



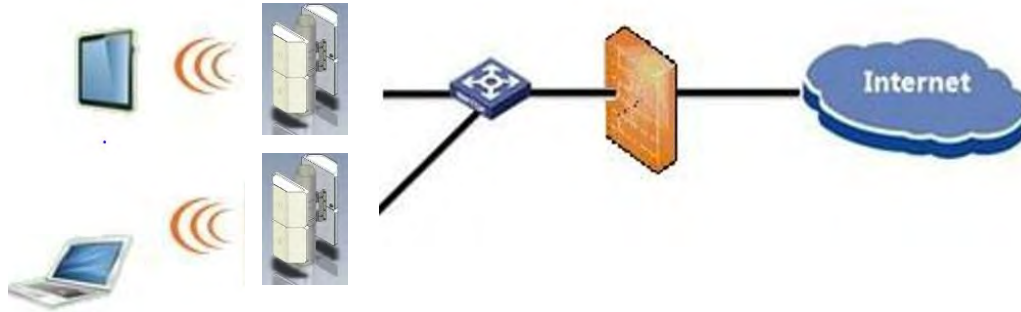
UniCAP UC-12-EXP User Manual

Universal Carrier Aggregation Platform

TABLE OF CONTENTS

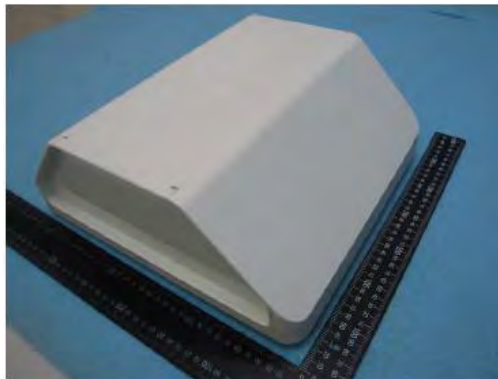
1	UniCAP Access Point (AP) Network Topology	3
1.1	Connect PoE Adapter to UniCAP AP	3
1.2	Configure PC IP address.....	4
1.3	Visit AP Web page	5
1.4	Configure IP address for AP	5
1.5	Connect AP to Switch.....	6
1.6	Configure location, Language and Country code for AP	6
1.7	Configure detailed WiFi parameters for AP	7
1.8	Configure Radius parameters for AP	8
1.9	Configure Portal parameters for AP.....	9
1.10	Configure security parameters for AP	10
1.11	Configure Rate limit rule (Optional).....	11
1.12	Configure Group ID (Optional)	12
1.13	Configure MAC ACL rule (Optional).....	13
1.14	Configure SSID.....	14
2	AP WDS Network Topology	16
2.1	Enable WDS function	16
2.2	Configure CPE WDS	17
3	NAWDS Network Topology.....	18
3.1	Configure WDS bridge mode	18
3.2	Input remote AP MAC	19
3.3	The configuration in remote AP.....	19
3.4	NAWDS Auto Find.....	20
4	Troubleshooting	22
4.1	Ping Diagnose	22
4.2	TraceRT Diagnose	22
4.3	How to backup/restore setting.....	23
4.4	How to upgrade AP	23
4.5	How to reset AP to default setting.....	24
4.6	How to check AP Setting by console	24
5	FCC Statement	30

1 UniCAP Access Point (AP) Network Topology



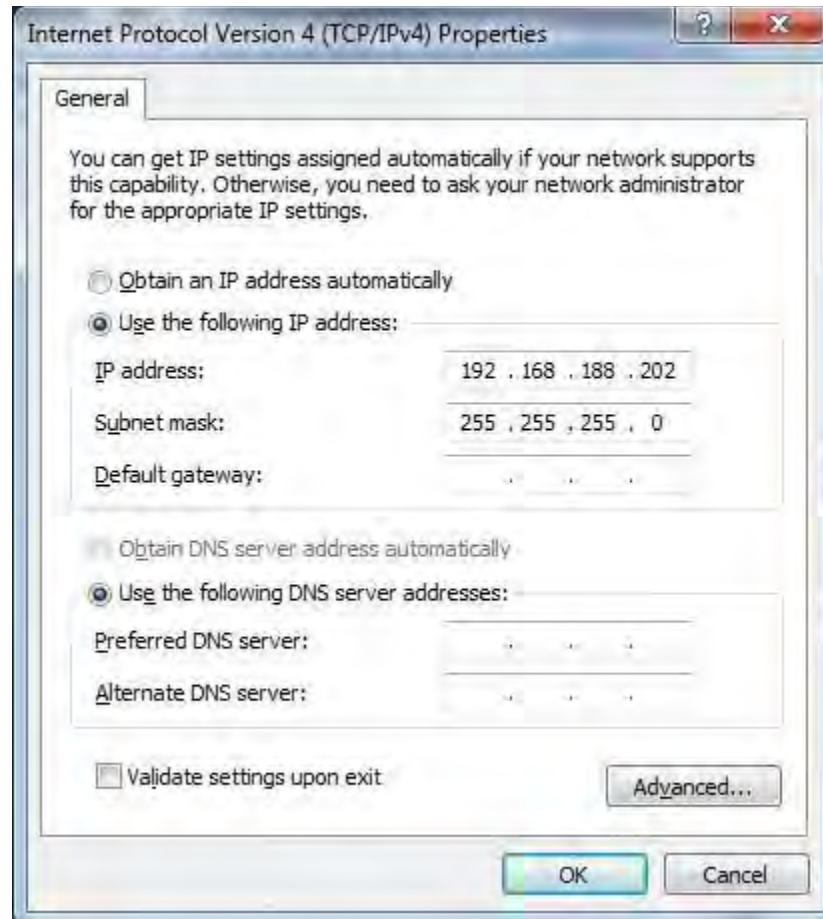
1.1 Connect PoE Adapter to UniCAP AP

UC



Notes: Please connect PoE to UniCAP Expansion Unit AP port and the Ethernet Port labeled "LAN-IN" on PoE Adapter to your PC or Switch.

1.2 Configure PC IP address



Notes: Connect your PC to the "LAN-IN" port on PoE Adapter of AP, manually configure your wired NIC with a static IP address on the 192.168.188.x subnet (e.g. 192.168.188.202).

1.3 Visit AP Web page



The screenshot shows a web browser at the address 192.168.188.251/index.html. The interface has a sidebar menu with options: Status, Network, Radio, Wireless, Security, QoS, Tools, and Management. The main content area is titled 'Overview' and contains the following information:

Overview	
Device Name	2x2 Dualband Indoor AP
Location	Shanghai
Device Model	WF-180
Device SN	CIGW12345678
Hardware Version	80010101
Software Version	R2.0.03.017
Working Mode	FAT AP
PoE Type	Standard
CPU Utilization	2.0%
Up Time	0 Hours 9 Minutes 46 Seconds

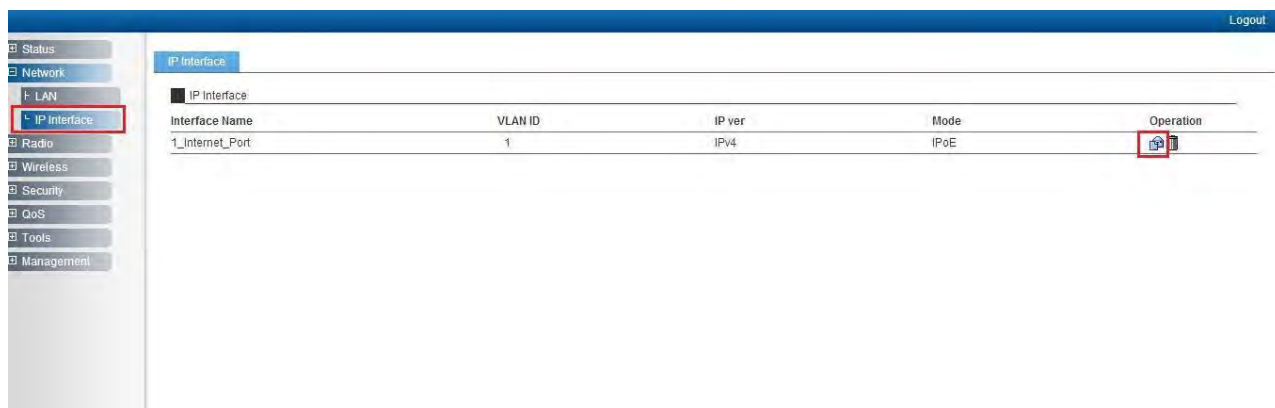
IP Interface			
Interface Name	VLAN ID	IPv4 Address	State
1_Internet_Port	1	192.168.188.251	UP

Radio	
Type	2.4G
Radio	Enable
Radio Mode	802.11 n
Service Mode	AP
Bandwidth Mode	20M
Channel	11(Auto)
Transmit Power	20
Recv Noise Floor	0

Copyright (C) 2005-2015 XXXXXXXXX

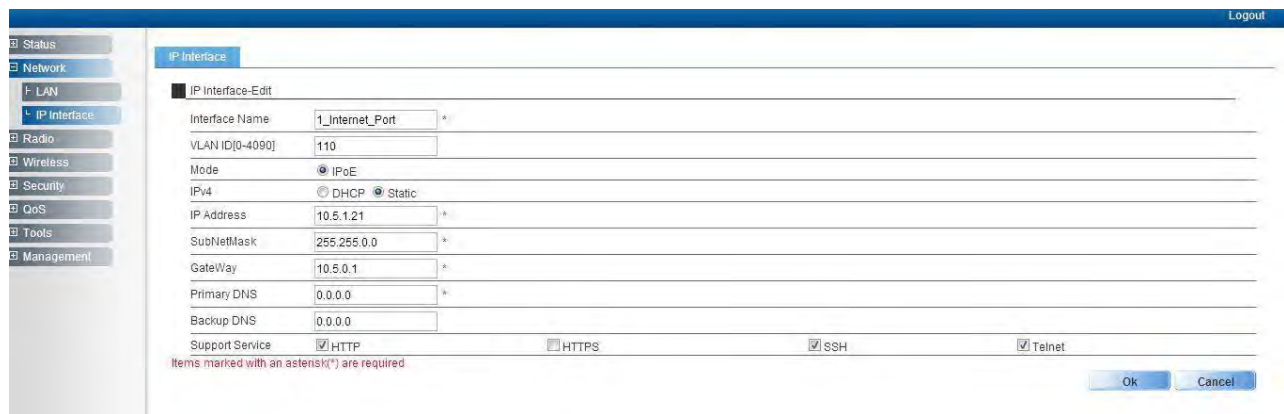
Notes: Input the default IP address "192.168.188.251" in the address bar of browser. Then enter the default username and password (username: admin, password: password) to enter the Web interface of AP.

