目 录

1 WLAN接入配置

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，用户在该区域内就可以通过无线接入的方式接入无线网络。

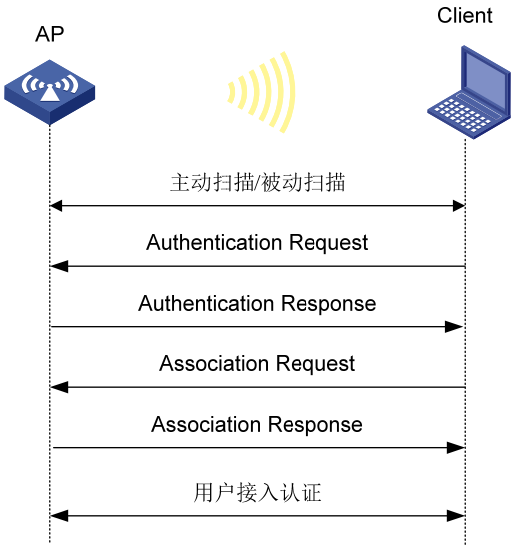
1.1.1 无线扫描

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。

说明

- 有关链路层认证的详细介绍及相关配置请参见“WLAN 配置指导”中的“WLAN 用户安全”。
- 有关用户接入认证的详细介绍及相关配置请参见“WLAN 配置指导”中的“WLAN 用户接入认证”。

图1-1 建立无线连接过程



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。

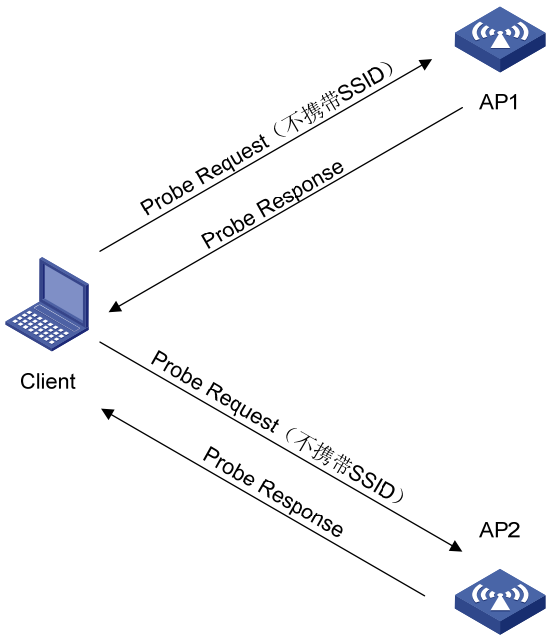
1. 主动扫描

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：

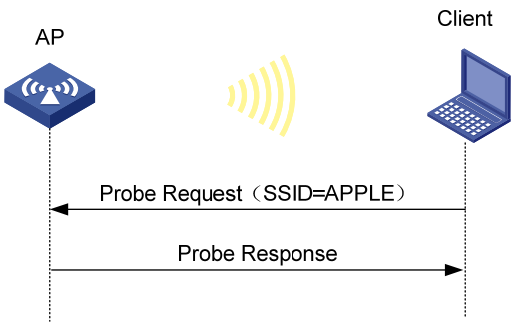
- 客户端发送Probe Request帧（Probe Request中SSID为空，也就是SSID这个信息元素的长度为 0）：客户端会定期地在其支持的信道列表中，发送Probe Request帧扫描无线网络。当AP收到Probe Request帧后，会回复Probe Response帧通告可以提供服务的无线网络信息。客户端通过主动扫描，可以主动获知可使用的无线服务，之后客户端可以根据需要选择适当的无线网络接入。客户端主动扫描方式的过程如 图 1-2 所示。

