3 Wi-Fi 6 校园无线网络部署最佳实践

关于本章

3.1 使用的产品和版本
3.2 校园WLAN网络方案概述
3.3 校园WLAN网络规划和推荐配置

3.1 使用的产品和版本

本文档基于WLAN V200R020版本写作，不同版本的操作界面和步骤可能存在差异，请根据现网实际版本酌情参考。

推荐使用V200R020最新版本和补丁的AC和AP部署网络，产品选型建议参考WLAN建网标准。

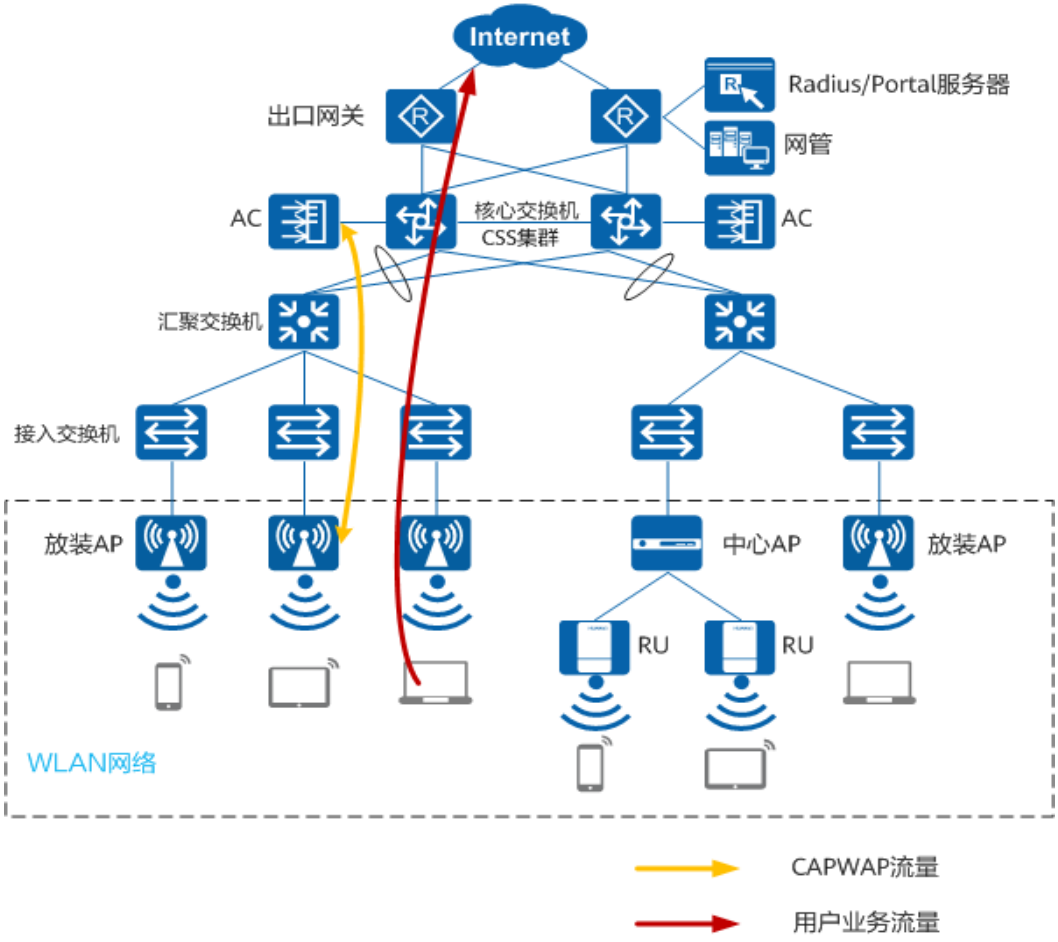
3.2 校园 WLAN 网络方案概述

校园网络的典型组网图如**图3-1**所示，其中：

- 园区网络的核心层采用2台华为框式交换机，组成CSS集群系统，构成网络的交换核心，保证承载业务的可靠性。对于距离不远的两个校区之间或者业务功能区分比较严格的网络之间，可以通过部署区域核心的方式进行区分，区域核心部署框式交换机堆叠，所有区域核心采用2条万兆光纤做聚合，双上联到无线网络总核心上，保证组网的层次性、便捷管理性。
- 园区网络的汇聚层，根据流量、用户规格采用不同性能的华为交换机，上联2条万兆光纤做聚合，提高链路的高可用性。
- 园区网络的接入层采用与AP供电模式匹配的交换机，连接各种款型AP，提供PoE供电及网络接入功能。
- 无线网络的管理推荐使用盒式的AC旁挂，提供AP管理以及用户接入；AC配置VRRP热备，提升可靠性；根据AP数量和用户规模，可以部署多台AC来提升AP管理能力和用户接入数量，AC之间建立漫游组以支持用户跨AC漫游。
- 计费授权控制根据管理用户规模、性能采用2台ME设备作热备，对用户进行计费授权，保证用户业务安全、可靠。

- 网络管理采用华为一体化CampusInsight，对多类型的设备进行统一的监控管理，并对网络和业务质量进行监视和分析，实现对企业资源、业务、用户的统一管理以及关联分析。

图 3-1 校园无线网络组网图



3.3 校园 WLAN 网络规划和推荐配置

3.3.1 AC 组网架构

根据AC在园区网络中部署位置不同，可分为AC旁挂式组网和AC直连式组网。两种组网方式的对比与选择建议如表1 所示，推荐采用旁挂式组网。

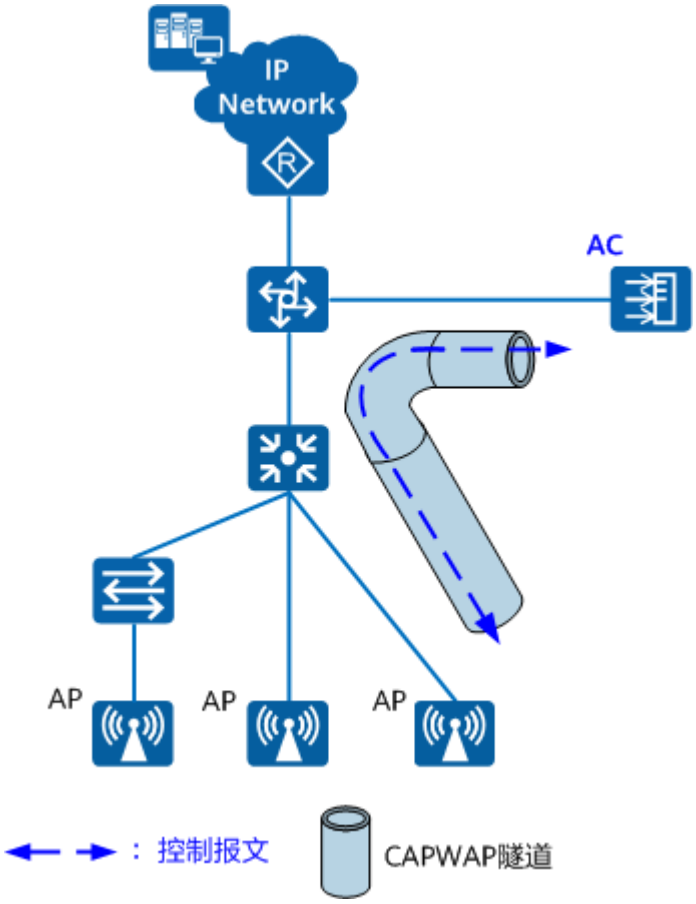
表 3-1 独立 AC 的组网类型对比

组网类型	适用场景	优点	缺点
直连式组网	• 单节点AC能够满足网络规模诉求，且未来网络规模也可预期满足。	• 网络结构简单，可同时提供AC与交换能力。	• 规模能力依赖单节点能力（如支持AP数量）。 • 扩容难度大。

组网类型	适用场景	优点	缺点
旁挂式组网	• AC只需要提供AP、终端与网络的管理功能。 • AC不需要处理业务流量时（例如本地转发）。 • 大规模网络（例如AP数量大于10K）。	• 新增WLAN网络时部署简单。 • 扩容简单。	当采用集中转发模式时，对交换机的带宽消耗大。

根据AC所管控的区域和吞吐量的不同，AC可以出现在汇聚层，也可以出现在核心层。考虑到可靠性问题，AC通常建议部署在核心层。AC旁挂组网拓扑如图3-2所示。

图 3-2 AC 旁挂组网



3.3.2 AP 管理

为了便于管理大量AP，通常对AP进行分组管理，以进行批量配置与升级等。

AP 组划分

当需要对多个AP进行同样的配置时，可以将AP都加入到同一个AP组，直接在AP组下进行配置，配置会对AP组下的AP生效，免除了对每个AP进行单独配置的繁琐操作。如

果不手动配置AP加入到指定AP组中，则AP会自动加入到名为**default**的缺省AP组中。当这些AP需要执行不同业务而需要下发不同的配置的时候，在一个AP组下就很难操作，因此，在AC上添加AP前，需要合理地划分AP组，以方便对AP进行更加精细化地管理。

从方便管理和配置的角度出发，建议将在同一物理区域的AP划分到一个AP组，例如同一楼层或者同一栋楼的AP划分到同一个AP组。一般情况下，同一物理区域的AP所承载的WLAN业务是相同的，所需进行的配置也是相同的，所以建议按照这种方式划分AP组。

AP 版本升级

为了减少AP版本升级过程对网络的影响，建议在网络业务处于非运行状态时，分批次对网络中的设备进行升级。

通过规划升级任务，可灵活的对网络进行升级，在线升级AP时，支持的升级方式包括：

- 基于单个AP的升级：对单个AP进行升级。
- 基于AP类型的升级：批量升级同一类型的AP。
- 基于AP组的升级：批量升级同一组的AP。
- 基于信道分组对AP升级：批量升级同一个信道分组的AP。这种升级方式也被称为“插花升级”，是将同一信道的AP划分到一个信道分组中，然后按信道分组依次重启升级。在信道分组重启过程中，周边AP会自动对覆盖区域进行补盲，保证网络业务不中断。

