

网络应用技术



第9讲 无线局域网

河南中医药大学信息技术学院
《网络应用技术》课程教学组

-
1. 为什么需要WLAN?
 2. 认识802.11
 3. 认识频谱
 4. WLAN的结构
 5. WLAN的各种标准
 6. WLAN的加密与认证

1.为什么需要WLAN?

1. 为什么需要WLAN

□ 什么是WLAN?

- WLAN即无线局域网的英文缩写，其全称是Wireless Local Area Networks，是一种利用射频（Radio Frequency, RF）技术，使用电磁波，取代双绞铜线（或光纤）所构成的局域网络，在空中进行通信连接，从而实现数据传输的系统。
- 通俗地说，它是一种通过电磁波进行数据传输的、无线形式的局域网。



1. 为什么需要WLAN

□ 为什么需要WLAN?

- 传统的有线局域网会受到布线的限制
 - 建筑物中没有预留的线路，布线以及调试的工程量将非常大；
 - 线路容易损坏，维护不便；
 - 网络中各节点的搬迁和移动麻烦
- WLAN的出现并不是用来取代有线局域网络，而是用来弥补有线局域网络的不足，以达到网络延伸的目的。



2. 什么是802.11?

2. 什么是802.11?

□ IEEE的802项目

- 电气和电子工程师协会（IEEE）制定了各种不同的通信技术的标准。其中最著名的IEEE项目就是负责开发局域网标准的802项目。
- 在802项目中，还划分了许多工作组，负责解决某个特定方面问题的标准。工作组同样会被赋予一个编号，例如Ethernet就是由第3个工作组负责标准化，因此该标准被称为802.3。
- Wireless LAN的标准则是由**第11个工作组**负责的，因此WLAN的标准被称为802.11。

2. 什么是802.11?

□ 802家族和OSI模型的关系

- IEEE802规范的重心放在OSI模型最下面的两层，它们同时涵盖了物理层（简称PHY）和数据链路层（data link）组件。只要是802网络，就必然会同时具备MAC（媒体访问控制）与PHY（物理层）两种组件。MAC是一组用以决定如何访问媒介与传送数据的规则，至于传送与接收的细节则交由PHY负责。
- 802网络的管理功能规范于802.1中，而802.1的范围又涵盖了桥接（802.1D）和虚拟局域网（802.1Q）。
- 802.2所规范的链路层（link layer）称为逻辑链路控制层（简称LLC），可供所有底层局域网技术使用，例如802.3、802.5等。

2. 什么是802.11?

□ 802.11的物理层

- 802.11基本规范涵盖了802.11MAC以及两种物理层：
 - 调频扩频（简称FHSS）物理层
 - 直接序列扩频（简称 DSSS）物理层
- 后来改版时，802.11陆续加入了其他不同的物理层：
 - 802.11a: 正交频分复用（OFDM）物理层、工作在5G频段
 - 802.11b: 高速直接序列扩频（HR/DSSS）物理层、工作在2.4G频段
 - 802.11g: 正交频分复用（OFDM）物理层、**工作在2.4G频段**
 - 802.11n: OFDM + MIMO技术、**工作在2.4G频段或5G频段**
 - **802.11ac**: OFDM + MIMO技术、**工作在5G频段**

802家族和OSI模型的关系



寻址及网际互连

网络层

802.1

数据链路层

管理及体系结构

802.2逻辑链路控制层 LLC

LLC子层

802.3
MAC

802.5
MAC

802.11 MAC子层

MAC子层

802.3
PHY

802.5
PHY

802.11
FHSS
PHY

802.11
DSSS
PHY

802.11a

802.11b

802.11g

物理层

2. 什么是802.11?

□ 802.11与Ethernet的渊源

- 802.11网络与Ethernet的渊源之深，以至于从用户的角度来看，802.11和Ethernet没有两样。有时它甚至被称为“无线Ethernet”。
- 802.11里同样可以找到Ethernet的核心成分。它同样是以长度为48位的IEEE 802 MAC地址来区分工作站（例如无线局域网中的手机），帧的传递是根据MAC地址的。

802.11
Ethernet



3. 认识无线电频谱

3. 认识无线电频谱

□ 无线电频谱是关键资源

- 无线设备被限定在某个特定频带上工作，每个频带都有相应的带宽，即该频带可供使用的频率空间总和。带宽是评价链路（link）数据传输能力的基准
- 无线电频谱的使用受到主管当局的严格控制，主要是通过核发许可证的方式。例如，在美国的主管机关是联邦通信委员会，欧洲的主管机关是欧洲无线电通信局。其他地区，则由国际电信联盟（ITU）把关。