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。

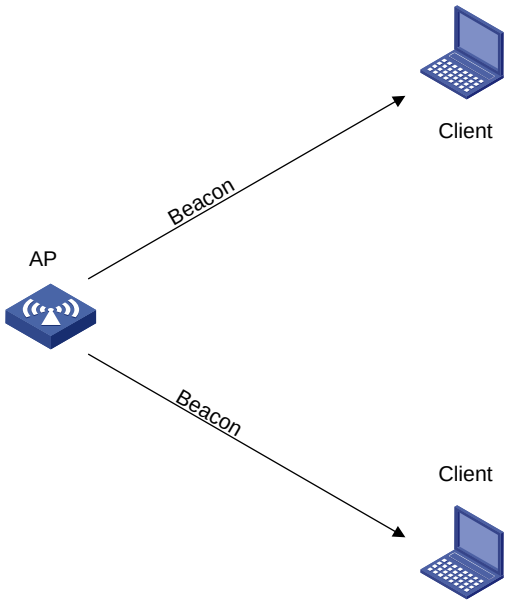
图1-3 主动扫描过程（Probe Request 携带指定为“APPLE”的 SSID）



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



1.1.2 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

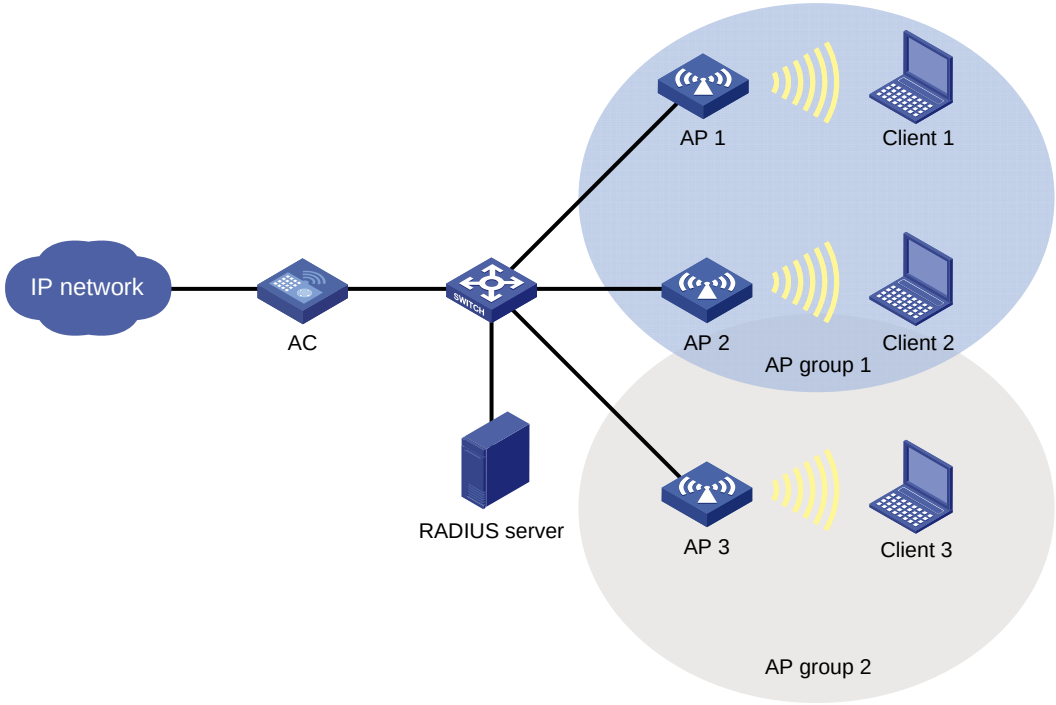
WLAN 接入控制的主要目的为对用户接入网络和访问网络进行控制，WLAN 接入控制的方式有基于 AP 组的接入控制、基于 SSID 的接入控制和基于名单的接入控制三种方式。

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帐户绑定的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。

