

团 体 标 准

T/WAPIA 043.1—2021

无线局域网接入控制 第1部分：组网架构规范

Wireless LAN cloud access control—Part 1: Networking architecture
specification

2021-11-25 发布

2022-01-01 实施

中关村无线网络安全产业联盟 发布

版权声明

本文件版权归中关村无线网络安全产业联盟（WAPI产业联盟）©所有。

本文件以电子文档形式面向公众公开。本声明在此授权所有组织或者个人对本文件进行使用和复制。任何组织或者个人对本文件的修改、翻译、摘编、汇编、销售行为，应事先获得WAPI产业联盟书面授权，否则视为侵权。

联系WAPI产业联盟标准化部（lmbz@wapia.org）可获取本文件授权相关信息。

目 次

版权声明	I
前言	V
引言	VII
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	2
5 云 AC 组网架构及工作机制	2
5.1 网络构成	2
5.2 工作机制	3
6 AP 入流程	3
6.1 云 AC 分配流程	4
6.2 AP 上线流程	4
7 基于 CADP 的云 AC 设备切换机制	5
7.1 云 AC 分配流程	5
7.2 主备云 AC 切换流程	6
8 CADP 双机热备	7
9 云 AC 池组网技术	8

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是 T/WAPIA 043《无线局域网接入控制》的第1部分。T/WAPIA 043 已经发布了以下部分：

- 第1部分：组网架构规范；
- 第2部分：调度平台技术规范。

本文件由中关村无线网络安全产业联盟与工业和信息化部宽带无线 IP 标准工作组联合提出。

本文件由无线网络安全标准化委员会归口。

本文件起草单位：中国电信集团有限公司，中关村无线网络安全产业联盟，西安西电捷通无线网络通信股份有限公司，新华三技术有限公司。

本文件主要起草人：高波，潘毅明，简练，张变玲，傅嘉嘉，张璐璐，王月辉，万晓兰。

WAPI Alliance

引 言

公众无线局域网（WLAN）组网有大量设备管理、部署和维护等重要需求，考虑到当规模部署 WLAN 网络时，面对数量众多、不同区域的接入点（AP），如何更加合理、更加智能地为其分配最佳的云接入控制器（云 AC），使 WLAN 网络规模部署和运营更加便捷、高效和降低成本，成为规模部署 WLAN 网络的关键要求之一。目前无相关技术规范，为此 WAPI 产业联盟无线网络安全标准化委员会组织开展了 T/WAPIA 043《无线局域网接入控制》系列团体标准的制定工作。

针对行业应用需求，联盟成员单位和业内厂商迫切需要一份明确的技术指标指南，规范无线局域网接入控制技术，确保产品设计、生产和采购、部署等环节的合规性和一致性。T/WAPIA 043 拟由两个部分构成。

— 第 1 部分：组网架构规范。目的在于制定云 AC 组网架构规范。

— 第 2 部分：调度平台技术规范。目的在于制定云 AC 调度平台技术规范。

本文件的发布机构提请注意，声明符合本文件时，可能涉及到与第 5 章和第 6 章相关的 ZL201110229 专利使用；可能涉及到与第 9 章相关的 ZL201310330350.X 专利使用。

本文件的发布机构对于该专利的真实性、有效性和范围无任何立场。

该专利持有人已向本文件的发布机构承诺，他愿意同任何申请人在合理且无歧视的条款和条件下，就专利授权许可进行谈判。该专利持有人的声明已在本文件发布机构备案。相关信息可通过以下联系方式获得：

