

网络构建与运维管理

第2章：越来越重要的无线局域网

阮晓龙

13938213680 / rxl@hactcm.edu.cn
<http://ethernet.book.51xueweb.cn>

河南中医学院管理信息工程学科
河南中医学院网络信息中心

2015.9

本章主要内容

- 无线局域网概述
- 无线局域网标准
- 接入认证
- 无线通信加密
- 案例：家庭无线局域网
- 案例：无线企业网



1.无线局域网概述

1.1无线局域网

- 无线局域网（WLAN）是计算机与无线通信技术相结合的产物。
 - WLAN是无线形式的局域网，即利用射频（RF）技术来取代传统的双绞线缆，以无线的方式来实现各端点间的数据传输。



1.无线局域网概述

1.2 无线局域网特点

- 无线局域网与生俱来的很多优越性决定了它的迅速崛起。与有线网络相比，无线局域网具有以下特点：
 - 安装便捷
 - 使用灵活
 - 易于扩展
 - 经济节约
 - 安全保密

1.无线局域网概述

1.3 无线局域网组成结构

- 无线局域网的组成，由站（STA）、无线介质（WM）、基站（BS）或接入点（AP）和分布式系统（DS）等几部分组成。
- 站
 - 站又称点、主机和终端，是无线局域网的最基本组成单元，实际上无线局域网的通信就是站间的数据传输。站在无线局域网中通常用作客户端，它是具有无线网络接口的计算设备，包括终端用户设备、无线网络接口和网络软件三部分。
 - 无线局域网中的站是可移动的，因此又可称为移动主机或移动终端。根据移动性又可分为固定站、半移动站和移动站。

1.无线局域网概述

1.3 无线局域网组成结构

□ 无线介质

无线介质是站与站之间、站与接入点之间通信的传输介质。

□ 无线接入点AP



TP-LINK TL-AP302C-PoE

1.无线局域网概述

1.3 无线局域网组成结构

- 无线接入点类似蜂窝结构中的基站，是无线局域网重要组成单元。它通常处于基本服务区（BSA）的中心，固定不动。
- 基本功能：
 - 作为接入点，完成其他非AP站对分布式系统的接入访问和同一基本服务区（BSS）中的不同站间通信连接。
 - 作为无线网络和分布式系统的桥接点完成无线局域网与分布式系统间的桥接功能。
 - 作为BSS（Basic Service Set）的控制中心完成对其他非AP站的控制和管理。

1.无线局域网概述

1.3 无线局域网组成结构

- 无线接入点是具有无线网络接口的网络设备，它主要包括以下几部分：
 - 与分布式系统的接口（至少一个）。
 - 无线网络接口（至少一个）和相关软件。
 - 桥接软件、接入控制软件、管理软件等AP软件和网络软件。
- 无线接入点也可作为普通站使用，称为AP Client。

1.无线局域网概述

1.3 无线局域网组成结构

□ 分布式系统DS

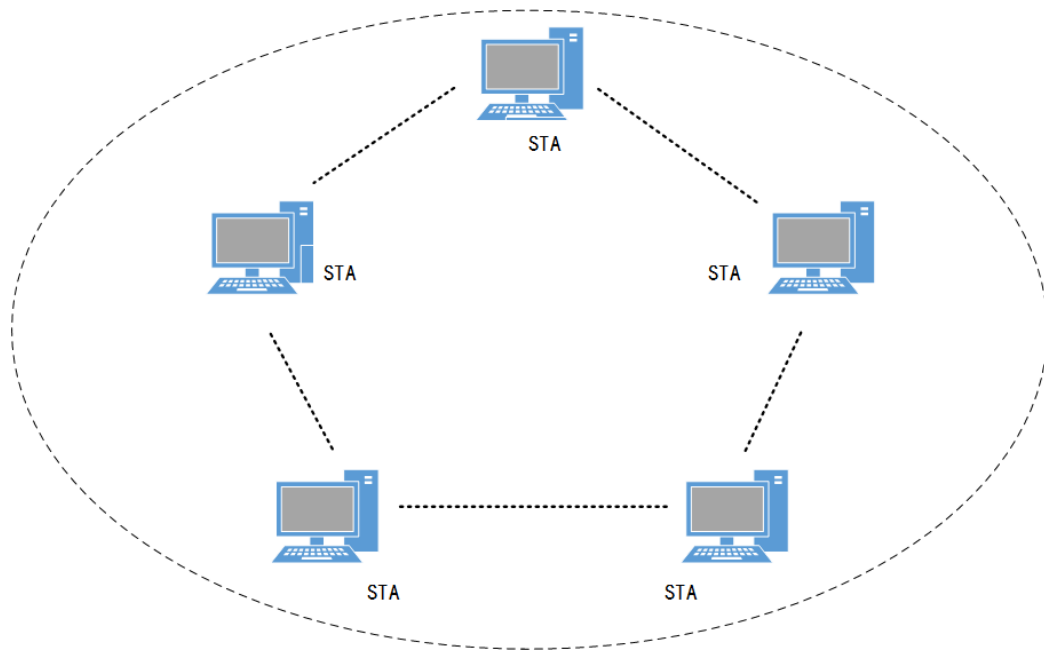
- 为了覆盖更大的区域，需要把多个BSA通过分布式系统连接起来，形成一个扩展业务区（ESA），而通过DS互相连接的属于同一个ESA的所有主机组成一个扩展业务组（ESS）。
- 分布式系统是用来连接不同BSA的通信信道，称为**分布式系统信道（DSM）**。DSM可以是有线信道，也可以是频段多变的无线信道。在多数情况下，有线DS系统与骨干网都采用有线局域网，而无线分布式系统（WDS）可通过AP间的无线通信（通常为无线网桥）取代有线电缆来实现不同BSS连接。

1.无线局域网概述

1.4 无线局域网拓扑结构

□ 点对点模式Ad-hoc/对等模式

- 无中心拓扑结构，由无线工作站组成，用于一台无线工作站和另外一台或多台无线工作站的直接通讯，该网络无法接入到有线网络中，只能独立使用。网络内无需AP，安全由各个客户端自行维护。
- 点对点模式中的一个节点必须能同时“看”到网络中的其他节点，否则就认为网络中断，因此对等网络只能用于少数用户的组网环境。



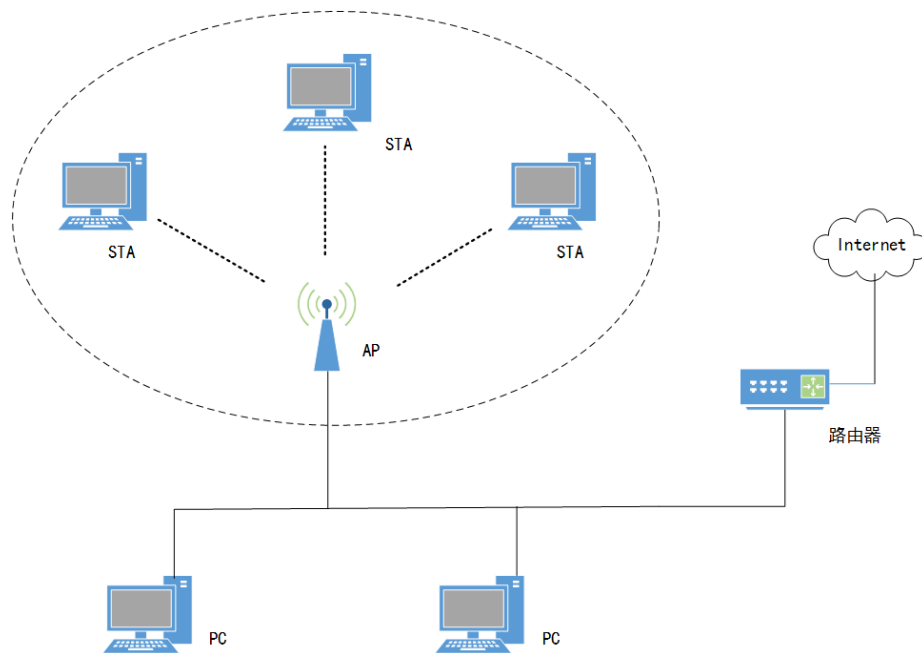
点对点模式

1.无线局域网概述

1.4 无线局域网拓扑结构

□ 基础架构模式

- 基础架构模式由无线接入点AP、无线工作站STA以及分布式系统DSS构成，覆盖区域称基本服务区BSS。无线接入点AP用于在无线工作站STA和有线网络之间接收、缓存和转发数据，所有无线通讯都经过AP完成。
- AP通常能覆盖几十至几百用户，覆盖半径达上百米。AP可连接有线网络，实现无线网络和有线网络的互联。



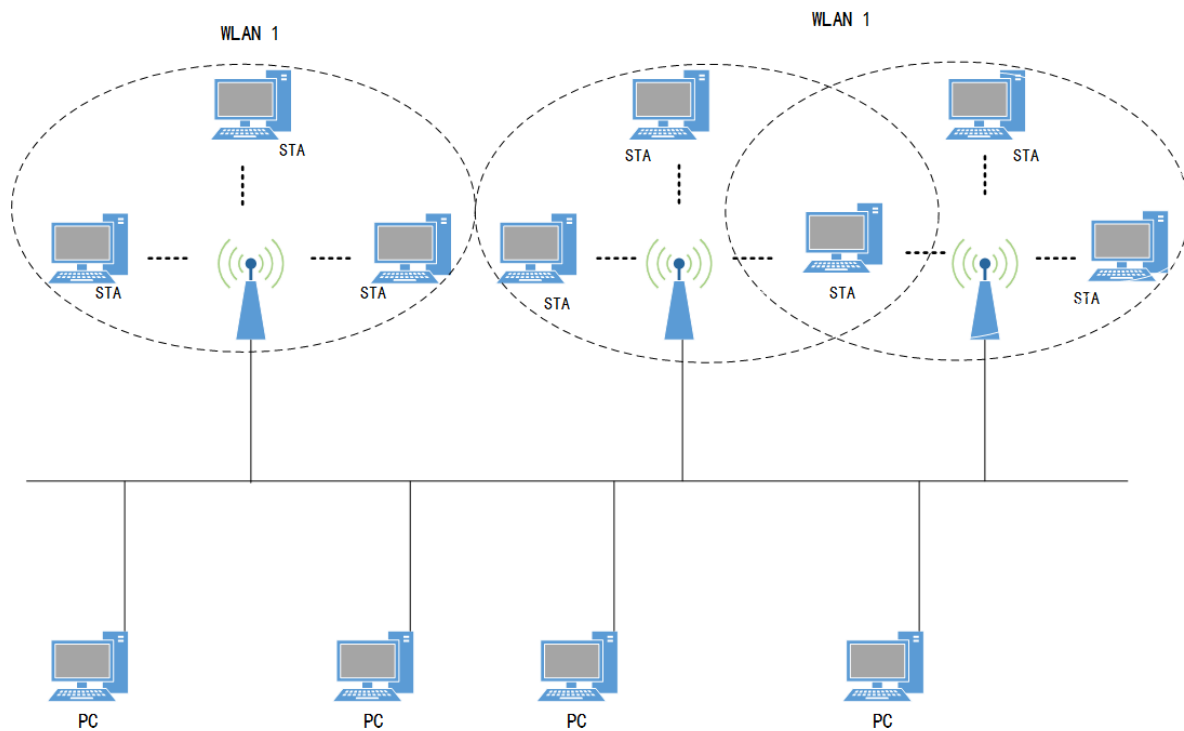
基础架构模式

1.无线局域网概述

1.4 无线局域网拓扑结构

□ 多AP模式

- 多AP模式指由多个AP以及连接它们的分布式系统DSS组成的基础架构模式网络，也称为扩展服务区ESS。
- 扩展服务区内的每个AP都是一个独立的无线网络基本服务区BSS，所有AP共享同一个扩展服务区标示符ESSID。
- 多AP模式也称为“多蜂窝结构”。各个蜂窝之间建议由15%的重叠范围，便于无线工作站的漫游，漫游时必须进行不同AP接入点之间的切换。切换可以通过交换机以集中的方式控制，也可以通过移动节点、监测节点的信号强度来控制（非集中控制方式）。



