H3C WAC&WiNet&WX2500H-LI&WX3500H-LI 系列无线控制器

WLAN 接入配置指导

新华三技术有限公司
http://www.h3c.com

资料版本：6W101-20200230
产品版本：CMW710-E5423P04
CMW710-R5426P02

前 言

H3C WAC&WiNet&WX2500H-LI&WX3500H-LI 系列无线控制器配置指导介绍了各软件特性的原理及其配置方法，包含原理简介、配置任务描述和配置举例，本手册主要介绍了如何配置 WLAN 接入功能的配置。

前言部分包含如下内容：

产品版本

表-1 产品型号及产品版本说明

产品型号	产品版本
WX2510H-PWR-WiNet无线控制器	WX2510H-PWR-WiNet-CMW710-E5423P04
WX2560H-WiNet无线控制器	WX2560H-WiNet-CMW710-E5423P04
WX3500H-WiNet系列无线控制器	WX3500H-WiNet-CMW710-E5423P04
WAC380-30无线控制器	WAC380-30-CMW710-E5423P04
WAC380-60无线控制器	WAC380-60-CMW710-E5423P04
WAC380-90无线控制器	WAC380-90-CMW710-E5423P04
WAC380-120无线控制器	WAC380-120-CMW710-E5423P04
WAC381无线控制器	WAC381-CMW710-E5423P04
WX2540H-LI无线控制器	WX2540H-LI-CMW710-R5426P02
WX2560H-LI无线控制器	WX2560H-LI-CMW710-R5426P02
WX3510H-LI无线控制器	WX3510H-LI-CMW710-R5426P02
WX3520H-LI无线控制器	WX3520H-LI-CMW710-R5426P02

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 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 | ... }	表示从多个选项中仅选取一个。
[x | y | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... }*	表示从多个选项中至少选取一个。
[x | y | ...]*	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
说明	对操作内容的描述进行必要的补充和说明。
窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 示例约定

由于设备型号不同、配置不同、版本升级等原因，可能造成本手册中的内容与用户使用的设备显示信息不一致。实际使用中请以设备显示的内容为准。

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 WLAN 接入

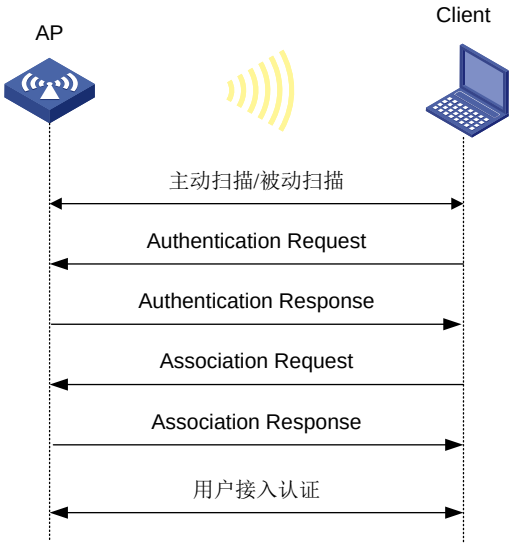
1.1 WLAN接入简介

WLAN 接入为用户提供接入网络的服务。无线服务的骨干网通常使用有线电缆作为线路连接安置在固定网络，接入点设备安置在需要覆盖无线网络的区域，用户在该区域内可以通过无线接入的方式接入无线网络。

1.1.1 WLAN 接入过程

客户端首先需要通过主动/被动扫描方式发现周围的无线网络，再通过链路层认证、关联和用户接入认证三个过程后，才能和 AP 建立连接，最终接入无线服务。整个过程如图 1-1 所示。有关链路层认证、用户接入认证的详细介绍及相关配置请参见“WLAN 安全指导”中的“WLAN 用户安全”和“用户接入与认证”中的“WLAN 用户接入认证”。

图1-1 建立无线连接过程



1.1.2 无线扫描

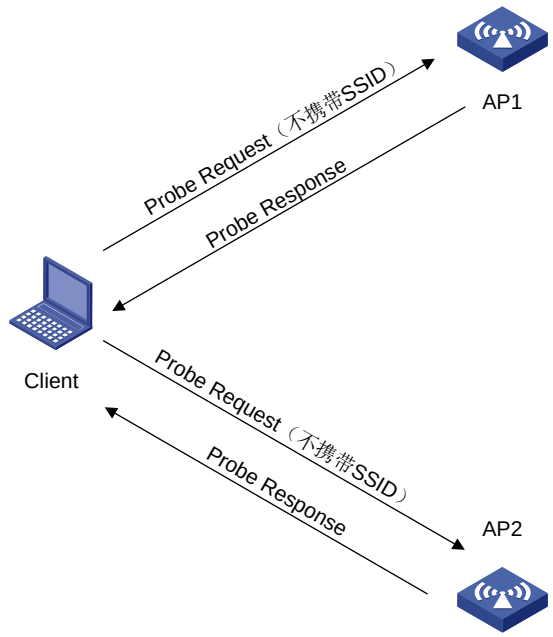
客户端在实际工作过程中，通常同时使用主动扫描和被动扫描获取周围的无线网络信息。

1. 主动扫描

主动扫描是指客户端在工作过程中，会定期地搜索周围的无线网络，也就是主动扫描周围的无线网络。客户端在扫描的时候，会主动广播 Probe Request 帧（探测请求帧），通过收到 Probe Response 帧（探测响应帧）获取无线网络信息。根据 Probe Request 帧是否携带 SSID（Service Set Identifier，服务集标识符），可以将主动扫描分为两种：

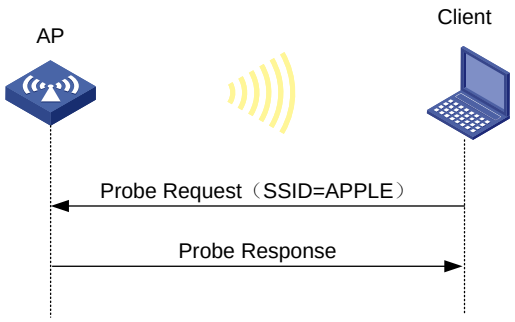
- 客户端发送 Probe Request 帧（Probe Request 中 SSID 为空，也就是 SSID 这个信息元素的长度为 0）：客户端会定期地在其支持的信道列表中，发送 Probe Request 帧扫描无线网络。当 AP 收到 Probe Request 帧后，会回复 Probe Response 帧通告可以提供服务的无线网络信息。客户端通过主动扫描，可以主动获知可使用的无线服务，之后客户端可以根据需要选择适当的无线网络接入。客户端主动扫描方式的过程如图 1-2 所示。

  图1-2 主动扫描过程（Probe Request 中 SSID 为空，也就是不携带任何 SSID 信息）



- 客户端发送 Probe Request 帧（携带指定的 SSID）：在客户端上配置了希望连接的无线网络或者客户端已经成功连接到一个无线网络的情况下，客户端会定期发送 Probe Request 帧（携带已经配置或者已经连接的无线网络的 SSID），能够提供指定 SSID 无线服务的 AP 接收到 Probe Request 帧后，会回复 Probe Response 帧。通过这种方法，客户端可以主动扫描指定的无线网络。这种客户端主动扫描方式的过程如图 1-3 所示。

  图1-3 主动扫描过程（Probe Request 携带指定为“APPLE”的 SSID）

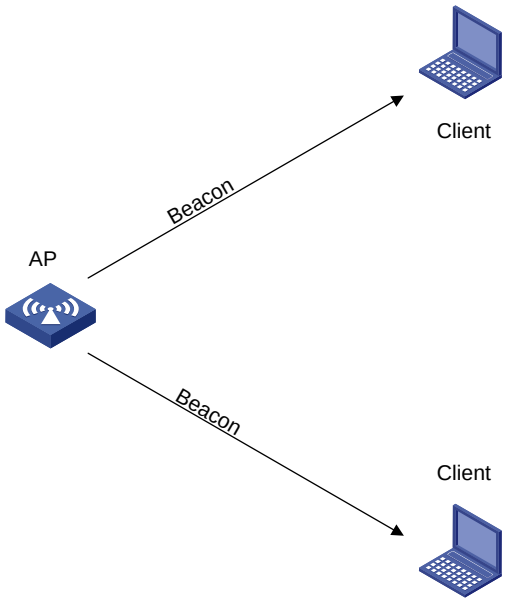


2. 被动扫描

被动扫描是指客户端通过侦听 AP 定期发送的 Beacon 帧（信标帧）发现周围的无线网络。提供无线服务的 AP 设备都会周期性地广播发送 Beacon 帧，所以客户端可以定期在支持的信道列表监听

Beacon 帧获取周围的无线网络信息，从而接入 AP。当客户端需要节省电量时，可以使用被动扫描。被动扫描的过程如图 1-4 所示。

图1-4 被动扫描过程



1.1.3 关联

当客户端通过指定 SSID 选择无线网络，并通过 AP 链路认证后，就会立即向 AP 发送 Association Request 帧（关联请求帧），AP 会对 Association Request 帧携带的能力信息进行检测，最终确定该客户端支持的能力，并回复 Association Response 帧（关联响应帧）通知客户端链路是否关联成功。

1.2 WLAN客户端接入控制

WLAN 接入控制的主要目的为对用户接入网络和访问网络进行控制，WLAN 接入控制的方式有以下几种：

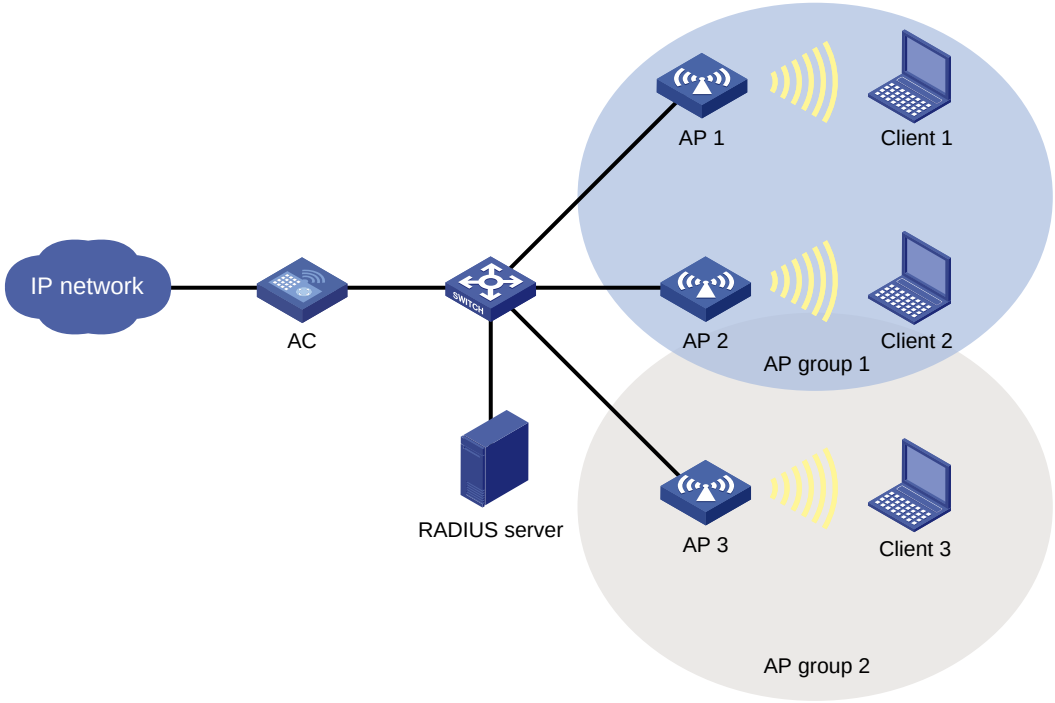
- 基于 AP 组的接入控制。
- 基于 SSID 的接入控制。
- 基于名单的接入控制。
- 基于 ACL 的接入控制。

1.2.1 基于 AP 组的接入控制

如图 1-5 所示，无线网络中有 3 个 AP，要求 Client 1 和 Client 2 只能通过 AP 1 或 AP 2 接入网络，Client 3 只能通过 AP 3 接入网络。为实现上述要求，将 AP 1 和 AP 2 添加进 AP 组 1 中，AP 3 添加进 AP 组 2 中。AC 上配置 Client 1 和 Client 2 对应的 User Profile 指定允许接入的 AP 组为 AP 组 1，Client 3 对应的 User Profile 指定允许接入的 AP 组为 AP 组 2。当 Client 1、Client 2 和 Client 3 准备接入网络并通过身份认证后，认证服务器会将与用户账户绑定的 User Profile 名称下发给 AC，

AC 根据指定 User Profile 里配置的内容查看客户端关联的 AP 是否在允许接入的 AP 组中，如果客户端关联的 AP 在允许接入的 AP 组中，客户端成功上线，否则上线失败。

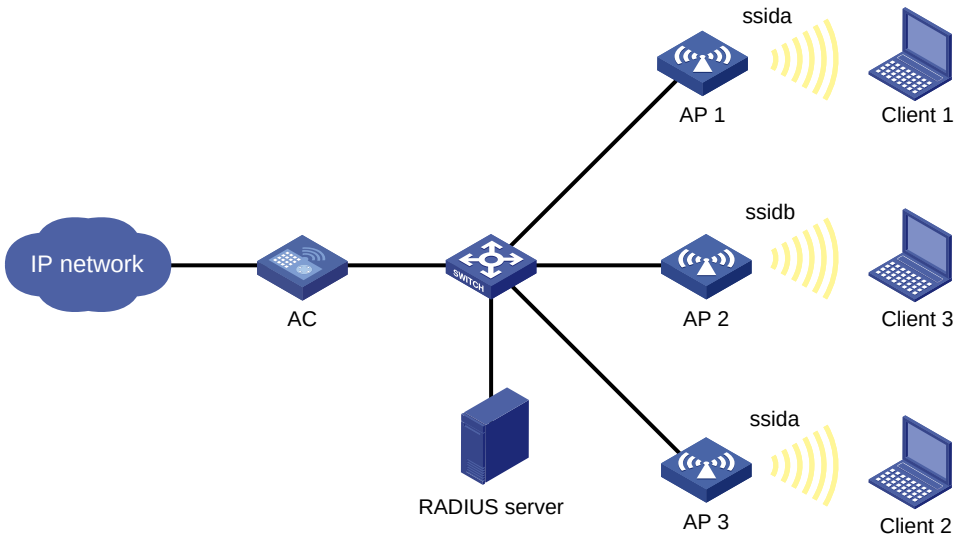
图1-5 基于 AP 组的接入控制组网应用



1.2.2 基于 SSID 的接入控制

如图 1-6 所示，无线网络中有 3 个 AP，要求 Client 1 和 Client 2 只能接入的 SSID 名称为 ssida 的无线服务，Client 3 只能接入的 SSID 名称为 ssidb 的无线服务。为实现上述要求，AC 上配置 Client 1 和 Client 2 对应的 User Profile 指定允许接入的 SSID 名称为 ssida，Client 3 对应的 User Profile 指定允许接入的 SSID 名称为 ssidb。当 Client 1、Client 2 和 Client 3 准备接入网络并通过身份认证后，认证服务器会将与用户账户绑定的 User Profile 名称下发给 AC，AC 根据指定 User Profile 里配置的内容查看客户端关联的 SSID 是否为允许接入的 SSID，如果客户端关联的 SSID 为指定允许接入的 SSID，客户端成功上线，否则上线失败。