1.4 Configure IP address for AP



The screenshot shows the 'IP Interface' configuration page. The sidebar menu has 'IP Interface' highlighted. The main content area shows the following table:

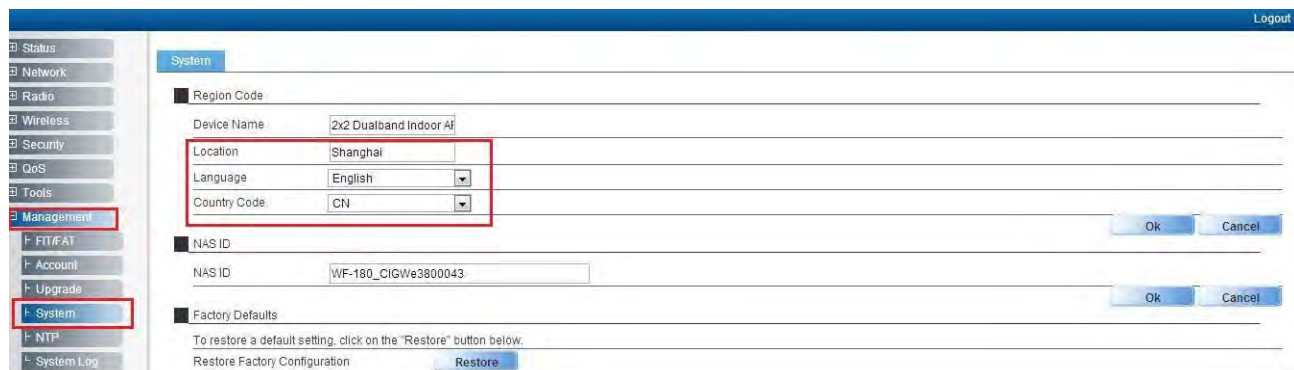
IP Interface				
Interface Name	VLAN ID	IP ver	Mode	Operation
1_Internet_Port	1	IPv4	IPoE	



1.5 Connect AP to Switch

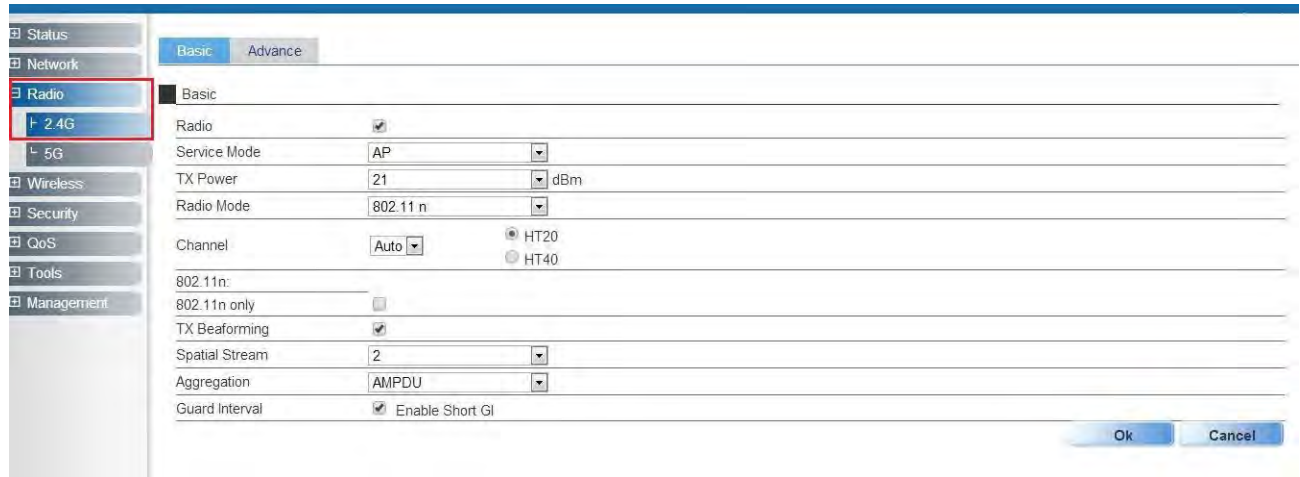
Notes: Connect AP to Switch and confirm it can visit Internet, then configure your PC to the same subnet and connect to the same Switch in order to continue to configuring the AP.

1.6 Configure location, Language and Country code for AP



Notes: After change the country code, the AP will be set to factory default.

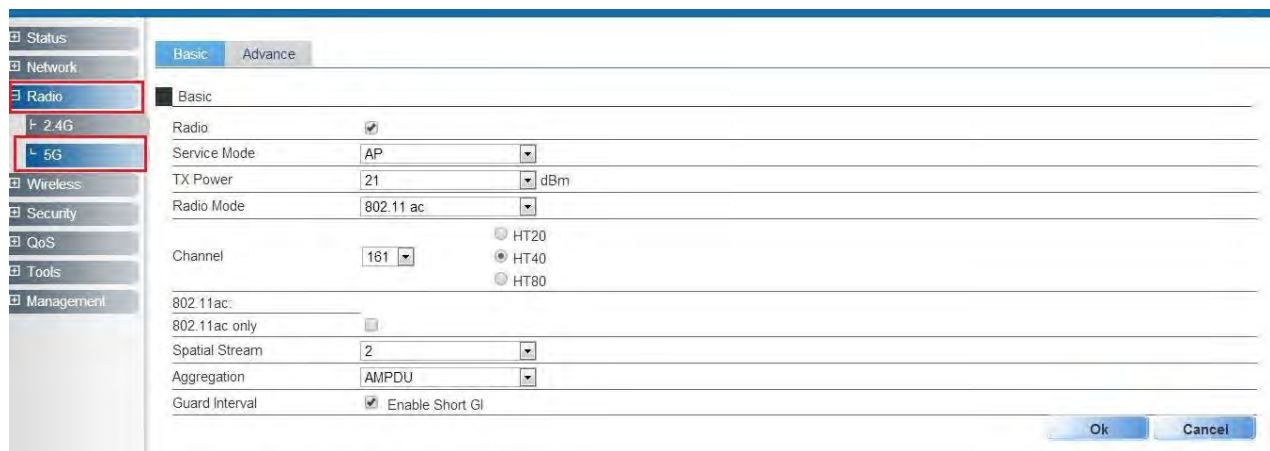
1.7 Configure detailed WiFi parameters for AP



The screenshot shows the 'Radio' configuration page for the 2.4G band. The left sidebar has 'Radio' selected, and '2.4G' is highlighted. The main area shows the 'Basic' tab with the following settings:

Radio	☒
Service Mode	AP
TX Power	21 dBm
Radio Mode	802.11 n
Channel	Auto
☒ HT20 ☐ HT40	
802.11n:	
802.11n only	☐
TX Beamforming	☒
Spatial Stream	2
Aggregation	AMPDU
Guard Interval	☒ Enable Short GI

Buttons: Ok, Cancel



The screenshot shows the 'Radio' configuration page for the 5G band. The left sidebar has 'Radio' selected, and '5G' is highlighted. The main area shows the 'Basic' tab with the following settings:

Radio	☒
Service Mode	AP
TX Power	21 dBm
Radio Mode	802.11 ac
Channel	161
☐ HT20 ☒ HT40 ☐ HT80	
802.11ac:	
802.11ac only	☐
Spatial Stream	2
Aggregation	AMPDU
Guard Interval	☒ Enable Short GI

Buttons: Ok, Cancel

1.8 Configure Radius parameters for AP

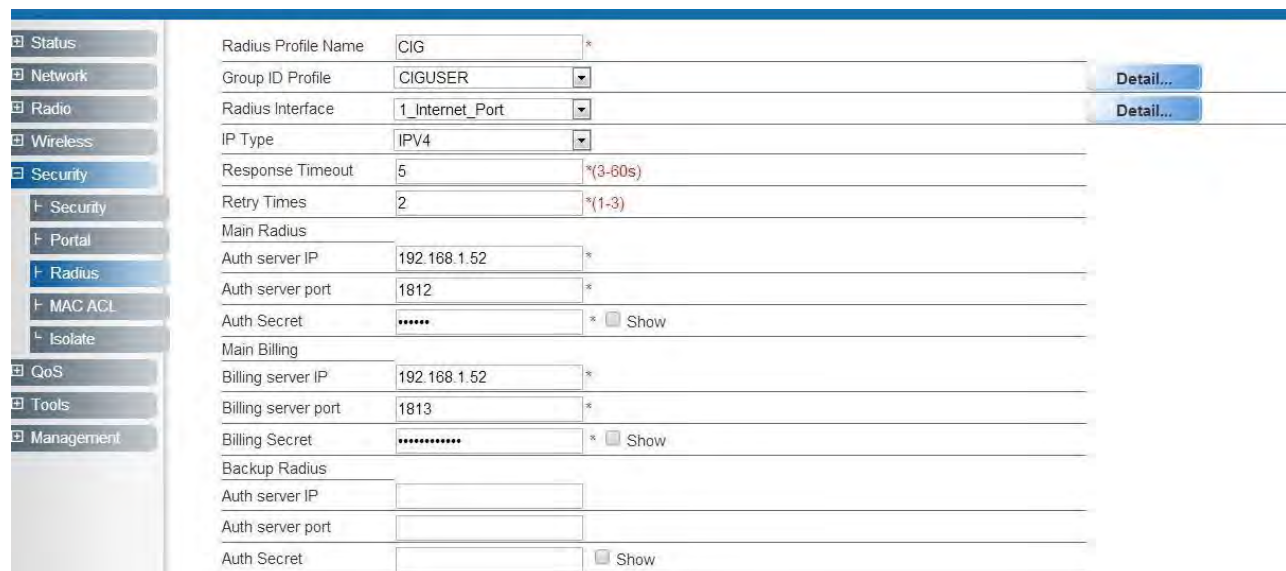
Notes: If want to use the 802.1x authentication, it need to configure the Radius profile firstly. Then in the security profile, the radius profile will be presented in the drop-down list.



Radius

Radius List

Profiles Name	Main Radius	Backup Radius	Main Billing	Backup Billing	Operation
Add					



Radius Profile Name: CIG *

Group ID Profile: CIGUSER

Radius Interface: 1_Internet_Port

IP Type: IPV4

Response Timeout: 5 *(3-60s)

Retry Times: 2 *(1-3)

Main Radius

Auth server IP: 192.168.1.52 *

Auth server port: 1812 *

Auth Secret: ***** *

Main Billing

Billing server IP: 192.168.1.52 *

Billing server port: 1813 *

Billing Secret: ***** *

Backup Radius

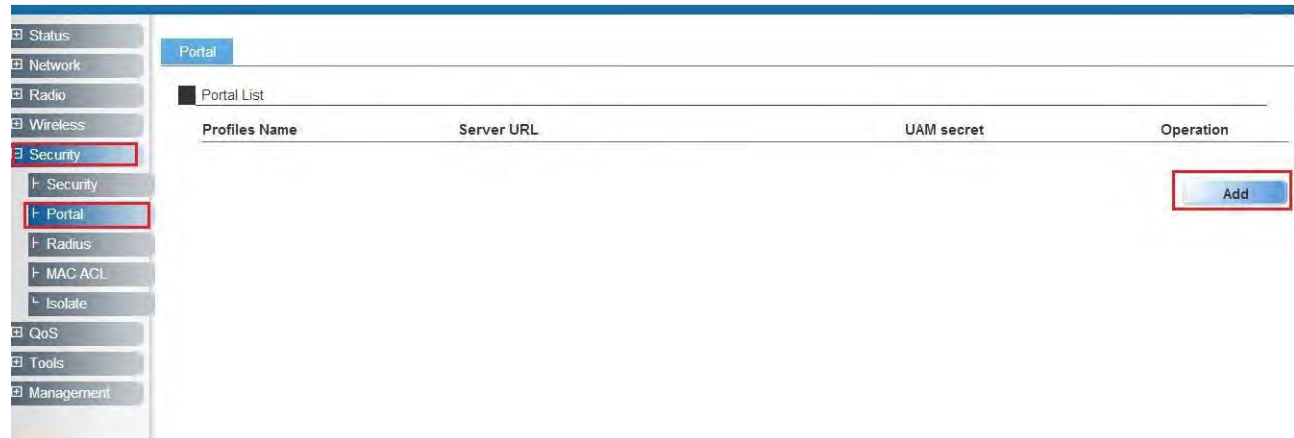
Auth server IP:

Auth server port:

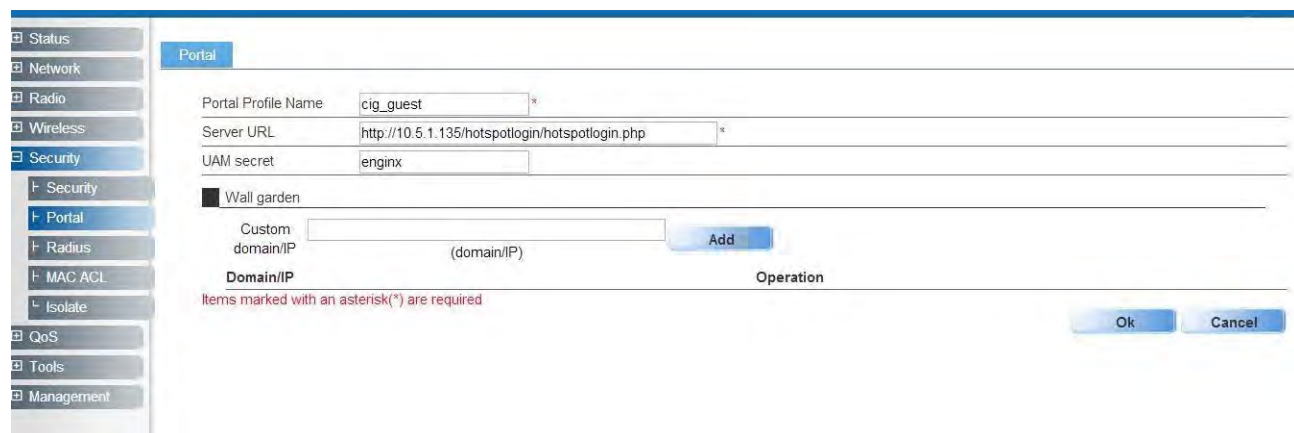
Auth Secret:

1.9 Configure Portal parameters for AP

Notes: The AP can support Web authentication based on Chillispot. If want to use the Web authentication, it need to configure the Portal profile and Radius profile firstly. Then in the security profile, the Portal profile and Radius profile will be presented in the drop-down list. Above all, you need to setup a Web authentication server and radius server.



