

目 录

1 AP管理	1-1
1.1 AP管理简介.....	1-1
1.1.1 CAPWAP隧道.....	1-1
1.1.2 AP配置方式.....	1-3
1.1.3 APDB.....	1-3
1.1.4 协议规范.....	1-3
1.2 AP管理配置任务简介.....	1-3
1.3 配置准备.....	1-4
1.4 配置AC与AP建立CAPWAP隧道.....	1-4
1.4.1 创建手工AP.....	1-5
1.4.2 配置自动AP.....	1-5
1.4.3 配置AP连接AC的优先级.....	1-6
1.4.4 配置单播发现策略功能.....	1-7
1.5 配置二次发现AC功能.....	1-7
1.6 配置AP版本升级.....	1-8
1.6.1 配置版本升级功能.....	1-9
1.6.2 配置AP型号的软硬件版本对应关系.....	1-9
1.7 配置AP的VLAN.....	1-10
1.7.1 配置VLAN基本属性.....	1-10
1.7.2 配置基于端口的VLAN.....	1-11
1.7.3 向AP下发VLAN配置.....	1-13
1.8 配置CAPWAP隧道.....	1-14
1.8.1 配置CAPWAP隧道延迟检测.....	1-14
1.8.2 配置CAPWAP隧道保活.....	1-14
1.8.3 配置AP发送CAPWAP数据隧道keep alive报文的时间间隔.....	1-15
1.8.4 配置CAPWAP报文分片的最大长度.....	1-15
1.8.5 配置CAPWAP隧道的TCP最大报文段长度.....	1-16
1.9 配置请求报文重传.....	1-16
1.10 配置上报Radio统计信息.....	1-17
1.11 配置Remote AP功能.....	1-18
1.12 开启/关闭AP的USB接口.....	1-18
1.13 重启AP.....	1-19
1.14 重命名手工AP.....	1-19

1.15 管理AP的文件系统.....	1-19
1.16 配置AP组.....	1-20
1.16.1 AP组简介.....	1-20
1.16.2 创建AP组.....	1-20
1.17 预配置.....	1-21
1.17.1 预配置简介.....	1-21
1.17.2 配置AP预配置.....	1-22
1.17.3 配置AP组预配置.....	1-22
1.17.4 下发预配置.....	1-23
1.17.5 配置预配置智能加载功能.....	1-24
1.18 开启告警功能.....	1-24
1.18.1 告警功能简介.....	1-24
1.18.2 开启AP管理的告警功能.....	1-24
1.18.3 开启CAPWAP的告警功能.....	1-25
1.19 加载APDB用户脚本.....	1-25
1.20 配置重启业务异常AC功能.....	1-26
1.21 AP管理显示和维护.....	1-26
1.21.1 配置LED闪烁模式.....	1-26
1.21.2 显示AP管理信息.....	1-27
1.21.3 清除AP管理信息.....	1-27
1.22 AP管理典型配置举例.....	1-28
1.22.1 配置通过DHCP发现方式建立CAPWAP隧道举例.....	1-28
1.22.2 配置通过DHCPv6发现方式建立CAPWAP隧道举例.....	1-32
1.22.3 配置通过DNS发现方式建立CAPWAP隧道举例.....	1-36
1.22.4 配置开启自动AP功能建立CAPWAP隧道举例.....	1-40
1.22.5 AP组配置举例.....	1-44

1 AP管理



说明
仅 WX2500H-WiNet 系列不支持 slot 参数。

1.1 AP管理简介

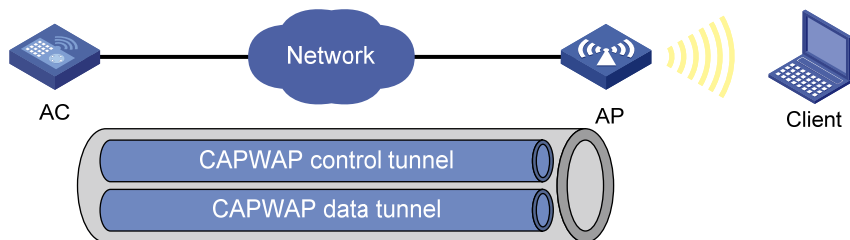
随着无线网络的大规模发展，当大量部署 AP（Access Point，接入点）时，AP 升级软件、射频参数的配置和调整等管理工作将给用户带来高昂的管理成本。为解决这一问题，WLAN 采用 AC+Fit AP 架构，即通过 AC（Access Controller，接入控制器）对下属的 AP 进行集中控制和管理，AP 不需要任何配置，所有的配置都保存在 AC 上并由 AC 下发，同时由 AC 对 AP 进行统一的管理和维护，AP 和 AC 间采用 CAPWAP（Controlling and Provisioning of Wireless Access Point，无线接入点控制与供应）隧道进行通讯，用于传递数据报文和控制报文。

1.1.1 CAPWAP隧道

CAPWAP 隧道为 AP 和 AC 之间的通信提供了通用的封装和传输机制，CAPWAP 隧道使用 UDP 协议作为传输协议，并支持 IPv4 和 IPv6 协议。

如 [图 1-1](#) 所示，AC 通过 CAPWAP 协议与 AP 建立控制隧道和数据隧道，AC 通过控制隧道对 AP 进行管理和监控，通过数据隧道转发客户端的数据报文。

图1-1 CAPWAP 隧道典型组网图



1. 获取AC地址

AP 零配置启动后，AP 会自动创建 VLAN-interface 1，并在该接口上默认开启 DHCP 客户端、DHCPv6 客户端和 DNS 客户端功能，完成上述操作后，AP 将使用获取的 AC 地址发现 AC 并建立 CAPWAP 隧道。AP 获取 AC 地址的方式如下：

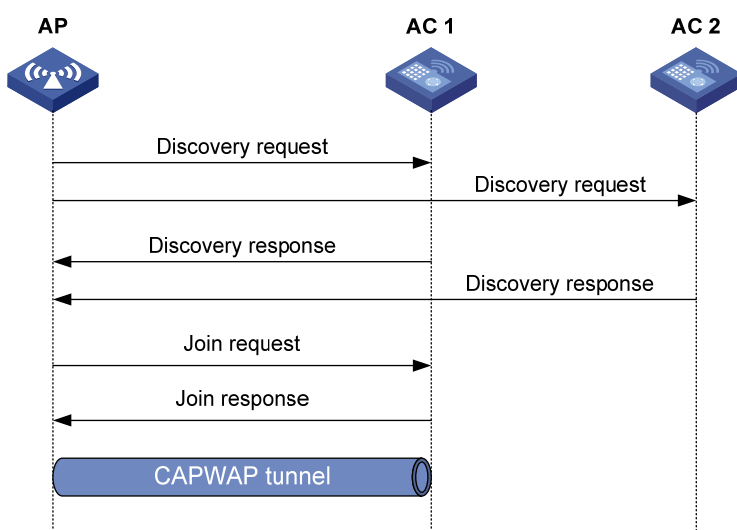
- 静态配置：通过预配置为 AP 手工指定 AC 的 IP 地址。
- DHCP 选项：通过 DHCP 服务器返回的 Option 138 或 Option 43 选项获取 AC 的 IPv4 地址，或 Option 52 选项获取 AC 的 IPv6 地址，通过三个选项获取 AC 地址的优先级为 Option 138 > Option 43 > Option 52。获取到 AC 的 IP 地址后，AP 向 AC 发送单播 Discovery request 报文

来发现、选择 AC 并建立 CAPWAP 隧道。有关 Option 选项的详细介绍请参见“三层技术-IP 业务”中的“DHCP”。

- DNS: AP 通过 DHCP 服务器获取 AC 的域名后缀及 DNS server 的 IP 地址, 再将自身获取的主机名与域名后缀形成 AC 的完整域名进行 DNS 解析, 获取 AC 地址, AP 向获取的所有 AC 地址发送单播 Discovery request 报文来发现、选择 AC 并建立 CAPWAP 隧道。
- 广播: AP 通过向 IPv4 广播地址 255.255.255.255 发送 Discovery request 广播报文来发现、选择 AC 并建立隧道。
- IPv4 组播: AP 通过向 IPv4 组播地址 224.0.1.140 发送 Discovery request 组播报文来发现、选择 AC 并建立隧道。
- IPv6 组播: AP 通过向 IPv6 组播地址 FF0E::18C 发送 Discovery request 组播报文来发现、选择 AC 并建立隧道。

2. CAPWAP隧道建立过程

图1-2 CAPWAP 隧道建立过程



AP 发现 AC 并建立 CAPWAP 隧道过程如下:

- (1) AP 向 AC 地址发送 Discovery request 报文。
- (2) AC 收到 Discovery request 报文后, 根据本地策略和报文内容决定是否对 AP 进行回复 Discovery response 报文, Discovery response 报文中会携带优先级值、AC 上是否存在该 AP 的信息和 AC 上的负载信息等, 以此实现 AC 选择 AP。
- (3) AP 收到各个 AC 的 Discovery response 报文后, 根据报文中携带的内容, 选择最优 AC。
- (4) AP 向选择的最优 AC 发送 Join request 报文。
- (5) AC 根据报文内容, 检查是否为该 AP 提供服务, 并回复 Join response 报文。
- (6) AP 若收到 Result Code 为失败的 Join response 报文, 则不建立隧道; 若 AP 收到 Result Code 为成功的 Join response 报文, 则 AP 和 AC 成功建立隧道。

AP 依次使用静态配置、DHCPv4 选项、广播/IPv4 组播、IPv4 DNS、IPv6 组播、DHCPv6 选项、IPv6 DNS 获取的 AC 地址进行发现 AC 并建立隧道过程, 若某一种方式成功建立 CAPWAP 隧道, 则停止发现 AC 的过程。

1.1.2 AP配置方式

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。

1.1.3 APDB

APDB (Access Point Information Database, 接入点信息数据库) 是 AC 内存中的 AP 信息数据库，数据库中保存的信息包括 AP 型号和软硬件版本对应关系，AP 型号支持的射频数量、类型、合法区域码、合法天线类型和功率表等。仅当 APDB 中存在某 AP 型号的信息时，AC 才能和该型号的 AP 建立 CAPWAP 隧道。

APDB中存储的数据通过脚本文件管理，包括系统脚本文件和用户脚本文件。其中，系统脚本文件随AC版本发布，并在AC启动时自动加载；用户脚本文件由用户自行配置并加载到APDB中。如果要让AC支持新型号的AP，可以通过升级AC的软件版本或加载APDB用户脚本文件的方式实现。有关软件版本升级的详细介绍请参见“基础配置指导”中的“软件升级”，有关加载APDB用户脚本的详细介绍请参见“[1.19 加载APDB用户脚本](#)”。

1.1.4 协议规范

与 CAPWAP 相关的协议规范有：

- RFC 5415: Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification
- RFC 5416: Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11
- RFC 5417: Control And Provisioning of Wireless Access Points (CAPWAP) Access Controller DHCP Option

1.2 AP管理配置任务简介

表1-1 AP 管理配置任务简介

配置任务	说明	详细配置
配置AC与AP建立CAPWAP隧道	必选	1.4
配置二次发现AC功能	可选	1.5
配置AP版本升级	可选	1.6
配置AP的VLAN	可选	1.7
配置CAPWAP隧道	可选	1.8
配置请求报文重传	可选	1.9
配置上报Radio统计信息	可选	1.10

配置任务	说明	详细配置
配置Remote AP功能	可选	1.11
开启/关闭AP的USB接口	可选	1.12
重启AP	可选	1.13
重命名手工AP	可选	1.14
管理AP的文件系统	可选	1.15
配置AP组	可选	1.16
预配置	可选	1.17
开启告警功能	可选	1.18
加载APDB用户脚本	可选	1.19
配置重启业务异常AC功能	可选	1.20