图1-6 基于 SSID 的接入控制组网应用



1.2.3 基于名单的接入控制

无线网络很容易受到各种网络威胁的影响，非法设备对于无线网络来说是一个很严重的威胁，因此需要对客户端的接入进行控制。通过黑名单和白名单功能来过滤客户端，对客户端进行控制，防止非法客户端接入无线网络，可以有效的保护企业网络不被非法设备访问，从而保证无线网络的安全。

1. 白名单

白名单定义了允许接入无线网络的客户端 MAC 地址表项，不在白名单中的客户端不允许接入。白名单表项只能手工添加和删除。

2. 黑名单

黑名单定义了禁止接入无线网络的客户端 MAC 地址表项，在黑名单中的客户端不允许接入。黑名单分为静态黑名单和动态黑名单，以下分别介绍。

- 静态黑名单

  静态添加、删除表项的黑名单称为静态黑名单，当无线网络明确拒绝某些客户端接入时，可以将这些客户端加入静态黑名单。

- 动态黑名单

  动态添加、删除表项的黑名单称为动态黑名单。在配置了对非法设备进行反制、无线客户端二次接入认证等场景下，设备会将明确拒绝接入的客户端 MAC 地址加入到动态黑名单，当动态黑名单表项到达老化超时时间后，删除该表项。基于 AC 生效的动态黑名单会对所有与 AC 相连的 AP 生效，基于 AP 生效的动态黑名单仅对客户端接入的 AP 生效。有关反制功能的详细介绍，请参见“WLAN 安全配置指导”中的“WIPS”。

3. 客户端过滤机制

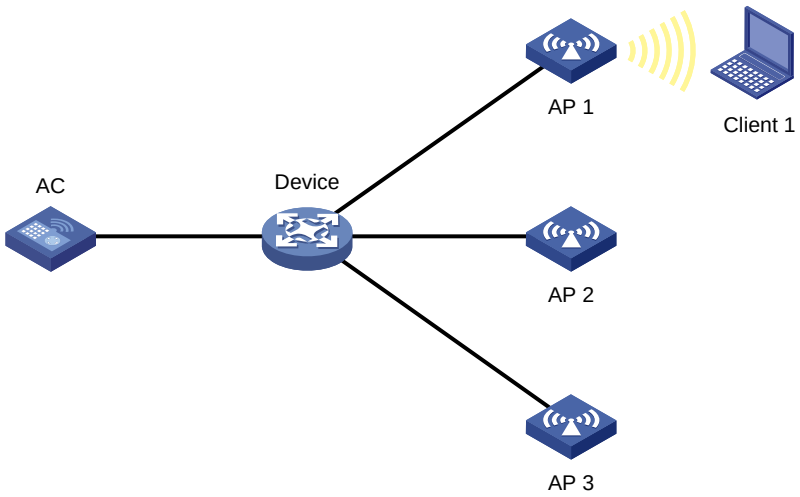
当收到客户端关联请求报文或 AP 向 AC 发送的 Add mobile 报文时，无线设备将使用白名单和黑名单对客户端的 MAC 地址进行过滤。以图 1-7 为例，具体的过滤机制如下：

(1) 当 AC 上存在白名单时，AC 将判断 Client 1 的 MAC 地址是否在白名单中，如果在白名单中，则允许客户端从任意一个 AP 接入无线网络，如果 Client 1 不在白名单中，则拒绝 Client 1 从任何一个 AP 接入。

(2) 当 AC 上不存在白名单时，AC 则判断 Client 1 的 MAC 地址是否在静态黑名单中，若 Client 1 在静态黑名单中则拒绝 Client 1 从任何一个 AP 接入无线网络。

(3) 当 AC 上不存在白名单且 Client 1 的 MAC 地址不在静态黑名单中时，为 Client 1 配置了二次接入认证时间间隔或者 AP 收到 Client 1 的攻击报文：如果配置了动态黑名单基于 AP 生效，则 AC 会将 Client 1 的 MAC 地址添加到动态黑名单中，并仅拒绝 Client 1 从 AP 1 上接入无线网络，但仍允许 Client 1 从 AP 2 或 AP 3 接入无线网络；如果配置了动态黑名单基于 AC 生效，则拒绝 Client 1 从任何一个 AP 接入无线网络。

图1-7 客户端过滤机制组网图



1.2.4 基于 ACL 的接入控制

基于ACL的接入控制是指，设备根据指定ACL中配置的规则对新接入的无线客户端进行接入控制。当无线客户端接入无线网络时，设备通过判断无线客户端 MAC 地址与指定的 ACL 规则的匹配情况对客户端进行过滤，具体的过滤机制如下：

- 如果匹配上某 permit 规则，则允许无线客户端接入无线网络；
- 如果匹配上某 deny 规则，则拒绝无线客户端接入无线网络；
- 如果未匹配上任何规则，则拒绝其接入。

1.3 访客隧道

1.3.1 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	说明
WX2500H-WiNet系列	WX2510H-PWR-WiNet WX2560H-WiNet	支持

产品系列	产品型号	说明
WX3500H-WiNet系列	WX3508H-WiNet	支持
WAC系列	WAC380-30 WAC380-60 WAC380-90 WAC380-120 WAC381	不支持
WX2500H-LI系列	WX2540H-LI WX2560H-LI	支持
WX3500H-LI系列	WX3510H-LI WX3520H-LI	支持

1.3.2 访客隧道简介

无线网络在提供内部用户接入的同时，还需要为访客用户提供无线接入，而访客数据可能会给网络带来潜在的安全威胁。在这种情况下，可以使用访客隧道功能，将访客的所有数据通过访客隧道重定向到企业的外网，在保证访客用户能够接入无线网络的同时，也能保障内网数据的安全。

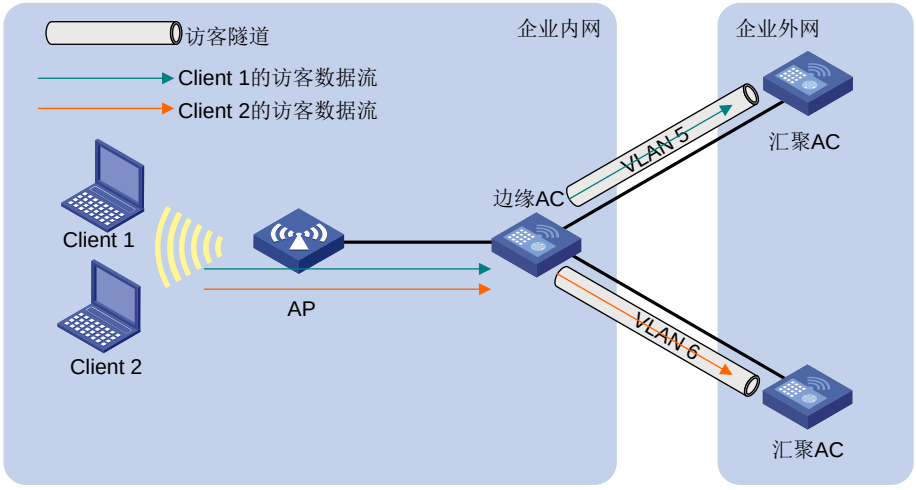
访客隧道建立在边缘 AC 和汇聚 AC 之间。其中边缘 AC 位于用户内部网络中，为内部用户和访客用户提供接入和认证；汇聚 AC 位于外部网络，处理访客用户的数据流量。访客用户会从指定的访客 VLAN 上线，其数据流量则从访客隧道的接口转发至汇聚 AC，实现访客数据与内网数据隔离，同时可以通过配置 IKE 协商方式生成 IPSec SA 的 IPv4 IPSec 隧道实现访客隧道的加密。

访客隧道支持 NAT 穿越功能，即当边缘 AC 和汇聚 AC 之间存在 NAT 设备时，AC 之间能够建立访客隧道。

1.3.3 访客隧道建立过程

在边缘 AC 和汇聚 AC 上完成访客隧道的相关配置后，边缘 AC 会向汇聚 AC 发送用于建立访客隧道的保活请求报文，当边缘 AC 收到保活回应报文后，访客隧道建立成功。

图1-8 访客隧道组网图



1.4 WLAN接入配置限制和指导

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。

1.5 WLAN接入配置任务简介

WLAN 接入配置任务如下：

(1) （可选）配置区域码

- 配置 AP 的区域码
- 配置 Beacon 帧和 Probe Response 帧携带区域码功能

(2) 配置无线服务模板

- 创建无线服务模板
- （可选）配置描述信息
- 配置 SSID
- （可选）配置无线服务模板允许关联的最大客户端数目
- 使能无线服务模板
- 绑定无线服务模板
- （可选）配置 AP 不继承 AP 组下绑定的指定无线服务模板

(3) （可选）配置客户端数据转发功能

- 配置客户端数据报文转发位置
- 开启客户端数据报文转发功能

- 配置客户端数据报文在 CAPWAP 隧道中的封装格式
- 配置对未知客户端数据报文处理方式

(4) （可选）配置客户端管理功能
- 配置客户端关联位置
- 开启快速关联功能
- 配置接收客户端信息的 Web 服务器信息
- 配置客户端上线日志的格式
- 配置客户端的 VLAN 分配方式
- 配置客户端优先使用授权 VLAN
- 关闭仅本地认证无线客户端信息上报成功才允许客户端上线功能
- 配置客户端 Cache 老化时间
- 配置客户端二次接入认证的时间间隔
- 配置无线客户端区别计费功能
- 开启网络侧设备的漫游增强功能

(5) （可选）配置客户端维护功能
- 配置客户端空闲时间
- 配置客户端保活功能
- 对客户端进行无线链路质量测量
- 配置 AP 上报无线客户端统计信息功能
- 配置网络接入服务器标识
- 配置 NAS-Port-Type
- 配置客户端关联 AP 的优化参数值
- 配置 iMC 服务器的 IP 地址和端口号

(6) （可选）配置 VIP 客户端功能
- 配置 VIP 客户端监控功能
- 配置非 VIP 客户端限速功能

(7) （可选）配置无线转发策略

(8) （可选）配置访客隧道功能

(9) （可选）配置客户端接入控制功能
- 配置允许用户接入的 AP 组
- 配置允许用户接入的 SSID 名称
- 配置白名单
- 配置静态黑名单
- 配置动态黑名单
- 配置基于 ACL 的接入控制

(10) （可选）配置 AP 不回应客户端广播 Probe request 报文

(11) （可选）开启告警功能

1.6 配置区域码

1.6.1 配置 AP 的区域码

1. 功能简介

区域码决定了射频可以使用的工作频段、信道、发射功率级别等。在配置 WLAN 设备时，必须正确地设置区域码，以确保不违反当地的管制规定。为了防止区域码的修改导致射频的工作频段、信道等与所在国家或地区的管制要求冲突，可以开启区域码锁定功能。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 AP 视图、AP 组视图、全局配置视图、AP 预配置视图或 AP 组预配置视图。

- 进入 AP 视图。

  wlan ap *ap-name*

- 进入 AP 组视图。

  wlan ap-group *group-name*

- 进入全局配置视图。

  wlan global-configuration

- 请依次执行以下命令进入 AP 预配置视图。

  wlan ap *ap-name*

  provision

- 请依次执行以下命令进入 AP 组预配置视图。

  wlan ap-group *group-name*

  provision

(3) 配置区域码。

region-code *code*

缺省情况下：

AP 视图：AP 组有配置的情况下，继承 AP 组配置；AP 组无配置的情况下，继承全局配置。

AP 组视图：继承全局配置。

全局配置视图：区域码为 CN。

AP 预配置视图：继承 AP 组预配置。

AP 组预配置视图：未配置 AP 使用的区域码。

(4) （可选）开启区域码锁定功能。

region-code-lock enable

缺省情况下：

AP 视图：AP 组有配置的情况下，继承 AP 组配置；AP 组无配置的情况下，继承全局配置。

AP 组视图：继承全局配置。

全局配置视图：区域码锁定功能处于关闭状态。

1.6.2 配置 Beacon 帧和 Probe Response 帧携带区域码功能

1. 功能简介

环境标识主要用来标记 AP 是室内 AP 还是室外 AP。

2. 配置限制和指导

同一 AP 的不同 Radio 下需要绑定具有相同环境标记的无线服务模板。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建无线服务模板。

wlan service-template *service-template-name*

(3) 配置 Beacon 帧和 Probe Response 帧携带区域码功能。

region-code-ie { **disable** | **enable** { **any** | **indoor** | **outdoor** } }

缺省情况下，Beacon 帧和 Probe Response 帧中携带区域码信息并且无环境标记。

1.7 配置无线服务模板

1.7.1 创建无线服务模板

1. 功能简介

无线服务模板即一类无线服务属性的集合，如无线网络的 SSID、认证方式（开放系统认证或者共享密钥认证）等。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建无线服务模板。

wlan service-template *service-template-name*

(3) （可选）配置无线客户端从指定无线服务模板上线后所属的 VLAN。

vlan *vlan-id*

缺省情况下，无线客户端从指定无线服务模板上线后将被加入到 VLAN 1。

1.7.2 配置描述信息

(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) 配置无线服务模板的描述信息。

description *text*

缺省情况下，未配置无线服务模板的描述信息。

1.7.3 配置 SSID

1. 功能简介

AP 将 SSID 置于 Beacon 帧中向外广播发送。若 BSS（Basic Service Set，基本服务集）的客户端数量已达到上限或 BSS 一段时间内不可用即客户端不能上线，不希望其它客户端上线，则可以配置 SSID 隐藏。若配置了 SSID 隐藏，AP 不将 SSID 置于 Beacon 帧中，还可以借此保护网络免遭攻击。为了进一步保护无线网络，AP 对于广播 Probe Request 帧也不会回复。此时客户端若想连接此 BSS，则需要手工指定该 SSID，这时客户端会直接向该 AP 发送认证及关联报文连接该 BSS。

