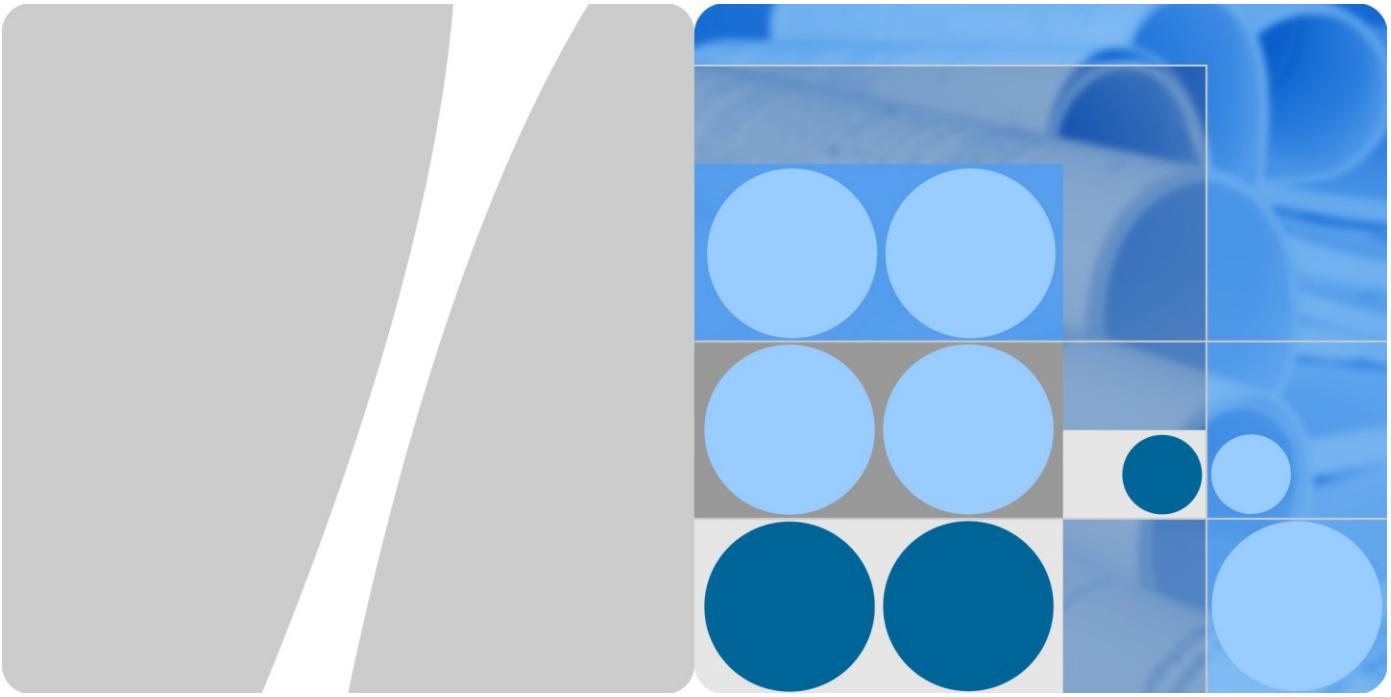


WLAN 漫游白皮书

文档版本 02

发布日期 2012-09-24

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

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

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

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

前 言

读者对象

本文档针对 WLAN 特性，从简介、原理描述和应用三个方面介绍了 WLAN 特性。

本文档与其它类型手册相结合，便于读者深入掌握特性的实现原理。

本文档主要适用于以下工程师：

- 网络规划工程师
- 调测工程师
- 数据配置工程师
- 系统维护工程师

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
 危险	表示有高度潜在危险，如果不能避免，会导致人员死亡或严重伤害。
 警告	表示有中度或低度潜在危险，如果不能避免，可能导致人员轻微或中等伤害。
 注意	表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
 窍门	表示能帮助您解决某个问题或节省您的时间。
 说明	表示是正文的附加信息，是对正文的强调和补充。

命令行格式约定

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

修订记录

修改记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本 02 (2012-09-24)

相对于版本 01 (2011-12-13)的变化如下：

修改：

- 1.2.1 二层漫游
- 1.2.2 跨 VLAN 漫游

文档版本 01 (2011-12-13)

第一次正式发布。

目 录

1 WLAN 漫游技术

关于本章

1.1 介绍

定义

简单来说，WLAN 漫游策略是指 STA 可以在 WLAN 网络范围内任意移动；具体来说，STA 可以在同属一个 ESS 的 AP 接入，并且在移动的过程中保证已有的业务不中断。

WLAN 的漫游策略包括下面两种：

- 二层漫游：在同一个子网内的漫游。根据用户是否支持快速漫游，又可以将二层漫游分为快速漫游和非快速漫游两种方式。
  - 快速漫游，又称为二层安全漫游。它是指如果 STA 使用的是 WPA/WPA2+802.1X 的安全策略，并且支持 Key Caching 快速漫游技术时，这时的用户漫游即为快速安全漫游，不需要重新完成 802.1X 认证过程，只需要完成四步密钥交互即可。
  - 非快速漫游：当用户使用的是非 WPA/WPA2+802.1X 的安全策略时，用户的漫游都属于非快速漫游。此外，如果用户使用的是 WPA/WPA2+802.1X 的安全策略，但用户不支持快速漫游，则改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。
- 跨 VLAN 的三层漫游：用户漫游过程中的新老 AP 对应的业务 VLAN 不同。为了保证漫游过程中用户业务不断，则必须保持用户的 VLAN 不变。即用户数据报文的 VLAN 仍然为初始 VLAN，而不是被切换到新 AP 的 VLAN 上。

目的

WLAN 漫游策略主要解决以下问题：

- 避免漫游过程中的认证时间过长导致丢包甚至业务中断。

  采用 WPA/WPA2+802.1X 认证模式的终端发生漫游时，802.1X 认证认证过程报文交互次数和时间，大于 WLAN 用户连接新 AP 的过程，所以实现快速漫游需要避免重新进行用户认证。
- 保证用户授权信息不变。

