

WLAN

维护宝典（分销）

文档版本 01
发布日期 2023-11-16



版权所有 © 华为技术有限公司 2023。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址：深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址：<https://e.huawei.com>

安全声明

产品生命周期声明

华为公司对产品生命周期的规定以“产品生命周期终止政策”为准，该政策可参考华为公司官方网站的网址：<https://support.huawei.com/ecolumnsweb/zh/warranty-policy>。

漏洞声明

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该政策可参考华为公司官方网站的网址：<https://www.huawei.com/cn/psirt/vul-response-process>。

如企业客户须获取漏洞信息，请访问：<https://securitybulletin.huawei.com/enterprise/cn/security-advisory>。

预置数字证书声明

华为公司对随设备出厂的预置数字证书，发布了“华为预置数字证书免责声明”，声明内容详见华为公司官方网站的网址：<https://support.huawei.com/enterprise/zh/bulletins-service/ENEWS2000015766>。

产品资料生命周期声明

华为公司针对随产品版本发布的售后客户资料（产品资料），发布了“产品资料生命周期政策”，该政策的内容请参见华为公司官方网站的网址：<https://support.huawei.com/enterprise/zh/bulletins-website/ENEWS2000017760>。

关于本文档

文档简介





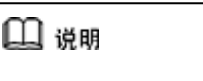
本文档提供了WLAN分销产品的例行维护指导和故障处理指导。发生故障时请先评估故障是否为紧急故障。如果是紧急故障，请使用预先制定的紧急故障处理方法，尽快修复故障模块，进而恢复业务。所有的重大操作，如重启设备等均应作记录，并在操作前仔细确认操作的可行性，在做好相应的备份、应急和安全措施后，方可由有资格的操作人员执行。如您需要查询安装、配置部署、命令、MIB、日志和告警相关内容，请查询对应设备软件版本的产品文档，比如“AC V200R022C00 产品文档”。

适用产品和版本

本文档适用于WLAN分销产品V200R019及之后版本。

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
	表示如不避免则将会导致死亡或严重伤害的具有高等级风险的危害。
	表示如不避免则可能导致死亡或严重伤害的具有中等级风险的危害。
	表示如不避免则可能导致轻微或中度伤害的具有低等级风险的危害。
	用于传递设备或环境安全警示信息。如不避免则可能会导致设备损坏、数据丢失、设备性能降低或其它不可预知的结果。 “须知”不涉及人身伤害。
	对正文中重点信息的补充说明。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。

命令行格式约定

在本文中可能出现下列命令行格式，它们所代表的含义如下。

格式	意义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用 加粗 字体表示。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 表示。
[]	表示用“[]”括起来的部分在命令配置时是可选的。
{ x y ... }	表示从两个或多个选项中选取一个。
[x y ...]	表示从两个或多个选项中选取一个或者不选。
{ x y ... } *	表示从两个或多个选项中选取多个，最少选取一个，最多选取所有选项。
[x y ...] *	表示从两个或多个选项中选取多个或者不选。
&<1-n>	表示符号“&”前面的参数可以重复1～n次。
#	表示由“#”开始的行为注释行。

公网IP地址使用的声明

出于特性介绍及配置示例的需要，本文档可能会使用公网IP地址，如无特殊说明出现的公网IP地址均为示意，不指代任何实际意义。

目录

关于本文档.....	iii
1 故障处理：SOHO 分销问题.....	1
2 故障处理：Leader AP 类问题.....	2
2.1 Leader AP 类故障定位指导.....	2
2.1.1 忘记了 AP 的登录密码.....	2
2.1.2 终端连不上 Wi-Fi 信号.....	4
2.1.3 部分 AP 不上线.....	12
2.1.4 Wi-Fi 测速慢.....	13
2.1.5 Wi-Fi 网络卡顿.....	22
3 故障处理：AP 上下线类问题.....	27
3.1 AP 在 AC 上无法上线.....	27
3.2 AP 异常掉线.....	31
4 故障处理：无线终端认证类问题.....	35
4.1 802.1x 认证失败.....	35
4.2 Portal 认证失败.....	38
5 故障处理：终端体验类问题.....	40
5.1 终端异常掉线.....	40
5.2 终端搜不到 WiFi 信号.....	43
5.3 终端上线失败.....	44
5.4 终端获取不到地址.....	45
5.5 终端网络慢.....	51
5.6 终端漫游问题.....	56
5.7 终端业务不通.....	58
5.8 终端 station-trace 解析.....	59
6 故障处理：设备登录类问题.....	63
6.1 SSH 登录失败.....	63
6.2 Web 网管登录失败.....	64
7 故障处理：双机备份类问题.....	67
7.1 VRRP 热备未建立.....	67
7.2 无线配置同步失败.....	69

8 故障处理：AC/AP 升级类问题.....71

9 故障处理：设备管理类问题.....74

9.1 License 激活失败..... 74

9.2 CPU 占用率高..... 75

9.3 供电异常..... 88

10 故障处理：无线桥接类问题..... 90

10.1 Mesh 组网中 MP 上线失败..... 90

11 故障处理：CampusInsight 对接问题..... 96

11.1 CampusInsight 上不显示性能上报数据..... 96

12 故障处理：云管理类问题..... 98

12.1 云 AC/云 AP 无法上线..... 98

13 联系华为技术支持..... 101

1 故障处理：SOHO 分销问题

SOHO分销常见问题故障处理请参见：[智能园区SOHO解决方案 维护宝典](#)。

2 故障处理：Leader AP 类问题

2.1 Leader AP类故障定位指导

2.1 Leader AP 类故障定位指导

2.1.1 忘记了 AP 的登录密码

现象描述

Leader AP组建的Wi-Fi网络使用一段时间后，想要登录Leader AP管理Wi-Fi网络，忘记了Leader AP的登录密码，需要重新设置登录密码。

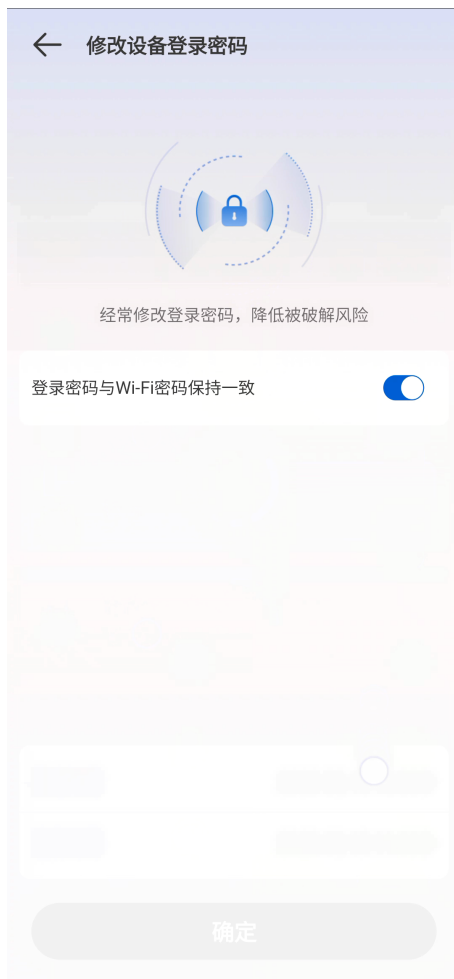
可能原因

未使用手机APP管理Wi-Fi网络。

操作步骤

- 步骤1** 配置Wi-Fi网络时，如果是使用手机APP配置的，则可以尝试使用上网的Wi-Fi密码来登录AP。手机APP配置过程中，可以设置上网的Wi-Fi密码和登录密码一致，登录的用户名默认为**admin**。
- 步骤2** 如果使用上网的Wi-Fi密码无法登录成功，则需要使用配置Wi-Fi网络的手机，通过手机APP修改AP的登录密码。

进入Leader AP的管理界面，点击“查看更多 > 修改设备登录密码”，可设置AP的登录密码。



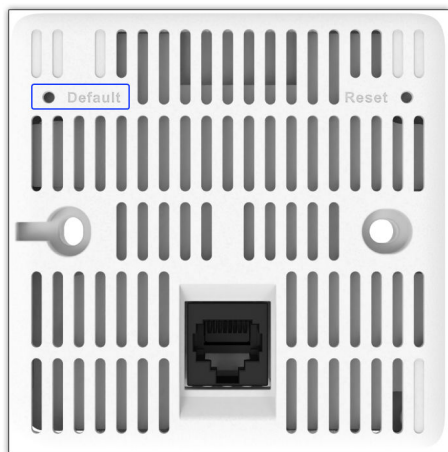
步骤3 如果配置Wi-Fi网络时未使用手机APP，而是通过Web网管等其他方式配置的，则需要将AP恢复出厂设置，重新配置Wi-Fi网络。

长按Leader AP上的Default按键，恢复出厂设置。如果不知道哪台AP是Leader AP，则需对所有AP恢复出厂设置。

AP的Default按键一般位于AP侧面。



86面板AP的Default按键隐藏在前面板的后面，取下前面板后可以看到。



步骤4 请保存好AP的登录密码。建议定期更换AP的登录密码，提升网络的安全性。

----结束

2.1.2 终端连不上 Wi-Fi 信号

现象描述

使用Leader AP配置Wi-Fi网络后，部分终端在连接Wi-Fi上网时，搜不到Wi-Fi信号；或者搜到Wi-Fi信号后，无法连接成功。

可能原因

如果终端上搜不到Wi-Fi信号，可能是如下原因。

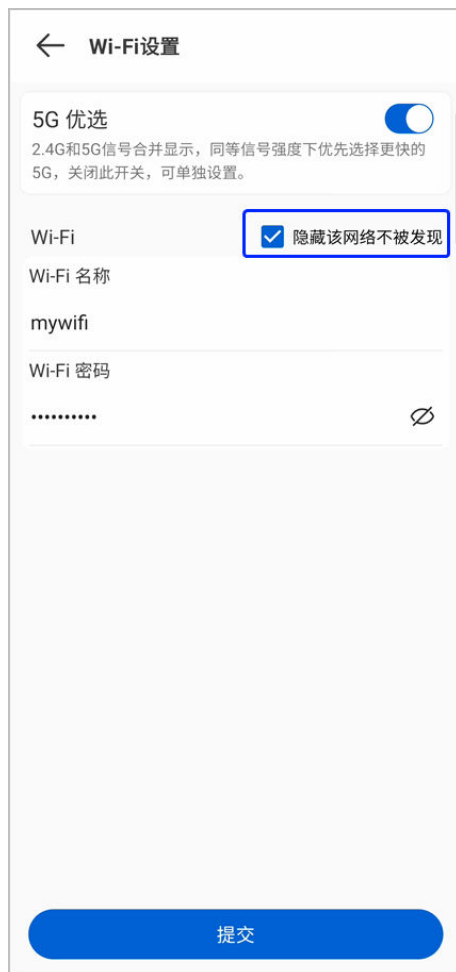
- 开启了Wi-Fi名称（SSID）隐藏功能。
- Wi-Fi名称配置错误。
- Wi-Fi信号强度配置过小。

如果终端上可以搜到Wi-Fi信号，但连不上，可能是如下原因。

- Wi-Fi密码输入错误。
- 配置了终端黑白名单功能。
- DHCP地址池IP地址耗尽。

操作步骤

- **手机APP方式**
 - a. 关闭Wi-Fi名称（SSID）隐藏功能，终端重新搜索Wi-Fi信号。
进入Leader AP的管理界面，点击“Wi-Fi设置”，取消勾选“隐藏该网络不被发现”。



- b. 修改Wi-Fi名称，终端重新搜索Wi-Fi信号。
- # 进入Leader AP的管理界面，点击“Wi-Fi设置”，修改Wi-Fi名称。



- c. 修改Wi-Fi的信号强度，终端重新搜索Wi-Fi信号。
进入Leader AP的管理界面，点击“信号强度”，设置为穿墙模式。

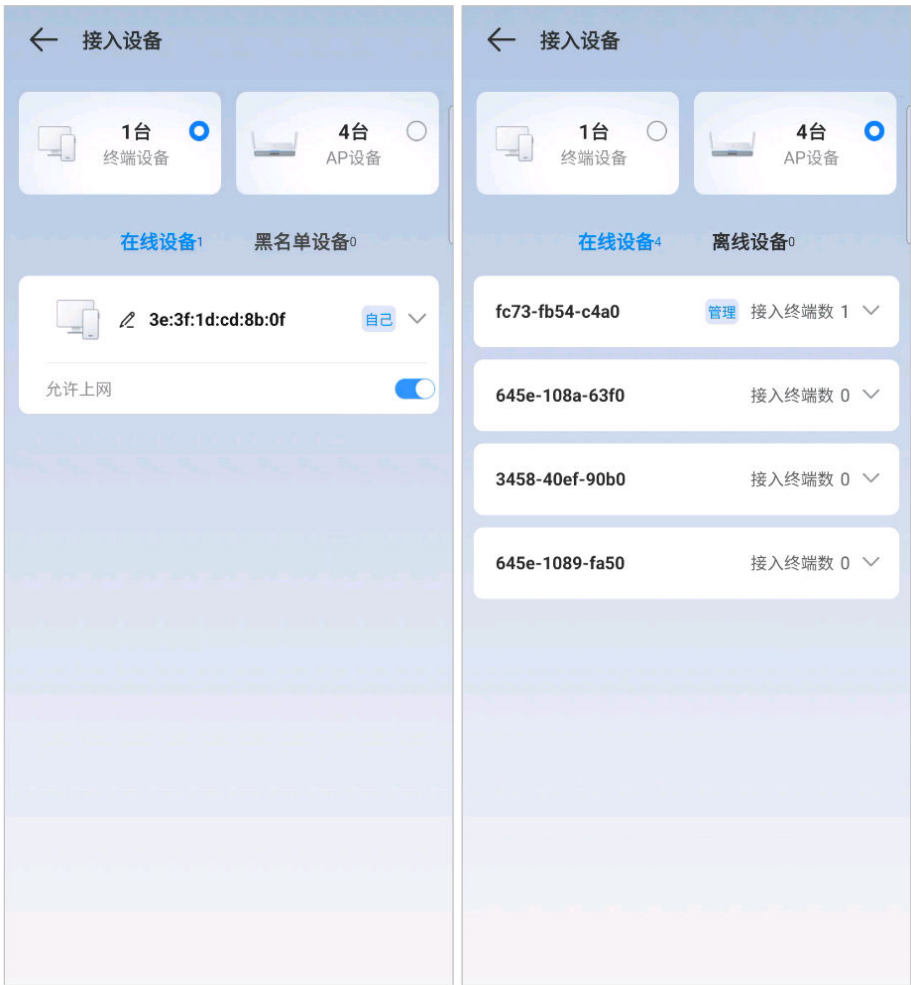


- d. 查看设置的Wi-Fi密码。然后在终端的WLAN列表中选择忘记网络，再重新搜索Wi-Fi名称和输入密码。

进入Leader AP的管理界面，点击“Wi-Fi设置”，点击Wi-Fi密码后的眼睛图标，查看Wi-Fi密码。



- e. 查看终端是否在黑名单，设置允许上网。
进入Leader AP的管理界面，点击“接入设备”，查看终端的MAC地址是否在黑名单设备中，如果在则点击允许上网，从黑名单中移除。



• Web网管方式

- a. 关闭Wi-Fi名称（SSID）隐藏功能，终端重新搜索Wi-Fi信号。
选择“配置 > 无线网络配置”，点击SSID名称进入修改界面。
在基本信息中展开“高级”，展开“SSID配置”，关闭隐藏SSID功能。



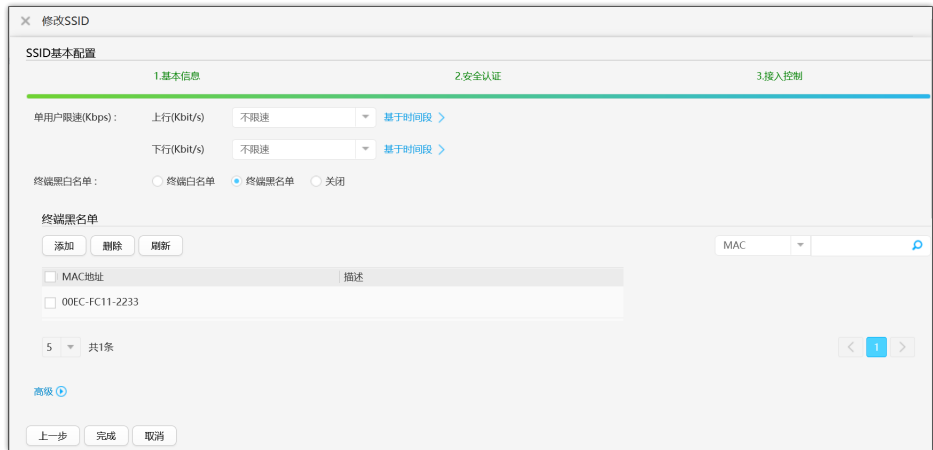
- b. 修改Wi-Fi名称，终端重新搜索Wi-Fi信号。
选择“配置 > 无线网络配置”，点击SSID名称进入修改界面。
在基本信息中修改“SSID名称”。



- c. 修改Wi-Fi的信号强度，终端重新搜索Wi-Fi信号。
选择“高级 > 射频配置 > 射频规划”，在射频列表中单击对应AP射频后的操作按钮，修改射频参数。



- d. 在终端的WLAN列表中选择忘记网络，再重新搜索Wi-Fi名称和输入密码。
e. 查看是否配置了终端的黑白名单，将终端加入白名单，或者从黑名单中移除。
选择“配置 > 无线网络配置”，点击SSID名称进入修改界面。
在接入控制步骤修改“终端黑白名单”的配置。



- f. 将上网模式修改为网关模式，减少对光猫的DHCP地址池的消耗。
参考产品文档的举例：配置Leader AP Wi-Fi上网 网关模式DHCP。

● 命令行方式（供技术人员使用）

- a. 关闭Wi-Fi名称（SSID）隐藏功能，终端重新搜索Wi-Fi信号。
i. 查看SSID隐藏相关的功能是否开启。

```
<HUAWEI> display ssid-profile name xxx
-----
Profile ID      : 8
SSID           : XXX
SSID hide      : enable
Association timeout(min) : 5
Max STA number : 64
Action upon reaching the max STA number : SSID hide
```

SSID hide：表示SSID隐藏功能。

Action upon reaching the max STA number：表示VAP接入用户数达到设置的数目（**Max STA number**）时，自动隐藏SSID。

```
<HUAWEI> display rrm-profile name xxx
-----
...
UAC client number access threshold          : 64
UAC client number roam threshold           : 64
Action upon reaching the UAC threshold      : SSID hide
...
```

Action upon reaching the UAC threshold：表示射频接入的用户数达到设置的门限时，控制新接入用户采取的动作。**SSID hide**会禁止新用户接入，并自动隐藏SSID。

- ii. 在SSID模板下关闭隐藏SSID相关的功能。

```
undo ssid-hide enable
reach-max-sta hide-ssid disable
```

- iii. 在RRM模板下关闭隐藏SSID相关的功能。

```
undo uac reach-access-threshold
```

- b. 修改Wi-Fi名称，终端重新搜索Wi-Fi信号。

- i. 查看当前配置的SSID名称。

```
<HUAWEI> display vap-profile all
-----
Name      FMode  Type  VLAN  AuthType  STA U/D(Kbps)  VAP U/D(Kbps)
BR2G/5G/6G(Mbps) Reference SSID
-----
default   direct service VLAN 1  -        -/-        -/-        5.5/6/6
0         HUAWEI-WLAN
dd        direct service VLAN 1  Open     -/-        -/-        5.5/6/6
1         HUAWEI-WLAN
...
```

- ii. 根据配置的VAP模板，查看引用的SSID模板。

```
<HUAWEI> display vap-profile name xxx
-----
...
SSID profile          : xxx
Security profile      : default
...
```

- iii. 进入SSID模板，重新配置SSID名称。

```
system-view
wlan
ssid-profile name xxx
ssid ssidname
```

- c. 修改Wi-Fi的信号强度，终端重新搜索Wi-Fi信号。

在AP射频视图下，配置最大发射功率。

```
system-view
wlan
ap-id x
radio x
calibrate auto-txpower-select disable
eirp 127
```

- d. 在终端的WLAN列表中选择忘记网络，再重新搜索Wi-Fi名称和输入密码。

- e. 查看是否配置了终端的黑白名单，将终端加入白名单，或者从黑名单中移除。

- i. 查看AP或VAP是否开启了黑白名单功能。

```
<HUAWEI> display ap-system-profile name xxx
```

```
-----
```

```
...
STA whitelist profile      : -
STA blacklist profile      : black
...
```

```
<HUAWEI> display vap-profile name xxx
```

```
-----
```

```
...
STA access mode           : blacklist
STA blacklist profile      : black
STA whitelist profile      :
...
```

- ii. 如果配置了黑名单，则在黑名单模板视图下，删除终端MAC。

```
system-view
wlan
sta-blacklist-profile name xxx
undo sta-mac xxxx-xxxx-xxxx
```

- iii. 如果配置了白名单，则在白名单模板视图下，添加终端MAC。

```
system-view
wlan
sta-whitelist-profile name xxx
undo sta-mac xxxx-xxxx-xxxx
```

- f. 检查DHCP地址池是否还有空余地址，如果地址耗尽的话终端也会因无法获取地址而连接失败。可以调小DHCP服务器中IP地址的租期，或者扩大DHCP的地址池资源。

2.1.3 部分 AP 不上线

现象描述

使用Leader AP配置Wi-Fi网络后，等待一段时间后，只能看到部分FIT AP在线，其他FIT AP不上线。

可能原因

- FIT AP的网线连接存在问题。
- AP不是出厂配置，工作模式不是FIT AP。
- 网络中存在其他Leader AP，FIT AP在其他Leader AP上线。
- FIT AP和Leader AP间网络不通，未放通管理VLAN。

操作步骤

1. 检查网线连接是否正常。

查看交换机上的端口指示灯是否正常。如果指示灯不亮，检查交换机侧和AP侧的网线连接是否松动、脱落。

在交换机上将正常上线和未上线的FIT AP的网线互换，进行交叉验证。网线互换后AP会重启，需要等待2分钟，如果原来正常上线的AP无法上线，原来未上线的AP正常上线，则可判断是网线问题，需要更换网线。

说明

AP上线后名称默认是MAC地址，建议修改为房间、位置等易于识别位置的名称，方便快速找到AP。

如果需要确认已上线的AP位置，可以控制指定AP的指示灯开关，观察AP的指示灯是否做出相应的变化，以确认AP的位置。

手机APP方式：

进入Leader AP的管理界面，点击“AP管理”，可修改AP的名称，控制AP的指示灯开关。

Web网管方式：

进入“配置 > 接入点配置 > AP配置”，在“AP列表”中找到要操作的AP。

单击对应AP“操作”列的修改图标，可在“AP名称”列修改对应AP的名称，修改后在操作列单击确定图标。

勾选要操作的AP，单击列表上方的“闪灯”按钮，控制AP的指示灯闪灯状态。

命令行方式（供技术人员使用）：

WLAN视图下，使用命令`ap-rename { ap-name name | ap-mac ap-mac-address | ap-id ap-id } new-name ap-new-name`，修改指定AP的名称。

WLAN视图下，使用命令`led blink-time blink-time { ap-mac ap-mac | ap-name ap-name | ap-id ap-id }`，控制指定AP的指示灯闪灯状态。

2. 找到未上线的AP，将其切换为FIT模式的出厂配置。

V200R022C00版本开始，长按AP上的Default按钮，即可恢复为FIT模式的出厂配置。

V200R021C10及之前版本，可以先长按AP上的Default按钮，恢复为当前模式的出厂配置，再通过APP的模式切换功能，将其切换为FIT模式的出厂配置。

3. 排查网络中是否存在其他Leader AP，存在的话将其移出网络，或者切换为FIT模式，使其在规划的Leader AP上线。

在终端的WLAN列表中，查看是否能搜到包含AP MAC地址后4位的Wi-Fi名称。如果可以搜到，则AP未在任何Leader AP上线。如果搜不到，则AP可能在其他Leader AP上线，可继续排查未上线的AP，都切换为FIT模式的出厂配置。

4. FIT AP和Leader AP之间通常连接在同一台交换机，并处于同一局域网内，此时FIT AP可以发现Leader AP并自动上线。如果交换机上支持VLAN功能，在连接AP的接口上被配置了不同的VLAN，则FIT AP和Leader AP无法连通。

检查交换机上连接AP端口的VLAN配置，应放通VLAN 1。

2.1.4 Wi-Fi 测速慢

现象描述

终端连接Wi-Fi后，使用测速应用测试网速，发现网速很低。

可能原因

- 终端接入2.4G频段，未接入速率更高的5G频段。
- 5G频段上未使用大的频宽。
- 有线连接的网线的物理速率异常。
- 上网的带宽较低。

操作步骤

- 手机APP方式

a. 将终端接入5G频段的Wi-Fi信号。

在手机的WLAN设置中，可以查看已连接的Wi-Fi信息，包括建链速率（连接速度），信号频段（频率），Wi-Fi标准（WLAN能力）。不同型号的手机，显示信息有所差异。



打开APP，首页上方可以看到当前连接的Wi-Fi信号的频段，Wi-Fi标准，协商速率等信息。



如果接入Wi-Fi信号的是2.4G，则重新接入5G频段的Wi-Fi信号。

- 在终端的WLAN设置中，忘记已连接的WLAN网络，重新搜索和连接，再检查频段是否为5G。
- 如果频段仍为2.4G，则需要先确认下终端型号是否支持5G频段。建议更换支持5G频段的手机进行测速。

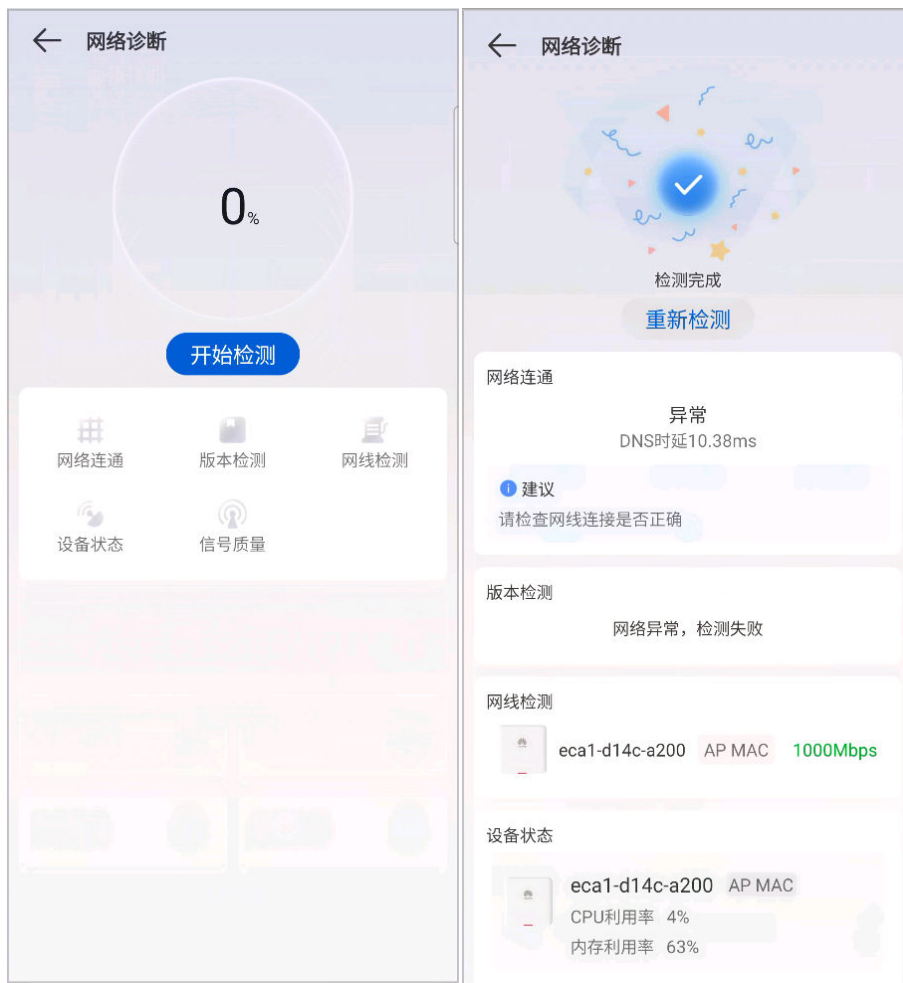
- iii. 如果手机支持5G频段，但仍接入2.4G频段的信号，则可以修改5G频段的Wi-Fi名称，在WLAN设置中搜索和连接5G频段的Wi-Fi信号。
- 从APP进入Leader AP的管理界面，点击“Wi-Fi设置”，取消勾选“5G优选”，修改“5G Wi-Fi”的“Wi-Fi名称”。



- b. 将5G频宽修改成160 MHz。
- # 点击“本地管理网络 > 选择网络卡片 > 查看更多 > 极速漫游”，建议组网的AP数量小于8个时，开启极速漫游功能。



- c. 检查网线的物理协商速率是否为千兆及以上。
进入Leader AP的管理界面，点击“网络诊断”，查看网线检测结果。如果结果是百兆，则需检查网线规格是否为超5类（CAT5E）及以上，水晶头线序是否正确等。



d. 确认上网的出口带宽。

使用有线终端接入网络测速，查看测速结果。如果测速较低，则需联系运营商检查网络，或者升级出口带宽。

- **Web网管方式**

a. 将终端接入5G频段的Wi-Fi信号。

在手机的WLAN设置中，可以查看已连接的Wi-Fi信息，包括建链速率（连接速度），信号频段（频率），Wi-Fi标准（WLAN能力）。不同型号的手机，显示信息有所差异。



登录Web网管，进入“监控 > 概览”，在用户版块点击测速低的终端，在下面的详情里查看当前连接的Wi-Fi信号的频段，Wi-Fi标准，协商速率等信息。

用户名: 

在线

 用户当前在线,已连接 1M:1S

用户体验优质!

