WLAN Troubleshooting Guide V1.0

Copyright Statement

Exemption Statement

This document is provided “as is”. The contents of this document are subject to change without any notice. Please obtain the latest information through the Ruijie Networks website. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

Preface

This article provides a systematic approach to identifying and remedying problems that may arise as you use your WLAN devices over a period of time. This guide is not intended to replace configuration guide or to be an all-inclusive guide for every application. Rather, it is an attempt to provide you with the knowledge and skills necessary to correct the most common issues that you may encounter.

This article introduces the basic concepts, methodology, and general troubleshooting guidelines for problems that may occur when you configure and use RG WLAN devices.

Audience

- Network Engineers
- Network Administrator

Obtain Technical Assistance

- Ruijie Networks Websites: https://www.ruijienetworks.com
- Ruijie Service Portal: https://case.ruijienetworks.com

Revision History

Date	Change contents	Reviser
2018.7	Initial publication V1.0	Ruijie GTAC

Content

1 Common AC/AP Management-related FAQs

1.1 Does the CAPWAP tunnel support cross-NAT networking?

Yes, it supports.

If the AP is on the NAT intranet,

You do not need to configure the static IP address mapping or port mapping for the AP. You just need to configure the source IP address conversion to ensure the connectivity between the AP and the AC.

If the AC is on the NAT intranet,

1. On the egress router, configure mapping for UDP ports 5246 (control channel) and 5247 (data channel) with an AC address indicated by option 138.

2. The IP address of the AC (optional 138 IP address) on the AP is the public network address of the AC after mapping.

If the AP and the AC are on its own NAT intranet, the above three configurations must be met.

1.2 what traffic is need to be allowed to pass the firewall between the AC and the RADIUS server?

Interaction between the AC and the RADIUS server is generally based on the RADIUS protocol and SNMP. The ports to be opened are:

RADIUS port: Based on UDP. The default authentication port is 1812 and the default accounting port is 1813, which are both on the RADIUS server.

SNMP port: Based on UDP. The port is 161, which is on the AC.

1.3 How to kick a user offline

Check the user's MAC address:

WS#***show ac-con client by-ap-name***

Total Sta Num : 4

Cnt STA MACAP NAMEWlan Id Radio Id Vlan Id Valid

------ --------------- ------------------- --------- --------- --------- ---------

10021.6a99.6c5aBF2_AP_031122091

2701a.04a9.a1b2BF2_AP_062123091

3 0026.c690.0a06 BF7_AP_011122091

4001f.3b3b.b435BF7_AP_011122091

Kick the user offline:

WS(config)#ac-controller

WS(config-ac)#client-kick H.H.H----->H.H.H is the user's MAC address.

Because the client will be automatically reconnected, when the show ac-con client by-ap-name command is run after the user is forced offline, the offline STA is still displayed.

1.4 Where is the ap-config file saved on the AC?

It's saved in the ap-config.text file in AC flash.

1.5 Does the wireless network support VLAN-Group?

A VLAN-Group contains multiple VLANs. By associating with a VLAN-Group, a WLAN can map to multiple VLANs and VLANs can be flexibly allocated to STAs connected to the WLAN. The VLANs are allocated mainly in the following two modes:

After the STA passes the 802.1x authentication, the authentication server assigns a VLAN for the STA. The STA must be deployed in the 802.1x authentication mode and the authentication mode must be supported by the authentication server.

The server assigns the VLAN for the STA according to the idle status of the address pool.

1.6 How to view the wireless terminal type and operating system information on the AC?

Enable ip dhcp snooping and run the following command on AC:

```
ruijie#sh terminal-identify user
User entry list: 3
   mac-address        aging-time    terminal-type
-----------------------------------------
   68df.ddc7.de5a        --:--       XIAOMI Phone Android 4.2
   3859.f98b.658b        --:--       PC Windows 7
   a844.8130.c304        --:--       Nokia Phone Windows 8
```

Note: Due to terminal restrictions, the terminal may not be identified completely correct. When the terminal is connected to the wireless network, a DHCP packet is sent. The device reads the option 60 field in the packet. The field carries the terminal type information. However, not the DHCP packet of all the terminals carries the field, and thus the read success rate is not 100%.

1.7 Which of “ap-conf all” and “ap-config name” takes effect first?

The AP configuration under ap-config name takes effect first. If the AP under ap-config name is not configured, the ap-config all configuration takes effect.

1.8 How to fix when the device cannot ping the domain name?

Supplement the configuration AC(config)#ip name-server 8.8.8.8, which is used to set the DNS domain name for the device. You can modify the configuration based on the actual environment. Ensure that the AC normally communicates with the extranet.

1.9 How to delete an offline AP?

Perform the following operation:

Ruijie(config)#no ap-config *ap-name1*

Ruijie(config)#no ap-config all ----Delete the ap-config of all the offline APs.

Only configurations of offline APs can be deleted.

1.10 How to configure the location of a fit AP?

Refer to the following configuration:

Ruijie(config)#ap-config 001a.a9bf.ffdc

Ruijie(config-ap)#location meeting room

1.11 How to modify the address used by the AC to create the CAPWAP tunnel?

Ruijie(config)#ac-controller

Ruijie(config-ac)#capwap ctrl-ip 2.2.2.2

1.12 How to modify the SSID of the wireless network?

Go to the WLAN configuration mode:

Ruijie(config)#wlan-config 1 (“1” is the wlan sequence)

Ruijie(config-wlan)#ssid yy (yy is the new SSID)

1.13 How to configure the static AP IP address in fit AP mode?

Refer to the command: (when this parameter is modified, a tunnel is re-created.)

(1) Log on to the AP through the Console or Telnet port, and enter the global mode (the password is *apdebug*) to configure the static AP IP address, default route, and AC IP address:

Ruijie(config)#acip ipv4 1.1.1.1 // Configure the IP address for the AC.

Ruijie(config)#apip ipv4 172.16.1.34 255.255.255.0 172.16.1.109

(2) After the tunnel between the AP and the AC is created, log on to the AC to configure a static IP address for the AP:

Ruijie(config)#ap-config 220e

Ruijie(config-ap)#acip ipv4 1.1.1.1 ---->Configure the IP address of the AC.

Ruijie(config-ap)#ip address 172.16.1.34 255.255.255.0 172.16.1.109 ---->Configure the IP address, mask, and gateway for the AP. After configuration, the capwap tunnel will be re-created.

The configurations retain even the AP is restarted.

1.14 How to disable a radio of the AP?

In fat mode, directly go to this radio and shut it down.

Ruijie(config)#interface dot11radio 1/0

Ruijie(config-if-dot11radio 1/0)#shutdown

In fit mode:

Ruijie(config)#ap-config ap-name ---->Go to the AP configuration mode

Ruijie(config-ap)#no enable-radio 1 ---->Disable the radio 1.

1.15 How to disable automatic adjustment for the RRM channel?

Ruijie(config)#advanced 802.11a channel global off

Ruijie(config)#advanced 802.11b channel global off

1.16 How to cancel AAA authentication for AC logon when AAA authentication is enabled on the AC?

You can cancel AAA authentication for AC logon by modifying the configurations.

Ruijie(config)#aaa new-model

Ruijie(config)#aaa authentication login no-login none ---->Create an AAA logon authentication list named "no-login" and set the configuration to none (no authentication).

Ruijie(config)#line con 0

Ruijie(config-line)#login authentication no-login ---->Apply the no-login to the console line, which indicates that the AAA authentication is not used.

Ruijie(config-line)#line vty 0 35

Ruijie(config-line)#login authentication no-login ---->No password is needed for logon through the Telnet port.

1.17 How to configure switchover of the AC/AP O/E multiplexing interface

1. On AP:

   Ruijie(config)#interface gigabitEthernet0/1

   Ruijie(config-if-GigabitEthernet 0/1)# media-type baset ---->Enable the electrical interface.

   Ruijie(config-if-GigabitEthernet 0/1)#media-type basex ---->Enable the optical interface.

2. On AC:

   Ruijie(config)#interface gigabitEthernet 0/1

   Ruijie(config-if-GigabitEthernet 0/1)#medium-type copper

   Ruijie(config-if-GigabitEthernet 0/1)#medium-type fiber

   Ruijie(config-if-GigabitEthernet 0/1)#end

   Ruijie#write

1.18 How to synchronize the AC time to the AP

Ruijie(config)# ap-config *AP0001* //Enter the specified AP configuration mode.

Ruijie(config-ap)# timestamp /Configure AP0001 to synchronize the time of the local AC to the AP.

1.19 How to configure daily timed restart for the AP?

To prevent that the network connection is affected by too large load caused by long-time running of the AP, the daily timed restart can be set for the AP to ensure the network connection quality.

Configure Ruijie-AP1 to restart the AP at 1:00:00 each day on AC:

Ruijie(config)#ap-config Ruijie-AP1

Ruijie(config-ap)#reload at 1:00:00

1.20 How to close the LED indicator of the AP?

(1) Define a schedule session.

AC(config)#schedule session 1

AC(config)#schedule session 1 time-range 1 period Sun to Sat time 00:00 to 23:59

(2) Apply the schedule session on the AP

AC(config)#ap-config *ap-name*

AC(config-ap)#quiet-mode session 1

2 Daily Device Maintenance

2.1 How to check the number of APs that can be supported by a device?

ruijie#sh ac-config

AC Configuration info:

max_wtp:32

sta_limit:1024

license wtp max:32

license sta max:1024

serial auth :Disable

password auth :Disable

certificate auth :Disable

Bind AP MAC :Disable

AP Priority :Disable

supp_psk_cer :Disable

ac_name:end

ac location :Ruijie_COM

2.2 How to view the MAC address of the AC?

WS6108#sh ac-config

AC State info:

sta_num :0

act_wtp :6

localIpAddr :1.1.1.1

localIpAddr6 :::

used wtp :6.0(6 normal 0 half 0 zero)

remain wtp :42 normal 84 half 634 zero

HW Ver :1.01

SW Ver :AC_RGOS 11.1(5)B7, Release(02231014)

Mac address :5869.6c20.726a

Product ID :WS6108

NET ID :9876543210012345

NAS ID :5869.6c20.726a

For VAC:

WS6108#show member

System description : WS6108

System Mac Address : 58:69:6C:20:72:6A

2.3 How to fix when the AP management address is forgotten?

1. Networking Requirements

The administrator forgets the management address of WALL-AP but does not want to modify the device configurations or the factory settings of the device cannot be restored. This method is also applicable for devices with a Console port but cannot be logged onto through the Console port.

2. Configuration Tips

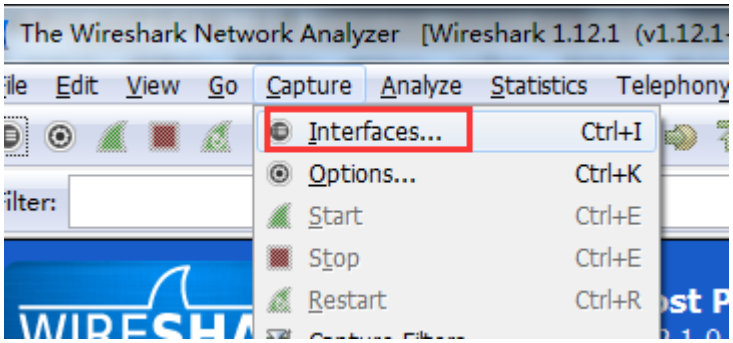
1. Execute the packet capture software on a PC to capture packets from the interface of the wired network.

