# 9 漫游配置

9.1 漫游介绍
介绍漫游的定义、由来和作用。
9.2 漫游原理描述
9.3 漫游配置注意事项
9.4 漫游缺省配置
9.5 配置同一业务VLAN的AP间漫游功能
9.6 配置不同业务VLAN的AP间漫游功能
9.7 配置AC间漫游
9.8 配置敏捷分布式SFN漫游
9.9 漫游配置举例

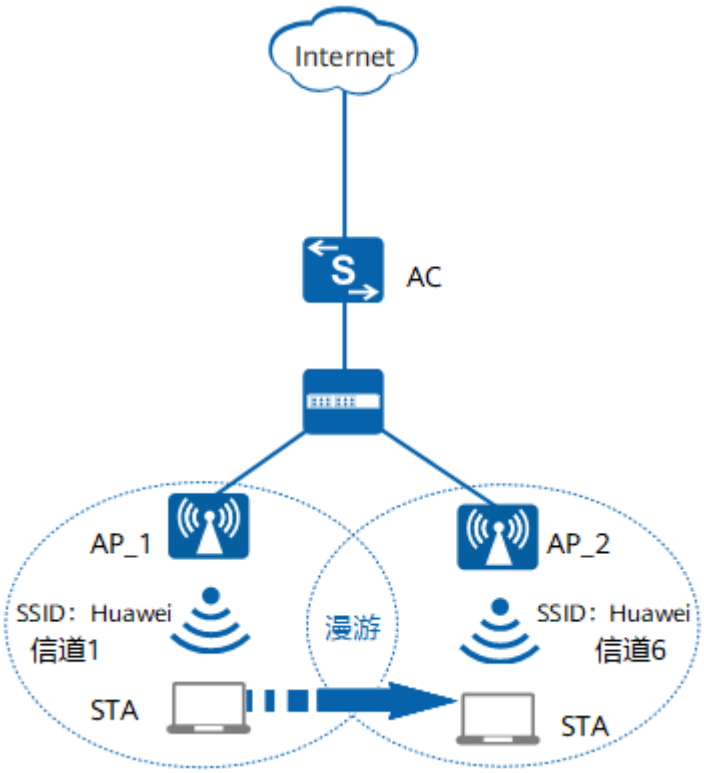
## 9.1 漫游介绍

介绍漫游的定义、由来和作用。

### 定义

WLAN漫游是指STA在同属于一个ESS内的AP之间移动且保持用户业务不中断。如**图9-1**所示，STA从AP_1的覆盖范围移动到AP_2的覆盖范围的行为就叫做漫游。

**图 9-1** WLAN 漫游组网图




WLAN漫游包括同一业务VLAN的AP间漫游和不同业务VLAN的AP间漫游：

- 同一业务VLAN的AP间漫游：STA漫游前后的AP对应同一个业务VLAN。
- 不同业务VLAN的AP间漫游：用户漫游前后的AP对应的业务VLAN不同。为了保证漫游过程中用户业务不中断，必须保持用户的业务VLAN不变，即数据报文的VLAN仍然为切换前VLAN，而不是切换后AP对应的VLAN。

## WLAN 漫游类型比较

**表 9-1** WLAN 漫游类型比较

| 漫游类型 | 是否需要STA支持 | 适用安全策略 |
| --- | --- | --- |
| 普通漫游 | 不涉及 | 所有安全策略 |
| PMK快速漫游 | 是 | WPA2–802.1X/<br>WPA3-802.1X |
| 802.11r漫游 | 是 | 开放式系统认证/WPA2–PSK/WPA2–802.1X |

| 漫游类型 | 描述 |
| --- | --- |
| 普通漫游 | 适用所有场景，配置简单，漫游过程中业务可能有短暂中断。 |
| PMK快速漫游 | 适用场景较少，漫游时省略了802.1X认证过程，只需要密钥协商，延时较低。 |
| 802.11r漫游 | 适用场景较多，漫游时省略了认证和密钥协商过程，延时低。 |

### 目的

WLAN网络的最大优势就是STA不受物理介质所处位置的影响，可以在WLAN覆盖范围内四处移动，这样就需要STA在移动过程中能够保持业务不中断，WLAN漫游技术因此而产生。同一个ESS内包含多个AP设备，当STA从一个AP覆盖区域移动到另外一个AP覆盖区域时，利用WLAN漫游技术可以实现STA用户业务的平滑过渡。

WLAN漫游解决了以下问题：

- 避免漫游过程中用户的认证时间过长而导致数据丢包甚至业务中断。

  如果STA接入Internet需要用户接入认证，认证过程（例如802.1X认证）时间较长。快速漫游避免STA重新认证的过程，保证了用户业务不中断。
- 保证用户IP地址不变。

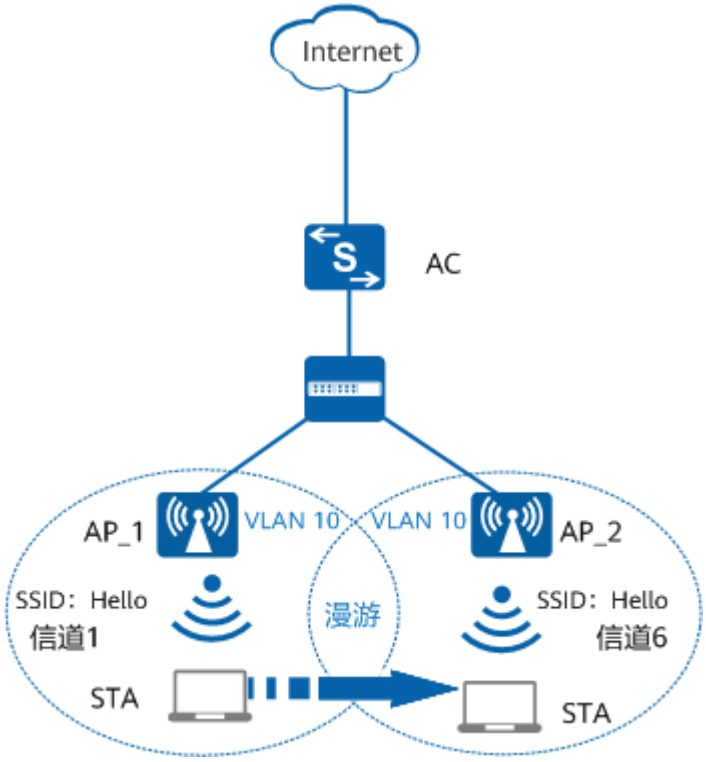
  应用层协议是以IP地址和TCP/UDP协议承载用户业务，漫游后的用户必须能够保持原IP地址不变，对应的TCP/UDP连接才能不中断，应用层数据才能保持正常转发。

## 9.2 漫游原理描述

### 9.2.1 同一业务 VLAN 的 AP 间漫游

同一业务VLAN的AP间漫游是针对同一AC下对应同一业务VLAN的AP，STA从一个AP的覆盖范围移动到另一个AP的覆盖范围时保持业务不中断，如图9-2所示。

**图 9-2** 同一业务 VLAN 的 AP 间漫游组网图




根据用户是否支持PMK快速漫游，可以将同一业务VLAN的AP间漫游分为PMK快速漫游和非快速漫游两种方式。

## 非快速漫游原理

当用户使用的安全策略不是WPA2-802.1X、WPA3-802.1X时，用户的漫游都属于非快速漫游。此外，如果用户使用的是WPA2-802.1X、WPA3-802.1X的安全策略，但STA不支持PMK快速漫游，则该漫游仍然不属于快速漫游，用户仍需要完成802.1X认证过程才能完成漫游。

**说明**

实现WLAN漫游的各AP必须使用相同的SSID（例如，图9-2所示的SSID都为Hello）和安全模板（安全模板名称可以不同，但是安全模板下的配置必须相同）。

如图9-2所示，STA已经通过AP_1接入Internet。此时，STA需要从AP_1的覆盖范围移动到AP_2的覆盖范围，按照如下的流程实现漫游功能：

1. STA在各个信道中发送探测请求帧，周围AP收到该请求帧后发送回应帧进行响应。例如，AP_2在信道6（AP_2使用的信道）中收到请求后，通过在信道6中发送应答帧来进行响应。STA收到周围各AP的应答帧后，根据信号强度、信号质量等信息进行评估，确定与哪个AP关联最合适。假设如图9-2所示的，STA最终确定跟AP_2关联。
2. STA通过信道6向AP_2发送重认证请求，认证成功后，AP_2向STA返回重认证响应。
3. STA向AP_2发送重关联请求，AP_2收到后上报AC，AC使用重关联响应做出应答，建立STA与AP_2间的关联。
4. STA与AP_2关联成功后，删除STA与AP_1的连接。STA通过信道1（AP_1使用的信道）向AP_1发送802.11解除关联信息，解除STA与AP_1间的关联。

- 如果用户使用的安全策略是WEP，此时，漫游过程已经完成。
- 如果用户使用的安全策略是WPA/WPA2-PSK或WPA/WPA2-802.1X，STA还需要重新进行接入认证和密钥协商。密钥协商的详细内容请参见**14.1.2 WPA/WPA2**中的“**密钥协商阶段**”。

### PMK 快速漫游原理

当用户使用WPA2-802.1X、WPA3-802.1X安全策略，且STA支持PMK快速漫游技术时，用户在漫游过程中不需要重新完成802.1X认证过程，只需要完成密钥协商过程即可。这样，通过PMK快速漫游，可以缩短802.1X用户的漫游延时，提升用户上网体验。

快速漫游是通过成对主密钥PMK（Pairwise Master Key）缓存技术实现的。如**图9-2**所示，快速漫游的实现原理如下：

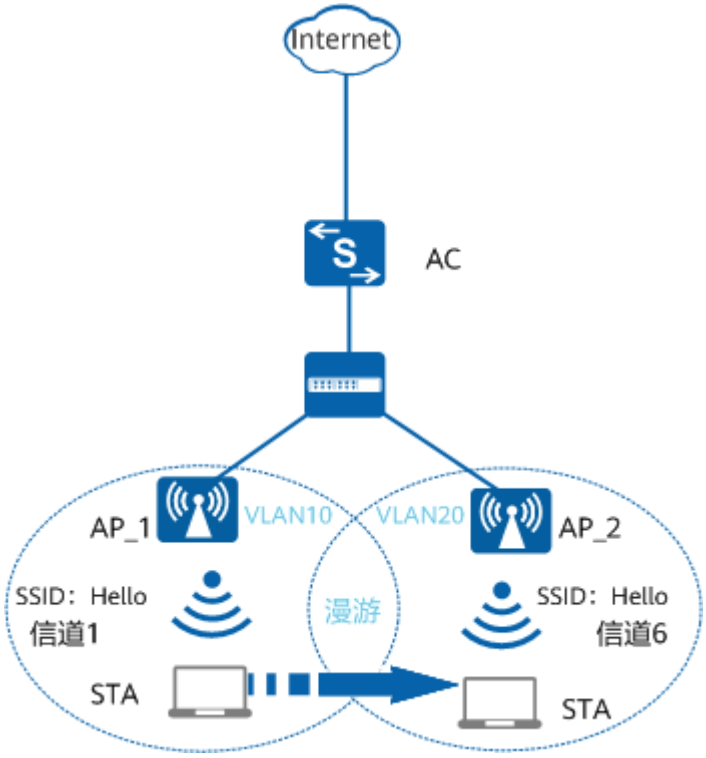
1. STA首次通过AP_1接入Internet时，当STA与AC认证成功生成PMK后，STA和AC分别保存PMK信息，每个PMK信息对应一个PMK-ID，PMK-ID是由PMK、SSID、STA的MAC地址和BSSID计算出来的。
2. 当STA在漫游过程中向AP_2发起重关联请求时，重关联请求帧中包含了PMK-ID信息。
3. AP_2收到请求后及时向AC通报用户切换消息。
4. AC根据STA携带的PMK-ID信息查找PMK缓存表中STA对应的PMK，如果查找到，就认为STA已经进行过802.1X认证，直接跳过认证过程，利用缓存的PMK开始进行密钥协商。

## 9.2.2 不同业务 VLAN 的 AP 间漫游

类似于有线局域网，为了避免广播风暴，企业内部的WLAN网络也会根据楼层、部门等将不同用户群划分到不同VLAN。假设不同楼层部署的AP所属VLAN不同，当用户从一个楼层AP覆盖范围移动到另外一个楼层AP覆盖范围时，就会导致用户业务中断。为了提升用户体验，产生了跨VLAN的三层漫游技术。

不同业务VLAN的AP间漫游是指用户漫游前后的AP对应的业务VLAN不同。为了保证漫游过程中业务VLAN不中断，必须保持用户的VLAN不变，即数据报文的VLAN仍然为切换前VLAN，而不是切换后AP的VLAN。

**图 9-3** 不同业务 VLAN 的 AP 间漫游组网图




根据用户是否支持快速漫游，可以将同一业务VLAN的AP间漫游分为快速漫游和非快速漫游两种方式，其实现原理请参见**9.2.1 同一业务VLAN的AP间漫游**。以下通过**图9-3**说明下STA漫游过程中是如何保证业务VLAN不变的。

如**图9-3**所示，用户的漫游过程为：

1. STA通过AP_1（属于VLAN10）接入Internet时，AC判断该STA为首次接入用户，为其创建并保存相关的业务数据信息(包括AP所属的业务VLAN、AP名称、射频以及VAP信息等)。
2. STA从AP_1覆盖区域向AP_2（属于VLAN20）覆盖区域移动时，STA通过AP_2重新与AC进行关联，AC通过业务数据信息判断该STA为漫游用户，更新业务数据库信息，将AP名称、射频以及VAP信息更新为切换后AP_2的信息，但是VLAN ID保持不变，仍然为切换前AP_1所属的业务VLAN。
3. STA断开与AP_1的关联。尽管漫游前后不在同一个子网中，AC仍然把STA视为从原始子网（VLAN10）接入，允许STA保持原有IP以保证用户业务不中断。

## 9.2.3 AC 间漫游

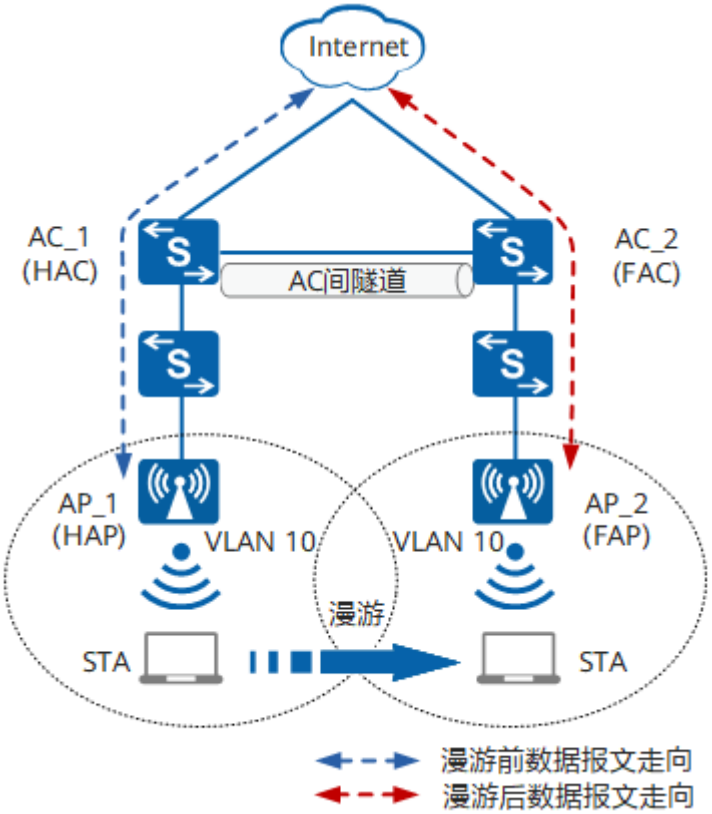
### 网络架构

WLAN AC间漫游的网络架构如**图9-4**所示。WLAN网络通过AC_1和AC_2两个AC对AP进行管理，其中AP_1与AC_1进行关联，AP_2与AC_2进行关联。现STA在WLAN网络中进行漫游，漫游过程中与不同的AP进行关联，漫游过程如下：

STA从AP_1覆盖范围漫游到AP_2覆盖范围的过程中，因为AP_1和AP_2分别与AC_1和AC_2关联，漫游需要跨越不同的AC，所以此次漫游为**AC间漫游**。AP_1即为STA的**HAP**，AC_1即为STA的**HAC**，AP_2即为STA的**FAP**，AC_2即为STA的**FAC**。AC间漫游

的前提是AC_1和AC_2分配到同一个**漫游组**内，只有同一个漫游组内的AC间才能进行漫游，漫游组内的AC可以通过**AC间隧道**进行数据同步和报文转发。

**图 9-4** 网络架构




- **HAC**（Home AC）：一个无线终端首次与某个AC进行关联，该AC即为它的HAC，如图9-4所示，AC_1即为STA的HAC。
- **HAP**（Home AP）：一个无线终端首次与某个AP进行关联，该AP即为它的HAP，如图9-4所示，AP_1即为STA的HAP。
- **FAC**（Foreign AC）：一个无线终端漫游后关联的AC即为它的FAC，如图9-4所示，AC_2即为STA的FAC。
- **FAP**（Foreign AP）：一个无线终端漫游后关联的AP即为它的FAP，如图9-4所示，AP_2即为STA的FAP。
- **AC间漫游**：如果漫游过程中关联的不是同一个AC，这次漫游就是AC间漫游，如图9-4所示，STA在从AP_1漫游到AP_2的过程即为AC间漫游。
- **漫游组**：在WLAN网络中，可以对不同的AC进行分组，STA可以在同一个组的AC间进行漫游，这个组就叫漫游组。
- **AC间隧道**：为了支持AC间漫游，漫游组内的所有AC需要同步每个AC管理的STA和AP设备的信息，因此在AC间建立一条隧道作为数据同步和报文转发的通道。AC间隧道也是利用CAPWAP协议创建的。如图9-4所示，AC_1和AC_2间建立AC间隧道进行数据同步和报文转发。

### 二层漫游

如图9-4所示，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。

| 漫游前 | 漫游后 |
| --- | --- |
| 1. STA发送业务报文给HAP<br>2. HAP接收到STA发送的业务报文并发送给HAC<br>3. HAC直接将业务报文发送给上层网络 | 1. STA发送业务报文给FAP<br>2. FAP接收到STA发送的业务报文并发送给FAC<br>3. FAC直接将业务报文发送给上层网络 |

## 9.2.4 802.11r 快速漫游

802.11r协议定义了在同一MD（Mobility Domain）中，通过FT（Fast BSS Transition）功能省略了用户漫游过程中的802.1X认证和密钥协商，减少信息交互次数，从而实现漫游过程中业务数据流低延时，用户不会感知业务中断，提高用户上网体验。

### AC 内 802.11r 快速漫游

AC内802.11r快速漫游过程如下。

**图 9-5** AC 内 802.11r 快速漫游过程示意（Over-the-Air 方式）

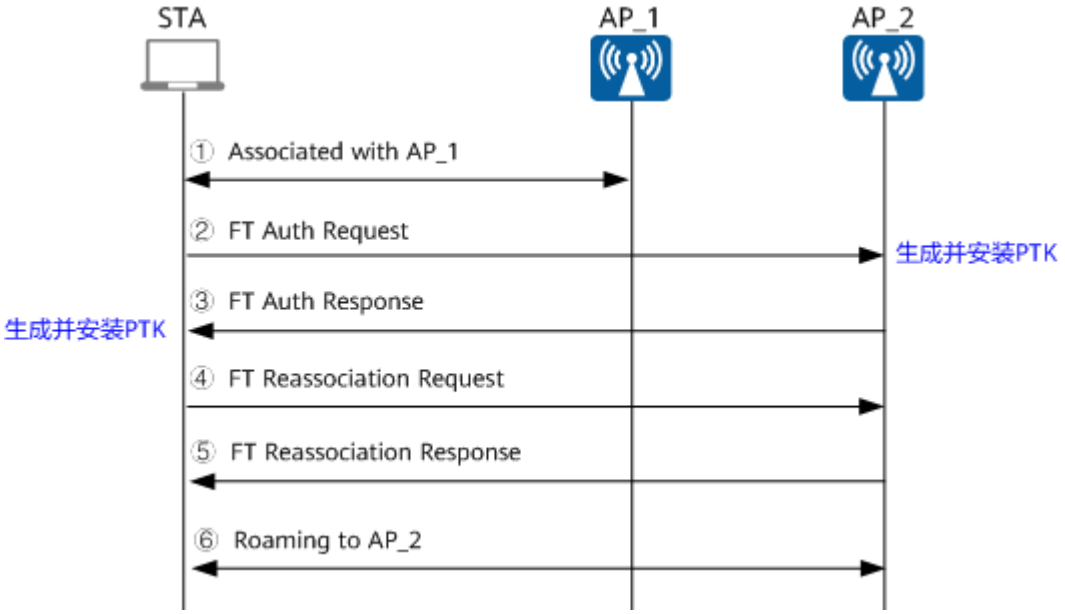
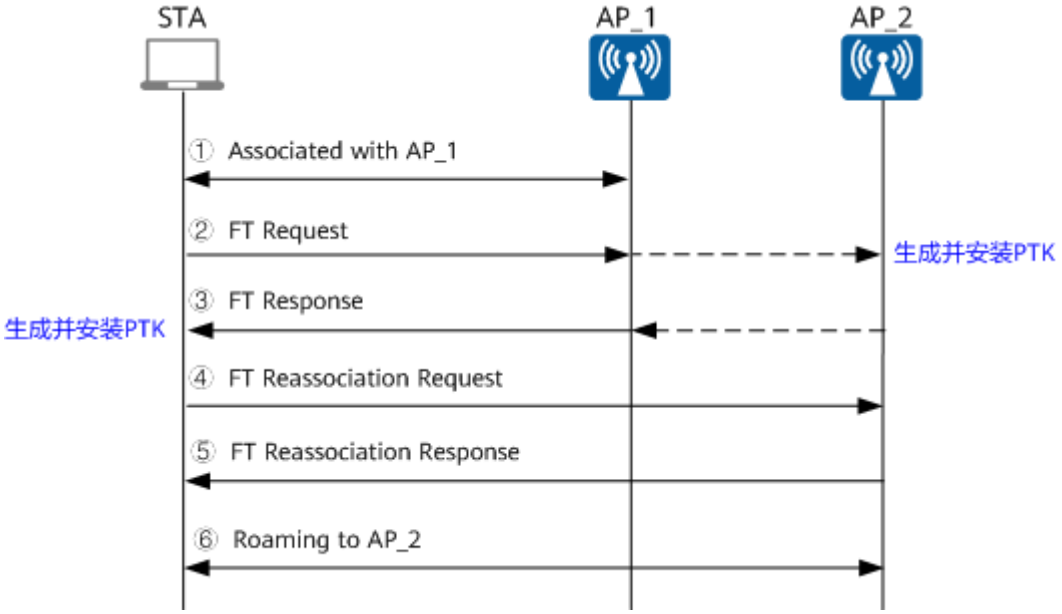


**图 9-6** AC 内 802.11r 快速漫游过程示意（Over-the-DS 方式）




**说明**

根据协议标准定义，802.11r快速漫游包括如下两种方式：

- Over-the-Air方式：STA直接与FAP（AP_2）进行FT认证。
- Over-the-DS方式：STA通过HAP（AP_1）与FAP（AP_2）进行FT认证。

1. STA首次通过AP_1接入网络时，STA与AC认证成功并生成PMK。
   a. AC根据PMK生成PMK-R0（由SSID、MDID、AC的MAC地址和STA的MAC地址计算得来）和每个AP对应的PMK-R1（由PMK-R0、AP的MAC地址和STA的MAC地址计算得来），并将PMK-R1下发给AP_1。
   b. STA和AC通过密钥协商的四次握手和二次握手分别生成并安装PTK和GTK。
   如果是开放式系统认证，不会生成PMK。
2. STA在漫游过程中向AP_2发起FT认证请求，并将PMK-R1下发给AP_2。
3. AP_2收到请求后，根据其中包含的信息和PMK-R1生成并安装PTK，同时启动重关联定时器，向STA发送802.11 FT认证应答。

   **说明**

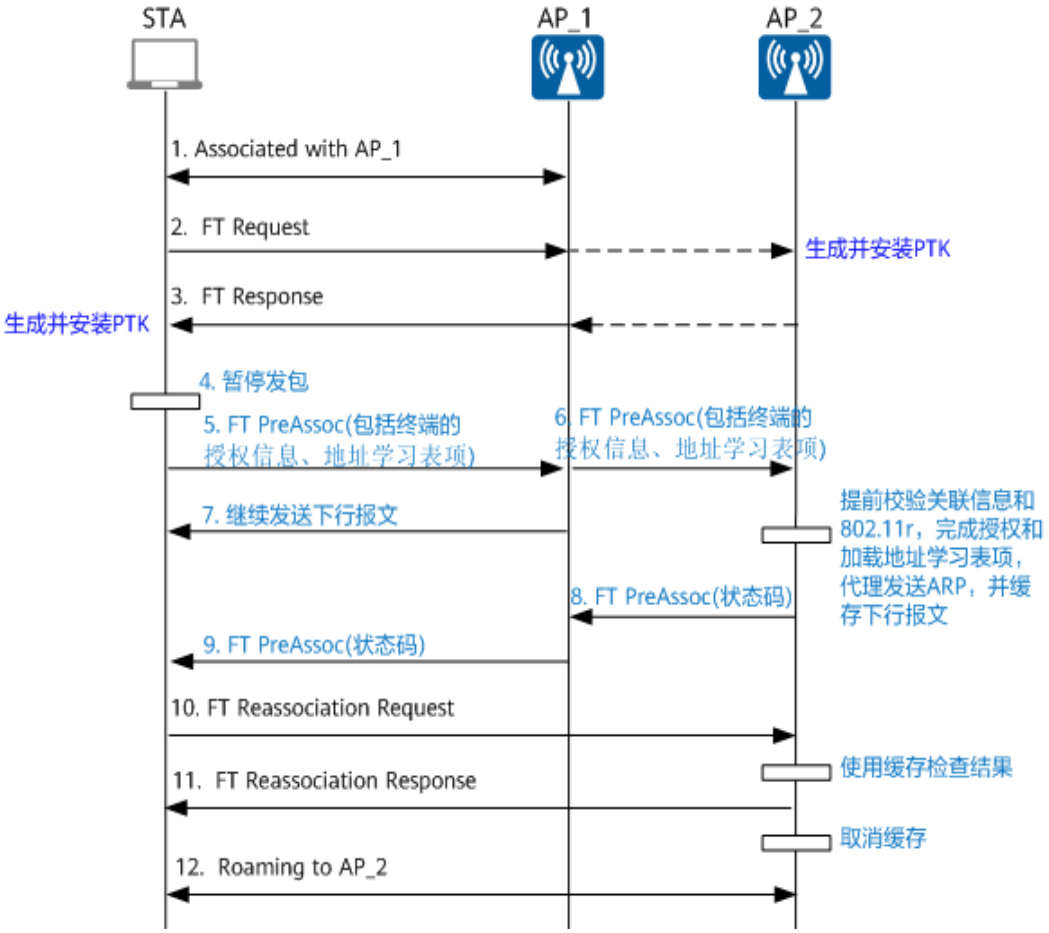
   如果是802.1X认证，在FT认证过程中，AP会向AC上报认证信息，等待AC处理。如果是开放式系统认证或PSK认证，则AP不会上报信息。
4. STA收到应答后，根据其中包含的信息生成并安装PTK。STA向AP_2发起重关联请求。
5. AP_2收到重关联请求后，关闭重关联定时器，并向STA发送重关联应答。
   如果AC配置了STA黑白名单，在FT重关联过程中，AP会先向STA发送重关联应答，然后向AC上报STA的重关联请求，等待AC处理。
6. STA收到应答后，完成漫游。

## 华为私有 802.11r 漫游（端管协同）

受限于Wi-Fi自身特点，以及不同终端在WLAN网络中行为的差异性，终端在WLAN网络中的实际漫游体验参差不齐，音视频、游戏等时延敏感业务的漫游体验往往无法得

到有效保障。由于终端（“端”）与AP（“管”）之间的漫游优化策略存在差异和冲突，单方面优化“端”或“管”无法从根本上解决问题。AirEngine系列AP（AirEngine 5760-10除外）与部分华为终端（如P40、P40 Pro、Mate 40、Mate 40 Pro、Mate 40 Pro+、Mate 40 RS、Mate X2、麒麟版P50 Pro等，以终端实际能力为准）进行了协同优化，通过开启华为私有802.11r功能，AP可以在Beacon帧和Probe Response帧中携带互通IE（Information Element），与华为终端之间按约定的报文格式和交互动作进行漫游协商，实现“端”与“管”之间的互信互通，减少漫游协商过程中的资源开销，从而有效提升漫游体验。