ZL201110229 专利持有人姓名：新华三技术有限公司

地址：北京海淀区永嘉北路 8 号

联系人：万晓兰

邮政编码：100094

电子邮件：wxlan@h3c.com

电话：15611208820

ZL201310330350.X 专利持有人姓名：中国电信股份有限公司

地址：上海市浦东新区浦东南路 1835 号

联系人：高波

邮政编码：200122

电子邮件：gaobo6@chinatelecom.cn

电话：18918588639

请注意除了上述专利外，本文件的某些内容仍可能涉及专利。本文件的发布机构不承担识别专利的责任。

无线局域网接入控制 第1部分：组网架构规范

1 范围

本文件规定了基于云接入控制器（云AC）的无线局域网组网架构，定义无线接入点（AP）接入流程、云AC切换机制和云AC池组网技术要求。

本文件适用于公共热点、行业等无线局域网组网场景。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB 15629.11—2003 信息技术 系统间通信和信息交换 局域网和城域网 特殊要求 第11部分：无线局域网媒体访问控制（MAC）和物理层（PHY）规范

GB 15629.11—2003/XG1—2006 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第11部分：无线局域网媒体访问控制和物理层规范 第1号修改单

ISO/IEC/IEEE 8802-11 信息技术—系统间通信和信息交换—局域网和城域网—特殊要求—第11部分：无线局域网媒体访问控制（MAC）和物理层（PHY）规范（Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications）

RFC 5415 无线接入点控制和配置（CAPWAP）协议规范（Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification）

3 术语和定义

GB 15629.11系列国家标准界定的以及下列术语和定义适用于本文件。

3.1

接入控制器 access controller

管理AP的设备。

3.2

云AC cloud AC

一个部署在核心网的AC实体，该实体通过CADP协调，实现对特定AP的控制和管理。

3.3

云AC池 cloud AC pool

一组云AC的集合。

3.4

轻量级AP fit AP

集中控制型AC和AP组网架构中的用户无线接入点设备。

3.5

WLAN网管系统 WLAN network management system

用于管理WLAN网络设备的应用系统，具有配置管理、性能管理、故障诊断和告警管理、安全管理、日志管理、操作维护管理等功能，本标准中新增为AP从云AC池中选择云AC的功能。

3.6

认证平台 authentication platform

基于AAA协议对WLAN用户进行认证的实体

3.7

云AC调度平台 cloud AC dispatch platform

根据WLAN网管系统下发的AP和AC的对应关系，为AP下发指定AC的调度实体。

4 缩略语

下列缩略语适用于本文件。

AAA	认证授权计费 (authentication authorization account)
AC	接入控制器 (access controller)
AP	无线接入点 (access point)
BRAS	宽带远程接入服务器 (broadband remote access server)
CADP	云AC调度平台 (cloud AC dispatch platform)
CAPWAP	无线接入点控制和配置协议 (control and provisioning of wireless access points protocol)
CPU	中央处理器 (central processing unit)
DHCP	动态主机配置协议 (dynamic host configuration protocol)
IP	互联网协议 (Internet protocol)
MAC	媒体访问控制 (medium access control)
WLAN	无线局域网 (wireless local area network)

5 云 AC 组网架构及工作机制

5.1 网络构成

WLAN 云 AC 组网架构主要由如下五部分组成：轻量级 AP（以下简称为 AP）、云 AC 池、WLAN 网管系统、认证平台和 CADP。其中，CADP、云 AC 池、WLAN 网管系统以及认证平台部署于核心网，AP 部署在本地网络。

AP 的技术要求应符合 GB 15629.11—2003 和 GB 15629.11—2003/XG1—2006，支持 ISO/IEC/IEEE 8802-11；AP 和云 AC 之间的通信应符合 RFC 5415 定义的接口协议；AP 和 CADP 之间的通信应符合 RFC 5415 定义的接口协议。

各网元设备的功能如下。

a) AP

AP 通过专线、互联网 (Internet) 或移动网等方式接入云 AC，使 WLAN 网络覆盖更灵活。AP 与云 AC 调度平台之间、AP 与云 AC 之间均通过 CAPWAP 协议通信。