3. 认识无线电频谱

□ 美国地区常用频带（部分）

频带	频率范围
UHF, ISM	902~928 MHz
S - 频带	2~4 GHz
S - 频带, ISM	2.4 ~2.5 GHz
C - 频带, 卫星下行链路	3.7 ~4.2 GHz
C - 频带, 雷达 (气象)	5.25 ~5.925 GHz
C - 频带, ISM	5.725 ~5.875 GHz
C - 频带, 卫星上行链路	5.925 ~6.425 GHz

3. 认识无线电频谱

□ 关于ISM频带

- 上表中，有三个标示为ISM的频带，即工业（industrial）、科学（scientific）、医疗（medical）。大致而言，ISM频带是保留给工业、科学或医疗设备使用的。
- 例如，微波炉就属于ISM设备，使用的是2.4G~2.5GHz ISM频带，因为该频段内的电磁辐射特别有利于加热含水物质。
- 之所以提到ISM，因为该频段的使用不需要申请许可证。802.11和许多其他设备均使用ISM频带。
- 例如802.11b/g/n设备使用2.4GHz ISM频带，而802.11a/n/ac使用5GHz频带。

4. 无线局域网的组成

4.无线局域网的组成

□ 无线局域网的组成

- 工作站 (Station, STA)
- 无线介质 (Wireless Medium, WM)
- 访问点 (Access Point, AP)
- 分布式系统 (Distribution System, DS)

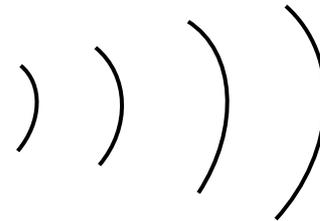
无线局域网的基本组件

分布式
系统
(DS)



无线接入点 (AP)

无线媒介

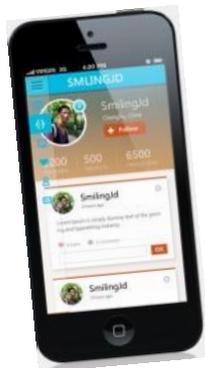


工作站

4.无线局域网的组成

□ 工作站

- 工作站又称站、主机（Host）和终端（Terminal），是无线局域网的最基本组成单元，实际上可以说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以移动的，因此又可称为移动主机或移动终端。



4.无线局域网的组成

□ 访问点 (AP)

- 无线接入点类似蜂窝结构中的基站，是无线局域网的重要组成部分。无线接入点是一种特殊的站，它通常处于基本服务集（BSS）的中心，固定不动。其基本功能如下。
 - ① 作为接入点，完成其他非AP的站对分布式系统的接入访问和同一基本服务集（BSS）中的不同站间的通信连接。
 - ② 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。
- 管理员在安装配置AP时，需要为该AP配置至少一个服务集标识符（又叫网络标识符）SSID和一个信道。



TP-LINK TL-AP451C 450M企业级无线吸顶式AP 无线wifi接入点

无线速率提升至450M，带机更多，覆盖更广！[如需双频无线AP，速度更快，点此查看！](#)

京 东 价：**¥269.00** (降价通知)

促销信息：**加价购** 满29.00另加6.90元，或满39.00另加12.90元，或满49.00另加36.00元，即可在购物车换购热销商品 [详情 >>](#)

配 送 至： **有货**，支持 99元免运费 | 货到付款

服 务：由 京 东 发 货，并 提 供 售 后 服 务。11:10前完成下单,预计今天(09月27日)送达

选择颜色： 无线控制器AC100 无线控制器AC200 300M波浪型AP(DC供电)







4.无线局域网的组成

□ 无线媒介

- 无线介质是无线局域网中站与站之间、站与接入点之间通信的传输介质。



4.无线局域网的组成

□ 分布式系统 (DS)

- 当WLAN需要覆盖更大区域时，通常需要多个AP连接起来，并且，彼此之间必须相互通信以掌握移动式工作站的行踪。
- 分布式系统 (distribution system) 属于802.11的逻辑组件，负责将帧转送至目的地。
- 802.11并未规范分布式系统的技术细节。大多数商用产品是以桥接引擎和分布式系统媒介共同组成分布式系统。
- 分布式系统是接入点间转发帧的骨干网络，所有在商业上获得成功的产品几乎都是以Ethernet为骨干网络。

