目 录

1 WLAN接入配置 ····· 1-1
1.1 WLAN接入简介 ····· 1-1
1.1.1 无线扫描 ····· 1-1
1.1.2 关联 ····· 1-3
1.2 WLAN客户端接入控制 ····· 1-3
1.2.1 基于名单的接入控制 ····· 1-3
1.3 WLAN接入配置任务简介 ····· 1-4
1.4 配置WLAN接入 ····· 1-5
1.4.1 创建无线服务模板 ····· 1-5
1.4.2 配置SSID ····· 1-5
1.4.3 配置无线服务模板允许关联的最大客户端数目 ····· 1-6
1.4.4 配置描述信息 ····· 1-6
1.4.5 开启快速关联功能 ····· 1-6
1.4.6 使能无线服务模板 ····· 1-7
1.4.7 绑定无线服务模板 ····· 1-7
1.4.8 配置区域码 ····· 1-8
1.4.9 配置AP不回应客户端广播Probe request报文 ····· 1-8
1.4.10 配置客户端空闲时间 ····· 1-8
1.4.11 配置客户端保活功能 ····· 1-9
1.4.12 配置网络接入服务器标识 ····· 1-9
1.4.13 配置对未知客户端数据报文处理方式 ····· 1-9
1.4.14 配置白名单 ····· 1-10
1.4.15 配置静态黑名单 ····· 1-10
1.4.16 配置动态黑名单表项的老化时间 ····· 1-10
1.4.17 配置客户端二次接入认证的时间间隔 ····· 1-10
1.5 开启告警功能 ····· 1-11
1.6 WLAN接入显示和维护 ····· 1-11
1.7 WLAN接入典型配置举例 ····· 1-12
1.7.1 WLAN接入配置举例 ····· 1-12
1.7.2 白名单配置举例 ····· 1-14
1.7.3 静态黑名单配置举例 ····· 1-14

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。

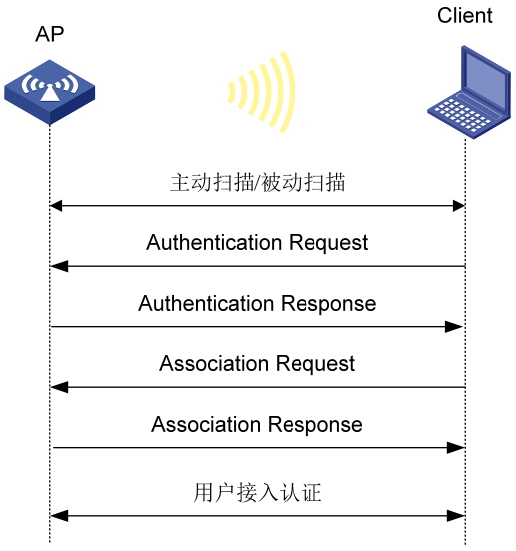
1.1.1 无线扫描

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。

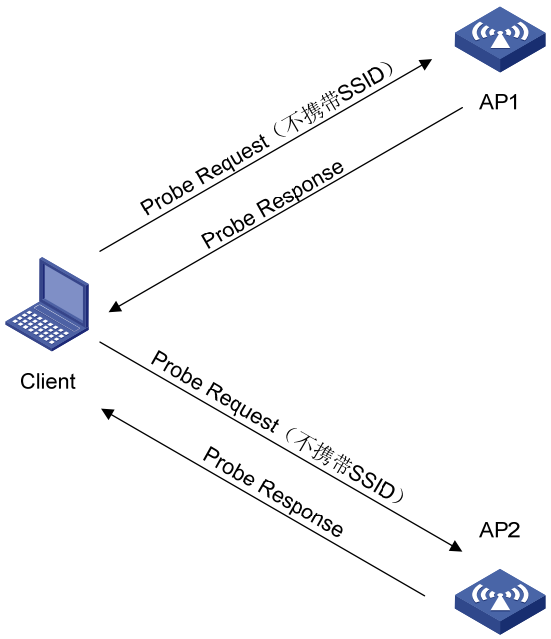
1. 主动扫描

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：

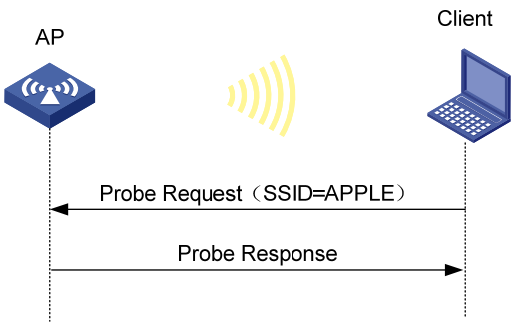
- 客户端发送Probe Request帧（Probe Request中SSID为空，也就是SSID这个信息元素的长度为 0）：客户端会定期地在其支持的信道列表中，发送Probe Request帧扫描无线网络。当AP收到Probe Request帧后，会回复Probe Response帧通告可以提供服务的无线网络信息。客户端通过主动扫描，可以主动获知可使用的无线服务，之后客户端可以根据需要选择适当的无线网络接入。客户端主动扫描方式的过程如 图 1-2 所示。