**图 9-7** 华为私有 802.11r 漫游（端管协同）




## 9.2.5 敏捷分布式 SFN 漫游

### 简介

在医疗场景中，由于医护人员的医疗手持终端不支持802.11k/802.11v/802.11r协议，因此在移动查房过程中通过手持医疗终端进行病房巡视、输液核对、生命体征录入等业务时终端漫游主动性较差，容易出现丢包或延时大的问题，导致需重新登录应用软件或重新扫码，上网业务被中断，严重影响医护人员的工作效率。

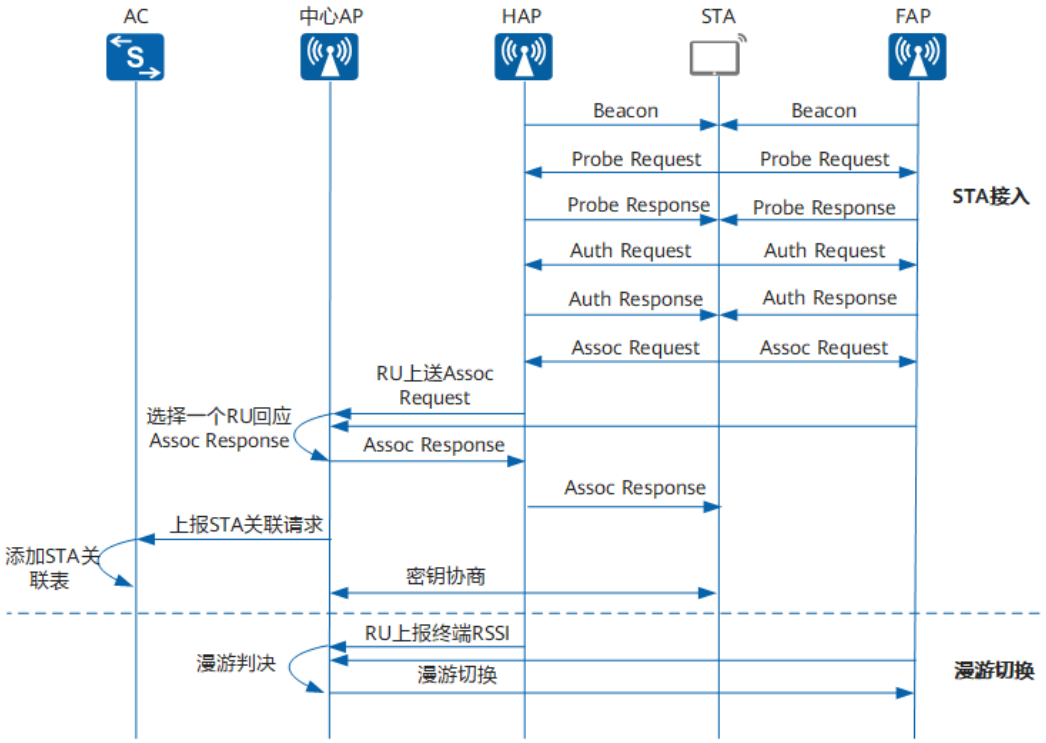
通过敏捷分布式SFN（Same Frequency Network）漫游功能，可以解决上述问题。敏捷分布式SFN漫游是指在敏捷分布式WLAN组网中，一个中心AP内的所有RU部署在相同工作信道上并使用公共BSSID和终端通信，终端在同一个SSID信号覆盖范围内自由移动时漫游无感知、业务不中断的漫游体验功能。

相比传统的中心AP内漫游，敏捷分布式SFN漫游屏蔽了终端差异对漫游效果的影响，同时在漫游切换阶段省去了用户重关联、认证及密钥协商的过程，漫游切换平滑且速度快，并且大大降低了丢包概率。

## 敏捷分布式 SFN 漫游实现机制

敏捷分布式SFN漫游实现机制如图9-8所示。

**图 9-8** 敏捷分布式 SFN 漫游实现机制示意图




敏捷分布式SFN漫游实现机制分为STA接入阶段和漫游切换阶段。

- STA接入阶段
  a. 所有RU采用中心AP根据MAC地址自动生成的公共BSSID向STA广播发送Beacon帧。
  b. STA发送Probe Request，所有RU收到Probe Request后均用公共BSSID回复Probe Response。
  c. STA发送Auth Request，所有RU收到Auth Request后均用公共BSSID回复Auth Response。
  d. STA发起Assoc Request，所有RU收到该Assoc Request后均上送至中心AP处理，并上报STA的SNR给中心AP。
  e. 中心AP选定一个SNR最优的RU回复Assoc Response，同时在一定时间内再次收到其他RU上报的Assoc Request报文做丢弃处理。后续只有被选定的RU和STA通信。
  f. 中心AP向AC上报STA关联请求，AC将STA信息添加到用户关联表。
  g. 中心AP、RU和STA进行单播和组播密钥协商。

- 漫游切换阶段
  a. HAP（首次关联的RU）周期性上报终端RSSI给中心AP，FAP（漫游后关联的RU）周期性上报邻居RSSI给中心AP。
  b. 中心AP通过漫游判断算法选择一个最优的RU作为漫游切换的FAP，然后同步终端信息给FAP。中心AP周期性依次判断以下三个切换条件是否满足，当符合任意一个切换条件时，即可以发生漫游切换，如果有多个RU同时满足以下三个条件，则选择信号强度最强的RU进行漫游切换。
     i. 终端RSSI累积变化值达到指定阈值。
     ii. 周边RU信号强度优于当前RU信号强度的次数达到配置的值。
     iii. 周边RU相比当前RU的信号强度差值达到配置的差值。

## 敏捷分布式 SFN 漫游报文处理流程

假设业务数据报文直接转发，敏捷分布式SFN漫游网络中内、外网数据报文处理流程如图9-9所示。业务数据报文隧道转发时，内、外网数据报文在RU和中心AP间的转发和直接转发时无差异。

**图 9-9** 敏捷分布式 SFN 漫游报文处理流程图

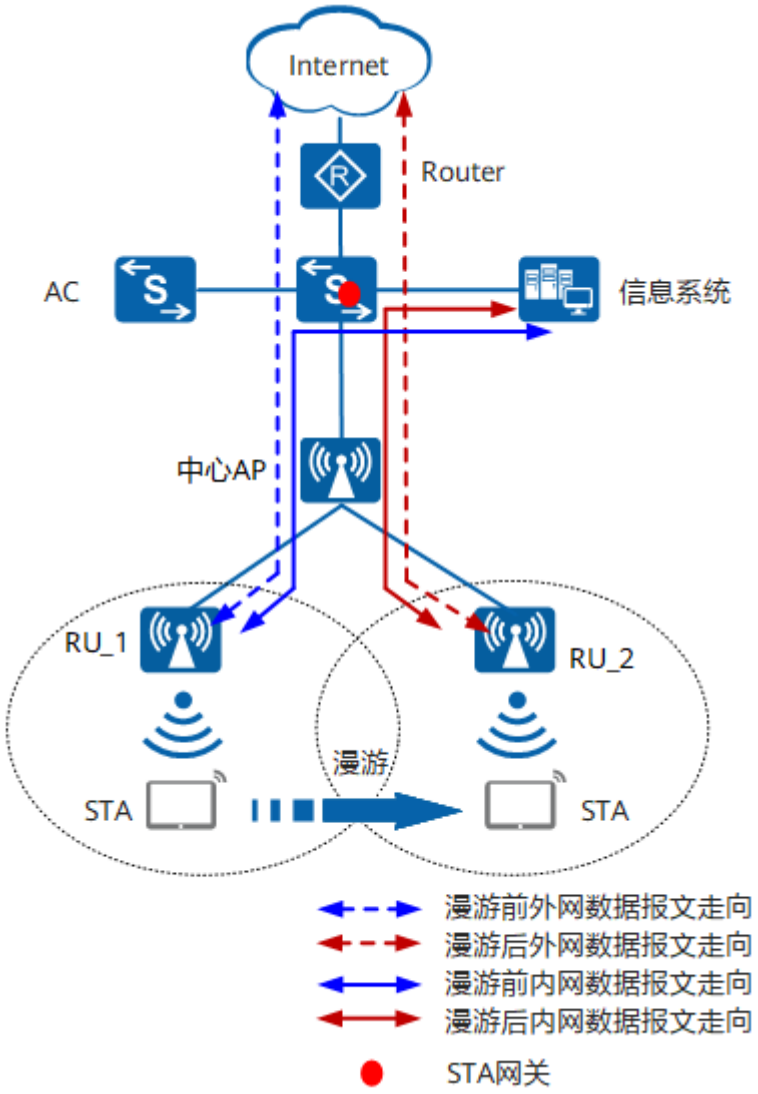


**表 9-2** 内网数据报文走向

| 漫游前 | 漫游后 |
| --- | --- |
| 1. STA发送业务报文给RU_1<br>2. RU_1接收到STA发送的业务报文并发送给中心AP<br>3. 中心AP接收到STA发送的业务报文通过用户网关发送给上层网络 | 1. STA发送业务报文给RU_2<br>2. RU_2接收到STA发送的业务报文并发送给中心AP<br>3. 中心AP接收到STA发送的业务报文通过用户网关发送给上层网络 |

**表 9-3** 外网数据报文走向

| 漫游前 | 漫游后 |
| --- | --- |
| 1. STA发送业务报文给RU_1<br>2. RU_1接收到STA发送的业务报文并发送给中心AP<br>3. 中心AP接收到STA发送的业务报文通过用户网关和出口路由发送给上层网络 | 1. STA发送业务报文给RU_2<br>2. RU_2接收到STA发送的业务报文并发送给中心AP<br>3. 中心AP接收到STA发送的业务报文通过用户网关和出口路由发送给上层网络 |

# 9.3 漫游配置注意事项

## 涉及网元

**AP**

- 本配置指南中提到的AP，均为华为公司的AP产品。推荐用户选择华为公司的AP设备与AC对接。
- 执行命令**display ap-type all**，可以查看设备缺省支持的AP设备类型。
- AC与AP之间的版本配套关系请参见**WLAN AP版本配套和形态速查表**。

**客户端**

- 配置快速漫游时，需要客户端支持快速漫游技术。

## License 支持

设备作为WLAN AC时，支持在线的AP数目受license控制。加载license之前，设备最多可以支持16个AP在线，如果需要增加在线AP的数目，请联系代理商申请并购买license：

- WLAN无线接入控制器AP资源授权-1AP
- WLAN无线接入控制器AP资源授权-16AP
- WLAN无线接入控制器AP资源授权-32AP
- WLAN无线接入控制器AP资源授权-64AP

- WLAN无线接入控制器AP资源授权-128AP
- WLAN无线接入控制器AP资源授权-512AP

License申请方法请参见《S1720, S5700, S6700系列交换机 License使用指南》中的“申请License”。

## V200R021C00、V200R021C01 版本特性支持情况

仅如下款型支持本特性：S5731-H、S5731-H-K、S5731S-H、S5732-H、S5732-H-K、S6730-H、S6730-H-K、S6730S-H。

## 特性依赖和限制

- 实现WLAN漫游的两个AP必须使用相同的SSID和安全模板（安全模板名称可以不同，但是安全模板下的配置必须相同），认证模板的认证方式和认证参数也要配置相同。
- 直接转发模式下，用户漫游后，与AP相连的接入设备的ARP表项未及时老化，会造成用户业务短暂中断，建议用户在AC上使能STA地址学习功能，AP会及时发送免费ARP报文给接入设备刷新ARP表项，保证漫游过程中用户业务不中断。

  使能STA地址学习功能的方法：
  - 在服务集视图下执行命令**learn client ip-address enable**
- 802.11r功能支持的安全策略包括开放式系统认证、WPA2+PSK+AES、WPA2+PPSK+AES和WPA2+802.1X+AES。
- 802.11r快速漫游与PMF功能互斥，即如果已配置了802.11r快速漫游，不能再配置PMF功能。
- 不兼容802.11r协议的终端无法关联使能了802.11r功能的WLAN网络。可以更换支持802.11r协议的终端，或者通过创建两个相同SSID的VAP，一个使能802.11r功能，另一个去使能，而其它配置均相同，便于用户正常使用网络服务。
- 802.11r使用802.1X认证时，如果开启了802.1X重认证功能，部分终端可能因兼容性问题，在重认证阶段掉线后重新上线。
- 部分终端可能与802.11r漫游功能存在兼容性问题，导致漫游失败。不建议开启802.11r漫游功能。
- 配置不同业务VLAN的AP间漫游时，请确保业务VLAN的网关在同一设备节点上。
- 如下AP不支持AGV漫游功能。
  - AirEngine x762系列AP
- 配置敏捷分布式SFN漫游功能时需注意：
  - 网络规划注意事项：
    - 支持敏捷分布式SFN漫游功能的款型仅包括AD9430DN-12（含配套RU）和AD9430DN-24（含配套RU）。其中，仅以下RU组合支持敏捷分布式SFN漫游：
      - R230D和R240D间，并且，R230D和R240D仅2.4G射频支持敏捷分布式SFN漫游，5G射频不支持。
      - R250D、R250D-E、R251D、R251D-E和R450D间。
    - 对于整个中心AP，开启敏捷分布式SFN漫游功能后，所有RU单频段（2.4G或5G）上支持的同频漫游终端数总数不超过128，单频段内其它VAP上终端总数不超过128。

- 开启敏捷分布式SFN漫游功能后，所有RU需配置在同一信道。在5G频段开启敏捷分布式SFN漫游时，需将信道配置在非雷达信道。
- 参与漫游的各个RU需要关联在同一中心AP上。不支持跨中心AP的敏捷分布式SFN漫游。
- RU间的漫游为中心AP内二层漫游。不支持三层漫游场景下的敏捷分布式SFN漫游。

– 配置注意事项：

- 如果2.4G或5G射频同时开启敏捷分布式SFN漫游，则建议使用不同的SSID，否则可能导致STA切换射频，影响用户体验。
- 一个射频上只能有一个VAP使能敏捷分布式SFN漫游功能。如果一个射频上配置了多个VAP，建议在没有配置敏捷分布式SFN漫游的所有VAP上配置VAP限速总和为5Mbps。

  **说明**

  如果AP组的某个射频上有VAP使能了敏捷分布式SFN漫游功能，则在对应中心AP下关联到该射频的所有STA的漫游轨迹均可能会带有s标记。

- 开启敏捷分布式SFN漫游功能的射频上不能再配置信道扫描、信道调优和智能漫游。
- 敏捷分布式SFN漫游不支持AP个性化配置，只能基于AP组配置。
- 参与漫游的各个RU需要配置：
  - 相同的SSID。
  - 相同的VAP模板，且VAP ID必须相同。
  - 相同的安全策略。敏捷分布式SFN漫游支持的加密方式包括WPA+PSK、WPA2+PSK、WPA-WPA2+PSK、WPA+802.1X（EAP认证）、WPA2+802.1X（EAP认证）、WPA-WPA2+802.1X（EAP认证）和Portal+PSK。

- 配置AC间漫游功能时需注意：
  – 仅VXLAN分布式网关组网场景下支持AC间漫游，且仅支持AC间二层漫游。
  – 同一漫游组内的AC必须使用相同的软件VRC版本，否则可能会导致AC间漫游失败。
  – 漫游组内每个AC上均需要配置AC间建链的IP地址、漫游组，并添加成员AC。
  – 配置的漫游组内AC间建链的IP地址必须是AC的CAPWAP源IP地址。当配置了多个CAPWAP源地址时，仅可以指定一个CAPWAP源地址作为AC间建链地址。
  – 每个AC上漫游组名称必须一致。
  – 漫游组内最多可以添加16个AC成员，AC一次只能加入到一个漫游组中，不可以同时加入多个漫游组。
  – WLAN AC和交换机之间不支持AC间漫游。

# 9.4 漫游缺省配置

**表 9-4** 漫游的缺省配置

| 参数 | 缺省值 |
| --- | --- |
| AC内跨VLAN漫游功能 | 使能 |
| AC间漫游功能 | 未使能 |
| 802.11r漫游功能 | 未使能 |
| 敏捷分布式SFN漫游功能 | 未使能 |

# 9.5 配置同一业务 VLAN 的 AP 间漫游功能

## 前置任务

如果相邻AP的业务VLAN相同，通过配置同一业务VLAN的AP间漫游功能，用户从一个AP覆盖范围移动到另外一个AP的覆盖范围时，可以实现用户业务不中断。

配置同一业务VLAN的AP间漫游功能前，需要完成以下任务

- **配置WLAN基本业务**
- 参与漫游的各个AP需要满足：
  - 关联在同一AC上
  - 配置相同的安全策略
  - 配置相同的SSID
  - 配置相同的业务VLAN

## 配置流程

以下配置任务为并列关系，请根据实际情况选择其中一种进行配置。

# 9.5.1 配置同一业务 VLAN 的 AP 间非快速漫游功能

## 操作步骤

**步骤1** 配置非快速漫游：

AP可以配置如下的任何一种安全策略：

- WEP(开放系统认证)
- WEP(共享密钥认证)
- WPA/WPA2-PSK
- WPA-802.1X

- WPA2-802.1X，并且STA不支持PMK快速漫游技术
- WPA3-802.1X，并且STA不支持PMK快速漫游技术

基本业务配置完成后，STA就可以实现非快速漫游。

**----结束**

## 9.5.2 配置同一业务 VLAN 的 AP 间 PMK 快速漫游功能

### 操作步骤

**步骤1** 配置PMK快速漫游：

要配置PMK快速漫游，STA必须支持PMK快速漫游技术，且参与漫游的各AP上配置的安全策略必须是WPA2-802.1X或WPA3-802.1X。基本业务配置完成后，STA就可以实现PMK快速漫游。

**----结束**

## 9.5.3 （可选）配置 802.11r 漫游

### 操作步骤

**步骤1** 执行命令**system-view**，进入系统视图。

**步骤2** 执行命令**wlan**，进入WLAN视图。

**步骤3** 执行命令**ssid-profile name** *profile-name*，进入SSID模板视图。

**步骤4** 执行命令**dot11r enable** [ **over-the-ds** ]，开启802.11r功能。

缺省情况下，802.11r功能未开启。

**步骤5** 执行命令**dot11r proprietary**，开启华为私有802.11r功能。

缺省情况下，华为私有802.11r功能未开启。

**步骤6** 执行命令**dot11r reassociate-timeout** *time*，配置802.11r重关联超时时间。

缺省情况下，802.11r重关联超时时间为1s。

**步骤7** 执行命令**quit**，返回WLAN视图。

**步骤8** 执行命令**vap-profile name** *profile-name*，进入VAP模板视图。

**步骤9** 执行命令**ssid-profile** *profile-name*，在VAP模板中引用SSID模板。

缺省情况下，VAP模板下引用名为**default**的SSID模板。

**----结束**

### 检查配置结果

- 执行命令**display ssid-profile** { **all** | **name** *profile-name* }，查看SSID模板中802.11r功能相关的信息。

### 9.5.4 检查配置结果

#### 操作步骤

- 执行命令**display station roam-track sta-mac** *mac-address*，查看指定STA的漫游轨迹。
- 执行命令**display station sta-mac** *mac-address*，查看指定STA的接入信息，以便了解该STA关联的AP是否发生了变化。

**----结束**

## 9.6 配置不同业务 VLAN 的 AP 间漫游功能

### 前置任务

如果相邻AP的业务VLAN不同，通过配置不同业务VLAN的AP间漫游功能，用户从一个AP覆盖范围移动到另外一个AP的覆盖范围时，可以实现用户业务不中断。

配置不同业务VLAN的AP间漫游功能前，需要完成以下任务

- **配置WLAN基本业务**
- 参与漫游的各个AP需要满足：
  - 关联在同一AC上
  - 配置相同的安全策略
  - 配置相同的SSID
  - 配置不同的业务VLAN

### 背景信息

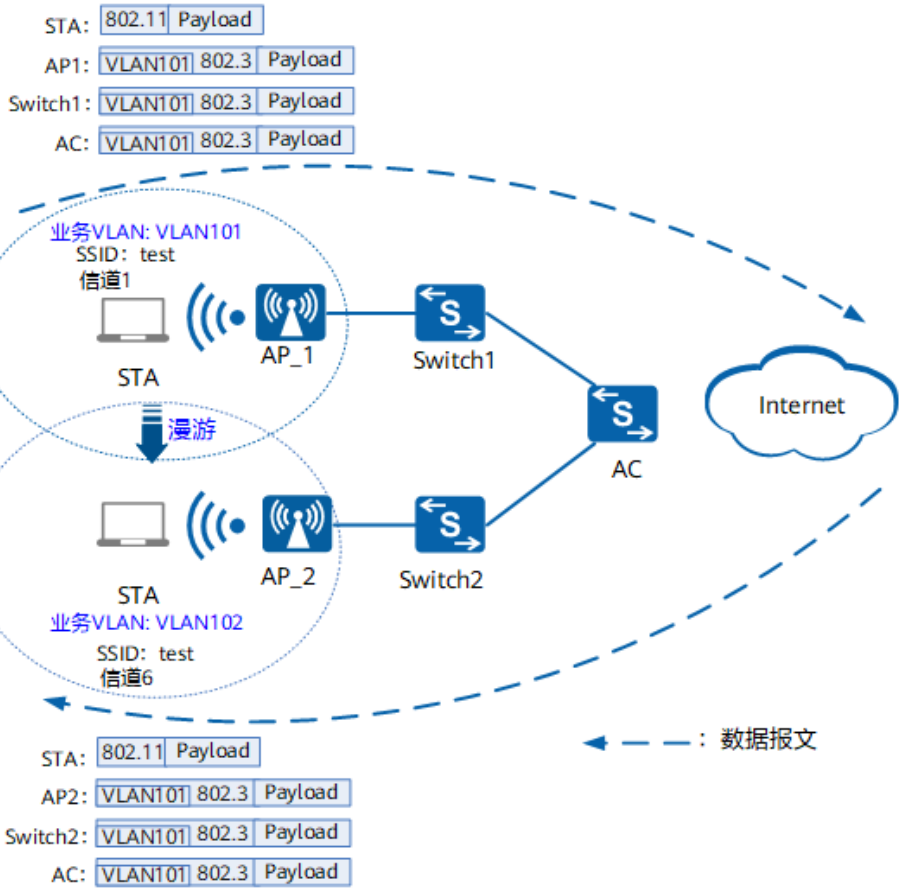
由于漫游前后AP的业务VLAN不同，在实现不同业务VLAN的AP间漫游时，需要做到STA切换AP后的数据报文的VLAN仍然是漫游前的业务VLAN。因此，针对直接转发和隧道转发模式，VLAN的配置有所不同。本文以AP与AC间二层组网为例，介绍VLAN的配置区别。

- 直接转发模式

  如**图9-10**所示，直接转发模式下，用户从AP_1漫游到AP_2时，当数据报文到达AP_2后，AP_2将数据报文打上VLAN101的标签，并向上层网络转发报文。反之，如果用户从AP_2漫游到AP_1时，当数据报文到达AP_1后，AP_1将数据报文打上VLAN102的标签，并向上层网络转发报文。

**图 9-10** 直接转发模式的不同业务 VLAN 的 AP 间漫游组网图




因此，如果采用直接转发模式，AP与AC之间的交换机Switch1和Switch2、AC上的接口（包括AC的下行接口、上行接口）都要配置允许VLAN101和VLAN102通过。

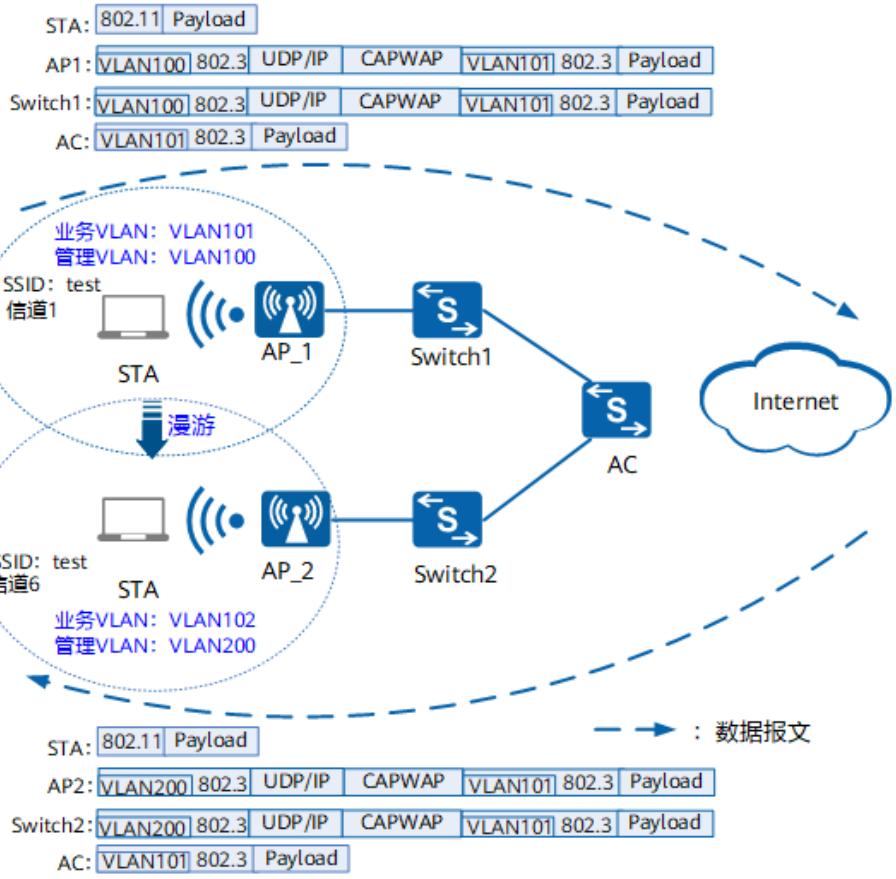
**说明**

如果AP与AC之间没有交换机，只需要在AC上的接口（包括AC的下行接口、上行接口）上配置允许VLAN101和VLAN102通过。

- 隧道转发模式

  如图9-11所示，隧道转发模式下，用户从AP_1漫游到AP_2时，当数据报文到达AP2后，AP_2直接将数据报文打上VLAN101的标签，同时进行CAPWAP隧道封装，打上VLAN200的标签并转发给AC。数据报文到达AC后，解封装CAPWAP报文，然后继续向上层网络设备转发报文。反之，用户从AP_2漫游到AP_1时，当数据报文到达AP_1后，AP_1直接将数据报文打上VLAN102的标签，同时进行CAPWAP隧道封装，打上VLAN100的标签并转发给AC。数据报文到达AC后，解封装CAPWAP报文，然后继续向上层网络设备转发报文。

**图 9-11** 隧道转发模式的不同业务 VLAN 的 AP 间漫游组网图




因此，如果采用隧道转发模式，AC上的上行接口需要配置允许VLAN101和VLAN102通过。

## 配置流程

以下配置任务为并列关系，请根据实际情况选择其中一种进行配置。

# 9.6.1 配置不同业务 VLAN 的 AP 间非快速漫游功能

## 操作步骤

**步骤1** 配置非快速漫游：

AP可以配置如下的任何一种安全策略：

- WEP(开放系统认证)
- WEP(共享密钥认证)
- WPA/WPA2-PSK
- WPA-802.1X
- WPA2-802.1X，并且STA不支持PMK快速漫游技术

- WPA3-802.1X，并且STA不支持PMK快速漫游技术

基本业务配置完成后，STA就可以实现非快速漫游。

**----结束**

## 9.6.2 配置不同业务 VLAN 的 AP 间快速漫游功能

### 操作步骤

**步骤1** 配置快速漫游：

要配置PMK快速漫游，STA必须支持PMK快速漫游技术，且参与漫游的各AP上配置的安全策略必须是WPA2-802.1X或WPA3-802.1X。基本业务配置完成后，STA就可以实现PMK快速漫游。

**----结束**

## 9.6.3 （可选）配置 802.11r 漫游

### 操作步骤

**步骤1** 执行命令**system-view**，进入系统视图。

**步骤2** 执行命令**wlan**，进入WLAN视图。

**步骤3** 执行命令**ssid-profile name** *profile-name*，进入SSID模板视图。

**步骤4** 执行命令**dot11r enable** [ **over-the-ds** ]，开启802.11r功能。

缺省情况下，802.11r功能未开启。

**步骤5** 执行命令**dot11r proprietary**，开启华为私有802.11r功能。

缺省情况下，华为私有802.11r功能未开启。

**步骤6** 执行命令**dot11r reassociate-timeout** *time*，配置802.11r重关联超时时间。

缺省情况下，802.11r重关联超时时间为1s。

**步骤7** 执行命令**quit**，返回WLAN视图。

**步骤8** 执行命令**vap-profile name** *profile-name*，进入VAP模板视图。

**步骤9** 执行命令**ssid-profile** *profile-name*，在VAP模板中引用SSID模板。

缺省情况下，VAP模板下引用名为**default**的SSID模板。

**----结束**

### 检查配置结果

- 执行命令**display ssid-profile** { **all** | **name** *profile-name* }，查看SSID模板中802.11r功能相关的信息。

## 9.6.4 检查配置结果

### 操作步骤

- 执行命令**display station roam-track sta-mac** *mac-address*，查看指定STA的漫游轨迹。
- 执行命令**display station sta-mac** *mac-address*，查看指定STA的接入信息，以便了解该STA关联的AP是否发生了变化。

