

目 录

1 WLAN 漫游	1-1
1.1 WLAN 漫游简介	1-1
1.2 WLAN 漫游实现方式介绍	1-1
1.3 三层漫游	1-1
1.4 配置客户端漫游表项老化时间	1-2
1.5 WLAN 漫游显示和维护	1-2
1.6 WLAN 漫游典型配置举例	1-3
2 漫游增强技术	2-1
2.1 802.1X 快速漫游	2-1
2.1.1 802.1X 快速漫游工作机制	2-1
2.1.2 802.1X 快速漫游配置限制和指导	2-2
2.2 MAC 快速漫游	2-2
2.2.1 MAC 快速漫游工作机制	2-2
2.2.2 MAC 快速漫游配置限制和指导	2-3
2.2.3 配置 MAC 地址认证成功后的快速连接功能	2-3
2.3 802.11r	2-4
2.3.1 802.11r 简介	2-4
2.3.2 802.11r 配置限制和指导	2-6
2.3.3 配置 802.11r	2-6
2.3.4 FT Over-the-DS 方式 802.11r 典型配置举例（PSK 模式）	2-7
2.3.5 FT Over-the-DS 方式 802.11r 典型模式配置举例（802.1X）	2-13
2.4 802.11v	2-18
2.4.1 802.11v 简介	2-18
2.4.2 802.11v 配置限制和指导	2-18
2.4.3 开启 BSS 切换管理功能	2-18
2.4.4 配置 BSS 切换解除关联功能	2-19
2.4.5 802.11v 典型配置举例	2-19
2.5 虚拟 BSS 漫游	2-22
2.5.1 虚拟 BSS 漫游简介	2-22
2.5.2 虚拟 BSS 漫游与硬件适配关系	2-22
2.5.3 虚拟 BSS 漫游配置限制和指导	2-24
2.5.4 配置虚拟 BSS 漫游	2-24

2.6 协同漫游	2-24
2.6.1 协同漫游简介	2-24
2.6.2 协同漫游配置限制和指导	2-25
2.6.3 配置无线客户端反粘滞功能	2-25
2.6.4 配置设备对异常 802.11kv 无线客户端进行非 802.11kv 处理	2-26
2.6.5 配置获取 BSS 候选列表功能	2-27
2.6.6 开启漫游优化流量保持高级功能	2-27
2.6.7 协同漫游显示和维护	2-28
2.6.8 协同漫游典型配置举例	2-28
3 漫游组	3-1
3.1 漫游组简介	3-1
3.2 WLAN 漫游基本概念	3-1
3.3 漫游组实现方式介绍	3-1
3.4 IADTP 隧道建立过程	3-2
3.5 漫游组配置限制和指导	3-3
3.6 漫游组配置任务简介	3-3
3.7 创建漫游组	3-4
3.8 配置漫游组认证模式	3-4
3.9 配置漫游组 IADTP 隧道 IP 地址类型	3-4
3.10 配置设备加入漫游组时建立 IADTP 隧道的源 IP 地址	3-5
3.11 配置设备发送的 IADTP 隧道控制报文的 DSCP 优先级	3-5
3.12 添加漫游组内的成员设备	3-6
3.12.1 手动添加漫游组内的成员设备	3-6
3.12.2 自动添加漫游组内的成员设备	3-6
3.13 配置本成员设备在漫游组中的角色	3-7
3.14 关闭 IADTP 数据隧道功能	3-7
3.15 开启漫游中继功能	3-8
3.16 开启漫游组功能	3-9
3.17 开启漫游组隧道隔离功能	3-9
3.18 开启漫游组告警功能	3-9
3.19 漫游组显示和维护	3-10
3.20 漫游组典型配置举例	3-10
3.20.1 漫游组典型配置举例	3-10

1 WLAN 漫游

1.1 WLAN漫游简介

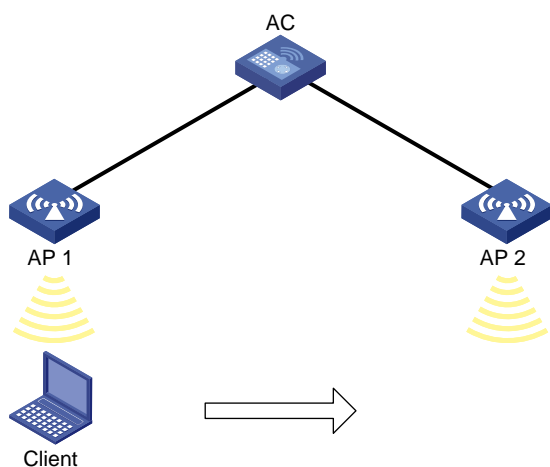
在同属于一个 ESS（Extended Service Set，拓展服务集）区域中的不同 AP 覆盖范围内，无线客户端从一个 AP 上接入转移到另一个 AP 上接入的过程称为漫游。在漫游期间，客户端的 IP 地址、授权信息等维持不变。

1.2 WLAN漫游实现方式介绍

如[图 1-1](#)所示，客户端漫游的具体过程如下：

- (1) 客户端在 AP 1 上初始上线，在 AC 上会创建该客户端的漫游表项信息（漫游表项信息主要包括客户端上线 SSID、PMKID、认证方式、安全认证模式以及漫游 VLAN 等）。
- (2) 客户端漫游到 AP 2，AC 查找该客户端的漫游表项。
- (3) 客户端重新认证，在 AP 2 上上线。

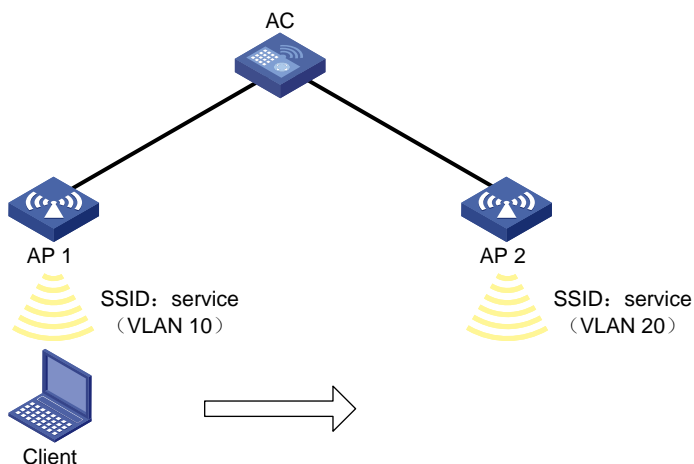
图1-1 WLAN 漫游实现方式示意图



1.3 三层漫游

如[图 1-2](#)所示，当客户端从 AP 1 漫游到 AP 2 时，设备无需任何特殊配置，即可完成跨 VLAN 的漫游。漫游具体过程请参见“[1.2 WLAN 漫游实现方式介绍](#)”。

图1-2 三层漫游示意图



1.4 配置客户端漫游表项老化时间

1. 功能简介

无线客户端漫游表项记录了客户端的 PMK 列表、接入 VLAN 以及其他授权信息。无线客户端断开连接之后，如果在客户端漫游表项老化时间内再次成功关联 AP，则可继承表项记录的各种授权信息，实现快速漫游。如果客户端离线时间超过了老化时间，系统会自动清除该客户端的记录。

2. 配置限制和指导

配置无线客户端漫游表项的老化时间为 0 时，表示客户端下线之后会立即删除客户端漫游表项相关信息，客户端无法实现快速漫游。

本命令仅支持配置 AC 内漫游客户端的 Cache 老化时间，不支持 AC 间漫游场景。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入无线服务模板视图。

```
wlan service-template service-template-name
```

- (3) 配置客户端漫游表项老化时间。

```
client cache aging-time aging-time
```

缺省情况下，无线客户端漫游表项的老化时间为 180 秒。

1.5 WLAN漫游显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后的漫游运行情况，通过查看显示信息验证配置的效果。

表1-1 WLAN 漫游显示和维护

操作	命令
显示客户端的漫游跟踪信息	<code>display wlan mobility roam-track mac-address mac-address</code>

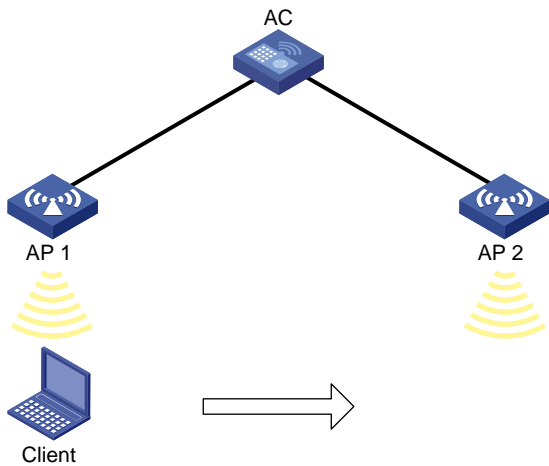
1.6 WLAN漫游典型配置举例

1. 组网需求

如图 1-3 所示，要求客户端在不同 AP 间进行漫游。

2. 组网图

图1-3 WLAN 漫游典型配置组网图



3. 配置步骤

创建无线服务模板 **service**，配置 SSID 为 1，并使能服务模板。

```
<AC> system-view
[AC] wlan service-template service
[AC-wlan-st-service] ssid 1
[AC-wlan-st-service] service-template enable
[AC-wlan-st-service] quit
```

创建手工 AP，名称为 **ap1**，选择 AP 型号并配置序列号。

```
[AC] wlan ap ap1 model WA6320
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

将服务模板绑定到 **ap1** 的 Radio 接口。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] service-template service
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
```

创建手工 AP，名称为 **ap2**，选择 AP 型号并配置序列号。

```
[AC] wlan ap ap2 model WA6320
[AC-wlan-ap-ap2] serial-id 219801A28N819CE0003T
# 将无线服务模板绑定到 ap2 的 Radio 接口。
[AC-wlan-ap-ap2] radio 1
[AC-wlan-ap-ap2-radio-1] radio enable
[AC-wlan-ap-ap2-radio-1] service-template service
[AC-wlan-ap-ap2-radio-1] quit
[AC-wlan-ap-ap2] quit
```

4. 验证配置

- (1) 客户端在 AP 1 初次上线后，在 AC 上查看客户端的漫游信息。

通过 **display wlan client** 命令可以查看到客户端关联的 AP 为 AP 1，漫游状态为初始上线。

```
[AC] display wlan client verbose
Total number of clients: 1
```

```
MAC address           : 9cd3-6d9e-6778
IPv4 address           : 10.1.1.114
IPv6 address           : N/A
Username               : N/A
AID                    : 1
AP ID                  : 1
AP name                : ap1
Radio ID               : 1
Channel                : 36
SSID                   : 1
BSSID                  : 000f-e200-4444
VLAN ID                : 1
VLAN ID2               : N/A
Sleep count           : 242
Wireless mode          : 802.11ac
Channel bandwidth      : 80MHz
SM power save          : Enabled
SM power save mode     : Dynamic
Short GI for 20MHz     : Supported
Short GI for 40MHz     : Supported
Short GI for 80MHz     : Supported
Short GI for 160/80+80MHz : Not supported
STBC RX capability     : Not supported
STBC TX capability     : Not supported
LDPC RX capability     : Not supported
SU beamformee capability : Not supported
MU beamformee capability : Not supported
Beamformee STS capability : N/A
Block Ack              : TID 0 In
Supported VHT-MCS set  : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8
                        : NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8
Supported HT MCS set   : 0, 1, 2, 3, 4, 5, 6, 7,
```

```

8, 9, 10, 11, 12, 13, 14,
15, 16, 17, 18, 19, 20,
21, 22, 23
Supported rates      : 6, 9, 12, 18, 24, 36,
                     48, 54 Mbps
QoS mode             : WMM
Listen interval      : 10
RSSI                 : 62
Rx/Tx rate           : 130/11
Authentication method : Open system
Security mode         : PRE-RSNA
AKM mode              : Not configured
Cipher suite         : N/A
User authentication mode : Bypass
Authorization ACL ID   : 3001(Not effective)
Authorization user profile : N/A
Roam status           : N/A
Key derivation         : SHA1
PMF status            : Enabled
Forward policy name    : Not configured
Online time           : 0days 0hours 1minutes 13seconds
FT status             : Inactive

```

通过 **display wlan mobility roam-track mac-address** 可以查看到客户端的漫游跟踪信息。

```
[AC] display wlan mobility roam-track mac-address 9cd3-6d9e-6778
```

```
Total entries : 1
```

```
Current entries: 1
```

BSSID	Created at	Online time	AC IP address	RID	AP name
000f-e200-4444	2016-06-14 11:12:28	00hr 01min 16sec	127.0.0.1	1	ap1

- (2) 客户端漫游到 AP 2 后，在 AC 上查看客户端的漫游信息。

通过 **display wlan client** 可以查看到客户端关联的 AP 变成 AP 2，漫游状态为 AC 内漫游。

```
[AC] display wlan client verbose
```

```
Total number of clients: 1
```

```

MAC address          : 9cd3-6d9e-6778
IPv4 address          : 10.1.1.114
IPv6 address          : N/A
Username              : N/A
AID                   : 1
AP ID                 : 2
AP name               : ap2
Radio ID              : 1
SSID                  : 1
BSSID                 : 000f-e203-7777
VLAN ID               : 1
VLAN ID2              : N/A

```

```

Sleep count                : 242
Wireless mode              : 802.11ac
Channel bandwidth          : 80MHz
SM power save              : Enabled
SM power save mode         : Dynamic
Short GI for 20MHz         : Supported
Short GI for 40MHz         : Supported
Short GI for 80MHz         : Supported
Short GI for 160/80+80MHz  : Not supported
STBC RX capability         : Not supported
STBC TX capability         : Not supported
LDPC RX capability         : Not supported
SU beamformee capability   : Not supported
MU beamformee capability   : Not supported
Beamformee STS capability  : N/A
Block Ack                  : TID 0 In
Supported VHT-MCS set      : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8
                           NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8
Supported HT MCS set       : 0, 1, 2, 3, 4, 5, 6, 7,
                           8, 9, 10, 11, 12, 13, 14,
                           15, 16, 17, 18, 19, 20,
                           21, 22, 23
Supported rates             : 6, 9, 12, 18, 24, 36,
                           48, 54 Mbps
QoS mode                   : WMM
Listen interval            : 10
RSSI                       : 62
Rx/Tx rate                 : 130/11
Authentication method      : Open system
Security mode              : PRE-RSNA
AKM mode                   : Not configured
Cipher suite               : N/A
User authentication mode    : Bypass
Authorization ACL ID        : 3001(Not effective)
Authorization user profile  : N/A
Roam status                : Intra-AC roam
Key derivation              : SHA1
PMF status                 : Enabled
Forward policy name        : Not configured
Online time                : 0days 0hours 5minutes 13seconds
FT status                  : Inactive