Profiles Name	Server URL	UAM secret	Operation
Add			



Portal Profile Name: *

Server URL: *

UAM secret:

Wall garden

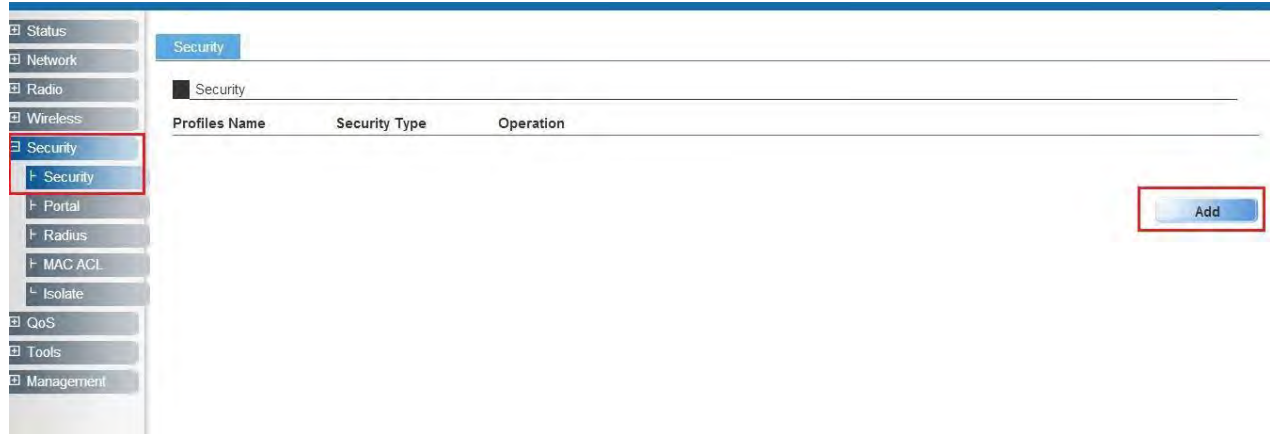
Custom domain/IP: (domain/IP) Add

Domain/IP: Operation:

Items marked with an asterisk(*) are required

Ok Cancel

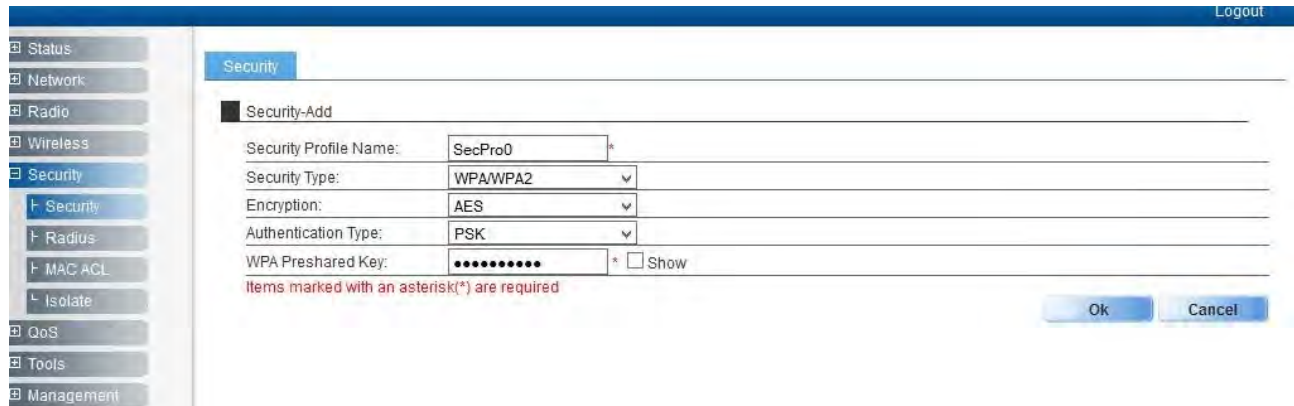
1.10 Configure security parameters for AP



Security

Profiles Name	Security Type	Operation
Add		

PSK



Security-Add

Security Profile Name: SecPro0 *

Security Type: WPA/WPA2

Encryption: AES

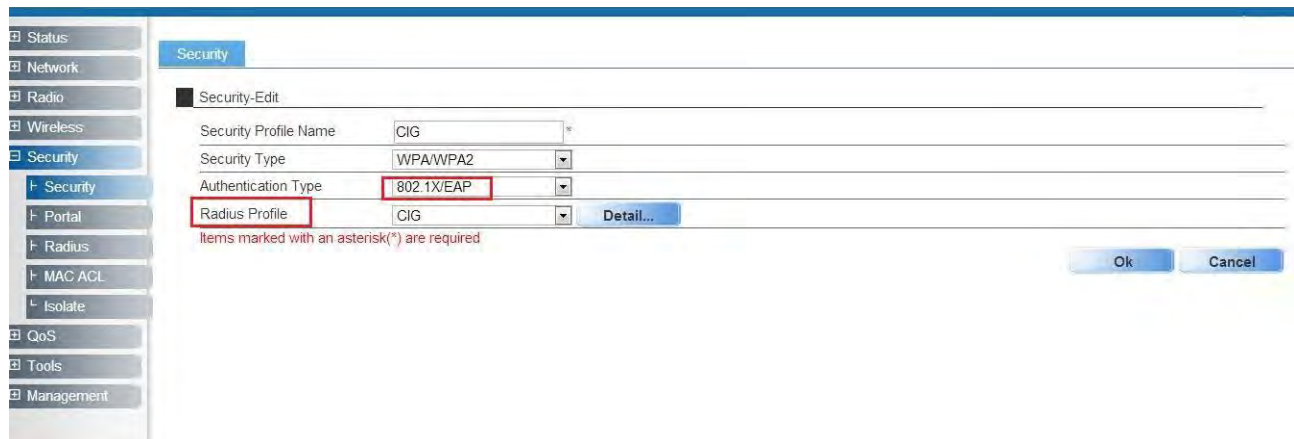
Authentication Type: PSK

WPA Preshared Key: * ☐ Show

Items marked with an asterisk(*) are required

Ok Cancel

802.1x Authentication



Security-Edit

Security Profile Name: CIG *

Security Type: WPA/WPA2

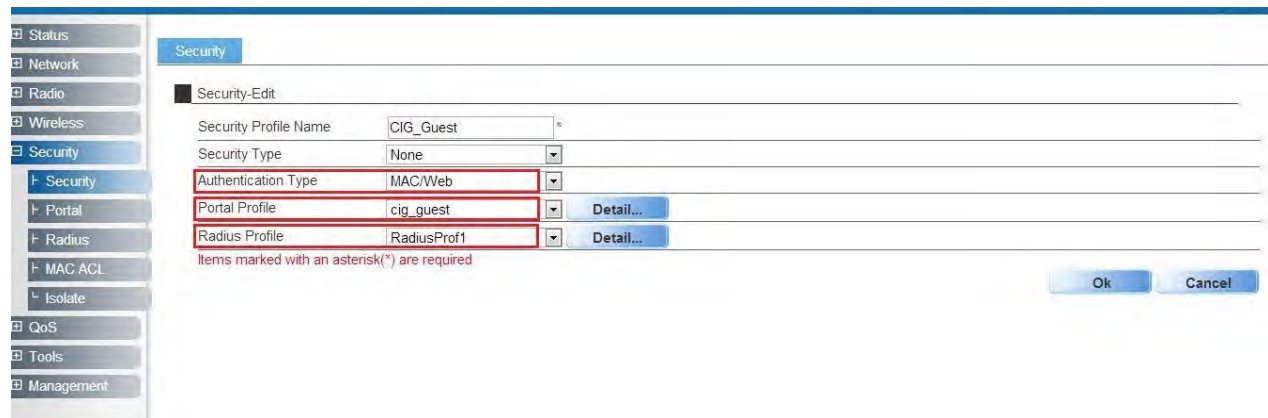
Authentication Type: 802.1X/EAP

Radius Profile: CIG

Items marked with an asterisk(*) are required

Ok Cancel

Web Authentication



Security

Security-Edit

Security Profile Name: CIG_Guest *

Security Type: None

Authentication Type: MAC/Web

Portal Profile: cig_guest Detail...

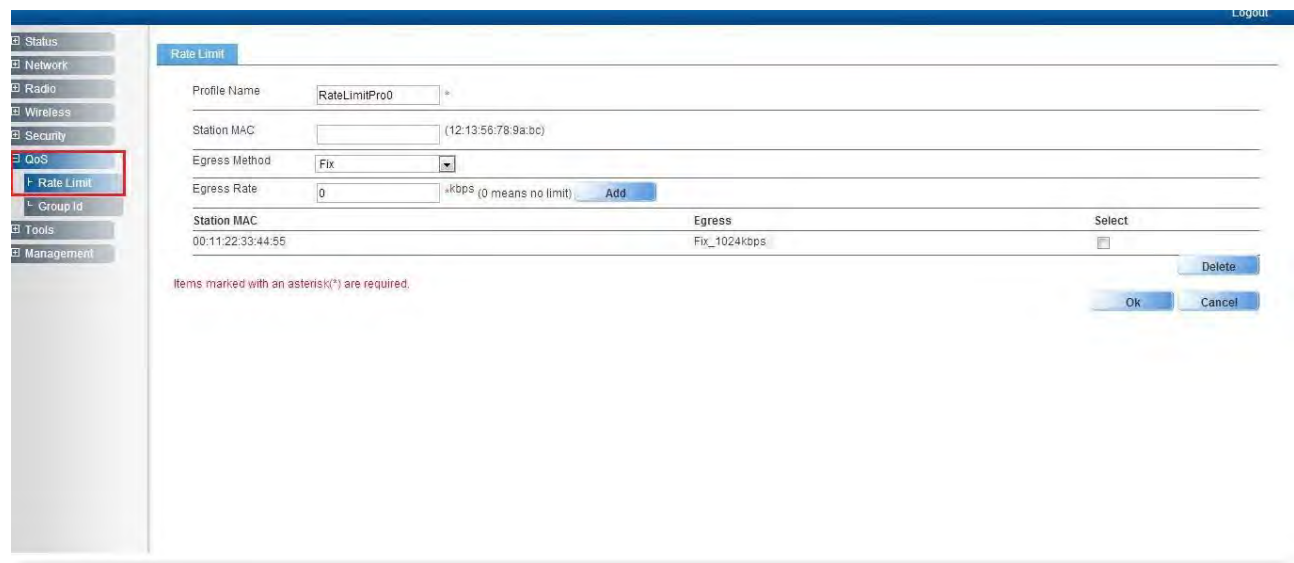
Radius Profile: RadiusProf1 Detail...

