大型WLAN组网部署

一、大型WLAN组网的应用

二、大型WLAN组网的特点

1、网络规模大 —— 设备型号繁杂、分布位置广且设备数量庞大，运维成本高

2、用户多分布广 —— 用户数量庞大，分布较广，网络体验要求高

3、可靠性要求高 —— AC控制器掌控全网的无线网络，出现故障会带来极大的经济损失

4、接入安全要求高 —— 访客、员工、合作伙伴等人员会在不定期接入到内部网络，一个密码就能接入网络的场景不再适用

三、华为大型WLAN方案功能

1、设备统一管理 —— 全网设备统一纳管，配置自动备份，告警实时上报，网管不再有烦恼

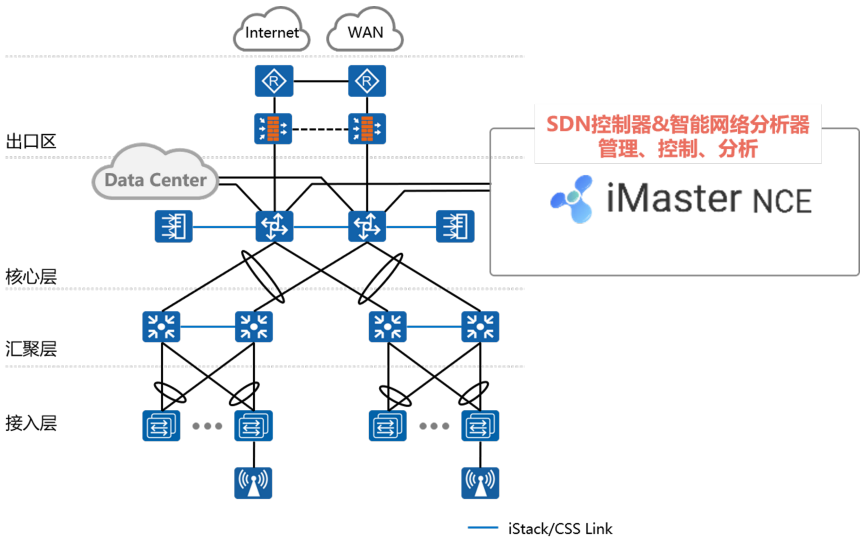
2、漫游&业务随行 —— 无缝漫游，用户在园区网络内移动时，只要身份不变，则其网络访问权限及体验将随之而动

3、高可靠性技术 —— 双机冷备、双机热备、N+1备份等多种高可靠性技术保障WLAN网络稳定运行

4、接入&终端安全保障 —— 准入控制技术以及终端安全防护确保安全无死角

四、WLAN网络解决方案

1、WLAN配合SDN控制器使用，由SDN控制器统一管理和配置，能够实现业务发放自动化、网络全生命周期管理，结合大数据和AI技术可实现园区网络的智能、极简和安全。园区网络更具备有线与无线的深度融合能力



2、大型WLAN网络关键技术

技术	作用
VLAN Pool	通过VLAN Pool把接入的用户分配到不同的VLAN，可以减少广播域，减少网络中的广播报文，提升网络性能
DHCP Option 43 & 52	当AC和AP间是三层组网时，AP通过发送广播请求报文的方式无法发现AC，这时需要通过DHCP服务器回应给AP的报文中携带的Option43字段（IPv4）或Option52（IPv6）来通告AC的IP地址
漫游技术	WLAN漫游是指STA在不同AP覆盖范围之间移动且保持用户业务不中断的行为
高可靠性技术	为了保证WLAN业务的稳定运行，保证在主设备故障时业务能够顺利切换到备份设备的技术
准入控制	准入控制技术是通过对接入网络的客户端和用户的认证来保证网络的安全，是一种“端到端”的安全技术

五、VLAN Pool的概念

1、现有网络面临的挑战

1.1、无线网络终端的移动性导致特定区域IP地址请求较多

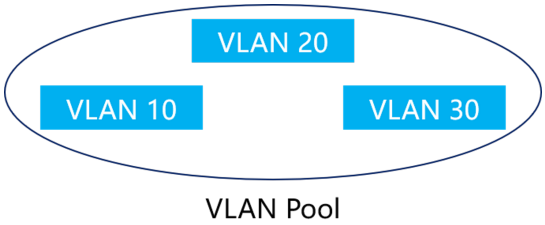
1.2、通过情况下，一个SSID只能对应一个业务VLAN，如果通过扩大子网增加IP地址则会导致广播域扩大，大量的广播报文造成网络拥塞

2、VLAN Pool是一种把多个VLAN放在一个池中并提供分配算法的VLAN分配技术，又称为VLAN池

3、通过VLAN Pool把接入的用户分配到不同的VLAN，可以减少广播域，减少网络中的广播报文，提升网络性能

4、由于无线终端的移动性，在无线网络中经常有大量用户从某个区域接入后，随着用的移动，再漫游到其他区域，导致该区域的用户接入多，对IP地址数目要求大。比如：场馆入口、酒店的大堂等。目前一个SSID只能对应一个VLAN，一个VLAN对应一个子网，如果大量用户从某一区域接入，只能扩大VLAN的子网，保证用户能够获取到IP地址。这样带来的问题就是广播域扩大，导致大量的广播报文（如：ARP、DHCP等）带来严重的网络拥塞

5、基于此问题考虑，一个SSID需要能够对应多个VLAN，把大量用户分散到不同的VLAN减少广播域。VLAN Pool提供多个VLAN的管理和分配算法，实现SSID对应多个VLAN的方案



6、VLAN Pool分配VLAN的算法

6.1、顺序分配算法：把用户按上线顺序依次划分到不同的VLAN中，用户上下线用户VLAN容易变化，IP地址变更

6.2、HASH分配算法：根据用户MAC地址HASH值分配VLAN，用户分配的VLAN固定，可能导致VLAN间用户划分不均匀，有的VLAN用户较多，有的较少

两种分配方式的比较：

分配算法	优点	缺点
顺序分配	各个VLAN用户数目划分均匀	重新上线VLAN容易变更、IP变化
HASH分配	用户多次上线可分配相同的VLAN、IP不变	各个VLAN用户数划分不均衡