1.3 配置准备

CAPWAP 隧道的建立需要 DHCP 和 DNS 的配合。因此，首先需要完成以下配置任务：

- AP 需要获取到自身的 IP 地址，因此需要在 DHCP server 上配置地址池为 AP 分配 IP 地址。
- 若获取 AC 地址的方式为 DHCP 选项方式，则需要在 DHCP server 上将对应地址池的 Option 138 或 Option 43 配置为 AC 的 IPv4 地址，或使用 Option 52 配置 AC 的 IPv6 地址。
- 若获取 AC 地址的方式为 DNS 方式，则需要在 DHCP server 对应的地址池上配置 DNS server 的 IP 地址和 AC 的域名后缀。并在 DNS server 上创建区域，添加 AC 的 IP 地址和域名的映射。
- 保证 AC 和 AP 之间的路由可达。

有关 DHCP 和域名解析的详细介绍和相关配置，请参见“三层技术-IP 业务配置指导”中的“DHCP 服务器”、“DHCPv6 服务器”和“域名解析”。

1.4 配置AC与AP建立CAPWAP隧道

在 CAPWAP 隧道建立过程中提到，AC 收到 Discovery request 报文后，根据本地策略和报文内容决定是否对 AP 进行回复 Discovery response 报文，详细步骤如下：

- (1) AC 检查收到的 Discovery request 报文是否为单播报文，如果是单播报文则直接进行下一步。如果是广播或组播报文，将检查单播发现策略功能是否处于开启状态，如果处于开启状态，AC 不回复 Discovery response 报文；如果处于关闭状态，再进行下一步检查。
- (2) AC 根据 Discovery request 报文中携带的 AP 型号信息检查自身是否存在手工 AP，如果存在手工 AP，则向 AP 回复 Discovery response 报文，并在报文中携带存在手工 AP 的标记、优先级值和负载情况；如果不存在手工 AP，再进行下一步检查。
- (3) AC 检查自动 AP 功能的开启状态，如果自动 AP 功能处于开启状态，AC 向 AP 回复 Discovery response 报文，并在报文中携带自动 AP 功能处于开启状态的标记、优先级值和负载情况；如果自动 AP 功能处于关闭状态，则不回复 Discovery response 报文。

AP 收到各个 AC 的 Discovery response 报文后，根据报文中携带的内容，选择最优 AC 建立 CAPWAP 隧道。最优 AC 的判断条件按优先级为：存在手工 AP > 开启自动 AP 功能 > AP 连接 AC 的优先级 > AC 的负载情况。

1.4.1 创建手工AP

创建手工 AP 是指用户根据 AP 的实际信息，包括 AP 型号、序列号和 MAC 地址，在 AC 上手动创建 AP。在 AP 发现 AC 时，会优先选择存在手工 AP 的 AC 建立 CAPWAP 隧道连接。

表1-2 创建手工 AP

操作	命令	说明
进入系统视图	system-view	-
创建手工AP，并进入AP视图	wlan ap ap-name [model model-name]	缺省情况下，未创建手工AP创建AP时，需要输入型号名称
配置AP的序列号	serial-id serial-id	二者选其一
配置AP的MAC地址	mac-address mac-address	
（可选）配置AP的描述信息	description text	缺省情况下，未设置AP的描述信息

1.4.2 配置自动AP



说明

开启自动 AP 功能后，AC 将以 AP 的 MAC 地址来命名上线的自动 AP。

当无线网络中部署的 AP 数量较多时，开启自动 AP 功能可以简化配置，即 AC 上可以不创建手工 AP。AP 发现没有 AC 存在手工 AP 的情况下，会从开启自动 AP 功能的 AC 中选择最优 AC 进行 CAPWAP 隧道连接。

自动 AP 上线后，没有自己的视图，用户无法对自动 AP 进行单独配置，仅能通过 AP 组进行集中配置。可以通过配置固化功能将自动 AP 固化为手工 AP，用户可以进入手工 AP 视图对 AP 进行参数的修改。

1. 开启自动AP功能

表1-3 开启自动 AP 功能

操作	命令	说明
进入系统视图	system-view	-
开启自动AP功能	wlan auto-ap enable	缺省情况下，自动AP功能处于关闭状态

2. 开启自动AP自动固化功能

出于网络安全因素考虑,自动 AP 功能应该在需要部署的 AP 全都接入后关闭,以防止非法 AP 接入。因此需要将已接入的所有 AP 固化为手工 AP, AP 才能在出现 AC 重启或与 AC 连接断开的情况下再次接入 AC。

表1-4 开启自动 AP 自动固化功能

操作	命令	说明
进入系统视图	system-view	-
将自动AP固化为手工AP	wlan auto-ap persistent { all name <i>auto-ap-name</i> [<i>new-ap-name</i>] }	二者至少选其一 wlan auto-persistent enable 命令仅对配置本命令后新上线的自动AP生效,对于已上线的自动AP,只能使用 wlan auto-ap persistent 命令将自动AP转换为固化AP
开启自动AP自动固化功能	wlan auto-persistent enable	缺省情况下,自动AP自动固化功能处于关闭状态

1.4.3 配置AP连接AC的优先级

配置 AP 连接该 AC 的优先级,该优先级会携带在 Discovery response 中下发给 AP 供 AP 进行 AC 选择。以下两种情况下, AP 会优先选择优先级高的 AC 建立 CAPWAP 隧道连接。

- 有多个 AC 存在手工 AP。
- 没有 AC 存在手工 AP,但是有多个 AC 开启了自动 AP 功能。

表1-5 配置 AP 连接 AC 的优先级 (AP 视图)

操作	命令	说明
进入系统视图	system-view	-
进入AP视图	wlan ap <i>ap-name</i> [model <i>model-name</i>]	-
配置AP连接AC的优先级	priority <i>priority</i>	缺省情况下,继承AP组配置

表1-6 配置 AP 连接 AC 的优先级 (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 <i>group-name</i>	进入AP组视图
配置AP连接AC的优先级	priority <i>priority</i>	缺省情况下, AP连接的优先级为4

1.4.4 配置单播发现策略功能

AP 可以通过单播、组播及广播三种方式发现 AC 并建立 CAPWAP 隧道。开启了单播发现策略功能后, AC 只对发送单播 Discovery request 报文的 AP 进行响应, 不对发送组播、广播 Discovery request 报文的 AP 进行响应, 即只允许单播发现的 AP 与 AC 建立 CAPWAP 隧道连接。

表1-7 配置单播发现策略功能

操作	命令	说明
进入系统视图	system-view	-
开启单播发现策略功能	wlan capwap discovery-policy unicast	缺省情况下, 单播发现策略功能处于关闭状态

1.5 配置二次发现AC功能

二次发现 AC 功能用于向 AP 提供建立 CAPWAP 隧道的目的 AC 的 IP 地址。开启该功能后, AC 发送的 Discovery response 报文中会携带 CAPWAP Control IP Address 消息元素, AP 收到 Discovery response 报文后, 将向消息元素中的 IP 地址发送 Discovery request 报文, 达到二次发现 AC 的目的。

开启二次发现 AC 功能后, AP 与 AC 建立隧道的过程如下:

- (1) AP 发送 Discovery request 报文给 AC。
- (2) AC 收到 Discovery request 报文后, 在 Discovery response 报文中添加 CAPWAP Control IPv4 Address 消息元素或 CAPWAP Control IPv6 Address 消息元素来携带分配给 AP 的 IP 地址。
- (3) AP 收到 Discovery response 报文后, 判断是否已经向消息元素中的 IP 地址发送过 Discovery request 报文。如果已经向消息元素中的 IP 地址发送过 Discovery request 报文, 则直接向该 IP 地址发送 Join request 请求建立 CAPWAP 隧道; 否则, AP 会向消息元素中的 IP 地址发送 Discovery request 报文, 重新发起 AC 发现过程。

关闭二次发现 AC 功能后, AC 发送的 Discovery response 报文中不会携带 CAPWAP Control IP Address 消息元素, AP 收到此类 Discovery response 报文后, 直接向 Discovery response 报文的源 IP 地址发送 Join request 请求来建立 CAPWAP 隧道。

表1-8 配置二次发现 AC 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]	-
配置二次发现AC功能	control-address { disable 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

操作	命令	说明
配置CAPWAP Control IP Address消息元素中的IP地址	control-address { ip <i>ipv4-address</i> ipv6 <i>ipv6-address</i> }	最多可配置三个IPv4地址和三个IPv6地址 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1-9 配置二次发现 AC 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 <i>group-name</i>	-
配置二次发现AC功能	control-address { disable enable }	缺省情况下，继承全局配置
配置CAPWAP Control IP Address消息元素中的IP地址	control-address { ip <i>ipv4-address</i> ipv6 <i>ipv6-address</i> }	最多可配置三个IPv4地址和三个IPv6地址 缺省情况下，继承全局配置

表1-10 配置二次发现 AC 功能（全局配置视图）

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	-
配置二次发现AC功能	control-address { disable enable }	缺省情况下，二次发现AC功能处于关闭状态
配置CAPWAP Control IP Address消息元素中的IP地址	control-address { ip <i>ipv4-address</i> ipv6 <i>ipv6-address</i> }	最多可配置三个IPv4地址和三个IPv6地址 缺省情况下，CAPWAP Control IP Address消息元素中的IP地址为AC自身的IP地址

1.6 配置AP版本升级

版本升级功能处于开启状态下，AP的版本升级过程如下：

- (1) AP 将版本和型号信息上送给 AC。
- (2) AC 比较 AP 的软件版本。缺省情况下，AC 比较 AP 的软件版本与 APDB 中的 AP 型号和软硬件版本关系是否一致。配置 AP 型号的软硬件版本对应关系后，AC 将比较 AP 的软件版本与配置的软硬件版本关系是否一致。
- (3) 如果软件版本一致，则允许 CAPWAP 隧道建立；如果软件版本不一致，则将此情况告知 AP。AP 收到版本不一致的消息后，会向 AC 请求版本。
- (4) AC 收到 AP 的版本请求后，会向 AP 下发软件版本。
- (5) AP 收到版本文件后，将进行版本升级并进行重启后再与 AC 建立 CAPWAP 隧道。

1.6.1 配置版本升级功能

只有版本升级功能处于开启状态时，AC 才会在 CAPWAP 隧道建立过程中比较 AP 的软件版本。否则，AC 不对 AP 的软件版本进行比较，直接与 AP 建立 CAPWAP 隧道。

表1-11 配置版本升级功能（AP 视图）

操作	命令	说明
进入系统视图	system-view	-
进入AP视图	wlan ap <i>ap-name</i> [model <i>model-name</i>]	-
配置AP版本升级	firmware-upgrade { disable enable }	缺省情况下，若AP组存在版本升级配置，则继承AP组配置，若AP组不存在版本升级配置，则继承全局配置

表1-12 配置版本升级功能（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 <i>group-name</i>	进入AP组视图
配置AP版本升级	firmware-upgrade { disable enable }	缺省情况下，继承全局配置

表1-13 配置版本升级功能（全局配置视图）

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	进入全局配置视图
配置AP版本升级	firmware-upgrade { disable enable }	缺省情况下，AP版本升级功能处于开启状态

1.6.2 配置AP型号的软硬件版本对应关系



注意

该配置通常用于向 AP 下发临时版本，建议用户不要自行配置，以免导致 AP 无法与 AC 建立 CAPWAP 隧道。

配置 AP 型号的软硬件版本对应关系用来指定 AP 上线时使用的软件版本，仅当期望 AP 使用的软件版本与 APDB 中存储的该 AP 型号对应的软件版本不一致时才需要配置，APDB 中存储的各 AP 型号对应的软件版本可以通过 **display wlan ap-model** 命令查询。

表1-14 配置 AP 型号的软硬件版本对应关系

操作	命令	说明
进入系统视图	system-view	-
配置AP型号的软硬件版本对应关系	wlan apdb <i>model-name</i> <i>hardware-version software-version</i>	缺省情况下，AP型号的硬件版本所对应的软件版本为APDB脚本文件中存储的软件版本