**----结束**

# 9.7 配置 AC 间漫游

### 前置任务

对于大中型的WLAN网络，需要多个AC才能满足WLAN网络的覆盖需求，当用户在不同的AC间进行漫游时，网络业务不中断。

**配置WLAN基本业务**且参与漫游的各个AP需要满足：

- 关联在不同的AC上
- 配置相同的安全策略
- 配置相同的SSID
- 如果AC上配置了NAC业务，需要保证参与漫游的各个AC上配置了相同的认证策略和授权策略，同时下发给各个AP的认证策略和授权策略也是相同的。

**说明**

对于AC间的802.11r漫游，如果HAC和FAC不在同一个漫游组，会导致漫游后终端接入失败、无法继续使用WLAN业务。

### 配置流程

## 9.7.1 配置 AC 间隧道 DTLS 加密

### 背景信息

在AC间漫游场景中，AC设备是通过AC间隧道进行数据同步和报文转发，配置AC间隧道DTLS加密后，AC通过发现机制获取其他AC的IP地址后，进入DTLS协商阶段，即AC根据此IP地址与其他AC协商建立AC间隧道，这个过程中AC间隧道采用DTLS来加密传输UDP报文，提高报文传输的安全性。

建议先配置预共享密钥，使AC上的预共享密钥一致，再使能AC间隧道DTLS加密功能。如果先使能AC间隧道DTLS加密功能，此时若各AC的预共享密钥不同，DTLS协商会失败，AC间隧道建立链路失败。

### 操作步骤

**步骤1** 执行命令**system-view**，进入系统视图。

**步骤2** 执行命令**capwap dtls inter-controller psk** *psk-value*，配置AC间隧道DTLS加密使用的预共享密钥。

缺省情况下，未配置DTLS加密使用的预共享密钥。

**步骤3** 执行命令**capwap dtls inter-controller control-link encrypt**，配置AC间控制隧道的DTLS加密功能。

缺省情况下，AC间控制隧道的DTLS加密功能关闭。

**----结束**

## 9.7.2 （可选）配置 AC 间敏感信息加密

### 背景信息

在AC间漫游的组网中，AC之间需要传输一些敏感信息（如用户名、密码等），因此需要配置预共享密钥来保护AC间传输的数据。

### 操作步骤

**步骤1** 执行命令**system-view**，进入系统视图。

**步骤2** 执行命令**capwap inter-controller sensitive-info psk** *key-value*，配置AC间敏感信息加密使用的预共享密钥。

缺省情况下，未配置AC间敏感信息加密使用的共享加密密钥。

**----结束**

## 9.7.3 配置漫游组

### 背景信息

在WLAN网络中，并不是任意两个AC间都可以实现漫游，STA只能在同一个漫游组内的AC间进行漫游。需要加入漫游组的每个AC上均需要按照如下步骤配置AC间建链的本地IP地址、漫游组，并添加成员AC。

### 操作步骤

**步骤1** 执行命令**system-view**，进入系统视图。

**步骤2** 执行命令**wlan**，进入WLAN视图。

**步骤3** 执行命令**mobility-server local ip-address** *ipv4-address*，配置漫游组内AC间建链的本地IP地址。

缺省情况下，未配置漫游组内AC间建链的本地IP地址。

**步骤4** 执行命令**mobility-group name** *group-name*，进入漫游组的配置视图。

缺省情况下，没有创建漫游组。

**步骤5** 执行命令**member ip-address** *ipv4-address* [ **description** *description* ]，向漫游组中添加成员。

缺省情况下，系统没有向漫游组中添加成员。

此处添加的AC的IP地址为AC的源IP地址。

**----结束**

## 9.7.4 （可选）配置 802.11r 漫游

### 操作步骤

**步骤1** 执行命令**system-view**，进入系统视图。

**步骤2** 执行命令**wlan**，进入WLAN视图。

**步骤3** 执行命令**ssid-profile name** *profile-name*，进入SSID模板视图。

**步骤4** 执行命令**dot11r enable** [ **over-the-ds** ]，开启802.11r功能。

缺省情况下，802.11r功能未开启。

**步骤5** 执行命令**dot11r proprietary**，开启华为私有802.11r功能。

缺省情况下，华为私有802.11r功能未开启。

**步骤6** 执行命令**dot11r reassociate-timeout** *time*，配置802.11r重关联超时时间。

缺省情况下，802.11r重关联超时时间为1s。

**步骤7** 执行命令**quit**，返回WLAN视图。

**步骤8** 执行命令**vap-profile name** *profile-name*，进入VAP模板视图。

**步骤9** 执行命令**ssid-profile** *profile-name*，在VAP模板中引用SSID模板。

缺省情况下，VAP模板下引用名为**default**的SSID模板。

**----结束**

### 检查配置结果

- 执行命令**display ssid-profile** { **all** | **name** *profile-name* }，查看SSID模板中802.11r功能相关的信息。

## 9.7.5 检查 AC 间漫游配置结果

### 前提条件

已完成WLAN漫游的相关配置。

### 操作步骤

- 执行命令**display mobility-group** { **name** *group-name* | **all** }，查看指定漫游组的配置信息。

**----结束**

# 9.8 配置敏捷分布式 SFN 漫游

### 背景信息

在敏捷分布式WLAN组网中，对于某些网络连接稳定性有较高要求的场景，如医疗场景，可以开启敏捷分布式SFN漫游功能。所有RU部署在相同工作信道上并使用相同的

BSSID和终端通信，终端在同一个SSID信号覆盖范围内自由移动时可实现无感知漫游、上网业务不中断。

## 前置任务

在配置敏捷分布式SFN漫游之前，需完成以下任务：

- **4.10 配置中心AP和RU上线**。
- **4.12 配置STA上线（敏捷分布式WLAN组网）**。
- 所有RU部署在同一工作信道，具体配置方法请参见**4.11.1.1 配置基本射频参数**。

## 操作步骤

**步骤1** 执行命令**system-view**，进入系统视图。

**步骤2** 执行命令**wlan**，进入WLAN视图。

**步骤3** 执行命令**vap-profile name** *profile-name*，进入VAP模板视图。

缺省情况下，系统上存在名为**default**的VAP模板。

**步骤4** 执行命令**sfn-roam enable**，开启敏捷分布式SFN漫游功能。

缺省情况下，敏捷分布式SFN漫游功能未开启。

**步骤5** 将指定VAP模板绑定到AP组。VAP模板绑定的具体步骤参见**4.11.2.12 引用VAP模板**。

**步骤6** 执行命令**quit**，返回WLAN视图。

**步骤7** （可选）配置敏捷分布式SFN漫游相关参数。

1. 执行命令**rrm-profile name** *profile-name*，创建RRM模板并进入模板视图。

   缺省情况下，系统已经存在名为“default”的缺省RRM模板。
2. 配置敏捷分布式SFN漫游判决相关参数。
   - 执行命令**sfn-roam roam-check check-interval** *check-interval-value*，配置敏捷分布式SFN漫游判决周期。

     缺省情况下，敏捷分布式SFN漫游判决周期为700毫秒。
   - 执行命令**sfn-roam report-interval** *report-interval-value*，配置RU上报终端RSSI的周期。

     缺省情况下，RU向中心AP上报终端RSSI的周期为400毫秒。
   - 执行命令**sfn-roam roam-check sta-holding times** *sta-holding-times*，配置敏捷分布式SFN漫游终端保持次数。

     缺省情况下，敏捷分布式SFN漫游终端保持次数为3次。
   - 配置影响终端RSSI累积变化值判断条件的参数。
     - 执行命令**sfn-roam roam-check rssi-accumulate threshold** *rssi-accumulate-value*，配置敏捷分布式SFN漫游终端RSSI变化累计阈值。

       缺省情况下，敏捷分布式SFN漫游终端RSSI变化累计阈值为8dB。
   - 配置影响信号强度差值判断条件的参数。
     - 执行命令**sfn-roam roam-check gap-rssi** *gap-rssi*，配置敏捷分布式SFN漫游RU信号强度差值。

       缺省情况下，敏捷分布式SFN漫游RU信号强度差值为6dB。

- 配置影响信号强度较优次数判断条件的参数。
  - 执行命令**sfn-roam roam-check better-times** *better-times*，配置敏捷分布式SFN漫游RU信号强度较优次数。
    缺省情况下，敏捷分布式SFN漫游RU信号强度较优次数为2次。
  - 执行命令**sfn-roam roam-check high-threshold** *high-threshold-value*，配置敏捷分布式SFN漫游终端RSSI高阈值。
    缺省情况下，敏捷分布式SFN漫游终端RSSI高阈值为-55dBm。
  - 执行命令**sfn-roam roam-check low-threshold** *low-threshold-value*，配置敏捷分布式SFN漫游终端RSSI低阈值。
    缺省情况下，敏捷分布式SFN漫游终端RSSI低阈值为-60dBm。

3. 执行命令**quit**，返回WLAN视图。
4. 进入AP组射频视图。
   a. 执行命令**ap-group name** *group-name*，进入AP组视图。
   b. 执行命令**radio** *radio-id*，进入射频视图。
5. 配置敏捷分布式SFN漫游相关射频参数。
   - 执行命令**cts disable**，关闭RU回复终端CTS报文功能。
     缺省情况下，RU回复终端CTS报文功能已开启。
   - 执行命令**cts delay** *delay-time*，配置RU向终端回复CTS报文的延迟时间。
     缺省情况下，没有配置RU向终端回复CTS报文的延迟时间。
   - 执行命令**beacon disable**，关闭RU发送Beacon帧功能。
     缺省情况下，RU上允许发送Beacon帧。
6. 执行命令**quit**，返回AP组视图。
7. 执行命令**quit**，返回WLAN视图。
8. 执行命令**radio-2g-profile name** *profile-name*或**radio-5g-profile name** *profile-name*，进入2G或5G射频模板视图。
9. 执行命令**rrm-profile** *profile-name*，将RRM模板绑定到2G或5G射频模板。
10. 执行命令**quit**，返回WLAN视图。
11. 将指定射频模板绑定到AP组。具体步骤参见**4.11.1.5 引用射频模板**。

**----结束**

### 检查配置结果

- 执行命令**display vap-profile** { **all** | **name** *profile-name* }，查看VAP模板中敏捷分布式SFN漫游功能使能情况。
- 执行命令**display rrm-profile** { **all** | **name** *profile-name* }，查看RRM模板中敏捷分布式SFN漫游功能相关参数的信息。

# 9.9 漫游配置举例

## 9.9.1 配置同一业务 VLAN 的 AP 间非快速漫游功能示例

## 配置流程

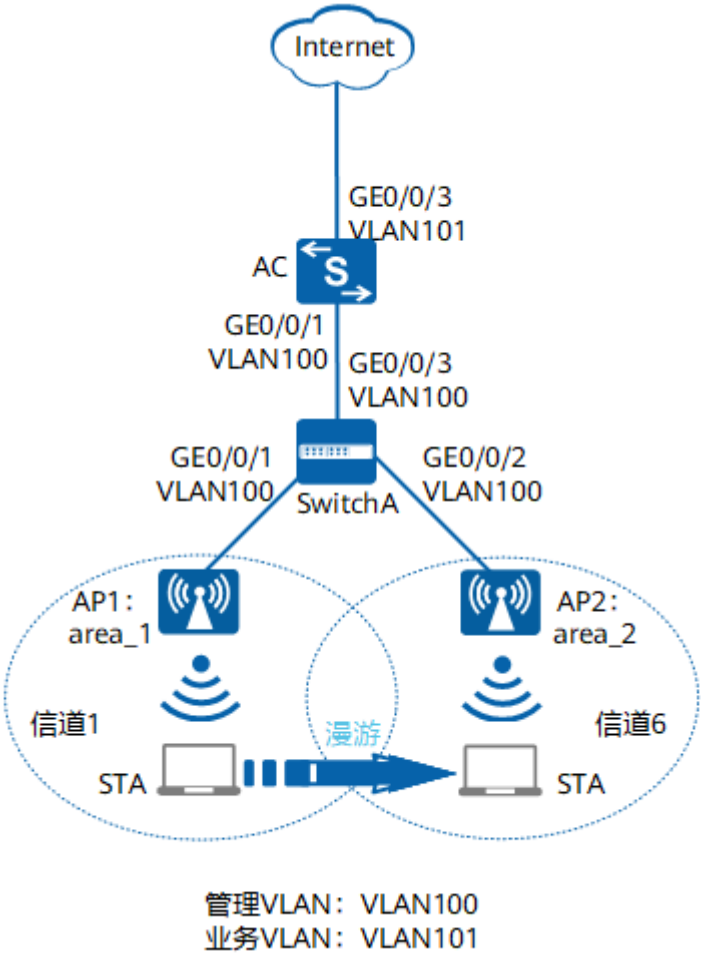
WLAN不同的特性和功能需要在不同类型的模板下进行配置和维护，这些模板统称为WLAN模板，如域管理模板、射频模板、VAP模板、AP系统模板、AP有线口模板、WIDS模板、WDS模板、Mesh模板。当用户在配置WLAN业务功能时，需要在对应功能的WLAN模板中进行参数配置，配置完成后，须将此模板引用到AP组或AP中，配置才会自动下发到AP，进而配置的功能在AP上生效。由于模板之间是存在相互引用关系的，因此在用户配置过程中，需要先了解各个模板之间存在的逻辑关系。模板的逻辑关系和基本配置流程请参见**WLAN业务配置流程**。

## 组网需求

如**图9-12**所示，某园区网内的某部门部署两台AP，通过AC集中管理和控制。AC为AP和STA动态分配IP地址。部门内所有用户同属于一个VLAN内，即AP1和AP2采用相同的业务VLAN。用户的数据转发模式为隧道转发。

用户希望STA从AP1的无线信号覆盖区域移动到AP2的无线信号覆盖区域时业务不会中断。

**图 9-12** 配置同一业务 VLAN 的 AP 间非快速漫游组网图




## 配置思路

采用如下的思路配置同一业务VLAN的AP间非快速漫游：

1. 配置网络互通，使AP与AC之间能够传输CAPWAP报文。
2. 配置AC作为DHCP服务器，为STA和AP分配IP地址。
3. 配置WLAN基本业务，保证用户能够连接到无线网络。

**表 9-5** 数据规划表

| 配置项 | 数据 |
| --- | --- |
| DHCP服务器 | AC作为DHCP服务器为STA和AP分配IP地址 |
| AP的IP地址池 | 10.23.100.2～10.23.100.254/24 |
| STA的IP地址池 | 10.23.101.2～10.23.101.254/24 |
| AC的源接口IP地址 | VLANIF100：10.23.100.1/24 |
| AP组 | ● 名称：ap-group1<br>● 引用模板：VAP模板wlan-vap、域管理模板domain1 |
| 域管理模板 | ● 名称：domain1<br>● 国家码：CN |
| SSID模板 | ● 名称：wlan-ssid<br>● SSID名称：wlan-net |
| 安全模板 | ● 名称：wlan-security<br>● 安全策略：WPA2+PSK+AES<br>● 密码：a1234567 |
| VAP模板 | ● 名称：wlan-vap<br>● 转发模式：隧道转发<br>● 业务VLAN：VLAN101<br>● 引用模板：SSID模板wlan-ssid、安全模板wlan-security |

## 配置注意事项

- 纯组播报文由于协议要求在无线空口没有ACK机制保障，且无线空口链路不稳定，为了纯组播报文能够稳定发送，通常会以低速报文形式发送。如果网络侧有大量异常组播流量涌入，则会造成无线空口拥堵。为了减小大量低速组播报文对无线网络造成的冲击，建议配置组播报文抑制功能。配置前请确认是否有组播业务，如果有，请谨慎配置限速值。
  - 业务数据转发方式采用直接转发时，建议在直连AP的交换机接口上配置组播报文抑制。
  - 业务数据转发方式采用隧道转发时，建议在AC的流量模板下配置组播报文抑制。

配置方法请参见：**如何配置组播报文抑制，减小大量低速组播报文对无线网络造成的冲击？**

- 建议在与AP直连的设备接口上配置端口隔离，如果不配置端口隔离，尤其是业务数据转发方式采用直接转发时，可能会在VLAN内形成大量不必要的广播报文，导致网络阻塞，影响用户体验。
- 隧道转发模式下，管理VLAN和业务VLAN不能配置为同一VLAN，且AP和AC之间只能放通管理VLAN，不能放通业务VLAN。
- V200R021C00版本开始，配置CAPWAP源接口或源地址时，会检查和安全相关的配置是否已存在，包括DTLS加密的PSK、AC间DTLS加密的PSK、登录AP的用户名和密码、全局离线管理VAP的登录密码，均已存在才能成功配置，否则会提示用户先完成相关的配置。
- V200R021C00版本开始，AC默认开启CAPWAP控制隧道的DTLS加密功能。开启该功能，添加AP时AP会上线失败，此时需要先开启CAPWAP DTLS不认证方式（**capwap dtls no-auth enable**）让AP上线，以便AP获取安全凭证，AP上线后应及时关闭该功能（**undo capwap dtls no-auth enable**），避免未授权AP上线。

## 操作步骤

**步骤1** 在AC上配置NAC模式为统一模式，以保证用户能够正常接入网络

```
<HUAWEI> system-view
[HUAWEI] authentication unified-mode
```

**说明**

如果当前NAC模式为传统模式，则配置NAC模式为统一模式后，需要保存配置并重启设备后生效。

**步骤2** 配置Switch_A和AC，使AP与AC之间能够传输CAPWAP报文

# 配置Switch_A的接口GE0/0/1～GE0/0/3都加入VLAN100（管理VLAN）。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch_A
[Switch_A] vlan batch 100
[Switch_A] interface gigabitethernet 0/0/1
[Switch_A-GigabitEthernet0/0/1] port link-type trunk
[Switch_A-GigabitEthernet0/0/1] port trunk pvid vlan 100
[Switch_A-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[Switch_A-GigabitEthernet0/0/1] port-isolate enable
[Switch_A-GigabitEthernet0/0/1] quit
[Switch_A] interface gigabitethernet 0/0/2
[Switch_A-GigabitEthernet0/0/2] port link-type trunk
[Switch_A-GigabitEthernet0/0/2] port trunk pvid vlan 100
[Switch_A-GigabitEthernet0/0/2] port trunk allow-pass vlan 100
[Switch_A-GigabitEthernet0/0/2] port-isolate enable
[Switch_A-GigabitEthernet0/0/2] quit
[Switch_A] interface gigabitethernet 0/0/3
[Switch_A-GigabitEthernet0/0/3] port link-type trunk
[Switch_A-GigabitEthernet0/0/3] port trunk allow-pass vlan 100
[Switch_A-GigabitEthernet0/0/3] quit
```

# 配置AC连接Switch_A的接口GE0/0/1加入VLAN100。

```
<HUAWEI> system-view
[HUAWEI] sysname AC
[AC] vlan batch 100
[AC] interface gigabitethernet 0/0/1
[AC-GigabitEthernet0/0/1] port link-type trunk
[AC-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[AC-GigabitEthernet0/0/1] quit
```

**步骤3** 配置AC与上层网络设备互通

# 配置AC上行接口GE0/0/3加入VLAN101。

```
[AC] vlan batch 101
[AC] interface gigabitethernet 0/0/3
[AC-GigabitEthernet0/0/3] port link-type trunk
[AC-GigabitEthernet0/0/3] port trunk allow-pass vlan 101
[AC-GigabitEthernet0/0/3] quit
```

**步骤4** 配置AC作为DHCP服务器，为STA和AP分配IP地址

# 配置基于接口地址池的DHCP服务器，其中，VLANIF100接口为AP1和AP2提供IP地址，VLANIF101为STA提供IP地址。

**说明**

DNS服务器地址请根据实际需要配置。常用配置方法如下：

- 接口地址池场景，需要在VLANIF接口视图下执行命令**dhcp server dns-list** *ip-address* &<1-8>。
- 全局地址池场景，需要在IP地址池视图下执行命令**dns-list** *ip-address* &<1-8>。

```
[AC] dhcp enable
[AC] interface vlanif 100
[AC-Vlanif100] ip address 10.23.100.1 24
[AC-Vlanif100] dhcp select interface
[AC-Vlanif100] quit
[AC] interface vlanif 101
[AC-Vlanif101] ip address 10.23.101.1 24
[AC-Vlanif101] dhcp select interface
[AC-Vlanif101] quit
```

**步骤5** 配置AP上线

# 创建AP组，用于将相同配置的AP都加入同一AP组中。

```
[AC] wlan
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] quit
```

# 创建域管理模板，在域管理模板下配置AC的国家码并在AP组下引用域管理模板。

```
[AC-wlan-view] regulatory-domain-profile name domain1
[AC-wlan-regulate-domain-domain1] country-code cn
[AC-wlan-regulate-domain-domain1] quit
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] regulatory-domain-profile domain1
Warning: This configuration change will clear the channel and power configurations of radios, and may restart APs. Continue?[Y/N]:y
[AC-wlan-ap-group-ap-group1] quit
[AC-wlan-view] quit
```

# 配置AC的源接口。

```
[AC] capwap source interface vlanif 100
```

# 在AC上离线导入AP，并将AP加入AP组“ap-group1”中。假设AP的MAC地址为00e0-fc76-e360和00e0-fc74-9640，并且根据AP的部署位置为AP配置名称，便于从名称上就能够了解AP的部署位置。例如MAC地址为00e0-fc76-e360的AP部署在1号区域，命名此AP为area_1。

**说明**

**ap auth-mode**命令缺省情况下为MAC认证，如果之前没有修改其缺省配置，可以不用执行**ap auth-mode mac-auth**命令。

举例中使用的AP为AP5030DN，具有射频0和射频1两个射频。AP5030DN的射频0为2.4GHz射频，射频1为5GHz射频。

```
[AC] wlan
[AC-wlan-view] ap auth-mode mac-auth
[AC-wlan-view] ap-id 0 ap-mac 00e0-fc76-e360
[AC-wlan-ap-0] ap-name area_1
Warning: This operation may cause AP reset. Continue? [Y/N]:y
[AC-wlan-ap-0] ap-group ap-group1
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configuration s of the radio, Whether to continue? [Y/N]:y
[AC-wlan-ap-0] quit
[AC-wlan-view] ap-id 1 ap-mac 00e0-fc74-9640
[AC-wlan-ap-1] ap-name area_2
Warning: This operation may cause AP reset. Continue? [Y/N]:y
[AC-wlan-ap-1] ap-group ap-group1
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configuration s of the radio, Whether to continue? [Y/N]:y
[AC-wlan-ap-1] quit
```

# 将AP上电后，当执行命令**display ap all**查看到AP的“State”字段为“nor”时，表示AP正常上线。

```
[AC-wlan-view] display ap all
Total AP information:
nor  : normal          [2]
Extrainfo : Extra information
P  : insufficient power supply
-------------------------------------------------------------------------------------------------
ID   MAC            Name   Group     IP            Type           State STA Uptime     ExtraInfo
-------------------------------------------------------------------------------------------------
0    00e0-fc76-e360 area_1 ap-group1 10.23.100.254 AP5030DN       nor   0   5M:2S      -
1    00e0-fc74-9640 area_2 ap-group1 10.23.100.253 AP5030DN       nor   0   5M:4S      -
-------------------------------------------------------------------------------------------------
Total: 2
```

**步骤6** 配置WLAN业务参数

# 创建名为“wlan-security”的安全模板，并配置安全策略。

**说明**

举例中以配置WPA2+PSK+AES的安全策略为例，密码为“a1234567”，实际配置中请根据实际情况，配置符合实际要求的安全策略。

```
[AC-wlan-view] security-profile name wlan-security
[AC-wlan-sec-prof-wlan-security] security wpa2 psk pass-phrase a1234567 aes
[AC-wlan-sec-prof-wlan-security] quit
```

# 创建名为“wlan-ssid”的SSID模板，并配置SSID名称为“wlan-net”。

```
[AC-wlan-view] ssid-profile name wlan-ssid
[AC-wlan-ssid-prof-wlan-ssid] ssid wlan-net
[AC-wlan-ssid-prof-wlan-ssid] quit
```

# 创建名为“wlan-vap”的VAP模板，配置业务数据转发模式、业务VLAN，并且引用安全模板和SSID模板。

```
[AC-wlan-view] vap-profile name wlan-vap
[AC-wlan-vap-prof-wlan-vap] forward-mode tunnel
[AC-wlan-vap-prof-wlan-vap] service-vlan vlan-id 101
[AC-wlan-vap-prof-wlan-vap] security-profile wlan-security
[AC-wlan-vap-prof-wlan-vap] ssid-profile wlan-ssid
[AC-wlan-vap-prof-wlan-vap] 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“wlan-vap”的配置。

```
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] vap-profile wlan-vap wlan 1 radio all
[AC-wlan-ap-group-ap-group1] quit
```

**步骤7** 配置AP射频的信道和功率

**说明**

射频的信道和功率自动调优功能默认开启，如果不关闭此功能则会导致手动配置不生效。举例中AP射频的信道和功率仅为示例，实际配置中请根据AP的国家码和网规结果进行配置。

# 关闭AP射频0的信道和功率自动调优功能，并配置AP射频0的信道和功率。

```
[AC-wlan-view] ap-id 0
[AC-wlan-ap-0] radio 0
[AC-wlan-radio-0/0] calibrate auto-channel-select disable
[AC-wlan-radio-0/0] calibrate auto-txpower-select disable
[AC-wlan-radio-0/0] channel 20mhz 6
Warning: This action may cause service interruption. Continue?[Y/N]y
[AC-wlan-radio-0/0] eirp 127
[AC-wlan-radio-0/0] quit
```

# 关闭AP射频1的信道和功率自动调优功能，并配置AP射频1的信道和功率。

```
[AC-wlan-ap-0] radio 1
[AC-wlan-radio-0/1] calibrate auto-channel-select disable
[AC-wlan-radio-0/1] calibrate auto-txpower-select disable
[AC-wlan-radio-0/1] channel 20mhz 149
Warning: This action may cause service interruption. Continue?[Y/N]y
[AC-wlan-radio-0/1] eirp 127
[AC-wlan-radio-0/1] quit
[AC-wlan-ap-0] quit
```

**步骤8** 验证配置结果

配置完成后，执行命令**display vap ssid wlan-net**查看VAP信息，当“Status”显示为“ON”时，表示AP对应射频上的VAP已创建成功。

```
[AC-wlan-view] display vap ssid wlan-net
Info: This operation may take a few seconds, please wait.
WID : WLAN ID
--------------------------------------------------------------------------------
AP ID AP name RfID WID     BSSID         Status  Auth type     STA   SSID
--------------------------------------------------------------------------------
0     area_1  0    1       00E0-FC76-E360 ON      WPA2-PSK      0     wlan-net
0     area_1  1    1       00E0-FC76-E370 ON      WPA2-PSK      0     wlan-net
1     area_2  0    1       00E0-FC74-9640 ON      WPA2-PSK      0     wlan-net
1     area_2  1    1       00E0-FC74-9650 ON      WPA2-PSK      0     wlan-net
--------------------------------------------------------------------------------
Total: 4
```

STA在AP1的覆盖范围内搜索到SSID为“wlan-net”的无线网络，输入密码“a1234567”并正常关联后，在AC上执行命令**display station ssid wlan-net**，查看STA的接入信息，可以看到STA关联到了AP1，STA的MAC地址为“00e0-fc12-3458”。

```
[AC-wlan-view] display station ssid wlan-net
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  IP address
--------------------------------------------------------------------------------
00e0-fc12-3458 0     area_1   1/1      5G    11n   38/64     -68   101   10.23.101.254
--------------------------------------------------------------------------------
Total: 1 2.4G: 0 5G: 1
```

当STA从AP1的覆盖范围移动到AP2的覆盖范围时，在AC上执行命令**display station ssid wlan-net**，查看STA的接入信息，可以看到STA关联到了AP2。

```
[AC-wlan-view] display station ssid wlan-net
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  IP address
--------------------------------------------------------------------------------
00e0-fc12-3458  1     area_2   1/1      5G    11n   46/59     -58   101   10.23.101.254
--------------------------------------------------------------------------------
Total: 1 2.4G: 0 5G: 1
```

在AC上执行命令**display station roam-track sta-mac 00e0-fc12-3458**，可以查看该STA的漫游轨迹。

```
[AC-wlan-view] display station roam-track sta-mac 00e0-fc12-3458
Access SSID:example
Rx/Tx:link receive rate/link transmit rate(Mbps)
c:PMK Cache Roam r:802.11r Roam s:Same Frequency Network
--------------------------------------------------------------------------------
L2/L3           AC IP                 AP name              Radio ID
BSSID           TIME                  In/Out RSSI          Out Rx/Tx
--------------------------------------------------------------------------------
--              10.23.100.1           area_1               0
00e0-fc76-e360  2015/02/07 17:48:30   -51/-48              46/13
L2              10.23.100.1           area_2               0
00e0-fc74-9640  2015/02/07 17:54:50   -58/-                -/-
--------------------------------------------------------------------------------
Number: 1
```