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) 配置 SSID。

ssid *ssid-name*

缺省情况下，未配置 SSID。

(4) （可选）配置 SSID 隐藏。

beacon ssid-hide

缺省情况下，信标帧不隐藏 SSID。

1.7.4 配置无线服务模板允许关联的最大客户端数目

1. 功能简介

配置无线服务模板上允许关联的最大客户端数目，可以防止无线服务模板上由于关联的客户端数量过多而过载。当无线服务模板上关联的客户端数达到允许关联的最大客户端数目，将不再接受新的客户端关联且 SSID 会自动隐藏。

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) 配置无线服务模板允许关联的最大客户端数目。

client max-count *max-number*

缺省情况下，不限制无线服务模板允许关联的最大客户端数目。

1.7.5 使能无线服务模板

(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) 开启无线服务模板。

service-template enable

缺省情况下，无线服务模板处于关闭状态。

1.7.6 绑定无线服务模板

1. 功能简介

无线服务模板跟 AP 的 Radio 存在多对多的映射关系，将无线服务模板绑定在某个 AP 的射频上，AP 会根据射频上绑定的无线服务模板的无线服务属性创建无线服务 BSS。BSS 是提供无线服务的基本单元。在一个 BSS 的服务区域内（这个区域是指射频信号覆盖的范围），客户端能够相互通信。

绑定无线服务模板时，可以进行如下配置：

- 可以为该 BSS 指定一个 VLAN 组，该 BSS 下连接的客户端会被均衡地分配在 VLAN 组的所有 VLAN 中，既能将客户端划分在不同广播域中，又能充分利用不连续的地址段为客户端分配 IP 地址。
- 可以绑定 NAS-Port-ID（Network Access Server Port Identifier，网络接入服务器端口标识）和 NAS-ID（Network Access Server Identifier，网络接入服务器标识），用于网络服务提供商标识客户端的接入位置，区分流量来源。按照网络服务提供者的标准，不同的 NAS-Port-ID 对应不同的位置信息。
- 可以配置 SSID 隐藏。

2. 配置限制和指导

射频能绑定的最大无线服务模板的个数为 16 个。

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) 绑定无线服务模板。

service-template *service-template-name* [**vlan** *vlan-id1* [*vlan-id2*] | **vlan-group** *vlan-group-name*] [**ssid-hide**] [**nas-port-id** *nas-port-id*] [**nas-id** *nas-id*]

缺省情况下：

Radio 视图：继承 AP 组 Radio 配置。

AP 组 Radio 视图：未绑定无线服务模板。

有关 *vlan-id2* 参数的支持情况，请参见命令手册中对应描述。

1.7.7 配置 AP 不继承 AP 组下绑定的指定无线服务模板

1. 功能简介

AP 会继承 AP 组下同型号 AP 对应的射频下绑定的服务模板，同时创建无线服务 BSS。如果 AP 不需要或不需要全部继承 AP 组下绑定的无线服务模板，通过配置 AP 不继承 AP 组下绑定的指定无线服务模板，不对指定的无线服务模板进行继承。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 AP 视图。

wlan ap *ap-name*

(3) 进入 Radio 视图。

radio *radio-id*

(4) 配置 AP 不继承 AP 组下绑定的指定无线服务模板。

inherit exclude service-template *service-template-name*

缺省情况下，AP 继承 AP 组下绑定的无线服务模板。

1.8 配置客户端数据转发功能

1.8.1 配置客户端数据报文转发位置

1. 功能简介

可以在 AC 上将客户端数据报文转发位置配置在 AC 或者 AP 上。

- 将数据报文转发位置配置在 AC 上时，为集中式转发，客户端的数据流量由 AP 通过 CAPWAP 隧道透传到 AC，由 AC 转发数据报文。
- 将数据报文转发位置配置在 AP 上时，为本地转发，客户端的数据流量直接由 AP 进行转发。将转发位置配置在 AP 上缓解了 AC 的数据转发压力。
- 将转发位置配置在 AP 上时，可以指定 VLAN，即只有处于指定 VLAN 的客户端，在 AP 上转发其数据流量。

2. 配置限制和指导

若配置客户端数据报文转发位置在 AC 上，则需要保证客户端数据报文转发功能处于开启状态，否则配置不生效。

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) 配置客户端数据报文转发位置。

client forwarding-location { **ac** | **ap** [**vlan** { *vlan-start* [**to** *vlan-end*] }] }

缺省情况下，客户端数据报文转发位置请参见命令参考手册。

1.8.2 开启客户端数据报文转发功能

1. 功能简介

在分层 AC 架构下，如果客户端数据报文转发位置在 AC（Central AC 或 Local AC）上，则建议在 Central AC 上关闭客户端数据报文转发功能，Local AC 上开启此功能。当 AP 与管理员所指定的 Local AC 关联时，由 Local AC 转发客户端报文。如果指定的 Local AC 发生故障，AP 将关联到 Central AC 上，由于 Central AC 上的客户端数据报文转发功能处于关闭状态，客户端数据报文的转发位置将自动迁移到 AP 上，从而保障 Central AC 对整个无线网络的管理性能。

有关分层 AC 的配置请参见“WLAN 高级功能配置指导”中的“分层 AC”。

2. 配置限制和指导

若指定了客户端数据报文转发位置在 AC 上，则必须开启此功能才能使得 AC 能够转发客户端数据报文；若指定了客户端数据报文转发位置在 AP 上，则此功能无效。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 开启客户端数据报文转发功能。

wlan client forwarding enable

缺省情况下，客户端数据报文转发功能处于开启状态。

1.8.3 配置客户端数据报文在 CAPWAP 隧道中的封装格式

1. 功能简介

集中式转发架构下，客户端的数据报文由 AP 通过 CAPWAP 隧道透传到 AC。可以配置客户端数据报文封装在 CAPWAP 隧道中的格式为 802.3 或 802.11 格式，建议将客户端数据报文封装在 CAPWAP 中的格式为 802.3 格式，AC 在收到客户端报文后不需要进行报文格式转换。

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) 配置客户端数据报文在 CAPWAP 隧道中的封装格式。

client frame-format { **dot3** | **dot11** }

缺省情况下，客户端数据报文在 CAPWAP 隧道中的封装格式为 802.3 格式。

1.8.4 配置对未知客户端数据报文处理方式

1. 功能简介

通过配置对未知客户端数据报文处理方式，可以选择设备在收到未知客户端发送的数据报文后，仅丢弃客户端发送的数据报文不作处理，或丢弃客户端发送的数据报文并向客户端发送解除认证报文通知客户端断开连接。

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) 配置对未知客户端数据报文处理方式。

unknown-client [**deauthenticate** | **drop**]

缺省情况下，丢弃未知客户端发送的数据报文并向客户端发送解除认证报文。

1.9 配置客户端管理功能

1.9.1 配置客户端关联位置

1. 功能简介

客户端关联位置在 AC 上时，客户端与 AP 关联的过程将由 AC 处理，管理报文通过 CAPWAP 隧道透传到 AC。选择客户端关联位置在 AC 上具有安全和管理上的优势，但是当 AC 与 AP 之间的网络复杂，由于管理报文到达 AC 所需时间较长影响到关联过程时，建议将客户端关联位置配置在 AP 上，直接由 AP 处理客户端的关联过程。

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) 配置客户端关联位置。

client association-location { **ac** | **ap** }

缺省情况下，客户端的关联位置在 AC 上。

1.9.2 开启快速关联功能

1. 功能简介

如果 WLAN 环境中启动了负载均衡和频谱导航，客户端关联 AP 的效率将受到影响。对于不需要负载均衡和频谱导航功能或注重低延迟的网络服务，可以在无线服务模板下开启快速关联功能。无线服务模板开启快速关联功能后，即使 AP 上启动了负载均衡和频谱导航功能，也不会对该无线服务模板下接入的无线客户端进行频谱导航和负载均衡计算，从而让客户端可以快速的关联到 AP 上。

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) 开启快速关联功能。

quick-association enable

缺省情况下，快速关联功能处于关闭状态。

1.9.3 配置接收客户端信息的 Web 服务器信息

1. 功能简介

设备支持与特定第三方厂商的 Web 服务器通过 HTTP 协议传输客户端信息。配置 Web 服务器信息后，设备将与 Web 服务器建立 HTTP 连接，将关联客户端的信息（如客户端 MAC 地址、接入 AP 的 MAC 及接入时间等信息）发送给 Web 服务器，由服务器进行存储并由用户进行查看。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置接收客户端信息的 Web 服务器的域名和端口号。

wlan web-server host *host-name* **port** *port-number*

缺省情况下，未配置接收客户端信息的 Web 服务器的域名和端口号。

(3) 指定接收客户端信息的 Web 服务器的路径。

wlan web-server api-path *path*

缺省情况下，未指定接收客户端信息的 Web 服务器的路径。

(4) （可选）配置设备一次向 Web 服务器上报客户端信息的最大数目。

wlan web-server max-client-entry *number*

缺省情况下，设备一次向 Web 服务器上报客户端信息的最大数目为 10。

1.9.4 配置客户端上线日志的格式

1. 功能简介

客户端上线时，设备会自动生成客户端上线日志来记录该事件。客户端上线日志的格式有两种，格式不同，记录的内容不同。

- H3C 格式：日志内容为客户端上线的 AP 名称、Radio ID、客户端 MAC 地址、关联的 SSID、BSSID 及客户端的上线状态。
- normal 格式：日志内容为客户端上线的 AP 的 MAC 地址、AP 名称、客户端 IP 地址、客户端 MAC 地址、关联的 SSID 及 BSSID。
- sangfor 格式：日志内容为客户端上线的 AP 的 MAC 地址、客户端 IP 地址和客户端 MAC 地址。

缺省情况下，客户端上线时，设备会自动生成 H3C 格式的客户端上线日志。配置本功能后，设备在生成 H3C 格式日志的同时，还会生成 normal 格式或者 sangfor 格式的客户端上线日志。所有格式的客户端上线日志均会发送给设备的信息中心模块，由信息中心模块决定日志最终的输出方向。有关信息中心的详细介绍，请参见“设备管理配置指导”中的“信息中心”。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置客户端上线日志的格式。

customlog format wlan { **normal** | **sangfor** }

缺省情况下，仅输出 H3C 格式的客户端上线日志。

1.9.5 配置客户端的 VLAN 分配方式

1. 功能简介

客户端首次上线时，AP 会为动态分配方式下的客户端随机分配无线服务模板绑定 Radio 时指定的 VLAN 组内的一个 VLAN，根据客户端的 MAC 地址为静态分配、静态兼容分配方式下的客户端分配 VLAN。客户端再次上线时被分配的 VLAN 将由配置的 VLAN 分配方式决定：

- 静态分配方式下，直接继承上次 VLAN 组分配的 VLAN。若客户端的 IP 地址在租约内，仍为客户端分配同一个 IP 地址。采用该分配方式，可以减少 IP 地址的消耗。
- 动态分配方式下，VLAN 组再次随机为客户端分配 VLAN。采用该分配方式，客户端会被均衡地分配在 VLAN 组的所有 VLAN 中。
- 静态兼容分配方式下，可以保证客户端在采用静态分配方式的 Comware V5 版本 AC 设备与 ComwareV7 版本的 AC 之间漫游时，被分配相同的 VLAN。

2. 配置限制和指导

当客户端的 VLAN 分配方式为 **static** 或 **static-compatible** 时，修改 VLAN 组内的 VLAN，会导致已在该 VLAN 上线的客户端再次上线时被分配到不同的 VLAN。

当配置客户端的 VLAN 分配方式为 **dynamic** 时，修改 VLAN 组内的 VLAN，仅对新上线的客户端生效。

客户端上线后，将客户端的 VLAN 分配方式从 **dynamic** 修改为 **static** 或 **static-compatible**，该客户端再次上线时被分配到的 VLAN 可能和前一次分配到的 VLAN 不同。

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) 配置客户端的 VLAN 分配方式。

client vlan-alloc { **dynamic** | **static** | **static-compatible** }

缺省情况下，客户端的 VLAN 分配方式为动态分配方式。

1.9.6 配置客户端优先使用授权 VLAN

1. 功能简介

客户端上线时，如果客户端进行漫游，由于授权 VLAN 的优先级高于漫游 VLAN，此时如果 iMC 安全策略服务器配置了安全策略，客户端执行了 iMC 安全策略中对其的限制操作进而触发安全告警时，iMC 安全策略服务器重新下发的用于隔离客户端的授权 VLAN 将生效。例如，iMC 安全策略服务器设置了一个安全策略，不允许使用客户端的计算器功能。如果打开计算器功能就会触发安全告警，iMC 安全策略服务器重新下发的授权 VLAN 将生效。

关闭本功能后，漫游 VLAN 的优先级将高于授权 VLAN 的优先级当 iMC 安全策略服务器对客户端下发授权 VLAN 时，授权 VLAN 不生效。

2. 配置限制和指导

AC 为客户端选择 VLAN 的优先级从高到低依次为：授权 VLAN（授权服务器下发的 VLAN 或者 iMC 安全策略服务器下发的 VLAN）、漫游 VLAN（漫游表项中记录的 VLAN）、初始 VLAN（无线服务模板绑定的 VLAN）。

在 AC 上配置客户端优先使用授权 VLAN 功能后，当客户端需要进行 AC 间漫游时，为了保障漫游功能的实现，漫游组内的其他 AC 均需要开启本功能。

该配置只对采用 802.1X 或 MAC 地址认证方式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) 进入无线服务模板视图。

wlan service-template *service-template-name*

(3) 配置客户端优先使用授权 VLAN。

client preferred-vlan authorized

缺省情况下，授权 VLAN 的优先级高于漫游 VLAN 的优先级。

1.9.7 关闭仅本地认证无线客户端信息上报成功才允许客户端上线功能

1. 功能简介

对于本地认证的无线客户端，客户端认证完成后，AP 会上报客户端信息给 AC，由 AC 创建客户端表项并通知 AP 允许客户端上线。若 CAPWAP 隧道异常，AP 将无法成功向 AC 上报客户端信息，导致客户端无法上线，且在 CAPWAP 隧道恢复正常之前，客户端会反复进行认证，尝试上线。

为避免客户端频繁进行认证，可关闭仅本地认证无线客户端信息上报成功才允许客户端上线功能，允许通过本地认证的客户端在 AP 上线，此时 AP 可以为客户端转发数据并提供接入功能。当 CAPWAP 隧道恢复正常后，AP 会同步已上线客户端信息给 AC。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入无线服务器模板视图。

wlan service-template *service-template-name*

(3) 关闭仅本地认证无线客户端信息上报成功才允许客户端上线功能。

undo client report-mandatory

缺省情况下，仅本地认证无线客户端信息上报成功才允许客户端上线功能处于开启状态。

1.9.8 配置客户端 Cache 老化时间

1. 功能简介

无线客户端 Cache 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 Cache 老化时间内再次成功关联 AP，则可继承 Cache 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 Cache。