  用户的认证和授权信息，是用户访问网络的通行证，如果终端漫游接入的 AC 无法获取用户原来的认证和授权信息，则用户必须重新认证上线，使得用户切换过程缓慢、用户当前业务中断。
- 如何保证用户 IP 地址不变。

  应用层协议均以 IP 地址和 TCP/UDP Session 为用户业务承载，漫游后的用户必须能够保持原 IP 地址不变，对应的 TCP/UDP Session 才能够不中断，应用层数据才能够保持正常转发。

  漫游技术必须通过认证和授权信息及 PMK 预同步机制，解决认证时间过长问题，同时解决认证授权信息保持问题。

受益

用户受益

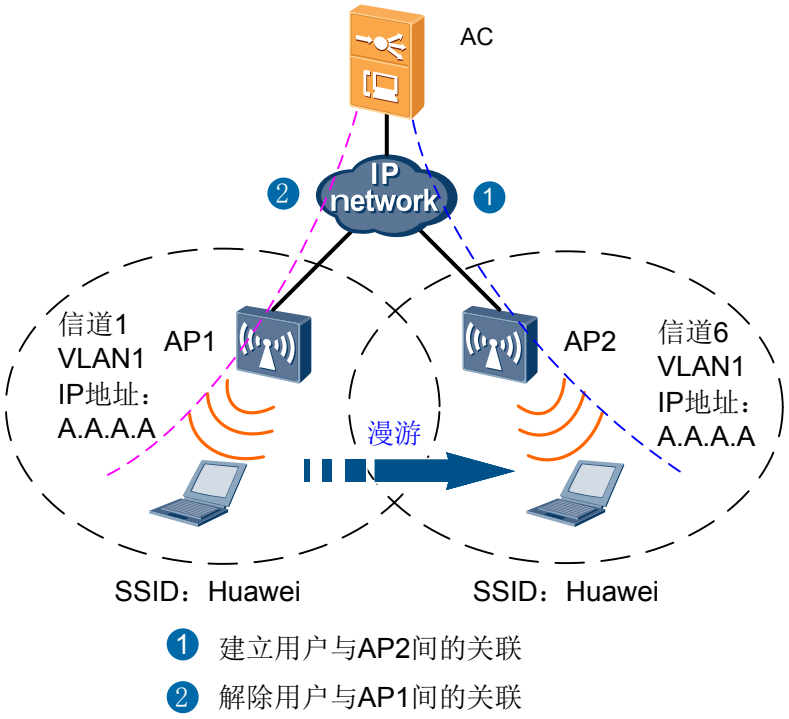
- 当用户使用的安全策略为 Open、Share-key、WPA+PSK、WPA2+PSK、WPA2+802.1X（快速漫游）时，用户漫游切换时间<100ms，漫游前后业务不中断。
- 当用户使用的安全策略为 WPA+802.1X、WPA2+802.1X（非快速漫游）、WAPI 时，用户漫游切换时间>100ms，漫游前后业务不中断。

1.2 原理描述

1.2.1 二层漫游

AP 与 AC 直连组网，多个 AP 连接在同一个 VLAN 内，由于 STA 在不同的 AP 间切换时，始终在一个 VLAN 子网内，从而保证业务不中断。

图1-1 AC 内二层漫游



如图 1-1 所示，AC 判断 STA 是否是首次接入，如果不是首次接入，即为用户从 AP1 的覆盖范围切换到 AP2 的覆盖范围，AC 会按照如下的流程实现漫游功能：

1. AC 已经与 AP1 建立关联信息，STA 在各种信道中发送 802.11 请求帧。AP2 在信道 6（AP2 使用的信道）中收到请求后，通过在信道 6 中发送应答来进行响应。STA 收到应答后，对其进行评估，确定同哪个 AP 关联最合适。
2. 如图中的标号 1 所示，STA 通过信道 6 向 AP2 发送关联请求，AP2 使用关联响应做出应答，建立用户与 AP2 间的关联。
3. 如图中的标号 2 所示，删除用户与 AP1 现有的关联。STA 通过信道 1（AP1 使用的信道）向 AP1 发送 802.11 解除关联信息，解除用户与 AP1 间的关联。

上述过程完成后：

- 如果用户使用的是 Open 或 Share-key 的安全策略，则用户漫游已完成。
- 如果用户使用的是 WPA/WPA2+PSK 的安全策略，则还需要完成四步密钥协商。
- 如果用户不支持快速漫游，即使使用的是 WPA2+802.1X 的安全策略，则用户仍需要完成 802.1X 认证过程才能完成漫游。
- 只有在用户既支持快速漫游，同时用户使用的是 WPA2+802.1X 的安全策略，用户才会快速漫游，没有重认证的过程，只需要完成四步密钥交互即可。

快速漫游

二层漫游中，根据用户是否支持快速漫游，可将漫游分为快速漫游和非快速漫游两种方式。

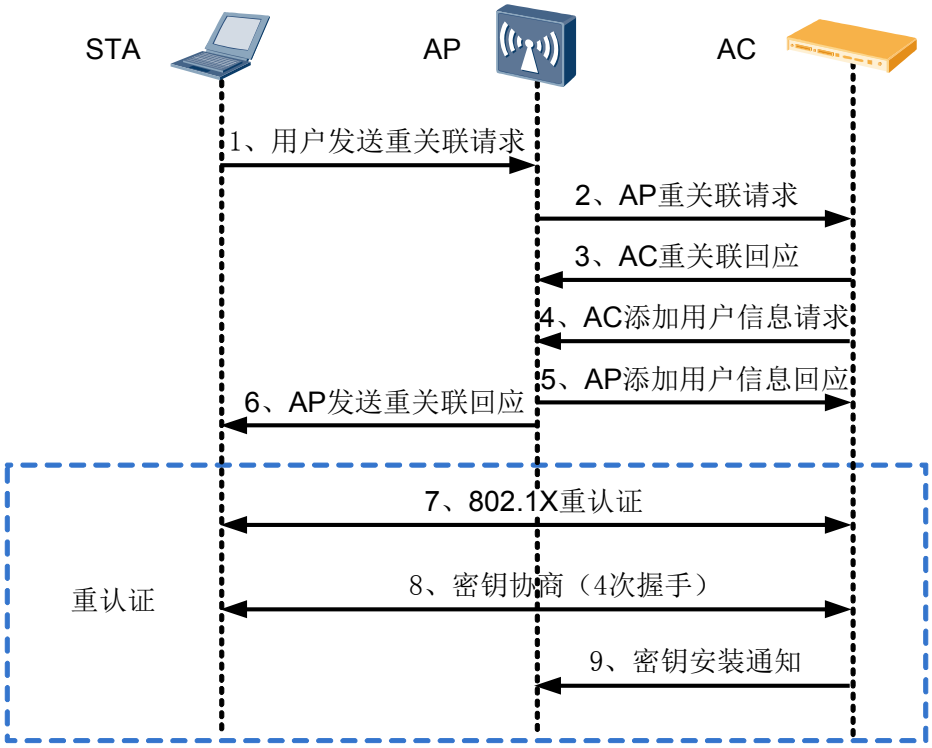
快速漫游中，由于采用了 Key Cache 机制，跳过了重新认证过程，使得用户的漫游切换过程加速。具体如下：