1.7 配置AP的VLAN



说明

本功能的支持情况与 AP 设备的型号有关，请以设备的实际情况为准。

执行本配置后，AC 会将 VLAN 配置下发到 AP，以实现 AP 的报文转发和报文隔离业务。例如，将客户端数据报文转发位置配置在 AP 上时，需要配置 AP 的接口允许不同 VLAN 的客户端报文通过。关于 VLAN 的详细介绍请参见“二层技术-以太网交换配置指导”中的“VLAN”，关于配置客户端数据报文转发位置的详细介绍请参见“WLAN 配置指导”中的“WLAN 接入”。

1.7.1 配置VLAN基本属性

表1-15 配置 VLAN 基本属性（AP 视图）

操作	命令	说明
进入系统视图	system-view	-
进入AP视图	wlan ap <i>ap-name</i> [model <i>model-name</i>]	-
（可选）创建一个VLAN并进入VLAN视图，或批量创建VLAN	vlan { <i>vlan-id1</i> [to <i>vlan-id2</i>] all }	缺省情况下，AP上只有一个缺省VLAN（VLAN 1）
进入VLAN视图	vlan <i>vlan-id</i>	批量创建VLAN时，为必选；否则，无需执行本命令
指定当前VLAN的名称	name <i>text</i>	缺省情况下，继承AP组配置
配置当前VLAN的描述信息	description <i>text</i>	缺省情况下，继承AP组配置

表1-16 配置 VLAN 基本属性（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 <i>group-name</i>	-
（可选）创建一个VLAN并进入VLAN视图，或批量创建VLAN	vlan { <i>vlan-id1</i> [to <i>vlan-id2</i>] all }	缺省情况下，AP上只有一个缺省VLAN（VLAN 1）

操作	命令	说明
进入VLAN视图	vlan <i>vlan-id</i>	批量创建VLAN时，为必选；否则，无需执行本命令
指定当前VLAN的名称	name <i>text</i>	缺省情况下，VLAN的名称为“VLAN <i>vlan-id</i> ”，其中 <i>vlan-id</i> 为该VLAN的四位数编号，如果该VLAN的编号不足四位，则会在编号前增加0，补齐四位。例如，VLAN 100的名称为“VLAN 0100”
配置当前VLAN的描述信息	description <i>text</i>	缺省情况下，VLAN的描述信息为“VLAN <i>vlan-id</i> ”，其中 <i>vlan-id</i> 为该VLAN的四位数编号，如果该VLAN的编号不足四位，则会在编号前增加0，补齐四位。例如，VLAN 100的描述信息为“VLAN 0100”

1.7.2 配置基于端口的VLAN

1. 配置基于Access端口的VLAN

表1-17 配置基于 Access 端口的 VLAN（AP 的二层以太网接口视图）

操作	命令	说明
进入系统视图	system-view	-
进入AP视图	wlan ap <i>ap-name</i> [model <i>model-name</i>]	-
进入AP的GE接口视图	gigabitethernet <i>interface-number</i>	-
配置端口的链路类型为Access类型	port link-type access	缺省情况下，继承AP组配置
将当前Access端口加入到指定VLAN	port access vlan <i>vlan-id</i>	缺省情况下，继承AP组配置

表1-18 配置基于 Access 端口的 VLAN（AP 组的二层以太网接口视图）

操作	命令	说明
进入系统视图	system-view	-
进入AP组视图	wlan ap-group <i>group-name</i>	-
进入AP型号视图	ap-model <i>ap-model</i>	-
进入AP的GE接口视图	gigabitethernet <i>interface-number</i>	-
配置端口的链路类型为Access类型	port link-type access	缺省情况下，AP端口的链路类型为Access
将当前Access端口加入到指定VLAN	port access vlan <i>vlan-id</i>	缺省情况下，所有Access端口都属于VLAN 1 在将Access端口加入到指定VLAN

操作	命令	说明
		之前，该VLAN必须已经存在

2. 配置基于Trunk端口的VLAN

表1-19 配置基于 Trunk 端口的 VLAN（AP 的二层以太网接口视图）

操作	命令	说明
进入系统视图	system-view	-
进入AP视图	wlan ap <i>ap-name</i> [model <i>model-name</i>]	-
进入AP的GE接口视图	gigabitethernet <i>interface-number</i>	-
配置端口的链路类型为Trunk类型	port link-type trunk	缺省情况下，继承AP组配置
允许指定的VLAN通过当前Trunk端口	port trunk permit vlan { <i>vlan-id-list</i> all }	缺省情况下，继承AP组配置
（可选）配置Trunk端口的缺省VLAN	port trunk pvid vlan <i>vlan-id</i>	缺省情况下，继承AP组配置

表1-20 配置基于 Trunk 端口的 VLAN（AP 组的二层以太网接口视图）

操作	命令	说明
进入系统视图	system-view	-
进入AP组视图	wlan ap-group <i>group-name</i>	-
进入AP型号视图	ap-model <i>ap-model</i>	-
进入AP的GE接口视图	gigabitethernet <i>interface-number</i>	-
配置端口的链路类型为Trunk类型	port link-type trunk	缺省情况下，AP端口的链路类型为Access类型
允许指定的VLAN通过当前Trunk端口	port trunk permit vlan { <i>vlan-id-list</i> all }	缺省情况下，AP的Trunk端口只允许VLAN 1的报文通过
（可选）配置Trunk端口的缺省VLAN	port trunk pvid vlan <i>vlan-id</i>	缺省情况下，AP的Trunk端口的缺省VLAN为VLAN 1

3. 配置基于Hybrid端口的VLAN

表1-21 配置基于 Hybrid 端口的 VLAN（AP 的二层以太网接口视图）

操作	命令	说明
进入系统视图	system-view	-
进入AP视图	wlan ap <i>ap-name</i> [model <i>model-name</i>]	-
进入AP的GE接口视图	gigabitethernet <i>interface-number</i>	-
配置端口的链路类型为Hybrid类型	port link-type hybrid	缺省情况下，继承AP组配置

操作	命令	说明
允许指定的VLAN通过当前Hybrid端口	port hybrid vlan <i>vlan-id-list</i> { tagged untagged }	缺省情况下，继承AP组配置
(可选) 配置Hybrid端口的缺省VLAN	port hybrid pvid vlan <i>vlan-id</i>	缺省情况下，继承AP组配置

表1-22 配置基于 Hybrid 端口的 VLAN（AP 组的二层以太网接口视图）

操作	命令	说明
进入系统视图	system-view	-
进入AP组视图	wlan ap-group <i>group-name</i>	-
进入AP型号视图	ap-model <i>ap-model</i>	-
进入AP的GE接口视图	gigabitethernet <i>interface-number</i>	-
配置端口的链路类型为Hybrid类型	port link-type hybrid	缺省情况下，AP端口的链路类型为Access类型
允许指定的VLAN通过当前Hybrid端口	port hybrid vlan <i>vlan-id-list</i> { tagged untagged }	缺省情况下，AP的Hybrid端口只允许该端口在链路类型为Access时的所属VLAN的报文以Untagged方式通过
(可选) 配置Hybrid端口的缺省VLAN	port hybrid pvid vlan <i>vlan-id</i>	缺省情况下，AP的Hybrid端口的缺省VLAN为该端口在链路类型为Access时的所属VLAN

1.7.3 向AP下发VLAN配置

开启远程配置同步功能后，AC 才会向 AP 下发 AP 视图或 AP 组视图下的 VLAN 相关配置。

表1-23 向 AP 下发 VLAN 配置（AP 视图）

操作	命令	说明
进入系统视图	system-view	-
进入AP视图	wlan ap <i>ap-name</i> [model <i>model-name</i>]	-
配置远程配置同步功能	remote-configuration { disable enable }	缺省情况下，继承AP组配置

表1-24 向 AP 下发 VLAN 配置（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 <i>group-name</i>	-
配置远程配置同步功能	remote-configuration { disable	缺省情况下，远程配置同步功能处

操作	命令	说明
	enable }	于关闭状态

1.8 配置CAPWAP隧道

1.8.1 配置CAPWAP隧道延迟检测

CAPWAP 控制隧道延迟是指 AC 发送 Configuration update request 报文与收到 Configuration update response 响应报文的时间间隔，CAPWAP 数据隧道延迟是指 AP 发送 Data channel keep alive 报文与收到 Data channel keep alive 回复报文的时间间隔。CAPWAP 隧道延迟检测用于统计 AP 和 AC 之间的 CAPWAP 隧道延迟时间，便于及时了解 CAPWAP 隧道报文传输的延迟状况。

只有在 AP 和 AC 建立了 CAPWAP 隧道并且当前 AC 为主 AC 时，CAPWAP 隧道延迟检测功能才生效。当 AP 下线，CAPWAP 隧道延迟检测将自动停止。AP 重新上线后，如果需要再次进行 CAPWAP 隧道延迟检测，则需要重新执行 CAPWAP 隧道延迟检测。

用户可以使用 **display wlan tunnel latency ap name** 命令查看 CAPWAP 隧道延迟检测信息。

表1-25 配置 CAPWAP 隧道延迟检测

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CAPWAP隧道延迟检测	tunnel latency-detect { start stop }	缺省情况下，未启动CAPWAP隧道延迟检测

1.8.2 配置CAPWAP隧道保活

AP 和 AC 之间通过保活机制来检查控制隧道是否正常工作。AP 周期性地向 AC 发送回声请求 Echo request 报文，若在保活时间内没有收到 AC 回复的 Echo response 报文，则 AP 断开控制隧道；若 AC 在保活时间内没有收到 Echo request 报文，则 AC 断开控制隧道。保活时间为 Echo request 报文的发送时间间隔乘以最大发送次数。

表1-26 配置 CAPWAP 隧道保活（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发送回声请求的时间间隔	echo-interval interval	缺省情况下，继承AP组配置
AP发送回声请求报文的最大发送次数	echo-count count	缺省情况下，继承AP组配置

表1-27 配置 CAPWAP 隧道保活（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 <i>group-name</i>	进入AP组视图
配置AP发送回声请求的时间间隔	echo-interval <i>interval</i>	缺省情况下，AP发送回声请求的时间间隔为10秒
AP发送回声请求报文的最大发送次数	echo-count <i>count</i>	缺省情况下，AP发送回声请求报文的最大次数为3次

1.8.3 配置AP发送CAPWAP数据隧道keep alive报文的时间间隔

AP 与 AC 建立 CAPWAP 隧道后，AP 会定时发送 Data channel keep alive 报文，可以通过该功能配置 AP 发送 CAPWAP 数据隧道 keep alive 报文的时间间隔。

表1-28 配置 AP 发送 CAPWAP 数据隧道 keep alive 报文的时间间隔（AP 视图）

操作	命令	说明
进入系统视图	system-view	-
进入AP视图	wlan ap <i>ap-name</i> [model <i>model-name</i>]	-
配置AP发送CAPWAP数据隧道 keep alive报文的时间间隔	keepalive-interval <i>interval</i>	缺省情况下，继承AP组配置

表1-29 配置 AP 发送 CAPWAP 数据隧道 keep alive 报文的时间间隔（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 <i>group-name</i>	进入AP组视图
配置AP发送CAPWAP数据隧道 keep alive报文的时间间隔	keepalive-interval <i>interval</i>	缺省情况下，AP发送CAPWAP数据隧道keep alive报文的时间间隔为10秒

1.8.4 配置CAPWAP报文分片的最大长度

当 AC 与 AP 跨越 Internet 建立连接时，由于传输路径上的设备可能对报文分片大小进行限制，超过分片门限的报文将被丢弃，因此，需要配置 CAPWAP 控制报文与数据报文分片长度，使其顺利通过中间设备。

修改 CAPWAP 报文分片长度后，新配置对已在线的 AP 立即生效。

表1-30 配置 CAPWAP 报文分片的最大长度（AP 视图）

操作	命令	说明
进入系统视图	system-view	-
进入AP视图	wlan ap <i>ap-name</i> [model <i>model-name</i>]	-
配置CAPWAP控制报文或数据报文分片的最大长度	fragment-size { control <i>control-size</i> data <i>data-size</i> }	缺省情况下，继承AP组配置