b) 云 AC 池

云 AC 集中部署形成云 AC 池，实现资源统一管理和统一调度。

c) WLAN 网管系统

WLAN 网管系统维护云 AC 的负载参数，包括接入用户数、接入 AP 数、转流量、CPU 利用率、网络延迟等。

d) 认证平台

认证平台包括门户网站服务器 (Portal Server) 和 AAA 等，实现对 WLAN 用户的认证、计费等功能。

e) CADP

CADP 是新增的网络实体，该实体从 WLAN 网管系统侧获取 AP 与云 AC 的对应关系，并为上线 AP 分配云 AC 的 IP 地址。

云 AC 组网架构示意图见图 1。

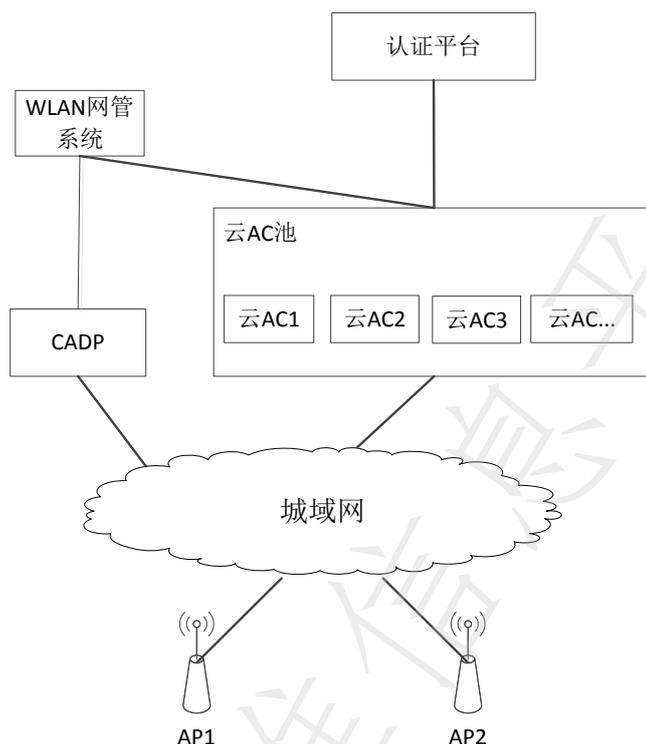


图 1 云AC组网架构示意图

5.2 工作机制

在云 AC 组网架构下，云 AC 集中部署形成云 AC 池。云 AC 无需为 AP 预先指定云 AC，取而代之的是为 AP 预先配置统一的 CADP 域名或 IP 地址。当 AP 上线时，根据预先配置的域名或 IP 地址找到 CADP，并从 CADP 处获取 WLAN 网管系统为其分配的云 AC 的 IP 地址，然后通过该 IP 地址找到并接入云 AC。该机制解决了传统架构中不同区域云 AC 利用率存在很大的差异问题，并增加了为 AP 灵活分配云 AC 的能力。

WLAN 网管系统为 AP 选择云 AC 时，需考虑网络中各云 AC 的负载参数，如：接入用户数、接入 AP 数、转发流量、CPU 利用率、网络延迟等；为每个负载参数赋予不同的权重，进行动态负载均衡。WLAN 网管系统将 AP 与云 AC 的对应关系下发给 CADP 和相应的云 AC。

WLAN 网络中如果新增云 AC 或为 AP 更换云 AC，只需由 WLAN 网管系统调整 AP 与云 AC 的对应关系，并通过 CADP 下发给 AP，无需对 AP 作任何配置。

通过 CADP，不仅可以提供云 AC 设备的 1+1 备份（1 台主云 AC、1 台备云 AC）和 N+1 备份（N 台主云 AC、1 台备云 AC），也可以实现 N+M 备份（N 台主云 AC、M 台备云 AC）和端口级备份（当某台云 AC 发生故障时，将这台云 AC 上的 AP 分散切换到其它有空余能力的多台云 AC），减少备份云 AC 设备数量，以节省成本。

负载参数的权重分配策略以及负载均衡策略，由网络运营者确定，不属本标准范围。

6 AP 接入流程

根据 WLAN 网管系统获取需要上线的 AP 信息，实时获取的云 AC 池中各云 AC 的负载情况，为 AP 分配一个特定的云 AC，并将 AP 信息（如：MAC 地址、序列号）、AP 与其云 AC 的对应关系下发给 CADP，同时将 AP 信息下发给相应的云 AC。