Items marked with an asterisk(*) are required

Ok Cancel

1.11 Configure Rate limit rule (Optional)

Notes: Rate Limit profile will be cited in the AP configuration.



Rate Limit

Profile Name: RateLimitPro0 *

Station MAC: (12:13:56:78 9a:bc)

Egress Method: Fix

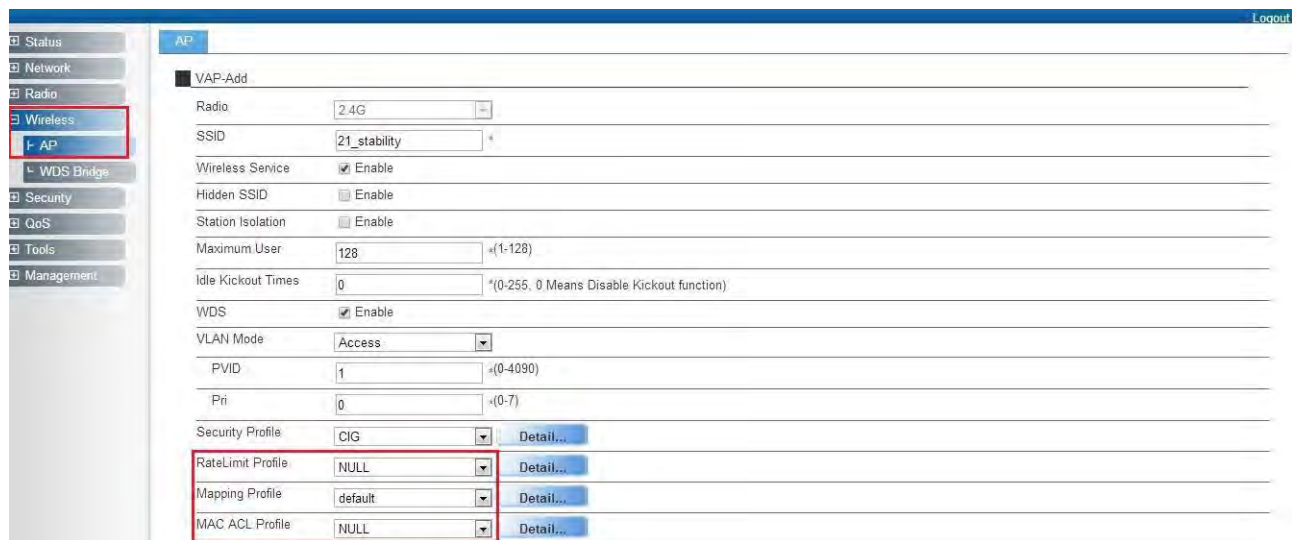
Egress Rate: 0 kbps (0 means no limit) Add

Station MAC	Egress	Select
00:11:22:33:44:55	Fix_1024Kbps	☐

Delete

Items marked with an asterisk(*) are required

Ok Cancel



VAP-Add

Radio: 2.4G

SSID: 21_stability

Wireless Service: ☒ Enable

Hidden SSID: ☐ Enable

Station Isolation: ☐ Enable

Maximum User: 128 (1-128)

Idle Kickout Times: 0 (0-255, 0 Means Disable Kickout function)

WDS: ☒ Enable

VLAN Mode: Access

PVID: 1 (0-4090)

Pri: 0 (0-7)

Security Profile: CIG [Detail...](#)

RateLimit Profile: NULL [Detail...](#)

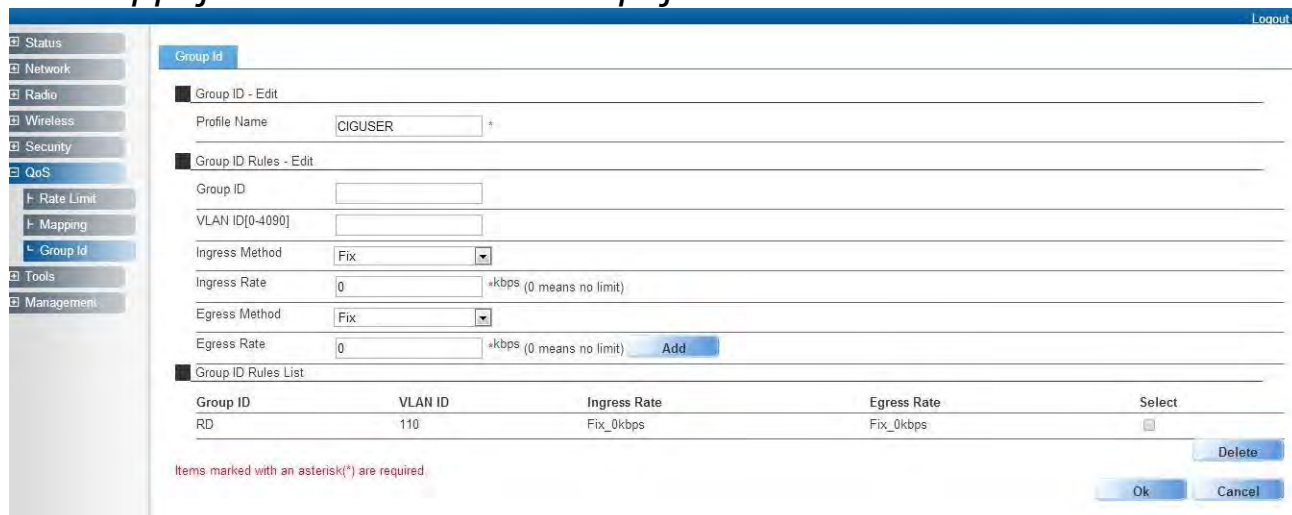
Mapping Profile: default [Detail...](#)

MAC ACL Profile: NULL [Detail...](#)

1.12 Configure Group ID (Optional)

Notes: Group profile is used for 802.1x/Web authentication. Group is classified by Filter-ID attribute in radius access accept message. The Group is bound with the role of the user. Different group has different VLAN and rate limit configuration. When a station sends the username and password to the Radius server for authentication, the server can respond with a Filter-ID (optional) to the AP. After AP gets the Filter-ID attribute, AP will search the Filter-ID in the Group profiles. If the Filter-ID can be matched in one profile, the traffic VLAN and rate limit will be applied to the station.

The Group profile is cited in the Radius server profile.



Group ID

Group ID - Edit

Profile Name: CIGUSER

Group ID Rules - Edit

Group ID:

VLAN ID[0-4090]:

Ingress Method: Fix

Ingress Rate: 0 kbps (0 means no limit)

Egress Method: Fix

Egress Rate: 0 kbps (0 means no limit) [Add](#)

Group ID Rules List

Group ID	VLAN ID	Ingress Rate	Egress Rate	Select
RD	110	Fix_0kbps	Fix_0kbps	☐

Items marked with an asterisk(*) are required.

[Delete](#) [Ok](#) [Cancel](#)

Radius-Edit

Radius Profile Name	CIG *	
Group ID Profile	CIGUSER	Detail...
Radius Interface	1_Internet_Port	Detail...
IP Type	IPv4	
Response Timeout	5	*(3-60s)
Retry Times	2	*(1-3)
Main Radius		
Auth server IP	192.168.1.52 *	
Auth server port	1812 *	
Auth Secret	*****	* Show
Main Billing		
Billing server IP	192.168.1.52 *	
Billing server port	1813 *	
Billing Secret	*****	* Show
Backup Radius		
Auth server IP		
Auth server port		
Auth Secret		Show
Backup Billing		
Billing server IP		

1.13 Configure MAC ACL rule (Optional)

MAC ACL

MAC-ACL-Profile-Edit

MAC ACL Profile Name: Black-1 *

Access Control Mode: ☒ Black ☐ white

MAC ACL List

Enter MAC Address: 18-03-73-58-e6-d3 (XX:XX:XX:XX:XX:XX) [Add](#)

Items marked with an asterisk(*) are required

[Ok](#) [Cancel](#)

1.14 Configure SSID

Logout

AP

VAP List

Radio	SSID Name	Service State	Security Profile	Operation
2.4G	2g_ssid1	Enable	NULL	 
5G	5g_ssid1	Enable	NULL	 

Add

Logout

AP

VAP-Edit

Radio: 2.4G

SSID: 2g_ssid1 *

Wireless Service: ☒ Enable

Hidden SSID: ☐ Enable

Station Isolation: ☐ Enable

Maximum User: 128 *(1-256)

Idle Kickout Times: 0 *(0-255, 0 Means Disable Kickout function)

WDS: ☐ Enable

VLAN Mode: Access

PVID: 1 *(0-4095)

Pri: 0 *(0-7)

Security Profile: NULL [Detail...](#)

RateLimit Profile: NULL [Detail...](#)

Mapping Profile: default [Detail...](#)

MAC ACL Profile: NULL [Detail...](#)

Items marked with an asterisk(*) are required

Ok Cancel

Logout

- Status
- Network
- Radio
- Wireless
- AP
- WDS Bridge
- Security
- QoS
- Tools
- Management

AP

VAP-Edit

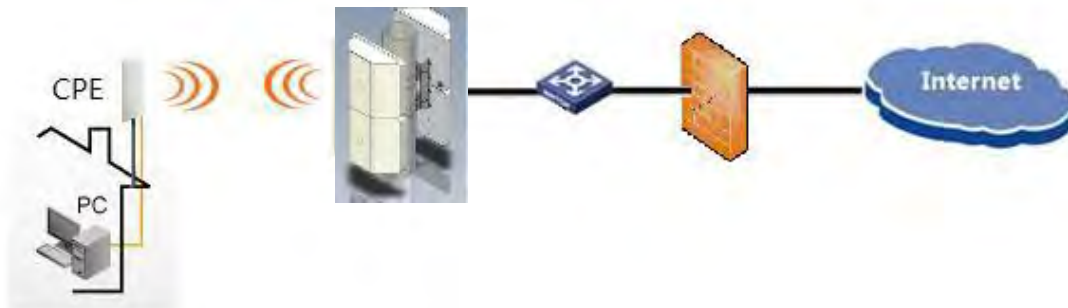
Radio:	5G	
SSID:	5g_ssid1	*
Wireless Service:	☒ Enable	
Hidden SSID:	☐ Enable	
Station Isolation:	☐ Enable	
Maximum User:	128	*(1-256)
Idle Kickout Times:	0	*(0-255, 0 Means Disable Kickout function)
WDS:	☐ Enable	
VLAN Mode:	Access	
PVID:	1	*(0-4095)
Pri:	0	*(0-7)
Security Profile:	NULL	Detail...
RateLimit Profile:	NULL	Detail...
Mapping Profile:	default	Detail...
MAC ACL Profile:	NULL	Detail...