协商速率(Mbps) ↓↑

1441/1441

信噪比(dB)

44.0

用户明细 [更多](#)

用户名:



MAC地址:



AP名称:



IPv4地址:

192.168.101.183

频段:

5G

PHY模式:

11ax HE 160MHz

协商速率(Mbps) ↓↑:

1441/1441

RSSI(dBm):

-51

信噪比(dB):

44.0

空口时延(ms):

8

- # 如果接入Wi-Fi信号的是2.4G，则重新接入5G频段的Wi-Fi信号。
- i. 在终端的WLAN设置中，忘记已连接的WLAN网络，重新搜索和连接，再检查频段是否为5G。
 - ii. 如果频段仍为2.4G，则需要先确认下终端型号是否支持5G频段。建议更换支持5G频段的手机进行测试。
 - iii. 如果手机支持5G频段，但仍接入2.4G频段的信号，则可以修改5G频段的Wi-Fi名称，在WLAN设置中搜索和连接5G频段的Wi-Fi信号。
- # 登录Web网管，进入“配置 > 无线网络配置”。

SSID列表				
<div>新建 删除 刷新</div>				
SSID名称	频段	业务VLAN	安全配置	AP Zone
<input type="checkbox"/> mywifi_5G	5G(Radio1)+5G/6G(Radio2)	101	WPA-WPA2	default
<input type="checkbox"/> mywifi	2.4G+5G(Radio1)+5G/6G(Radio2)...	101	WPA-WPA2	default
10 共2条				

单击“新建”按钮，配置新的SSID，选中5G射频。



- b. 将5G频宽修改成160 MHz。
登录Web网管，进入“高级 > 射频配置 > 射频规划”，在射频列表中找到5G信号，单击操作图标，手动设置频宽。



- c. 确认上网的出口带宽。
使用有线终端接入网络测速，查看测速结果。如果测速较低，则需联系运营商检查网络，或者升级出口带宽。
- 命令行方式（供技术人员使用）
 - a. 将终端接入5G频段的Wi-Fi信号。
在手机的WLAN设置中，可以查看已连接的Wi-Fi信息，包括建链速率（连接速度），信号频段（频率），Wi-Fi标准（WLAN能力）。不同型号的手机，显示信息有所差异。



在Leader AP上查看测速低的终端连接的Wi-Fi信号频段，Wi-Fi标准，协商速率等信息。

```
<HUAWEI> display station all | include 00e0-fc12-3456
```

Rf/WLAN: Radio ID/WLAN ID

Rx/Tx: link receive rate/link transmit rate(Mbps)

STA MAC SSID	Ap name Status	Rf/WLAN	Band	Type	Rx/Tx	RSSI	VLAN	IP address
00e0-fc12-3456 mywifi	00e0-fc07-6f80 Normal	1/2	5G	11ax	2162/1297	-42	101	192.168.101.253

Total: 1 2.4G: 0 5G: 1 6G: 0

如果接入Wi-Fi信号的是2.4G，则重新接入5G频段的Wi-Fi信号。

- 在终端的WLAN设置中，忘记已连接的WLAN网络，重新搜索和连接，再检查频段是否为5G。
- 如果频段仍为2.4G，则需要先确认下终端型号是否支持5G频段。建议更换支持5G频段的手机进行测速。
- 如果手机支持5G频段，但仍接入2.4G频段的信号，则可以修改5G频段的Wi-Fi名称，在WLAN设置中搜索和连接5G频段的Wi-Fi信号。

配置5G频段信号的SSID名称。

```
system-view
wlan
ssid-profile name mywifi5g
ssid mywifi_5G
quit
```

配置5G频段信号的SSID生效，除SSID模板和生效射频ID，其他配置和原VAP相同。

```
system-view
wlan
vap-profile name mywifi5g
service-vlan 101
ssid-profile mywifi5g
security-profile huawei-leaderap-business
traffic-profile huawei-leaderap-business
ap-zone default
radio 1
```

- b. 将5G频宽修改成160 MHz。

在AP射频视图下，配置频宽。

```
system-view
wlan
ap-id x
radio 1
calibrate auto-channel-select disable
channel 160mhz 36
```

- c. 检查网线的物理协商速率是否为千兆及以上。

在AP上查看具体接口的协商速率。

```
<HUAWEI> display interface gigabitethernet 0/0/0
...
Speed : 100, Loopback: NONE
```

如果结果是百兆，则需检查网线规格是否为超5类（CAT5E）及以上，水晶头线序是否正确等。

- d. 确认上网的出口带宽。

使用有线终端接入网络测速，查看测速结果。如果测速较低，则需联系运营商检查网络，或者升级出口带宽。

2.1.5 Wi-Fi 网络卡顿

现象描述

终端连接Wi-Fi后，进行音视频通话时出现卡顿。

可能原因

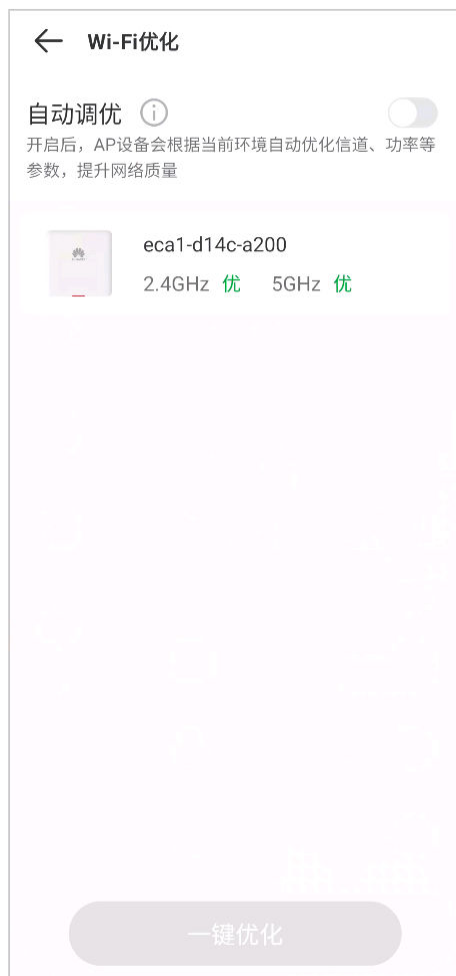
- 同频干扰大。
- 2.4G信号配置的频宽过大。
- AP的信号弱。

操作步骤

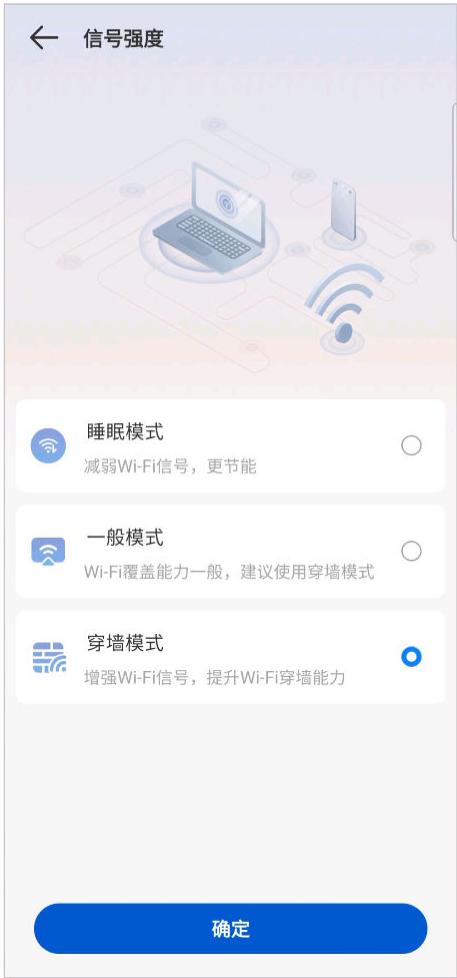
- 手机APP方式

- a. 开启自动调优，降低同频干扰。

点击“本地管理网络 > 选择网络卡片 > 查看更多 > Wi-Fi优化”，开启自动调优功能。



- b. 修改Wi-Fi的信号强度，终端重新搜索Wi-Fi信号。
进入Leader AP的管理界面，点击“信号强度”，设置为穿墙模式。



• Web网管方式

- a. 开启自动调优，降低同频干扰。

登录Web网管，进入“配置 > 系统配置 > 射频调优”，开启自动调优功能。



进入“高级 > 射频配置 > 射频规划”，在射频列表中单击对应AP射频后的操作按钮，修改信道为自动方式。修改后单击“立即调优”按钮，手动触发一次调优。



- b. 将2.4G频宽修改成20 MHz。
登录Web网管，进入“高级 > 射频配置 > 射频规划”，在射频列表中单击对应AP射频后的操作按钮，修改2.4G射频的频宽为手动方式。



- c. 修改Wi-Fi的信号强度，终端重新搜索Wi-Fi信号。
选择“高级 > 射频配置 > 射频规划”，在射频列表中单击对应AP射频后的操作按钮，修改射频参数。



• 命令行方式（供技术人员使用）

- a. 开启自动调优，降低同频干扰。
在终端接入的AP上查看射频上的信道利用率和同频干扰。
[HUAWEI-diagnose] display lmac base-info radio 1
...
ChannelUtilizationRate(%) : 76
CoChanInterferenceRate(%) : 64
...
如果信道利用率高并且大部分是同频干扰导致，可在Leader AP上进入AP的射频视图，开启信道自动调优功能。
system-view
wlan
ap-id x
radio 1
undo calibrate auto-channel-select disable
开启定时调优功能，并触发一次立即调优。
system-view
wlan
calibrate enable schedule time 03:00:00
calibrate manual startup
Warning: The operation may cause business interruption, Continue? [Y/N]:y
- b. 将2.4G频宽修改成20 MHz。
在AP射频视图下，配置频宽。
system-view
wlan


```
ap-id x
radio 0
calibrate auto-channel-select disable
channel 20mhz 6
```

- c. 修改Wi-Fi的信号强度，终端重新搜索Wi-Fi信号。

在AP射频视图下，配置最大发射功率。

```
system-view
wlan
ap-id x
radio x
calibrate auto-txpower-select disable
eirp 127
```

3 故障处理：AP 上下线类问题

3.1 AP在AC上无法上线

3.2 AP异常掉线

3.1 AP 在 AC 上无法上线

步骤1 查询AP上线失败记录

执行命令**display ap online-fail-record**查看AP上线失败的具体原因。

```
<AC> display ap online-fail-record mac 1047-80b1-56a0
-----
MAC          Last fail time    Reason
-----
1047-80b1-56a0  2015-01-20/15:48:06  The AP is added to the AP blacklist.
-----
Total records: 1
```

根据对应的失败原因，查询产品文档进行相应处理。

步骤2 检查AP状态

执行命令**display ap all**查看AP状态。

```
<AC> display ap all
Total AP information:
idle : idle          [1]
nor  : normal        [2]
-----
ID  MAC          Name          Group IP          Type          State STA Uptime
-----
0   60de-4476-e360 L1_003        default 192.168.109.254 AirEnginexxxxS nor 0 2D:5H:48M:44S
1   dcd2-fc04-b500 dcd2-fc04-b500 default -        AirEnginexxxxS idle 0 -
2   dcd2-fc9d-0bb0 area_3        default 192.168.109.253 AirEnginexxxxS nor 0 2D:5H:52M:38S
-----
Total: 3
```

AP常见的状态主要有：

- normal，表示AP在AC上成功注册。
- fault，表示AP未能在AC上成功注册。请执行下一步检查。
- download，表示AP版本升级加载系统软件中，请等待AP升级完成后再次查看AP状态。

- committing，表示AC正在向AP下发业务。
- config-failed，表示AP初始化配置失败，请检查网络连接是否正常，AC和AP互ping是否丢包，ping长度大于1600的报文检查中间网络MTU值是否过小，如果中间网络配置了NAT穿越，请检查NAT通信是否正常。执行命令**display cpu-defend statistics wired**查看cpu-defend的统计信息中capwap项的丢包情况，如果丢包严重，请评估设置的阈值是否合理。如果长时间无法恢复，请收集相关信息，寻求技术支持。
- name-conflicted，表示AP名称冲突，请在WLAN视图下执行命令**ap-rename ap-id ap-id new-name ap-name**更改AP名称。
- ver-mismatch，表示AP软件类型与AC软件版本不匹配，执行命令**display ap version all**检查AP的版本，执行命令**display version**检查AC的版本，检查AC和AP是否配套。如果不配套请参考《AC版本说明书》中“软件版本兼容性”章节，并下载配套的AP大包文件，参照升级指导书升级单个AP，升级后再查看AP状态。AC和AP之间的版本配套关系请参考[WLAN AP版本配套和形态速查表](#)。
如果采用自动升级或者在线升级方式升级AP，请确保AC上或者FTP/TFTP目录中有AP的升级文件且升级文件正确，否则也有可能导致AP无法上线。
- standby，备用AC上AP的状态。
- idle，表示AP处于空闲状态，离线添加AP后AP的状态。请确认AP是否正常接入到网络中。

步骤3 检查AP是否分配到IP地址

AP获取到IP地址，是AP与AC建立CAPWAP隧道的前提条件之一。通常使用DHCP服务器为AP提供IP地址，可在DHCP服务器上查看AP是否分配到IP地址。也可以为AP配置静态IP地址上线。

可以通过在AP的网关设备上输入命令**display arp**查看所有的ARP映射表项，通过MAC地址对比看AP是否已经获取到地址，并用ping测试该地址。

```
[AC] display arp
IP ADDRESS      MAC ADDRESS      EXPIRE(M) TYPE      INTERFACE  VPN-INSTANCE
                VLAN/CEVLAN PVC
-----
.....
10.1.1.2         0200-0000-0017    I -      Vlanif1219
10.1.15.251      dcd2-fc22-d880 2    D-0      GE0/0/1
                1219/-
10.1.15.247      1047-80af-fbc0 16    D-0      GE0/0/1
                1219/-
10.1.15.246      dcd2-fc9a-c800 15    D-0      GE0/0/1
                1219/-
10.1.15.248      dcd2-fcf4-6420 6     D-0      GE0/0/1
                1219/-
10.1.1.219       4c1f-cc6b-c248 16    D-0      GE0/0/1
```

用ping测试该MAC对应的IP地址。如果能够ping通说明AP已经获取到了地址；如果ping不通，说明AP获取的地址已经过期或没有获取到地址。

步骤4 检查AP与AC间的网络是否通畅

在AC和AP上分别执行ping命令，查看能否相互ping通。

- 如果无法ping通，须检查IP地址是否过期，中间网络设备的链路是否良好，同时检查链路相关配置。
- 如果出现ping时延过大或丢包的情况，请检查中间网络是否出现环路（可通过各端口的统计信息进行判断）。

- 如果ping包没问题，进一步测试ping大包是否可达，如果ping大包不通，则capwap报文也无法发送到AP侧。
`<AC> ping -s 2000 <ap-ip>`
- 如果ping包不丢包，延时正常，执行下一步检查。

步骤5 查看AC是否支持当前的AP款型

执行**display ap-type all**，如果AP款型不在列表中，说明当前版本的AC不支持此AP款型，请参考升级指导书升级AC版本，或在AC上手动添加ap-type。

AC和AP之间的版本配套关系，请参考[WLAN AP版本配套和形态速查表](#)。

AC上手动添加ap-type方法：

- 通过命令行**display ap-type undefined record**确认目标AP类型已被AC识别为未知AP款型。

```
<AC> display ap-type undefined record
```

AP type	Type ID	Report AP MAC	Report Time
AirEnginexxxxS xx		00e0-fc76-e360	2019-04-28/23:39:00

Total : 1

如果列表中没有目标AP的未识别记录，则应先解决AC/AP网络不通的问题，或不是该原因导致的AP上线失败，需从其他方面入手排查。

- 通过命令**auto create ap-type all**将未识别AP款型添加到AP支持列表中。

```
<AC> system-view
```

```
[AC] wlan
```

```
[AC-wlan-view] auto create ap-type all
```

步骤6 查看CAPWAP链路是否已经创建

在AP诊断视图下执行命令**display capwap link all**查看CAPWAP链路是否已经创建。

```
[AP-diagnose] display capwap link all
```

Info: This operation may take a few seconds. Please wait for a moment.done.

ID	MAC	CPort	DPort	Type	State	Role	VPN	DstAddr	SrcAddr
0	7079-90ba-8ea0	5246	5247	AC	RUN	Client -		10.120.1.1	10.120.5.60
1	7079-90ba-8ea0	5246	5247	AC	RUN	Client -		10.120.1.2	10.120.5.60
2	4cfa-caff-f560	55450	65535	INAP	RUN	Server -		10.120.7.6	10.120.5.60

关注DstAddr为目的AC的capwap source地址的链路。如果不存在目的AC的CAPWAP链路信息，关注Type为AC的其他链路状态，如果存在链路且状态为RUN，说明AP在其他AC上线，可通过DstAddr找到这台AC，尤其是支持Leader AP功能的AP，可能被误切为FAT模式，使其他AP都在该Leader AP上线。

步骤7 检查AP上行端口模式

检查AP上行端口模式是否为endpoint或middle，AC和root AP相连的有线口必须工作在root模式，尤其是中心AP+RU的场景，默认情况下中心AP的XGE口才可作为上行口连AC，GE口才可作为下行口连RU，不可共用或者用反。

更多信息请参见：[AP上行有线口配置了endpoint模式，AP重启后无法上线](#)。

步骤8 检查AP是否通过AC认证

执行命令**display ap global configuration**查看当前认证模式（默认AP是MAC-auth模式）。

```
[AC-wlan-view] display ap global configuration
```

```
AP auth-mode          : MAC-auth
AP LLDP switch        : disable
AP username/password  : -/*****
AP data collection     : disable
AP data collection interval(minute): 5
-----
```

如果认证模式为MAC认证或SN认证。执行命令**display ap unauthorized record**查看是否存在认证未通过的AP信息。

```
<AC> display ap unauthorized record
Unauthorized AP record: Total number: 1
-----
AP type: AirEnginexxxxS
AP SN: xxxxxxxxxxxxxxxxx
AP MAC address: xxxx-xxxx-xxxx
AP IP address: 192.168.109.252
Record time: 2020-01-22 17:23:17
-----
```

如果存在，可以在WLAN视图下执行**ap-confirm**命令让AP认证通过。

```
[AC-wlan-view] ap-confirm mac dcd2-fc22-d880
```

或执行**ap-whitelist { mac mac-address | sn ap-sn }**命令添加AP到白名单中。

```
[AC-wlan-view] ap whitelist mac dcd2-fc22-d880
```

也可以在WLAN视图下执行**ap-id ap-id ap-mac mac-address**命令离线添加该AP，解决认证不通过问题。

```
[AC-wlan-view] ap-id 10 ap-mac dcd2-fc22-d880
```

步骤9 检查AP的MAC地址是否发生漂移

如果在AC上通过命令**display ap all**和**display ap online-fail-record**无法查询到AP的表项，则考虑可能是AP MAC地址出现漂移或者DHCP服务器发出的offer报文dst.port=src.port。

建议观察AP的MAC地址从哪个端口学到，是不是存在变化，并跟踪该地址到各交换机上查询。

登录核心交换机，连续多次执行命令查询指定AP的MAC地址从哪个端口学习到，若学习端口出现变化，则可能是MAC地址漂移。

```
[Switch] display mac-address | include 9017-acb9-39e0
```

MAC Address	VLAN/VSI	Learned-From	Type
9017-acb9-39e0	2009/-	GE0/0/1	dynamic

如果确认AP MAC地址出现漂移，则需要排查组网问题。

步骤10 打开全流程跟踪查看相关信息

在AC全局视图下执行命令**trace enable**打开全流程跟踪开关，然后输入要跟踪对象的MAC地址（可以是AP或终端STA的MAC）**trace object mac-address ap-mac**。

```
[AC] trace enable //打开全流程跟踪开关
```

```
[AC] trace object mac-address dcd2-fc22-d880 //输入要跟踪对象的MAC地址
```

全流程跟踪能够根据对象的MAC地址或IP等信息进行跟踪，打印显示被跟踪对象与AC或AP的报文交互过程，并打印一些故障信息，可对比正常流程，查看故障AP进行到哪一步骤，然后重点进行排查。

----结束

3.2 AP 异常掉线

步骤1 检查AP下线原因记录

在AC上执行命令**display ap offline-record all**，查看AP下线原因。

```
<AC> display ap offline-record all
-----
MAC                Last offline time    Reason
-----
0023-0024-0080     2015-01-31/16:21:50  Reboot by ap-reset command
60de-4476-e360     2015-01-31/14:02:35  Reboot by ap update reset command
1047-80b1-56a0     2015-01-31/13:52:35  Reboot by ap update reset command
-----
Total records: 3
```

根据对应的失败原因，针对性查询产品文档进行相应处理。

步骤2 如果AP下线原因为AC从iMaster-NCE控制器上离线超过90天，则确认AC是否被误切换为云模式，将其切换回传统模式。

```
<AC> display ac-mode
Ac mode is : Cloud
```

切换AC到传统模式。

```
<AC> system-view
[AC] ac-mode standard
```

步骤3 如果AP的下线原因是License过期，请联系华为售前或代理商购买新的License，然后参考《[无线接入控制器 License使用指南](#)》，加载新的License。

步骤4 如果AP下线原因为心跳超时，请按如下步骤进行排查。

1. 如果使用交换机作为AP网关，需要排查交换机上是否存在大量TC报文，导致AP的ARP表项频繁刷新，引发AP掉线。

正常情况下，当STP检测到网络的拓扑发生变化，会发送TC报文通知ARP模块对ARP表项进行老化或者删除，此时设备需要重新进行ARP学习，以获得最新的ARP表项信息。但是如果网络的拓扑变化频繁，或者网络中设备的ARP表项很多，ARP的重新学习会导致网络中的ARP报文过多，极大地占用系统资源，影响其他业务的正常运行。

为了尽量避免这种情况的发生，可以让ARP表不响应TC报文，这样即使网络的拓扑发生了变化，网络中设备的ARP表项也不会被老化或者删除。同时，开启MAC刷新ARP功能，避免ARP表项没有得到及时刷新，可能导致用户业务中断。

```
<Switch> display stp topology-change //查看拓扑变化
<Switch> display stp tc-bpdu statistics //查看端口TC报文收发计数
```

如果交换机上存在大量TC报文，可以执行如下命令解决。

```
<Switch> system-view
[Switch] mac-address update arp //开启MAC刷新ARP功能，即MAC地址的出接口变化时，通知更新ARP表项的出接口
[Switch] arp topology-change disable //关闭设备响应TC报文的功能，即当设备收到TC报文时，不对ARP表项进行老化或删除
```

