Ruijie Networks – Innovation Beyond Networks

Wireless Network Optimization Solution for Higher Education Sector V1.0

Revision History

Date	Change contents	Reviser
2017.02.01	Initial Release	TAC Oersea

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.

1 Abstract

This document details questions frequently asked during network deployment with reference to the use limit of the simplified network, to help after-sales personnel on deploying the simplified network solution and improve the deployment efficiency and quality.

Audience

- Network Engineers
- Network Administrator

Obtain Technical Assistance

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

Welcome to report error and give advice in any Ruijie manual to Ruijie Service Portal

Related Documents

- Wireless Network Optimization Solution for Higher Education Sector V1.0

2 Index Description

This document describes questions that frequently occur on the simplified network. The questions are categorized based on the question description. Certain type of questions are centralized answered. A specific index is not available. However, you can search the keywords using the shortcut keys Ctrl+F.

3 Contents

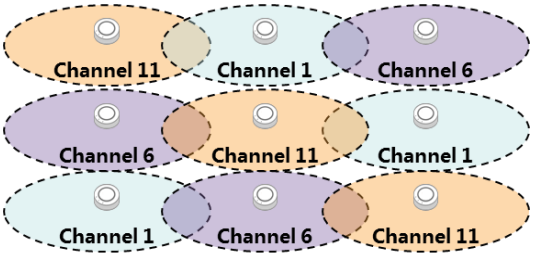
4 Wireless Network Optimization Solution for Higher Education Sector

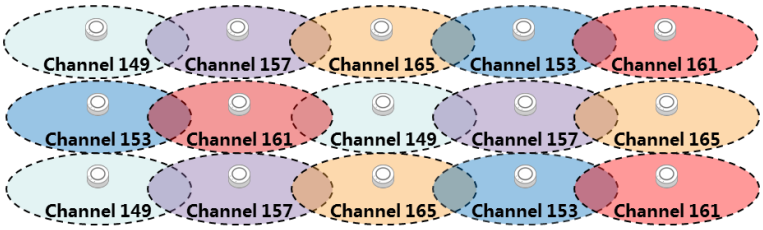
4.1 [Mandatory Configuration for Network Optimization of Higher Education Sector]

4.1.1 Make channel adjustment.

Proper channel adjustment and design help reduce frequency interference.

- When adjusting channels, take environmental factors (such as Ruijie APs, APs from other vendors, and personal hotspot Wi-Fi networks) into consideration. Stagger channels to reduce frequency interference.





Case of 2.4 GHz/5.8 GHz channel adjustment in University XX

Room No.	Channel	Corridor	Channel	Room No.		Room No.	Channel	Corridor	Channel	Room No.
3-101	1		6	3-102		3-201	11		1	3-202
3-103	11		1	3-104		3-203	6		11	3-204
3-105	6		11	3-106		3-205	1		6	3-206
3-107	1		6	3-108		3-207	11		1	3-208
3-109	11		1	3-110		3-209	6		11	3-210
3-111	6		11	3-112		3-211	1		6	3-212
3-113	1		6	3-114		3-213	11		1	3-214
3-115	11		1	3-116		3-215	6		11	3-216
3-117	6		11	3-118		3-217	1		6	3-218
3-119	1		6	3-120		3-219	11		1	3-220
3-121	11		1	3-122		3-221	6		11	3-222
3-123	6		11	3-124		3-223	1		6	3-224
3-125	1		6	3-126		3-225	11		1	3-226

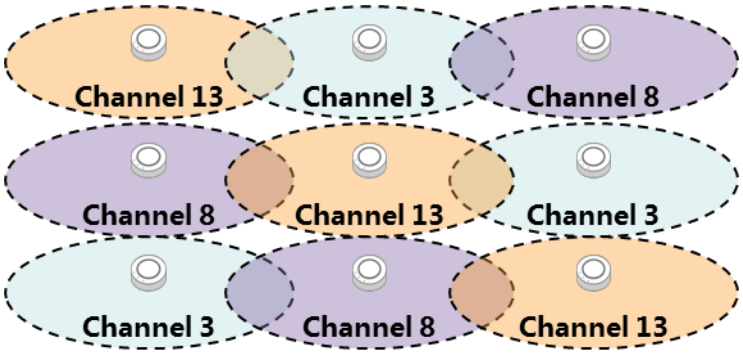
Room No.	Channel	Corridor	Channel	Room No.		Room No.	Channel	Corridor	Channel	Room No.
3-101	149		153	3-102		3-201	153		149	3-202
3-103	157		161	3-104		3-203	161		157	3-204
3-105	165		149	3-106		3-205	149		165	3-206
3-107	153		157	3-108		3-207	157		153	3-208
3-109	161		165	3-110		3-209	165		161	3-210
3-111	149		153	3-112		3-211	153		149	3-212
3-113	157		161	3-114		3-213	161		157	3-214
3-115	165		149	3-116		3-215	149		165	3-216
3-117	153		157	3-118		3-217	157		153	3-218
3-119	161		165	3-120		3-219	165		161	3-220
3-121	149		153	3-122		3-221	153		149	3-222
3-123	157		161	3-124		3-223	161		157	3-224
3-125	165		149	3-126		3-225	149		165	3-226

Note:

Even floors use the same channel adjustment method and odd floors use the same channel adjustment method.

- When there are considerable ISP private Wi-Fi networks, the conflict between Channels 1, 6, and 11 and other Wi-Fi channels cannot be prevented in most areas regardless of how Channels 1, 6, and 11 are adjusted. For the 2.4 GHz band, use three non-conventional channels: Channels 3, 8, and 13, to prevent conflict with Channels 1, 6, and 11 and with ISP signals, thereby effectively reducing co-frequency interference (adjacent-channel interference will be increased) and the entire interference.

  Note: A few STAs do not support Channel 13. In this case, upgrade software driver for rectification.



