled by default, If this option is disabled, the wireless Optimization function will be turned off. Note: Using this function, when all the channels of the AP are set to be automatic, when there is no client connected to the AP, the AC will automatically optimize the channel.
AP Watchdog	Disabled by default, If this option is enabled, when the Address Do not Alive, AP will Open Rescue Network Automatically (SSID: RESCUE_99_XXXX, Password: 99999999)

Country For All AP

Select the corresponding country from the drop-down menu.

You can view the current AP status and device status.



10.2. AP Group

The wireless parameters of APs can be synchronized in batches through AP groups. An AP can belong to one AP group at a time.

Choose the menu **Wireless > AP Group** to load the following page.

	Configure	Group Name	AP Num	WxApp Support
<input type="checkbox"/>	Edit	default	0	Disable

Records per page: 20 ▾ 1-1 of 1 < >

Click **Add** an AP group and click the **Edit** button in the **Wireless > AP Group** table to display this page.

Group Name

2.4GHz 5GHz Other Configuration

Wireless Template Configuration

[Add](#)

1

SSID

Encryption

Advance Features Isolate Hidden

MAX Num of User

AuthType

VLAN BINDING [Delete](#)

Advanced

Channel

Roaming Threshold

U-APSD Enable
U-APSD is a new energy-saving processing mode, which can enhance the terminal energy-saving capacity. However, due to the problems in supporting U-APSD functions in some terminals, it is necessary to turn off U-APSD functions in this case.

FILS Support Enable
Support 802.11ai, fast initial link setup, Reduce the waiting time for networking to less than 100 ms

802.11kvr Roaming Enable
Enable Fast Roaming between access points in the group. Note that it is only valid in encrypted cases

RTS Threshold
Resolve wireless data conflicts. When the data length exceeds this value, the wireless access point needs to send the RTS signal to the station, then receive the feedback from the station, before sending the data

Signal

Channel Bandwidth

5GHz First Enable
Note: When the Configuration of 2.4GHz and 5GHz is the same, WiFi User will preferentially connect to 5GHz WiFi

WMM Enable

GBK SSID Enable
Enable GBK can solve the problem that some station (computers, etc.) do not display wireless ssid property

WhiteBlack List

CONFIRM GO BACK

Parameter	Describe
Group Name	Specify a name for the group.
SSID	Enter an SSID name contains up to 32 characters.

	Note: A maximum of 8 SSID profiles can be created in each AP group.
Encryption	Select the security mode of the wireless network WPA-Enterprise / WPA2-Enterprise
KEY	Enter the password for the SSID.
Advance Features	Isolate: Check this option box, wireless clients connected to the same SSID cannot access each other. Hidden: Check this option box, the AP will not broadcast the SSID and wireless clients will not be able to scan and search for the SSID.
MAX Num of User	Number of users connected to this SSID.
AuthType	It is associated with authentication. The default is none.
VLAN BINDING	Enter a VLAN ID for the wireless VLAN. Wireless networks with the same VLAN ID are grouped to a VLAN.
delete	Delete wireless parameter profile.

Advanced

Channel	Automatic by default,you can manually specify the channel. The range of available channels is determined by the radio mode and the country setting. If you select Auto for the channel setting, the AP scans available channels and selects a channel where the least amount of traffic is detected.
Roaming Threshold	minimum signal level required for a client to remain connected.
U-APSD	Enabled by default, U-APSD is a new energy-saving processing mode, which can enhance the terminal energy-saving capacity. However, due to the problems in supporting U-APSD functions in some terminals, it is necessary to turn off U-APSD functions in this case.
FILS Support	Enabled by default, supports 802.11ai, fast initial link setup, Reduce the waiting time for networking to less than 100 ms
802.11kvr Roaming	Enable Fast Roaming between access points in the group. Note that it is only valid in encrypted cases.

RTS Threshold	Resolve wireless data conflicts. When the data length exceeds this value, the wireless access point needs to send the RTS signal to the station, then receive the feedback from the station, before sending the data
Signal	Select the corresponding value according to the actual transmit power of the AP.
Channel Bandwidth	Select the wireless channel bandwidth.
5GHz First	Enabled by default, when the Configuration of 2.4GHz and 5GHz is the same, Wi-Fi User will preferentially connect to 5GHz Wi-Fi.
WMM	Enabled by default, the AP maintains the priority of audio and video packets for better media performance.
GBK SSID	Enable GBK can solve the problem that some station (computers, etc.) do not display wireless ssid property
WhiteBlack List	Select the created black/white list from the drop-down menu.

You can set the radio in the AP group to run at a specified time.


Choose the menu **Wireless > AP Group > Other Configuration** to load the following page.


2.4GHz 5GHz **Other Configuration**

Basic Configuration

WiFi Schedule Enable

Repeat Monday Tuesday Wednesday
 Thursday Friday Saturday
 Sunday

Start Time 

Stop Time 

10.3. AP List

Display Cloud AP from AC discovery to Wi Tek here.

Choose the menu **Wireless > AP List** to load the following page. By default, devices are displayed in a spread out form OVERVIEW.