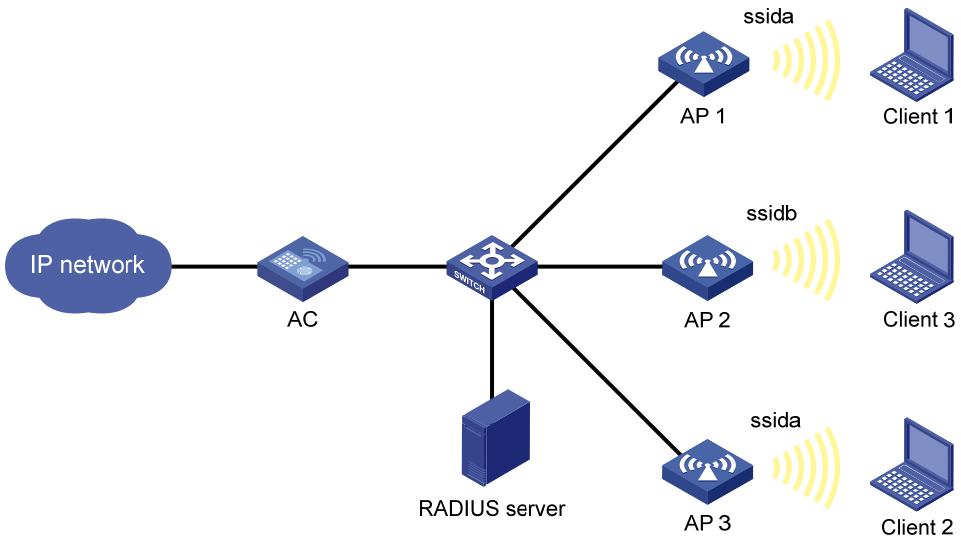
图1-5 基于 AP 组的接入控制组网应用



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帐户绑定的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。

(1) 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。

(2) 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。有关反制功能的详细介绍，请参见“WLAN 配置指导”中的“WIPS”。

3. 客户端过滤机制

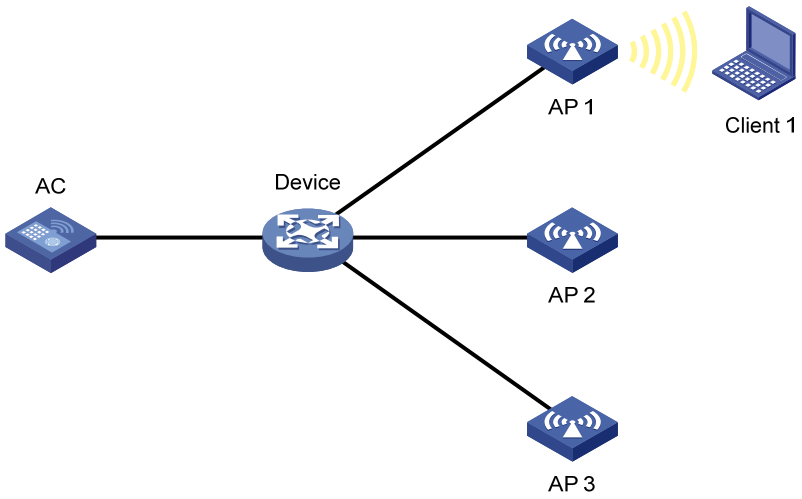
当收到客户端关联请求报文或AP向AC发送的Add mobile报文时，无线设备将使用白名单和黑名单对客户端的MAC地址进行过滤。静态黑名单、白名单和基于AC生效的动态黑名单会对所有与AC相连的AP生效，基于AP生效的动态黑名单仅对客户端接入的AP生效。以 图 1-7 为例，具体的过滤机制如下：

(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



1.3 WLAN接入配置限制和指导

AC 上的配置对 AP 生效的优先级从高到底为：AP 视图下的配置、AP 组视图下的配置、全局配置视图下的配置。

1.4 WLAN接入配置任务简介

表1-1 WLAN 接入配置任务简介

配置任务	说明	详细配置
创建无线服务模板	必选	1.5.1
配置SSID	必选	1.5.2
配置描述信息	可选	1.5.3
配置客户端的VLAN分配方式	可选	1.5.4
配置客户端优先使用授权VLAN	可选	1.5.5
配置客户端Cache老化时间	可选	1.5.6