无线局域网的组成

DS: 分布式系统, 负责将帧传送到目的地

DS

AP



无线
媒介



工作站



AP

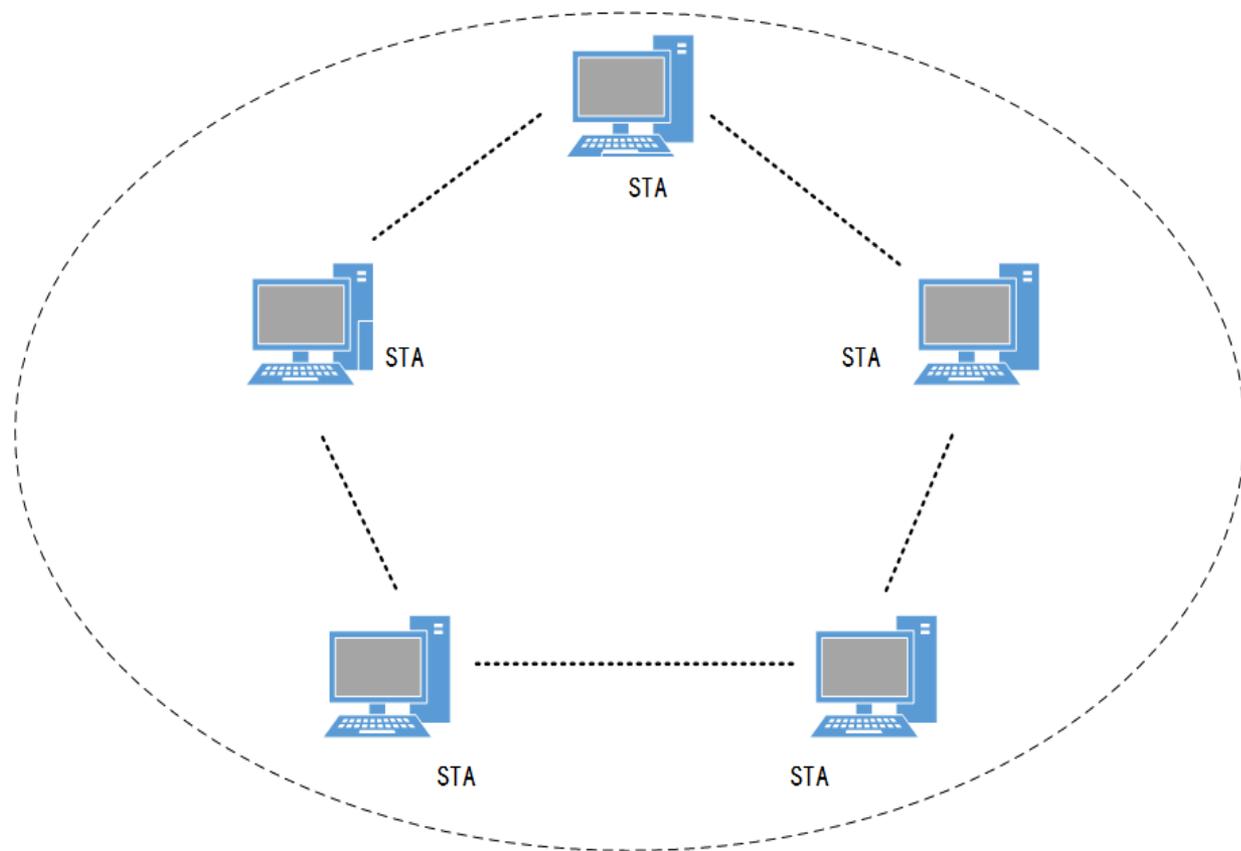


AP: 接入点, 管理员在安装配置AP时, 需要为该AP配置至少一个服务集标识符 (又叫网络标识符) SSID和一个信道。

5. 无线局域网的拓扑结构

5.无线局域网的拓扑结构