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) 配置客户端 Cache 老化时间。

client cache aging-time *aging-time*

缺省情况下，无线客户端 Cache 的老化时间为 180 秒。

1.9.9 配置客户端二次接入认证的时间间隔

1. 功能简介

客户端二次接入认证的时间间隔是指客户端通过 802.1X 认证或 MAC 地址认证（包括通过 URL 重定向功能完成 MAC 地址认证）后，RADIUS 服务器强制客户端下线到再次对其进行认证的时间间隔。

配置了客户端二次接入认证的时间间隔之后，设备将已通过认证的客户端的 MAC 地址加入到动态黑名单中，并在指定的时间间隔内禁止客户端接入。通过此方式加入动态黑名单的 MAC 地址不受动态黑名单老化时间的影响。

如果在该时间间隔内使用 **reset wlan dynamic-blacklist** 命令清除动态黑名单，则设备将允许该客户端接入并进行认证。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置客户端二次接入认证的时间间隔。

wlan client reauthentication-period [*period-value*]

缺省情况下，客户端二次接入认证的时间间隔为 10 秒。

1.9.10 配置无线客户端区别计费功能

1. 功能简介

无线客户端区别计费功能是指，对无线客户端的上网流量基于不同的计费级别进行分别计费，该功能是通过对在线用户授权 User Profile，并在 User Profile 中指定计费级别的计费策略来实现的，具体机制如下：

- 客户端认证位置在 AC 上时，认证服务器会将客户端账户绑定的 User Profile 名称下发给 AC，由 AC 再将 User Profile 下发给 AP，AP 根据指定 User Profile 下应用的计费策略对客户端进行流量统计并将数据上报给 AC，AC 最终将数据上报给计费服务器进行计费。
- 客户端认证位置在 AP 上时，认证服务器会将客户端账户绑定的 User Profile 名称下发给 AP，AP 根据指定 User Profile 下应用的计费策略对客户端进行流量统计并将数据上报给计费服务器进行计费。

如果 User Profile 下没有应用计费策略，则采用 AAA 进行计费。

2. 配置限制和指导

同一计费策略下可以指定多个流量计费级别，可创建计费策略的个数为 4 个。

修改或删除 User Profile 下应用的计费策略后，再次认证或新认证上线的客户端将使用新的计费策略。

3. 配置准备

认证服务器上为无线客户端用户绑定了需要下发的 User Profile 名称。

4. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入计费策略视图。

wlan accounting-policy *policy-name*

(3) 指定需要进行计费的流量计费级别。

accounting-level *level* **acl** { *acl-number* | **ipv6** *ipv6-acl-number* }

缺省情况下，未指定需要进行计费的流量计费级别。

(4) 退回系统视图。

quit

(5) 进入 User Profile 视图。

user-profile *profile-name*

(6) 在 User Profile 下应用计费策略。

wlan apply accounting-policy *policy-name*

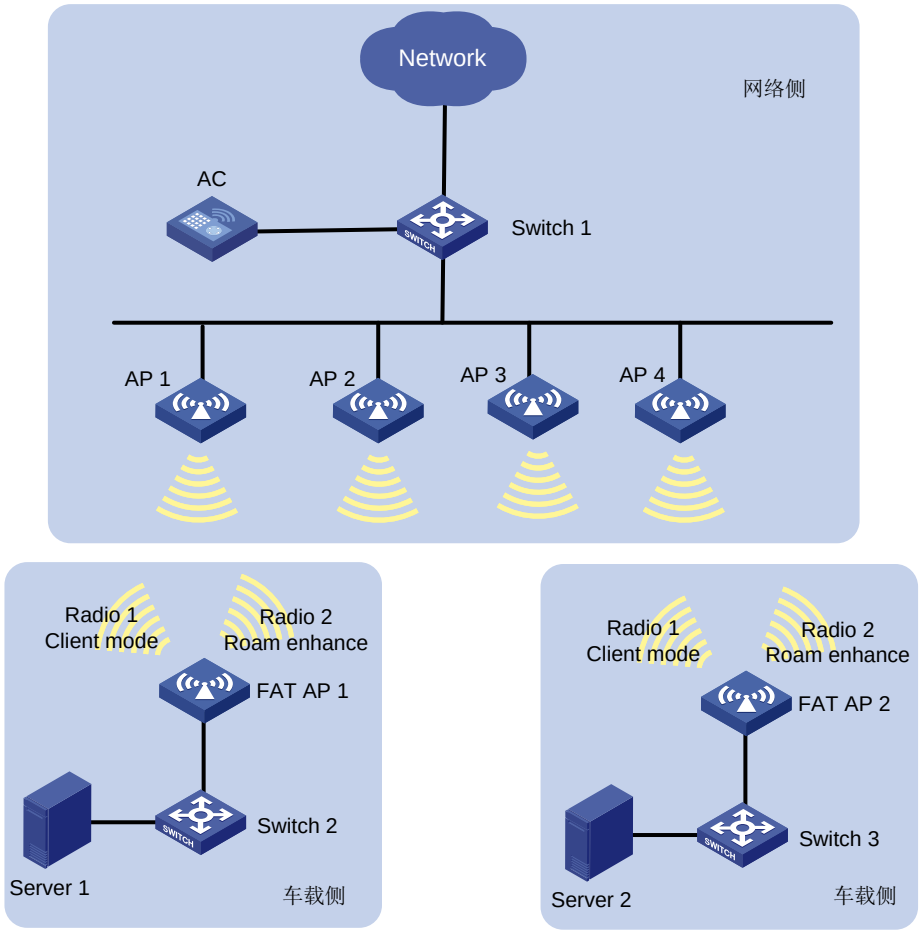
缺省情况下，User Profile 下未应用计费策略。

1.9.11 开启网络侧设备的漫游增强功能

1. 功能简介

如图 1-9 所示，在 AGV（Automated Guided Vehicle，自动导引运输车）无线网络中，网络系统由网络侧设备和车载侧设备两部分组成。网络侧设备为AC+FIT AP架构，FIT AP通过绑定了指定SSID对应的服务模板的 5G 射频为车载侧工作在 Client 模式的 FAT AP 提供无线接入服务，车载侧工作在 Client 模式的 FAT AP 为没有安装无线网卡的设备提供公共无线网卡功能。FAT AP 的 Client 模式的详细介绍请参见 FAT AP 产品“WLAN 接入配置指导”中的“Client 模式”。

图1-9 开启网络侧设备的漫游增强功能



2. 硬件适配关系

仅 WX3500H-LI 系列无线控制器支持本命令。

3. 配置限制和指导

本功能只能在网络侧 FIT AP 设备的 2.4G 射频下配置，多次执行本命令，最后一次执行的命令生效。

配置本功能时，绑定指定 SSID 对应的服务模板的 5G 射频不能工作在雷达信道。建议手工配置非雷达信道或者配置自动信道以及信道黑白名单。

仅当 AP 的 5G 射频绑定指定 SSID 对应的服务模板后，漫游增强功能才会生效。

AP 的 5G 射频最多只能绑定指定 SSID 对应的 5 个不同服务模板。

配置漫游增强功能后，绑定指定 SSID 的服务模板的 5G 射频不要用作业务扫描射频，否则会导致报文丢包数量增加，影响漫游效果。

使用本功能时，车载侧 Client 模式 FAT AP 和网络侧 AC 设备上都需要开启漫游增强功能。

4. 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) 开启漫游增强功能并指定漫游增强的 SSID。

roam-enhance ssid *ssid*

缺省情况下：

- Radio 视图：继承 AP 组 Radio 配置。
- AP 组 Radio 视图：漫游增强功能处于关闭状态。

1.10 配置客户端维护功能

1.10.1 配置客户端空闲时间

1. 功能简介

客户端空闲时间，是指 AP 与客户端成功连接后，客户端与 AP 无任何报文交互的状态的最大时间，当达到最大空闲时间时，AP 会自动与客户端断开连接。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 AP 视图或 AP 组视图。

- 进入 AP 视图。

  wlan ap *ap-name*

- 进入 AP 组视图。

  wlan ap-group *group-name*

(3) 配置客户端空闲时间。

client idle-timeout *interval*

缺省情况下：

AP 视图：继承 AP 组配置。

AP 组视图：AP 和客户端之间连接允许的最大空闲时间为 3600 秒。

1.10.2 配置客户端保活功能

1. 功能简介

开启客户端保活功能后，AP 每隔保活时间向客户端发送空数据报文，以确认其是否在线。若在三个保活时间内未收到客户端回应应答报文或数据报文，则 AP 断开与客户端的连接。若在此期间内收到，则认为客户端在线。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 AP 视图或 AP 组视图。

- 进入 AP 视图。

  wlan ap *ap-name*

- 进入 AP 组视图。

  wlan ap-group *group-name*

(3) 开启客户端保活功能。

client keep-alive enable

缺省情况下：

AP 视图：继承 AP 组配置。

AP 组视图：客户端保活功能处于关闭状态。

(4) （可选）配置客户端保活时间。

client keep-alive interval *value*

缺省情况下：

AP 视图：继承 AP 组配置。

AP 组视图：客户端保活时间为 300 秒。

1.10.3 对客户端进行无线链路质量测量

1. 功能简介

无线链路质量检测，即 AP 根据客户端上线时协商的速率集，以每个速率发送 5 个空数据报文进行链路质量检测。AP 根据客户端的响应报文可以获取 AP 客户端之间的无线链路质量信息，如信号强度、报文重传次数、RTT（Round-Trip Time，往返时间）等。

无线链路质量检测的超时时间为 10 秒，如果 AP 在超时时间内没有完成链路质量检测，将无法得到链路质量检测结果。

2. 配置步骤

请在用户视图下执行本命令，对客户端进行链路质量测量。

wlan link-test *mac-address*

1.10.4 配置 AP 上报无线客户端统计信息功能

1. 功能简介

为了对无线客户端的状态进行有效的监控，通过开启本功能，由 AP 周期性的向 AC 上报客户端统计信息。AC 接收到客户端统计信息后会对本地客户端表项进行更新，未与本地客户端表项匹配上的客户端将被强制下线。

当用户网络状况较差时，请关闭本功能，AP 会停止上报客户端统计信息且 AC 不会更新本地客户端表项，客户端正常在线。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 AP 视图或 AP 组视图。

- 进入 AP 视图。

  wlan ap *ap-name*

- 进入 AP 组视图。

  wlan ap-group *group-name*

(3) 配置 AP 向 AC 上报无线客户端统计信息功能。

client-statistics-report { disable | enable [interval *interval* **] }**

缺省情况下：

AP 视图：继承 AP 组配置。

AP 组视图：AP 向 AC 上报无线客户端统计信息功能处于开启状态。

1.10.5 配置网络接入服务器标识

1. 功能简介

NAS-ID、NAS-Port-ID 和 NAS-VLAN-ID（Network Access Server VLAN Identifier，网络接入服务器 VLAN 标识）主要用于网络服务提供商标识客户端的接入位置，区分流量来源。

2. 配置限制和指导

如果在配置无线服务模板时绑定了 NAS-ID/NAS-Port-ID，则优先使用无线服务模板绑定的 NAS-ID/NAS-Port-ID。

当使用某特定第三方厂商的 SAM（Security Accounting Management，安全审计管理）服务器作为 RADIUS 服务器时，需要在我司设备上配置 NAS-VLAN-ID，以便 SAM 服务器使用该 VLAN ID 定位客户端位置。

如果同时配置了 **wlan nas-port-id format** 和 **nas-port-id**，则以 **nas-port-id** 命令配置的为准。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置无线客户端的 NAS-Port-ID 属性的格式。

wlan nas-port-id format { **2** | **4** }

缺省情况下，NAS-Port-ID 的消息格式为格式 2。

(3) 进入 AP 视图、AP 组视图或全局配置视图。

- 进入 AP 视图。

  wlan ap *ap-name*

- 进入 AP 组视图。

  wlan ap-group *group-name*

- 进入全局配置视图。

  wlan global-configuration

(4) 配置网络接入服务器标识。

nas-id *nas-id*

缺省情况下：

AP 视图：AP 组有配置的情况下，继承 AP 组配置；AP 组无配置的情况下，继承全局配置。

AP 组视图：继承全局配置。

全局配置视图：未配置网络接入服务器标识。

(5) 配置网络接入服务器端口标识。

nas-port-id *nas-port-id*

缺省情况下：

AP 视图：AP 组有配置的情况下，继承 AP 组配置；AP 组无配置的情况下，继承全局配置。

AP 组视图：继承全局配置。

全局配置视图：未配置网络接入服务器标识。

(6) 配置网络接入服务器的 VLAN ID。

nas-vlan *vlan-id*

缺省情况下，未配置网络接入服务器的 VLAN ID，即 AC 向 RADIUS 服务器发送的请求认证报文中未携带 NAS-VLAN-ID 字段。

仅 AP 视图下支持配置此功能。

1.10.6 配置 NAS-Port-Type

1. 功能简介

RADIUS 标准属性 NAS-Port-Type 用于表示用户接入的端口类型。

缺省情况下，无线服务模板上有 802.1X 或者 MAC 地址认证用户上线时，设备向 RADIUS 服务器发送的 RADUIS 请求报文中填充的为自动获取到的 NAS-Port-Type 属性值 WLAN-IEEE 802.11。若无线服务模板配置了 NAS-Port-Type，则使用本命令配置的值填充该属性。

2. 配置限制和指导

本命令只能在无线服务模板关闭的状态下配置。

对于要使用 RADIUS 服务器进行 802.1X 或者 MAC 地址认证的用户，需要通过本命令将 RADIUS 请求报文的 NAT-Port-Type 类型配置为 RADIUS 服务器支持的类型。

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*

(3) 配置 NAS-Port-Type。

nas-port-type *value*

缺省情况下，设备发送的 RADIUS 请求报文中的 NAS-Port-Type 属性值为 19。

1.10.7 配置客户端关联 AP 的优化参数值

1. 功能简介

关联成功率是指客户端关联 AP 成功的次数占客户端关联 AP 的总次数的百分比。关联拥塞率是指在 AP 满载的情况下，客户端在关联 AP 过程中被拒绝的次数占关联 AP 的总次数的百分比。终端异常下线率是指终端异常断开连接的总次数占终端关联成功的总次数与当前在线用户总数之和的百分比。

