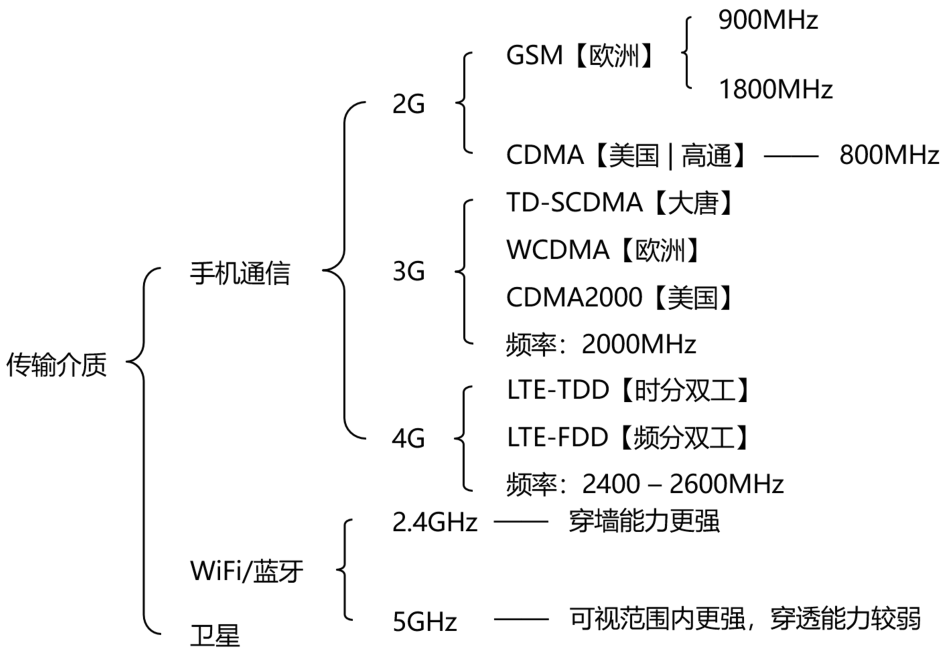
WLAN【Wireless Local Area Network】

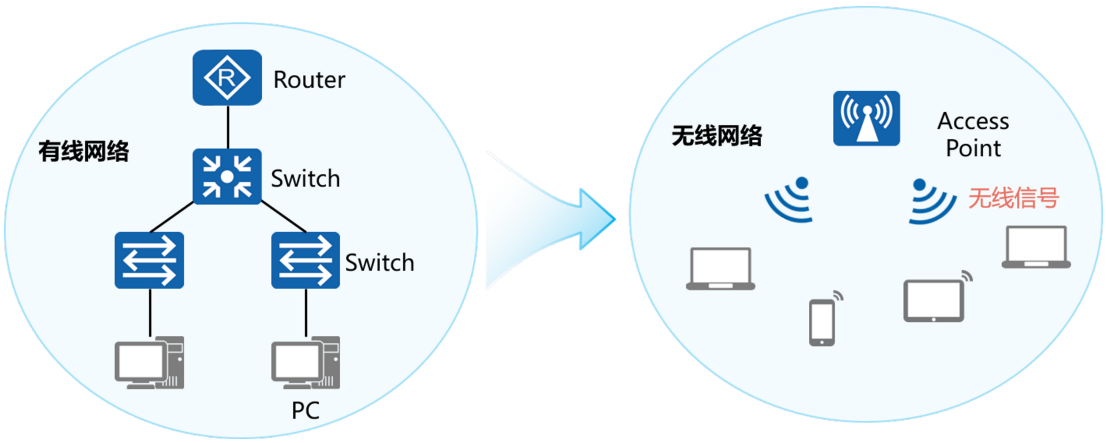
一、传输介质的概念



二、WLAN的概念

1、WLAN【Wireless Local Area Network | 无线局域网】，是指通过无线技术构建的无线局域网络。WLAN广义上是指以无线电波、激光、红外线等无线信号来代替有线局域网中的部分或全部传输介质所构成的网络