- When there are a few private Wi-Fi networks and Ruijie devices are densely distributed — the interference mainly comes from mutual interference between Ruijie APs. Use four non-conventional channels: Channels 1, 5, 9, and 13, to reduce interference. Disable the 802.11b rate set with the rate lower than 11 Mbps (excluding 11 Mbps) and disable the 802.11g rate set with the rate lower than 11 Mbps (including 11 Mbps), and **set 9 Mbps in the 802.11g rate set as the forcible rate.** In this way, the conflict among Channels 1, 5, 9, and 13 can be prevented. The configuration is as follows:

```
ac-controller
802.11b network rate 1 disabled
    802.11b network rate 2 disabled
    802.11b network rate 5 disabled
    802.11b network rate 11 mandatory
802.11g network rate 1 disabled
    802.11g network rate 2 disabled
    802.11g network rate 5 disabled
```

```
802.11g network rate 6 disabled
802.11g network rate 9 mandatory
802.11g network rate 11 disabled
802.11g network rate 12 supported
802.11g network rate 18 supported
802.11g network rate 24 supported
802.11g network rate 36 supported
802.11g network rate 48 supported
802.11g network rate 54 supported
```

Principle analysis:

The 802.11b rate set adopts the Direct Sequence Spread Spectrum (DSSS) modulation mode and 802.11b signals occupy 22 Mbps bandwidth. The 802.11a and 802.11g rate sets adopt the Orthogonal Frequency Division Multiplexing (OFDM) modulation mode and the signals occupy 20 Mbps bandwidth. The gap between channels of the 2.4 GHz band is 5 Mbps and the gap between Channels 1, 5, 9, 13 is 20 Mbps.

Channels 1, 2, 5, and 11 of 802.11g also adopt the DSSS modulation mode, so as to be compatible with 802.11b. Therefore, disable Channels 1, 2, 5, and 11 in 802.11b and 802.11g rate sets (Channel 11 in 802.11b rate set cannot be disabled due to configuration restriction but it will not exert any effect). Disable 6 Mbps in the 802.11g rate set and set 9 Mbps in the 802.11g rate set as the forcible rate — management packets are transmitted at the minimum forcible rate by default. This disables low-rate nodes and reduces interference.

Note:

Management packets are transmitted at 9 Mbps rate of the 802.11g rate set. As a result, STAs that support only 802.11b cannot associate with the wireless network, but a few STAs support only 802.11b in the market. **In addition, some STAs do not support Channel 13. In this case, upgrade the driver for rectification.**

4.1.2 Adjust the RF power.

Proper RF power adjustment helps prevent interference between devices.

Disable low rate sets (see the section of disabling the low rate) prior to power adjustment, so as to obtain more authentic results.

- Wall AP scenario in dormitories:

Wall APs are usually deployed in scenarios of dense dormitories. The interference between APs is very severe if the power is not adjusted properly.

Step 1: At the outmost edge of the normal coverage area of the AP (position that is within the normal coverage of the AP but has the lowest RSSI), use the wirelessmon software to scan the AP RSSI in this room. Adjust the transmit power of the AP to ensure that the RSSI at this point is about -65 dB (the receiver sensitivity varies a lot according to STAs and iPhone is used here).

```
(config-ap)#power local xxx radio 1
```

Step 2: Telnet to the AP and run the following command to display the actual transmit power of the AP:

```
show dot11 wireless 1/0 | include Actual Tx Power
Actual Tx Power.............. 13 dbm
```

Step 3: Repeat Step 1 and Step 2 to adjust the value of **power local** for the APs in the upper room, lower room, left room, and right room. Properly reduce the management packet power of the AP (the value of **coverage-area-control**). It is recommended that the value be 3-5 dB lower than the value of **Actual Tx Power** displayed after the **show** command is executed in Step 2. Disconnect and then reconnect the STA repeatedly. The probability that the STA associates with the AP in this room is up to 95% or higher. If this probability cannot be reached, properly reduce the value of **coverage-area-control** on the precondition that the coverage is normal (after the APs in the upper room, lower room, left room, and right room are all shut down, the STA can associate with the AP in this room successfully each time).

```
WS5708(config)#ap-config xxx
WS5708(config-ap)#coverage-area-control 8 radio 1  (13-5=8dB)
```

Note: In RGOS10.x, the **coverage-area-control** function is unavailable.

Description of the **coverage-area-control** command: The **coverage-area-control** command can be executed to configure the transmit power of management frames. Higher transmit power of management frames (excluding 0) indicates that the distance between a wireless user who is allowed to access and the AP is longer.

Step 4: After the power is adjusted for the 2.4 GHz band, raise the power for the 5.8 GHz band. For detailed adjustment method, see the 5.8 GHz user guide.

- i-Share 1 and i-Share 2 solution scenario in dormitories:

The major difference between the i-Share 1 solution and the i-Share 2 solution used in dormitory scenarios lies in large signal attenuation of device feeders in the i-Share 1 solution and i-Share 2 solution. Focus on the attenuation when adjusting **power local** (it cannot be set to a very small value). The adjustment method is as follows:

The adjustment is the same as that in the wall AP scenario in dormitories.

Note:

When selecting a room, select a room whose feeder is the longest and whose adjacent room is not within the coverage of the feeder of the radio card. In addition, the device with the hardware version of v2.x in the i-Share 1 solution does not support the coverage-area-control function, and the coverage-area-control command does not need to be executed to make adjustment.

- i-Share 3 solution scenario in dormitories:

The i-Share 3 solution does not support the **coverage-area-control** function, and the **coverage-area-control** command does not need to be executed to make adjustment.

Step 1: At the outmost edge of the normal coverage area of the AP (position that is within the normal coverage of the AP but has the lowest RSSI), use the wirelessmon software to scan the AP RSSI in this room. Adjust the transmit power of the AP to ensure that the RSSI at this point is about -65 dB (the receiver sensitivity varies a lot according to STAs and iPhone is used here).

```
(config-ap)#power local xxx radio 1
```

Step 2: Slightly adjust the value of **power local** for the device as follows: Disconnect and then reconnect the STA repeatedly. The probability that the STA associates with the AP in this room is up to 95% or higher. If this probability cannot be reached, properly reduce the value of **power local** on the precondition that the coverage is normal (after

the APs in the upper room, lower room, left room, and right room are all shut down, the STA can associate with the AP in this room successfully each time).