表1-31 配置 CAPWAP 报文分片的最大长度（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 <i>group-name</i>	进入AP组视图
配置CAPWAP控制报文或数据报文分片的最大长度	fragment-size { control <i>control-size</i> data <i>data-size</i> }	缺省情况下，CAPWAP控制报文分片的最大长度为1450字节，CAPWAP数据报文分片的最大长度为1500字节

1.8.5 配置CAPWAP隧道的TCP最大报文段长度

1. 功能简介

MSS（Max Segment Size，TCP 最大报文段长度）表示 TCP 连接的对端发往本端的最大 TCP 报文段的长度。当一个 TCP 连接建立时，连接的双方要将 MSS 作为 SYN 报文的一个选项通告给对端，对端会记录下这个 MSS 值，后续在发送 TCP 报文时，会限制 TCP 报文的大小不超过该 MSS 值。当对端发送的 TCP 报文的长度小于等于本端的 TCP 最大报文段长度时，TCP 报文不需要分段；否则，对端需要对 TCP 报文按照最大报文段长度进行分段处理后再发给本端。

配置本功能后，当通过 CAPWAP 封装发送 SYN 报文时，会将 SYN 报文中携带的 TCP 最大报文段长度设置为指定值。

2. 配置步骤

表1-32 配置 CAPWAP 隧道的 TCP 最大报文段长度

操作	命令	说明
进入系统视图	system-view	-
配置CAPWAP隧道的TCP最大报文段长度	wlan tcp mss <i>value</i>	缺省情况下，CAPWAP隧道的TCP最大报文段长度为1460字节

1.9 配置请求报文重传

AC 发送给 AP 的请求报文可能由于各种原因导致未能传输到 AP，为了使 AC 的请求报文尽可能的发送到 AP，提高报文的可靠传输能力，可以配置对请求报文重传。

表1-33 配置请求报文重传（AP 视图）

操作	命令	说明
进入系统视图	system-view	-
进入AP视图	wlan ap <i>ap-name</i> [model <i>model-name</i>]	-
配置请求报文重传次数	retransmit-count <i>value</i>	缺省情况下，继承AP组配置
配置请求报文重传时间间隔	retransmit-interval <i>interval</i>	缺省情况下，继承AP组配置

表1-34 配置请求报文重传（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 <i>group-name</i>	进入AP组视图
配置请求报文重传次数	retransmit-count <i>value</i>	缺省情况下，请求报文重传次数为3次
配置请求报文重传时间间隔	retransmit-interval <i>interval</i>	缺省情况下，请求报文重传的时间间隔为5秒

1.10 配置上报Radio统计信息

为了对 AP 上的 Radio 的运行情况进行有效监控，AP 会周期性的向 AC 上报 Radio 统计信息。

表1-35 配置 AP 上报 Radio 统计信息（AP 视图）

操作	命令	说明
进入系统视图	system-view	-
进入AP视图	wlan ap <i>ap-name</i> [model <i>model-name</i>]	-
配置AP向AC上报Radio统计信息的时间间隔	statistics-interval <i>interval</i>	缺省情况下，继承AP组配置

表1-36 配置 AP 上报 Radio 统计信息（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 <i>group-name</i>	进入AP组视图
配置AP向AC上报Radio统计信息的时间间隔	statistics-interval <i>interval</i>	缺省情况下，AP向AC上报Radio统计信息的时间间隔为50秒

1.11 配置Remote AP功能

缺省情况下，当 AP 与 AC 之间的隧道断开后，AP 将停止为客户端提供服务。Remote AP 功能支持在 AP 与 AC 之间的隧道断开后，AP 能够继续为客户端提供服务。开启 Remote AP 功能后，如果认证方式为本地认证且客户端关联位置在 AP 上时，AP 能够继续为客户端转发数据并提供接入功能；否则 AP 仅支持继续为客户端转发数据，不能提供接入功能。

仅当客户端数据报文的转发位置在 AP 上时，Remote AP 功能才会生效。

当 AP 与 AC 重新建立隧道后，用户接入认证位置在 AC 上的客户端需要重新上线，用户接入认证位置在 AP 上的客户端保持在线状态。

远程 AP 功能可以用于远程办公、小分支机构或家庭办公解决方案。

表1-37 配置 Remote AP 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 <i>ap-name</i> [model <i>model-name</i>]	-
配置Remote AP功能	hybrid-remote-ap { disable / enable }	缺省情况下，继承AP组配置

表1-38 配置 Remote AP 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 <i>group-name</i>	-
配置Remote AP功能	hybrid-remote-ap { disable / enable }	缺省情况下，Remote AP功能处于关闭状态

1.12 开启/关闭AP的USB接口



说明

本功能的支持情况与 AP 设备的型号有关，请以设备的实际情况为准。

表1-39 开启/关闭 AP 的 USB 接口（AP 视图）

操作	命令	说明
进入系统视图	system-view	-
进入AP视图	wlan ap <i>ap-name</i> [model <i>model-name</i>]	-
开启/关闭AP的USB接口	usb { enable disable }	缺省情况下，继承AP组配置

表1-40 开启/关闭 AP 的 USB 接口（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 <i>group-name</i>	-
进入AP型号视图	ap-model <i>ap-model</i>	-
开启/关闭AP的USB接口	usb { enable disable }	缺省情况下，AP的USB接口处于关闭状态

1.13 重启AP

表1-41 在用户视图下重启 AP

操作	命令	说明
重启AP	reset wlan ap { all ap-group <i>group-name</i> model <i>model-name</i> name <i>ap-name</i> }	-

1.14 重命名手工AP

表1-42 重命名手工 AP

操作	命令	说明
进入系统视图	system-view	-
重命名手工AP	wlan rename-ap <i>ap-name</i> <i>new-ap-name</i>	-

1.15 管理AP的文件系统

当 CAPWAP 隧道建立成功后，用户可以查看、删除 AP 上的文件，也可以将 AC 上存储的文件下发给 AP。需要注意的是，只有在 AP 和 AC 建立了 CAPWAP 隧道并且当前 AC 为主 AC 时，才能执行以上操作。

表1-43 管理 AP 的文件系统

操作	命令	说明
显示AP上的文件及文件夹信息	display wlan ap files <i>name</i> <i>ap-name</i>	-
进入系统视图	system-view	-
进入AP视图	wlan ap <i>ap-name</i> [model <i>model-name</i>]	-

操作	命令	说明
删除AP上的文件	delete file filename	-
下载指定文件到AP	download file file-name	-

1.16 配置AP组

1.16.1 AP组简介

AP 组用来实现对批量 AP 的配置管理，通过使 AP 继承其所属组的配置来达到对大量 AP 的配置的目的。AP 组配置，全局配置及 AP 配置共同构成了分级继承的 AP 运行配置。在大规模无线网络中，同一 AC 管理的 AP 数量可达几万台，对每一台 AP 逐一配置将导致网络管理难度极大提高。AP 组用来降低逐个配置 AP 的操作成本，用户可以创建多个组，对不同的组用户可以根据需要配置不同的 AP 配置。

所有 AP 缺省情况下均属于默认组，默认组组名为 **default-group**，默认组不需创建、不可删除。

AP 组可以指定多个 AP 名字、AP 序列号、AP MAC 地址和 IP 网段四种入组规则，AP 的入组匹配顺序为：优先根据 AP 名字入组规则匹配入组，其次是 AP 序列号入组规则，然后是 AP MAC 地址入组规则，最后是 IP 网段入组规则，若未匹配到任何入组规则，则 AP 将被加入到默认组。

需要注意的是：

- AP 必须属于一个 AP 组，且只能属于一个 AP 组。
- 同一入组规则不能重复出现在不同的 AP 组中，若将同一入组规则配置在新 AP 组中，将导致原 AP 组中对应的入组规则自动删除（相当于迁移组）。
- 默认组不能配置任何 AP 入组规则。
- 删除 AP 入组规则，AP 会根据 AP 的入组规则匹配顺序重新匹配 AP 组。
- AP 组下有 AP 已经入组（手工 AP 或自动 AP），则该 AP 组不允许删除；配置了入组规则，但是没有 AP 入组的 AP 组可以被删除。
- AP 的生效配置取决于 AP、AP 组及 AP 全局配置中优先级最高的配置，优先级从高到低为 AP 配置、AP 组配置、全局配置。若优先级高的配置不存在，则 AP 使用优先级低的配置。若都不存在 AP 的配置，则使用缺省值。
- 同一 AP 组（或者不同 AP 组）的 IPv4 网段入组规则或 IPv6 网段入组规则不能重叠或相互包含。
- 同一 AP 组下最多能够配置 32 条 IPv4 网段入组规则或 IPv6 网段入组规则。

1.16.2 创建AP组

创建 AP 组，在 AP 组视图下可以配置 AP 名称、序列号、MAC 地址入组规则和 IPv4 或 IPv6 网段入组规则。AP 将按照如下先后顺序匹配入组规则：AP 名称入组规则-->AP 序列号入组规则-->AP MAC 地址入组规则-->IPv4 网段入组规则或 IPv6 网段入组规则。若 AP 未匹配到入组规则，则将被加入默认组。

表1-44 创建 AP 组

操作	命令	说明
进入系统视图	system-view	-
创建AP组并进入AP组视图	wlan ap-group <i>group-name</i>	缺省情况下，存在默认组 default-group ，不允许删除
(可选) 配置AP组描述信息	description <i>text</i>	缺省情况下，未配置AP组描述信息
配置AP名称入组规则	ap <i>ap-name-list</i>	请根据实际需要进行选择
配置AP序列号入组规则	serial-id <i>serial-id</i>	
配置AP MAC地址入组规则	mac-address <i>mac-address</i>	
配置IPv4网段入组规则	if-match ip <i>ip-address</i> { <i>mask-length</i> <i>mask</i> }	
配置IPv6网段入组规则	if-match ipv6 { <i>ipv6-address</i> <i>prefix-length</i> <i>ipv6-address/prefix-length</i> }	
(可选) 配置迁移入组规则	wlan re-group { ap <i>ap-name</i> ap-group <i>old-group-name</i> mac-address <i>mac-address</i> serial-id <i>serial-id</i> } <i>group-name</i>	-

1.17 预配置

1.17.1 预配置简介

通常情况下，可以通过终端连接到 AP 之后，对 AP 进行配置，但这种逐台配置 AP 的操作方式不利于大规模的 AP 部署以及集中化管理。AP 预配置提供了一种在 AC 上对 AP 的基本网络参数进行配置，并将预配置信息下发至 AP 的方法。下发到 AP 的配置会保存为 AP 私有预配置文件 `wlan_ap_prvs.xml`。

需要注意的是：

- AC 只能将预配置信息发送给与它建立 CAPWAP 隧道的 AP（即 AP 当前处于 Run 状态），同时只有主 AC 才能对已经与它建立 CAPWAP 隧道的 AP 进行预配置。
- 预配置可以在 AP provision 视图下和 AP 组 provision 视图下同时配置，AP provision 视图和 AP 组 provision 视图都可以配置的参数，则 AP provision 视图下的配置优先级高。
- 如果在 AC 上对预配置作了修改，则需要将预配置重新下发到 AP 上。
- 如果不存在预配置，执行 **save wlan ap-provision** 命令等效于执行 **reset wlan ap provision** 命令。
- 在 provision 视图下进行的预配置在执行 **save wlan ap-provision** 命令后会立即生效。
- 在 provision 视图下进行取消预配置的 undo 操作时，在执行 **save wlan ap-provision** 命令后不会立即生效，在 AP 重启后生效。
- 执行 **reset wlan ap provision** 命令后不会立即生效，在 AP 重启后生效。