□ (1) 点对点模式Ad-hoc/对等模式



通过无线网卡
连接

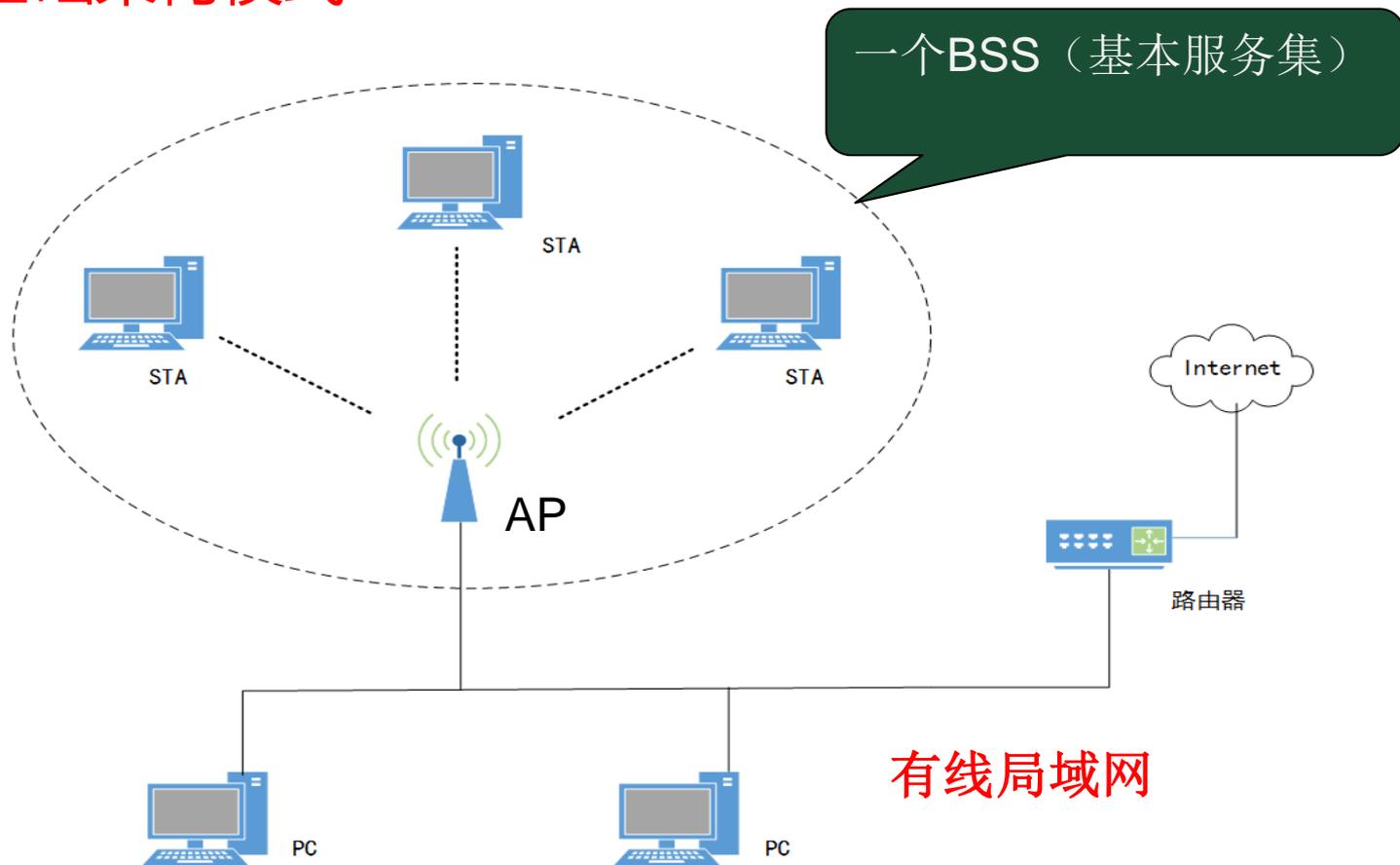
5.无线局域网的拓扑结构

□ (1) 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其他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。