AP版本升级模式包括AC模式、FTP模式和SFTP模式。当需要对AP批量升级时，在确保网络安全的前提下，建议使用FTP模式进行升级；如果无法确保网络安全，则建议使用SFTP模式进行升级。在不需要进行批量升级时，建议将AP升级模式修改为AC模式。

在对AP版本进行升级时，建议先对单个AP进行升级测试，检查升级版本是否存在异常，然后再进行批量升级，保证后期的批量升级成功执行。批量升级时可以结合实际情况选择升级方式。例如，在针对某一楼层或某一栋楼的AP进行升级时，建议按照AP组进行批量升级。

推荐配置：

```
<AC> system-view
[AC] wlan
[AC-wlan-view] ap update mode ftp-mode  //配置AP升级模式
[AC-wlan-view] ap update ftp-server ip-address 192.168.1.100 ftp-username admin ftp-password cipher wlanadmin  //配置FTP服务器
[AC-wlan-view] ap update update-filename airenginex760-v200r019c10spc300.cc ap-type 133  //配置AP版本升级文件
[AC-wlan-view] ap-patch update update-filename AirEngineX760_V200R019C10SPH006.pat ap-type 133  //配置AP补丁文件
[AC-wlan-view] ap update load ap-id 1 update-filename airenginex760-v200r019c10spc300.cc  //对单个AP升级版本
[AC-wlan-view] ap update multi-load ap-group ap-group1  //对同一AP组下的AP批量升级
[AC-wlan-view] ap update multi-load ap-type 133  //对同一型号的AP批量升级
```

AP 设备管理

对于宿舍等场景，为了不影响用户休息，可以关闭AP指示灯，减少对用户的影响。

推荐配置：

```
[AC-wlan-view] ap-system-profile name ap-system1
[AC-wlan-ap-system-prof-ap-system1] led off
```

3.3.3 IP 地址规划

WLAN网络的IP地址规划主要包括：AC的IP地址规划，AP的IP地址规划和无线终端的IP地址规划。

网络中AC的数量较少，IP地址一般通过静态手工配置。

AP数量较多，配置工作量大，一般建议使用DHCP动态分配。如表3-2所示，一般可使用如下几种地址分配方式。

表 3-2 AP IP 地址分配方式

地址分配方式	地址分配说明	特点	应用场景
根据VLAN分配	AP相连交换机端口以Trunk方式加入VLAN，通过VLAN对应的地址池分配IP地址。	• AP与无线用户的IP地址分离。 • 网络配置工作量较大，不利于AP即插即用。	适用于对设备IP地址管理与用户IP地址管理要求隔离的场景。
根据MAC地址分配	在DHCP Server上配置AP的MAC以及对应的IP地址。	• AP与无线用户的IP地址分离。 • 配置工作量较大，IP地址管理难度加大。	适用于对少量AP设备管理有特殊要求的场景。
统一分配	AP地址分配和无线用户一样，统一分配，不再区别。	• 网络配置简单。 • AP设备地址和无线用户地址无法分开管理。	适用于对AP IP管理没有要求的场景。

AP的DHCP Server可以部署在AC上，也可以部署在交换机上。DHCP Server部署在交换机上时，交换机需要支持配置Option43携带AC的IP地址通告给AP，使AP能够发现AC。

对于无线终端，不同终端可采用不同的分配方式，包括：

- 普通移动终端，例如手机、便携机等，建议通过DHCP动态分配IP地址。
- 对外提供公共服务的无线终端（比如：无线打印机），建议静态配置。
- 哑终端，很多哑终端不支持通过DHCP动态获取IP地址，对于该类终端只能静态配置。

由于无线终端数量较多，建议规划独立的DHCP服务器，且一般是根据VLAN来进行地址分配。

3.3.4 业务数据转发模式

WLAN网络中的数据包括控制报文和数据报文。控制报文是通过CAPWAP的控制隧道转发的，用户的数据报文按照是否通过CAPWAP的数据隧道转发分为隧道转发（集中转发）方式和直接转发（本地转发）方式。

两种转发方式的对比和适用场景如表3-3所示，建议采用直接转发模式，由上层网络设备（如核心交换机）作为DHCP服务器给终端分配IP地址并配置用户网关。

表 3-3 转发模式说明

转发模式	适用场景	优点	缺点
隧道转发	● 适用于需要AC承担用户网关、用户策略管理、认证计费网关、DHCP服务器等角色的场景。 ● 用户业务数据由AC集中处理与转发。	AC集中转发数据报文，安全性好，方便集中管理和控制。	业务数据必须经过AC转发，报文转发效率低，AC所受压力大。
直接转发	● 适用于用户业务数据由本地网络直接转发的场景，节省AP与AC间链路带宽。 ● 用户网关和DHCP服务器均在本地网络中。	业务数据不需要经过AC转发，报文转发效率高，AC所受压力小。	业务数据不便于集中管理和控制。

推荐配置：

缺省情况下，VAP模板下的用户业务数据转发方式为直接转发，因此，建议采用缺省配置。

```
<AC> system-view
[AC] wlan
[AC-wlan-view] vap-profile name vap1
[AC-wlan-vap-prof-vap1] forward-mode direct-forward
Warning: This action may cause service interruption. Continue?[Y/N]y
```

3.3.5 VLAN

管理 VLAN 设计

设备管理VLAN主要用于对所有网络设备的管理，本方案为独立物理组网方式，为保证设备使用的安全、可靠，设备的管理、控制应与其他网络流量及无线接入客户流量分开，因此，需要为核心交换机、AC无线控制器、汇聚交换机、POE接入交换机及AP设备划分单独VLAN进行管理。

同时，由于AC与AP之间采用CAPWAP隧道发送管理报文，所以还需要规划单独的AP管理VLAN。

推荐配置：

```
<AC> system-view
[AC] vlan batch 100
[AC] interface vlanif 100
[AC-Vlanif100] ip address 10.23.100.1 24
[AC-Vlanif100] quit
[AC] capwap source interface vlanif 100
```

业务 VLAN 设计

如果一个SSID只能对应一个VLAN，一个VLAN对应一个子网，如果大量用户从某一区域接入，只能扩大SSID对应VLAN的子网，保证用户能够获取到IP地址。这样带来的问题就是广播域扩大，导致大量的广播报文（如：ARP、DHCP等)带来严重的网络拥塞。为了解决该问题，一个SSID需要能够对应多个VLAN，把大量用户分散到不同的

VLAN减少广播域。VLAN Pool提供多个VLAN的管理和分配算法，实现SSID对应多个VLAN的方案。

同时，为了方便客户端地址的管理，业务VLAN推荐使用VLAN Pool，通常按照每1000人/1个VLAN来评估VLAN Pool中实际需要的VLAN数。

推荐配置：

```
<AC> system-view
[AC] vlan batch 101 to 103
[AC] vlan pool vlanpool
[AC-vlan-pool-vlanpool] vlan 101 to 103
[AC-vlan-pool-vlanpool] quit
[AC] wlan
[AC-wlan-view] vap-profile name vap1
[AC-wlan-vap-prof-vap1] service-vlan vlan-pool vlanpool
```

注意事项

- 直接转发方式下，建议管理VLAN和业务VLAN分别使用不同的VLAN，否则可能导致业务不通。例如，业务VLAN如果和管理VLAN相同，且交换机连接AP的端口配置了PVID为管理VLAN，则下行到用户的报文出连接AP的交换机时业务VLAN会被终结，从而导致业务不通。
- 隧道转发方式下，管理VLAN和业务VLAN不能配置为同一VLAN，否则会导致MAC漂移，报文转发出错。并且AP和AC之间只能放通管理VLAN，不能放通业务VLAN。
- 建议不要使用VLAN 1作为管理VLAN或者业务VLAN。如果管理VLAN和业务VLAN都配置为VLAN1，报文从AP上行口以untag方式发送出去，此时，需要在连接AP的交换机的端口上配置PVID，使用AP和用户的地址池对应的VLANIF作为该PVID。

3.3.6 SSID

一般按照不同的用户角色或者不同的业务类型来规划SSID，在校园场景下，一般规划3个SSID：学生使用的SSID、教职工使用的SSID和高校联盟SSID。

学生 SSID

推荐方案：

- 转发方式：直接转发
- 用户接入认证：MAC优先的Portal认证，接入认证推荐配置请参考**MAC优先的Portal接入方式**。

推荐配置：

```
[AC-wlan-view] security-profile name student
[AC-wlan-security-prof-student] quit
[AC-wlan-view] ssid-profile name student
[AC-wlan-ssid-prof-student] ssid student
[AC-wlan-ssid-prof-student] quit
[AC-wlan-view] vap-profile name student
[AC-wlan-vap-prof-student] forward-mode direct-forward
[AC-wlan-vap-prof-student] service-vlan vlan-pool student
[AC-wlan-vap-prof-student] security-profile student
[AC-wlan-vap-prof-student] ssid-profile student
```

教职工 SSID

推荐方案：

- 转发方式：直接转发
- 用户接入认证：WPA2+802.1X认证，接入认证推荐配置请参考**WPA2+802.1X的接入方式**。

推荐配置：

```
[AC-wlan-view] security-profile name teacher
[AC-wlan-security-prof-teacher] security wpa2 dot1x aes
[AC-wlan-security-prof-teacher] quit
[AC-wlan-view] ssid-profile name teacher
[AC-wlan-ssid-prof-teacher] ssid teacher
[AC-wlan-ssid-prof-teacher] quit
[AC-wlan-view] vap-profile name teacher
[AC-wlan-vap-prof-teacher] forward-mode direct-forward
[AC-wlan-vap-prof-teacher] service-vlan vlan-pool teacher
[AC-wlan-vap-prof-teacher] security-profile teacher
[AC-wlan-vap-prof-teacher] ssid-profile teacher
[AC-wlan-vap-prof-teacher] quit
```