1.17.2 配置AP预配置

表1-45 配置 AP 预配置

操作	命令	说明
进入系统视图	system-view	-
进入AP视图	wlan ap <i>ap-name</i> [model <i>model-name</i>]	-
开启预配置功能，并进入AP预配置视图	provision	缺省情况下，继承AP组配置
配置AP静态发现使用的AC的IP地址或主机名	ac { host-name <i>host-name</i> ip <i>ipv4-address</i> ipv6 <i>ipv6-address</i> }	缺省情况下，继承AP组配置
配置AP的管理VLAN接口的IP地址	ip address <i>ip-address</i> { mask mask-length }	缺省情况下，未配置AP的管理VLAN接口的IP地址
配置AP的管理VLAN接口的IPv6地址	ipv6 address { <i>ipv6-address</i> prefix-length <i>ipv6-address/prefix-length</i> }	缺省情况下，未配置AP的管理VLAN接口的IPv6地址
配置AP的网关地址	gateway { ip <i>ipv4-address</i> ipv6 <i>ipv6-address</i> }	缺省情况下，未配置AP的网关地址
配置AP使用的域名服务器的IP地址	dns server { ip <i>ipv4-address</i> ipv6 <i>ipv6-address</i> }	缺省情况下，继承AP组配置
配置AP使用的域名服务器的域名后缀	dns domain <i>domain-name</i>	缺省情况下，继承AP组配置

1.17.3 配置AP组预配置

AP 组预配置仅对 AP 组内的 AP 生效。

表1-46 配置 AP 组预配置

操作	命令	说明
进入系统视图	system-view	-
进入AP组视图	wlan ap-group <i>group-name</i>	-
开启预配置功能，并进入AP组预配置视图	provision	缺省情况下，预配置功能处于关闭状态
配置AP静态发现使用的AC的IP地址或主机名	ac { host-name <i>host-name</i> ip <i>ip-address</i> ipv6 <i>ipv6-address</i> }	缺省情况下，未配置AP静态发现使用的AC的IP地址或主机名
配置AP使用的域名服务器的IP地址	dns server { ip <i>ip-address</i> ipv6 <i>ipv6-address</i> }	缺省情况下，未配置AP使用的域名服务器的IP地址
配置AP使用的域名服务器的域名后缀	dns domain <i>domain-name</i>	缺省情况下，未配置AP使用的域名服务器的域名后缀

1.17.4 下发预配置

AC 可以将预配置信息下发给与它建立 CAPWAP 隧道的 AP，并保存到该 AP 的私有预配置文件中。下发的预配置信息将完全覆盖私有预配置文件中保存的预配置。

- 通过手工下发预配置，可以将预配置下发给已经在线的 AP；
- 通过开启自动下发预配置功能，可以为正在上线的 AP 下发预配置，AP 将与预配置中指定的 AC 建立 CAPWAP 隧道并完成上线。有关 AP 选择最优 AC 进行上线的流程，请参考 [1.1.1](#) [2. CAPWAP 隧道建立过程](#)。



说明

由于手工下发预配置的方式可以立即在已上线 AP 上生效，因而更改预配置中的 AC 地址会触发 AP 立即重新选择最优 AC，如果 AP 选择了其它 AC 进行上线，会拆除原 CAPWAP 隧道并中断流量转发，直至在新的 AC 上完成上线。

1. 手工下发预配置

表1-47 手工下发预配置（任意视图）

操作	命令	说明
手工下发预配置	save wlan ap provision { all name ap-name }	-

2. 自动下发预配置

表1-48 自动下发预配置（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AC自动下发预配置功能	provision auto-update { disable enable }	缺省情况下，继承AP组配置

表1-49 自动下发预配置（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	进入AP组视图
配置AC自动下发预配置功能	provision auto-update { disable enable }	缺省情况下，AC自动下发预配置功能处于关闭状态

1.17.5 配置预配置智能加载功能

预配置智能加载功能用于确保 AP 尽可能的与 AC 建立 CAPWAP 连接。开启预配置智能加载功能后：

- 如果 AP 使用预配置无法找到存在手工 AP 或自动 AP 配置的 AC，当 AP 重启后，则不使用预配置来发现 AC。
- 如果 AP 不使用预配置也无法找到存在手工 AP 或自动 AP 配置的 AC，当 AP 重启后，将再次使用预配置来发现 AC。

如果 AP 一直无法找到 AC 来建立 CAPWAP 隧道，将重复上述过程。

表1-50 配置预配置智能加载功能（AP 视图）

操作	命令	说明
进入系统视图	system-view	-
进入AP视图	wlan ap <i>ap-name</i> [model <i>model-name</i>]	-
配置预配置智能加载功能	provision auto-recovery { disable enable }	缺省情况下，继承AP组配置

表1-51 配置预配置智能加载功能（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 <i>group-name</i>	-
配置预配置智能加载功能	provision auto-recovery { disable enable }	缺省情况下，预配置智能加载功能处于开启状态

1.18 开启告警功能

1.18.1 告警功能简介

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”。）

1.18.2 开启AP管理的告警功能

表1-52 开启 AP 管理的告警功能

操作	命令	说明
进入系统视图	system-view	-
开启AP管理的告警功能	snmp-agent trap enable wlan ap	缺省情况下，AP管理的告警功能处于关闭状态

1.18.3 开启CAPWAP的告警功能

表1-53 开启 CAPWAP 告警功能

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

1.19 加载APDB用户脚本

当用户需要在不升级 AC 版本的情况下，让 AC 支持新 AP 型号，可以使用新 AP 型号的信息生成用户脚本文件，并将其加载到 APDB 中。

加载 APDB 用户脚本文件时，需要注意以下几点：

- 加载 APDB 脚本文件时，需要保证脚本文件的合法性，不合法的脚本文件会导致加载失败。
- 用户脚本中的 AP 型号加载时不能与系统脚本中 AP 型号重复。
- 用户脚本只能加载一个，多次加载用户脚本，最后一次加载的脚本生效。
- 若 AC 上已加载的脚本中某个 AP 型号已经被配置为手工 AP 或者已经存在上线的自动 AP，则不允许重新加载脚本文件，需要将对应的 AP 型号删除后才能重新加载。
- 若已加载的脚本中的某个 AP 型号已经被加入 AP 组，则不允许重新加载脚本文件，需要将对应的 AP 型号从 AP 组删除后才能重新加载。
- 若在文件系统中将用户脚本文件进行重命名，需要重新加载脚本文件，否则当 AC 重启后将丢失对应用户脚本文件的 AP 型号配置。
- 若在文件系统中将用户脚本文件进行替换，需要重新加载新脚本文件，如果新脚本中不包含被替换脚本中的 AP 型号信息，当 AC 重启后将丢失对应被替换脚本文件的 AP 型号配置。
- 若在文件系统中将用户脚本文件进行删除，当 AC 重启后将丢失该用户脚本文件的 AP 型号配置。
- 若旧脚本中的某个 AP 型号已经进行了软件版本配置，则不允许替换操作，需要使用 **wlan apdb** 命令将对应的软件版本还原到初始版本后才能重新加载。关于 **wlan apdb** 命令的详细介绍，请参见“WLAN 命令参考”中的“AP 管理”。

表1-54 加载 APDB 用户脚本文件

操作	命令	说明
进入系统视图	system-view	-
加载APDB用户脚本	wlan apdb file user.apdb	缺省情况下，未加载APDB用户脚本文件

1.20 配置重启业务异常AC功能

1. 功能简介

开启该功能后，AC 会检测自身的业务状态，当关联的 AP 数为 0 时 AC 会创建定时器，定时器超时时间为 10 分钟，定时器超时后 AC 会进行重启，如果在定时器超时之前有 AP 上线，则 AC 会删除定时器。

2. 配置步骤

表1-55 配置重启业务异常 AC 功能

操作	命令	说明
进入系统视图	system-view	-
开启重启业务异常AC功能	wlan detect-anomaly enable	缺省情况下，重启业务异常AC功能处于关闭状态

1.21 AP管理显示和维护

1.21.1 配置LED闪烁模式

LED 闪烁模式包括四种模式：

- **Quiet 模式：**表示所有 LED 常灭。
- **Awake 模式：**表示所有 LED 每分钟闪烁一次。Awake 模式的支持情况与 AP 设备的型号有关，请以设备的实际情况为准。
- **Always-on 模式：**表示所有 LED 常亮。Always-on 模式的支持情况与 AP 设备的型号有关，请以设备的实际情况为准。
- **Normal 模式：**用来标识 AP 的运行状态，该模式 LED 闪烁情况与 AP 设备的型号有关，请以设备实际情况为准。

在 AP 组视图下配置 LED 闪烁模式为 Awake 模式或 Always-on 模式时，仅对组内支持该模式的 AP 生效。

表1-56 配置 LED 闪烁模式（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LED闪烁模式	led-mode { always-on awake normal quiet }	缺省情况下，继承AP组配置

表1-57 配置 LED 闪烁模式（AP 组视图）

操作	命令	说明
进入系统视图	system-view	-

操作	命令	说明
创建AP组并进入AP组视图	wlan ap-group <i>group-name</i>	缺省情况下，存在默认组 default-group，不允许删除
配置LED闪烁模式	led-mode { always-on awake normal quiet }	缺省情况下，LED的闪烁模式为 Normal模式

1.21.2 显示AP管理信息

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

表1-58 显示 AP 管理信息

操作	命令
显示指定AP或所有AP的信息	display wlan ap { all name <i>ap-name</i> } [verbose]
显示AP地址信息	display wlan ap { all name <i>ap-name</i> } address
显示CAPWAP隧道的配置状态	display wlan ap all feature capwap
显示AC上的AP连接记录	display wlan ap connection record { all name <i>ap-name</i> }
显示AP的关联时长	display wlan ap online-time { all name <i>ap-name</i> }
显示指定AP的重启日志信息	display wlan ap reboot-log name <i>ap-name</i>
显示指定AP或所有AP的运行配置	display wlan ap running-configuration { all ap-name <i>ap-name</i> } [verbose]
显示AP上线失败原因	display wlan ap statistics association-failure-record
显示AP在线数量的统计信息	display wlan ap statistics online-record [datetime <i>date time</i> [count <i>count</i>]]
显示AC与AP间CAPWAP隧道断开的原因	display wlan ap statistics tunnel-down-record
显示AP组信息	display wlan ap-group [brief name <i>group-name</i>]
显示AP型号的信息	display wlan ap-model { all name <i>model-name</i> }
显示指定AP的隧道延迟信息	display wlan tunnel latency ap name <i>ap-name</i>
显示AC上的AP负载信息	display wlan ap-distribution { all slot <i>slot-number</i> }
显示指定AP的负载位置	display wlan ap-distribution ap-name <i>ap-name</i>

1.21.3 清除AP管理信息

在用户视图下执行 **reset** 命令清除 AP 管理的相关信息。

表1-59 清除 AP 管理信息

操作	命令
清除指定AP或全部AP的重启日志信息	<code>reset wlan ap reboot-log { all name ap-name }</code>
清除AP的隧道延迟信息	<code>reset wlan tunnel latency ap { all name ap-name }</code>
删除AP的预配置文件	<code>reset wlan ap provision { all name ap-name }</code>

1.22 AP管理典型配置举例

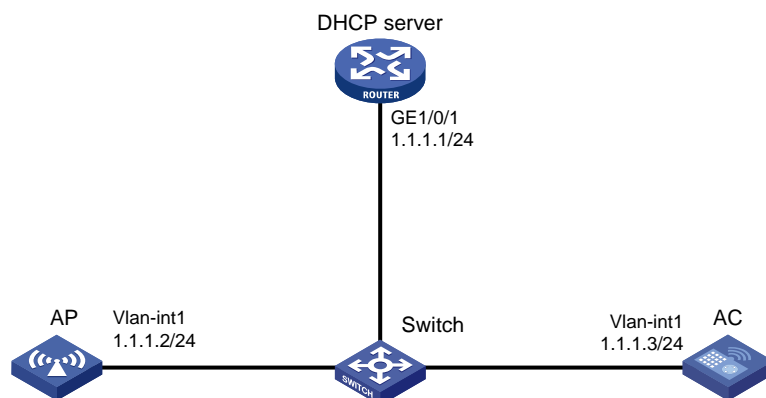
1.22.1 配置通过DHCP发现方式建立CAPWAP隧道举例

1. 组网需求

AP 通过 DHCP 选项方式从 DHCP server 上获取 AP 和 AC 的 IP 地址，发现 AC 并与 AC 建立 CAPWAP 隧道连接。

2. 组网图

图1-3 通过 DHCP 发现方式建立 CAPWAP 隧道典型组网图



3. 配置步骤

(1) 配置 DHCP server

使能 DHCP 服务器功能。

```
<DHCP Server> system-view
[DHCP Server] dhcp enable
```

配置 DHCP 地址池 1。

```
[DHCP Server] dhcp server ip-pool 1
[DHCP Server-dhcp-pool-1] network 1.1.1.0 mask 255.255.255.0
```