5.无线局域网的拓扑结构

□ (2) 基础架构模式



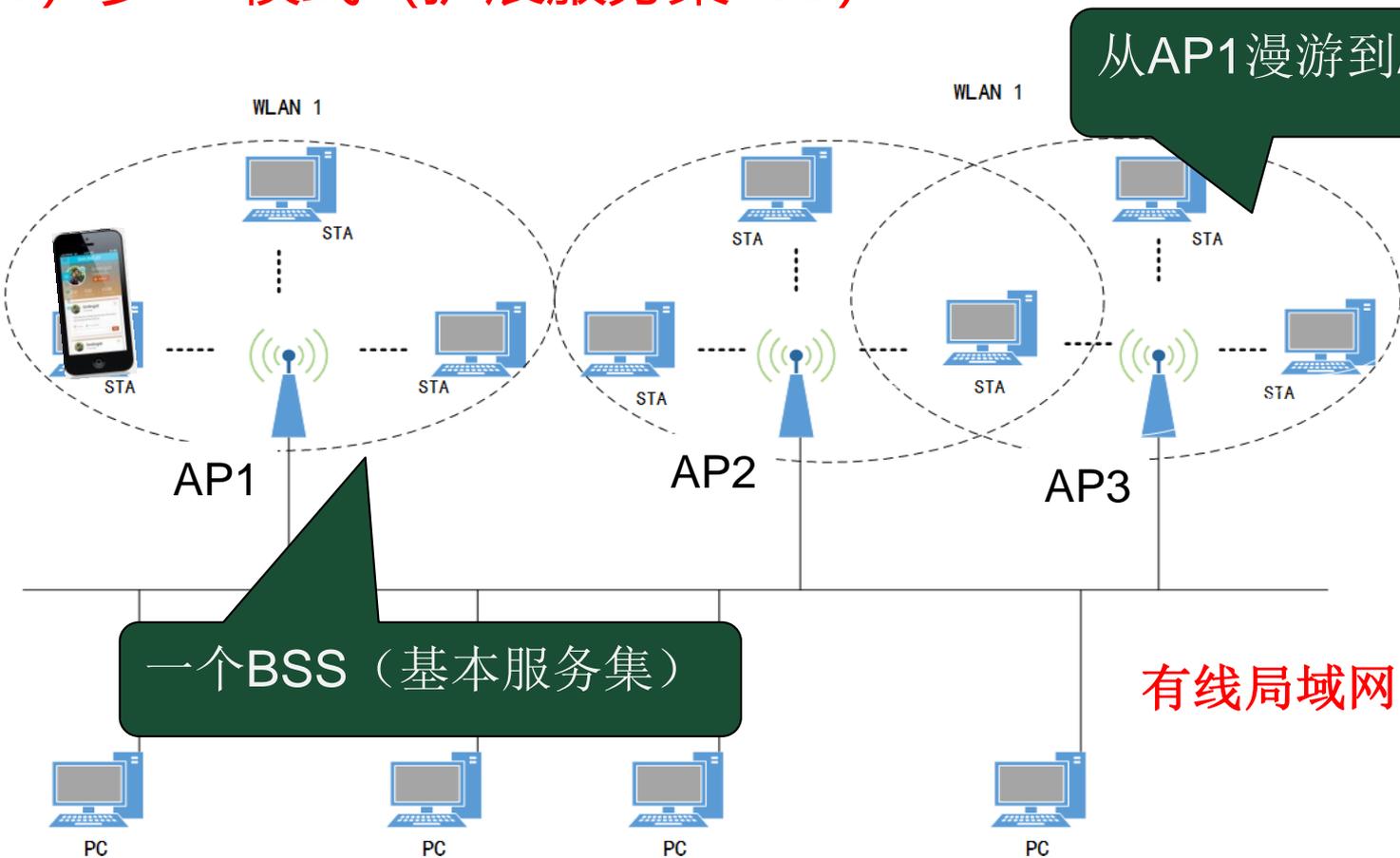
5.无线局域网的拓扑结构

□ (2) 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DS构成，覆盖区域称基本服务集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，是有中心拓扑结构。
- 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。

5.无线局域网的拓扑结构

□ (3) 多AP模式 (扩展服务集ESS)



5.无线局域网的拓扑结构

□ (3) 多AP模式

- 一个BSS的服务范围可以涵盖整个小型办公室或家庭，不过无法服务较广的区域。
- 802.11允许我们将几个BSS串联为扩展服务集（extended service set，简称ESS），借此扩展无线网络的覆盖区域。
- 所谓的**多AP模式**就是指由多个AP以及连接它们的分布式系统DS组成的更大范围的无线网络，即扩展服务集ESS。
- 扩展服务集内的每个AP都是一个独立的无线网络基本服务集BSS，**所有AP可以共享同一个服务集标识符（又叫网络标识符）SSID，这样，一个工作站就可以在不同的AP间漫游了。**

6. 无线局域网的标准（略）

标准	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g	IEEE 802.11n	IEEE 802.11ac	IEEE 802.11i
发布时间	1999	1999	2003	2009	2012	2003
工作频段	5GHz	2.4GHz	2.4GHz	2.4/5GHz	5GHz	无线网络 安全方面 的补充
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	
调制方式	OFDM	CCK/DSSS	CCK/DSSS/ OFDM	4*4MIMO- OFDM/DSSS /CKK	8*8MIMO- OFDM/16~2 56QAM	
兼容性	802.11a	802.11b	802.11b/g	802.11a/b/ g/n	802.11a/b/g /n	

无线局域网的标准

6.无线局域网的标准

□ 最早的标准：802.11

- 1997年，IEEE制定发布了最早的无线局域网标准802.11，工作在2.4GHz频带。主要用于解决办公室局域网和校园网中用户与用户终端的无线接入，业务主要限于数据存取，速率最高只能达到2Mbps。由于它在速率和传输距离上都不能满足人们的需要，所以在后期很快出现了后续的一系列新的标准。

6.无线局域网的标准

□ 802.11a (1999年)

- 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规范的主要特性如下。
- （1）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。

6.无线局域网的标准

□ 802.11a (1999年)

■ (2) 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。

■ (3) 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。如表2-1列出了可用的24个信道及所适用的环境。