2. Connect the WALL-AP cable to the PC and power on the AP.

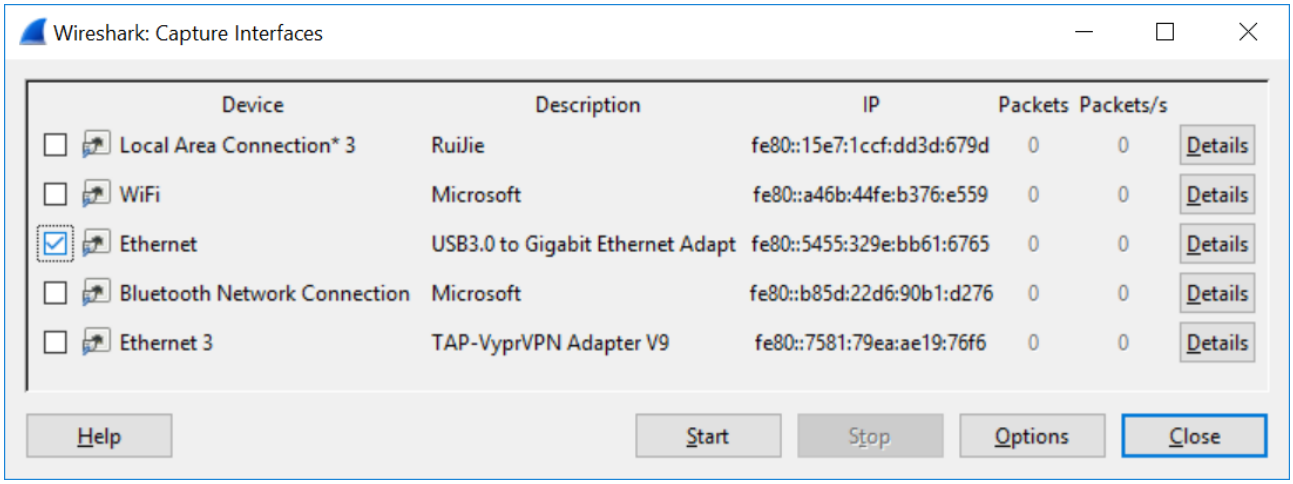
3. Configuration Steps

1. Execute the packet capture software (using Wireshark for an example) to capture packets from the wired interface.

(1) Select the interface.



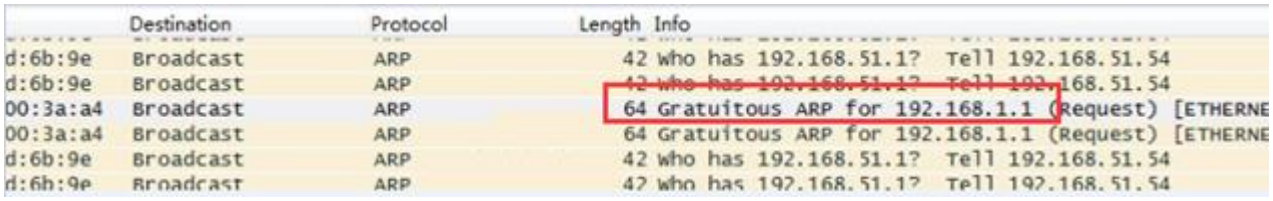
(2) Select the wired interface of the AP and click **Start** to capture the packets.



(3) Connect the wired interface of the PC to the AP Ethernet port that is not powered on.

(4) Power on the AP to view packets output by the packet capture software on the PC. Pay attention to the ARP packets.

Because the PC is directly connected to the AP, all the ARP packets except those sent by the PC are ARP packets sent by the AP.



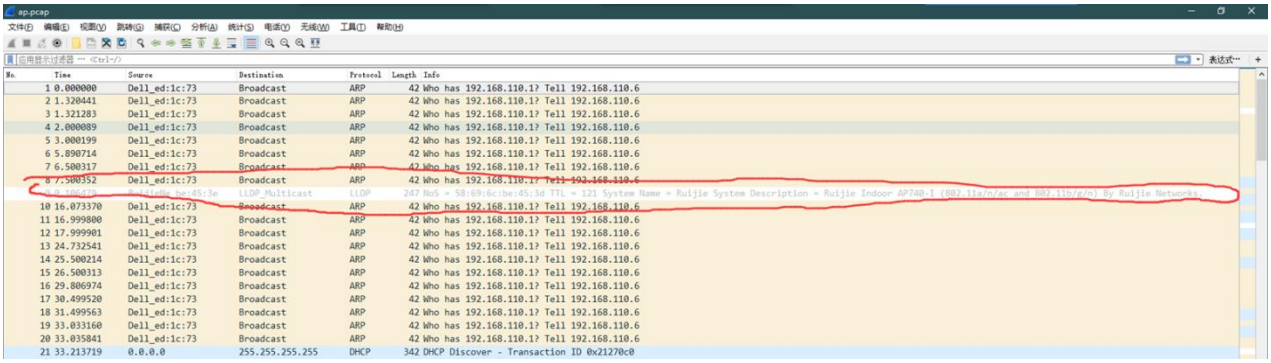
(5) After getting the AP IP address from the ARP packets, try to log on to the AP through the Telnet port.

(6) The AP may not send the ARP resolution packets. In this case, you can use the LLDP packets to obtain the AP management address. The Management Address in the LLDP packets is the management address of the AP.

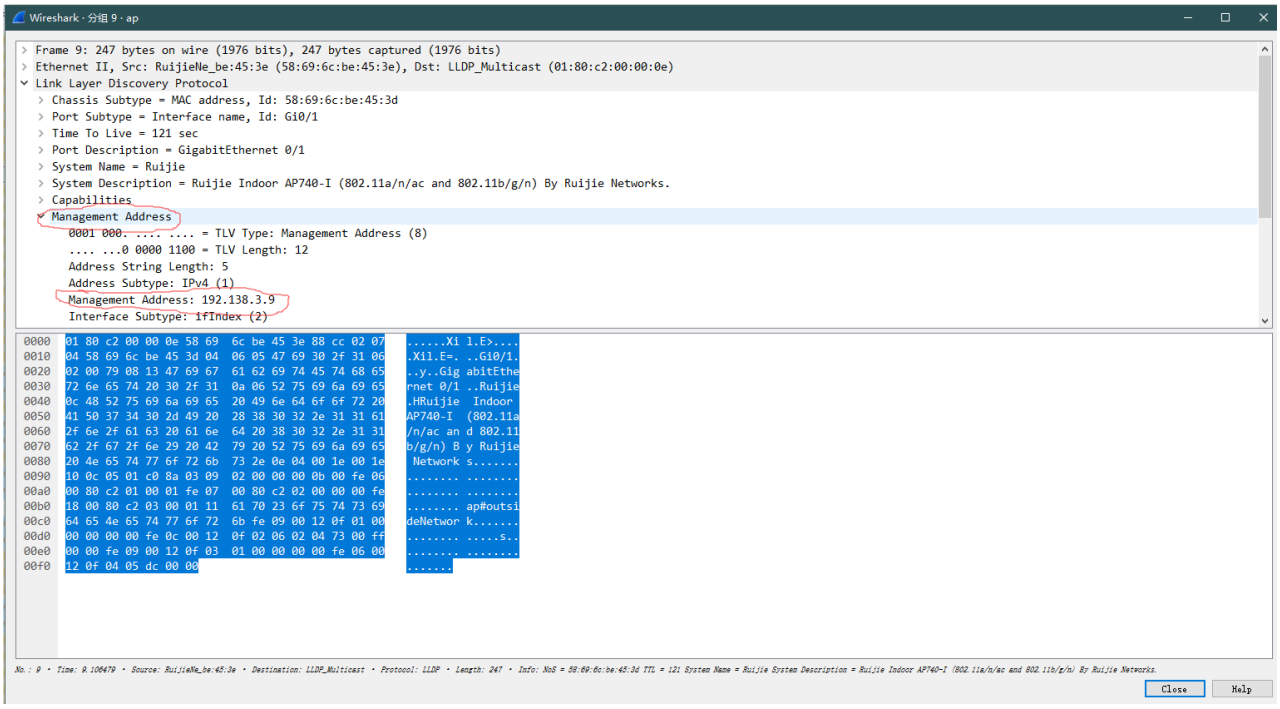
(7) If you still cannot log on to the AP, restore the factory settings of WALL-AP, which results in loss of all configurations. You can try to log on to APs with the Console port from a serial port.

It is found that during actual packet capture, the AP often does not send the ARP resolution packets. In this case, you can use the LLDP packets to obtain the AP management address.

1. The following is a packet capture screenshot:



2. Click to open the LLDP packet. The part in the red frame below is the management address of the AP:



2.4 How to fix when the system can output information but cannot be operated during CRT-based logon through the Console port?

1. Symptom

According to the AP320-I users, in case of logon through the Console port, there is information prompted, but no response is returned after Enter is pressed. Besides, no command can be entered.

2. Network Environment

The AP is new and just installed. It is logged onto through CRT.

3. Troubleshooting Steps

(1) Check whether the CRT or the HyperTerminal is used. If CRT is used, uncheck CTS/RTS.

(2) If an additional cable is used, confirm whether the driver is installed correctly.

(3) Change the baud rate. The baud rate for the version 1T8 is 115200 bps.

(4) Change the console cable and the PC.

4. Solution

Uncheck CTS/RTS.

5. Summary and Precautions

Summary: Other faults caused by the CRT traffic control function.

(1) You cannot use CRT to log on to the console.

(2) After CRT-based logon, the operation window is blank, the system outputs no information but the cursor flashes. The system has no response after you press Enter.

(3) After CRT-based logon, the operation window is blank, the system outputs no information but the cursor flashes. After you press Enter, the cursor moves but the system still outputs no information.

(4) After CRT-based logon, the system outputs information, but has no response after your press Enter and does not allow you to perform any operation.

(5) After HyperTerminal-based logon, the Data Traffic Control in COM attribute settings must be set to **None**.

2.5 How many APs can different AC Model manage?

Model	Default	Maximum
WS6008	32	224
WS6108	32	320
WS6024	24	24
WS6812	128	1024
WS6816	128	2560（WALL AP <=4000）
RG-M8600E-WS-ED	128	2560（WALL AP <=4000）
RG-M18000-WS-ED	128	2560（WALL AP <=4000）
M6000-WS	32	128

A WALL-AP occupies only 0.5 license. "<=4000" means up to4,000 WALL-APs are supported.

Run the **show ac-c** command in AC to display license occupation information. The meaning of four, normal, half, and zero is described below.

four: The AP occupies four licenses. Currently, only APs of the model AM5528 and AM5528(ES) occupy four licenses each. APs of the model AM5514 only occupy two licenses each.

normal: An ordinary AP occupies only one license, including AP220-E, AP320-I, and AP520.

half: A WALL-AP occupies only 0.5 license.

zero: The AP occupies no license. The AP is AP(MAP552(SR)) and APD-M.

2.6 How to view the number of licenses occupied by different AP model on AC?

AC#show ap-config product

Product ID	Hardware Version	Count	Used Wtp
AM5528	1.00	245	980.0
AP520	1.00	906	906.0
AP630(IDA)	1.50	33	33.0
AP630(IODA)	1.00	83	83.0

2.7 How to migrate a wireless AC license to another device (unbinding license)

(1) Upgrade the device version to RGOS 11.1(5)B9 or a later version.

For authentication code:

Run the **AC(config)#no set license *activation-key*** command to unbind the authorized code. (The activation-key is a 32-bit activation code.)

For authentication file:

Run the **AC#license unbind authorized file name** command to unbind the authorized file to get the verification code.

You can run the **show license unbind-code** or **show apmg debug unbind** command to display the verification code.

Note: after activation code of the unbound license is deleted, the license cannot be installed on the device again.

(2) Submit the device serial number, the license activation code, and verification code on Ruijie authentication system(http://pa.ruijie.com.cn:8001/main_wireless.jsf) to unbind the license on the authorization system. Contact Ruijie TAC to approve the unbinding.

(3) To bind the license again, submit the serial number of the new device and authorization code to register the license. A new activation code is obtained.

(4) Install the new activation code to the new AC.