1. WPA2-802.1x 安全用户接入网络认证成功时，AC 通过认证过程获得本次认证的用户 PMK。AC 本地保存该用户的 PMK 信息，直到其下线。
2. AC 将 PMK 下发给用户接入的 AP1，AP1 依据 PMK 和用户协商生成空口加密密钥。
3. 当用户发生漫游，向邻居 AP2 发起关联请求时，AP2 及时向 AC 通报用户切换消息。
4. AC 查找到该用户对应的 PMK，并发送给 AP2。
5. 当终端发起重认证请求时，AP2 直接反馈认证成功、并发起密钥协商。

为了进一步提高快速漫游的切换时间，可以通过密钥协商下移来实现，即将原 STA 和 AC 间进行的密钥协商过程优化为 STA 和 AP 间进行密钥协商，减少了报文转发的开销和 AC 集中处理时的负担。

普通的 WPA/WPA2 802.1X 方式的无线无线用户漫游的流程如图 1-2 所示。

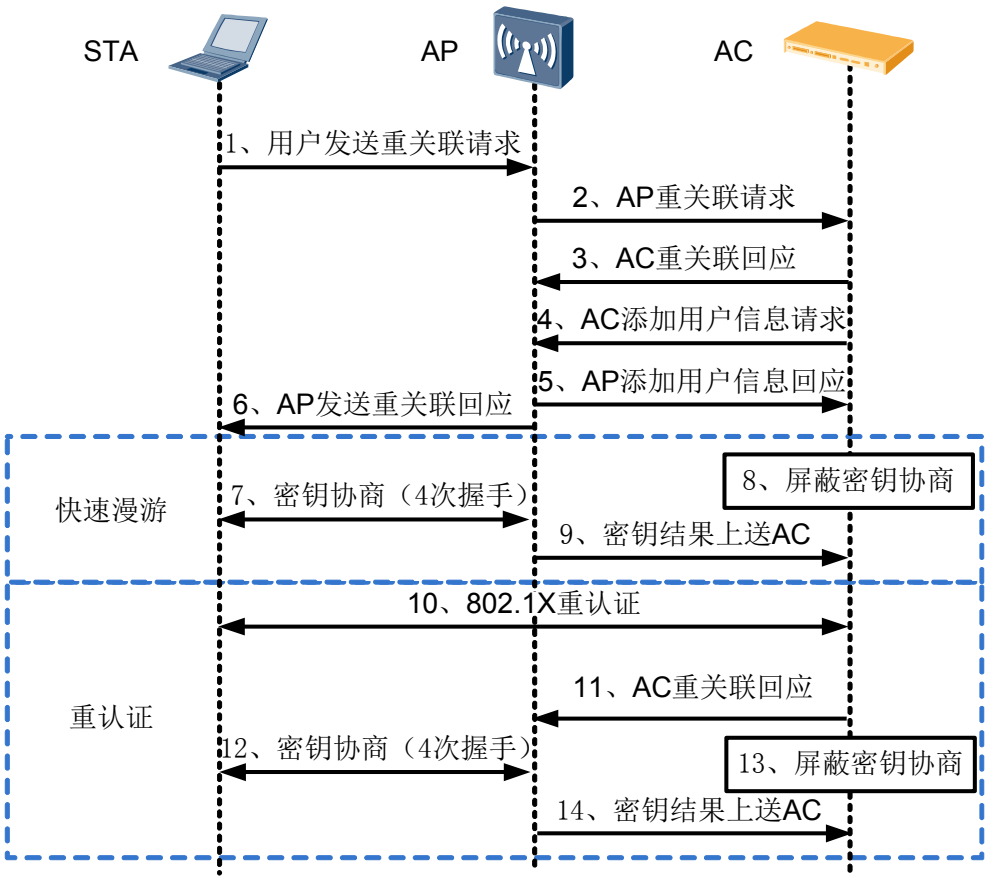
图1-2 密钥协商在 STA 与 AC 间



WPA/WPA2 802.1X 方式的无线用户漫游流程分为 5 个阶段：扫描阶段、链路认证阶段、关联阶段（步骤 1 到步骤 6）、802.1X 认证阶段（步骤 7）、密钥协商阶段（步骤 8）。交互流程如上图所示，其中扫描阶段、链路认证阶段在 AP 完成，没有在上图中描述。

密钥下移后 STA 认证上线流程如图 1-3 所示。

图1-3 密钥协商在 STA 与 AP 间



在上图步骤 2 中，需要 AP 在关联、重关联请求中将用户的 PMKID 上送到 AC；（WPA2 802.1X 方式的无线用户支持上送 PMKID，WPA 802.1x 方式的无线用户漫游时候没有携带 PMKID）

步骤 6，AC 判断密钥协商功能在 AP，则根据用户的 PMKID 选择对应的 PMK，在关联、重关联回应中传给 AP，包括：AP 进行密钥协商的标记、以及 PMK 信息；如果密钥协商功能在 AC 或者用户非快速漫游或者没有 PMKID 或者没有找到对应的 PMK 信息，则不携带标记和 PMK 信息；