2. 检查AC、中间交换机上是否存在IP冲突或者ARP miss。

可通过命令行**display trapbuffer**查看设备Trap缓冲区信息，看是否存在大量“ARP detects IP conflict”或“arp-miss”相关告警。排查网络中是否存在与AP网关冲突的IP地址。

如果是AC VRRP双机热备场景且AC作为地址池给AP分配IP地址，需要确保地址池中已排除VRRP的虚地址，否则会出现AC将虚地址分配出去导致网络中出现IP地址冲突的场景。

查看是否存在VRRP虚地址冲突。

```
<AC> display arp ip-conflict track
Conflict type      : Local IP conflict
IP address        : 192.168.1.1
System time       : 2011-11-19 03:22:16+08:00
Conflict count     : 1
Suppress count     : 0
Local interface    : Vlanif100
Receive interface  : GE0/0/1
Receive VLAN/CEVLAN : 100/0
Receive MAC        : 0000-0a88-36f5
```

将VRRP虚地址从地址池中排除。

```
<AC> system-view
[AC] interface vlanif 100
[AC-Vlanif100] dhcp server excluded-ip-address 192.168.1.1
Warning: The address is in used or conflict state. Are you sure to continue excluding the address?[Y/N]y
```

3. 检查AC长ping AP时是否存在丢包。

- 如果不能ping通或丢包严重，请检查网络是否正常、网线等连接线是否老化。
- 如果能够ping通，请登录AP获取日志文件，查看AP掉线时间点记录的网络ping结果。如果ping包结果超时，则AP下线为网络异常导致，请联系技术支持人员进行定位。

4. 检查中间网络是否存在某类型报文过量的情况。

大量报文（如ND报文等）上送设备，会导致设备CPU使用率过高，很可能导致AP掉线。在AC上执行命令**display cpu-defend statistics**，查看上送CPU的报文统计。如果存在某些报文数量过多，则需要排查网络，找到该类报文的来源，具体请联系技术支持人员寻求技术支持。

```
<AC> display cpu-defend statistics wireless
```

Packet Type	Pass Packets	Drop Packets
8021X	0	0
8021X-ident	0	0
8021X-start	0	0
arp-miss	0	0
arp-reply	0	0
arp-request	0	0
dhcp-client	0	0
dhcp-server	0	0
dns	0	0
fib-hit	0	0
ftp-client	0	0
ftp-server	0	0
http-client	0	0
icmp	0	0
ip-option	0	0
snmp	0	0
ssh-server	0	0
tcp	0	0
telnet-client	0	0
telnet-server	0	0
ttl-expired	0	0
unknown-multicast	0	0
unknown-packet	0	0

5. 排查接入层交换机的配置，检查是否存在风暴告警或存在大量广播报文。

在交换机上执行命令**display interface**，查看接口上的组播和广播报文的统计信息，并观察组播、广播报文增长速率。

```
<Switch> display interface gigabitethernet 0/0/1
GigabitEthernet 0/0/1 current state : UP
```

```
Line protocol current state : UP
Description:
Switch Port,Link-type : access(negotiated),
PVID : 1, TPID : 8100(Hex), The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0025-9ef4-abcd
Last physical up time : -
Last physical down time : 2015-12-21 16:12:29 UTC+08:00
Current system time: 2012-06-05 18:56:41
Port Mode: COMMON FIBER, Transceiver: 1000_BASE_SX_SFP
Speed : 1000, Loopback: NONE
Duplex: FULL, Negotiation: ENABLE
Mdi : -, Flow-control: DISABLE
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 0 bits/sec, Record time: -
Output peak rate 0 bits/sec, Record time: -
Input: 7650 packets, 1327062 bytes
  Unicast: 0, Multicast: 7650
  Broadcast: 0, Jumbo: 0
Discard: 0, Pause: 0
Total Error: 0
CRC: 0, Giants: 0
Runts: 0, Fragments: 0
Alignments: 0, Symbols: 0
Output: 38348 packets, 3683776 bytes
  Unicast: 0, Multicast: 32314
  Broadcast: 6034, Discard: 0
  Pause: 0
Input bandwidth utilization threshold : 80.00%
Output bandwidth utilization threshold: 80.00%
Input bandwidth utilization : 0%
Output bandwidth utilization : 0%
```

如果该接口接收到的广播、组播报文过多，则需要继续检查是否配置了风暴控制。

在交换机上执行命令**display storm-control**，查看对应接口上配置的风暴控制信息。

```
<Switch> display storm-control interface gigabitethernet 0/0/1
PortName   Type      Rate      Mode Action Punish- Trap Log Int Last-
              (Min/Max)      Status      Punish-Time
-----
GE0/0/1    Multicast 1000      Pps Block Normal Off On 90 -
              /2000
GE0/0/1    Broadcast 1000      Pps Block Normal Off On 90 -
              /2000
GE0/0/1    Unicast   1000      Pps Block Normal Off On 90 -
              /2000
```

如果“Action”显示为“Error-Down”，则建议先排除引起接口Error-Down的原因。有以下两种方式可以恢复接口状态。

- 手动恢复（Error-Down发生后）

当处于Error-Down状态的接口数量较少时，可在该接口视图下依次执行命令**shutdown**和**undo shutdown**，或者执行命令**restart**，重启接口。

- 自动恢复（Error-Down发生前）

如果处于Error-Down状态的接口数量较多，逐一手动恢复接口状态将产生大量重复工作，且可能出现部分接口配置遗漏。为避免这一问题，用户可在系统视图下执行命令**error-down auto-recovery cause storm-control interval interval-value**使能接口状态自动恢复为Up的功能，并设置接口自动恢复为Up的延时时间。可以通过执行命令**display error-down recovery**查看接口状态自动恢复信息。

6. 如果有获取报文头的条件，可同时获取AP、AC侧CAPWAP报文，查看中间链路是否存在丢包。

----结束

4 故障处理：无线终端认证类问题

- 4.1 802.1x认证失败
- 4.2 Portal认证失败

4.1 802.1x 认证失败

问题现象确认

确认是新部署网络还是已有网络出现问题；是单个终端无法认证，还是所有终端都无法正常认证。

信息收集

- 1) AC和AP的一键式诊断信息以及故障时间点的AC和AP的日志和诊断日志文件。
- 2) 故障终端的mac信息以及trace和station-trace信息。

关键配置检查

- 1) 检查SSID的业务VLAN配置是否正确：

```
[HUAWEI] display vap-profile all
FMode : Forward mode
STA U/D : Rate limit client up/down
VAP U/D : Rate limit VAP up/down
BR2G/5G : Beacon 2.4G/5G rate
```

Name	FMode	Type	VLAN	AuthType	STA U/D(Kbps)	VAP U/D(Kbps)	BR2G/5G(Mbps)
default	direct	service	VLAN 1	Open	-/-	1/6	0
vap_dot1x	tunnel	service	VLAN 1	WPA2+802.1X	-/-	1/6	3

Total: 2

如果没有配置业务VLAN，或者业务VLAN使用VLAN 1、CAPWAP源地址所在VLAN、AP管理网段所在VLAN，会出现终端认证失败的情况，需要修改业务VLAN

```
<HUAWEI> system-view
[HUAWEI] vap-profile name dot1x_test
[HUAWEI-wlan-vap-prof-dot1x_test] service-vlan vlan-id 100
```

2) 通过命令**display aaa online-fail-record mac-address H-H-H**查看终端上线失败记录，确认用户授权是否正常，如果用户上线失败原因（User online fail reason）显示Authorization data error，则表示授权失败。

```
[HUAWEI] display aaa online-fail-record mac-address 00e0-fc76-e360 //替换为实际用户MAC
```

```
-----
User name           : test
Domain name         : domaintest
User MAC            : 00e0-fc76-e360
User access type     : 802.1x
User access interface : Wlan-Dbss17496
Qinq vlan/User vlan  : 0/200
User IP address      : -
User IPV6 address    : -
User ID              : 32873
User login time      : 2020/10/24 16:32:34
User online fail reason : Authorization data error
Authen reply message : -
User name to server   : test
AP ID                : 0
Radio ID             : 0
AP MAC               : xxxx-xxxx-xxxx
SSID                  : dot1x_test
-----
```

RADIUS服务器授权了相关权限（如VLAN或者ACL等），但设备上无对应的授权内容配置（如未创建授权VLAN或者未创建授权ACL），会因为授权失败而导致认证失败。

通过业务诊断功能，追踪终端用户上线认证过程，看到RADIUS服务器下发的授权内容：

```
[HUAWEI] trace object mac-address 00e0-fc76-e360
[HUAWEI] trace enable
```

- 授权VLAN检查失败

```
[BTRACE][2020/10/24 16:48:14][6144][RADIUS][00e0-fc76-e360]:
Received a authentication accept packet from radius server(server ip = xx.xx.xx.xx).
[BTRACE][2020/10/24 16:48:14][6144][RADIUS][00e0-fc76-e360]:
Server Template: 4
Server IP : xx.xx.xx.xx
Server Port : 1812
Protocol: Standard
Code : 2
Len : 194
ID : 194
[Tunnel-Type] [6] [13]
[Tunnel-Medium-Type] [6] [6]
[Tunnel-Private-Group-ID] [6] [201]
[EAP-Message] [6] [03 4a 00 04 ]
[State] [16] [\001uY\311\025N]
[MS-MPPE-Send-Key] [52] [fb a1 e9 55 16 62 a3 e5 da 35 fc ce 3e 8f ae 7d ac 0a d6 0b
20 59 ad 82 a8 66 88 06 6a 81 10 82 61 95 2e cf 44 50 c0 79 e5 3f a4 32 43 45 a5 9e 2b c4 ]
[MS-MPPE-Recv-Key] [52] [fb a1 e9 65 b1 18 6d 60 8f 0a ed af 53 1e 26 8a e6 18 9d 26
8c 21 c8 4f c2 8a 6a d5 a8 85 8a 9d ba d8 be 8d 97 b8 b8 d3 24 04 21 23 90 71 33 35 f4 6b ]
[Message-Authenticator] [18] [00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ]
[BTRACE][2020/10/24 16:48:14][6144][RADIUS][00e0-fc76-e360]:Send authentication reply message
to AAA.
[BTRACE][2020/10/24 16:48:14][6144][AAA][00e0-fc76-e360]:
AAA receive AAA_RD_MSG_AUTHENACCEPT message(50) from RADIUS module(235).
[BTRACE][2020/10/24 16:48:14][6144][AAA][00e0-fc76-e360]:
CID:57 TemplateNo:4 SerialNo:73
SrcMsg:AAA_RD_MSG_AUTHENREQ
PriyServer::: Vrf:0
SendServer:12.12.12.1 Vrf:0
SessionTimeout:0 IdleTimeout:0
AcctInterimInterval:0 RemanentVolume:0
InputPeakRate:0 InputAverageRate:0
OutputPeakRate:0 OutputAverageRate:0
InputBasicRate:0 OutputBasicRate:0
```

```
InputPBS:0 OutputPBS:0
Priority:[0,0] DNS:[0.0.0.0, 0.0.0.0]
ServiceType:0 LoginService:0 AdminLevel:0 FramedProtocol:0
LoginIpHost:0 NextHop:0
EapLength:4 ReplyMessage:
TunnelType:13 MediumType:6 PrivateGroupID:201
WlanReasonCode:0
[BTRACE][2020/10/24 16:48:14][6144][AAA][00e0-fc76-e360]:
[AAA ERROR]AAA check authen ack, check VLANID error!
[BTRACE][2020/10/24 16:48:14][6144][AAA][64e5-99f3-18f6]:Radius authorization data error.
[BTRACE][2020/10/24 16:48:14][6144][AAA][64e5-99f3-18f6]:
[AAA ERROR]authen finish,the authen fail code is:16,reason is:Radius authorization data error.
```

- 授权ACL检查失败

```
Received a authentication accept packet from radius server(server ip = xx.xx.xx.xx).
[BTRACE][2020/10/24 16:52:19][6144][RADIUS][00e0-fc76-e360]:
Server Template: 4
Server IP : xx.xx.xx.xx
Server Port : 1812
Protocol: Standard
Code : 2
Len : 182
ID : 205
[Filter-Id ] [6 ] [3000]
[EAP-Message ] [6 ] [03 4c 00 04 ]
[State ] [16] [\001uY\314\321\003]
[MS-MPPE-Send-Key ] [52] [bd ce 7f 1d bf 78 33 d4 6c 45 d8 d0 1b f7 ee d2 02 16 7a ac
fd 62 25 88 f7 84 7a 22 44 d8 01 8a 99 a3 33 66 7d 47 e9 a7 ed 88 d5 01 f8 62 4f 9d cd 56 ]
[MS-MPPE-Recv-Key ] [52] [bd ce 7f 54 6f 27 35 d1 01 5c f1 5e aa e8 27 91 c7 8b 89 2f
06 8f ac 46 13 5c 92 78 ec cf 39 aa dc bb f8 ff b1 b8 5c 42 6b f8 ca 80 76 b1 e8 35 c9 ed ]
[Message-Authenticator ] [18] [00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ]
[BTRACE][2020/10/24 16:52:19][6144][RADIUS][00e0-fc76-e360]:Send authentication reply message
to AAA.
[BTRACE][2020/10/24 16:52:19][6144][AAA][00e0-fc76-e360]:
AAA receive AAA_RD_MSG_AUTHENACCEPT message(50) from RADIUS module(235).
[BTRACE][2020/10/24 16:52:19][6144][AAA][00e0-fc76-e360]:
CID:58 TemplateNo:4 SerialNo:75
SrcMsg:AAA_RD_MSG_AUTHENREQ
PriServer::: Vrf:0
SendServer:12.12.12.1 Vrf:0
SessionTimeout:0 IdleTimeout:0
AcctInterimInterval:0 RemanentVolume:0
InputPeakRate:0 InputAverageRate:0
OutputPeakRate:0 OutputAverageRate:0
InputBasicRate:0 OutputBasicRate:0
InputPBS:0 OutputPBS:0
Priority:[0,0] DNS:[0.0.0.0, 0.0.0.0]
ServiceType:0 LoginService:0 AdminLevel:0 FramedProtocol:0
LoginIpHost:0 NextHop:0
EapLength:4 ReplyMessage:
TunnelType:0 MediumType:0 PrivateGroupID:
ACLID:3000
WlanReasonCode:0
[BTRACE][2020/10/24 16:52:19][6144][AAA][00e0-fc76-e360]:
[AAA ERROR]AAA check radius authen ack, check acl error!
[BTRACE][2020/10/24 16:52:19][6144][AAA][00e0-fc76-e360]:Radius authorization data error.
[BTRACE][2020/10/24 16:52:19][6144][AAA][00e0-fc76-e360]:
[AAA ERROR]authen finish,the authen fail code is:16,reason is:Radius authorization data error.
```

确认是否需要对应的授权。

- 如果需要，则需要在设备上创建对应的授权内容，如授权VLAN需要在设备上创建对应VLAN；如授权ACL需要创建对应ACL，并且在ACL中配置相应规则。
- 如果不需要，可以修改RADIUS服务器上的授权策略，将对应授权内容删除，也可以在设备通过配置忽略对应的授权内容，配置命令如下：
忽略授权VLAN：

```
[HUAWEI] radius-server template radius_test
[HUAWEI] radius-server attribute translate
[HUAWEI] radius-attribute disable Tunnel-Private-Group-ID receive
```

忽略授权ACL：

```
[HUAWEI] radius-server template radius_test
[HUAWEI] radius-server attribute translate
[HUAWEI] radius-attribute disable Filter-Id receive
```

3) 认证完成后如果需要由认证服务器下发CoA/DM，需要在AC上提前配置监听CoA/DM消息的源接口，否则会导致AC上无法处理CoA/DM消息。

```
<HUAWEI> system-view
[HUAWEI] radius-server authorization server-source all-interface
```

常规处理建议

- 1) display aaa online-fail-record mac-address <mac-address>根据终端掉线原因查询产品文档，根据产品文档描述的每种掉线原因的处理建议进行处理；
- 2) 收集现网trace信息、AC/AP日志、mac地址等必要信息，根据日志内容对终端掉线行为进行具体分析。

4.2 Portal 认证失败

问题现象确认

确认是新部署网络还是已有网络出现问题；是单个终端无法认证，还是所有终端都无法正常认证。

信息收集

- 1) AC和AP的一键式诊断信息以及对应时间点的AC/AP的日志和诊断日志文件。
- 2) 对故障终端mac和ip-address的trace和station-trace信息，需同时采集。

关键配置检查

1) 检查监听接口配置，V200R021C00及之后版本增加了全零监听接口配置，如果没有预先配置监听接口，会导致AC侧无法处理portal认证请求：

```
<HUAWEI> system-view
[HUAWEI] portal local-server server-source all-interface
```

HTTP/HTTPS协议的Portal认证（如Aruba ClearPass、Cisco的ISE服务器），配置外置Portal服务器的监听接口：

```
<HUAWEI> system-view
[HUAWEI] portal web-authen-server server-source all-interface
```

Portal认证协议的外置Portal服务器的监听接口配置：

```
<HUAWEI> system-view
[HUAWEI] web-auth-server server-source all-interface
```

2) 检查DNS放通配置。查看系统视图，有没有配置**portal pass dns enable**（默认不使能），如果没有配置，需要通过free rule的方式将DNS服务器地址放通，如下示例，将DNS服务器地址8.8.8.8通过free rule放通。

```
[HUAWEI] free-rule-template name default
[HUAWEI-free-rule-default] display this
```

```
#
free-rule-template name default_free_rule
free-rule 1 destination ip 8.8.8.8 mask 255.255.255.0 source ip any
#
[HUAWEI-free-rule-default] quit
[HUAWEI] authentication-profile name authen_portal
[HUAWEI-authentication-profile-authen_portal] display this
#
authentication-profile name authen_portal
portal-access-profile access_portal
access-domain domain_test
free-rule-template default_free_rule
#
```

3) 终端在Portal认证成功之前无法访问DNS服务器，出现无法重定向到Portal页面的情况，有如下三个可能原因：

- 网络中没有DNS服务器（一般是测试阶段，还没有部署DNS服务器）。
- AC和AP没有通过free-rule放通DNS服务器IP地址。
- 终端与DNS服务器网络不通。

可以按如下步骤检查网络相关配置：

1. 检查网络中是否有DNS服务器，DHCP Server是否给终端分配了DNS服务器；如果网络中没有DNS服务器，则访问域名无法触发重定向。
2. 检查free-rule是否放通DNS服务器IP地址，如果没有放通，在free-rule模板下放通DNS服务器IP地址，再将free-rule模板绑定到认证模板。
3. 在终端网关上以网关地址作为源IP地址ping DNS服务器，看路由是否可达，如果路由不可达，需要排查中间网络。
4. 在终端上通过nslookup命令测试DNS服务器是否能正确解析访问的域名，如果不能解析，请排查DNS服务器。

常规处理建议

收集现网trace、station-trace、AC/AP日志、mac地址等必要信息，根据日志内容对终端掉线行为进行具体分析。

5 故障处理：终端体验类问题

- 5.1 终端异常掉线
- 5.2 终端搜不到WiFi信号
- 5.3 终端上线失败
- 5.4 终端获取不到地址
- 5.5 终端网络慢
- 5.6 终端漫游问题
- 5.7 终端业务不通
- 5.8 终端station-trace解析

5.1 终端异常掉线

问题现象确认

确认终端异常掉线的现象：

- 是终端关联的SSID信号断开，还是终端正常关联SSID但是上网业务终端。基本判断指标如是否WiFi图标消失，还是显示为小地球或提示无互联网连接等。
- 是多个终端批量掉线，还是单个终端或某一类特定终端异常掉线。

信息收集

- 终端的MAC地址和终端掉线的时间点。
- 终端掉线前关联AP的一键诊断信息和包含掉线时间点的AC/AP设备的日志文件。

关键配置检查

步骤1 确认射频调优配置是否合理：

```
<HUAWEI> display wlan calibrate global configuration
```

```
-----  
Mode                : auto  
Auto start time      : 03:00:00  
Auto interval(min)   : 30
```

```
Schedule time          : -
Schedule time-range    : -
Flexible radio mode     : auto-switch
Policy                 : -
Sensitivity             : high
Virtual group size     : 50
K-value                : 70
Reference data analysis : enable
Reference rogue ap interference : enable
Environment deterioration blacklist threshold : 16
-----
```

若调优模式为auto，则会出现业务时间段触发局部射频调优的情况，频繁触发局部射频调优会导致终端关联状态不稳定，需修改调优模式为非业务时间段定时调优。

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] calibrate enable schedule time 03:00:00
```

步骤2 确认是否频繁触发雷达信道避让，AP射频的工作信道检测到雷达信号时需调整信道进行避让，频繁的雷达信道避让切换会导致终端关联状态不稳定。

```
<HUAWEI> display channel switch-record all
OldCh/NewCh: Old channel/New channel
OldBw/NewBw: Old bandwidth/New bandwidth
RfID : Radio ID
-----
```

AP ID	AP name	RfID	OldCh/NewCh	OldBw/NewBw	Switch reason	Switch time
15	AirEnginexxxxS	1	52/149	20M/20M	dfs	2020-07-13/14:43:46

Total : 1, printed : 1

若存在大量dfs信道切换记录，则证明环境中存在雷达信号，需将雷达信道（**52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144**）从射频调优集中去除。

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] regulatory-domain-profile name default //根据现网配置填写域管理模板名称
[HUAWEI-wlan-regulate-domain-default] dca-channel 5g channel-set <选择除雷达信道外的其他信道>
```

步骤3 确认SSID模板下是否开启了802.11r功能，Windows终端和iPhone终端对802.11r功能存在一定兼容性问题，会导致终端使用过程中异常掉线，关闭802.11r功能。对于dot1x认证的终端，本身可以通过pmk免认证方式完成免认证流程，而802.11r功能与PMF功能互斥，因此建议保持802.11r功能关闭。

```
<HUAWEI> display ssid-profile name default //根据现网配置查询相应的ssid模板名称
-----
```

```
Profile ID          : 0
SSID                : GUEST-WLAN
SSID hide           : disable
Association timeout(min) : 5
Max STA number      : 64
Action upon reaching the max STA number : SSID broadcast
Legacy station      : enable
DTIM interval       : 1
Beacon 2.4G rate(Mbps) : 1
Beacon 5G rate(Mbps) : 6
Deny-broadcast-probe : disable
Probe-response-retry num : 1
802.11r             : enable
802.11r authentication : -
802.11r private      : disable
802.11r reassociation timeout (s) : 5
```


.....