Items marked with an asterisk(*) are required

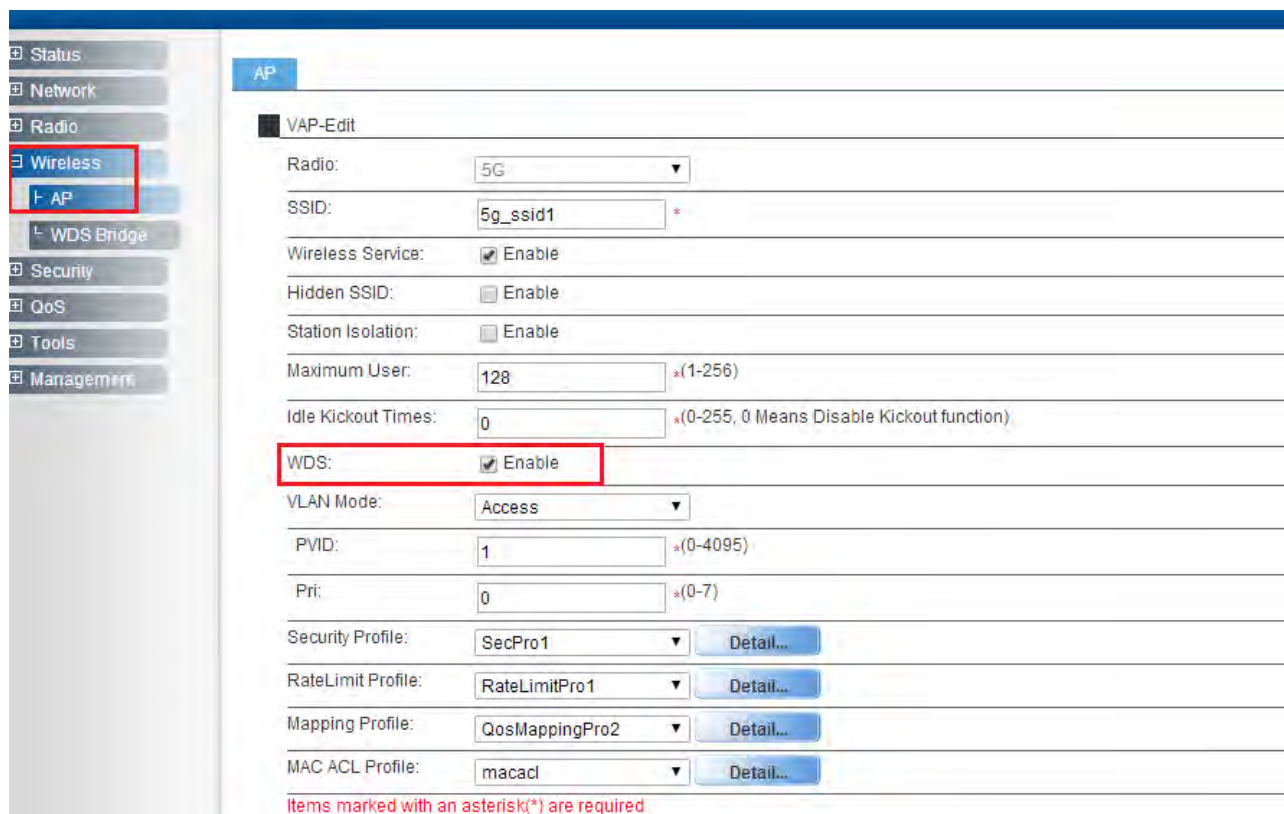
[Ok](#)
[Cancel](#)

Notes: You may apply the relevant Security, Rate Limit, Mapping or MAC ACL profiles which you configured here. After the above setting, wireless stations can connect to the relevant SSID of AP and get IP address from DHCP server of firewall to visit Internet.

2 AP WDS Network Topology



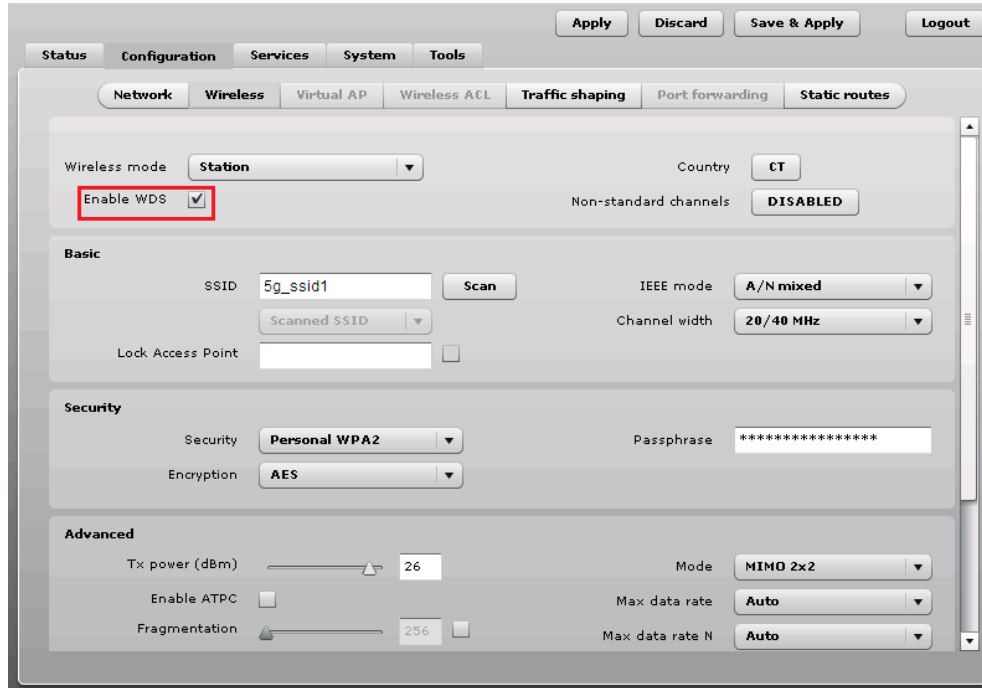
2.1 Enable WDS function



The screenshot shows the configuration interface for an AP. The left sidebar contains a menu with the following items: Status, Network, Radio, Wireless, AP, WDS Bridge, Security, QoS, Tools, and Management. The 'Wireless' and 'AP' items are highlighted with a red box. The main area displays the 'AP' configuration page, which includes a 'VAP-Edit' section. The 'WDS' checkbox is checked and highlighted with a red box. The 'WDS' checkbox is labeled 'WDS: Enable'. Below the 'WDS' checkbox, there are several other configuration options: VLAN Mode (Access), PVID (1), Pri (0), Security Profile (SecPro1), RateLimit Profile (RateLimitPro1), Mapping Profile (QosMappingPro2), and MAC ACL Profile (macacl). Each of these options has a 'Detail...' button next to it. At the bottom of the page, a note states: 'Items marked with an asterisk(*) are required'.

Note: Enable WDS function when you configure SSID.

2.2 Configure CPE WDS



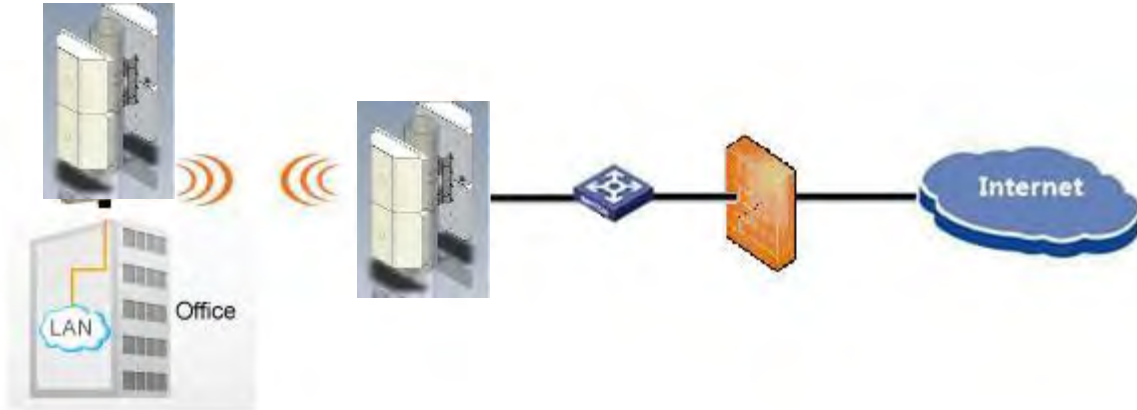
The screenshot shows the CapWave configuration interface with the following settings:

- Wireless mode:** Station
- Country:** CT
- Non-standard channels:** DISABLED
- Basic:**
 - SSID:** 5g_ssid1
 - Scan:** Button
 - Scanned SSID:** Dropdown menu
 - Lock Access Point:** ☐
 - IEEE mode:** A/N mixed
 - Channel width:** 20/40 MHz
- Security:**
 - Security:** Personal WPA2
 - Encryption:** AES
 - Passphrase:** *****
- Advanced:**
 - Tx power (dBm):** 26
 - Enable ATPC:** ☐
 - Fragmentation:** 256 ☐
 - Mode:** MIMO 2x2
 - Max data rate:** Auto
 - Max data rate N:** Auto

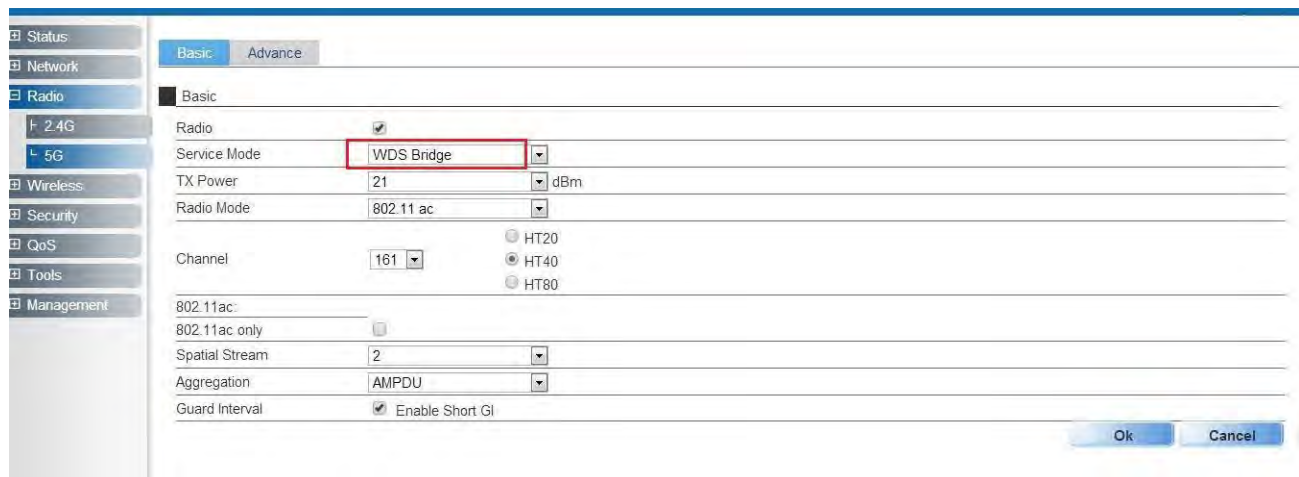
Buttons at the top: Apply, Discard, Save & Apply, Logout.

Note: Enable WDS function too when you configure CPE to connect to AP.