通过自定义选项的方式配置 Option 43 的内容，为 AP 指定 AC 的 IP 地址 1.1.1.3，注意 Option 43 选项内容中最后四字节为 01010103（1.1.1.3），即为 AC 的 IP 地址。

```
[DHCP Server-dhcp-pool-1] option 43 hex 800700000101010103
[DHCP Server-dhcp-pool-1] quit
[DHCP Server] quit
```

(2) 配置 AC

配置 AC 的 VLAN-interface 1 的 IP 地址为 1.1.1.3/24。

```
<AC> system-view
[AC] interface vlan-interface 1
[AC-Vlan-interface1] ip address 1.1.1.3 24
```

创建 ap1，配置序列号为 219801A1FF8171E00361。

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

AP 启动后，DHCP server 会给 AP 自动分配 IP 地址 1.1.1.2，同时由于 Option 43 选项携带 AC 的 IP 地址 1.1.1.3。AP 拥有了自动分配的本地 IPv4 地址和需要建立关联的 AC 的 IP 地址 1.1.1.3，就会开始发现 AC 的过程并建立 CAPWAP 隧道。

4. 验证配置

查看 AP 的详细信息，可以看到 AP 与 AC 成功建立隧道连接并进入 Run 状态，发现方式为 DHCP 选项方式。

```
[AC] display wlan ap name ap1 verbose
AP name                : ap1
AP ID                   : 1
AP group name          : default-group
State                   : Run
Backup type             : Master
Online time             : 0 days 1 hours 25 minutes 12 seconds
System up time         : 0 days 2 hours 22 minutes 12 seconds
Model                   : WA5320E-WiNet
Region code            : CN
Region code lock       : Disable
Serial ID               : 219801A1FF8171E00361
MAC address             : 0AFB-423B-893C
IP address              : 192.168.1.50
UDP port number        : 18313
H/W version             : Ver.C
S/W version             : R2206P02
Boot version           : 1.01
USB state               : N/A
Power Level             : N/A
PowerInfo               : N/A
Description             : wtpl
Priority                 : 4
Echo interval          : 10 seconds
Echo count              : 3 counts
Keepalive interval     : 10 seconds
Statistics report interval : 50 seconds
Fragment size (data)   : 1500
Fragment size (control) : 1450
MAC type                : Local MAC & Split MAC
Tunnel mode             : Local Bridging & 802.3 Frame & Native Frame
```

```

Discovery type           : DHCP
Retransmission count    : 3
Retransmission interval : 5 seconds
Firmware upgrade        : Enabled
Sent control packets    : 1
Received control packets : 1
Echo requests           : 147
Lost echo responses     : 0
Average echo delay      : 3
Last reboot reason      : User soft reboot
Latest IP address       : 10.1.0.2
Tunnel down reason      : Request wait timer expired
Connection count        : 1
Backup Ipv4             : Not configured
Backup Ipv6             : Not configured
Tunnel encryption       : Disabled
LED mode                 : Normal
Remote configuration    : Enabled
Radio 1:
  Basic BSSID           : 7848-59f6-3940
  Admin state           : Up
  Radio type            : 802.11ac
  Antenna type          : internal
  Client dot11lac-only  : Disabled
  Client dot11n-only    : Disabled
  Channel band-width    : 20/40/80MHz
  Active band-width     : 20/40/80MHz
  Secondary channel offset : SCB
  Short GI for 20MHz    : Supported
  Short GI for 40MHz    : Supported
  Short GI for 80MHz    : Supported
  Short GI for 160MHz   : Not supported
  A-MSDU                : Enabled
  A-MPDU                : Enabled
  LDPC                  : Not Supported
  STBC                  : Supported
Operational VHT-MCS Set:
  Mandatory             : Not configured
  Supported              : NSS1 0,1,2,3,4,5,6,7,8,9
                        NSS2 0,1,2,3,4,5,6,7,8,9
  Multicast             : Not configured
Operational HT MCS Set:
  Mandatory             : Not configured
  Supported              : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                        10, 11, 12, 13, 14, 15
  Multicast             : Not configured
Channel                 : 44(auto)
Channel usage(%)        : 15

```



```

Max power                : 20 dBm
Operational rate:
  Mandatory               : 6, 12, 24 Mbps
  Multicast               : Auto
  Supported               : 9, 18, 36, 48, 54 Mbps
  Disabled               : Not configured
Distance                 : 1 km
ANI                     : Enabled
Fragmentation threshold : 2346 bytes
Beacon interval         : 100 TU
Protection threshold    : 2346 bytes
Long retry threshold    : 4
Short retry threshold   : 7
Maximum rx duration     : 2000 ms
Noise Floor             : -102 dBm
MU-TxBF                 : Enabled
SU-TxBF                 : Enabled
Protection mode         : rts-cts
Continuous mode         : N/A
HT protection mode      : No protection
Radio 2:
  Basic BSSID            : 7848-59f6-3950
  Admin state           : Down
  Radio type            : 802.11b
  Antenna type         : internal
  Client dot11n-only   : Disabled
  Channel band-width    : 20MHz
  Active band-width     : 20MHz
  Secondary channel offset : SCN
  Short GI for 20MHz    : Supported
  Short GI for 40MHz    : Supported
  A-MSDU               : Enabled
  A-MPDU               : Enabled
  LDPC                 : Not Supported
  STBC                 : Supported
Operational HT MCS Set:
  Mandatory             : Not configured
  Supported             : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                        10, 11, 12, 13, 14, 15
  Multicast             : Not configured
Channel                 : 5(auto)
Channel usage(%)       : 0
Max power               : 20 dBm
Preamble type          : Short
Operational rate:
  Mandatory             : 1, 2, 5.5, 11 Mbps
  Multicast             : Auto
  Supported             : 6, 9, 12, 18, 24, 36, 48, 54 Mbps

```

```

        Disabled                : Not configured
Distance                : 1 km
ANI                      : Enabled
Fragmentation threshold : 2346 bytes
Beacon interval         : 100 TU
Protection threshold     : 2346 bytes
Long retry threshold     : 4
Short retry threshold    : 7
Maximum rx duration     : 2000 ms
Noise Floor              : 0 dBm
Protection mode          : rts-cts
Continuous mode          : N/A
HT protection mode       : No protection

```

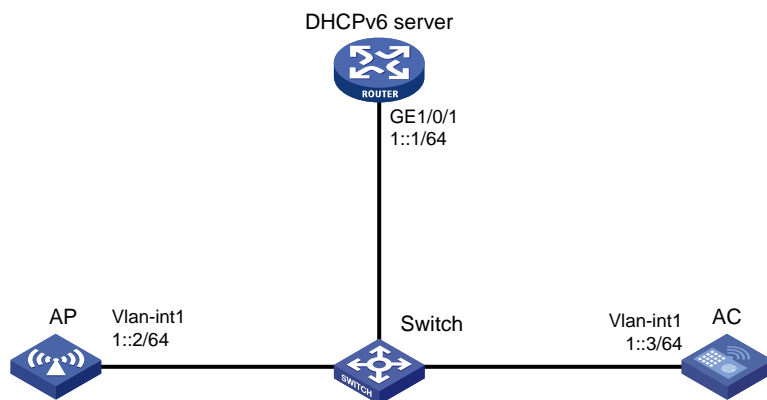
1.22.2 配置通过DHCPv6 发现方式建立CAPWAP隧道举例

1. 组网需求

AP 通过 DHCPv6 选项方式从 DHCPv6 server 上获取 AP 和 AC 的 IP 地址，发现 AC 并与 AC 建立 CAPWAP 隧道连接。

2. 组网图

图1-4 通过 DHCPv6 发现方式建立 CAPWAP 隧道典型组网图



3. 配置步骤

(1) 配置 DHCPv6 server

配置接口 GigabitEthernet1/0/1 的 IPv6 地址。取消设备发布 RA 消息的抑制。配置被管理地址的配置标志位为 1，即主机通过 DHCPv6 服务器获取 IPv6 地址。配置其他信息配置标志位为 1，即主机通过 DHCPv6 服务器获取除 IPv6 地址以外的其他信息。

```

<DHCPv6 Server> system-view
[DHCPv6 Server] interface gigabitethernet 1/0/1
[DHCPv6 Server-GigabitEthernet1/0/1] ipv6 address 1::1/64
[DHCPv6 Server-GigabitEthernet1/0/1] undo ipv6 nd ra halt
[DHCPv6 Server-GigabitEthernet1/0/1] ipv6 nd autoconfig managed-address-flag
[DHCPv6 Server-GigabitEthernet1/0/1] ipv6 nd autoconfig other-flag

```

配置接口 GigabitEthernet1/0/1 工作在 DHCPv6 服务器模式。

```
[DHCPv6 Server-GigabitEthernet1/0/1] ipv6 dhcp select server
[DHCPv6 Server-GigabitEthernet1/0/1] quit
```

配置 DHCPv6 地址池 1。

```
[DHCPv6 Server] ipv6 dhcp pool 1
[DHCPv6 Server-dhcp6-pool-1] network 1::0/64
```

通过自定义选项的方式配置 Option 52 的内容，为 AP 指定 AC 的 IPv6 地址 1::3。

```
[DHCPv6 Server-dhcp6-pool-1] option 52 hex 00010000000000000000000000000003
[DHCPv6 Server-dhcp6-pool-1] quit
[DHCPv6 Server] quit
```

(2) 配置 AC

配置 AC 的 VLAN-interface 1 的 IPv6 地址为 1::3/64。

```
<AC> system-view
[AC] interface vlan-interface 1
[AC-Vlan-interface1] ipv6 address 1::3 64
```

创建手工 AP，名称为 ap1，配置序列号为 219801A1FF8171E00361。

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

AP 启动后，DHCPv6 server 会给 AP 自动分配 IPv6 地址 1::2，同时由于 Option 52 选项携带 AC 的 IPv6 地址 1::3。AP 拥有了自动分配的本地 IPv6 地址和需要建立关联的 AC 的 IPv6 地址 1::3，就会开始发现 AC 的过程并建立 CAPWAP 隧道。

4. 验证配置

查看 AP 的详细信息，可以看到 AP 与 AC 成功建立隧道连接并进入 Run 状态，发现方式为 DHCP 选项方式。

```
[AC] display wlan ap name ap1 verbose
AP name                : ap1
AP ID                   : 1
AP group name          : default-group
State                   : Run
Backup type             : Master
Online time             : 0 days 1 hours 25 minutes 12 seconds
System up time         : 0 days 2 hours 22 minutes 12 seconds
Model                  : WA5320E-WiNet
Region code            : CN
Region code lock       : Disable
Serial ID              : 219801A1FF8171E00361
MAC address            : 0AFB-423B-893C
IP address              : 1::2
UDP port number        : 18313
H/W version            : Ver.C
S/W version            : R2206P02
Boot version           : 1.01
USB state               : N/A
Power Level            : N/A
PowerInfo              : N/A
Description            : wtp1
```

```

Priority : 4
Echo interval : 10 seconds
Echo count : 3 counts
Keepalive interval : 10 seconds
Statistics report interval : 50 seconds
Fragment size (data) : 1500
Fragment size (control) : 1450
MAC type : Local MAC & Split MAC
Tunnel mode : Local Bridging & 802.3 Frame & Native Frame
Discovery type : DHCP
Retransmission count : 3
Retransmission interval : 5 seconds
Firmware upgrade : Enabled
Sent control packets : 1
Received control packets : 1
Echo requests : 147
Lost echo responses : 0
Average echo delay : 3
Last reboot reason : User soft reboot
Latest IP address : 10.1.0.2
Tunnel down reason : Request wait timer expired
Connection count : 1
Backup Ipv4 : Not configured
Backup Ipv6 : Not configured
Tunnel encryption : Disabled
LED mode : Normal
Remote configuration : Enabled
Radio 1:
    Basic BSSID : 7848-59f6-3940
    Admin state : Up
    Radio type : 802.11ac
    Antenna type : internal
    Client dot11ac-only : Disabled
    Client dot11n-only : Disabled
    Channel band-width : 20/40/80MHz
    Active band-width : 20/40/80MHz
    Secondary channel offset : SCB
    Short GI for 20MHz : Supported
    Short GI for 40MHz : Supported
    Short GI for 80MHz : Supported
    Short GI for 160MHz : Not supported
    A-MSDU : Enabled
    A-MPDU : Enabled
    LDPC : Not Supported
    STBC : Supported
    Operational VHT-MCS Set:
        Mandatory : Not configured
        Supported : NSS1 0,1,2,3,4,5,6,7,8,9