AP 接入流程主要分为如下两部分：

a) 云 AC 分配流程；

b) AP 上线流程。

6.1 云 AC 分配流程

WLAN 网管系统为新上线 AP 选择合适的 AC: 优先保证同一连续覆盖区域内的多个 AP 对应同一云 AC, 目的是确保 WLAN 终端在不同的 AP 之间实现无缝漫游切换; 其次根据当前各 AC 的负载情况分配云 AC。新 AP 上线前的云 AC 分配流程见图 2。

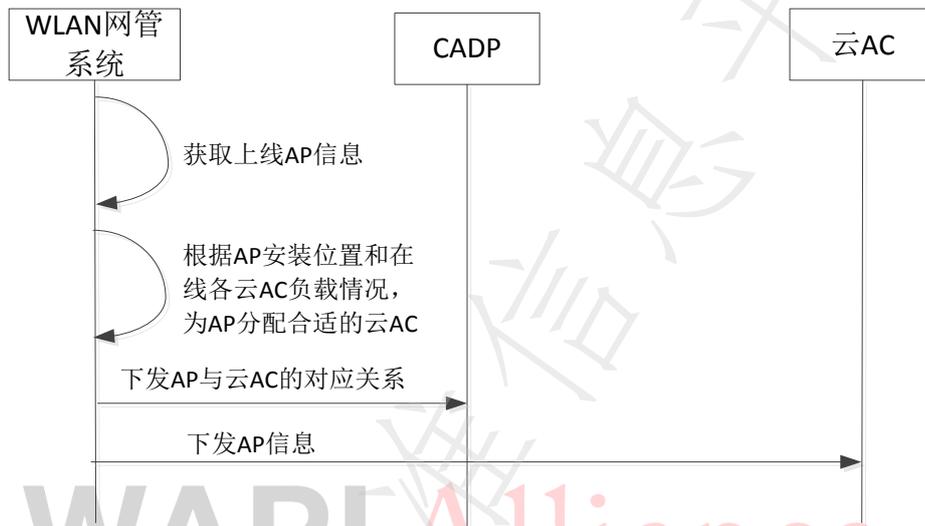


图 2 云AC分配流程图

6.2 AP 上线流程

预先在 AP 的“云 AC 域名”字段处配置为 CACP 域名。AP 每次上线都是通过 CACP 域名解析, 向 CACP 发起关联请求, 从 CACP 处获取为其分配的云 AC 的 IP 地址, 再向云 AC 注册。AP 接入云 AC 的流程见图 3。