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。

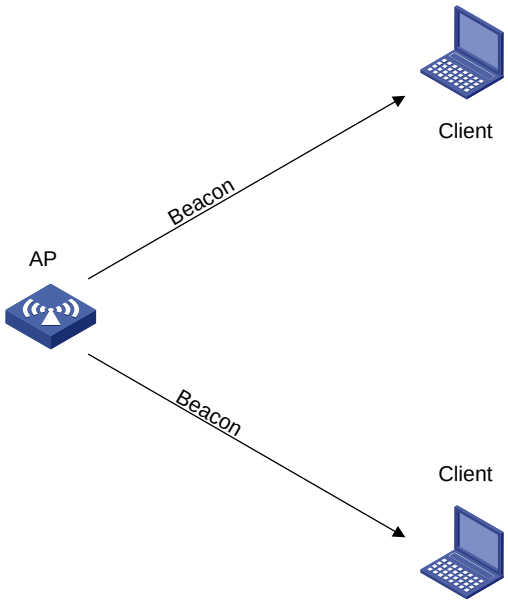
图1-3 主动扫描过程（Probe Request 携带指定为“APPLE”的 SSID）



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 接入控制的方式为基于名单的接入控制。

1.2.1 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

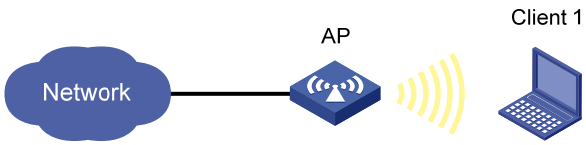
当收到客户端关联请求报文时，无线设备将使用白名单和黑名单对客户端的MAC地址进行过滤。以图 1-5 为例，具体的过滤机制如下：

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

(2) 当 AP 上不存在白名单时，AP 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 接入无线网络。

(3) 当 AP 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,则 AP 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 上接入无线网络。

图1-5 客户端过滤机制组网图



1.3 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	1.4.1
配置SSID	必选	1.4.2
配置无线服务模板允许关联的最大客户端数目	可选	1.4.3
配置描述信息	可选	1.4.4
开启快速关联功能	可选	1.4.5
使能无线服务模板	必选	1.4.6

配置任务	说明	详细配置
绑定无线服务模板	必选	1.4.7
配置区域码	可选	1.4.8
配置AP不回应客户端广播Probe request报文	可选	1.4.9
配置客户端空闲时间	可选	1.4.10
配置客户端保活时间	可选	1.4.11
配置网络接入服务器标识	可选	1.4.12
配置对未知客户端数据报文处理方式	可选	1.4.13
配置白名单	可选	1.4.14
配置静态黑名单	可选	1.4.15
配置动态黑名单表项的老化时间	可选	1.4.16
配置客户端二次接入认证的时间间隔	可选	1.4.17
开启告警功能	可选	1.5

1.4 配置WLAN接入

1.4.1 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，不存在无线服务模板
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

1.4.2 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

1.4.3 配置无线服务模板允许关联的最大客户端数目

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。

表1-4 配置无线服务模板允许关联的最大客户端数目

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

1.4.4 配置描述信息

表1-5 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

1.4.5 开启快速关联功能

如果 WLAN 环境中启动了频谱导航，客户端关联 AP 的效率将受到影响。对于不需要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计算，从而让客户端可以快速的关联到 AP 上。

表1-6 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

1.4.6 使能无线服务模板

表1-7 打开无线服务模板

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

1.4.7 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 的射频接口上，AP 会根据射频接口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 是无线服务提供服务的基本单元。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。

表1-8 绑定无线无线服务模板

操作	命令	说明
进入系统视图	**system-view**	-
进入WLAN射频接口视图	**interface wlan-radio** *interface-number*	-
绑定无线服务模板	**service-template** *service-template-name*	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。

1.4.8 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1-9 配置区域码

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

1.4.9 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1-10 配置不回应客户端广播 Probe request 报文

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

1.4.10 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1-11 配置客户端空闲时间

操作	命令	说明
进入系统视图	**system-view**	-
配置客户端空闲时间	**wlan 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

1.4.11 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1-12 配置客户端保活功能

操作	命令	说明
进入系统视图	**system-view**	-
开启客户端保活功能	**wlan client keepalive** *interval*	缺省情况下，客户端保活功能处于关闭状态

1.4.12 配置网络接入服务器标识

NAS-ID 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，则优先使用无线服务模板绑定的 NAS-ID。

表1-13 配置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

1.4.13 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 AP 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1-14 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

1.4.14 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1-15 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

1.4.15 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1-16 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

1.4.16 配置动态黑名单表项的老化时间

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，AP 会将该客户端的 MAC 地址添加到动态黑名单中。

动态黑名单表项具有一定的老化时间。当到达老化时间时，AP 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1-17 配置动态黑名单表项的老化时间

操作	命令	说明
进入系统视图	**system-view**	-
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

1.4.17 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1-18 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