配置任务	说明	详细配置
配置客户端关联位置	可选	1.5.7
配置客户端数据报文转发位置	可选	1.5.8
开启客户端数据报文转发功能	可选	1.5.9
配置客户端数据报文在CAPWAP隧道中的封装格式	可选	1.5.10
开启快速关联功能	可选	1.5.11
开启无线服务模板	必选	1.5.12
绑定无线服务模板	必选	1.5.13
配置区域码	可选	1.5.14
配置AP不回应客户端广播Probe request报文	可选	1.5.15
配置客户端空闲时间	可选	1.5.16
配置客户端保活时间	可选	1.5.17
配置AP不继承AP组下绑定的指定无线服务模板	可选	1.5.18
配置网络接入服务器标识	可选	1.5.19
配置对未知客户端数据报文处理方式	可选	1.5.20
配置无线转发策略	可选	1.5.21
配置允许用户接入的AP组	可选	1.5.22
配置允许用户接入的SSID名称	可选	1.5.23
配置白名单	可选	1.5.24
配置静态黑名单	可选	1.5.25
配置动态黑名单	可选	1.5.26
配置客户端二次接入认证的时间间隔	可选	1.5.27
指定AP的配置文件	可选	1.6
配置接收客户端信息的Web服务器信息	可选	1.7
开启告警功能	可选	1.8
配置客户端上线日志的格式	可选	1.9

1.5 配置WLAN接入

1.5.1 创建无线服务模板

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。

表1-2 创建无线服务模板

操作	命令	说明
进入系统视图	**system-view**	-
创建无线服务模板	**wlan service-template** *service-template-name*	缺省情况下，未创建无线服务模板
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

1.5.2 配置SSID

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。

表1-3 配置 SSID

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-
配置SSID	**ssid** *ssid-name*	缺省情况下，未配置SSID
（可选）配置SSID隐藏	**beacon ssid-hide**	缺省情况下，信标帧不隐藏SSID

说明

SSID 的名称应该尽量具有唯一性。从安全方面考虑，不应该体现公司名称。

1.5.3 配置描述信息

表1-4 配置描述信息

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-
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

1.5.4 配置客户端的VLAN分配方式

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，客户端仍被分配到同一个 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。

表1-5 配置客户端的 VLAN 分配方式

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-
配置客户端的VLAN分配方式	**client vlan-alloc** { **dynamic** | **static** }	缺省情况下，客户端的VLAN分配方式为动态分配方式

1.5.5 配置客户端优先使用授权VLAN

说明

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。

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）。

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。

开启本功能后，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。

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。

表1-6 配置客户端优先使用授权 VLAN

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-

操作	命令	说明
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

1.5.6 配置客户端Cache老化时间

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。

表1-7 配置客户端 Cache 的老化时间

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-
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

1.5.7 配置客户端关联位置


说明

客户端关联位置在 AP 上时，不支持客户端进行三层漫游，所以连续覆盖区域的所有 AP 上相同无线服务模板的指定 VLAN 需要相同。

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。

表1-8 配置客户端关联位置

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-
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

1.5.8 配置客户端数据报文转发位置

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。

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。

表1-9 配置客户端数据报文转发位置

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-
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，客户端的数据报文转发位置在AC上

1.5.9 开启客户端数据报文转发功能

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。

表1-10 开启客户端数据报文转发功能

操作	命令	说明
进入系统视图	**system-view**	-
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

1.5.10 配置客户端数据报文在CAPWAP隧道中的封装格式

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。

表1-11 配置客户端数据报文在 CAPWAP 隧道中的封装格式

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-

操作	命令	说明
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

1.5.11 开启快速关联功能

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。

表1-12 开启快速关联功能

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-
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

1.5.12 开启无线服务模板

表1-13 开启无线服务模板

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-
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

1.5.13 绑定无线服务模板

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。

表1-14 绑定无线服务模板（Radio 视图）

操作	命令	说明
进入系统视图	**system-view**	-
进入AP视图	**wlan ap** *ap-name* [**model** *model-name*]	-
进入Radio视图	**radio** *radio-number*	-
绑定无线服务模板	**service-template** *service-template-name* [**vlan** *vlan-id* | **vlan-group** *vlan-group-name*] [**ssid-hide**] [**nas-id** *nas-id* | **nas-port-id** *nas-port-id*]	缺省情况下，继承AP组配置