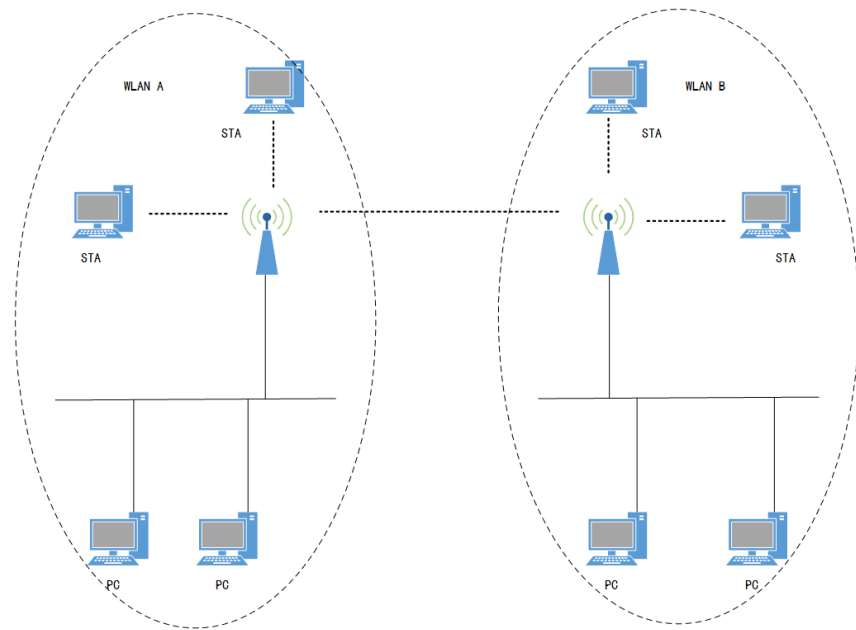
多AP模式

1.无线局域网概述

1.4 无线局域网拓扑结构

□ 无线网桥模式

- 利用一对无线网桥连接两个有线或者无线局域网网段。

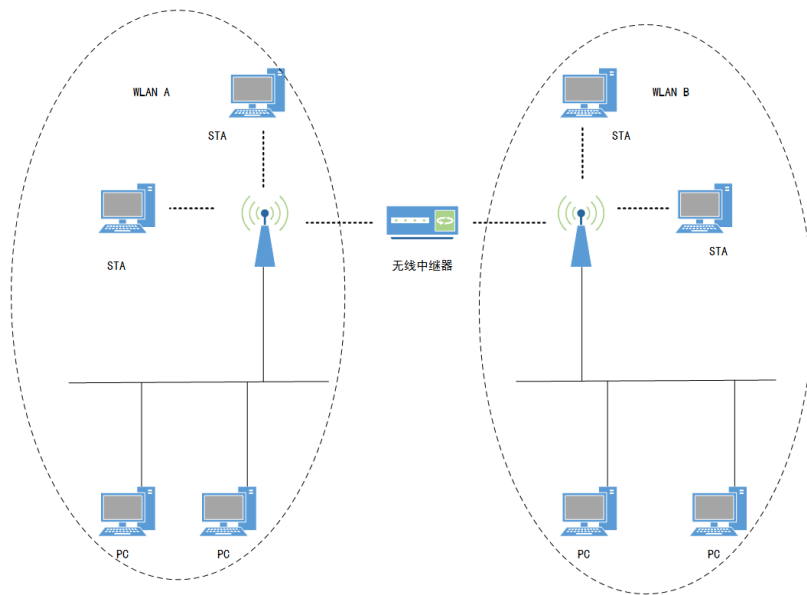


1.无线局域网概述

1.4 无线局域网拓扑结构

□ 无线中继器模式

- 无线中继器用来在通讯路径中间转发数据，延伸系统的覆盖范围。



1.无线局域网概述

1.4 无线局域网拓扑结构

□ 客户端模式

- AP Client客户端模式，也俗称“主从模式”，在此模式下工作的AP会被主AP（中心AP）看做是一台无线客户端，其地位就和无线网卡等同。

1.无线局域网概述

1.5 无线局域网服务

- 与WLAN体系结构和工作原理密切相关的服务主要有两种类型：
STA服务（SS）和分布式系统服务（DSS），这两种服务均在MAC层使用。

1.无线局域网概述

1.5 无线局域网服务

- IEEE 802.11标准中定义了九种服务，三种用来移动数据，六种是管理操作。
 - STA服务 (SS)

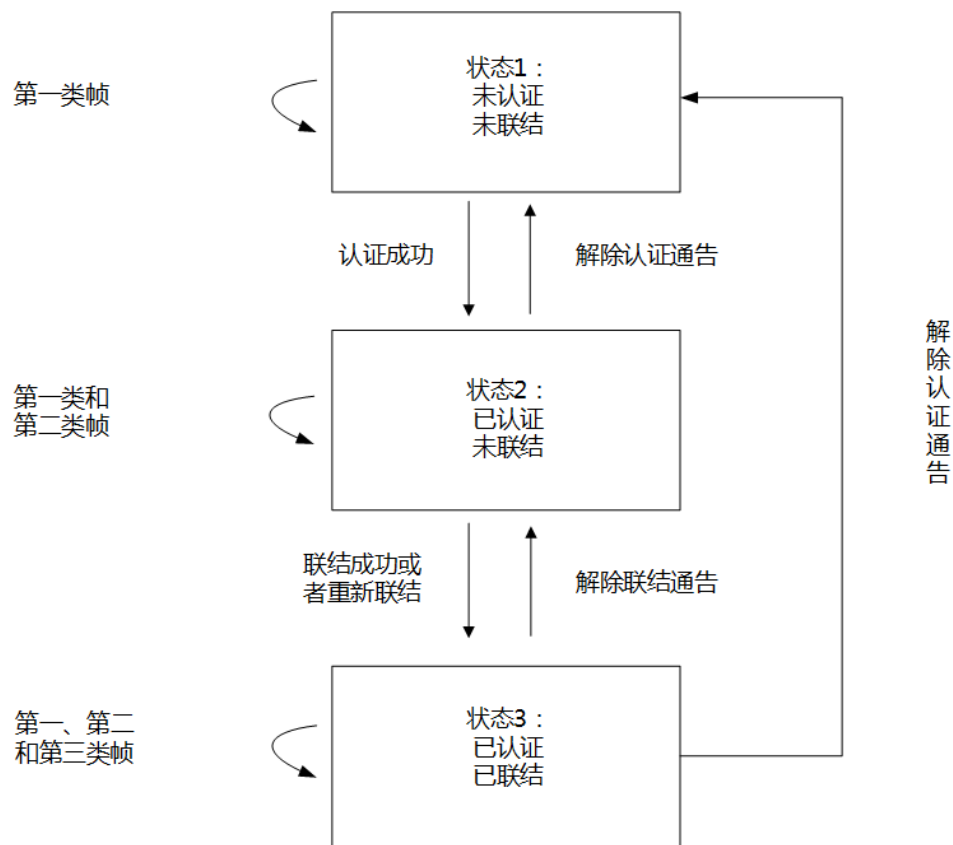
由STA提供的服务被称为STA服务，它存在于每个STA和AP中。
包括：认证、解除认证、保密。
 - 分布式系统服务 (DSS)

由DS提供的服务被称为分布式系统服务。在WLAN中，DSS通常由AP提供。
包括：联结、重新联结、解除联结、分布、集成。

1.无线局域网概述

1.5 无线局域网服务

- IEEE 802.11标准中定义了九种服务，三种用来移动数据，六种是管理操作。
 - 服务之间的关系
 - 对于通过WM进行直接通信的STA均有认证状态（值为未被认证和已认证）和联结状态（值为未联结和已联结）两个状态变量。这两个变量为每个远端STA建立了三种本地状态。
 - 状态1：初始启动状态，未认证，未联结。
 - 状态2：已认证，未联结。
 - 状态3：已认证，已联结。



状态变量与业务之间的关系

2.无线局域网标准

2.1 802.11a

- IEEE 802.11a是美国电气和电子工程师协会（IEEE）为了改进其最初推出的无线标准IEEE 802.11而推出的无线局域网络协议标准，是IEEE 802.11的有益补充。
- IEEE 802.11a规范主要特性：
 - 工作频段
 - IEEE 802.11a规范工作频段为商业的5GHz频段（不是采用IEEE 802.11b规范中的2.4GHz免费频段，所以不与IEEE 802.11b设备兼容），室内有效传输距离35m，室外有效传输距离120m。
 - 传输速率
 - IEEE 802.11a规范的最高数据传输速率为54Mb/s，根据实际网络环境，还可调整为6Mb/s、9Mb/s、12Mb/s、18Mb/s、36Mb/s、48Mb/s。

2.无线局域网标准

2.1 802.11a

□ 信道划分

- IEEE 802.11a规范的每个信道的带宽有两种选择：20MHz或40MHz，如果为20MHz带宽，则共有24个不相互重叠的信道，如果是40MHz带宽，则共有12个不相互重叠的信道。

表 2-01 IEEE 802.11a 规范中的信道划分

信道 ID	信道中心频率/MHz	适用环境
36	5180	室内
40	5200	室内
44	5220	室内
48	5240	室内
52	5260	室内或室外
56	5280	室内或室外
60	5300	室内或室外
64	5320	室内或室外
100	5500	室内或室外
104	5520	室内或室外
108	5540	室内或室外
112	5560	室内或室外
116	5580	室内或室外
120	5600	室内或室外
124	5620	室内或室外
128	5640	室内或室外
132	5660	室内或室外
136	5680	室内或室外
140	5700	室内或室外
149	5745	主要用于室外
153	5765	主要用于室外
157	5785	主要用于室外
161	5805	主要用于室外
165	5825	主要用于室外

2.无线局域网标准

2.1 802.11a

□ 调制方法

- IEEE 802.11a规范采用52个OFDM（正交频分复用）调制扩频技术，可提高信道的利用率。在52个OFDM中的52个载波中，48个用于传输数据，4个是引示载波（pilot carrier，即载波里面没有携带任何数据），每一个带宽为0.3125MHz（20MHz/64），可以应用BPSK（二相移相键控）、QPSK（四相移相键控）、16-QAM或者64-QAM调制技术。
- OFDM技术将信道分成若干正交子信道，将高速数据信号转换成并行的低速子数据流，再调制到每个子信道上进行传输。正交信号可以通过在接收端采用相关技术来分开，这样可以减少子信道之间的相互干扰。