2、通过WLAN技术，用户可以方便地接入到无线网络，并在无线网络覆盖区域内自由移动，彻底摆脱有线网络的束缚

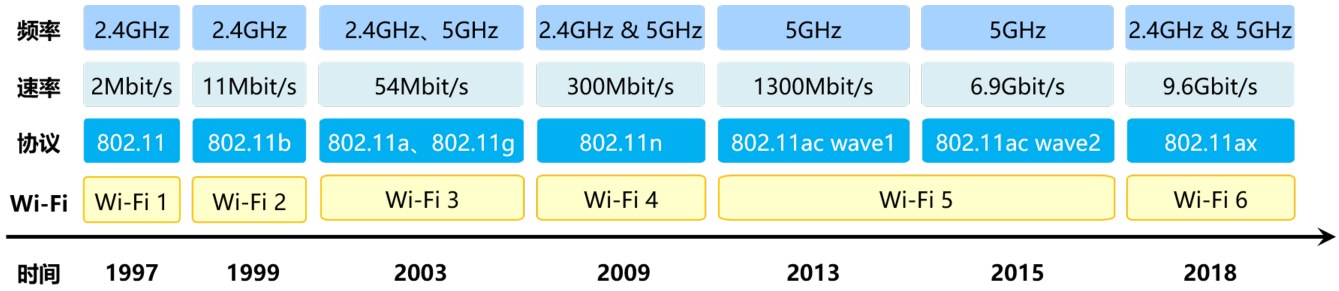


三、IEEE 802.11主要标准、WLAN与Wi-Fi

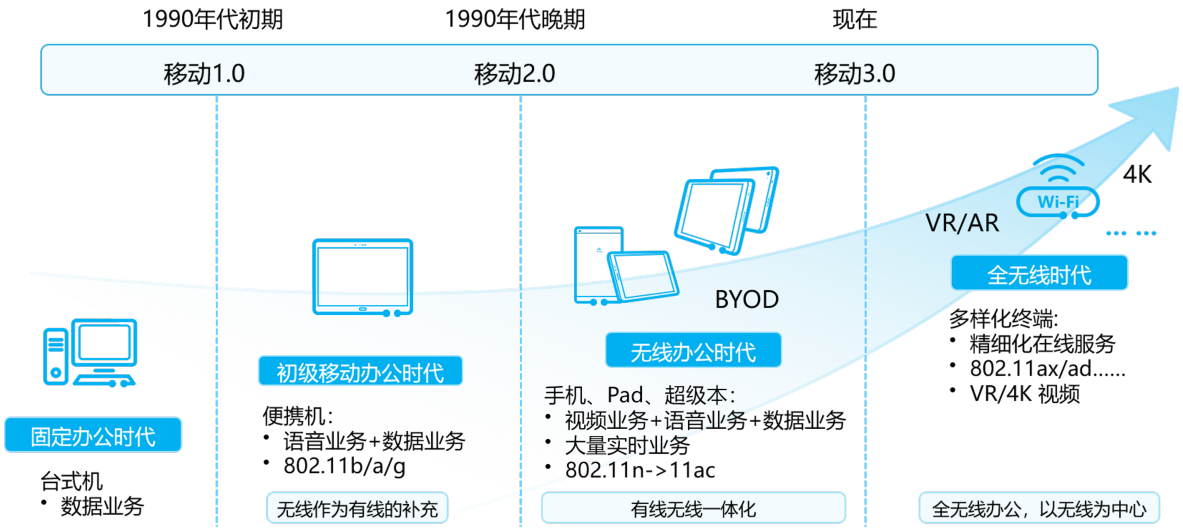
1、IEEE 802.11是现今无线局域网通用的标准。它是由国际电机电子工程学会(IEEE)定义的无线网络通信的标准

2、Wi-Fi联盟制造商的商标，并做为产品的品牌认证，是一种创建于IEEE 802.11标准上的无线局域网技术。在大多数场景下，Wi-Fi可等同于802.11

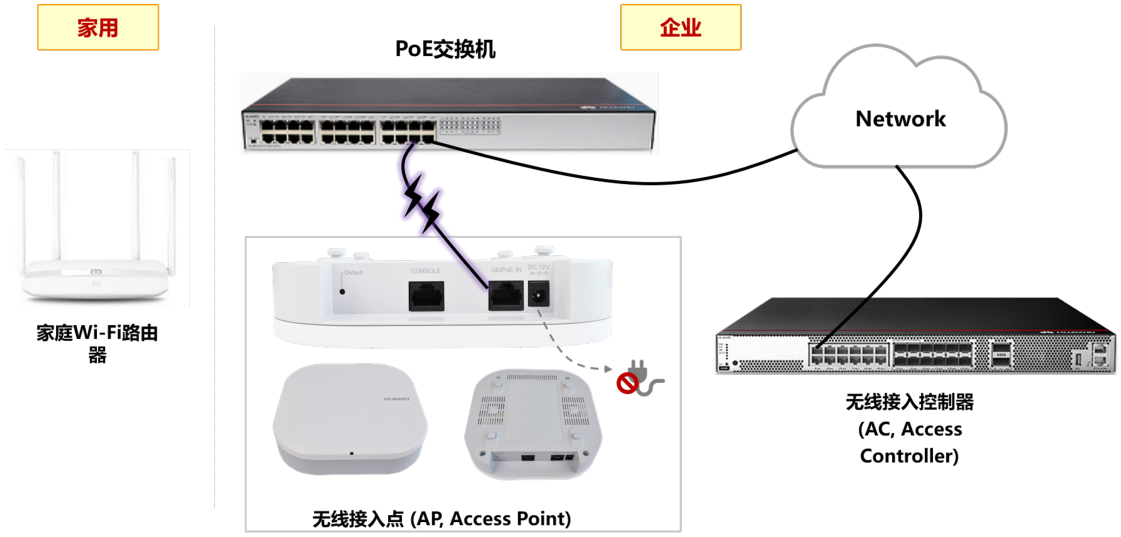
版本	年代	频段	速率
802.11【1997】	1997	2.4 GHz	2 Mbps
802.11 b	1999	2.4 GHz	11 Mbps
802.11 a	1999	5 GHz	54 Mbps
802.11 g	2003	2.4 GHz	54 Mbps
802.11 n	2009	2.4 GHz/5 GHz	600 Mbps
802.11 ac	2013	5 GHz	> 1 Gbps