6. 无线用

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	5580	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

6.无线局域网的标准

□ 802.11b (1999年)

■ ①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。

■ ②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。

6.无线局域网的标准

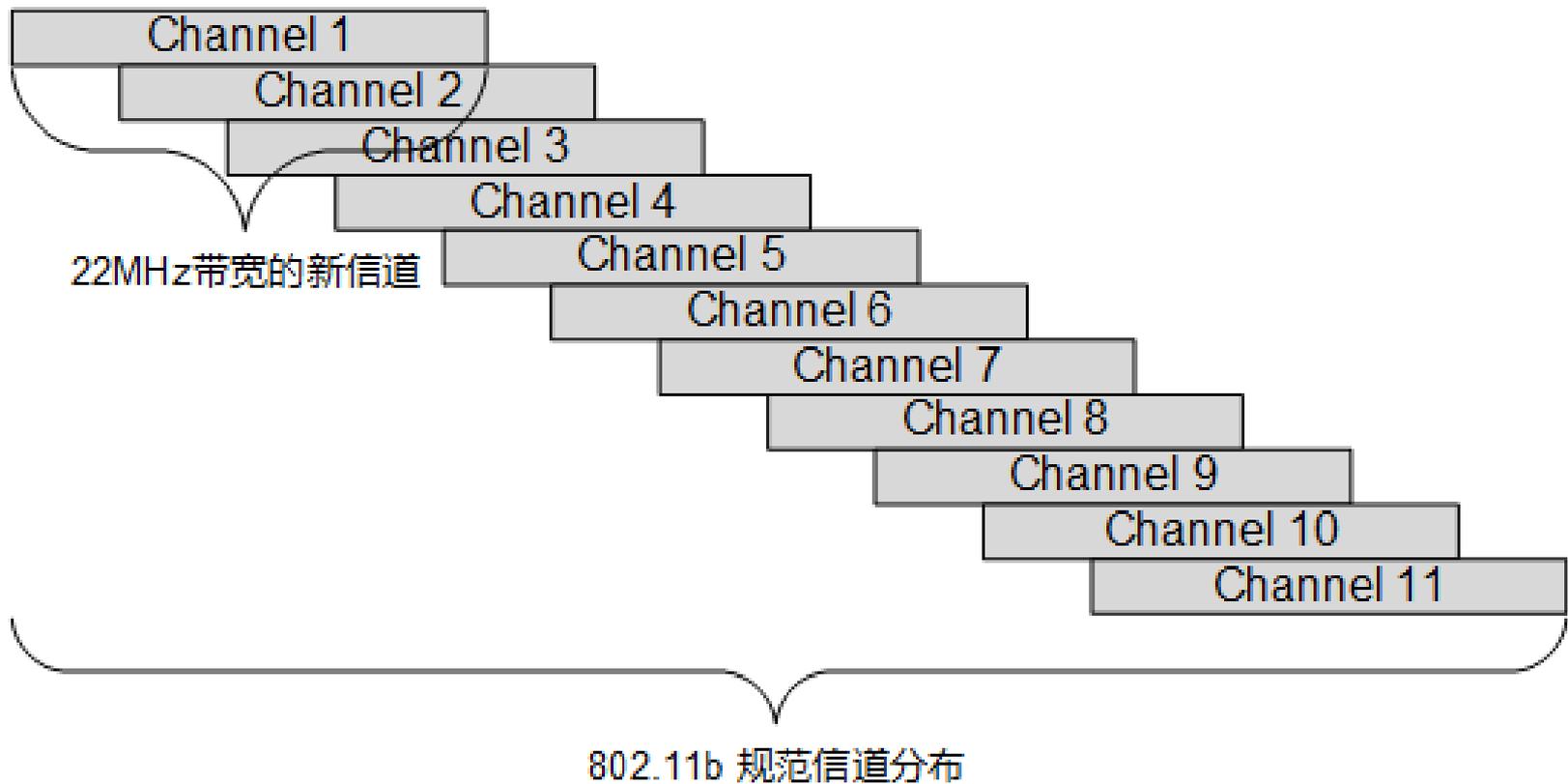
□ 802.11b (1999年)

■ ④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），因为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。

6.无线局域网的标准

□ 802.11b (1999年)



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)

6.无线局域网的标准

□ 802.11g (2003年)

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

- ①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。

- ②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。

6.无线局域网的标准

□ 802.11g (2003年)

■ ③信道划分

IEEE 802.11g规范共划分了13个信道，从前表中可以得出，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。

■ ④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。

⑤安全方面

支持IEEE802.11i标准中的WPA、WPA2、EAP、AES，支持802.1x访问控制技术

6.无线局域网的标准

□ 802.11n (2009年)