**----结束**

## 配置文件

- 接入交换机的配置文件

```
#
sysname Switch_A
#
vlan batch 100
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100
 port-isolate enable group 1
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100
 port-isolate enable group 1
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 100
#
return
```

- AC的配置文件

```
#
sysname AC
#
vlan batch 100 to 101
#
dhcp enable
#
interface Vlanif100
 ip address 10.23.100.1 255.255.255.0
 dhcp select interface
#
interface Vlanif101
```

```
 ip address 10.23.101.1 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 101
#
capwap source interface vlanif100
#
wlan
 security-profile name wlan-security
  security wpa2 psk pass-phrase %^%#m"tz0f>~7.[`^6RWdzwCy16hJj/Mc!,}s`X*B]}A%^%# aes
 ssid-profile name wlan-ssid
  ssid wlan-net
 vap-profile name wlan-vap
  forward-mode tunnel
  service-vlan vlan-id 101
  ssid-profile wlan-ssid
  security-profile wlan-security
 regulatory-domain-profile name domain1
 ap-group name ap-group1
  regulatory-domain-profile domain1
  radio 0
   vap-profile wlan-vap wlan 1
  radio 1
   vap-profile wlan-vap wlan 1
 ap-id 0 type-id 35 ap-mac 00e0-fc76-e360 ap-sn 210235554710CB000042
  ap-name area_1
  ap-group ap-group1
  radio 0
   channel 20mhz 6
   eirp 127
   calibrate auto-channel-select disable
   calibrate auto-txpower-select disable
  radio 1
   channel 20mhz 149
   eirp 127
   calibrate auto-channel-select disable
   calibrate auto-txpower-select disable
 ap-id 1 type-id 35 ap-mac 00e0-fc74-9640 ap-sn 210235419610D2000097
  ap-name area_2
  ap-group ap-group1
#
return
```

## 9.9.2 配置同一业务 VLAN 的 AP 间快速漫游功能示例

### 配置流程

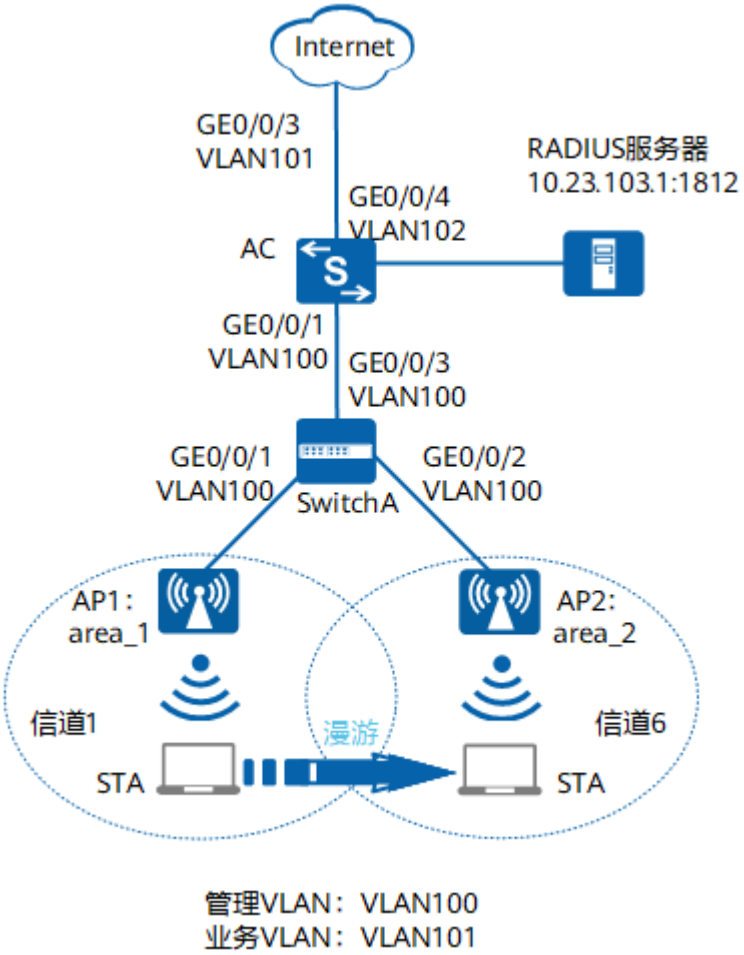
WLAN不同的特性和功能需要在不同类型的模板下进行配置和维护，这些模板统称为WLAN模板，如域管理模板、射频模板、VAP模板、AP系统模板、AP有线口模板、WIDS模板、WDS模板、Mesh模板。当用户在配置WLAN业务功能时，需要在对应功能的WLAN模板中进行参数配置，配置完成后，须将此模板引用到AP组或AP中，配置才会自动下发到AP，进而配置的功能在AP上生效。由于模板之间是存在相互引用关系的，因此在用户配置过程中，需要先了解各个模板之间存在的逻辑关系。模板的逻辑关系和基本配置流程请参见**WLAN业务配置流程**。

## 组网需求

如图9-13所示，某园区网内的某部门部署两台AP，通过AC集中管理和控制。AC为AP和STA动态分配IP地址。部门内所有用户同属于一个VLAN内，即AP1和AP2采用相同的业务VLAN。用户采用的安全策略为WPA2-802.1X，数据转发模式为隧道转发。

用户希望STA从AP1的无线信号覆盖区域移动到AP2的无线信号覆盖区域时业务不会中断。

**图 9-13** 配置同一业务 VLAN 的 AP 间快速漫游组网图




## 配置思路

采用如下的思路配置同一业务VLAN的AP间快速漫游：

1. 用户采用的安全策略为WPA2+802.1X+AES，需要进行接入认证，漫游切换时间较长。因此，通过配置同一业务VLAN的AP间快速漫游，实现用户在漫游过程中业务不中断。
2. 配置网络互通，使AP与AC之间能够传输CAPWAP报文。
3. 配置AC作为DHCP服务器，为STA和AP分配IP地址。
4. 配置WLAN基本业务，保证用户能够连接到无线网络。

**表 9-6** 数据规划表

| 配置项 | 数据 |
| --- | --- |
| DHCP服务器 | AC作为DHCP服务器为STA和AP分配IP地址 |
| AP的IP地址池 | 10.23.100.2～10.23.100.254/24 |
| STA的IP地址池 | 10.23.101.2～10.23.101.254/24 |
| AC的源接口IP地址 | VLANIF100：10.23.100.1/24 |
| RADIUS认证参数 | • RADIUS服务器模板名称：radius_huawei<br>• IP地址：10.23.103.1<br>• 认证端口号：1812<br>• 共享密钥：huawei@123<br>• 认证方案：radius_huawei |
| STA的用户名和密码 | • 用户名：test@huawei.com<br>• 密码：123456 |
| 802.1X接入模板 | • 名称：wlan-dot1x<br>• 认证方式：EAP |
| 认证模板 | • 名称：wlan-authentication<br>• 引用模板和认证方案：802.1X接入模板wlan-dot1x、认证方案radius_huawei、RADIUS服务器模板radius_huawei |
| AP组 | • 名称：ap-group1<br>• 引用模板：VAP模板wlan-vap、域管理模板domain1 |
| 域管理模板 | • 名称：domain1<br>• 国家码：CN |
| SSID模板 | • 名称：wlan-ssid<br>• SSID名称：wlan-net |
| 安全模板 | • 名称：wlan-security<br>• 安全策略：WPA2+802.1X+AES |
| VAP模板 | • 名称：wlan-vap<br>• 转发模式：隧道转发<br>• 业务VLAN：VLAN101<br>• 引用模板：SSID模板wlan-ssid、安全模板wlan-security |

## 配置注意事项

- 纯组播报文由于协议要求在无线空口没有ACK机制保障，且无线空口链路不稳定，为了纯组播报文能够稳定发送，通常会以低速报文形式发送。如果网络侧有大量异常组播流量涌入，则会造成无线空口拥堵。为了减小大量低速组播报文对无线网络造成的冲击，建议配置组播报文抑制功能。配置前请确认是否有组播业务，如果有，请谨慎配置限速值。
  - 业务数据转发方式采用直接转发时，建议在直连AP的交换机接口上配置组播报文抑制。
  - 业务数据转发方式采用隧道转发时，建议在AC的流量模板下配置组播报文抑制。

  配置方法请参见：**如何配置组播报文抑制，减小大量低速组播报文对无线网络造成的冲击?**
- 建议在与AP直连的设备接口上配置端口隔离，如果不配置端口隔离，尤其是业务数据转发方式采用直接转发时，可能会在VLAN内形成大量不必要的广播报文，导致网络阻塞，影响用户体验。
- 隧道转发模式下，管理VLAN和业务VLAN不能配置为同一VLAN，且AP和AC之间只能放通管理VLAN，不能放通业务VLAN。
- V200R021C00版本开始，配置CAPWAP源接口或源地址时，会检查和安全相关的配置是否已存在，包括DTLS加密的PSK、AC间DTLS加密的PSK、登录AP的用户名和密码、全局离线管理VAP的登录密码，均已存在才能成功配置，否则会提示用户先完成相关的配置。
- V200R021C00版本开始，AC默认开启CAPWAP控制隧道的DTLS加密功能。开启该功能，添加AP时AP会上线失败，此时需要先开启CAPWAP DTLS不认证方式（**capwap dtls no-auth enable**）让AP上线，以便AP获取安全凭证，AP上线后应及时关闭该功能（**undo capwap dtls no-auth enable**），避免未授权AP上线。

## 操作步骤

**步骤1** 在AC上配置NAC模式为统一模式，以保证用户能够正常接入网络

```
<HUAWEI> system-view
[HUAWEI] authentication unified-mode
```

**说明**

如果当前NAC模式为传统模式，则配置NAC模式为统一模式后，需要保存配置并重启设备后生效。

**步骤2** 配置Switch_A和AC，使AP与AC之间能够传输CAPWAP报文

# 配置Switch_A的接口GE0/0/1～GE0/0/3都加入VLAN100（管理VLAN）。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch_A
[Switch_A] vlan batch 100
[Switch_A] interface gigabitethernet 0/0/1
[Switch_A-GigabitEthernet0/0/1] port link-type trunk
[Switch_A-GigabitEthernet0/0/1] port trunk pvid vlan 100
[Switch_A-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[Switch_A-GigabitEthernet0/0/1] port-isolate enable
[Switch_A-GigabitEthernet0/0/1] quit
[Switch_A] interface gigabitethernet 0/0/2
[Switch_A-GigabitEthernet0/0/2] port link-type trunk
[Switch_A-GigabitEthernet0/0/2] port trunk pvid vlan 100
[Switch_A-GigabitEthernet0/0/2] port trunk allow-pass vlan 100
[Switch_A-GigabitEthernet0/0/2] port-isolate enable
[Switch_A-GigabitEthernet0/0/2] quit
```

```
[Switch_A] interface gigabitethernet 0/0/3
[Switch_A-GigabitEthernet0/0/3] port link-type trunk
[Switch_A-GigabitEthernet0/0/3] port trunk allow-pass vlan 100
[Switch_A-GigabitEthernet0/0/3] quit
```

# 配置AC连接Switch_A的接口GE0/0/1加入VLAN100。

```
<HUAWEI> system-view
[HUAWEI] sysname AC
[AC] vlan batch 100
[AC] interface gigabitethernet 0/0/1
[AC-GigabitEthernet0/0/1] port link-type trunk
[AC-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[AC-GigabitEthernet0/0/1] quit
```

**步骤3** 配置AC与上层网络设备互通

# 配置AC上行接口GE0/0/3加入VLAN101并配置AC连接RADIUS服务器的接口GE0/0/4加入VLAN102。

```
[AC] vlan batch 101 102
[AC] interface gigabitethernet 0/0/3
[AC-GigabitEthernet0/0/3] port link-type trunk
[AC-GigabitEthernet0/0/3] port trunk allow-pass vlan 101
[AC-GigabitEthernet0/0/3] quit
[AC] interface gigabitethernet 0/0/4
[AC-GigabitEthernet0/0/4] port link-type trunk
[AC-GigabitEthernet0/0/4] port trunk pvid vlan 102
[AC-GigabitEthernet0/0/4] port trunk allow-pass vlan 102
[AC-GigabitEthernet0/0/4] quit
```

**步骤4** 配置AC作为DHCP服务器，为STA和AP分配IP地址。配置VLANIF102，使AC和RADIUS服务器之间能够通信

# 配置基于接口地址池的DHCP服务器，其中，VLANIF100接口为AP1和AP2提供IP地址，VLANIF101为STA提供IP地址。

**说明**

DNS服务器地址请根据实际需要配置。常用配置方法如下：

- 接口地址池场景，需要在VLANIF接口视图下执行命令**dhcp server dns-list** *ip-address* &<1-8>。
- 全局地址池场景，需要在IP地址池视图下执行命令**dns-list** *ip-address* &<1-8>。

```
[AC] dhcp enable
[AC] interface vlanif 100
[AC-Vlanif100] ip address 10.23.100.1 24
[AC-Vlanif100] dhcp select interface
[AC-Vlanif100] quit
[AC] interface vlanif 101
[AC-Vlanif101] ip address 10.23.101.1 24
[AC-Vlanif101] dhcp select interface
[AC-Vlanif101] quit
```

# 配置VLANIF102。

```
[AC] interface vlanif 102
[AC-Vlanif102] ip address 10.23.103.2 24
[AC-Vlanif102] quit
```

**步骤5** 配置AP上线

# 创建AP组，用于将相同配置的AP都加入同一AP组中。

```
[AC] wlan
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] quit
```

# 创建域管理模板，在域管理模板下配置AC的国家码并在AP组下引用域管理模板。

```
[AC-wlan-view] regulatory-domain-profile name domain1
[AC-wlan-regulate-domain-domain1] country-code cn
[AC-wlan-regulate-domain-domain1] quit
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] regulatory-domain-profile domain1
Warning: This configuration change will clear the channel and power configurations of radios, and may restart APs. Continue?[Y/N]:y
[AC-wlan-ap-group-ap-group1] quit
[AC-wlan-view] quit
```

# 配置AC的源接口。

```
[AC] capwap source interface vlanif 100
```

# 在AC上离线导入AP，并将AP加入AP组“ap-group1”中。假设AP的MAC地址为00e0-fc76-e360和00e0-fc74-9640，并且根据AP的部署位置为AP配置名称，便于从名称上就能够了解AP的部署位置。例如MAC地址为00e0-fc76-e360的AP部署在1号区域，命名此AP为area_1。

**说明**

**ap auth-mode**命令缺省情况下为MAC认证，如果之前没有修改其缺省配置，可以不用执行**ap auth-mode mac-auth**命令。

举例中使用的AP为AP5030DN，具有射频0和射频1两个射频。AP5030DN的射频0为2.4GHz射频，射频1为5GHz射频。

```
[AC] wlan
[AC-wlan-view] ap auth-mode mac-auth
[AC-wlan-view] ap-id 0 ap-mac 00e0-fc76-e360
[AC-wlan-ap-0] ap-name area_1
Warning: This operation may cause AP reset. Continue? [Y/N]:y
[AC-wlan-ap-0] ap-group ap-group1
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configuration s of the radio, Whether to continue? [Y/N]:y
[AC-wlan-ap-0] quit
[AC-wlan-view] ap-id 1 ap-mac 00e0-fc74-9640
[AC-wlan-ap-1] ap-name area_2
Warning: This operation may cause AP reset. Continue? [Y/N]:y
[AC-wlan-ap-1] ap-group ap-group1
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configuration s of the radio, Whether to continue? [Y/N]:y
[AC-wlan-ap-1] quit
```

# 将AP上电后，当执行命令**display ap all**查看到AP的“State”字段为“nor”时，表示AP正常上线。

```
[AC-wlan-view] display ap all
Total AP information:
nor  : normal          [2]
Extrainfo : Extra information
P  : insufficient power supply
-------------------------------------------------------------------------------------------------
ID   MAC            Name   Group     IP            Type           State STA Uptime     ExtraInfo
-------------------------------------------------------------------------------------------------
0    00e0-fc76-e360 area_1 ap-group1 10.23.100.254 AP5030DN       nor   0   5M:2S      -
1    00e0-fc74-9640 area_2 ap-group1 10.23.100.253 AP5030DN       nor   0   5M:4S      -
-------------------------------------------------------------------------------------------------
Total: 2
```

**步骤6** 配置RADIUS认证参数

**说明**

请确保AC与RADIUS服务器的共享密钥相同。

# 创建RADIUS服务器模板。

```
[AC] radius-server template radius_huawei
[AC-radius-radius_huawei] radius-server authentication 10.23.103.1 1812
[AC-radius-radius_huawei] radius-server shared-key cipher huawei@123
[AC-radius-radius_huawei] quit
```

# 创建RADIUS方式的认证方案。

```
[AC] aaa
[AC-aaa] authentication-scheme radius_huawei
[AC-aaa-authen-radius_huawei] authentication-mode radius
[AC-aaa-authen-radius_huawei] quit
```

# 创建AAA域并配置域的RADIUS服务器模板和认证方案。

```
[AC-aaa] domain huawei.com
[AC-aaa-domain-huawei.com] radius-server radius_huawei
[AC-aaa-domain-huawei.com] authentication-scheme radius_huawei
[AC-aaa-domain-huawei.com] quit
[AC-aaa] quit
```

**说明**

配置了域“huawei.com”后，认证用户名后面需要加上域名。

# 测试用户是否能够通过RADIUS模板的认证。（已在RADIUS服务器上配置了测试用户test@huawei.com，用户密码123456）

```
[AC] test-aaa test@huawei.com 123456 radius-template radius_huawei
Info: Account test succeed.
```

**步骤7** 配置802.1X接入模板，管理802.1X接入控制参数

# 创建名为“wlan-dot1x”的802.1X接入模板。

```
[AC] dot1x-access-profile name wlan-dot1x
```

# 配置认证方式为EAP中继模式。

```
[AC-dot1x-access-profile-wlan-dot1x] dot1x authentication-method eap
[AC-dot1x-access-profile-wlan-dot1x] quit
```

**步骤8** 创建名为“wlan-authentication”的认证模板，绑定802.1X接入模板，并配置用户强制域

```
[AC] authentication-profile name wlan-authentication
[AC-authen-profile-wlan-authentication] dot1x-access-profile wlan-dot1x
[AC-authen-profile-wlan-authentication] access-domain huawei.com dot1x force
[AC-authen-profile-wlan-authentication] quit
```

**步骤9** 配置WLAN业务参数

# 创建名为“wlan-security”的安全模板，并配置安全策略。

```
[AC-wlan-view] security-profile name wlan-security
[AC-wlan-sec-prof-wlan-security] security wpa2 dot1x aes
[AC-wlan-sec-prof-wlan-security] quit
```

# 创建名为“wlan-ssid”的SSID模板，并配置SSID名称为“wlan-net”。

```
[AC-wlan-view] ssid-profile name wlan-ssid
[AC-wlan-ssid-prof-wlan-ssid] ssid wlan-net
[AC-wlan-ssid-prof-wlan-ssid] quit
```

# 创建名为“wlan-vap”的VAP模板，配置业务数据转发模式、业务VLAN，并且引用安全模板和SSID模板。

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

```
[AC-wlan-vap-prof-wlan-vap] service-vlan vlan-id 101
[AC-wlan-vap-prof-wlan-vap] security-profile wlan-security
[AC-wlan-vap-prof-wlan-vap] authentication-profile wlan-authentication
[AC-wlan-vap-prof-wlan-vap] ssid-profile wlan-ssid
[AC-wlan-vap-prof-wlan-vap] 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“wlan-vap”的配置。

```
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] vap-profile wlan-vap wlan 1 radio 0
[AC-wlan-ap-group-ap-group1] vap-profile wlan-vap wlan 1 radio 1
[AC-wlan-ap-group-ap-group1] quit
```

**步骤10** 配置AP射频的信道和功率

**说明**

射频的信道和功率自动调优功能默认开启，如果不关闭此功能则会导致手动配置不生效。举例中AP射频的信道和功率仅为示例，实际配置中请根据AP的国家码和网规结果进行配置。

# 关闭AP射频0的信道和功率自动调优功能，并配置AP射频0的信道和功率。

```
[AC-wlan-view] ap-id 0
[AC-wlan-ap-0] radio 0
[AC-wlan-radio-0/0] calibrate auto-channel-select disable
[AC-wlan-radio-0/0] calibrate auto-txpower-select disable
[AC-wlan-radio-0/0] channel 20mhz 6
Warning: This action may cause service interruption. Continue?[Y/N]y
[AC-wlan-radio-0/0] eirp 127
[AC-wlan-radio-0/0] quit
```

# 关闭AP射频1的信道和功率自动调优功能，并配置AP射频1的信道和功率。

```
[AC-wlan-ap-0] radio 1
[AC-wlan-radio-0/1] calibrate auto-channel-select disable
[AC-wlan-radio-0/1] calibrate auto-txpower-select disable
[AC-wlan-radio-0/1] channel 20mhz 149
Warning: This action may cause service interruption. Continue?[Y/N]y
[AC-wlan-radio-0/1] eirp 127
[AC-wlan-radio-0/1] quit
[AC-wlan-ap-0] quit
```

**步骤11** 验证配置结果

完成配置后，用户可通过无线终端搜索到SSID为**wlan-net**的无线网络。用户在STA上使用802.1X客户端进行认证，输入正确的用户名和密码，STA认证成功后，可以正常访问Internet上的资源。需要根据设置的认证方式（peap）对客户端进行相应的配置。

- WINDOWS XP系统下的配置
  a. 首先在无线网络属性中，添加SSID为**wlan-net**，并选择认证方式为**WPA2**，加密方式为CCMP使用的算法**AES**。
  b. 在“验证”选项卡中，选择EAP类型为**PEAP**，单击“属性”，去掉验证服务器证书选项（此处不验证服务器证书），单击“配置”，去掉自动使用Windows登录名和密码选项，然后单击“确定”。
- WINDOWS 7系统下的配置
  a. 进入管理无线网络页面，单击“添加”，选择“手动创建网络配置文件”，添加SSID为**wlan-net**，并选择认证方式为**WPA2-企业**，加密使用的算法**AES**，单击“下一步”。
  b. 单击“更改连接设置”，进入“无线网络属性”界面，选择“安全”页签，单击“设置”，取消勾选“验证服务器证书”（此处不验证服务器证书），单击“配置”，取消勾选“自动使用Windows登录名和密码”，单击“确定”。

c. 单击“确定”，返回“无线网络属性”界面，单击“高级设置”，在“高级设置”界面，勾选“指定身份验证模式”，并选择身份验证模式为“用户身份验证”，单击“确定”。

STA在AP1的覆盖范围内搜索到SSID为“wlan-net”的无线网络，输入密码“123456”并正常关联后，在AC上执行命令**display station ssid wlan-net**，查看STA的接入信息，可以看到STA关联到了AP1，STA的MAC地址为“00e0-fc12-3458”。

```
[AC-wlan-view] display station ssid wlan-net
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  IP address
--------------------------------------------------------------------------------
00e0-fc12-3458 0     area_1   1/1      5G    11n   38/64      -68   101   10.23.101.254
--------------------------------------------------------------------------------
Total: 1 2.4G: 0 5G: 1
```

当STA从AP1的覆盖范围移动到AP2的覆盖范围时，在AC上执行命令**display station ssid wlan-net**，查看STA的接入信息，可以看到STA关联到了AP2。

```
[AC-wlan-view] display station ssid wlan-net
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  IP address
--------------------------------------------------------------------------------
00e0-fc12-3458 1     area_2   1/1      5G    11n   46/59      -58   101   10.23.101.254
--------------------------------------------------------------------------------
Total: 1 2.4G: 0 5G: 1
```

在AC上执行命令**display station roam-track sta-mac 00e0-fc12-3458**，可以查看该STA的漫游轨迹。

```
[AC-wlan-view] display station roam-track sta-mac 00e0-fc12-3458
Access SSID:example
Rx/Tx:link receive rate/link transmit rate(Mbps)
c:PMK Cache Roam r:802.11r Roam s:Same Frequency Network
--------------------------------------------------------------------------------
L2/L3          AC IP                AP name              Radio ID
BSSID          TIME                 In/Out RSSI          Out Rx/Tx
--------------------------------------------------------------------------------
--             10.23.100.1          area_1               0
00e0-fc76-e360 2015/02/07 17:48:30  -51/-48              46/13
L2             10.23.100.1          area_2               0
00e0-fc74-9640 2015/02/07 17:54:50  -58/-                -/-
--------------------------------------------------------------------------------
Number: 1
```

**----结束**

## 配置文件

- 接入交换机的配置文件

```
#
sysname Switch_A
#
vlan batch 100
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100
 port-isolate enable group 1
#
interface GigabitEthernet0/0/2
 port link-type trunk
```

```
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100
 port-isolate enable group 1
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 100
#
return
```

- AC的配置文件

```
#
sysname AC
#
vlan batch 100 to 102
#
authentication-profile name wlan-authentication
 dot1x-access-profile wlan-dot1x
 authentication-scheme radius_huawei
 radius-server radius_huawei
#
dot1x-access-profile name wlan-dot1x
#
dhcp enable
#
radius-server template radius_huawei
 radius-server shared-key cipher %^%#*7d1;XNof/|Q0:DsP!,W51DIYPx}`AARBdJ'0B^$%^%#
 radius-server authentication 10.23.103.1 1812 weight 80
#
aaa
 authentication-scheme radius_huawei
  authentication-mode radius
#
interface Vlanif100
 ip address 10.23.100.1 255.255.255.0
 dhcp select interface
#
interface Vlanif101
 ip address 10.23.101.1 255.255.255.0
 dhcp select interface
#
interface Vlanif102
 ip address 10.23.103.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 101
#
interface GigabitEthernet0/0/4
 port link-type trunk
 port trunk pvid vlan 102
 port trunk allow-pass vlan 102
#
capwap source interface vlanif100
#
wlan
 security-profile name wlan-security
  security wpa2 dot1x aes
 ssid-profile name wlan-ssid
  ssid wlan-net
 vap-profile name wlan-vap
  forward-mode tunnel
  service-vlan vlan-id 101
  ssid-profile wlan-ssid
  security-profile wlan-security
  authentication-profile wlan-authentication
```

```
 regulatory-domain-profile name domain1
 ap-group name ap-group1
  regulatory-domain-profile domain1
  radio 0
   vap-profile wlan-vap wlan 1
  radio 1
   vap-profile wlan-vap wlan 1
 ap-id 0 type-id 35 ap-mac 00e0-fc76-e360 ap-sn 210235554710CB000042
  ap-name area_1
  ap-group ap-group1
  radio 0
   channel 20mhz 6
   eirp 127
   calibrate auto-channel-select disable
   calibrate auto-txpower-select disable
  radio 1
   channel 20mhz 149
   eirp 127
   calibrate auto-channel-select disable
   calibrate auto-txpower-select disable
 ap-id 1 type-id 35 ap-mac 00e0-fc74-9640 ap-sn 210235419610D2000097
  ap-name area_2
  ap-group ap-group1
#
return
```

## 9.9.3 配置不同业务 VLAN 的 AP 间非快速漫游功能示例

### 配置流程

WLAN不同的特性和功能需要在不同类型的模板下进行配置和维护，这些模板统称为WLAN模板，如域管理模板、射频模板、VAP模板、AP系统模板、AP有线口模板、WIDS模板、WDS模板、Mesh模板。当用户在配置WLAN业务功能时，需要在对应功能的WLAN模板中进行参数配置，配置完成后，须将此模板引用到AP组或AP中，配置才会自动下发到AP，进而配置的功能在AP上生效。由于模板之间是存在相互引用关系的，因此在用户配置过程中，需要先了解各个模板之间存在的逻辑关系。模板的逻辑关系和基本配置流程请参见**WLAN业务配置流程**。

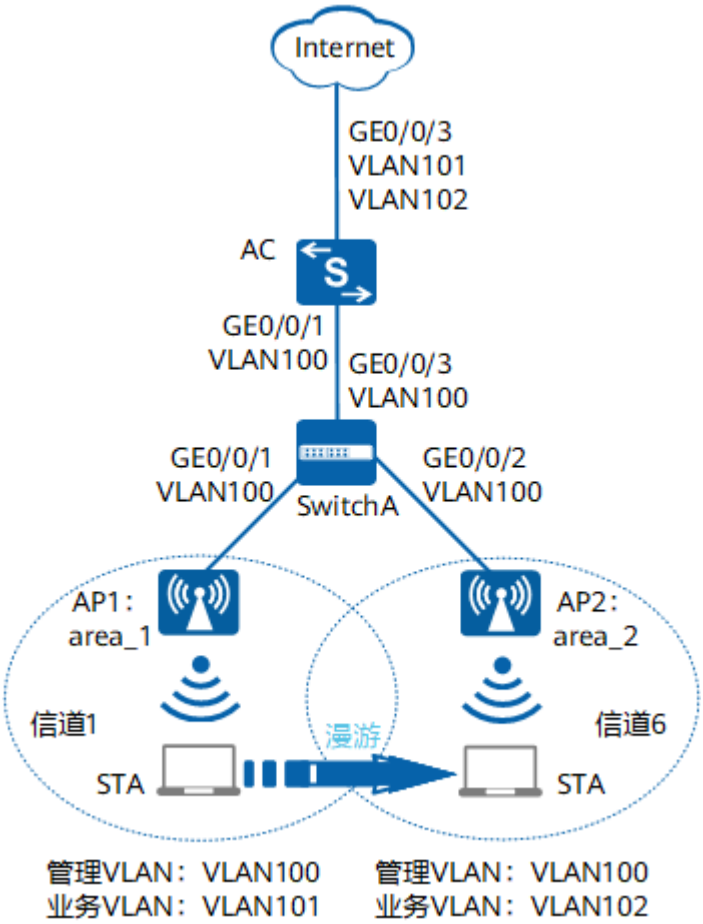
### 组网需求

如**图9-14**所示，某园区网部署两台AP，分别为两个部门的员工提供WLAN接入服务，通过AC集中管理和控制。AC为AP和STA动态分配IP地址。两个部门的用户分属于不同VLAN，即AP1和AP2采用不同的业务VLAN，分别为101和102。用户采用缺省安全策略，即WEP开放系统认证策略。用户的数据转发模式为隧道转发。