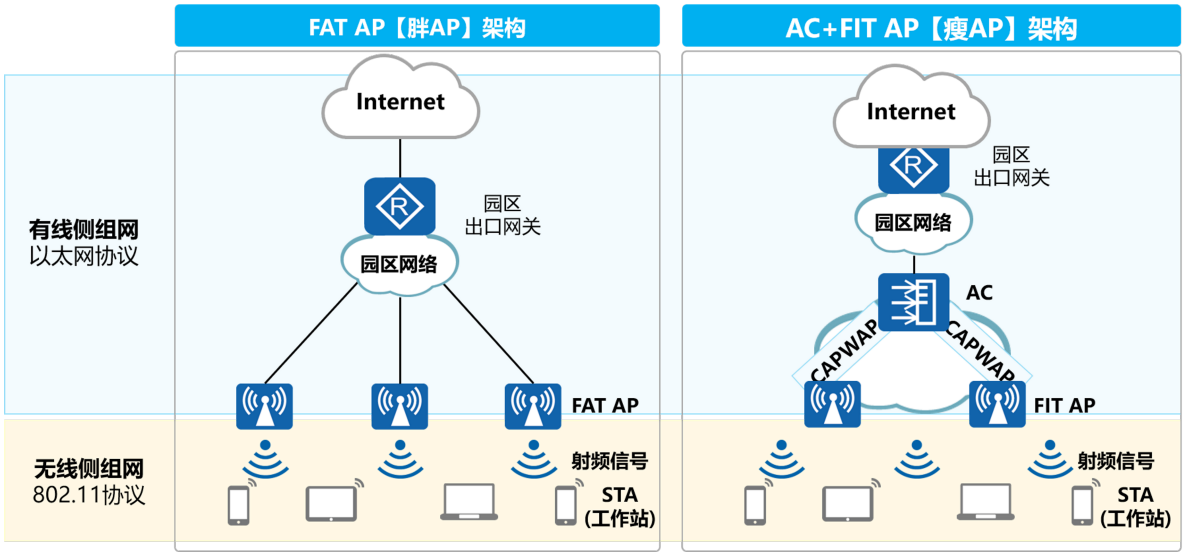
四、Wi-Fi在办公场景的发展趋势



五、WLAN设备介绍



六、基本的WLAN组网架构



七、有线侧组网概念 — CAPWAP协议

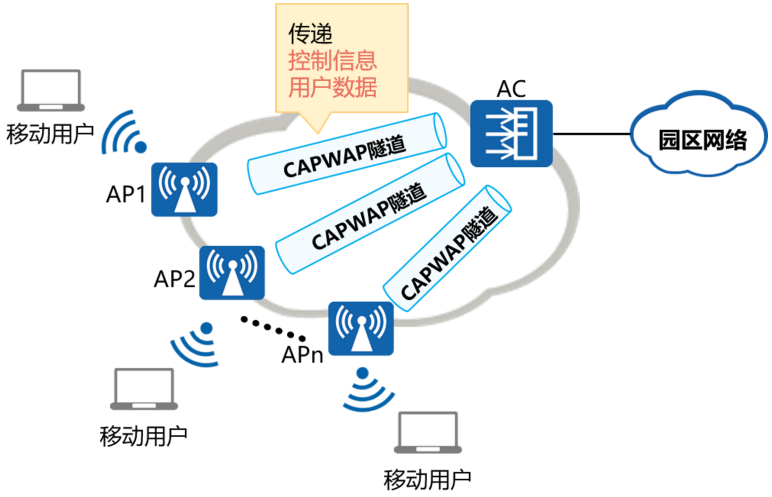
1、CAPWAP【Control And Provisioning of Wireless Access Points Protocol | 无线接入点控制和配置协议】：该协议定义了如何对AP进行管理、业务配置，即AC通过CAPWAP隧道来实现对AP的集中管理和控制

2、CAPWAP隧道的功能：

2.1、AP与AC间的状态维护

2.2、AC通过CAPWAP隧道对AP进行管理、业务配置下发

2.3、当采用隧道转发模式时，AP将STA发出的数据通过CAPWAP隧道实现与AC之间的交互



八、有线侧组网概念 — AP-AC组网方式

AP和AC间的组网分为：二层组网和三层组网

1、二层组网：AP与AC之间的网络为直连或者二层网络

由于二层组网比较简单，适用于简单临时的组网，能够进行比较快速的组网配置，但不适用于大型组网架构

2、三层组网：AP与AC之间的网络为三层网络

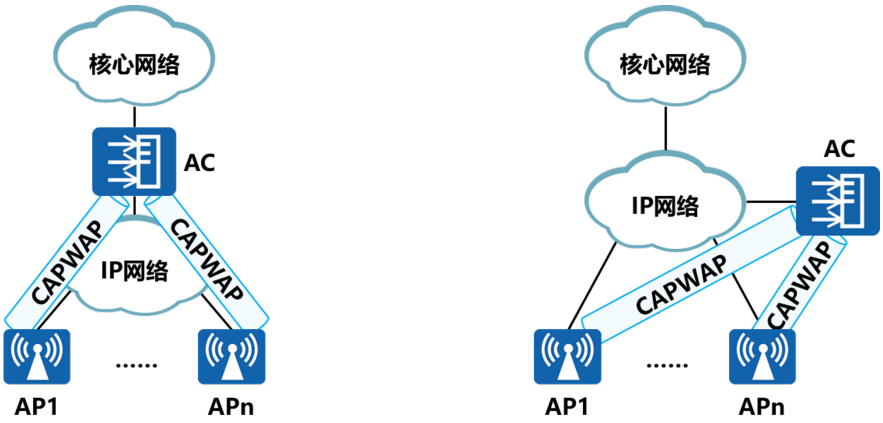
在实际组网中，一台AC可以连接几十甚至几百台AP，组网一般比较复杂，在大型组网中一般采用三层组网

九、有线侧组网概念 — AC连接方式

AC的连接方式分为：直连式组网和旁挂式组网

1、直连式组网可以认为AP、AC与上层网络串联在一起，所有数据必须通过AC到达上层网络。直连式组网中AC同时扮演AC和汇聚交换机的功能，AP的数据业务和管理业务都由AC集中转发和处理

2、旁挂式组网，AC旁挂在AP与上行网络的直连网络中，不再直接连接AP。旁挂式组网，AC旁挂在AP与上行网络的直连网络上，AP的业务数据可以不经AC而直接到达上行网络