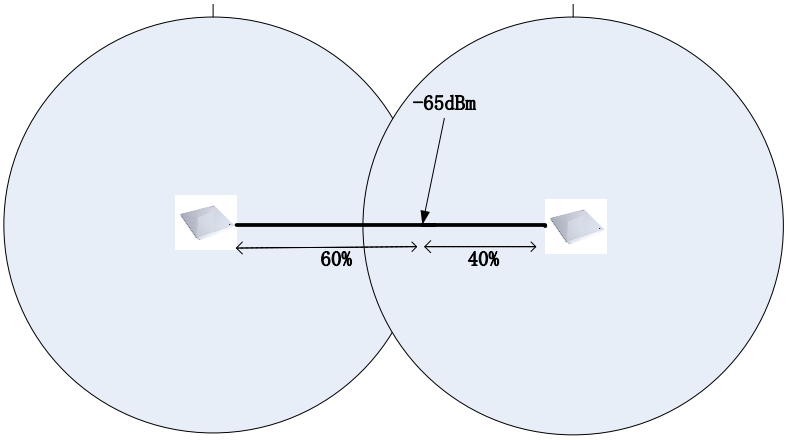
Step 3: After the power is adjusted for the 2.4 GHz band, raise the power for the 5.8 GHz band. For detailed adjustment method, see the 5.8 GHz user guide.

- X-Sense Smart AP scenario in offices:

The adjustment method is the same as that in the wall AP scenario in dormitories.

- Dense deployment scenario in venues:

Step 1: The maximum modulation rate needs to be reached at the coverage edge. If the transmit power is greater than the power required for maximum modulation rate, excessive power is a waste and will cause interference. Therefore, configure the power first. Draw a line to connect two adjacent APs, find out the point that is 60% away from one AP in distance, and perform a test at this point. Adjust the transmit power for the 2.4 GHz band (value of power local). The RSSI at this position should be about -65 dB (the receiver sensitivity varies a lot according to STAs and iPhone is used here).




```
(config-ap)#power local xxx radio 1
```

Step 2: Telnet to the AP and run the following command to display the actual transmit power of the AP:

```
show dot11 wireless 1/0 | include Actual Tx Power
Actual Tx Power.............. 13 dbm
```

Step 3: Repeat Step 1 and Step 2 to adjust the value of **power local** for APs in the upper room, lower room, left room, and right room. Properly reduce the management packet power of the AP (the value of **coverage-area-control**). It is recommended that the value be 3-5 dB lower than the value of **Actual Tx Power** displayed after the **show** command is executed in Step 2. Disconnect and then reconnect the STA repeatedly. The STA is capable of connecting to the nearby AP. If the STA cannot connect to the nearby AP, properly reduce the value of **coverage-area-control** on the precondition that the coverage is normal.

```
WS5708(config)#ap-config xxx
WS5708(config-ap)#coverage-area-control 8 radio 1  (13-5=8dB)
```

Note: In RGOS10.x, the **coverage-area-control** function is unavailable.

Step 4: If APs are deployed every 5-10 m in the open space, run the **mcell** command for the 2.4 GHz band.

```
WS5708(config)#ap-config xxx
WS5708(config-ap)#mcell enable radio 1
```

Note: The RGOS10.x does not support the mcell function.

Step 5: After the power is adjusted for the 2.4 GHz band, raise the power for the 5.8 GHz band. For detailed adjustment method, see the 5.8 GHz user guide.

The following provides the empirical power configuration of some APs for reference.

Case 1: In i-Share 1 solution, dual radio cards use the 2.4 GHz band, the power of the 2.4 GHz band is set to 20%. If the 5.8 GHz band is used, its power can be set to 100%.

Case 2: In i-Share 2 solution, the power is set to 60% for the 2.4 GHz band and 100% for the 5.8 GHz band.

Case 3: In i-Share 3 solution, the power is set to 15% for the 2.4 GHz band and 100% for the 5.8 GHz band.

Case 4: The AP120-W is used in University XX. The power is set to 2% and **coverage-area-control** is set to 7 dB.

Case 5: The AP130(L) is used in College XX. The power is set to 4% for the 2.4 GHz band and 50% for the 5.8 GHz band.

4.1.3 Lead STAs to associate with the 5.8 GHz band.

The most direct and effective method is to enable the device to separately transmit one signal in the 5.8 GHz band and map the signal only to the 5.8 GHz radio card.

```
wlan-config 100 xynu
 wlan-based per-user-limit up-streams average-data-rate 350 burst-data-rate 500
 wlan-based per-user-limit down-streams average-data-rate 350 burst-data-rate 500
!
wlan-config 111 xynu_highspeed
 wlan-based per-user-limit up-streams average-data-rate 700 burst-data-rate 900
 wlan-based per-user-limit down-streams average-data-rate 700 burst-data-rate 900
!
ap-group 100
 interface-mapping 100 51 ap-wlan-id 1
 interface-mapping 111 51 radio 2 ap-wlan-id 2
```

In addition, you can use the following method to lead STAs to associate with the 5.8 GHz band.

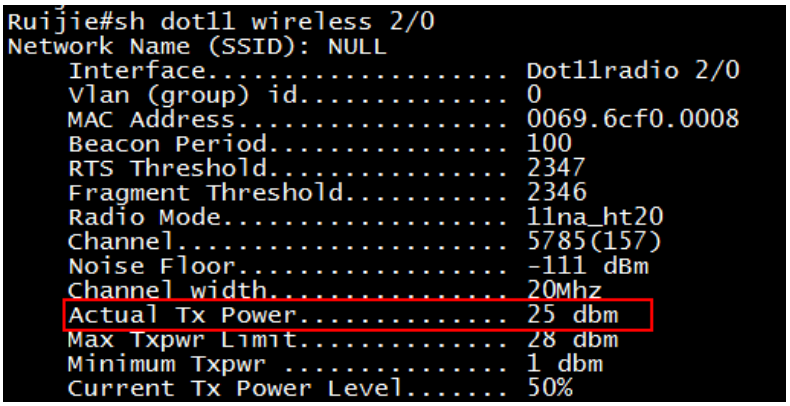
The attenuation of 5.8 GHz signals is more severe than that of 2.4 GHz signals. 5.8 GHz signals received by STAs are often weaker than 2.4 GHz signals. As a result, STAs often connect to the 2.4 GHz band. Increase the power of the 5.8 GHz band so that the RSSI of 5.8 GHz signals received by users is greater than that of 2.4 GHz signals and STAs are lead to associate with the 5.8GHz band. Empirical value: In dormitory scenarios, after the power of the 2.4 GHz band is adjusted, increase the transmit power of the 5.8 GHz (run the **show dot11 wireless 1/0** command to display the transmit power) to be 8-10 dB higher than that of the 2.4 GHz band, so as to achieve the effect.