用户希望STA从AP1的无线信号覆盖区域移动到AP2的无线信号覆盖区域时业务不会中断。

**图 9-14** 配置不同业务 VLAN 的 AP 间非快速漫游组网图




## 配置思路

采用如下的思路配置不同业务VLAN的AP间非快速漫游：

1. 配置网络互通，使AP与AC之间能够传输CAPWAP报文。
2. 配置AC作为DHCP服务器，为STA和AP分配IP地址。
3. 配置WLAN基本业务，保证用户能够连接到无线网络。

**表 9-7** 数据规划表

| 配置项 | 数据 |
| --- | --- |
| DHCP服务器 | AC作为DHCP服务器为STA和AP分配IP地址 |
| AP的IP地址池 | 10.23.100.2～10.23.100.254/24 |
| STA的IP地址池 | 10.23.101.2～10.23.101.254/24<br>10.23.102.2～10.23.102.254/24 |
| AC的源接口IP地址 | VLANIF100：10.23.100.1/24 |

| 配置项 | 数据 |
| --- | --- |
| AP组 | • 名称：ap-group1<br>• 引用模板：VAP模板wlan-vap1、域管理模板domain1 |
| | • 名称：ap-group2<br>• 引用模板：VAP模板wlan-vap2、域管理模板domain1 |
| 域管理模板 | • 名称：domain1<br>• 国家码：CN |
| SSID模板 | • 名称：wlan-ssid<br>• SSID名称：wlan-net |
| 安全模板 | • 名称：wlan-security<br>• 安全策略：WPA2+PSK+AES<br>• 密码：a1234567 |
| VAP模板 | • 名称：wlan-vap1<br>• 转发模式：隧道转发<br>• 业务VLAN：VLAN101<br>• 引用模板：SSID模板wlan-ssid、安全模板wlan-security |
| | • 名称：wlan-vap2<br>• 转发模式：隧道转发<br>• 业务VLAN：VLAN102<br>• 引用模板：SSID模板wlan-ssid、安全模板wlan-security |

## 配置注意事项

- 纯组播报文由于协议要求在无线空口没有ACK机制保障，且无线空口链路不稳定，为了纯组播报文能够稳定发送，通常会以低速报文形式发送。如果网络侧有大量异常组播流量涌入，则会造成无线空口拥堵。为了减小大量低速组播报文对无线网络造成的冲击，建议配置组播报文抑制功能。配置前请确认是否有组播业务，如果有，请谨慎配置限速值。
  - 业务数据转发方式采用直接转发时，建议在直连AP的交换机接口上配置组播报文抑制。
  - 业务数据转发方式采用隧道转发时，建议在AC的流量模板下配置组播报文抑制。

  配置方法请参见：**如何配置组播报文抑制，减小大量低速组播报文对无线网络造成的冲击？**
- 建议在与AP直连的设备接口上配置端口隔离，如果不配置端口隔离，尤其是业务数据转发方式采用直接转发时，可能会在VLAN内形成大量不必要的广播报文，导致网络阻塞，影响用户体验。
- 隧道转发模式下，管理VLAN和业务VLAN不能配置为同一VLAN，且AP和AC之间只能放通管理VLAN，不能放通业务VLAN。

- V200R021C00版本开始，配置CAPWAP源接口或源地址时，会检查和安全相关的配置是否已存在，包括DTLS加密的PSK、AC间DTLS加密的PSK、登录AP的用户名和密码、全局离线管理VAP的登录密码，均已存在才能成功配置，否则会提示用户先完成相关的配置。
- V200R021C00版本开始，AC默认开启CAPWAP控制隧道的DTLS加密功能。开启该功能，添加AP时AP会上线失败，此时需要先开启CAPWAP DTLS不认证方式（**capwap dtls no-auth enable**）让AP上线，以便AP获取安全凭证，AP上线后应及时关闭该功能（**undo capwap dtls no-auth enable**），避免未授权AP上线。

## 操作步骤

**步骤1** 在AC上配置NAC模式为统一模式，以保证用户能够正常接入网络

```
<HUAWEI> system-view
[HUAWEI] authentication unified-mode
```

**说明**

如果当前NAC模式为传统模式，则配置NAC模式为统一模式后，需要保存配置并重启设备后生效。

**步骤2** 配置Switch_A和AC，使AP与AC之间能够传输CAPWAP报文

# 配置Switch_A的接口GE0/0/1～GE0/0/3都加入VLAN100（管理VLAN）。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch_A
[Switch_A] vlan batch 100
[Switch_A] interface gigabitethernet 0/0/1
[Switch_A-GigabitEthernet0/0/1] port link-type trunk
[Switch_A-GigabitEthernet0/0/1] port trunk pvid vlan 100
[Switch_A-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[Switch_A-GigabitEthernet0/0/1] port-isolate enable
[Switch_A-GigabitEthernet0/0/1] quit
[Switch_A] interface gigabitethernet 0/0/2
[Switch_A-GigabitEthernet0/0/2] port link-type trunk
[Switch_A-GigabitEthernet0/0/2] port trunk pvid vlan 100
[Switch_A-GigabitEthernet0/0/2] port trunk allow-pass vlan 100
[Switch_A-GigabitEthernet0/0/2] port-isolate enable
[Switch_A-GigabitEthernet0/0/2] quit
[Switch_A] interface gigabitethernet 0/0/3
[Switch_A-GigabitEthernet0/0/3] port link-type trunk
[Switch_A-GigabitEthernet0/0/3] port trunk allow-pass vlan 100
[Switch_A-GigabitEthernet0/0/3] quit
```

# 配置AC连接Switch_A的接口GE0/0/1加入VLAN100。

```
<HUAWEI> system-view
[HUAWEI] sysname AC
[AC] vlan batch 100
[AC] interface gigabitethernet 0/0/1
[AC-GigabitEthernet0/0/1] port link-type trunk
[AC-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[AC-GigabitEthernet0/0/1] quit
```

**步骤3** 配置AC与上层网络设备互通

# 配置AC上行接口GE0/0/3加入VLAN101和VLAN102。

```
[AC] vlan batch 101 102
[AC] interface gigabitethernet 0/0/3
[AC-GigabitEthernet0/0/3] port link-type trunk
[AC-GigabitEthernet0/0/3] port trunk allow-pass vlan 101 102
[AC-GigabitEthernet0/0/3] quit
```

**步骤4** 配置AC作为DHCP服务器，为STA和AP分配IP地址

# 配置基于接口地址池的DHCP服务器，其中，VLANIF100接口为AP1和AP2提供IP地址，VLANIF101为AP1下的STA提供IP地址，VLANIF102为AP2下的STA提供IP地址。

**说明**

DNS服务器地址请根据实际需要配置。常用配置方法如下：

- 接口地址池场景，需要在VLANIF接口视图下执行命令**dhcp server dns-list** *ip-address* &<1-8>。
- 全局地址池场景，需要在IP地址池视图下执行命令**dns-list** *ip-address* &<1-8>。

```
[AC] dhcp enable
[AC] interface vlanif 100
[AC-Vlanif100] ip address 10.23.100.1 24
[AC-Vlanif100] dhcp select interface
[AC-Vlanif100] quit
[AC] interface vlanif 101
[AC-Vlanif101] ip address 10.23.101.1 24
[AC-Vlanif101] dhcp select interface
[AC-Vlanif101] quit
[AC] interface vlanif 102
[AC-Vlanif102] ip address 10.23.102.1 24
[AC-Vlanif102] dhcp select interface
[AC-Vlanif102] quit
```

**步骤5** 配置AP上线

# 创建AP组，用于将相同配置的AP都加入同一AP组中。

```
[AC] wlan
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] quit
[AC-wlan-view] ap-group name ap-group2
[AC-wlan-ap-group-ap-group2] quit
```

# 创建域管理模板，在域管理模板下配置AC的国家码并在AP组下引用域管理模板。

```
[AC-wlan-view] regulatory-domain-profile name domain1
[AC-wlan-regulate-domain-domain1] country-code cn
[AC-wlan-regulate-domain-domain1] quit
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] regulatory-domain-profile domain1
Warning: This configuration change will clear the channel and power configurations of radios, and may restart APs. Continue?[Y/N]:y
[AC-wlan-ap-group-ap-group1] quit
[AC-wlan-view] ap-group name ap-group2
[AC-wlan-ap-group-ap-group2] regulatory-domain-profile domain1
Warning: This configuration change will clear the channel and power configurations of radios, and may restart APs. Continue?[Y/N]:y
[AC-wlan-ap-group-ap-group2] quit
[AC-wlan-view] quit
```

# 配置AC的源接口。

```
[AC] capwap source interface vlanif 100
```

# 在AC上离线导入AP1和AP2，并将AP1和AP2分别加入AP组“ap-group1”和“ap-group2”中。假设AP的MAC地址为00e0-fc76-e360和00e0-fc74-9640，并且根据AP的部署位置为AP配置名称，便于从名称上就能够了解AP的部署位置。例如MAC地址为00e0-fc76-e360的AP部署在1号区域，命名此AP为area_1。

**说明**

**ap auth-mode**命令缺省情况下为MAC认证，如果之前没有修改其缺省配置，可以不用执行**ap auth-mode mac-auth**命令。

举例中使用的AP为AP5030DN，具有射频0和射频1两个射频。AP5030DN的射频0为2.4GHz射频，射频1为5GHz射频。

```
[AC] wlan
[AC-wlan-view] ap auth-mode mac-auth
[AC-wlan-view] ap-id 0 ap-mac 00e0-fc76-e360
[AC-wlan-ap-0] ap-name area_1
Warning: This operation may cause AP reset. Continue? [Y/N]:y
[AC-wlan-ap-0] ap-group ap-group1
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configuration s of the radio, Whether to continue? [Y/N]:y
[AC-wlan-ap-0] quit
[AC-wlan-view] ap-id 1 ap-mac 00e0-fc74-9640
[AC-wlan-ap-1] ap-name area_2
Warning: This operation may cause AP reset. Continue? [Y/N]:y
[AC-wlan-ap-1] ap-group ap-group2
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configuration s of the radio, Whether to continue? [Y/N]:y
[AC-wlan-ap-1] quit
```

# 将AP上电后，当执行命令**display ap all**查看到AP的“State”字段为“nor”时，表示AP正常上线。

```
[AC-wlan-view] display ap all
Total AP information:
nor  : normal          [2]
-------------------------------------------------------------------------------------------------
ID   MAC            Name   Group     IP            Type          State STA Uptime     ExtraInfo
-------------------------------------------------------------------------------------------------
0    00e0-fc76-e360 area_1 ap-group1 10.23.100.254 AP5030DN      nor   0   5M:2S      -
1    00e0-fc74-9640 area_2 ap-group2 10.23.100.253 AP5030DN      nor   0   5M:4S      -
-------------------------------------------------------------------------------------------------
Total: 2
```

**步骤6** 配置WLAN业务参数

# 创建名为“wlan-security”的安全模板，并配置安全策略。

**说明**

举例中以配置WPA2+PSK+AES的安全策略为例，密码为“a1234567”，实际配置中请根据实际情况，配置符合实际要求的安全策略。

```
[AC-wlan-view] security-profile name wlan-security
[AC-wlan-sec-prof-wlan-security] security wpa2 psk pass-phrase a1234567 aes
[AC-wlan-sec-prof-wlan-security] quit
```

# 创建名为“wlan-ssid”的SSID模板，并配置SSID名称为“wlan-net”。

```
[AC-wlan-view] ssid-profile name wlan-ssid
[AC-wlan-ssid-prof-wlan-ssid] ssid wlan-net
[AC-wlan-ssid-prof-wlan-ssid] quit
```

# 分别创建名为“wlan-vap1”和“wlan-vap2”的VAP模板，配置业务数据转发模式、业务VLAN，并且引用安全模板和SSID模板。

```
[AC-wlan-view] vap-profile name wlan-vap1
[AC-wlan-vap-prof-wlan-vap1] forward-mode tunnel
[AC-wlan-vap-prof-wlan-vap1] service-vlan vlan-id 101
[AC-wlan-vap-prof-wlan-vap1] security-profile wlan-security
[AC-wlan-vap-prof-wlan-vap1] ssid-profile wlan-ssid
[AC-wlan-vap-prof-wlan-vap1] quit
[AC-wlan-view] vap-profile name wlan-vap2
```

```
[AC-wlan-vap-prof-wlan-vap2] forward-mode tunnel
[AC-wlan-vap-prof-wlan-vap2] service-vlan vlan-id 102
[AC-wlan-vap-prof-wlan-vap2] security-profile wlan-security
[AC-wlan-vap-prof-wlan-vap2] ssid-profile wlan-ssid
[AC-wlan-vap-prof-wlan-vap2] quit
```

# 配置AP组“ap-group1”和“ap-group2”分别引用VAP模板“wlan-vap1”和“wlan-vap2”，AP上射频0和射频1都使用VAP模板的配置。

```
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] vap-profile wlan-vap1 wlan 1 radio 0
[AC-wlan-ap-group-ap-group1] vap-profile wlan-vap1 wlan 1 radio 1
[AC-wlan-ap-group-ap-group1] quit
[AC-wlan-view] ap-group name ap-group2
[AC-wlan-ap-group-ap-group2] vap-profile wlan-vap2 wlan 1 radio 0
[AC-wlan-ap-group-ap-group2] vap-profile wlan-vap2 wlan 1 radio 1
[AC-wlan-ap-group-ap-group2] quit
```

**步骤7** 配置AP射频的信道和功率

**说明**

射频的信道和功率自动调优功能默认开启，如果不关闭此功能则会导致手动配置不生效。举例中AP射频的信道和功率仅为示例，实际配置中请根据AP的国家码和网规结果进行配置。

# 关闭AP射频0的信道和功率自动调优功能，并配置AP射频0的信道和功率。

```
[AC-wlan-view] ap-id 0
[AC-wlan-ap-0] radio 0
[AC-wlan-radio-0/0] calibrate auto-channel-select disable
[AC-wlan-radio-0/0] calibrate auto-txpower-select disable
[AC-wlan-radio-0/0] channel 20mhz 6
Warning: This action may cause service interruption. Continue?[Y/N]y
[AC-wlan-radio-0/0] eirp 127
[AC-wlan-radio-0/0] quit
```

# 关闭AP射频1的信道和功率自动调优功能，并配置AP射频1的信道和功率。

```
[AC-wlan-ap-0] radio 1
[AC-wlan-radio-0/1] calibrate auto-channel-select disable
[AC-wlan-radio-0/1] calibrate auto-txpower-select disable
[AC-wlan-radio-0/1] channel 20mhz 149
Warning: This action may cause service interruption. Continue?[Y/N]y
[AC-wlan-radio-0/1] eirp 127
[AC-wlan-radio-0/1] quit
[AC-wlan-ap-0] quit
```

**步骤8** 验证配置结果

配置完成后，执行命令**display vap ssid wlan-net**查看VAP信息，当“Status”显示为“ON”时，表示AP对应射频上的VAP已创建成功。

```
[AC-wlan-view] display vap ssid wlan-net
Info: This operation may take a few seconds, please wait.
WID : WLAN ID
--------------------------------------------------------------------------------
AP ID AP name RfID WID  BSSID       Status  Auth type     STA  SSID
--------------------------------------------------------------------------------
0     area_1  0    1    00E0-FC76-E360 ON    WPA2-PSK      0    wlan-net
0     area_1  1    1    00E0-FC76-E370 ON    WPA2-PSK      0    wlan-net
1     area_2  0    1    00E0-FC74-9640 ON    WPA2-PSK      0    wlan-net
1     area_2  1    1    00E0-FC74-9650 ON    WPA2-PSK      0    wlan-net
--------------------------------------------------------------------------------
Total: 4
```

STA在AP1的覆盖范围内搜索到SSID为“wlan-net”的无线网络，输入密码“a1234567”并正常关联后，在AC上执行命令**display station ssid wlan-net**，查看STA的接入信息，可以看到STA关联到了AP1，STA的MAC地址为“00e0-fc12-3458”。

```
[AC-wlan-view] display station ssid wlan-net
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  IP address
--------------------------------------------------------------------------------
00e0-fc12-3458  0     area_1   1/1      5G    11n   38/64      -68   101   10.23.101.254
--------------------------------------------------------------------------------
Total: 1 2.4G: 0 5G: 1
```

当STA从AP1的覆盖范围移动到AP2的覆盖范围时，在AC上执行命令**display station ssid wlan-net**，查看STA的接入信息，可以看到STA关联到了AP2。

```
[AC-wlan-view] display station ssid wlan-net
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  IP address
--------------------------------------------------------------------------------
00e0-fc12-3458  1     area_2   1/1      5G    11n   46/59      -58   101   10.23.101.254
--------------------------------------------------------------------------------
Total: 1 2.4G: 0 5G: 1
```

在AC上执行命令**display station roam-track sta-mac e019-1dc7-1e08**，可以查看该STA的漫游轨迹。

```
[AC-wlan-view] display station roam-track sta-mac e019-1dc7-1e08
Access SSID:huawei
Rx/Tx:link receive rate/link transmit rate(Mbps)
c:PMK Cache Roam r:802.11r Roam s:Same Frequency Network
--------------------------------------------------------------------------------
L2/L3           AC IP                AP name              Radio ID
BSSID           TIME                 In/Out RSSI          Out Rx/Tx
--------------------------------------------------------------------------------
--              10.23.100.1          area_1               0
00e0-fc76-e360  2015/02/07 17:48:30  -51/-48              46/13
L2              10.23.100.1          area_2               0
00e0-fc74-9640  2015/02/07 17:54:50  -58/-                -/-
--------------------------------------------------------------------------------
Number: 1
```

**----结束**

## 配置文件

- 接入交换机的配置文件

```
#
sysname Switch_A
#
vlan batch 100
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100
 port-isolate enable group 1
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100
 port-isolate enable group 1
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 100
#
return
```

- AC的配置文件

```
#
sysname AC
```

```
#
vlan batch 100 to 102
#
dhcp enable
#
interface Vlanif100
 ip address 10.23.100.1 255.255.255.0
 dhcp select interface
#
interface Vlanif101
 ip address 10.23.101.1 255.255.255.0
 dhcp select interface
#
interface Vlanif102
 ip address 10.23.102.1 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 101 to 102
#
capwap source interface vlanif100
#
wlan
 security-profile name wlan-security
  security wpa2 psk pass-phrase %^%#m"tz0f>~7.[`^6RWdzwCy16hJj/Mc!,}s`X*B]}A%^%# aes
 ssid-profile name wlan-ssid
  ssid wlan-net
 vap-profile name wlan-vap1
  forward-mode tunnel
  service-vlan vlan-id 101
  ssid-profile wlan-ssid
  security-profile wlan-security
 vap-profile name wlan-vap2
  forward-mode tunnel
  service-vlan vlan-id 102
  ssid-profile wlan-ssid
  security-profile wlan-security
 regulatory-domain-profile name domain1
 ap-group name ap-group1
  regulatory-domain-profile domain1
  radio 0
   vap-profile wlan-vap1 wlan 1
  radio 1
   vap-profile wlan-vap1 wlan 1
 ap-group name ap-group2
  regulatory-domain-profile domain1
  radio 0
   vap-profile wlan-vap2 wlan 1
  radio 1
   vap-profile wlan-vap2 wlan 1
 ap-id 0 type-id 35 ap-mac 00e0-fc76-e360 ap-sn 210235554710CB000042
  ap-name area_1
  ap-group ap-group1
  radio 0
   channel 20mhz 6
   eirp 127
   calibrate auto-channel-select disable
   calibrate auto-txpower-select disable
  radio 1
   channel 20mhz 149
   eirp 127
   calibrate auto-channel-select disable
   calibrate auto-txpower-select disable
 ap-id 1 type-id 35 ap-mac 00e0-fc74-9640 ap-sn 210235554710CB000078
```

```
 ap-name area_2
 ap-group ap-group2
 #
return
```

## 9.9.4 配置不同业务 VLAN 的 AP 间快速漫游功能示例

### 配置流程

WLAN不同的特性和功能需要在不同类型的模板下进行配置和维护，这些模板统称为WLAN模板，如域管理模板、射频模板、VAP模板、AP系统模板、AP有线口模板、WIDS模板、WDS模板、Mesh模板。当用户在配置WLAN业务功能时，需要在对应功能的WLAN模板中进行参数配置，配置完成后，须将此模板引用到AP组或AP中，配置才会自动下发到AP，进而配置的功能在AP上生效。由于模板之间是存在相互引用关系的，因此在用户配置过程中，需要先了解各个模板之间存在的逻辑关系。模板的逻辑关系和基本配置流程请参见**WLAN业务配置流程**。

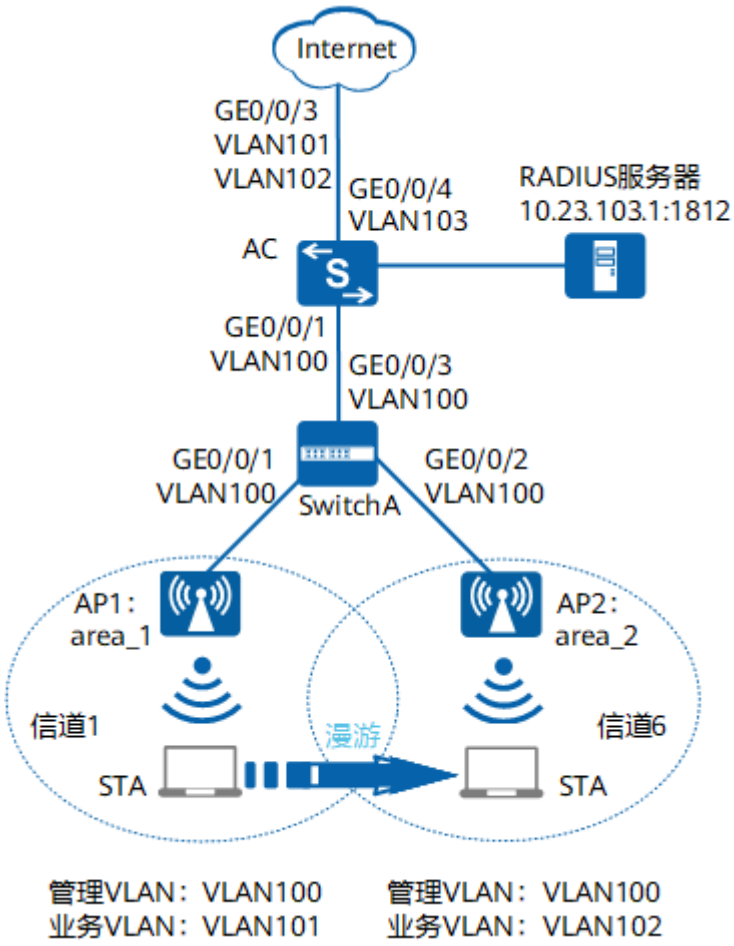
### 组网需求

如**图9-15**所示，某园区网部署两台AP，分别为两个部门的员工提供WLAN接入服务，通过AC集中管理和控制。AC为AP和STA动态分配IP地址。两个部门的用户分属于不同VLAN，即AP1和AP2采用不同的业务VLAN，分别为101和102。用户采用的安全策略为WPA2+802.1X+AES，数据转发模式为隧道转发。

用户希望STA从AP1的无线信号覆盖区域移动到AP2的无线信号覆盖区域时业务不会中断。

**图 9-15** 配置不同业务 VLAN 的 AP 间快速漫游组网图




## 配置思路

采用如下的思路配置不同业务VLAN的AP间快速漫游：

1. 用户采用的安全策略为WPA2+802.1X+AES，需要进行接入认证，漫游切换时间较长。因此，通过配置同一业务VLAN的AP间快速漫游，实现用户在漫游过程中业务不中断。
2. 配置网络互通，使AP与AC之间能够传输CAPWAP报文。
3. 配置AC作为DHCP服务器，为STA和AP分配IP地址。
4. 配置WLAN基本业务，保证用户能够连接到无线网络。
5. 配置密钥协商下移功能，缩短用户漫游的切换时间。

**表 9-8** 数据规划表

| 配置项 | 数据 |
| --- | --- |
| DHCP服务器 | AC作为DHCP服务器为STA和AP分配IP地址 |
| AP的IP地址池 | 10.23.100.2～10.23.100.254/24 |

| 配置项 | 数据 |
| --- | --- |
| STA的IP地址池 | 10.23.101.2～10.23.101.254/24<br>10.23.102.2～10.23.102.254/24 |
| AC的源接口IP地址 | VLANIF100：10.23.100.1/24 |
| RADIUS认证参数 | • RADIUS服务器模板名称：radius_huawei<br>• IP地址：10.23.103.1<br>• 认证端口号：1812<br>• 共享密钥：huawei@123<br>• 认证方案：radius_huawei |
| STA的用户名和密码 | • 用户名：test@huawei.com<br>• 密码：123456 |
| 802.1X接入模板 | • 名称：wlan-dot1x<br>• 认证方式：EAP |
| 认证模板 | • 名称：wlan-authentication<br>• 引用模板和认证方案：802.1X接入模板wlan-dot1x、认证方案radius_huawei、RADIUS服务器模板radius_huawei |
| AP组 | • 名称：ap-group1<br>• 引用模板：VAP模板wlan-vap1、域管理模板domain1 |
| | • 名称：ap-group2<br>• 引用模板：VAP模板wlan-vap2、域管理模板domain1 |
| 域管理模板 | • 名称：domain1<br>• 国家码：CN |
| SSID模板 | • 名称：wlan-ssid<br>• SSID名称：wlan-net |
| 安全模板 | • 名称：wlan-security<br>• 安全策略：WPA2+802.1X+AES |
| VAP模板 | • 名称：wlan-vap1<br>• 转发模式：隧道转发<br>• 业务VLAN：VLAN101<br>• 引用模板：SSID模板wlan-ssid、安全模板wlan-security、认证模板wlan-authentication |

| 配置项 | 数据 |
| --- | --- |
| | • 名称：wlan-vap2<br>• 转发模式：隧道转发<br>• 业务VLAN：VLAN102<br>• 引用模板：SSID模板wlan-ssid、安全模板wlan-security、认证模板wlan-authentication |

## 配置注意事项

- 纯组播报文由于协议要求在无线空口没有ACK机制保障，且无线空口链路不稳定，为了纯组播报文能够稳定发送，通常会以低速报文形式发送。如果网络侧有大量异常组播流量涌入，则会造成无线空口拥堵。为了减小大量低速组播报文对无线网络造成的冲击，建议配置组播报文抑制功能。配置前请确认是否有组播业务，如果有，请谨慎配置限速值。
  - 业务数据转发方式采用直接转发时，建议在直连AP的交换机接口上配置组播报文抑制。
  - 业务数据转发方式采用隧道转发时，建议在AC的流量模板下配置组播报文抑制。

  配置方法请参见：**如何配置组播报文抑制，减小大量低速组播报文对无线网络造成的冲击?**
- 建议在与AP直连的设备接口上配置端口隔离，如果不配置端口隔离，尤其是业务数据转发方式采用直接转发时，可能会在VLAN内形成大量不必要的广播报文，导致网络阻塞，影响用户体验。
- 隧道转发模式下，管理VLAN和业务VLAN不能配置为同一VLAN，且AP和AC之间只能放通管理VLAN，不能放通业务VLAN。
- V200R021C00版本开始，配置CAPWAP源接口或源地址时，会检查和安全相关的配置是否已存在，包括DTLS加密的PSK、AC间DTLS加密的PSK、登录AP的用户名和密码、全局离线管理VAP的登录密码，均已存在才能成功配置，否则会提示用户先完成相关的配置。
- V200R021C00版本开始，AC默认开启CAPWAP控制隧道的DTLS加密功能。开启该功能，添加AP时AP会上线失败，此时需要先开启CAPWAP DTLS不认证方式（**capwap dtls no-auth enable**）让AP上线，以便AP获取安全凭证，AP上线后应及时关闭该功能（**undo capwap dtls no-auth enable**），避免未授权AP上线。

## 操作步骤

**步骤1** 在AC上配置NAC模式为统一模式，以保证用户能够正常接入网络