十、无线侧组网概念 — 无线电磁波

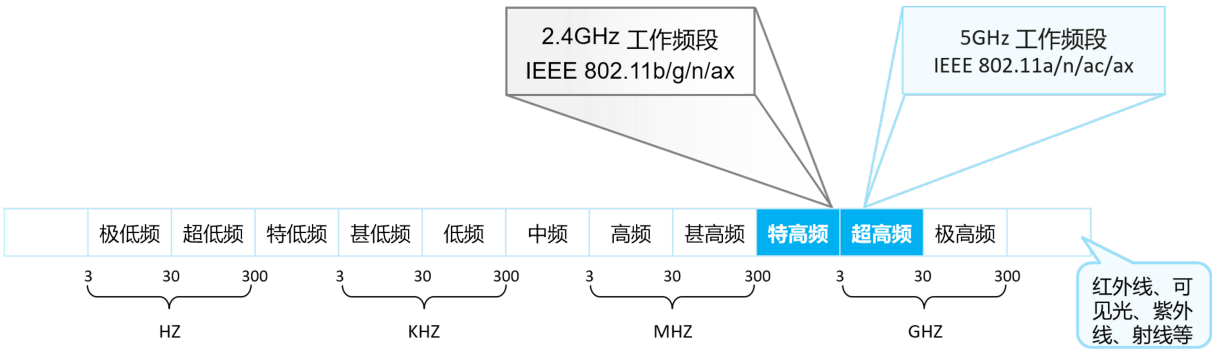
1、无线电磁波是频率介于3赫兹和约300G赫兹之间的电磁波，也叫作射频电波，或简称射频、射电。无线电技术将声音讯号或其他信号经过转换，利用无线电磁波传播

2、WLAN技术就是通过无线电磁波在空间中传输信息。当前我们使用的频段是：

2.1、2.4GHz频段【2.4GHz — 2.4835GHz】

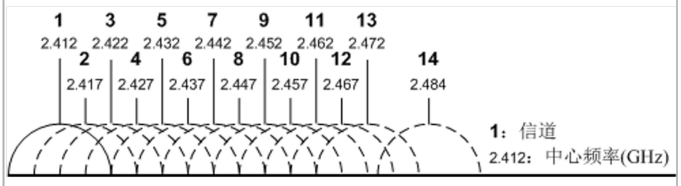
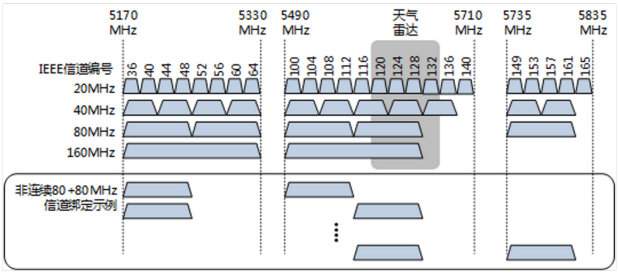
2.2、5GHz频段【5.15GHz — 5.35GHz | 5.725GHz — 5.85GHz】

3、无限电磁波频谱：



十一、无线侧组网概念 — 无线信道

信道是传输信息的通道，无线信道就是空间中的无线电磁波。无线电磁波无处不在，如果随意使用频谱资源，那将带来无穷无尽的干扰问题，所以无线通信协议除了要定义出允许使用的频段，还要精确划分出频率范围，每个频率范围就是信道

2.4GHz频段	5GHz频段
 • 2.4GHz频段被划分为14个有重叠的、频率宽度是20MHz的信道；其中包含重叠信道和非重叠信道 ▫ 重叠信道：在一个空间内同时存在重叠信道，则会产生干扰问题 ▫ 非重叠信道：在一个空间内可以同时存在非重叠信道，不会产生干扰问题	 • 对于5G频段，支持更宽频谱，频率资源更为丰富，AP不仅支持20MHz带宽的信道，还支持40MHz、80MHz及更大带宽的信道

十二、无线侧组网概念 — BSS | SSID | BSSID

1、基本服务集BSS【Basic Service Set】：

1.1、一个AP所覆盖的范围

1.2、在一个BSS的服务区域内，STA可以相互通信

2、基本服务集标识符BSSID【Basic Service Set Identifier】：是无线网络的一个身份标识，用AP的MAC地址表示。

3、服务集标识符SSID【Service Set Identifier】：

3.1、是无线网络的一个身份标识，用字符串表示

3.2、为了便于用户辨识不同的无线网络，用SSID代替BSSID

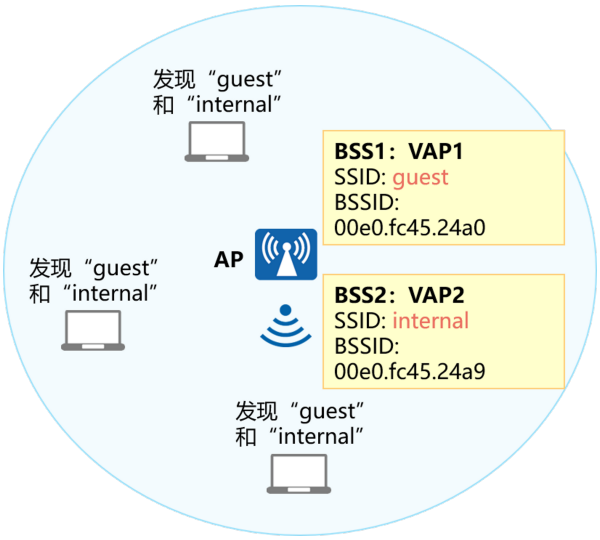
十三、无线侧组网概念 — VAP

1、早期的AP只支持1个BSS，如果要在同一空间内部署多个BSS，则需要安放多个AP，这不但增加了成本，还占用了信道资源。为了改善这种状况，现在的AP通常支持创建出多个虚拟AP【Virtual Access Point | VAP】