```

通过 **display wlan mobility roam-track mac-address** 可以查看到漫游跟踪信息
增添了客户端漫游到 AP 2 的漫游轨迹。

```
[AC] display wlan mobility roam-track mac-address 9cd3-6d9e-6778
```

```
Total entries : 2
```

```
Current entries: 2
```

BSSID	Created at	Online time	AC IP address	RID	AP name
000f-e203-7777	2016-06-14 11:12:28	00hr 01min 02sec	127.0.0.1	1	ap2

000f-e200-4444 2016-06-14 11:12:04 00hr 03min 51sec 127.0.0.1 1 apl

2 漫游增强技术

WLAN 漫游增强技术目前包括以下几种：

- **802.1X 快速漫游：**当客户端认证方式为 RSN+802.1X 认证，可以进行 802.1X 快速漫游，客户端不需要再次认证即可完成漫游上线。
- **MAC 快速漫游：**当客户端认证方式为 MAC 地址认证时，可以进行 MAC 快速漫游，客户端不需要再次认证即可完成漫游上线。
- **802.11r：**用来缩短无线客户端在漫游过程中的时间延迟，从而降低无线客户端连接中断率，提高漫游服务质量。
- **802.11v：**用来辅助 802.11v 客户端接入更合适的 AP，提高 802.11v 无线客户端的漫游服务质量。
- **虚拟 BSS 漫游：**AC 通过实时监控无线客户端信号强度，使客户端接入服务质量更好的 AP，实现客户端在一个 ESS（Extended Service Set，拓展服务集）区域中的无缝漫游。
- **协同漫游：**结合 IEEE802.11k、IEEE802.11r 和 IEEE802.11v 协议实现无线客户端在一个 ESS 区域中的无缝漫游。

2.1 802.1X快速漫游

2.1.1 802.1X 快速漫游工作机制

如图 2-1 所示，802.1X 快速漫游机制的具体过程如下。

- (1) 客户端在 AP 1 上通过 802.1X 认证初始上线，在 AC 上会创建该客户端的漫游表项。有关 802.1X 认证的详细介绍，请参见“用户接入与认证配置指导”中的“WLAN 用户接入认证”。
- (2) 客户端漫游到 AP 2，AC 查找该客户端的漫游表项，当客户端认证方式为 RSN+802.1X 认证，且客户端携带的 PMKID 和设备缓存的 PMKID 检验一致时，就认为客户端已经进行过 802.1X 认证，直接跳过认证过程，利用缓存的 PMK 进行密钥协商以及后续的漫游上线。



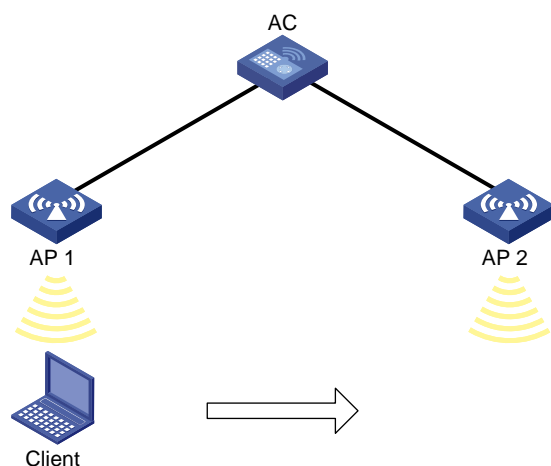
说明

设备支持以下两种方式缓存 PMKID：

- **SKC 方式（Sticky Key Caching，粘滞密钥缓存）：**直接缓存无线客户端在 802.1X 认证过程中产生的 PMKID。
- **OKC 方式（Opportunistic Key Caching，机会密钥缓存）：**使用无线客户端当前进行关联的 BSSID 以及客户端 MAC 地址、设备缓存的 PMK 等重新计算出 PMKID。

无论是 SKC 方式还是 OKC 方式，均不需要配置，即可完成 802.1X 快速漫游。

图2-1 802.1X 快速漫游示意图



2.1.2 802.1X 快速漫游配置限制和指导

802.1X 快速漫游功能目前支持同一 AC 内的漫游组网方式和漫游组。

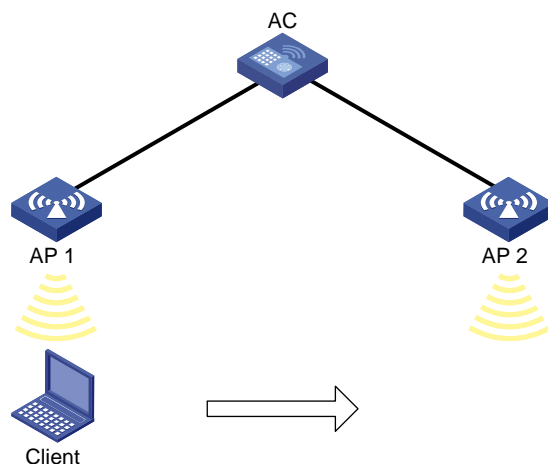
2.2 MAC快速漫游

2.2.1 MAC 快速漫游工作机制

如[图 2-2](#)所示，MAC 快速漫游机制的具体过程如下。

- (1) 客户端在 AP 1 上通过 MAC 地址认证初始上线，在 AC 上会创建该客户端的漫游表项。有关 MAC 地址认证的详细介绍，请参见“用户接入与认证配置指导”中的“WLAN 用户接入认证”。
- (2) 客户端漫游到 AP 2，AC 查找该客户端的漫游表项，当客户端认证方式为 MAC 认证，且开启 MAC 地址认证成功后的快速连接功能后，就认为客户端已经进行过 MAC 认证，直接跳过认证过程，继续后续的漫游上线。

图2-2 MAC 快速漫游示意图



2.2.2 MAC 快速漫游配置限制和指导

MAC 快速漫游功能目前仅支持同一 AC 内的漫游组网方式。

2.2.3 配置 MAC 地址认证成功后的快速连接功能

1. 功能简介

开启 MAC 地址认证成功后的快速连接功能后，已经通过 MAC 地址认证的客户端在 AC 内漫游时，不需要再次进行 MAC 地址认证，可提高客户端 AC 内漫游的上线速度。

2. 配置限制和指导

对于进行 AC 间漫游的 MAC 地址认证的客户端，配置本命令后，客户端可以继承漫游 VLAN，但是漫游状态显示为 N/A。当 AC 间漫游的客户端所属 VLAN 不同时，同一漫游组内的 AC 上行接口需要允许 MAC 地址认证的客户端 VLAN 通过。

本功能仅对在 AC 上进行认证和关联的无线客户端生效。

该命令只能在无线服务模板处于关闭状态时配置。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入无线服务模板视图。

```
wlan service-template service-template-name
```

- (3) 开启 MAC 地址认证成功后的快速连接功能。

```
mac-authentication fast-connect enable
```

缺省情况下，MAC 地址认证成功后的快速连接功能处于开启状态。

2.3 802.11r

2.3.1 802.11r 简介

802.11r 的核心功能是 FT（Fast BSS Transition，快速 BSS 切换），它主要用来减少客户端在漫游过程中的时间延迟，从而降低连接中断概率、提高漫游服务质量。

FT 支持两种实现方式：

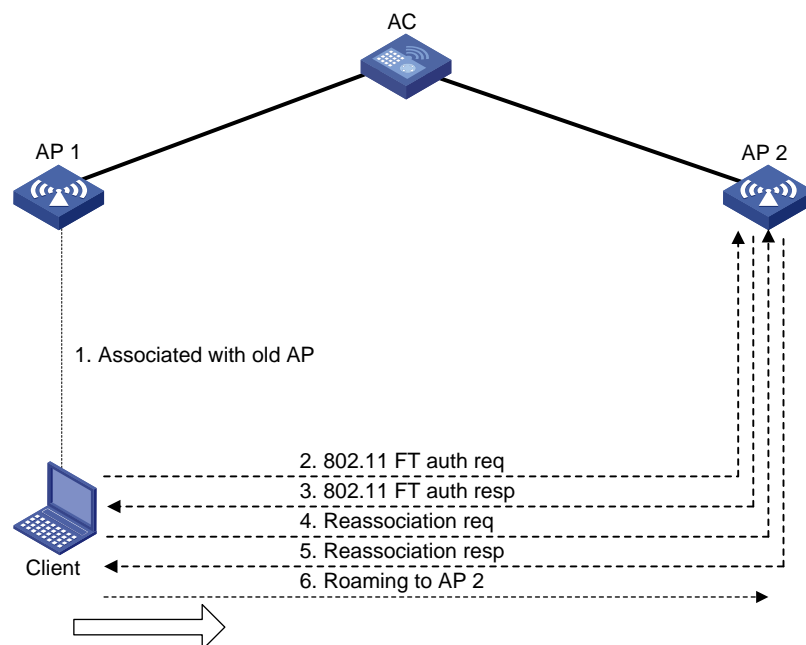
- **Over-the-Air:** 客户端直接与目标 AP 通信，进行漫游前的认证，适用于对漫游兼容性要求高的场景。建议采用本方式配置 FT 功能。
- **Over-the-DS:** 客户端通过当前 AP 与目标 AP 通信，进行漫游前的认证，适用于对漫游性能要求高的场景。

1. AC 内 Over-the-Air 方式漫游

如图 2-3 所示，客户端在 AP 间（AP 1 到 AP 2）漫游时，信息交互过程如下：

- (1) 客户端已经与 AP 1 连接并且要漫游到 AP 2；
- (2) 客户端向 AP 2 发送认证请求；
- (3) 客户端收到 AP 2 的认证请求回应；
- (4) 客户端向 AP 2 发送重关联请求；
- (5) 客户端收到 AP 2 的重关联请求回应；
- (6) 客户端完成从 AP 1 到 AP 2 的漫游。

图2-3 Over-the-Air 方式漫游示意图



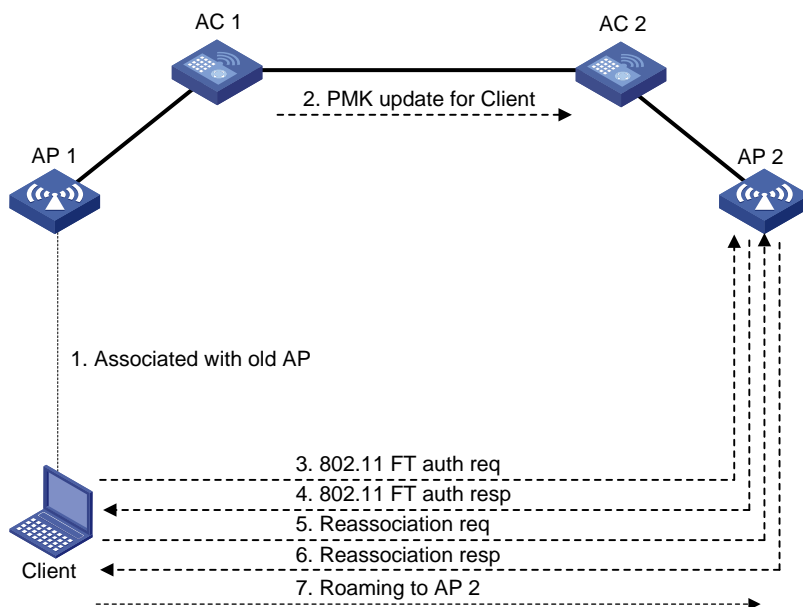
2. AC 间 Over-the-Air 方式漫游

如图 2-4 所示，AP 1 和 AP 2 分别连接 AC 1 和 AC 2，在同一移动域内漫游的信息交互过程如下：

- (1) 客户端与 AP 1 建立连接；

- (2) AC 1 同步客户端漫游信息（PMK、VLAN 等信息）到 AC 2；
- (3) 客户端准备漫游，发送 FT 认证请求到 AP 2；
- (4) 客户端收到 AP 2 发送的 FT 认证回复；
- (5) 客户端向 AP 2 发送重关联请求；
- (6) 客户端收到 AP 2 的重关联请求回应；
- (7) 客户端完成从 AP 1 到 AP 2 的漫游。

图2-4 AC 间 Over-the-Air 方式漫游示意图

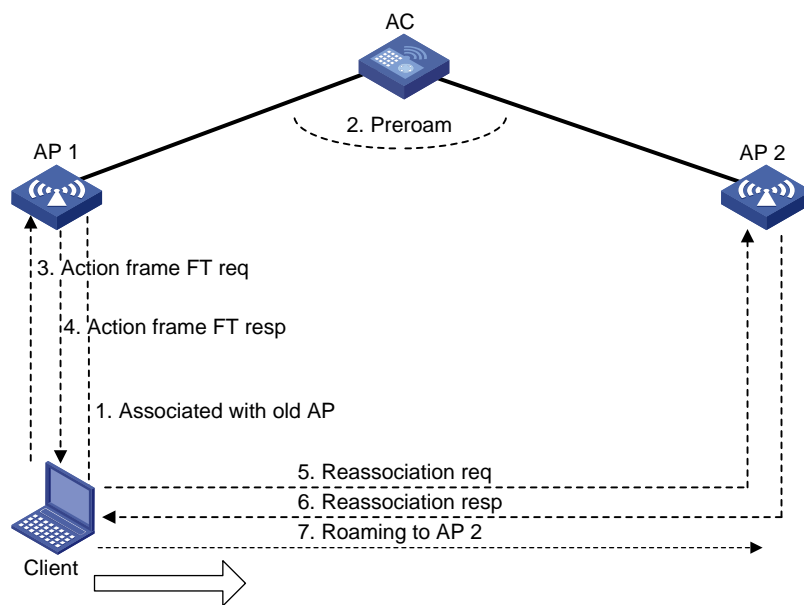


3. AC 内 Over-the-Ds 方式漫游

如图 2-5 所示，客户端在 AP 间（AP 1 到 AP 2）漫游时，信息交互过程如下：

- (1) 客户端与 AP 1 建立连接；
- (2) AC 生成、同步、保存客户端的漫游表项；
- (3) 客户端准备漫游，向 AP 1 发送 FT 认证请求；
- (4) 客户端收到 AP 1 的 FT 认证回复；
- (5) 客户端向 AP 2 发送重关联请求；
- (6) 客户端收到 AP 2 的重关联请求回应；
- (7) 客户端完成从 AP 1 到 AP 2 的漫游。

