CAPWAP（瘦AP）技术概述

中太数据
ZOOM NETWORKS

为什么需要瘦AP

- 大型无线网络的挑战
  - 管理、监测及控制大量AP所产生的挑战
  - 对大量AP的配置及升级
  - 无线局域网的空口传输不稳定，易受干扰，因而需要对多个AP之间的无线干扰、信道转换、功率调整等进行集中控制，从而避免干扰，防止入侵，稳定整体性能
  - 无线局域网的安全要求
- 规模化的组网运营下必须采用瘦AP的架构
  - 集中化完成配置更改、监控和管理，增强对用户和业务的控制
  - 在各种组网模式下完成对AP的统一管理，去除了胖AP到BAS缺省路由的限制。网络组网设计可以更为灵活。
  - 整体降低了网络故障率

FAT/FIT方案比较

	FAT AP方案	FIT AP方案
技术模式	传统主流	新生方式，增强管理
安全性	传统加密、认证方式，普通安全性	增加射频环境监控，基于用户位置安全策略，高安全性
网络管理	对每AP下发配置文件	AC上分组批量配置，AP本身零配置
WLAN组网规模	适合小规模组网	拓扑无关性，适合大规模组网
增值业务能力	实现简单数据接入	可扩展更多丰富业务

瘦AP协议的发展历程

- LWAPP：Airspace（被Cisco收购）、 Nexthop Technologies提出， Split MAC方式，使用UDP隧道，UDP12222和UDP12223传输数据报文和控制报文。
- SLAPP：Aruba、 Trapeze提出，支持桥接和隧道两种本地MAC模式，支持WTP端加解密和AC端加解密2种分离MAC机制，支持直连、2层和3层3种连接方式。数据信道使用GRE技术，控制信道则使用安全的DTLS技术。
- CTP(CAPWAP Tunneling Protocol)： Chantry Networks（被Siemens收购）、 Propagate Networks（改名叫AutoCell Laboratories了），，利用扩展的SNMP对WTP进行配置和管理，虽然实现了AP与WTP互相认证及一套基于AES-CCM的加密规则，但是并不完善。CTP的控制消息着重于STA连接状态、WTP配置和状态几方面。
- WiCoP（ Wireless LAN Control Protocol ）： Panasonic提出，定义了包括WTP-AC性能协商功能在内的AC发现机制，定义了QoS参数。协议建议使用IPsec和EAP安全标准，却并未详细说明实现方法。
- CAPWAP=LWAPP+SLAPP+CTP+WiCoP

CAPWAP协议的主要构成

RFC4118(Architecture for CAPWAP)：2004年2月通过Draft0，2005年6月通过最终版本（一共8个版本）。
RFC5415(CAPWAP Protocol Specification)：2006年3月通过Draft0，2009年3月发布最新版本（一共17个版本）。
RFC5416(CAPWAP Protocol Binding for IEEE802.11)：2006年10月通过Draft0，2009年3月发布最新版本（一共14个版本）。
RFC5417(CAPWAP Access Controller DHCP Option)：2007年7月通过Draft0，2009年3月发布最新版本（一共4个版本）。
RFC5418(CAPWAP Threat Analysis for 802.11 Deployments)：2007年2月通过Draft0，2009年3月发布最新版本（一共5个版本）。

draft-ietf-capwap-eval -00 2005-09-15 RFC 4565
draft-ietf-capwap-objectives -04 2005-09-28 RFC 4564
draft-ietf-capwap-problem-statement -02 2004-09-08 RFC 3990