For More details, please refer to *WLAN License Activation Guide:*

2.8 Can multiple temporary licenses be imported to the same device?

You can apply for a temporary license for an AC three times. The application is automatically reviewed and approved. Only one temporary license of the same specifications can be imported into an AC. The second license overwrites the first.

Multiple temporary licenses of different specifications can coexist in one AC. For example, when two temporary licenses can manage 32 APs are applied for the same AC, only one license can be imported to the AC. When a license can manage 32 APs and a license can management 128 APs are applied for the same AC, both licenses can be imported to the AC.

2.9 How to bind a license on VAC

(1) When VAC deployment is not finished yet, the procedure is same to that of normal AC

(2) When VAC deployment is finished, the procedure is basically the same. Bind the corresponding license authorization code to the device according to its serial number.

For authentication code, use **set license** command to bind the authentication code on main AC.

For authentication files, all the authorization files must be imported to the main AC and operated by running the following commands.

AC#license auto-install flash: LIC-WLAN-AP-51200000001765223.lic

The authorization files can be automatically uploaded.

If the authorization file is operated on the standby AC, the message "% Can’t execute this command in redundancy slave" is prompted.

(3**) AC#license install** means that the authorization file is only installed in this host.

2.10 Will APs go offline immediately if the license is unblind from AC?

No. The AP will not go offline unless it goes offline actively or the AC is restarted. As long as the current AP does not actively go offline and the AC is not restarted, the AP will always be online.

2.11 Will online Aps be kicked offline when the licenses are insufficient after temporary authorization expires?

No. APs will not be kicked offline due to deletion of temporary or formal authorization. The system judges whether the licenses are sufficient only when the AP is getting online. APs that go offline after authorization expire cannot go online again.

3 General Wireless Functions

3.1 Wireless Fit AP Deployment

3.1.1 The CAPWAP tunnel cannot be created.

(1) Communication between the AP and the AC is abnormal.

The AP fails to get the IP address.

The AP fails to get the Option 138 field.

The AP fails to ping the AC to create the tunnel.

The CAPWAP UDP ports 5246 and 5247 are discarded or filtered out by an intermediate device.

(2) The AC and AP are in abnormal status.

The AP cannot go online due to a high AC CPU usage.

show cpu

The AC license is insufficient.

show ac-config

show license

show ap-config summary

The AC and AP version span is large (recommend to use same version for AP and AC).

The AP name is not unique.

19 16:37:19: CD-AC4 %APMG-6-AP_ADD: Add AP(1414.4b5d.03af) fail. Online-AP(1414.4b5d.097f) with **same name(XS10A4-1)** has exist in this AC

Modifies name of online AP.

Collect the following information and contact Ruijie TAC.

(1) Collect the following information on the AC:

show version

show running

show ac-config

show license

show ap-config summary

show capwap sta

show cpu

show memory

show ip route

show ip interface brief

(2) Collect the following information on the AP:

show version

show ap-mode

show capwap sta

show ip route

show log

show capwap client state

3.1.2 How to check the reason why the AP is rejected from going online.

When the link is normal and the AC has received the packet from the AP but the capwap tunnel cannot be established between the AP and the AC, run the ***show ap-config summary deny-ap*** command to display the specific cause or in combination with the logs displayed on the AC.

Ruijie#**show ap-config summary deny-ap**

Deny ap num: 1

Mac Address AP Name Reason

---------- ---------- ----------

1414.4b71.98a1 By conflict

By bind-ap-mac //The AP-MAC binding is rejected. The MAC whitelist bind-ap-mac is enabled on the AC but the MAC of this AP does not exist in ap-config.

By wtp-limit //Indicates that the maximum number of online APs has reached. A common cause is that the license is insufficient or the maximum number of online APs has reached. It is rarely caused by the wtp-limit configuration.

By conflict //Indicates that the AP name conflicts with the MAC name. It is because the AP name has already existed on the AC or other APs of this MAC are online or configured.

By deny-flag //The AC denies the AP to join it. A common cause is that deny-join is configured during networking and debugging.

By ap-auth //Indicates that the AP certification is restricted. Certification by the certificate, serial number or password is enabled on the AC but the AP does not carry any certification information.

By user-class //Indicates the APs belong to different classes. For example, SMB-AP can only access SMB-AC but cannot access ordinary ACs.

By overdue-ap //Indicates the AC has an expired AP. This problem is temporary generally. The AC will automatically clears expired APs and then the expired APs can join the AC again.

By master-ap-mac //Indicates that the satellite AP does not carry the master AP MAC. This problem is temporary generally and is caused by quick AP join during startup of the satellite AP.

By unknown //Indicates an unknown cause.

By radio num //Indicates that interconnection is not supported because the AP has too many RF interfaces. For example, the B7-version AC does not support AM5528.

By vendor id //Indicates that the interconnection is not supported because the AP of another vendor is used.

By new-ap-limit //Indicates that the number of the new APs reaches the upper limit. For example, WS5708 supports up to 100 B9-version APs of wave 2.

By local-limit //Indicates that the number of APs connected to the AC is limited due to the AC protection in VAC scenario. It is possibly because the switch load is unbalanced or the working ACs are insufficient.

By hot-backup //Indicates a hot-backup limit. For example, the AP uses the AP virtualization technology which does not support the hot-backup function. But hot-backup is enabled for this AP in the configuration.

By total-ap-num //The total number of APs (online + offline) and AP tunnels has reached the upper limit. Delete unwanted offline APs.

By none-radio //The AP is rejected because it does not carry radio. This problem is temporary generally and is caused by quick AP join during startup.

When the packet interaction between the AP and the AC is abnormal, capture packets from the intermediate line to locate the packet loss point and troubleshoot the wired network.

3.1.3 The AC cannot distribute the configuration to the AP.

[Symptom]

The AC cannot distribute the configuration to the AP.

[Environment]

The AP goes online to the AC across the public network.

[Possible Causes]

(1) The AP does not go online.

(2) The software version conflicts.

(3) The extranet is restricted.

(4) The software has a fault (due to causes such as large version span).

[troubleshooting Steps]

(1) Remotely view whether the AP version is consistent with the AC version and whether the AP has gone online successfully.

(2) Run the **show ap-conf run** command to check whether the AP has joined the group and whether the active/standby configurations are consistent.

(3) Ping the AP to the AC. If the package size is 1500 bytes, the AC cannot be pinged. The dichotomic test result shows that the maximum package size that can be pinged is 1410 bytes. Modify the control tunnel MTU to 1410 to solve the problem:

ac-controller

capwap ctrl-mtu 1410

[Summary and Precautions]

In the cross-NAT go-online environment, the following problems may occur: the AC configuration cannot be issued, the tunnel cannot be established or is repeatedly established, and the terminal cannot be accessed. After troubleshooting, check whether the large-package communication between the AP and the AC is normal. For repeated tunnel establishment, check whether the NAT entry aging time of the egress is too short by testing the tunnel keepalive time.

3.1.4 In the cross-public-network scenario, only part of APs can go online on the AC.

[Symptom]

In cross-public-network mode, only part of APs can go online on the AC.

[Troubleshooting Steps]

(1) Check the network topology, wireless configuration and version.

A. Deploy the APs and the AC (a single AC, no active-standby ACs) across the public network. In hot-backup mode, check whether configurations of the active and standby ACs are the same. Configurations of normal APs and failed APs are exactly the same and the **bind-ap-mac** configuration is not set.

B. Requests of local users are locally forwarded, and gateway of APs and wireless users and the DHCP address pool are on the local aggregation switch. Troubleshot the local device.

C. The AC, normal APs and abnormal APs are all of the latest version, and online APs are of the same model. It means that the problem is not caused by the version and public network line of the carrier.

(2) Log on to the failed AP to check the AP mode and confirm whether any IP address is obtained. Check whether the large packet can be communicated on the tunnel used for the AP to ping the AC.

Onsite check finds that the failed APs are in fit mode, the IP address can be obtained, and the large packet can be communicated on the tunnel.

(3) After check, we do not find any configuration difference between the access switch and the normal and failed AP interfaces, and the switch is in normal status.

(4) Collect logs and debugs on the failed APs and the AC.

The failed APs are always sending discovery request packets. However, after the **show capwap statistics** command is run on the AC, the number of received discovery request packets does not increase. It is suspected that the discovery request packets are discarded by intermediate link. Since the APs go online cross the public network and there are normal and failed APs, the problem is not caused by the public network line. It may be caused by the local device.

(5) Check the local device topology, egress EG, aggregation switch, access AC, and APs and capture packets at the uplink interface of the aggregation switch. Discovery request packets of failed APs are found. It is suspected that the packets are discarded at the egress EG device. Because we cannot directly capture packets for analysis at the egress, it is suspected that the application cannot identify the packets or the packets are discarded because traffic of packets from the APs to the AC is too large, and thus some tunnels between APs and the AC cannot be created.

(6) Add the AP network segment to the egress device free of auditing and flow control, and place resources of users at this segment to the EG key channel for preferential forwarding. The test result shows that the failed APs can go online normally. After the resources are moved out of the key channel, the APs go offline after a period of time and cannot go online again.

[Cause]

Traffic on the key channel of the egress traffic control device is too large and thus the interaction packet for creating a tunnel between the AP and the AC is discarded.

[Solution]

Add traffic in the AP IP address segment to the key channel of EG egress, to ensure that the AP packets are preferentially forwarded.

[Other Operation Commands]

Ø On the AC, run the **debug apmg join** command to check whether the discovery request packet is received.

Ø On the AP, run the **debug capwap client fsm** command to check whether the packet is successfully sent.

Ø On the AP, run the **debug capwap packet** command to check whether the discover response packet is received. The prompt is displayed later.

If no response packet is received, run the following command on the AC:

debug efmp packet filter ipv4_sport range 5246 5247 counter 30

Ø If the AP tunnel cannot be created, run the following command on the AC to see whether a prompt is displayed:

debug efmp packet filter ipv4_sip host AP IP address ipv4_sport eq

10000 counter 10

run-system-shell

dmesg

Ø On the AC, run the **show capwap ap tunnel id detail** command to see the following information:

```
WS#show capwap 1 detail
CAPWAP process "capwap 1" with state [ Run ]
Process uptime is 0 days 16 hours 20 minutes 0 seconds
Echo interval is 5 secs, Dead interval is 15 secs Expire 11 secs
Current timers EchoInterval
Peer address 192.168.253.251
The MAC of AP is 5869.6c1b.0ae7
The Session ID of AP is 58696c1b.0ae7dc04.672dfe2e.195a9aac
Capwap fragment is enable
The Path MTU is 1400
Recent received request's sequence number 137
Recent received response's sequence number 117
Recent send request's sequence number 117
Retransmit Count 0, Failed DTLS Session Count 0
Max Retransmit Count 5
Config maxretransmit 5
Sending queue length 0, Receive queue length 0
Peer control port is 10000, data port is 10001
My address is 1.1.1.1
CTI ifx is 12.
IPv4 control socket 4, data socket 5
IPv6 control socket 6, data socket 7
Local IPv4 address is 192.168.253.251
UDP checksum is disable
Peer notify in NAT: NO
Data crypt capacity plain
Am I AP :NO
DTLS is Not connect
Am I sw ap: NO
```

If the data port changes frequently, the traffic table is aging. You are recommended to adjust the channel keepalive time to a smaller value.

ap-config xxx

echo-interval xx (default: 30s; minimum: 5s; maximum: 255s)

3.1.5 The AC and AP versions are the same but the AP cannot go online on the AC and the progress stops at Join.

[Symptom]

The AC and AP versions are the same but the AP cannot go online on the AC.