802.11r处于开启状态，进入SSID模板关闭802.11r功能。

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name default
[HUAWEI-wlan-ssid-prof-default] undo dot11r enable
```

步骤4 通过如下方法确认终端是否符合被外部环境反制的现象。

- 方法一：根据AP上采集的用户日志中记录的终端上下线信息（STA_EVENT_ASSOCIATED、STA_EVENT_DISASSOCIATED），确认终端是否不断重复上线下线行为，且上线和下线时终端的RSSI信息差异较大。
- 方法二：在AP诊断视图下执行如下命令，快速确认终端关联、去关联时是否信号强度差异较大。
 - V200R019C00及之前版本：**display wifi sta-trace-info**
 - V200R019C10及之后版本：**display umac sta-trace-info**

若符合，则可以判断终端被周围环境中的其他Wi-Fi设备反制，需排查周围环境中的其他Wi-Fi设备并清除反制源。

AC侧可通过配置pmf功能以避免终端被其他外部Wi-Fi设备反制，要求SSID的加密方式为wpa2或wpa3（wpa3强制使能pmf）。需要特别说明的是，配置pmf功能后，老旧终端可能会因为不支持pmf功能而无法接入Wi-Fi网络。

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name default //根据现网配置填写安全模板名称
[HUAWEI-wlan-sec-prof-default] pmf optional
```

步骤5 Windows类型终端在终端关联的AP的诊断视图下执行如下命令时出现STA_DEAUTH的原因为Unspecified reason(1)

- V200R019C00及之前版本：**display wifi sta-trace-info**
- V200R019C10及之后版本：**display umac sta-trace-info**

优化方法1：

1. 在Windows终端上选择“开始 > 运行”，输入“regedit”后单击“确定”。系统显示“注册表编辑器”界面。
2. 在注册表编辑器中打开路径“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NlaSvc\Parameters\Internet”，在界面右侧找到并打开“EnableActiveProbing”，将数据数值修改为“0”。
3. 重启电脑。

优化方法2：

1. 在Windows终端上选择“开始 > 运行”，输入“gpedit.msc”后单击“确定”。系统显示“本地组策略编辑器”界面。
2. 在本地组策略编辑器中依次选择“计算机设置 > 管理模板 > 系统 > Internet通信管理 > Internet通信设置”，在界面右侧找到并打开“关闭Windows网络连接状态指示器活动测试”，将该功能修改为“已启用”。
3. 重启电脑。

----结束

常规处理建议

1. 执行命令**display station offline-record sta-mac sta-mac**，根据《[WLAN产品文档](#)》中终端掉线原因和处理建议进行针对性地处理。
2. 根据信息收集要求正确收集现网必要信息，根据日志内容对终端掉线行为进行具体分析。

5.2 终端搜不到 WiFi 信号

问题现象确认

确认终端搜不到WiFi信号的现象：

- 是所有终端都搜不到SSID信号还是某特定类型的终端搜不到。
- 是部分区域搜不到还是所有区域都搜不到。

信息收集

AC和AP的一键式诊断信息

关键配置检查

步骤1 确认AP下是否正确创建了VAP。

```
<HUAWEI> display vap ap-id 3
WID : WLAN ID
-----
AP ID AP name  RfID WID  BSSID      Status Auth type  STA  SSID
-----
Total: 1
```

正常创建的VAP，BSSID字段值不为全0；处于工作状态的VAP，Status字段值为**ON**。

如果VAP未正常创建，请执行命令**display vap create-fail-record all**查看VAP创建失败的原因，常见的原因如下表所示。更具体的原因以及处理措施请参考产品文档中对应的命令**display vap create-fail-record all**（以V200R023C00版本为例）。

几种常见的VAP创建失败原因：

- 配置了WPA3的加密方式但是V200R021C00SPC200之前的AP版本不支持WPA3，导致配置无法下发。需修改SSID加密方式为WPA2方式，或升级AP版本至V200R021C00SPC200及更新版本。
- 安全模板下未配置安全策略，需要到安全模板下配置安全策略，否则会导致VAP不会创建。

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name default
[HUAWEI-wlan-sec-prof-default] security open
```

步骤2 确认射频状态是否正常。

```
<HUAWEI> display radio all
CH/BW:Channel/Bandwidth
CE:Current EIRP (dBm)
ME:Max EIRP (dBm)
CU:Channel utilization
ST:Status
WM:Working Mode (normal/monitor/monitor dual-band-scan/monitor proxy dual-band-scan)
```

AP ID	Name	RfID	Band	Type	ST	CH/BW	CE/ME	STA	CU	WM
0	00e0-fc76-e360	0	2.4G	ax	off	6/20M	24/24	0	55%	monitor
0	00e0-fc76-e360	1	5G	ax	off	56/20M	25/25	0	3%	monitor

Total:2

- 如果radio状态为off，则检查是否在对应的radio视图下配置了radio disable，并使能当前radio。如果使能了radio后状态仍然为off，则排查一下AP是否存在PoE供电不足的情况。

[AC-wlan-radio-59/1] undo radio disable //使能当前radio

- 如果radio的work mode不是normal，不能进行普通WLAN业务，需在对应的radio视图下通过命令行work-mode将工作模式配置为normal。

[AC-wlan-radio-59/1] work-mode normal //设置当前radio的工作模式为normal

步骤3 确认是否配置了WPA3的加密方式，部分终端不支持WPA3会导致无法搜索到WPA3加密的SSID信号。

```
<HUAWEI> display vap all
WID : WLAN ID
```

AP ID	AP name	RfID	WID	BSSID	Status	Auth type	STA	SSID
3	ap1	0	1	00e0-fc12-3456	ON	WPA3-SAE	0	GUEST-WLAN

Total: 1

配置了WPA3加密的SSID，建议修改为传统的WPA2加密。

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name default
[HUAWEI-wlan-sec-prof-default] security wpa2 psk pass-phrase YsHsjx_202206 aes
```

步骤4 确认AP的供电功率是否满足射频正常释放SSID的能力。

```
<HUAWEI> display ap power-workmode all
```

ID	MAC	Name	Group	Power-workmode	Decided by
0	00e0-fc76-e360	ap_1	default	AF(Insufficient)	LLDP

Total: 1

当AP的供电模式为Insufficient模式时，AP射频无法正常释放SSID（其他两种状态Normal和Limited都不会影响AP正常释放SSID），若AP供电不足，需更换满足AP供电要求的POE交换机或电源适配器。

步骤5 部分终端的网卡驱动版本较低，无法搜索到Wi-Fi6信号，可以参考[关于Intel 部分无线网卡无法接入11ax协议AP问题的预警](#)进行排查和处理。

----结束

5.3 终端上线失败

步骤1 执行命令display station online-fail-record sta-mac sta-mac，查看用户上线失败原因。

```
[AC-wlan-view] display station online-fail-record sta-mac f06b-ca63-313d
```

STA MAC	AP ID	Ap name	Rf/WLAN	Last record time	Reason
---------	-------	---------	---------	------------------	--------

```
f06b-ca63-313d 2 ap-10 0/1 2015-12-03/19:05:12
The STA is in the VAP's blacklist.
```

```
-----  
Total stations: 1 Total records: 1
```

终端上线失败的具体原因以及处理措施请参考产品文档中对应的命令 **display station online-fail-record**（以V200R023C00版本为例）。

步骤2 对于dot1x认证的SSID，需要同时采集终端接入过程的trace object信息和station-trace信息，或采集终端关联AP的日志文件，通过station-trace信息或者高精度日志中纪录的关联过程，确认是否出现dot1x认证和4步握手流程同时进行的现象（EAPoL报文还未交互结束AP侧即发送了1/4握手报文），出现这种情况说明AC/AP侧对终端的pmk缓存信息匹配出现不一致的现象导致关联认证过程混乱，可通过配置空白的终端接入黑名单模板使关联响应上移到AC，以保证终端关联流程不会同时出现认证和握手流程同时发起的现象。

```
<HUAWEI> system-view  
[HUAWEI] wlan  
[HUAWEI-wlan-view] vap-profile name vap-profile1  
[HUAWEI-wlan-vap-prof-vap-profile1] sta-access-mode blacklist sta-blacklist-profile1
```

步骤3 其他场景，可参考终端接入认证异常或终端无法获取IP地址的问题进行排查，或采集AC一键诊断信息，AC/AP的日志和诊断日志文件对问题终端mac地址的关联行为进一步进行分析。

----结束

5.4 终端获取不到地址

步骤1 检查STA与服务器之间链路是否正常。

1. 检查接口相关VLAN是否放通，端口VLAN配置是否正确。
2. 检查网关能否学习到STA的MAC表。

```
<HUAWEI> display mac-address 14d6-4da7-3725
```

```
-----  
MAC Address  VLAN/VSI                Learned-From  Type  
-----  
14d6-4da7-3725  4094/-                GE0/0/1      dynamic  
-----
```

```
Total items displayed = 1
```

- 若能够学到STA的MAC表，说明STA和网关之间链路正常。
 - 若不能学习到STA的MAC表，说明STA和网关之间链路不通。
3. 直接转发模式下，检查业务VLAN配置是否正确。
 - 检查AP和网关之间的设备是否创建业务VLAN，若没有创建，会导致转发业务VLAN的报文失败，需要创建业务VLAN
 - 检查AP和网关之间的设备是否允许业务VLAN通过，若没有允许业务VLAN通过，会导致转发业务VLAN的报文失败，需要允许业务VLAN通过
 4. 隧道转发模式下，检查业务VLAN配置是否正确。

DHCP服务器不是AC时，AC需要创建并透传业务VLAN，否则会导致AC转发业务VLAN的报文失败。

步骤2 检查WLAN配置是否正确。

1. 直接转发模式，检查AP有线口是否取消了DHCP snooping信任端口。

直接转发模式，如果AP有线口模板配置了**undo dhcp trust port**，AP上行口又绑定了该有线口模板，AP上行口会取消DHCP snooping信任端口，导致STA的DHCP请求报文无法从AP发出

```
筛选查看undo dhcp trust port配置
[HUAWEI] display current-configuration | include trust
undo dhcp trust port
AP上行口绑定了AP有线口模板
wired-port-profile name wired1
undo dhcp trust port
ap-group name group1
wired-port-profile wired1 gigabitethernet 0
```

为了解决该问题，AC需要删除**undo dhcp trust port**配置，或者AP上行口取消绑定AP有线口模板。

2. 检查业务VLAN和管理VLAN是否相同

建议管理VLAN和业务VLAN分别使用不同的VLAN。只有直接转发模式，AP配置**management-vlan**，接入交换机连接AP的接口对管理VLAN不打PVID场景，才允许管理VLAN和业务VLAN相同，其他场景管理VLAN和业务VLAN相同会导致STA无法获取IP地址

3. 对于业务VLAN为VLAN pool的场景，需要确保网关设备上的VLAN pool配置和业务VLAN下配置的VLAN pool相对应。

步骤3 检查DHCP配置是否正确

1. 检查接入交换机是否配置了DHCP Snooping

无线用户流动性大，用户离线通常不会发送DHCP Release报文释放IP地址，导致DHCP Snooping绑定表经常出现满规格，新用户无法获取IP地址。

```
[S5720-36C-EI] display dhcp snooping
DHCP snooping global running information :
DHCPv4 snooping           : Enable
DHCPv6 snooping           : Enable
Static user max number     : 256
Current static user number : 0
Dhcp user max number       : 256 (default)
Current dhcp user number   : 256
```

AP已经默认开启针对无线用户的DHCP snooping功能，建议接入交换机删除DHCP Snooping配置，如果接入交换机下挂了有线终端，确实需要开启DHCP Snooping功能，建议在连接AP的端口配置**dhcp snooping enable no-user-binding**命令，该端口下挂的用户不生成DHCP Snooping绑定表。

2. 检查地址池是否有空闲地址

执行命令**display ip pool**命令，查看地址池中是否有可用的IP地址。

```
<HUAWEI> display ip pool interface Vlanif100
Pool-name: Vlanif100
Pool-No: 0
...
-----
Network section
StartEndTotalUsed Idle(Expired) Conflict Disabled
-----
192.168.4.1192.168.4.2542540254(0)00
-----
```

如果Idle(Expired)数量为0(0)，说明服务器没有可用地址，可以扩充地址池的IP地址范围，或者使用**lease**命令（接口地址池为**dhcp server lease**命令）减小地址租期，注意执行**lease**命令后仅对新上线的用户生效，已经在线的用户需要重新上线或者续租成功才使用新租期，否则继续使用老租期。

步骤4 检查有线口模式

当中心AP接RU场景下用户无法获取IP地址时，在中心AP接RU的接口的有线口模板视图下，查看是否配置了root模式。

```
[HUAWEI-wlan-wired-port-a] display this | include mode
mode root
```

如果配置了root模式，则执行**undo mode**命令取消root模式，使其恢复默认模式，重启AP后生效。

```
[HUAWEI-wlan-wired-port-a] undo mode
Warning: If the AP goes online through a wired port, the incorrect port mode configuration will cause the
AP to go out of management
. This fault can be recovered only by modifying the configuration on the AP. Continue? [Y/N]:y
Warning: This action will take effect after resetting AP.
Warning: After configuration synchronization is enabled, an exception of the local or backup controller may
lead to a configuration
synchronization failure.
[HUAWEI-wlan-wired-port-a] display this | include mode
```

步骤5 AC诊断视图下开启基于用户的station-trace功能，检查DHCP部分的Trace信息。

```
# 开启station-trace功能
[HUAWEI-diagnose] station-trace sta-mac 482c-a042-8227
```

DHCP服务器常见Trace信息如下表所示。

Trace信息	说明
[BTRACE][2015/12/28 17:17:51][DHCPPRO] [dc00-07c4-023c]:Receive DHCP packet (srcif:Vlanif127 orgif:GigabitEthernet1/0/7 length:321 mflg:UC/BC). [BTRACE][2015/12/28 17:17:51][DHCPPRO] [dc00-07c4-023c]:ReceivesDHCP DISCOVERpacket from interface GigabitEthernet1/0/7. [BTRACE][2015/12/28 17:17:51][DHCPPRO] [dc00-07c4-023c]: Receive DHCP DISCOVER message.orgif:GE1/0/7 srcif:Vlanif127 L3if:Vlanif127 dstif:GE1/0/7 srcmac:dc00-07c4-023c dstmac:ffff-ffff- ffff vsi:- vlan:127/0 srcip:0.0.0.0 dstip:255.255.255.255 VPN:- src-port:68 dst-port:67 msgtype:BOOT-REQUEST dhcp msgtype:DHCP DISCOVER bflag:bc chaddr:dc00-07c4-023c ciaddr:0.0.0.0 reqip:0.0.0.0 giaddr:0.0.0.0 serverid:0.0.0.0 yiaddr:0.0.0.0 xid:0x7531 [BTRACE][2015/12/28 17:17:51][DHCPPRO] [dc00-07c4-023c]:Find old soft l2fdb entry(mac:dc00-07c4-023c interface:GE1/0/7 vsi:65535 vlan:127/0 vt-mode:0) [BTRACE][2015/12/28 17:17:51][DHCPPRO] [dc00-07c4-023c]:Update packet option.(BitMap:0x0 Total length:321, IP:303, UDP:283)	收到Discover报文， bflag决定Offer是广播 (bc) 还是单播 (uc)。
[BTRACE][2015/12/28 17:17:51][DHCPPRO] [dc00-07c4-023c]:Broadcast packet within VLAN 127(pri:0) succeed(Except:GE1/0/7)!	VLAN内广播发送一份 Discover报文。

Trace信息	说明
<p>[BTRACE][2015/12/28 17:17:51][DHCP] [dc00-07c4-023c]:Receives DHCP DISCOVER message from interface Vlanif127.(chaddr=dc00-07c4-023c, ciaddr=0.0.0.0, giaddr=0.0.0.0, serverid=0.0.0.0, VPN=-, expect leasetime=0)</p> <p>[BTRACE][2015/12/28 17:17:51][DHCP] [dc00-07c4-023c]:Gateway=192.168.127.1, mask=255.255.255.0.</p> <p>[BTRACE][2015/12/28 17:17:51][DHCP] [dc00-07c4-023c]:Get pool Vlanif127 by gateway 192.168.127.1 and vrf 0.</p> <p>[BTRACE][2015/12/28 17:17:51][DHCP] [dc00-07c4-023c]:Req static IP(poolname: Vlanif127, usermac:dc00-07c4-023c).</p> <p>[BTRACE][2015/12/28 17:17:51][DHCP] [dc00-07c4-023c]:Get pool Vlanif127 by gateway 192.168.127.1 and vrf 0.</p> <p>[BTRACE][2015/12/28 17:17:51][AM] [dc00-07c4-023c]:Receive REQUEST message. (ClientId:UserType: DHCP, MAC: dc00-07c4-023c pool:22 vrf:0 expect-time:0)</p> <p>[BTRACE][2015/12/28 17:17:51][AM] [dc00-07c4-023c]:Try allocate expired ip for client id. (ClientId: UserType: DHCP, MAC: dc00-07c4-023c , pool:22)</p> <p>[BTRACE][2015/12/28 17:17:51][AM] [dc00-07c4-023c]:Offer ip 192.168.127.52 to cid(UserType: DHCP, MAC: dc00-07c4-023c) with lease time 86400 seconds.</p> <p>[BTRACE][2015/12/28 17:17:51][DHCP] [dc00-07c4-023c]:Assigned ip address 192.168.127.52 for dc00-07c4-023c.</p>	DHCP服务器处理 Discover报文，分配IP地址。
<p>[BTRACE][2015/12/28 17:17:51][DHCP] [dc00-07c4-023c]:Sending ICMP ECHO to target ip address: 192.168.127.52.</p>	发送Offer前先ICMP探测。
<p>[BTRACE][2015/12/28 17:17:51][DHCP] [dc00-07c4-023c]:DHCP server protocol stack ends with stop.</p>	Discover报文被DHCP服务器业务接管，是正常打印信息。
<p>[BTRACE][2015/12/28 17:17:52][DHCP] [dc00-07c4-023c]:Sending ICMP ECHO to target ip address: 192.168.127.52.</p> <p>[BTRACE][2015/12/28 17:17:52][DHCP] [dc00-07c4-023c]:ICMP timeout and send DHCP OFFER to client. (ciaddr=192.168.127.52, chaddr=dc00-07c4-023c).</p>	ICMP探测完成，没有探测到冲突，准备发送 Offer报文。

Trace信息	说明
<p>[BTRACE][2015/12/28 17:17:52][DHCPPRO] [dc00-07c4-023c]:Receive DHCP packet (srcif:null orgif:null length:346 mflg:BC/BC).</p> <p>[BTRACE][2015/12/28 17:17:52][DHCPPRO] [dc00-07c4-023c]:Receive DHCP OFFER message.orgif:null srcif:null L3if:null dstif:GE1/0/7 srcmac:5439-dfcd-c668 dstmac:ffff-ffff-ffff vsi:-vlan:127/0 srcip:192.168.127.1 dstip:255.255.255.255 VPN:- src-port:67 dst-port:68 msgtype:BOOT-REPLY dhcp msgtype:DHCP OFFER bflag:bc chaddr:dc00-07c4-023c ciaddr:0.0.0.0 reqip:0.0.0.0 giaddr:0.0.0.0 serverid:192.168.127.1 yiaddr:192.168.127.52 xid:0x7531</p> <p>[BTRACE][2015/12/28 17:17:52][DHCPPRO] [dc00-07c4-023c]:L3IF IPv4 protocol status is down.</p> <p>[BTRACE][2015/12/28 17:17:52][DHCPPRO] [dc00-07c4-023c]:Update packet option.(BitMap:0x0 Total length:346, IP:328, UDP:308)</p> <p>[BTRACE][2015/12/28 17:17:52][DHCPPRO] [dc00-07c4-023c]:Broadcast packet within VLAN 127(pri:0) succeed!</p>	广播发送Offer报文成功（单播发送Offer时打印Unicast packet to interface GE1/0/7 within VLAN 127(pri:0) succeed）。
<p>[BTRACE][2015/12/28 17:17:52][DHCPPRO] [dc00-07c4-023c]:Receive DHCP packet (srcif:Vlanif127 orgif:GigabitEthernet1/0/7 length:344 mflg:UC/BC).</p> <p>[BTRACE][2015/12/28 17:17:52][DHCPPRO] [dc00-07c4-023c]:Receives DHCP REQUEST packet from interface GigabitEthernet1/0/7.</p> <p>[BTRACE][2015/12/28 17:17:52][DHCPPRO] [dc00-07c4-023c]:Receive DHCP REQUEST message.orgif:GE1/0/7 srcif:Vlanif127 L3if:Vlanif127 dstif:GE1/0/7 srcmac:dc00-07c4-023c dstmac:ffff-ffff-ffff vsi:-vlan:127/0 srcip:0.0.0.0 dstip:255.255.255.255 VPN:- src-port:68 dst-port:67 msgtype:BOOT-REQUEST dhcp msgtype:DHCP REQUEST bflag:bc chaddr:dc00-07c4-023c ciaddr:0.0.0.0 reqip:192.168.127.52 giaddr:0.0.0.0 serverid:192.168.127.1 yiaddr:0.0.0.0 xid:0x7531</p> <p>[BTRACE][2015/12/28 17:17:52][DHCPPRO] [dc00-07c4-023c]:Find old soft l2fdb entry(mac:dc00-07c4-023c interface:GE1/0/7 vsi:65535 vlan:127/0 vt-mode:0)</p> <p>[BTRACE][2015/12/28 17:17:52][DHCPPRO] [dc00-07c4-023c]:Update packet option.(BitMap:0x0 Total length:344, IP:326, UDP:306)</p>	收到Request报文，bflag决定ACK是广播（bc）还是单播（uc）。
<p>[BTRACE][2015/12/28 17:17:52][DHCPPRO] [dc00-07c4-023c]:Broadcast packet within VLAN 127(pri:0) succeed(Except:GE1/0/7)!</p>	VLAN内广播发送一份Request报文。

Trace信息	说明
<p>[BTRACE][2015/12/28 17:17:52][DHCPS] [dc00-07c4-023c]:Receives DHCP REQUEST message from interface Vlanif127.(chaddr=dc00-07c4-023c, ciaddr=0.0.0.0, giaddr=0.0.0.0, serverid=192.168.127.1, reqip=192.168.127.52, VPN=-, expect leasetime=0)</p> <p>[BTRACE][2015/12/28 17:17:52][DHCPS] [dc00-07c4-023c]:Process request_of_selecting message.</p> <p>[BTRACE][2015/12/28 17:17:52][DHCPS] [dc00-07c4-023c]:Gateway=192.168.127.1, mask=255.255.255.0.</p> <p>[BTRACE][2015/12/28 17:17:52][DHCPS] [dc00-07c4-023c]:Select gateway 192.168.127.1 and mask 255.255.255.0 by request address 192.168.127.52.</p> <p>[BTRACE][2015/12/28 17:17:52][AM] [dc00-07c4-023c]:Receive REQUEST message. (ClientId:UserType: DHCP, MAC: dc00-07c4-023c pool:22 vrf:0 expect-ip:192.168.127.52 expect-time:0)</p> <p>[BTRACE][2015/12/28 17:17:52][AM] [dc00-07c4-023c]:Try allocate leased ip for client. (ClientId : UserType: DHCP, MAC: dc00-07c4-023c, pool:22, Section:256)</p> <p>[BTRACE][2015/12/28 17:17:52][AM] [dc00-07c4-023c]:Get gateway and mask failed. (pool:22)</p> <p>[BTRACE][2015/12/28 17:17:52][AM] [dc00-07c4-023c]:Offer ip 192.168.127.52 to cid UserType: DHCP, MAC: dc00-07c4-023c.</p> <p>[BTRACE][2015/12/28 17:17:52][DHCPS] [dc00-07c4-023c]:DHCP process Request. (ulServerAddr=192.168.127.1, ulMask=255.255.255.0)</p> <p>[BTRACE][2015/12/28 17:17:52][DHCPS] [dc00-07c4-023c]:Send DHCP ACK packet. (Chaddr=dc00-07c4-023c, Offer IP=192.168.127.52).</p>	<p>DHCP服务器处理 Request报文，准备发送ACK报文。</p>
<p>[BTRACE][2015/12/28 17:17:52][DHCPPRO] [dc00-07c4-023c]:DHCP server protocol stack ends with stop.</p>	<p>Request报文被DHCP服务器业务接管，是正常打印。</p>

Trace信息	说明
[BTRACE][2015/12/28 17:17:52][DHCPPRO] [dc00-07c4-023c]:Receive DHCP packet (srcif:null orgif:null length:346 mflg:BC/BC). [BTRACE][2015/12/28 17:17:52][DHCPPRO] [dc00-07c4-023c]:Receive DHCP ACK message.orgif:null srcif:null L3if:null dstif:GE1/0/7 srcmac:5439-dfcd-c668 dstmac:ffff-ffff-ffff vsi:- vlan:127/0 srcip:192.168.127.1 dstip:255.255.255.255 VPN:- src-port:67 dst-port:68 msgtype:BOOT-REPLY dhcp msgtype:DHCP ACK bflag:bc chaddr:dc00-07c4-023c ciaddr:0.0.0.0 reqip:0.0.0.0 giaddr:0.0.0.0 serverid:192.168.127.1 yiaddr:192.168.127.52 xid:0x7531 [BTRACE][2015/12/28 17:17:52][DHCPPRO] [dc00-07c4-023c]:L3IF IPv4 protocol status is down. [BTRACE][2015/12/28 17:17:52][DHCPPRO] [dc00-07c4-023c]:Update packet option.(BitMap:0x0 Total length:346, IP:328, UDP:308) [BTRACE][2015/12/28 17:17:52][DHCPPRO] [dc00-07c4-023c]: Broadcast packet within VLAN 127(pri:0) succeed!	广播发送ACK成功（单 播发送ACK时打印 Unicast packet to interface GE1/0/7 within VLAN 127(pri:0) succeed）。

----结束

5.5 终端网络慢

步骤1 通过ping包确定故障范围是否在网关以下网络

在处理故障之前，通过ping包的方式来确认故障的范围，从而明确故障排查的范围。

从STA分别ping网关和外网地址，观察ping包的情况，从而确定故障范围。

- 如果从STA ping网关出现不稳定的情况，如频繁丢包、延迟波动等，说明故障出现在网关以下的网络中。
- 如果从STA ping网关正常，但是ping外网地址出现不稳定的情况，说明故障出现在网关以上的网络中。

步骤2 检查业务VLAN和管理VLAN配置是否合理

管理VLAN和业务VLAN在不同转发方式下的配置推荐如下表所示。

说明

为方便描述，表格中的VLAN均为示例。

表 5-1 管理 VLAN 和业务 VLAN 在不同转发方式下的配置推荐

转发方式	业务 VLAN	管理 VLAN	配置影响	配置推荐
直接转发	1	100	用户业务报文打上管理VLAN，导致业务混乱。	不推荐
	100	1	可能会受VLAN1广播域过大、广播泛洪的影响，导致网络阻塞，影响用户体验。	不推荐
	1	1	可能会受VLAN1广播域过大、广播泛洪的影响，导致网络阻塞，影响用户体验。	不推荐
	100	100	数据转发异常。	不推荐
	100	50	标准推荐配置。	推荐
隧道转发	1	100	可能会受VLAN1广播域过大、广播泛洪的影响，导致网络阻塞，影响用户体验。	不推荐
	100	1	可能会受VLAN1广播域过大、广播泛洪的影响，导致网络阻塞，影响用户体验。	不推荐
	1	1	MAC漂移，导致数据转发异常。	不推荐
	100	100	MAC漂移，导致数据转发异常。	不推荐
	100	50	标准推荐配置。	推荐

步骤3 检查AP的信道利用率是否正常

WLAN网络中所有终端共享带宽，相互竞争带宽资源，如果周围环境中无线终端很多，或网络中有很多广播、组播报文（组播、广播报文都是低速率发送，消耗空口资源多），相互抢占信道的情况就会很严重，最终导致信道利用率高，无线网络不稳定，出现ping包延迟大、丢包等情况。

```
<Huawei> display radio all
CH/BW:Channel/Bandwidth
CE:Current EIRP (dBm)
ME:Max EIRP (dBm)
CU:Channel utilization
ST:Status
WM:Working Mode (normal/monitor/monitor dual-band-scan/monitor proxy dual-band-scan)
-----
AP ID Name      RfID Band Type  ST CH/BW  CE/ME STA  CU  WM
-----
0  60de-4474-9640 0   2.4G bgn  on 6/20M  24/24 0   55% normal
0  60de-4474-9640 1   5G  an   on 56/20M 25/25 0   3%  normal
-----
Total:2
```

一般情况下，如果信道利用率超过60%，则可能会对用户造成网络波动。导致信道利用率高的原因和解决方法如下：

- 无线网络环境干扰严重，此时，需要对AP的信道进行合理的规划，降低干扰。可以手动将信道切换至信道利用率低的信道，或者在无业务影响时进行调优操作。
- 网络中组播、广播报文很多，此时，需要查看网络中的组播、广播报文的情况。

步骤4 检查AP接口上接收到的组播和广播报文的统计信息是否正常

WLAN网络中发送组播、广播报文时，因为报文不会重传，所以为了确保接收端的收包成功率，都是以较低速率发送。如果网络中有大量的组播、广播报文往空口发送，会导致空口资源浪费严重，出现信道利用率持续升高，影响无线终端正常的上网体验，出现延迟大、丢包的情况。