2、虚拟接入点VAP：

2.1、VAP就是在一个物理实体AP上虚拟出的多个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

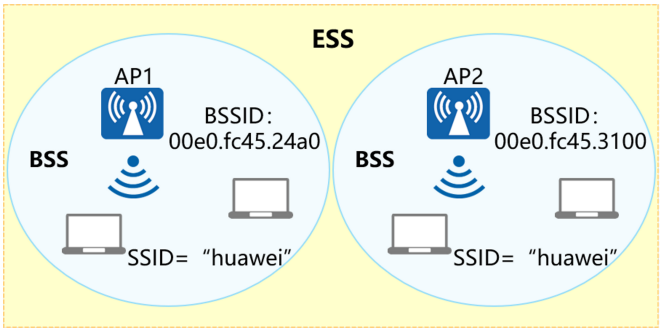
2.2、每个VAP对应1个BSS。这样1个AP，就可以提供多个BSS，可以再为这些BSS，设置不同的SSID



十四、无线侧组网概念 — ESS

1、为了满足实际业务的需求，需要对BSS的覆盖范围进行扩展。同时用户从一个BSS移动到另一个BSS时，不能感知到SSID的变化，则可以通过扩展服务集ESS实现

2、扩展服务集ESS【Extend Service Set】：由多个使用相同SSID的BSS组成，是采用相同的SSID的多个BSS组成的更大规模的虚拟BSS



十五、WLAN工作流程概述

1、AP上线：AP获取IP地址并发现AC，与AC建立连接

FIT AP需完成上线过程，AC才能实现对AP的集中管理和控制，以及业务下发。AP的上线过程包括如下步骤：

1.1、AP获取IP地址

AP获取IP地址的方式包括以下：

a、静态方式：登录到AP设备上手工配置IP地址

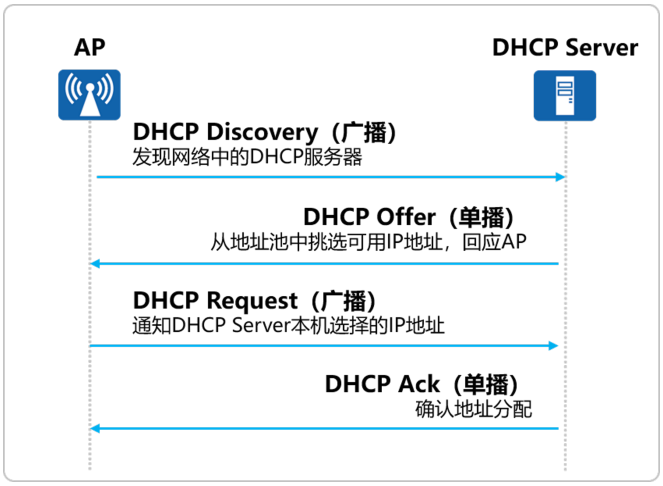
b、DHCP方式：通过配置DHCP服务器，使AP作为DHCP客户端向DHCP服务器请求IP地址