```

```

                                NSS2 0,1,2,3,4,5,6,7,8,9
Multicast                       : Not configured
Operational HT MCS Set:
  Mandatory                     : Not configured
  Supported                     : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                                10, 11, 12, 13, 14, 15
  Multicast                     : Not configured
Channel                         : 44(auto)
Channel usage(%)               : 15
Max power                      : 20 dBm
Operational rate:
  Mandatory                     : 6, 12, 24 Mbps
  Multicast                     : Auto
  Supported                     : 9, 18, 36, 48, 54 Mbps
  Disabled                     : Not configured
Distance                       : 1 km
ANI                            : Enabled
Fragmentation threshold       : 2346 bytes
Beacon interval               : 100 TU
Protection threshold          : 2346 bytes
Long retry threshold          : 4
Short retry threshold         : 7
Maximum rx duration           : 2000 ms
Noise Floor                   : -102 dBm
Protection mode                : rts-cts
MU-TxBF                       : Enabled
SU-TxBF                       : Enabled
Continuous mode               : N/A
HT protection mode            : No protection
Radio 2:
  Basic BSSID                  : 7848-59f6-3950
  Admin state                  : Down
  Radio type                   : 802.11b
  Antenna type                 : internal
  Client dot11n-only          : Disabled
  Channel band-width           : 20MHz
  Active band-width            : 20MHz
  Secondary channel offset     : SCN
  Short GI for 20MHz           : Supported
  Short GI for 40MHz           : Supported
  A-MSDU                      : Enabled
  A-MPDU                      : Enabled
  LDPC                        : Not Supported
  STBC                        : Supported
Operational HT MCS Set:
  Mandatory                     : Not configured
  Supported                     : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                                10, 11, 12, 13, 14, 15

```

```

Multicast                : Not configured
Channel                  : 5(auto)
Channel usage(%)        : 0
Max power                : 20 dBm
Preamble type           : Short
Operational rate:
  Mandatory              : 1, 2, 5.5, 11 Mbps
  Multicast              : Auto
  Supported               : 6, 9, 12, 18, 24, 36, 48, 54 Mbps
  Disabled               : Not configured
Distance                 : 1 km
ANI                      : Enabled
Fragmentation threshold : 2346 bytes
Beacon interval         : 100 TU
Protection threshold    : 2346 bytes
Long retry threshold    : 4
Short retry threshold   : 7
Maximum rx duration     : 2000 ms
Noise Floor             : 0 dBm
Protection mode         : rts-cts
Continuous mode         : N/A
HT protection mode      : No protection

```

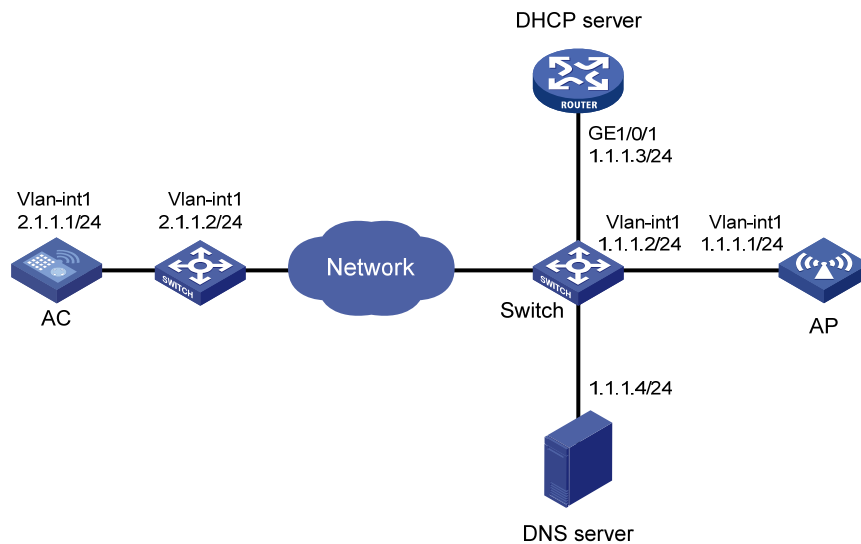
1.22.3 配置通过DNS发现方式建立CAPWAP隧道举例

1. 组网需求

DHCP server、DNS server、AP 和 AC 通过交换机连接。在 AP 上配置 DNS 客户端功能，AP 会通过动态域名解析功能，将 AC 域名 abc 解析为 IP 地址；DNS server 的 IP 地址是 1.1.1.4/24，域名服务器上存在 abc 域，且 abc 域中包含域名“h3c.abc”和 AC 的 IP 地址 2.1.1.1/24 的对应关系。

2. 组网图

图1-5 通过 DNS 发现方式建立 CAPWAP 隧道典型组网图



3. 配置步骤

(1) 配置 DHCP server

使能 DHCP 服务，配置 DHCP 地址池 1，配置 AC 域名后缀为 abc。

```
<DHCP server> system-view
[DHCP server] dhcp enable
[DHCP server] dhcp server ip-pool 1
[DHCP server-dhcp-pool-1] network 1.1.1.0 mask 255.255.255.0
[DHCP server-dhcp-pool-1] domain-name abc
[DHCP server-dhcp-pool-1] dns-list 1.1.1.4
[DHCP server-dhcp-pool-1] gateway-list 1.1.1.2
[DHCP server-dhcp-pool-1] quit
[DHCP server] quit
```

(2) 配置 DNS server

在 DNS server 上配置域名 “h3c.abc” 和 AC 的 IP 地址 2.1.1.1/24 的映射关系。（略）

(3) 配置 AC

配置 AC 的 VLAN-interface 1 的 IP 地址为 2.1.1.1/24。

```
<AC> system-view
[AC] interface vlan-interface 1
[AC-Vlan-interface1] ip address 2.1.1.1 24
[AC-Vlan-interface1] quit
```

配置缺省路由，指定下一跳为 2.1.1.2。

```
[AC] ip route-static 0.0.0.0 0 2.1.1.2
```

创建 ap1，并配置序列号为 219801A1FF8171E00361。

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

AP 启动后，AP 会从 DHCP server 自动获取 IP 地址 1.1.1.1，同时获取 AC 的域名后缀 abc 和 DNS 服务器地址 1.1.1.4，AP 将从自身获取到的主机名 h3c 和 DHCP 服务器返回的域名后缀合在一起形成完整的 AC 域名 h3c.abc，AP 通过 DNS server 进行 AC 域名解析。解析成功后，AP 拥有了自动分配的本地 IPv4 地址和需要建立 CAPWAP 隧道连接的 AC 的 IP 地址 2.1.1.1，开始发现 AC 的过程并建立 CAPWAP 隧道。

4. 验证配置

查看 AP 的详细信息，可以看到 AP 与 AC 成功建立 CAPWAP 隧道连接并进入 Run 状态，发现方式为 DNS 方式。

```
[AC] display wlan ap name ap1 verbose
AP name                : ap1
AP ID                   : 1
AP group name          : default-group
State                   : Run
Backup type             : Master
Online time             : 0 days 1 hours 25 minutes 12 seconds
System up time         : 0 days 2 hours 22 minutes 12 seconds
Model                   : WA5320E-WiNet
Region code            : CN
```

```

Region code lock          : Disable
Serial ID                 : 219801A1FF8171E00361
MAC address               : 0AFB-423B-893C
IP address                : 1.1.1.1
UDP port number           : 18313
H/W version               : Ver.C
S/W version               : R2206P02
Boot version              : 1.01
USB state                  : N/A
Power Level               : N/A
PowerInfo                 : N/A
Description                : wtpl
Priority                   : 4
Echo interval             : 10 seconds
Echo count                 : 3 counts
Keepalive interval        : 10 seconds
Statistics report interval : 50 seconds
Fragment size (data)      : 1500
Fragment size (control)   : 1450
MAC type                   : Local MAC & Split MAC
Tunnel mode                : Local Bridging & 802.3 Frame & Native Frame
Discovery type             : DNS
Retransmission count      : 3
Retransmission interval   : 5 seconds
Firmware upgrade           : Enabled
Sent control packets      : 1
Received control packets  : 1
Echo requests              : 147
Lost echo responses       : 0
Average echo delay        : 3
Last reboot reason        : User soft reboot
Latest IP address         : 10.1.0.2
Tunnel down reason        : Request wait timer expired
Connection count          : 1
Backup Ipv4                : Not configured
Backup Ipv6                : Not configured
Tunnel encryption         : Disabled
LED mode                   : Normal
Remote configuration       : Enabled
Radio 1:
  Basic BSSID              : 7848-59f6-3940
  Admin state               : Up
  Radio type                : 802.11ac
  Antenna type              : internal
  Client dot11ac-only      : Disabled
  Client dot11n-only       : Disabled
  Channel band-width       : 20/40/80MHz
  Active band-width        : 20/40/80MHz

```



```

Secondary channel offset : SCB
Short GI for 20MHz      : Supported
Short GI for 40MHz     : Supported
Short GI for 80MHz     : Supported
Short GI for 160MHz    : Not supported
A-MSDU                 : Enabled
A-MPDU                 : Enabled
LDPC                   : Not Supported
STBC                   : Supported
Operational VHT-MCS Set:
    Mandatory          : Not configured
    Supported           : NSS1 0,1,2,3,4,5,6,7,8,9
                        : NSS2 0,1,2,3,4,5,6,7,8,9
    Multicast           : Not configured
Operational HT MCS Set:
    Mandatory          : Not configured
    Supported           : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                        : 10, 11, 12, 13, 14, 15
    Multicast           : Not configured
Channel                 : 44(auto)
Channel usage(%)        : 15
Max power               : 20 dBm
Operational rate:
    Mandatory          : 6, 12, 24 Mbps
    Multicast           : Auto
    Supported           : 9, 18, 36, 48, 54 Mbps
    Disabled           : Not configured
Distance                 : 1 km
ANI                      : Enabled
Fragmentation threshold : 2346 bytes
Beacon interval         : 100 TU
Protection threshold    : 2346 bytes
Long retry threshold    : 4
Short retry threshold   : 7
Maximum rx duration     : 2000 ms
Noise Floor             : -102 dBm
MU-TxBF                 : Enabled
SU-TxBF                 : Enabled
Protection mode         : rts-cts
Continuous mode         : N/A
HT protection mode      : No protection
Radio 2:
Basic BSSID             : 7848-59f6-3950
Admin state             : Down
Radio type              : 802.11b
Antenna type            : internal
Client dot11n-only     : Disabled
Channel band-width     : 20MHz