CAPWAP的问题

CAPWAP协议太新
CAPWAP的框架性太强
CAPWAP不支持WAPI
业务型功能无法支持

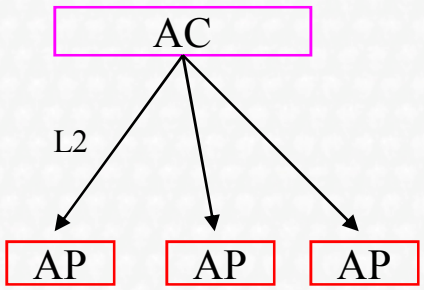
WLAN接入网络按体系架构区分的三种类型

- Autonomous WLAN Architecture： 自治型WLAN网络
  - WTP是执行802.11功能的唯 一物理实体，包括分布和集成服务，及端口（portal)功能.
  - WTP的配置及控制都是独立的
  - 监控和管理可通过SNMP进行。
  - WTP也被称为胖AP或独立型AP
  - WTP提供802.11无线接口及802.3以太网接口
  - 一个物理WTP可通过支持多个SSID成为几个虚拟WTP
- Centralized WLAN Architecture： 会聚型WLAN网络
  - 通过AC集中管理、控制及配置WTP
  - AC在无线网络中成为会聚点
  - AC在物理上常和二层网桥、交换机、三层路由器、接入服务器等放置在一起
  - 执行CAPWAP功能的AC是逻辑概念，不一定集中在一个物理设备上。
  - WTP被称为轻量级AP或瘦AP（light weight 或 和thin AP)
- Distributed WLAN Architecture： 分布型WLAN网络
  - 无线节点间自组网成为分布式网络，如网状网（MESH)
  - 具有有线连接的对外出口成为网关