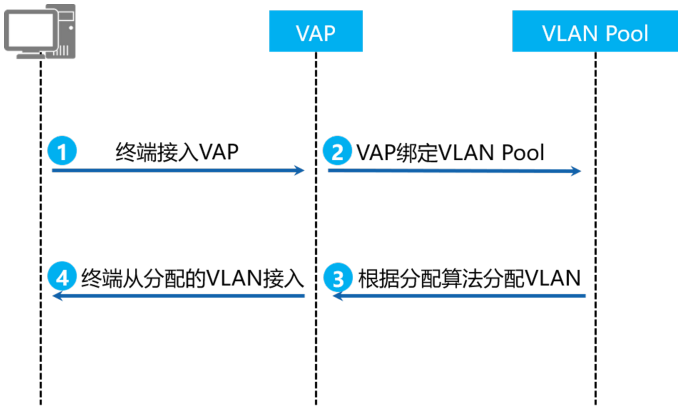
7、VLAN Pool分配VLAN流程

7.1、用户终端从某个VAP接入，判断VAP是否有绑定VLAN Pool

7.2、若该VAP对应的模板绑定了VLAN Pool，使用VLAN Pool的分配算法分配一个VLAN, VLAN Pool有顺序分配和hash分配两种分配算法

7.3、给终端分配一个VLAN

7.4、终端从VLAN Pool分配的VLAN上线

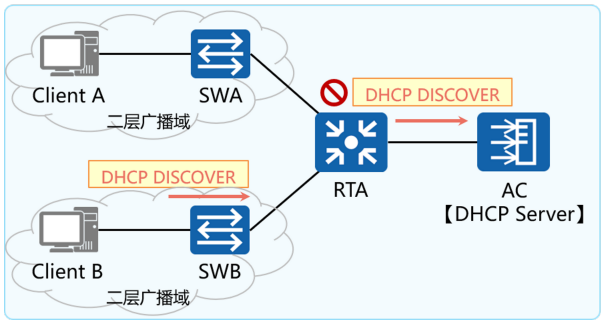


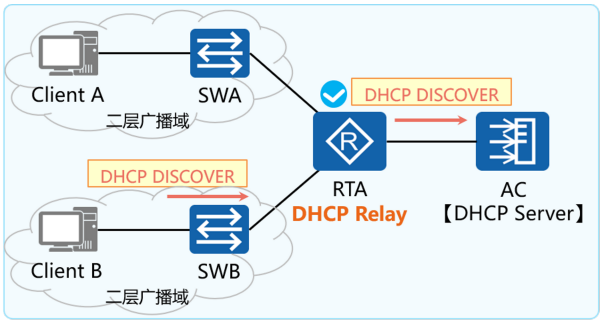
注：VAP【Virtual Access Point | 虚拟接入点】：VAP就是在一个物理实体AP上虚拟出多个AP，每一个被虚拟出的AP就是一个VAP，每个VAP提供和物理实体AP一样的功能。用户可以在一个AP上创建不同的VAP来为不同的用户群体提供无线接入服务

六、DHCP中继

1、DHCP客户端使用IP广播来寻找同一网段上的DHCP服务器。当服务器和客户段处在不同网段，即被路由器分割开来时，路由器是不会转发这样的广播包

2、DHCP中继能够跨网段【透传】DHCP报文，使得一个DHCP服务器同时为多个网段服务成为可能

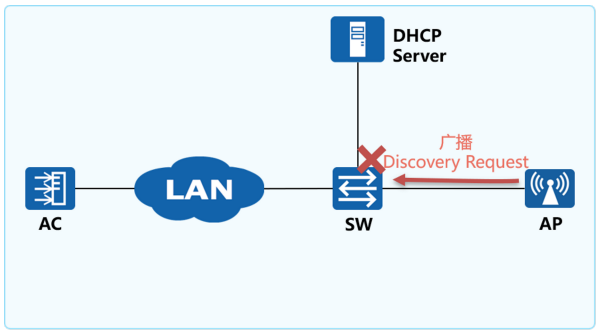




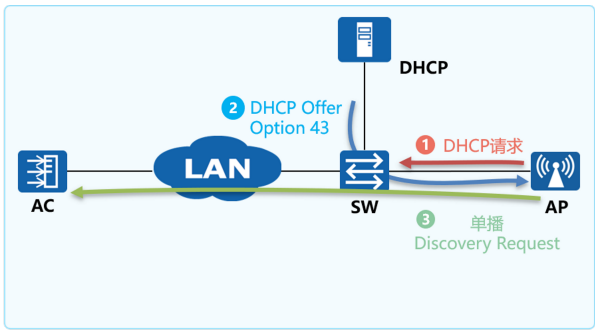
3、随着网络规模的不断扩大，网络设备不断增多，企业内不同的用户可能分布在不同的网段，一台DHCP服务器在正常情况下无法满足多个网段的地址分配需求。企业内网各个网段通常都没有与DHCP Server在同一个二层广播域内，如果还需要通过DHCP服务器分配IP地址，则需要跨网段发送DHCP协议报文

七、WLAN三层组网AC发现机制

1、当AC和AP间是三层组网时，AP通过发送广播请求报文的方式无法发现AC，这时需要通过DHCP服务器回应给AP的报文中携带的Option43字段（IPv4）或Option52（IPv6）来通告AC的IP地址



WLAN三层组网场景，AP的广播Discovery Request报文无法发现AC，导致CAPWAP隧道无法建立



WLAN三层组网场景，配置DHCP Option 43后，在AP获取IP地址阶段，同时获取了AC的IP地址，直接通过单播与AC建立联系

2、在AC和AP间是二层组网的情况下，也可以配置Option43，AP会根据Option43的内容先向指定IP地址的AC发送单播请求报文，如果发送十次报文，AP都没有收到回应，则AP会继续以广播的方式来发现同一网段的AC。所以在二层组网的情况下Option 43不是必配的参数，但在三层组网的情况下则是必配的

3、Option 43即为Type值为43（0x2B）的Option字段，又称为厂商特定信息选项，DHCP服务器和DHCP客户端通过Option43交换厂商特定的信息。当DHCP服务器接收到请求Option43信息的DHCP请求报文后，将在回复报文中携带Option43，为DHCP客户端分配厂商指定的信息

八、WLAN漫游概述

1、WLAN漫游是指STA在不同AP覆盖范围之间移动且保持用户业务不中断的行为

2、实现WLAN漫游的两个AP必须使用相同的SSID和安全模板（安全模板名称可以不同，但是安全模板下的配置必须相同），认证模板的认证方式和认证参数也要配置相同

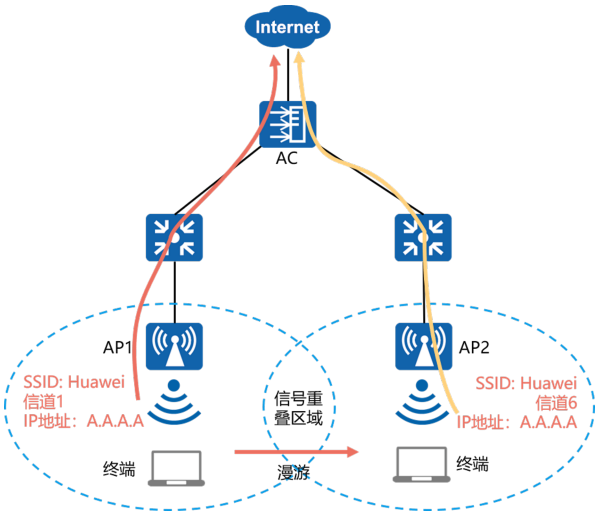
3、WLAN漫游策略主要解决以下问题：

3.1、避免漫游过程中的认证时间过长导致丢包甚至业务中断

3.2、保证用户授权信息不变

3.3、保证用户IP地址不变

4、终端在移动过程中若逐渐远离接入AP，则链路的信号质量也会逐步下降。当终端感知到信号质量降低一定程度（漫游门限）时，终端会主动漫游到附近AP来提高信号质量



5、如上图所示，漫游一般包括如下动作：

5.1、终端已经与AP1建链，终端在各种信道中发送Probe Request。AP2在信道6（AP2使用的信道）中收到请求后，通过在信道6中发送应答来进行响应。终端收到应答后，对其进行评估，确定同哪个AP关联最合适。此时通过评估，终端与AP2关联最合适