步骤 8，AC 判断该用户的密钥协商功能下发到 AP，则屏蔽密钥协商功能；

条件选择流程：

- 快速漫游：

1. 步骤 7，AP 根据下发的 PMK 信息，在给用户发送重关联回应后和用户进行密钥协商；
2. 步骤 9，AP 和用户密钥协商成功后，发消息通知 AC。如果密钥协商失败走删除用户流程；

- 重认证：

1. 如果步骤 6 后，如果用户主动发起 802.1X 认证，则在步骤 10 中走重认证。AP 感知用户的 802.1X 认证报文，如果发现密钥协商过程中用户走重认证，需要停止密

钥协商流程。AC 和用户进行 802.1X 认证，认证后判断密钥协商功能在 AP，则在步骤 11 下发 PMK 到 AP，包括：AP 进行密钥协商的标记、以及 PMK 信息；

2. 步骤 12，AP 收到 AC 的密钥协商通知，和用户进行密钥协商；
3. 步骤 13，AC 判断该用户的密钥协商功能下发到 AP，则屏蔽调密钥协商功能；
4. 步骤 14，AP 和用户密钥协商成功后，发消息通知 AC。如果密钥协商失败走删除用户流程；

1.2.2 跨 VLAN 漫游

随着无线网络的发展，越来越多的人开始使用 WLAN。由于 AP 覆盖范围有限，往往在不同楼层会部署多台 AP，同时 AP 在不同的 VLAN 内。此时，如果用户在无线网络的覆盖区域内从某一个楼层漫游到另外一个楼层时，就会导致业务中断，严重影响用户体验。

在这样的背景下，跨 VLAN 漫游应运而生，它使用户在不同 VLAN 间漫游时，依旧保持用户的 VLAN 为初始 VLAN，从而保证用户在不同 VLAN 间漫游而业务不中断。

图1-4 跨 VLAN 漫游

如图 1-4 所示，跨 VLAN 漫游的具体过程为：

1. STA 通过 AP1（属于 VLAN1）申请同 AC 发生关联，AC 判断该 STA 为首次接入用户，为其创建并保存相关的用户数据信息，以备将来漫游时使用。
2. 该 STA 从 AP1 覆盖区域向 AP2（属于 VLAN2）覆盖区域移动；STA 通过 AP2 重新同 AC 发生关联，AC 通过用户数据信息判断该 STA 为漫游用户，更新用户数据库信息。

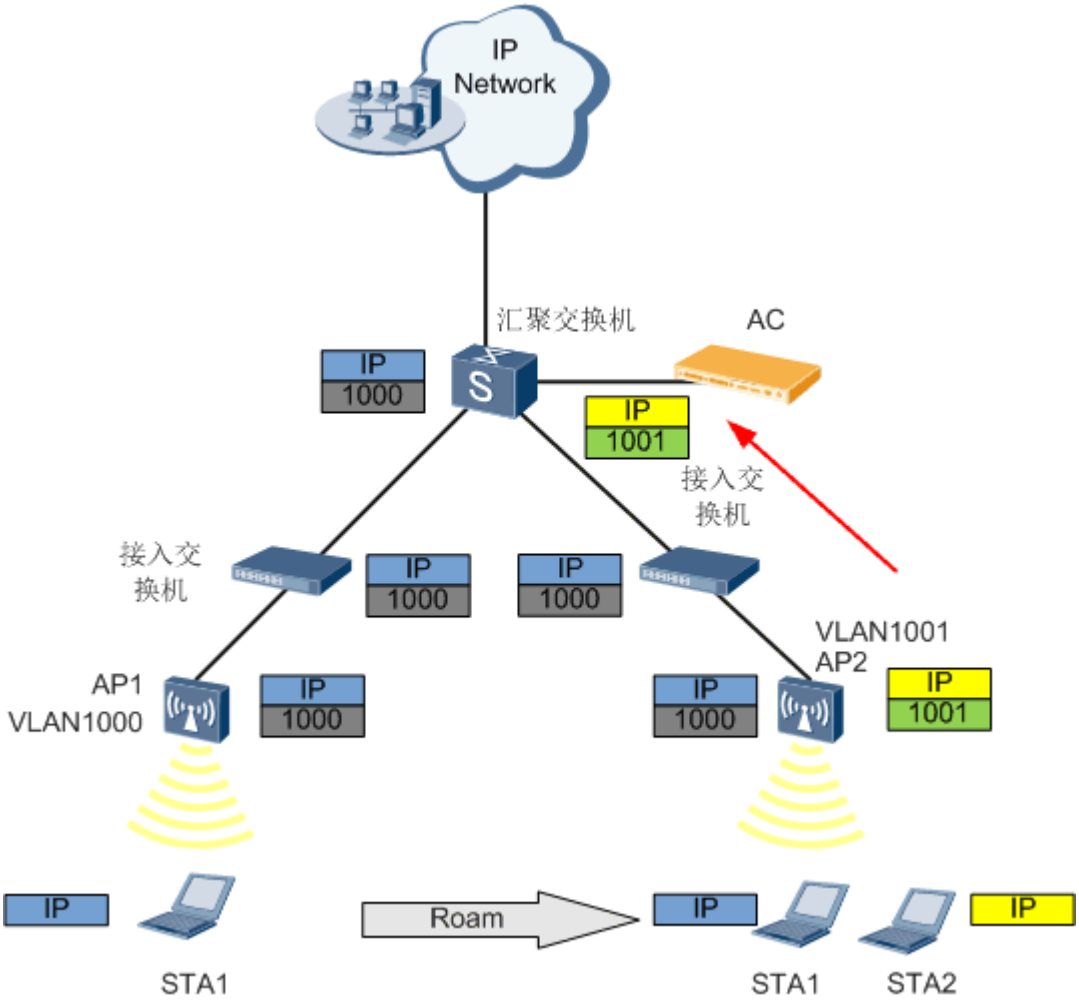
3. STA 断开同 AP1 的关联。尽管漫游前后不在同一个子网中，AC 仍然把 STA 视为从原始子网（VLAN1）连过来一样，允许 STA 保持其原有 IP 并支持已建立的 IP 通讯。