高校联盟 eduroam SSID

eduroam(education roaming)是专为科研和教育机构开发的安全的环球跨域无线漫游认证服务，目前已覆盖全球一百余个国家和地区的超过6000家科研机构和教育机构。加入eduroam联盟的机构成员可使用本机构提供的合法账号，在全球已加入eduroam联盟的机构内实现无线网络访问的无障碍漫游。

构建校园级eduroam网络的指导请参考eduroam官网中的相关文档。

推荐方案：

- 转发方式：隧道转发
- 用户接入认证：WPA2+802.1X认证，接入认证推荐配置请参考**WPA2+802.1X的接入方式**。
- 认证服务器数据库共享，全球漫游

推荐配置：

```
[AC-wlan-view] security-profile name eduroam
[AC-wlan-view-sec-prof-eduroam] security wpa2 dot1x aes
[AC-wlan-view-sec-prof-eduroam] quit
[AC-wlan-view] ssid-profile name eduroam
[AC-wlan-ssid-prof-eduroam] ssid eduroam
[AC-wlan-ssid-prof-eduroam] quit
[AC-wlan-view] vap-profile name eduroam
[AC-wlan-vap-prof-eduroam] forward-mode tunnel
[AC-wlan-vap-prof-eduroam] service-vlan vlan-pool eduroam
[AC-wlan-vap-prof-eduroam] ssid-profile eduroam
[AC-wlan-vap-prof-eduroam] security-profile eduroam
[AC-wlan-vap-prof-eduroam] quit
```

SSID 模板下其他推荐配置

- Beacon帧发送速率

  高密场景下，周围AP都在周期发送此报文，会带来很大的空口开销。增大Beacon的发送周期，可以减少其带来的开销，从而提升空口有效带宽。同时，为了保证Beacon报文发送的成功率，系统默认以最低速率发送，但这会带来空口资源的开销，提升这类报文的发送速率，能有效降低网络信道利用率，提升网络的有效带宽。

  - Beacon报文发送速率提高后，AP覆盖范围会有所减小，因此建议在AP部署比较密集的场景调整此配置，在降低AP间干扰的同时提升有效网络带宽。

- 一般不建议配置超过11Mbps，另外如果配置为非11b速率（1、2、5.5、11），会导致仅支持802.11b协议的终端无法发现网络。
- 2.4G射频上配置的VAP超过4个时，会导致信道利用率偏高，建议调整此配置。由于5G频段最低速率为6Mbps，且信道多，所以5G一般不调整此参数。
- 修改Beacon帧发送速率会中断业务，建议用户谨慎使用。

在SSID模板下配置Beacon速率。

```
[AC-wlan-view] ssid-profile name test
[AC-wlan-ssid-prof-test] beacon-2g-rate 5.5  //配置2G射频的Beacon速率，配置此参数是为了提高beacon报文的发送速率，降低空口利用率，同时兼容802.11b协议的老终端。如果确认网络中没有802.11b协议的老终端时，可以将此参数配置的更高。
```

- Probe Response报文重传次数

  Probe Response报文是Wi-Fi通信中最常见的报文，无线设备基本都会周期性发送Probe Request广播请求扫描无线信号，周围AP收到后以Probe Response报文进行单播响应，如果报文发送重传，则带来很大的空口资源浪费。降低AP重传Probe Response报文次数，能有效改善网络环境。

  # 在SSID模板下配置probe-response重传次数。

  ```
  [AC-wlan-ssid-prof-test] probe-response-retry 1
  ```

- 单个VAP下能够关联成功的最大用户数

  限制STA的接入个数，可以保证已经接入的STA的业务质量。

  ```
  [AC-wlan-ssid-prof-test] max-sta-number 64
  ```

- STA关联老化时间

  在用户流动性很大的覆盖场景，如商超、室外覆盖等，由于用户接入网络后，很快会离开覆盖区域，此时终端在离开前并未知会设备下线，导致WLAN设备侧保留用户表项，如果AP达到用户上限，会影响新用户接入。因此在这些场景下，可以让AP快速老化离开覆盖区域的终端，将缺省的5分钟老化时间设置为1分钟，提升效果。

  # 在SSID模板下配置STA老化时间

  ```
  [AC-wlan-ssid-prof-test] association-timeout 1
  ```

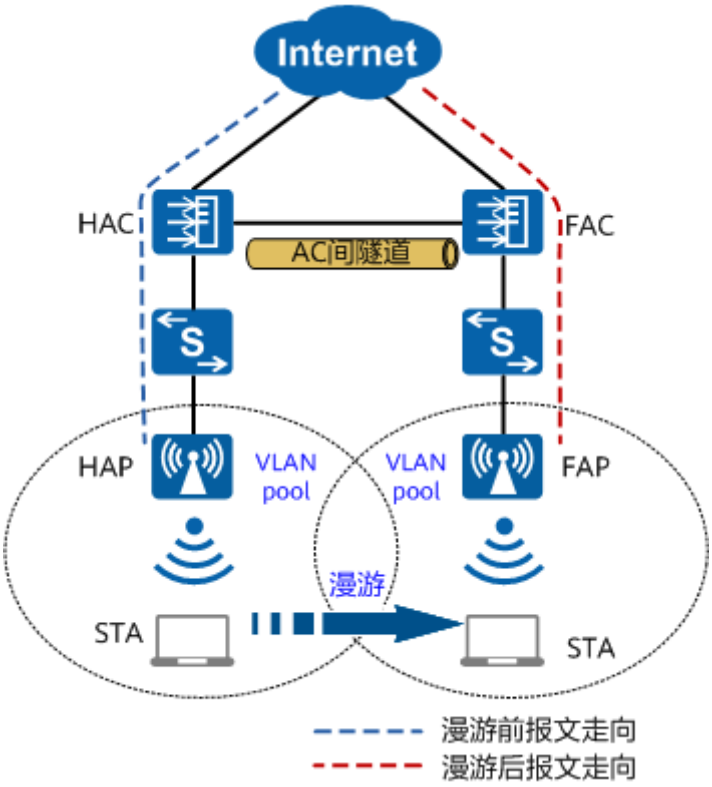
3.3.7 漫游

漫游是指用户在部署了WLAN网络的场所移动时，用户终端可以从一个AP的覆盖范围移动到另一个AP的覆盖范围，用户无需重新登录和认证。

根据STA是否在同一个子网内漫游，可以将漫游分为二层漫游和三层漫游。

- 二层漫游

  二层漫游后STA仍然在原来的子网中，FAP/FAC对二层漫游用户的报文转发同普通新上线用户没有区别，直接在FAP/FAC本地的网络转发，不需要通过AC间隧道转回到HAP/HAC中转。

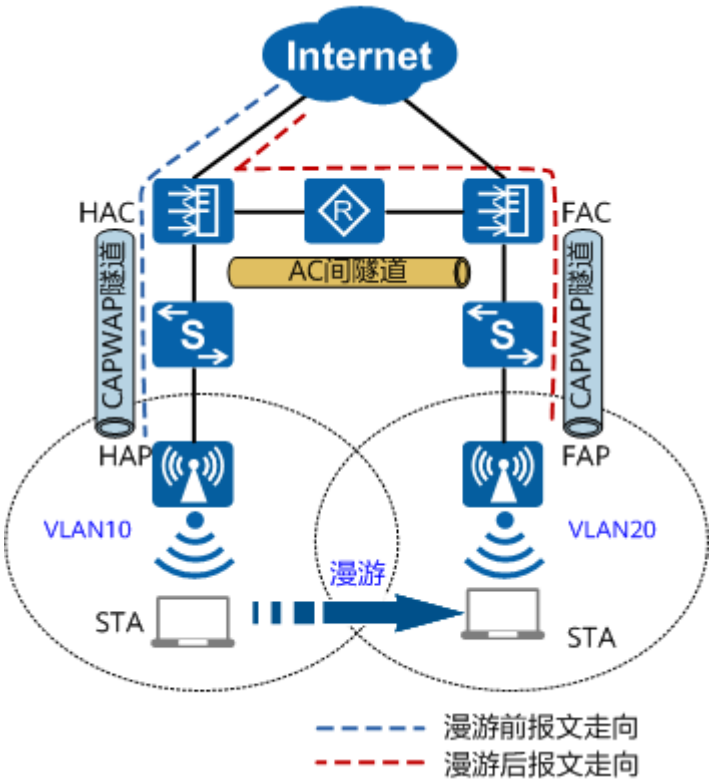


- 三层漫游

  三层漫游时，用户漫游前后不在同一个子网中，为了支持用户漫游后仍能正常访问漫游前的网络，需要将用户流量通过隧道转发到原来的子网进行中转。

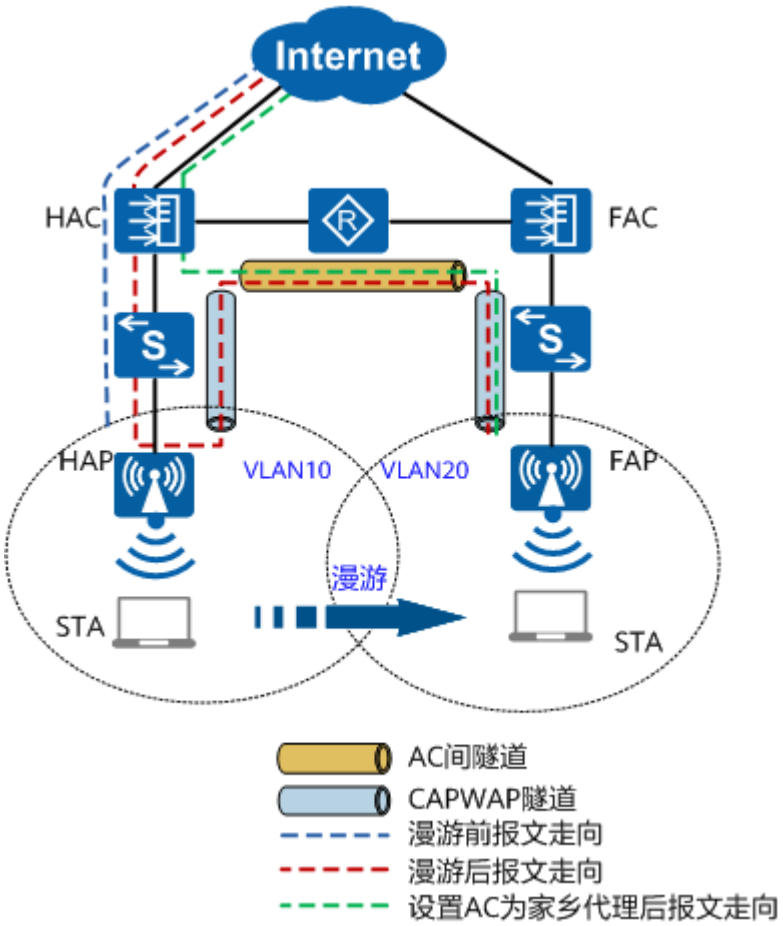
  - 隧道转发模式下，HAP和HAC之间的业务报文通过CAPWAP隧道封装，此时可以将HAP和HAC看作在同一个子网内，报文无需返回到HAP，直接通过HAC进行中转到上层网络。