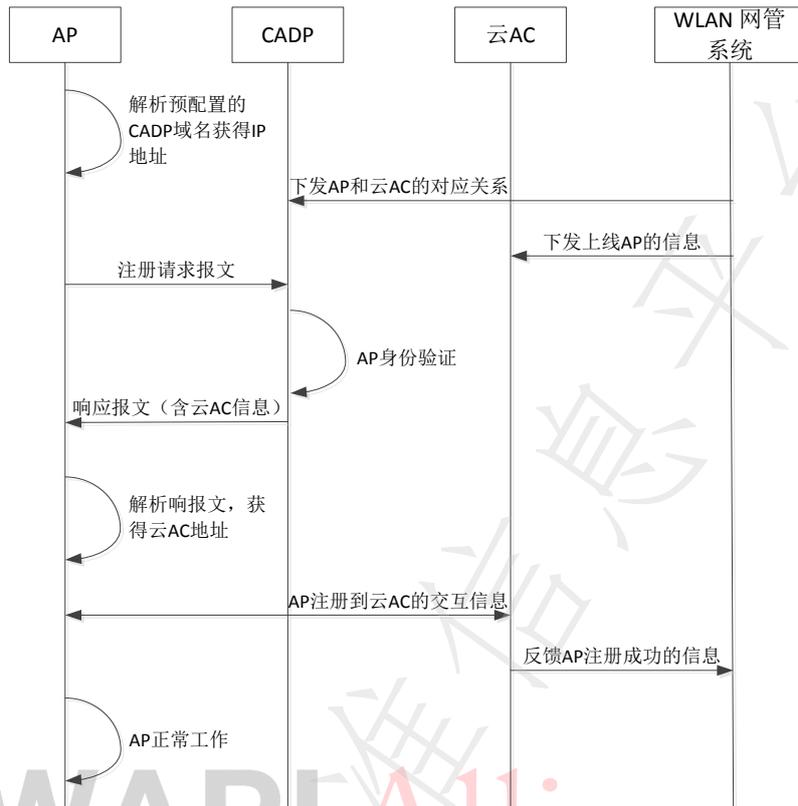


图 3 AP接入云AC流程图

7 基于 CACP 的云 AC 设备切换机制

7.1 云 AC 分配流程

在做网络优化时，如：网络上云 AC 间的负载有较大差异，需要将负载高的云 AC 上部分 AP 割接到负载低的云 AC；老旧设备（如：性能下降、型号淘汰）退网，需要将所接入的 AP 割接到其它云 AC 设备上。

在 AP 正常工作后，当需要将 AP 割接到其他云 AC 时，由 WLAN 网管系统为 AP 选择新的云 AC（云 AC2）。WLAN 网管系统将 AP 与新的云 AC（云 AC2）关系下发给 CACP，CACP 更新 AP 与云 AC 的对应关系，即在 CACP 的 AP 列表中，删除该 AP 原有的云 AC 信息（云 AC1），增加新的云 AC 信息（云 AC2）。同时 WLAN 网管系统下发该 AP 信息给新的云 AC（云 AC2）。最后，WLAN 网管系统通知原来云 AC（云 AC1），删除该 AP 的信息，并下发 AP 重启的命令。

AP 重启后通过 CACP 域名解析，向 CACP 发起关联请求，CACP 告知新云 AC（云 AC2）的 IP 地址，AP 将向云 AC2 进行注册关联，注册成功后重新正常工作。