[Analysis]

1. View the log to check the CAPWAP tunnel status of the AP. The result shows the AP has communicated with the AC and its status after the join status is:

   DTLS Teardown;

   *Jan1 00:01:10: %CAPWAP-6-STATE_CHANGE: (peer - 1) [1.1.1.1] capwap state changed, from <DTLS Setup> to <Join>

   *Jan1 00:01:10: %CAPWAP-6-STATE_CHANGE: (peer - 1) [1.1.1.1] capwap state changed, from <Join> to <DTLS TearDown>

2. After confirming the link between the AC and the AP is normal, run the **show ap-config summary deny-ap** command. The result shows that the fault reason is "By conflict", which means the AP name is not unique in the system and thus the AP cannot join the AC.

```
JH_M8600WS_Master#show ap-c summary deny-ap
Deny ap num: 5
Mac Address    AP Name                                  Reason
-------------- ---------------------------------------- ----------------
5869.6c89.61f0 yk_rsyl_ap2                              By conflict
5869.6c5d.2739 yk_rsykzb_3fap2                          By conflict
5869.6c89.61a0 yk_rsjz_ap1                              By conflict
5869.6c89.5b8c yk_rsyl_ap1                              By conflict
5869.6c88.e996 yk_rsykzb_2fap2                          By conflict
```

3. After you restore the default settings of the AP or change its name, the AP goes online successfully.

[Summary]

During the go-online process of the AP, the CAPWAP tunnel status is idle-->discover-->DTLS Setup-->Join-->config-->Data Check-->Run respectively. When the CAPWAP tunnel reaches the Run status, the AP has gone online successfully.

If the progress stops when the CAPWAP tunnel reaches the Join status, run the **show ap-config summary deny-ap** command to display the reason for access denying (the reason is not displayed when the AC version is 11.x and the AP version is 10.x due to a large version span).

The following are common causes for that the progress stops when the CAPWAP tunnel reaches the Join status:

(1) The AP name conflicts.

(2) The versions are inconsistent.

(3) The license is incorrect.

(4) The line has a fault.

(5) The AC has security restrictions, for example, bind-ap-mac.

3.1.6 An offline AP is still displayed as "Online" on the AC.

[Symptom]

An offline AP is still displayed as "Online" on the AC.

[Analysis]

(1) Run the **show run** and **show ap-configrun** commands to display the configuration and check whether echo-interval is changed. (The default value is 30s.)

2. The result shows that the parameter value is still the default value. On the AC, run the **show capwap index detail** command several times. The keepalive value remains unchanged. It is suspected that the AP status is not updated on the AC because the keepalive function is disabled. Run the **show capwap [ip addr] detail | inc Echo** command. The result shows that the echo-interval is 0s.

AC-branch(config-ap)#show capwap 10.121.121.129 detail | in Echo

Echo interval is 0 secs, Dead interval is 0 secs Expire 4294967237 secs

3. Run the **show cli record** command to display the AC historical command records. The result shows that echo-interval disable is set for the AP-Group of the AP. Delete the configuration, the problem is solved.

[Summary]

This fault is caused by incorrect configuration of the hidden command. echo-interval disable is used to disable the echo function of the CAPWAP tunnel. After configuration, the AP echo function is disabled and the status of the AP is still displayed as "Run" after the AP goes offline. Besides, echo-interval disable is not displayed in the **show run** command.

The default echo interval between an AP and an AC is 30s. If the AC does not receive any echo packet from the AP within 30s, the AP goes offline.

The AP keeps alive the tunnel by sending an echo request every 30s. After receiving the echo request, the AC sends an echo response. If receiving no echo response within a certain period of time, the AP resends the echo request. The first retransmit starts at the 3rd second. When the time reaches the half of the echo interval, the AP deems that the tunnel is disconnected. The AP performs five retransmits within the 30s echo interval, that is, the 3rd second, 6th second, 12th second, 15th second, and 15th second.

Even if the echo interval is changed to another value, the calculation method for the retransmit time and count is still the same. The echo interval range is 5-255s, which is configured by the **echo-interval ***command in AP or AP group configuration mode.

3.1.7 Most APs cannot go online, online APs often go offline and the tunnel status frequently changes.

I. Symptom

Most APs cannot go online, online APs often go offline and the tunnel status frequently changes.

II. Troubleshooting Steps

(1) Check the network topology, wireless configuration, version, and log.

The version configurations are consistent.

Oct 16 00:24:27: %CAPWAP-5-RETRANS_MAX: (*2) (peer - 47) [172.17.6.30 : 10000] reach maximum retransmit count [5], msg is [configuration update request], seq is [1], elem length is [34].

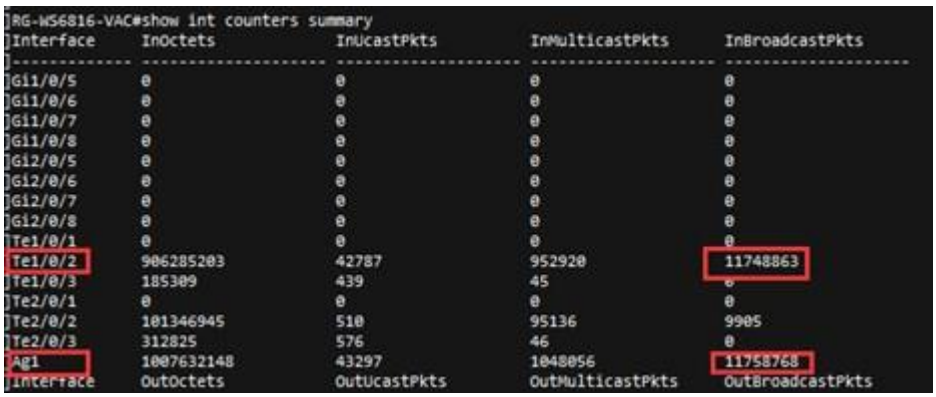
Oct 16 00:24:27: %CAPWAP-6-PEER_NOTIFY_DOWN: (*2) Peer <172.17.6.30 : 10000 : 5869.6cea.d18d> DOWN, reason <Retransmit MAX>.

The intermediate line may have a fault.

(2) Log on to the failed AP to check the AP mode and confirm whether any IP address is obtained. Check whether the large packet can be communicated on the tunnel used for the AP to ping the AC.

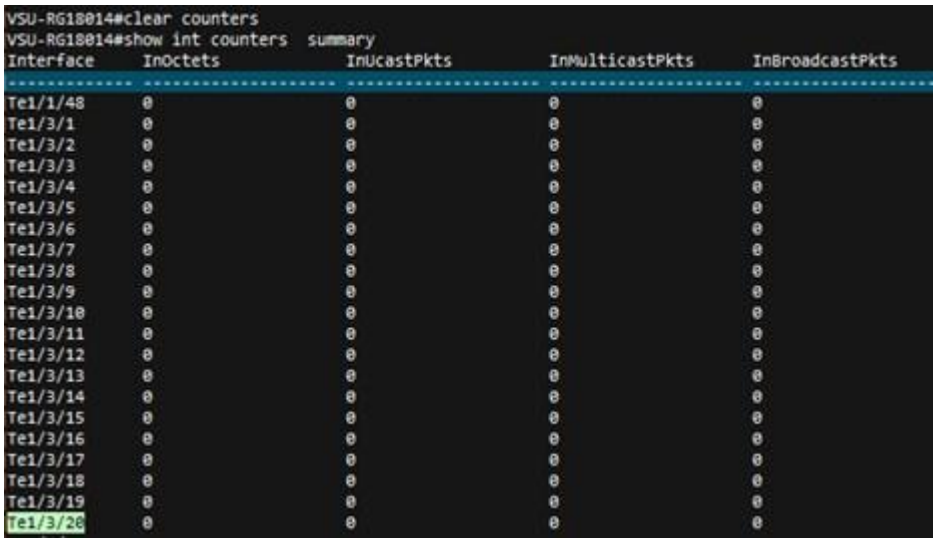
Packet loss is rare during AC ping on the AP. The intermediate line may have a loop or the broadcast traffic is too large.

(3) Log on to the AC and run the **clear counters** command to clear the interface traffic statistics. After **show int counters summary** is collected for three consecutive times, the broadcast packets at the interconnected interface increases quickly, as shown in the following figure:



```
RG-WS6816-VAC#show int counters summary
Interface     InOctets            InUcastPkts         InMulticastPkts     InBroadcastPkts
------------- ------------------- ------------------- ------------------- -------------------
Gi1/0/5       0                   0                   0                   0
Gi1/0/6       0                   0                   0                   0
Gi1/0/7       0                   0                   0                   0
Gi1/0/8       0                   0                   0                   0
Gi2/0/5       0                   0                   0                   0
Gi2/0/6       0                   0                   0                   0
Gi2/0/7       0                   0                   0                   0
Gi2/0/8       0                   0                   0                   0
Te1/0/1       0                   0                   0                   0
Te1/0/2       906285203           42787               952920              11748863
Te1/0/3       185309              439                 45                  0
Te2/0/1       0                   0                   0                   0
Te2/0/2       101346945           510                 95136               9905
Te2/0/3       312825              576                 46                  0
Ag1           1007632148          43297               1048056             11758768
Interface     OutOctets           OutUcastPkts        OutMulticastPkts    OutBroadcastPkts
```

(4) Log on to the interconnected core devices and run the **clear counters** command to clear the interface traffic statistics. After **show int counters summary** is collected for three consecutive times, the following figures are displayed:



```
VSU-RG18014#clear counters
VSU-RG18014#show int counters  summary
Interface     InOctets            InUcastPkts         InMulticastPkts     InBroadcastPkts
------------- ------------------- ------------------- ------------------- -------------------
Te1/1/48      0                   0                   0                   0
Te1/3/1       0                   0                   0                   0
Te1/3/2       0                   0                   0                   0
Te1/3/3       0                   0                   0                   0
Te1/3/4       0                   0                   0                   0
Te1/3/5       0                   0                   0                   0
Te1/3/6       0                   0                   0                   0
Te1/3/7       0                   0                   0                   0
Te1/3/8       0                   0                   0                   0
Te1/3/9       0                   0                   0                   0
Te1/3/10      0                   0                   0                   0
Te1/3/11      0                   0                   0                   0
Te1/3/12      0                   0                   0                   0
Te1/3/13      0                   0                   0                   0
Te1/3/14      0                   0                   0                   0
Te1/3/15      0                   0                   0                   0
Te1/3/16      0                   0                   0                   0
Te1/3/17      0                   0                   0                   0
Te1/3/18      0                   0                   0                   0
Te1/3/19      0                   0                   0                   0
Te1/3/20      0                   0                   0                   0
```

```
VSU-RG18014#show int counters  summary
Interface     InOctets            InUcastPkts         InMulticastPkts     InBroadcastPkts
------------ ------------------- ------------------- ------------------- -------------------
Te1/1/48      0                   0                   0                   0
Te1/3/1       4390                2                   3                   44
Te1/3/2       0                   0                   0                   0
Te1/3/3       6245                1                   3                   55
Te1/3/4       0                   0                   0                   0
Te1/3/5       4133                3                   4                   30
Te1/3/6       0                   0                   0                   0
Te1/3/7       5313                4                   2                   39
Te1/3/8       956                 1                   0                   12
Te1/3/9       0                   0                   0                   0
Te1/3/10      9938                5                   2                   53
Te1/3/11      5636                3                   4                   47
Te1/3/12      2166                0                   2                   18
Te1/3/13      1071                3                   1                   8
Te1/3/14      6301                1                   4                   56
Te1/3/15      4412                5                   2                   38
Te1/3/16      4496                3                   3                   41
Te1/3/17      4664                2                   3                   38
Te1/3/18      12609               3                   16                  77
Te1/3/19      5716                3                   4                   54
Te1/3/20      593079485           6366                167837              3226569
Te1/3/21      0                   0                   0                   0
Te1/3/22      5051                0                   6                   44
```

A great amount of broadcast packets increase at the Te1/3/20, indicating that a loop may exist.