2.无线局域网标准

2.1 802.11a

□ 主要安全技术

- IEEE 802.11a规范在安全方面一开始主要使用WEP加密技术和SSID。
- 2003年以后生产的IEEE 802.11a规范的WLAN一般还支持WPA和IEEE 802.1x安全技术，但这通常是在同时支持IEEE 802.11a和IEEE 802.11g两种规范的设备中提供，单独的IEEE 802.11a设备不支持。

2.无线局域网标准

2.2 802.11b

- 在WLAN的发展史中，影响最大的WLAN标准是1999年9月正式发布的IEEE 802.11b。
- 该规范的主要特性：
 - 工作频段
 - IEEE 802.11b规范工作频段为免费的2.4GHz频段，室内有效传输距离为35m，室外有效传输距离为140m。
 - 传输速率
 - IEEE 802.11b规范最高传输速率为11Mb/s，可根据实际网络环境调整为1Mb/s、2Mb/s和5.5Mb/s。

2.无线局域网标准

2.2 802.11b

□ 调制方法

- IEEE 802.11b规范可根据不同接入速率采用不同的调制技术：
 - 传输速率为1Mb/s和2Mb/s时，采用原来IEEE 802.11规范中的DSSS（直接序列扩展）、DBPSK（差分二相位键控）、DQPSK（差分四相位键控）等数字调制方法；
 - 传输速率为5.5Mb/s和11Mb/s时，采用CCK（互补编码键控）调制方法。

2.无线局域网标准

2.2 802.11b

□ 信道划分

- IEEE 802.11b规范全球使用的是同一无线电模式，共有11个信道，每个信道带宽为22MHz，但相邻信道间只有5MHz带宽不重叠（也就是会重叠17MHz带宽）。
- 每两个相邻信道都会有大部分的频段重叠，所以在IEEE 802.11b规范的整个频段中，真正完全不重叠的信道只有3个。

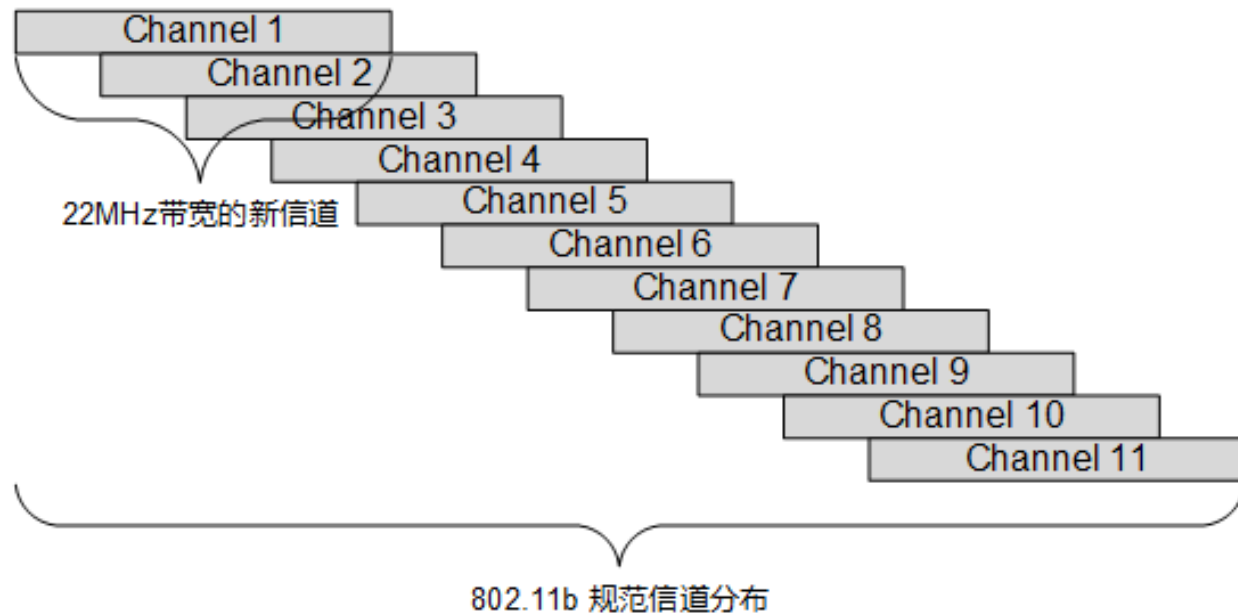


表 2-02 IEEE 802.11b 和 IEEE 802.11g 规范中的信道划分

信道 ID	IEEE802.11b 信道中心频率 (单位: GHz)	IEEE 802.11g 信道中心频率 (单位: GHz)
1	2.412	2.412
2	2.417	2.417
3	2.422	2.422
4	2.427	2.427
5	2.432	2.432
6	2.437	2.437
7	2.442	2.442
8	2.447	2.447
9	2.452	2.452
10	2.457 (法国仅允许使用的频道)	2.457 (法国仅允许使用的频道)
11	2.462 (法国仅允许使用的频道)	2.462 (法国仅允许使用的频道)
12	——	2.467 (法国仅允许使用的频道)
13	——	2.472 (法国仅允许使用的频道)

2.无线局域网标准

2.2 802.11b

□ 主要安全技术

- IEEE 802.11b规范主要采用的安全技术包括：
 - SSID（服务集标识符）和WEP（有线等效保密）链路加密。
 - 在2003年以后生产的IEEE 802.11b规范的WLAN一般还支持WPA和IEEE 802.1x安全技术，但这通常是在同时支持IEEE 802.11b和IEEE 802.11g两种规范的设备中提供，单独的IEEE 802.11b设备不支持。

2.无线局域网标准

2.2 802.11g

- 为了进一步提升IEEE 802.11b规范的最大速率，2003年6月IEEE推出802.11g规范。
- IEEE 802.11g规范的主要特性如下：
 - 工作频段

IEEE 802.11g规范工作频率为**免费的2.4GHz频段**，与IEEE 802.11b兼容，但不与IEEE 802.11a兼容。室内有效传输距离38m，室外有效传输距离140m。
 - 传输速率

IEEE 802.11g规范**最大传输速率为54Mb/s**，总带宽为20MHz。可根据实际网络环境调整为48Mb/s、36Mb/s、24Mb/s、18Mb/s、12Mb/s、19Mb/s、6Mb/s。

2.无线局域网标准

2.2 802.11g

■ 信道划分

IEEE 802.11g规范共划分了13个信道，IEEE 802.11g比IEEE 802.11b多两个可用信道，但完全不重叠的信道最多只有3个。

■ 调制方法

IEEE 802.11g规范同时采用了IEEE 802.11a标准中的OFDM与IEEE 802.11b中的DSSS、CCK等多种调制技术。

■ 主要安全技术

在安全性方面，IEEE 802.11g规范全面支持IEEE 802.11i标准中的WPA、WPA2、EAP（可扩展身份认证）AES（高级加密标准）加密，以及用于访问控制的IEEE802.1x标准。

2.无线局域网标准

2.2 802.11n

- IEEE 802.11n是2009年9月正式发布的规范，也是目前最主要应用的WLAN接入规范。其主要特性如下：

- 工作频段

IEEE 802.11n规范工作频段为2.4GHz和5GHz两个频段，所以可全面向下兼容以前发布的IEEE802.11b/a/g三个规范。

- 传输速率

IEEE 802.11n规范在标准带宽（20MHz）单倍MIMO上支持的速率有7.2Mb/s、14.4Mb/s、21.7Mb/s、28.9Mb/s、43.3Mb/s、57.8Mb/s、65Mb/s、72.2Mb/s。

使用标准带宽和4倍MIMO时，最高速率为300Mb/s。

使用2倍带宽（40MHz）和4倍MIMO时，最高速率为600Mb/s。

2.无线局域网标准

2.2 802.11n

□ 信道划分

- IEEE 802.11n规范共有15个不相互重叠的信道，其中在2.4GHz频段有3个不相互重叠的信道，在5GHz频段有12个不相互重叠的信道。
- 通过将两个相邻的20MHz带宽捆绑在一起组成一个40MHz通信带宽，在实际工作时可以作为两个20MHz的带宽使用，收发数据时既能以40MHz带宽工作，也能以单个20MHz带宽工作，可将速率提高一倍。

2.无线局域网标准

2.2 802.11n

□ 调制方法

- IEEE 802.11n规范采用IEEE 802.11g规范中相同的OFDM调制技术，只是选择的正交载波数更多。
- OFDM可将信道分成许多进行窄带调制信道和传输正交子信道，并使每个子信道上的信号带宽小于信道的相关带宽，用以减少各个载波之间的相互干扰，同时提高频谱的利用率。
- MIMO（多进多出）与OFDM技术的结合，就产生了MIMO OFDM技术，通过在OFDM传输系统中采用阵列天线实现空间分集，提高了信号质量，并增加多径的容限，使无线网络有效传输速率得到提升。

2.无线局域网标准

2.2 802.11n

□ 主要安全技术

- IEEE 802.11n规范与IEEE 802.11g规范所使用的安全技术类似，主要是IEEE 802.11i所引入的WPA、WPA2和AES加密，以及IEEE 802.1x访问控制技术。



真正3天线，性能更出众
3*3 MIMO架构，高规格3数据流并发

TL-WR886N采用高规格的3数据流并发、3*3MIMO架构，3个数据流通过3根天线同时进行收发，能够大幅提升无线性能，同时提高信号强度，增大覆盖范围，增强连接稳定性。



2.无线局域网标准

2.3 802.11ac

- IEEE 802.11ac是802.11无线局域网通信标准。
- 802.11ac作为IEEE无线技术的新标准，借鉴了802.11n的各种优点并进一步优化，除了高吞吐特点外，还提升了多项技术。
- 802.11ac标准在物理层上的变化：**更宽的通道带宽、更多的空间流、更高阶的调制。**

2.无线局域网标准

2.3 802.11ac

□ 更宽的通道带宽

- 802.11ac支持80MHz频宽，可选择使用连续的160MHz频带，或者不连续的80+80频带。
- 频带的提升带来了可用数据子载波的增加。80MHz可用的子载波数量达234个，而40MHz只有108个，这样80MHz就可以带来2.16倍的增速。
- 不足之处在于需要将相同的传输功率分隔到更多子载波上，从而造成信号覆盖范围有所减少。

2.无线局域网标准

2.3 802.11ac

□ 更多的空间流

- 802.11ac最多支持8路空间流，支持多个空间流是可选的，但空间流数量的增加与802.11ac多用户多进多出（MU-MIMO）的新功能结合最为有效。
- 802.11ac技术在单用户和多用户MIMO模式下，支持最多8路空间流、最多4个用户；并且在用户模式下，每个无线终端不超过4路空间流。

2.无线局域网标准

2.3 802.11ac

□ 更高阶的调制

- 802.11ac使用了正交频分复用（OFDM）技术来调制数据比特在无线介质上传输。802.11ac可视情况选用256QAM，256QAM增加了每个子载波的数据比特数量从6到8个，从而使吞吐量增加了33%，其中256QAM只适用于高信噪比的环境。