AUTO REFRESH STOPPED
OVERVIEW
REVERSE
RESTART AP
BIND
UNBIND
NETWORK CONFIG
SET TXPOWER
SET CHANNEL
SET BANDWIDTH

SET AC ADDRESS
EXPORT AP INFO
UPGRADE
SYNC LOGIN PASSWORD
REFRESH

<input type="checkbox"/>	Model	Online State	Device Name	IP Protocol	Manager	Apmode	IP Address	MAC Address	Uptime	AP Group	Last Updated
<input type="checkbox"/>	Wi-AP217-Lite	Online	AP217-Lite	dhcp	Local Admin	FIT_AP	192.168.25.132	54:3d:92:02:41:fa	1Day 2h48m	default	2022-9-28 17:07
<input type="checkbox"/>	Wi-AP217	Online	AP217	dhcp	Local Admin	FIT_AP	192.168.25.137	44:d1:fa:c5:40:35	1Day 2h47m	default	2022-9-28 17:07

Records per page: 20 ▾ 1-2 of 2 < >

Tips:

Any AP that is assigned to a group can be configured independently. These settings will take a higher priority over the group settings.
 Any Batch configuration will override any other configuration on ALL selected APs
 Unbinding any APs will remove any independent configurations from them.

Parameter	Describe
AUTO REFRESHING	Click to automatically refresh the AP list.
REVERSE	Select all APs and click REVERSE to quickly deselect AP.
RESTART AP	Select an AP and click it to restart the AP.
BIND	Select the AP and bind it to the specified AP group.
UNBIND	Select the AP to unbind it from the AP group.
NETWORK CONFIG	Select AP to set IP address
SET TXPOWER	Select AP to set TX power.
SET CHANNEL	Select AP to set bandwidth.
SET BANDWIDTH	Select AP to set bandwidth.
SET AC ADDRESS	Select AP to manually set AC address for AP.
EXPORT AP INFO	Select AP to export AP information
UPGRADE	Select AP to upgrade the firmware. * It needs to be matched with 6.6 Firmware
SYNC LOGIN PASSWORD	Select AP and click it to synchronize the same password as AC
REFRESH	Click it to refresh the AP list.

OVERVIEW: Display the most basic parameters of AP.

<input type="checkbox"/>	Model	Online State	Device Name	IP Protocol	Manager	Apmode	IP Address	MAC Address	Uptime	AP Group	Last Updated
<input type="checkbox"/>	Wi-AP317	Offline	AP317	dhcp	Local Admin	FIT_AP	192.168.25.184	44:d1:fa:a3:7d:c9	1Day 1h17m	-	2022-9-29 11:30
<input type="checkbox"/>	Wi-AP217-Lite	Online	AP217-Lite	dhcp	Local Admin	FIT_AP	192.168.25.132	54:3d:92:02:41:fa	0Day 2h16m	-	2022-9-29 11:30
<input type="checkbox"/>	Wi-AP217	Online	AP217	dhcp	Local Admin	FIT_AP	192.168.25.137	44:d1:fa:c5:40:35	0Day 2h17m	default	2022-9-29 11:30

Records per page: 20 1-3 of 3 < >

WiFi VIEW: Display parameters related to wireless.

<input type="checkbox"/>	Model	Online State	AP Group	WiFi User	Channel	Txpower	Upload Flow	Download Flow	Device Name	MAC Address
<input type="checkbox"/>	Wi-AP317	Offline	-	0/ 1	9/ 56	26/ 26	33.851 MB	290.285 MB	AP317	44:d1:fa:a3:7d:c9
<input type="checkbox"/>	Wi-AP217-Lite	Online	-	0/ 1	1/ 44	23/ 26	885.517 MB	2.138 GB	AP217-Lite	54:3d:92:02:41:fa
<input type="checkbox"/>	Wi-AP217	Online	default	0/ 0	2/ 40	24/ 23	874.167 KB	10.092 MB	AP217	44:d1:fa:c5:40:35

Records per page: 20 1-3 of 3 < >

DETAILS VIEW: Display the most comprehensive parameters of AP.

<input type="checkbox"/>	Model	Online State	Device Name	SN	IP Protocol	IP Address	MAC Address	Uptime	AP Group	WiFi User	CPU Usage	Channel	Txpower	Upload Flow
<input type="checkbox"/>	Wi-AP317	Offline	AP317	AP317EN2109250003	dhcp	192.168.25.184	44:d1:fa:a3:7d:c9	1Day 1h17m	-	0/ 1	7%	9/ 56	26/ 26	33.851 M
<input type="checkbox"/>	Wi-AP217-Lite	Online	AP217-Lite	AP217L22207EN0303	dhcp	192.168.25.132	54:3d:92:02:41:fa	0Day 2h16m	-	0/ 1	7%	1/ 44	23/ 26	885.517 M
<input type="checkbox"/>	Wi-AP217	Online	AP217	AP217EN2109250082	dhcp	192.168.25.137	44:d1:fa:c5:40:35	0Day 2h17m	default	0/ 0	7%	2/ 40	24/ 23	874.167 K

10.4. RF Planning

The purpose of this function is to assist in the rapid optimization of the wireless channel. Analyze and calculate the busyness of the channel according to the scanning situation, and choose the lower one first. Choose the menu **Wireless > RF Planning** to load the following page.

👁️ 2.4G AP:0 📶 Dual-Band AP:3 🛑 Offline Device:0

INIT CHANNELS START SCAN SAVE RESULT

Configure	SN	Online State	Plan Status	MAC Address	2.4G Channel	5G Channel	2.4G Noise	5G Noise	2.4G Interference	5G Interference
View	AP317EN2109250003	Online	Init Channels OK	44:d1:fa:a3:7d:c9	1	161	-95	-95	-	-
View	AP217L22207EN0303	Online	Init Channels OK	54:3d:92:02:41:fa	1	44	-95	-95	-	-
View	AP217EN2109250082	Online	Init Channels OK	44:d1:fa:c5:40:35	11	48	-95	-95	-	-

Records per page: 20 1-3 of 3 < >

Tips:
 Note: An AP must be bound to a group before it can be managed by the Controller.
 Each AP takes about 5 to 15 seconds to scan, this may cause users to lose connection and go offline.