云 AC 切换流程见图 4。

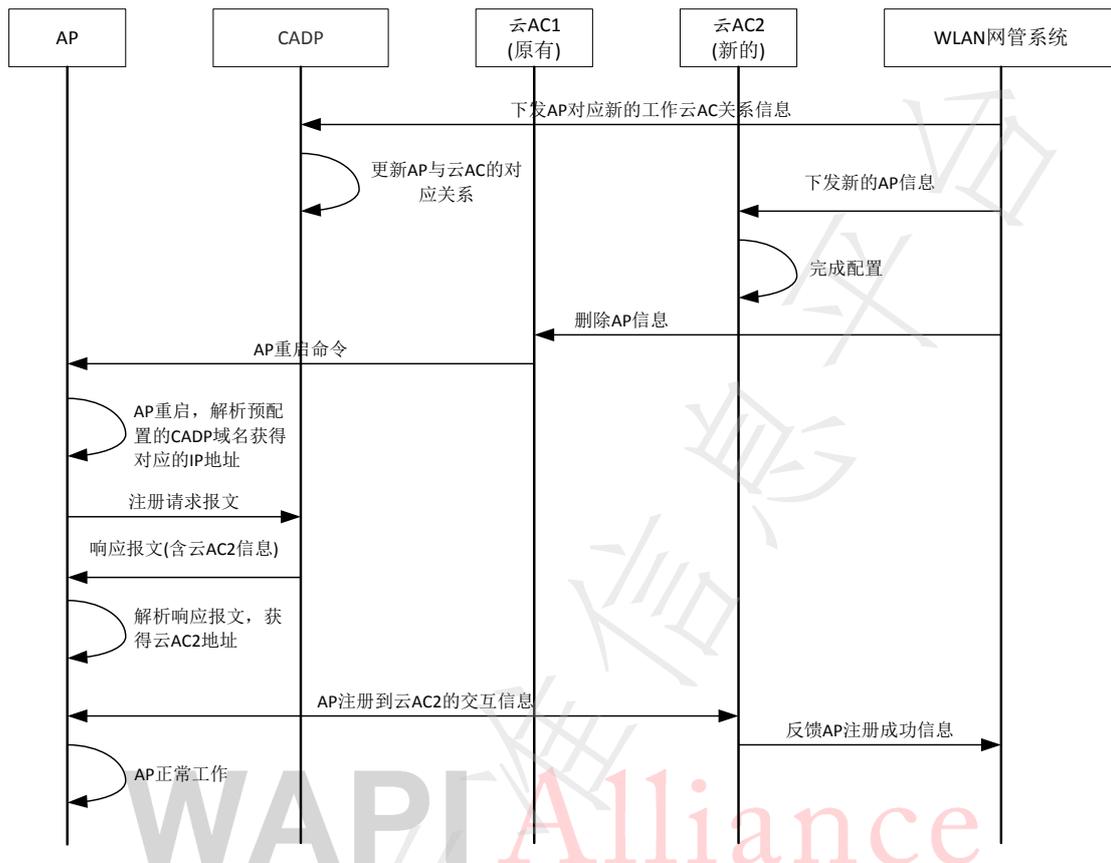


图 4 云AC切换流程示意图

7.2 主备云 AC 切换流程

WLAN 网管系统定期向云 AC 发探测报文，如果连续多次没有收到云 AC 的回应报文，则判断云 AC 出故障。当 AP 的云 AC（云 AC1）发生故障后，WLAN 网管系统将收不到云 AC1 的回应报文，即发现云 AC1 不能正常工作，因此为 AP 重新选择云 AC（云 AC2）。WLAN 网管系统将 AP 与云 AC2 的对应关系下发给 CADP 和云 AC2。

由于 AP 无法连接到云 AC1，通过预配置的 CADP 域名解析获得 CADP 的 IP 地址，通过 CADP 找到新的云 AC（云 AC2），注册关联后重新正常工作。