表1-15 绑定无线服务模板（AP 组 Radio 视图）

操作	命令	说明
进入系统视图	**system-view**	-
进入AP组视图	**wlan ap-group** *group-name*	-
进入AP型号视图	**ap-model** *ap-model*	-
进入Radio视图	**radio** *radio-id*	-
绑定无线服务模板	**service-template** *service-template-name* [**vlan** *vlan-id* | **vlan-group** *vlan-group-name*] [**ssid-hide**] [**nas-id** *nas-id* | **nas-port-id** *nas-port-id*]	缺省情况下，未绑定无线服务模板

说明

射频能绑定的最大无线服务模板个数为 16 个。

1.5.14 配置区域码

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。

表1-16 配置区域码（AP 视图）

操作	命令	说明
进入系统视图	**system-view**	-
进入AP视图	**wlan ap** *ap-name* [**model** *model-name*]	-

操作	命令	说明
配置区域码	**region-code** *code*	缺省情况下，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
开启区域码锁定功能	**region-code-lock enable**	缺省情况下，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

表1-17 配置区域码（AP 组视图）

操作	命令	说明
进入系统视图	**system-view**	-
进入AP组视图	**wlan ap-group** *group-name*	-
配置区域码	**region-code** *code*	缺省情况下，继承全局配置
开启区域码锁定功能	**region-code-lock enable**	缺省情况下，继承全局配置

表1-18 配置全局区域码

操作	命令	说明
进入系统视图	**system-view**	-
进入全局配置视图	**wlan global-configuration**	-
配置区域码	**region-code** *code*	缺省情况下，区域码为CN
开启区域码锁定功能	**region-code-lock enable**	缺省情况下，区域码锁定功能处于关闭状态

1.5.15 配置AP不回应客户端广播Probe request报文

广播 Probe request 报文即报文中不携带服务的 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。

表1-19 配置不回应客户端广播 Probe request 报文（AP 视图）

操作	命令	说明
进入系统视图	**system-view**	-
进入AP视图	**wlan ap** *ap-name* [**model** *model-name*]	-
配置AP不回应广播probe request报文	**broadcast-probe reply disable**	缺省情况下，继承AP组配置

表1-20 配置回应客户端广播 Probe request 报文（AP 组视图）

操作	命令	说明
进入系统视图	**system-view**	-
进入AP组视图	**wlan ap-group** *group-name*	-
配置AP组不回应广播probe request报文	**broadcast-probe reply disable**	缺省情况下，AP回应广播probe request报文

1.5.16 配置客户端空闲时间

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。

表1-21 配置客户端空闲时间（AP 视图）

操作	命令	说明
进入系统视图	**system-view**	-
进入AP视图	**wlan ap** *ap-name* [**model** *model-name*]	-
配置客户端空闲时间	**client idle-timeout** *interval*	缺省情况下，继承AP组配置

表1-22 配置客户端空闲时间（AP 组视图）

操作	命令	说明
进入系统视图	**system-view**	-
进入AP组视图	**wlan ap-group** *group-name*	-
配置客户端空闲时间	**client idle-timeout** *interval*	缺省情况下，AP和客户端之间连接允许的最大空闲时间为3600秒

1.5.17 配置客户端保活功能

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。

表1-23 配置客户端保活功能（AP 视图）

操作	命令	说明
进入系统视图	**system-view**	-
进入AP视图	**wlan ap** *ap-name* [**model** *model-name*]	-

操作	命令	说明
开启客户端保活功能	**client keep-alive enable**	缺省情况下，继承AP组配置
（可选）配置客户端保活时间	**client keep-alive interval** *value*	缺省情况下，继承AP组配置

表1-24 配置客户端保活功能（AP 组视图）

操作	命令	说明
进入系统视图	**system-view**	-
进入AP组视图	**wlan ap-group** *group-name*	-
开启客户端保活功能	**client keep-alive enable**	缺省情况下，客户端保活功能处于关闭状态
（可选）配置客户端保活时间	**client keep-alive interval** *value*	缺省情况下，客户端保活时间为300秒

1.5.18 配置AP不继承AP组下绑定的指定无线服务模板

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。

表1-25 配置 AP 不继承 AP 组下绑定的指定无线服务模板

操作	命令	说明
进入系统视图	**system-view**	-
进入AP视图	**wlan ap** *ap-name* [**model** *model-name*]	-
进入Radio视图	**radio** *radio-id*	-
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