```

```

Active band-width      : 20MHz
Secondary channel offset : SCN
Short GI for 20MHz     : Supported
Short GI for 40MHz     : Supported
A-MSDU                : Enabled
A-MPDU                : Enabled
LDPC                  : Not Supported
STBC                  : Supported
Operational HT MCS Set:
    Mandatory          : Not configured
    Supported          : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                        10, 11, 12, 13, 14, 15
    Multicast          : Not configured
Channel                : 5(auto)
Channel usage(%)       : 0
Max power              : 20 dBm
Preamble type          : Short
Operational rate:
    Mandatory          : 1, 2, 5.5, 11 Mbps
    Multicast          : Auto
    Supported          : 6, 9, 12, 18, 24, 36, 48, 54 Mbps
    Disabled           : Not configured
Distance               : 1 km
ANI                    : Enabled
Fragmentation threshold : 2346 bytes
Beacon interval        : 100 TU
Protection threshold   : 2346 bytes
Long retry threshold   : 4
Short retry threshold   : 7
Maximum rx duration    : 2000 ms
Noise Floor            : 0 dBm
Protection mode        : rts-cts
Continuous mode        : N/A
HT protection mode     : No protection

```

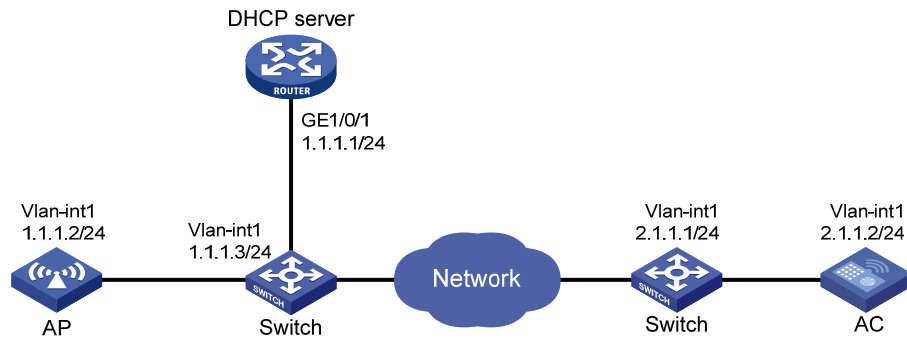
1.22.4 配置开启自动AP功能建立CAPWAP隧道举例

1. 组网需求

在 AC 上开启自动 AP 功能，MAC 地址为 0011-2200-0101 的 AP 通过 DHCP 选项方式获取到 AC 的 IP 地址，AP 通过获取到的 AC 的 IP 地址发现 AC 并与 AC 建立 CAPWAP 隧道连接。

2. 组网图

图1-6 开启自动 AP 功能建立 CAPWAP 隧道典型组网图



3. 配置步骤

(1) 配置 DHCP server

使能 DHCP 服务器功能。

```
<DHCP Server> system-view
[DHCP Server] dhcp enable
```

配置 DHCP 地址池 1。

```
[DHCP Server] dhcp server ip-pool 1
[DHCP Server-dhcp-pool-1] network 1.1.1.0 mask 255.255.255.0
```

通过自定义选项的方式配置 Option 43 的内容，为 AP 指定 AC 的 IP 地址。注意 Option 43 选项内容中最后四字节为 02010102（2.1.1.2），即为 AC 的 IP 地址。

```
[DHCP Server-dhcp-pool-1] option 43 hex 800700000102010102
[DHCP Server-dhcp-pool-1] gateway-list 1.1.1.3
[DHCP Server-dhcp-pool-1] quit
[DHCP Server] quit
```

(2) 配置 AC

配置 AC 的 VLAN-interface 1 的 IP 地址为 2.1.1.2/24。

```
<AC> system-view
[AC] interface vlan-interface 1
[AC-Vlan-interface1] ip address 2.1.1.2 24
[AC-Vlan-interface1] quit
```

配置缺省路由，指定下一跳为 2.1.1.1。

```
[AC] ip route-static 0.0.0.0 0 2.1.1.1
```

开启自动 AP 功能。

```
[AC] wlan auto-ap enable
```

4. 验证配置

通过 **display wlan ap name 0011-2200-0101 verbose** 命令查看 ap 的详细信息，可以看到该 AP 已成功建立 CAPWAP 隧道连接。

```
[AC] display wlan ap name 0011-2200-0101 verbose
AP name          : 0011-2200-0101
AP ID            : 1
```

```

AP group name          : default-group
State                  : Run
Backup type            : Master
Online time            : 0 days 1 hours 25 minutes 12 seconds
System up time         : 0 days 2 hours 22 minutes 12 seconds
Model                  : WA5320E-WiNet
Region code            : CN
Region code lock       : Disable
Serial ID              : 219801A1FF8171E00361
MAC address            : 0011-2200-0101
IP address             : 1.1.1.2
UDP port number        : 18313
H/W version            : Ver.C
S/W version            : R2206P02
Boot version           : 1.01
USB state              : N/A
Power Level            : N/A
PowerInfo              : N/A
Description            : wtpl
Priority               : 4
Echo interval          : 10 seconds
Echo count             : 3 counts
Keepalive interval    : 10 seconds
Statistics report interval : 50 seconds
Fragment size (data)   : 1500
Fragment size (control) : 1450
MAC type               : Local MAC & Split MAC
Tunnel mode            : Local Bridging & 802.3 Frame & Native Frame
Discovery type         : DHCP
Retransmission count   : 3
Retransmission interval : 5 seconds
Firmware upgrade       : Enabled
Sent control packets   : 1
Received control packets : 1
Echo requests          : 147
Lost echo responses    : 0
Average echo delay     : 3
Last reboot reason     : User soft reboot
Latest IP address      : 10.1.0.2
Tunnel down reason     : Request wait timer expired
Connection count       : 1
Backup Ipv4            : Not configured
Backup Ipv6            : Not configured
Tunnel encryption      : Disabled
LED mode               : Normal
Remote configuration   : Enabled
Radio 1:
  Basic BSSID          : 7848-59f6-3940

```

```

Admin state           : Up
Radio type           : 802.11ac
Antenna type        : internal
Client dot11ac-only : Disabled
Client dot11n-only  : Disabled
Channel band-width  : 20/40/80MHz
Active band-width   : 20/40/80MHz
Secondary channel offset : SCB
Short GI for 20MHz   : Supported
Short GI for 40MHz   : Supported
Short GI for 80MHz   : Supported
Short GI for 160MHz  : Not supported
A-MSDU              : Enabled
A-MPDU              : Enabled
LDPC                 : Not Supported
STBC                 : Supported
Operational VHT-MCS Set:
    Mandatory        : Not configured
    Supported         : NSS1 0,1,2,3,4,5,6,7,8,9
                       NSS2 0,1,2,3,4,5,6,7,8,9
    Multicast         : Not configured
Operational HT MCS Set:
    Mandatory        : Not configured
    Supported         : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                       10, 11, 12, 13, 14, 15
    Multicast         : Not configured
Channel              : 44(auto)
Channel usage(%)    : 15
Max power            : 20 dBm
Operational rate:
    Mandatory        : 6, 12, 24 Mbps
    Multicast         : Auto
    Supported         : 9, 18, 36, 48, 54 Mbps
    Disabled         : Not configured
Distance             : 1 km
ANI                  : Enabled
Fragmentation threshold : 2346 bytes
Beacon interval      : 100 TU
Protection threshold : 2346 bytes
Long retry threshold : 4
Short retry threshold : 7
Maximum rx duration  : 2000 ms
Noise Floor          : -102 dBm
Protection mode      : rts-cts
MU-TxBF              : Enabled
SU-TxBF              : Enabled
Continuous mode      : N/A
HT protection mode    : No protection

```

```

Radio 2:
  Basic BSSID           : 7848-59f6-3950
  Admin state          : Down
  Radio type           : 802.11b
  Antenna type         : internal
  Client dot11n-only   : Disabled
  Channel band-width   : 20MHz
  Active band-width    : 20MHz
  Secondary channel offset : SCN
  Short GI for 20MHz    : Supported
  Short GI for 40MHz    : Supported
  A-MSDU               : Enabled
  A-MPDU               : Enabled
  LDPC                 : Not Supported
  STBC                 : Supported
  Operational HT MCS Set:
    Mandatory          : Not configured
    Supported          : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                       10, 11, 12, 13, 14, 15
    Multicast          : Not configured
  Channel              : 5(auto)
  Channel usage(%)    : 0
  Max power            : 20 dBm
  Preamble type       : Short
  Operational rate:
    Mandatory          : 1, 2, 5.5, 11 Mbps
    Multicast          : Auto
    Supported          : 6, 9, 12, 18, 24, 36, 48, 54 Mbps
    Disabled          : Not configured
  Distance             : 1 km
  ANI                  : Enabled
  Fragmentation threshold : 2346 bytes
  Beacon interval      : 100 TU
  Protection threshold : 2346 bytes
  Long retry threshold : 4
  Short retry threshold : 7
  Maximum rx duration  : 2000 ms
  Noise Floor          : 0 dBm
  Protection mode      : rts-cts
  Continuous mode      : N/A
  HT protection mode   : No protection

```

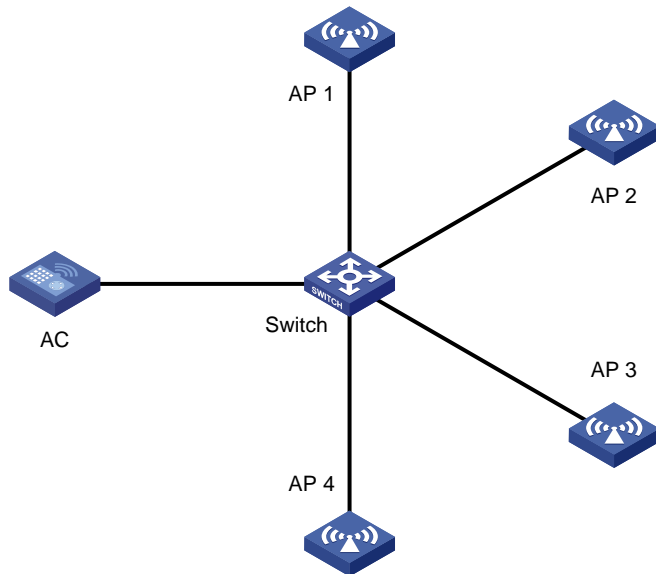
1.22.5 AP组配置举例

1. 组网需求

AC 通过交换机和 AP1、AP2、AP3、AP4 相连；将 AP1 加入 group1，AP2、AP3 和 AP4 加入 group2。AP1、AP2、AP3 和 AP4 名字分别为 ap1、ap2、ap3 和 ap4。

2. 组网图

图1-7 AP 组配置举例



3. 配置步骤

- (1) 配置 AP 通过 DHCP 方式获取本机 IP 地址及 AC IP 地址（略）
- (2) 配置手工 AP（略）
- (3) 配置 AP 组

创建 group1。

```
<AC> system-view
[AC] wlan ap-group group1
```

将 AP1 加入 group1。

```
[AC-wlan-ap-group-group1] ap ap1
[AC-wlan-ap-group-group1] quit
```

创建 group2。

```
[AC] wlan ap-group group2
```

将 AP2、AP3 和 AP4 加入 group2。

```
[AC-wlan-ap-group-group2] ap ap2 ap3 ap4
[AC-wlan-ap-group-group2] quit
[AC] quit
```

4. 验证配置

通过 **display wlan ap-group** 命令查看 AP 组详细信息,可以看到 ap1 被加入到 group1 组, ap2、ap3、和 ap4 被加入到 group2 组。

```
<AC> display wlan ap-group
Total number of AP groups: 3
AP group name      : default-group
Description       : Not configured
AP model          : Not configured
APs               : Not configured
```

AP group name : group1
Description : Not configured
AP model : WA5320E-WiNet
AP grouping rules:
 AP name : ap1
 Serial ID : Not configured
 MAC address : Not configured
 IPv4 address : Not configured
 IPv6 address : Not configured
APs : ap1 (AP name)

AP group name : group2
Description : Not configured
AP model : WA5320E-WiNet
AP grouping rules:
 AP name : ap2, ap3, ap4
 Serial ID : Not configured
 MAC address : Not configured
 IPv4 address : Not configured
 IPv6 address : Not configured
APs : ap2 (AP name), ap3 (AP name), ap4 (AP name)