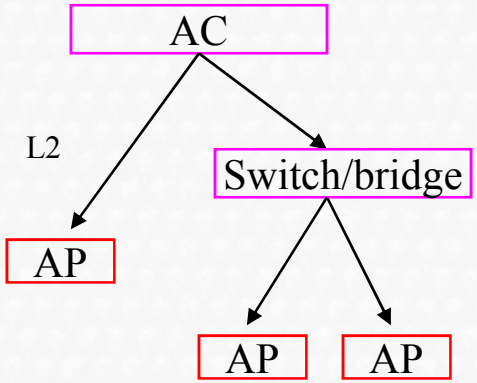
会聚型网络中AC和WTP的三种互联模式

- 直连
- 二层网络连接模式
- 三层网络连接模式

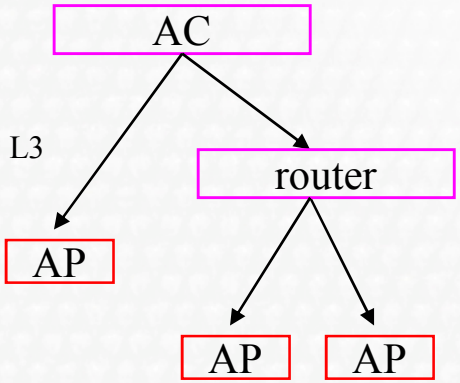
Directly Connected



Via L2 cloud

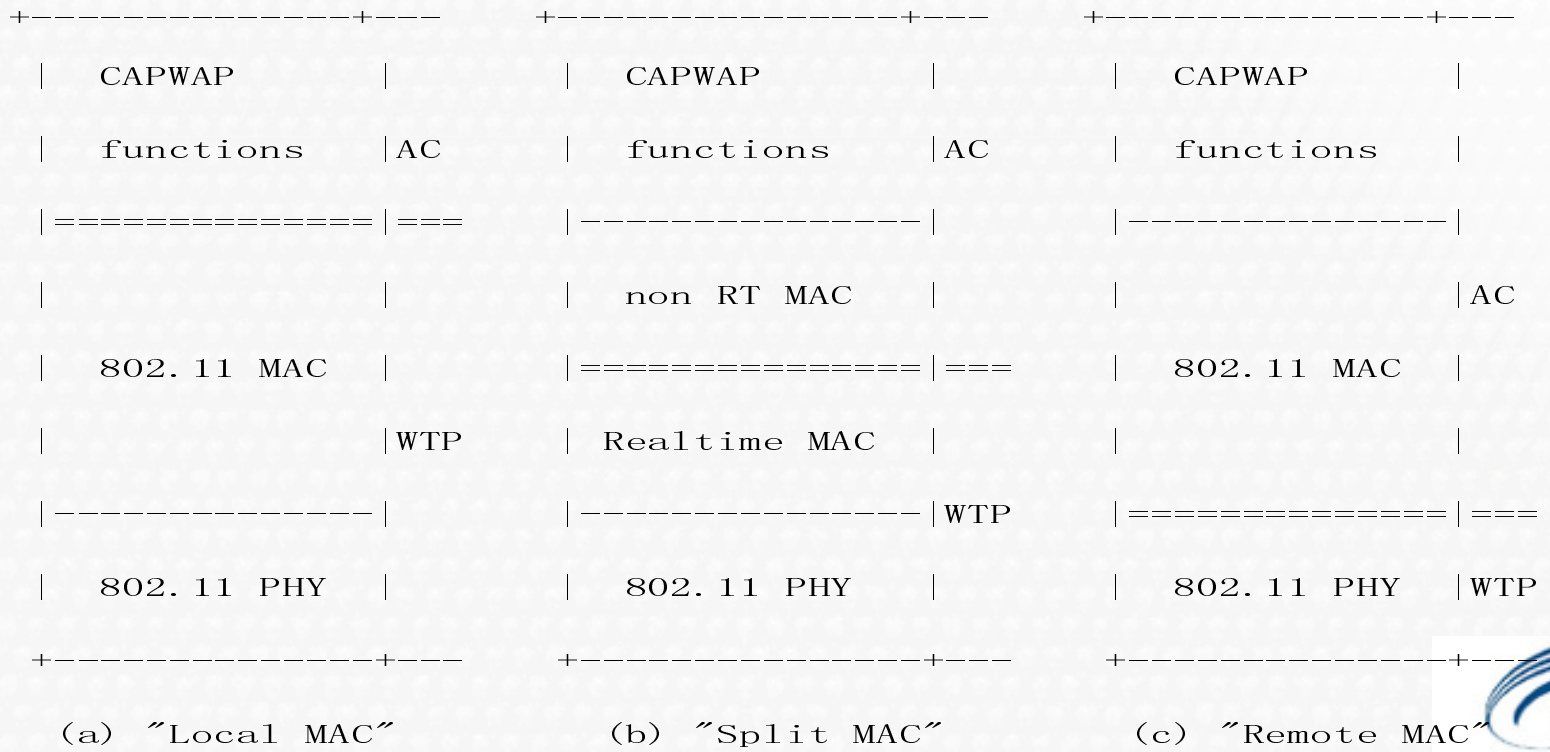


Via L3 cloud



会聚型网络的三种分支类型

- Local MAC：MAC功能驻留在WTP上，包括管理及控制帧。AC仅负责网络接入策略及AP的管理，如WTP的统一配置。这是目前最主要使用的方式
- Split MAC：时间敏感性功能在WTP上，非时间敏感性的功能在AC上
- Remote MAC ：MAC功能驻留在AC上



三种类型的对比

- Local MAC：本地MAC方式中，MAC功能实现在AP上，AP的配置和管理功能实现在AC上。Local MAC是CAPWAP协议的主要推荐方式。
- Split MAC：分离MAC方式是依据实时性的敏感度把MAC功能分别实现在AP和AC上。AP支持无线网络的物理层和MAC层的实时性功能，AC处理MAC层的非实时功能和高层服务。其优点是：减轻了AP负担，使得AC能够统一有效地管理大规模轻量型接入点，降低了AP的成本。但IEEE802.11标准对MAC功能的实时性并没有作明确规定，分离MAC没有统一的方案可循。
- Remote MAC：远程MAC方式目的是使AP尽量保持轻量级，只提供物理层功能，而AC提供所有的MAC功能。这种方式的AP功能简单，但由于MAC的实时性功能实现在AC上，不利于开展时延敏感型业务。