5.2、终端通过信道6向AP2发送关联请求，AP2使用关联响应做出应答，建立用户与AP2间的关联，至此，用户与AP1的关联一直保持

5.3、删除用户与AP1现有的关联。终端通过信道1（AP1使用的信道）向AP1发送802.11解除关联信息，解除用户与AP1间的关联

6、WLAN漫游的相关术语

6.1、AC内漫游：若漫游过程中关联的是同一个AC，这次漫游就是AC内漫游

6.2、AC间漫游：若漫游过程中关联的不是同一个AC，这次漫游就是AC间漫游

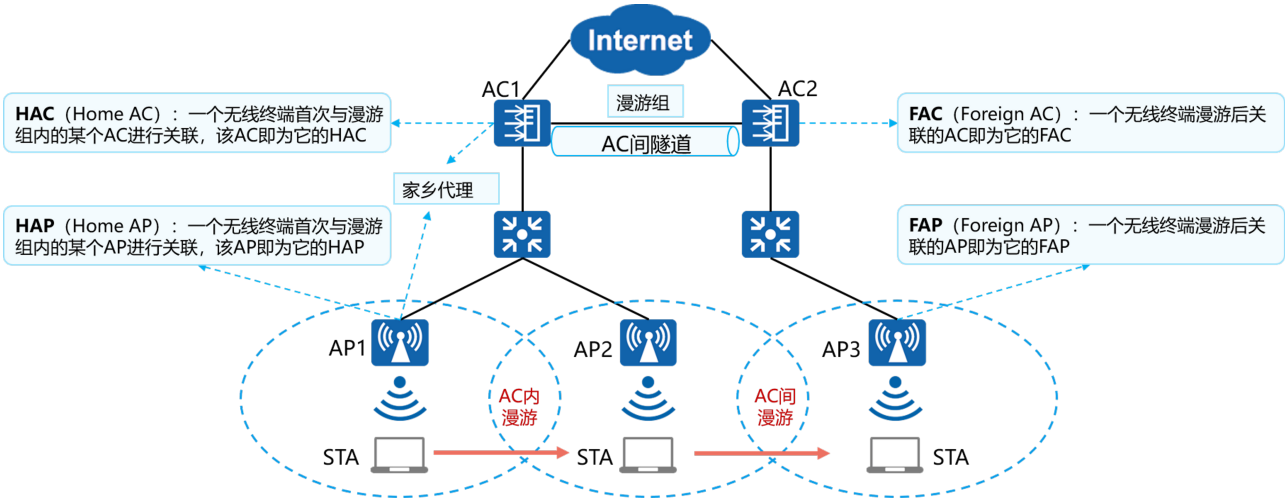
6.3、AC间隧道：为了支持AC间漫游，漫游组内的所有AC需要同步每个AC管理的STA和AP设备的信息，因此在AC间建立一条隧道作为数据同步和报文转发的通道；AC间隧道也是利用CAPWAP协议创建的

6.4、漫游组服务器：STA在AC间进行漫游，通过选定一个AC作为漫游组服务器，在该AC上维护漫游组的成员表，并下发到漫游组内的各AC，使漫游组内的各AC间相互识别并建立AC间隧道

6.4.1、漫游组服务器管理其它AC的同时不能被其它的漫游组服务器管理；也就是说若一个AC是作为漫游组服务器角色负责向其它AC同步漫游配置的，则它无法再作为被管理者接受其它AC向其同步漫游配置（即配置了漫游组就不能再配置漫游组服务器）

6.4.2、漫游组服务器作为一个集中配置点，不需要有特别强的数据转发能力，只需要能够和各个AC互通即可

6.5、家乡代理：能够和STA家乡网络的网关二层互通的一台设备。为了支持STA漫游后仍能正常访问家乡网络，需要将STA的业务报文通过隧道转发到家乡代理，再由家乡代理中转。STA的家乡代理由HAC或HAP兼任，用户可以选取AC1或AP1作为STA的家乡代理

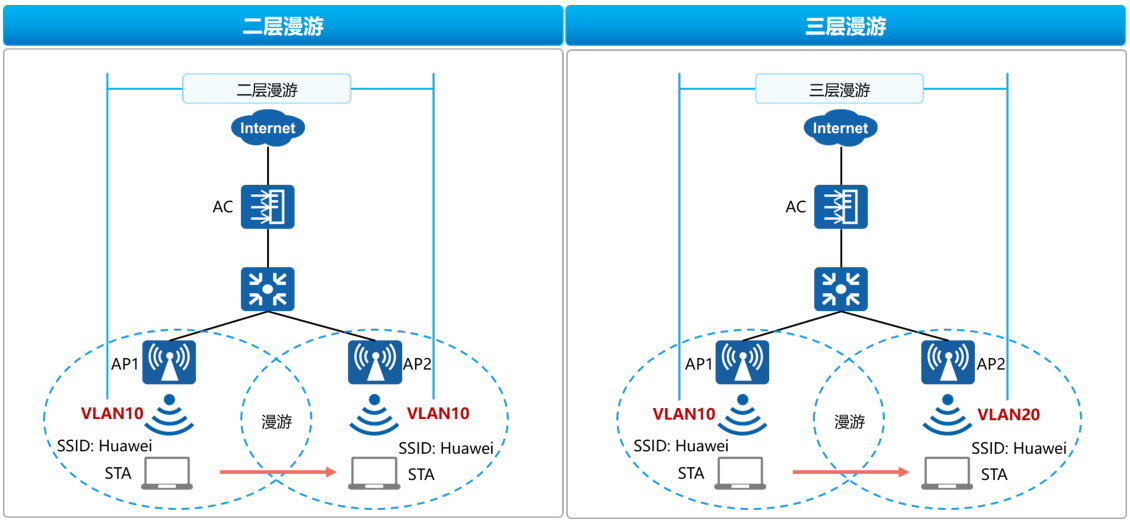


7、WLAN漫游类型

7.1、二层漫游：1个无线客户端在2个AP（或多个AP）之间来回切换连接无线，前提是这些AP都绑定的是同1个SSID并且业务VLAN都在同1个VLAN内（在同一个IP地址段），漫游切换的过程中，无线客户端的接入属性（比如无线客户端所属的业务VLAN、获取的IP地址等属性）不会有任何变化，直接平滑过渡，在漫游的过程中不会有丢包和断线重连的现象