在AP上查看AP对应接口上接收到的组播和广播报文的统计信息，观察组播、广播报文增长速率。可以多执行几次，观察报文统计计数增长的情况。

```
<AP> display interface gigabitethernet 0/0/1
GigabitEthernet 0/0/1 current state : UP
Line protocol current state : UP
Description:
Switch Port,Link-type : access(negotiated),
PVID : 1, TPID : 8100(Hex), The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0025-9ef4-abcd
Last physical up time : -
Last physical down time : 2015-12-21 16:12:29 UTC+08:00
Current system time: 2012-06-05 18:56:41
Port Mode: COMMON FIBER, Transceiver: 1000_BASE_SX_SFP
Speed : 1000, Loopback: NONE
Duplex: FULL, Negotiation: ENABLE
Mdi : -, Flow-control: DISABLE
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 0 bits/sec, Record time: -
Output peak rate 0 bits/sec, Record time: -
Input: 7650 packets, 1327062 bytes
  Unicast: 0, Multicast: 7650
  Broadcast: 0, Jumbo: 0
Discard: 0, Pause: 0
Total Error: 0
CRC: 0, Giants: 0
Runts: 0, Fragments: 0
Alignments: 0, Symbols: 0
Output: 38348 packets, 3683776 bytes
  Unicast: 0, Multicast: 32314
  Broadcast: 6034, Discard: 0
Pause: 0
Input bandwidth utilization threshold : 80.00%
Output bandwidth utilization threshold: 80.00%
Input bandwidth utilization : 0%
Output bandwidth utilization : 0%
```

如果广播或组播报文的增长速率超过100pps，说明该接口接收到的广播、组播报文较多。

解决方法如下：

1. 开启二层网络的隔离功能。

在交换机或AC的接口下配置接口二层隔离功能。以AC为例。

```
<AC> system-view
[AC] interface GigabitEthernet 0/0/1
[AC-GigabitEthernet0/0/1] port-isolate enable
[AC-GigabitEthernet0/0/1] quit
```

在AC的流量模板下配置用户二层隔离功能。

```
AC] wlan
[AC-wlan-view] traffic-profile name default
[AC-wlan-traffic-prof-default] user-isolate l2
[AC-wlan-traffic-prof-default] quit
[AC-wlan-view] quit
```

2. 在交换机或AC上开启接口的广播和组播报文限速功能。以AC为例。

```
[AC] interface GigabitEthernet 0/0/1
[AC-GigabitEthernet0/0/1] broadcast-suppression packets 1000
[AC-GigabitEthernet0/0/1] multicast-suppression packets 1000
```

步骤5 检查是否存在建链速率低的终端在做大流量业务

AP下关联低速率下做大流量业务的终端，可能会导致该AP下的其他用户无法正常上网，该终端停止业务后，其他用户恢复正常。

1. 通过display station ap-id X 查看该AP下是否存在建链速率低的终端。

```
<AC> display station ap-id 3
Rf/WLAN: Radio ID/WLAN ID
Rx/Tx: link receive rate/link transmit rate(Mbps)
-----
STA MAC      AP ID Ap name      Rf/WLAN Band Type Rx/Tx    RSSI  VLAN  IPv4 address
SSID        Status
-----
14cf-9208-9abf 0 1047-8007-6f80 0/2 2.4G 11n 65/58 -70 10 10.10.10.253 tap1
Normal
-----
Total: 1 2.4G: 1 5G: 0
```

在有业务的情况下，如果终端的建链速率（Tx或Rx）小于30Mbps，说明该终端的建链速率低。

2. 执行命令display station statistics sta-mac sta-mac查看该终端下的统计。

```
<AC> display station statistics sta-mac 14cf-9208-9abf
-----
Packets sent to the station          : 7
Packets received from the station    : 40
Bytes sent to the station             : 1170
Bytes received from the station       : 3911
Wireless data rate sent to the station(kbps) : 0
Wireless data rate received from the station(kbps) : 0
Trigger roam total                   : 0
Trigger roam failed                   : 0
STA power save percent                : 0%
```

一般认为，如果终端流量超过10M，说明该终端在进行大流量业务。具体还需要结合实际网络情况来判断。

为保证其他终端能够正常上网，可以通过如下方法进行处理：

- 对单个终端进行限速，具体的限制速率请结合实际网络情况来配置。

```
<AC> system-view
[AC] wlan
[AC-wlan-view] traffic-profile name p1
[AC-wlan-traffic-prof-p1] rate-limit client up 2000
[AC-wlan-traffic-prof-p1] rate-limit client down 2000
```

步骤6 排查终端空口丢包

1. 在AC诊断视图下开启基于用户的station-trace功能，进行ping包测试，确认ping包在Wi-Fi无线侧收发是否正常。

```
# 开启station-trace功能
[AC-diagnose] station-trace sta-mac 482c-a042-8227
```

进行ping包测试

可以通过AC ping用户，如果用户网关不在AC上，可以通过用户ping网关。

根据station-trace打印信息判断问题是在有线侧还是无线侧。station-trace信息说明请参考[5.8 终端station-trace解析](#)。

2. 检查是否终端个体问题

- a. 在AC或网关上ping与问题终端接入相同AP以及相同射频的其他终端，观察ping包丢包情况，确认是终端个体问题，还是普遍现象。如果是终端终端个体问题，查看终端是否处于节电状态。

```
<AC> display station sta-mac 482c-a042-8227
```

```
-----
Station MAC-address          : 482c-a042-8227
Station IP-address          :
FE80::D287:F82B:9D2C:827C   : 10.10.10.49
Station gateway              : 10.10.10.1
Associated SSID              : test
Station online time(ddd:hh:mm:ss) : 000:00:03:36
.....
Station current state
.....
Power save mode enabled      : YES
.....
```

当终端处于节电状态时，发包时延会增加，具体时延大小正常情况下和 beacon 间隔配置相关，beacon间隔配置越低则时延越小，反之时延越大。

- b. 从设备侧ping终端，确认时延和丢包情况。

当前大多数移动终端，如智能手机、笔记本等，在没有进行业务时，大部分时间都是处于节电状态的，因此从设备上往终端上ping包时，出现ping包时延大以及偶尔的丢包是正常的，可以通过在设备侧快ping终端的方式进行实际时延以及丢包确认。

```
[AC] ping -c 1000 -m 10 10.1.1.49
```

```
PING 10.1.1.49: 56 data bytes, press CTRL_C to break
Reply from 10.1.1.49: bytes=56 Sequence=1 ttl=64 time=326 ms
Reply from 10.1.1.49: bytes=56 Sequence=2 ttl=64 time=1 ms
Reply from 10.1.1.49: bytes=56 Sequence=3 ttl=64 time=1 ms
Reply from 10.1.1.49: bytes=56 Sequence=4 ttl=64 time=1 ms
Reply from 10.1.1.49: bytes=56 Sequence=5 ttl=64 time=2 ms
Reply from 10.1.1.49: bytes=56 Sequence=6 ttl=64 time=4 ms
Reply from 10.1.1.49: bytes=56 Sequence=7 ttl=64 time=5 ms
Reply from 10.1.1.49: bytes=56 Sequence=8 ttl=64 time=2 ms
Reply from 10.1.1.49: bytes=56 Sequence=9 ttl=64 time=1 ms
Reply from 10.1.1.49: bytes=56 Sequence=10 ttl=64 time=1 ms
Reply from 10.1.1.49: bytes=56 Sequence=11 ttl=64 time=5 ms
Reply from 10.1.1.49: bytes=56 Sequence=12 ttl=64 time=5 ms
Reply from 10.1.1.49: bytes=56 Sequence=13 ttl=64 time=3 ms
Reply from 10.1.1.49: bytes=56 Sequence=14 ttl=64 time=4 ms
Reply from 10.1.1.49: bytes=56 Sequence=15 ttl=64 time=5 ms
Reply from 10.1.1.49: bytes=56 Sequence=16 ttl=64 time=5 ms
Reply from 10.1.1.49: bytes=56 Sequence=17 ttl=64 time=3 ms
```

如果快ping正常，则说明之前的时延以及丢包是由于终端处于节电导致，此种情况一般对终端的实际业务无影响，因为终端在实际做业务时，会退出节电状态。但是有些手持PDA，比如语音话机、扫码枪、医疗终端等，为了提高待机时间，即便在做业务时，也可能处于节电状态里面，此时会通过ps-poll或U-aspd的方式和AP进行节电状态下的报文收发，遇到这些终端，需要检查beacon间隔配置。

- c. 检查并合理配置beacon间隔。

默认情况下beacon间隔配置值为100，因此一般终端在节电情况下，进行ping包时，平均时延在100ms左右。如果平均时延远大于100ms，比如500ms以上或甚至丢包，则需要检查beacon间隔是否被修改成较大值，具体可在射频模板下进行查询：

```
<AC> system-view
[AC] wlan
[AC-wlan-view] radio-5g-profile name abc
[AC-wlan-radio-5g-prof-abc] display this
#
beacon-interval 500
```

```
#  
return
```

如果beacon间隔确认被修改成较大值，则需要适当降低；如果beacon间隔没有被修改，或恢复默认值后，延迟还是很大或频繁丢包，可能存在终端兼容性问题，则需要及时联系技术支持人员。

d. 建议将终端的网卡驱动更新到最新版本。

如果确认和终端节电状态无关或射频下用户均存在丢包，请继续下一步排查。

3. 检查射频扫描参数配置是否合理

```
[AC-wlan-view] display air-scan-profile name  
default
```

```
-----  
Scan switch      : enable  
Scan period(ms)  : 100      //扫描持续时间  
Scan interval(ms): 2000     //扫描间隔  
Scan channel-set : country-channel  
Voice scan aware : enable  
Video scan aware : enable  
Scan enhancement : disable  
-----
```

扫描参数主要涉及扫描间隔以及扫描持续时间，如果配置不合理，比如扫描间隔配置的很短（低于3s）或扫描持续时间配置的较大（如100ms），由于AP频繁切换到非工作信道进行信息收集，会导致工作信道上的用户业务受损，表现为丢包或时延大。

可以尝试关闭扫描功能，确认STA丢包是够和扫描功能相关。

```
[AC-wlan-view] air-scan-profile name default  
[AC-wlan-air-scan-prof-default] scan-disable
```

- 如果关闭扫描后，ping包不丢包或丢包率明显降低，说明是扫描参数配置过于极端导致。如果没有特殊业务需要，比如终端定位等业务，扫描间隔以及扫描持续时间使用默认值即可。
- 如果扫描关闭后，ping包没有改善，说明和扫描功能关系不大。

----结束

5.6 终端漫游问题

步骤1 检查漫游前后VLAN配置是否正确。

- 漫游前后的业务VLAN需要正确创建，尤其对于AC间漫游，参与漫游的所有AC上都需要创建漫游前和漫游后的业务VLAN。
- 如果是直接转发，漫游后AP到漫游前AP这条链路上所有的端口必须放通业务VLAN，且AC上的业务VLAN必须创建，保证漫游后用户的数据报文转发正常。
- 如果是交换机的随板AC，三层漫游的中间网络必须放通漫游前后的业务VLAN。

步骤2 检查漫游前后两个AP的信号覆盖是否连续。

漫游前后两个AP的距离如果太远，则用户在走动过程中可能会因为信号覆盖不连续而先离线再上线，导致漫游失败。

此时，需要使用CloudCampus APP、inSSIDer和Wifi分析仪等常用的AP信号强度探测工具来检查AP的信号覆盖情况。

如果确认AP之间的信号不连续，可以通过增加AP发射功率或增加AP来满足信号连续覆盖。

步骤3 检查功率配置是否合理。

```
<AC> display radio ap-id 25
CH/BW:Channel/Bandwidth
CE:Current EIRP (dBm)
ME:Max EIRP (dBm)
CU:Channel utilization

-----
AP ID Name   RfID Band  Type   Status CH/BW   CE/ME STA   CU
-----
25  ap-yuan 0   2.4G bgn  on     8/20M   29/29 1    21%
25  ap-yuan 1   5G   an11ac on     165/20M 23/30 0    4%
-----
Total:2
```

- 如果功率配置过小，容易造成信号覆盖盲点。此时，需要在射频视图下执行**eirp**命令增大发射功率。
- 如果功率配置过大（如满功率），容易导致终端关联远端AP而出现漫游不灵敏。此时，需要在射频视图下执行**eirp**命令适当降低发射功率或者配置智能漫游功能。

步骤4 检查WLAN网络环境中是否存在同名的非法SSID。

确定发生漫游失败问题的AP ID后，在AC上执行命令**display ap neighbor ap-id ap-id**，查看Uncontrol AP中是否存在同名的非法SSID。如果存在则需要关闭此非法SSID信号。

```
<AC> display ap neighbor ap-id 0
Radio: Radio ID of AP
.....
Uncontrol AP:

-----
Radio BSSID      Channel RSSI(dBm) Last Update Time   SSID
-----
0    d0d0-4b22-df00 1    -50    2019-08-24/15:32:18
0    c4b8-b4f0-6980 1    -44    2019-08-24/15:31:06
0    10c1-72dd-12e0 11   -41    2019-08-24/15:28:27 test
0    9c50-ee45-6240 1    -54    2019-08-24/15:32:06
-----
Total: 4
```

步骤5 对于PDA等非通用终端，需要确认当前设备信道集是否支持。

确认PDA等非通用终端支持的信道集，确保漫游前后AP上配置的信道集包含终端支持的信道。

步骤6 检查问题是否解决。

将终端在两个AP间移动，执行命令**display station roam-track**查看终端的漫游轨迹，如果漫游轨迹显示正常则问题解决，如果仍然漫游失败，请收集漫游时系统的日志和诊断日志并收集如下故障诊断信息，然后寻求技术支持。

命令	使用说明
[AC] trace enable [AC] trace object mac-address	查看STA上线或者漫游全流程跟踪信息。
[AC] display station online-fail-record [AC] display station offline-record	查看用户上线失败或下线原因。

命令	使用说明
[AC-diagnose] display wlan wsta block-sta-number all [AC-diagnose] display wlan wsta online-statistics [AC-diagnose] display wlan wsta online-fail-record by-mac [AC-diagnose] display wlan wsta peak-statistics	查看用户上线失败或下线原因码。
[AC-diagnose] display diagnostic-information	获取系统的一键诊断信息，该信息包括版本、补丁版本、当前配置和已保存配置、异常、部分日志等。

----结束

5.7 终端业务不通

步骤1 查看设备上ARP是否正常

ping报文发送要依赖于网关设备上是否有对端设备的ARP表项，执行命令**display arp**查看是否可以获取到对端ARP，如存在ARP则需按后续步骤检查。

- 如不能获取到ARP，可以通过station-trace功能界定ARP报文去向，并进行ping操作，查看打印出的ARP报文收发是否正常。

- 开启station-trace功能。（以MAC地址为d0ff-98b2-31fd的STA为例）

[AC-diagnose] **station-trace sta-mac d0ff-98b2-31fd**

- AC上ping终端地址，观察ARP报文的交互过程。

[AC-diagnose] **ping 10.99.99.54**

```
PING 10.99.99.54: 56 data bytes, press CTRL_C to break
Reply from 10.99.99.54: bytes=56 Sequence=1 ttl=64 time=71 ms<7>Oct 15 2017
21:06:19.580.1 5c1a-6f8b-d5a0 WIFI/7/BTRACE:[BTRACE]
[WLAN_WIFI][D0FF-98B2-31FD]:SeqNo[1] [ARP] ARP request : who has 10.99.99.54 ? tell
10.99.99.1 Recved from software switch
<7>Oct 15 2017 21:06:19.580.2 5c1a-6f8b-d5a0 WIFI/7/BTRACE:[BTRACE][WLAN_WIFI]
[D0FF-98B2-31FD]:SeqNo[1] [ARP] ARP request : who has 10.99.99.54 ? tell 10.99.99.1
elapsed[0 ms] Sending pkt to target(Single)
<7>Oct 15 2017 21:06:19.580.3 5c1a-6f8b-d5a0 WIFI/7/BTRACE:[BTRACE][WLAN_WIFI]
[D0FF-98B2-31FD]:SeqNo[1] [ARP] ARP request : who has 10.99.99.54 ? tell 10.99.99.1
elapsed[0 ms] Success to send pkt to air
<7>Oct 15 2017 21:06:19.580.4 5c1a-6f8b-d5a0 WIFI/7/BTRACE:[BTRACE][WLAN_WIFI]
[D0FF-98B2-31FD]:SeqNo[2] [ARP] ARP response : 10.99.99.54 is at d0ff-98b2-31fd Recved from
target
<7>Oct 15 2017 21:06:19.580.5 5c1a-6f8b-d5a0 WIFI/7/BTRACE:[BTRACE][WLAN_WIFI]
[D0FF-98B2-31FD]:SeqNo[2] [ARP] ARP response : 10.99.99.54 is at d0ff-98b2-31fd elapsed[0
ms] Entering rx reorder
<7>Oct 15 2017 21:06:19.580.6 5c1a-6f8b-d5a0 WIFI/7/BTRACE:[BTRACE][WLAN_WIFI]
[D0FF-98B2-31FD]:SeqNo[2] [ARP] ARP response : 10.99.99.54 is at d0ff-98b2-31fd elapsed[0
ms] Exiting rx reorder for release
<7>Oct 15 2017 21:06:19.580.7 5c1a-6f8b-d5a0 WIFI/7/BTRACE:[BTRACE][WLAN_WIFI]
[D0FF-98B2-31FD]:SeqNo[2] [ARP] ARP response : 10.99.99.54 is at d0ff-98b2-31fd elapsed[0
ms] Success to send pkt to software switch
```

station-trace功能是在AP上进行的，如果没有ARP回应过程，需要检查终端或进行空口报文捕获，看终端是否响应了ARP请求；如果ARP的交互过程是完整的，但

网关上仍旧无用户的ARP表项，需要进行有线报文捕获，确认ARP报文在什么设备上丢失。

- 如果网关上已经学习到用户的ARP表项，但却ping不通用户，可借助ACL流统计配置方法（大部分华为数通产品通用）：

inbound为相对本端设备的入方向，**outbound**为相对本端设备的出方向。例如：终端A（192.168.1.2）Ping设备B（192.168.1.1）请参考如下配置。

📖 说明

若中间网络设备也支持流量统计，可依次按此方法定位丢包的原因。

- 配置GigabitEthernet 0/0/1接口流量统计策略。

```
[AC] acl 3000
[AC-acl-adv-3000] rule 5 permit icmp source 192.168.1.2 0.0.0.0 //根据ACL过滤192.168.1.2发
过来的ICMP报文
[AC-acl-adv-3000] quit
[AC] traffic classifier test
[AC-classifier-test] if-match acl 3000
[AC-classifier-test] quit
[AC] traffic behavior test
[AC-behavior-test] statistic enable
[AC-behavior-test] quit
[AC] traffic policy test
[AC-trafficpolicy-test] classifier test behavior test
[AC-trafficpolicy-test] quit
[AC] interface GigabitEthernet 0/0/1
[AC-GigabitEthernet0/0/1] traffic-policy test inbound //将策略绑定到接口上
```

- 查询GigabitEthernet 0/0/1接口上统计的ICMP报文。

```
[AC] ping 192.168.1.2
[AC] display traffic policy statistics interface GigabitEthernet 0/0/1 inbound
```

步骤2 检查网络是否成环。

常见现象：网络丢包严重，主要是由于MAC表项漂移。

确认方式：建议串口登录设备，重复执行命令**display mac-address**检查MAC地址是否学习到了正确的端口，或在不同端口出现漂移状况，并检查网络是否有环路。

```
<AC> display mac-address
```

MAC Address	VLAN/VSI	Learned-From	Type
4c1f-cc25-611b	100/-	GE0/0/1	security

```
Total items displayed = 1
```

----结束

5.8 终端 station-trace 解析

正常情况下，设备侧ping用户（有线侧往无线侧ping包，下行），一个ping包的完整打印如下

V200R019C00及之前版本：

```
<7>Oct 18 2018 14:41:21.320.1 c88d-833a-8d40 WIFI/7/BTRACE:[BTRACE][WLAN_WIFI][482C-
A042-8227]:SeqNo[7] [ICMP] Ping request from [31.1.1.1] to [31.1.1.49] id[43991] seq[1548] payload[56]
Recvd from software switch
<7>Oct 18 2018 14:41:21.320.2 c88d-833a-8d40 WIFI/7/BTRACE:[BTRACE][WLAN_WIFI][482C-
A042-8227]:SeqNo[7] [ICMP] Ping request from [31.1.1.1] to [31.1.1.49] id[43991] seq[1548] payload[56]
elapsed[0 ms] Sending pkt to target(Single)
<7>Oct 18 2018 14:41:21.320.3 c88d-833a-8d40 WIFI/7/BTRACE:[BTRACE][WLAN_WIFI][482C-
```

```
A042-8227]:SeqNo[7] [ICMP] Ping request from [31.1.1.1] to [31.1.1.49] id[43991] seq[1548] payload[56]
elapsed[10 ms] Success to send pkt to air
<7>Oct 18 2018 14:41:21.340.1 c88d-833a-8d40 WIFI/7/BTRACE:[BTRACE][WLAN_WIFI][482C-
A042-8227]:SeqNo[8] [ICMP] Ping reply from [31.1.1.49] to [31.1.1.1] id[43991] seq[1548] payload[56]
Recvd from target
<7>Oct 18 2018 14:41:21.340.2 c88d-833a-8d40 WIFI/7/BTRACE:[BTRACE][WLAN_WIFI][482C-
A042-8227]:SeqNo[8] [ICMP] Ping reply from [31.1.1.49] t [31.1.1.1] id[43991] seq[1548] payload[56]
elapsed[0 ms] Entering rx reorder
<7>Oct 18 2018 14:41:21.340.3 c88d-833a-8d40 WIFI/7/BTRACE:[BTRACE][WLAN_WIFI][482C-
A042-8227]:SeqNo[8] [ICMP] Ping reply from [31.1.1.49] to [31.1.1.1] id[43991] seq[1548] payload[56]
elapsed[0 ms] Exiting rx reorder for release
<7>Oct 18 2018 14:41:21.340.4 c88d-833a-8d40 WIFI/7/BTRACE:[BTRACE][WLAN_WIFI][482C-
A042-8227]:SeqNo[8] [ICMP] Ping reply from [31.1.1.49] to [31.1.1.1] id[43991] seq[1548] payload[56]
elapsed[0 ms] Success to send pkt to software switch
```

其中前面三行表示设备侧发送给用户的ping request报文，下行；后面四行表示设备侧接收用户的ping response报文，上行。几个关键记录信息含义如下：

- Seq[xxx]：表示该ping包内携带的序列号，通过该序列号可以将trace和某个具体ping报文对应起来。
- Recvd from software switch：表示Wi-Fi驱动侧收到转发侧发给用户的ping request报文。
- Success to send pkt to air：表示Wi-Fi驱动成功将ping request报文通过空口发送给用户。
- Recvd from target：表示Wi-Fi驱动接收到用户通过空口回应的ping response报文。
- Success to send pkt to software switch：表示Wi-Fi驱动将ping response报文成功送到转发侧，后面将会由转发侧处理，并通过AP网口发送到有线侧网络设备。

如果ping包是从用户ping网关，即从无线侧往有线侧ping（上行），station-trace的打印信息类似，区别是此时Wi-Fi驱动模块从转发模块收到的报文是发给用户的ping response报文，Wi-Fi驱动模块从空口收到的是用户发送的ping request报文。

V200R020C00及之后版本（AirEngine X760系列AP）：

```
<7>Aug 02 2021 16:26:31.355.1 8c68-3a11-ebc0 WSRV/7/BTRACE:(BTRACE)(WLAN_AP)(94e6-
f741-9f83):SeqNo[7] [ICMP] Ping request from [192.190.190.2] to [192.190.190.139] id[11436] seq[BE:1
LE:256] payload[56] Receive from fwd
<7>Aug 02 2021 16:26:31.435.1 8c68-3a11-ebc0 WSRV/7/BTRACE:(BTRACE)(WLAN_AP)(94e6-
f741-9f83):SeqNo[7] [ICMP] Ping request from [192.190.190.2] to [192.190.190.139] id[11436] seq[BE:1
LE:256] payload[56] elapsed[4294964076 ms] send to rt ok format :4 seqType:2 eof:0 total_mpdum_num:0
<7>Aug 02 2021 16:26:31.435.2 8c68-3a11-ebc0 WSRV/7/BTRACE:(BTRACE)(WLAN_AP)(94e6-
f741-9f83):SeqNo[7] [ICMP] Ping request from [192.190.190.2] to [192.190.190.139] id[11436] seq[BE:1
LE:256] payload[56] elapsed[4294964077 ms] send to air ok, rate:229400 Kbps, ack_rssi:-30
<7>Aug 02 2021 16:26:31.435.3 8c68-3a11-ebc0 WSRV/7/BTRACE:(BTRACE)(WLAN_AP)(94e6-
f741-9f83):SeqNo[8] [ICMP] Ping reply from [192.190.190.139] to [192.190.190.2] id[11436] seq[BE:1
LE:256] payload[56] sec rx pkt ok. radio:0, userId:0, len:122, msduNum:1, msduLen:98, fc:0x0188, seq:413,
addr1-8c:68:3a:11:eb:c8 addr2-94:e6:f7:41:9f:83
<7>Aug 02 2021 16:26:31.435.4 8c68-3a11-ebc0 WSRV/7/BTRACE:(BTRACE)(WLAN_AP)(94e6-
f741-9f83):SeqNo[9] [ICMP] Ping reply from [192.190.190.139] to [192.190.190.2] id[11436] seq[BE:1
LE:256] payload[56] send to np ok
```

- SeqNo[xxx]：表示该ping包内携带的序列号，通过该序列号可以将trace和某个具体ping报文对应起来。
- seq[BE: x LE:y]：表示trace的报文序列号，同一个ping包的request与response seq相同，BE和LE分别表示seq的大端和小端数。
- Receive from fwd：表示Wi-Fi侧收到转发侧发给用户的ping request报文。
- send to rt ok：表示Wi-Fi侧PMAC模块成功将ping request报文发送给SMAC模块。

- send to air ok: 表示Wi-Fi侧成功将ping request报文通过空口发送给用户。
- sec rx pkt ok: 表示Wi-Fi侧成功接收到ping response报文。
- send to np ok: 表示Wi-Fi侧将ping response报文成功送到转发侧，后面将会由转发侧处理，并通过AP网口发送到有线侧网络设备。
- send to air fail: 表示Wi-Fi侧发送ping request报文失败，如果有打印reason code，表示该报文已发送到空口，没有收到对应的ACK；若有打印other reason，表示该报文被丢弃，没有发送到空口。