(5) After confirming that the device connected to the Te1/3/20 interface is the AP of the access switch, down the Te1/3/20 interface to check whether all the APs under the Te1/3/20 interface go online one after another and the network is recovered.

(6) Log on to the access switch and enable RLDP. It is found that one interface is in down state. Check connection status of the associated device. The result shows that the switch is a private switch and has a loop.

III. Cause

The switch connected to the access switch has a loop at a single port.

IV. Solution

shutdown the loop interface.

V. Summary

(1) When a tunnel cannot be established or is established repeatedly for some APs, a loop may exist. Even if no loop exists, packet loss is impossible when you ping the AC on the AP.

(2) After a similar fault occurs, check the fault scope and active-standby configuration consistency.

(3) If the load balancing policy is incorrectly configured in VAC, the AP may often go online and offline frequently or cannot go online.

(4) In case a loop exists, enable the tree generation or RLDP function and query the switch logs to check the information of the failed port having the loop.

3.1.8 Troubleshooting Method and Fault Information Collection for Tunnel Establishment Failure Due to the AP Fault

Troubleshooting Method and Fault Information Collection for Tunnel Establishment Failure Due to the AP Fault

(1) Check the module and version of the AP and AC, and networking topology and solution.

(2) Run the following command to check whether the communication on loopback0 (or capwap ctrl-ip x.x.x.x) between the AP and the AC is normal:

(3) Check the logs on the AP and AC and collect the debug information about the AP and AC.

Log on to the AP:

show log //Collects the AP logs.

more ap_down.txt //Displays the cause for AP offline.

show capwap statistic //Collects the AP tunnel establishment status information. The information can be collected for multiple times, up to consecutive three times.

show capwap client state

//When the AP does not identify efmp, enable debug efmp for the run-system-shell configuration.

run-system-shell cd sbin

./efmp_demo &

exit

Collect the Debug Information

terminal monitor

debug capwap client fsm

debug capwap packet

debug efmp packet filter ipv4_sport range 5246 5247 count 30

Log on to the AC:

show log

show ap-config summary deny-ap

terminal monitor

debug capwap [apip] packet

debug apmg join

debug efmp packet filter ipv4_sport eq 5247 ipv4_sip host [apip] count 10

(4) If no log or debug information is returned from the device end, troubleshoot the intermediate line. Run the **traceroute ip tunnel ip source [apip]** command to trace the tunnel IP address record route on the AP to view which devices the AP packet has passed.

(5) Perform segmented packet capturing in the dichotomic method to check the sending and receiving of the packet that is used for establishing a tunnel between the AP and the AC and locate the packet loss point.

3.1.9 Can the AP and the user be in the same VLAN in the fit AP local forwarding mode?

Yes. The following configurations must be set:

Ruijie(config)# ap-config ap-name

Ruijie(config-ap)# ap-vlan vlan-id (The vlan-id must be the ID of VLAN of the AP and wireless user and must be configured; otherwise, the wireless user cannot obtain the IP address.)

ap-vlan command parsing: In local forwarding mode, the vlan-id configured by this command must be same to that allocated by STA. The actual VLAN of STA is assigned by the access switch of the AP instead of the VLAN configured by this command or assigned by the vlan-group. If the ap-vlan command is not configured, VLAN 1 is used by default.

Note: In local forwarding mode, even when the wireless user resides on VLAN 1, ap-vlan id must be configured on the AP. Otherwise, the wireless user can obtain the IP address of the AP network segment but cannot obtain the IP address of VLAN 1.

3.1.10 How to check whether the forwarding mode is local forwarding on the AP?

Run the following command on AP 11.x:

Ruijie#debug fwd dump-mode

wlan 1 tunnel local

Besides, you can query the MAC address table of the connected AP interface on the access switch of the AP. In local forwarding mode, the MAC address table of the wireless user is displayed.

3.1.11 When the wireless user resides on VLAN 1 while the AP resides on another VLAN in local forwarding mode, the IP address of the AP VLAN is obtained by the wireless user?

When the wireless user resides on VLAN 1 in local forwarding mode, the ap-vlan of the AP must be configured on the AC.

Ruijie(config)#ap-config 5869.6c84.b278 ---5869.6c84.b278 is the AP name.

Ruijie(config-ap)#ap-vlan 11 ---11 is the AP VLAN ID.

3.2 Wireless Security Functions

3.2.1 Will own Ruijie APs be countered if the wireless AP countering is enabled?

No in fit mode but yes in fat mode.

The becon frame contains a friendly flag which is used to judge whether the AP is a friendly AP. If the APs are all associated with the Ruijie AC, the friendly flags are the same by default, and Ruijie APs are not countered. When the friendly flags are modified to be different, countering is enabled for APs on Ruijie AC. By default, the friendly flag for all Ruijie APs is the same and thus Ruijie APs are not deemed as rogue APs. The configuration method of the friendly flag is as follows:

```
Ruijie(config-wids)#device friendly-flags ?
  <1-4294967295>  1 ~ 4294967295
```

3.2.2 How to display rogue APs?

Run the ***show wids detected rogue ap*** command.

```
WuLiu-WS5708#sh wids detected rogue ap
---------------------- Rogue    AP    Information ----------------------
SSID                          BSSID              CHAN     RATE     S:N
RGWLAN_1T13_wireless          021a.a9c5.8931     157      54.0M    15:0
```

3.2.3 How to display all SSID in the environment?

Run the ***show wids detected all*** command.

```
WuLiu-WS5708#sh wids detected all
---------------------- DETECTED   ADHOC   Information -------------------
SSID                             BSSID              CHAN      RATE      S:N
---------------------- DETECTED   AP   Information ----------------------
SSID                             BSSID              CHAN      RATE      S:N
vlan41                           0627.1d05.2680     1         18.0M     37:0
chenfang_cf668_ssid50            061b.b18e.394b     1         18.0M     35:0
2b15-mib                         061b.b120.58e0     1         18.0M     57:0
2b15-mib                         d21a.a9c1.ec9e     1         54.0M     63:0
RGWLAN_1T13_wireless             061b.b120.6916     1         54.0M     26:0
RGWLAN_IT13_wireless_1X          0a1b.b120.6916     1         54.0M     26:0
wcy1234567                       5c63.bf3e.c8a2     1         18.0M     19:0
LO1                              001a.a9c1.eae4     1         54.0M     52:0
fanqx-fat-ap2.0                  321a.a9c1.e7c4     1         54.0M     83:0
wxw_cmcc_612                     42d0.f822.33b0     1         54.0M     18:0
wxw_cmcc_601                     42d0.f822.33b5     1         54.0M     20:0
lulihua_2t106                    8614.f822.33bb     1         54.0M     22:0
icbc_ruijie                      061b.b122.364e     1         18.0M     15:0
RGWLAN_2B15_iphone               061b.b120.67b8     1         36.0M     33:0
```

3.2.4 How to judge whether an AP is under countering?

1. Symptom

Users in Building 12 in old campus cannot be associated with China UNICOM-WLAN SSID. Users associated with this SSID are often disconnected and cannot visit the Internet.

Onsite Problem Locating:

In the dormitory with poor user experience, we found that after the computer is connected to China UNICOM-WLAN SSID, the SSID signal often disappears, the ping packet loss rate is high, and the computer is often disconnected from the Internet.

2. Possible Cause

The AP countering function is configured.

3. Troubleshooting Steps

We used a professional tool (Ominpeek) to capture packets in the corridor on the second floor. A great amount of deauthentication (Deauth) packets were found, as shown in Figure 1. We located the AP (MAC address: 9614 4B1B 34FA) of the broadcast Deauth packet and found that it is an AP of China Unicom. After searching on the AC, we found that the i-Share AP was deployed here, covering the surrounding six rooms. But the log shows that the AP does not send any Deauth packet. Then it is confirmed that it is not this AP that sends the invalid Deauth packet.

After analysis, we suspected that there was a rogue AP. The rogue AP sent dissociated Deauth packets to the associated users in the name of China UNICOM AP, as shown in Figure 2. According to signal strength comparison, the signal strength of normal packet was about 26%, while that of the Deauth packet sent by the rogue AP was 100%, as shown in Figure 3. Therefore, we confirmed the existence of the rogue AP and knew that the rogue AP was close to the test place, resulting in frequent disconnection of users within the coverage of this rogue AP from the WLAN.

Figure 1: Too many Deauth packets

Protocol	Percentage	Bytes	Packets
802.11 Ack	.607%	86,158	6,145
802.11 RTS	.749%	106,280	5,314
UDP	9.279%	1,317,282	2,243
802.11 Beacon	2.275%	322,894	2,031
802.11 Deauth	.239%	33,928	1,131
802.11 CTS	.069%	9,793	687
802.11 Probe Rsp	.617%	87,550	555

Figure 2: The rogue AP broadcasting Deauth packets in the name of China UNICOM MAC

6053	96:14:4B:1B:34:FA	Ethernet Broadcast	96:14:4B:1B:34:FA	*	11	100%	1.0	30	0.774114	3.956366	802.11 Deauth
6999	96:14:4B:1B:34:FA	Ethernet Broadcast	96:14:4B:1B:34:FA	*	11	100%	1.0	30	0.803632	4.759998	802.11 Deauth
9038	96:14:4B:1B:34:FA	Ethernet Broadcast	96:14:4B:1B:34:FA	*	11	100%	1.0	30	1.591501	6.351499	802.11 Deauth
11447	96:14:4B:1B:34:FA	Ethernet Broadcast	96:14:4B:1B:34:FA	*	11	100%	1.0	30	1.560242	7.911741	802.11 Deauth
13899	96:14:4B:1B:34:FA	Ethernet Broadcast	96:14:4B:1B:34:FA	*	11	100%	1.0	30	1.536886	9.448627	802.11 Deauth
15367	96:14:4B:1B:34:FA	Ethernet Broadcast	96:14:4B:1B:34:FA	*	11	100%	1.0	30	0.835872	10.284499	802.11 Deauth
16365	96:14:4B:1B:34:FA	Ethernet Broadcast	96:14:4B:1B:34:FA	*	11	100%	1.0	30	0.815100	11.099599	802.11 Deauth
17712	96:14:4B:1B:34:FA	Ethernet Broadcast	96:14:4B:1B:34:FA	*	11	100%	1.0	30	0.799638	11.899237	802.11 Deauth
18986	96:14:4B:1B:34:FA	Ethernet Broadcast	96:14:4B:1B:34:FA	*	11	100%	1.0	30	0.770739	12.669976	802.11 Deauth
19028	96:14:4B:1B:34:FA	Ethernet Broadcast	96:14:4B:1B:34:FA	*	11	100%	1.0	30	0.024885	12.694861	802.11 Deauth
20098	96:14:4B:1B:34:FA	Ethernet Broadcast	96:14:4B:1B:34:FA	*	11	100%	1.0	30	0.755135	13.449996	802.11 Deauth

Figure 3: Signal length of normal packets lower than that of Deauth packets

122	96:14:4B:1B:34:FA	Ethernet Broadcast	96:14:4B:1B:34:FA	*	11	13%	24.0	162	0.100250	0.100250	802.11 Beacon
139	96:14:4B:1B:34:FA	B8:46:96:6B:67:64	Xerox:21:00:00	CW	11	0%	24.0	34	0.032784	0.133034	802.11
429	96:14:4B:1B:34:FA	Ethernet Broadcast	96:14:4B:1B:34:FA	*	11	23%	24.0	162	0.274487	0.407521	802.11 Beacon
585	96:14:4B:1B:34:FA	Ethernet Broadcast	96:14:4B:1B:34:FA	*	11	26%	24.0	162	0.102387	0.509908	802.11 Beacon
598	96:14:4B:1B:34:FA	Ethernet Broadcast	96:14:4B:1B:34:FA	*	11	100%	1.0	30	0.009490	0.519398	802.11 Deauth
703	96:14:4B:1B:34:FA	Ethernet Broadcast	96:14:4B:1B:34:FA	*	11	26%	24.0	162	0.092876	0.612274	802.11 Beacon
716	96:14:4B:1B:34:FA	00:1E:4C:8D:93:55	96:14:4B:1B:34:FA	*	11	26%	1.0	156	0.011125	0.623399	802.11 Probe Rsp
717	96:14:4B:1B:34:FA	00:1E:4C:8D:93:55	96:14:4B:1B:34:FA	*+	11	26%	1.0	156	0.001753	0.625152	802.11 Probe Rsp
722	96:14:4B:1B:34:FA	00:1E:4C:8D:93:55	96:14:4B:1B:34:FA	*+	11	26%	1.0	156	0.003485	0.628637	802.11 Probe Rsp

4. Collecting the Fault Information

Locating the Rogue AP

During onsite survey, we found an AP of another carrier near the test place and the data light of this AP flashed very fast, indicating transmission of a great amount of data. This AP was suspected to be a rogue AP.