Parameter	Describe
INIT CHANNELS	Click it to assign channels based on APs within the group.
START SCAN	Click it to automatically scan the Wi-Fi interference sources around the AP.

SAVE RESULT

After scanning, you need to click it to save the result.

Click **View** to view the surrounding Wi-Fi signals.

SSID	MAC Address	Band	Signal	Channel
TP-LINK_5G_D6D6	F4:6D:2F:77:D6:D6	5G	-83	44
ChinaNet-asfZ-5G	30:3F:7B:51:E3:71	5G	-56	161
CPE511-KIT	B0:96:6C:2C:30:91	5G	-75	149
TLF	B0:AC:D2:0B:CF:D1	5G	-78	149
Wi-Tek-FQ	20:76:93:54:23:6C	5G	-60	149
YunZhong-5G	44:D1:FA:B1:A3:05	5G	-82	52
WI-TEK-402	44:D1:FA:B2:62:94	5G	-48	52
AP218_10	44:D1:FA:BC:10:D9	5G	-73	48
	44:D1:FA:C4:A5:93	5G	-83	40
	76:D6:CB:65:02:CF	5G	-69	36
AP717MP	8A:12:4C:B0:1D:72	5G	-68	36
	88:12:4C:B0:1D:72	5G	-69	36
AP717MP	8A:12:4C:B0:14:2A	5G	-20	36
	88:12:4C:B0:14:2A	5G	-20	36
TRF-5G	76:D6:CB:75:02:CF	5G	-69	36
	56:3D:92:01:FE:CE	5G	-71	149
AC50 V2-test	54:3D:92:02:41:FB	5G	-67	60
DIRECT-14-HP Laser 178nw	06:0E:3C:86:53:14	2.4G	-88	6
YunZhong-2.4G	44:D1:FA:B1:A3:04	2.4G	-84	11
	74:D6:CB:95:02:CF	2.4G	-73	13

Records per page: 20 ▼ 1-20 of 30 < >

Note:


- An AP must be bound to a group before it can be managed by the Controller.
- Each AP takes about 5 to 15 seconds to scan, this may cause users to lose connection and go offline.

10.5. WhiteBlack List

White/Black List can be used to allow or block the listed clients to access the network. The reby it can effectively control the client's access to the wireless network.

Whitelist: Only allow wireless clients in the list to connect to Wi-Fi. **Blacklist:** Except for the wireless clients in the blacklist, other wireless clients can connect to Wi-Fi.

Choose **Wireless > White Black List** to load the following page.

	Configure	Name	Strategy	MAC Num
	No data available			

Choose **ADD** to load the following page.

Name

Strategy Black List White List

MAC List


56:f1:c4:eb:cc:a6

Parameter	Describe
Name	Enter any name for easy recognition.
Strategy	Specify policy type for wireless clients.
MAC List	Specify the MAC address of the wireless client.


10.6. Firmware

If AC manages multiple APs, you can use this function when you want to upgrade the APs in batches.

Click **Wireless > Firmware** to load the following page.

<input type="checkbox"/>	Model	Version	Remarks	MD5
 No data available				

Click **ADD** button to upload the firmware file from a local disk.

Model	WI-AP217
Version	v4.3.build20220919-1922-f87d958
Remarks	v4.3.build20220919-1922-f87d958
Firmware	1 (10.4 MB) + ^ <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;">  WiTek-v4.3.build20220919-1922-f87d958-ar71xx-generic-A782-squashfs-sysupgrade.web.bin 0% X </div> <div style="margin-top: 10px; text-align: center;"> CONFIRM CANCEL </div>

Upload succeeded.

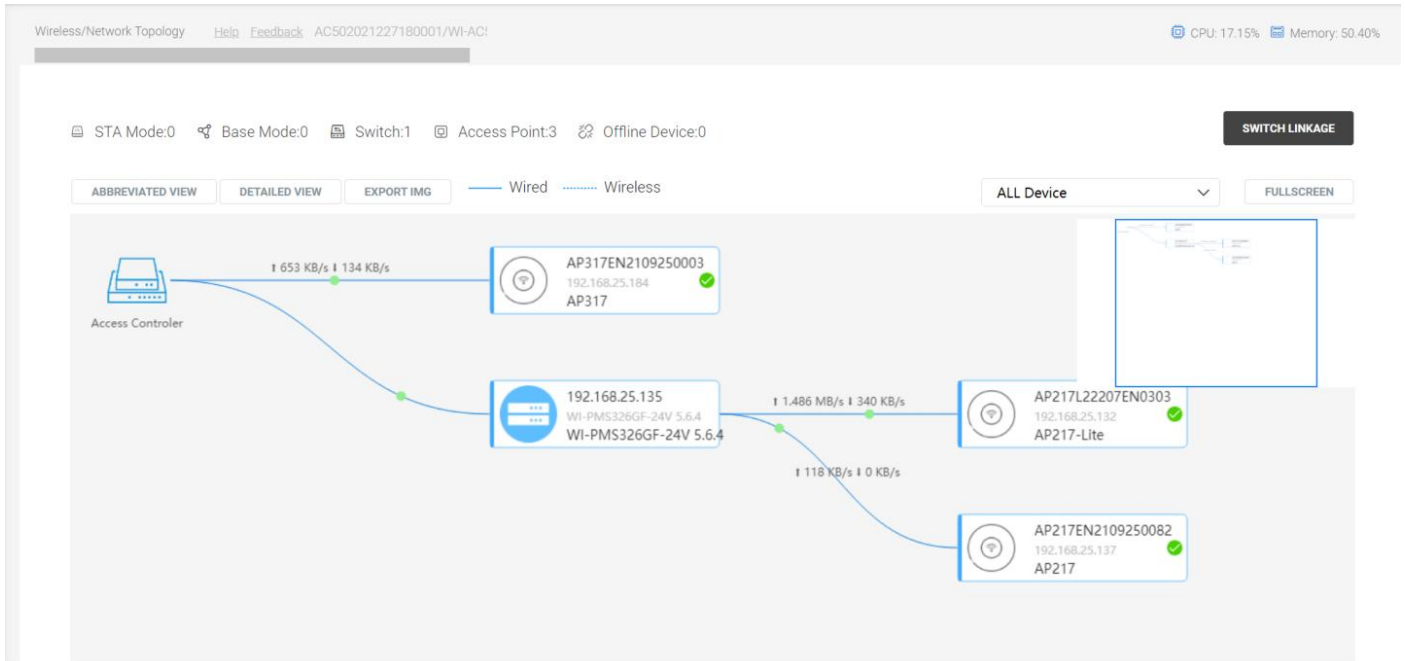
<input type="checkbox"/>	Model	Version	Remarks	MD5
<input type="checkbox"/>	WI-AP217	v4.3.build20220919-1922-f87d958	v4.3.build20220919-1922-f87d958	c3710fa62798eb7417fe637c7f1c08e3