7.2、三层漫游：漫游前后SSID的业务VLAN不同，AP所提供的业务网络为不同的三层网络，对应不同的网关。此时，为保持漫游用户IP地址不变的特性，需要将用户流量迂回到初始接入网段的AP，实现跨VLAN漫游

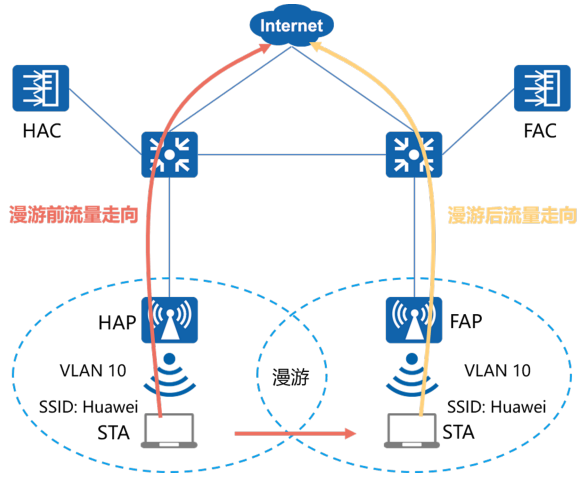
注：网络中有时候会出现以下情况：两个业务VLAN的VLAN ID相同，但是这两个子网又属于不同的子网。此时为了避免系统仅仅依据VLAN ID将用户在两个子网间的漫游误判为二层漫游，需要通过漫游域来确定设备是否在同一个子网内，只有当VLAN相同且漫游域也相同的时候才是二层漫游，否则是三层漫游



8、根据WLAN数据转发类型以及跨三层与否，可将漫游流量转发模型划分为四种：

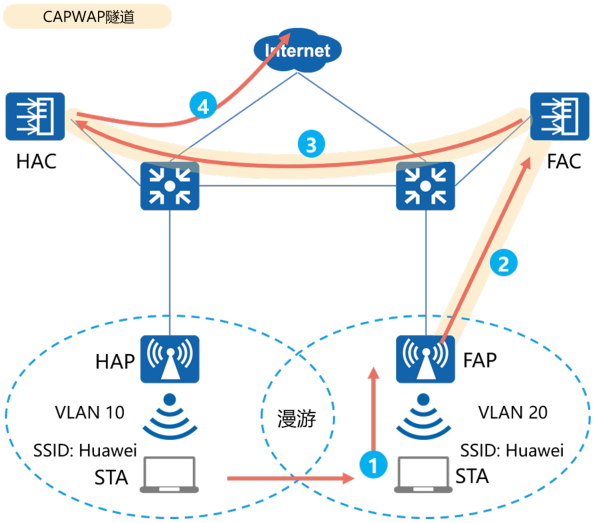
转发模型	特点
二层漫游直接转发	由于二层漫游后STA仍然在原来的子网中，所以FAP/FAC对二层漫游用户的流量转发和平台新上线的用户没有区别，直接在FAP/FAC本地的网络转发，不需要通过隧道转发回家乡代理中转
二层漫游隧道转发	
三层漫游直接转发	HAP和HAC之间的业务报文不通过CAPWAP隧道封装，无法判定HAP和HAC是否在同一个子网内，此时设备默认报文需返回到HAP进行中转
三层漫游隧道转发	HAP和HAC之间的业务报文通过CAPWAP隧道封装，此时可以将HAP和HAC看作在同一个子网内，所以报文无需返回HAP，可直接通过HAC中转到上层网络

9、AC间二层漫游 — 直接转发



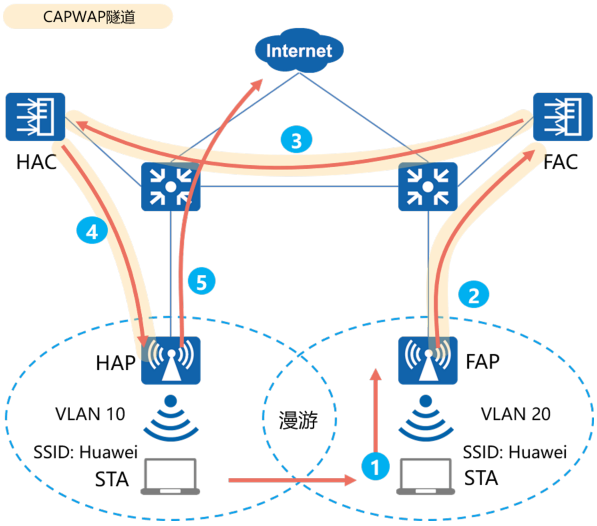
漫游前：
STA发送业务报文给HAP
HAP接收到业务报文后经由网关（交换机）发送给上层网络
漫游后：
STA发送业务报文给FAP
FAP接收到业务报文后经由网关（交换机）发送给上层网络

10、AC间三层漫游 — 隧道转发



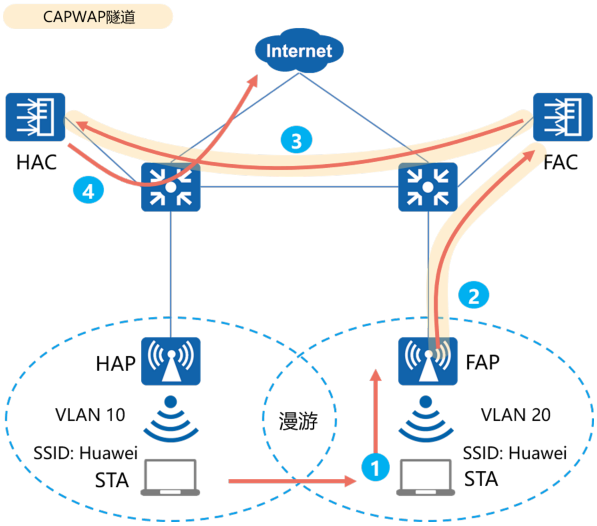
漫游前：
STA发送业务报文给HAP
HAP接收到业务报文后通过CAPWAP隧道发送给HAC
HAC直接将业务报文经过交换机发送给上层网络
漫游后：
STA发送业务报文给FAP
FAP接收到业务报文后通过CAPWAP隧道发送给FAC
FAC通过HAC和FAC之间的AC间隧道将业务报文转发给HAC
HAC直接将业务报文经由交换机发送给上层网络