注：典型方案：

部署专门的DHCP Server为AP分配IP地址

使用AC的DHCP服务为AP分配IP地址

使用网络中的设备，例如核心交换机为AP分配IP地址



1.2、AP发现AC并与之建立CAPWAP隧道

Step 1：Discovery阶段【AP发现AC阶段】

AP通过发送Discovery Request报文，找到可用的AC

AP发现AC有两种方式：

a、静态方式：AP上预先配置AC的静态IP地址列表

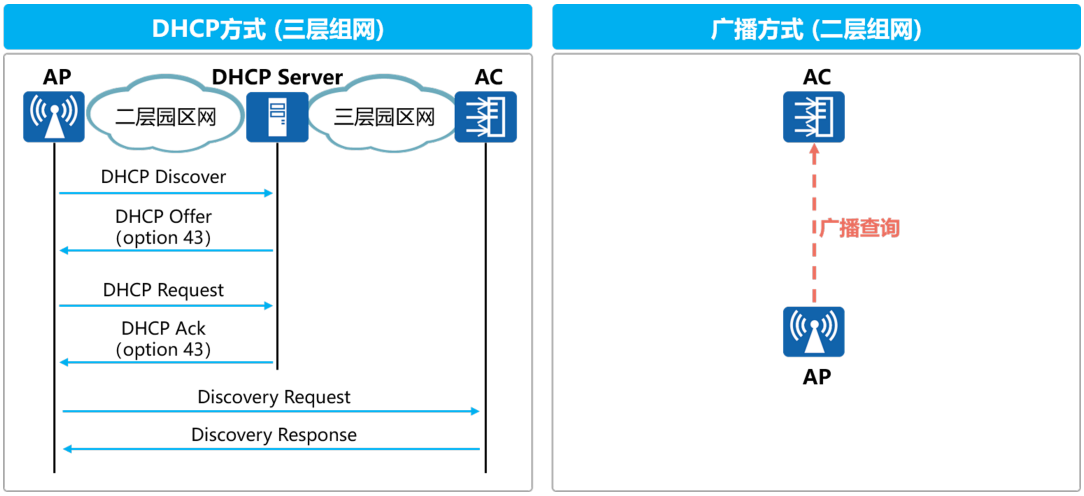
b、动态方式：DHCP方式、DNS方式和广播方式

Step 2：建立CAPWAP隧道阶段

AP与AC关联，完成CAPWAP隧道建立；包括数据隧道和控制隧道：

数据隧道：AP接收的业务数据报文经过CAPWAP数据隧道集中到AC上转发

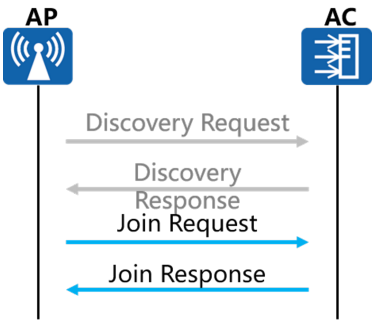
控制隧道：通过CAPWAP控制隧道实现AP与AC之间的管理报文的交互



1.3、AP接入控制

AP发现AC后，会发送Join Request报文。AC收到后会判断是否允许该AP接入，并响应Join Response报文

AC上支持三种对AP的认证方式：MAC认证、序列号【SN】认证和不认证



1.4、AP版本升级【可选项】

1、AP根据收到的Join Response报文中的参数判断当前的系统软件版本是否与AC上指定的一致。如果不一致，则AP通过发送Image Data Request报文请求软件版本，然后进行版本升级，升级方式包括AC模式、FTP模式和SFTP模式

2、AP在软件版本更新完成后重新启动，重复进行前面三个步骤

1.5、CAPWAP隧道维持

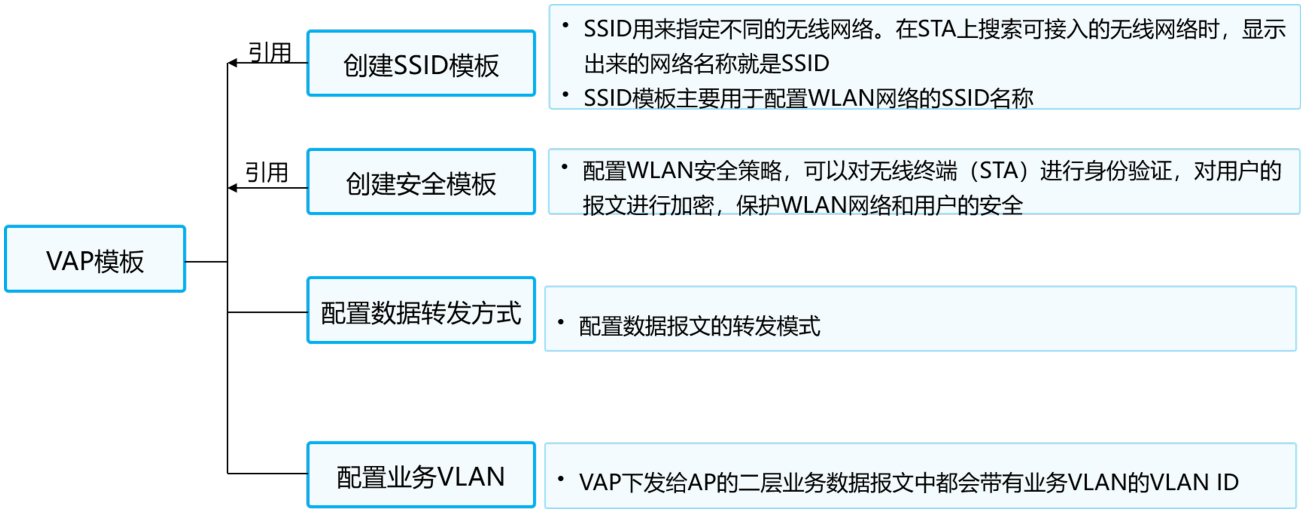
1.5.1、数据隧道维持：AP与AC之间交互Keepalive报文来检测数据隧道的连通状态

1.5.2、控制隧道维持：AP与AC交互Echo报文来检测控制隧道的连通状态

2、WLAN业务配置下发：AC将WLAN业务配置下发到AP生效

2.1、为了方便用户配置和维护WLAN的各个功能，针对WLAN的不同功能和特性设计了各种类型的模板，这些模板统称为WLAN模板

2.2、VAP模板



3、STA接入：STA搜索到AP发射的SSID并连接、上线，接入网络

3.1、扫描阶段

STA可以通过主动扫描，定期搜索周围的无线网络，获取到周围的无线网络信息

根据Probe Request帧【探测请求帧】是否携带SSID，可以将主动扫描分为两种：

3.1.1、携带有指定SSID的主动扫描方式：客户端发送携带有指定SSID的Probe Request：STA依次在每个信道发出Probe Request帧，寻找与STA有相同SSID的AP，只有能够提供指定SSID无线服务的AP接收到该探测请求后才回复探查响应

3.1.2、携带空SSID的主动扫描方式：客户端发送广播Probe Request，客户端会定期地在其支持的信道列表中，发送Probe Request帧扫描无线网络。当AP收到Probe Request帧后，会回应Probe Response帧通告可以提供的无线网络信息

3.2、链路认证阶段 — 无线接入安全协议

3.2.1、WLAN技术是以无线射频信号作为业务数据的传输介质，这种开放的信道使攻击者很容易对无线信道中传输的业务数据进行窃听和篡改。因此，安全性成为阻碍WLAN技术发展的最重要因素