直接转发模式下的跨 VLAN 漫游

直接转发又称为数据本地转发，即用户报文没有经过 CAPWAP 隧道封装，而是直接转发到上层网络，从而提高报文的转发效率。

如图 1-5 所示，直接转发模式下的跨 VLAN 漫游的具体过程为：

图1-5 直接转发下的跨 VLAN 漫游原理



1. STA1 通过 AP1 上线，此时 STA1 的用户 VLAN 为 VLAN1000。
2. AC 在用户漫游过程中下发用户 VLAN 给 AP，同时 AP 根据用户打上用户 VLAN 的 Tag。
3. 当 STA1 漫游到 AP2 后，为了保证业务不中断，当用户报文上传到 AP2 时，AP2 给用户报文打上漫游前的 VLAN1000 的 Tag 发往上层网络。而对于 AP2 下的未漫游用户 STA2，则 AP2 仍然打上用户 VLAN 1001 发往上层网络。

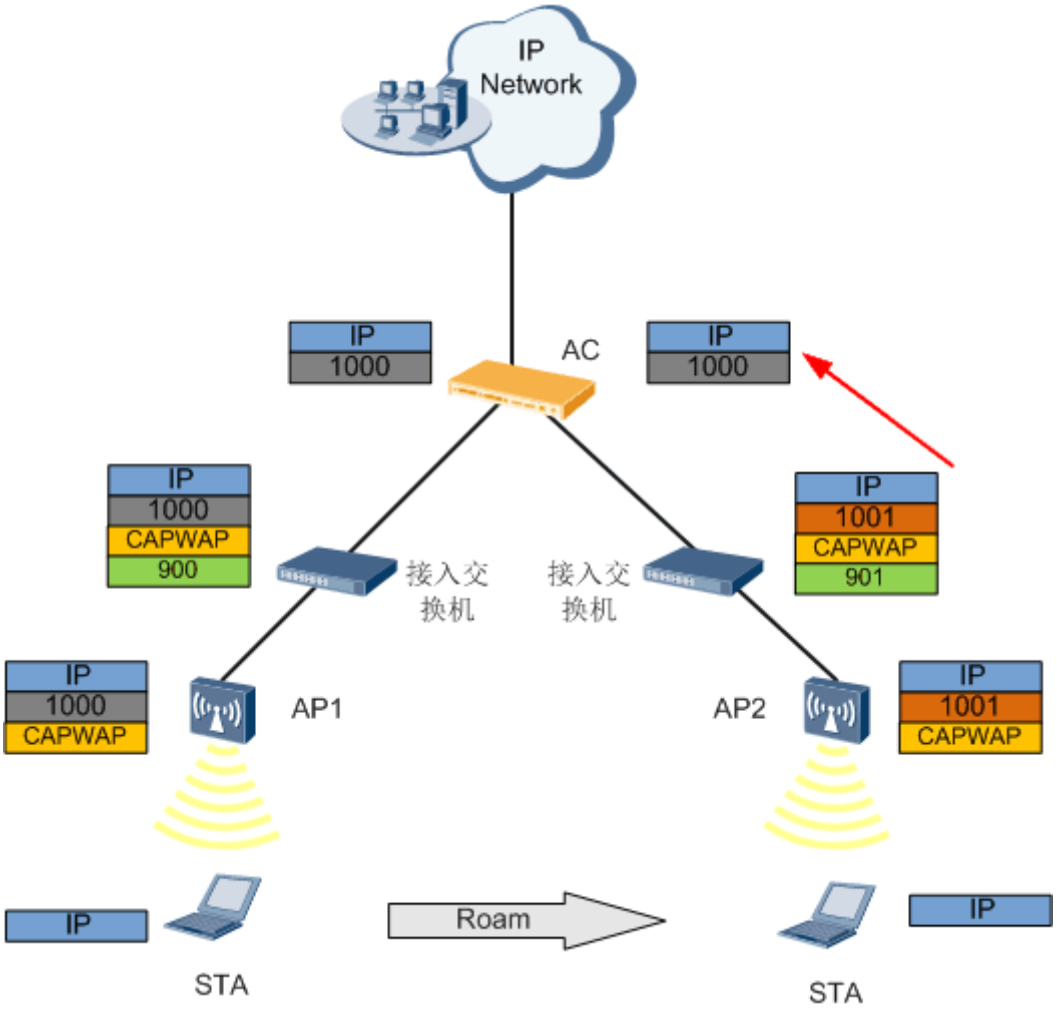
说明

直接转发模式下的跨 VLAN 漫游，需要漫游后 AP2 对用户报文打漫游前的 VLAN，同时交换机需要允许这个 VLAN 接入。

隧道转发下的跨 VLAN 漫游

CAPWAP 隧道转发又称为集中转发，即用户报文必须先经过 CAPWAP 隧道封装后上传给 AC，然后再由 AC 转发到上层网络，从而提高报文的转发安全性。隧道转发模式下的跨 VLAN 漫游：