V200R020C00及之后版本（AirEngine X761系列AP）：

```
<7>Aug 02 2021 15:36:12.650.1 38eb-4821-3300 WSRV/7/BTRACE:(BTRACE)(WLAN_AP)(94e6-f741-9f83):SeqNo[35] elapsed[0 ms][ICMP] Ping request from [192.190.190.2] to [192.190.190.139] id[11180] seq[BE:1 LE:256] payload[56] rcv from cap vapid:1
<7>Aug 02 2021 15:36:12.650.2 38eb-4821-3300 WSRV/7/BTRACE:(BTRACE)(WLAN_AP)(94e6-f741-9f83):SeqNo[35] elapsed[0 ms][ICMP] Ping request from [192.190.190.2] to [192.190.190.139] id[11180] seq[BE:1 LE:256] payload[56] send to fw len:98
<7>Aug 02 2021 15:36:12.910.1 38eb-4821-3300 WSRV/7/BTRACE:(BTRACE)(WLAN_AP)(94e6-f741-9f83):SeqNo[35] elapsed[257 ms][ICMP] Ping request from [192.190.190.2] to [192.190.190.139] id[11180] seq[BE:1 LE:256] payload[56] send to air success status :0 ack_rssi:63 bw:0 mcs:9 trans_cnt:1 tid:0 rate:114 Mbps
<7>Aug 02 2021 15:36:12.910.2 38eb-4821-3300 WSRV/7/BTRACE:(BTRACE)(WLAN_AP)(94e6-f741-9f83):SeqNo[36] elapsed[0 ms][ICMP] Ping reply from [192.190.190.139] to [192.190.190.2] id[11180] seq[BE:1 LE:256] payload[56] send pkt to cap vapid:18
```

- SeqNo[xxx]: 表示该ping包内携带的序列号，通过该序列号可以将trace和某个具体ping报文对应起来。
- seq[BE: x LE:y]: 表示trace的报文序列号，同一个ping包的request与response seq相同，BE和LE分别表示seq的大端和小端数。
- rcv from cap: 表示Wi-Fi侧收到转发侧发给用户的ping request报文。
- send to fw: 表示Wi-Fi侧LMAC模块成功将ping request报文发送给firmware模块。
- send to air: success status 0则表示Wi-Fi侧成功将ping request报文通过空口发送给用户；fail status x则表示Wi-Fi侧发送ping request报文失败，x为失败原因码，解释如下：
 - /* 0: 发送成功 */
 - /* 2: 在fw，因为Remove_mpdus 命令而丢弃 */
 - /* 3: 在fw，因为Remove_transmitted_mpdus 命令而丢弃 */
 - /* 4: 在fw，因为Remove_untransmitted_mpdus命令而丢弃 */
 - /* 5: 在fw，因为fw_reason1 命令而丢弃 */
 - /* 6: 在fw，因为fw_reason2 命令而丢弃 */
 - /* 7: 在fw，因为fw_reason3 命令而丢弃 */
 - /* 8: 在fw，因为queue_disable 而丢弃 */
- send pkt to cap: 表示Wi-Fi侧将ping response报文成功送到转发侧，后面将会由转发侧处理，并通过AP网口发送到有线侧网络设备。

V200R019C00及之前版本：

- 如果打印信息中没有出现Recved from software switch，则说明ping request报文没有从转发模块发送到WiFi驱动模块，此时有线侧出现问题的可能性比较大。
- 如果打印信息中出现Recved from software switch打印，但是没有出现Success to send pkt to air，则说明WiFi驱动模块没有成功将报文发送给用户，问题出现在无线侧。

- 如果打印信息中出现Success to send pkt to software switch，则说明用户已经回应了ping response报文，并上送到转发模块，此时有线侧出现问题的可能性比较大。
- 如果打印信息中确认ping request报文已经成功发给用户，但是没有出现Success to send pkt to software switch打印，则说明问题出现在无线侧。

V200R020C00及之后版本（AirEngine X760系列AP）：

- 如果打印信息中没有出现Receive from fwd打印，则说明ping request报文没有从转发模块发送到WiFi模块，此时有线侧出现问题的可能性比较大。
- 如果打印信息中没有出现send to rt ok打印，则说明ping request报文没有被发送至SMAC，问题出现在无线PMAC侧。
- 如果打印信息中出现send to air fail打印，此时无线侧出现问题的可能性比较大。
- 如果打印信息中出现send to np ok，则说明用户已经回应了ping response报文，并上送到转发模块，此时有线侧出现问题的可能性比较大。
- 如果打印信息中确认ping request报文已经成功发给用户，但是没有出现send to np ok打印，则说明问题出现在无线侧。

V200R020C00及之后版本（AirEngine X761系列AP）：

- 如果打印信息中没有出现recv from cap打印，则说明ping request报文没有从转发模块发送到WiFi模块，此时有线侧出现问题的可能性比较大。
- 如果打印信息中没有出现send to fw打印，则说明ping request报文没有被发送至firmware，问题出现在无线侧。
- 如果打印信息中出现send to air success status 0打印，没有出现send pkt to cap打印，则说明用户收到了ping response报文，但AP没有收到ping response报文，此时无线侧出现问题的可能性比较大。
- 如果打印信息中出现send to air fail status x打印，则说明WiFi模块没有成功将报文发送给用户，问题出现在无线侧。
- 如果打印信息中出现send pkt to cap打印，则说明用户已经回应了ping response报文，并wifi已上送ping response到转发模块，此时有线侧出现问题的可能性比较大。

针对上行ping包，即用户从无线侧往有线侧网络设备ping包，判断方法和下行ping基本一致。

6 故障处理：设备登录类问题

6.1 SSH登录失败

6.2 Web网管登录失败

6.1 SSH 登录失败

以下故障处理步骤均是在通过Console口登录设备后进行的操作。

步骤1 检查是否配置了管理面隔离功能

对于具有管理网口的设备，需要检查是否开启了管理面隔离功能，如果开启了，则系统会禁止通过业务口访问设备管理面，也就是说用户通过非管理口登录设备时会登录失败。

1. 检查配置是否开启了管理面隔离功能

缺省情况下，设备是开启了管理面隔离功能的，如果希望通过业务口登录设备，可以执行命令**mgmt isolate disable**关闭管理面隔离功能。

2. 执行命令**display mgmt interface**查看当前设备的管理网口，检查用户是否是通过非管理口登录设备。

查看设备的管理网口。

```
<AC> display mgmt interface
```

```
-----  
Interface name
```

```
MEth0/0/1  
-----
```

```
Count:1
```

步骤2 检查是否配置了SSH服务器源接口

对于AC设备，如果指定了源接口，那么用户就只能通过指定的接口登录设备。

缺省情况下，未指定源接口。出厂配置文件中，有管理网口的设备，源接口为管理网口；无管理网口的设备，源接口为VLANIF 1。

如果指定的接口不合理，可以通过执行命令**ssh server-source -i { interface-type interface-number | all }**，重新配置SSH服务器源接口。

步骤3 确保SSH客户端使用的加解密算法与设备匹配

- 为确保设备的安全性，当前设备默认关闭了部分不安全的加密算法，可以通过以下命令开启。配置不安全的加密算法需加载弱加密算法插件。

```
<AC> system-view
Enter system view, return user view with Ctrl+Z.
[AC] ssh server secure-algorithms cipher aes256_ctr aes128_ctr 3des aes128 aes256_cbc
Info:Insecure encryption algorithm is enabled,It is recommended to disable the insecure encryption algorithm.
[AC] ssh server secure-algorithms hmac sha2_256 md5 md5_96 sha1 sha2_256_96 sha1_96
Info:Insecure encryption algorithm is enabled,It is recommended to disable the insecure encryption algorithm.
[AC] ssh server key-exchange dh_group14_sha1 dh_group1_sha1 dh_group_exchange_sha1
Info:Insecure exchange algorithm is enabled,It is recommended to disable the insecure exchange algorithm.
```

- 更换SSH客户端，使用最新版本的PuTTY等客户端。

步骤4 检查客户端IP是否在允许列表中

```
<AC> display current-configuration | include ssh
ssh server permit interface GigabitEthernet0/0/1 //配置了SSH服务器上允许连接GigabitEthernet0/0/1，但会限制其它接口的连接
```

缺省情况下，SSH服务器允许客户端通过所有物理接口连接。可以在系统视图下执行命令**undo ssh server permit interface**，取消对物理接口连接的限制。

步骤5 检查VTY用户界面配置是否正确

通过Console登录设备，查看VTY配置，确认VTY通道绑定SSH协议和使用AAA认证模式。

例如：通过命令查看，可以确认已正确配置AAA认证模式和绑定SSH协议。

```
<AC> system-view
[AC] user-interface vty 0 4
[AC-ui-vty0-4] display this
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %^%#3]qy<(%O)95+
 ([Fe0>o7PbnY=>Qr.05%,INA&}t1g}*^FA~qAL*($vVJa"]*%^%
#
user-interface vty 0 4
 authentication-mode aaa //已配置AAA模式
 protocol inbound all //已绑定了SSH协议
user-interface vty 16 20
 protocol inbound all
#
```

如果未绑定SSH协议，请执行以下操作：

```
[AC-ui-vty0-4] protocol inbound ssh
```

或

```
[AC-ui-vty0-4] protocol inbound all
```

----结束

6.2 Web 网管登录失败

步骤1 检查是否配置了管理面隔离功能

对于具有管理网口的设备，需要检查是否开启了管理面隔离功能，如果开启了，则系统会禁止通过业务口访问设备管理面，也就是说用户通过非管理口登录设备时会登录失败。

1. 检查配置是否开启了管理面隔离功能
缺省情况下，设备是开启了管理面隔离功能的，如果希望通过业务口登录设备，可以执行命令**mgmt isolate disable**关闭管理面隔离功能。
2. 执行命令**display mgmt interface**查看当前设备的管理网口，检查用户是否是通过非管理口登录设备。

查看设备的管理网口。

```
<AC> display mgmt interface
```

```
-----  
Interface name  
-----
```

```
MEth0/0/1  
-----
```

```
Count:1
```

步骤2 检查是否配置了HTTP/HTTPS服务器源接口

对于AC设备，如果指定了源接口，那么用户就只能通过指定的接口登录设备。

缺省情况下，未指定源接口。出厂配置文件中，有管理网口的设备，源接口为管理网口；无管理网口的设备，源接口为VLANIF 1。

如果指定的接口不合理，可以通过执行命令**http secure-server server-source -i { interface-type interface-number | all }**，重新配置HTTP/HTTPS服务器源接口，或者将某源接口设置为management-interface并且该源接口下必须配置IP地址。

步骤3 检查是否配置HTTP服务器的访问控制列表

1. 在任意视图下执行命令**display current-configuration | include http acl**，查看是否有**http acl acl-number**的配置。

```
<Huawei> display current-configuration | include http acl  
http acl 2000
```

如果有，请记录该[acl-number](#)。

2. 在任意视图下执行命令**display acl acl-number**，查看该访问控制列表中是否拒绝了Web用户客户端的IP地址。

如果是，则在ACL视图下执行命令**undo rule rule-id**，删除拒绝规则，再执行相应的命令修改访问控制列表，允许Web用户客户端的IP地址通过。

步骤4 检查HTTP/HTTPS服务是否正常开启

```
<Huawei> display http server  
HTTP server status : Enabled (default: disable)  
HTTP server port : 80 (default: 80)  
HTTP timeout interval : 10 (default: 10 minutes)  
Current online users : 0  
Maximum users allowed : 5  
HTTPS server status : Enabled (default: enable)  
HTTPS server port : 443 (default: 443)  
HTTPS SSL Policy : default_policy
```

在通过HTTP方式登录设备时，设备会强制跳转到HTTPS的方式。因此，需要确保HTTPS server是正常开启的，否则设备无法跳转到HTTPS的方式，会导致登录失败。

如果**HTTP server status**为**disable**，设备无法通过HTTP方式登录设备，请在系统视图下执行命令**http server enable**开启HTTP服务，或者通过HTTPS的方式登录设备，即通过在浏览器地址栏输入“[https://ip-address](#)”的方式来登录设备。

如果**HTTPS server status**为**disable**，设备将无法通过Web网管方式登录，请在系统视图下执行命令**http secure-server enable**开启HTTPS服务。

如果地址栏中输入的IP address带的端口号与服务器端口号不一致时，在系统视图下执行命令**http server port**和**http secure-server port**可配置服务器端口号。

步骤5 检查设备是否使用的旧证书

在诊断视图下，执行**display pki certificate local realm default**命令查看当前证书中OU字段是否存在‘&’符号。

Subject: C=CN, O=HUAWEI, **OU**=Switch & Enterprise Gateway Product Line,
CN=2102352QVG1234567890.huawei.com

预置证书中存在‘&’符号，Chrome浏览器无法识别证书中的‘&’符号，判断证书不合法，导致无法在Chrome浏览器中登录WEB页面或者无法访问内置Portal认证页面。

具体请参见：<https://support.huawei.com/carrier/docview!docview?nid=ENEWS2000009212&partNo=&path=false>

----结束

7 故障处理：双机备份类问题

7.1 VRRP热备未建立

7.2 无线配置同步失败

7.1 VRRP 热备未建立

步骤1 检查主备AC之间的HSB通道是否正常。

分别登录主备AC，执行**display hsb-service 0**命令，查看主备AC之间的链路是否畅通。链路状态为Connected表示链路畅通，Disconnected表示链路已断开，需检查链路使其恢复Connected状态。

HSB主备两端的端口号需要保持一致，Local IP地址和Peer IP地址之间需要能够相互ping通。

```
[AC1] display hsb-service 0
Hot Standby Service Information:
```

```
-----
Local IP Address      : 10.1.1.1
Peer IP Address       : 10.1.1.2
Source Port           : 10241
Destination Port      : 10242
Keep Alive Times      : 5
Keep Alive Interval   : 2
Service State         : Connected
Service Batch Modules :
-----
```

步骤2 检查主备AC上热备业务是否配置。

分别登录主备AC，执行**display hsb-group 0**命令，查看HSB备份组的配置信息。

主AC和备AC的VRRP状态分别为Master和Backup。HSB备份组绑定的业务模块中，备份AP信息需要绑定AP模块，备份用户信息需要绑定Access-user模块。

```
[AC1] display hsb-group 0
Hot Standby Group Information:
```

```
-----
HSB-group ID          : 0
Vrrp Group ID         : 1
Vrrp Interface         : Vlanif100
Service Index         : 0
Group Vrrp Status      : Master
Group Status           : Active
-----
```

```
Group Backup Process      : Realtime
Backup Start Time        : -
Peer Group Device Name   : AC6805
Peer Group Software Version : V200R022C00SPC100
Group Backup Modules     : Access-user
                        DHCP
                        AP
-----
[AC2] display hsb-group 0
Hot Standby Group Information:
-----
HSB-group ID             : 0
Vrrp Group ID           : 1
Vrrp Interface           : Vlanif100
Service Index            : 0
Group Vrrp Status        : Backup
Group Status             : Inactive
Group Backup Process     : Realtime
Backup Start Time        : THU, 13 Jul 2023 06:16:00
Peer Group Device Name   : AC6805
Peer Group Software Version : V200R022C00SPC100
Group Backup Modules     : Access-user
                        DHCP
                        AP
-----
```

步骤3 检查主备AC上VRRP虚地址、优先级、回切时延等配置是否正确。

分别登录主备AC，在VLANIF接口视图下执行**display this**命令，查看VLANIF接口下的VRRP配置。

主AC配置的VRRP优先级 > 备AC配置的VRRP优先级；主AC的回切延时建议配置为1800，备AC的则建议保持缺省值。

```
[AC1] interface vlanif 100
[AC1-Vlanif100] display this
interface Vlanif100
 ip address 10.1.1.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.3 //VRRP虚地址
 admin-vrrp vrid 1
 vrrp vrid 1 priority 120 //VRRP优先级
 vrrp vrid 1 preempt-mode timer delay 1800 //VRRP回切时延
[AC2] interface vlanif 100
[AC2-Vlanif100] display this
interface Vlanif100
 ip address 10.1.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.3 //VRRP虚地址
 admin-vrrp vrid 1
```

检查是否配置了VRRP备份组的状态恢复延迟时间。

VRRP备份组中，接口状态或联动的BFD会话状态不稳定时，容易造成VRRP状态频繁震荡，导致用户流量丢失。配置VRRP备份组的状态恢复延迟时间可以有效解决这个问题。配置后，VRRP备份组在接收到接口、BFD会话的Up事件时不会立刻响应，而是等配置的状态恢复延迟时间超时后，再进行相应的处理。

```
<AC1> system-view
[AC1] vrrp recover-delay 30
<AC2> system-view
[AC2] vrrp recover-delay 30
```

步骤4 检查Source ip-address是否正确配置。

执行**display capwap configuration**命令查看CAPWAP源地址。VRRP备份场景下，CAPWAP源地址需配置为VRRP虚地址。

```
[AC1] display capwap configuration
-----
```

```
Source interface          : -
Source ip-address         : 10.1.1.3
Echo interval(seconds)   : 25
Echo times                : 6
Control priority(server to client) : 7
Control priority(client to server) : 7
Control-link DTLS encrypt : disable
DTLS PSK value           : *****
PSK mandator match switch : enable
Control-link inter-controller DTLS encrypt : disable
Inter-controller DTLS PSK value : *****
IPv6 status              : disable
-----
```

步骤5 检查hsb是否已使能。

进入hsb-group视图，执行**display this**命令进行查看。

```
[AC1-hsb-group-0] display this
#
hsb-group 0
track vrrp vrid 1 interface Vlanif100
bind-service 0
hsb enable
#
return
```

----结束

7.2 无线配置同步失败

步骤1 检查无线配置同步链路是否正常建立。

```
[AC] display sync-configuration status
Info: This operation may take a few seconds. Please wait for a moment.done.
Controller role:Master/Backup/Local
```

Controller IP	Role	Device Type	Version	Status	Last synced
192.168.10.1	Local	-	-	up	-

Total: 1

- 如果无线配置同步链路状态是up，说明主备AC配置已同步。
- 如果无线配置同步链路状态是down，说明配置同步链路未建立。需要确保主备AC能够Ping通，并参考产品文档检查无线配置同步的配置是否正确。除此之外还需要确认是否开启了AC间CAPWAP链路加密。

确认AC间CAPWAP链路加密是否使能以及主备AC的psk密钥配置是否正确，一般情况下在主备AC间连通性正常但是链路状态为down，可确认为AC间CAPWAP链路加密psk不一致导致的。

```
<AC> display capwap configuration
-----
Source interface IPv4      : vlanif100
Source interface IPv6      : -
Source IPv4 address       : -
Source IPv6 address       : -
Echo interval(seconds)    : 25
Echo times                : 6
Control priority(server to client) : 7
Control priority(client to server) : 7
Data-link DTLS encrypt    : disable
Data-link inter-controller DTLS encrypt : disable
Control-link DTLS encrypt : disable
DTLS PSK value            : *****
Control-link inter-controller DTLS encrypt : enable
```

```
Inter-controller DTLS PSK value      : *****
IP version                          : IPv4
Message-integrity PSK value         : *****
Message-integrity check switch      : enable
Sensitive-info PSK value            : *****
Sensitive-info inter-controller PSK value : *****
DTLS no-auth status                 : disable
DTLS cert-mandatory-match status    : disable
DTLS version1.0 status              : disable
DTLS CBC status                     : disable
-----
```

关闭主备AC间CAPWAP DTLS加密相关配置（主备AC同时配置）：

```
<HUAWEI> system-view
[HUAWEI] capwap dtls inter-controller control-link encrypt off
Warning: This operation may cause devices using CAPWAP connections to reset or go offline.
Continue? [Y/N]:y
[HUAWEI] capwap message-integrity check disable
Warning: In a backup scenario, the PSK and status of CAPWAP message integrity check must be the
same between the master and backup e nds. This operation may cause devices using CAPWAP
connections to reset or go offline. Continue? [Y/N]:y
```

步骤2 检查当前主备AC配置是否一致。

如果无线配置同步链路状态是cfg-mismatch（config check fail），说明当前主备AC配置不一致。执行如下操作：

1. 在备AC诊断视图下执行命令**display unresumed-configuration**，检查是否存在配置恢复失败记录。
2. 检查具体是哪些配置不一致：
 - V200R019C00之前版本，分别在主备AC上执行命令**display current-configuration sync**，查看AC上当前生效的公有配置，然后进行对比，检查具体是哪些配置不一致。
 - V200R019C00及之后版本，在Master AC上执行命令**display sync-configuration compare**，检查无线配置同步两AC的公有配置的一致性。

步骤3 检查是否存在配置同步执行失败的命令行。

如果无线配置同步链路状态是cfg-mismatch（config proc fail），说明配置同步建链成功，但是主AC上配置同步到备AC的命令行执行失败。检查哪些命令行同步时执行失败：

- V200R019C00之前版本，查看用户操作日志operation.log里命令行失败记录。
Line 29080: 2019-12-04 11:42:51.972.2+08:00 AC6800V-Bei %%%01SHELL/5/CMDRECORDFAILED(I)
[13974]:Record command information. (Task=WMP_, Ip=192.168.2.20, User=beiwai, Command="wired-port-profile name xinzhongxin", Result=**ExecutionFailure**)
- V200R019C00及之后版本，在备AC上执行命令**display sync-configuration fail-record**检查哪些命令执行失败。

步骤4 在主AC的WLAN视图下执行命令**synchronize-configuration**，手动触发无线配置同步。

步骤5 如上述步骤仍然无法解决问题，请收集AC的一键诊断信息及对应时间段的用户日志、诊断日志，并联系技术支持人员。

----结束

8 故障处理：AC/AP 升级类问题

步骤1 在AC上执行命令**display ap update status all**查看AP升级进度、状态的信息。

```
<AC> display ap update status all
FT : File Type
```

ID	Name	AP Type	AP Group	AP MAC	FT	Update Version	Last Update Time	Update Status
0	ap0	AirEnginexxxxS	default	60de-4476-e320	FIT	V200R020C00B008	2020/08/22 18:51	succeed
1	ap1	AirEnginexxxxS	default	60de-4476-e340	FIT	V200R020C00B008	2020/08/22 18:51	downloading(progress: 80%/0%)
2	ap2	AirEnginexxxxS	default	60de-4476-e360	FIT	V200R020C00B008	2020/08/22 18:51	downloading(progress: 100%/50%)
3	ap3	AirEnginexxxxS	default	60de-4476-e380	FIT	-	-	-
4	ap4	AirEnginexxxxS	default	60de-4476-e3a0	FIT	-	-	-
5	ap5	AirEnginexxxxS	default	60de-4476-e3c0	FIT	-	-	-
Total: 6								

根据升级结果对应的失败原因，针对性查询产品文档进行相应处理。

步骤2 检查AP软件包是否存在且文件名是否正确

升级设备前请确保升级文件已存放在文件服务器相关目录下且可以读取；AP升级文件名和大小需要和源文件一致，不可以修改。如果升级文件不存在或文件名、文件大小不正确，请登录华为公司企业业务支持网站（<http://support.huawei.com/enterprise>）获取正确的升级文件，上传至AC或者文件服务器。

- 如果通过ac-mode方式或者AC作为SFTP/FTP服务器方式，需将AP软件版本存储在AC默认存储器路径。
- 如果是使用其他软件作为SFTP/FTP服务器，确保软件版本已存放在SFTP/FTP目录下且可读取，同时需要确保文件名和文件大小和源文件一致。

步骤3 检查AP软件包同设备类型是否匹配

AP软件版本必须同设备类型一致，不同类型AP的软件包不可互相加载。

步骤4 检查AP和服务器网络之间是否可以Ping通且网络质量良好

以PC作为文件服务器为例，升级AP时，以PC作为文件服务器，利用FTP、TFTP或SFTP软件进行上传操作，PC的网口必须与AP网口直连，并且需要保证PC和AP之间能够正常通信。

1. 在PC上进入Windows的命令行提示符，执行命令**ping**，查看PC是否能够ping通AP。
当系统显示“Request time out”时，表示目标设备不可达。
2. 如果ping不通AP，则需要修改PC的IP地址，使得PC的IP地址与AP的IP地址同网段。
FIT AP缺省的IP地址为169.254.1.1，所以PC的IP地址必须在169.254.1.0网段（169.254.1.1除外，建议使用169.254.1.100），子网掩码是255.255.255.0。
如果FIT AP的IP地址已经修改，可在AC上执行**display ap all**命令查看AP的IP地址。
3. 修改完成后，在PC上再次执行**ping**命令，确认能够ping通AP。
4. 如果设备与服务器之间网络延时大或者丢包，会导致AP下载软件版本超时失败，需要排查中间网络。

步骤5 检查FTP/SFTP服务器用户名或密码是否正确

服务器用户名或密码配置不正确会导致下载AP软件版本失败。

1. 执行**display ap update configuration**命令查看AP版本升级时的配置信息。

[AC-wlan-view] **display ap update configuration**

```
-----
AP update mode      : ftp-mode
FTP configuration
FTP IP              : 192.168.0.11
FTP username        : ftp
FTP password         : *****
FTP max number      : 50
SFTP configuration
SFTP IP             : -
SFTP username        : anonymous
SFTP password        : *****
SFTP max number      : 50
-----
```

2. 检查登录服务器的用户名和密码是否配置正确，如果配置错误，执行如下命令进行重新配置。

- 配置升级模式为SFTP模式并配置SFTP服务器。

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap update mode sftp-mode
[AC-wlan-view] ap update sftp-server ip-address 192.168.1.100 sftp-username admin sftp-
password cipher YsHsjx_202206
```

- 配置升级模式为FTP模式并配置FTP服务器。