2.无线局域网标准

2.3 802.11ac

□ 802.11ac技术改进

- 选择5GHz频带、支持MIMO技术、增强载波侦听技术、增强报文聚合。
- 选择5GHz频带
 - 802.11ac性能大幅提升最重要的原因是采用了5GHz频段。
 - 蓝牙耳机、监视器、甚至微波炉等工作频率同样为2.4GHz频段，802.11b/g/n规范就不可避免的需要和这些设备争抢信道，使得传输速度慢且容易受到干扰。
 - 802.11ac工作在5GHz频段上，争用带宽的无线设备较少，速度和稳定性就更有保障。
 - 802.11ac标准具有向下兼容性，确保802.11ac设备可用于现有WiFi网络。

2.无线局域网标准

2.3 802.11ac

□ 支持MIMO技术

- MIMO技术要求系统使用多个发射和接收天线同时同频的发射和接收数据。**MIMO系统的重要特性**就是通过空分复用、发射分集技术以及波束成形技术来提高数据传输率。
- 空分复用是在接收端和发射端使用多副天线，充分利用空间传播中的多径分量，在同一频带上使用多个数据通道发射信号，从而使得容量随着天线数量的增加而增加。这种信道容量的增加不需要占用额外的带宽，也不需要消耗额外的发射功率，因此是**提高信道系统容量**的一种非常有效的手段。

2.无线局域网标准

2.3 802.11ac

□ 增强载波侦听技术

- 802.11ac标准应用许多MAC层增强技术来进一步加强高性能的射频和多用户多进多出（MU-MIMO）特性。在802.11ac中，由于80Mhz使用更多信道，因此需要提升RTS/CTS的机制来处理辅助信道上的通信冲突问题，改进后RTS/CTS同时支持“动态频宽”模式。
- 在MAC层，802.11n 设备依靠发送“请求发送/清除发送（RTS/CTS）”帧来宣告传输的意向。这些帧让附近的802.11a/g设备感知到信道正在使用中，从而避免冲突。

2.无线局域网标准

2.3 802.11ac

□ 增强报文聚合

- 802.11ac的基本MAC协议中，为了确保各个站都能公平地取得媒质的使用机会并尽量避免冲突，使用了一系列控制机制。
- 802.11ac引入了两种帧聚合的方法：MAC服务数据单元（MSDU）聚合和信息协议数据单元（MPDU）聚合。两种帧聚合方法降低了每个聚合帧传输时的单路射频前导码的开销。

2.无线局域网标准

2.3 802.11ac

□ 802.11规范对比

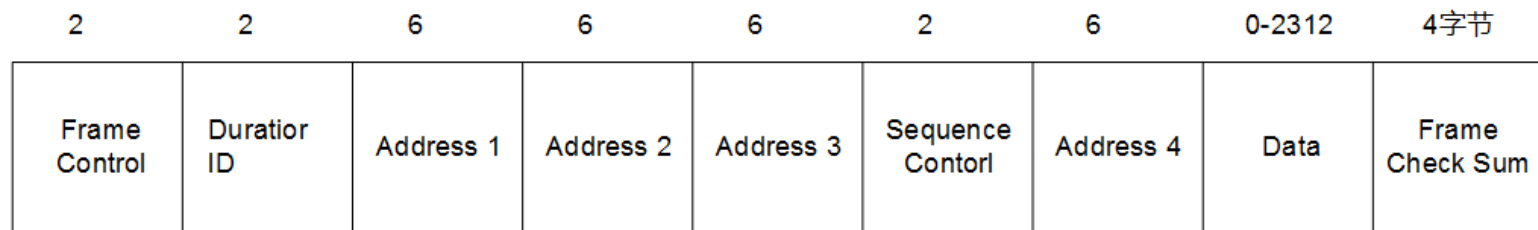
表 2-03 802.11 标准对比表

标准	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g	IEEE 802.11n	IEEE 802.11ac
发布时间	1999 年 9 月	1999 年 9 月	2003 年 6 月	2009 年 9 月	2012 年 2 月
工作频段	5GHz	2.4GHz	2.4GHz	2.4/5GHz	5GHz
非重叠信道数	12 或 24	3	3	15	8
最高接入速率	54Mb/s	11Mb/s	54Mb/s	600Mb/s	3.2Gb/s
频段	20MHz	20MHz	20MHz	20MHz/40MHz	20/40/80/160MHz
调制方式	OFDM	CCK/DSSS	CCK/DSSS/OFDM	4*4MIMO-OFDM/DSSS/CKK	8*8MIMO-OFDM/16~256QAM
兼容性	802.11a	802.11b	802.11b/g	802.11a/b/g/n	802.11a/b/g/n

2.无线局域网标准

2.4 WLAN MAC帧格式

- 在WLAN体系结构中，MAC子层虽然有分布式协调功能（DCF）和点协调功能（PCF）两种工作方式，但MAC子层帧结构是一致的。
- 具体结构图：



WLAN/RM中的MAC帧结构

2.无线局域网标准

2.4 WLAN MAC帧格式

□ Frame Control (FC, 帧控制) 字段

FC字段占2个字节，用于控制MAC子层帧信息和行为。在这个字段的2个字中又分为多位。

2	2	4	1	1	1	1	1	1	1	1位
Protocol Version	Type	Subtype	To DS	From DS	More Flag	Retry	Pwr Mgt	More Data	WEP	Order

FC字段结构

- Protocol Version: 协议版式本字段，占2位。表示IEEE 802.11规范版本。
- Type: 帧类型字段，占2位。帧类型包括管理、控制和数据三种类型。

2.无线局域网标准

2.4 WLAN MAC帧格式

▣ Subtype：帧子类型字段，占4位。帧子类型包括：

认证帧 (Authentication Frame)

解除认证帧 (Deauthentication Frame)

连接请求帧 (Association Request Frame)

连接响应帧 (Association Response Frame)

重新连接请求帧 (Reassociation Request Frame)

重新连接响应帧 (Reassociation Response Frame)

解除连接帧 (Disassociation Frame)

信标帧 (Beacon Frame)

Probe帧 (Probe Frame)

Probe请求帧 (Probe Request Frame)

2	2	4	1	1	1	1	1	1	1	1位
Protocol Version	Type	Subtype	To DS	From DS	More Flag	Retry	Pwr Mgt	More Data	WEP	Order

2.无线局域网标准

2.4 WLAN MAC帧格式

- To DS：到分布式系统的帧字段，占1位。当帧时发送给Distribution System (DS) 时，该值设置为1。
- From DS：来自分布式系统的帧字段。当帧是从DS处接收到时，该值设置为1。
- More Flag：更多分片字段，占1位。表示当前帧后面还有更多分段属于相同帧时，该帧设置为1，否则设为0。
- Retry：重传字段，占1位。如是重传帧则用1表示，否则用0表示。

2	2	4	1	1	1	1	1	1	1	1位
Protocol Version	Type	Subtype	To DS	From DS	More Flag	Retry	Pwr Mgt	More Data	WEP	Order

2.无线局域网标准

2.4 WLAN MAC帧格式

- Pwr Mgt: Power Management, 电源管理字段, 占1位。表示在帧传输后, 站点所采用的电源管理模式。1表示采用节能模式, 0表示活动模式。
- More Data: 更多数据字段, 占1位。1表示在AP缓存中还有从分布式系统到节能模式站点的帧, 0表示没有。
- WEP: 加密字段, 占1位。1表示采用WEP (Wired Equivalent Privacy) 算法对帧数据进行加密, 0表示不加密。
- Order: 顺序字段, 占1位。1表示按顺序发送帧或者分段, 0表示不按顺序发送。

2	2	4	1	1	1	1	1	1	1	1位
Protocol Version	Type	Subtype	To DS	From DS	More Flag	Retry	Pwr Mgt	More Data	WEP	Order

2.无线局域网标准

2.4 WLAN MAC帧格式

□ Duration/ID

- Duration/ID为持续时间字段，占2字节。
- 当第15位为0时，用于设置NAV（Network Allocation Vector，网络分配向量），NAV等于在当前传输中介质忙的时间（以毫秒计）长。这样所有站点就会监控接收到的帧，并更新NAV。
- 在没有冲突发生时，第15位为1，所有其他位为0。这样得出的NAV值为32768，所有站点会在无冲突期间更新NAV值，以免发生冲突。

2	2	6	6	6	2	6	0-2312	4字节
Frame Control	Duration ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Data	Frame Check Sum

2.无线局域网标准

2.4 WLAN MAC帧格式

- 在IEEE 802.11WLAN网络内，所有接收到RTS（请求发送）与CTS（清理后发送）信号的无线设备，都将采用**虚拟介质检测（VCS）机制设置NAV**，并使用在RTS和CTS中包含的Duration/ID字段信息来设置MAC参数。
- NAV指针打开时，设备将认为此时的物理介质正被其他设备所占有而停止发送与接收数据。NAV的值随着时间推移不断减小，在NAV值减到零之前，主机不会发起传输尝试。
- VCS机制设置使其他主机预先知道信道正在进行的传输情况，从而有效提高了数据帧成功传输的概率。

2.无线局域网标准

2.4 WLAN MAC帧格式

□ Address

- Address为地址列表字段，包括上图中的地址（Address 1、Address 2、Address 3、Address 4）字段，它们依次对应：接收者MAC地址、发送者MAC地址、源MAC地址和目标MAC地址。
- 每个地址字段占6字节（48位）。
- 这4个字段对于所有MAC帧来说并不是都需要的，是否需要取决于帧类型。

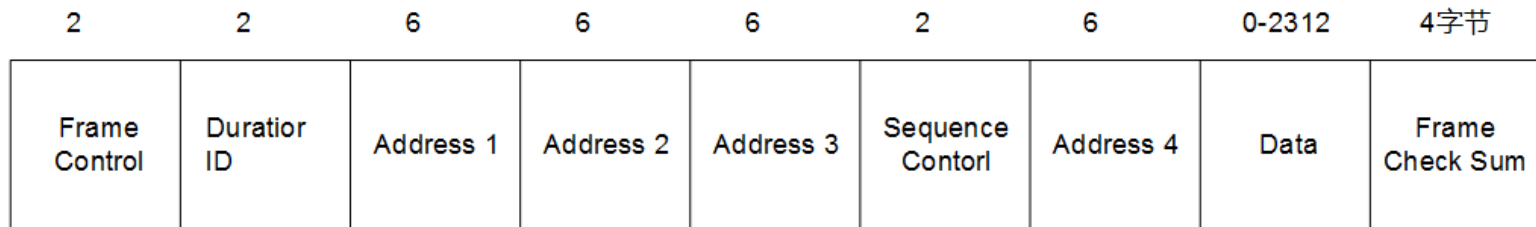
2	2	6	6	6	2	6	0-2312	4字节
Frame Control	Duration ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Data	Frame Check Sum