图2-5 Over-the-Ds 方式漫游示意图



2.3.2 802.11r 配置限制和指导

配置 802.11r 的 FT 功能，需要注意的是：

- 如果有客户端无法关联使能了 FT 功能的服务，可能是由于客户端的型号较早而不支持 FT 协议。此时可以创建两个 SSID 相同的服务，一个使能 FT 功能，另一个不使能 FT 功能，而其它配置均相同，以便客户端可以正常使用网络服务。
- 不建议在服务模板下同时开启 FT 功能和 802.1X 周期性重认证功能，否则会导致客户端在每次重认证时间间隔到达时重新上线。关于 802.1X 周期性重认证功能的介绍和配置请参见“用户接入与认证配置指导”中的“WLAN 用户接入认证”。
- 快速 BSS 切换协商成功的客户端，不支持 PTK 更新。关于 PTK 更新的介绍和配置请参见“WLAN 安全配置指导”中的“WLAN 用户安全”。
- 未配置身份认证与密钥管理模式时，不支持开启 FT 功能。
- 802.11r 功能需配置 AP 发送信标和探查响应帧时携带 RSN IE，认证方式不为本地认证、加密套件为 CCMP 时生效。
- 802.11r 功能仅对关联位置在 AC 上的无线客户端生效。
- 802.11r 功能仅能在服务模板未使能的情况下进行配置。
- 请不要同时开启 FT 功能、WPA3 安全模式或增强开放系统认证服务，否则会导致无线服务模板使能失败。WPA3 安全模式和增强开发系统认证服务的详细信息请参见“WLAN 安全配置指导”中的“WLAN 用户安全”。
- Over-the-Ds 方式目前支持同一 AC 内的漫游组网方式。

2.3.3 配置 802.11r

- (1) 进入系统视图。

system-view

- (2) 配置无线服务模板。

wlan service-template *service-template-name*

- (3) 开启 FT 功能。

ft enable

缺省情况下，FT 功能处于关闭状态。

- (4) （可选）配置 FT 方式。

ft method { **over-the-air** | **over-the-ds** }

缺省情况下，FT 方式为 over-the-air。

- (5) （可选）配置重关联超时时间。

ft reassociation-timeout *timeout*

缺省情况下，重关联超时时间为 20 秒。

重关联超时时间指的是，客户端在完成认证后，客户端发起重关联请求的最大时间间隔。如果在此时间内客户端没有发起重关联，则会终止此次漫游。

- (6) （可选）配置设备的漫游域 ID

ft mobility-domain-id *mobility-domain-id*

缺省情况下，未配置漫游域 ID。

本功能用于减少跨设备接入的客户端的接入时间。在设备上配置漫游域 ID，漫游域 ID 相同的设备允许通过 FT 的方式跨设备漫游，漫游域 ID 不同的设备不允许通过 FT 的方式跨设备漫游。

本功能只能在服务模板未使能的情况下进行配置，并且只有开启了 FT 功能才生效。

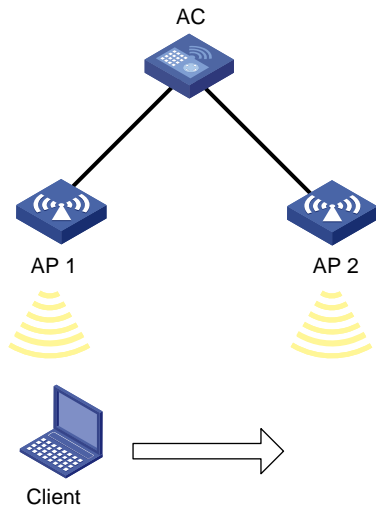
2.3.4 FT Over-the-DS 方式 802.11r 典型配置举例（PSK 模式）

1. 组网需求

如[图 2-6](#)所示，客户端在不同 AP 间进行漫游，使用 Over-the-DS 方式，通过 PSK 模式对客户端进行身份认证与密钥管理。

2. 组网图

图2-6 FT Over-the-DS 方式 PSK 身份认证与密钥管理模式配置组网图



3. 配置步骤

创建无线服务模板 **acstname**。

```
<AC> system-view
[AC] wlan service-template acstname
```

配置无线服务的 SSID 为 **service**。

```
[AC-wlan-st-acstname] ssid service
```

配置身份认证与密钥管理的模式是 **PSK** 模式，配置使用明文字符串 **12345678** 作为 **PSK** 密钥。

```
[AC-wlan-st-acstname] akm mode psk
[AC-wlan-st-acstname] preshared-key pass-phrase simple 12345678
```

配置 **AES-CCMP** 加密套件，配置在 **AP** 发送信标和探查响应帧时携带 **RSN IE**。

```
[AC-wlan-st-acstname] cipher-suite ccmp
[AC-wlan-st-acstname] security-ie rsn
```

开启 **FT** 功能。

```
[AC-wlan-st-acstname] ft enable
```

配置重关联超时时间为 **50** 秒。

```
[AC-wlan-st-acstname] ft reassociation-timeout 50
```

配置 **FT** 方式为 **Over-the-DS**。

```
[AC-wlan-st-acstname] ft method over-the-ds
```

使能无线服务。

```
[AC-wlan-st-acstname] service-template enable
[AC-wlan-st-acstname] quit
```

创建 **AP**，名称为 **1**，并将无线服务模板 **acstname** 绑定到 **AP 1** 的 **Radio1** 上。

```
[AC] wlan ap 1 model WA6320
[AC-wlan-ap-1] serial-id 219801A28N819CE0002T
[AC-wlan-ap-1] radio 1
[AC-wlan-ap-1-radio-1] service-template acstname
```

```
[AC-wlan-ap-1-radio-1] radio enable
[AC-wlan-ap-1-radio-1] quit
[AC-wlan-ap-1] quit
```

创建 AP，名称为 2，并将无线服务模板 acstname 绑定到 AP 2 的 Radio1 上。

```
[AC] wlan ap 2 model WA6320
[AC-wlan-ap-2] serial-id 219801A28N819CE0007T
[AC-wlan-ap-2] radio 1
[AC-wlan-ap-2-radio-1] service-template acstname
[AC-wlan-ap-2-radio-1] radio enable
[AC-wlan-ap-2-radio-1] quit
[AC-wlan-ap-2] quit
```

4. 验证配置

在 AC 上通过 **display wlan service-template** 命令可以查看服务模板的配置情况。

```
[AC] display wlan service-template acstname verbose
Service template name           : acstname
Description                     : Not configured
SSID                           : service
SSID-hide                      : Disabled
User-isolation                  : Disabled
Service template status        : Enabled
Maximum clients per BSS        : Not configured
Frame format                    : Dot3
Seamless-roam status           : Disabled
Seamless-roam RSSI threshold   : 50
Seamless-roam RSSI gap         : 20
VLAN ID                        : 1
Service VLAN ID                 : N/A
Service VLAN TPID               : dot1q
AKM mode                       : PSK
Security IE                     : RSN
Cipher suite                    : CCMP
TKIP countermeasure time       : 0 sec
PTK lifetime                    : 43200 sec
PTK rekey                      : Enabled
GTK rekey                      : Enabled
GTK rekey method               : Time-based
GTK rekey time                 : 86400 sec
GTK rekey client-offline       : Disabled
WPA3 status                    : Disabled
PPSK                           : Disabled
PPSK Fail Permit               : Disabled
Enhance-open status            : Disabled
Enhanced-open transition-mode service-template : N/A
User authentication mode        : Bypass
Intrusion protection           : Disabled
Intrusion protection mode      : Temporary-block
Temporary block time           : 180 sec
```

Temporary service stop time	: 20 sec
Fail VLAN ID	: Not configured
802.1X handshake	: Disabled
802.1X handshake secure	: Disabled
802.1X domain	: Not configured
MAC-auth domain	: Not configured
Max 802.1X users per BSS	: 4096
Max MAC-auth users per BSS	: 4096
802.1X re-authenticate	: Disabled
Authorization fail mode	: Online
Accounting fail mode	: Online
Authorization	: Permitted
Key derivation	: SHA1
PMF status	: Disabled
Hotspot policy number	: Not configured
Forwarding policy status	: Disabled
Forwarding policy name	: Not configured
Forwarder	: AC
FT Status	: Enable
FT Method	: over-the-ds
FT Reassociation Deadline	: 50 sec
QoS trust	: Port
QoS priority	: 0
QoS U-APSD mode	: 1
BTM status	: Disabled

客户端上线后，在 AC 上通过 **display wlan client verbose** 命令可以查看客户端的详细信息。

```
[AC] display wlan client verbose
Total number of clients: 1
```

MAC address	: fc25-3f03-8361
IPv4 address	: 10.1.1.114
IPv6 address	: N/A
Username	: N/A
AID	: 1
AP ID	: 1
AP name	: 1
Radio ID	: 1
Channel	: 36
SSID	: service
BSSID	: 000f-e266-7788
VLAN ID	: 1
VLAN ID2	: N/A
Sleep count	: 242
Wireless mode	: 802.11ac
Channel bandwidth	: 80MHz
SM power save	: Enabled
SM power save mode	: Dynamic

```

Short GI for 20MHz           : Supported
Short GI for 40MHz           : Supported
Short GI for 80MHz           : Supported
Short GI for 160/80+80MHz    : Not supported
STBC RX capability           : Not supported
STBC TX capability           : Not supported
LDPC RX capability           : Not supported
SU beamformee capability     : Not supported
MU beamformee capability     : Not supported
Beamformee STS capability    : N/A
Block Ack                    : TID 0 In
Supported VHT-MCS set        : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8
                               NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8
Supported HT MCS set         : 0, 1, 2, 3, 4, 5, 6, 7,
                               8, 9, 10, 11, 12, 13, 14,
                               15, 16, 17, 18, 19, 20,
                               21, 22, 23
Supported rates               : 6, 9, 12, 18, 24, 36,
                               48, 54 Mbps
QoS mode                     : WMM
Listen interval               : 10
RSSI                          : 62
Rx/Tx rate                   : 130/11
Authentication method         : Open system
Security mode                 : RSN
AKM mode                     : PSK
Encryption cipher             : CCMP
User authentication mode      : Bypass
Authorization ACL ID          : 3001(Not effective)
Authorization user profile    : N/A
Roam status                   : N/A
Key derivation                 : SHA1
PMF status                    : Enabled
Forward policy name           : Not configured
Online time                   : 0days 0hours 1minutes 13seconds
FT status                     : Active

```

客户端漫游成功后，在 AC 上通过 **display wlan client verbose** 命令，可以看到结果如下。

```

[AC] display wlan client verbose
Total number of clients: 1

```

```

MAC address                   : fc25-3f03-8361
IPv4 address                  : 10.1.1.114
IPv6 address                  : N/A
Username                      : N/A
AID                           : 1
AP ID                         : 2
AP name                       : 2

```

Radio ID	: 1
Channel	: 36
SSID	: service
BSSID	: 000f-e211-2233
VLAN ID	: 1
VLAN ID2	: N/A
Sleep count	: 242
Wireless mode	: 802.11ac
Channel bandwidth	: 80MHz
SM power save	: Enabled
SM power save mode	: Dynamic
Short GI for 20MHz	: Supported
Short GI for 40MHz	: Supported
Short GI for 80MHz	: Supported
Short GI for 160/80+80MHz	: Not supported
STBC RX capability	: Not supported
STBC TX capability	: Not supported
LDPC RX capability	: Not supported
SU beamformee capability	: Not supported
MU beamformee capability	: Not supported
Beamformee STS capability	: N/A
Block Ack	: TID 0 In
Supported VHT-MCS set	: NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8 NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8
Supported HT MCS set	: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23
Supported rates	: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
QoS mode	: WMM
Listen interval	: 10
RSSI	: 62
Rx/Tx rate	: 130/11
Authentication method	: FT
Security mode	: RSN
AKM mode	: PSK
Encryption cipher	: CCMP
User authentication mode	: Bypass
Authorization ACL ID	: 3001(Not effective)
Authorization user profile	: N/A
Roam status	: Intra-AC roam
Key derivation	: SHA1
PMF status	: Enabled
Forward policy name	: Not configured
Online time	: 0days 0hours 5minutes 13seconds
FT status	: Active

2.3.5 FT Over-the-DS 方式 802.11r 典型模式配置举例（802.1X）

1. 组网需求

如图 2-6 所示，客户端在不同 AP 间进行漫游，使用 Over-the-DS 方式，通过 802.1X 模式对客户端进行身份认证与密钥管理。

2. 配置步骤

创建无线服务模板 stname。

```
<AC> system-view
[AC] wlan service-template stname
```

配置无线服务的 SSID 为 service。

```
[AC-wlan-st-stname] ssid service
```

配置身份认证与密钥管理的模式是 802.1X 模式。

```
[AC-wlan-st-stname] akm mode dot1x
```

配置 AES-CCMP 加密套件，配置在 AP 发送信标和探查响应帧时携带 RSN IE。

```
[AC-wlan-st-stname] cipher-suite ccmp
[AC-wlan-st-stname] security-ie rsn
```

配置客户端安全认证方式为 802.1X。

```
[AC-wlan-st-stname] client-security authentication-mode dot1x
[AC-wlan-st-stname] dot1x domain imc
```