11、AC间三层漫游 — 直接转发【HAP为家乡代理】



漫游前：
STA发送业务报文给HAP
HAP接收到业务报文后直接将业务报文经过交换机发送给上层网络
漫游后：
STA发送业务报文给FAP
FAP接收到STA发送的业务报文并通过CAPWAP隧道发送给FAC
FAC通过HAC和FAC之间的AC间隧道将业务报文转发给HAC
HAC通过CAPWAP隧道将业务报文发送给HAP
HAP直接将业务报文发送给上层网络
注：直接转发模式下，HAP和HAC之间的业务报文不通过CAPWAP隧道封装，无法判定HAP和HAC是否在同一个子网内，此时设备默认报文需要返回到HAP进行中转。如果HAP和HAC在同一个子网时，可以将家乡代理设置为性能更强的HAC，减少HAP的负荷并提高转发效率

12、AC间三层漫游 — 直接转发【HAC为家乡代理】



漫游前：
STA发送业务报文给HAP
HAP接收到业务报文后直接将业务报文经过交换机发送给上层网络
漫游后：
STA发送业务报文给FAP
FAP接收到STA发送的业务报文并通过CAPWAP隧道发送给FAC
FAC通过HAC和FAC之间的AC间隧道将业务报文转发给HAC
HAC直接将业务报文发送给上层网络

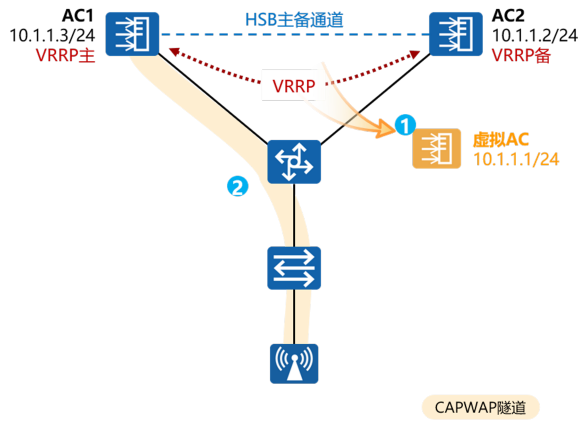
九、AC高可靠性概述

在WLAN组网中，为保证组网可靠性，常见的备份技术有：

1、VRRP双机热备份【主备】

1.1、主备AC两个独立的IP地址，通过VRRP对外虚拟为同一个IP地址，单个AP和虚拟IP建立一条CAPWAP链路

1.2、主AC备份AP信息、STA信息和CAPWAP链路信息，并通过HSB主备服务将信息同步给备AC；主AC故障后，备AC直接接替工作



1.2.1、两台AC组成一个VRRP组，主、备AC对AP始终显示为同一个虚拟IP地址，主AC通过Hot Standby（HSB）主备通道同步业务信息到备AC上

1.2.2、两台AC通过VRRP协议产生一台“虚拟AC”，缺省情况下，主AC担任虚拟AC的具体工作，当主AC故障时，备AC接替其工作；所有AP与“虚拟AC”建立CAPWAP隧道

1.2.3、AP只看到一个AC的存在，AC间的切换由VRRP决定

1.2.4、这种方式一般将主备AC部署在同一地理位置，和其它备份方式比较，其业务切换速度非常快

注1：AC目前支持VRRP单实例整机热备，不支持负载均衡。整机热备具有以下特点:

上行链路可以互为备份，主备VRRP可以track上行口状态，AC整机主备状态可能与各下行链路通断状态不一致

下行多条链路(包括有线、无线) 采用MSTP破环，MSTP状态变更时会自动清除链路上的MAC/ARP表

注2：HSB的相关概念

1、HSB【Hot Standby | 热备份】是华为主备公共机制，其由2部分组成：

1.1、主备服务【HSB service】：建立和维护主备通道，为各个主备业务模块提供通道通断事件和报文发送/接收接口

1.1.1、HSB主备服务负责在两个互为备份的设备间建立主备备份通道，维护主备通道的链路状态，为其它业务提供报文的收发服务，并在主链路发生故障时通知主备业务备份组进行相应的处理

1.1.2、HSB主备服务主要包括两个方面：

a、建立主备备份通道

b、维护主备通道的链路状态

1.2、主备备份组【HSB group】：HSB备份组内部绑定HSB service，为各个主备业务模块提供数据备份通道；HSB备份组与一个VRRP实例绑定，借用VRRP机制协商出主备实例；同时，HSB备份组还负责通知各个业务模块处理批量备份、实时备份、主备切换等事件

2、数据同步

基于VRRP双机热备备份信息包括用户表项、CAPWAP链路信息以及AP表项等信息，备份的方式有实时备份，批量备份，定时备份

2.1、批量备份：主用设备会将已有的会话表项一次性同步到新加入的备份设备上，使主备AC信息对齐，这个过程称为批量备份。批量备份会在AC主备确立时进行触发

2.2、实时备份：主用设备在产生新表项或表项变化后会及时备份到备份设备上

2.3、定时同步：备用设备会每隔30分钟检查其已有的会话表项与主用设备是否一致，若不一致则将主用设备上的会话表项同步到备用设备

1.3、VRRP双机热备配置流程

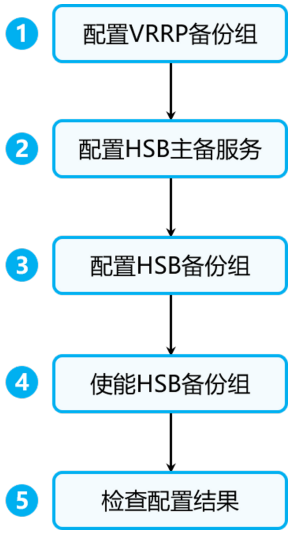
1.3.1、创建VRRP备份组并配置虚拟IP地址

1.3.2、创建HSB主备服务，建立HSB主备备份通道的IP地址和端口号

1.3.3、创建HSB备份组，配置HSB备份组绑定HSB主备服务、VRRP备份组、WLAN业务以及DHCP

1.3.4、使能HSB备份组，HSB备份组使能后，对HSB备份组的相关配置才会生效

1.3.5、检查VRRP热备份配置结果



2、双链路热备份【主备&负载分担】

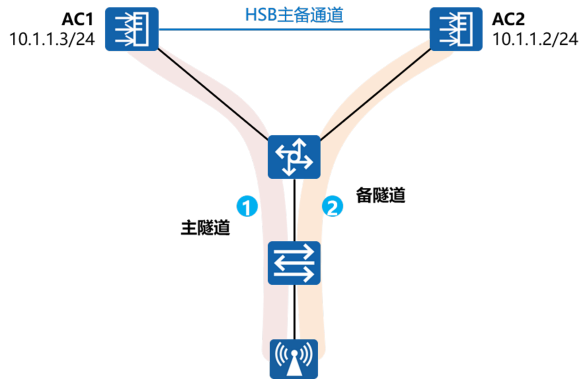
2.1、单个AP分别和主备AC建立CAPWAP链路，一条主链路，一条备链路

2.2、主AC仅备份STA信息，并通过HSB主备服务将信息同步给备AC；主AC故障后，AP切换到备链路上，备AC接替工作

2.3、双链路双机热备场景下，业务直接绑定HSB备份服务，这样HSB对业务仅提供备份数据收发的功能，用户的主备状态由双链路机制进行维护

2.4、双链路热备份除了支持主备备份之外，还支持负载分担模式。负载分担模式下可以指定一部分AP的主AC为AC1，与其建立CAPWAP主链路，一部分AP的主AC为AC2，与其建立CAPWAP主链路