2.无线局域网标准

2.4 WLAN MAC帧格式

□ Sequence Control

- Sequence Control为序列控制字段，占2字节。
- 由分段号和序列号两部分组成，用于表示同一帧中不同分段的顺序，并用于识别数据包副本。其中高4位表示分段号，从0开始计数，步长为1，后12位是序列号（也就是优先级号），用于决定以模为4096的传输帧计数器，也是从0开始的，步长为1，同一帧的分段，序列号是一样的。



2.无线局域网标准

2.4 WLAN MAC帧格式

□ Data

- Data为数据字段，即发送或接收的信息。
- 最大帧为2312字节，其中包括8字节的802.11 LLC头，加上2296字节的净负荷和WEF开销。
- 如果此字段为空，则表示该帧为控制和管理帧。

2	2	6	6	6	2	6	0-2312	4字节
Frame Control	Duration ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Data	Frame Check Sum

2.无线局域网标准

2.4 WLAN MAC帧格式

□ Frame Check Sum

- Frame Check Sum为帧校验序列，即CRC（Cyclic Redundancy Check，循环冗余校验），占4字节。
- 用于校验帧的完整性，校验时必须对除FCS字段的其他字段一起进行计算。

2	2	6	6	6	2	6	0-2312	4字节
Frame Control	Duration ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Data	Frame Check Sum

3.接入认证

3.1 PPPoE接入认证

□ PPPoE简介

- PPPoE (Point-to-Point Protocol over Ethernet) , 即以太网上的点对点协议, 它可以使以太网上的主机通过一个简单接入设备连到Internet上, 对接入的用户进行控制、计费管理。
- PPPoE协议采用Client/Server (客户端/服务器) 方式, 它将PPP报文封装在以太网帧内, 在以太网上提供点对点的连接。

□ PPPoE连接

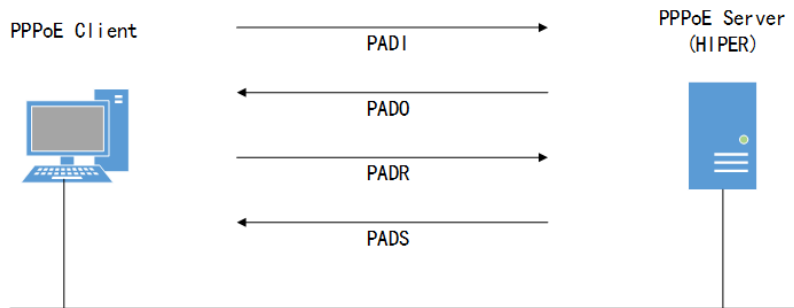
- PPPoE拨号连接包括Discovery (发现) 和Session (PPP会话) 两个阶段。

3.接入认证

3.1 PPPoE接入认证

Discovery阶段

- 此阶段用来建立连接，当用户主机开始创建一个PPPoE会话时，首先必须进行发现阶段以识别PPPoE Server的以太网MAC地址，并建立一个PPPoE会话标识（Session ID）。
- Discovery阶段由四个步骤组成，其基本工作流程：



3.接入认证

3.1 PPPoE接入认证

- **PADI**：如果要建立PPPoE连接，首先PPPoE客户端就要以广播的方式发送一个PADI（PPPoE Active Discovery Initiation）数据包，PADI数据包包括客户端请求的服务。
- **PADO**：当PPPoE服务器（BRAS）收到一个PADI包之后，会判断自己是否能够提供服务，如果能够提供服务的话，就会向客户端发送PADO（PPPoE Active Discovery Offer）数据包来进行回应。PADO数据包包括PPPoE服务器名称和与PADI数据包中相同的服务名。如果PPPoE服务器不能为PADI提供服务，则不响应。

3.接入认证

3.1 PPPoE接入认证

- **PADR**: 由于PADI是以广播的形式发送出去的, PPPoE客户端可能收到不止一个PADO数据包, 它将审查所有接收到的PADO数据包并根据其中的服务器名或所提供的服务选择一个PPPoE服务器, 并向选中的服务器发送PADR (PPPoE Active Discovery Request) 数据包。PADR数据包包括客户端所请求的服务。
- **PADS**: 当PPPoE服务器收到客户端发送的PADR包时, 就准备开始一个PPPoE会话。首先为PPPoE会话创建一个唯一的PPPoE会话ID, 并向客户端发送PADS (PPPoE Active Discovery Session-confirmation) 包作为响应。
- 当发现阶段正常结束后, 通信的两端都获得会话标识 (Session ID) 和对方的MAC地址, 两端共同唯一定义一个PPPoE会话。

3.接入认证

3.1 PPPoE接入认证

□ PPPoE会话阶段

- 当PPPoE进入PPP会话阶段后，客户端和服务端将进行标准的PPP协商，PPP协商通过后，数据通过PPP封装发送。
- PPP报文作为PPPoE帧的数据部分被封装在以太网帧内，发送到PPPoE链路的对端。
- Session ID必须是Discovery阶段确定的ID，且在会话过程中保持不变，MAC地址必须是对端的MAC地址。

3.接入认证

3.1 PPPoE接入认证

□ PPPoE连接断开

- 在会话阶段的任意时刻，PPPoE服务器和客户端都可向对方发送PADT (PPPoE Active Discovery Terminate) 包通知对方结束本会话。当收到PADT以后，就不允许再使用该会话发送PPP流量了。
- 在发送或接收到PADT数据包后，即使是常规的PPP结束数据包也不允许发送。
- 一般情况下，PPP通信双方使用PPP协议自身来结束PPPoE会话，但在无法使用时可以使用PADT来结束会话。

3.接入认证

3.2 WEB接入认证

- 通常情况下，WEB认证方式和DHCP服务器结合使用。在此认证方式下，用户通过Web页面进行认证，不存在跨越IP层和组播协议的限制问题。
- 这种认证方式最大的优势在于客户端不需要安装任何拨号软件，认证完全依靠浏览器完成。WEB认证服务器不需要与客户端认证建立PPP连接，因而不会成为系统瓶颈。

3.接入认证

3.2 WEB接入认证

□ WEB认证的主要过程：

- 客户机开机后，DHCP服务器通过DHCP协议为客户机分配动态IP地址。
- 客户机获得动态IP地址后，如果系统有重定向功能，没有通过认证的客户机登陆任何网页都会被重定向到认证页面，否则需要手动输入认证页面的URL。客户机在认证页面中输入用户名和密码等认证信息，提交认证请求。
- 认证服务器提取客户机认证请求信息，访问后台数据库进行用户信息核对。如果通过认证，客户机则可以访问外部资源；否则，系统要求客户机重新认证。
- 客户机认证通过后，认证页面将会向认证服务器发送计费请求，认证服务器收到请求后将会对此用户计费。

3.接入认证

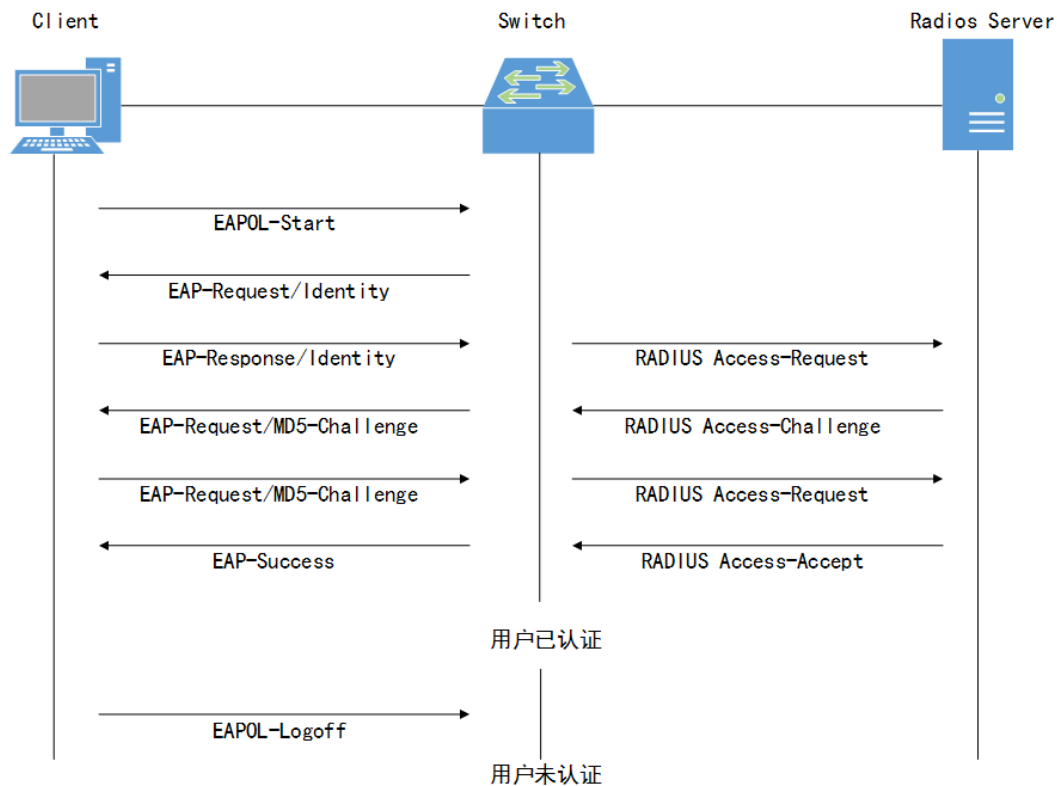
3.3 802.1x接入认证

□ 802.1x协议简介

- 802.1x协议是基于Client/Server的访问控制和认证协议。它可限制未经授权的用户/设备通过接入端口（Access Port）访问LAN/WLAN。在获得交换机或LAN提供的各种业务之前，802.1x对连接到交换机端口上的用户/设备进行认证。
- 在认证通过之前，802.1x只允许EAPoL（基于局域网的扩展认证协议）数据通过连接的交换机端口，认证通过后，数据方可通过。

□ 802.1x协议的主要特点：

- 实现简单
- 认证和业务数据分离



802.1x认证过程

3.接入认证

3.3 802.1x接入认证

□ 802.1x认证过程:

- Client向接入设备发送一个EAPoL报文，开始802.1x认证接入。
- 接入设备向Client发送EAP-Request/Identity报文，要求Client提交用户名信息。
- Client回应EAP-Response/Identity给接入设备请求，其中包括用户名信息。
- 接入设备将EAP-Response/Identity报文封装到RADIUS Access-Request报文中，发送到认证服务器。

3.接入认证

3.3 802.1x接入认证

□ 802.1x认证过程:

- 认证服务器产生一个Challenge，通过接入设备将RADIUS Access-Challenge报文发送给客户端，其中包含有EAP-Request/MD5-Challenge。
- 接入设备通过EAP-Request/MD5-Challenge发送给客户端，要求客户端进行认证。
- 客户端收到EAP-Request/MD5-Challenge报文后，将密码和Challenge做MD5算法计算后的Challenged-Password，再通过EAP-Response/MD5-Challenge回应给接入设备。
- 接入设备将Challenge，Challenged Password和用户名信息一并提交到RADIUS服务器，由RADIUS服务器进行认证。

3.接入认证

3.3 802.1x接入认证

□ 802.1x认证过程:

- RADIUS服务器对用户信息进行MD5算法计算后，判断用户是否合法，然后回应认证成功/失败报文到接入设备。如果成功，携带协商参数，以及用户的相关业务属性给用户授权。如果认证失败，则认证流程结束。
- 如果认证通过，用户通过标准DHCP协议（支持DHCP Relay），通过接入设备获取规划的IP地址。
- 如果认证通过，接入设备发起计费开始请求给RADIUS用户认证服务器。
- RADIUS用户认证服务器回应计费开始请求报文，用户认证流程结束。

4.无线通信加密

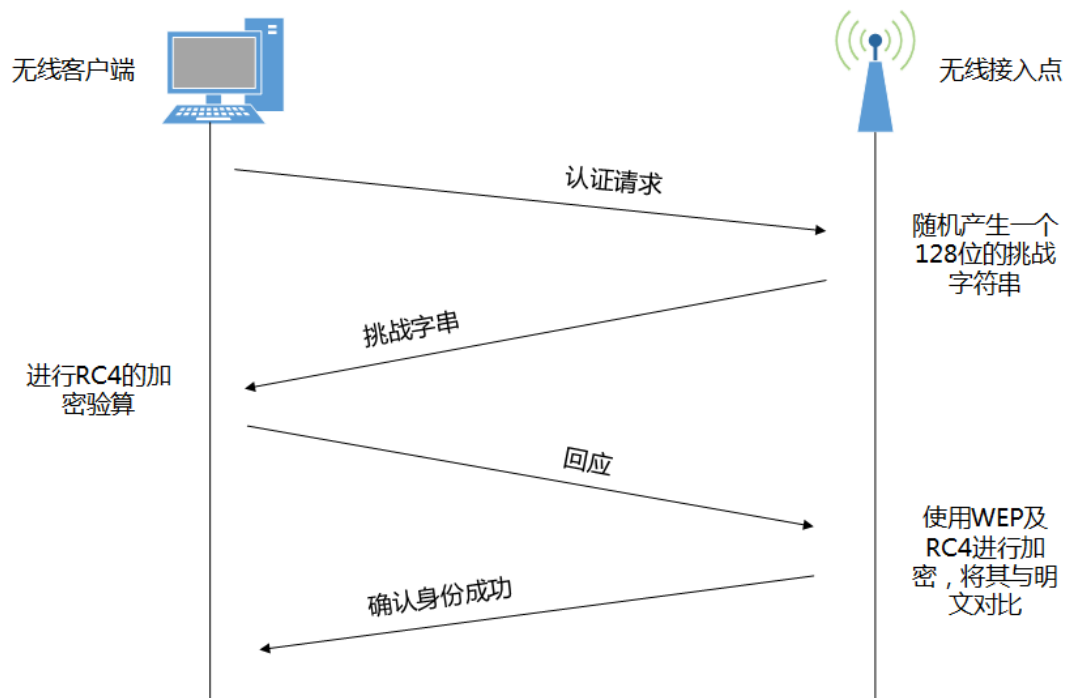
4.1 WEP

- 无线通信常见的加密技术有WEP、AES、WPA-PSK/WPA2PSK等。
- WEP简介
 - WEP (Wired Equivalent Privacy) 叫做有线等效加密，是一种可选的链路层安全机制，用来提供访问控制、数据加密和安全性检验等功能，是无线领域第一个安全协议。
 - WEP实现在802.11中是可选项，是目前无线加密的基础，其本意是实现一种与有线等价的安全程度。WEP的设计相对简单，它包括一个简单的基于挑战与应答的认证协议和一个加密协议，这两者都是使用RC4的加密算法。

4.无线通信加密

4.1 WEP

- WEP的密钥在802.11 (1999) 以前的版本中规定为64bits，包括40bits静态Key 和24bits的初始向量 (IV)。后来有些厂家将静态共享 Key 扩展到104bits，再加上24bits初始向量便构成128bits的WEP密钥。
- WEP包括一个使用32位CRC的校验机制叫ICV (Integrity Check Value)，其目的是用来保护信息不在传输过程中被修改。
- WEP加密网络上传输的数据，只让预定接收对象访问。WEP用“密钥”给数据编码再通过无线电波发送出去。密钥越长，加密性越强，任何接收设备只有知道相同的密钥才能解密数据。



WEP加密的验证及加密过程

4.无线通信加密

4.1 WEP

□ WEP漏洞

表 2-04 WEP 漏洞一览表

存在漏洞	相关描述
漏洞 1	认证机制过于简单，很容易通过异或的方式破解，而且一旦破解，由于使用的与加密用的密钥是同一个，所以还会危及以后的加密部分
漏洞 2	认证是单向的，AP 能认证客户端，但客户端没法认证 AP
漏洞 3	初始向量 (IV) 太短，重用很快，为攻击者提供很大的方便
漏洞 4	RC4 算法被发现有“弱密钥”(WeakKey) 的问题，WEP 在使用 RC4 的时候没有采用避免措施
漏洞 5	WEP 没有办法应对所谓的“重传攻击 (ReplayAttack)”
漏洞 6	ICV 被发现有弱点，有可能传输数据被修改而不被检测到
漏洞 7	没有密钥管理、更新、分发机制，完全要手工配置，因为不方便，用户往往常年不会去更改。

4.无线通信加密

4.1 WEP

□ WEP的改进

- 由于WEP强大的生存能力和广泛的市场应用程度，许多厂商对WEP进行了改进，以期能够提升WEP的安全性。对WEP的改进主要有两种思路：**高位WEP和动态WEP**。
- 高位WEP
 - 无线产品供应商现在普遍提供一种**用104位密钥的WEP**（加上24位IV，共128位），还有部分产品能够提供152、256位甚至512位密钥来改进WEP加密的脆弱性，对WEP的安全性实现了轻微改进。

4.无线通信加密

4.1 WEP

□ WEP的改进

■ 动态WEP

- 为了加强WEP的安全性，一些供应商提出了动态密钥的WEP方案。WEP的密钥不再是静态不变的，而是能定期动态更新。
- 例如，思科（Cisco）提供的LEAP（Lightweight Extensible Authentication Protocol）就是动态WEP，LEAP同时还提供双向的基于802.1x的认证。
- 这些方案在一定程度上缓解了WEP的危机，但由于动态WEP方案是无线设备供应商的私有方案而非标准，所以离完全解决WEP问题还有很大差距，而LEAP也已被彻底破解。

4.无线通信加密

4.2 WPA/WPA2加密认证

- 由于WEP加密技术使用静态共享密钥和未加密循环冗余码校验（CRC），无法保证加密数据的完整性，并存在弱密钥等。使得WEP加密技术在安全保护方面存在明显的缺陷，很容易被攻破。
- 于是诞生了新的WLAN加密技术WPA（Wi-Fi Protected Access, Wi-Fi保护访问）和WPA2。WPA2技术是WPA技术的升级版。
- 从技术角度看，WPA/WPA2主要解决了WEP在共享密钥上的漏洞，添加了数据完整性检查和用户级认证措施。

4.无线通信加密

4.2 WPA/WPA2加密认证

□ WPA加密技术

- Wi-Fi联盟给出的WPA定义为： $WPA = 802.1x + EAP + TKIP + MIC$ 。
- 其中，802.1x是指IEEE的802.1x身份认证标准；EAP（扩展身份认证协议）是一种扩展身份认证协议。这两者就是新添加的用户级身份认证方案。
- TKIP（临时密钥完整性协议）是一种密钥管理协议；MIC（消息完整性编码）是用来对消息进行完整性检查的，用来防止攻击者拦截、篡改甚至重发数据封包。
- WPA已不再是单一的链路加密，还包括了身份认证和完整性检查两个重要方面。

4.无线通信加密

4.2 WPA/WPA2加密认证

- WPA采用TKIP和MIC这两个协议全面保障了WLAN无线网络数据链路的加密和数据完整性检查功能。
- TKIP
 - TKIP采用了802.1x/EAP的架构，密钥位数最高达128位，并且是临时动态的（这也是“临时密钥完整性协议”名称的由来），然后再通过认证服务器分配的多组密钥进行认证，取代了WEP的单一静态密钥。

4.无线通信加密

4.2 WPA/WPA2加密认证

□ TKIP

- TKIP的一个重要特性就是它的“动态”性。
- TKIP密钥最重要的部分是基本密钥（Base Key）。
- 认证服务器在接收用户的身份认证信息后，使用802.1x来为运算阶段产生一组唯一的配对密钥。TKIP将这组密钥分配给无线客户端以及无线AP或无线路由器，建立密钥层级以及管理系统，然后使用配对密钥来动态产生唯一的数据加密密钥，并以此加密在无线传输阶段所传输的数据封包。

4.无线通信加密

4.2 WPA/WPA2加密认证

□ MIC

- MIC作用是防止攻击者拦截、篡改以及重发数据封包。
- MIC提供了一个强壮的计算公式，其中接收端与传送端必须各自计算值，并与MIC值比较。如果不符，它便假设数据已遭篡改，而该封包也会被丢弃。

4.无线通信加密

4.2 WPA/WPA2加密认证

□ WPA2加密技术

- WPA2是WPA的改进版本，可认为：
- **WPA2** = IEEE 802.11i = IEEE 802.1x/EAP + AES-CCMP。

表 2-05 WPA 和 WPA2 比较

应用模式	WPA	WPA2
企业应用模式	身份认证: IEEE 802.1x/EAP	身份认证: IEEE 802.1x/EAP
	加密: TKIP	加密: AES-CCMP
个人应用模式	身份认证: PSK	身份认证: PSK
	加密: TKIP/MIC	加密: AES-CCMP

4.无线通信加密

4.2 WPA/WPA2加密认证

□ WPA2加密技术

- 在WPA2中，采用了加密性能更好、安全性更高的加密技术**AES-CCMP**（Advanced Encryption Standard – Counter mode with Cipher-block chaining Message authentication code Protocol，**高级加密标准 – 计数器模式密码区块链接消息身份验证代码协议**），取代了原WPA中的TKIP/MIC加密协议。
- **AES-CCMP是民用范围内最高级无线安全协议**。总体来说，CCMP提供了加密、认证、完整性检查和重放保护四重功能。

4.无线通信加密

4.2 WPA/WPA2加密认证

- WPA和WPA2设计了两种应用模式：WPA/WPA2个人版和WPA/WPA2企业版。
- WPA/WPA2企业版需要一台具有802.1x功能的RADIUS服务器，没有RADIUS服务器的用户可以使用WPA/WPA2个人版，其口令长度为20个以上的随机字符。

4.无线通信加密

4.2 WPA/WPA2加密认证

□ WPA/WPA2中的IEEE 802.11x身份认证系统

- IEEE 802.1x是一种为了适应宽带接入不断发展的需要而推出一种身份认证协议，是基于端口的访问控制协议，但并不是专为WLAN设计的。当无线工作站（STA）与无线访问点（AP）关联后，是否可以使用AP的服务要取决于802.1x的认证结果。如果认证通过，则AP为STA打开对应逻辑端口，否则不允许用户连接网络。
- 802.1x协议仅仅关注端口的打开与关闭，当合法用户（根据账号和密码）接入时，该端口打开，而非法用户接入或没有用户接入时，则该端口处于关闭状态。
- 认证结果在于端口状态的改变，而不涉及通常认证技术必须考虑的IP地址协商和分配问题，是各种认证技术中最简化的实现方案。