Records per page: 20 1-1 of 1 < >

Then go back to the **AP group** option, select the check box to access the point group from the list, and click Upgrade.

10.7. Network Topology

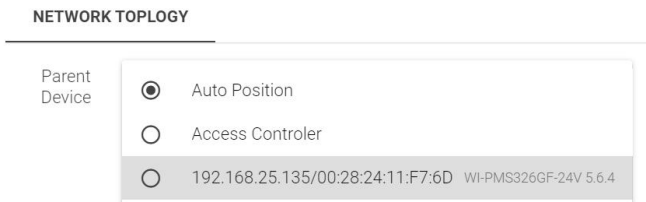
With this feature, if you have AP and Switch deployed in your network, you will be able to see a visual view of the topology of all supported devices in the network. Click **Wireless > Network Topology** to load the following page..



Parameter	Describe
ABBREVIATED VIEW	Click it to display only the devices managed by AC.
DETAILED VIEW	Click it to display which AP is connected to the wireless client
EXPORT IMG	Click it to export the topology map as an image

Note: Only supports simple topology display.

If you click the AP on the topology diagram, the following interface will pop up, and manually adjust the uplink device of the AP.



11. CPE Management

11.1. CPE Global Configuration

Using this function, once the wireless CPE is managed by AC50, the following configuration information will be automatically synchronized.

Click **CPE Management > CPE Global Configuration** to load the following page.

Global Config

- CPE Scheduled Reboot Enable Disable
- Wireless Optimization Enable Disable
- Transport Scenario Common Scenario Elevator Scenario PTP Scenario Roaming Scenario
 Custom Scenario

CONFIRM

Select Roaming Scenario option, and the following content pops up.

RTS/CTS Threshold

Min Sta Signal(dBm)

Distance(KM) ▼

Parameter	Describe
CPE Scheduled Reboot	Disabled by default,If this option is enabled, you can periodically reboot all CPE in the network as needed.
Wireless Optimization	Enable by default, it automatically optimize wireless CPE.
Transport Scenario	Select the scenario according to the actual application. You can choose to have 4 built-in Scenarios or customize parameters.
RTS/CTS Threshold	Keep the default value: 2347.
Ms Sta Signal(dBm)	Number of minimum received and transmitted signals between CPEs.
Distance(KM)	Select the corresponding value according to the actual transmission distance of the CPE.

11.2. CPE List

Using this function, multiple groups of CPEs in the network can be centralized.

For the explanation of CPE List parameters, refer to 6.3 AP List. Click **CPE Management > CPE List** to load the following page.

Input Content

AUTO REFRESH STOPPED OVERVIEW REVERSE SET CHANNEL SET TXPOWER RESTART CPE DELETE CPE EXPORT CPE INFO

SYNC LOGIN PASSWORD REFRESH

<input type="checkbox"/>	Model	Mode	Group	Online State	Device Name	IP Address	MAC Address	Uptime
<input type="checkbox"/>	WI-CPE513P-KIT	Base Mode	Group 1	Online	WI-TEK-CPE	192.168.25.220	44:d1:fa:c4:b2:e6	0Day 0h20m
<input type="checkbox"/>	WI-CPE513P-KIT	STA Mode	Group 1	Online	WI-TEK-CPE	192.168.25.140	44:d1:fa:c4:af:5f	0Day 0h14m

Records per page: 20 1-2 of 2

Tips:
 Devices with different country codes can not configure channels at the same time. Devices with different working frequency bands can not configure channels at the same time
 CPE Configurations will be applied immediately, and will not be saved in AC device after applying.

Note:

- Only available for CPE that supports cloud management.
- Devices with different country codes can not configure channels at the same time.
- Devices with different working frequency bands can not configure channels at the same time.
- CPE Configurations will be applied immediately, and will not be saved in AC device after applying.

11.3. Unified Cloud

You can bind your device to the cloud platform.