配置本特性后，设备会重新对客户端关联 AP 的关联成功率、关联拥塞率以及终端异常下线率进行优化计算。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置客户端关联 AP 的关联成功率、关联拥塞率以及终端异常下线率的优化参数值。

wlan association optimization *value*

缺省情况下，客户端关联 AP 的关联成功率、关联拥塞率以及终端异常下线率的优化参数值为 0，即不对客户端关联 AP 的关联成功率、关联拥塞率以及终端异常下线率进行优化，采用实际值。

1.10.8 配置 iMC 服务器的 IP 地址和端口号

1. 功能简介

配置 iMC 服务器的 IP 地址和端口号后，设备可以将 AP 上下线、客户端上下线以及 Portal 认证用户上下线等消息同步到 iMC 服务器，用户可以在 iMC 业务软件上查看到相关信息。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置 iMC 服务器的 IP 地址和端口号。

wlan imc ip *ip-address* **port** *port-number*

缺省情况下，未配置 iMC 服务器的 IP 地址和端口号。

1.11 配置VIP客户端功能

1.11.1 配置 VIP 客户端监控功能

1. 功能简介

VIP 客户端组为被监控客户端的集合，用户可以通过绿洲平台 VIP 客户端监控页面查看添加到 VIP 客户端组中的上线客户端信息。

2. 配置限制和指导

最多可以添加 64 个客户端到 VIP 客户端组。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 VIP 客户端组，并进入 VIP 客户端组视图。

wlan vip-client-group

(3) 添加客户端到 VIP 客户端组。

client-mac *mac-address*

缺省情况下，VIP 客户端组中无客户端。

(4) （可选）配置 AP 向 AC 上报 VIP 客户端信息的时间间隔。

report-interval *interval*

缺省情况下，AP 向 AC 上报 VIP 客户端信息的时间间隔为 50 秒。

1.11.2 配置非 VIP 客户端限速功能

1. 功能简介

通过配置非 VIP 客户端的限速速率，当有 VIP 客户端在线时，VIP 客户端所在射频下的每个非 VIP 客户端的速率都会被限制为固定值；当某射频下的所有 VIP 客户端下线后，该射频下的非 VIP 客户端的速率限制会自动解除；如果某射频下一直没有 VIP 客户端上线，则该射频下的客户端速率不会被限制。

本功能配置的所有非 VIP 客户端的限速速率为固定值。

2. 配置限制和指导

可以同时指定出方向和入方向的速率限制。

如果同时配置了基于射频的客户端限速速率和非 VIP 客户端的限速速率，非 VIP 客户端的速率取两种配置的最小值，VIP 客户端速率不会被限制。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 VIP 客户端组，并进入 VIP 客户端组视图。

wlan vip-client-group

(3) 配置非 VIP 客户端的限速速率。

non-vip limit rate { **inbound** | **outbound** } **cir** *cir*

缺省情况下，未配置非 VIP 客户端的限速速率。

1.12 配置无线转发策略

1.12.1 配置限制和指导

配置无线转发策略，AC 和 AP 必须处于不同网段中。

当无线服务模板和 User Profile 下均应用无线转发策略时，设备优先使用 User Profile 下应用的无线转发策略对客户端数据进行处理。如果上线用户的 User Profile 下没有应用无线转发策略，则设备将使用无线服务模板下的无线转发策略处理客户端数据。

1.12.2 配置准备

应用无线转发策略前，请使用 **client-security authentication-location** 命令将无线用户的接入认证位置配置在 AC 上，此时无线转发策略才能生效。关于用户接入认证位置的介绍和配置，请参见“用户接入与认证配置指导”中的“WLAN 用户接入认证”。

1.12.3 创建无线转发策略

1. 功能简介

无线转发策略由一条或多条无线转发规则组成，每条无线转发规则中包含匹配报文特征的规则及采取的转发方式。匹配报文特征的规则可以为基本 ACL、高级 ACL 和二层 ACL，可选择的转发方式包括本地转发和集中转发。无线转发策略仅识别 ACL 规则中的匹配条件，不识别允许和拒绝操作，即只要是匹配条件的报文，无论在 ACL 规则中是被允许还是被拒绝，都会被按转发策略处理。

有关 ACL 的详细介绍，请参见“安全配置指导”中的“ACL”。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建无线转发策略，并进入无线转发策略视图。

wlan forwarding-policy *policy-name*

(3) 配置无线转发规则。

classifier acl { *acl-number* | **ipv6** *ipv6-acl-number* } **behavior** { **local** | **remote** }

重复执行该命令可以创建多条无线转发规则。

1.12.4 开启本地转发模式下的外网流量转发功能

1. 功能简介

本功能主要用于客户端需要访问外网，但客户端数据报文转发位置又在 AP 上的场景。开启本功能后，设备会将客户端数据报文中的目的地址替换成 AP 的 MAC 地址，再通过 NAT 地址转换功能，将客户端数据报文的源地址自动转换成和 AP 同网段的 IP 地址。完成以上配置后，客户端可以正常访问外网，否则，访问外网的报文将被 AP 丢弃。

2. 配置限制和指导

本功能需要与支持 NAT 功能的 AP 配合使用。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入无线转发策略视图。

wlan forwarding-policy *policy-name*

(3) 开启本地转发模式下的外网流量转发功能。

client behavior-local network-flow-forwarding enable

缺省情况下，本地转发模式下的外网流量转发功能处于关闭状态。

1.12.5 在无线服务模板下应用无线转发策略

(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) 在无线服务模板下应用无线转发策略。

client forwarding-policy-name *policy-name*

缺省情况下，没有应用无线转发策略。

应用无线转发策略后，请开启无线转发策略功能。

(4) 开启无线转发策略功能。

client forwarding-pollicy enable

缺省情况下，无线转发策略功能处于关闭状态。

1.12.6 在 User Profile 下应用无线转发策略

1. 功能简介

在 User Profile 下应用无线转发策略后，当客户端准备接入网络并通过身份认证后，认证服务器会将与客户端账户绑定的 User Profile 名称下发给 AC，AC 根据指定 User Profile 下应用的无线转发策略对客户端数据报文进行转发。

2. 配置限制和指导

修改或删除 User Profile 下应用的无线转发策略时，该配置会在客户端再次上线时生效。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 User Profile 视图。

user-profile *profile-name*

(3) 在 User Profile 下应用无线转发策略。

wlan client forwarding-policy-name *policy-name*

缺省情况下，没有应用无线转发策略。

应用无线转发策略后，请开启无线转发策略功能。

(4) 退回系统视图。

quit

(5) 进入服务模板视图。

wlan service-template *service-template-name*

(6) 开启无线转发策略功能。

client forwarding-pollicy enable

缺省情况下，无线转发策略功能处于关闭状态。

1.13 配置访客隧道功能

1.13.1 在边缘 AC 上配置汇聚 AC 信息

1. 功能简介

访客隧道成功建立后，边缘 AC 会周期性的向汇聚 AC 发送保活请求报文，如果在三个保活周期内未收到汇聚 AC 的保活回应报文，则删除与该汇聚 AC 建立的访客隧道。对于汇聚 AC，如果在向边缘 AC 发送保活回应报文之后的三个保活周期内未收到来自该边缘 AC 的保活请求报文，则会删除与其建立的访客隧道。

2. 配置限制和指导

已经配置为边缘 AC 的 AC 就不能再配置为汇聚 AC，如果要修改角色，请先恢复缺省情况，再进行配置。

删除边缘 AC 视图后，视图下的所有配置和所有已建立的访客隧道也会被删除。

每个边缘 AC 可以与汇聚 AC 建立多条访客隧道，每个访客隧道必须属于不同的 VLAN。

每个边缘 AC 可以与同一个汇聚 AC 建立多条隧道，但必须使用不同的源接口 IP 地址和该汇聚 AC 的不同接口 IP 地址建立访客隧道。

当配置的多个不同汇聚 AC 地址属于同一台 AC 时，汇聚 AC 使用接收到的第一个保活请求报文的 IP 地址与边缘 AC 建立隧道。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 指定当前 AC 为边缘 AC，并创建边缘 AC 视图。

wlan guest-tunnel edge-ac

缺省情况下，当前 AC 不是边缘 AC。

(3) 配置汇聚 AC 信息。

aggregation-ac ip *ipv4-address* **tunnel-source ip** *ipv4-address* **vlan** *vlan-id-list*

缺省情况下，未配置汇聚 AC 的信息。

(4) （可选）配置访客遂道保活请求报文的发送周期。

keep-alive interval *interval*

缺省情况下，保活请求报文的发送周期为 10 秒。

1.13.2 在汇聚 AC 上配置边缘 AC 信息

1. 功能简介

在汇聚 AC 上配置边缘 AC 地址和访客 VLAN 后，汇聚 AC 会等待边缘 AC 发起的保活请求报文，收到该报文之后，汇聚 AC 会检查报文中携带的源地址是否在其配置的边缘 AC 列表中，如果在列表中，汇聚 AC 会发送保活回应报文，访客隧道建立成功。如果不在列表中，汇聚 AC 会直接丢弃该报文。

2. 配置限制和指导

已经配置为汇聚 AC 的 AC 就不能再配置为边缘 AC，如果要修改角色，请先恢复缺省情况，再进行配置。

删除汇聚 AC 视图时，视图下的所有配置和所有已建立的访客隧道也会被删除。

每个边缘 AC 可以与汇聚 AC 建立多条访客隧道，每个访客隧道必须属于不同的 VLAN。

每个汇聚 AC 可以与同一个边缘 AC 建立多条隧道，但必须使用不同的源接口 IP 地址和该边缘 AC 的不同接口 IP 地址建立访客隧道。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 指定当前 AC 为汇聚 AC，并创建汇聚 AC 视图。

wlan guest-tunnel aggregation-ac

缺省情况下，当前 AC 不是汇聚 AC。

(3) 配置边缘 AC 信息。

edge-ac ip ipv4-address vlan *vlan-id-list*

缺省情况下，未配置边缘 AC 的信息。

1.13.3 开启访客隧道加密时的流量分发功能

1. 功能简介

开启本功能后，设备会先将访客隧道的流量分发到设备不同 CPU 上，然后通过 IPSec 进行加密，因为业务流量进行了分流，所以提高了 IPSec 隧道加密流量的转发性能。

2. 配置限制和指导

本功能当且仅当对访客隧道配置了 IPSec 加密的情况下需要开启。

本功能需要同时在边缘 AC 和对应的汇聚 AC 上开启或关闭。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入汇聚 AC 视图或者进入边缘 AC 视图。

wlan guest-tunnel { aggregation-ac | edge-ac }

(3) 开启访客隧道加密时的流量分发功能。

wlan guest-tunnel flow-distribute enable

缺省情况下，访客隧道加密功能处于关闭状态。

1.14 配置客户端接入控制功能

1.14.1 配置允许用户接入的 AP 组

1. 功能简介

通过配置允许用户接入的 AP 组，让用户只能够在指定 AP 组内的 AP 上接入，控制用户在无线网络中接入位置。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 User Profile 视图。

user-profile *profile-name*

(3) 配置允许用户接入的 AP 组。

wlan permit-ap-group *ap-group-name*

缺省情况下，未配置允许用户接入的 AP 组。

1.14.2 配置允许用户接入的 SSID 名称

1. 功能简介

在用户需要接入网络时，可通过指定允许用户接入的 SSID 控制用户只能在指定的 SSID 接入。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 User Profile 视图。

user-profile *profile-name*

(3) 配置 SSID 用户接入控制。

wlan permit-ssid *ssid-name*

缺省情况下，未配置允许用户接入的 SSID 名称。

1.14.3 配置白名单

1. 配置限制和指导

第一次配置白名单时，系统会提示用户是否解除与所有在线客户端的关联，如果选择解除关联，才能配置白名单，否则不能配置白名单。当删除白名单中所有客户端时，则不存在白名单。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置白名单。

wlan whitelist mac-address *mac-address*

1.14.4 配置静态黑名单

1. 配置限制和指导

同一 MAC 地址表项不能同时配置到白名单中和静态黑名单中。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置静态黑名单。

wlan static-blacklist mac-address *mac-address*

1.14.5 配置动态黑名单

1. 功能简介

当配置了客户端二次接入认证的时间间隔或者 AP 收到客户端的攻击报文时，AC 会将该客户端的 MAC 地址添加到动态黑名单中：

- 配置动态黑名单基于 AP 生效，AP 将拒绝该客户端的接入，但仍可以从 AC 下的其他 AP 接入。
- 配置动态黑名单基于 AC 生效，AC 下相连的所有 AP 都将拒绝该客户端接入。

动态黑名单表项具有一定的老化时间。当到达老化时间时，AC 会将 MAC 地址从动态黑名单中删除。

2. 配置限制和指导

在 AP 部署较密集的无线网络环境下，建议用户配置动态黑名单基于 AC 生效。

新配置的动态黑名单老化时间只对新加入动态黑名单的客户端生效。

若客户端同时存在于白名单和动态黑名单中时，则白名单生效。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置动态黑名单。请选择其中一项进行配置。

- 配置动态黑名单基于 AP 生效。

  wlan dynamic-blacklist active-on-ap

- 配置动态黑名单基于 AC 生效。

  undo wlan dynamic-blacklist active-on-ap

  缺省情况下，动态黑名单基于 AP 生效。

(3) （可选）配置动态黑名单表项的老化时间。

wlan dynamic-blacklist lifetime *lifetime*

缺省情况下，动态黑名单表项的老化时间为 300 秒。

1.14.6 配置基于 ACL 的接入控制

1. 配置限制与指导

基于 ACL 的接入控制的优先级高于基于名单的接入控制的优先级，建议两种接入控制单独使用。如果同时配置了两种接入控制，当设备上没有配置无线客户端访问控制规则时，按照基于名单的接入控制规则对无线客户端进行访问控制。

在 ACL 中配置 deny 规则来拒绝指定客户端接入时，请在 deny 规则之后配置允许所有客户端接入的 permit 规则，否则会导致所有客户端无法接入。

AP 视图下配置的优先级高于无线服务模板视图下的配置。

基于 ACL 的接入控制只匹配 source mac 地址二层 ACL 规则。

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或 AP 视图。

- 进入无线服务模板视图。

  wlan service-template *service-template-name*

- 进入 AP 视图。

  wlan ap *ap-name*

(3) 配置基于 ACL 的接入控制。

access-control acl *acl-number*

缺省情况下，未配置基于 ACL 的接入控制。

基于 ACL 的接入控制只能引用二层 ACL 规则。

1.15 配置AP不回应客户端广播Probe request报文

1. 功能简介

广播 Probe request 报文即报文中不携带无线服务的 SSID，AP 收到广播报文后，将 AP 提供的所有服务的信息封装在 Probe reponse 报文中，回应给客户端。可以配置不回应客户端的广播 Probe request 报文，可以减少 AP 回应的 Probe response 报文，并使发送携带 SSID 的 Probe request 报文的客户端更容易接入无线网络。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 AP 视图或 AP 组视图。