1.5.19 配置网络接入服务器标识

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。

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。

表1-26 配置网络接入服务器标识（AP 视图）

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
进入AP视图	**wlan ap** *ap-name* [**model** *model-name*]	-
配置网络接入服务器标识	**nas-id** *nas-id*	缺省情况下，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
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
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 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

表1-27 配置网络接入服务器标识（AP 组视图）

操作	命令	说明
进入系统视图	**system-view**	-
进入AP组视图	**wlan ap-group** *group-name*	-
配置网络接入服务器标识	**nas-id** *nas-id*	缺省情况下，继承全局配置
配置网络接入服务器端口标识	**nas-port-id** *nas-port-id*	缺省情况下，继承全局配置

表1-28 配置全局网络接入服务器标识

操作	命令	说明
进入系统视图	**system-view**	-
进入全局配置视图	**wlan global-configuration**	-
配置网络接入服务器标识	**nas-id** *nas-id*	缺省情况下，未配置网络接入服务器标识
配置网络接入服务器端口标识	**nas-port-id** *nas-port-id*	缺省情况下，未配置网络接入服务器标识

1.5.20 配置对未知客户端数据报文处理方式

通过配置对未知客户端数据报文处理方式，可以选择 AC 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。

表1-29 配置对未知客户端数据报文处理方式

操作	命令	说明
进入系统视图	**system-view**	-
进入服务模板视图	**wlan service-template** *service-template-name*	-
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

1.5.21 配置无线转发策略

通过配置无线转发策略，设备可以对具备不同特征的客户端数据报文进行不同的转发处理。

无线转发策略可以在无线服务模板或 User Profile 下应用。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。

说明

- 只有无线用户的接入认证位置在 AC 上时，无线服务模板和 User Profile 下应用的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“WLAN 配置指导”中的“WLAN 用户接入认证”。
- 当配置无线转发策略时，AC 和 AP 必须处于不同网段中。

1. 创建无线转发策略

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“ACL 和 Qos 配置指导”中的“ACL”。

表1-30 创建无线转发策略

操作	命令	说明
进入系统视图	**system-view**	-
创建无线转发策略，并进入无线转发策略视图	**wlan forwarding-policy** *policy-name*	缺省情况下，不存在无线转发策略
配置无线转发规则	**classifier acl** { *acl-number* | **ipv6** *ipv6-acl-number* } **behavior** { **local** | **remote** }	缺省情况下，不存在无线转发规则 重复执行该命令可以创建多条无线转发规则

2. 在无线服务模板下应用无线转发策略

在无线服务模板下应用无线转发策略后，还需要开启无线转发策略功能，无线转发策略才能生效。

表1-31 在无线服务模板下应用无线转发策略

操作	命令	说明
进入系统视图	**system-view**	-
进入服务模板视图	**wlan service-template** *service-template-name*	-
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
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

3. 在User Profile下应用无线转发策略

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帐户绑定的 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。

在 User Profile 下应用无线转发策略后，还需要在服务模板下开启无线转发策略功能，无线转发策略才能生效。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。

表1-32 在 User Profile 下应用无线转发策略

操作	命令	说明
进入系统视图	**system-view**	-
进入User Profile视图	**user-profile** *profile-name*	-
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
退回系统视图	**quit**	-
进入服务模板视图	**wlan service-template** *service-template-name*	-
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

1.5.22 配置允许用户接入的AP组

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。

表1-33 配置允许用户接入的 AP 组

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
进入User Profile视图	**user-profile** *profile-name*	-
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

1.5.23 配置允许用户接入的SSID名称

在用户需要接入网络时，可指定允许用户接入的 SSID。

表1-34 配置允许用户接入的 SSID 名称

操作	命令	说明
进入系统视图	**system-view**	-
进入User Profile视图	**user-profile** *profile-name*	-
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

1.5.24 配置白名单

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。

表1-35 配置白名单

操作	命令	说明
进入系统视图	**system-view**	-
配置白名单	**wlan whitelist mac-address** *mac-address*	缺省情况下，不存在白名单