Alternatively, use the following method to make adjustment:

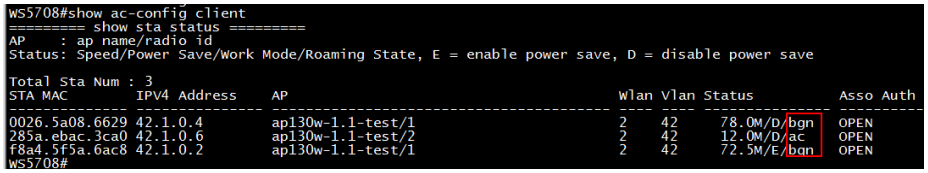
Prerequisite: Basic channels and the power of the 2.4 GHz band are properly adjusted.

Operation method:

From the angle of the AP: Use the AP to cover an open space and increase the transmit power of 5.8 GHz signals. It is recommended to set the transmit power of the 5.8 GHz band to be 7-8 dB higher than that of the 2.4 GHz band (the AP is an X-Sense Smart AP and attenuation needs to be considered for feeders of i-Share APs). You can run the **show dot11 wireless 1/0** command on the AP (2/0 represents RF Port 2) to display the actual transmit power of the AP. See the following figure.



From the angle of STAs: Select two STAs that support the 5 GHz band, including one laptop and one mobile phone. Find out the point that is within the normal coverage of the AP and is close to the edge of the normal coverage area. Disable and then enable the Wi-Fi network repeatedly, and wait for STAs to associate with the SSID. Run the **show ac-config client** command on the AC to collect statistics on 2.4 GHz band association count and 5.8 GHz band association count of the STAs. Increase the transmit power for the 5.8 GHz band progressively and perform association tests till the STAs successfully associate with the 5.8 GHz band in more than 80% tests of total 20 tests.



In the preceding figure, "b" indicates the 2.4 GHz band and "a" indicates the 5.8 GHz band.

Note:

It is not recommended to run the **band-select enable** command because the band selection function will cause slow association of STAs that support only the 2.4 GHz band and some 5.8 GHz NICs may fail to associate with the wireless network because of incompatibility. Even if an STA associates with the 5.8 GHz band successfully, the STA switches between two RF ports because the transmit power of the 2.4 GHz band is stronger, affecting user experience. According to experience, the method of leading STAs to associate with the 5.8 GHz band is to raise the transmit power for the 5.8 GHz band so that the power of 5.8 GHz signals received by STAs is higher than that of 2.4 GHz signals. Even if the **band-select enable** command is executed to enable the band selection function, the power of the 5.8 GHz band should also be adjusted and optimized.

4.1.1 Set the access threshold response-rssi to reduce remote association in scenarios where coverage-area-control is not configured.

Note: In RGOS10.x, the **coverage-area-control** function is unavailable, and therefore, **response-rssi** needs to be configured.

Description of the **response-rssi** command: After the minimum RSSI is set for wireless STAs, if the RSSI of request frames from a wireless STA is lower than the minimum RSSI, the wireless STA is not allowed to access the wireless network.

Proper configuration of **response-rssi** can prevent STAs from associating with a remote AP and prevent poor experience. Configure **response-rssi** by referring to the following case:

Refer to the following data:

RSSI of the STA in the corner of this room to associate with the AP in the room: for example, the actual test value is 35 dBm.

RSSI of the STA to associate with the APs in the upper room, lower room, left room, and right room after the AP in this room is disabled: for example, the actual test value is 30 dBm.

Note: You can run the **show dot11 a a** command to check the RSSI of the STA.

```
Ruijie#show dot11 associations all-client
RADIO-ID WLAN-ID ADDR              AID  CHAN RATE_DOWN RATE_UP RSSI ASSOC_TIME
1        1       38:59:f9:8b:65:8b 1    11    58.5M     26.0M  17       0:11:55
1        1       20:a2:e4:ac:0a:59 2    11    39.0M     19.5M  12       0:05:25
2        1       f0:f6:1c:4e:18:de 1    153   65.0M     26.0M  22       1:51:06
2        1       64:9a:be:ce:b4:91 2    153   86.5M     86.5M  27       0:35:57
Ruijie#
```

In conclusion, set **response-rssi** to **31** or **32** for STAs in the dormitory area, to effectively prevent remote association and ensure user experience.

The RSSI varies with STAs. Therefore, select more types of STAs for the test.

Note: If **response-rssi** is set to a small value, remote association cannot be prevented effectively. If it is set to a large value, the STA association will be rejected when the STA associates with the AP, because the upstream RSSI is smaller than the configured value. Therefore, when adjusting the value of **response-rssi**, **use multiple mobile phones from different mainstream manufacturers for the test.**

4.1.4 Enable intra-VLAN Layer-2 isolation for wireless STAs, to reduce Layer-2 packets in the network.

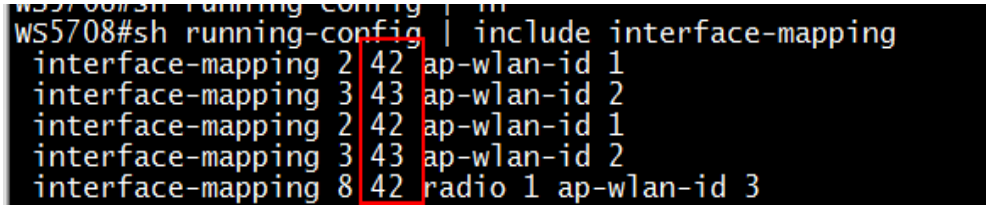
For networks that do not have Layer-2 mutual access requirements, the Layer-2 isolation must be enabled to reduce network packets and multicast packets that are to be transmitted to all APs in the same VLAN and prevent consumption of wired and wireless air interface resources.

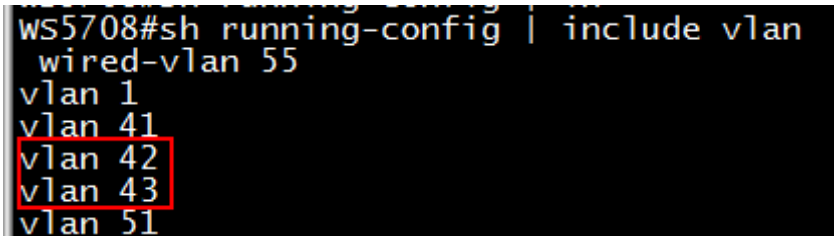
```
WS5708(config)#wids
WS5708(config-wids)#user-isolation ac enable
WS5708(config-wids)#user-isolation ap enable
or
WS5708(config)#wids
WS5708(config-wids)#user-isolation ssid-ac enable
WS5708(config-wids)#user-isolation ssid-ap enable
```

In addition, the function needs to be enabled in simplified network scenarios.