- 进入 AP 视图。

  wlan ap *ap-name*

- 进入 AP 组视图。

wlan ap-group *group-name*

(3) 配置 AP 不回应广播 Probe request 报文。

broadcast-probe reply disable

缺省情况下：

AP 视图：继承 AP 组配置。

AP 组视图：AP 回应广播 Probe request 报文。

1.16 开启告警功能

1. 功能简介

开启了告警功能之后，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) 开启告警功能。请至少选择其中一项进行配置。

- 开启客户端的告警功能。

  snmp-agent trap enable wlan client

- 开启客户端审计的告警功能。

  snmp-agent trap enable wlan client-audit

缺省情况下，客户端告警功能处于关闭状态。

1.17 开启无线客户端智能接入功能

1. 功能简介

开启无线客户端智能接入功能后，可以在仅创建无线服务模板或身份认证与密钥管理模式配置为 PSK 的情况下，自动将我司配套的无线客户端接入到无线网络。

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) 开启无线客户端智能接入功能。

client smart-access enable

缺省情况下，无线客户端智能接入功能处于关闭状态。

1.18 WLAN接入显示和维护

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 WLAN 接入的运行情况，通过查看显示信息验证配置效果。

在用户视图下执行 **reset** 命令可以清除动态黑名单或断开 AP 与客户端的连接。

表1-1 WLAN 接入显示和维护

操作	命令
显示AP上2.4GHz及5GHz频段的在线客户端数量	**display wlan ap all client-number**
显示AP的所有Radio接口下在线客户端数量和信道信息	**display wlan ap all radio client-number**
显示AP的区域码信息	**display wlan ap** { **all** | **name** *ap-name* } **region-code**
显示所有AP组内在线客户端数量	**display wlan ap-group all client-number**
显示黑名单	**display wlan blacklist** { **dynamic** | **static** }
显示BSS（Basic Service Set，基本服务集）信息	（独立运行模式） **display wlan bss** { **all** | **ap** *ap-name* | **bssid** *bssid* } [**verbose**] （IRF模式） **display wlan bss** { **all** | **ap** *ap-name* | **bssid** *bssid* } [**slot** *slot-number*] [**verbose**]
显示客户端的信息	**display wlan client** [**ap** *ap-name* [**radio** *radio-id*] | **mac-address** *mac-address* | **service-template** *service-template-name* | **frequency-band** { **2.4** | **5** }] [**verbose**]
显示客户端的IPv6地址信息	**display wlan client ipv6**
显示客户端在线时长	**display wlan client online-duration** [**ap** *ap-name*] [**verbose**]
显示客户端状态信息	**display wlan client status** [**mac-address** *mac-address*] [**verbose**]
显示无线转发策略信息	**display wlan forwarding-policy**
显示当前AC上的访客隧道信息	**display wlan guest-tunnel** { **all** | **ip** *ipv4-address* }
显示无线服务模板信息	**display wlan service-template** [*service-template-name*] [**verbose**]
查看无线客户端的统计信息	**display wlan statistics client** [**mac-address** *mac-address*]
查看客户端连接历史信息	**display wlan statistics connect-history** { **ap** { **all** | **name** *ap-name* } | **service-template** *service-template-name* }
查看无线服务模板的统计信息	**display wlan statistics service-template** *service-template-name*
显示AP向AC上报的VIP客户端的统计信息	**display wlan statistics vip-client**
显示白名单	**display wlan whitelist**

操作	命令
断开与客户端的连接	**reset wlan client** { **all** | **mac-address** *mac-address* }
清除动态黑名单	**reset wlan dynamic-blacklist** [**mac-address** *mac-address*]
删除访客隧道	**reset wlan guest-tunnel** { **all** | **ip** *ipv4-address* }
清除无线客户端的统计信息	**reset wlan statistics client** { **all** | **mac-address** *mac-address* }
清除无线服务模板的统计信息	**reset wlan statistics service-template** *service-template-name*

1.19 WLAN接入典型配置举例

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。

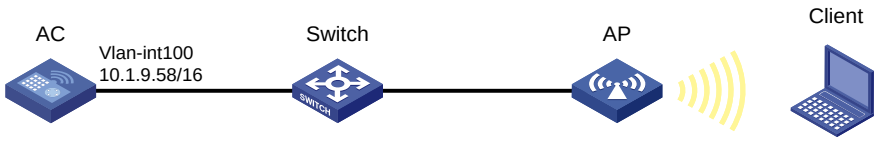
1.19.1 WLAN 接入配置举例

1. 组网需求

- AP 通过交换机与 AC 相连。在 Switch 上开启 DHCP server 功能，为 AP 和客户端分配 IP 地址。
- 使用手工输入序列号方式输入序列号。AP 提供 SSID 为 trade-off 的无线接入服务。

2. 组网图

图1-10 无线接入组网图



3. 配置步骤

(1) 配置 IP 地址

创建 VLAN 100，并配置 VLAN 100 接口的 IP 地址。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100]quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 10.1.9.58 16
```

(2) 创建手工 AP

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 WA4320i-ACN
[AC-wlan-ap-ap1] serial-id 219801A0CNC138011454
```

(3) 创建无线服务模板，并将无线服务模板绑定到 AP 的 Radio 接口。

配置无线服务模板 service1，配置 SSID 为 trade-off，配置客户端从无线服务模板 service1 上线后将被加入到 VLAN 100，并开启服务模版。

```
<AC> system-view
[AC] wlan service-template service1
[AC-wlan-st-service1] ssid trade-off
[AC-wlan-st-service1] vlan 100
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

配置射频，指定工作信道为 157。

```
[AC] wlan ap ap1
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] channel 157
```

将无线服务模板 service1 绑定到 Radio 1 接口。

```
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] service-template service1
```

4. 验证配置

(1) 配置完成后，在 AC 上执行 **display wlan service-template** 命令，可以看到所有已经创建的无线服务模板。无线服务模板 service1 的 SSID 为 trade-off，无线服务模板已经使能，其它配置项都使用缺省值。

```
[AC] display wlan service-template verbose
Service template name          : service1
Description                    : Not configured
SSID                           : trade-off
SSID-hide                      : Disabled
User-isolation                 : Disabled
Service template status        : Enabled
Maximum clients per BSS        : 64
Frame format                   : Dot3
Seamless roam status           : Disabled
Seamless roam RSSI threshold   : 50
Seamless roam RSSI gap         : 20
VLAN ID                        : 100
AKM mode                       : Not configured
Security IE                    : Not configured
Cipher suite                   : Not configured
TKIP countermeasure time       : 0 sec
PTK life time                  : 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
```

```
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                   : 1
Critical VLAN ID               : Not configured
802.1X handshake               : Enabled
802.1X handshake secure        : Disabled
802.1X domain                  : my-domain
MAC-auth domain                : Not configured
Max 802.1X users per BSS       : 4096
Max MAC-auth users per BSS     : 4096
802.1X re-authenticate         : Enabled
Authorization fail mode        : Online
Accounting fail mode           : Online
Authorization                  : Permitted
Key derivation                 : N/A
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
```

(2) MAC 地址为 0023-8933-223b 的客户端可以连接无线网络名称为 trade-off 的无线网络。在 AC 上执行 **display wlan client** 命令，可以看到所有连接成功的客户端。

```
[AC] display wlan client service-template service1
Total number of clients: 1

MAC address       Username   AP name    RID   IP address      VLAN
0023-8933-223b    N/A        ap1        1     3.0.0.3         100
```

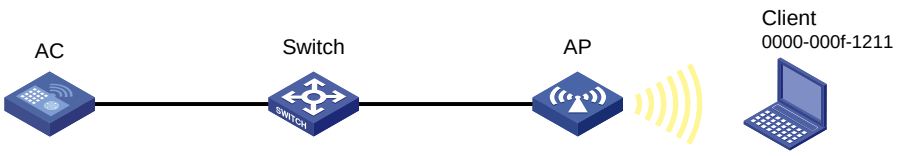
1.19.2 白名单配置举例

1. 组网需求

AC 和 AP 通过交换机连接，通过将客户端的 MAC 地址 0000-000f-1211 加入到白名单中，仅允许该客户端接入无线网络，拒绝其它客户端接入无线网络。

2. 组网图

图1-11 白名单配置组网图



3. 配置步骤

将客户端的 MAC 地址 0000-000f-1211 添加到白名单。

```
<AC> system-view
[AC] wlan whitelist mac-address 0000-000f-1211
```

4. 验证配置

配置完成后，在 AC 上执行 **display wlan whitelist** 命令，可以看到 AC 已经将客户端的 MAC 地址表项加入到白名单。

```
[AC] display wlan whitelist
Total number of clients: 1
 MAC addresses:
  0000-000f-1211
```

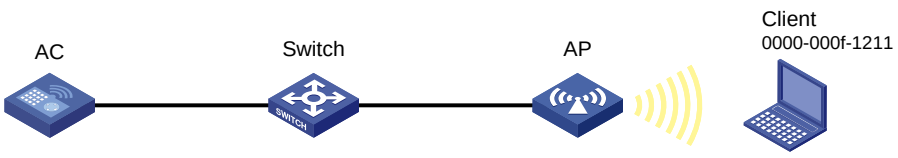
1.19.3 静态黑名单配置举例

1. 组网需求

AC 和 AP 通过交换机连接，客户端为已知非法客户端，通过将客户端的 MAC 地址 0000-000f-1211 加入到静态黑名单中，拒绝该客户端接入无线网络。

2. 组网图

图1-12 静态黑名单配置组网图



3. 配置步骤

将客户端的 MAC 地址 0000-000f-1211 添加到静态黑名单。

```
<AC> system-view
[AC] wlan static-blacklist mac-address 0000-000f-1211
```

4. 验证配置

配置完成后，在 AC 上执行 **display wlan blacklist static** 命令，可以看到 AC 已经将客户端的 MAC 地址表项加入到静态黑名单。

```
[AC] display wlan blacklist static
Total number of clients: 1
 MAC addresses:
 0000-000f-1211
```

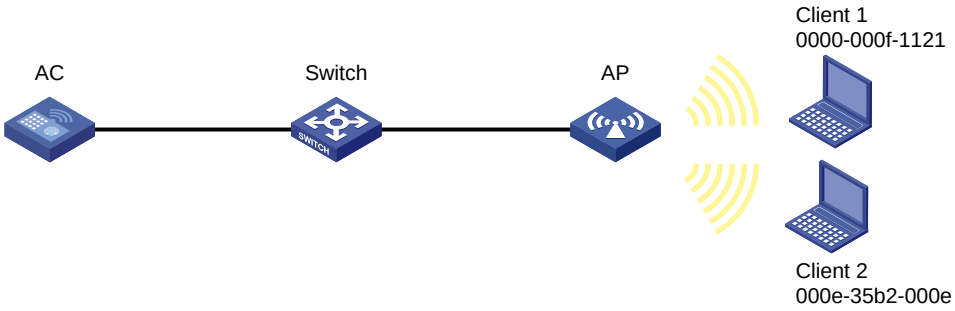
1.19.4 ACL 接入控制配置举例

1. 组网需求

AC 和 AP 通过交换机连接，如图 1-13 所示，通过配置基于 ACL 的接入控制规则，实现仅匹配上 MAC 地址规则及 OUI 规则的客户端可以接入无线网络，其他客户端无法接入无线网络的目的。

2. 组网图

图1-13 ACL 接入控制配置组网图



3. 配置步骤

将 Client 1 和 Client 2 分别按照 MAC 地址匹配规则及 OUI 匹配规则添加到 ACL 4000 中。

```
<Sysname> system-view
[Syname] acl mac 4000
[Syname-acl-mac-4000] rule 0 permit source-mac 0000-000f-1121 ffff-ffff-ffff
[Syname-acl-mac-4000] rule 1 permit source-mac 000e-35b2-000e ffff-ff00-0000
[Syname-acl-mac-4000] quit
```

在无线服务模板 service1 上应用 ACL 4000。

```
[Syname] wlan service service1
[Sysname-wlan-st-service1] access-control acl 4000
```

4. 验证实现

配置完成之后，在 AC 上执行 **display wlan client** 命令，可以看到除 Client 1 及匹配上 OUI 规则的客户端（包括但不限于 Client 2）可以接入无线网络外，其它客户端均无法接入无线网络。

```
[AC] display wlan client
Total number of clients: 2

MAC address    Username         AP name       RID   IPv4 address        VLAN
0000-000f-1121 N/A              ap            1     192.168.100.12      1
000e-35b2-000e N/A              ap            1     192.168.100.13      1
```

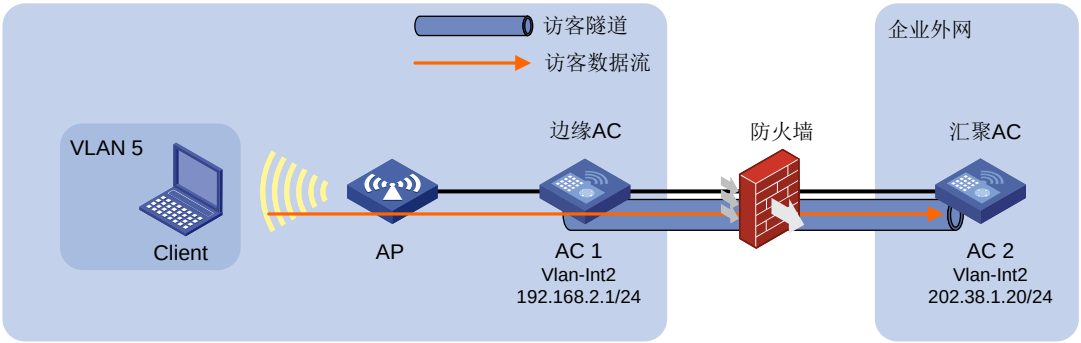
1.19.5 访客接入典型配置举例

1. 组网需求

在如图 1-14 所示的组网环境中，AC 1 作为边缘 AC 位于企业内网，AC 2 作为汇聚 AC 位于企业外网。访客用户 Client 通过访客 VLAN 5 接入 AP。当 AC 1 收到访客用户的数据流量时，会通过访客隧道直接将数据流量转发至防火墙外的 AC 2，由 AC 2 处理访客用户的数据流量，实现访客数据流量与企业内网数据的隔离。

2. 组网图

图1-14 访客接入配置组网图



3. 配置步骤

(1) 配置 AC 1

配置 AC 1 各接口的 IP 地址（略）。

配置 AC 1 为边缘 AC。