图 3-3 隧道转发



- 直接转发模式下，HAP和HAC之间的业务报文不通过CAPWAP隧道封装，无法判定HAP和HAC是否在同一个子网内，此时设备默认报文需要返回到HAP进行中转。如果HAP和HAC在同一个子网时，可以将家乡代理设置为性能更强的HAC，减少HAP的负荷并提高转发效率。

图 3-4 直接转发



对于三层漫游，不管是直接转发还是隧道转发，漫游后的流量仍然会通过CAPWAP隧道从HAP或HAC转发，HAP或HAC的性能压力较大。因此，推荐使用AC间二层漫游。

推荐配置：

分别在漫游组的成员AC上配置漫游组，并添加漫游组成员。

```
[AC-wlan] mobility-group name roaming
[AC-wlan-mc-mg-roaming] member ip-address 10.23.100.1
[AC-wlan-mc-mg-roaming] member ip-address 10.23.100.2
```

3.3.8 射频

在WLAN网络中，特别是2.4G频段，带外干扰、带内的同频干扰与邻频干扰都存在，而且不同品牌、不同类型、不同款型终端的行为差异也很大，为提供最优化的无线接入服务，需对射频资源与用户接入进行协调管理，具体的射频资源管理能力包括：

- 射频调优

  通过射频调优功能，动态调整网络各个AP的信道和功率，使同一AC管理的各AP的信道和功率保持相对平衡，保证整网AP工作在最佳状态。建议使用定时调优方式且将调优时间定为用户业务空闲时段（如当地时间凌晨00:00-06:00时段）。

- 频谱导航（5G优先）

  现网应用中，大多数终端同时支持2.4G和5G频段，且通常默认选择2.4G，这导致信道本身就少的2.4G频段更加拥挤，负载高，干扰大；而信道多且干扰小的5G频段优势得不到发挥，特别是在高密或者2.4G干扰严重的环境中。通过频谱导航功

能，AP可以引导STA优先接入5G，减少2.4G频段上的负载和干扰，提升用户体验。

频谱导航功能缺省开启，建议保持缺省值。

- 智能漫游

  对于部分老旧款型终端与哑终端，漫游主动性差，主要表现为：始终“坚持”关联在其最初关联的AP上，即使已经与当前关联的AP距离很远、信号很弱、速率很低，依旧不能漫游到其他信号更好的邻居AP，这种终端一般叫粘性终端。

  粘性终端的影响：

  - 自身业务体验差：终端始终关联在信号差的AP上，无线信道速率下降严重。
  - 影响无线信道整体性能：终端因信号差、速率低而经常传输丢包或者重传，长时间占用无线信道，影响其他终端不能得到足够的信道资源。

  智能漫游功能主动促使终端及时漫游到信号更好的邻居AP，从而带来收益：

  - 性能提升

    通过将信号差的终端漫游到信号更好的AP上，提升终端自身地业务体验和无线信道整体性能。

  - 负载均衡

    通过智能漫游，确保每个终端都关联到离自己最近的AP下，实现了AP间负载均衡。

  智能漫游功能缺省开启，建议保持缺省值。

调优模式推荐配置

射频调优涉及全网AP的信道、功率的调整，如果在正常办公期间进行调整，会造成用户无线连接闪断，建议定在凌晨，前提是AC的系统时间要准确。

推荐配置：

```
[AC-wlan-view] calibrate enable schedule time 02:00:00  //配置定时调优
```

调优信道推荐配置

每个国家都有对应的信道集合，以20MHz频段信道集的表示。在信道数足够的情况下，尽量配置宽的频宽。室内和室外的信道集可能不一样，所以针对室内AP和室外AP建议分组配置。

以中国国家码为例：

- 室内覆盖场景：2.4G频宽只有1,6,11共3个不重叠信道，频宽建议使用默认的20MHz，调优信道集建议配置为1,6,11，如果AP数目较多，布放紧密时，调优信道集建议配置为1,9,5,13。5G有36~64，149~165共13个不重叠20MHz频宽的信道，可组成6个40MHz频宽信道，故建议5G配置成40MHz频宽。5G信道建议根据频宽按需配置。此处需注意雷达信道的选用，经验发现部分终端存在对非雷达信道的偏好性，并且雷达信道本身有法规规定的规避策略限制，如果信道够用的情况下，建议不要使用雷达信道。

  推荐配置：

  ```
  [AC-wlan-view] regulatory-domain-profile name huawei
  [AC-wlan-regulate-domain-huawei] dca-channel 2.4g channel-set 1,5,9,13  //2.4G频段的调优信道集
  [AC-wlan-regulate-domain-huawei] dca-channel 5g bandwidth 40mhz  //5G频段的调优带宽
  [AC-wlan-regulate-domain-huawei] dca-channel 5g channel-set
  36,40,44,48,149,153,157,161,165  //5G频段的调优信道集
  [AC-wlan-regulate-domain-huawei] quit
  ```

- 室外覆盖场景（外置定向天线）/高密覆盖场景：不支持调优，建议按照网规结果手动配置AP信道。

  推荐配置：

  ```
  [AC-wlan-view] ap-id 0  //单独配置室外AP的信道
  [AC-wlan-ap-0] radio 0
  [AC-wlan-radio-0/0] calibrate auto-channel-select disable  //关闭信道自动调优功能
  [AC-wlan-radio-0/0] channel 20mhz 5  //指定射频的带宽为20MHz，信道为5
  Warning: This action may cause service interruption. Continue?[Y/N]y
  [AC-wlan-radio-0/0] quit
  [AC-wlan-ap-0] radio 1
  [AC-wlan-radio-0/1] calibrate auto-channel-select disable  //关闭信道自动调优功能
  [AC-wlan-radio-0/1] channel 40mhz-plus 149  //指定射频的带宽为40MHz，信道为149
  Warning: This action may cause service interruption. Continue?[Y/N]y
  [AC-wlan-radio-0/1] quit
  ```

调优功率推荐配置

一般情况下，WLAN网络覆盖区域的信号强度（RSSI）需要达到-65dBm才能满足良好的网络覆盖体验。

2.4G和5G射频的功率建议控制一定的差值，从而降低支持5G的终端关联2.4G射频的概率。

- 室内覆盖场景：室内场景主要为蜂窝式部署，可以采用自动调优方式进行信道功率部署，避免因为配置的信号发射功率过小导致出现覆盖盲区或配置的信号功率过大导致出现信号相互干扰。该功能默认开启。

  如果希望在自动调优方式下，依然能够达到固化信号强度的目的，建议配置调优功率上下限来实现，便于后期灵活控制。同时，功率上下限的差值不要过大，减少因为相邻AP之间信号强度差值引起不必要的漫游。功率上下限的具体取值需要结合AP具体款型和实际场景进行调整。

  推荐配置：

  ```
  [AC-wlan-view] rrm-profile name 2g
  [AC-wlan-rrm-prof-2g] calibrate min-tx-power 7
  [AC-wlan-rrm-prof-2g] calibrate max-tx-power 11
  [AC-wlan-view] rrm-profile name 5g
  [AC-wlan-rrm-prof-5g] calibrate min-tx-power 19
  [AC-wlan-rrm-prof-5g] calibrate max-tx-power 20
  ```

- 室外覆盖场景：建议按照网规结果进行功率配置。

  推荐配置：

  ```
  [AC-wlan-view] ap-id 0  //单独配置室外AP的功率
  [AC-wlan-ap-0] radio 0
  [AC-wlan-radio-0/0] calibrate auto-txpower-select disable  //关闭功率自动调优功能
  [AC-wlan-radio-0/0] eirp 20  //指定射频的发射功率为20dBm
  [AC-wlan-radio-0/0] quit
  [AC-wlan-ap-0] radio 1
  [AC-wlan-radio-0/1] calibrate auto-txpower-select disable  //关闭功率自动调优功能
  [AC-wlan-radio-0/1] eirp 20  //指定射频的发射功率为20dBm
  [AC-wlan-radio-0/1] quit
  ```

射频资源管理模板下推荐配置

- 终端迁移

  终端迁移功能综合了频谱导航、负载均衡和智能漫游等功能：

  - 在终端关联前，通过Probe抑制来引导终端优先接入5G射频。
  - 在终端关联后，通过目标AP选择算法，综合衡量终端的双频能力、AP的负载和信号质量，引导终端接入更优的AP。