4.1.5 On the AC, create all VLANs to which wireless STAs belong.

The STA VLAN must be manually created on the AC. Otherwise, severe issues such as authentication failures and failures to obtain IP addresses may occur.





As shown in the preceding figure, the VLANs displayed by the **show running | include interface-mapping** command must be created on the AC.

4.1.6 Disable the low rate to reduce low-rate nodes in the network.

There are many low-rate nodes in the actual network. Packets from low-rate nodes are transmitted at a low rate and occupy many air interface resources, reducing the experience of users served by the AP. In the environment where private Wi-Fi interference is not severe, rates lower than 11 Mbps can be disabled.

```
802.11g network rate 1 disabled
802.11g network rate 2 disabled
802.11g network rate 5 disabled
802.11g network rate 6 disabled
802.11g network rate 9 disabled
802.11b network rate 1 disabled
802.11b network rate 2 disabled
802.11b network rate 5 disabled
```

Note:

In the environment where the private Wi-Fi interference is severe or the coverage is insufficient, disabling rates lower than 11 Mbps may degrade network experience. There is a high probability that packet loss or packet error occurs in high-rate packets because of interference or long transmission distance. In this case, properly retaining some low rate sets (for example, 5 Mbps, 6 Mbps, and even 2 Mbps) can improve user experience to a certain extent.

For example, the coverage of some areas is insufficient in College XX. The rate sets with the rate lower than 11 Mbps are disabled at first. Remote STAs send packets at a high rate and packets are retransmitted due to packet loss or CRC error, resulting in poor user experience. After some low rate sets are enabled, user experience is improved substantially.

4.1.7 Conduct QoS rate limit on STAs.

Conduct QoS rate limit on STAs to prevent STAs with good NIC performance from preempting channels all the time and causing poor user experience to STAs with poor NIC performance.

```
wlan-config 3 xynu_dx
wlan-based per-user-limit up-streams average-data-rate 300 burst-data-rate 350
     wlan-based per-user-limit down-streams average-data-rate 400 burst-data-rate 500
```

In the configuration, **the unit is 8 kbps.** It is recommended that the burst rate be set to 1.2 to 1.5 times the average value.

In addition, if a WLAN associates with only the 5.8 GHz band, the rate limit of the WLAN can be higher than the average rate limit of transmitted signals in the 2.4 GHz band.

Note: The heavy traffic of the AP5280 can easily cause high CPU usage, AP restart, or tunnel disconnection. Therefore, the performance of the AP5280 needs to be limited to 60 Mbps.

```
ap-config ap5280
     ap-based total-user-limit up-streams average-data-rate 6000 burst-data-rate 6000
     ap-based total-user-limit down-streams average-data-rate 6000 burst-data-rate 6000
```

4.1.8 Restrict the number of STAs served by an AP.

Restrict the number of STAs served by an AP so as to prevent poor user experience when excessive STAs connect to one AP. The following table provides the recommended number of STAs served by an AP.

Model	Recommended Number of Users	Description
AP120 (dormitory and office)	12	There are four users in each room and each user has two STAs.
AP130 (dormitory and office)	24	There are eight users in each room and each user has two STAs.
i-Share 1 solution (dormitory and office)	32	The single-band single-stream mode (dual 2.4 GHz radio cards) is adopted. In 1-to-4 scenarios, there are four users in each room and each user has two STAs.
i-Share 2 solution (dormitory and office)	32	The dual-band dual-stream mode is adopted. In 1-to-4 scenarios, there are four users in each room and each user has two STAs.
i-Share 3 solution (dormitory and office)	48	In 1-to-6 scenarios, there are four users in each room and each user has two STAs.
X-Sense Smart AP	64	
Outdoor AP	96	

The recommended values are an adjustment to default values. Recommended values are more proper than default values in normal cases. Adjust the values as required in actual application. For example, if the 2.4 GHz band is mainly used, adjust the STA-limit of the 2.4 GHz radio card properly; if the 5.8 GHz band is mainly used, adjust the STA-limit of the 5.8 GHz radio card properly. The common proportion of 2.4 GHz users to 5.8 GHz users is 2:1.

Configuration example:

```
sta-limit 64
```

4.1.9 Configure the antenna and feeder detection function for i-Share APs.

Feeder detection can be configured to find out the rooms where the feeder installation is incorrect according to the deployment table.

Note: The i-Share 1 solution does not support feeder detection, all versions of the i-Share 2 solution support feeder detection, and the i-Share 3 solution of B8 or a later version supports feeder detection.

```
ap-config xxx
 antdetect enable
```

The following figure provides an example of the feeder detection results.

```
STU-2#show antenna all
ap's antenna state
                                                                  R1        R2        R3        R4
                        ap                                        0 1 2 3   0 1 2 3   0 1 2 3   0 1 2 3
------------------------------------------------------------------------  -------   -------   -------   -------
sushe14_5f_6                                                      N Y Y Y   Y Y Y Y   - - - -   - - - -
sushe10_2f_5                                                      Y Y Y Y   N Y Y Y   - - - -   - - - -
sushe14_2f_6                                                      N Y Y Y   Y Y Y Y   - - - -   - - - -
sushe14_1f_6                                                      N Y Y Y   Y Y Y Y   - - - -   - - - -
sushe14_4f_6                                                      N Y Y Y   Y Y Y Y   - - - -   - - - -
sushe14_3f_6                                                      N Y Y Y   Y Y Y Y   - - - -   - - - -
sushe10_3f_5                                                      Y Y Y Y   N Y Y Y   - - - -   - - - -
sushe10_4f_5                                                      Y Y Y Y   N Y Y Y   - - - -   - - - -
sushe10_5f_5                                                      Y Y Y Y   N Y Y Y   - - - -   - - - -
sushe10_6f_5                                                      Y Y Y Y   N Y Y Y   - - - -   - - - -
sushe10_7f_5                                                      Y Y Y Y   N Y Y Y   - - - -   - - - -
wenyage_2f_1                                                      Y Y Y Y   Y Y Y Y   - - - -   - - - -
sushe10_8f_5                                                      Y Y Y Y   N Y Y Y   - - - -   - - - -
sushe10_9f_5                                                      Y Y Y Y   N Y Y Y   - - - -   - - - -
```

- "R" indicates a radio card, for example, R1 indicates radio card 1 and R2 indicates radio card 2.
- "N" indicates that no feeder is connected, or a feeder is connected but the feeder malfunctions.
- "Y" indicates that a feeder is connected and the feeder works properly.
- "-" indicates that the radio card does not exist, or feeder detection is disabled.