For Cloud1.0: <http://cloud.wireless-tek.com/>

Login the Unified Cloud Control Platform -> Obtain the Binding Code -> Input the Binding Code and Note Name On Device -> Save and complete the binding;

For Cloud2.0: <http://cloud2.wireless-tek.com> (Recommend)

Login the Unified Cloud Control Platform -> Add Group -> Add NetWork --> Add Device -> Input the Serial Number -> Save and complete the binding;

Click **Unified Cloud** to load the following page.

Serial Number	AC105FD00007280004
Binding Code	<input type="text" value="Input Binding Code"/>
Longitude	<input type="text" value="Input Longitude"/>
Latitude	<input type="text" value="Input Latitude"/>
Description	<input type="text" value="NGROUTER"/>

CONFIRM

Parameter	Describe
Serial Number	Applicable to CCloud2.0, copying projects created on cloud platforms with SN added.
Binding Code	Applicable to Cloud1.0, fill in the binding code of the cloud platform account.
Longitude/Latitude	Suitable for Cloud1.0, synchronizing longitude and latitude to the cloud platform.
Description	Enter any name for easy recognition.

11.4. SD-LAN

SD-LAN is a practical application of SDN (Software Defined Network) technology. Wi-Tek launched the SD-LAN intelligent networking scheme, which can quickly establish a dedicated virtual LAN on the Internet, so as to realize one-key interconnection and data interchange between different branch nodes.

For example, the gateways of the headquarters and branch offices are bound to the same cloud account, and remote access to the internal network is achieved through SD-LAN networking.

Click **Unified Cloud > SD-LAN** to load the following page. You can check the SD-LAN link status and latency.

START SD-LAN

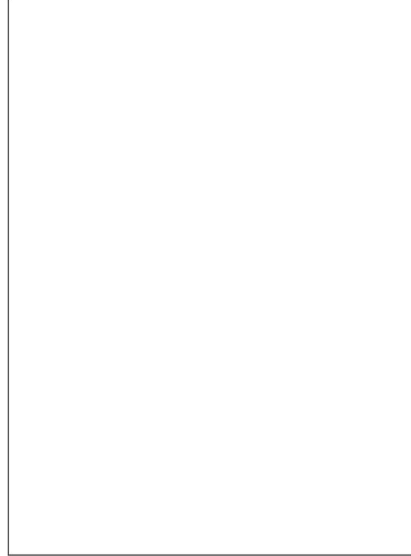
— Line OK - - - - - Line DEAD

SD-LAN Peers Status

■ Current Device ■ Peers Online ■ Peers Offline

● NGROUTER A 30004

Latency Of Peers (Ms)



SubNet List

SN

Model

Hostname

SubNet

⚠ No data available

12. Application

12.1. UPnP Server

With the development of networking and advanced computing techniques, great numbers of devices feature in networks. UPnP is designed to solve the problem of communication between these network devices. UPnP function allows devices dynamically discover and communicate with each other without additional configurations. For example, allows the download of P2P software without opening ports. Click **Application > UPNP Server** to load the following page.

Internal IP Address	Protocol	Internal Port	External Port	Description	Create Time
<div style="display: flex; justify-content: space-between; align-items: center; margin-bottom: 10px;"> <input type="text" value="Input Content"/> <div> <input type="button" value="RESTART SERVICE"/> <input type="button" value="CLEANUP WHEN OFFLINE"/> <input type="button" value="SERVICE CONFIG"/> </div> </div> <div style="text-align: center;"> No data available </div>					

12.2. DDNS

Nowadays, network protocols such as PPPoE and DHCP are widely employed by ISPs to assign public IP addresses to users. The use of these protocols can cause the user's public address to change dynamically. DDNS is an internet service that ensures a fixed domain name can be used to access a network with a varying public IP address. This means the user's network can be more easily accessed by internet hosts. Click **Application > DDNS** to load the following page.

Configure	Status	Service Provider	Domain	Binding Type	Binding Interface/Binding Host MAC	Update Results	IP Address
<div style="display: flex; justify-content: space-between; align-items: center; margin-bottom: 10px;"> <input type="text" value="Input Content"/> <div> <input type="button" value="ADD"/> <input type="button" value="EXPORT"/> <input type="button" value="ENABLE"/> <input type="button" value="STOP"/> <input type="button" value="REVERSE"/> <input type="button" value="DELETE"/> </div> </div> <div style="text-align: center;"> No data available </div>							

Click the **ADD** button to fill in the DDNS entry.

Service Provider

Enable Yes No

Domain *

AppKey(Access Key ID) *

Password *

Protocol IPv4 IPv6

Binding Type Interface MAC Address

Binding Host MAC *

CONFIRM

Parameter	Describe
Service Provider	Select the service providers, including Alibaba DNS, dynv6.com, dyndns.org, Oray.net, 3322.org.
Enable	Enable or disable DNS entries.
Domain	Input Domain
AppKey	Get the secret key from the service provider.
Password	Enter the password from the service provider.
Protocol	Select IPV4 or IPV6.
Binding Type	Select interface or MAC.
Binding Host MAC	Enter the MAC mapping the intranet device.
Binding Interface	Enter the MAC mapping the intranet interface.

12.3. Wake on LAN

Wake-on-LAN (WoL) is an Ethernet or Token ring computer networking standard that allows a computer to be turned on or awakened by a network message. The message is usually sent by a program executed on another computer on the same local area network. It is also possible to initiate the message from another network by using subnet directed broadcasts or a WOL gateway service. Click **Application > Wake on LAN** to load the following page.