4.无线通信加密

4.2 WPA/WPA2加密认证

□ WPA/WPA2中的IEEE 802.11x身份认证系统

- IEEE 802.11x包括3个重要的部分：

Supplicant System (应用系统, 也就是“客户端”)

Authenticator System (认证系统)

Authentication Server System (认证服务器系统)



4.无线通信加密

4.2 WPA/WPA2加密认证

□ WPA/WPA2中的IEEE 802.11x身份认证系统

- 802.1x认证系统使用EAP (Extensible Authentication Protocol, 可扩展认证协议) 来实现客户端、设备端和认证服务器之间认证信息的交换。
- 在客户端与设备端之间, EAP协议报文使用EAPOL封装格式。
- 在设备端与RADIUS服务器之间, 可以使用两种方式来交换信息: 一种是EAP协议报文使用EAPOR (EAP over RADIUS) 封装格式承载于RADIUS协议中; 另一种是EAP协议报文由设备端进行终结, 采用包含PAP (Password Authentication Protocol, 密码验证协议) 或CHAP (Challenge Handshake Authentication Protocol, 质询握手验证协议) 属性的报文与RADIUS服务器进行认证交互。

4.无线通信加密

4.2 WPA/WPA2加密认证

□ WPA2相对WEP的改进

表 2-06 WPA2 针对 WEP 的改进

WEP 存在的缺陷	WPA2 的解决方法
初始化向量 (IV) 太短	在 AES-CCMP 中, IV 被替换为“数据包编号”字段, 并且其大小将倍增至 48 位
不能保证数据完整性	采用 WEP 加密的校验和计算已替换为可严格实现数据完整性的 AES CBC-MAC 算法。CBC-MAC 算法算得出一个 128 位的值, 然后 WPA2 使用高阶 64 位作为消息完整性代码 (MIC)。WPA2 采用 AES 计数器模式加密方式对 MIC 进行加密
适应主密钥而非派生密钥	与 WPA 和“暂时密钥完整性协议” (EAP) 类似, AES-CCMP 使用一组从主密钥和其他值派生的暂时密钥。主密钥是从“可扩展身份验证协议-传输层安全性” (EAP-TLS) 或“受保护的 EAP” (PEAP) 802.1x 身份验证过程派生而来的
不重新生成密钥	AES-CCMP 自动重新生成密钥以派生新的暂时密钥组
无重播保护	AES-CCMP 使用“数据包编号”字段作为计数器来提供重播保护
无身份认证	采用 IEEE 802.1x 进行身份认证

4.无线通信加密

4.3 无线局域网的安全管理

□ 安全风险因素

- 拒绝服务攻击
- 人为干扰
- 插入攻击
- 充放攻击
- 广播监测
- ARP欺骗
- 会话劫持
- 流氓接入点
- 密码分析攻击
- 旁信道攻击

4.无线通信加密

4.3 无线局域网的安全管理

- 提升无线局域网安全的一般建议：
 - 采用无线加密协议防止未授权用户接入
 - 改变AP的身份标识符并禁止SSID广播
 - 静态IP与MAC地址绑定
 - 无线入侵检测系统
 - 采用身份验证和授权
 - 其他安全措施

5.案例：家庭无线局域网

5.1 需求

- 家庭搭建一个无线局域网需求：
 - 两台电脑和一台移动终端能够通过无线路由器访问Internet，并且要求在家庭中每个地方都能够连接到无线路由器，所有接入设备能够形成局域网。

5.案例：家庭无线局域网

5.2 方案

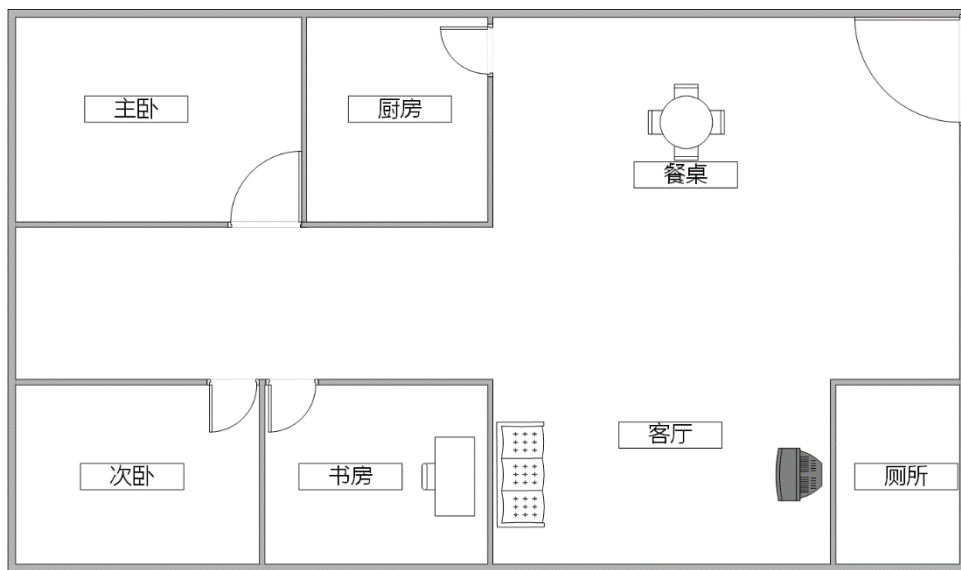
□ 组网方式：

- 家庭无线局域网的组网方式和有线局域网有一些区别，最简单、最便捷的方式就是选择对等网。该组网方式具有安装方便、扩充性强、故障易排除等特点。
- 对等网组网方式可不通过无线AP或无线路由器，直接通过无线网卡来实现数据传输，但计算机之间的距离较短、网络设置要求较高、相对麻烦，故不建议采用此方案。

5.案例：家庭无线局域网

5.2 方案

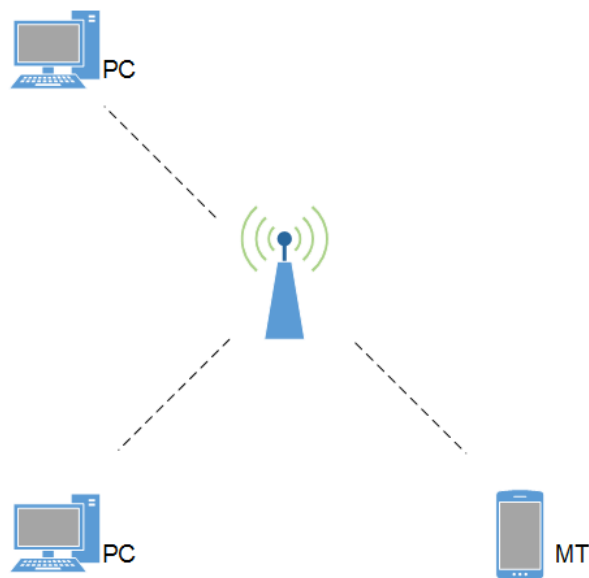
□ 家庭平面图：



5.案例：家庭无线局域网

5.2 方案

□ 拓扑设计：



家庭无线拓扑

5.案例：家庭无线局域网

5.2 方案

□ 设备选型：

表 2-07 无线局域网所涉及设备型号一览表

序号	设备类别	品牌	型号	数量(台)
1	计算机	联想	H3050	2
2	网卡		NW360 300M USB	2
3	移动终端设备	Apple	Apple iPod touch	1
4	无线路由器	TP-LINK	TL-R20441N	1

5.案例：家庭无线局域网

5.2 方案

□ 网络地址规划：

表 2-08 网络地址规划表

序号	区域	设备名	IP 地址	子网掩码
1	书房	PC1	192.168.1.101	255.255.255.0
2	卧室	PC2	192.168.1.102	255.255.255.0
3	家庭	MT	192.168.1.103	255.255.255.0
4	家庭	AP	192.168.1.1	255.255.255.0



现场演示：

- 使用两台笔记本电脑，通过无线网卡建立对等网。
- 使用无线路由器和计算机、移动设备结合建立对等网。
- 局域网建立的连通性测试。

5.案例：家庭无线局域网

5.4 应用测试

表 2-09 设备连接无线路由器测试结果表

序号	设备	是否能连接成功
1	PC1	√
2	PC2	√
3	MT	√

表 2-10 无线局域网接入设备间 Ping 连通性测试结果表

序号	请求主机	相应主机	Ping 测试结果
1	PC1	PC2	√
2	PC1	MT	√
3	PC2	PC1	√
4	PC2	MT	√
5	MT	PC1	-
6	MT	PC2	-

6.案例：无线企业网

6.1 需求

- 某软件企业有员工30人，拥有办公场所4间，分别是研发部1间、会议室1间、办公室1间、会客室1间。
- 具体需求有五个方面：
 - 无线局域网和企业现有有线网络要能够完全融合，使用同一套IP地址管理体系、同一网络接入互联网的出口。
 - 无线局域网要能够覆盖到企业的所有位置，员工在企业内随意移动时，要确保网络不中断，使用网络的体验要平滑统一。
 - 需要根据人群不同而广播多个SSID，且每个SSID均能够覆盖企业任何位置，每个SSID使用独立的接入验证方式，以满足不同人群的使用。
 - 不需要为无线局域网进行独立布线，能够使用现有的布线系统完成无线局域网建设。
 - 要支持集中且统一的管理，以提升管理水平，降低维护成本。

6.案例：无线企业网

6.2 方案

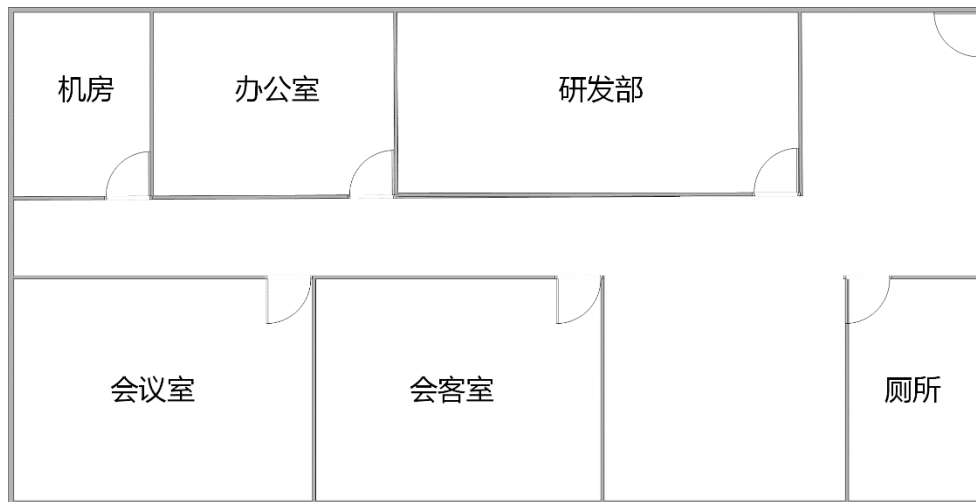
□ 组网方式

- 由于企业的区域范围比较大，使用一个AP无法全面覆盖企业区域，需要使用多个AP才能对企业进行全面区域覆盖，因此选用多AP模式，**多AP模式**也就是多蜂窝结构。