Local MAC及Splic MAC下，各厂家对功能的切分

功能项	子功能项	Local MAC					Split MAC					
		模型1	模型2	模型3	模型4	模型5	模型1	模型2	模型3	模型4	模型5	模型6
体系划分	WTP-AC连接方式	L3	L3	L3	L3	L3	L3	L3	L3	L2	L3	L3
	管理帧终结	WTP	WTP	WTP	WTP	WTP	AC	AC	AC	AC	AC/WTP	AC
	控制帧终结	WTP	WTP	WTP	WTP	WTP	WTP	WTP	WTP	WTP	WTP	WTP
	数据帧分发、集成	AC	AC	WTP	AC	WTP	AC	AC	AC	AC	AC	AC
Capwap功能	射频监控	WTP	WTP	AC/WTP	WTP	WTP	WTP	WTP	WTP	WTP	WTP	WTP
	射频配置	AC	AC	AC	AC	AC	AC/WTP		AC/WTP	WTP	WTP	WTP
	WTP配置	AC	AC	AC	AC	AC	AC		AC	AC	AC	AC
	WTP固件管理	AC	AC	AC	AC	AC	AC		AC	AC	AC	AC
	STA数据库	AC	AC/WTP	AC/WTP	AC/WTP	AC	AC		AC	AC	AC	AC
	AC/WTP交互认证	AC/WTP	AC/WTP	AC/WTP	AC/WTP	AC/WTP	AC/WTP	AC/WTP	AC/WTP	AC/WTP		
802.11功能	分发服务	AC	AC	WTP	AC	WTP	AC	AC	AC	AC	AC	AC
	集成服务	WTP	WTP	WTP	WTP	WTP	AC	AC	AC	AC	AC	AC
	Beacon处理	WTP	WTP	WTP	WTP	WTP	WTP	WTP	WTP	WTP	WTP	WTP
	Probe处理	WTP	WTP	WTP	WTP	WTP	WTP	AC/WTP	WTP	WTP	WTP	WTP
	节电管理/报文缓冲	WTP	WTP	WTP	WTP	WTP	WTP	WTP	WTP	AC	AC/WTP	WTP
	分片、重组	WTP	WTP	WTP	WTP	WTP	WTP		WTP	AC	AC	AC
	关联/解除关联/重关联	AC	WTP	WTP	WTP	WTP	AC	AC	AC	AC	WTP	AC
802.11e QOS	(WMM)流分类	AC				WTP			AC	AC	AC	AC
	(WMM)调度	WTP	AC/WTP	WTP	WTP	WTP	WTP/AC	AC	WTP	AC	AC	WTP/AC
	(WMM)队列	WTP		WTP	WTP	WTP	WTP/AC	WTP	WTP	AC	WTP	WTP/AC
802.11i认证和加密	802.1X/EAP	AC	AC	AC/WTP	AC	AC/WTP	AC	AC	AC	AC	AC	AC
	KEY管理	AC	AC	WTP	AC	AC	AC	AC	AC	AC	AC	AC
	加解密	WTP	WTP	WTP	WTP	WTP	WTP	AC	WTP	AC	AC	AC
	WAI	WTP	WTP	WTP	WTP	WTP	WTP	WTP	WTP	WTP	WTP	WTP
	WPI	WTP	WTP	WTP	WTP	WTP	WTP	WTP	WTP	WTP	WTP	WTP

CAPWAP协议中对Splic MAC及Local MAC的功能划分

Function	Splic MAC	Local MAC
Distribution Service	AC	WTP/AC
Integration Service	AC	WTP
Beacon Generation	WTP	WTP
Probe Response Generation	WTP	WTP
Power Mgmt/Packet Buffering	WTP	WTP
Fragmentation/Defragmentation	WTP/AC	WTP
Assoc/Disassoc/Reassoc	AC	WTP/AC
IEEE 802.11 QoS		
Classifying	AC	WTP
Scheduling	WTP/AC	WTP
Queuing	WTP	WTP
IEEE 802.11 RSN		
IEEE 802.1X/EAP	AC	AC
RSNA Key Management	AC	AC
IEEE 802.11 Encryption/Decryption	WTP/AC	WTP

瘦AP产品中的隧道技术

- 控制隧道
  - CAPWAP控制隧道
- 数据隧道
  - CAPWAP数据隧道
  - IPIP隧道
  - GRE隧道
  - IPSec隧道
  - 自定义隧道