3 NAWDS Network Topology



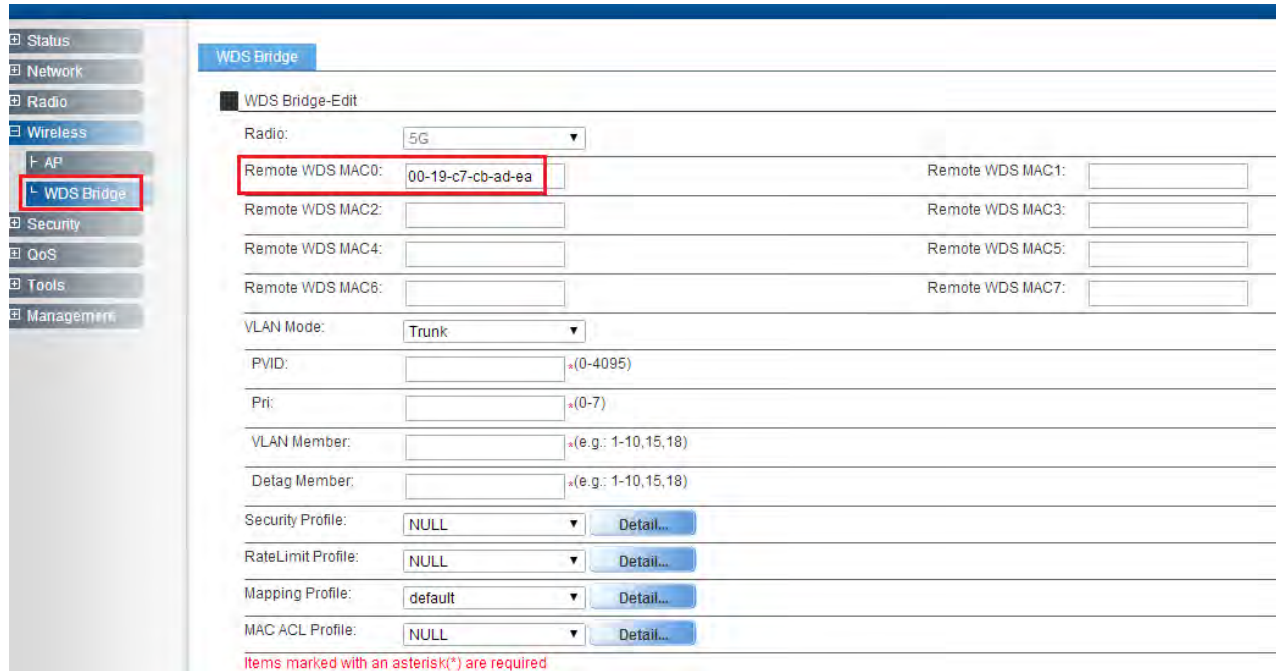
3.1 Configure WDS bridge mode



The screenshot shows the 'Basic' configuration tab for a radio device. The 'Service Mode' is set to 'WDS Bridge' (highlighted with a red box). The 'TX Power' is set to 21 dBm. The 'Radio Mode' is set to '802.11 ac'. The 'Channel' is set to 161. The '802.11ac' section is expanded, showing '802.11ac only' is checked, 'Spatial Stream' is set to 2, 'Aggregation' is set to 'AMPDU', and 'Guard Interval' is set to 'Enable Short GI'. The 'Ok' and 'Cancel' buttons are at the bottom right.

Note: Please select a specified Channel (for example 161) here.

3.2 Input remote AP MAC



WDS Bridge

WDS Bridge-Edit

Radio: 5G

Remote WDS MAC0: 00-19-c7-cb-ad-ea

Remote WDS MAC1:

Remote WDS MAC2:

Remote WDS MAC3:

Remote WDS MAC4:

Remote WDS MAC5:

Remote WDS MAC6:

Remote WDS MAC7:

VLAN Mode: Trunk

PVID: (0-4095)

Pri: (0-7)

VLAN Member: (e.g.: 1-10,15,18)

Detag Member: (e.g.: 1-10,15,18)

Security Profile: NULL [Detail...](#)

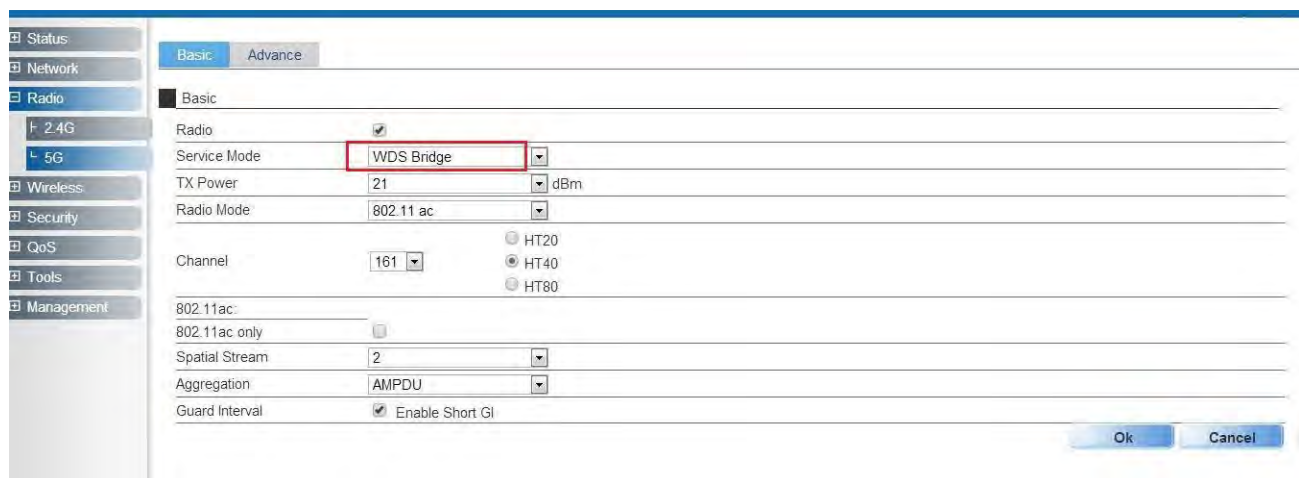
RateLimit Profile: NULL [Detail...](#)

Mapping Profile: default [Detail...](#)

MAC ACL Profile: NULL [Detail...](#)

Items marked with an asterisk(*) are required

3.3 The configuration in remote AP



Basic **Advance**

Basic

Radio ☒

Service Mode: WDS Bridge

TX Power: 21 dBm

Radio Mode: 802.11ac

Channel: 161

802.11ac:

802.11ac only: ☒

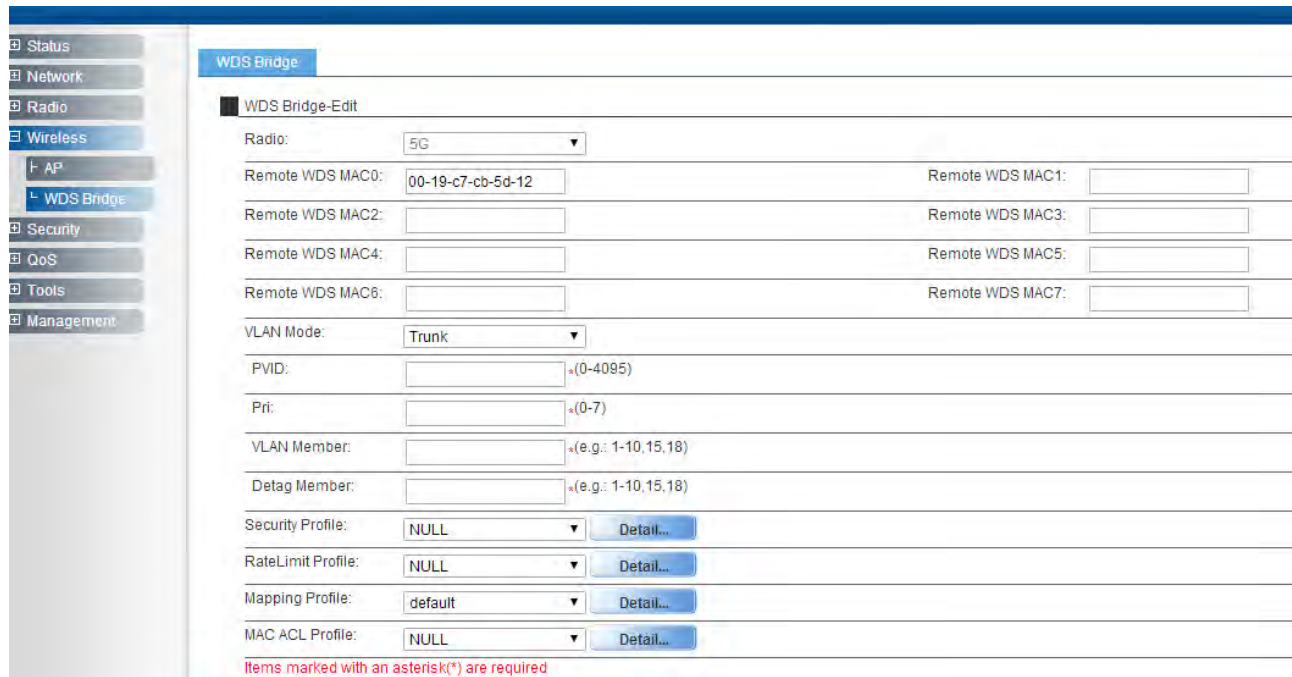
Spatial Stream: 2

Aggregation: AMPDU

Guard Interval: ☒ Enable Short GI

[Ok](#) [Cancel](#)

Note: Please select the same Channel as the Channel of AP which you want to connect via WDS.

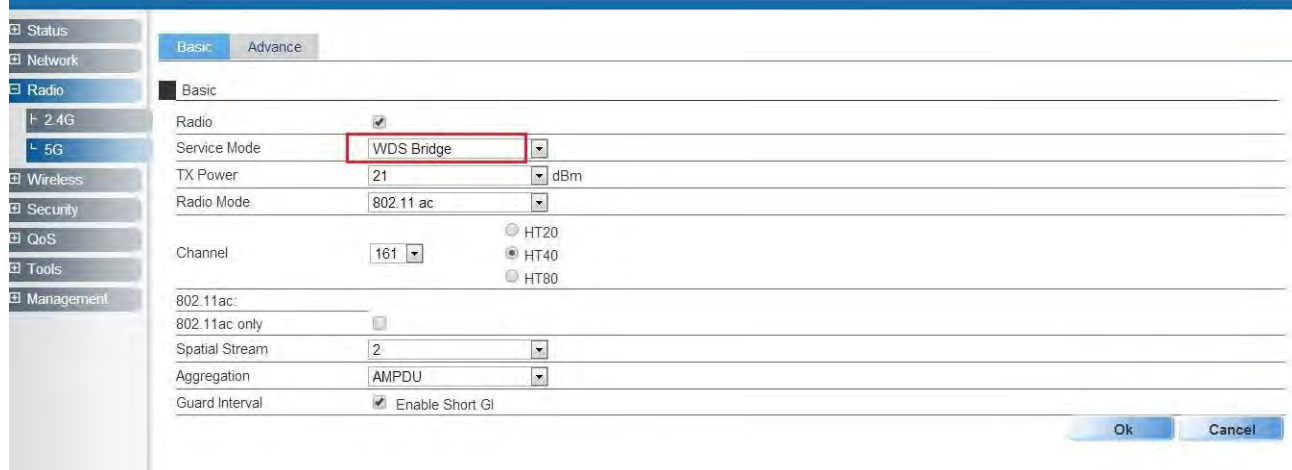


The image shows the 'WDS Bridge' configuration page in a web interface. On the left is a sidebar with navigation tabs: Status, Network, Radio, Wireless, AP, WDS Bridge (selected), Security, QoS, Tools, and Management. The main area is titled 'WDS Bridge' and contains a 'WDS Bridge-Edit' section. This section includes various configuration fields: Radio (set to 5G), Remote WDS MAC0 through MAC7 (with MAC0 set to 00-19-c7-cb-5d-12), VLAN Mode (set to Trunk), PVID, Pri, VLAN Member, Detag Member, Security Profile (set to NULL), RateLimit Profile (set to NULL), Mapping Profile (set to default), and MAC ACL Profile (set to NULL). Each profile field has a 'Detail...' button. At the bottom, a red note states: 'Items marked with an asterisk(*) are required'.

Note: Please input the MAC address of AP which you want to connect via WDS.