图1-6 隧道转发下的跨 VLAN 漫游原理



如图 1-6 所示，隧道转发模式下的跨 VLAN 漫游的具体过程为：

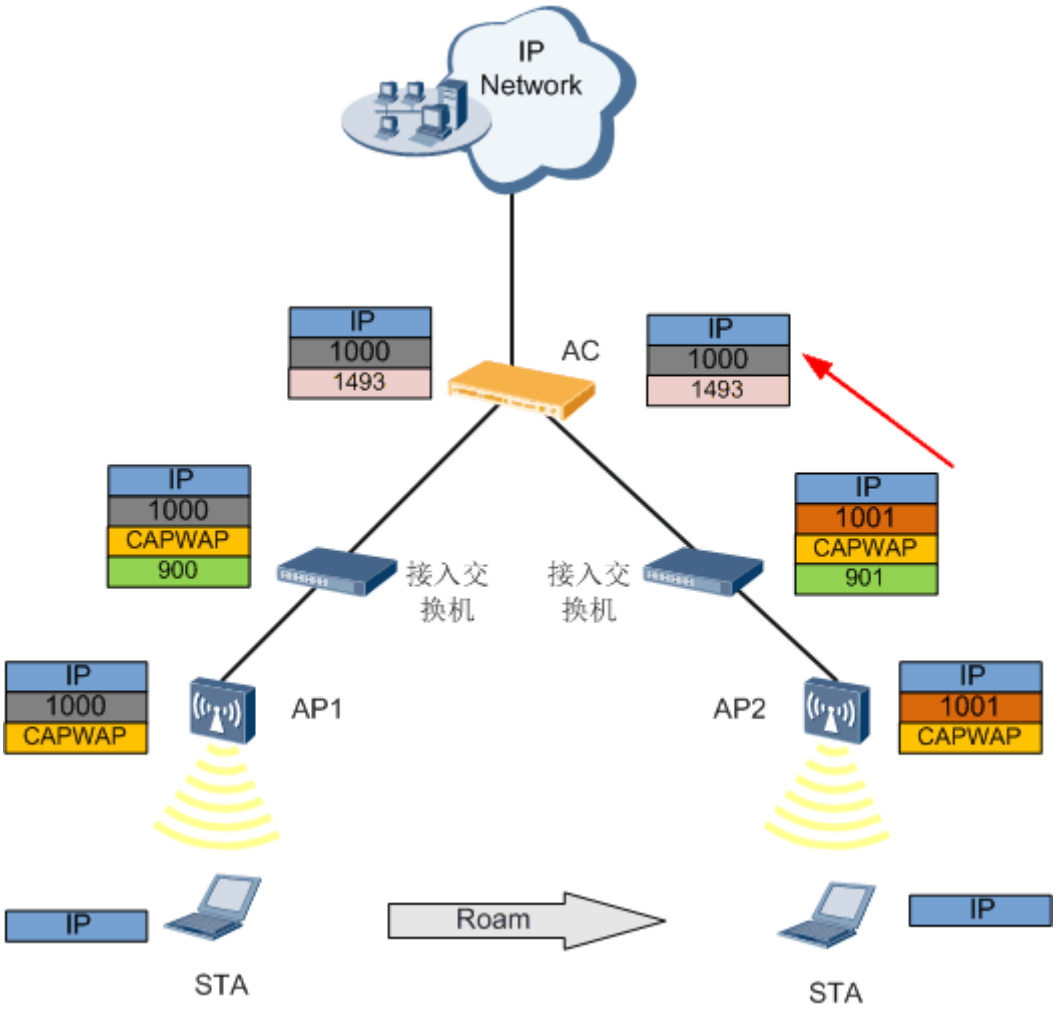
1. 未漫游前，用户 VLAN 为 1000，当 STA 的报文经过 AP1 时，AP1 给用户报文打上 VLAN1000 的 Tag 并进行隧道封装。在到达交换机时，由交换机给封装后的报文打上 VLAN900 的 Tag 并转发给 AC。到达 AC 后，AC 去除 VLAN900 的 Tag，并将用户报文解封装后直接发送至网络侧。

2. 当 STA 漫游到 AP2 后，当 STA 的报文经过 AP2 时，AP2 给用户报文打上 VLAN1001 的 Tag 并进行隧道封装。在到达交换机时，由交换机给封装后的报文打上 VLAN901 的 Tag 并转发给 AC，到达 AC 后，AC 去除 VLAN901 的 Tag，将用户报文解封装，并将用户报文中的 VLAN1001 替换为 VLAN1000 后发往有线侧。从而使得业务不中断。

QinQ 场景下的跨 VLAN 漫游

QinQ 是在 802.1Q VLAN 的基础上增加了一层 802.1Q VLAN 标签，拓展了 VLAN 空间。为了适应城域以太网的发展，QinQ 封装、终结的方式也越来越丰富，在运营商的业务精细化运营方面得到了越来越深入的应用。

图1-7 QinQ 场景下的跨 VLAN 三层漫游原理



如图 1-7 所示，QinQ 场景下的跨 VLAN 三层漫游的具体过程为：

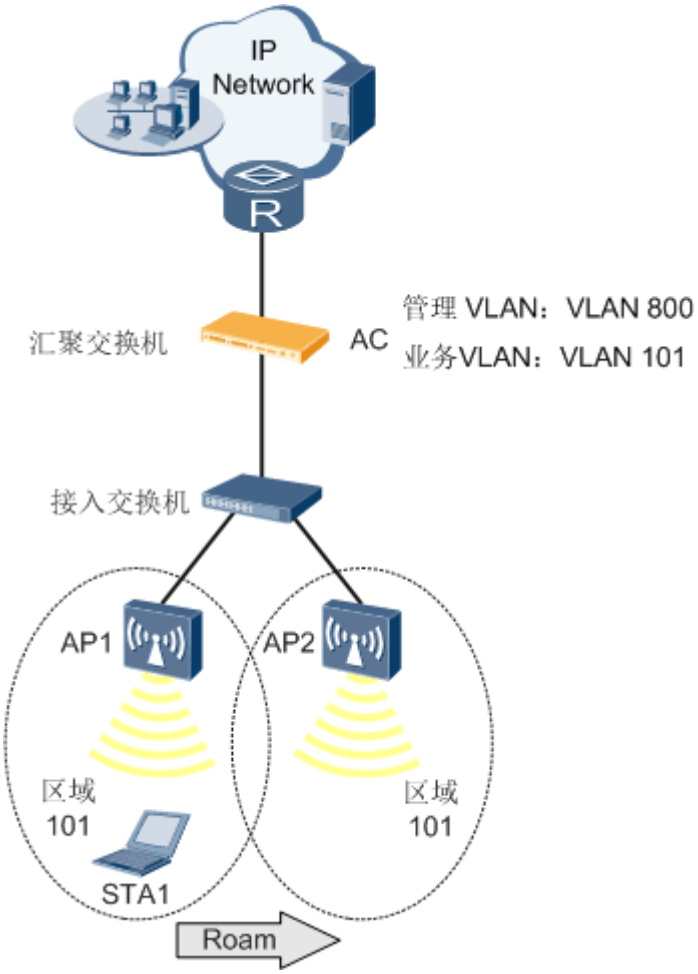
1. 假设漫游前内层用户 VLAN 为 1000，外层 VLAN 为 1493。