AC的发现过程

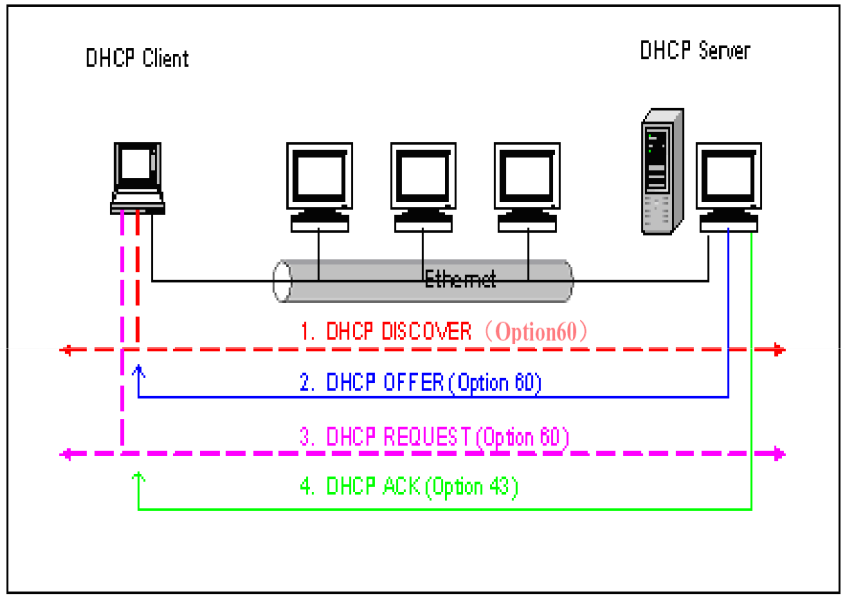
- AC的发现过程，是指当WTP进入网络时，通过发送AC发现请求信息，并获得AC发现响应信息，从而，找到可用的AC，并选择最为合适的AC以建立CAPWAP会话的过程。
  - 静态发现：可以在WTP上预置AC地址，则不需要发现过程。
  - 动态发现：通常情况下WTP需要对备选AC进行动态发现，此时，就会有AC的发现过程。
    - 二层发现
      - 当WTP和AC在同一个第二层VLAN和IP子网时，WTP可以通过广播AC发现请求信息发现AC。位于同一个子网的AC都将进行应答。
    - 三层发现：AP首先通过DHCP或DNS方式得到AC的IP地址，然后向AC发送发现请求信息，进而认证建立连接的过程。
      - DHCP发现过程
      - DNS发现过程
  - 目前在项目过程中，通常会采用DHCP发现方法

二层发现过程

1. AP接入网络后，会发起AC Discover请求。
2. AC会响应请求并返回AC地址。
3. AP取得AC地址后，主动发起与AC的认证连接。
4. AC对AP进行验证后，与AP建立CAPWAP连接。
5. AP从AC上获得配置信息，完成配置过程。

DHCP发现过程

- 1） DHCP Client（AP）上电或重启时，就像所有的DHCP Client 第一次登录一样，会寻找DHCP Server。它会向网络广播一个DHCP DISCOVER 封包。因为客户端还不知道自己属于哪一个网络，所以封包的源地址会为0.0.0.0，而目的地址则为255.255.255.255，然后再附上DHCP DISCOVER及Option 60 的信息，向网络进行广播。DHCP Option 60 信息，主要包括企业码（Enterprise Code）、Vender、Category、Model、Version、Protocol Type/Port Number（for Port forwarding)信息。
- 2） DHCP Server 接收到来自DHCP Client 的DHCP DISCOVER 信息，然后发出DHCP OFFER响应报文，其中包括分配的可用的IP 地址，TCP/IP 信息等。
- 3） DHCP Client 可能会收到多个DHCP OFFER 报文，最终DHCP Client 应依据DHCP OFFER报文，优先选择DHCP Option 60 企业码与自己相同DHCP Server 发来的报文。
- 4） DHCP Client 将广播一个DHCP REQUEST 封包，其中包含了自己所选的server 信息，DHCP Client 的Vender、Category、Model 等信息则包含在DHCP Option 60 中一起发送。
- 5） DHCP Server 收到DHCP REQUEST 封包后，将依据Vender，Category，Model 的内容，及DHCP Client 的MAC 地址等信息查询DHCP Server 内部的策略表，给予相应的DHCP ACK 响应报文，其中包括完成自动配置的DHCP Option 43 信息。可用的AC 地址列表也包含在DHCP Option 43 信息中。
- 6） DHCP Client 收到DHCP ACK 报文后，从中获取自动配置信息，并选择合适的AC。从这一点上说，DHCPServer对设备的自动配置已经完成了，
- 7） DHCP Client 在断开时应该主动给DHCP Server 发送DHCP RELEASE 报文，DHCP Server 也将释放分配给DHCP Client 的资源。
- 8）之后，WTP向AC发送AC发现请求包，并从收到的响应包中选择AC.



注：DHCP方式可以部署在二层和三层组网中，但是当采用三层组网时，需要所有开启DHCP Relay的设备都支持Option43，并保证AP可以正确获得Option43的值。

DNS发现过程

1. AP中预设AC的域名。
2. AP接入网络中，通过DHCP，或者手工设定IP信息。
3. AP通过DNS服务器对预设AC域名的解析获得AC的IP地址。
4. AP取得AC地址后，主动发起与AC的认证连接。
5. AC对AP进行验证后，与AP建立CAPWAP连接。
6. AP从AC上获得配置信息，完成配置过程。

Q&A

中太数据
ZOOM NETWORKS