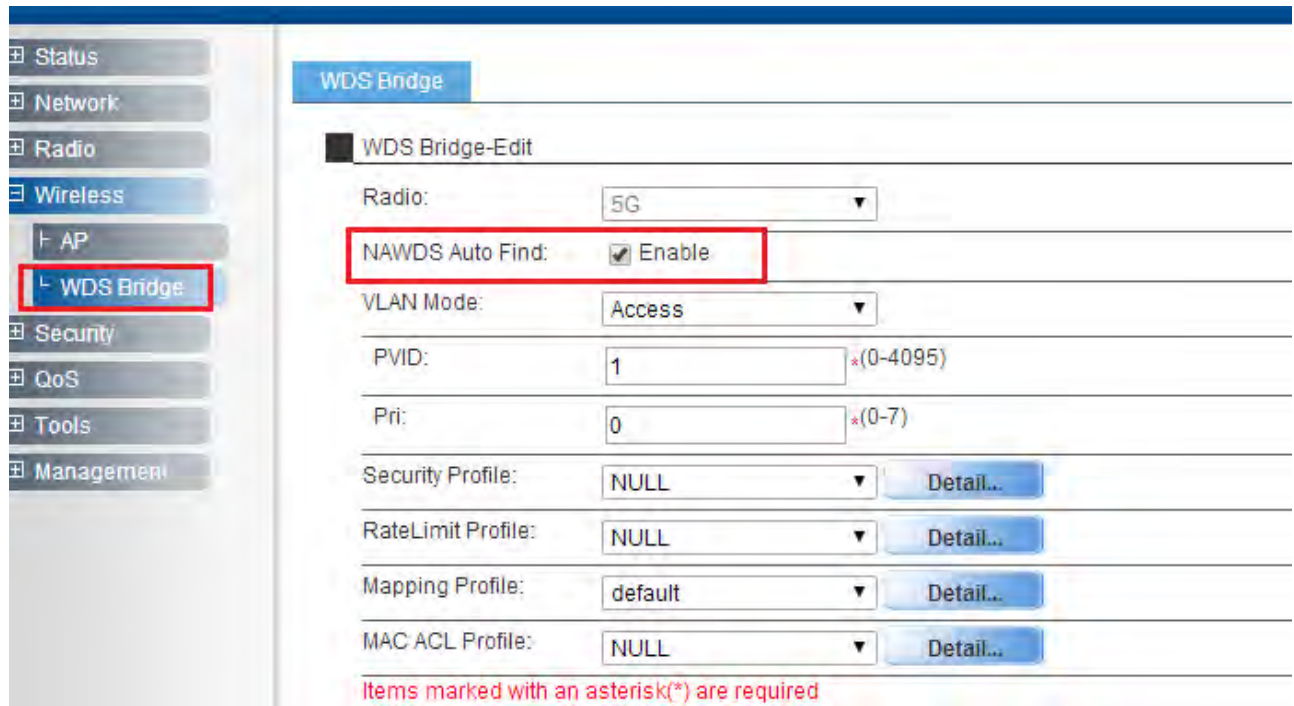
3.4 NAWDS Auto Find

UniCAP AP also supports “NAWDS Auto Find” function, after you configure master AP, you may enable “NAWDS Auto Find” function in slave AP.



The image shows the 'Basic' configuration page in a web interface. On the left is a sidebar with navigation tabs: Status, Network, Radio, Wireless, 2.4G, 5G (selected), Security, QoS, Tools, and Management. The main area is titled 'Basic' and contains various configuration fields: Radio (checked), Service Mode (set to WDS Bridge, highlighted with a red box), TX Power (set to 21 dBm), Radio Mode (set to 802.11ac), Channel (set to 161), HT20, HT40, HT80 (radio buttons), 802.11ac only (checkbox), Spatial Stream (set to 2), Aggregation (set to AMPDU), and Guard Interval (checked, with 'Enable Short GI' text). At the bottom right are 'Ok' and 'Cancel' buttons.

Note: Please select the same Channel as the Channel of AP which you want to connect via WDS.



WDS Bridge

WDS Bridge-Edit

Radio: 5G

NAWDS Auto Find: ☒ Enable

VLAN Mode: Access

PVID: 1 *(0-4095)

Pri: 0 *(0-7)

Security Profile: NULL Detail..

RateLimit Profile: NULL Detail..

Mapping Profile: default Detail..

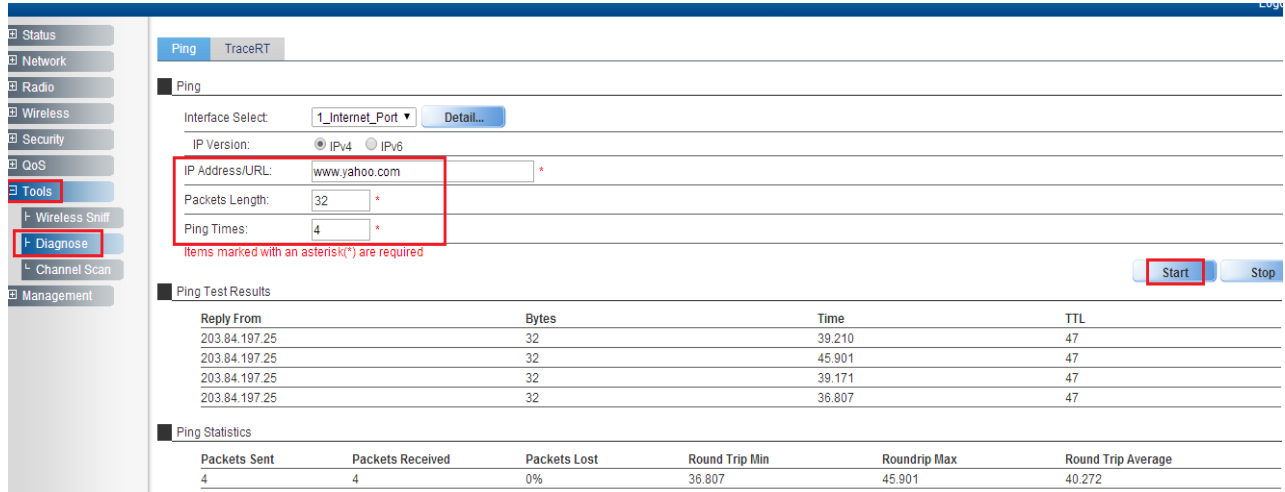
MAC ACL Profile: NULL Detail..

Items marked with an asterisk(*) are required

Note: After you enable "NAWDS Auto Find" function, the AP will connect to the master AP via WDS automatically.

4 Troubleshooting

4.1 Ping Diagnose



Ping | TraceRT

Interface Select: [Detail...](#)

IP Version: ☒ IPv4 ☐ IPv6

IP Address/URL: *

Packets Length: *

Ping Times: *

Items marked with an asterisk(*) are required

[Start](#) [Stop](#)

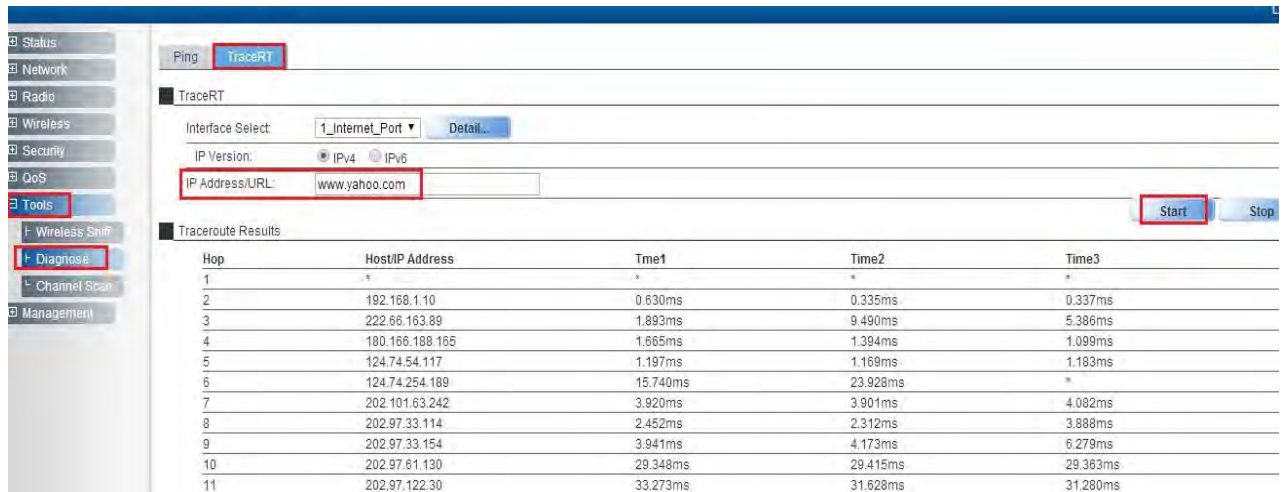
Ping Test Results

Reply From	Bytes	Time	TTL
203.84.197.25	32	39.210	47
203.84.197.25	32	45.901	47
203.84.197.25	32	39.171	47
203.84.197.25	32	36.807	47

Ping Statistics

Packets Sent	Packets Received	Packets Lost	Round Trip Min	Roundtrip Max	Round Trip Average
4	4	0%	36.807	45.901	40.272

4.2 TraceRT Diagnose



Ping | **TraceRT**

Interface Select: [Detail...](#)

IP Version: ☒ IPv4 ☐ IPv6

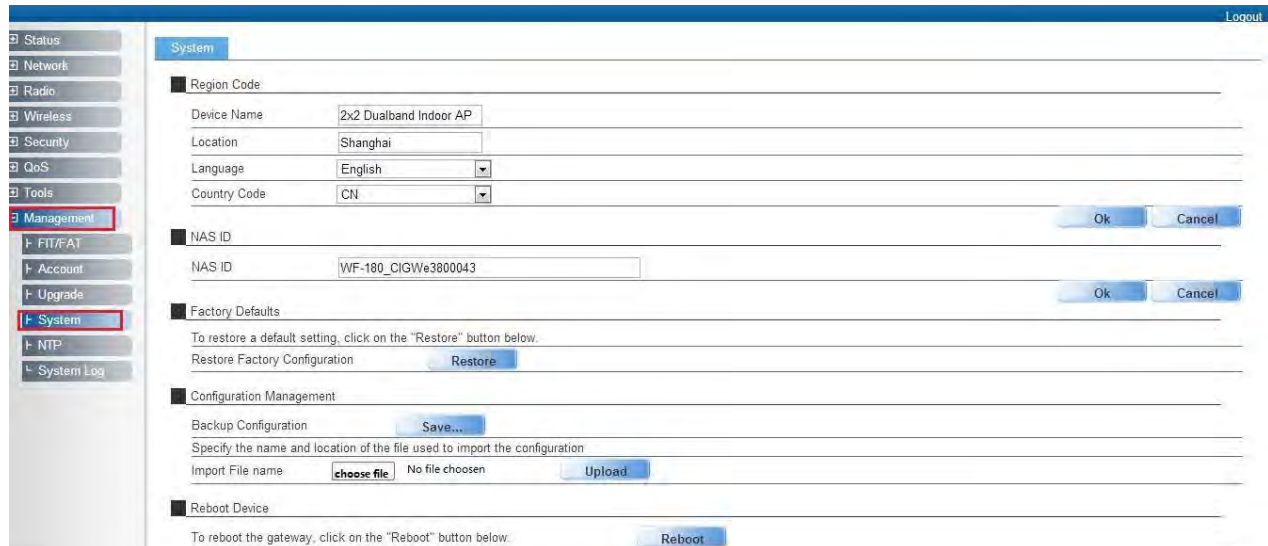
IP Address/URL:

[Start](#) [Stop](#)

Traceroute Results

Hop	Host/IP Address	Time1	Time2	Time3
1	*	*	*	*
2	192.168.1.10	0.630ms	0.335ms	0.337ms
3	222.66.163.89	1.893ms	9.490ms	5.386ms
4	180.166.188.165	1.665ms	1.394ms	1.099ms
5	124.74.54.117	1.197ms	1.169ms	1.183ms
6	124.74.254.189	15.740ms	23.928ms	*
7	202.101.63.242	3.920ms	3.901ms	4.082ms
8	202.97.33.114	2.452ms	2.312ms	3.888ms
9	202.97.33.154	3.941ms	4.173ms	6.279ms
10	202.97.61.130	29.348ms	29.415ms	29.363ms
11	202.97.122.30	33.273ms	31.628ms	31.280ms

4.3 How to backup/restore setting



System

Region Code

Device Name: 2x2 Dualband Indoor AP

Location: Shanghai

Language: English

Country Code: CN

Ok Cancel

NAS ID

NAS ID: WF-180_CIGWe3800043

Ok Cancel

Factory Defaults

To restore a default setting, click on the "Restore" button below.

Restore Factory Configuration: Restore

Configuration Management

Backup Configuration: Save...