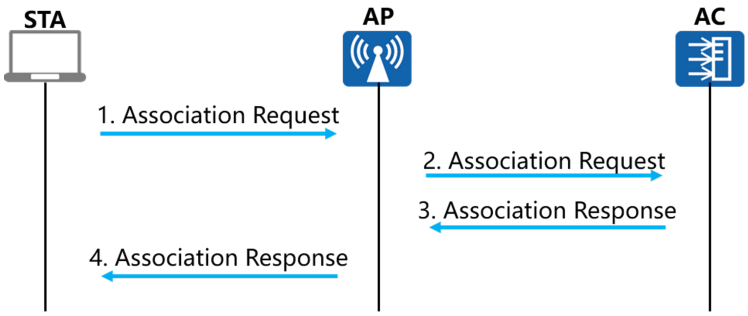
3.2.2、常用安全策略：

安全策略	链路认证方式	接入认证方式	数据加密方式	说明
WEP	Open	不涉及	不加密或WEP加密	不安全的安全策略
	Shared-key Authentication	不涉及	WEP加密	不安全的安全策略
WPA/ WPA2-802.1X	Open	802.1X（EAP）	TKIP或CCMP	安全性高的安全策略，适用于大型企业
WPA/ WPA2-PSK	Open	PSK	TKIP或CCMP	安全性高的安全策略，适用于中小型企业或家庭用户

3.3、关联阶段

3.3.1、完成链路认证后，STA会继续发起链路服务协商，具体的协商通过Association报文实现

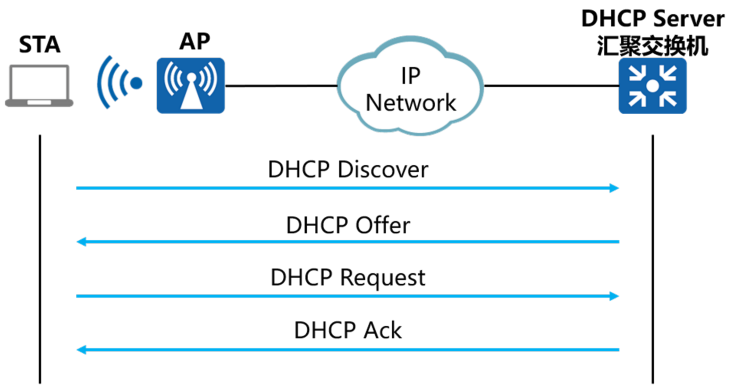
3.3.2、终端关联过程实质上就是链路服务协商的过程，协商内容包括：支持的速率、信道等



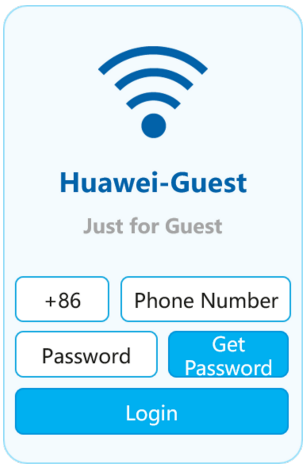
3.4、接入认证阶段

3.4.1、接入认证即对用户进行区分，并在用户访问网络之前限制其访问权限。相对于链路认证，接入认证安全性更高
3.4.2、主要包含：PSK认证和802.1X认证

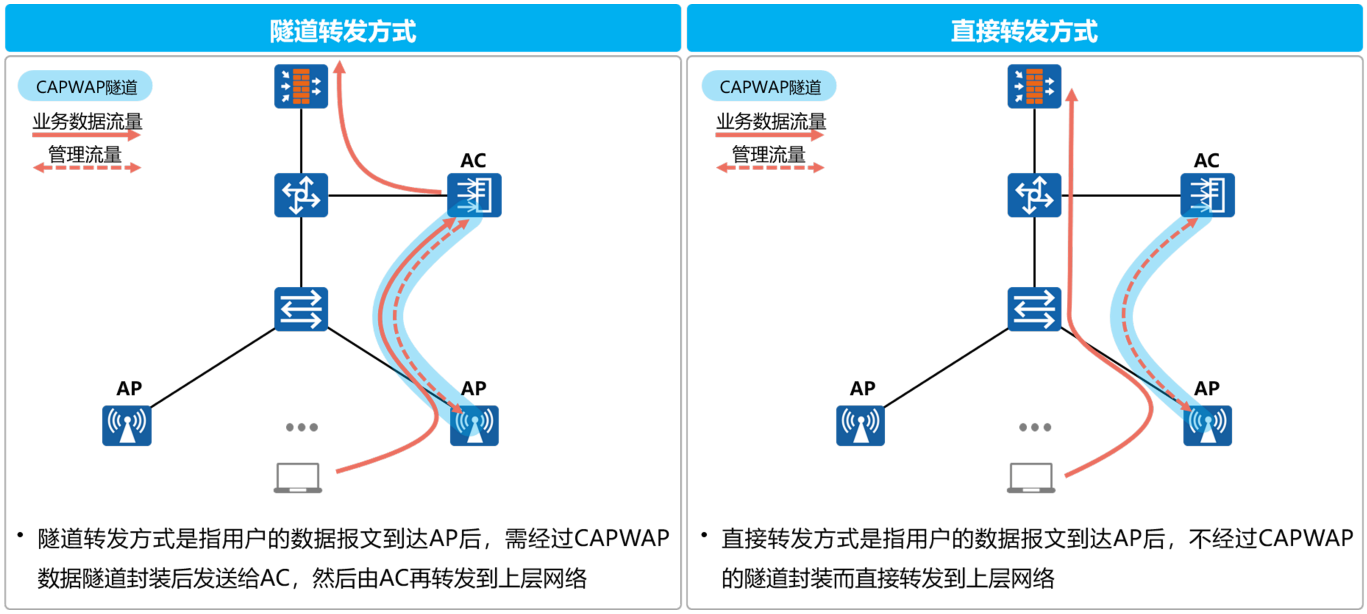
3.5、DHCP阶段 — STA地址分配
3.5.1、STA获取到自身的IP地址，是STA正常上线的前提条件
3.5.2、若STA是通过DHCP方式获取IP地址，可以用AC设备或汇聚交换机作为DHCP服务器为STA分配IP地址。一般情况下使用汇聚交换机作为DHCP服务器