Wake Now

MAC Address

WAKE ON LAN

Parameter	Describe
MAC Address	Enter the MAC address, such as 54: AB: 3A: 59:95:69.
WAKE ON LAN	After entering the MAC address, tap it to wake up immediately.

Wake Scheduled

Configure
MAC
Device Status
Cycle
Date
Time
Remarks
Scheduled

 No data available

Click the **ADD** button to add an entry.

MAC

*

Cycle

Once

▼

Date



*

Time



*

Remarks

CONFIRM

CANCEL

Parameter	Describe
MAC	Specify MAC Address
Cycle	Specify cycle (Once / Daily / Weekly / Monthly).
Date	Specify date.
Time	Specify time range.
Remarks	Specify input comments.

12.4. Switch Linkage

Use this function to manage switches that support the SNMP protocol through the AC, and only support reading simple port information. Click **Application > Switch Linkage** to load the following page.

Input Content

QUICK-SCAN SWITCHES ADD EXPORT REVERSE DELETE REFRESH

	Configure	Status	Proxy Access	Description	Model	Hostname	MAC Address	Switch Address	PoE Max Power(W)	PoE Allocated Power(mW)	
<input type="checkbox"/>	Edit View/Configure	Online	Click View	PoE Switch	WI-PMS326GF-24V 5.6.4	WI-PMS326GF-24V 5.6.4	00:28:24:11:F7:6D	192.168.25.135	-	-	25Days :

Records per page: 20 1-1 of 1 < >

12.5. Smart device

With this feature, the gateway can automatically discover devices with Onvif in the same subnet, such as IP cameras. After the gateway is bound to the cloud 2.0 platform, use the EWEB function to remotely access the web interface. Click **Application > Smart device** to load the following page.

Input Content

SERVICE CONFIG REFRESH

Model	Hostname	IP Address	MAC Address
DS-2CD3386FWDV2-IS	HIKVISION DS-2CD3386FWDV2-IS	192.168.10.106	c0:51:7e:e0:75:da

Records per page: 20 1-1 of 1 < >

13. Security

13.1. Health Monitoring

This section is used in conjunction with the Examination function to set the detection cycle. Click **System > Health Monitoring** to load the following page.

Active Health Monitoring DHCP Server Monitoring PPPoE Server Monitoring IP Monitoring Loop Monitoring







Checking Interval Seconds

CONFIRM

13.2. Examination

This part can locate simple network failures in the intranet. Click **System > Examination** to load the following page.

System Examination Quick Scan Your Network And Device **QUICK SCAN**

<input checked="" type="checkbox"/>  Hard Disk Check	<input checked="" type="checkbox"/>  Memory Check.	<input checked="" type="checkbox"/>  WAN Check	<input checked="" type="checkbox"/>  Internal DHCP Server Detection	<input checked="" type="checkbox"/>  Internal PPPoE Server Detection	<input checked="" type="checkbox"/>  IP Conflict Check
---	---	---	--	---	---

13.3. Email Notice

With this function, when the device has the following 4 states, send an alarm email through the bound mailbox. Click **System > Email Notice** to load the following page.


Event Type

- apwarning apdown apreboot
- securitywarning ipconflict netloop

CONFIRM

Email List

ADD **REVERSE** **DELETE**

<input type="checkbox"/>	Configure	Email	Remarks
 No data available			

13.4. Audit


This part is the URL and IP behavior records for LAN clients to access the Internet. Click **Security > Audit > URL ACCESS RECORDS** to load the following page.

URL ACCESS RECORDS **IP ACCESS RECORDS**

AUDIT CONFIGURATION

EXPORTING REALTIME RECORDS

EXPORTING URL HISTORICAL RECORDS

Time	IP	MAC	Protocol	URL access Records
 No data available				


Click **Security > Audit > IP ACCESS RECORDS** to load the following page.

URL ACCESS RECORDS **IP ACCESS RECORDS**

AUDIT CONFIGURATION

EXPORTING REALTIME RECORDS

EXPORTING IP HISTORICAL RECORDS

Time	Source IP	Dest IP	Protocol	Source port	Dest Port
 No data available					

You can enable URL or IP access records and set the storage of log records. Click **AUDIT CONFIGURATION** to load the following page.

Audit Configuration

URL access Records Enable

IP access Records Enable

Saving Log Configuration

Saving Log Configuration Save Locally
 Save In Server
 Save Disk

CONFIRM

CANCEL

14. System

14.1. System Maintenance

Click **System > System Maintenance** to load the following page.

System Information

Device Name	<input type="text" value="NGROUTER"/> *
Network Mode	<input type="text" value="Gateway Mode"/> ▼
<input type="button" value="CONFIRM"/>	

Tips:

1. Router Work mode: NAT mode and Routing mode
2. NAT mode: "Network Address Translation", which allows a whole organization to appear on the WAN with one public IP address. Namely, the internal private network address will be converted into a legitimate public network IP address
3. Routing mode: All data are not forwarded by NAT, and the intranet IP is transmitted directly to the extranet without Change and Camouflage.

Parameter	Describe
Device Name	Specify a name for gateway.
Network Mode	<p>Network mode: Gateway mode and Router mode.</p> <p>Gateway mode: "Network Address Translation", which allows a whole organization to appear on the WAN with one public IP address. Namely, the internal private network address will be converted into a legitimate public network IP address.</p> <p>Router mode: All data are not forwarded by NAT, and the intranet IP is transmitted directly to the extranet without Change and Camouflage.</p>

Reboot

Uptime	1Days 20Hours 31Minutes 33Seconds
Reboot	<input type="button" value="REBOOT NOW"/>

Parameter	Describe
-----------	----------

Uptime	Display device running time.
Reboot	Click it to reboot the device.