```
<AC> system-view
[AC] wlan
[AC-wlan-view] ap update mode ftp-mode
[AC-wlan-view] ap update ftp-server ip-address 192.168.1.100 sftp-username admin sftp-
password cipher YsHsjx_202206
```

步骤6 检查AC是否未开启FTP/SFTP Server

- 配置AC为FTP服务器时，执行**display ftp-server**命令检查是否开启FTP服务。
如果FTP服务功能没有开启，请在系统视图下执行**ftp server enable**命令开启设备的FTP服务。
- 配置AC为SFTP服务器时，执行**display ssh server status**命令检查是否开启SFTP服务。
如果SFTP服务功能没有开启，请在系统视图下执行**sftp server enable**命令开启SSH服务器端的SFTP服务。

步骤7 检查AP当前是否为normal状态

AP为“normal”状态时，能够正常升级；AP为其他状态时，升级方式会有限制。

如果AP状态为“normal”，能够正常升级；如果AP状态为“ver-mismatch”或“config-failed”，只能进行自动升级；如果AP为其他状态，可通过连接AP串口进行命令行升级或通过Uboot的方式进行升级。

通过Uboot方式进行升级的具体操作请参见升级指导书，升级指导书获取路径：请先登录华为公司企业业务支持网站（<http://support.huawei.com/enterprise>），登录后，根据AP类型和版本名称，获取相应的升级指导书。

步骤8 检查AP当前空闲内存是否足够

在AP上执行**display memory-usage**命令，检查AP当前空闲内存是否足够。

如果当前AP剩余内存空间不够容纳新的系统软件包，则需要重启AP后再尝试进行升级或者通过Uboot的方式进行升级。

通过Uboot方式进行升级的具体操作请参见升级指导书，升级指导书获取路径：请先登录华为公司企业业务支持网站（<http://support.huawei.com/enterprise>），登录后，根据AP类型和版本名称，获取相应的升级指导书。

步骤9 以PC作为FTP、SFTP或TFTP服务器时，建议暂时关闭防火墙，并检查AP能否正常访问文件服务器。**步骤10 检查AAA视图下用户是否具有FTP/SFTP权限，以及是否配置FTP/SFTP路径。**

```
local-user admin privilege level 15
local-user admin ftp-directory flash:/
local-user admin service-type telnet terminal ssh ftp http
```

步骤11 采集故障信息

1. 在AC上执行如下命令收集相关信息。

信息类别	命令视图	命令
AC配置信息	所有视图	display current-configuration
AP升级配置信息	所有视图	display ap update configuration
AP升级结果信息	所有视图	display ap update status { ap-name ap-name ap-id ap-id all }
AP在升级过程中产生的错误记录	诊断视图	display wlan debuginfo [process process-id] type 1 from 0 to 1000
AC日志信息	所有视图	display logbuffer

2. 在AP上执行如下命令收集相关信息。

信息类别	命令视图	命令
AP日志信息	所有视图	display logbuffer

----结束

9 故障处理：设备管理类问题

9.1 License激活失败

9.2 CPU占用率高

9.3 供电异常

9.1 License 激活失败

步骤1 检查License文件是否存在且存储路径正确

执行命令**dir flash:/*.dat**，检查License文件是否存在且路径为“flash:/”。

```
<HUAWEI> dir flash:/*.dat
Directory of flash:/
Idx Attr  Size(Byte) Date      Time(LMT) FileName
0 -rw-    1,578 Sep 08 2015 19:49:22 LICQPZQ6F901HL_210235791710F9000002.dat
```

如果设备flash:/目录下没有License文件。可通过FTP/SFTP等方式上传License文件至设备根目录。

步骤2 检查License文件名输入是否正确

检查License文件激活时文件名是否输入正确且完整。

```
<HUAWEI> license active LICQPZQ6F901HL_210235791710F9000002.dat
```

如果设备提示“Error: The specified file does not exist or is illegal.”，请确保License文件名输入正确。

步骤3 检查设备类型和设备ESN号与License文件中的是否一致

1. 执行命令**display version**，查看设备型号。

```
<HUAWEI> display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.160 (AC6805 V200R022C00SPC100)
Copyright (C) 2011-2015 HUAWEI TECH CO., LTD
```

2. 执行命令**display esn**，查看设备ESN号。

```
<HUAWEI> display esn
ESN of device: 210235791710F9000002
```

3. 用文本编辑器打开License源文件，查看设备类型和设备ESN号与License文件中的是否一致（源文件不可作任何修改）。

```
Product=AC6805
Feature=Service
```

```
Esn="210235791710F9000002"  
Attrib="COMM, NULL, NULL, NULL, NULL, NULL"  
Version=V200R021  
Libver=1.2  
Sign=
```

说明

第一次允许激活ESN号不匹配的License，有效期60天，后续不再允许激活ESN不匹配的License。

4. 如果设备类型或设备ESN与License文件中的相应字段不一致，请根据设备类型和设备ESN号，重新获取License文件并加载激活。

请采集如下信息并反馈到邮箱：license@huawei.com。

- 华为数通产品License Key重新申请及承诺函。
- 合同号和项目名称。
- 错误的ESN号码和需要申请的正确的ESN号码。
- 错误的license文件。
- 版本信息、补丁信息、配置信息、License信息和日志信息。

步骤4 查看设备License资源备份

1. 执行命令**display license resource usage**查看License文件中定义的资源项的使用情况。

```
<HUAWEI> display license resource usage  
Activated License: flash:/LIC92680232*****_*****5396810CB000006.dat      FeatureName |  
ConfigureItemName |  
ResourceUsage  
CRFEA1          LH85WLANAP01          0/256
```

2. 如果是云AC，执行命令**display cloud license**来查看从iMaster NCE-Campus下发到AC的License资源。

```
<HUAWEI> display cloud license  
-----  
License type      Expire time  
-----  
Indoor AP         -  
Outdoor AP        2020-12-11  
Indoor AP-S        2020-12-11  
Outdoor AP-S       2020-12-11  
Indoor AP-EC       -  
Outdoor AP-EC      2020-12-11  
Common AP         -  
Indoor Wi-Fi 6 AP  2020-12-11  
Outdoor Wi-Fi 6 AP 2020-12-11  
Agile distributed AP 2020-12-11  
-----  
Total: 10
```

----结束

9.2 CPU 占用率高

步骤1 检查软件和补丁版本是否需要更新

检查软件和补丁版本，如最新补丁中存在类似问题解决描述信息，请更新到最新版本和补丁。

```
<AC> display version  
Huawei Versatile Routing Platform Software  
VRP (R) software, Version 5.130 (AC6805 V200R022C00SPC100)
```

```
Copyright (C) 2015-2017 HUAWEI TECH CO., LTD
...
<AC> display patch-information
Patch version   : V200R022C00SPH120
Patch package name: flash:/V200R022C00SPH120.pat
```

步骤2 处理CPU占用率高的任务

1. 查看当前CPU占用率。

```
AC-diagnose] display cpu-usage
CPU Usage Stat. Cycle: 30 (Second)
usr: 3.4% sys: 1.1% irq: 0.0% softirq: 0.0%
CPU Usage: 4.7% Max: 46.7%
CPU Usage Stat. Time : 2019-10-14 10:59:16 (core 0)
CPU Usage Max. Time : 2019-10-14 10:56:43 (core 0)
Core-0 Usage: 4.7%  usr: 3.4% sys: 1.1% irq: 0.0% softirq: 0.0%
Core-1 Usage: 3.7%  usr: 2.6% sys: 1.2% irq: 0.0% softirq: 0.0%
PID ProcessName CPU% Runtime State
188 vos.o 4.7 66380 S
191 wmi 0.6 5990 S
190 wmi 0.6 6035 S
194 nac 0.5 4791 S
195 nac 0.5 4807 S
189 wmc 0.5 4675 S
196 ucm_gc 0.3 3774 S
192 dhcp 0.3 3764 S
.....
[AC-diagnose] display cpu-usage pid 188 //对应的ProcessName为vos.o
The Thread CPU usage: % of ProcessId: 188
-----
VosTaskId ThreadID ThreadName CPU% Runtime State
45 441 SessionWorkerTask 54.4 24499 S
54 450 bcmCNTR.0 4.9 3668 S
0 402 vos.o 4.0 2820 R
189 782 ROUT 3.2 2541 S
171 567 POE 2.8 1876 S
57 453 bmLINK.0 2.5 1897 S
3 344 TICK 2.3 1813 S
202 795 STP 1.9 1407 S
169 565 AREM 1.6 1146 S
50 446 bcmINTR 1.5 1131 S
255 1047 We0 1.4 146 S
43 439 WebT 0.9 854 S
.....
```

2. 查看CPU使用率，结合日志，确认导致CPU高的任务及原因

查看日志，确认CPU高及CPU恢复时间，通过日志确认导致CPU高的任务。

```
2018-2-24 10:52:34+00:00 AC6605 %%%01MON/4/CPU_USAGE_HIGH(l)[50]:The CPU is overloaded,
and the top three thread CPU occupancy are TASK1 TASK2 TASK3. (CpuUsage=xx%, Threshold=xx%)
```

TASK1 TASK2 TASK3为引起CPU高的前三个任务，请根据[表9-1](#)来查询引起CPU占用率高的原因及解决措施。

表 9-1 常见 CPU 占用率高任务及解决措施

任务名称	任务描述	该任务导致CPU占用率高的原因	解决措施
ARP	实现ARP协议栈，管理协议状态机，维护协议相关的数据库	<ul style="list-style-type: none">底层报文上送CAR太大，并且收到大量ARP报文老化时间太短	调整底层报文上送CAR和老化时间

任务名称	任务描述	该任务导致CPU占用率高的原因	解决措施
SOCK	报文接收和发送类任务	大量协议报文上送CPU时，该任务的CPU占用率会出现显著的升高，通常是导致系统CPU占用率高的主要原因。 通常由以下原因引起： <ul style="list-style-type: none"> - CPU遭受网络攻击 - 网络环路 - 业务流量过大 	<ul style="list-style-type: none"> - 判断是由网络环路、网络攻击引起时需进行相应排查 - 联系技术支持人员确认是否为业务流量过大的情况并做相应处理
CFM	配置管理任务，主要处理主控配置恢复、接口配置恢复等配置管理业务	配置恢复	无需处理
DHCP	实现DHCP协议栈处理，完成DHCP Snooping及DHCP Relay等功能	CPU遭受DHCP协议报文攻击	增加网络防攻击配置
DSO/D S1	网管同步数据任务	同步过于频繁	网管上调低同步周期
FIB/FIB6	ipv4/ipv6 FIB表项管理	下发大量路由时，路由持续震荡	无需处理
FTPS	提供FTP服务功能（FTP服务器），伴随FTP业务还会存在FC0、FC1等任务	FC任务在大文件传输时会CPU冲高，例如传软件包甚至并发传多个软件包等	文件传输结束后自然恢复，或尽量减少并行多个大文件同时传输
IC	信息中心主任务，接收、输出业务模块产生的日志、告警、debug等	频繁触发日志、debug输出信息	降低日志、debug等触发操作的操作频率
IP	负责IP协议任务统一调度	IPv6报文收发量大	降低报文收发量，例如调整CPCAR
PM/PM S	性能管理任务，性能统计数据处理、PM配置命令处理、性能数据上报	PM配置较多时（统计数据较多），触发性能数据采集、处理则可能CPU占用率较高	<ul style="list-style-type: none"> - 降低性能统计数据采集频率 - 不同的统计任务配置不同统计周期（相互错开统计时间点）

任务名称	任务描述	该任务导致CPU占用率高的原因	解决措施
vt0/vt1 /vt2 ...	对编号为0/1/2 ... 的登录设备的用户 进行认证、命令处 理	用户操作，尤其输入输出操 作频繁，例如黏贴命令到屏 幕（输入）或执行大量回显 命令（输出）	降低输入输出频 率，并且操作结束 后会自然恢复
Co0/Co 1	对编号为0/1的串 口登录设备的用户 进行认证、命令处 理	串口下用户操作，尤其输入 输出操作频繁，例如黏贴命 令到屏幕（输入）或执行大 量回显命令（输出）	降低输入输出频 率，并且操作结束 后会自然恢复
We0/W e1 ...W ebT/ Session Admin Task/ Session Worker Task	WEB业务处理任 务，处理所有 WEB用户的请求	WEB网管操作频繁	降低WEB网管操作 频率
WMT_ PM	eSight网管获取 PM性能采集数据	eSight网管周期性采集AP数 据	调整PM性能采集 周期
_S0fSN MP/ SNP6	处理IPv4/IPv6 SNMP协议网管操 作任务	接入SNMP网管较多，或者 SNMP网管操作频繁	降低SNMP网管操 作频率
SNMP trap task	设备上报SNMP告 警	设备告警较多	无需处理
LYNC	对接微软Lync功能	微软Lync服务器上数据较 多	无需处理
FM	设备告警抑制功能	设备产生告警较多	无需处理
COMM /MFPI	处理转发上报控制 面报文	大量协议报文上送CPU时， 该任务的CPU占用率会出现 显著的升高，通常是导致系 统CPU占用率高的重要原 因。 通常由以下原因引起： - CPU遭受网络攻击 - 网络环路 - 业务流量过大	<ul style="list-style-type: none"> - 判断是由网络环路、网络攻击引起时需进行相应排查 - 联系技术支持人员确认是否为业务流量过大的情况并做相应处理
WAPI_ RCV_P KT	WAPI认证报文收 发	大量用户并发WAPI认证	一般不会出现，若 出现尝试降低并发 量或建议换其他认 证方式

任务名称	任务描述	该任务导致CPU占用率高的原因	解决措施
WLAN_AgeList	WPA/WPA2用户老化	wpa密钥协商超时重传，wpa用户并发大	暂无，一般不会出现
ArrmThread	射频调优	调优期间不断处理AP上报的邻居信息，算法复杂计算量大	配置在夜间进行定时调优
WDM_FILE_READ	AP升级读取文件任务	使用AC模式批量升级AP	采用FTP模式，或者将大批量AP分多批次升级
WDM_MAIN_CTRL	AP升级控制任务	批量升级AP	采用FTP模式，将大批量AP分多批次升级
WMT_NB	探测邻居信息	调优期间，处理AP上报邻居信息。AP数量过多情况下可能会导致CPU高	配置夜间定时调优
WMT_LKM	CAPWAP链路管理	漫游组、无线配置同步等业务触发CAPWAP反复建链	观察对应业务触发建立的CAPWAP链路是否经常反复UP/DOWN，如果存在解决该问题
WMT_CLUS/WMT_CSP	无线配置同步	反复修改配置或执行配置同步批量备份动作	一般不会出现CPU高的情况
WMT_DBG	日志、VAP、SSID、流量诊断功能	反复创建VAP业务、业务数据量大	调整日志记录级别
WMT_WPM	处理AP上报性能统计数据	开启性能统计数据上报esight网管，采集的性能数据较多	调整PM性能采集周期
WMT_IDS	负责无线入侵检测： <ul style="list-style-type: none">- 探测表项合法性判断，探测表项映射关系处理及反制表项的生成- 攻击检测表项生成，攻击告警上报	探测AP多，探测的设备多或上报的周期短	一般不会出现CPU高的情况

任务名称	任务描述	该任务导致CPU占用率高的原因	解决措施
WMT_SEC	用户管理： <ul style="list-style-type: none"> - 用户上下线、漫游处理 - 用户密钥协商流程处理 	用户并发量大，漫游大并发（大于20个/秒的接入或者漫游量）	该任务在用户并发大于20个/秒时会出现占用15%左右的情况，用来处理用户的接入、认证、漫游等。超过该规格时需要进行扩容。
WMT_SRV	WLAN组件任务，配置下发与数据批量备份： <ul style="list-style-type: none"> - 配置下发消息处理（MAP、定时器消息） - 处理CAPWAP分发的消息 - 维护配置下发模块状态变迁 - WESS、WQOS、WGLB任务初始化 - 射频模块收到其他模块的模块间消息处理 - WVAP主动上报消息处理 - 射频定位信息上报处理 - HSB事件通知及HSB报文接收处理 - 通知外部模块AP状态发生改变 	<ul style="list-style-type: none"> - AP批量上线时配置下发 - 双链路热备或VRRP备份时，主备之间数据备份 - 链路震荡时，触发的HSB频繁抖动，引入的批删批量备份处理 - 定时备份 	一般不会出现CPU高的情况

任务名称	任务描述	该任务导致CPU占用率高的原因	解决措施
WMT_DEV	设备管理任务，主要负责： <ul style="list-style-type: none"> - AP定时check - ap-ping处理 - 漫游组定时同步消息 - MAP消息处理 - 处理CAPWAP分发的消息 - DEV本模块消息处理 - 处理AP上线时的状态变迁，维护状态机（含升级处理）AP批量上下线、AP升级、射频周期上报的采集信息 	AP批量上下线、升级、射频调优，终端定位时，并发处理大量来自AP的消息，会导致该任务占用CPU高	配置空口扫描周期为较大值，排查AP是否频繁掉线
WMT_SYS	WLAN组件系统管理任务	WLAN组件系统管理任务 AP性能数据统计、WMNG模块间消息处理	如果周期性升高，无需处理，如果持续性升高，需采集日志
CWP_BUP	MAP消息处理	MAP消息处理和MAP定时器处理，一般情况不会出现CPU高	降低业务并发、进行扩容或者更换高性能设备
CWP_DTLS	DTLS加密处理任务	创建/关闭DTLS链路，DTLS协商，AP批量DTLS建链时可能出现CPU高	AP通过DTLS上线，使用场景少，一般不会出现。如果出现可以评估网络具体情况，关闭DTLS
CWP_CWP	CAPWAP业务分发任务，CAPWAP报文接收分发	消息队列维护，报文分发、统计，CAPWAP定时器处理（重传、分片、重组、状态机），报文量大时，持续性打流，攻击时会出现	降低业务并发、进行扩容或者更换高性能设备
CWP_FWD	CAPWAP socket创建，socket报文收发，快速收发包	CAPWAP控制报文业务量大时，持续性打流，或者遭遇CAPWAP攻击等	用户量大并发的情况下(大于20个/秒接入)该任务在15%以内属于正常，只能通过扩容解决

任务名称	任务描述	该任务导致CPU占用率高的原因	解决措施
WLAN_NSTRANS	服务场所信息配置与上报	设备会向公共场所无线上网安全后台管理系统的服务器，定时自动上报一次场所、设备、AP状态等信息。上报数据量较大时可能会导致CPU高	关闭或减少上报数据量
WLAN_NS	服务场所信息配置与上报	设备会向公共场所无线上网安全后台管理系统的服务器，定时自动上报一次场所、设备、AP状态等信息。上报数据量较大时可能会导致CPU高	关闭或减少上报数据量
WLAN_SHELL	热备相关消息、数据处理	热备操作频繁	检查热备链路是否存在震荡
AGENT_CAPWAP/AGENT_WLAN	主副核Agent消息通信	主副核之间存在大量Agent消息通信	找到Agent消息的来源，比如大量网管Mib查询、备份、批量AP/用户上下线等。然后针对不同业务降低其触发频率
HTPSRD	Portal报文处理任务	大量的Portal认证HTTP报文上送处理	<ul style="list-style-type: none"> - 减少认证用户 - 对上送CPU的HTTP报文进行限速，检查是否有外部攻击、网络环路等情况引起HTTP报文过多
STA_TRACE_TASK	处理station trace诊断功能的任务	开启station trace功能	关闭station trace功能
STP	实现STP协议栈，管理协议状态机，维护协议相关的数据库	部署协议之后，有错误连线，收到TC报文攻击	检查配置，需要配置TC抑制
WADP	WLAN适配层任务	大量AP上下线、大量AP接入端口变化、大量无线用户并发上下线等情况可能会导致该任务对应的CPU占用率升高	网络承载能力有限，可能需要考虑重新规划网络，限制并发上线数量

任务名称	任务描述	该任务导致CPU占用率高的原因	解决措施
PTAL	Portal认证任务	大量的Portal认证HTTP报文上送处理	<ul style="list-style-type: none"> - 减少认证用户 - 对上送CPU的HTTP报文进行限速，检查是否有外部攻击、网络环路等情况引起HTTP报文过多
HTPD	内置Portal处理任务	大量的Portal认证HTTP报文上送处理	<ul style="list-style-type: none"> - 减少认证用户 - 对上送CPU的HTTP报文进行限速，检查是否有外部攻击、网络环路等情况引起HTTP报文过多
EAP	MAC和DOT1X认证协议处理任务	大量MAC和DOT1X用户进行认证	减少认证用户
UCM	认证用户管理任务	大量用户上线	减少认证用户
UTSK	用户框架处理任务，用于优化协议栈的处理，保证协议处理的优先级	任务功能是设备注册时负责注册UTASK命令行，创建定时器，设备注册后这个任务不处理消息，不会导致CPU高	不会导致CPU高，无需处理
NTPT	提供NTP时钟同步功能	收到大量的NTP协议报文攻击	配置NTP认证
POE	以太网供电任务，包括检测PD在位、分级状态、上下电策略等	不会触发CPU占用率高	无需处理
ACL	访问控制列表	一次下发的ACL过多	配置ACL的时间间隔为更长间隔
bcmDPC	芯片失效，中断上报任务	单板存在不可修复软失效表项且未中断抑制	升级补丁、重启设备
bcmL2MOD.0	芯片2 MAC表项学习任务	存在MAC漂移或HASH冲突	<ul style="list-style-type: none"> - MAC漂移：采取破坏措施 - HASH冲突：更改VLAN或更换单板

任务名称	任务描述	该任务导致CPU占用率高的原因	解决措施
bmLINK.0	芯片0 linkscan任务，扫描端口状态，变化时通知应用模块处理	Link中断上报过多或者miim访问耗时。Link中断由光模块LOS中断产生，非认证光模块以及光模块故障都会产生过多的异常中断（一般非标准光模块会引起此类情况）	更换华为标准光模块
bcmTX	CPU发包任务	发送报文过多	无需处理
bcmINTR	内核中断处理函数	内核中断上报过多	无需处理
bcmCNTR.0	芯片0流量统计	-	无需处理
DEFD	cpu-defend事件任务处理	上送CPU的报文过多	对上送CPU的报文进行限速
RDS	Radius协议处理任务	大量的Radius报文上送处理	减少认证用户 对上送CPU的Radius报文进行限速，检查是否有外部攻击、网络环路等情况引起Radius报文过多
RMON	远程系统监控	不会触发CPU占用率高	无需处理
GRSA/RSA	RSA任务，进行RSA、DSA密钥对创建	不会触发CPU占用率高	无需处理
APP	负责三层业务任务统一调度	当业务发送的消息多，多任务处理耗时，会导致CPU高	可以通过命令行display utask-info utask-id slice-time，查看具体是哪个UTASK任务运行耗时
HSB	HSB备份业务	不会触发CPU占用率高	-
SNPG	二层组播协议栈任务，处理二层组播协议收发包，以及二层组播表项下发	<ul style="list-style-type: none"> - 设备上收到大量二层组播协议报文 - 由于环网或者端口震荡，二层组播表项反复刷新 	检查是否存在大量二层组播攻击报文 检查是否存在环网或者端口震荡的情况
VRPT	定时器测试任务系统启动过程中的临时任务，系统启动后该任务停止运行	不会触发CPU占用率高	无需处理

任务名称	任务描述	该任务导致CPU占用率高的原因	解决措施
VRRP	实现VRRP协议栈，管理协议状态机，维护协议相关的数据库	配置大规格VRRP且接口状态震荡	出现机率小，如出现时可以将VRRP所在接口shutdown，避免震荡
WEB	WEB认证业务	大量的Portal认证报文上送处理	对上送CPU的Portal报文进行限速，检查是否有外部攻击、网络环路等情况引起Portal报文过多
BOX_Out	输出黑盒子中存储的信息（黑盒子用于记录产品运行过程中出现的错误、异常等信息）。 黑盒子只提供一种信息记录、查询、获取的机制，需要用户根据黑匣子提供的功能来实现具体信息的记录。	产品设备出现大量的error、断言、异常或deadloop等黑匣子信息	无需处理
FECD	FECD层的消息处理的任务	诊断信息打印过于频繁	无需处理
Printu	处理内核printu打印信息	不会触发CPU占用率高	无需处理
LBS	终端定位和频谱分析任务，终端定位功能，非WIFI设备的频谱分析	扫描时间间隔较小、射频环境复杂	适当增加空口扫描周期，调整空口扫描周期至合理值（根据实际情况，权衡定位精度和CPU任务占用率）
VCLK	用于唤醒TICK任务的时钟任务	-	无需处理
TICK	定时器处理任务	-	无需处理
MIMC	设备内部用户态与内核态通信机制	-	无需处理
SECE	实现ARP安全、IP安全以及CPU安全等功能，管理协议状态机，维护协议相关的数据库信息	大量协议报文上送CPU	合理配置协议报文限速，并部署适当的防攻击功能

任务名称	任务描述	该任务导致CPU占用率高的原因	解决措施
AAA	用户认证、授权、计费管理任务	大量用户进行认证、授权、计费操作	减少上线用户
AM	负责地址池以及地址的管理，为DHCP等模块提供地址管理服务	大量业务进行地址申请	减少申请地址的用户
BFD	实现双向链路检测（BFD）协议栈，管理协议状态机，维护协议相关的数据库	-	-
BFDA	BFD适配任务，处理IPC消息和ARP，MAC变化消息	-	-
BTRC	trace内部调试功能任务	开启了trace功能	关闭trace功能
COMT	提交ACL配置到AP的任务	大量AP并发上线	合理规划网络，避免大量AP并发上线
CSPF	CSPF任务处理，为TE隧道提供路径计算服务	CSPF的TEDB频繁变化	排查是否存在链路或者IGP震荡
EFMT	发送802.3ah的测试报文	-	无需处理
FCAT	获取报文任务	获取报文过多，打印过于频繁	无需处理
GRES	标签、Token资源管理模块对应的任务	不会触发CPU占用率高	无需处理
IFLP	管理接口流量定时统计	大量接口，且配置的统计周期过小	无需处理
IFNT	负责接口状态变化事件的处理	接口频繁震荡	无需处理
IFPD	提供接口管理功能，维护设备的接口数据库，处理各种接口状态变化事件	在接口数量较多、接口link状态震荡、光模块异常等情况下可能会导致该任务对应的CPU占用率升高	无需处理

任务名称	任务描述	该任务导致CPU占用率高的原因	解决措施
ITSK	发送、接收及分发各种协议报文	协议报文收发量高	无需处理
L2	负责二层业务任务统一调度，支持MGR、ErrorDown、BPTNL、LNP、VCMP、MFLP、VLAN、QinQ特性	<ul style="list-style-type: none">- LNP：接口较多- VCMP：VLAN删除创建频繁- BPTNL：透传报文数量较大	<ul style="list-style-type: none">- LNP：出现机率小，检查接口震荡原因，避免反复震荡- VCMP：不要频繁创建删除VLAN- BPTNL：接口上配置协议透传功能
L2_P	支持LACP、HGMP、3AH、ELMI特性	-	-
L2_R	支持ERPS、RRPP、SEP特性	部署协议之后，有错误连线，收到TC报文攻击	检查物理环路，确保物理环路闭合
L2IF	处理MAC与VLAN的实时备份和批量备份	-	-
LLDP	LLDP邻居发现协议的报文收发和处理	设备上LLDP邻居太多，导致收到LLDP协议报文比较多	减少设备上的LLDP邻居
LINK	负责链路层任务统一调度	当业务发送的消息多，多任务处理耗时，会导致CPU高	无需处理
PARITY_CHECK	表项软失效检测任务	表项出现软失效	-
QOS	QoS业务处理任务	QoS的消息过多	减少QoS的相关配置
SAM	处理认证表项下发接口板的任务	大量用户上线	减少认证用户
SAPP	负责应用层协议字典以及白名单管理，维护软件表项并通知适配层设置芯片状态	不会触发CPU占用率高	无需处理
SPM	节能功能管理任务	不会触发CPU占用率高	无需处理
TARP	提供ARP-Ping检测功能频繁	手动执行ARP-Ping检测	降低ARP Ping检测频率

任务名称	任务描述	该任务导致CPU占用率高的原因	解决措施
TM	认证表项分发任务	大量用户上线	减少认证用户
TNLM	隧道管理任务	一般由隧道震荡导致	建议分析震荡的隧道，屏蔽震荡源
TNQA	提供NQA客户端功能	NQA测试例配置过多，执行周期过短	控制NQA规格，或者调长执行周期
TRUN	Eth-Trunk适配层任务，处理Eth-Trunk接口各种状态变化事件，处理LACP协议报文	Eth-Trunk接口数量较多、接口状态震荡、光模块异常等情况下可能会导致该任务对应的CPU占用率升高	排查端口和光模块是否异常：通过输出日志或告警查看设备上是否存在端口频繁Up/Down的情况，如果存在，请检查端口上光模块是否发生故障，是否使用了华为非认证光模块。同时需要对端口配置和端口流量
TUNL	处理TUNNEL模块的控制和配置消息	配置大量隧道使用相同源接口并诊断源接口状态或配置，或者在大量GRE Tunnel口上配置keepalive	出现机率小，避免配置过大规格的GRE keepalive

3. FAT模式AP打开WEB页面慢，CPU使用高，可通过如下方法修改加密套件。