Note: For the RGOS10.X, only APs used in i-share 2 solution support feeder detection.

4.1.10 Enable ARP-guard and add all STA gateways to the trust entries when the STA gateway is not deployed on the AC in the case of centralized forwarding.

When the STA gateway is not deployed on the AC in the case of centralized forwarding, the source MAC address of ARP packets transmitted/responded by the gateway is the address of the STA gateway. In addition, packets need to pass through the AC and therefore, the threshold restricted by NFPP can be easily reached on the AC. As a result, ARP packets transmitted/responded by the gateway are discarded, and STAs are slow in learning ARP entries of the gateway and even fail to learn the ARP entries. Therefore, all STA gateways need to be added to trust entries to prevent this issue.

```
nfpp
   arp-guard trusted-host 172.110.16.1 1414.4b81.3dba
   arp-guard trusted-host 172.110.32.1 1414.4b81.3dba
   arp-guard trusted-host 172.110.48.1 1414.4b81.3dba
   arp-guard trusted-host 172.110.64.1 1414.4b81.3dba
```

4.1.11 Enable DHCP-guard and add the MAC address of the DHCP server to the trust entries when the DHCP server of the STA is deployed on a core device in the case of centralized forwarding

The DHCP server of the STA is deployed on a core device in the case of centralized forwarding. The source MAC address of DHCP packets responded by the DHCP server is the MAC address of the core device, the packets need to pass through the AC, and therefore, the threshold restricted by NFPP can be easily reached on the AC. As a result, the STA is slow in obtaining an IP address. Therefore, the MAC addresses of all DHCP servers need to be added to trust entries to prevent this issue.

```
nfpp
  dhcp-guard trusted-host 1414.4b81.3dba
```

4.1.12 Conduct VLAN tailoring on wired ports on the AC to reduce unnecessary multicast packets, so as not to affect wireless performance.

When the STA gateway is deployed on the AC in the case of centralized forwarding, traffic only from the interconnection VLAN is allowed to pass; when the STA gateway is not deployed on the AC in the case of centralized forwarding, traffic only from the STA and interconnection VLAN is allowed to pass; traffic only from the interconnection VLAN is allowed to pass in the case of local forwarding.

```
WS5708(config)#interface XX
WS5708 (config-if-XX)#switchport trunk allowed vlan remove xx-xx
```

4.1.13 Adjust the threshold of cpu-protect type tcp80 in the Web authentication.

In the Web authentication, if multiple users require redirection simultaneously, the default threshold of **cpu-protect type tcp80** may be exceeded, resulting in loss of redirection packets. The Web authentication page is displayed slowly on the STA. In this case, increase the threshold as required.

Judgment method: Run the **show** command every 20 seconds in peak hours and check whether the value in the **Drop** column increases. If yes, redirection packets are discarded.

```
WS18K#show cpu-protect type tcp80
 Type             Pps       Total         Drop
 -------------------   -----------    ------------    ------------

 tcp80            1200      78904545    578110
```

Command for Threshold adjustment:

```
WS18K(config)#cpu-protect type tcp80 pps 3000
```

The threshold does not need to be changed for the WS5308 and WS5302 and the default threshold is used. For the WS5708, the threshold can be adjusted to the maximum value **4000**; for the WS18000 and WS6816, the threshold can be adjusted to the maximum value **6000**; if the threshold is very large, the CPU usage may be high during redirection in the Web authentication and other adverse effects may be incurred.

Note: The RGOS10.x does not support the threshold adjustment.

4.1.14 Add all APs to the AP-group.

An AP that is not added to an AP-group may fail to send signals. Even if WLAN VLAN mapping is configured for the default group and an AP in the default group can transmit signals, it is not recommended to use the default group because the default group cannot facilitate management.

4.1.15 Disable the countermeasure function.

The countermeasure function severely affects user experience. If necessary, enable the countermeasure function on a specific AP.

```
WS5708(config)#wids
WS5708(config-wids)#no countermeasures enable
```

4.1.16 Disable dot1x scheduled re-authentication function in dot1x authentication scenarios. (dot1x re-authentication)

If dot1x re-authentication is enabled in dot1x authentication, users who pass dot1x authentication go offline easily. Therefore, do not enable the dot1x scheduled re-authentication function in actual wireless dot1x authentication deployment scenarios.

The command for disabling dot1x scheduled re-authentication function is as follows:

```
WS5708(config)#no dot1x re-authentication
```

4.1.17 Disable HTTPS for re-authentication in Web authentication scenarios.

HTTPS uses a complex encryption technology and therefore, it is poor in performance. If HTTPS (disabled by default) is enabled in actual scenarios, the Web authentication redirection may be slow and even the redirection page is not displayed, severely affecting user experience.

The command for disabling HTTPS redirection is as follows:

```
WS5708(config)#no http redirect port 443
WS5708(config)#no http redirect port 8443
```

4.1.18 Disable the promiscuous mode.

The promiscuous mode affects experience of wireless users in actual deployment and therefore must be changed to the normal mode. If the promiscuous mode is required indeed, enable it only on a specific AP.

```
WS5708(config-ap)#device mode normal
```

4.1.19 Disable the data-plane wireless-broadcast enable function.

The **data-plane wireless-broadcast enable** function enables the device to forward all broadcast packets to the air interface, which occupies a large number of wireless air interface resources and severely affects user experience. Therefore, disable the **data-plane wireless-broadcast enable** function (disabled by default).

```
WS5708(config)#data-plane wireless-broadcast disable
```

4.1.20 Disable the assoc-rssi xx radio xx function.

Different positions of STAs results in a large difference in the upstream power (the difference is especially significant for Samsung STAs). STAs may go offline frequently after this function is enabled.