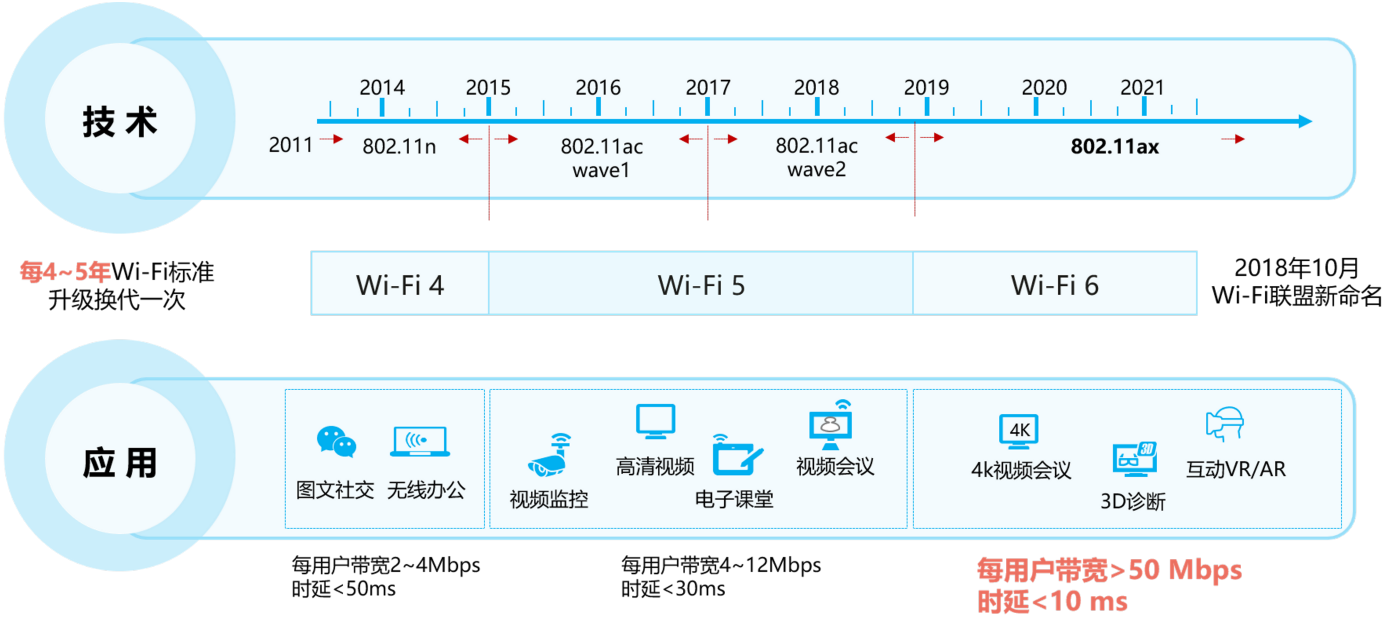
3.6、用户认证阶段
3.6.1、用户认证是一种【端到端】的安全结构，包括：802.1X认证、MAC认证和Portal认证
3.6.2、Portal认证：也称Web认证，一般将Portal认证网站称为门户网站，用户上网时，必须在门户网站进行认证。只有认证通过后才可以使用网络资源



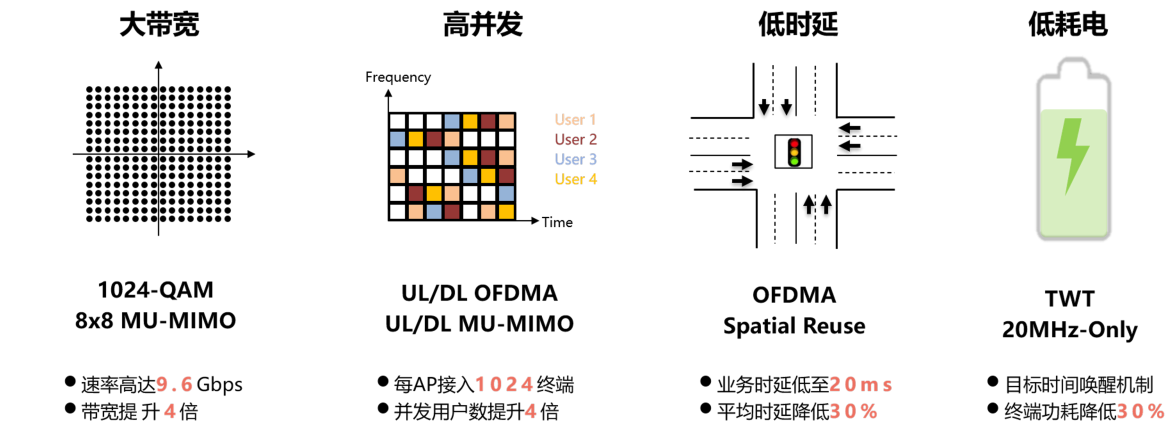
4、WLAN业务数据转发：WLAN网络开始转发业务数据
4.1、CAPWAP中的数据包括控制报文【管理报文】和数据报文
4.2、控制报文是通过CAPWAP的控制隧道转发的；
4.3、用户的数据报文分为隧道转发【又称为“集中转发”】方式和直接转发【又称为“本地转发”】方式



十六、双轮驱动：技术与应用发展助推Wi-Fi 6时代到来



十七、Wi-Fi 6 Vs Wi-Fi 5



十八、WLAN【Wireless Local Area Network】的配置

详细配置见实验手册