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

- ①工作频段

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

- ②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; 在2倍带宽 (40MHz) 和4倍MIMO时, 最高速率为600Mb/s。

6.无线局域网的标准

□ 802.11n (2009年)

■ ③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。另外，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。

6.无线局域网的标准

□ 802.11n (2009年)

■ ④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 (Multiple-Input and Multiple-Output, 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。**

6.无线局域网的标准

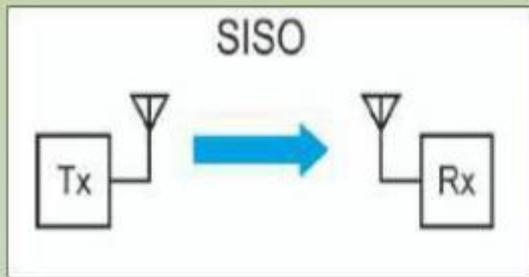
□ 关于MIMO

- 多输入多输出技术（Multiple-Input Multiple-Output, MIMO）是指在发射端和接收端分别使用多个发射天线和接收天线，使信号通过发射端与接收端的多个天线传送和接收，从而改善通信质量。
- 它能充分利用空间资源，通过多个天线实现多发多收，在不增加频谱资源和天线发射功率的情况下，可以成倍的提高系统信道容量，显示出明显的优势、被视为下一代移动通信的核心技术。

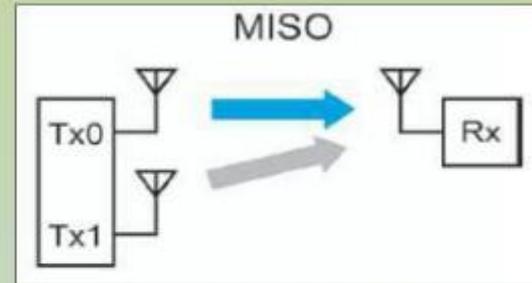
6.无线局域网的标准

□ 关于MIMO

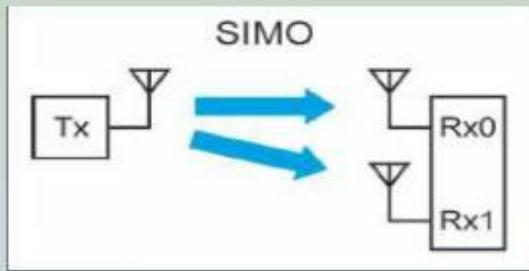
几种传输模型



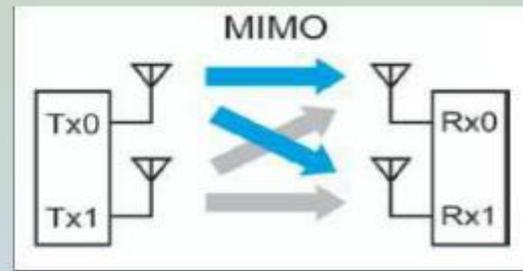
单输入单输出系统



多输入单输出系统



单输入多输出系统



多输入多输出系统

一款无线AP的规格参数



飞鱼星VAP300 300M企业级无线ap吸顶 24V无线覆盖ap接入点 企业酒店AP 送POE供电模块

【京东自营-满499立减40】 30无线带机，配合飞鱼星AC用，WiFi无缝连接

京 东 价：**¥399.00** (降价通知)

促销信息：以下促销可在购物车任选其一

加价购 满99.00元另加199.00元即可在购物车换购热销商品 详情 >>

满减 满499.00减40.00，满999.00减100.00，满1999.00减200.00 详情 >>

配 送 至： **有货**，仅剩5件，支持 99元免运费 | 货到付款

服 务：由 京 东 发 货，并 提 供 售 后 服 务。11:10前完成下单,预计今天(09月29日)送达

无线AP规格

Wan口数量（无线路由）	1个
Qos限速功能	支持
无线桥接	支持
无线传输率	300Mbps
<u>传输标准</u>	<u>IEEE 802.11b/g/n</u>
<u>传输频段</u>	<u>2.4GHz</u>
尺寸	160mm*37mm
重量	0.54kg
电源	24V POE受电(标配供电模块)

802.11n兼容802.11b/g

一款无线无线路由器的规格参数



TP-LINK TL-WR886N 450M无线路由器 (水蓝) WIFI无线穿墙王
【京东自营】百万好评，路由就选TP 450M[TP行车记录仪](#)，[专业安霸A12芯](#)
[护行车安全，点击抢购！](#)

京 东 价：**¥99.00** (降价通知)