To confirm it, we powered off this AP and captured packets at the air interface on site. The result showed that the percentage of deauth packets decreased immediately from 0.239% to 0.031%, as shown in Figure 4.

Figure 4: Decreasing of deauth packets after the rogue AP is powered off

Protocol	Percentage	Bytes	Packets
802.11 Ack	.371%	56,644	4,046
UDP	17.039%	2,600,100	3,177
HTTP	18.050%	2,754,428	2,434
802.11 CTS	.139%	21,168	1,512
802.11 Beacon	1.156%	176,443	1,059
802.11 BA	.182%	27,778	817
802.11 RTS	.099%	15,100	755
HTTPS	.609%	92,858	343
Null SAP	.370%	56,411	335
802.11 Probe Rsp	.208%	31,742	187
TCP	.939%	143,217	182
802.11 Deauth	.031%	4,800	160
802.11 Null Data	.013%	2,044	73
DNS	.057%	8,700	65

Then, the users can be associated with the AP and access the WLAN. No ping packet is lost.

After the carrier's AP is restored, the problem occurs again. Therefore, it can be confirmed that the carrier's AP is a rogue AP and the AP countering function is enabled.

3.3 Wireless Rate Limit Functions

3.3.1 How to display the rate limit configuration

If the AC configuration is as follows:

wlan-config 1 ruijie

wlan-based per-user-limit down-streams average-data-rate 10 burst-data-rate 10

Method is shown as follow: (same for the AC and the AP)

Command description:

show dot11 ratelimit {wlan | ap | user }

wlan: Indicates displaying all rate limit information of all WLANs.

ap: Indicates displaying all rate limit information of all APs.

user: Indicates displaying all rate limit information of all users.

3.3.2 What is the unit of the rate limit parameter in the rate limit command?

8 kbps.

For example, to set the download rate to 80 kbps, the command is

Ruijie(config-wlan)#wlan-based per-user-limit down-streams average-data-rate 10 burst-data-rate 10.

3.3.3 Precautions for Rate Limit in Local Forwarding Mode

In local forwarding mode, you can only limit the download traffic but cannot limit the upload traffic from STA to STA, because the traffic from STA to STA passes through the express forwarding path only once.

3.3.4 Can rate limit be set for WLAN-based users in local forwarding mode?

No. Because rate limit configured by the **wlan-based total-user-limit** command is realized on the AC, the configuration is only applicable for WLAN-based users in centralized forwarding mode.

3.3.5 Does the AP support multiple rate limits?

AP supports multiple rate limits.

When wlan-based per-ap, ap–based total-user, and netuser are configured simultaneously, the final rate limit is the effect when these three configurations take effect at the same time.

3.3.6 Which rate limit mode has a higher priority on the AC?

The AC supports AP-based, STA-based, and WLAN-based rate limit modes. The modes are described as follows:

(1) The rate limit modes wlan-based per-user-limit, wlan-based per-ap-limit intelligent, ap-based per-user-limit, ap-based total-limit intelligent, and netuser all function on STA but only one of them can work on STA at a time. The priority is wlan-based per-user-limit > wlan-based per-ap-limit intelligent > wlan-based per-user-limit > ap-based total-limit intelligent > ap-based per-user-limit.

(2) The rate limit modes wlan-based total-limit, wlan-based per-ap-limit, and ap-based total-limit and the STA-based rate limit modes function on different objects and thus can take effect simultaneously,

3.3.7 What's intelligent rate limit?

AP in 11.x version supports intelligent rate limit. When wlan-based per-ap or ap-based total-user intelligent rate limit is configured, the AP intelligently assigns the total rate to all online users on average.

Command:

wlan-based per-ap-limit { **down-streams** | **up-streams** } **intelligent**

ap-based total-user-limit{ **down-streams** | **up-streams** } **intelligent**

Configuration Method:

Before configuring intelligent rate limit of a certain range, you need to configure the total rate limit in the range. Currently, the following two intelligent rate limit modes are supported:

In **wlan-based per-ap-limit** mode, the wlan-based total rate limit is configured for the WLAN of all the APs in the AC. If wlan-based per-ap-limit is configured and intelligent rate limit is enabled, all the APs intelligently allocate the total bandwidth to all the STAs in the WLAN on average.

In **ap-based total-user-limit** mode, a total rate limit is configured to the specified AP. If ap-based total-user-limit is configured and intelligent rate limit is enabled, this AP intelligently allocates the total bandwidth to all the STAs in this AP.

Example:

(1) When the per-ap-limit downlink rate limit of WLAN 1 on the AC is set to 1000 kbps and the intelligent rate limit is enabled, all the APs associated with WLAN 1 allocate 1000 kbps to all STAs of WLAN 1 on average. If five STAs are associated with WLAN 1, then the downlink rate limit is 200 kbps.

Ruijie(config)#wlan-config 1

Ruijie(config-wlan)#wlan-based per-ap-limit down-streams average-data-rate 1000 burst-data-rate 1000

Ruijie(config-wlan)#wlan-based per-ap-limit down-streams intelligent

(2) When the ap-based total-user-limit upload rate limit of AP 320 is set to 500 kbps on the AC and the intelligent rate limit is enabled, AP 320 allocates the 500 kbps to all STAs of AP 320. If five users are associated with AP 320, the upload rate limit of each user is 100 kbps.

Ruijie(config)#ap-config ap320

Ruijie(config-ap)#ap-based total-user-limit up-streams average-data-rate 500 burst-data-rate 500

Ruijie(config-ap)#ap-based total-user-limit up-streams intelligent

3.4 Wireless Web Authentication Functions

3.4.1 How to view the information of authenticated users in Web authentication mode?

WS#show web-auth user ?

all Process all users ------Displays all the authentication users.

escape Web-auth user escape ------Display escaped users who connect WeChat accounts to Wi-Fi through MCP.

ip User ip address ------Displays authentication information of an IP address.

mac User MAC ------Displays authentication information of an MAC address.

name User name ------Displays authentication information of a user.

3.4.2 How to force a web-auth user offline?

WS#clear web-auth user ?

all Process all users

ip User ip address

mac User MAC

name User name

Note: Before going online, the cleared terminal must be authenticated again.

3.4.3 How to display the HTTP redirection configuration

Ruijie#**show http redirect**

HTTP redirection settings:

server: 172.20.1.100 // Indicates the IP address of the Portal server.

port: 80

homepage: http://172.20.1.100:8888/eportal /index.jsp // Indicates the authentication homepage URL of the Portal server.

session-limit: 255

timeout: 3

Direct sites:

Address MASK ARP Binding

---------- ---------- ----------

172.18.10.1 255.255.255.255 Off // Indicates that the resources can be accessed without authentication.

Direct hosts:

Address Mask Port Binding ARP Binding

---------- ---------- ---------- ----------

192.168.20.1 255.255.255.255 Off // Indicates that users do not to be authenticated.

3.4.4 How to display Web authentication configurations

Ruijie#show web-auth portal

Portal Servers Settings:

Ip: 172.18.159.48

Key: ruijie

ref: 2

Ip: 172.18.159.46

Key: ruijie

ref: 1

portalv2 list show

Ip: 172.18.159.48

port: 50100

ref: 2

URL format: default

Status: Enable

Ip: 172.18.159.46

port: 50100

ref: 1

URL format: default

Status: Enable

3.4.5 How to display the template and port parameters configured by the device on the AC?

WS#sh web-auth template

Name: zzs2

BindMode: ip-mac-mode

Type: v2

Port: 50100

Ip: 2.2.2.2

Url: http://2.2.2.2/eportal/index.jsp

The Portal server uses the local port 50100 to monitor and authenticate non-response packets send by the device and uses the target port 2000 to send all packets to the authentication device.

NAS uses the local port 2000 to monitor all packets send by the Portal server and uses the target port 50100 to send non-response packets to the Portal server.

3.4.6 How does the traffic Detection of Web Authentication work

Traffic detection is enabled in Web authentication mode by default. When a user having passing Web authentication has no traffic passing through the device within the specified no traffic period, the device deems that the user has gone offline and kicks the user out.

AP 11.x supports global no traffic detection and wlansec no traffic detection. The wlansec no traffic detection has a higher priority. When wlansec no traffic detection takes effect, global no traffic detection does not take effect.

In global no traffic detection mode, if the user has no traffic in eight hours, the user is kicked off by default. The command is as follows:

Ruijie(config)# **offline-detect interval xx threshold yy**

xx indicates the time, which is an integer ranging from 1 to 65535, and the unit is minute. The default value is 8 hours.

yy indicates the traffic size, which is an integer ranging from 0 to 4,294,967,294, and the unit is byte. The default value is 0.

In wlansec no traffic detection mode, if the user has no traffic in 15 minutes, the user is kicked off by default. The command is as follows:

The wlansec no traffic detection has a higher priority. Therefore, users having no traffic in 15 minutes are kicked out in 15 minutes by default.

WS(config)#wlansec 7 -------It is the actual authenticated wlansec serial number.

WS(config-wlansec)#**web-auth offline-detect** ?

flow Configure no flow threshold

interval Configure no flow interval

3.4.7 Does built-in Web authentication support pushing advertisement without authentication or pushing advertisement after authentication?

No.

3.4.8 Can an account be logged on by only a single user in local built-in Web authentication mode?

No. To control the number of simultaneous logons to the terminal, a separate authentication server should be configured and the server should support this function.

3.4.9 the traffic keepalive detection is based on the user MAC address or user name in Web authentication mode?

It is based on the user MAC address.

3.4.10 What are the protocol and port used by wireless second-generation Web authentication?

The protocol is UDP.

The packet target port of the Portal server is port 2000, which means that the port used by the AC to send packets is port 2000.

3.4.11 Is wireless user data encrypted at the air interface in wireless Web authentication?

If only Web authentication is enabled, the data is not encrypted at the air interface. You can configure WPA2 to encrypt the data.

3.4.12 Can the Portal server IP address be configured to a domain name on the AC?

Yes. The URL should be added to the URL whitelist. On AC 11.1(5)b8 or a later version, you are recommended to run the **free-url url xx** command to make the configuration in global mode.

For example, run the **WS(config)#free-url url www.google.com** command to add www.google.com in the whitelist.

3.4.13 Does the AC support https redirection and which redirection port need to be configured?

Currently, only ACs of 11.1(5)B8p3, 11.1(5)B9P5, office-wifi and later versions support https redirection. The redirection ports 433 and 8433 must be configured as follows:

Ruijie(config)#http redirect port 443

Ruijie(config)#http redirect port 8443

3.4.14 If the terminal uses a static IP address in Web authentication mode, can the IP address of the terminal be uploaded to the server?

The AC 11.1(5)b8p3 and later versions allow you to run the ***dot1x get-static-ip enable*** command to upload the static IP address of the wireless terminal to the server.