  推荐配置：

```
[AC-wlan-view] rrm-profile name default
[AC-wlan-rrm-prof-default] smart-roam roam-threshold check-snr  //配置智能漫游功能基于终端信噪比的触发方式
[AC-wlan-rrm-prof-default] smart-roam roam-threshold snr 25  //配置智能漫游信噪比阈值为25dB，底噪为-95dBm，因此，当STA信号强度低于25dB + (-95dBm) = -70dBm时，则认为低于信噪比阈值
[AC-wlan-rrm-prof-default] smart-roam unable-roam-client expire-time 360  //配置STA漫游静默期为360分钟，在静默期内不再主动迁移STA漫游
[AC-wlan-rrm-prof-default] smart-roam quick-kickoff-threshold check-snr  //配置强制低信号强度用户下线功能基于终端信噪比的触发方式
[AC-wlan-rrm-prof-default] smart-roam quick-kickoff-threshold snr 15  //配置强制低信号强度阈值为15dB，即STA信号强度低于-80dBm时，强制STA下线
[AC-wlan-rrm-prof-default] sta-load-balance dynamic rssi-threshold -55  //配置动态负载均衡成员的RSSI值（默认是-65）。当STA的RSSI高于此RSSI值时，AP才会把邻居上报给AC，此配置是为了过滤信号弱的AP
[AC-wlan-rrm-prof-default] sta-load-balance dynamic sta-number start-threshold 15  //基于用户数的动态负载均衡起始终端数门限（默认10）。比如在宿舍场景，一个宿舍一个AP，评估单宿舍的终端数，建议将此参数配置成大于终端数
[AC-wlan-rrm-prof-default] sta-load-balance dynamic deauth-fail-times 0  //如果当前网络信号覆盖效果一般，存在漫游掉线的情况，或者对于漫游需求不是很高的场景，例如宿舍场景，建议降低智能漫游阈值或关闭deauth功能
[AC-wlan-rrm-prof-default] band-steer balance start-threshold 100  //配置5G优先的接入用户数起始门限
[AC-wlan-rrm-prof-default] band-steer balance gap-threshold 90  //配置5G射频接入用户数占比门限
```

- EDCA参数调整

  WMM协议将数据报文分为4个接入类别AC（Access Category），分别为AC_VO（Voice）、AC_VI（Video）、AC_BE（Best Effort）、AC_BK（Background）。每个AC类别定义了一套信道竞争EDCA参数，这些参数决定了AC类别占用信道的能力。通过配置不同类别报文的EDCA参数，可以针对不同类别的报文区分优先级，提供不同的信道抢占能力，实现不同的服务质量。

  EDCA不建议随意配置，参考值分为以下几种场景：

  - 语音场景

报文类别	ECWmax	ECWmin	AIFSN	TXOPLimit	ACK策略
AC_VO	4	2	2	0	normal
AC_VI	5	3	5	0	normal
AC_BE	10	6	5	0	normal
AC_BK	10	8	12	0	normal

  - 语音和视频场景

报文类别	ECWmax	ECWmin	AIFSN	TXOPLimit	ACK策略
AC_VO	4	2	2	0	normal
AC_VI	5	3	5	0	normal
AC_BE	10	6	12	0	normal
AC_BK	10	8	12	0	normal

  - 高密场景

    经过实践经验，在高密场景下，调整EDCA参数能减少冲突，提升业务体验，建议在高密场景做配置调整。

动态EDCA参数调整通过感知用户数量，灵活调整物理信道竞争参数，降低碰撞几率，大大提升整体吞吐量，有效提升用户体验。

- 其他场景：建议使用缺省值。

推荐配置：

```
# 在2G射频模板和5G射频模板下配置下行的EDCA参数
[AC-wlan-view] radio-2g-profile name default
[AC-wlan-radio-2g-prof-default] wmm edca-ap ac-be ecw ecwmin 6 ecwmax 10

# 在SSID模板下配置上行的EDCA参数
[AC-wlan-view] ssid-profile name default
[AC-wlan-ssid-prof-default] wmm edca-client ac-be ecw ecwmin 6 ecwmax 10

# 在RRM模板下配置动态EDCA功能
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] dynamic-edca enable    //开启动态EDCA功能
[HUAWEI-wlan-rrm-prof-default] dynamic-edca threshold be-service 6
```

射频模板下推荐配置

- 速率集

  删除老终端速率集中较低的速率（1Mbps和2Mbps），提升AP整体吞吐量。

  推荐配置：

  ```
  <AC> system-view
  [AC] wlan
  [AC-wlan-view] radio-2g-profile name default
  [AC-wlan-radio-2g-prof-default] dot11bg basic-rate 6 9 12 18 24 36 48 54
  [AC-wlan-radio-2g-prof-default] dot11bg supported-rate 6 9 12 18 24 36 48 54
  ```

- Beacon周期

  AP通过beacon帧来通告某个802.11网络（bssid）的存在。建议基于VAP数量和漫游、空口利用率这几个角度配置此参数。默认100，为了减少漫游、降低空口利用率，可以考虑增大beacon间隔，建议配置成100、200、300这样的固定值，否则可能会有其他业务影响。

  Beacon周期配置太大，会导致STA休眠时间变长，甚至掉线；Beacon周期配置太小，会导致空口开销变大。因此，建议用户根据VAP的数量调整Beacon周期的大小。

  - 4个VAP及以内：100TUs左右
  - 5～8个VAP：200TUs左右
  - 9～12个VAP：300TUs左右
  - 13～16个VAP：400TUs左右

  推荐配置：

  ```
  # 在2G射频模板和5G射频模板下配置Beacon周期。
  [AC-wlan-view] radio-2g-profile name default
  [AC-wlan-radio-2g-prof-default] beacon-interval 200
  [AC-wlan-radio-2g-prof-default] quit
  [AC-wlan-view] radio-5g-profile name default
  [AC-wlan-radio-5g-prof-default] beacon-interval 200
  ```

- RTS-CTS的工作模式和阈值

  RTS/CTS（Request To Send/Clear To Send）握手协议，可以避免信道冲突导致的数据传输失败。但如果每个工作站每次发送数据前都要执行该机制，则会导致过多的RTS帧占用信道带宽。建议使用缺省值。

  - 如果不启用该机制，可能存在“隐藏终端”问题，即基站A和C同时向基站B发送信息，但基站C未侦测到A也向B发送，故A和C同时将信号发送至B，引起信号冲突，最终导致数据传输失败。

- 如果启用该机制，则会降低传输速率，甚至引起网络延时，因此，需要配置合适的阈值。

  这个阈值设置表示对报文长度大于此阈值的报文，AP发送之前会发送RTS来清空信道，小于此阈值长度的报文，AP不使用此机制，主要目的是防止有隐藏终端带来的冲突，该阈值默认为1400Byte。

  为了避免信道冲突，可以适当降低这个数值。但是由于RTS/CTS机制会在报文发送时带来额外开销，如果设置过小的话，对整体空口吞吐量有一定影响，可根据设置后的实际效果做调整。

```
[AC-wlan-view] radio-2g-profile name default
[AC-wlan-radio-2g-prof-default] rts-cts-mode rts-cts
[AC-wlan-radio-2g-prof-default] rts-cts-threshold 1400
[AC-wlan-radio-2g-prof-default] quit
[AC-wlan-view] radio-5g-profile name default
[AC-wlan-radio-5g-prof-default] rts-cts-mode rts-cts
[AC-wlan-radio-5g-prof-default] rts-cts-threshold 1400
[AC-wlan-radio-5g-prof-default] quit
```

- 组播速率

  组播发送范围广，提高发送速率，能够降低空口开销。

  推荐配置：

```
[AC-wlan-view] radio-2g-profile name default
[AC-wlan-radio-2g-prof-default] multicast-rate 24  //配置组播速率
[AC-wlan-radio-2g-prof-default] quit
[AC-wlan-view] radio-5g-profile name default
[AC-wlan-radio-5g-prof-default] multicast-rate 24
```

- GI模式

  GI参数是指无线设备发送报文时，前后两个报文的最小间隔，防止前后两个报文在空口传输时相互冲突。保护间隔默认值为800ns，对于室内办公、球馆高密等近距离覆盖场景，Guard Interval可以配置成400ns，以提升空口有效带宽。

  GI模式缺省为short,在室外覆盖、网桥数据回传等场景，由于传输距离较远，不要更改此参数。

  推荐配置：

```
[AC-wlan-view] radio-2g-profile name default
[AC-wlan-radio-2g-prof-default] guard-interval-mode short
[AC-wlan-radio-2g-prof-default] guard-interval-mode dot11ax dot8
```

3.3.9 用户接入认证

根据用户身份认证的方式不同，WLAN网络常见的认证方案有802.1X、MAC和Portal三种，不同认证方案的对比如表3-4所示。

表 3-4 用户认证方案对比

对比项	802.1X认证	MAC认证	Portal认证/MAC优先Portal认证
客户端需求	需要	不需要	不需要
优点	安全性高	无需安装客户端	部署灵活
缺点	部署不灵活	需登记MAC地址，管理复杂	安全性不高

对比项	802.1X认证	MAC认证	Portal认证/MAC优先Portal认证
适合场景	通常适用于对安全要求较高的办公用户的网络认证	打印机、传真机等哑终端接入认证的场景	通常适用于流动性较大，终端类型复杂的访客用户网络认证

MAC优先的Portal认证：是指用户终端进行Portal认证成功后，认证服务器会在一定时间内缓存用户终端地址，这段时间用户终端能够直接通过MAC认证接入，无需重新输入用户名密码进行Portal认证。