开启 FT 功能。

```
[AC-wlan-st-stname] ft enable
```

配置 FT 方法为 Over-the-DS。

```
[AC-wlan-st-stname] ft method over-the-ds
```

使能无线服务。

```
[AC-wlan-st-stname] service-template enable
[AC-wlan-st-stname] quit
```

配置 802.1X 认证方式为 EAP。

```
[AC] dot1x authentication-method eap
```

创建 RADIUS 方案 imcc。配置主认证服务器的 IP 地址为 10.1.1.3，与认证服务器交互报文时的共享密钥为明文 12345678。配置主计费服务器的 IP 地址为 10.1.1.3，与计费服务器交互报文时的共享密钥为明文 12345678。配置发送给 RADIUS 服务器的用户名不带 ISP 域名。

```
[AC] radius scheme imcc
[AC-radius-imcc] primary authentication 10.1.1.3
[AC-radius-imcc] primary accounting 10.1.1.3
[AC-radius-imcc] key authentication simple 12345678
[AC-radius-imcc] key accounting simple 12345678
[AC-radius-imcc] user-name-format without-domain
[AC-radius-imcc] quit
```

创建认证域并配置使用 RADIUS 方案进行认证、授权、计费。

```
[AC] domain imc
[AC-isp-imc] authentication lan-access radius-scheme imcc
[AC-isp-imc] authorization lan-access radius-scheme imcc
[AC-isp-imc] accounting lan-access radius-scheme imcc
[AC-isp-imc] quit
```

创建 AP，名称为 1，并将无线服务模板 acstname 绑定到 AP 1 的 Radio1 上。

```
[AC] wlan ap 1 model WA6320
[AC-wlan-ap-1] serial-id 219801A28N819CE0002T
[AC-wlan-ap-1] radio 1
[AC-wlan-ap-1-radio-1] service-template acstname
[AC-wlan-ap-1-radio-1] radio enable
[AC-wlan-ap-1-radio-1] quit
[AC-wlan-ap-1] quit
```

创建 AP，名称为 2，并将无线服务模板 acstname 绑定到 AP 2 的 Radio1 上。

```
[AC] wlan ap 2 model WA6320
[AC-wlan-ap-2] serial-id 219801A28N819CE0007T
[AC-wlan-ap-2] radio 1
[AC-wlan-ap-2-radio-1] service-template acstname
[AC-wlan-ap-2-radio-1] radio enable
[AC-wlan-ap-2-radio-1] quit
[AC-wlan-ap-2] quit
```

3. 验证配置

在 AC 上通过 **display wlan service-template** 命令可以查看服务模板的配置情况。

```
[AC] display wlan service-template stname verbose
Service template name           : stname
Description                     : Not configured
SSID                           : service
SSID-hide                      : Disabled
User-isolation                 : Disabled
Service template status        : Enabled
Maximum clients per BSS        : Not configured
Frame format                   : Dot3
Seamless-roam status          : Disabled
Seamless-roam RSSI threshold   : 50
Seamless-roam RSSI gap        : 20
VLAN ID                        : 1
Service VLAN ID                : N/A
Service VLAN TPID              : dot1q
AKM mode                       : 802.1X
Security IE                    : RSN
Cipher suite                   : CCMP
TKIP countermeasure time       : 0 sec
PTK lifetime                   : 43200 sec
PTK rekey                      : Enabled
GTK rekey                     : Enabled
GTK rekey method               : Time-based
GTK rekey time                 : 86400 sec
GTK rekey client-offline       : Disabled
WPA3 status                    : Disabled
PPSK                          : Disabled
PPSK Fail Permit               : Disabled
Enhance-open status            : Disabled
```

```

Enhanced-open transition-mode service-template : N/A
User authentication mode : 802.1X
Intrusion protection : Disabled
Intrusion protection mode : Temporary-block
Temporary block time : 180 sec
Temporary service stop time : 20 sec
Fail VLAN ID : Not configured
802.1X handshake : Disabled
802.1X handshake secure : Disabled
802.1X domain : imc
MAC-auth domain : Not configured
Max 802.1X users per BSS : 4096
Max MAC-auth users per BSS : 4096
802.1X re-authenticate : Disabled
Authorization fail mode : Online
Accounting fail mode : Online
Authorization : Permitted
Key derivation : SHA1
PMF status : Disabled
Hotspot policy number : Not configured
Forwarding policy status : Disabled
Forwarding policy name : Not configured
Forwarder : AC
FT Status : Enable
FT Method : over-the-ds
FT Reassociation Deadline : 20 sec
QoS trust : Port
QoS priority : 0
QoS U-APSD mode : 1
BTM status : Disabled

```

客户端上线后，在 AC 上通过 **display wlan client verbose** 命令可以看到结果如下。

```

[AC] display wlan client verbose
Total number of clients: 1

```

```

MAC address : fc25-3f03-8361
IPv4 address : 10.1.1.114
IPv6 address : N/A
Username : N/A
AID : 1
AP ID : 1
AP name : 1
Radio ID : 1
Channel : 36
SSID : service
BSSID : 000f-e266-7788
VLAN ID : 1
VLAN ID2 : N/A
Sleep count : 242

```



```

Wireless mode                : 802.11ac
Channel bandwidth             : 80MHz
SM power save                 : Enabled
SM power save mode           : Dynamic
Short GI for 20MHz            : Supported
Short GI for 40MHz           : Supported
Short GI for 80MHz           : Supported
Short GI for 160/80+80MHz     : Not supported
STBC RX capability           : Not supported
STBC TX capability           : Not supported
LDPC RX capability           : Not supported
SU beamformee capability     : Not supported
MU beamformee capability     : Not supported
Beamformee STS capability    : N/A
Block Ack                    : TID 0 In
Supported VHT-MCS set        : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8
                               NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8
Supported HT MCS set         : 0, 1, 2, 3, 4, 5, 6, 7,
                               8, 9, 10, 11, 12, 13, 14,
                               15, 16, 17, 18, 19, 20,
                               21, 22, 23
Supported rates               : 6, 9, 12, 18, 24, 36,
                               48, 54 Mbps
QoS mode                     : WMM
Listen interval               : 10
RSSI                          : 62
Rx/Tx rate                   : 130/11
Authentication method         : Open system
Security mode                 : RSN
AKM mode                     : 802.1X
Encryption cipher             : CCMP
User authentication mode      : 802.1X
Authorization ACL ID          : 3001(Not effective)
Authorization user profile    : N/A
Roam status                   : N/A
Key derivation                 : SHA1
PMF status                    : Enabled
Forward policy name           : Not configured
Online time                   : 0days 0hours 1minutes 13seconds
FT status                     : Active

```

客户端漫游成功后，在 AC 上通过 **display wlan client verbose** 命令可以看到结果如下。

```

[AC] display wlan client verbose
Total number of clients: 1

```

```

MAC address                  : fc25-3f03-8361
IPv4 address                  : 10.1.1.114
IPv6 address                  : N/A
Username                      : N/A

```

AID	: 1
AP ID	: 2
AP name	: 2
Radio ID	: 1
Channel	: 36
SSID	: service
BSSID	: 000f-e211-2233
VLAN ID	: 1
VLAN ID2	: N/A
Sleep count	: 242
Wireless mode	: 802.11ac
Channel bandwidth	: 80MHz
SM power save	: Enabled
SM power save mode	: Dynamic
Short GI for 20MHz	: Supported
Short GI for 40MHz	: Supported
Short GI for 80MHz	: Supported
Short GI for 160/80+80MHz	: Not supported
STBC RX capability	: Not supported
STBC TX capability	: Not supported
LDPC RX capability	: Not supported
SU beamformee capability	: Not supported
MU beamformee capability	: Not supported
Beamformee STS capability	: N/A
Block Ack	: TID 0 In
Supported VHT-MCS set	: NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8 NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8
Supported HT MCS set	: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23
Supported rates	: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
QoS mode	: WMM
Listen interval	: 10
RSSI	: 62
Rx/Tx rate	: 130/11
Authentication method	: FT
Security mode	: RSN
AKM mode	: 802.1X
Encryption cipher	: CCMP
User authentication mode	: 802.1X
Authorization ACL ID	: 3001(Not effective)
Authorization user profile	: N/A
Roam status	: Intra-AC roam
Key derivation	: SHA1
PMF status	: Enabled
Forward policy name	: Not configured

Online time : 0days 0hours 5minutes 13seconds
FT status : Active

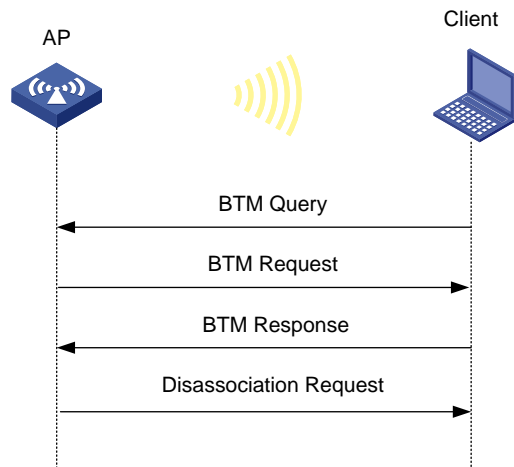
2.4 802.11v

2.4.1 802.11v 简介

802.11v 的核心功能是 BTM (BSS Transition Management, BSS 切换管理), 它主要用来通知 802.11v 无线客户端离开当前 BSS, 接入更合适的 AP, 从而提高 802.11v 无线客户端的接入质量。如图 2-7 所示, BSS 切换管理的基本流程如下:

- (1) 802.11v 无线客户端 RSSI 值过低或找到一个更合适的 AP 时, 会主动向 AP 发送 BSS 切换查询, 请求连接到其它 BSS 上。AP 接收到客户端的 BSS 切换查询后, 会向其发送 BSS 切换请求。
- (2) 802.11v 无线客户端接收到 BSS 切换请求后, 有可能向 AP 发送切换响应, 通知 AP BSS 切换的结果。
- (3) 经过一段时间后, 若无线客户端还未离开当前 BSS, AP 会主动向无线客户端发送解除关联请求, 强制无线客户端下线。

图2-7 BSS 切换管理



2.4.2 802.11v 配置限制和指导

802.11v 功能目前仅支持同一 AC 内的漫游组网方式。

2.4.3 开启 BSS 切换管理功能

1. 配置限制和指导

本功能只能在无线服务模板处于关闭状态时配置。

建议开启 BSS 切换管理功能的同时, 通过 `bss transition-management disassociation` 命令配置 BSS 切换解除关联时间, 否则某些客户端可能无法进行 BSS 切换。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入无线服务模板视图。

```
wlan service-template service-template-name
```

- (3) 开启 BSS 切换管理功能。

```
bss transition-management enable
```

缺省情况下，BSS 切换管理功能处于关闭状态。

2.4.4 配置 BSS 切换解除关联功能

1. 功能简介

配置 BSS 切换解除关联功能后，当设备收到无线客户端发送的 BSS 切换查询时，会向无线客户端发出请求切换 BSS，引导客户端进行 BSS 切换。

若配置了强制客户端进行 BSS 切换，则当超过配置的 BSS 切换解除关联时间客户端还未离开时，设备会强制断开与客户端的连接，请谨慎使用该功能。

2. 配置限制和指导

只有开启了 BSS 切换管理功能，BSS 切换解除关联功能才能生效。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入无线服务模板视图。

```
wlan service-template service-template-name
```

- (3) 配置 BSS 切换解除关联功能。

```
bss transition-management disassociation { forced | recommended }  
[ timer time ]
```

缺省情况下，BSS 切换解除关联功能处于开启状态，即设备会推荐客户端进行 BSS 切换，推荐解除关联时间为 90s。

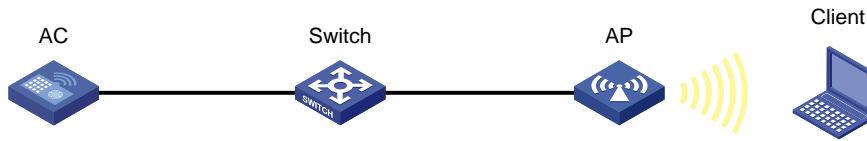
2.4.5 802.11v 典型配置举例

1. 组网需求

如图 2-8 所示，通过 BSS 切换管理功能，当 AP 发现 802.11v 无线客户端 RSSI 值过低时，会对客户端进行 BSS 切换管理引导，引导客户端去更合适的 AP 上线。

2. 组网图

图2-8 BSS 典型配置组网图



3. 配置步骤

创建无线服务模板 **service**。

```
<AC> system-view
[AC] wlan service-template service
```

配置无线服务的 SSID 为 **service**。

```
[AC-wlan-st-service] ssid service
```

开启 **BSS** 切换管理功能。

```
[AC-wlan-st-service] bss transition-management enable
```

配置切换解除关联时间为 **45** 秒。

```
[AC-wlan-st-service] bss transition-management disassociation recommended timer 45
```

使能无线服务。

```
[AC-wlan-st-service] service-template enable
[AC-wlan-st-service] quit
```

创建 **AP**，名称为 **ap1**，开启获取 **BSS** 候选列表功能并将无线服务模板 **service** 绑定到 **AP 1** 的 **Radio1** 上。

```
[AC] wlan ap ap1 model WA6320
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] sacp roam-optimize bss-candidate-list enable
[AC-wlan-ap-ap1-radio-1] service-template service
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
```

4. 验证配置

在 **AC** 上通过 **display wlan service-template** 命令可以查看 **BSS** 切换管理功能处于开启状态。

```
[AC] display wlan service-template service verbose
Service template name           : service
Description                     : Not configured
SSID                           : service
SSID-hide                      : Disabled
User-isolation                  : Disabled
Service template status        : Disabled
Maximum clients per BSS        : Not configured
Frame format                   : Dot3
Seamless roam status           : Disabled
```