1.5.25 配置静态黑名单

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。

表1-36 配置静态黑名单

操作	命令	说明
进入系统视图	**system-view**	-
配置静态黑名单	**wlan static-blacklist mac-address** *mac-address*	缺省情况下，不存在静态黑名单

1.5.26 配置动态黑名单

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。

在 AP 分布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。

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。

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。

需要注意的是，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。

表1-37 配置动态黑名单

操作	命令	说明
进入系统视图	**system-view**	-
配置动态黑名单基于AP生效	**wlan dynamic-blacklist active-on-ap**	缺省情况下，动态黑名单基于AP生效
配置动态黑名单基于AC生效	**undo wlan dynamic-blacklist active-on-ap**	
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

1.5.27 配置客户端二次接入认证的时间间隔

在客户端进行二次接入认证并切换 VLAN 的组网环境中，建议配置客户端二次接入认证的时间间隔。

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。

表1-38 配置客户端二次接入认证的时间间隔

操作	命令	说明
进入系统视图	**system-view**	-
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0秒

1.6 指定AP的配置文件

在需要更新 AP 配置文件的情况下，可以在 AC 上指定 AP 配置文件的文件名（在 AC 的存储介质中必须已经存在该配置文件），将配置文件中的命令下载到 AP，配置文件会在隧道处于 Run 时生效。配置文件生效后，AP 会使用配置文件中的命令，但 AP 不会保存这些配置。

表1-39 指定 AP 的配置文件（AP 视图）

操作	命令	说明
进入系统视图	**system-view**	-
进入AP模板视图	**wlan ap** *ap-name* [**model** *model-name*]	-
将配置文件下载到AP	**map-configuration** *filename*	可选 缺省情况下，没有指定AP的配置文件

表1-40 指定 AP 的配置文件（AP 组 ap-model 视图）

操作	命令	说明
进入系统视图	**system-view**	-
进入AP组视图	**wlan ap-group** *group-name*	-
进入AP型号视图	**ap-model** *ap-model*	-
将配置文件下载到AP	**map-configuration** *filename*	可选 缺省情况下，没有指定AP的配置文件

说明

- 使用 **map-configuration** 命令指定的配置文件，文件中的内容必须是完整的命令行形式。
- 在使用某些功能时，需要使用配置文件对 AP 进行配置，例如：在本地转发模式下配置用户方案时，需要事先将用户方案、相关的 QoS 策略和 ACL 等命令写入配置文件，并将配置文件下载到 AP。
- 通过配置文件配置的 AP 只能通过主 IP 地址与 AC 建立 CAPWAP 隧道。
- 在 IRF 组网中，当需要使用 **map-configuration** 命令指定 AP 的配置文件时，请将配置文件分别导入到各成员设备的存储介质中，防止在发生主备倒换后找不到 AP 的配置文件，通过 **map-configuration** 命令下发的 AP 配置文件只能在 IRF 的主设备上生效，同时必须指定配置文件的存储路径为主设备。

1.7 配置接收客户端信息的Web服务器信息

AC 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，AC 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。

表1-41 配置接收客户端信息的 Web 服务器信息

操作	命令	说明
进入系统视图	**system-view**	-
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
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
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

1.8 开启告警功能

1.8.1 功能简介

开启客户端告警功能之后，一旦客户端状态发生变化，该模块就会生成告警信息；开启客户端升级告警功能之后，只有客户端上线、下线、漫游或获取 IP 地址时，该模块才会生成告警信息。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”。）

1.8.2 开启客户端的告警功能

表1-42 开启客户端的告警功能

操作	命令	说明
进入系统视图	**system-view**	-
开启客户端的告警功能	**snmp-agent trap enable wlan client**	缺省情况下，客户端的告警功能处于关闭状态

1.8.3 开启客户端审计的告警功能

表1-43 开启客户端审计的告警功能

操作	命令	说明
进入系统视图	**system-view**	-
开启客户端审计的告警功能	**snmp-agent trap enable wlan client-audit**	缺省情况下，客户端审计的告警功能处于关闭状态