Note: The RGOS10.x does not support this function.

4.1.21 Check whether ARP packets of the STA gateway are allowed to pass when ARP-check is enabled in Web authentication.

When ARP-check is enabled in Web authentication, if ARP packets from the gateway are not allowed to pass, wireless STAs fail to learn the ARP entries of the gateway. As a result, users cannot be authenticated or access the Internet.

```
http redirect direct-arp 51.1.1.1
http redirect direct-arp 52.1.1.1
http redirect direct-arp 53.1.1.1
```

Case: Web authentication is configured and ARP-check is enabled on the AC in a university. A wireless user network segment of a new dormitory building is added. ARP bypass is not configured for the gateway of the new network segment on the AC. As a result, users cannot be authenticated or access the Internet, affecting student registration at the beginning of a new term.

4.1.22 Disable ip verify source in the case of WLAN Sec.

The performance of the **ip verify source** function is poor, and it may cause high CPU usage of the AC, and even cause the random discarding of user packets. If required, replace **ip verify source** with **ip verify source port-security** command to achieve the same effect.

```
WS5708(config)#wlansec 1
WS5708(config-wlansec)#no ip verify source
WS5708(config-wlansec)#ip verify source port-security
```

4.1.23 Use the 20 MHz band rather than 40 MHz and 80 MHz bands in actual scenarios.

The 40 MHz and 80 MHz bands can cause severe frequency interference in actual deployment scenarios. Therefore, do not use the 40 MHz and 80 MHz bands in actual scenarios. Use the default 20 MHz band instead.

The following configuration is incorrect:

```
WS5708(config-ap)#chan-width 40 radio 1
```

```
WS5708(config-ap)#chan-width 40 radio 2
WS5708(config-ap)#chan-width 80 radio 2
```

Change it to the following configuration:

```
WS5708(config-ap)#no chan-width radio 1
WS5708(config-ap)#no chan-width radio 2
```

Note: The actual deployment scenarios here exclude pre-sales, centralized procurement, and shortlisted test.

4.1.24 Adjust RRM-relevant functions.

The Dynamic Channel Allocation (DCA) and Transmit Power Control (TPC) in the Radio Resource Management (RRM) function of wireless devices occupy a large amount of CPU and memory. Frequent running of the DCA and TPC may cause wireless network instability. In some scenarios, the TPC function may reduce the power to a very low value, resulting in poor user experience. Therefore, disable the DCA and TPC.

Disable the RRM TPC (disabled by default). The TPC function may reduce the power to a very low value, affecting user experience. Therefore, disable the RRM TPC in actual deployment scenarios.

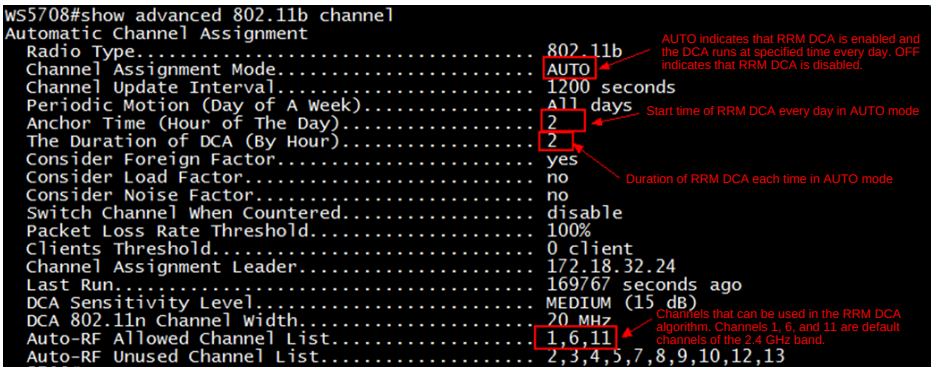
```
advanced 802.11b txpower dtpc disable
advanced 802.11a txpower dtpc disable
```

Use the DCA (enabled by default) as follows:

1. Disable the RRM DCA and manually adjust channels.

```
advanced 802.11b channel global off
advanced 802.11a channel global off
```

2. Enable RRM and set the RRM channel adjustment time to the default value (the adjustment starts from 02:00 a.m. and lasts for 2 hours by default).**(This method is not recommended because it is still in the effect verification and revision phase.)**



Check RRM DCA-relevant information. See the preceding figure.

The command for restoring the default running time is as follows:

```
no advanced 802.11b channel dca anchor-time
no advanced 802.11a channel dca anchor-time
```

In addition, if a non-conventional channel is used and RRM is required for channel adjustment, adjust the available channels used in the RRM channel algorithm. For example, use the 3, 8, and 13 non-conventional channels. The configuration is as follows:

Add Channels 3, 8, and 13 first.

```
WS5708(config)#advanced 802.11b channel add 3
WS5708(config)#advanced 802.11b channel add 8
WS5708(config)#advanced 802.11b channel add 13
```

Delete the default Channels 1, 6, and 11.

```
WS5708(config)#advanced 802.11b channel delete 11
```

The result is as shown in the following figure.

```
WS5708#show advanced 802.11b channel
Automatic Channel Assignment
  Radio Type..................................... 802.11b
  Channel Assignment Mode........................ AUTO
  Channel Update Interval........................ 1200 seconds
  Periodic Motion (Day of A Week)................ All days
  Anchor Time (Hour of The Day).................. 2
  The Duration of DCA (By Hour).................. 2
  Consider Foreign Factor........................ yes
  Consider Load Factor........................... no
  Consider Noise Factor.......................... no
  Switch Channel When Countered.................. disable
  Packet Loss Rate Threshold..................... 100%
  Clients Threshold.............................. 0 client
  Channel Assignment Leader...................... 172.18.32.24
  Last Run....................................... 171512 seconds ago
  DCA Sensitivity Level.......................... MEDIUM (15 dB)
  DCA 802.11n Channel Width...................... 20 MHz
  Auto-RF Allowed Channel List................... 3,8,13
  Auto-RF Unused Channel List.................... 1,2,4,5,6,7,9,10,11,12
```