Specify the name and location of the file used to import the configuration

Import File name: choose file No file chosen Upload

Reboot Device

To reboot the gateway, click on the "Reboot" button below.

Reboot

Notes: Press "Save" button to save current setting. Press "Upload" button to load saved setting.



4.4 How to upgrade AP



Upgrade

Upgrade Software Image

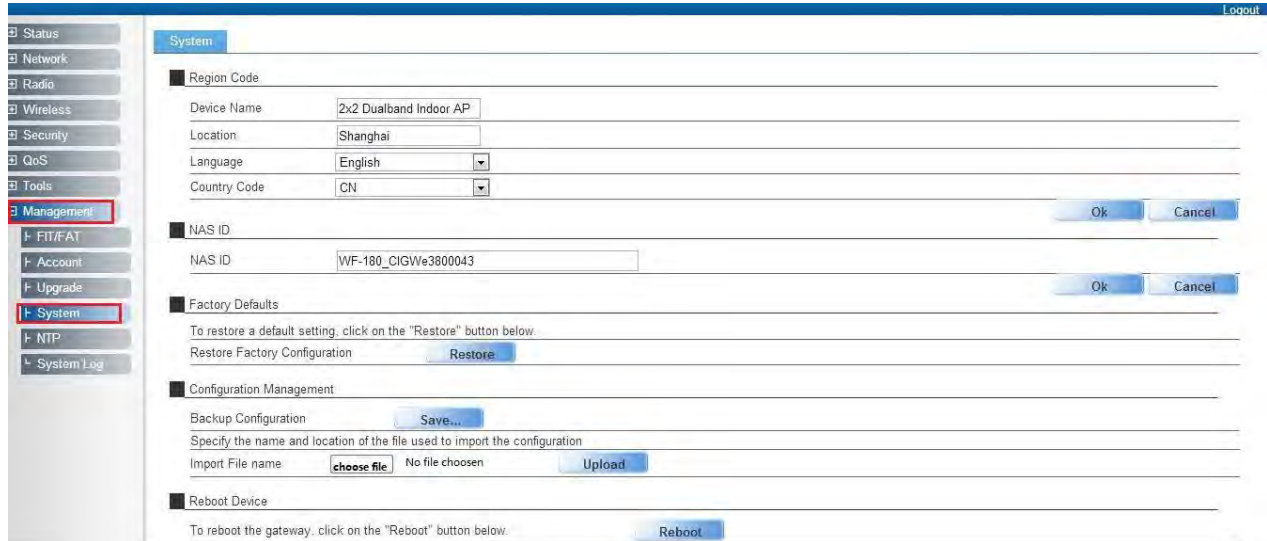
Current Firmware Version: R1.2.02.003

Downloaded file: Choose File No file chosen

Upgrade

Notes: Press "Choose File" button to select firmware file, then press "Upgrade" button to upgrade AP.

4.5 How to reset AP to default setting



Notes: If you can't visit AP web page, please press the "Reset" button of AP and hold for more than 5 seconds, the AP will reset to default setting automatically. Or you can do it by the Web GUI.

4.6 How to check AP Setting by console

Serial cable definition

Notes: For the serial cable, one side is a standard DB-9 female serial port and the other side is a RJ11 connector. For the RJ11 connector PIN sequence you can use below picture as a reference.



DB9 Female

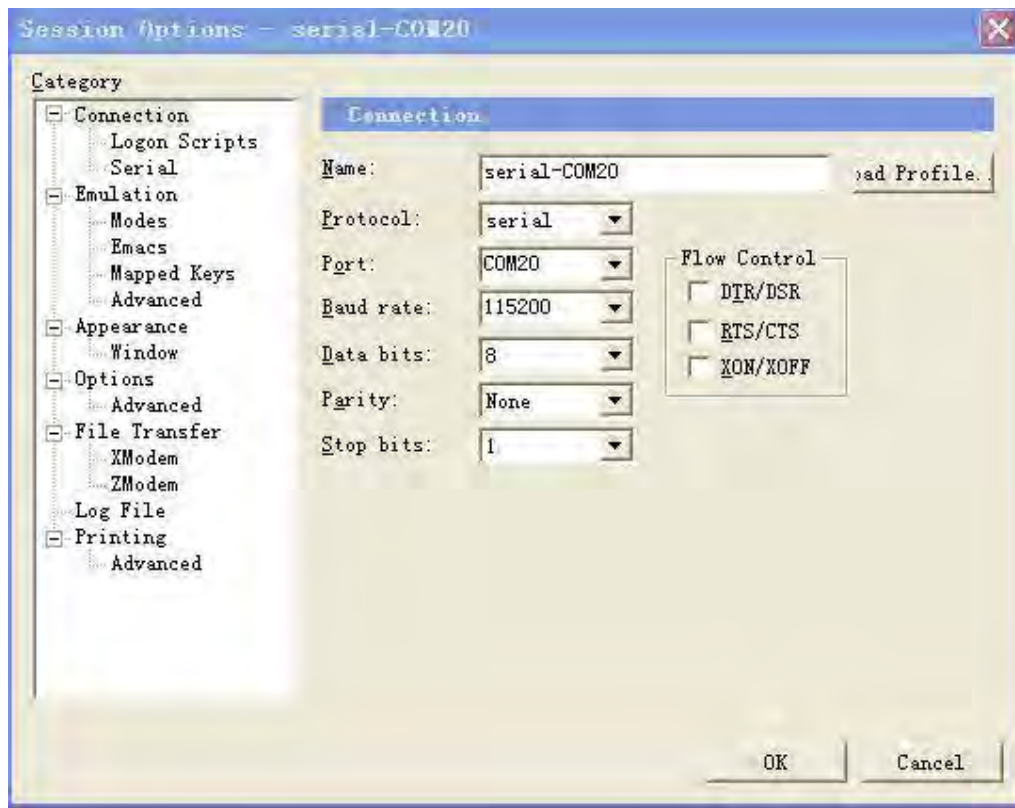
5 4 3 2 1



9 8 7 6



RJ11 PIN	DB-9 hole
2	3
3	5
4	5
5	2



```

10.100.11.166 - SecureCRT
File Edit View Options Transfer Script Tools Window Help

Login as: admin
Password:

AP >enable
#AP >/system/shell/
#AP >/system/shell/ifconfig

ath0 Link encap:Ethernet HWaddr E0:1D:3B:FF:CB:60
      inet6 addr: fe80::e21d:3bff:feff:cb60/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:1946 errors:0 dropped:0 overruns:0 frame:0
      TX packets:33404 errors:0 dropped:151379 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:265914 (259.6 KiB) TX bytes:7630872 (7.2 MiB)

ath1 Link encap:Ethernet HWaddr E0:1D:3B:FF:CB:61
      inet6 addr: fe80::e21d:3bff:feff:cb61/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:1826 errors:0 dropped:0 overruns:0 frame:0
      TX packets:28792 errors:0 dropped:148975 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:236928 (231.3 KiB) TX bytes:6168301 (5.8 MiB)

ath16 Link encap:Ethernet HWaddr E0:1D:3B:FF:CB:70
      inet6 addr: fe80::e21d:3bff:feff:cb70/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:2121 errors:0 dropped:0 overruns:0 frame:0
      TX packets:89618 errors:0 dropped:151209 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:328282 (320.5 KiB) TX bytes:25674613 (24.4 MiB)

eth0 Link encap:Ethernet HWaddr E0:1D:3B:FF:CB:8D
      inet addr: 10.100.11.166 Bcast:10.100.11.255 Mask:255.255.255.0
      inet6 addr: fe80::e21d:3bff:feff:cb8d/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:452126 errors:0 dropped:0 overruns:0 frame:0
      TX packets:172753 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:64818930 (61.8 MiB) TX bytes:11878929 (11.3 MiB)

ge0 Link encap:Ethernet HWaddr E0:1D:3B:FF:CB:80
      inet6 addr: fe80::e21d:3bff:feff:cb80/64 Scope:Link
      UP BROADCAST RUNNING PROMISC MULTICAST MTU:1500 Metric:1
      RX packets:4857992 errors:0 dropped:231979 overruns:0 frame:0
      TX packets:434690 errors:0 dropped:2 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:522774124 (498.5 MiB) TX bytes:42937056 (40.9 MiB)

```

Note: Input "enable" first and "ifconfig" command in "system/shell" folder to check AP IP address.

```

10.100.11.166 - SecureCRT
File Edit View Options Transfer Script Tools Window Help
[Icons]

#AP/system/shell>
#AP/system/shell>
#AP/system/shell>iwconfig
lo        no wireless extensions.

ge0       no wireless extensions.

ge1       no wireless extensions.

tunl0     no wireless extensions.

ath16     IEEE 802.11na  ESSID:"Capaciti Networks"
          Mode:Master  Frequency:5.745 GHz  Access Point: E0:1D:3B:FF:CB:70
          Bit Rate:450 Mb/s   Tx-Power=28 dBm
          RTS thr=2346 B   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=94/94  Signal level=-96 dBm  Noise level=-95 dBm
          Rx invalid nwid:63242  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0  Missed beacon:0

ath0      IEEE 802.11ng  ESSID:"Capaciti Networks"
          Mode:Master  Frequency:2.412 GHz  Access Point: E0:1D:3B:FF:CB:60
          Bit Rate:216.7 Mb/s   Tx-Power=28 dBm
          RTS thr=2346 B   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=94/94  Signal level=-96 dBm  Noise level=-95 dBm
          Rx invalid nwid:81119  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0  Missed beacon:0

ath17     IEEE 802.11na  ESSID:"Columbus Hotspot"
          Mode:Master  Frequency:5.745 GHz  Access Point: E0:1D:3B:FF:CB:71

```

Note: Input "iwconfig" command in "system/shell" folder to check AP WiFi setting.

```

10.100.11.166 - SecureCRT
File Edit View Options Transfer Script Tools Window Help
[Icons]

ath6 IEEE 802.11ng ESSID:"Pretty Fly 4 WiFi"
Mode:Master Frequency:2.412 GHz Access Point: E0:1D:3B:FF:CB:66
Bit Rate:216.7 Mb/s Tx-Power=28 dBm
RTS thr=2346 B Fragment thr:off
Encryption key:off
Power Management:off
Link Quality=94/94 Signal level=-96 dBm Noise level=-95 dBm
Rx invalid nwid:81138 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:0 Missed beacon:0

ath23 IEEE 802.11na ESSID:"Columbus WiFi"
Mode:Master Frequency:5.745 GHz Access Point: E0:1D:3B:FF:CB:77
Bit Rate:450 Mb/s Tx-Power=28 dBm
RTS thr=2346 B Fragment thr:off
Encryption key:off
Power Management:off
Link Quality=94/94 Signal level=-96 dBm Noise level=-95 dBm
Rx invalid nwid:63083 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:0 Missed beacon:0

ath7 IEEE 802.11ng ESSID:"Columbus WiFi"
Mode:Master Frequency:2.412 GHz Access Point: E0:1D:3B:FF:CB:67
Bit Rate:216.7 Mb/s Tx-Power=28 dBm
RTS thr=2346 B Fragment thr:off
Encryption key:off
Power Management:off
Link Quality=94/94 Signal level=-96 dBm Noise level=-95 dBm
Rx invalid nwid:81108 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:0 Missed beacon:0

#AP/system/shell>wlanconfig ath16 list
ADDR AID CHAN TXRATE RXRATE RSSI IDLE TXSEQ RXSEQ CAPS ACAPS ERP STATE MAXRATE(DOT11) HTCAPS
44:94:fc:87:74:e8 1 149 250M 297M 37 0 2915 57520 EPs - 0 b 0 WPS RSN WME
#AP/system/shell>

```

Note: Input "wlanconfig athx list" command to check if there is any WiFi station connects to AP. In the command, "athx" means the different SSID, if you want to check if there is any WiFi station connects to AP SSID, please input the relevant athx of the SSID.

5 FCC Statement

Federal Communication Commission Interference Statement

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

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

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

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

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 47 cm between the radiator & your body.