综合考虑以上认证方案的特点，在WLAN网络中，不同用户的认证方案的选择建议如表3-5所示。

表 3-5 用户认证方案的选择建议

用户角色	认证类型
学生/访客	MAC优先Portal认证
教职工	802.1X认证
哑终端（打印机、传真机等）	MAC认证

MAC 优先的 Portal 接入方式

推荐配置：

说明

以下配置以AC作为认证点为例。

```
# 配置RADIUS服务器模板。
[AC] radius-server template student
[AC-radius-student] radius-server authentication 10.23.102.1 1812
[AC-radius-student] radius-server shared-key cipher Huawei123
[AC-radius-student] quit
# 创建认证方案并配置认证方式为RADIUS。
[AC] aaa
[AC-aaa] authentication-scheme student
[AC-aaa-authen-student] authentication-mode radius
[AC-aaa-authen-student] quit
# 创建计费方案并配置计费方式为RADIUS。
[AC-aaa] accounting-scheme student
[AC-aaa-accounting-student] accounting-mode radius
[AC-aaa-accounting-student] accounting realtime 15
[AC-aaa-accounting-student] quit
[AC-aaa] quit
# 配置Portal认证页面URL地址，在用户认证成功前，AC将用户的访问地址重定向到Portal服务器
[AC] web-auth-server student
[AC-web-auth-server-student] server-ip 10.23.103.1
[AC-web-auth-server-student] shared-key cipher Huawei123
[AC-web-auth-server-student] port 50200
[AC-web-auth-server-student] url-template student ciphered-parameter-name cpname iv-parameter-name iv-value key cipher Huawei123
# 配置Portal接入模板“student”，并配置Portal认证为二层Portal认证
```

```
[AC] portal-access-profile name student
[AC-portal-access-profile-student] web-auth-server student direct
[AC-portal-access-profile-student] quit
# 配置MAC接入模板，用于MAC优先的Portal认证
[AC] mac-access-profile name student
[AC-mac-access-profile-student] quit
# 配置免认证规则模板
[AC] free-rule-template name default_free_rule
[AC-free-rule-default_free_rule] free-rule 1 destination ip 8.8.8.8 mask 32
[AC-free-rule-default_free_rule] quit
# 配置认证模板“student”，并启用MAC优先的Portal认证
[AC] authentication-profile name student
[AC-authentication-profile-student] portal-access-profile student
[AC-authentication-profile-student] mac-access-profile student
[AC-authentication-profile-student] free-rule-template default_free_rule
[AC-authentication-profile-student] authentication-scheme student
[AC-authentication-profile-student] radius-server student
[AC-authentication-profile-student] quit
配置WLAN业务参数
# 创建名为“student”的安全模板，并配置安全策略为open方式的开放认证。缺省情况下，安全策略为open方式的开放认证。
[AC] wlan
[AC-wlan-view] security-profile name student
[AC-wlan-sec-prof-student] quit
# 创建名为“student”的SSID模板，并配置SSID名称为“student”。
[AC-wlan-view] ssid-profile name student
[AC-wlan-ssid-prof-student] ssid student
# 创建名为“student”的VAP模板，配置业务数据转发模式、业务VLAN，并且引用安全模板、SSID模板和认证模板。
[AC-wlan-view] vap-profile name student
[AC-wlan-vap-prof-student] forward-mode direct-forward
[AC-wlan-vap-prof-student] service-vlan vlan-pool student
[AC-wlan-vap-prof-student] security-profile student
[AC-wlan-vap-prof-student] ssid-profile student
[AC-wlan-vap-prof-student] authentication-profile student
[AC-wlan-vap-prof-student] quit
# 配置AP组引用VAP模板，AP上射频0和射频1都使用VAP模板“student”的配置。
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] vap-profile student wlan 1 radio 0
[AC-wlan-ap-group-ap-group1] vap-profile student wlan 1 radio 1
[AC-wlan-ap-group-ap-group1] quit
[AC-wlan-view] quit
```

WPA2+802.1X 的接入方式

802.1X认证适用于对安全要求较高的办公用户的网络认证，教职工接入网络时建议采用802.1X认证方式。

RADIUS认证参数推荐配置：

```
# 创建RADIUS服务器模板
[AC] radius-server template teacher
[AC-radius-teacher] radius-server authentication 10.23.103.1 1812
[AC-radius-teacher] radius-server shared-key cipher huawei@123
[AC-radius-teacher] quit
# 创建RADIUS方式的认证方案
[AC] aaa
[AC-aaa] authentication-scheme teacher
[AC-aaa-authen-teacher] authentication-mode radius
[AC-aaa-authen-teacher] quit
[AC-aaa] accounting-scheme teacher
[AC-aaa-accounting-teacher] accounting-mode radius
[AC-aaa-accounting-teacher] accounting realtime 15
[AC-aaa] quit
# 创建名为“teacher”的802.1X接入模板
[AC] dot1x-access-profile name teacher
# 创建名为“teacher”的认证模板，并引用802.1X接入模板、认证方案和RADIUS服务器模板
[AC] authentication-profile name teacher
```

```
[AC-authentication-profile-teacher] dot1x-access-profile teacher
[AC-authentication-profile-teacher] authentication-scheme teacher
[AC-authentication-profile-teacher] accounting-scheme teacher
配置WLAN业务参数
# 创建名为“teacher”的安全模板，并配置安全策略
[AC-authentication-profile-teacher] quit
[AC] wlan
[AC-wlan-view] security-profile name teacher
[AC-wlan-sec-prof-teacher] security wpa-wpa2 dot1x aes
[AC-wlan-sec-prof-teacher] quit
# 创建名为“teacher”的SSID模板，并配置SSID名称为“teacher”
[AC-wlan-view] ssid-profile name teacher
[AC-wlan-ssid-prof-teacher] ssid teacher
[AC-wlan-ssid-prof-teacher] quit
# 创建名为“teacher”的VAP模板，配置业务数据转发模式为直接转发、业务VLAN，并且引用安全模板、认证模板和SSID模板
[AC-wlan-view] vap-profile name teacher
[AC-wlan-vap-prof-teacher] forward-mode direct-forward
[AC-wlan-vap-prof-teacher] service-vlan vlan-pool teacher
[AC-wlan-vap-prof-teacher] security-profile teacher
[AC-wlan-vap-prof-teacher] authentication-profile teacher
[AC-wlan-vap-prof-teacher] ssid-profile teacher
[AC-wlan-vap-prof-teacher] quit
# 配置AP组引用VAP模板，AP上射频0和射频1都使用VAP模板“teacher”的配置
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] vap-profile teacher wlan 1 radio 0
[AC-wlan-ap-group-ap-group1] vap-profile teacher wlan 1 radio 1
[AC-wlan-ap-group-ap-group1] quit
[AC-wlan-view] quit
```

RADIUS 授权

为了更好的实现对用户权限的控制，推荐配置RADIUS授权，RADIUS协议支持通过独立的RADIUS授权服务器对已在线的用户进行授权。RADIUS的授权方法包括CoA（Change of Authorization）和DM（Disconnect Messages）两种：

- CoA：用户认证成功后，管理员可以通过RADIUS授权服务器来修改在线用户的权限。例如，通过CoA为用户下发VLAN，可以保证某一部门的员工无论从哪个设备端口接入网络，均属于同一个VLAN。
- DM：管理员可以通过RADIUS授权服务器主动强迫在线用户下线。

只有配置了RADIUS授权服务器的IP地址、共享密钥等参数后，设备才能正常接受服务器发送过来的授权请求信息并根据此信息对用户进行授权。完成授权后，设备通过授权回应报文将授权结果反馈给服务器。

推荐配置：

```
[AC] radius-server authorization 10.1.1.116 shared-key cipher Huawei@2020
```

3.3.10 可靠性

AC支持VRRP热备份、双链路热备份、双链路冷备份和N+1备份，各备份方式的差异比较如表3-6所示。

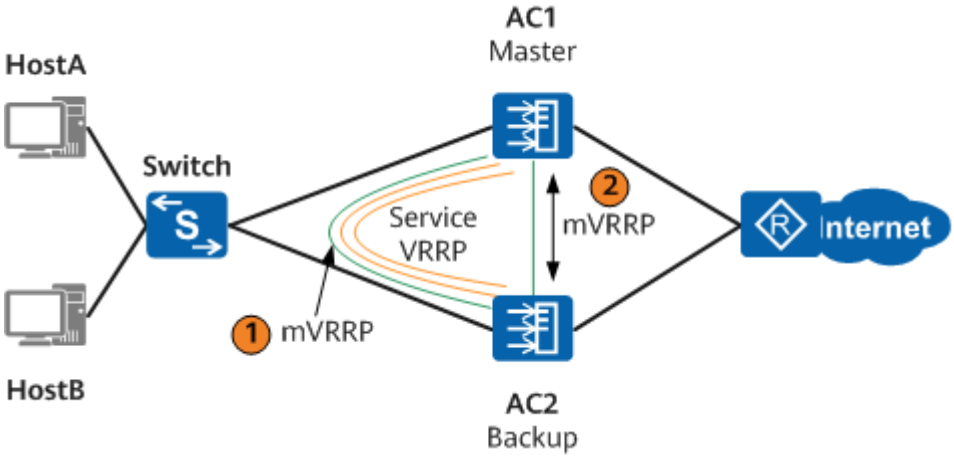
表 3-6 备份方式比较

对比项	VRRP热备份	双链路热备份	双链路冷备份	N+1备份
实现方式	主备AC两个独立的IP地址，通过VRRP对外虚拟为同一个IP地址，单个AP和虚拟IP建立一条CAPWAP链路。 主AC备份AP信息、STA信息和CAPWAP链路信息，并通过HSB主备服务将信息同步给备AC。主AC故障后，备AC直接接替工作。	单个AP分别和主备AC建立CAPWAP链路，一条主链路，一条备链路。 主AC仅备份STA信息，并通过HSB主备服务将信息同步给备AC。主AC故障后，AP切换到备链路上，备AC接替工作。	单个AP分别和主备AC建立CAPWAP链路，一条主链路，一条备链路。 AC不备份同步信息。主AC故障后，AP切换到备链路上，备AC接替工作。	单个AP只和一个AC建立CAPWAP链路。 AC不备份同步信息。主AC故障后，AP重新与备AC建链CAPWAP链路，备AC接替工作。
切换速度比较	最快 主备切换速度快，对业务影响小。通过配置VRRP抢占时间，相比于其他备份方式可以实现更快的主备切换。	快 AP状态切换慢，需等待检测到CAPWAP断链超时后才会切换，主备切换过后STA不需要掉线重连。	慢 AP状态切换慢，需等待检测到CAPWAP断链超时后才会切换，STA需要重新上线，业务会出现短暂中断。	最慢 AP状态切换慢，需等待检测到CAPWAP断链超时后才会切换，AP、STA均需要重新上线，业务会出现短暂中断，中断时间比双链路冷备份中断时间长。
主备AC异地部署	不支持。 VRRP协议是二层协议，不支持主备AC异地跨三层部署。	支持。	支持。	支持。
约束条件	主备AC的型号和软件版本需完全一致。	主备AC的型号和软件版本需完全一致。	主备AC产品型号可以不同，AC的软件版本必须一致。	主备AC产品型号可以不同，AC的软件版本必须一致。
适用范围	对可靠性要求高，且无需异地部署主备AC的场景。	对可靠性要求高，且要求异地部署主备AC的场景。	对可靠性要求较低的场景。	对可靠性要求较低，对成本控制要求较高的场景。