1.9 配置客户端上线日志的格式

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三种，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“网络管理和监控配置指导”中的“信息中心”。

表1-44 配置客户端上线日志的格式

操作	命令	说明
进入系统视图	**system-view**	-
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

1.10 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。

在用户视图下执行 **wlan link-test** 命令可以检测 AP 与指定客户端之间的无线链路质量，检测内容包括：信号强度、报文重传次数、RTT（Round-Trip Time，往返时间）等。

表1-45 WLAN 接入显示和维护

操作	命令
显示黑名单	**display wlan blacklist** { **dynamic** | **static** }
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** [*policy-name*]
显示AP的区域码信息	**display wlan region-code**

操作	命令
显示无线服务模板信息	**display wlan service-template** [*service-template-name*] [**verbose**]
查看客户端的统计信息或服务模板的统计信息	**display wlan statistics** { **ap** { **all** | **name** *ap-name* } **connect-history** | **client** [**mac-address** *mac-address*] | **service-template** *service-template-name* [**connect-history**] }
显示白名单	**display wlan whitelist**
清除动态黑名单	**reset wlan dynamic-blacklist** [**mac-address** *mac-address*]
断开与客户端的连接	**reset wlan client** { **all** | **mac-address** *mac-address* }
清除无线客户端的统计信息	**reset wlan statistics client** { **all** | **mac-address** *mac-address* }
对客户端进行无线链路质量检测	**wlan link-test** *mac-address*

1.11 WLAN接入典型配置举例

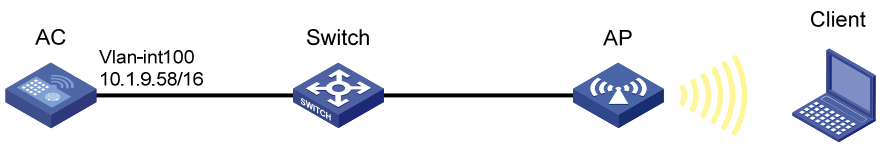
1.11.1 WLAN接入配置举例

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1-8 无线接入组网图



3. 配置步骤

(1) 配置 IP 地址

创建 VLAN100，并配置 VLAN100 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
[AC-Vlan-interface100] quit
```

(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 WA5320E-WiNet
[AC-wlan-ap-ap1] serial-id 219801A1FF8171E00361
```

```
[AC-wlan-ap-ap1] quit
```

(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，并开启无线服务模板。

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

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模板。无线服务模板 service1 的 SSID 为 trade-off，无线服务模板已经开启，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        : Not configured
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 s
PTK life time                  : 43200 s
PTK rekey                      : Enabled
GTK rekey                      : Enabled
GTK rekey method               : Time-based
GTK rekey time                 : 86400 s
GTK rekey client-offline       : 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                   : Not configured
802.1X handshake               : Disabled
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                 : 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
```

(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      IPv6 address   VLAN
0023-8933-223b N/A         ap1       1     3.0.0.3                        100
```

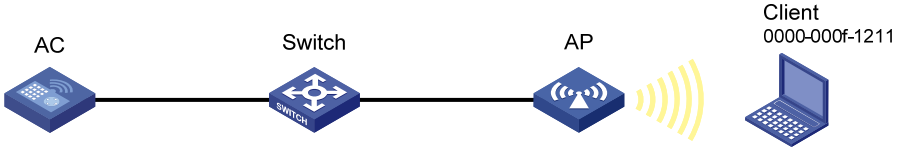
1.11.2 白名单配置举例

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1-9 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
```

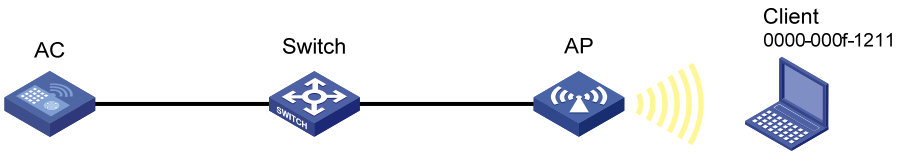
1.11.3 静态黑名单配置举例

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1-10 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
```