2. 未漫游前，用户 VLAN 为 1000，当 STA 的报文经过 AP1 时，AP1 给用户报文打上 VLAN1000 的 Tag 并进行隧道封装，到达 AC 后，AC 将用户报文解封装，并在 VLAN1000 的基础上增加了 VLAN 1493 的 Tag 后发送至网络侧。
3. 当 STA 漫游到 AP2 后，当 STA 的报文经过 AP2 时，AP2 给用户报文打上 VLAN1001 的 Tag 并进行隧道封装，到达 AC 后，AC 将用户报文解封装，并将用户报文中的 VLAN1001 替换为 VLAN1000，并在 VLAN1000 的基础上增加了 VLAN 1493 的 Tag 后发送至网络侧，从而使得业务不中断。

1.3 应用

1.3.1 集中转发模式下的快速漫游

图1-8 集中转发模式下的快速漫游组网图



组网配置注意事项：

- AP 都接在同一 AC 下。
- WLAN-ESS 接口下配的认证方式相同。

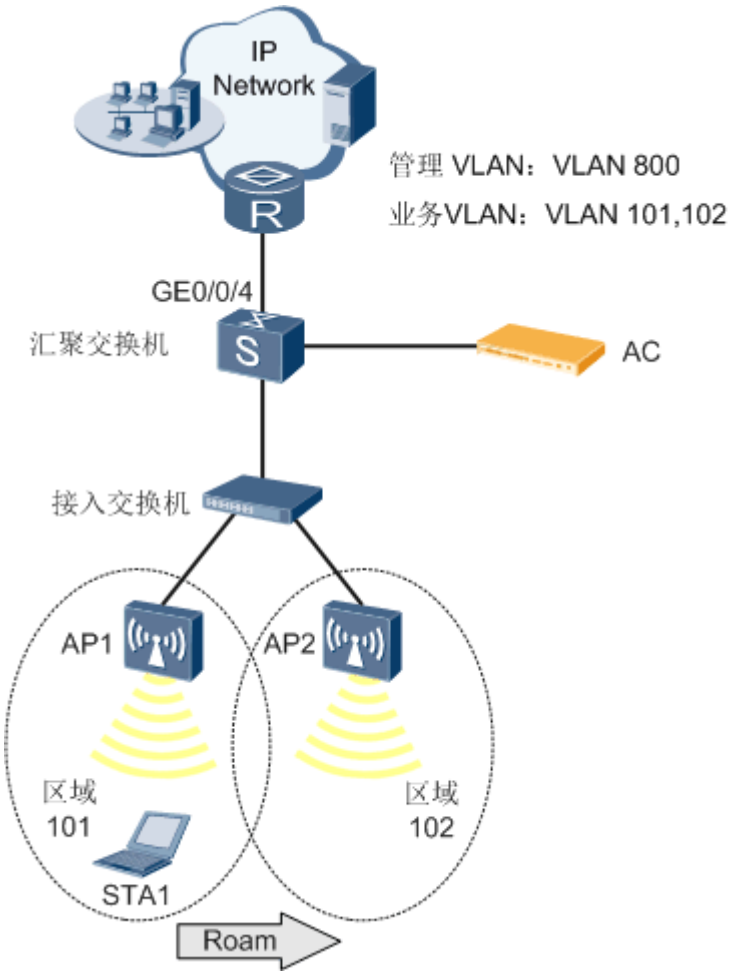
- 每个 WLAN-ESS 接口下都必须配置两个业务 VLAN。
- 安全模板配置必须保持一致。
- 服务集模板中配置的 SSID 和数据转发模式必须相同。

```
#
 sysname AC
#
 vlan batch 101 800
#
 dhcp enable
#
 wlan ac-global carrier id other ac id 1
#
interface Vlanif101
 ip address 128.1.1.1 255.255.255.0
 dhcp select interface
#
interface Vlanif800
 ip address 10.1.1.1 255.255.255.0
 dhcp select interface
#
interface Wlan-Ess0
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101 800
 dhcp enable
#
wlan
 wlan ac source interface vlanif800
 ap-profile name huawei id 1
  4-way-handshake roam-policy ap
 ap-region id 101
 ap-auth-mode mac-auth
 ap id 0 type-id 6 mac 286E-D42B-0CE5 sn AB34002078
  region-id 101
  profile-id 1
 ap id 1 type-id 6 mac 0025-9EE8-DF70 sn AB36015000
  region-id 101
  profile-id 1
 wmm-profile name huawei id 0
 traffic-profile name huawei id 0
 security-profile name huawei id 0
  security-policy wpa
  wpa authentication-method dot1x peap encryption-method ccmp
 service-set name huawei-1 id 0
  forward-mode tunnel
  wlan-ess 0
  ssid huawei
  traffic-profile id 0
  security-profile id 0
  service-vlan 101
 service-set name huawei-2 id 1
```

```
 forward-mode tunnel
 wlan-ess 0
 ssid huawei
 traffic-profile id 0
 security-profile id 0
 service-vlan 101
radio-profile name huawei id 0
 wmm-profile id 0
ap 1 radio 0
 radio-profile id 0
 service-set id 0 wlan 1
ap 2 radio 0
 radio-profile id 0
 service-set id 1 wlan 2
#
return
```