结合对比情况，无线网络推荐使用VRRP+HSB AC间热备份方案，保证在主设备故障时业务能够不中断的顺利切换到备份设备。

该备份模式下AP只能获取到一个AC的IP地址，该IP地址为用户为同一VRRP备份组中的主备AC配置的虚拟IP地址。VPPR备份组中的AC根据优先级选举出主AC，只有主AC负责管理和控制所有AP和用户，同时通过双机热备份HSB功能定时向备AC发送状态信息和需要备份的信息（AP的表项、CAPWAP链路信息、用户信息）。当主AC故障时，备AC可以快速检测到主AC的故障，及时切换为新的主AC，保证用户业务不会中断。

同时，搭配上无线配置同步功能，只需要在主AC上配置WLAN相关业务，就可以通过该功能将配置同步给备AC，大大减少了配置工作量；同时，也避免了完成主AC上的配置后遗漏备AC上的配置，优化了维护操作。



推荐配置

- **主AC（AC1）配置**

```
# 配置VRRP备份组的状态恢复延迟时间为60秒。
[AC1] vrrp recover-delay 60
# 在AC1上创建管理VRRP备份组，配置AC1在该备份组中的优先级为120，并配置抢占时间为1800秒。
[AC1] interface vlanif 100  //AC1的管理VLAN接口
[AC1-Vlanif100] vrrp vrid 1 virtual-ip 10.23.100.3  //管理VRRP备份组的虚拟IP地址
[AC1-Vlanif100] vrrp vrid 1 priority 120
[AC1-Vlanif100] vrrp vrid 1 preempt-mode timer delay 1800
[AC1-Vlanif100] admin-vrrp vrid 1
# 在AC1上创建业务VRRP备份组，并配置抢占时间为1800秒。
[AC1] interface vlanif 101  //AC1的业务VLAN接口
[AC1-Vlanif101] vrrp vrid 2 virtual-ip 10.23.101.3  //业务VRRP备份组的虚拟IP地址
[AC1-Vlanif101] vrrp vrid 2 preempt-mode timer delay 1800
[AC1-Vlanif101] vrrp vrid 2 track admin-vrrp interface vlanif 100 vrid 1 unflowdown
# 在AC1上创建HSB主备服务0，并配置其主备通道IP地址和端口号，配置HSB主备服务报文的重传次数和发送间隔。
[AC1] hsb-service 0
[AC1-hsb-service-0] service-ip-port local-ip 10.23.102.1 peer-ip 10.23.102.2 local-data-port 10241 peer-data-port 10241
[AC1-hsb-service-0] service-keep-alive detect retransmit 3 interval 6
[AC1-hsb-service-0] quit
# 在AC1上创建HSB备份组0，并配置其绑定HSB主备服务0和管理VRRP备份组。
[AC1] hsb-group 0
[AC1-hsb-group-0] bind-service 0
[AC1-hsb-group-0] track vrrp vrid 1 interface vlanif 100
[AC1-hsb-group-0] quit
# 配置NAC业务绑定HSB备份组。
[AC1] hsb-service-type access-user hsb-group 0
# 配置WLAN业务绑定HSB备份组。
[AC1] hsb-service-type ap hsb-group 0
# 配置DHCP业务绑定HSB备份组。
[AC1] hsb-service-type dhcp hsb-group 0
```



```
# 使能双机热备功能。
[AC1] hsb-group 0
[AC1-hsb-group-0] hsb enable
[AC1-hsb-group-0] quit
# 配置无线配置同步功能。
[AC1] wlan
[AC1-wlan-view] master controller
[AC1-master-controller] master-redundancy peer-ip ip-address 10.23.102.2 local-ip ip-address 10.23.102.1 psk H@123456
[AC1-master-controller] master-redundancy track-vrrp vrid 1 interface vlanif 100
[AC1-master-controller] quit
[AC1-wlan-view] quit
```

- **备AC（AC2）配置**

```
# 配置VRRP备份组的状态恢复延迟时间为60秒。
[AC2] vrrp recover-delay 60
# 在AC2上创建管理VRRP备份组。
[AC2] interface vlanif 100  //AC2的管理VLAN接口
[AC2-Vlanif100] vrrp vrid 1 virtual-ip 10.23.100.3  //管理VRRP备份组的虚拟IP地址
[AC2-Vlanif100] admin-vrrp vrid 1
# 在AC2上创建业务VRRP备份组。
[AC2] interface vlanif 101  //AC2的业务VLAN接口
[AC2-Vlanif101] vrrp vrid 2 virtual-ip 10.23.101.3  //业务VRRP备份组的虚拟IP地址
[AC2-Vlanif101] vrrp vrid 2 track admin-vrrp interface vlanif 100 vrid 1 unflowdown
# 在AC2上创建HSB主备服务0，并配置其主备通道IP地址和端口号，配置HSB主备服务报文的重传次数和发送间隔。
[AC2] hsb-service 0
[AC2-hsb-service-0] service-ip-port local-ip 10.23.102.2 peer-ip 10.23.102.1 local-data-port 10241 peer-data-port 10241
[AC2-hsb-service-0] service-keep-alive detect retransmit 3 interval 6
# 在AC2上创建HSB备份组0，并配置其绑定HSB主备服务0和管理VRRP备份组。
[AC2] hsb-group 0
[AC2-hsb-group-0] bind-service 0
[AC2-hsb-group-0] track vrrp vrid 1 interface vlanif 100
[AC2-hsb-group-0] quit
# 配置NAC业务绑定HSB备份组。
[AC2] hsb-service-type access-user hsb-group 0
# 配置WLAN业务绑定HSB备份组。
[AC2] hsb-service-type ap hsb-group 0
# 配置DHCP业务绑定HSB备份组。
[AC2] hsb-service-type dhcp hsb-group 0
# 使能双机热备功能。
[AC2] hsb-group 0
[AC2-hsb-group-0] hsb enable
[AC2-hsb-group-0] quit
# 配置无线配置同步功能。
[AC2] wlan
[AC2-wlan-view] master controller
[AC2-master-controller] master-redundancy peer-ip ip-address 10.23.102.1 local-ip ip-address 10.23.102.2 psk H@123456
[AC2-master-controller] master-redundancy track-vrrp vrid 1 interface vlanif 100
[AC2-master-controller] quit
[AC2-wlan-view] quit
```

3.3.11 流量

用户限速

网络带宽资源有限的情况下，为了保证每个用户都能有相对公平的网络体验，建议对VAP内所有STA或VAP内每个STA的上下行的报文进行速率限制。限速值可以根据网络规划时不同场景下需要满足的用户业务带宽需求来配置。

推荐配置：

```
<AC> system-view
[AC] wlan
[AC-wlan-view] traffic-profile name p1
[AC-wlan-traffic-prof-p1] rate-limit client up 8192    //VAP内每个STA上行报文速率限制
[AC-wlan-traffic-prof-p1] rate-limit client down 8192  //VAP内每个STA下行报文速率限制
```

空口上行广播/组播报文流量抑制

广播/组播报文在空口中以较低速率发送，大量的此类报文会占用较大的空口资源，影响用户正常业务数据报文传输。

- 对于没有组播业务的场景，建议通过提升组播广播报文发送速率和抑制组播广播报文个数，来有效减少组播/广播对空口资源的占用。

  推荐配置：

  - 空口上行VAP级别广播/组播/未知单播报文流量抑制

    ```
    [AC-wlan-traffic-prof-p1] traffic-optimize broadcast-suppression packets 128  //广播报文流量抑制
    [AC-wlan-traffic-prof-p1] traffic-optimize multicast-suppression packets 128  //组播报文流量抑制
    [AC-wlan-traffic-prof-p1] traffic-optimize unicast-suppression packets 64  //未知单播报文流量抑制
    [AC-wlan-traffic-prof-p1] quit
    ```

  - 空口上行STA级别广播/组播报文流量抑制

    ```
    [AC-wlan-view] vap-profile name p1
    [AC-wlan-vap-prof-test] anti-attack flood igmp sta-rate-threshold 1
    [AC-wlan-vap-prof-test] anti-attack flood other-multicast sta-rate-threshold 1
    [AC-wlan-vap-prof-test] anti-attack flood other-broadcast sta-rate-threshold 1
    [AC-wlan-vap-prof-test] anti-attack flood mdns sta-rate-threshold 2
    [AC-wlan-vap-prof-test] anti-attack flood nd sta-rate-threshold 1
    [AC-wlan-vap-prof-test] anti-attack flood dhcpv6 sta-rate-threshold 1
    ```

- 对于存在组播业务的场景，如多媒体教室的视频点播业务等，建议关闭组播报文抑制功能，避免影响组播业务。

  推荐配置：

  - 空口上行VAP级别广播/未知单播报文流量抑制

    ```
    [AC-wlan-traffic-prof-p1] traffic-optimize broadcast-suppression packets 128  //广播报文流量抑制
    [AC-wlan-traffic-prof-p1] undo traffic-optimize multicast-suppression  //不对组播报文流量进行抑制
    [AC-wlan-traffic-prof-p1] traffic-optimize unicast-suppression packets 64  //未知单播报文流量抑制
    [AC-wlan-traffic-prof-p1] quit
    ```