```
<AC1> system-view
[AC1] wlan guest-tunnel edge-ac
```

指定 AC 2 作为汇聚 AC，访客 VLAN 为 VLAN 5。

```
[AC1-wlan-edge-ac] aggregation-ac ip 202.38.1.20 tunnel-source ip 192.168.2.1 vlan 5
[AC1-wlan-edge-ac] quit
```

创建无线服务模板，配置 SSID 为 guest，用于访客接入。

```
[AC1] wlan service-template 1
[AC1-wlan-st-1] ssid guest
[AC1-wlan-st-1] service-template enable
[AC1-wlan-st-1] quit
```

创建 AP 模板，名称为 ap1。

```
[AC1] wlan ap ap1 model WA4320i-ACN
[AC1-wlan-ap-ap1] serial-id 210235A35U007B000010
```

将服务模板绑定到 ap1 的 Radio 2 上，并指定客户端从访客 VLAN 5 接入。

```
[AC1-wlan-ap-ap1] radio 2
[AC1-wlan-ap-ap1-radio-2] service-template 1 vlan-id 5
[AC1-wlan-ap-ap1-radio-2] radio enable
[AC1-wlan-ap-ap1-radio-2] quit
[AC1-wlan-ap-ap1] quit
```

(2) 配置 AC 2

配置 AC 2 各接口的 IP 地址（略）。

配置 AC 2 为汇聚 AC。

```
<AC2> system-view
[AC2] wlan guest-tunnel aggregation-ac
```

指定 AC 1 作为边缘 AC，访客 VLAN 为 VLAN 5。

```
[AC2-wlan-aggregation-ac] edge-ac ip 192.168.2.1 vlan 5
```

```
[AC2-wlan-aggregation-ac] quit
```

4. 验证配置

(1) 在 AC 1 和 AC 2 上使用 **display wlan guest-tunnel all** 命令查看访客隧道状态，通过下述显示信息可以确认访客隧道处于 Up 状态。

```
[AC1]display wlan guest-tunnel all
                              Guest access tunnel information
 Local Mode: Edge AC                                Tunnel Count: 1
Peer IP Address   Local IP Address     VLANs          State    Interface
202.38.1.20       192.168.2.1          5              Up       WLAN-Tunnel1

<AC2> display wlan guest-tunnel all
                              Guest access tunnel information
 Local Mode: Aggregation AC                         Tunnel Count: 1

 Peer IP Address         VLANs           State            Interface
192.168.2.1              5               Up               WLAN-Tunnel1
```

(2) 使用 **display wlan client** 命令查看访客用户的详细信息，在 VLAN 字段可以看到访客用户通过访客 VLAN 5 上线。

```
<AC1> display wlan client
MAC address    User name         AP name              RID  IP address      VLAN
508f-4c40-f3a6 N/A               ap1                  1    192.168.1.2     5
```

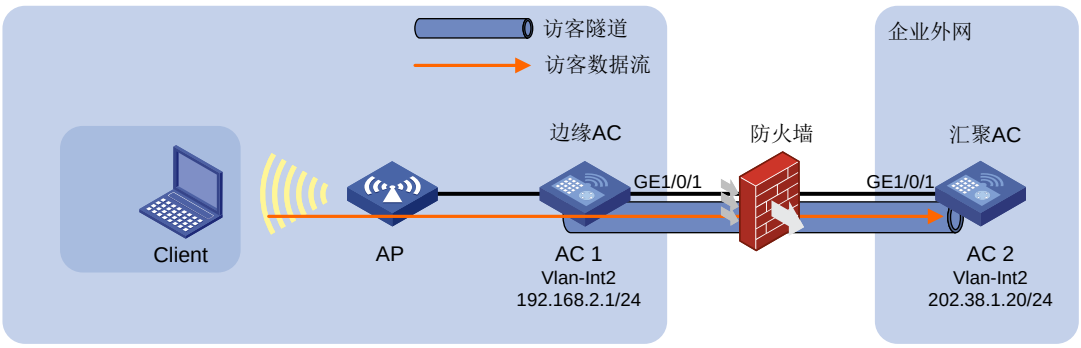
1.19.6 访客隧道加密模式下访客接入典型配置举例

1. 组网需求

在如图 1-15 所示的组网环境中，AC 1 作为边缘 AC 位于企业内网，AC 2 作为汇聚 AC 位于企业外网。访客用户 Client 通过访客 VLAN 5 接入 AP。当 AC 1 收到访客用户的数据流量时，先将数据流量通过 IPSec 加密，再通过访客隧道将加密后的数据流量转发至防火墙外的 AC 2，由 AC 2 处理访客用户的加密数据流量，实现访客隧道数据流量的加密。

2. 组网图

图1-15 访客隧道加密模式下访客接入配置组网图



3. 配置步骤

(1) 配置 AC 1

配置 AC 1 各接口的 IP 地址（略）。

配置 AC 1 为边缘 AC。

```
<AC1> system-view
[AC1] wlan guest-tunnel edge-ac
```

指定 AC 2 作为汇聚 AC，访客 VLAN 为 VLAN 5。

```
[AC1-wlan-edge-ac] aggregation-ac ip 202.38.1.20 tunnel-source ip 192.168.2.1 vlan 5
```

开启访客隧道加密时的流量分发功能。

```
[AC1-wlan-edge-ac] wlan guest-tunnel flow-distribute enable
[AC1-wlan-edge-ac] quit
```

创建无线服务模板，配置 SSID 为 guest，并且开启无线服务模板。

```
[AC1] wlan service-template 1
[AC1-wlan-st-1] ssid guest
[AC1-wlan-st-1] service-template enable
[AC1-wlan-st-1] quit
```

创建手工 AP，名称为 ap1，选择 AP 型号并配置序列号，指定客户端从访客 VLAN 5 上线，并将无线服务模板绑定到 AP 的 Radio 2 接口。

```
[AC1] wlan ap ap1 model WA4320i-ACN
[AC1-wlan-ap-ap1] serial-id 210235A35U007B000010
[AC1-wlan-ap-ap1] radio 2
[AC1-wlan-ap-ap1-radio-2] service-template 1 vlan-id 5
[AC1-wlan-ap-ap1-radio-2] radio enable
[AC1-wlan-ap-ap1-radio-2] quit
[AC1-wlan-ap-ap1] quit
```

(2) 配置 AC 2

配置 AC 2 各接口的 IP 地址（略）。

配置 AC 2 为汇聚 AC。

```
<AC2> system-view
[AC2] wlan guest-tunnel aggregation-ac
```

指定 AC 1 作为边缘 AC，访客 VLAN 为 VLAN 5。

```
[AC2-wlan-aggregation-ac] edge-ac ip 192.168.2.1 vlan 5
```

开启访客隧道加密时的流量分发功能。

```
[AC1-wlan-aggregation-ac] wlan guest-tunnel flow-distribute enable
[AC1-wlan-aggregation-ac] quit
```

(3) 配置 IPsec 加密

创建 IPv4 高级 ACL 3111。

```
[AC1] acl advanced 3111
```

定义由源端口 18002 去往目的端口 18002 的 UDP 数据流将被加密。

```
[AC1-acl-ipv4-adv-3111] rule permit udp source-port eq 18002 destination-port eq 18002
```

定义由源端口 60016～60031 去往目的端口 60016～60031 的 UDP 数据流将被加密。

```
[AC1-acl-ipv4-adv-3111] rule permit udp source-port range 60016 60031 destination-port
range 60016 60031
[AC1-acl-ipv4-adv-3111] quit
```

创建 IPsec 安全提议 tran1。

```
[AC1] ipsec transform-set tran1
```

配置安全协议对 IP 报文的封装形式为隧道模式。

```
[AC1-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

配置采用的安全协议为 ESP。

```
[AC1-ipsec-transform-set-tran1] protocol esp
```

配置 ESP 协议采用的加密算法为 128 比特的 AES，认证算法为 HMAC-SHA1。

```
[AC1-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
[AC1-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[AC1-ipsec-transform-set-tran1] quit
```

创建并配置 IKE keychain，名称为 keychain1。

```
[AC1] ike keychain keychain1
```

配置与 IP 地址为 202.38.1.20 的对端使用的预共享密钥为明文 123456TESTplat&!。

```
[AC1-ike-keychain-keychain1] pre-shared-key address 202.38.1.20 255.255.255.0 key
simple 123456TESTplat&!
[AC1-ike-keychain-keychain1] quit
```

创建并配置 IKE profile，名称为 profile1。

```
[AC1] ike profile profile1
```

指定引用的 keychain，名称为 keychain1。

```
[AC1-ike-profile-profile1] keychain keychain1
```

指定需要匹配对端身份类型为 IP 地址，取值为 202.38.1.20。

```
[AC1-ike-profile-profile1] match remote identity address 202.38.1.20 255.255.255.0
[AC1-ike-profile-profile1] quit
```

创建一条 IKE 协商方式的 IPsec 安全策略，名称为 map1，序列号为 10。

```
[AC1] ipsec policy map1 10 isakmp
```

指定引用 ACL 3111。

```
[AC1-ipsec-policy-isakmp-map1-10] security acl 3111
```

指定引用的安全提议为 tran1。

```
[AC1-ipsec-policy-isakmp-map1-10] transform-set tran1
```

指定 IPsec 隧道的本端 IP 地址为 192.168.2.1，对端 IP 地址为 202.38.1.20。

```
[AC1-ipsec-policy-isakmp-map1-10] local-address 192.168.2.1
[AC1-ipsec-policy-isakmp-map1-10] remote-address 202.38.1.20
```

指定引用的 IKE profile 为 profile1。

```
[AC1-ipsec-policy-isakmp-map1-10] ike-profile profile1
[AC1-ipsec-policy-isakmp-map1-10] quit
```

在 VLAN 2 上应用安全策略 map1。

```
[AC1] interface Vlan-interface 2
[AC1-Vlan-interface2] ip address 192.168.2.1 255.255.255.0
[AC1-Vlan-interface2] ipsec apply policy map1
[AC1-Vlan-interface2] quit
```

配置端口 GigabitEthernet 1/0/1（Trunk 类型）的缺省 VLAN 为 2，并允许 VLAN 2 通过。

```
[AC1] interface GigabitEthernet 1/0/1
[AC1-GigabitEthernet 1/0/1] port link-type trunk
[AC1-GigabitEthernet 1/0/1] port trunk pvid vlan 2
[AC1-GigabitEthernet 1/0/1] port trunk permit vlan 2
[AC1-GigabitEthernet 1/0/1] quit
```

AC 2 上的配置与 AC 1 相同，此处不再赘述。

4. 验证配置

(1) 以上配置完成后，AC 1 和 AC 2 之间如果有源端口 18002 与目的端口 18002 之间的报文通过，将触发 IKE 进行 IPsec SA 的协商。IKE 成功协商出 IPsec SA 后，源端口 18002 与目的端口 18002 之间数据流的传输将受到 IPsec SA 的保护。可通过以下显示查看到协商生成的 IPsec SA。

```
[AC1] display ipsec sa
-------------------------------
Interface: Vlan-interface5
-------------------------------

  -----------------------------
  IPsec policy: map1
  Sequence number: 10
  Mode: ISAKMP
  -----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect Forward Secrecy:
    Inside VPN:
    Extended Sequence Numbers enable: N
    Traffic Flow Confidentiality enable: N
    Path MTU: 1428
    Tunnel:
        local  address: 192.168.2.1
        remote address: 202.38.1.20
    Flow:
        sour addr: 0.0.0.0/0.0.0.0  port: 18002  protocol: udp
        dest addr: 0.0.0.0/0.0.0.0  port: 18002  protocol: udp

    [Inbound ESP SAs]
      SPI: 2485516269 (0x9425f7ed)
      Connection ID: 38654705664
      Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843187/986
      Max received sequence-number: 264
      Anti-replay check enable: Y
      Anti-replay window size: 64
      UDP encapsulation used for NAT traversal: N
      Status: Active

    [Outbound ESP SAs]
      SPI: 3088244842 (0xb812e06a)
      Connection ID: 38654705665
      Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 1843200/3600
```

```
SA remaining duration (kilobytes/sec): 1843187/986
Max sent sequence-number: 264
UDP encapsulation used for NAT traversal: N
Status: Active
```

(2) 在 AC 1 和 AC 2 上使用 **display wlan guest-tunnel all** 命令可以看到访客隧道的状态已经处于 Up 状态。

在 AC 1 上查看访客隧道状态。

```
[AC1] display wlan guest-tunnel all
                              Guest access tunnel information
 Local Mode: Edge AC                                Tunnel Count: 1

Peer IP Address   Local IP Address     VLANs          State    Interface
202.38.1.20       192.168.2.1          5              Up       WLAN-Tunnel1
```

在 AC 2 上查看访客隧道状态。

```
[AC2] display wlan guest-tunnel all
                              Guest access tunnel information
 Local Mode: Aggregation AC                         Tunnel Count: 1

Peer IP Address   Local IP Address     VLANs          State    Interface
192.168.2.1       202.38.1.20          5              Up       WLAN-Tunnel1
```

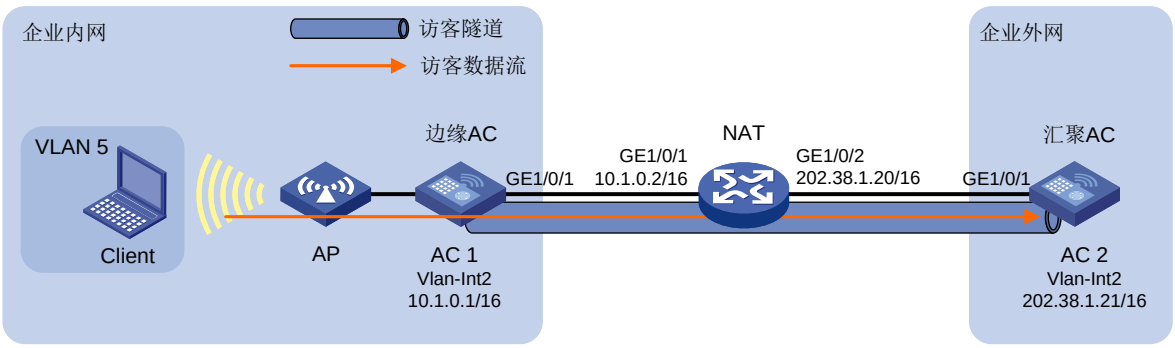
1.19.7 访客隧道加密模式下跨 NAT 设备访客接入典型配置举例

1. 组网需求

在如图 1-16 所示的组网环境中，AC 1 作为边缘 AC 位于企业内网，AC 2 作为汇聚 AC 位于企业外网。访客用户 Client 通过访客 VLAN 5 接入 AP。当 AC 1 收到访客用户的数据流量时，先将数据流量通过 IPSec 加密再通过访客隧道将加密后的数据流量转发至 NAT 设备，然后由 NAT 设备把加密后的数据流量转发至 AC 2，由 AC 2 处理访客用户的加密数据流量，实现访客隧道数据流量在加密模式下跨 NAT 设备到达企业外网，与企业内网数据隔离。