```
<HUAWEI> system-view
[HUAWEI] authentication unified-mode
```

**说明**

如果当前NAC模式为传统模式，则配置NAC模式为统一模式后，需要保存配置并重启设备后生效。

**步骤2** 配置Switch_A和AC，使AP与AC之间能够传输CAPWAP报文

# 配置Switch_A的接口GE0/0/1～GE0/0/3都加入VLAN100（管理VLAN）。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch_A
[Switch_A] vlan batch 100
[Switch_A] interface gigabitethernet 0/0/1
[Switch_A-GigabitEthernet0/0/1] port link-type trunk
[Switch_A-GigabitEthernet0/0/1] port trunk pvid vlan 100
[Switch_A-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[Switch_A-GigabitEthernet0/0/1] port-isolate enable
[Switch_A-GigabitEthernet0/0/1] quit
[Switch_A] interface gigabitethernet 0/0/2
[Switch_A-GigabitEthernet0/0/2] port link-type trunk
[Switch_A-GigabitEthernet0/0/2] port trunk pvid vlan 100
[Switch_A-GigabitEthernet0/0/2] port trunk allow-pass vlan 100
[Switch_A-GigabitEthernet0/0/2] port-isolate enable
[Switch_A-GigabitEthernet0/0/2] quit
[Switch_A] interface gigabitethernet 0/0/3
[Switch_A-GigabitEthernet0/0/3] port link-type trunk
[Switch_A-GigabitEthernet0/0/3] port trunk allow-pass vlan 100
[Switch_A-GigabitEthernet0/0/3] quit
```

# 配置AC连接Switch_A的接口GE0/0/1加入VLAN100。

```
<HUAWEI> system-view
[HUAWEI] sysname AC
[AC] vlan batch 100
[AC] interface gigabitethernet 0/0/1
[AC-GigabitEthernet0/0/1] port link-type trunk
[AC-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[AC-GigabitEthernet0/0/1] quit
```

**步骤3** 配置AC与上层网络设备互通

# 配置AC上行接口GE0/0/3加入VLAN101和VLAN102并配置AC连接RADIUS服务器的接口GE0/0/4加入VLAN103。

```
[AC] vlan batch 101 to 103
[AC] interface gigabitethernet 0/0/3
[AC-GigabitEthernet0/0/3] port link-type trunk
[AC-GigabitEthernet0/0/3] port trunk allow-pass vlan 101 102
[AC-GigabitEthernet0/0/3] quit
[AC] interface gigabitethernet 0/0/4
[AC-GigabitEthernet0/0/4] port link-type trunk
[AC-GigabitEthernet0/0/4] port trunk pvid vlan 103
[AC-GigabitEthernet0/0/4] port trunk allow-pass vlan 103
[AC-GigabitEthernet0/0/4] quit
```

**步骤4** 配置AC作为DHCP服务器，为STA和AP分配IP地址。配置VLANIF103，使AC和RADIUS服务器之间能够通信

# 配置基于接口地址池的DHCP服务器，其中，VLANIF100接口为AP1和AP2提供IP地址，VLANIF101为AP1下的STA提供IP地址，VLANIF102为AP2下的STA提供IP地址。

**说明**

DNS服务器地址请根据实际需要配置。常用配置方法如下：

- 接口地址池场景，需要在VLANIF接口视图下执行命令**dhcp server dns-list** *ip-address* &<1-8>。
- 全局地址池场景，需要在IP地址池视图下执行命令**dns-list** *ip-address* &<1-8>。

```
[AC] dhcp enable
[AC] interface vlanif 100
[AC-Vlanif100] ip address 10.23.100.1 24
[AC-Vlanif100] dhcp select interface
[AC-Vlanif100] quit
[AC] interface vlanif 101
[AC-Vlanif101] ip address 10.23.101.1 24
[AC-Vlanif101] dhcp select interface
```

```
[AC-Vlanif101] quit
[AC] interface vlanif 102
[AC-Vlanif102] ip address 10.23.102.1 24
[AC-Vlanif102] dhcp select interface
[AC-Vlanif102] quit
```

# 配置VLANIF103。

```
[AC] interface vlanif 103
[AC-Vlanif103] ip address 10.23.103.2 24
[AC-Vlanif103] quit
```

**步骤5** 配置RADIUS认证参数

**说明**

请确保AC与RADIUS服务器的共享密钥相同。

# 创建RADIUS服务器模板。

```
[AC] radius-server template radius_huawei
[AC-radius-radius_huawei] radius-server authentication 10.23.103.1 1812
[AC-radius-radius_huawei] radius-server shared-key cipher huawei@123
[AC-radius-radius_huawei] quit
```

# 创建RADIUS方式的认证方案。

```
[AC] aaa
[AC-aaa] authentication-scheme radius_huawei
[AC-aaa-authen-radius_huawei] authentication-mode radius
[AC-aaa-authen-radius_huawei] quit
```

# 创建AAA域并配置域的RADIUS服务器模板和认证方案。

```
[AC-aaa] domain huawei.com
[AC-aaa-domain-huawei.com] radius-server radius_huawei
[AC-aaa-domain-huawei.com] authentication-scheme radius_huawei
[AC-aaa-domain-huawei.com] quit
[AC-aaa] quit
```

**说明**

配置了域“huawei.com”后，认证用户名后面需要加上域名。

# 测试用户是否能够通过RADIUS模板的认证。（已在RADIUS服务器上配置了测试用户test@huawei.com，用户密码123456）

```
[AC] test-aaa test@huawei.com 123456 radius-template radius_huawei
Info: Account test succeed.
```

**步骤6** 配置802.1X接入模板，管理802.1X接入控制参数

# 创建名为“wlan-dot1x”的802.1X接入模板。

```
[AC] dot1x-access-profile name wlan-dot1x
```

# 配置认证方式为EAP中继模式。

```
[AC-dot1x-access-profile-wlan-dot1x] dot1x authentication-method eap
[AC-dot1x-access-profile-wlan-dot1x] quit
```

**步骤7** 创建名为“wlan-authentication”的认证模板，绑定802.1X接入模板，并配置用户强制域

```
[AC] authentication-profile name wlan-authentication
[AC-authen-profile-wlan-authentication] dot1x-access-profile wlan-dot1x
[AC-authen-profile-wlan-authentication] access-domain huawei.com dot1x force
[AC-authen-profile-wlan-authentication] quit
```

**步骤8** 配置AP上线

# 创建AP组，用于将相同配置的AP都加入同一AP组中。

```
[AC] wlan
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] quit
[AC-wlan-view] ap-group name ap-group2
[AC-wlan-ap-group-ap-group2] quit
```

# 创建域管理模板，在域管理模板下配置AC的国家码并在AP组下引用域管理模板。

```
[AC-wlan-view] regulatory-domain-profile name domain1
[AC-wlan-regulate-domain-domain1] country-code cn
[AC-wlan-regulate-domain-domain1] quit
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] regulatory-domain-profile domain1
Warning: This configuration change will clear the channel and power configurations of radios, and may restart APs. Continue?[Y/N]:y
[AC-wlan-ap-group-ap-group1] quit
[AC-wlan-view] ap-group name ap-group2
[AC-wlan-ap-group-ap-group2] regulatory-domain-profile domain1
Warning: This configuration change will clear the channel and power configurations of radios, and may restart APs. Continue?[Y/N]:y
[AC-wlan-ap-group-ap-group2] quit
[AC-wlan-view] quit
```

# 配置AC的源接口。

```
[AC] capwap source interface vlanif 100
```

# 在AC上离线导入AP1和AP2，并将AP1和AP2分别加入AP组“ap-group1”和“ap-group2”中。假设AP的MAC地址为00e0-fc76-e360和00e0-fc74-9640，并且根据AP的部署位置为AP配置名称，便于从名称上就能够了解AP的部署位置。例如MAC地址为00e0-fc76-e360的AP部署在1号区域，命名此AP为area_1。

**说明**

**ap auth-mode**命令缺省情况下为MAC认证，如果之前没有修改其缺省配置，可以不用执行**ap auth-mode mac-auth**命令。

举例中使用的AP为AP5030DN，具有射频0和射频1两个射频。AP5030DN的射频0为2.4GHz射频，射频1为5GHz射频。

```
[AC] wlan
[AC-wlan-view] ap auth-mode mac-auth
[AC-wlan-view] ap-id 0 ap-mac 00e0-fc76-e360
[AC-wlan-ap-0] ap-name area_1
Warning: This operation may cause AP reset. Continue? [Y/N]:y
[AC-wlan-ap-0] ap-group ap-group1
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configuration s of the radio, Whether to continue? [Y/N]:y
[AC-wlan-ap-0] quit
[AC-wlan-view] ap-id 1 ap-mac 00e0-fc74-9640
[AC-wlan-ap-1] ap-name area_2
Warning: This operation may cause AP reset. Continue? [Y/N]:y
[AC-wlan-ap-1] ap-group ap-group2
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configuration s of the radio, Whether to continue? [Y/N]:y
[AC-wlan-ap-1] quit
```

# 将AP上电后，当执行命令**display ap all**查看到AP的“State”字段为“nor”时，表示AP正常上线。

```
[AC-wlan-view] display ap all
Total AP information:
nor  : normal          [2]
--------------------------------------------------------------------------------
ID   MAC            Name   Group     IP           Type           State STA Uptime     ExtraInfo
```

```
-------------------------------------------------------------------------------------------------
0    00e0-fc76-e360 area_1 ap-group1 10.23.100.254 AP5030DN      nor  0   5M:2S      -
1    00e0-fc74-9640 area_2 ap-group2 10.23.100.253 AP5030DN      nor  0   5M:4S      -
-------------------------------------------------------------------------------------------------
Total: 2
```

**步骤9** 配置WLAN业务参数

# 创建名为“wlan-security”的安全模板，并配置安全策略。

```
[AC-wlan-view] security-profile name wlan-security
[AC-wlan-sec-prof-wlan-security] security wpa2 dot1x aes
[AC-wlan-sec-prof-wlan-security] quit
```

# 创建名为“wlan-ssid”的SSID模板，并配置SSID名称为“wlan-net”。

```
[AC-wlan-view] ssid-profile name wlan-ssid
[AC-wlan-ssid-prof-wlan-ssid] ssid wlan-net
[AC-wlan-ssid-prof-wlan-ssid] quit
```

# 分别创建名为“wlan-vap1”和“wlan-vap2”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 wlan-vap1
[AC-wlan-vap-prof-wlan-vap1] forward-mode tunnel
[AC-wlan-vap-prof-wlan-vap1] service-vlan vlan-id 101
[AC-wlan-vap-prof-wlan-vap1] security-profile wlan-security
[AC-wlan-vap-prof-wlan-vap1] authentication-profile wlan-authentication
[AC-wlan-vap-prof-wlan-vap1] ssid-profile wlan-ssid
[AC-wlan-vap-prof-wlan-vap1] quit
[AC-wlan-view] vap-profile name wlan-vap2
[AC-wlan-vap-prof-wlan-vap2] forward-mode tunnel
[AC-wlan-vap-prof-wlan-vap2] service-vlan vlan-id 102
[AC-wlan-vap-prof-wlan-vap2] security-profile wlan-security
[AC-wlan-vap-prof-wlan-vap2] authentication-profile wlan-authentication
[AC-wlan-vap-prof-wlan-vap2] ssid-profile wlan-ssid
[AC-wlan-vap-prof-wlan-vap2] quit
```

# 配置AP组“ap-group1”和“ap-group2”分别引用VAP模板“wlan-vap1”和“wlan-vap2”，AP上射频0和射频1都使用VAP模板的配置。

```
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] vap-profile wlan-vap1 wlan 1 radio 0
[AC-wlan-ap-group-ap-group1] vap-profile wlan-vap1 wlan 1 radio 1
[AC-wlan-ap-group-ap-group1] quit
[AC-wlan-view] ap-group name ap-group2
[AC-wlan-ap-group-ap-group2] vap-profile wlan-vap2 wlan 1 radio 0
[AC-wlan-ap-group-ap-group2] vap-profile wlan-vap2 wlan 1 radio 1
[AC-wlan-ap-group-ap-group2] quit
```

**步骤10** 配置AP射频的信道和功率

**说明**

射频的信道和功率自动调优功能默认开启，如果不关闭此功能则会导致手动配置不生效。举例中AP射频的信道和功率仅为示例，实际配置中请根据AP的国家码和网规结果进行配置。

# 关闭AP射频0的信道和功率自动调优功能，并配置AP射频0的信道和功率。

```
[AC-wlan-view] ap-id 0
[AC-wlan-ap-0] radio 0
[AC-wlan-radio-0/0] calibrate auto-channel-select disable
[AC-wlan-radio-0/0] calibrate auto-txpower-select disable
[AC-wlan-radio-0/0] channel 20mhz 6
Warning: This action may cause service interruption. Continue?[Y/N]y
[AC-wlan-radio-0/0] eirp 127
[AC-wlan-radio-0/0] quit
```

# 关闭AP射频1的信道和功率自动调优功能，并配置AP射频1的信道和功率。

```
[AC-wlan-ap-0] radio 1
[AC-wlan-radio-0/1] calibrate auto-channel-select disable
[AC-wlan-radio-0/1] calibrate auto-txpower-select disable
[AC-wlan-radio-0/1] channel 20mhz 149
Warning: This action may cause service interruption. Continue?[Y/N]y
[AC-wlan-radio-0/1] eirp 127
[AC-wlan-radio-0/1] quit
[AC-wlan-ap-0] quit
```

**步骤11** 验证配置结果

完成配置后，用户可通过无线终端搜索到SSID为**wlan-net**的无线网络。用户在STA上使用802.1X客户端进行认证，输入正确的用户名和密码，STA认证成功后，可以正常访问Internet上的资源。需要根据设置的认证方式（peap）对客户端进行相应的配置。

- WINDOWS XP系统下的配置
  a. 首先在无线网络属性中，添加SSID为**wlan-net**，并选择认证方式为**WPA2**，加密方式为CCMP使用的算法**AES**。
  b. 在“验证”选项卡中，选择EAP类型为**PEAP**，单击“属性”，去掉验证服务器证书选项（此处不验证服务器证书），单击“配置”，去掉自动使用Windows登录名和密码选项，然后单击“确定”。
- WINDOWS 7系统下的配置
  a. 进入管理无线网络页面，单击“添加”，选择“手动创建网络配置文件”，添加SSID为**wlan-net**，并选择认证方式为**WPA2-企业**，加密使用的算法**AES**，单击“下一步”。
  b. 单击“更改连接设置”，进入“无线网络属性”界面，选择“安全”页签，单击“设置”，取消勾选“验证服务器证书”（此处不验证服务器证书），单击“配置”，取消勾选“自动使用Windows登录名和密码”，单击“确定”。
  c. 单击“确定”，返回“无线网络属性”界面，单击“高级设置”，在“高级设置”界面，勾选“指定身份验证模式”，并选择身份验证模式为“用户身份验证”，单击“确定”。

STA在AP1的覆盖范围内搜索到SSID为“wlan-net”的无线网络，输入密码“123456”并正常关联后，在AC上执行命令**display station ssid wlan-net**，查看STA的接入信息，可以看到STA关联到了AP1，STA的MAC地址为“00e0-fc12-3458”。

```
[AC-wlan-view] display station ssid wlan-net
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  IP address
--------------------------------------------------------------------------------
00e0-fc12-3458 0     area_1   1/1      5G    11n   38/64     -68   101   10.23.101.254
--------------------------------------------------------------------------------
Total: 1 2.4G: 0 5G: 1
```

当STA从AP1的覆盖范围移动到AP2的覆盖范围时，在AC上执行命令**display station ssid wlan-net**，查看STA的接入信息，可以看到STA关联到了AP2。

```
[AC-wlan-view] display station ssid wlan-net
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  IP address
--------------------------------------------------------------------------------
00e0-fc12-3458 1     area_2   1/1      5G    11n   46/59     -58   101   10.23.101.254
--------------------------------------------------------------------------------
Total: 1 2.4G: 0 5G: 1
```

在AC上执行命令**display station roam-track sta-mac e019-1dc7-1e08**，可以查看该STA的漫游轨迹。

```
[AC-wlan-view] display station roam-track sta-mac e019-1dc7-1e08
Access SSID:huawei
Rx/Tx:link receive rate/link transmit rate(Mbps)
c:PMK Cache Roam r:802.11r Roam s:Same Frequency Network
--------------------------------------------------------------------------------
L2/L3          AC IP                AP name             Radio ID
BSSID          TIME                 In/Out RSSI         Out Rx/Tx
--------------------------------------------------------------------------------
--             10.23.100.1          area_1              0
00e0-fc76-e360  2015/02/07 17:48:30    -51/-48             46/13
L2             10.23.100.1          area_2              0
00e0-fc74-9640  2015/02/07 17:54:50    -58/-               -/-
--------------------------------------------------------------------------------
Number: 1
```

**----结束**

# 配置文件

- 接入交换机的配置文件

```
#
sysname Switch_A
#
vlan batch 100
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100
 port-isolate enable group 1
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100
 port-isolate enable group 1
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 100
#
return
```

- AC的配置文件

```
#
sysname AC
#
vlan batch 100 to 103
#
authentication-profile name wlan-authentication
 dot1x-access-profile wlan-dot1x
 access-domain huawei.com dot1x force
#
dhcp enable
#
radius-server template radius_huawei
 radius-server shared-key cipher %^%#*7d1;XNof/|Q0:DsP!,W51DIYPx}`AARBdJ'0B^$%^%#
 radius-server authentication 10.23.103.1 1812 weight 80
#
aaa
 authentication-scheme radius_huawei
  authentication-mode radius
 domain huawei.com
  authentication-scheme radius_huawei
  radius-server radius_huawei
#
```

```
interface Vlanif100
 ip address 10.23.100.1 255.255.255.0
 dhcp select interface
#
interface Vlanif101
 ip address 10.23.101.1 255.255.255.0
 dhcp select interface
#
interface Vlanif102
 ip address 10.23.102.1 255.255.255.0
 dhcp select interface
#
interface Vlanif103
 ip address 10.23.103.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 101 to 102
#
interface GigabitEthernet0/0/4
 port link-type trunk
 port trunk pvid vlan 103
 port trunk allow-pass vlan 103
#
capwap source interface vlanif100
#
wlan
 security-profile name wlan-security
  security wpa2 dot1x aes
 ssid-profile name wlan-ssid
  ssid wlan-net
 vap-profile name wlan-vap1
  forward-mode tunnel
  service-vlan vlan-id 101
  ssid-profile wlan-ssid
  security-profile wlan-security
  authentication-profile wlan-authentication
 vap-profile name wlan-vap2
  forward-mode tunnel
  service-vlan vlan-id 102
  ssid-profile wlan-ssid
  security-profile wlan-security
  authentication-profile wlan-authentication
 regulatory-domain-profile name domain1
 ap-group name ap-group1
  regulatory-domain-profile domain1
  radio 0
   vap-profile wlan-vap1 wlan 1
  radio 1
   vap-profile wlan-vap1 wlan 1
 ap-group name ap-group2
  regulatory-domain-profile domain1
  radio 0
   vap-profile wlan-vap2 wlan 1
  radio 1
   vap-profile wlan-vap2 wlan 1
 ap-id 0 type-id 35 ap-mac 00e0-fc76-e360 ap-sn 210235554710CB000042
  ap-name area_1
  ap-group ap-group1
  radio 0
   channel 20mhz 6
   eirp 127
   calibrate auto-channel-select disable
   calibrate auto-txpower-select disable
  radio 1
```

```
 channel 20mhz 149
 eirp 127
 calibrate auto-channel-select disable
 calibrate auto-txpower-select disable
ap-id 1 type-id 35 ap-mac 00e0-fc74-9640 ap-sn 210235554710CB000078
 ap-name area_2
 ap-group ap-group2
#
dot1x-access-profile name wlan-dot1x
#
return
```

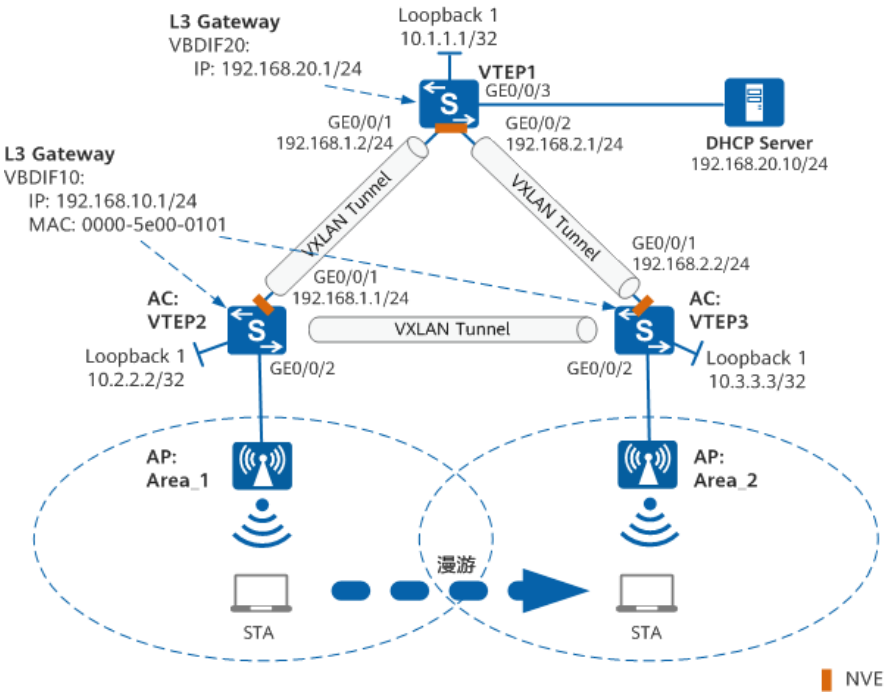
# 9.9.5 配置 VXLAN 分布式网关组网下 AC 间二层漫游示例

## 组网需求

某企业有部署在不同区域的AC设备，AC设备上配置VXLAN分布式网关及DHCP Relay功能，无线用户通过AC设备下挂的AP设备接入网络，由DHCP Server分配IP地址。现在需求为实现AC设备间用户的二层漫游。

图9-16所示，STA在Area_1和Area_2之间实现二层漫游。

**图 9-16** 配置 VXLAN 分布式网关组网下 AC 间二层漫游组网图




**说明**

本举例中交换机仅S5731-H、S5731-H-K、S5731S-H、S5732-H、S5732-H-K、S6730-H-K、S6730S-H和S6730-H支持。

## 数据准备

**表 9-9** 配置 BGP EVPN 相关数据

| 设备 | EVPN实例 | RD值 | BD | VNI | Router id | Peer IP |
| --- | --- | --- | --- | --- | --- | --- |
| VTEP1 | evpn20：<br>● IRT：20:1<br>● ERT：20:1；1:100 | 1:20 | 20 | 20 | 10.1.1.1 | 10.2.2.2；10.3.3.3 |
| VTEP2 | evpn10：<br>● IRT：10:1<br>● ERT：10:1；1:100 | 2:10 | 10 | 10 | 10.2.2.2 | 10.1.1.1；10.3.3.3 |
| VTEP3 | evpn10：<br>● IRT：10:1<br>● ERT：10:1；1:100 | 3:10 | 10 | 10 | 10.3.3.3 | 10.1.1.1；10.2.2.2 |

**表 9-10** 配置 VPN 实例相关数据

| 设备 | 接口 | VPN实例 | VNI | RD值 |
| --- | --- | --- | --- | --- |
| VTEP1 | VBDIF 20 | vpn1：<br>● IRT(EVPN): 1:100<br>● ERT(EVPN): 1:100 | 100 | 1:100 |
| VTEP2 | VBDIF 10 | vpn1：<br>● IRT(EVPN): 1:100<br>● ERT(EVPN): 1:100 | 100 | 2:100 |

| 设备 | 接口 | VPN实例 | VNI | RD值 |
| --- | --- | --- | --- | --- |
| VTEP3 | VBDIF 10 | vpn1：<br>• IRT(EVPN): 1:100<br>• ERT(EVPN): 1:100 | 100 | 3:100 |

**表 9-11** AC 数据规划表

| 配置项 | VTEP2 | VTEP3 |
| --- | --- | --- |
| AP的IP地址分配 | VTEP2配置基于接口VLANIF100的DHCP服务器，为相连的AP分配IP地址。 | VTEP3配置基于接口VLANIF200的DHCP服务器，为相连的AP分配IP地址。 |
| AP的IP地址池 | 192.168.100.2～192.168.100.254/24 | 192.168.200.2～192.168.200.254/24 |
| STA的IP地址池 | 192.168.10.2～192.168.10.254/24 | 192.168.10.2～192.168.10.254/24 |
| AC的源接口IP地址 | 源接口：<br>VLANIF100：192.168.100.1/24 | 源接口：<br>VLANIF200：192.168.200.1/24 |
| AP组 | • 名称：ap-group1<br>• 引用模板：VAP模板wlan-net、域管理模板default | |
| 域管理模板 | • 名称：default<br>• 国家码：中国 | |
| SSID模板 | • 名称：wlan-net<br>• SSID名称：wlan-net | |
| 安全模板 | • 名称：wlan-net<br>• 安全策略：WPA-WPA2+PSK+AES<br>• 密码：a1234567 | |
| VAP模板 | • 名称：wlan-net<br>• 转发模式：隧道转发<br>• 业务VLAN：VLAN10<br>• 引用模板：SSID模板wlan-net、安全模板wlan-net | |
| 漫游参数 | • 漫游组内AC间建链的IP地址：192.168.100.1<br>• 漫游组名称：mobility<br>• 漫游组成员：VTEP1和VTEP2 | • 漫游组内AC间建链的IP地址：192.168.200.1<br>• 漫游组名称：mobility<br>• 漫游组成员：VTEP1和VTEP2 |

## 配置思路

采用如下思路配置VXLAN分布式网关组网下AC间二层漫游：

1. 配置VXLAN网络。
   a. 分别在VTEP1、VTEP2、VTEP3上配置路由协议，保证网络三层互通。
   b. 分别在VTEP1、VTEP2、VTEP3上配置VXLAN接入业务部署方式。
   c. 分别在VTEP1、VTEP2、VTEP3上配置EVPN实例并绑定BD域。
   d. 分别在VTEP1、VTEP2、VTEP3上配置VPN实例并绑定VBDIF接口。
   e. 分别在VTEP1、VTEP2、VTEP3上配置它们之间的BGP EVPN对等体关系。
   f. 分别在VTEP1、VTEP2、VTEP3上配置VXLAN隧道目的端地址。
   g. 分别在VTEP1、VTEP2、VTEP3上配置VXLAN网关。
2. 配置分布式网关的DHCP Relay功能。
3. 在VTEP2、VTEP3上配置VXLAN隧道侧接口加入端口防攻击的白名单。
4. 配置DHCP Server，为STA用户分配IP地址。
5. 在VTEP2和VTEP3上配置AP管理VLAN的接入，并配置DHCP服务器功能，为AP分配管理IP。
6. 在VTEP2和VTEP3上配置路由协议，实现AP管理IP网关之间的互通。
7. 在VTEP2和VTEP3上配置AP上线。
8. 在VTEP2和VTEP3上配置WLAN业务参数，实现STA访问WLAN网络功能。
9. 在VTEP2和VTEP3上配置WLAN漫游功能，实现AC间二层漫游。

**说明**

园区网络的三层互通是构建虚拟网络的基础条件，现网中，如果园区网络已经实现三层网络的互通，那么该举例中的步骤1可以省略。

## 配置注意事项

- 同一漫游组内的AC必须使用相同的软件C版本，否则可能会导致AC间漫游失败。
- 漫游组内每个AC上均需要配置AC间建链的IP地址、漫游组，并添加成员AC。
- 配置的漫游组内AC间建链的IP地址必须是AC的CAPWAP源IP地址。当配置了多个CAPWAP源地址时，仅可以指定一个CAPWAP源地址作为AC间建链地址。
- 每个AC上漫游组名称必须一致。

## 操作步骤

**步骤1** 配置VXLAN网络

1. 配置路由协议

   # 配置VTEP1各接口IP地址。VTEP2和VTEP3的配置与VTEP1类似，这里不再赘述。配置OSPF时，注意需要发布设备上的Loopback接口地址。

```
<HUAWEI> system-view
[HUAWEI] sysname VTEP1
[VTEP1] interface loopback 1
[VTEP1-LoopBack1] ip address 10.1.1.1 32
[VTEP1-LoopBack1] quit
[VTEP1] interface gigabitethernet 0/0/1
[VTEP1-GigabitEthernet0/0/1] undo portswitch
[VTEP1-GigabitEthernet0/0/1] ip address 192.168.1.2 24
```

```
[VTEP1-GigabitEthernet0/0/1] quit
[VTEP1] interface gigabitethernet 0/0/2
[VTEP1-GigabitEthernet0/0/2] undo portswitch
[VTEP1-GigabitEthernet0/0/2] ip address 192.168.2.1 24
[VTEP1-GigabitEthernet0/0/2] quit
[VTEP1] ospf router-id 10.1.1.1
[VTEP1-ospf-1] area 0
[VTEP1-ospf-1-area-0.0.0.0] network 10.1.1.1 0.0.0.0
[VTEP1-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[VTEP1-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[VTEP1-ospf-1-area-0.0.0.0] quit
[VTEP1-ospf-1] quit
```

# OSPF成功配置后，VTEP1、VTEP2和VTEP3之间可通过OSPF协议发现对方的Loopback接口的IP地址，并能互相ping通。以VTEP1 ping VTEP2的显示为例。