Seamless roam RSSI threshold	: 50
Seamless roam RSSI gap	: 20
VLAN ID	: 1
Service VLAN ID	: N/A
Service VLAN TPID	: dot1q
AKM mode	: Not configured
Security IE	: Not configured
Cipher suite	: Not configured
TKIP countermeasure time	: 0 sec
PTK lifetime	: 43200 sec
PTK rekey	: Enabled
GTK rekey	: Enabled
GTK rekey method	: Time-based
GTK rekey time	: 86400 sec
GTK rekey client-offline	: Disabled
WPA3 status	: Disabled
PPSK	: Disabled
PPSK Fail Permit	: Enabled
Enhance-open status	: Disabled
Enhanced-open transition-mode service-template	: N/A
User authentication mode	: Bypass
Intrusion protection	: Disabled
Intrusion protection mode	: Temporary-block
Temporary block time	: 180 sec
Temporary service stop time	: 20 sec
Fail VLAN ID	: Not configured
802.1X handshake	: Disabled
802.1X handshake secure	: Disabled
802.1X domain	: Not configured
MAC-auth domain	: Not configured
Max 802.1X users per BSS	: 512
Max MAC-auth users per BSS	: 512
802.1X re-authenticate	: Disabled
Authorization fail mode	: Online
Accounting fail mode	: Online
Authorization	: Permitted
Key derivation	: SHA1
PMF status	: Disabled
Hotspot policy number	: Not configured
Forwarding policy status	: Disabled
Forwarding policy name	: Not configured
Forwarder	: AC
FT status	: Disabled
QoS trust	: Port
QoS priority	: 0
QoS U-APSD mode	: 1
BTM status	: Enabled

在 AC 上通过 **display wlan client** 命令可以查看客户端已经上线，经过 45 秒后，在查看客户端，发现已经被强制下线。

```
<AC> display wlan client
Total number of clients: 3
```

MAC address	Username	AP name	R IP address	VLAN
4581-61ac-885a	N/A	ap1	1 192.168.66.230	1

2.5 虚拟BSS漫游

2.5.1 虚拟 BSS 漫游简介

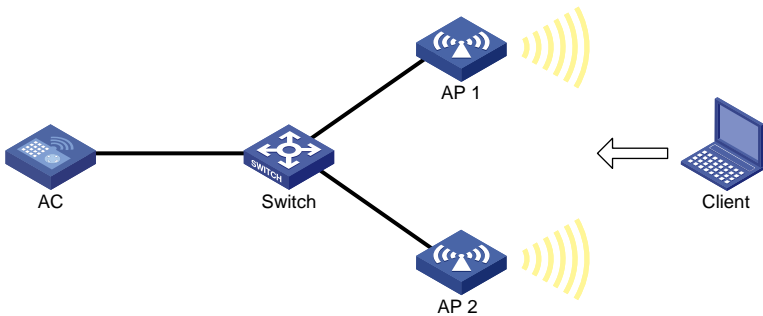
开启虚拟 BSS 漫游功能的多个 AP 为客户端提供统一的虚拟服务，客户端选择接入一个 AP 后，其余 AP 实时监控客户端的信号强度。当 AC 发现其它 AP 能够比当前 AP 提供更高质量的服务时，将指定新 AP 为客户端提供无线服务。

如图 2-9 所示，无线网络中存在两个 AP，虚拟 BSS 漫游的实现方式如下所述：

- (1) AP 上开启虚拟 BSS 漫游功能后，当网络中的 AP 收到来自客户端的 Probe Request 帧，AC 会为该客户端生成一个虚拟的服务，该虚拟服务的 BSSID 将由 AC 的桥 MAC 地址、AP ID 和客户端的 MAC 地址组成，AP 会用这个虚拟 BSSID 来与客户端进行交互。
- (2) 如果客户端选择通过 AP 1 上线，则 AC 会将 AP 1 的虚拟 BSSID 通告到 AP 2 上。AP 2 将替换本地的虚拟 BSSID，并监控该客户端的信号强度。
- (3) 当 AC 发现 AP 2 对客户端而言服务质量更好时，即 AP 2 接收到客户端报文的 RSSI(Received Signal Strength Indicator，接收信号强度指示) 值达到/超过 RSSI 门限值，并且与 AP 1 所接收到的客户端报文 RSSI 值的差值达到/超过 RSSI 差值门限，那么 AC 将指定 AP 2 为客户端提供无线服务。

由于客户端始终使用相同的虚拟 BSSID 发送数据，所以即使为客户端提供无线服务的 AP 发生变化，对客户端而言使用的无线服务却是相同的。

图2-9 虚拟 BSS 漫游示意图



2.5.2 虚拟 BSS 漫游与硬件适配关系

本特性的支持情况与设备型号有关，请以设备的实际情况为准。

产品系列	产品型号	产品代码	说明
WX1800H系列	WX1804H-PWR	EWP-WX1804H-PWR-CN	不支持
WX2500H系列	WX2508H-PWR-LTE WX2510H-PWR WX2510H-F-PWR WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	支持
MAK系列	MAK204 MAK206	EWP-MAK204 EWP-MAK206	支持
WX3000H系列	WX3010H WX3010H-X-PWR WX3010H-L-PWR WX3024H WX3024H-L-PWR WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	支持
WX3500H系列	WX3508H WX3508H WX3510H WX3510H WX3520H WX3520H-F WX3540H WX3540H	EWP-WX3508H EWP-WX3508H-F EWP-WX3510H EWP-WX3510H-F EWP-WX3520H EWP-WX3520H-F EWP-WX3540H EWP-WX3540H-F	支持
WX5500E系列	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	支持
WX5500H系列	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	支持
AC插卡系列	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	支持

产品系列	产品型号	产品代码	说明
WX1800H系列	WX1804H-PWR WX1810H-PWR WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	不支持

产品系列	产品型号	产品代码	说明
WX3800H系列	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	不支持
WX5800H系列	WX5860H	EWP-WX5860H-GL	不支持

2.5.3 虚拟 BSS 漫游配置限制和指导

仅部分 Wi-Fi 5 标准的产品支持虚拟 BSS 漫游功能。

2.5.4 配置虚拟 BSS 漫游

1. 功能简介

虚拟 BSS 漫游功能是针对无线服务模板的，对某个无线服务模板配置虚拟 BSS 漫游功能后，仅对接入该无线服务模板的客户端进行漫游，通过其它无线服务模板接入的客户端不受影响。

虚拟 BSS 漫游目前仅支持 AC 内漫游组网方式。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入服务模板视图。

```
wlan service-template service-template-name
```

- (3) 开启虚拟 BSS 漫游功能。

```
seamless-roaming enable
```

缺省情况下，虚拟 BSS 漫游功能处于关闭状态。

- (4) 配置虚拟 BSS 漫游 RSSI 门限和 RSSI 差值。

```
seamless-roaming switch rssi-threshold value [ rssi-gap gap-value ]
```

缺省情况下，虚拟 BSS 漫游 RSSI 门限值为 50，RSSI 差值门限为 20。

2.6 协同漫游

2.6.1 协同漫游简介

协同漫游是我司研发的结合 IEEE802.11k、IEEE802.11r 和 IEEE802.11v 协议的一种漫游技术，由 AP 和无线客户端协同引导，实现了无线客户端在一个 ESS（Extended Service Set，拓展服务集）区域中的无缝漫游。其中：

- 802.11k 协议中定义的 Beacon 射频测量功能，实现了对 2.4GHz 和 5GHz 频段的信道质量及可用资源性能的监控。
- 802.11r 协议中定义的 FT（Fast BSS Transition，快速 BSS 切换）功能用来减少客户端在漫游过程中的时间延迟，从而降低连接中断概率、提高漫游服务质量。

- 802.11v 协议中定义的 BTM（BSS Transition Management，BSS 切换管理）功能用来被动引导支持 802.11v 协议的无线客户端离开当前 BSS，接入更合适的 AP，从而提高 802.11v 无线客户端的接入质量。
- 协同漫游功能新增支持通过 AP 监测 802.11v 无线客户端信号强度，主动引导无线客户端接入更合适的服务。

2.6.2 协同漫游配置限制和指导

协同漫游目前仅支持同一 AC 内的漫游组网方式，且协同漫游要求 AP 必须支持 Wi-Fi 6 标准。

2.6.3 配置无线客户端反粘滞功能

1. 功能简介

开启无线客户端反粘滞功能后，AP 将按照配置的时间间隔检测无线客户端的信号强度。当无线客户端信号强度低于门限值时：

- 若该无线客户端关联过程中协商为支持 802.11v 协议，则按照 BSS 切换管理功能，引导无线客户端连接到其它的 BSS。
- 若该无线客户端关联过程中协商为不支持 802.11v 协议，则不会引导无线客户端连接到其它 BSS 上。

对于无线客户端频繁进行 BSS 切换的场景，建议配置基于 ACL 的无线客户端反粘滞，通过将不同类型客户端加入到不同 ACL 中，由设备对不同类型的客户端根据 ACL 下配置的信号强度门限值进行针对性反粘滞控制。

2. 配置限制和指导

只有开启了无线客户端反粘滞功能，基于 ACL 对无线客户端进行反粘滞才能生效。

同一 AP 的同一射频下仅支持绑定一个 ACL 规则。

可以通过 **display wlan client verbose** 命令查看客户端信号强度 RSSI，根据该 RSSI，配置基于 ACL 的无线客户端反粘滞 RSSI。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 AP 视图或 AP 组 ap-model 视图。

- 进入 AP 视图。

```
wlan ap ap-name
```

- 请依次执行以下命令进入 AP 组 ap-model 视图。

```
wlan ap-group group-name
```

```
ap-model ap-model
```

- (3) 进入 Radio 视图。

```
radio radio-id
```

- (4) 配置无线客户端反粘滞功能。

```
sacp anti-sticky { disable | enable [ rssi rssi-value ] [ interval interval ] [ forced-logoff ] }
```

缺省情况下：

Radio 视图：继承 AP 组 Radio 配置。

AP 组 Radio 视图：无线客户端反粘滞功能处于开启状态。

- (5) （可选）配置基于 ACL 的无线客户端反粘滞。

Radio 视图：

```
sacp anti-sticky acl { acl-number rssi rssi-value | remove }
```

AP 组 Radio 视图：

```
sacp anti-sticky acl acl-number [ rssi rssi-value ]
```

缺省情况下：

Radio 视图：继承 AP 组 Radio 配置。

AP 组 Radio 视图：未配置基于 ACL 的无线客户端反粘滞。

配置基于 ACL 的无线客户端反粘滞后，若指定 **remove** 关键字，则表示该 Radio 不基于 ACL 进行无线客户端反粘滞。

2.6.4 配置设备对异常 802.11kv 无线客户端进行非 802.11kv 处理

1. 功能简介

当网络环境中同时存在 802.11kv 协议支持较好（即支持正常，可以通过 802.11kv 处理接入更合适的 BSS）和支持不够好（即支持异常，客户端与设备通信时，时延过大或无法通信，无法通过 802.11kv 处理接入更合适的 BSS）的无线客户端时：

- 不配置本功能，设备会对所有客户端进行 802.11kv 处理，这样就会导致异常客户端网络通信异常。
- 配置本功能后，通过 ACL 规则过滤的客户端被认为是异常 802.11kv 客户端，对这些客户端进行非 802.11kv 处理，这样既可以保证正常客户端的 BSS 切换，又可以保证异常客户端的网络性能。未通过 ACL 规则过滤的无线客户端，设备会继续对其进行 802.11kv 处理。

2. 配置限制和指导

本功能仅对从未匹配过异常 ACL 规则的已在线客户端和新上线客户端生效。当需要对已在线客户端重新进行 ACL 规则匹配时，需要该客户端重新上线。

本功能仅对关联位置在 AC 上的无线客户端生效。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入无线服务模板视图。

```
wlan service-template service-template-name
```

- (3) 配置设备对异常 802.11kv 无线客户端进行非 802.11kv 处理。

```
sacp roam-optimize abnormal-802.11kv acl acl-number
```

缺省情况下，设备对所有 802.11kv 无线客户端进行 802.11kv 处理。

2.6.5 配置获取 BSS 候选列表功能

1. 功能简介

开启获取 BSS 候选列表功能后，AP 将按照配置的时间间隔周期性地向支持 Beacon 测量的客户端发送 Beacon Request 帧以请求获取无线客户端检测到的 BSS 信息，无线客户端通过 Beacon Report 帧上报当前工作信道检测到的 BSS 信息。关闭该功能后，已获取到的 BSS 候选列表的 BSS 信息到达老化时间后会被删除。

开启 BSS 切换管理功能后，设备将使用 BSS 候选列表的 BSS 信息，引导无线客户端漫游到信号质量更好的无线服务上。

2. 配置限制和指导

仅对配置本功能后新上线的无线客户端生效。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 AP 视图或 AP 组 ap-model 视图。

- 进入 AP 视图。

```
wlan ap ap-name
```

- 请依次执行以下命令进入 AP 组 ap-model 视图。

```
wlan ap-group group-name
```

```
ap-model ap-model
```

- (3) 进入 Radio 视图。

```
radio radio-id
```

- (4) 配置获取 BSS 候选列表功能。

```
sacp roam-optimize bss-candidate-list { disable | enable [ interval  
interval ] }
```

缺省情况下：

Radio 视图：继承 AP 组 Radio 配置。

AP 组 Radio 视图：获取 BSS 候选列表功能处于关闭状态。

2.6.6 开启漫游优化流量保持高级功能

1. 功能简介

漫游优化流量保持高级功能开启期间，当设备检测到客户端信号强度低于无线客户端反粘滞功能配置的门限值时，会缓存需要发送给客户端的数据报文，一段时间后，再将缓存的数据报文发送给客户端，减少了客户端信号强度较弱情况下的丢包数量。关闭本功能后，设备一段时间后会缓存的数据报文做老化处理，不再重新发送给客户端。对于开启了无线客户端反粘滞控制功能的协同漫游场景，建议开启本功能。

2. 配置限制和指导

本功能仅当客户端关联位置和数据报文转发位置在 AC 上时生效。

本功能不支持分层 AC 组网。

3. 配置步骤

- (1) 进入系统视图。
`system-view`
- (2) 进入无线服务模板视图。
`wlan service-template service-template-name`
- (3) 开启漫游优化流量保持高级功能。
`sacp roam-optimize traffic-hold enable advanced`
缺省情况下，漫游优化流量保持高级功能处于关闭状态。