当原有云 AC 恢复正常工作后，可以通过相同的流程将 AP 切换到原有云 AC。

通过本机制，可以实现云 AC 间的 M+N 冷备份，其间需要 AP 断线后重连云 AC。

云 AC 原有传统组网中的备份机制仍可保留。

AP 基于 CADP 进行的主备云 AC 切换流程见图 5。

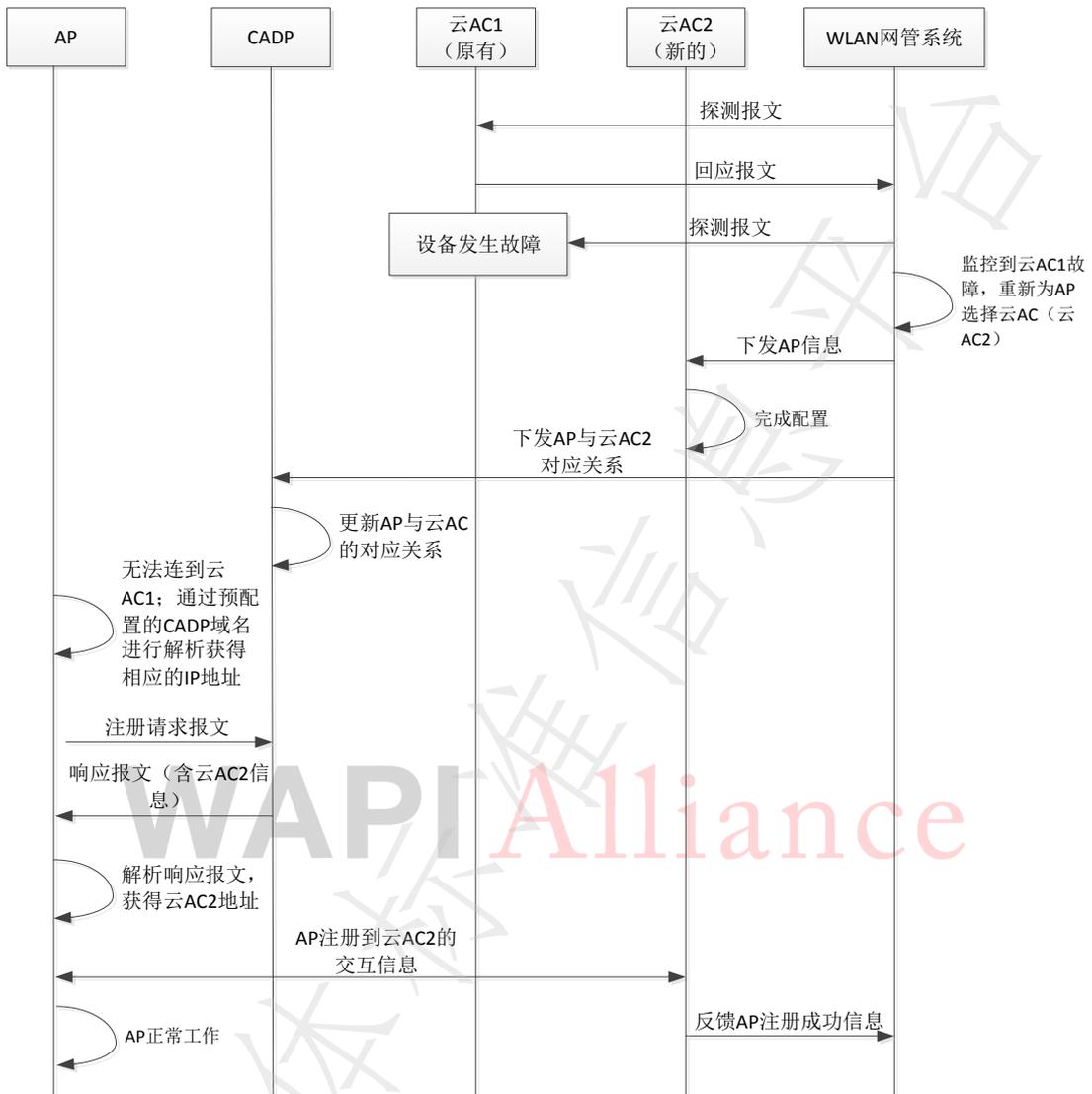


图 5 基于CADP的主备云AC切换流程图

8 CADP 双机热备

为了提高CADP的可靠性，建议同时部署两套CADP。CADP双机热备的组网示意图 6图 6。

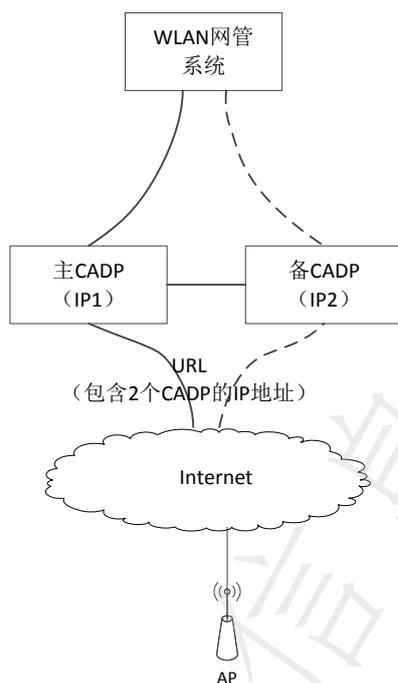


图 6 CADP 双机热备的组网示意图

当 AP 与云 AC 的对应关系发生变化时，WLAN 网管系统将 AP 与云 AC 的对应关系实时同步到主、备 CADP。

为了保证 CADP 与 WLAN 网管系统的对应表相同，主、备 CADP 每天与 WLAN 网管系统进行一次同步，发现差异的话，以 WLAN 网管系统为主。

主、备 CADP 分别配置两个公网地址，对外提供同一个 URL 访问。AP 获得两个 CADP 的地址，会尝试向两个 CADP 分别发起请求，一般会选择第一个 IP 地址的响应；如果第一个 IP 地址没有获得响应，则响应第二个 IP 地址。