  - 空口上行STA级别广播报文流量抑制

    ```
    [AC-wlan-view] vap-profile name p1
    [AC-wlan-vap-prof-test] anti-attack flood igmp sta-rate-threshold 1
    [AC-wlan-vap-prof-test] anti-attack flood other-multicast disable  //关闭组播报文抑制功能
    [AC-wlan-vap-prof-test] anti-attack flood other-broadcast sta-rate-threshold 1
    [AC-wlan-vap-prof-test] anti-attack flood mdns sta-rate-threshold 2
    [AC-wlan-vap-prof-test] anti-attack flood nd sta-rate-threshold 1
    [AC-wlan-vap-prof-test] anti-attack flood dhcpv6 sta-rate-threshold 1
    ```

有线下行广播/组播报文流量抑制

当网络中存在泛洪攻击时，AP有线口的广播报文、组播报文和未知单播报文增多，这些报文占用的网络资源也将随之增多，进而会影响网络业务的正常运行。为了减小大量低速广播/组播报文对网络造成的冲击，建议配置广播/组播报文抑制功能。

推荐配置：

- 对于没有组播业务的场景，有线下行CAPWAP ARP、IGMP、ND、other广播报文流量抑制，组播报文采用默认值。

  ```
  [AC-wlan-ap-system-prof-test] traffic-optimize broadcast-suppression arp rate-threshold 128
  [AC-wlan-ap-system-prof-test] traffic-optimize broadcast-suppression igmp rate-threshold 128
  [AC-wlan-ap-system-prof-test] traffic-optimize broadcast-suppression nd rate-threshold 128
  [AC-wlan-ap-system-prof-test] traffic-optimize broadcast-suppression other rate-threshold 128
  ```

- 对于存在组播业务的场景，如多媒体教室的视频点播业务等，建议另外配置关闭组播报文抑制功能，避免影响组播业务。


```
[AC-wlan-ap-system-prof-test] traffic-optimize broadcast-suppression other-multicast disable
```

3.3.12 安全性

- 用户隔离和端口隔离

  网络中二层广播域大，正常的广播报文（如ARP）会对网络产生冲击，对于无线网络更是如此。广播报文在无线侧发送时是以最低速率发送，会造成很大的空口资源开销，因此对于无线组网，如果没有用户二层互访的需求，建议开启二层隔离功能。开启二层隔离之后，会出现同一网段的终端之间不能进行局域网互传文件、互ping等操作。因此如果有局域网互访需求的局点，不要开启二层隔离功能。

  推荐配置：

```
# 在AC上配置用户隔离
<AC> system-view
[AC] wlan
[AC-wlan-view] traffic-profile name p1
[AC-wlan-traffic-prof-p1] user-isolate l2
Warning: Enabling user isolation may interrupt services. Are you sure you want to continue? [Y/N]:y

# 在AP上联的交换机端口上配置端口隔离。
[LSW] interface GigabitEthernet 0/0/5
[LSW-GigabitEthernet0/0/5] port-isolate enable
```

- VAP安全性

  通过在VAP模板中开启STA地址学习功能、STA地址严格DHCP获取功能、AP的IPSG功能、动态ARP检测功能，提高VAP的安全性。严格地址学习配置之后，终端侧不能设置静态IP。

  推荐配置：

```
<AC> system-view
[AC] wlan
[AC-wlan-view] vap-profile name vap1
[AC-wlan-vap-prof-vap1] learn-client-address dhcp-strict        //STA地址严格DHCP获取功能
[AC-wlan-vap-prof-vap1] ip source check user-bind enable        //AP的IPSG功能
[AC-wlan-vap-prof-vap1] arp anti-attack check user-bind enable  //动态ARP检测功能
```

3.3.13 网络管理

在网络中部署网管服务器，通过简单的操作来对设备以及网络拓扑进行管理，来实现可视化界面管理，提高操作体验和管理效率。

推荐配置：

```
<AC> system-view
[AC] snmp-agent
[AC] snmp-agent sys-info version v3
[AC] snmp-agent mib-view iso-view include iso
[AC] snmp-agent group v3 group001 privacy write-view iso-view notify-view iso-view
[AC] snmp-agent usm-user version v3 user001 group group001
[AC] snmp-agent usm-user version v3 user001 authentication-mode sha
Please configure the authentication password (8-64)
Enter Password:                 //输入认证密码
Confirm Password:               //确认认证密码
[AC] snmp-agent usm-user version v3 user001 privacy-mode aes128
Please configure the privacy password (8-64)
Enter Password:                 //输入加密密码
Confirm Password:               //确认加密密码
[AC] snmp-agent trap enable
Warning: All switches of SNMP trap/notification will be open. Continue? [Y/N]:y
[AC] snmp-agent target-host trap-paramsname NetCenter v3 securityname user001 privacy  //
securityname必须与SNMPv3用户名相同
[AC] snmp-agent target-host trap-hostname NetCenter address 10.23.1.1 udp-port 162 trap-
paramsname NetCenter
```

3.3.14 网络分析

华为CampusInsight网络智能分析平台，颠覆传统聚焦资源状态的监控方式，将人工智能应用于运维领域，基于已有的运维数据（设备性能指标、终端日志等数据），通过大数据、人工智能算法及更多高级分析技术，将网络中的用户体验数字化，辅助客户及时发现网络问题，改善用户体验。

推荐配置：

1. 配置AC的KPI和Syslog上报

```
<AC> system-view
[AC] wmi-server2
[AC-wmi-server] server ip-address ip-address port port
//ip-address和port为配置AC上报性能指标信息的目的地址和端口。CampusInsight集群场景中，ip-address为CampusInsight南向浮动IP地址；CampusInsight单机场景中，ip-address为CampusInsight南向IP地址；如172.16.1.100。port为固定值27371。
[AC-wmi-server] collect-item device-data interval 60
[AC-wmi-server] collect-item interface-data interval 60
[AC-wmi-server] collect-item cpcar-data interval 60
[AC-wmi-server] collect-item security-data interval 60
[AC-wmi-server] collect-item log-data interval 60
//配置AC设备上的各种性能指标数据采集上报到CampusInsight，设置数据采集周期。
[AC-wmi-server2] log module mid ff760000
//配置设备上报指定模块ID为ff760000的Portal2.0认证日志信息。
[AC-wmi-server2] log module mid ff5f0000
//配置设备上报指定模块ID为ff5f0000的802.1x接入日志信息。
[AC-wmi-server2] log module mid ff630000
//配置设备上报指定模块ID为ff630000的认证日志信息。
[AC-wmi-server2] log module mid fff30000
//配置设备上报指定模块ID为fff30000的离线日志信息。
[AC-wmi-server2] log module mid ff5d0000
//配置设备上报指定模块ID为ff5d0000的DHCP日志信息。
[AC-wmi-server2] log module mid ff050000
//配置设备上报指定模块ID为ff050000的端口状态日志信息。
[AC-wmi-server2] log module mid d0410000
//配置设备上报指定模块ID为d0410000的设备操作日志信息。
[AC-wmi-server2] log module mid ff5a0000
//配置设备上报指定模块ID为ff5a0000的AAA日志信息。
```

2. 配置AP的KPI和Syslog上报

   a. 开启AC主动上报STA的流量信息和在AP中的上线时长信息的功能，开启用户上线成功信息记录到日志功能。

```
[AC] wlan
[AC-wlan-view] report-sta-info enable
//使能AC主动上报STA的流量信息和在AP中的上线时长信息的功能
[AC-wlan-view] report-sta-assoc enable
//使能用户上线成功信息记录到日志功能。
```

   b. 开启AC业务体验分析SEA（Service Experience Analysis）功能。

```
[AC-wlan-view] vap-profile name default
//进入到每个vap-profile，这里以default模板为例
[AC-wlan-view-vap-prof-default] service-experience-analysis enable
//打开业务体验分析SEA功能。
[AC-wlan-view-vap-prof-default] quit
```

   c. 创建WMI模板，并配置WMI模板相关参数。

```
[AC-wlan-view] wmi-server name test
//创建WMI模板test。
[AC-wlan-wmi-server-prof-test] server ip-address 10.10.27.19 port 27371
//在模板test中配置AP上报性能指标数据的目的地址和端口。10.10.27.19为CampusInsight南向浮动IP地址；端口号为固定值27371。
[AC-wlan-wmi-server-prof-test] report-interval 60
[AC-wlan-wmi-server-prof-test] collect-item device-data interval 60
[AC-wlan-wmi-server-prof-test] collect-item radio-data interval 60
[AC-wlan-wmi-server-prof-test] collect-item terminal-data interval 60
[AC-wlan-wmi-server-prof-test] collect-item log-data interval 60
//在模板test中配置AP的各种性能指标数据采集周期为60秒。
```



```
[AC-wlan-wmi-server-prof-test] ap log module mid ff600000
//配置AP上报指定模块ID为ff600000的Https重定向日志信息。
[AC-wlan-wmi-server-prof-test] ap log module mid d0410000
// 配置AP上报指定模块ID为d0410000的设备操作日志信息。
[AC-wlan-wmi-server-prof-test] ap log module mid ff620000
// 配置AP上报指定模块ID为ff620000的DHCP日志信息。
[AC-wlan-wmi-server-prof-test] ap log module mid ffed0000
// 配置AP上报指定模块ID为ffed0000的音视频日志信息。
[AC-wlan-wmi-server-prof-test] ap log module mid ffef0000
// 配置AP上报指定模块ID为ffef0000的关联日志信息。
[AC-wlan-wmi-server-prof-test] ap log module mid fff30000
// 配置AP上报指定模块ID为fff30000的WLAN日志信息。
[AC-wlan-wmi-server-prof-test] quit
[AC-wlan-view] ap-system-profile name default
//进入到每个ap-system-profile中，以default为例。
[AC-wlan-ap-system-prof-default] wmi-server test index 2
//将WMI模板test引用到AP系统模板default。
[AC-wlan-ap-system-profile] quit
```