6.案例：无线企业网

6.2 方案

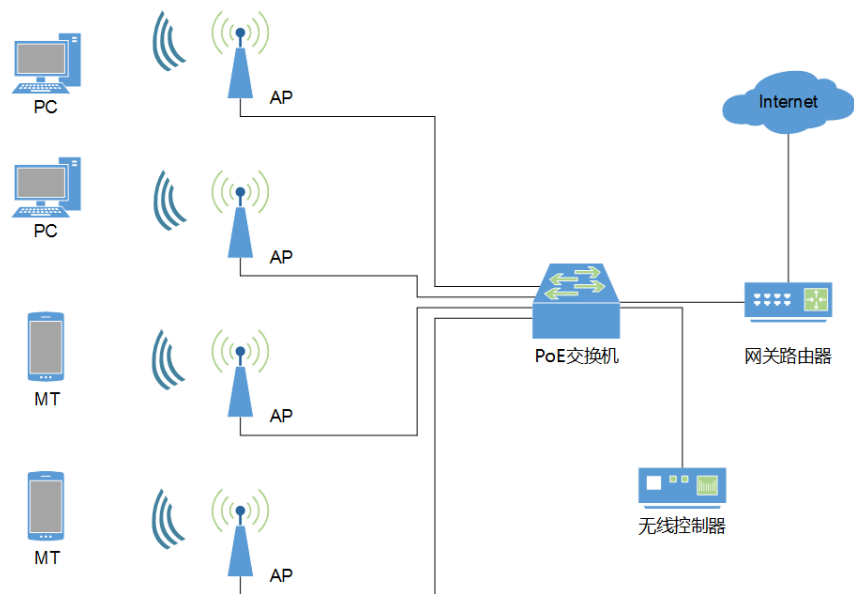
□ 企业平面图：



6.案例：无线企业网

6.2 方案

□ 拓扑设计：



无线企业网拓扑结构设计

6.案例：无线企业网

6.2 方案

□ 设备选型：

表 2-11 无线企业网设备选型一览表

序号	品牌	型号	类型	速度	POE 供电	协议	特性
1	TP-LINK	TL-AC200	无线控制器 (AC)				自动发现统一管理吸顶式 AP 与面板式 AP、实时监控 AP 工作状态、统一配置所有 AP、统一升级 AP 软件、无线 MAC 地址白名单、无线网络与 Tag VLAN 绑定, 隔离不同无线网络。
2	TP-LINK	TL-1009P	百兆非网管 PoE 交换机				单端口 PoE 功率达 15.4W, 整机最大 PoE 输出功率为 60W、支持 IEEE 802.3x 全双工流控与 Backpressure 半双工流控、支持端口自动翻转 (Auto MDI/MDIX) 功能、所有端口均具备线速转发能力。
3	TP-LINK	TL-AP302C-POE	无线接入点 (AP)	300M	支持	802.11n	吸顶/壁挂, 802.3af/a 标准 POE 供电、无线发射功率线性可调、支持 8 个 SSID、内置独立硬件保护电路, 可自动恢复工作异常 AP。

6.案例：无线企业网

6.2 方案

□ 设备选型：

表 2-12 设备购买预算单

序号	品牌	型号	类型	数量 (台)	价格 (元)	总价 (元)
1	TP-LINK	TL-AC200	无线控制器 (AC)	1	479	1555
2	TP-LINK	TL-1009P	PoE 交换机	1	320	
3	TP-LINK	TL-AP302C-POE	无线接入点 (AP)	4	189	

6.案例：无线企业网

6.2 方案

- 企业无线局域网不同家庭无线局域网，无线企业网要使多台AP，并广播三套SSID以供日常办公人员、研发人员和外来人员使用，不同SSID接入的IP地址分配段不同。

6案例：无线企业网

6.2 方案

表 2-13 无线企业网 IP 地址规划表

序号	区域	SSID	网段	IP 地址范围	子网掩码
1	内部	OfficeNetwork	192.168.1.0/24	192.168.1.100~192.168.1.130	255.255.255.0
2	内部	DevNetwork	192.168.1.0/24	192.168.1.131~192.168.1.170	255.255.255.0
3	内部	OpenNetwork	192.168.1.0/24	192.168.1.171~192.168.1.199	255.255.255.0

表 2-14 无线企业网 SSID 规划与安全设计表

序号	SSID	加密方式	密码	访问范围
1	OfficeNetwork	WPA-PSK/WPA2-PSK	12345678	可访问企业办公服务器和 Internet
2	DevNetwork	WPA-PSK/WPA2-PSK	87654321	可访问企业研发服务器和 Internet
3	OpenNetwork			可访问 Internet

6案例：无线企业网

6.3 部署实施

□ 部署设备：

表 2-15 无线企业网设备连接规划表

序号	设备名称	安装区域	PoE 交换机端口
1	AP1	办公室	1
2	AP2	研发部	2
3	AP3	会议室	3
4	AP4	会客室	4
5	网管路由器	机房	Uplink
6	AC	机房	8

6.案例：无线企业网

6.3 部署实施

□ 设备与网络配置：

- 选择一台计算机作为管理终端设备，在建设过程中用于设备配置和测试。设置管理终端的IP地址为192.168.1.251，子网掩码为255.255.255.0。
- 使用管理终端计算机，通过浏览器访问无线控制器，以进行配置。无线控制器的管理采用Web界面，访问地址为：
<http://192.168.1.253>。
- 无线控制器的默认管理账号用户名为admin，密码为admin。



现场演示：

- 无线AP、无线AP控制器、POE交换机的结构。
- 无线AP、无线AP控制器、POE交换机的安装与配置。
- 无线企业网建设过程。
- 多终端接入和测试。



The image shows a TP-LINK login interface. At the top is a blue header with the "TP-LINK®" logo. Below the header, the interface has a light gray background. In the center, there are two input fields. The first is labeled "用户名:" (Username) and contains the text "admin". The second is labeled "密 码:" (Password) and contains five black dots. Below these fields are two buttons: "登录" (Login) on the left and "清除" (Clear) on the right.

Copyright © 2015 普联技术有限公司 版权所有

无线控制器登录



无线控制器总览


AP列表

AP总数：4 在线：4 离线：0 异常：0

备注

搜索

显示全部

<input type="checkbox"/>	序号	备注	型号	MAC地址	硬件版本	软件版本	运行状态	2.4GHz频段		5GHz频段		设置
								客户端	信道	客户端	信道	
<input type="checkbox"/>	1	AP1	TL-AP302C-PoE	88:25:93:4A:1E:27	2.0	1.0.1	在线	0/100	1(手动)	---	---	   
<input type="checkbox"/>	2	AP2	TL-AP302C-PoE	88:25:93:4A:1E:54	2.0	1.0.1	在线	0/100	6(手动)	---	---	   
<input type="checkbox"/>	3	AP3	TL-AP302C-PoE	88:25:93:4A:1D:F2	2.0	1.0.1	在线	0/100	11(手动)	---	---	   
<input type="checkbox"/>	4	AP4	TL-AP302C-PoE	88:25:93:4A:1E:83	2.0	1.0.1	在线	0/100	13(自动)	---	---	   

编辑

重启

删除

打开LED灯


关闭LED灯

刷新















帮助

无线局域网AP管理

2.4GHz 无线服务

序号	无线网络名称	网络类型	加密方式	密码	状态	客户端数目	设置
1	OfficeNetwork	员工网络	WPA-PSK/WPA2-PSK	12345678	已启用	1	 
2	OpenNetwork	访客网络	不加密	---	已启用	0	 
3	DevNetwork	员工网络	WPA-PSK/WPA2-PSK	87654321	已启用	0	 
4	Office3_2.4GHz	员工网络	不加密	---	已禁用	0	 
5	Office4_2.4GHz	员工网络	不加密	---	已禁用	0	 
6	Office5_2.4GHz	员工网络	不加密	---	已禁用	0	 
7	Office6_2.4GHz	员工网络	不加密	---	已禁用	0	 
8	Office7_2.4GHz	员工网络	不加密	---	已禁用	0	 

5GHz 无线服务

序号	无线网络名称	网络类型	加密方式	密码	状态	客户端数目	设置
1	OfficeNetwork	员工网络	WPA-PSK/WPA2-PSK	12345678	已启用	0	 
2	OpenNetwork	访客网络	不加密	---	已启用	0	 
3	DevNetwork	员工网络	WPA-PSK/WPA2-PSK	87654321	已禁用	0	 
4	Office3_5GHz	员工网络	不加密	---	已禁用	0	 
5	Office4_5GHz	员工网络	不加密	---	已禁用	0	 
6	Office5_5GHz	员工网络	不加密	---	已禁用	0	 
7	Office6_5GHz	员工网络	不加密	---	已禁用	0	 

无线局域网SSID管理

AP地址范围

起始地址：

...

结束地址：

...

VLAN ID范围：

 (可选，最多200个ID，格式：2-13;15)

AP可接受IP地址配置

6.案例：无线企业网

6.4 无线漫游

- 无线客户端使用同一个无线登录账号，可以在多个AP之间切换。无线客户端接入无线网络后，不需要任何手动设置，即可实现在多个AP间的无线漫游。
- 实现无线漫游必须遵守：
 - 无线路由器SSID设置必须相同。
 - 无线路由器分配的地址必须属于同一网段，且归属于同一个VLAN。
 - 无线AP必须采用相同的加密方式WPA-PSK/WPA2-PSK，并设置相同验证密码。

6.案例：无线企业网

6.4 无线漫游

□ 实现无线漫游必须遵守：

- 信号相互覆盖的无线路由器，必须使用不同的信道。AP之间的信号必须相互覆盖，否则会出现不能上网的盲区。相互覆盖的AP不能采用相同的信道，不然会造成AP信号传输时相互干扰。在可用的11个信道中，仅有3个信道是完全不覆盖的，分别为 Channel 1、Channel 6、Channel 11，利用这三个信道做多蜂窝覆盖是最合适。
- 无线局域网内在无线漫游时，客户端配置与接入点网络中的配置完全相同，用户在移动过程中完全感受不到无线AP之间的切换操作。

6.案例：无线企业网

6.5 应用测试

表 2-16 连接测试表

序号	SSID	请求主机 IP	接入位置	相应主机 IP	接入位置	Ping 测试结果
1	OfficeNetwork	192.168.1.100	办公室	192.168.1.101	会议室	√
2	OfficeNetwork	192.168.1.100	办公室	192.168.1.102	会客室	√
3	OfficeNetwork	192.168.1.100	办公室	192.168.1.103	研发部	√
4	DevNetwork	192.168.1.131	研发部	192.168.1.132	办公室	√
5	DevNetwork	192.168.1.131	研发部	192.168.1.133	会客室	√
6	DevNetwork	192.168.1.131	研发部	192.168.1.134	会议室	√
7	OpenNetwork	192.168.1.171	会客室	192.168.1.172	办公室	√
8	OpenNetwork	192.168.1.171	会客室	192.168.1.173	会议室	√
9	OpenNetwork	192.168.1.171	会客室	192.168.1.174	研发部	√

Thanks.