4.1.25 Check the hot backup configuration.

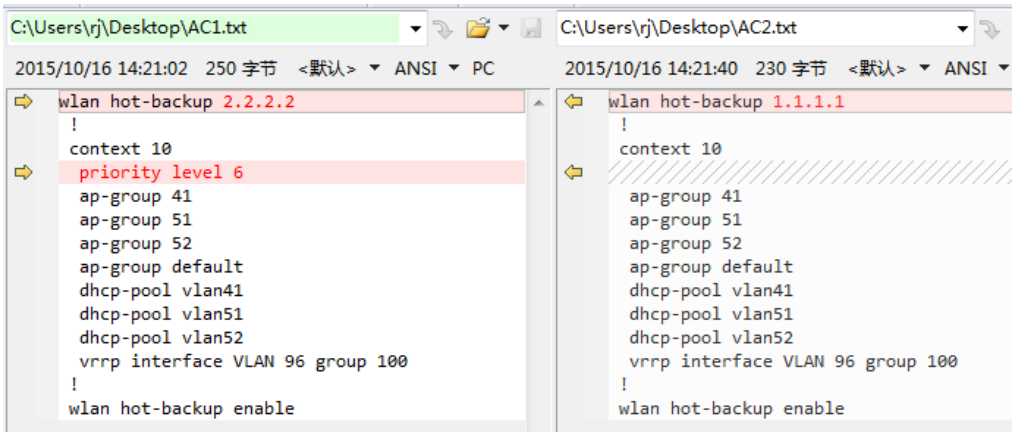
Two ACs working in hot backup mode need to use consistent configuration except specific configuration such as the AC names, IP addresses, and hot backup priority. Use a comparison tool to compare the configuration. Information to be compared includes the outputs of the **show run**,**show ap-config running**, and **show ap-group aps summary** commands; alternatively, directly export the **config.text** and **ap-config.text** to the local device and use a tool to compare the configuration.

If authentication is conducted on the AC, configure VRRP, use the VRRP address as the NAS IP address for authentication (run the **ip radius source-interface** *xxx*/ **ip portal source-interface** *xxx* command), and add the VRRP address to the hot backup configuration. Otherwise, an authentication exception will occur after hot backup switching.

a. If the STA gateway is deployed on the AC in the case of centralized forwarding, use the VRRP address as the STA gateway address and add the VRRP address to the hot backup configuration. Otherwise, users fail to access the network after hot backup switching.

b. The DHCP pool, AP-group, and VRRP need to be added to the hot backup configuration. If DHCP pool is not added to hot backup configuration, allocation entries of the address pool are not synchronized. If the AP-group is inconsistent, users cannot connect to the network or an association exception occurs after hot backup switching.

The following figure shows the typical hot backup configuration.



4.1.26 Disable AA hot backup because this function may cause an authentication exception and a roaming exception after users switch to another AP.

AA hot backup can cause an authentication exception and a roaming exception after users switch to another AP. In addition, the resource usage (for example, CPU usage) in AA mode is higher than that in AS mode. Therefore, AA mode must be changed to the AS mode.

The following issues arise in AA mode:

- Dual NAS IP address problem in A/A hot backup mode cannot be solved.

You can run the **ip radius source-interface vlan** command to set the NAS IP address. You can configure two VRRP groups in a VLAN, which map to two contexts. The actual verification shows that if two NAS IP addresses are specified on one device, an authentication error will occur and it cannot be ensured that the correct NAS IP address is selected for authentication each time.

- In AA hot backup mode, the intra-context roaming is normal but the inter-context roaming fails.

Layer-2 roaming is normal. In actual deployment, different contexts map to different VLANs. Therefore, Layer-2 roaming does not occur basically.

- Layer-3 roaming fails:

Based on whether the WLAN/IP address is changed:

1. If the WLAN/IP address keeps unchanged in the inter-context roaming, authentication entries are not deleted and STAs cannot access the wireless network.
2. If the WLAN/IP address is changed in the inter-context roaming, authentication entries are deleted and re-authentication is required, indicating that the roaming fails.

- In AA+Web+MAB authentication, when a user moves from Context 1 to Context 2, a problem also occurs even if the user does not roam.

The problem occurs due to MAB authentication (and also in dot1x authentication). An STA goes online in AC1. The authentication entry is synchronized to AC2. When the STA moves to the coverage area of AC2, AC2 rejects the STA to go online after checking that the entry exists. The root cause is that only the MAC address is indexed when the AC2 searches for the entry. If the MAC address + WLAN + VLAN are indexed, the STA can be authenticated successfully. For example, when a user moves from the dormitory to the canteen, the user fails to go online after applying for Web authentication repeatedly. The user can pass Web authentication till the entry ages.

4.2 [Optional Configuration for Network Optimization for Higher Education Sector]

4.2.1 Adjust the transmission interval of beacon packets.

The default transmission interval of beacon packets is 100 ms and beacon packets are transmitted at the lowest forcible rate. When the private Wi-Fi interference is low and Ruijie APs send considerable signals (for example, one AP transmits 4-8 signals), the beacon packets will occupy a large number of air interface resources, causing poor user experience. In this case, increase the transmission interval of beacon packets to 150-300 ms. Note: If the transmission interval of beacon packets is set to a very large value, the signals received by STAs are unstable, resulting in poor user experience.

```
WS5708(config-ap)#beacon period 200 radio 1
```

4.2.2 Disable the band-select enable function.

The **band-select enable** function causes slow association of STAs that support only the 2.4 GHz band and some 5 GHz NICs may fail to access the wireless network because of incompatibility. Even if an STA associates with the 5.8 GHz band successfully, the STA switches between two RF ports because the transmit power of the 2.4 GHz band is stronger, affecting user experience.

According to experience, the method of leading STAs to associate with the 5.8 GHz band is to increase the transmit power for the 5.8 GHz to ensure that the power of 5.8 GHz signals received by STAs is higher than that of 2.4 GHz signals. For detailed adjustment method, see the section of leading STAs to associate with the 5.8 GHz band.

Even if the **band-select enable** command is executed to enable the band selection function, the power of the 5.8 GHz band also should be adjusted and optimized.

4.2.3 Configuring 802.11n A-MPDU Transmission Protection

The A-MPDU transmission protection can reduce bandwidth loss caused by collision of hidden nodes but will increase the air interface overhead. It is recommended that the A-MPDU transmission protection be disabled by default. In i-Share 1 and i-Share 2 scenarios in dormitories, the same radio signal can be transmitted to APs in different rooms, which will greatly increase hidden nodes. Therefore, enable the function in this case.

```
WS5708(config-ap)# ampdu-rts radio 1
```