2.5、双链路双机热备的主备AC不受地理位置限制，部署灵活，可进行负载分担，有效利用资源，但业务切换速度较慢



2.6、双链路热备份的主备协商&建立主链路

AP与AC建立主链路，在Discovery阶段要优选出主AC

2.6.1、开启双链路备份功能后，AP开始发送Discovery Request报文

2.6.2、AC收到Request报文后回应Discovery Response报文

2.6.3、AP收集到主备AC回应的Discovery Response报文后，根据AC的优先级、设备的负载情况以及AC的IP地址来选择主AC

选择AC的优选顺序如下：

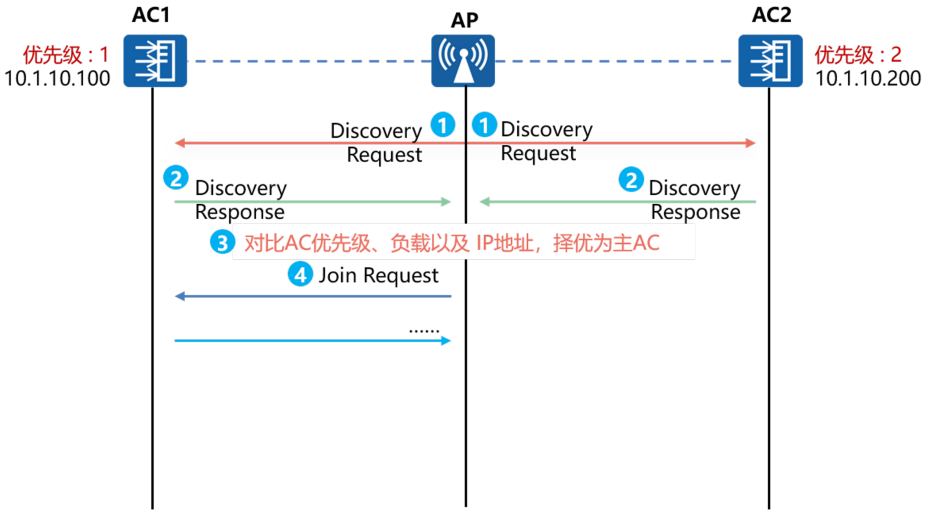
a、比较AC的优先级，优先级值小的为主AC，默认优先级为0，最大值为7，优先级值越小越优选；

b、若优先级相同，则比较AC设备的负载情况，即AP个数和STA个数，负载轻的为主AC。优先选择当前可接入AP数大的AC为主AC，如果当前可接入AP数相同，则选择当前可接入STA数大的AC为主AC；

c、若负载情况也相同，则比较IP地址，IP地址小的为主AC

注：当前可接入AP数=可接入的最大AP数-当前已接入的AP数，当前可接入STA数=可接入的最大STA数-当前已接入的STA数

2.6.4、AP开始与优选出的主AC建立CAPWAP主链路



建立主链路时，除了Discovery阶段要优选出主AC，其它过程跟正常情况下的CAPWAP隧道建立过程一致

在Discovery阶段，使能双链路备份功能后，AP开始发送Discovery Request报文，分为单播方式和广播方式：

a、若预先通过静态方式、DHCP服务器方式或DNS方式指定了主备AC的IP地址，AP向AC发送单播Discovery Request报文请求与主备AC关联

b、若没有配置AC的静态IP地址或者单播没有回应时，AP将发送广播Discovery Request报文请求同网段内可关联的AC

无论是单播发现还是广播发现，如果主备AC都正常，都会回应Discovery Response报文，并在该报文中携带双链路特性开关、优先级、负载情况以及IP地址

AP收集到主备AC回应的Discovery Response报文后，根据AC的优先级、设备的负载情况以及AC IP地址来选择主AC并开始与其建立CAPWAP主链路

2.7、建立备链路

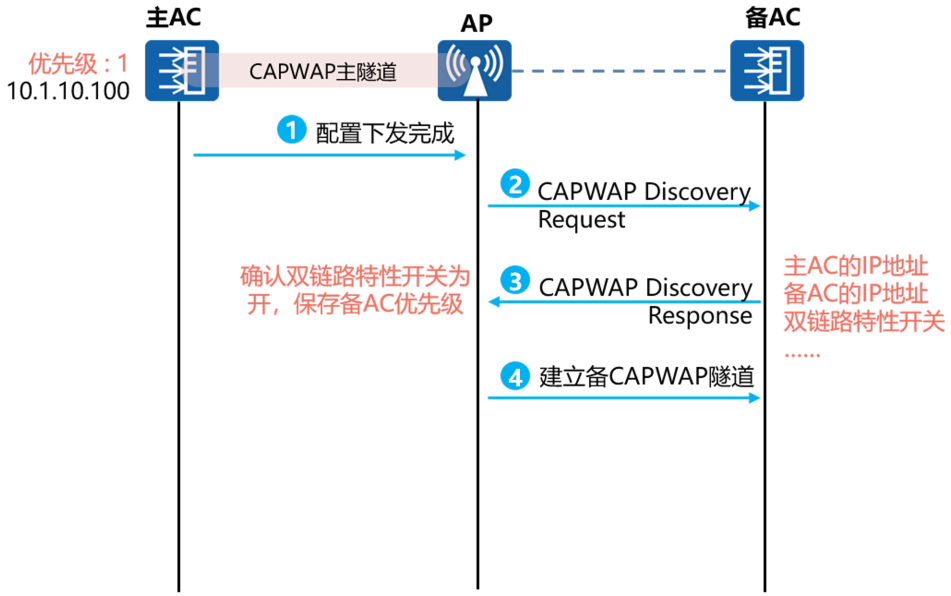
AP与AC建立备链路，为了避免业务配置重复下发导致错误，在AP和主AC建立主隧道并且配置下发完成后，才启动备CAPWAP链路的建立