2.6.7 协同漫游显示和维护

在完成上述配置后，在任意视图下执行 `display` 命令可以显示配置后协同漫游的运行情况，通过查看显示信息验证配置效果。



说明

- `display wlan service-template` 命令及 `display wlan client` 命令的详细信息，请参见“WLAN 接入命令参考”中的“WLAN 接入”。
- `display wlan ap name running-configuration` 命令的详细信息，请参见“AP 管理命令参考”中的“AP 管理”。

表2-1 协同漫游显示和维护

操作	命令
显示指定AP或所有AP的运行配置	<code>display wlan ap { all name ap-name } running-configuration [verbose]</code>
显示客户端的信息	<code>display wlan client [ap ap-name [radio radio-id] mac-address mac-address service-template service-template-name frequency-band { 2.4 5 }] [verbose]</code>
显示客户端上报的射频资源测量能力集	<code>display wlan client rm-capabilities [mac-address mac-address]</code>
显示无线客户端的迁移历史信息	<code>display wlan sacp move-history [mac-address mac-address]</code>
显示无线服务模板信息	<code>display wlan service-template [service-template-name] [verbose]</code>

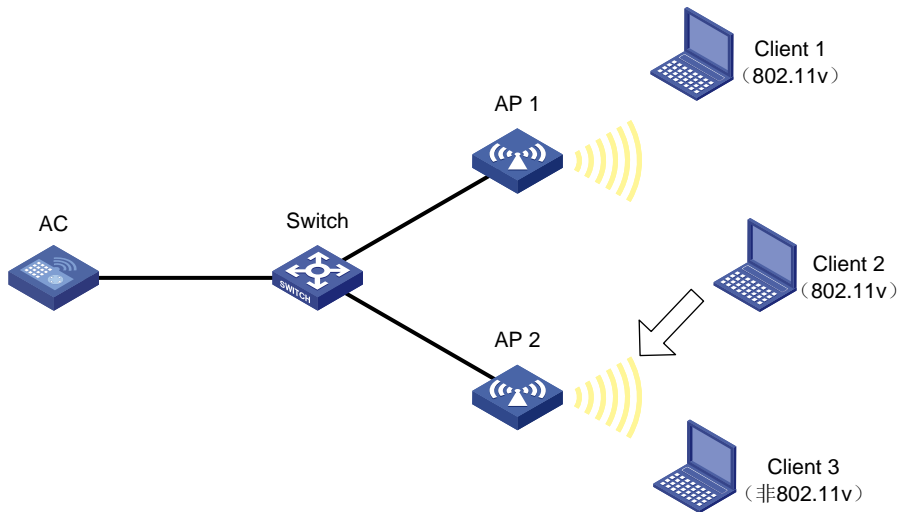
2.6.8 协同漫游典型配置举例

1. 组网需求

如图 2-10 所示，网络中的大部分无线客户端支持 802.11k 和 802.11v 协议，通过配置协同漫游功能，实现无线客户端在一个 ESS（Extended Service Set，拓展服务集）区域中的无缝漫游。

2. 组网图

图2-10 协同漫游配置组网图



3. 配置步骤

说明

- 配置设备接口 IP 地址及路由，保证各设备之间路由可达。
- 当网络中的大部分无线客户端不支持 802.11k 和 802.11v 协议时，只需要配置 BSS 切换管理功能、切换解除管理功能、反粘滞功能以及漫游优化流量保持高级功能，即可实现无线客户端在一个 ESS 区域中的无缝漫游。

创建无线服务模板 wifi6_zero。

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

```
[AC] wlan service-template wifi6_zero
```

配置无线服务的 SSID 为 wifi6_zero。

```
[AC-wlan-st-wifi6_zero] ssid wifi6_zero
```

开启 BSS 切换管理功能。

```
[AC-wlan-st-wifi6_zero] bss transition-management enable
```

（可选）配置切换解除关联功能。

```
[AC-wlan-st-wifi6_zero] bss transition-management disassociation recommended timer 45
```

（可选）开启漫游优化流量保持高级功能。

```
[AC-wlan-st-wifi6_zero] sacp roam-optimize traffic-hold enable advanced
```

开启 FT 功能。

```
[AC-wlan-st-wifi6_zero] ft enable
```

说明

如果网络中存在的客户端型号较早而不支持 FT 协议，建议不开启本功能。

使能无线服务。

```
[AC-wlan-st-wifi6_zero] service-template enable
[AC-wlan-st-wifi6_zero] quit
```

创建手工 AP，名称为 ap1，序列号为 219801A28N819CE0002T。

```
[AC] wlan ap ap1 model WA6320
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

进入 Radio 1 视图。

```
[AC-wlan-ap-ap1] radio 1
```

开启射频资源测量功能。

```
[AC-wlan-ap-ap1-radio-1] resource-measure enable
```

（可选）开启获取 BSS 候选列表功能。

```
[AC-wlan-ap-ap1-radio-1] sacp roam-optimize bss-candidate-list enable
```

（可选）配置射频每 2 秒进行信号强度检测，在支持 802.11v 的无线客户端信号强度低于-30dBm 时，引导其进行 BSS 切换，对不支持 802.11v 的客户端强制下线处理。

```
[AC-wlan-ap-ap1-radio-1] sacp anti-sticky enable rssi 30 interval 2 forced-logoff
```

将无线服务模板 wifi6_zero 绑定到 ap1 的 Radio1 上。

```
[AC-wlan-ap-ap1-radio-1] service-template wifi6_zero
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
```

（可选）配置对无线客户端进行差异化反粘滞管控制。



说明

当网络中存在不同类型的客户端且客户端发射功率差异较大，出现 AP 上行检测出的客户端信号强度差异较大时，建议配置基于 ACL 对无线客户端进行差异化反粘滞控制。

- 创建 ACL 规则，将 CCC9-5DE2-512D 终端按照 OUI 匹配规则加入到弱信号 ACL 匹配规则中。

```
[AC] acl number 4500
[AC-acl-mac-4500] rule permit source-mac ccc9-5de2-512d ffff-ff00-0000
[AC-acl-mac-4500] quit
```

- 指定编号为 4500 的 ACL 匹配的无线客户端，在信号强度低于-25dBm 时，由 AP 引导其进行 BSS 切换。

```
[AC] wlan ap ap1
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] sacp anti-sticky acl 4500 rssi 25
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
```

4. 验证配置

- # 在 AC 上通过 **display wlan service-template** 命令可以查看 BSS 切换管理功能处于开启状态。

```
[AC] display wlan service-template wifi6_zero verbose
Service template name           : wifi6_zero
Description                     : Not configured
```

SSID	: wifi6_zero
SSID-hide	: Disabled
User-isolation	: Disabled
Service template status	: enabled
Maximum clients per BSS	: Not configured
Frame format	: Dot3
Seamless roam status	: Disabled
Seamless roam RSSI threshold	: 50
Seamless roam RSSI gap	: 20
VLAN ID	: 1
Service VLAN ID	: N/A
Service VLAN TPID	: dot1q
AKM mode	: Not configured
Security IE	: Not configured
Cipher suite	: Not configured
TKIP countermeasure time	: 0 sec
PTK lifetime	: 43200 sec
PTK rekey	: Enabled
GTK rekey	: Enabled
GTK rekey method	: Time-based
GTK rekey time	: 86400 sec
GTK rekey client-offline	: Disabled
WPA3 status	: Disabled
PPSK	: Disabled
PPSK Fail Permit	: Enabled
Enhance-open status	: Disabled
Enhanced-open transition-mode service-template	: N/A
User authentication mode	: Bypass
Intrusion protection	: Disabled
Intrusion protection mode	: Temporary-block
Temporary block time	: 180 sec
Temporary service stop time	: 20 sec
Fail VLAN ID	: Not configured
802.1X handshake	: Disabled
802.1X handshake secure	: Disabled
802.1X domain	: Not configured
MAC-auth domain	: Not configured
Max 802.1X users per BSS	: 512
Max MAC-auth users per BSS	: 512
802.1X re-authenticate	: Disabled
Authorization fail mode	: Online
Accounting fail mode	: Online
Authorization	: Permitted
Key derivation	: SHA1
PMF status	: Disabled
Hotspot policy number	: Not configured
Forwarding policy status	: Disabled
Forwarding policy name	: Not configured

Forwarder	: AC
FT status	: Enabled
FT method	: Over-the-air
FT reassociation deadline	: 20 sec
QoS trust	: Port
QoS priority	: 0
QoS U-APSD mode	: 1
BTM status	: Enabled

- # 在 AC 上通过 **display wlan client rm-capabilities** 命令可以查看到新接入客户端的射频资源能力支持情况。

```
[AC] display wlan client rm-capabilities
Total number of clients: 1
```

MAC address	: ccc9-5de2-512d
Neighbor report capability	: Disabled
Beacon passive measurement	: Enabled
Beacon active measurement	: Enabled
Beacon table measurement	: Disabled

- # 在 AC 上通过 **display wlan client verbose** 命令可以查看新接入客户端支持 802.11v BSS 切换管理功能。

```
[AC] display wlan client verbose
Total number of clients: 1
```

MAC address	: ccc9-5de2-512d
IPv4 address	: 10.1.1.114
IPv6 address	: N/A
Username	: N/A
AID	: 1
AP ID	: 2
AP name	: ap1
Radio ID	: 1
Channel	: 64
SSID	: wifi6_zero
BSSID	: 0026-3e08-1150
VLAN ID	: 1
VLAN ID2	: N/A
Sleep count	: 0
Wireless mode	: 802.11ax
Channel bandwidth	: 80MHz
SM power save	: Disabled
Short GI for 20MHz	: Supported
Short GI for 40MHz	: Supported
Short GI for 80MHz	: Supported
Short GI for 160/80+80MHz	: Not supported
STBC RX capability	: Not supported
STBC TX capability	: Not supported
LDPC RX capability	: Not supported
SU beamformee capability	: Not supported

```

MU beamformee capability      : Not supported
Beamformee STS capability     : N/A
Block Ack                     : TID 0 In
Supported VHT-MCS set        : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
                               NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Supported HT MCS set         : 0, 1, 2, 3, 4, 5, 6, 7,
                               8, 9, 10, 11, 12, 13, 14,
                               15
Supported rates               : 6, 9, 12, 18, 24, 36,
                               48, 54 Mbps
5G 40And80MHz Channel bandwidth : Supported
5G 160MHz Channel bandwidth   : Not Supported
5G 8080MHz Channel bandwidth  : Not Supported
OFDMA random access RUs      : Not supported
Supported HE-MCS set         : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11
                               NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11
TWT scheduled                 : no
QoS mode                      : WMM
Listen interval               : 20
RSSI                          : 40
Rx/Tx rate                    : 54/6 Mbps
Speed                         : 0.968/0.104 Mbps
Authentication method         : Open system
Security mode                 : PRE-RSNA
AKM mode                      : Not configured
Cipher suite                  : N/A
User authentication mode      : Bypass
WPA3 status                   : N/A
Authorization CAR              : N/A
Authorization ACL ID          : N/A
Authorization user profile    : N/A
Roam status                   : N/A
Key derivation                 : SHA1
PMF status                    : N/A
Forwarding policy name        : Not configured
Online time                   : 0days 0hours 1minutes 53seconds
FT status                     : Inactive
BTM status                    : Active

```

- # 在 AC 上通过 **display wlan ap name ap1 running-config** 命令可以查看该 AP 下 Radio 1 生效的相关配置。

```

[AC] display wlan ap all running-configuration verbose
(i) -- Inherited from AP group
(g) -- Inherited from AP global-configuration

#
wlan ap ap1 model WA6320 id 2
    ap group name default-group
    serial-id 219801A28N819CE0002T

```

```

region code CN (g)
echo interval 10 (i)
...略...

radio 1
  radio type 802.11ax
  radio enable
  channel auto<52> (i)
  channel unlock (i)
  fragment-threshold 2346 (i)
  max-power 20 (i)
  power unlock (i)
  distance 1 kilometer (i)
  ANI Enabled (i)
...略...
  sacp anti-sticky enable rssi 35 interval 2 forced-logoff 1
  sacp anti-sticky acl 4500 rssi 30