Online Upgrade

Check For New Version

System Version

v5.0.build20230629-1419-c71c5a0

Model

WI-AC105P

Serial Number

AC105P07280004

Parameter	Describe
System Version	Display the firmware version of the device.
Model	Display device model.
Serial Number	Display the SN of the device.

Menu Upgrade

Local Upgrade

0 (0.0 B)



Visit the official website to download the latest version

Parameter	Describe
Local Upgrade	Display the name of the uploaded firmware.
+	Click on it to upload firmware.
	Click on it to upgrade the firmware.

Upload Backup file


Last Backup Time

-

Upload Backup file

0 (0.0 B)



Parameter	Describe
Last Backup Time	Display Last Backup Time.
+	Click on it to upload backup files.
	Click on it to upgrade backup files.

14.2. Remote Access

Click **System > Remote Access** to load the following page.

Access Control

WEB Access	<input checked="" type="checkbox"/> Allow access to Web Management through WAN
HTTPS Support	<input type="checkbox"/> Force to use https when access to Web Management
Allow Ping on WAN	<input checked="" type="checkbox"/> Allow Ping Packet From WAN Port
HTTP Port	<input type="text" value="80"/> *
HTTPS Port	<input type="text" value="443"/> *
HTTP Port For WAN	<input type="text" value="800"/>
HTTPS Port For WAN	<input type="text" value="4430"/>

CONFIRM

Parameter	Describe
WEB Access	Tick box allow access to Web Management through WAN.
HTTPS Support	Tick box force to use https when access to Web Management.
Allow Ping on WAN	Tick box allow Ping packet from WAN port.
HTTP Port	Specify the HTTP port for accessing the web interface through LAN.
HTTPS Port	Specify the HTTPS port for accessing the web interface through LAN.
HTTP Port For WAN	Specify the HTTP port for accessing the web interface through

	the WAN.
HTTPS Port For WAN	Specify the HTTPS port for accessing the web interface through the WAN.

With a third-party log server, device log records can be synchronized to the log server.

Remote Logging System

Log Server

Log Port

Log Protocol

CONFIRM

14.3. User Management

You can use different user account to log in to the AC50. The administration authority varies among different roles. Click **System > User Management** to load the following page.

ADD **ENABLE** **STOP** **DELETE**

<input type="checkbox"/>	Configure	Status	Username	Privilege Group	Allowed IP
<input type="checkbox"/>	Edit	Enable	admin	System administrator	0.0.0.0/0
<input type="checkbox"/>	Edit	Enable	voucher	Voucher administrator	0.0.0.0/0

Records per page: 20 1-2 of 2 < >

Then click **ADD** to load the following page.

Username *

Password

Confirm New Password

Allowed IP
Single address or network (e.g. 172.16.3.2 or 172.16.3.0/24), separate multiple items by space

User Role

Parameter	Describe
-----------	----------

Username	Specify account name.
Password	Assign a password for the account.
Confirm New Password	Confirm password again
Allowed IP	Restrict allowed access to IP addresses
User Role	Select the role type: Voucher administrator and System administrator.

Select the role of **System administrator**, you will be able to select the access rights of functional modules.

User Role

Authorization

Forbidden	Readonly
<input type="checkbox"/> Dashboard	<input type="checkbox"/> Dashboard
▶ <input type="checkbox"/> Network	▶ <input type="checkbox"/> Network
▶ <input type="checkbox"/> Status	▶ <input type="checkbox"/> Status
▶ <input type="checkbox"/> SmartQoS	▶ <input type="checkbox"/> SmartQoS
▶ <input type="checkbox"/> Firewall	▶ <input type="checkbox"/> Firewall
▶ <input type="checkbox"/> VPN Server	▶ <input type="checkbox"/> VPN Server
▶ <input type="checkbox"/> HotSpot	▶ <input type="checkbox"/> HotSpot
▶ <input type="checkbox"/> Wireless	▶ <input type="checkbox"/> Wireless
▶ <input type="checkbox"/> CPE Management	▶ <input type="checkbox"/> CPE Management
▶ <input type="checkbox"/> Unified Cloud	▶ <input type="checkbox"/> Unified Cloud
▶ <input type="checkbox"/> Application	▶ <input type="checkbox"/> Application
▶ <input type="checkbox"/> Security	▶ <input type="checkbox"/> Security
▶ <input type="checkbox"/> System	▶ <input type="checkbox"/> System
▶ <input type="checkbox"/> Logging	▶ <input type="checkbox"/> Logging

14.4. Diagnosis

Ping and traceroute are both used to test the connectivity between two devices in the network. In addition, ping can show the roundtrip time between the two devices directly and traceroute can show the IP address of routers along the route path. Click **System > Diagnosis** to load the following page.

PING

IP or Domain	<input type="text" value="Input IP or Domain,e.g. 192.168.1.1"/>	*
Protocol	<input type="text" value="IPV4"/>	▼
Interface	<input type="text" value="ANY"/>	▼
PING Count	<input type="text" value="4"/>	time
Result	<div style="border: 1px solid #ccc; height: 100px;"></div>	

START TESTING

Tracert

IP or Domain	<input type="text" value="Input IP or Domain,e.g. 192.168.1.1"/>	*
Protocol	<input type="text" value="IPV4"/>	▼
Interface	<input type="text" value="ANY"/>	▼
Result	<div style="border: 1px solid #ccc; height: 100px;"></div>	

START TESTING

14.5. Network Tools

The gateway is equipped with a built-in Telnet tool, making it convenient for administrators to log in remotely. Click **System > Network Tools** to load the following page.