3.4.15 How to bypass specific devices in Web authentication mode?

In some applications, after connecting to a wireless network, users can access some network resources (for example, intranet websites) without authentication. You can run the **http redirect direct-site x.x.x.x** command (**x.x.x.x** is the IP address of free-authenticated resources) to add the IP address of these websites to the free-authenticated network resource list.

3.4.16 How to fix when “the authentication device does not exist” error occurs during Web authentication?

After confirming that the AC is added to the server and the authentication key configurations are consistent, check whether the AC can ping the server and modify the source IP address of the Portal server and RADIUS server according to actual situation. Add the VLAN of IP addresses of servers that can be pinged.

Ruijie(config)#ip portal source-interface vlan 1

Ruijie(config)#ip radius source-interface vlan 1

3.5 The built-in Portal Web authentication page cannot pop up?

(1) Communication between the STA and the AC: The STA shall be able to learn the MAC address of the gateway. Run the **http redirect direct-arp** command to configure the direct communication ARP.

(2) The built-in portal server monitors port 8081 and **http redirect port 8081** is configured for the AC by default. The configuration cannot be deleted.

(3) The AC management address cannot be configured as free-authenticated address.

3.6 A timeout connection error is reported when the built-in portal web authentication fails.

(1) If the communication between the AC and the RADIUS server fails, check whether the routes are different because multiple IP addresses are set for the RADIUS server.

(2) No AC is added to the RADIUS server. Check whether the SAM is added with an AC.

(3) The RADIUS key configuration is inconsistent. Check whether the SAM is added to the AC for more than two times (the IP address of the uplink interface of the AC is added).

(4) The proxy is enabled for the Internet Explorer but the built-in Portal does not support the proxy. Disable the proxy of the Internet Explorer.

3.6.1 Error code analysis for User Offline in Second Generation Web Authentication Mode

01: The user actively goes offline.

02: The port is disconnected. On a wireless network, STAMG notifies STA to go offline. In this case, contact STAMG owner to locate the cause.

03: The service is unavailable mainly due to connection interruption.

04: Idle status times out. The user having no traffic is kicked out.

05: Session times out. The duration reaches.

06: The administrator resets the port or session to kick out users from the RADIUS server, kick out escaped users after restoring the Portal server, or run the clear command to delete users.

07: The administrator restarts NAS.

08: The port has an error and required to interrupt the session

09: NAS has an error and required interrupting the session.

10: NAS requires interrupting the session due to other reasons.

11: NAS is restarted accidentally.

12: NAS thinks there is no need to retain the port and interrupts the session.

13: NAS interrupts the session to allocate this port.

14: NAS interrupts the session to suspend the port.

15: NAS fails to provide the required service.

16: NAS interrupts the current session to call back the new session.

17: Information entered by the user is incorrect.

18: The host requires interrupting the session.

103: The IP or MAC address has changed or occupied.

115: The service is switched over.

122: The traffic is exhausted.

250: The low-traffic user is kicked out. It is a unique attribute of Ruijie AP and the cause is same to code 4.

500: Authentication times out. The RADIUS authentication packet is not responded within the time limit. This attribute is available for wireless wlog module and will be provided for SNC later.

501: Authentication is denied by the RADIUS server. This attribute is available for wireless wlog module and will be provided for SNC later.

502: The number of users on the device has reached the upper limit. This attribute is available for wireless wlog module and will be provided for SNC later.

3.6.2 Definition of errcode in the Portal Protocol

(1) When the Type value is set to 2, in ack_challenge:

ErrCode = 0: The AC informs the Portal server that the Challenge request is successful.

ErrCode = 1: The AC informs the Portal server that the Challenge request is denied because the portal packet has an error or the user does not exist on the AC.

ErrCode = 2: The AC informs the Portal server that the link is created. When another authentication request is sent after the user has passed authentication, errcode2 is returned.

ErrCode = 3: The AC informs the Portal server that a user is being authenticated and the request should be sent later. The AC has sent an authentication request to the RADIUS server but RADIUS server does not send response. If the Portal server sends req_challeage during this period of time, errcode3 is returned.

ErrCode = 4: The AC informs the Portal server that the user's Challenge request fails because the AC has an inner error.

Note: When the ErrCode is not 0, see the ErrID value to find the cause.

(2) When the Type value is set to 4, in ack_auth:

ErrCode = 0: The AC informs the Portal server that the user authentication is successful.

ErrCode = 1: The AC informs the Portal server that the user authentication request is denied because the portal packet has an error (due to incorrect req_id or portal attribute) or the RADIUS server returns the authentication rejection packet.

ErrCode = 2: The AC informs the Portal server that the link has been created.

ErrCode = 3: The AC informs the Portal server that a user is being authenticated and the request should be sent later.

ErrCode = 4: The AC informs the Portal server that the user's authentication request fails because of an error.

Note: When the ErrCode is not 0, see the ErrID value to find the cause.

3.6.3 The URL cannot be redirected

If this problem occurs, check whether the HTTP packet sent by the terminal is intercepted, processed, and redirected by the AC.

The following are common causes:

(1) The STA cannot access the Internet or communication is abnormal. You can add the STA to free-authentication test to check whether the terminal can obtain the correct IP address and learn the gateway ARP.

(2) The terminal cannot parse the domain name or the page cannot be redirected to the entered IP address. For example, if the access domain name or IP address is not in the direct-pass list of AC, the domain name must be able to be parsed.

(3) The user is not a free-authenticated user. Packets of free-authenticated users are certainly not interrupted by the AC.

(4) No user VLAN is configured for the AC and thus the packet is discarded by the AC after it is forwarded to the AC.

(5) An https IP address is entered but https redirection is not configured.

(6) The addresses conflict. The terminal of which the IP address is same to that of an online AP but the MAC address is different cannot be redirected. You can run the **web-auth sta-preemption enable** command to solve the problem.

(7) The web-auth dhcp-check is configured but ip dhcp snooping is not enabled on the AC.

(8) The portal server is not called under wlansec on the AC.

(9) The AC version is too low. Upgrade the AC to the latest version which is available on Ruijie official website.

3.6.4 The Portal page cannot popup.

(1) After obtaining the URL redirected by the AC, the terminal directly uses the URL to access the Portal page. If the Portal page is not displayed, check the interconnectivity between the terminal and the Portal Server. If the terminal can ping the Portal server, check whether intermediate devices filter out the http packets.

(2) The problem occurs when the parameter or format of the URL does not conform to the requirement of the Portal Server. Pay special attention during connection to a third-party server.

Some servers require checking the URL parameter or format, or specify the value of some parameter. Confirm whether the parameter or format is supported by the AC and the AC is configured accordingly.

3.6.5 The web-authentication user is forced offline.

(1) The dhcp snooping entry shows that the terminal IP address conflicts. In this case, authenticated users are forced to go offline.

(2) Different terminals use the same user name.

(3) The traffic keepalive time threshold reaches.

(4) When a user is disconnected from the wireless network for five minutes, the user's Web authentication entry is deleted by default.

(5) The accounting-update is not enabled or its configuration is different on the AC and the server.

(6) The user is forced by the server to go offline (due to the RADIUS extended attribute).

3.6.6 Web authentication fails and the server fails to receive auth_req response packets from the device.

Possible Cause:

The authentication request packet sent by the Portal server does not arrive at the AC and is discarded by intermediate devices.

Troubleshooting Method:

(1) When packets can be captured, create images for packets at uplink port of the AC to see whether the authentication request packet arrives at the AC. If not, when auth-req is resent by the Portal server, the AC returns ack_auth and the error code indicates that the user is being authenticated.

(2) The problem is generally because packets from the Portal server are not allowed to pass through due to firewall between the AC and the Portal server.

3.7 Wireless Bridge

3.7.1 How many bridges does AP630 support?

One root AP supports four none-root AP.

3.7.2 Is asso-rssi supported in a bridging environment?

No currently. The processing method in bridging mode is different from that when an ordinary terminal is connected to the underlying layer. The asso-rssi function is applicable for wireless users in normal access mode.

3.7.3 How to clear non-root AP configurations?

When the AP is online, run the following command:

ap-config xx

station-role root-ap radio 2

Or

ap-config xx

wds pre-config delete

The command must be run when the AP is online.

3.7.4 What are precautions for multi-hop bridging?

In multi-hop bridging mode, to guarantee the bridging link quality, channels for each of hops must be different.

For example, set channel 60 for the first hop, channel 100 for the second hop, and channel 149 for the third hop.

3.7.5 What is the signal strength requirement to guarantee the bridging link and video transmission quality?

Use the multi-hop bridging scenario in AP630 series products as an example.

The bridging uplink of the root bridge is called as the main link. To ensure the main link stability, the uplink RSSI must be **at least 30.** The link between the root bridge and a non-root bridge is called as a single link. To ensure the single link stability, t**he uplink RSSI must be at least 25**. If the signal strength is lower than the specified value, adjust or change the AP location, to avoid that the video cannot be transmitted due to too low bridging performance caused by weak signal.

3.7.6 How to fix when modification to the non-root AP do not take effect on the AC?

All the commands for modifying the non-root bridge configuration take effect only after the **wds config commit** command is run.

In **ap-config** mode, run the **wds config [clear | commit] radio radio-id** command. The parameters are described below:

clear: Clears WDS configuration that does not take effect.

commit: Commits WDS configuration that does not take effect. After the operation, the bridge is disconnected and then connected.

radio radio-id: Indicates the radio ID configured on the AC.

If the AP is in non-root mode, its radio enters the wds edit mode. At this time, most of wds commands do not take effect immediately. You can run the show ap-config wds-config command to display the configurations. After confirming that the configurations are correct, run this command to commit the modification.

3.7.7 Is local forwarding mode supported when fit AP630s are bridged? Can multiple VLANs be bridged transparently?

Yes. The root bridge AP and non-root bridge AP must bridge VLANs transparently (run the **bridge-vlan x** command in ap-config mode). Assuming vlanx and vlany are VLANs required by non-root APs, the configuration method is as follows:

ap-config *root bridge ap name*

bridge-vlan x

bridge-vlan y

exit

ap-config *non-root bridge ap name*

bridge-vlan x

bridge-vlan y

exit

3.8 Cross-AC Roaming Functions

3.8.1 How to check whether a user is roaming

On the AC, run the *show ac-config client detail* command. The user status is Roam.

AC#show ac-config client detail a088.b413.c754

Mac Address :a088.b413.c754

IP Address :::

Wlan Id :1

Vlan Id :111

Roam State :Roam

Associated Ap Information:

AP Name :AP-01

AP IP :192.168.97.10

3.8.2 View all roaming users

Ruijie# **show mobility user**

STA-MAC	IPv4-Address	IPv6-Address	WLAN	TYPE	ROC-VLAN	RIC-VLAN
00:26:0c:ef:6d:12	20.0.0.2		1	LC	2	2
00:40:0c:ef:6d:33	20.0.0.5		2	RIC	3	3
00:40:0c:ef:6d:44	20.0.0.6		3	ROC	2	4

LC indicates users roaming inside the AC. RIC indicates users roaming to the AC. ROC indicates users roaming from the AC.

3.8.3 What is Wireless Layer-2 Roaming

Wireless roaming is a process in which a wireless client switches from one AP to another AP of the same SSID.

Before and after Layer-2 roaming, the client resides on the same VLAN and the IP address remains the same.

Layer-2 and Layer-3 roaming in the same AC are enabled by default in Ruijie APs.

3.8.4 What is Wireless Layer-3 Roaming

Wireless roaming is a process in which a wireless client switches from one AP to another AP of the same SSID.

Before and after Layer-3 roaming, the client resides on different VLANs but the IP address remains the same.

Layer-2 and Layer-3 roaming in the same AC are enabled by default in Ruijie APs.

3.8.5 What is Cross-AC Wireless Roaming

Wireless roaming is a process in which a wireless client switches from one AP to another AP of the same SSID.

When the two APs are managed by two different ACs, the process in which the wireless user switches from one AP to another AP is called as cross-AC roaming.