radio 2
  radio type 802.11n(2.4GHz) (i)
  radio disable (i)
  channel auto<11> (i)
  channel unlock (i)
  fragment-threshold 2346 (i)
  max-power 20 (i)
  power unlock (i)
  distance 1 kilometer (i)
  ANI Enabled (i)
...略...
  sacp anti-sticky enable rssi 20 interval 3 forced-logoff 0 (i)
  sacp anti-sticky acl disable (i)

```

3 漫游组

3.1 漫游组简介

多个设备可以加入一个相同的组，客户端可以在组内漫游，该组即为漫游组，在漫游组漫游期间，客户端的 IP 地址、授权信息等维持不变，可以实现客户端在更大物理区域内的漫游。

3.2 WLAN漫游基本概念

- IADTP（Inter Access Device Tunneling Protocol，接入设备间隧道协议）：H3C 私有隧道协议，该协议提供了设备间报文的通用封装和传输机制。提供漫游服务的设备之间会建立 IADTP 隧道，用于保证设备间控制报文以及客户端漫游信息的安全传输。
- HA(Home-AC)：一个客户端首次与 IADTP 隧道内的某个 AC 进行关联，该 AC 即为它的 HA。
- FA (Foreign-AC)：客户端跨 AC 漫游后，客户端与某个不是 HA 的 AC 进行关联，该 AC 即为 FA。
- 漫游组：多个设备可以加入一个相同的组，客户端可以在组内漫游，该组即为漫游组。

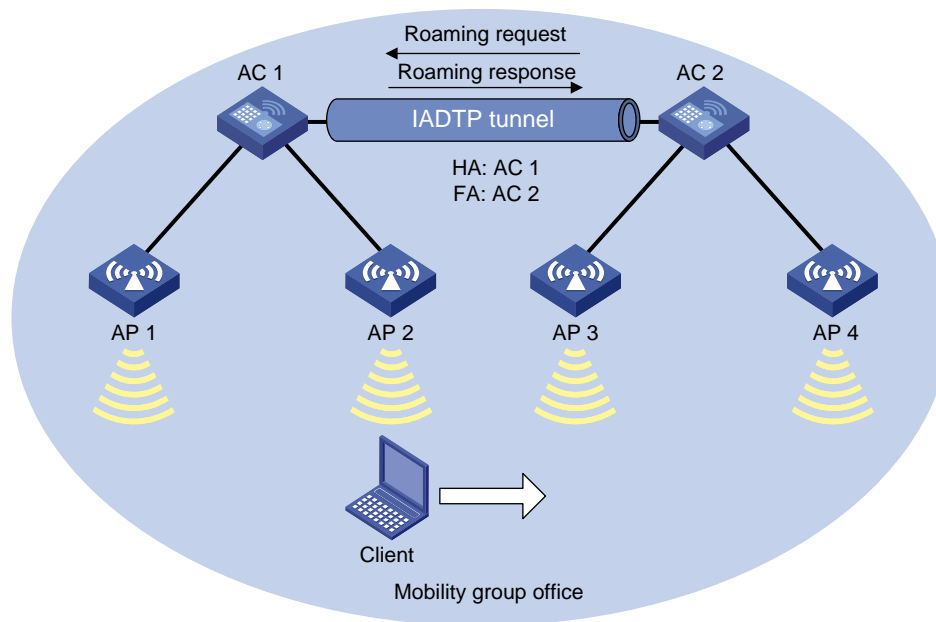
3.3 漫游组实现方式介绍

如图 3-1 所示，客户端从一个 AC 内的 AP 漫游到另一个 AC 内的 AP 上接入。该组网方式下，通过创建漫游组，统一管理参与漫游的 AC，没有加入漫游组的 AC 将不参与漫游。

客户端完成 AC 间漫游的过程如下：

- (1) 客户端在 AP 2 上初始上线，在 AC 1 上会创建该客户端的漫游表项，并通过 IADTP 隧道将漫游表项同步到漫游组成员 AC 2 上；
- (2) 客户端漫游到 AP 3，AC 2 查找该客户端的漫游表项，如果是 RSN+802.1X 认证方式，且客户端携带的 PMKID 和设备缓存的 PMKID 一致，则对其进行快速漫游，其他情况，则不对其进行快速漫游；
- (3) 如果进行快速漫游，客户端不需要再次认证，即可在 AP 3 上成功上线；否则需要重新认证；
- (4) 客户端在 AP 3 上线，AC 2 会给 AC 1 发送漫游请求消息；
- (5) AC 1 收到漫游请求消息，并校验漫游信息是否正确。如果校验失败，则给 AC 2 回复漫游失败的漫游响应消息。如果校验成功，AC 1 添加该客户端的漫游轨迹和漫出信息，并给 AC 2 回复漫游成功的漫游响应信息；
- (6) AC 2 收到 AC 1 回复的漫游响应信息。如果漫游失败，AC 2 将通知客户端下线；如果漫游成功，AC 2 添加该客户端的漫入信息。

图3-1 漫游组实现方式示意图



3.4 IADTP隧道建立过程

漫游组中的成员设备分为如下角色：

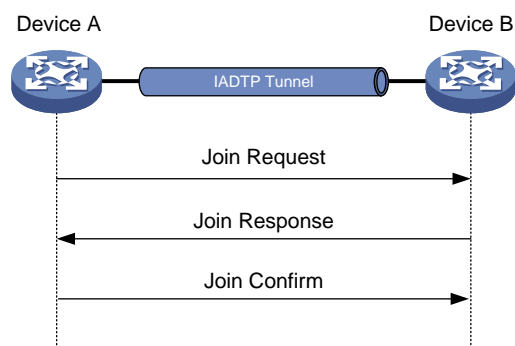
- **Client 端**：负责发起连接建立请求。
- **Server 端**：监听并应答连接建立请求。

缺省情况下，IP 地址小的成员设备作为 **Client 端**，IP 地址大的成员设备作为 **Server 端**。如果漫游组成员设备跨 NAT 设备，则需要手工指定成员设备在漫游组中的角色。

设备间建立 IADTP 隧道的具体过程如下：

- (1) Device A 向 Device B 发送 Join Request 报文。
- (2) Device B 收到 Join Request 报文后，根据本地配置和报文内容判断是否和 Device A 属于同一漫游组。当属于同一漫游组时，回复 Result Code 为成功的 Join Response 报文；否则，回复 Result Code 为失败的 Join Response 报文。
- (3) Device A 收到 Result Code 为成功的 Join Response 报文后，会向 Device B 发送 Join Confirm 报文，建立 IADTP 隧道；否则，不回复报文。
- (4) Device B 收到 Join Confirm 报文后，建立 IADTP 隧道。

图3-2 IADTP 隧道建立过程



3.5 漫游组配置限制和指导

在对 AP 进行配置时，可以采用如下方式：

- 针对单台 AP，在 AP 视图下进行配置。
- 针对同一个 AP 组内的 AP，在 AP 组视图下针对 AP 组进行配置。
- 在全局配置视图下针对所有 AP 进行全局配置。

对于一台 AP，这些配置的生效优先级从高到低为：针对 AP 的配置、AP 组中的配置、全局配置。配置漫游组，需要注意以下事项：

- 对于配置用户接入认证位置在 AP 的无线服务模板，不支持客户端漫游。有关用户接入认证位置相关配置的详细介绍请参见“用户接入与认证配置指导”中的“WLAN 用户接入认证”。
- 如果存在 RSN+802.1X 认证方式的客户端，且客户端所属的 VLAN 不同时，同一漫游组内的设备上接口需要允许所有 RSN+802.1X 认证方式的客户端 VLAN 通过。

3.6 漫游组配置任务简介

漫游组配置任务如下：

- (1) [创建漫游组](#)
- (2) （可选）[配置漫游组认证模式](#)
- (3) [配置漫游组 IADTP 隧道 IP 地址类型](#)
- (4) [配置设备加入漫游组时建立 IADTP 隧道的源 IP 地址](#)
- (5) （可选）[配置设备发送的 IADTP 隧道控制报文的 DSCP 优先级](#)
- (6) [添加漫游组内的成员设备](#)

在手动和自动添加漫游组内的成员设备中选择一项任务进行配置：

- [手动添加漫游组内的成员设备](#)
- [自动添加漫游组内的成员设备](#)

- (7) （可选）[配置本成员设备在漫游组中的角色](#)
- (8) （可选）[关闭 IADTP 数据隧道功能](#)
- (9) （可选）[开启漫游中继功能](#)

- (10) [开启漫游组功能](#)
- (11) (可选) [开启漫游组隧道隔离功能](#)
- (12) (可选) [开启漫游组告警功能](#)

3.7 创建漫游组

1. 配置限制和指导

属于同一个漫游组的每个设备上都必须创建漫游组，并互相添加漫游组成员。每个设备上只允许创建一个漫游组。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建漫游组，并进入漫游组视图。

```
wlan mobility group group-name
```

3.8 配置漫游组认证模式

1. 功能简介

配置认证模式后，所有在 IADTP 隧道中传输的控制消息都会附带一个摘要（完整性代码），当设备接收到控制消息后会使用相同的算法对消息内容进行计算，并与消息中所携带的摘要进行比较，以验证收到的消息的完整性。目前，漫游组认证模式仅支持 MD5 认证算法。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入漫游组视图。

```
wlan mobility group group-name
```

- (3) 配置漫游组认证模式。

```
authentication-mode authentication-mode { cipher | simple } string
```

缺省情况下，未配置漫游组认证模式。

3.9 配置漫游组IADTP隧道IP地址类型

1. 功能简介

创建漫游组之后，必须指定漫游组隧道 IP 地址类型。只有设备加入漫游组时建立 IADTP 隧道的源 IP 地址与隧道 IP 地址类型相同，设备加入漫游组时才会生效并建立隧道。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入漫游组视图。

```
wlan mobility group group-name
```

- (3) 配置漫游组 IADTP 隧道 IP 地址类型。

```
tunnel-type { ipv4 | ipv6 }
```

缺省情况下，IADTP 隧道 IP 地址类型为 IPv4。

3.10 配置设备加入漫游组时建立IADTP隧道的源IP地址

1. 功能简介

设备在加入漫游组后需要使用 IADTP 隧道源 IP 地址和同一漫游组内成员设备建立 IADTP 隧道。

2. 配置限制和指导

配置设备加入漫游组时建立 IADTP 隧道的源 IP 地址，需要注意的是：

- 只能在漫游组处于关闭状态的情况下，才能指定设备加入漫游组时建立 IADTP 隧道的源 IP 地址。
- 可以同时配置 IPv4 和 IPv6 类型的源地址，每种类型的源地址只能配置一个。
- 只有与漫游组 IADTP 隧道 IP 地址类型相同的源地址可以生效。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入漫游组视图。

```
wlan mobility group group-name
```

- (3) 配置设备加入漫游组时建立 IADTP 隧道的源 IP 地址。

```
source { ip ipv4-address | ipv6 ipv6-address }
```

缺省情况下，未配置建立 IADTP 隧道的源 IP 地址。

3.11 配置设备发送的IADTP隧道控制报文的DSCP优先级

1. 功能简介

DSCP（Differentiated Services Code Point，差分服务编码点）携带在 IP 报文中的 ToS 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。配置的 DSCP 优先级的取值越大，报文的优先级越高。

跨 NAT 设备建立 IADTP 隧道时，需要借助 IPsec 隧道功能完成 IADTP 控制隧道的加密和数据隧道的建立及加密。由于控制报文和数据报文缺省 DSCP 优先级都为 0，当漫游隧道通过 IPsec 加密后，为了防止在 IADTP 隧道繁忙时，成员设备因为长时接收不到 IADTP 隧道保活报文而断开 IADTP 隧道的连接，需要提高 IADTP 隧道保活报文发送的优先级。

2. 配置限制和指导

建议配置设备发送的 IADTP 隧道控制报文的 DSCP 优先级为 63。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```


- (2) 进入漫游组视图。

```
wlan mobility group group-name
```

- (3) 配置设备发送的 IADTP 隧道控制报文的 DSCP 优先级。

```
tunnel-dscp dscp-value
```

缺省情况下，设备发送的 IADTP 隧道控制报文的 DSCP 优先级为 0。

3.12 添加漫游组内的成员设备

3.12.1 手动添加漫游组内的成员设备

1. 功能简介

漫游组内的成员设备通过 IP 地址标识，该 IP 地址为成员设备建立 IADTP 隧道的源 IP 地址。漫游组内可以同时添加 IPv4 和 IPv6 类型的漫游组成员，但是只有与隧道类型相同的成员可以生效。当指定了漫游组内的成员设备所属 VLAN 后，漫游组内的其他设备就可以直接转发属于该 VLAN 的客户端的数据流量，而无需客户端漫游到该设备上。

2. 配置限制和指导

每一个成员只能属于一个漫游组，并且一个漫游组中最多可以添加 31 个 IPv4 漫游组成员或 31 个 IPv6 漫游组成员。配置漫游组内的成员设备所属 VLAN 后，该 VLAN 不能在应用于其它接口或业务。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入漫游组视图。

```
wlan mobility group group-name
```

- (3) 添加漫游组内的成员设备。

```
member { ip ipv4-address | ipv6 ipv6-address } [ vlan vlan-id-list ]
```

3.12.2 自动添加漫游组内的成员设备

1. 功能简介

漫游组内的成员设备通过 IP 地址标识，该 IP 地址为成员设备建立 IADTP 隧道的源 IP 地址。漫游组内可以同时添加 IPv4 和 IPv6 类型的漫游组成员，但是只有与隧道类型相同的漫游组成员可以生效。

开启漫游组成员自动添加功能后，要加入漫游组的设备会通过自动添加成员设备报文在漫游组内广播自己的 IP 地址。漫游组的其它开启自动添加功能的设备收到广播报文后与要加入漫游组的设备建立 IADTP 隧道。隧道建立成功后，则设备成功加入漫游组。

2. 配置限制和指导

每一个成员只能属于一个漫游组，并且一个漫游组中最多可以添加 31 个 IPv4 漫游组成员或 31 个 IPv6 漫游组成员，当漫游组成员达到最大数量后，当前设备不会再与其它设备建立 IADTP 隧道。

只能自动添加同一网段内的漫游组成员设备。

3. 配置准备

配置自动添加漫游组内的成员设备之前，请先通过 **source** 命令配置成员设备加入漫游组时建立 IADTP 隧道的源 IP 地址。

4. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入漫游组视图。

```
wlan mobility group group-name
```

- (3) 开启漫游组成员自动添加功能。

```
member auto-discovery [ interval interval ]
```

缺省情况下，漫游组成员自动添加功能处于关闭状态。

3.13 配置本成员设备在漫游组中的角色

1. 功能简介

当漫游组成员设备间跨 NAT 设备建立 IADTP 隧道时，外网设备无法主动向内网设备发起连接请求。缺省情况下 IP 地址小的成员设备作为 Client 端发起连接建立请求，IP 地址大的成员设备作为 Server 端监听并应答连接建立请求，通过报文的交互最终完成 IADTP 隧道的建立。此时，如果外网设备的 IP 地址小于内网设备的 IP 地址，将无法建立 IADTP 隧道。在这种情况下，需要通过配置内网成员设备作为 Client 端发起连接建立请求，以便完成 IADTP 隧道的建立。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入漫游组视图。

```
wlan mobility group group-name
```

- (3) 配置本成员设备在漫游组中的角色。

```
role { client | server }
```

缺省情况下，漫游组中 IP 地址大的成员设备作为 Server 端，IP 地址小的成员设备作为 Client 端。

3.14 关闭 IADTP 数据隧道功能

1. 功能简介

为了减轻漫游组成员设备处理 IADTP 数据隧道上接收的广播报文的负担，并减少设备维护 IADTP 数据隧道的资源消耗，如果客户端漫游后所在的 VLAN 在当前成员设备上有业务出口，可以通过本功能关闭 IADTP 数据隧道，不再通过 IADTP 数据隧道转发客户端数据，直接通过业务出口转发。如果客户端漫游后所在的 VLAN 在当前成员设备上没有业务出口，不能关闭 IADTP 数据隧道功能，否则会造成客户端数据丢失。

2. 配置限制和指导

漫游组内所有成员设备需要同时开启或者关闭 IADTP 数据隧道功能。
本功能只能在漫游组功能处于关闭状态时配置。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入漫游组视图。