```
[VTEP1] ping 10.2.2.2
 PING 10.2.2.2: 56  data bytes, press CTRL_C to break
   Reply from 10.2.2.2: bytes=56 Sequence=1 ttl=254 time=240 ms
   Reply from 10.2.2.2: bytes=56 Sequence=2 ttl=254 time=5 ms
   Reply from 10.2.2.2: bytes=56 Sequence=3 ttl=254 time=5 ms
   Reply from 10.2.2.2: bytes=56 Sequence=4 ttl=254 time=14 ms
   Reply from 10.2.2.2: bytes=56 Sequence=5 ttl=254 time=5 ms

 --- 10.2.2.2 ping statistics ---
   5 packet(s) transmitted
   5 packet(s) received
   0.00% packet loss
   round-trip min/avg/max = 5/53/240 ms
```

2. 分别在VTEP1、VTEP2、VTEP3上配置VXLAN业务接入点

   # 配置VTEP1。

   ```
   [VTEP1] vlan 20
   [VTEP1-vlan20] quit
   [VTEP1] bridge-domain 20
   [VTEP1-bd20] l2 binding vlan 20
   [VTEP1-bd20] quit
   [VTEP1] interface gigabitethernet 0/0/3
   [VTEP1-GigabitEthernet0/0/3] port link-type access
   [VTEP1-GigabitEthernet0/0/3] port default vlan 20
   [VTEP1-GigabitEthernet0/0/3] quit
   ```

   # 配置VTEP2。

   ```
   [VTEP2] vlan 10
   [VTEP2-vlan10] quit
   [VTEP2] bridge-domain 10
   [VTEP2-bd10] l2 binding vlan 10
   [VTEP2-bd10] quit
   ```

   # 配置VTEP3。

   ```
   [VTEP3] vlan 10
   [VTEP3-vlan10] quit
   [VTEP3] bridge-domain 10
   [VTEP3-bd10] l2 binding vlan 10
   [VTEP3-bd10] quit
   ```

3. 分别在VTEP1、VTEP2、VTEP3上配置EVPN实例并绑定BD域

   # 配置VTEP1。

   ```
   [VTEP1] evpn vpn-instance evpn20 bd-mode
   [VTEP1-evpn-instance-evpn20] route-distinguisher 1:20
   [VTEP1-evpn-instance-evpn20] vpn-target 20:1 both
   [VTEP1-evpn-instance-evpn10] vpn-target 1:100 export-extcommunity
   [VTEP1-evpn-instance-evpn20] quit
   [VTEP1] bridge-domain 20
   ```

```
[VTEP1-bd20] vxlan vni 20
[VTEP1-bd20] evpn binding vpn-instance evpn20
[VTEP1-bd20] quit
```

# 配置VTEP2。

```
[VTEP2] evpn vpn-instance evpn10 bd-mode
[VTEP2-evpn-instance-evpn10] route-distinguisher 2:10
[VTEP2-evpn-instance-evpn10] vpn-target 10:1 both
[VTEP2-evpn-instance-evpn10] vpn-target 1:100 export-extcommunity
[VTEP2-evpn-instance-evpn10] quit
[VTEP2] bridge-domain 10
[VTEP2-bd10] vxlan vni 10
[VTEP2-bd10] evpn binding vpn-instance evpn10
[VTEP2-bd10] quit
```

# 配置VTEP3。

```
[VTEP3] evpn vpn-instance evpn10 bd-mode
[VTEP3-evpn-instance-evpn10] route-distinguisher 3:10
[VTEP3-evpn-instance-evpn10] vpn-target 10:1 both
[VTEP3-evpn-instance-evpn10] vpn-target 1:100 export-extcommunity
[VTEP3-evpn-instance-evpn10] quit
[VTEP3] bridge-domain 10
[VTEP3-bd10] vxlan vni 10
[VTEP3-bd10] evpn binding vpn-instance evpn10
[VTEP3-bd10] quit
```

4. 分别在VTEP1、VTEP2、VTEP3上配置VPN实例并绑定VBDIF接口

# 配置VTEP1。

```
[VTEP1] ip vpn-instance vpn1
[VTEP1-vpn-instance-vpn1] ipv4-family
[VTEP1-vpn-instance-vpn1-af-ipv4] route-distinguisher 1:100
[VTEP1-vpn-instance-vpn1-af-ipv4] vpn-target 1:100 both evpn
[VTEP1-vpn-instance-vpn1-af-ipv4] quit
[VTEP1-vpn-instance-vpn1] vxlan vni 100
[VTEP1-vpn-instance-vpn1] quit
[VTEP1] interface vbdif 20
[VTEP1-Vbdif20] ip binding vpn-instance vpn1
[VTEP1-Vbdif20] quit
```

# 配置VTEP2。

```
[VTEP2] ip vpn-instance vpn1
[VTEP2-vpn-instance-vpn1] ipv4-family
[VTEP2-vpn-instance-vpn1-af-ipv4] route-distinguisher 2:100
[VTEP2-vpn-instance-vpn1-af-ipv4] vpn-target 1:100 both evpn
[VTEP2-vpn-instance-vpn1-af-ipv4] quit
[VTEP2-vpn-instance-vpn1] vxlan vni 100
[VTEP2-vpn-instance-vpn1] quit
[VTEP2] interface vbdif 10
[VTEP2-Vbdif10] ip binding vpn-instance vpn1
[VTEP2-Vbdif10] quit
```

# 配置VTEP3。

```
[VTEP3] ip vpn-instance vpn1
[VTEP3-vpn-instance-vpn1] ipv4-family
[VTEP3-vpn-instance-vpn1-af-ipv4] route-distinguisher 3:100
[VTEP3-vpn-instance-vpn1-af-ipv4] vpn-target 1:100 both evpn
[VTEP3-vpn-instance-vpn1-af-ipv4] quit
[VTEP3-vpn-instance-vpn1] vxlan vni 100
[VTEP3-vpn-instance-vpn1] quit
[VTEP3] interface vbdif 10
[VTEP3-Vbdif10] ip binding vpn-instance vpn1
[VTEP3-Vbdif10] quit
```

5. 配置VTEP1、VTEP2、VTEP3之间的BGP EVPN对等体关系

# 配置VTEP1。

```
[VTEP1] bgp 100
[VTEP1-bgp] router-id 10.1.1.1
[VTEP1-bgp] peer 10.2.2.2 as-number 100
[VTEP1-bgp] peer 10.2.2.2 connect-interface LoopBack1
[VTEP1-bgp] peer 10.3.3.3 as-number 100
[VTEP1-bgp] peer 10.3.3.3 connect-interface LoopBack1
[VTEP1-bgp] l2vpn-family evpn
[VTEP1-bgp-af-evpn] peer 10.2.2.2 enable
[VTEP1-bgp-af-evpn] peer 10.2.2.2 advertise irb
[VTEP1-bgp-af-evpn] peer 10.3.3.3 enable
[VTEP1-bgp-af-evpn] peer 10.3.3.3 advertise irb
[VTEP1-bgp-af-evpn] quit
[VTEP1-bgp] ipv4-family vpn-instance vpn1
[VTEP1-bgp-vpn1] advertise l2vpn evpn
[VTEP1-bgp-vpn1] import-route direct
[VTEP1-bgp-vpn1] quit
[VTEP1-bgp] quit
```

# 配置VTEP2。

```
[VTEP2] bgp 100
[VTEP2-bgp] router-id 10.2.2.2
[VTEP2-bgp] peer 10.1.1.1 as-number 100
[VTEP2-bgp] peer 10.1.1.1 connect-interface LoopBack1
[VTEP2-bgp] peer 10.3.3.3 as-number 100
[VTEP2-bgp] peer 10.3.3.3 connect-interface LoopBack1
[VTEP2-bgp] l2vpn-family evpn
[VTEP2-bgp-af-evpn] peer 10.1.1.1 enable
[VTEP2-bgp-af-evpn] peer 10.1.1.1 advertise irb
[VTEP2-bgp-af-evpn] peer 10.3.3.3 enable
[VTEP2-bgp-af-evpn] peer 10.3.3.3 advertise irb
[VTEP2-bgp-af-evpn] quit
[VTEP2-bgp] ipv4-family vpn-instance vpn1
[VTEP2-bgp-vpn1] advertise l2vpn evpn
[VTEP2-bgp-vpn1] import-route direct
[VTEP2-bgp-vpn1] quit
[VTEP2-bgp] quit
```

# 配置VTEP3。

```
[VTEP3] bgp 100
[VTEP3-bgp] router-id 10.3.3.3
[VTEP3-bgp] peer 10.1.1.1 as-number 100
[VTEP3-bgp] peer 10.1.1.1 connect-interface LoopBack1
[VTEP3-bgp] peer 10.2.2.2 as-number 100
[VTEP3-bgp] peer 10.2.2.2 connect-interface LoopBack1
[VTEP3-bgp] l2vpn-family evpn
[VTEP3-bgp-af-evpn] peer 10.1.1.1 enable
[VTEP3-bgp-af-evpn] peer 10.1.1.1 advertise irb
[VTEP3-bgp-af-evpn] peer 10.2.2.2 enable
[VTEP3-bgp-af-evpn] peer 10.2.2.2 advertise irb
[VTEP3-bgp-af-evpn] quit
[VTEP3-bgp] ipv4-family vpn-instance vpn1
[VTEP3-bgp-vpn1] advertise l2vpn evpn
[VTEP3-bgp-vpn1] import-route direct
[VTEP3-bgp-vpn1] quit
[VTEP3-bgp] quit
```

6. 在VTEP1、VTEP2、VTEP3上配置VXLAN隧道目的端地址

# 配置VTEP1。

```
[VTEP1] interface nve 1
[VTEP1-Nve1] source 10.1.1.1
[VTEP1-Nve1] vni 20 head-end peer-list protocol bgp
[VTEP1-Nve1] quit
```

# 配置VTEP2。

```
[VTEP2] interface nve 1
[VTEP2-Nve1] source 10.2.2.2
[VTEP2-Nve1] vni 10 head-end peer-list protocol bgp
[VTEP2-Nve1] quit
```

# 配置VTEP3。

```
[VTEP3] interface nve 1
[VTEP3-Nve1] source 10.3.3.3
[VTEP3-Nve1] vni 10 head-end peer-list protocol bgp
[VTEP3-Nve1] quit
```

7. 在VTEP2、VTEP3上配置VXLAN分布式网关，VTEP1上配置普通的VXLAN网关

   # 配置VTEP1。

   ```
   [VTEP1] interface vbdif 20
   [VTEP1-Vbdif20] ip address 192.168.20.1 24
   [VTEP1-Vbdif20] quit
   ```

   # 配置VTEP2。

   ```
   [VTEP2] interface vbdif 10
   [VTEP2-Vbdif10] ip address 192.168.10.1 24
   [VTEP2-Vbdif10] arp distribute-gateway enable
   [VTEP2-Vbdif10] arp collect host enable
   [VTEP2-Vbdif10] mac-address 0000-5e00-0101
   [VTEP2-Vbdif10] quit
   ```

   # 配置VTEP3。

   ```
   [VTEP3] interface vbdif 10
   [VTEP3-Vbdif10] ip address 192.168.10.1 24
   [VTEP3-Vbdif10] arp distribute-gateway enable
   [VTEP3-Vbdif10] arp collect host enable
   [VTEP3-Vbdif10] mac-address 0000-5e00-0101
   [VTEP3-Vbdif10] quit
   ```

8. 验证VXLAN网络配置结果

   # 上述配置成功后，在VTEP1、VTEP2、VTEP3上执行命令**display vxlan tunnel**可查看到VXLAN隧道的信息。以VTEP1显示为例。

   ```
   [VTEP1] display vxlan tunnel
   Tunnel ID       Source            Destination       State     Type
   --------------------------------------------------------------------------------
   11              10.1.1.1          10.2.2.2          up        l3 dynamic
   13              10.1.1.1          10.3.3.3          up        l3 dynamic
   --------------------------------------------------------------------------------
   Number of vxlan tunnel :
   Total : 2    Static: 0    L2 dynamic: 0    L3 dynamic: 2
   ```

**步骤2** 在VTEP2、VTEP3上配置DHCP Relay功能以及分布式网关的DHCP Relay重选路由功能

# 配置VTEP2。

```
[VTEP2] dhcp enable
[VTEP2] dhcp option82 vendor-specific format vendor-sub-option 2 ip-address 10.2.2.2
[VTEP2] bridge-domain 10
[VTEP2-bd10] dhcp option82 insert enable
[VTEP2-bd10] dhcp option82 encapsulation vendor-specific-id
[VTEP2-bd10] quit
[VTEP2] interface vbdif 10
[VTEP2-Vbdif10] dhcp select relay
[VTEP2-Vbdif10] dhcp relay server-ip 192.168.20.10
[VTEP2-Vbdif10] dhcp relay information enable
[VTEP2-Vbdif10] dhcp relay anycast gateway re-route enable
[VTEP2-Vbdif10] quit
```

# 配置VTEP3。

```
[VTEP3] dhcp enable
[VTEP3] dhcp option82 vendor-specific format vendor-sub-option 2 ip-address 10.3.3.3
[VTEP3] bridge-domain 10
[VTEP3-bd10] dhcp option82 insert enable
[VTEP3-bd10] dhcp option82 encapsulation vendor-specific-id
[VTEP3-bd10] quit
[VTEP3] interface vbdif 10
[VTEP3-Vbdif10] dhcp select relay
[VTEP3-Vbdif10] dhcp relay server-ip 192.168.20.10
[VTEP3-Vbdif10] dhcp relay information enable
[VTEP3-Vbdif10] dhcp relay anycast gateway re-route enable
[VTEP3-Vbdif10] quit
```

**步骤3** 在VTEP2、VTEP3上配置VXLAN隧道侧接口加入端口防攻击的白名单。

# 在VTEP2上配置VXLAN隧道侧接口GigabitEthernet0//0/1加入端口防攻击的白名单。

```
[VTEP2] cpu-defend policy vxlan_tunnel_side
[VTEP2-cpu-defend-policy-vxlan_tunnel_side] auto-port-defend whitelist 1 interface GigabitEthernet0/0/1
[VTEP2-cpu-defend-policy-vxlan_tunnel_side] quit
[VTEP2] cpu-defend-policy vxlan_tunnel_side global
```

# 在VTEP3上配置VXLAN隧道侧接口GigabitEthernet0//0/1加入端口防攻击的白名单。

```
[VTEP3] cpu-defend policy vxlan_tunnel_side
[VTEP3-cpu-defend-policy-vxlan_tunnel_side] auto-port-defend whitelist 1 interface GigabitEthernet0/0/1
[VTEP3-cpu-defend-policy-vxlan_tunnel_side] quit
[VTEP3] cpu-defend-policy vxlan_tunnel_side global
```

**步骤4** 验证DHCP Relay功能配置结果

# 上述配置成功后，在VTEP2、VTEP3上执行命令**display dhcp relay**可查看接口DHCP Relay配置情况。以VTEP2显示为例。

```
[VTEP2] display dhcp relay interface vbdif 10
 DHCP relay agent running information of interface Vbdif10 :
 Server IP address [00] : 192.168.20.10
 Gateway address in use : 192.168.10.1
```

**步骤5** 配置DHCP服务器

具体配置过程略。DHCP服务器需要满足以下条件：

- 在DHCP服务器上配置地址池，以便服务器端分配正确的IP地址给客户端。
- 建议配置地址池租期，提高IP地址的使用效率。

**步骤6** 在VTEP2和VTEP3上配置AP管理VLAN的接入，并配置DHCP服务器功能，为AP分配管理IP

# 配置VTEP2。

```
[VTEP2] vlan 100
[VTEP22-vlan100] quit
[VTEP2] interface gigabitethernet 0/0/2
[VTEP2-GigabitEthernet0/0/2] port link-type access
[VTEP2-GigabitEthernet0/0/2] port default vlan 100
[VTEP2-GigabitEthernet0/0/2] quit
[VTEP2] interface vlanif 100
[VTEP2-Vlanif100] ip address 192.168.100.1 24
[VTEP2-Vlanif100] dhcp select interface
[VTEP2-Vlanif100] quit
```

# 配置VTEP3。

```
[VTEP3] vlan 200
[VTEP3-vlan200] quit
[VTEP3] interface gigabitethernet 0/0/2
[VTEP3-GigabitEthernet0/0/2] port link-type access
[VTEP3-GigabitEthernet0/0/2] port default vlan 200
[VTEP3-GigabitEthernet0/0/2] quit
[VTEP3] interface vlanif 200
[VTEP3-Vlanif200] ip address 192.168.200.1 24
[VTEP3-Vlanif200] dhcp select interface
[VTEP3-Vlanif200] quit
```

**步骤7** 在VTEP2和VTEP3上配置其作为AC设备的CAPWAP隧道源IP地址

# 配置VTEP2

```
[VTEP2] capwap source interface vlanif 100
```

# 配置VTEP3

```
[VTEP3] capwap source interface vlanif 200
```

**步骤8** 在VTEP2和VTEP3上配置路由协议，实现CAPWAP隧道源IP地址之间互通。

# 配置VTEP2

```
[VTEP2] ospf
[VTEP2-ospf-1] area 0
[VTEP2-ospf-1-area-0.0.0.0] network 192.168.100.0 0.0.0.255
[VTEP2-ospf-1-area-0.0.0.0] quit
[VTEP2-ospf-1] quit
```

# 配置VTEP3

```
[VTEP3] ospf
[VTEP3-ospf-1] area 0
[VTEP3-ospf-1-area-0.0.0.0] network 192.168.200.0 0.0.0.255
[VTEP3-ospf-1-area-0.0.0.0] quit
[VTEP3-ospf-1] quit
```

**步骤9** 在VTEP2和VTEP3上分别配置AP上线，以VTEP2为例，VTEP3的配置同VTEP2类似

# 创建AP组，用于将相同配置的AP都加入同一AP组中。

```
[VTEP2] wlan
[VTEP2-wlan-view] ap-group name ap-group1
[VTEP2-wlan-ap-group-ap-group1] quit
```

# 创建域管理模板，在域管理模板下配置AC的国家码并在AP组下引用域管理模板。

```
[VTEP2-wlan-view] regulatory-domain-profile name default
[VTEP2-wlan-regulate-domain-default] country-code cn
[VTEP2-wlan-regulate-domain-default] quit
[VTEP2-wlan-view] ap-group name ap-group1
[VTEP2-wlan-ap-group-ap-group1] regulatory-domain-profile default
Warning: This configuration change will clear the channel and power configurations of radios, and may
restart APs. Continue?[Y/N]:y
[VTEP2-wlan-ap-group-ap-group1] quit
[VTEP2-wlan-view] quit
```

# 在AC上离线导入AP，并将AP加入AP组“ap-group1”中。假设AP的MAC地址为00e0-fc76-e360，并且根据AP的部署位置为AP配置名称，便于从名称上就能够了解AP的部署位置。例如MAC地址为00e0-fc76-e360的AP部署在1号区域，命名此AP为area_1。

**说明**

**ap auth-mode**命令缺省情况下为MAC认证，如果之前没有修改其缺省配置，可以不用执行**ap auth-mode mac-auth**命令。

举例中使用的AP为AP5030DN，具有射频0和射频1两个射频。AP5030DN的射频0为2.4GHz射频，射频1为5GHz射频。

```
[VTEP2] wlan
[VTEP2-wlan-view] ap auth-mode mac-auth
[VTEP2-wlan-view] ap-id 0 ap-mac 00e0-fc76-e360
[VTEP2-wlan-ap-0] ap-name area_1
Warning: This operation may cause AP reset. Continue? [Y/N]:y
[VTEP2-wlan-ap-0] ap-group ap-group1
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and
antenna gain configuration s of the radio, Whether to continue? [Y/N]:y
[VTEP2-wlan-ap-0] quit
```

# 将AP上电后，当执行命令**display ap all**查看到AP的“State”字段为“nor”时，表示AP正常上线。

```
[VTEP2-wlan-view] display ap all
Total AP information:
nor  : normal          [1]
Extra information:
P  : insufficient power supply
-------------------------------------------------------------------------------------------------
ID   MAC            Name   Group     IP            Type           State STA Uptime      ExtraInfo
-------------------------------------------------------------------------------------------------
0    00e0-fc76-e360 area_1 ap-group1 10.23.100.254 AP5030DN       nor   0   10S         -
-------------------------------------------------------------------------------------------------
Total: 1
```

**步骤10** 在VTEP2和VTEP3上配置WLAN业务参数，以VTEP2为例，VTEP3的配置同VTEP2类似

# 创建名为“wlan-net”的安全模板，并配置安全策略。

**说明**

举例中以配置WPA-WPA2+PSK+AES的安全策略为例，密码为“a1234567”，实际配置中请根据实际情况，配置符合实际要求的安全策略。

```
[VTEP2-wlan-view] security-profile name wlan-net
[VTEP2-wlan-sec-prof-wlan-net] security wpa-wpa2 psk pass-phrase a1234567 aes
[VTEP2-wlan-sec-prof-wlan-net] quit
```

# 创建名为“wlan-net”的SSID模板，并配置SSID名称为“wlan-net”。

```
[VTEP2-wlan-view] ssid-profile name wlan-net
[VTEP2-wlan-ssid-prof-wlan-net] ssid wlan-net
[VTEP2-wlan-ssid-prof-wlan-net] quit
```

# 创建名为“wlan-net”的VAP模板，配置业务数据转发模式、业务VLAN，并且引用安全模板和SSID模板。

```
[VTEP2-wlan-view] vap-profile name wlan-net
[VTEP2-wlan-vap-prof-wlan-net] forward-mode tunnel
[VTEP2-wlan-vap-prof-wlan-net] service-vlan vlan-id 10
[VTEP2-wlan-vap-prof-wlan-net] security-profile wlan-net
[VTEP2-wlan-vap-prof-wlan-net] ssid-profile wlan-net
[VTEP2-wlan-vap-prof-wlan-net] 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“wlan-net”的配置。

```
[VTEP2-wlan-view] ap-group name ap-group1
[VTEP2-wlan-ap-group-ap-group1] vap-profile wlan-net wlan 1 radio 0
[VTEP2-wlan-ap-group-ap-group1] vap-profile wlan-net wlan 1 radio 1
[VTEP2-wlan-ap-group-ap-group1] quit
```

**步骤11** 在VTEP2和VTEP3上配置的WLAN漫游功能

配置漫游组内AC间建链的IP地址。

# 配置VTEP2

```
[VTEP2-wlan-view] mobility-server local ip-address 192.168.100.1
```

# 配置VTEP3

```
[VTEP3-wlan-view] mobility-server local ip-address 192.168.200.1
```

创建漫游组，并配置AC_1和AC_2为漫游组成员。

# 配置VTEP2

```
[VTEP2-wlan-view] mobility-group name mobility
[VTEP2-mc-mg-mobility] member ip-address 192.168.100.1
[VTEP2-mc-mg-mobility] member ip-address 192.168.200.1
[VTEP2-mc-mg-mobility] quit
```

# 配置VTEP3

```
[VTEP3-wlan-view] mobility-group name mobility
[VTEP3-mc-mg-mobility] member ip-address 192.168.100.1
[VTEP3-mc-mg-mobility] member ip-address 192.168.200.1
[VTEP3-mc-mg-mobility] quit
```

**步骤12** 验证配置结果

# WLAN业务配置会自动下发给AP，配置完成后，分别在VTEP2和VTEP3上执行命令**display vap ssid wlan-net**查看VAP信息，当“Status”显示为“ON”时，表示AP对应射频上的VAP已创建成功。

```
[VTEP2-wlan-view] display vap ssid wlan-net
WID : WLAN ID
--------------------------------------------------------------------------------
AP ID AP name       RfID WID  BSSID         Status  Auth type        STA   SSID
--------------------------------------------------------------------------------
0     area_1        0    1    00E0-FC76-E360 ON      WPA/WPA2-PSK     0     wlan-net
0     area_1        1    1    00E0-FC76-E370 ON      WPA/WPA2-PSK     0     wlan-net
--------------------------------------------------------------------------------
Total: 2
[VTEP3-wlan-view] display vap ssid wlan-net
WID : WLAN ID
--------------------------------------------------------------------------------
AP ID AP name       RfID WID  BSSID         Status  Auth type        STA  SSID
--------------------------------------------------------------------------------
1     area_2        0    1    00E0-FC04-B500 ON      WPA/WPA2-PSK     0   wlan-net
1     area_2        1    1    00E0-FC04-B510 ON      WPA/WPA2-PSK     0   wlan-net
--------------------------------------------------------------------------------
Total: 2
```

# 在VTEP2上执行命令**display mobility-group name mobility**查看漫游组成员VTEP2和VTEP3的状态，当“State”显示为“normal”时，表示VTEP2和VTEP3正常。

# STA在area_1的覆盖范围内搜索到SSID为“wlan-net”的无线网络，输入密码“a1234567”并正常关联后，在VTEP2上执行命令**display station ssid wlan-net**，查看STA的接入信息，可以看到STA关联到了area_1，STA的MAC地址为“00e0-fcc7-1e08”。

```
[VTEP2-wlan-view] display station ssid wlan-net
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  IP address
--------------------------------------------------------------------------------
00e0-fcc7-1e08  0     area_1    1/1      5G    11n   46/59     -57   101   192.168.10.161
--------------------------------------------------------------------------------
Total: 1 2.4G: 0 5G: 1
```

# 当STA从area_1的覆盖范围移动到AP_2的覆盖范围时，在VTEP3上执行命令**display station ssid wlan-net**，查看STA的接入信息，可以看到STA关联到了AP_2。

```
[VTEP3-wlan-view] display station ssid wlan-net
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  IP address
--------------------------------------------------------------------------------
```

```
00e0-fcc7-1e08   1     area_2    1/1      5G    11n   46/59      -58   101   192.168.10.161
------------------------------------------------------------------------------------------
Total: 1 2.4G: 0 5G: 1
```

# 在VTEP3上执行命令**display station roam-track sta-mac 00e0-fcc7-1e08**，可以查看该STA的漫游轨迹。

```
[VTEP3-wlan-view] display station roam-track sta-mac 00e0-fcc7-1e08
Access SSID:wlan-net
Rx/Tx: link receive rate/link transmit rate(Mbps)
c:PMK Cache Roam r:802.11r Roam s:Same Frequency Network
------------------------------------------------------------------------------
L2/L3          AC IP                AP name              Radio ID
BSSID          TIME                 In/Out RSSI          Out Rx/Tx
------------------------------------------------------------------------------
--             192.168.100.1        area_1               1
00e0-fc76-e360  2018/06/09 16:11:51    -57/-57             22/3
L2             192.168.200.1        area_2               1
00e0-fc04-b500  2018/06/09 16:13:53    -58/-               -/-
------------------------------------------------------------------------------
Number: 1
```

**----结束**

## 配置文件

- VTEP1的配置文件

```
#
sysname VTEP1
#
vlan batch 20
#
ip vpn-instance vpn1
 ipv4-family
  route-distinguisher 1:100
  vpn-target 1:100 export-extcommunity evpn
  vpn-target 1:100 import-extcommunity evpn
 vxlan vni 100
#
evpn vpn-instance evpn20 bd-mode
 route-distinguisher 1:20
 vpn-target 1:100 20:1 export-extcommunity
 vpn-target 20:1 import-extcommunity
#
bridge-domain 20
 l2 binding vlan 20
 vxlan vni 20
 evpn binding vpn-instance evpn20
#
interface GigabitEthernet0/0/1
 undo portswitch
 ip address 192.168.1.2 255.255.255.0
#
interface GigabitEthernet0/0/2
 undo portswitch
 ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 20
#
interface LoopBack1
 ip address 10.1.1.1 255.255.255.255
#
interface Vbdif20
 ip binding vpn-instance vpn1
 ip address 192.168.20.1 255.255.255.0
#
interface Nve1
```

```
 source 10.1.1.1
 vni 20 head-end peer-list protocol bgp
#
bgp 100
 router-id 10.1.1.1
 peer 10.2.2.2 as-number 100
 peer 10.2.2.2 connect-interface LoopBack1
 peer 10.3.3.3 as-number 100
 peer 10.3.3.3 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 10.2.2.2 enable
  peer 10.3.3.3 enable
 #
 l2vpn-family evpn
  policy vpn-target
  peer 10.2.2.2 enable
  peer 10.2.2.2 advertise irb
  peer 10.3.3.3 enable
  peer 10.3.3.3 advertise irb
 #
 ipv4-family vpn-instance vpn1
  import-route direct
  advertise l2vpn evpn
#
ospf 1 router-id 10.1.1.1
 area 0.0.0.0
  network 10.1.1.1 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
#
return
```