2.7.1、主AC下发配置到AP上

2.7.2、AP开始建立备用隧道，向备AC发送单播CAPWAP Discovery Request报文

2.7.3、备AC收到Request报文后，回应Response报文，在该报文中携带优选AC的IP地址、备选AC的IP地址、双链路特性开关、负载情况及其优先级

2.7.4、AP收到备AC回应的Response报文后，获取到双链路特性开关为打开，并保存其优先级



a、若备份AC的优先级修改为比步骤1已经建立好CAPWAP链路的AC优先级高，也不进行主备倒换，待建立隧道完成后再进行倒换

b、AP发送的Join Request中，会携带一个自定义消息类型，告诉备AC配置已经下发过了，不需要再下发。AC收到Join Request，获取到该自定义消息时，在配置下发阶段，会跳过配置下发流程，避免对AP重复下发配置

c、备链路建立完成后，AP重新根据两个链路的优先级决策出主备AC

d、缺省情况下，CAPWAP心跳检测的间隔时间为25秒，心跳检测报文次数为6。如果开启了双链路备份功能，则CAPWAP心跳检测的间隔时间

为25秒，心跳检测报文次数为3

3、N+1备份

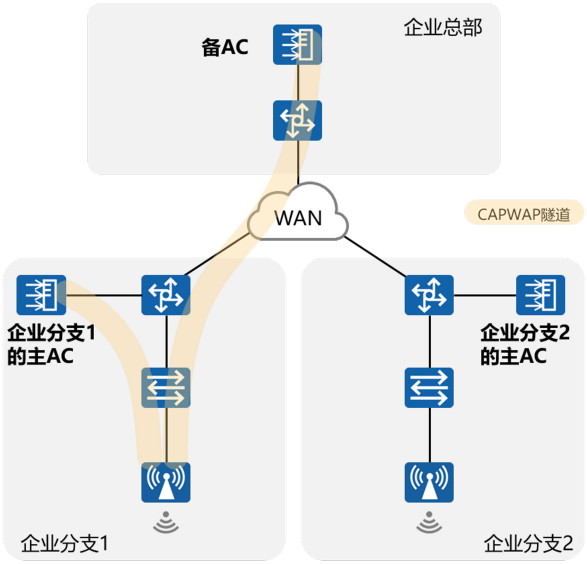
3.1、N+1备份是指在AC+FIT AP的网络架构中，使用一台AC作为备AC，为多台主AC提供备份服务的一种解决方案

3.2、网络正常情况下，AP只与各自所属的主AC建立CAPWAP链路

3.3、当主AC故障或主AC与AP间CAPWAP链路故障时，备AC替代主AC来管理AP，备AC与AP间建立CAPWAP链路，为AP提供业务服务

3.4、支持主备倒换，支持主备回切

3.5、当AP与主用AC之间的CAPWAP隧道中断时，将触发AP与备用AC建立CAPWAP隧道，此时AP会重新与该AC建链、重启并获取配置，在该过程中，业务将会受影响



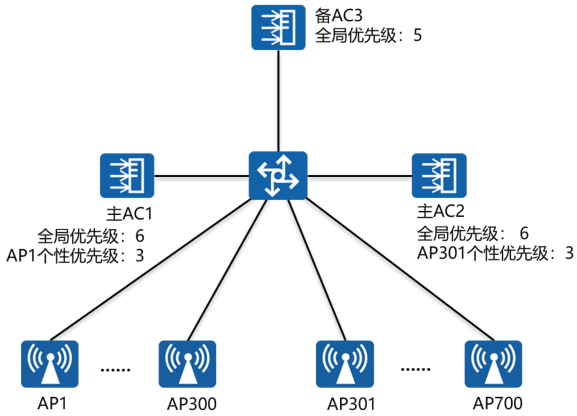
3.6、在Discovery阶段，AP发现AC后，要选择出最高优先级的AC作为主AC接入

3.7、AC上存在两种优先级：

3.7.1、全局优先级：针对所有AP配置的AC优先级，默认为0，最大值为7，优先级取值越小，优先级越高

3.7.2、个性优先级：针对指定的单个AP或指定AP组中的AP配置的AC优先级，没有默认值

注：AC全局优先级<AP在AC上优先级



3.8、当AC收到AP发送的Discovery Request报文时，若AC没有为该AP配置个性优先级，则在回应的Discovery Response报文中携带全局优先级

3.9、若AC已为该AP配置了个性优先级，则在回应的Discovery Response报文中携带个性优先级

3.10、正确配置主AC和备AC的不同优先级，可以控制AP能够在指定的主AC或备AC上线

4、双链路冷备份

4.1、单个AP分别和主备AC建立CAPWAP链路，一条主链路，一条备链路

4.2、AC不备份同步信息；主AC故障后，AP切换到备链路上，备AC接替工作

对比项	VRRP双机热备	双链路双机热备	N+1备份
切换速度	主备切换速度快，对业务影响小。通过配置VRRP抢占时间，相比于其他备份方式实现更快的切换	AP状态切换慢，需等待检测到CAPWAP断链超时后才会切换，主备切换后终端不需要重新上线	AP状态切换慢，需等待检测到CAPWAP断链超时后才会切换，AP、终端均需要重新上线，业务会出现短暂中断
主备AC异地部署	不建议主备AC异地部署	支持	支持
约束条件	主备AC的型号和软件版本需完全一致 一台备AC只支持为一台主AC提供备份	主备AC的型号和软件版本需完全一致 一台备AC只支持为一台主AC提供备份	主备AC产品形态可以不同，AC的软件版本必须一致 一台备AC支持为多台主AC提供备份，能降低购买设备的成本
适用范围	对可靠性要求高，且无须异地部署主备AC的场景	对可靠性要求高，且要求异地部署主备AC的场景	对可靠性要求较低，对成本控制要求较高的场景

十、NAC概述

NAC【Network Admission Control】称为网络接入控制，通过对接入网络的客户端和用户的认证保证网络的安全，是一种"端到端"的安全技术；其用于用户和接入设备之间的交互；负责控制用户的接入方式【802.1X，MAC或Portal认证】，接入过程中的各类参数和定时器；确保合法用户和接入设备建立安全稳定的连接

1、RADIUS概述

1.1、AAA可以通过多种协议来实现，在实际应用中，最常使用RADIUS协议

1.2、RADIUS是一种分布式的、客户端/服务器结构的信息交互协议，能保护网络不受未授权访问的干扰，常应用在既要求较高安全性、又允许远程用户访问的各种网络环境中

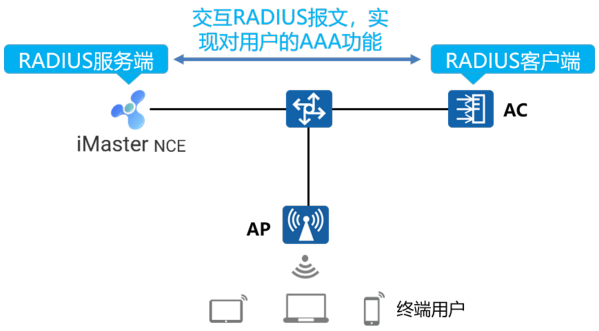
1.3、该协议定义了基于UDP【User Datagram Protocol】的RADIUS报文格式及其传输机制，并规定UDP端口1812、1813分别作为默认的认证、计费端口