Telnet

Telnet IP	<input type="text" value="Input IP or Domain,e.g. 192.168.1.1"/> *
Telnet Port	<input type="text" value="23"/>

START

14.6. Network Parameters

This displays the settings for TCP and UDP session parameters. If there are no special requirements, please keep the default parameters. Click **System > Network Parameters** to load the following page.

Access Control

MAX Connections of System	100000
MAX Connections Per ip	<input type="text" value="3000"/>
MAX TCP Connections Per IP	<input type="text" value="0"/>
MAX UDP Connections Per IP	<input type="text" value="800"/>

TCP Timeout

GENERIC	<input type="text" value="600"/>
SYNSend	<input type="text" value="120"/>
FINWait	<input type="text" value="120"/>
Close	<input type="text" value="10"/>
LastAck	<input type="text" value="30"/>
ESTABLISHED	<input type="text" value="1800"/>
SYNReceived	<input type="text" value="60"/>
TimeWait	<input type="text" value="120"/>
CloseWait	<input type="text" value="60"/>

UDP Timtout

Unreplied	<input type="text" value="60"/>
Assured	<input type="text" value="180"/>

CONFIRM RESET TO DEFAULT

14.7. System Time

This displays the settings for system time parameters. Click **System > System Time** to load the following page.

System Time	<input type="text" value="2023/07/12 14:43:50"/>	
	Sync System Time	
NTP Service	<input checked="" type="checkbox"/> Enable NTP	
Time Zone	<input type="text" value="Asia/Shanghai"/>	
Time Server 1	<input type="text" value="0.pool.ntp.org"/>	Sync Now
Time Server 2	<input type="text" value="1.pool.ntp.org"/>	Sync Now
Time Server 3	<input type="text" value="2.pool.ntp.org"/>	Sync Now
Time Server 4	<input type="text" value="3.pool.ntp.org"/>	Sync Now

CONFIRM

14.8. CA Configuration

Provide certificates and keys for OpenVPN. Click **System > CA Configuration** to load the following page.

Click the **GET CERT AND KEY** button, and the certificate and key will be automatically generated, and then automatically synchronized to the OpenVPN server.

CA AND Server Crt And Key

Static Key	<pre># # 2048 bit OpenVPN static key # -----BEGIN OpenVPN Static key V1----- c4ff9bc2986c05de2fc1d1045a9564d4 ca8c7567af67614de433c17a61554970</pre>
CA	<pre>-----BEGIN CERTIFICATE----- MIIFEjCCA/qgAwIBAgIJAL61U8I7boitMA0GCSqGSIb3DQEBCwUAMIG2MQswCQYD VQQGEwJUVzELMAkGA1UECBMCQ0ExFTATBgNVBAcTDGFhbnkZyYyYXNjbzEVMmBG A1UEChMMRm9ydC1GdW5zdG9uMR0wGwYDVQQLExRNeU9yZ2FuaXphdGlvbmFsVW5p dDEYMBYGA1UEAxMPRm9ydC1GdW5zdG9uIENBMRAwDgYDVQQPEwdFYXN5UINBMSEw HwYJKoZIhvcNAQkBFhJtZUBteWhvc3QubXlib21haW4wHhcNMjMwNzExMDkzNDIy</pre>
Server Crt	<pre>-----BEGIN CERTIFICATE----- MIIFaTCCBFGgAwIBAgIBATANBgkqhkiG9w0BAQsFADCBTjELMAkGA1UEBhMCVWx CzAJBgNVBAGTAkNBMRUwEwYDVQQHEWxTYW5GcmFuY2lyZ28xFTATBgNVBAoTDEZv cnQtRnVuc3RvbjEdMBSGA1UECxMUTXIPcmdhbmI6YXRpb25hbFVuaXQxGDAWBgNV BAMTD0ZvcnQtRnVuc3RvbjBDQTEQMA4GA1UEKRMHRWFzeVJTQTEhMB8GCsGSIb3 DQEJARYSbWVAbXlob3N0Lm15ZG9tYWluMB4XDTEzMDcxMTA5MzQyNVoXDTEzMDcw</pre>
Server Key	<pre>-----BEGIN PRIVATE KEY----- MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBCgwwgSkAgEAAoIBAQDGBhbINAegGYFe TaMwhLDpQX5cZE5vV5sL74kqRQ68g/3l5bwinTk/hXUizkpc1HAEIrlBvmdTgt xjcg9Xs0isQMb1x+haelploVtzXTnpsZu6Vu+oXfPvMmzn/7f728l/URL6gJmB DIIM1J9IKboZQLtL7pm58NK2SBNrDDDDW6xmsbr1hLLbzGlsa1Ob2V19+kFysiZg x8ICLJddG0ceD0Ntwlv8sJCAin+E1E8aiS7P6NBgD63EA0pMktGIkRgyvWfAG6Vi</pre>

GET CERT AND KEY

If there is an OpenVPN client connected to the OpenVPN server, it will appear in the following list.

Client Crt And Key

GET CLIENT CRT AND KEY

Client Name	Status	Remarks	Configure
client1689068568	Used	test3	Export Client-Crt And Client-Key Revoke

Records per page: 20 ▾ 1-1 of 1 < >

If you need to create a certificate and secret key for the OpenVPN client, Click on the **GET CLIENT CRT AND KEY** button to load the following page.

Client Name

Remarks

CONFIRM CANCEL

Tips:
These parameters do not support Chinese.