```
<HUAWEI> system-view
[HUAWEI] undo http secure-server ssl-policy
[HUAWEI] ssl policy default_policy type server
[HUAWEI-ssl-policy-default_policy] undo ciphersuite
[HUAWEI-ssl-policy-default_policy] ciphersuite rsa_3des_cbc_sha rsa_aes_128_sha256
rsa_aes_128_cbc_sha rsa_aes_256_sha256
[HUAWEI-ssl-policy-default_policy] quit
[HUAWEI] http secure-server ssl-policy default_policy
```

步骤3 收集信息

一键诊断信息，包含CPU高的时间段的设备日志文件和诊断日志文件。

----结束

9.3 供电异常

步骤1 配置强制供电模式

AirEngine系列AP可通过配置强制供电模式使AP工作在期望供电模式下，适用于对接PoE适配器或PoE交换机的场景，需确保PoE交换机支持对应的供电协议，且供电总功率满足给接口下的所有AP供电。

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name default
[HUAWEI-wlan-ap-system-prof-default] power force work-mode bt60
```

Warning: If the PSE does not reach the target power supply level, executing this command may cause the AP to repeatedly restart due to insufficient power. Continue? [Y/N]: y

步骤2 确保通过LLDP协商方式进行供电协议协商

登录到AP，执行命令**display current power-workmode**，查看AP当前工作的功率模式。

```
<HUAWEI> display current power-workmode  
Current power workmode is BT60 (Normal), decided by LLDP
```

缺省情况下，AP默认使用LLDP协商方式。如果不是通过LLDP协商进行PoE供电，则需要确认对端PoE交换机是否打开LLDP功能。

步骤3 采集LLDP诊断信息进一步分析

采集LLDP诊断信息，或通过镜像报文捕获方式捕获LLDP报文分析PoE供电和受电双方的LLDP协商过程，分析异常原因。

```
<HUAWEI> debugging lldp all all  
<HUAWEI> t d  
<HUAWEI> t m
```

采集或捕获报文的时间应达到3分钟以上。

----结束

10 故障处理：无线桥接类问题

10.1 Mesh组网中MP上线失败

10.1 Mesh 组网中 MP 上线失败

步骤1 检查根节点MPP是否上线

Mesh组网中，根节点MPP必须先上线，叶子节点MP才能进行桥接上线。

执行命令**display ap all**，查看MPP是否上线，以查看MAC地址为845b-1275-18c0的MPP为例。

```
[AC-wlan-view] display ap all | include 845b-1275-18c0
Info: This operation may take a few seconds. Please wait for a moment.done.
```

Total AP information:

fault: fault [2]

idle : idle [12]

nor : normal [3]

ID	MAC	Name	Group	IP	Type	State	STA	Uptime
11	845b-1275-18c0	mpp2	default	5.1.1.252	AirEnginexxxxS	nor	0	5M:34S
.....								

Total: 17

MPP上线和普通AP上线一样，如果发现MPP不能上线，可参考[3.1 AP在AC上无法上线的定位方法](#)。

步骤2 检查是否离线添加叶子节点MP

Mesh组网中，MP通过无线接入网络，在AC上线时需要预先离线添加MP。

执行命令**display ap all**，查看MP是否上线，以查看MAC地址为845b-1275-20c0的MP为例。

```
[AC-wlan-view] display ap all | include 845b-1275-20c0
Info: This operation may take a few seconds. Please wait for a moment.done.
```

Total AP information:

fault: fault [2]

idle : idle [12]

nor : normal [3]

ID	MAC	Name	Group	IP	Type	State	STA	Uptime
----	-----	------	-------	----	------	-------	-----	--------

```
11 845b-1275-20c0 mp2 default 5.1.1.252 AirEnginexxxS nor 0 5M:345
.....
Total: 17
```

如果没有离线添加MP，请在WLAN视图下执行命令**ap-id ap-id ap-mac ap-mac ap-sn ap-sn**手动添加。

步骤3 检查AP对接款型是否正确

在V200R020C10及之前版本，在Mesh组网中，仅支持相同协议类型芯片的射频之间建立链路。例如，802.11ac芯片的AP射频只能和使用了802.11ac芯片的邻居射频对接，不支持和非802.11ac芯片的邻居射频对接。从V200R021C00版本开始，除了支持相同协议类型芯片的射频之间建立Mesh链路外，还支持使用了802.11ax和802.11ac芯片的射频之间建立Mesh链路。例如，AirEngine 6760-51EI支持与AP8150DN建立Mesh链路。V200R020C00版本的AP不支持与V200R020C00之前版本的AP对接；但其中V200R020C00版本的云AP还可以和V200R019C00版本的云AP2051DN对接。

如果出现不能对接的款型，请选择正确的款型进行Mesh建链。

步骤4 检查是否建立Mesh链路

1. 在AC上查看Mesh型VAP的相关信息。

```
<HUAWEI> display mesh vap all
WID : WLAN ID
```

AP ID	AP name	Rfid	WID	Mesh ID	BSSID	Auth type	Mesh links
1	AP2	0	16	mesh	00E0-FC74-964F	WPA2-PSK	0
0	AP1	0	16	mesh	00E0-FC74-964F	Open	0

Total: 2

2. 在AC上查看Mesh链路信息。

```
[AC-wlan-view] display wlan mesh link all
Info: Mesh link does not exist.
```

如果使用5G进行桥接，且配置的是雷达信道，Mesh上线可能会慢些，需要多次查询此命令，查看Mesh是否建立链路或则链路是否稳定。

3. 在MPP上查看Mesh链路信息、Mesh建链和断链记录。

V200R019C00及之前版本：

```
<AP> system-view
[AP] diagnose
[AP-diagnose] display wsrp mesh-link-info
radio_0 mesh link info as follow:
```

Peer MAC state	Peer name	Link ID	Channel	Current RSSI(dBm)	Fwd ifIndex	Fwd
----	-----	-----	-----	-----	-----	-----
----	-----	-----	-----	-----	-----	-----

radio_1 mesh link info as follow:

Peer MAC state	Peer name	Link ID	Channel	Current RSSI(dBm)	Fwd ifIndex	Fwd
----	-----	-----	-----	-----	-----	-----
0012-1c67-080f	123	0	157	-56	21	send and receive

```
[AP-diagnose] display wsrp mesh-link-record
```

```
-----
Radio ID  Peer Radio MAC  Time
Action
-----
1          4CFA-CAC1-845F  2017-05-19/16:19:49  delete link (peer VAP
down)
1          4CFA-CAC1-845F  2017-05-19/16:19:02  create
link
-----
Total:2
```

V200R019C10及之后版本：

```
<AP> system-view
[AP] diagnose
[AP-diagnose] display umac mesh link-info
radio_0 mesh link info as follow:
-----
Peer MAC      Link ID  Channel  Current RSSI(dBm)
-----
radio_1 mesh link info as follow:
-----
Peer MAC      Link ID  Channel  Current RSSI(dBm)
-----
00e0-fc67-080f  123     157      -56
-----
[AP-diagnose] display umac mesh link-record
-----
RadioID PeerMac      Time          Action
-----
1        4CFA-CAC1-845F  2017-05-19/16:19:49  delete link (peer VAP down)
1        4CFA-CAC1-845F  2017-05-19/16:19:02  create link
-----
Total:2
```

步骤5 查看AP侧是否获取到对端AP的邻居信息

如果AC上配置、天线都无问题，网络中可以登录到MP的话，可以在MP上查看是否获取到对端AP的邻居信息及链路信息。

1. 查看MP上是否创建Mesh VAP信息。

V200R019C00及之前版本：

```
[mp-diagnose] iwconfig radio 1 vap 15
IEEE802.11ac ESSID:"mesh-net"
Mode:Master Frequency=5.785 GHz Access Point: D0:D0:4B:22:DE:8F
Bit Rate:540 Mb/s Tx-Power=25 dBm
RTS thr=2001 B Fragment thr:off
Encryption key:***** [2] Security mode:open
Power Management:off
Link Quality=--/-- Signal level=-- Noise level=--
Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:--
Tx excessive retries:-- Invalid misc:-- Missed beacon:--
```

V200R019C10及之后版本：

```
[mp-diagnose] display umac dot11 vap-obj radio 1 vap 15
VAP ID          : 15
BSSID           : e483-2623-5041
SSID            : carlos_psk
SSID hide       : 0
DTIM period     : 1
STA num         : 0
BSS Load switch : 0
UAPSD switch    : 0
EDCA param count : 1
VHT info:
```

```
SU Beamformer : 1
MU Beamformer : 1
TX MCS MAP   : 0xFFAA
RX MCS MAP   : 0xFFAA
HE info:
  UL OFDMA    : 0
  DL OFDMA    : 0
  Partial MU MIMO : 0
  ER SU       : 1
  TX MCS MAP   : 0xFFAA
  RX MCS MAP   : 0xFFAA
```

[mp-diagnose]dis umac mesh config
radio_0 mesh config as follow:

```
-----
Mesh switch      : Off
Mesh role        : -
Mesh id          : -
Mesh max link num : -
Mesh rssi threshold(dBm) : -
Mesh report interval(s) : -
Mesh link aging time(s) : -
Mesh whitelist num : 0
-----
```

radio_1 mesh config as follow:

```
-----
Mesh switch      : Off
Mesh role        : -
Mesh id          : -
Mesh max link num : -
Mesh rssi threshold(dBm) : -
Mesh report interval(s) : -
Mesh link aging time(s) : -
Mesh whitelist num : 0
-----
```

2. 查看AP上是否扫描到邻居信息。

V200R019C00及之前版本：

```
[mp-diagnose] display wifi mesh-neighbor radio 1
MESH neighbor list:1
=====
0      845b-1275-18c0
=====
[mp-diagnose] display wifi mesh-neighbor radio 1 peer-mac 845b-1275-18c0
MESH neighbor info
=====
MESH neighbor MAC : 845b-1275-18c0
Time to live      : 40
Same channel      : TRUE
Radio number      : 2
Online            : 1
Position number   : 0
Update time       : 2018/02/26 20:30:24

-----Radio 0-----
-----Radio 1-----
Radio MAC         : 845b-1275-18df
Role              : MPP
MESH enable       : TRUE
MESH ID           : mesh-net
Channel           : 157
RSSI              : -17
Key failure times : 0
Last PN RSSI      : -95 -95 -95 -95 -95 -95 -95 -95 -95
PN check result   : 0
PN check failure times : 0
MPP MAC          : 845b-1275-18c0
```

```
MPP path RSSI      : -17
Hop count          : 1
Is link full       : 0
=====
```

V200R019C10及之后版本：

```
[mp-diagnose] display umac mesh neighbor radio 1
MESH neighbor list:1
=====
0      60d7-55b5-3c00
=====
[mp-diagnose] display umac mesh neighbor radio 1 peer-mac 60d7-55b5-3c00
MESH neighbor info
=====
Neighbor MAC      : 60d7-55b5-3c00
Time to live      : 40
Same channel      : true
=====
[mp-diagnose] display umac mesh neighbor-info
F: Is link full
=====
Neighbour MAC  MPP MAC      RadioID Channel HopCount RSSI F
=====
60d7-55b5-3c00 00e0-fc74-9640 1      157      1      -33  0
=====
Total: 1
```

如果有邻居信息，但是不能建立链路，可以看下邻居表中对端AP的RSSI是否过小，如果RSSI较小，可以尝试降低建链阈值，让其进行建立链路。

根据绑定的Mesh模板，配置建链阈值。

```
[AC-wlan-view] mesh-profile name mesh
[AC-wlan-mesh-prof-mesh] link-rssi-threshold -80
Warning: This action may cause service interruption. Continue?[Y/N]Y
```

如果是AirEngine系列Wi-Fi6 AP之间组建Mesh链路，可尝试将射频类型修改为802.11ac模式，以降低建链灵敏度。

```
<AC> system-view
[AC] wlan
[AC-wlan-view] radio-5g-profile name default
[AC-wlan-radio-5g-prof-default] radio-type dot11ac
```

步骤6 检查硬件天线是否有问题

1. 查看天线型号是否正确，天线2.4G/5G选择是否正确，型号是否匹配。
2. 天线安装，查看天线安装是否良好，馈线安装是否正确。
3. 天线对准，检查天线是否对准。
4. 如果外置天线不是满配安装（天线口没有插满），或AP供电状态显示为降档状态时，则需根据产品文档硬件安装与维护指南确认天线是否按照要求正确安装。例如，AirEngine 6760R-51E如未配满天线，请按射频口D~A的优先顺序依次连接天线，在供电标准为802.3at的情况下，请使用射频口C和D连接天线。各个不同款型的室外AP天线安装要求，请参考产品文档说明按要求进行安装。

步骤7 检查信号强度配置是否合理

检查MPP功率配置是否合理。

```
[AC-wlan-view] display radio ap-id 11
CH/BW:Channel/Bandwidth
CE:Current EIRP (dBm)
ME:Max EIRP (dBm)
CU:Channel utilization
ST:Status
=====
AP ID Name RfID Band Type  ST CH/BW      CE/ME STA  CU
=====
```

```
11 mpp2 0 2.4G bgn on 6/20M 9/29 0 -
11 mpp2 1 5G an11ac on 157/40M+ 30/30 0 -
-----
Total:2
```

如果MPP的功率配置不是最大功率值，请配置为最大功率值。

```
[AC-wlan-view] ap-id 11
[AC-wlan-ap-11] radio 1
[AC-wlan-radio-11/1] eirp 127
Info: The EIRP value takes effect only when automatic transmit power selection is disabled, and the value
depends on the AP specifications and local laws and regulations.
[AC-wlan-radio-11/1] display this
#
 mesh-profile mesh
 mesh-whitelist-profile mesh
 channel 40mhz-plus 157
 eirp 127
 coverage distance 6
#
return
```

如果配置最大功率后，还是不能建链，对于室外型AP，请排查AP的天线安装是否正确，比如天线接口是否旋紧、天线接口位置是否正确等等。

同时检查天线是否对准，请参考[企业WLAN场景化设计（回传）](#)中的天线对准方法。

步骤8 检查距离参数配置是否合理

查看射频覆盖距离参数。

```
<AC> display ap config-info ap-id 1
Radio 0
.....
Coverage distance(100 m) : 3
.....
Radio 1
.....
Coverage distance(100 m) : 3
.....
```

如果发现配置的距离参数不合理，比如MPP与MP的实际距离为600m，而距离参数配置为300m，这时就需要修改距离参数为600m。距离参数修改方法如下：

```
[AC-wlan-view] ap-id 25
[AC-wlan-ap-25] radio 1
[AC-wlan-radio-25/1] coverage distance 6
```

说明

- 距离参数配置的值单位是100m，比如配置值是5，实际上配置的值是500m。
- 距离参数MPP和MP都需要配置。

步骤9 如上述步骤仍然无法解决问题，请收集AC的一键诊断信息及对应时间段的用户日志、诊断日志，并联系技术支持人员。

----结束

11

故障处理：CampusInsight 对接问题

11.1 CampusInsight上不显示性能上报数据

11.1 CampusInsight 上不显示性能上报数据

步骤1 检查WMI配置情况

1. 执行命令**display wmi status**，查看WMI的配置状态。

```
<HUAWEI> display wmi status
Config status
Server                : 10.1.1.1:10032
Backup server         : 10.1.1.2:10032
Current used          : 10.1.1.1:10032
Source interface      : Vlanif 100
Max packet size       : 5120Bytes
Report interval       : 60s
Connection            : heartbeat 3min; retry interval 5min; retry count 0.
Statistics info
Send Success(packets/bytes) : 0/0
Send Fail(packets/bytes)    : 0/0
Receive Success(packets/bytes): 0/0
Receive Fail(packets/bytes) : 0/0
```

Data-Type	Switch	Interval(s)	Trigger	Records	Direction
device-data	Enable	10	1	1	Send
interface-data	Enable	60	0	0	Send
log-data	Enable	300	47	0	Send
security-data	Enable	300	47	0	Send
application-statistics-data	Enable	300	0	0	Send
cpcar-data	Enable	300	0	0	Send
s-ipfpm-data	Enable	-	1612	65437	Send
topology-info	Enable	-	0	0	Receive
group-info	Enable	-	0	0	Receive
load-info	Enable	-	0	0	Receive
rogue-interference	Enable	-	0	0	Receive
edge-ap	Enable	-	0	0	Receive
analysis-result-request	Enable	-	46	46	Send
calibrate-result-report	Enable	-	6	7	Send
deteriorated-ap	Enable	-	0	0	Receive
sta-profile-data-request	Enable	-	4	4	Send
sta-profile-data-response	Enable	-	0	0	Receive

Info: Server2 has not been configured.

2. 确认相关数据项上报开关“Switch”是否已设置为开启状态“Enable”。若未开启，则需要在wmi-server模板中进行相应的配置。下面以配置上报**device-data**为例。

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wmi-server name abc
[HUAWEI-wlan-wmi-server-prof-abc] collect-item device-data interval 500
```
3. 确认相关数据项的收发数据计数“Records”是否为0。若计数为0，则推断相关功能模块未开启，需先开启相关功能模块。
4. 确认发送成功数据计数“Send Success”是否增加，若计数不增加或“Send Fail”计数增加，则需检查AC或AP到CampusInsight服务器的联通性。

步骤2 查看http2-client状态

执行命令**display http2-client { item *app-type* | variable | statistics [*app-type*] }**，查看HTTP 2.0的相关信息。

```
[HUAWEI-diagnose] display http2-client item 2
```

```
.....
usAppType = 2
ucConnStatus = 3 , CONN_UP
ucIfInitRetry = 1
.....
```

“ucConnStatus”描述HTTP通道连接状态。“ucConnStatus = 3”表示通道为连接状态，说明http2通道正常；否则，需检查AC/AP到CampusInsight服务器的联通性，并通过以下命令采集更多信息。

```
<HUAWEI> debugging http2-client all all
<HUAWEI> debugging syslog all all
<HUAWEI> debugging ssl all all
<HUAWEI> t d
<HUAWEI> t m
```

----结束

12 故障处理：云管理类问题

12.1 云AC/云AP无法上线

12.1 云 AC/云 AP 无法上线

步骤1 检查基本配置

1. 检查控制器是否已经添加设备。

站点:

模式:

* 设备信息:

类型: 型号:

数量: 角色:

2. 检查设备当前的运行模式是否是云模式。
登录设备后，会有信息提示当前设备的运行模式，如果是非云模式，则需要切换为云模式。
3. 执行命令**display cloud-mng info**查看设备上的iMaster NCE-Campus配置信息。

```
<Huawei> display cloud-mng info
-----
AP status           : Online
Controller URL       : -
Controller IP address : 10.1.1.1
Controller port      : 10020
Controller address source: configuration
-----
```
4. 执行命令**display cloud-mng register-center status**查看注册中心的状态信息。

```
<Huawei> display cloud-mng register-center status
-----
Register center URL : register.naas.huawei.com
Register center IP   : -
Register center port : 10020
Current status       : sleeping
-----
```

如果配置信息不正确，请按如下方式重新配置。

配置云AP/云AC上线需要获得iMaster NCE-Campus的IP地址/URL信息。

- 通过DHCP方式获取

设备通过DHCP请求获取iMaster NCE-Campus的IP地址时，DHCP Server回应的DHCP报文中携带iMaster NCE-Campus的IP地址/URL信息option 148字段，AP会通过iMaster NCE-Campus信息主动向iMaster NCE-Campus注册。

- 通过命令行方式获取

```
<Huawei> system-view  
[Huawei] cloud-mng controller ip-address 10.1.1.1 port 10020
```

- 通过注册中心获取

当设备无法通过DHCP方式和手动方式获取iMaster NCE-Campus地址，设备也会主动向注册中心发送查询报文，获取iMaster NCE-Campus地址。此时，设备不需要满足空配置和串口无输入两个条件。

设备通过iMaster NCE-Campus的IP地址直接进行注册或者通过解析出iMaster NCE-Campus的IP地址进行注册，如果在设备上通过命令行同时配置了二者，新配置会覆盖旧配置。

更具体的内容请参考：[云管理配置（AP）](#)和[云管理配置（AC）](#)。

步骤2 检查设备和云管理平台之间的网络连通性

1. 查看设备Ethernet0/0/47接口是否UP且有正确的IP地址。

```
#  
interface Ethernet0/0/47  
ip address 169.254.3.1 255.255.255.0  
#
```

2. 双向ping包检查是否能够ping通。

```
<Huawei> ping -c 1000 10.1.1.1  
PING 10.1.1.1: 56 data bytes, press CTRL_C to break  
Reply from 10.1.1.1: bytes=56 Sequence=1 ttl=128 time=3 ms  
Reply from 10.1.1.1: bytes=56 Sequence=2 ttl=128 time=1 ms  
Reply from 10.1.1.1: bytes=56 Sequence=3 ttl=128 time=1 ms  
Reply from 10.1.1.1: bytes=56 Sequence=4 ttl=128 time=1 ms  
Reply from 10.1.1.1: bytes=56 Sequence=5 ttl=128 time=1 ms  
--- 10.1.1.1 ping statistics ---  
5 packet(s) transmitted  
5 packet(s) received  
0.00% packet loss  
round-trip min/avg/max = 1/1/3 ms
```

3. 双向ping指定大小的包检查能否ping通

```
<Huawei> ping -s 1500 10.1.1.1  
PING 10.1.1.1: 1500 data bytes, press CTRL_C to break  
Reply from 10.1.1.1: bytes=1500 Sequence=1 ttl=128 time=3 ms  
Reply from 10.1.1.1: bytes=1500 Sequence=2 ttl=128 time=1 ms  
Reply from 10.1.1.1: bytes=1500 Sequence=3 ttl=128 time=1 ms  
Reply from 10.1.1.1: bytes=1500 Sequence=4 ttl=128 time=1 ms  
Reply from 10.1.1.1: bytes=1500 Sequence=5 ttl=128 time=1 ms  
--- 10.1.1.1 ping statistics ---  
5 packet(s) transmitted  
5 packet(s) received  
0.00% packet loss  
round-trip min/avg/max = 1/1/3 ms
```

如果无法Ping通，请检查设备和云管理平台之间的网络，确保相互之间能够互通。

步骤3 在诊断视图下执行命令display cloud-mng online-fail-record，查看设备上线失败的原因，结合失败原因进行故障排查。

步骤4 参考云管理平台侧的排查步骤进行排查。

具体请参见：[设备上线失败（设备未注册）](#)。

步骤5 收集信息

1. 收集debug信息

```
<Huawei> terminal debugging
<Huawei> terminal monitor
<Huawei> debugging syslog
[Huawei-diagnose] terminal diag-logging
```

执行以上命令后，等待10分钟后将屏幕上打印的信息保存。

2. 收集设备与日志信息

设备信息

信息类别	命令视图	命令
版本信息	诊断视图	vrbd
补丁信息	所有视图	display patch-information
启动信息	所有视图	display startup
配置信息	所有视图	display current-configuration
文件系统信息	所有视图	dir flash:/

日志文件

导出日志文件：使用FTP方式或通过Web网管将flash:/logfile目录下包含问题发生时间的所有日志文件（.dblg/.log/.dblg.zip/.log.zip）导出。

----结束

13 联系华为技术支持

故障发生后，如果无法自行定位，请收集相关故障信息，并将其提交给代理商或华为技术有限公司进行定位和处理。

信息收集

在联系技术支持之前，请首先收集故障相关信息，主要包括：

- 发生故障的时间、故障点的网络拓扑结构、导致故障的操作、故障现象、故障后已采取的措施和结果、故障影响的业务范围等信息。
- 发生故障的设备的名称、版本、当前配置、接口信息等。
- 发生故障时产生的日志信息。

联系技术支持

企业用户请通过如下方式获取技术支持：

- 访问华为[企业业务智能问答客服系统](#)。
- 联系华为技术有限公司客户服务中心。
 - 客户服务电话：[全球售后服务热线](#)
 - 客户服务邮箱：support_e@huawei.com
- 访问[华为企业业务技术支持网站](#)，搜索故障案例或在技术论坛中发帖寻求帮助。

运营商用户请通过如下方式获取技术支持：

- 联系华为技术有限公司客户服务中心。
 - 客户服务电话：[全球服务热线](#)
 - 客户服务邮箱：support@huawei.com
- 访问[华为运营商技术支持网站](#)，搜索故障案例或在技术论坛中发帖寻求帮助。