1.3.2 直接转发模式下的跨 VLAN 漫游

图1-9 本地转发模式下的跨 VLAN 的二层漫游



该组网为 AC 旁挂方式，在该组网中采用本地转发方式。

组网配置注意事项：

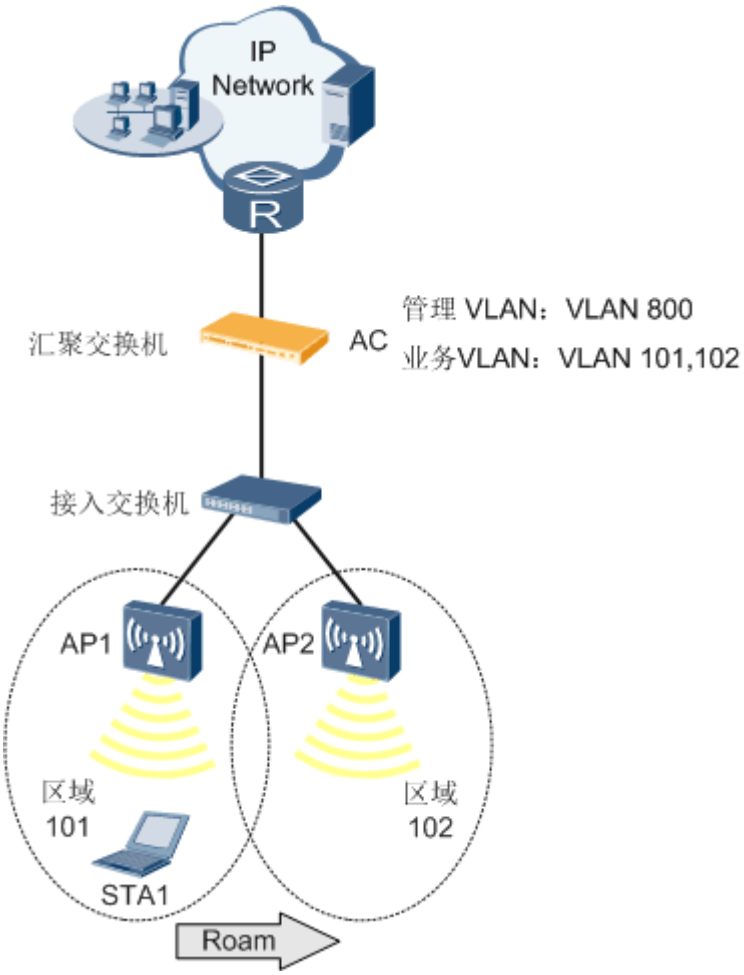
- AP 都接在同一 AC 下。
- WLAN-ESS 接口下配的认证方式相同。
- 每个 WLAN-ESS 接口下都必须配置两个业务 VLAN。
- 安全模板配置必须保持一致。
- 服务集模板中配置的 SSID 和数据转发模式必须相同。

```
#
 sysname AC
#
 vlan batch 101 102 800
#
 dhcp enable
#
 wlan ac-global carrier id other ac id 1
#
interface Vlanif101
 ip address 128.1.1.1 255.255.255.0
 dhcp select interface
#
interface Vlanif102
 ip address 128.1.2.1 255.255.255.0
 dhcp select interface
#
interface Vlanif800
 ip address 10.1.1.1 255.255.255.0
 dhcp select interface
#
interface Wlan-Ess0
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101 to 102
#
interface Wlan-Ess1
 port hybrid pvid vlan 102
 port hybrid untagged vlan 101 to 102
 dhcp enable
#
interface Ethernet2/0/0
 port link-type trunk
 port trunk allow-pass vlan 101 102 800
 dhcp enable
#
wlan
 wlan ac source interface vlanif800
 ap-region id 5
 ap-region id 6
 ap-auth-mode mac-auth
 ap id 0 type-id 6 mac 286E-D42B-0CE5 sn AB34002078
  region-id 5
 ap id 1 type-id 6 mac 0025-9EE8-DF70 sn AB36015000
  region-id 6
 wmm-profile name huawei id 0
 traffic-profile name huawei id 0
```

```
 security-profile name huawei id 0
 service-set name huawei-1 id 0
  wlan-ess 0
  ssid huawei
  traffic-profile id 0
  security-profile id 0
  service-vlan 101
 service-set name huawei-2 id 1
  wlan-ess 1
  ssid huawei
  traffic-profile id 0
  security-profile id 0
  service-vlan 102
 radio-profile name huawei id 0
  wmm-profile id 0
 ap 1 radio 0
  radio-profile id 0
  service-set id 0 wlan 1
 ap 2 radio 0
  radio-profile id 0
  service-set id 1 wlan 2
#
return
```

1.3.3 隧道转发下的跨 VLAN 漫游

图1-10 集中转发下的跨 VLAN 三层漫游原理



组网配置注意事项：

- AP 都接在同一 AC 下。
- WLAN-ESS 接口下配的认证方式相同。
- 每个 WLAN-ESS 接口下都必须配置两个业务 VLAN。
- 安全模板配置必须保持一致。
- 服务集模板中配置的 SSID 和数据转发模式必须相同。

```
#
 sysname AC
#
 vlan batch 101 102 800
#
 dhcp enable
#
 wlan ac-global carrier id other ac id 1
#
```

```
interface Vlanif101
 ip address 128.1.1.1 255.255.255.0
 dhcp select interface
#
interface Vlanif102
 ip address 128.1.2.1 255.255.255.0
 dhcp select interface
#
interface Vlanif800
 ip address 10.1.1.1 255.255.255.0
 dhcp select interface
#
interface Wlan-Ess0
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101 to 102
#
interface Wlan-Ess1
 port hybrid pvid vlan 102
 port hybrid untagged vlan 101 to 102
 dhcp enable
#
interface Ethernet2/0/0
 port link-type trunk
 port trunk allow-pass vlan 101 102 800
 dhcp enable
#
wlan
 wlan ac source interface vlanif800
 ap-region id 5
 ap-region id 6
 ap-auth-mode mac-auth
 ap id 0 type-id 6 mac 286E-D42B-0CE5 sn AB34002078
  region-id 5
 ap id 1 type-id 6 mac 0025-9EE8-DF70 sn AB36015000
  region-id 6
 wmm-profile name huawei id 0
 traffic-profile name huawei id 0
 security-profile name huawei id 0
 service-set name huawei-1 id 0
  forward-mode tunnel
  wlan-ess 0
  ssid huawei
  traffic-profile id 0
  security-profile id 0
  service-vlan 101
 service-set name huawei-2 id 1
  forward-mode tunnel
  wlan-ess 1
  ssid huawei
  traffic-profile id 0
  security-profile id 0
  service-vlan 102
 radio-profile name huawei id 0
  wmm-profile id 0
 ap 1 radio 0
```

```
  radio-profile id 0
  service-set id 0 wlan 1
 ap 2 radio 0
  radio-profile id 0
  service-set id 1 wlan 2
#
return
```