9 云 AC 池组网技术

云 AC 集中部署形成云 AC 中心（云 AC 池），云 AC 通过网状网（Mesh）方式与宽带远程接入服务器（BRAS）互通，使每台云 AC 与每台 BRAS 都能相互通信。AP、BRAS 和云 AC 松耦合，使 AP 能灵活接入云 AC 池中任一台云 AC，实现云 AC 负载均衡。实现采用云 AC 池技术提升云 AC 覆盖范围和负载均衡能力，资源全网统一调度，每台云 AC 覆盖范围拓展到了云 AC 中心的覆盖范围。

云 AC 池组网示意图见图 7。

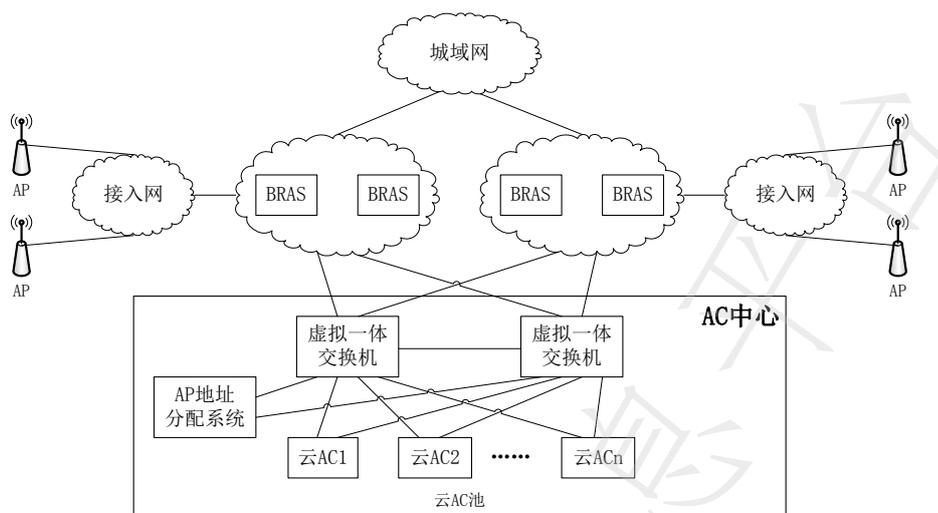


图 7 云 AC 池组网示意图

云 AC 双上联连接二台虚拟一体化交换机，均采用万兆接口跨框聚合。BRAS 分别采用二个端口与云 AC 接入交换机互联，端口绑定。任一台云 AC 与 BRAS 均可通过 IP 路由可达，因此 AP 通过上联 BRAS 可接入任一台云 AC。同时，部署 AP 专用地址分配系统，双上联连接二台虚拟一体化交换机。云 AC、AP 专用地址分配系统和云 AC 接入交换形成云 AC 池。

AP 获得管理地址和云 AC 地址的流程如下：

- AP 发起 DHCP 请求报文，经 BRAS 转发到 AP 专用地址分配系统；
- AP 专用地址分配系统接收到 BRAS 转发过来的 DHCP 报文，通过与 WLAN 网管系统/资源管理系统同步过来的 AP 配置信息（如：MAC 地址、序列号等）比对，确定是否是注册 AP；
- 如果是非注册 AP，可以将接收到的 DHCP 报文丢弃，或分配一个特定地址段的地址；
- 如果是注册 AP，通过网管系统或资源管理系统同步过来的 AP 配置信息，可获知 AP 对应的云 AC 信息（包括主、备云 AC）和厂家等信息；
- AP 地址分配系统为该 AP 分配管理地址，同时通过 DHCP 选项（Option）43（IPv4）属性下发云 AC 地址；AP 获得管理地址后，根据获得的云 AC 地址与云 AC 通信、并注册后，AP 正常工作。