2. 组网图

图1-16 访客隧道加密模式下跨 NAT 设备访客接入配置组网图



3. 配置步骤

(1) 配置 AC 1

配置 AC 1 各接口的 IP 地址（略）。

配置 AC 1 为边缘 AC。

```
<AC1> system-view
[AC1] wlan guest-tunnel edge-ac
```

指定 AC 2 作为汇聚 AC，访客 VLAN 为 VLAN 5。

```
[AC1-wlan-edge-ac] aggregation-ac ip 202.38.1.21 tunnel-source ip 10.1.0.1 vlan 5
```

配置访客隧道加密时的流量分发功能。

```
[AC1-wlan-edge-ac] wlan guest-tunnel flow-distribute enable
[AC1-wlan-edge-ac] quit
```

创建无线服务模板，配置 SSID 为 guest，用于访客接入。

```
[AC1] wlan service-template 1
[AC1-wlan-st-1] ssid guest
[AC1-wlan-st-1] service-template enable
```

创建 AP 模板，名称为 ap1。

```
[AC1] wlan ap ap1 model WA4320i-ACN
[AC1-wlan-ap-ap1] serial-id 210235A35U007B000010
```

将服务模板绑定到 ap1 的 Radio 2 上，并指定客户端从访客 VLAN 5 上线。

```
[AC1-wlan-ap-ap1] radio 2
[AC1-wlan-ap-ap1-radio-2] service-template 1 vlan 5
[AC1-wlan-ap-ap1-radio-2] radio enable
[AC1-wlan-ap-ap1-radio-2] quit
[AC1-wlan-ap-ap1] quit
```

(2) 配置 AC 2

配置 AC 2 各接口的 IP 地址（略）。

配置 AC 2 为汇聚 AC。

```
<AC2> system-view
[AC2] wlan guest-tunnel aggregation-ac
```

指定 AC 1 作为边缘 AC，访客 VLAN 为 VLAN 5。

```
[AC2-wlan-aggregation-ac] edge-ac ip 10.1.0.1 vlan 5
```

配置访客隧道加密时的流量分发功能。

```
[AC2-wlan-aggregation-ac] wlan guest-tunnel flow-distribute enable
[AC2-wlan-aggregation-ac] quit
```

(3) 配置 NAT 设备

配置 GigabitEthernet 1/0/1 使其与边缘 AC 相通。

```
<NAT> system-view
[NAT] interface GigabitEthernet 1/0/1
[NAT-GigabitEthernet 1/0/1] ip address 10.1.0.2 255.255.0.0
[NAT-GigabitEthernet 1/0/1] quit
```

配置地址组 0，包含一个外网地址 202.38.1.23。

```
[NAT] nat address-group 0
[NAT-address-group-0] address 202.38.1.23 202.38.1.23
[NAT-address-group-0] quit
```

配置 ACL 2000，允许对企业内网中 10.1.0.3/16 网段的用户报文进行地址转化。

```
[NAT] acl basic 2000
```

```
[NAT-acl-ipv4-basic-2000] rule permit source 10.1.0.3 0.0.0.255
[NAT-acl-ipv4-basic-2000] quit
```

配置 GigabitEthernet 1/0/2 使其与汇聚 AC 相通。

```
[NAT] interface GigabitEthernet 1/0/2
[NAT-GigabitEthernet 1/0/2] ip address 202.38.1.20 255.255.0.0
```

在接口 GigabitEthernet 1/0/2 上配置出方向动态地址转换，允许使用地址组 0 中的地址对匹配 ACL 2000 的报文进行源地址转换，并在转换过程中使用端口信息。

```
[NAT-GigabitEthernet 1/0/2] nat outbound 2000 address-group 0
[NAT-GigabitEthernet 1/0/2] quit
```

(4) 配置 IPsec 加密

a. 配置 AC 1

创建 IPv4 高级 ACL 3000。

```
[AC1] acl advanced 3000
```

定义由源端口 18002 去往目的端口 18002 的 UDP 数据流将被加密。

```
[AC1-acl-ipv4-adv-3000] rule permit udp source-port eq 18002 destination-port eq
18002
```

#定义由源端口 60016～60031 去往目的端口 60016～60031 的 UDP 数据流将被加密。

```
[AC1-acl-ipv4-adv-3000] rule permit udp source-port range 60016 60031
destination-port range 60016 60031[AC1-acl-ipv4-adv-3000] quit
```

创建 IPsec 安全提议 tran1。

```
[AC1] ipsec transform-set tran1
```

配置安全协议对 IP 报文的封装形式为隧道模式。

```
[AC1-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

配置采用的安全协议为 ESP。

```
[AC1-ipsec-transform-set-tran1] protocol esp
```

配置 ESP 协议采用的加密算法为 3DES，认证算法为 HMAC-MD5。

```
[AC1-ipsec-transform-set-tran1] esp encryption-algorithm 3des-cbc
[AC1-ipsec-transform-set-tran1] esp authentication-algorithm md5
[AC1-ipsec-transform-set-tran1] quit
```

创建并配置 IKE keychain，名称为 keychain1。

```
[AC1] ike keychain keychain1
```

配置与 IP 地址为 202.38.1.21 的对端使用的预共享密钥为明文 123456TESTplat&!。

```
[AC1-ike-keychain-keychain1] pre-shared-key address 202.38.1.21 255.255.0.0 key
simple 123456TESTplat&!
[AC1-ike-keychain-keychain1] quit
```

创建并配置 IKE profile，名称为 profile1。

```
[AC1] ike profile profile1
```

指定引用的 keychain，名称为 keychain1。

```
[AC1-ike-profile-profile1] keychain keychain1
```

配置协商模式为野蛮模式。

```
[AC1-ike-profile-profile1] exchange-mode aggressive
```

配置本端身份为 FQDN 名称为 h3c.com，两端配置的 FQDN 必须相同。

```
[AC1-ike-profile-profile1] local-identity fqdn h3c.com
[AC1-ike-profile-profile1] match remote identity address 202.38.1.21 255.255.0.0
```

```
[AC1-ike-profile-profile1] quit
```

创建一条 IKE 协商方式的 IPsec 安全策略，名称为 policy1，序列号为 1。

```
[AC1] ipsec policy policy1 1 isakmp
```

指定引用 ACL 3000。

```
[AC1-ipsec-policy-isakmp-policy1-1] security acl 3000
```

指定引用的安全提议为 tran1。

```
[AC1-ipsec-policy-isakmp-policy1-1] transform-set tran1
```

配置 IPsec 隧道的对端 IP 地址为 202.38.1.21。

```
[AC1-ipsec-policy-isakmp-policy1-1] remote-address 202.38.1.21
```

指定引用的 IKE profile 为 profile1。

```
[AC1-ipsec-policy-isakmp-policy1-1] ike-profile profile1
[AC1-ipsec-policy-isakmp-policy1-1] quit
```

在 VLAN 5 上应用安全策略 policy1。

```
[AC1] interface Vlan-interface 5
[AC1-Vlan-interface5] ip address 10.1.0.1 255.255.0.0
[AC1-Vlan-interface5] ipsec apply policy policy1
[AC1-Vlan-interface5] quit
```

配置端口 GigabitEthernet 1/0/1（Trunk 类型）的缺省 VLAN 为 2，并允许 VLAN 2 通过。

```
[AC1] interface GigabitEthernet 1/0/1
[AC1-GigabitEthernet 1/0/1] port link-type trunk
[AC1-GigabitEthernet 1/0/1] port trunk pvid vlan 2
[AC1-GigabitEthernet 1/0/1] port trunk permit vlan 2
[AC1-GigabitEthernet 1/0/1] quit
```

配置流量触发 IKE DPD 探测间隔时间为 10 秒，重传时间间隔为 5 秒，探测模式为按需探测。

```
[AC1] ike dpd interval 10 retry 5 on-demand
```

配置静态路由。

```
[AC1] ip route-static 0.0.0.0 0 10.1.0.2
```

（可选）如果是 IRF 堆叠环境，还需要打开 IPsec 冗余备份功能。

```
[AC1] ipsec redundancy enable
```

b. 配置 AC 2

创建 IPsec 安全提议 tran1。

```
[AC2] ipsec transform-set tran1
```

配置安全协议对 IP 报文的封装形式为隧道模式。

```
[AC2-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

配置采用的安全协议为 ESP。

```
[AC2-ipsec-transform-set-tran1] protocol esp
```

配置 ESP 协议采用的加密算法为 3DES，认证算法为 HMAC-MD5。

```
[AC2-ipsec-transform-set-tran1] esp encryption-algorithm 3des-cbc
[AC2-ipsec-transform-set-tran1] esp authentication-algorithm md5
[AC2-ipsec-transform-set-tran1] quit
```

创建并配置 IKE keychain，名称为 keychain1。

```
[AC2] ike keychain keychain1
```

配置与 IP 地址为 202.38.1.23 的对端使用的预共享密钥为明文 123456TESTplat&!。

```
[AC2-ike-keychain-keychain1] pre-shared-key address 202.38.1.23 255.255.0.0 key
simple 123456TESTplat&!
[AC2-ike-keychain-keychain1] quit
```

创建并配置 IKE profile，名称为 profile1。

```
[AC2] ike profile profile1
```

指定引用的 keychain，名称为 keychain1。

```
[AC2-ike-profile-profile1] keychain keychain1
```

配置协商模式为野蛮模式。

```
[AC2-ike-profile-profile1] exchange-mode aggressive
```

配置匹配对端身份的规则为 FQDN 名称 h3c.com，两端配置的 FQDN 必须相同。

```
[AC2-ike-profile-profile1] match remote identity fqdn h3c.com
[AC2-ike-profile-profile1] quit
```

创建一条 IKE 协商方式的 IPsec 安全策略，名称为 template1，序列号为 1。

```
[AC2] ipsec policy-template template1 1
```

指定引用的安全提议为 tran1。

```
[AC2-ipsec-policy-template-template1-1] transform-set tran1
```

指定 IPsec 隧道的本端 IP 地址为 202.38.1.21。

```
[AC2-ipsec-policy-template-template1-1] local-address 202.38.1.21
```

指定引用的 IKE profile 为 profile1。

```
[AC2-ipsec-policy-template-template1-1] ike-profile profile1
[AC2-ipsec-policy-template-template1-1] quit
```

引用 IPsec 安全策略模板创建一条 IKE 协商方式的 IPsec 安全策略，名称为 policy1，顺序号为 1。

```
[AC2] ipsec policy policy1 1 isakmp template template1
```

在 VLAN 2 上应用安全策略 policy1。

```
[AC2] interface Vlan-interface 2
[AC2-Vlan-interface2] ip address 202.38.1.21 255.255.0.0
[AC2-Vlan-interface2] ipsec apply policy policy1
[AC2-Vlan-interface2] quit
```

配置端口 GigabitEthernet 1/0/1（Trunk 类型）的缺省 VLAN 为 2，并允许 VLAN 2 通过。

```
[AC2] interface GigabitEthernet 1/0/1
[AC2-GigabitEthernet 1/0/1] port link-type trunk
[AC2-GigabitEthernet 1/0/1] port trunk pvid vlan 2
[AC2-GigabitEthernet 1/0/1] port trunk permit vlan 2
[AC2-GigabitEthernet 1/0/1] quit
```

配置流量触发 IKE DPD 探测间隔时间为 10 秒，重传时间间隔为 5 秒，探测模式为按需探测。

```
[AC2] ike dpd interval 10 retry 5 on-demand
```

配置静态路由。

```
[AC2] ip route-static 0.0.0.0 0 10.2.0.3
```

（可选）如果是 IRF 堆叠环境，还需要打开 IPsec 冗余备份功能。

```
[AC2] ipsec redundancy enable
```

4. 加密模式验证配置

(1) 以上配置完成后，AC 1 和 AC 2 之间如果有源端口 18002 与目的端口 18002 之间的报文通过，将触发 IKE 进行 IPsec SA 的协商。IKE 成功协商出 IPsec SA 后，源端口 18002 与目的端口 18002 之间数据流和源端口 60016～60031 去往目的端口 60016～60031 的数据流的传输将受到 IPsec SA 的保护。可通过以下显示查看到协商生成的 IPsec SA。

```
[AC1] display ipsec sa
-------------------------------
Interface: Vlan-interface5
-------------------------------

  -----------------------------
  IPsec policy: policy1
  Sequence number: 1
  Mode: Template
  -----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect Forward Secrecy:
    Inside VPN:
    Extended Sequence Numbers enable: N
    Traffic Flow Confidentiality enable: N
    Path MTU: 1436
    Tunnel:
        local  address: 10.1.0.1
        remote address: 202.38.1.21
    Flow:
        sour addr: 0.0.0.0/0.0.0.0  port: 18002  protocol: udp
        dest addr: 0.0.0.0/0.0.0.0  port: 18002  protocol: udp

    [Inbound ESP SAs]
      SPI: 3885901857 (0xe79e2821)
      Connection ID: 55834574848
      Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843199/3160
      Max received sequence-number: 5
      Anti-replay check enable: Y
      Anti-replay window size: 64
      UDP encapsulation used for NAT traversal: Y
      Status: Active
```

(2) 在 AC 1 和 AC 2 上使用 **display wlan guest-tunnel all** 命令可以看到访客隧道的状态已经处于 Up 状态。

在 AC 1 上查看访客隧道状态。

```
[AC1] display wlan guest-tunnel all
                              Guest access tunnel information
 Local Mode: Edge AC                                Tunnel Count: 1
```

```
Peer IP Address   Local IP Address     VLANs           State    Interface
202.38.1.21       10.1.0.1             5               Up       WLAN-Tunnel1
```

在 AC 2 上查看访客隧道状态。

```
[AC2] display wlan guest-tunnel all
                              Guest access tunnel information
 Local Mode: Aggregation AC                          Tunnel Count: 1

Peer IP Address        VLANs             State            Interface
10.1.0.1               5                 Up               WLAN-Tunnel1
```