1.5 开启告警功能

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”。）

表1-19 开启告警功能

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

1.6 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1-20 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 client-number**
显示无线服务模板信息	**display wlan service-template** [*service-template-name*] [**verbose**]
显示BSS（Basic Service Set，基本服务集）信息	**display wlan bss** { **all** | **bssid** *bssid* } [**verbose**]

操作	命令
显示客户端的信息	**display wlan client** [**interface wlan-radio** *interface-number* | **mac-address** *mac-address* | **service-template** *service-template-name*] [**verbose**]
显示客户端状态信息	**display wlan client status** [**mac-address** *mac-address*] [**verbose**]
显示白名单	**display wlan whitelist**
显示黑名单	**display wlan blacklist** { **dynamic** | **static** }
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* }
对客户端进行无线链路质量检测	**wlan link-test** *mac-address*
显示AP上工作在Client模式的Radio的相关信息	**display wlan client-mode radio**
显示当前扫描到的无线服务	**display wlan client-mode ssid** [*ssid*]

1.7 WLAN接入典型配置举例

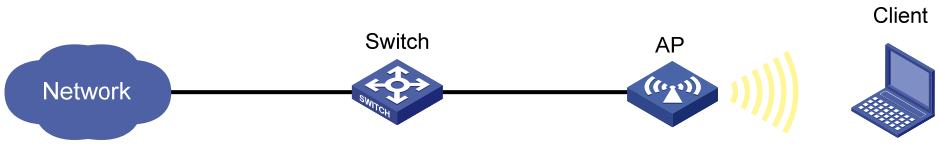
1.7.1 WLAN接入配置举例

1. 组网需求

- AP 通过交换机与有线网络相连。在 Switch 上开启 DHCP server 功能，为 AP 和客户端分配 IP 地址。
- AP 提供 SSID 为 trade-off 的无线接入服务。

2. 组网图

图1-6 无线接入组网图



3. 配置步骤

配置无线无线服务模板 service1，配置 SSID 为 trade-off，并开启服务模版。

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

将无线服务模板 service1 绑定到 WLAN-Radio 1/0/1 接口。

```
[AP] interface wlan-radio 1/0/1
[AP-WLAN-Radio1/0/1] undo shutdown
```

```
[AP-WLAN-Radio1/0/1] service-template service1
[AP-WLAN-Radio1/0/1] quit
```

4. 验证配置

(1) 配置完成后，在 AP 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，无线服务模板已经使能，其它配置项都使用缺省值。

```
[AP] 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
VLAN ID                        : 3
AKM mode                       : Not configured
Security IE                    : Not configured
Cipher suite                   : Not configured
TKIP countermeasure time       : 0 s
PTK life time                  : 43200 s
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
Critical 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         : Disabled
Authorization fail mode        : Online
Accounting fail mode           : Online
Authorization                  : Permitted
Key derivation                 : SHA1
PMF status                     : Disabled
Hotspot policy number          : Not configured
Forwarding policy status       : Disabled
Forwarding policy name         : Not configured
Forwarder                      : AC
```

```
FT status                      : Disabled
QoS trust                      : Port
QoS priority                   : 0
```

(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 AP 上执行 **display wlan client** 命令，可以看到所有连接成功的客户端。

```
[AP] 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  user        fatap     1     3.0.0.3                        3
```

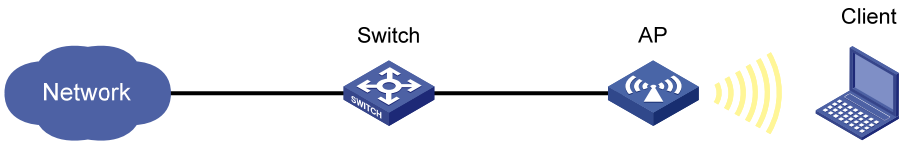
1.7.2 白名单配置举例

1. 组网需求

AP 通过交换机接入无线网络，客户端为已知合法客户端，通过将客户端的 MAC 地址 0000-000f-1211 加入到白名单中，仅允许白名单中的客户端接入无线网络，拒绝白名单以外的客户端接入无线网络。

2. 组网图

图1-7 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。

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

4. 验证配置

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

```
<AP> display wlan whitelist
Total number of clients: 1
 MAC addresses:
  0000-000f-1211
```

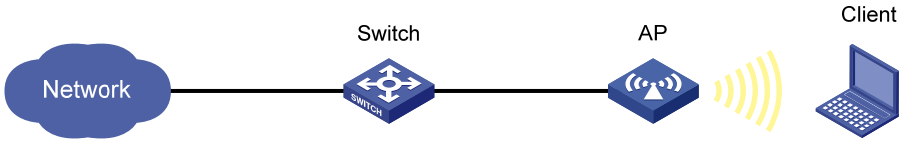
1.7.3 静态黑名单配置举例

1. 组网需求

AP 通过交换机接入无线网络。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，拒绝静态黑名单中的客户端接入无线网络。

2. 组网图

图1-8 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。

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

4. 验证配置

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

```
<AP> display wlan blacklist static
Total number of clients: 1
 MAC addresses:
  0000-000f-1211
```