In cross-ac roaming, a tunnel must be created between the two ACs (home AC and foreign AC) to switch the roamed data.

To enable cross-AC roaming, you must make relevant configurations on the AC. For details, see Roaming Configuration Cases.

3.8.6 Does fat AP support Layer-2 roaming?

No.

If all APs are in the same broadcast domain and all downlink clients use the same DHCP server to get the IP address, when a client is automatically associated with another AP, its effect is similar to roaming. At this time, the STA wireless network is temporarily disconnected and then reconnected to obtain the IP address. If STA gets the IP address from the same DHCP, the IP address obtained is same. It seems that the STA roams.

3.8.7 How to confirm whether a wireless user successfully roams?

If a wireless user successfully roams,

(1) The wireless network is not disconnected.

(2) The user's IP address remains unchanged.

(3) Only one to two packets are lost during roaming.

(4) On the AC, run the show ac-config client detail command. The user status is Roam.

AC#show ac-config client detail a088.b413.c754

Mac Address :a088.b413.c754

IP Address :::

Wlan Id :1

Vlan Id :111

Roam State :Roam

Associated Ap Information:

AP Name :AP-01

AP IP :192.168.97.10

3.8.8 What are precautions for deploying wireless roaming?

(1) The signal is not interrupted and signal between APs overlaps each other.

(2) The AP power must be appropriate.

(3) The adjacent AP channels must be different to avoid same frequency interference and packet loss.

(4) Move the wireless client during roaming test. Roaming fails when the AP is closed.

(5) Set the roaming aggressiveness of wireless NIC to the maximum.

3.8.9 How to reduce the client roaming frequency?

Client roaming depends on the signal strengthen and the distance between the client and the AP. There are two methods to adjust the client roaming frequency:

(1) Adjust the wireless transmit power of the AP.

(2) Adjust the roaming aggressiveness of wireless NIC to a lower value.

3.8.10 Does the STA roam when it switches signal between APs of same SSID but different WLAN-IDs?

Yes. The STA can roam in this situation

3.8.11 How to enable Layer-2 roaming on AP version 11.x?

There are two kind of Layer-2 roaming: roaming with roaming table entry and roaming without roaming table entry

In wireless AC 11.1(5)b8 and later versions, no Layer-2 roaming entry is generated by default. Which means the roaming user will be considered as a new user, the user cannot sense the roaming progress.

To generate the roaming entry in special cases, run the ***roaming layer2 with-entry*** command in global config mode.

Case study in which Layer-2 roaming is enabled (roaming entry needs to be generated):

Fault symptom: In local forwarding mode, connect the AP to the switch interface and enable Layer-2 roaming. The terminal roams between APs and re-authentication is required each time the terminal roams. When a Huawei wireless network is used, frequent re-authentication does not occur.

Fault analysis: Layer-2 roaming is enabled for Huawei wireless network. After Layer-2 roaming occurs, the data is transmitted to the home AP which contains the user authentication information at the uplink port. Thus, re-authentication is not required.

Solution: Run the r***oaming layer2 with-entry*** command in global mode to enable Layer-2 roaming and roaming entry generation for Ruijie APs.

3.8.12 Can Layer-3 roaming be disabled on the AC?

In AP 11.x (AC 11.1(5)b8 and later versions), Layer-3 roaming can be disabled by the following command:

ruijie(config)#roaming local-unroam Disables Layer-3 roaming in local forwarding mode.

ruijie(config)#roaming central-unroam Disables Layer-3 roaming in centralized forwarding mode.

ruijie(config)#no roaming support wlan x Disables Layer-3 roaming for a single WLAN.

3.8.13 Which port is used for roaming?

In cross-AC roaming mode, UDP 5248 is used. In local forwarding mode, the UDP 5249 is used. In Layer-3 roaming mode, when data roams, a virtual tunnel is created between the new AP and old AP, and the UDP 5249 is used.

3.8.14 How to view the roaming trace of terminal of which MAC address is xxx on the AC?

AC# show mobility user roam-track 520a.124a.0001

----- --------------- ---------------- ----------------------

ID AC-Info AP-Info Online-time(d:h:m:s)

----- --------------- ---------------- ----------------------

1 -HOME AC- 001a.a94e.d41E/2 0:00:10:49

2 -HOME AC- 001a.a94e.d42A/2 0:01:38:05

3 -HOME AC- 001a.a94e.d40d/2 7:02:18:07

Fields are explains as follows:

Field Description

ID Roaming sequence

AC-Info Information of the AC

AP-Info Information of the AP

Online-time(d:h:m:s) Online duration

3.9 Common 5G Preferential Access Problems

3.9.1 How to check whether the band-select function is enabled

Run the ***show band-select configuration*** command to see whether 5G preferential access is enabled.

```
Ruijie#show band-select configuration

Band Select Configuration
  Access denial.......................................... 2
  Probe Cycle Count...................................... 2
  Scan Cycle Period Threshold (milliseconds)............. 200
  Age Out Suppression (seconds).......................... 20
  Age Out Dual Band (seconds)............................ 60
  Acceptable Client RSSI (dBm)........................... -80
```

3.9.2 What are the influences when band-select is configured for AP?

AP does not respond to request from 2.4G frequency band before identifying STA. Thus, single-band 2.4G STA cannot detect WLAN in two second.

After AP identifies STA, dual-band STA does not respond to request of 2.4G frequency band but STA can still detect WLAN passively. In other words, some dual-band STAs can detect WLAN of 2.4G frequency band.

After AP identifies STA, dual-band STA responds to only one of N (which can be configured) authentication requests of 2.4G frequency band. Generally, if a dual-band STA detects that WLAN has the BSSID at both the 2.4G frequency band and 5G frequency band, when re-authentication request at one frequency band is not responded, it will try another frequency band. However, some dual-band STAs may always send authentication request to the same frequency band. Assuming that a dual-band STA sends M authentication requests to 2.4G frequency band before trying 5G frequency band, when N is larger than M, the STA can connect to 5G frequency band; otherwise, the STA connects to 2.4G frequency band. Whichever frequency band is used, if the dual-band STA try the 2.4G frequency band first, there is always min (M,N) requests are neglected, resulting in prolonged STA connection time. The prolonged STA connection time depend on the STA driver. For example, if STA sends authentication requests at an interval of 00 ms and four authentication requests are neglected, the STA connection time is prolonged by 400 ms.

3.9.3 What is the AP action when Band Select (5G preferential access) is enabled?

Before STA is identified:

AP does not respond to request of 2.4G frequency band.

AP responds to request of 5G frequency band.

After STA is identified:

Single-band 2.4G STA responds to only one of multiple requests and can connect to the WLAN.

Single-band 5G STA responds to all requests and can connect to the WLAN.

Dual-band STA does not respond to request of 2.4G frequency band but responds to 5G frequency band. It can connect to WLAN of 5G frequency band. It responds to only one of multiple requests from 2.4G frequency band and can connect to the WLAN.

3.9.4 Default 5G Preferential Access Parameters

Parameter	Default Value
Band Select	Disabled
Acceptable lower limit of STA RSSI	-80 dBm
Count of denies request of associating dual-band STA with 2.4G frequency band	4
Count of restrained STA	2
Aging scanning period of STA information	500 ms
Aging time of dual-band STA information	60s
Aging time of restrained STA information	20s

3.9.5 How to adjust 5G Preferential Access Parameters

Ruijie(config)# band-select acceptable-rssi value //Indicates acceptable lower limit of STA RSSI.

Ruijie(config)# band-select probe-count value //Indicates count of restrained STA.

Ruijie(config)# band-select scan-cycle period //Indicates aging scanning period of STA information.

Ruijie(config)# band-select age-out dual-band value //Indicates aging time of dual-band STA information.

Ruijie(config)# band-select age-out suppression value //Indicates aging time of restrained STA information.

3.10 Wireless Load Balancing

3.10.1 How to View the Flow Balancing Group

Run the **show ac-config flow-balance summary** command to display the flow balancing group.

```
show ac-config flow-balance summary
↵
Group          Threshold     AP NAME  ↵
-----------  --------------  -------------------------↵
name2          4*100kbps      ap1, ap2↵
↵
```

3.10.2 How to enable the flow-based load Balancing in local forwarding scenario?

In local forwarding mode, you can run the following command to enable flow balancing:

Ruijie(config-ac)#flow-balance-group radio-flow ?//Indicates the flow information of the flow balancing group reported by AP.

WORD Flow balance group name

Data packets in local forwarding mode do not pass through the AC and thus the AC cannot get the flow information. Load balancing must be judged by the traffic information reported by AP.

3.10.3 How many load balancing groups can an AC support now?

Up to 80 number-based balancing groups and 80 flow-based balancing groups.

3.10.4 How many APs at most can each load balancing group support?

10.

3.10.5 How to enable load balancing between AP radios on AC?

Under AP-config mode:

inter-radio-balance flow-balance enable //Based on flow

inter-radio-balance num-balance enable //Based on the number of users

You can configure the inter-radio load balancing parameters (optional) on AC based on actual requirements during network optimization.

Run the **inter-radio-balance flow-balance dual-band enable-load en-num threshold thrs-num** command to configure the enabling threshold of flow-based load balancing between radios of different bands. The lower the threshold, the easier the flow balancing can be enabled and the more even the flow is allocated.

Run the **inter-radio-balance flow-balance same-band enable-load en-num threshold thrs-num** command to configure the enabling threshold of flow-based load balancing between radios of same band. The lower the threshold, the easier the flow balancing can be enabled and the more even the flow is allocated.

Run the **inter-radio-balance num-balance dual-band enable-load en-num threshold thrs-num** command to configure the enabling threshold of number-based load balancing between radios of different bands. The lower the threshold, the easier the flow balancing can be enabled and the more even the flow is allocated.

Run the **inter-radio-balance num-balance same-band enable-load en-num threshold thrs-num** command to configure the enabling threshold of number-based load balancing between radios of same band. The lower the threshold, the easier the flow balancing can be enabled and the more even the flow is allocated.

3.11 Common Multicast Problems

3.11.1 How to adjust the wireless multicast packet sending rate

In fat mode:

Ruijie(config)#interface dot11radio 1/0

Ruijie(config-if-Dot11radio 1/0)#mcast_rate 54 ----->Adjusts the multicast rate to 54Mbps.

In fit mode:

Ruijie(config)#wlan-conf 1 wireless

Ruijie(config-wlan)#mcast_rate 54 ----->Adjusts the multicast rate to 54 Mbps.

3.11.2 How to configure the multicast-to-unicast function

The multicast-to-unicast function is used to make multicast video smoother.

Configuration reference:

(1) Enable the multicast routing protocol in a Layer-3 device in the same broadcast domain.

(2)

In fit (ap-config) mode, run the following command:

Ruijie(config)# ip igmp snooping ----->Enables igmp snooping for all VLANS. To enable this function for certain VLANs, run the **ip igmp snooping vlan 1** command.

Ruijie(config)#ap-config xxx

Ruijie(config-ap)# igmp snooping mcast-to-unicast enable

Ruijie(config-ap)# igmp snooping mcast-to-unicast group-range *ip-addr ip-addr* ----->(Optional) Defines the multicast-to-unicast scope.

In fat mode, run the following command:

Ruijie(config)#ip igmp snooping ----->Enables igmp snooping for all VLANS. To enable this function for certain VLANs, run the **ip igmp snooping vlan 1** command.

Ruijie(config)#ip igmp snooping mcast-to-unicast enable

3.11.3 Does AC support Layer-3 multicast?

No. But AC can transparently transmit Layer-2 multicast packets.

3.11.4 How to check whether CAPWAP multicast is enabled on AC or AP

Ruijie# **show ip multicast wlan**

Global multicast state: enable // Enables global multicast mode.

Multicast mode:multicast 239.0.0.1 // Enables CAPWAP multicast mode.