```
wlan mobility group group-name
```

- (3) 关闭 IADTP 数据隧道功能。

```
data-tunnel disable
```

缺省情况下，IADTP 数据隧道功能处于开启状态。

3.15 开启漫游中继功能

1. 功能简介

WLAN 客户端在 AC 间漫游时，需要在任意两个 AC 之间建立漫游组隧道，形成网状拓扑结构。当网络中 AC 设备数量比较多时，建立、维护漫游组隧道以及漫游信息同步都会占用一定的带宽资源，并且网络结构复杂、稳定性低。为了解决这一问题，可以在一台 AC 上开启漫游中继功能，使得该 AC 作为中继 AC，并在其上指定其余非中继 AC 为漫游组成员。中继 AC 与每个非中继 AC 分别建立一条 IADTP 隧道，形成一对多的星形漫游组网。非中继 AC 之间不需要建立漫游组隧道。漫游组中的非中继 AC 会通过 IADTP 隧道将漫游表项同步到中继 AC。当客户端在 AC 间发生漫游时，漫游后的 AC 会向中继 AC 请求查询当前客户端的漫游表项信息。

2. 配置限制和指导

本命令只能在漫游组功能处于关闭状态时配置。

同一漫游组内只能存在一个中继 AC，非中继 AC 只能指定中继 AC 为漫游组内唯一成员。

在漫游中继组网中，如果客户端所属的 VLAN 不同，中继 AC 的上行接口需要允许所有客户端的 VLAN 通过。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入漫游组视图。

```
wlan mobility group group-name
```

- (3) 开启漫游中继功能。

```
roam-relay enable
```

缺省情况下，漫游中继功能处于关闭状态。

3.16 开启漫游组功能

1. 功能简介

开启漫游组功能后，设备会使用 IADTP 隧道源 IP 地址与组内其他成员设备建立 IADTP 隧道，并同步漫游表项信息。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入漫游组视图。

```
wlan mobility group group-name
```

- (3) 开启漫游组功能。

```
group enable
```

缺省情况下，漫游组功能处于关闭状态。

3.17 开启漫游组隧道隔离功能

1. 功能简介

同一漫游组内的多台设备间存在环路时，需要开启漫游组隧道隔离功能，确保设备不会在漫游组的隧道之间转发报文，从而避免出现广播风暴等问题。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启漫游组隧道隔离功能。

```
wlan mobility-group-isolation enable
```

缺省情况下，漫游组隧道隔离功能处于开启状态。

3.18 开启漫游组告警功能

1. 功能简介

开启了漫游组告警功能之后，该模块会生成告警信息，用于报告该模块的重要事件。生成的告警信息将发送到设备的 SNMP 模块，通过设置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关属性。（有关告警信息的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”。）

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启漫游组告警功能。

```
snmp-agent trap enable wlan mobility
```

缺省情况下，漫游组告警功能处于关闭状态。

3.19 漫游组显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后的漫游运行情况，通过查看显示信息验证配置的效果。

表3-1 漫游组显示和维护

操作	命令
显示客户端漫游或漫游出的信息	display wlan mobility { roam-in roam-out } [member { ip ipv4-address ipv6 ipv6-address }]
显示漫游组的信息	display wlan mobility group

3.20 漫游组典型配置举例



说明

本手册中的 AP 型号和序列号仅为举例，具体支持的 AP 型号和序列号请以设备的实际情况为准。

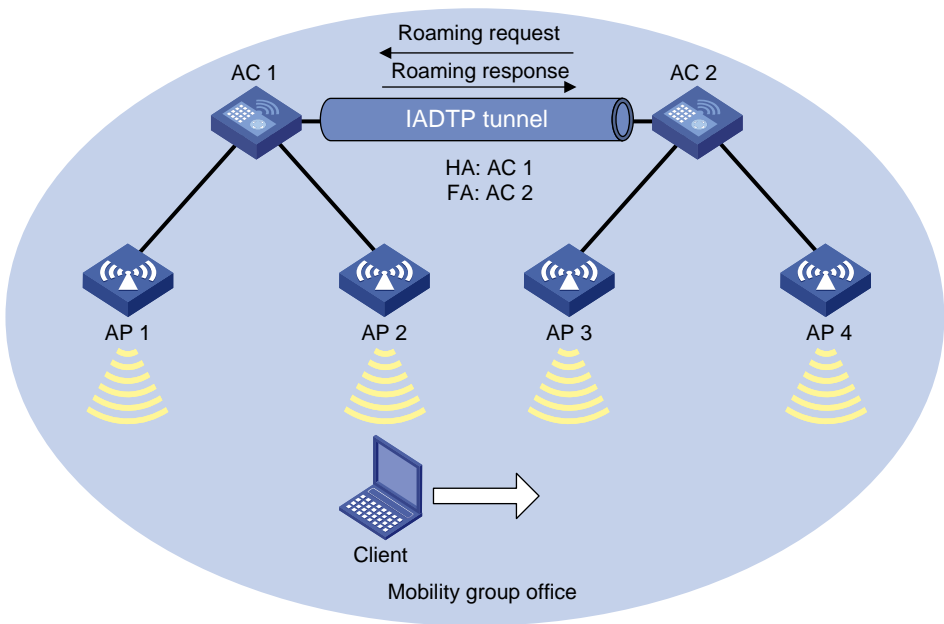
3.20.1 漫游组典型配置举例

1. 组网需求

如图 3-3 所示，在一个无线网络中，有两台 AC，现要求客户端可以在 AC 内漫游，也可以跨 AC 漫游。

2. 组网图

图3-3 漫游组配置组网图



3. 配置步骤

(1) 配置 AC 1

创建无线服务模板 **service**，配置 SSID 为 **office**，并使能服务模板。

```
<AC1> system-view
[AC1] wlan service-template service
[AC1-wlan-st-test] ssid office
[AC1-wlan-st-test] service-template enable
[AC1-wlan-st-test] quit
```

创建手工 AP，名称为 **ap1**，选择 AP 型号并配置序列号。

```
[AC1] wlan ap ap1 model WA6320
[AC1-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

将服务模板绑定到 **ap1** 的 Radio 1 接口

```
[AC1-wlan-ap-ap1] radio 1
[AC1-wlan-ap-ap1-radio-1] radio enable
[AC1-wlan-ap-ap1-radio-1] service-template service
[AC1-wlan-ap-ap1-radio-1] quit
[AC1-wlan-ap-ap1] quit
```

创建手工 AP，名称为 **ap2**，选择 AP 型号并配置序列号。

```
[AC1] wlan ap ap2 model WA6320
[AC1-wlan-ap-ap2] serial-id 219801A28N819CE0003T
```

将服务模板绑定到 **ap2** 的 Radio 1 接口。

```
[AC1-wlan-ap-ap2] radio 1
[AC1-wlan-ap-ap2-radio-1] radio enable
[AC1-wlan-ap-ap2-radio-1] service-template service
[AC1-wlan-ap-ap2-radio-1] quit
[AC1-wlan-ap-ap2] quit
```

创建漫游组 **office**。

```
[AC1] wlan mobility group office
```

配置漫游组 IADTP 隧道 IP 地址类型为 IPv4。

```
[AC1-wlan-mg-office] tunnel-type ipv4
```

配置 AC 加入漫游组时建立 IADTP 隧道的源 IP 地址为 10.1.4.22。

```
[AC1-wlan-mg-office] source ip 10.1.4.22
```

添加漫游组内的 AC 成员，该 AC 成员用于建立 IADTP 隧道的源 IP 地址为 10.1.4.23。

```
[AC1-wlan-mg-office] member ip 10.1.4.23
```

开启漫游组功能。

```
[AC1-wlan-mg-office] group enable
[AC1-wlan-mg-office] quit
```

(2) 配置 AC 2

创建无线服务模板 **service**，配置 SSID 为 **office**，并使能服务模板。

```
<AC2> system-view
[AC2] wlan service-template service
[AC2-wlan-st-service] ssid office
[AC2-wlan-st-service] service-template enable
[AC2-wlan-st-service] quit
```

创建手工 AP，名称为 ap3，选择 AP 型号并配置序列号。

```
[AC2] wlan ap ap3 model WA6320
[AC2-wlan-ap-ap3] serial-id 219801A28N819CE0004T
```

将服务模板绑定到 ap3 的 Radio 1 接口。

```
[AC2-wlan-ap-ap3] radio 1
[AC2-wlan-ap-ap3-radio-1] radio enable
[AC2-wlan-ap-ap3-radio-1] service-template service
[AC2-wlan-ap-ap3-radio-1] quit
[AC2-wlan-ap-ap3] quit
```

创建手工 AP，名称为 ap4，选择 AP 型号并配置序列号。

```
[AC2] wlan ap ap4 model WA6320
[AC2-wlan-ap-ap4] serial-id 219801A28N819CE0005T
```

将服务模板绑定到 ap4 的 Radio 1 接口。

```
[AC2-wlan-ap-ap4] radio 1
[AC2-wlan-ap-ap4-radio-1] radio enable
[AC2-wlan-ap-ap4-radio-1] service-template service
[AC2-wlan-ap-ap4-radio-1] quit
[AC2-wlan-ap-ap4] quit
```

创建漫游组 office。

```
[AC2] wlan mobility group office
```

配置漫游组 IADTP 隧道 IP 地址类型为 IPv4。

```
[AC2-wlan-mg-office] tunnel-type ipv4
```

配置 AC 加入漫游组时建立 IADTP 隧道的源 IP 地址为 10.1.4.23。

```
[AC2-wlan-mg-office] source ip 10.1.4.23
```

添加漫游组内的 AC 成员，该 AC 成员用于建立 IADTP 隧道的源 IP 地址为 10.1.4.22。

```
[AC2-wlan-mg-office] member ip 10.1.4.22
```

开启漫游组功能。

```
[AC2-wlan-mg-office] group enable
[AC2-wlan-mg-office] quit
```

4. 验证配置

在 AC 1 查看漫游组信息。

```
[AC1] display wlan mobility group
Mobility group name: office
Tunnel type: IPv4
Source IPv4: 10.1.4.22
Source IPv6: Not configured
Authentication method: Not configured
Mobility group status: Enabled
Member entries: 1
```

IP address	State	Online time
10.1.4.23	Up	00hr 00min 12sec

在 AC 2 查看漫游组信息。

```
[AC2] display wlan mobility group
Mobility group name: office
Tunnel type: IPv4
```

Source IPv4: 10.1.4.23
Source IPv6: Not configured
Authentication method: Not configured
Mobility group status: Enabled

Member entries: 1

IP address	State	Online time
10.1.4.22	Up	00hr 00min 05sec

在 AC 1 上通过 **display wlan mobility roam-track mac-address** 可以查看到客户端在 AP 2 初始上线, 随后从 AP 2 漫游到 AP 3 上。

[AC1] display wlan mobility roam-track mac-address 9cd3-6d9e-6778

Total entries : 2

Current entries: 2

BSSID	Created at	Online time	AC IP address	RID	AP name
000f-e203-8889	2016-06-14 11:12:28	00hr 06min 56sec	10.1.4.23	1	ap3
000f-e203-7777	2016-06-14 11:11:28	00hr 03min 30sec	127.0.0.1	1	ap2

在 AC 1 上通过 **display wlan mobility roam-out** 可以查看到客户端漫游出到 AP 3 上漫出信息。

[AC1] display wlan mobility roam-out

Total entries: 1

MAC address	BSSID	VLAN ID	Online time	FA IP address
9cd3-6d9e-6778	000f-e203-8889	1	00hr 01min 59sec	10.1.4.23

在 AC 2 上通过 **display wlan client** 可以查看到客户端关联的 AP 为 AP 3, 漫游状态为 AC 间漫游。

[AC2] display wlan client verbose

Total number of clients: 1

MAC address	: 9cd3-6d9e-6778
IPv4 address	: 10.1.1.114
IPv6 address	: N/A
Username	: N/A
AID	: 1
AP ID	: 3
AP name	: ap3
Radio ID	: 1
Channel	: 36
SSID	: 1
BSSID	: 000f-e203-8889
VLAN ID	: 1
VLAN ID2	: N/A
Sleep count	: 242
Wireless mode	: 802.11ac
Channel bandwidth	: 80MHz
SM power save	: Enabled
SM power save mode	: Dynamic
Short GI for 20MHz	: Supported
Short GI for 40MHz	: Supported
Short GI for 80MHz	: Supported


```

Short GI for 160/80+80MHz      : Not supported
STBC RX capability             : Not supported
STBC TX capability             : Not supported
LDPC RX capability             : Not supported
SU beamformee capability       : Not supported
MU beamformee capability       : Not supported
Beamformee STS capability      : N/A
Block Ack                      : TID 0 In
Supported VHT-MCS set          : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8
                                NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8
Supported HT MCS set           : 0, 1, 2, 3, 4, 5, 6, 7,
                                8, 9, 10, 11, 12, 13, 14,
                                15, 16, 17, 18, 19, 20,
                                21, 22, 23
Supported rates                 : 6, 9, 12, 18, 24, 36,
                                48, 54 Mbps
QoS mode                       : WMM
Listen interval                 : 10
RSSI                           : 62
Rx/Tx rate                     : 130/11
Authentication method           : Open system
Security mode                   : PRE-RSNA
AKM mode                       : Not configured
Cipher suite                    : N/A
User authentication mode        : Bypass
Authorization ACL ID            : 3001(Not effective)
Authorization user profile      : N/A
Roam status                     : Inter-AC roam
Key derivation                  : SHA1
PMF status                     : Enabled
Forward policy name             : Not configured
Online time                     : 0days 0hours 5minutes 13seconds
FT status                      : Inactive

```

在 AC 2 上通过 **display wlan mobility roam-in** 命令可以查看到客户端从 AP 3 漫入的漫入信息。

```

[AC2] display wlan mobility roam-in
Total entries: 1
MAC address      BSSID          VLAN ID  HA IP address
9cd3-6d9e-6778  000f-e203-8889  1        10.1.4.22

```