1.4、RADIUS协议的主要特征如下：

1.4.1、客户端/服务器模式

1.4.2、安全的消息交互机制

1.4.3、良好的扩展性



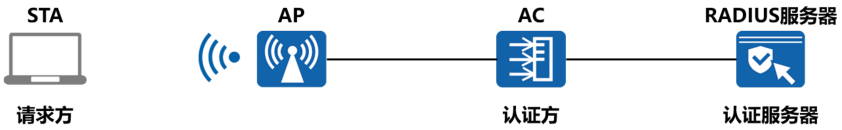
2、802.1X认证

2.1、802.1X是IEEE制定的关于用户接入网络的认证标准，主要解决以太网内认证和安全方面的问题

2.2、802.1X认证系统为典型的Client/Server结构，包括3个实体：请求方、认证方和认证服务器

2.3、认证服务器通常是RADIUS服务器，用于对申请者进行认证、授权和计费

2.4、对于大中型企业的员工，推荐使用802.1X认证



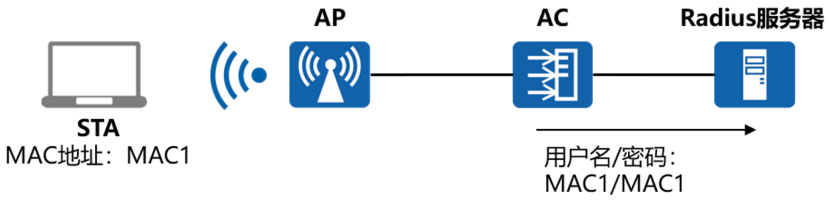
3、MAC认证

3.1、MAC认证是一种基于MAC地址对用户的网络访问权限进行控制的认证方法，它不需要用户安装任何客户端软件

3.2、接入设备在启动了MAC认证的接口上首次检测到用户的MAC地址后，即启动对该用户的认证操作

3.3、认证过程中，不需要用户手动输入用户名或者密码

3.4、MAC认证常用于哑终端【如打印机】的接入认证，或者结合认证服务器完成MAC优先的Portal认证，用户首次认证通过后，一定时间内免认证再次接入



4、Portal认证

4.1、Portal认证通常也称为Web认证，一般将Portal认证网站称为门户网站。用户上网时，必须在门户网站进行认证，如果未认证成功，仅可以访问特定的网络资源，认证成功后，才可以访问其他网络资源

4.2、用户上网时，必须在Portal页面进行认证，只有认证通过后才可以使用网络资源，同时服务提供商可以在Portal页面上开展业务拓展，如展示商家广告等

4.3、对于大中型企业的访客、商业会展和公共场所，推荐使用Portal认证

4.4、常用的Portal认证方式如下：

4.4.1、用户名和密码方式：由前台管理员给访客申请一个临时账号，访客使用临时账号认证

4.4.2、短信认证：访客通过手机验证码方式认证

4.5、Portal认证的优点：

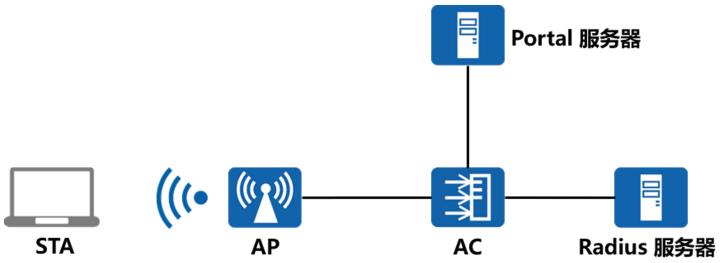
4.5.1、一般情况下，客户端不需要安装额外的软件，直接在Web页面上认证，简单方便

4.5.2、便于运营，可以在Portal页面上进行业务拓展，如广告推送、企业宣传等

4.5.3、技术成熟，被广泛应用于运营商、连锁快餐、酒店、学校等网络

4.5.4、部署位置灵活，可以在接入层或关键数据的入口作访问控制

4.5.5、用户管理灵活，可基于用户名与VLAN/IP地址/MAC地址的组合对用户进行认证



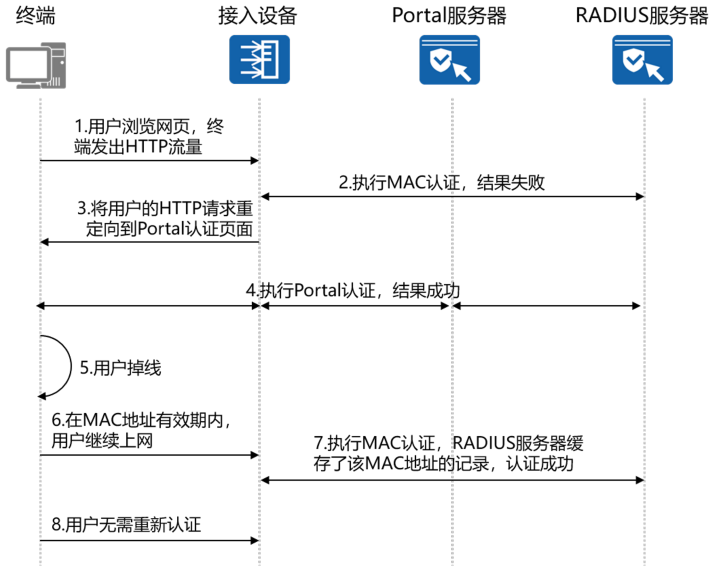
5、MAC优先的Portal认证

5.1、技术背景 —— 用户进行Portal认证成功后，如果断开网络，重新连接时需要再次输入用户名、密码，体验差

5.2、MAC优先的Portal认证

5.2.1、用户进行Portal认证成功后，在一定时间内断开网络重新连接，能够直接通过MAC认证接入，无需输入用户名密码重新进行Portal认证

5.2.2、该功能需要在设备配置MAC+Portal的混合认证，同时在认证服务器上开启MAC优先的Portal认证功能并配置MAC地址有效时间



6、三种认证方式比较

NAC包括三种认证方式：802.1X认证、MAC认证和Portal认证。由于三种认证方式认证原理不同，各自适合的场景也有所差异，实际应用中，可以根据场景部署某一种合适的认证方式，也可以部署几种认证方式组成的混合认证，混合认证的组合方式以设备实际支持为准

对比项	802.1X认证	MAC认证	Portal认证
适合场景	新建网络、用户集中、信息安全要求严格的场景	打印机、传真机等哑终端接入认证的场景	用户分散、用户流动性大的场景
客户端需求	需要	不需要	不需要
优点	安全性高	无需安装客户端	部署灵活
缺点	部署不灵活	需登记MAC地址，管理复杂	安全性不高

十一、VLAN Pool、DHCP中继、漫游、AC备份的配置

详细配置见实验手册