- VTEP2的配置文件

```
#
sysname VTEP2
#
dhcp enable
#
dhcp option82 vendor-specific format vendor-sub-option 2 ip-address 10.2.2.2
#
ip vpn-instance vpn1
 ipv4-family
  route-distinguisher 2:100
  vpn-target 1:100 export-extcommunity evpn
  vpn-target 1:100 import-extcommunity evpn
 vxlan vni 100
#
evpn vpn-instance evpn10 bd-mode
 route-distinguisher 2:10
 vpn-target 1:100 10:1 export-extcommunity
 vpn-target 10:1 import-extcommunity
#
bridge-domain 10
 l2 binding vlan 10
 vxlan vni 10
 evpn binding vpn-instance evpn10
 dhcp option82 insert enable
 dhcp option82 encapsulation vendor-specific-id
#
interface Vlanif100
 ip address 192.168.100.1 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/1
 undo portswitch
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/0/2
```

```
 port link-type access
 port default vlan 100
#
interface LoopBack1
 ip address 10.2.2.2 255.255.255.255
#
interface Vbdif10
 mac-address 0000-5e00-0101
 ip binding vpn-instance vpn1
 arp collect host enable
 arp distribute-gateway enable
 ip address 192.168.10.1 255.255.255.0
 dhcp select relay
 dhcp relay server-ip 192.168.20.10
 dhcp relay information enable
 dhcp relay anycast gateway re-route enable
#
interface Nve1
 source 10.2.2.2
 vni 10 head-end peer-list protocol bgp
#
bgp 100
 router-id 10.2.2.2
 peer 10.1.1.1 as-number 100
 peer 10.1.1.1 connect-interface LoopBack1
 peer 10.3.3.3 as-number 100
 peer 10.3.3.3 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 10.1.1.1 enable
  peer 10.3.3.3 enable
 #
 l2vpn-family evpn
  policy vpn-target
  peer 10.1.1.1 enable
  peer 10.1.1.1 advertise irb
  peer 10.3.3.3 enable
  peer 10.3.3.3 advertise irb
 #
 ipv4-family vpn-instance vpn1
  import-route direct
  advertise l2vpn evpn
#
ospf 1 router-id 10.2.2.2
 area 0.0.0.0
  network 10.2.2.2 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 192.168.100.0 0.0.0.255
#
cpu-defend policy vxlan_tunnel_side
 auto-defend whitelist 1 interface GigabitEthernet0/0/1
#
cpu-defend-policy vxlan_tunnel_side global
#
capwap source interface vlanif100
#
wlan
 security-profile name wlan-net
  security wpa2 psk pass-phrase %^%#]:krYrz_r<ee}|Cq@9V(W{ZD$"\-R-HD_y.4#U4,%^%# aes
 ssid-profile name wlan-net
  ssid wlan-net
 vap-profile name wlan-net
  forward-mode tunnel
  service-vlan vlan-id 10
  ssid-profile wlan-net
  security-profile wlan-net
 regulatory-domain-profile name default
 mobility-server local ip-address 192.168.100.1
```

```
 mobility-group name mobility
  member ip-address 192.168.100.1
  member ip-address 192.168.200.1
 ap-group name ap-group1
  radio 0
   vap-profile wlan-net wlan 1
  radio 1
   vap-profile wlan-net wlan 1
 ap-id 0 type-id 35 ap-mac 00e0-fc76-e360 ap-sn 210235554710CB000042
  ap-name area_1
  ap-group ap-group1
#
return
```

- VTEP3的配置文件

```
#
sysname VTEP3
#
dhcp enable
#
dhcp option82 vendor-specific format vendor-sub-option 2 ip-address 10.3.3.3
#
ip vpn-instance vpn1
 ipv4-family
  route-distinguisher 3:100
  vpn-target 1:100 export-extcommunity evpn
  vpn-target 1:100 import-extcommunity evpn
 vxlan vni 100
#
evpn vpn-instance evpn10 bd-mode
 route-distinguisher 3:10
 vpn-target 1:100 10:1 export-extcommunity
 vpn-target 10:1 import-extcommunity
#
bridge-domain 10
 l2 binding vlan 10
 vxlan vni 10
 evpn binding vpn-instance evpn10
 dhcp option82 insert enable
 dhcp option82 encapsulation vendor-specific-id
#
interface Vlanif200
 ip address 192.168.200.1 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/1
 undo portswitch
 ip address 192.168.2.2 255.255.255.0
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port default vlan 200
#
interface LoopBack1
 ip address 10.3.3.3 255.255.255.255
#
interface Vbdif10
 mac-address 0000-5e00-0101
 ip binding vpn-instance vpn1
 arp collect host enable
 arp distribute-gateway enable
 ip address 192.168.10.1 255.255.255.0
 dhcp select relay
 dhcp relay server-ip 192.168.20.10
 dhcp relay information enable
 dhcp relay anycast gateway re-route enable
#
interface Nve1
 source 10.3.3.3
 vni 10 head-end peer-list protocol bgp
```

```
#
bgp 100
 router-id 10.3.3.3
 peer 10.1.1.1 as-number 100
 peer 10.1.1.1 connect-interface LoopBack1
 peer 10.2.2.2 as-number 100
 peer 10.2.2.2 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 10.1.1.1 enable
  peer 10.2.2.2 enable
 #
 l2vpn-family evpn
  policy vpn-target
  peer 10.1.1.1 enable
  peer 10.1.1.1 advertise irb
  peer 10.2.2.2 enable
  peer 10.2.2.2 advertise irb
 #
 ipv4-family vpn-instance vpn1
  import-route direct
  advertise l2vpn evpn
#
ospf 1 router-id 10.3.3.3
 area 0.0.0.0
  network 10.3.3.3 0.0.0.0
  network 192.168.2.0 0.0.0.255
  network 192.168.200.0 0.0.0.255
#
cpu-defend policy vxlan_tunnel_side
 auto-defend whitelist 1 interface GigabitEthernet0/0/1
#
cpu-defend-policy vxlan_tunnel_side global
#
capwap source interface vlanif200
#
wlan
 security-profile name wlan-net
  security wpa2 psk pass-phrase %^%#]:krYrz_r<ee}|Cq@9V(W{ZD$"\-R-HD_y.4#U4,%^%# aes
 ssid-profile name wlan-net
  ssid wlan-net
 vap-profile name wlan-net
  forward-mode tunnel
  service-vlan vlan-id 10
  ssid-profile wlan-net
  security-profile wlan-net
 regulatory-domain-profile name default
  dca-channel 5g channel-set 149,153,157,161
 mobility-server local ip-address 192.168.200.1
 mobility-group name mobility
  member ip-address 192.168.100.1
  member ip-address 192.168.200.1
 ap-group name ap-group1
  radio 0
   vap-profile wlan-net wlan 1
  radio 1
   vap-profile wlan-net wlan 1
 ap-id 1 type-id 35 ap-mac 00e0-fc04-b500 ap-sn 210235554710CB000078
  ap-name area_2
  ap-group ap-group1
#
return
```

# 9.9.6 配置敏捷分布式 SFN 漫游示例

## 配置流程

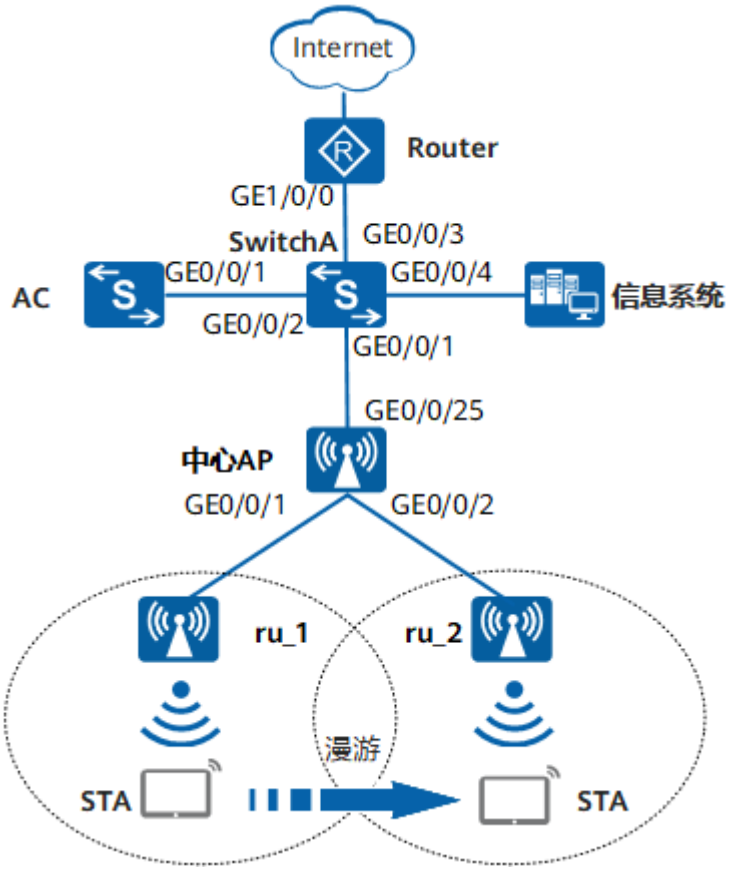
WLAN不同的特性和功能需要在不同类型的模板下进行配置和维护，这些模板统称为WLAN模板，如域管理模板、射频模板、VAP模板、AP系统模板、AP有线口模板、WIDS模板、WDS模板、Mesh模板。当用户在配置WLAN业务功能时，需要在对应功能的WLAN模板中进行参数配置，配置完成后，须将此模板引用到AP组或AP中，配置才会自动下发到AP，进而配置的功能在AP上生效。由于模板之间是存在相互引用关系的，因此在用户配置过程中，需要先了解各个模板之间存在的逻辑关系。模板的逻辑关系和基本配置流程请参见**WLAN业务配置流程**。

## 组网需求

某医院通过部署敏捷分布式网络给医护人员提供WLAN接入服务，以满足医护人员办公的最基本需求。管理员希望终端在覆盖区域内移动发生漫游时，终端无感知，业务不中断。

- AC组网方式：旁挂二层组网。
- DHCP部署方式：
  - AC作为DHCP服务器为中心AP和RU分配IP地址。
  - 交换机SwitchA作为DHCP服务器为STA分配IP地址。
- 业务数据转发方式：直接转发。

**图 9-17** 配置敏捷分布式 SFN 漫游示例组网图



## 配置思路

1. 配置中心AP、RU、AC和上层网络设备之间实现二层互通。
2. 配置DHCP服务器为STA、中心AP和RU分配IP地址。
3. 配置中心AP和RU上线。
4. 配置WLAN业务参数，实现STA访问WLAN网络功能。
5. 配置敏捷分布式SFN漫游。

**表 9-12** 数据规划表

| 配置项 | 数据 |
| --- | --- |
| DHCP服务器 | • AC作为DHCP服务器为中心AP和RU分配IP地址<br>• 交换机SwitchA作为DHCP服务器为STA分配IP地址 |
| 中心AP和RU的IP地址池 | 10.23.100.2～10.23.100.254/24 |
| STA的IP地址池 | 10.23.101.3～10.23.101.254/24 |
| AC的源接口IP地址 | VLANIF100：10.23.100.1/24 |
| AP组 | • 名称：ap-group1<br>• 引用模板：VAP模板wlan-net、域管理模板default |
| 域管理模板 | • 名称：default<br>• 国家码：中国 |
| SSID模板 | • 名称：wlan-net<br>• SSID名称：wlan-net |
| 安全模板 | • 名称：wlan-net<br>• 安全策略：WPA-WPA2+PSK+AES<br>• 密码：a1234567 |
| VAP模板 | • 名称：wlan-net<br>• 转发模式：直接转发<br>• 业务VLAN：VLAN101<br>• 引用模板：SSID模板wlan-net、安全模板wlan-net |
| RU工作信道 | • ru_1：工作信道为6<br>• ru_2：工作信道为6 |
| 敏捷分布式SFN漫游功能 | 开启 |

## 配置注意事项

- 网络规划注意事项：
  - 支持敏捷分布式SFN漫游功能的款型仅包括AD9430DN-12（含配套RU）和AD9430DN-24（含配套RU）。其中，仅以下RU组合支持敏捷分布式SFN漫游：
    - R230D和R240D间，并且，R230D和R240D仅2.4G射频支持敏捷分布式SFN漫游，5G射频不支持。
    - R250D、R250D-E、R251D、R251D-E和R450D间。
  - 对于整个中心AP，开启敏捷分布式SFN漫游功能后，所有RU单频段（2.4G或5G）上支持的同频漫游终端数总数不超过128，单频段内其它VAP上终端总数不超过128。
  - 开启敏捷分布式SFN漫游功能后，所有RU需配置在同一信道。在5G频段开启敏捷分布式SFN漫游时，需将信道配置在非雷达信道。
  - 参与漫游的各个RU需要关联在同一中心AP上。不支持跨中心AP的敏捷分布式SFN漫游。
  - RU间的漫游为中心AP内二层漫游。不支持三层漫游场景下的敏捷分布式SFN漫游。
- 配置注意事项：
  - 如果2.4G或5G射频同时开启敏捷分布式SFN漫游，则建议使用不同的SSID，否则可能导致STA切换射频，影响用户体验。
  - 一个射频上只能有一个VAP使能敏捷分布式SFN漫游功能。如果一个射频上配置了多个VAP，建议在没有配置敏捷分布式SFN漫游的所有VAP上配置VAP限速总和为5Mbps。

    **说明**

    如果AP组的某个射频上有VAP使能了敏捷分布式SFN漫游功能，则在对应中心AP下关联到该射频的所有STA的漫游轨迹均可能会带有s标记。
  - 开启敏捷分布式SFN漫游功能的射频上不能再配置信道扫描、信道调优和智能漫游。
  - 敏捷分布式SFN漫游不支持AP个性化配置，只能基于AP组配置。
  - 参与漫游的各个RU需要配置：
    - 相同的SSID。
    - 相同的VAP模板，且VAP ID必须相同。
    - 相同的安全策略。敏捷分布式SFN漫游支持的加密方式包括WPA+PSK、WPA2+PSK、WPA-WPA2+PSK、WPA+802.1X（EAP认证）、WPA2+802.1X（EAP认证）、WPA-WPA2+802.1X（EAP认证）和Portal+PSK。

## 操作步骤

**步骤1** 在AC上配置NAC模式为统一模式，以保证用户能够正常接入网络

```
<HUAWEI> system-view
[HUAWEI] authentication unified-mode
```

**说明**

如果当前NAC模式为传统模式，则配置NAC模式为统一模式后，需要保存配置并重启设备后生效。

**步骤2** 配置周边设备

# 配置SwitchA的GE0/0/1接口加入VLAN100（管理VLAN）和VLAN101（业务VLAN），缺省VLAN为VLAN100，GE0/0/2接口加入VLAN100，GE0/0/3和GE0/0/4接口加入VLAN101。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] vlan batch 100 101
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type trunk
[SwitchA-GigabitEthernet0/0/1] port trunk pvid vlan 100
[SwitchA-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 101
[SwitchA-GigabitEthernet0/0/1] port-isolate enable
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type trunk
[SwitchA-GigabitEthernet0/0/2] port trunk allow-pass vlan 100
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] port link-type trunk
[SwitchA-GigabitEthernet0/0/3] port trunk allow-pass vlan 101
[SwitchA-GigabitEthernet0/0/3] quit
[SwitchA] interface gigabitethernet 0/0/4
[SwitchA-GigabitEthernet0/0/4] port link-type trunk
[SwitchA-GigabitEthernet0/0/4] port trunk allow-pass vlan 101
[SwitchA-GigabitEthernet0/0/4] quit
```

# 配置Router的接口GE1/0/0的IP地址。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] interface gigabitethernet 1/0/0
[Router-GigabitEthernet1/0/0] ip address 10.23.101.2 24
[Router-GigabitEthernet1/0/0] quit
```

**步骤3** 配置AC与其它网络设备互通

# 配置AC的接口GE0/0/1加入VLAN100。

```
[HUAWEI] sysname AC
[AC] vlan batch 100 101
[AC] interface gigabitethernet 0/0/1
[AC-GigabitEthernet0/0/1] port link-type trunk
[AC-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[AC-GigabitEthernet0/0/1] quit
```

**步骤4** 配置DHCP服务器为STA、中心AP和RU分配IP地址

# 在AC上配置VLANIF100接口为中心AP和RU提供IP地址。

```
[AC] dhcp enable
[AC] interface vlanif 100
[AC-Vlanif100] ip address 10.23.100.1 24
[AC-Vlanif100] dhcp select interface
[AC-Vlanif100] quit
```

# 在SwitchA上配置VLANIF101接口为STA提供IP地址，并配置下一跳为Router的缺省路由。

**说明**

DNS服务器地址请根据实际需要配置。常用配置方法如下：

- 接口地址池场景，需要在VLANIF接口视图下执行命令**dhcp server dns-list** *ip-address* &<1-8>。
- 全局地址池场景，需要在IP地址池视图下执行命令**dns-list** *ip-address* &<1-8>。

```
[SwitchA] dhcp enable
[SwitchA] interface vlanif 101
[SwitchA-Vlanif101] ip address 10.23.101.1 24
[SwitchA-Vlanif101] dhcp select interface
[SwitchA-Vlanif101] dhcp server excluded-ip-address 10.23.101.2
[SwitchA-Vlanif101] quit
[SwitchA] ip route-static 0.0.0.0 0.0.0.0 10.23.101.2
```

**步骤5** 配置中心AP和RU上线

# 创建AP组，用于将相同配置的AP都加入同一AP组中。

```
[AC] wlan
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] quit
```

# 创建域管理模板，在域管理模板下配置AC的国家码并在AP组下引用域管理模板。

```
[AC-wlan-view] regulatory-domain-profile name default
[AC-wlan-regulate-domain-default] country-code cn
[AC-wlan-regulate-domain-default] quit
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] regulatory-domain-profile default
Warning: This configuration change will clear the channel and power configurations of radios, and may restart APs. Continue?[Y/N]:y
[AC-wlan-ap-group-ap-group1] quit
[AC-wlan-view] quit
```

# 配置AC的源接口。

```
[AC] capwap source interface vlanif 100
```

# 在AC上离线导入中心AP和RU，并将其加入AP组“ap-group1”中。假设中心AP的MAC地址为00e0-fc45-62fd，命名为central_AP，RU的MAC地址为00e0-fc97-c520和00e0-fc97-ca40，分别命名为ru_1和ru_2。

**说明**

**ap auth-mode**命令缺省情况下为MAC认证，如果之前没有修改其缺省配置，可以不用执行**ap auth-mode mac-auth**。

```
[AC] wlan
[AC-wlan-view] ap auth-mode mac-auth
[AC-wlan-view] ap-id 0 ap-mac 00e0-fc45-62fd
[AC-wlan-ap-0] ap-name central_AP
Warning: This operation may cause AP reset. Continue? [Y/N]:y
[AC-wlan-ap-0] ap-group ap-group1
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configuration s of the radio, Whether to continue? [Y/N]:y
[AC-wlan-ap-0] quit
[AC-wlan-view] ap-id 1 ap-mac 00e0-fc97-c520
[AC-wlan-ap-1] ap-name ru_1
Warning: This operation may cause AP reset. Continue? [Y/N]:y
[AC-wlan-ap-1] ap-group ap-group1
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configuration s of the radio, Whether to continue? [Y/N]:y
[AC-wlan-ap-1] quit
[AC-wlan-view] ap-id 2 ap-mac 00e0-fc97-ca40
[AC-wlan-ap-2] ap-name ru_2
Warning: This operation may cause AP reset. Continue? [Y/N]:y
[AC-wlan-ap-2] ap-group ap-group1
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configuration s of the radio, Whether to continue? [Y/N]:y
[AC-wlan-ap-2] quit
```

# 将AP上电后，当执行命令**display ap all**查看到AP的“State”字段为“nor”时，表示AP正常上线。

```
[AC-wlan-view] display ap all
Total AP information:
nor  : normal          [3]
Extrainfo : Extra information
P  : insufficient power supply
------------------------------------------------------------------------------------------------
ID   MAC            Name       Group     IP            Type            State STA Uptime      ExtraInfo
------------------------------------------------------------------------------------------------
0    00e0-fc45-62fd central_AP ap-group1 10.23.100.254 AD9430DN-24     nor   0   2M:25S      -
1    00e0-fc97-c520 ru_1       ap-group1 10.23.100.253 R240D           nor   0   3M:5S       -
2    00e0-fc97-ca40 ru_2       ap-group1 10.23.100.252 R240D           nor   0   3M:14S      -
------------------------------------------------------------------------------------------------
Total: 3
```

**步骤6** 配置WLAN业务参数

# 创建名为“wlan-net”的安全模板，并配置安全策略。

**说明**

举例中以配置WPA-WPA2+PSK+AES的安全策略为例，密码为“a1234567”，实际配置中请根据实际情况，配置符合实际要求的安全策略。

```
[AC-wlan-view] security-profile name wlan-net
[AC-wlan-sec-prof-wlan-net] security wpa-wpa2 psk pass-phrase a1234567 aes
[AC-wlan-sec-prof-wlan-net] quit
```

# 创建名为“wlan-net”的SSID模板，并配置SSID名称为“wlan-net”。

```
[AC-wlan-view] ssid-profile name wlan-net
[AC-wlan-ssid-prof-wlan-net] ssid wlan-net
[AC-wlan-ssid-prof-wlan-net] quit
```

# 创建名为“wlan-net”的VAP模板，配置业务数据转发模式、业务VLAN，并且引用安全模板和SSID模板。

```
[AC-wlan-view] vap-profile name wlan-net
[AC-wlan-vap-prof-wlan-net] forward-mode direct-forward
[AC-wlan-vap-prof-wlan-net] service-vlan vlan-id 101
[AC-wlan-vap-prof-wlan-net] security-profile wlan-net
[AC-wlan-vap-prof-wlan-net] ssid-profile wlan-net
[AC-wlan-vap-prof-wlan-net] quit
```

# 配置AP组引用VAP模板，AP上射频0上使用VAP模板“wlan-net”的配置。

```
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] vap-profile wlan-net wlan 1 radio 0
[AC-wlan-ap-group-ap-group1] quit
```

**步骤7** 配置RU射频的信道和功率

**说明**

射频的信道和功率自动调优功能默认开启，如果不关闭此功能则会导致手动配置不生效。举例中RU射频的信道和功率仅为示例，实际配置中请根据RU的国家码和网规结果进行配置。

# 关闭RU射频0的信道和功率自动调优功能，并配置RU射频0的信道和功率。

```
[AC-wlan-view] ap-id 1
[AC-wlan-ap-1] radio 0
[AC-wlan-radio-1/0] calibrate auto-channel-select disable
[AC-wlan-radio-1/0] calibrate auto-txpower-select disable
[AC-wlan-radio-1/0] channel 20mhz 6
Warning: This action may cause service interruption. Continue?[Y/N]y
[AC-wlan-radio-1/0] eirp 127
[AC-wlan-radio-1/0] quit
[AC-wlan-ap-1] quit
[AC-wlan-view] ap-id 2
[AC-wlan-ap-2] radio 0
```

```
[AC-wlan-radio-2/0] calibrate auto-channel-select disable
[AC-wlan-radio-2/0] calibrate auto-txpower-select disable
[AC-wlan-radio-2/0] channel 20mhz 6
Warning: This action may cause service interruption. Continue?[Y/N]y
[AC-wlan-radio-2/0] eirp 127
[AC-wlan-radio-2/0] quit
[AC-wlan-ap-2] quit
```

**步骤8** 使能敏捷分布式SFN漫游功能

```
[AC-wlan-view] vap-profile name wlan-net
[AC-wlan-vap-prof-wlan-net] sfn-roam enable
Warning: This feature requires that radios work on the same channel. Enabling th
is feature will disable the channel calibration, channel scanning, and smart roa
ming functions on the AP and disconnect STAs connected to the VAP. Open, WEP, an
d WAPI encryption modes are not supported. The PSK + WPA2 mode is recommended. A
 radio allows SFN to be enabled only for one VAP. Continue?[Y/N]:y
[AC-wlan-vap-prof-wlan-net] quit
```

**步骤9** 调整敏捷分布式SFN漫游相关参数

# 漫游判决参数建议使用缺省值。

# 漫游相关射频参数需根据实际网规结果配置，本例中略。

**步骤10** 验证配置结果

# 配置完成后，执行命令**display vap ssid wlan-net**查看VAP信息，当“Status”显示为“ON”时，表示RU对应射频上的VAP已创建成功。

```
[AC-wlan-view] display vap ssid wlan-net
WID : WLAN ID
--------------------------------------------------------------------------------
AP ID AP name    RfID WID  BSSID          Status  Auth type      STA  SSID
--------------------------------------------------------------------------------
1     ru_1       0    1    00E0-FC45-62E0 ON      WPA/WPA2-PSK   0    wlan-net
2     ru_2       0    1    00E0-FC45-62E0 ON      WPA/WPA2-PSK   0    wlan-net
--------------------------------------------------------------------------------
Total: 2
```

# STA在ru_1的覆盖范围内搜索到SSID为“wlan-net”的无线网络，输入密码“a1234567”并正常关联后，在AC上执行命令**display station ssid wlan-net**，查看STA的接入信息，可以看到STA关联到了ru_1。

```
[AC-wlan-view] display station ssid wlan-net
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  IP address
--------------------------------------------------------------------------------
00e0-fcc7-1e08  1     ru_1     0/1      2.4G  11n   38/64      -68   101   10.23.101.254
--------------------------------------------------------------------------------
Total: 1 2.4G: 1 5G: 0
```

# 当STA从ru_1的覆盖范围移动到ru_2的覆盖范围时，在AC上执行命令**display station ssid wlan-net**，查看STA的接入信息，可以看到STA关联到了ru_2。

```
[AC-wlan-view] display station ssid wlan-net
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  IP address
--------------------------------------------------------------------------------
00e0-fcc7-1e08  2     ru_2     0/1      2.4G  11n   38/64      -68   101   10.23.101.254
--------------------------------------------------------------------------------
Total: 1 2.4G: 1 5G: 0
```

# 在AC上执行命令**display station roam-track sta-mac 00e0-fcc7-1e08**，可以查看该STA的漫游轨迹。

```
[AC-wlan-view] display station roam-track sta-mac 00e0-fcc7-1e08
Access SSID:wlan-net
```

```
Rx/Tx:link receive rate/link transmit rate(Mbps)
c:PMK Cache Roam r:802.11r Roam s:Same Frequency Network
--------------------------------------------------------------------------------
L2/L3          AC IP                AP name             Radio ID
BSSID          TIME                  In/Out RSSI         Out Rx/Tx
--------------------------------------------------------------------------------
--             10.23.100.1          ru_1                0
00e0-fc45-62e0  2017/10/12 16:52:58    -51/-48             46/13
L2(s)          10.23.100.1          ru_2                1
00e0-fc45-62e0  2016/10/12 16:55:45    -58/-               -/-
--------------------------------------------------------------------------------
Number: 1
```

**----结束**

# 配置文件

- SwitchA的配置文件

```
#
sysname SwitchA
#
vlan batch 100 to 101
#
dhcp enable
#
interface Vlanif101
 ip address 10.23.101.1 255.255.255.0
 dhcp select interface
 dhcp server excluded-ip-address 10.23.101.2
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 to 101
 port-isolate enable group 1
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 100
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 101
#
interface GigabitEthernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 101
#
ip route-static 0.0.0.0 0.0.0.0 10.23.101.2
#
return
```

- Router的配置文件

```
#
sysname Router
#
interface GigabitEthernet1/0/0
 ip address 10.23.101.2 255.255.255.0
#
return
```

- AC的配置文件

```
#
sysname AC
#
vlan batch 100 to 101
#
dhcp enable
```

```
#
interface Vlanif100
 ip address 10.23.100.1 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
#
capwap source interface vlanif100
#
wlan
 security-profile name wlan-net
  security wpa-wpa2 psk pass-phrase %^%#m"tz0f>~7.[`^6RWdzwCy16hJj/Mc!,}s`X*B]}A%^%# aes
 ssid-profile name wlan-net
  ssid wlan-net
 vap-profile name wlan-net
  service-vlan vlan-id 101
  sfn-roam enable
  ssid-profile wlan-net
  security-profile wlan-net
 regulatory-domain-profile name default
 ap-group name ap-group1
  radio 0
   vap-profile wlan-net wlan 1
 ap-id 0 type-id 52 ap-mac 00e0-fc45-62fd ap-sn 2102350KGF10F8000012
  ap-name central_AP
  ap-group ap-group1
 ap-id 1 type-id 55 ap-mac 00e0-fc97-c520 ap-sn 21500826402SF4900166
  ap-name ru_1
  ap-group ap-group1
  radio 0
   channel 20mhz 6
   eirp 127
   calibrate auto-channel-select disable
   calibrate auto-txpower-select disable
 ap-id 2 type-id 55 ap-mac 00e0-fc97-ca40 ap-sn 21500826402SF4900207
  ap-name ru_2
  ap-group ap-group1
  radio 0
   channel 20mhz 6
   eirp 127
   calibrate auto-channel-select disable
   calibrate auto-txpower-select disable
#
return
```