促销信息：**加价购** 满29.00另加6.90元，或满39.00另加12.90元，或满49.00另加36.00元，即可在购物车换购热销商品 [详情 >>](#)

配 送 至： **有货**，支持 99元免运费 | 货到付款

服 务：由 京 东 发 货，并提供售后服务。11:10前完成下单,预计今天(09月29日)送达

选择颜色： **【450M旗舰】宝蓝** **【450M旗舰】水蓝** **【全金属机身】**

【千兆有线】450M无线 **【11AC双频新款】1200M**

无线路由器规格

Wan口数量（无线路由）	1个
Lan口数量（无线路由）	4个
无线桥接	支持
天线可拆卸	不支持
无线传输率	450Mbps
传输标准	IEEE 802.11b/g/n
网络协议	TCP/IP协议
尺寸	201mm x 142mm x 34mm（L x W x H）

6.无线局域网的标准

□ 802.11ac (2012年)

- 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。
- ①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。

6.无线局域网的标准

□ 802.11ac (2012年)

■ ②更多的空间流，与MIMO技术结合更有效

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。

6.无线局域网的标准

□ 802.11ac (2012年)

■ ③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。

一款双频无线路由器



【买就返399元】斐讯K2 1200M智能双频无线路由器 WIFI穿墙 PSG1218

【京东自营】“0”元购 买就返399元！白条免息，近92万用户成功提现了！双频 体验高速wifi快感

京 东 价：**¥399.00** (降价通知)

配 送 至： **有货**，支持 99元免运费 | 货到付款

服 务：由 京 东 发 货，供应商提供售后服务。11:10前完成下单,预计今天(09月29)

选择版本：

白条分期：

1 **加入购物车**

温馨提示：1. 本商品不能使用 东券 京券 2. 不支持7天无理由退货

双频无线路由器规格

Wan口数量（无线路由）	1个
Lan口数量（无线路由）	4个
支持WPS	支持
天线可拆卸	不支持
天线增益	5dbi
无线传输率	2.4GHz: 300Mbps, 5G: 867Mbps
传输标准	IEEE 802.11b/g/n/ac
传输频段	2.4GHz, 5GHz
尺寸	168×168×32mm
安全标准	WPA/WPA2-PSK

7.无线局域网的接入认证

7.无线局域网的接入认证

□ 为什么需要认证?

- 认证提供了关于用户的身份保证，这意味着当用户声称具有一个特别的身份时，认证将提供某种方法来证实这一声明是正确的。
- 用户在访问无线局域网之前，首先需要经过认证验证身份以决定其是否具有相关权限，再对用户进行授权，允许用户接入网络，访问权限内的资源。

7. 无线局域网的排

□ SSID的作用



7.无线局域网的接入认证

□ SSID的作用

- 服务集标识符（service set identifier，简称SSID）。SSID用来逻辑分隔无线局域网，防止一个工作站意外连接到邻居AP上，**其实质并不是提供认证服务而设计的。**
- 不过，一个工作站必须配置合适的SSID才能关联到AP上。管理者可以选择将SSID隐藏起来，用这种方法拒绝一些用户接入，从而实现一定的接入控制的功能。
- **存在问题：**由于SSID在AP广播的信标帧中是以明文形式传送的，非授权用户可以轻易得到它；即使在信标帧中关闭了SSID，非授权用户也可以通过监听轮询相应信息来得到SSID，因此，SSID并不能真正提供用户认证。

7.无线局域网的接入认证

□ MAC地址控制

- 在AP的非易失存储器中建立MAC地址控制列表，或者AP可以通过连接到RADIUS服务器来查询MAC地址控制列表，MAC地址不在表中的工作站不允许访问网络资源。
- **存在问题：**
 - （1）非法获取合法用户的MAC，然后修改自身MAC来获取资源访问权限。
 - （2）管理起来很不灵活。例如合法用户更换手机。
- **所以，该功能也不能真正阻止非法用户访问网络资源。**

7.无线局域网的接入认证

□ 802.11的认证方式及其缺陷

- 802.11规定了两种认证方式：开放系统认证和共享密钥认证。
- （1）开放系统认证。根据802.11规范的描述，开放系统认证实质上是空认证，采用这种认证方式的任何用户都可以成功认证并接入WLAN。

7.无线局域网的接入认证

□ 802.11的认证方式及其缺陷

- (2) 共享密钥认证。
- 第2种认证方式是WEP共享密钥身份验证。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。
- WEP推出以后，很快就被安全人员及黑客发现很多漏洞，因此已被802.11i拒用（不建议使用）。

7.无线局域网的接入认证

□ PPPoE接入认证

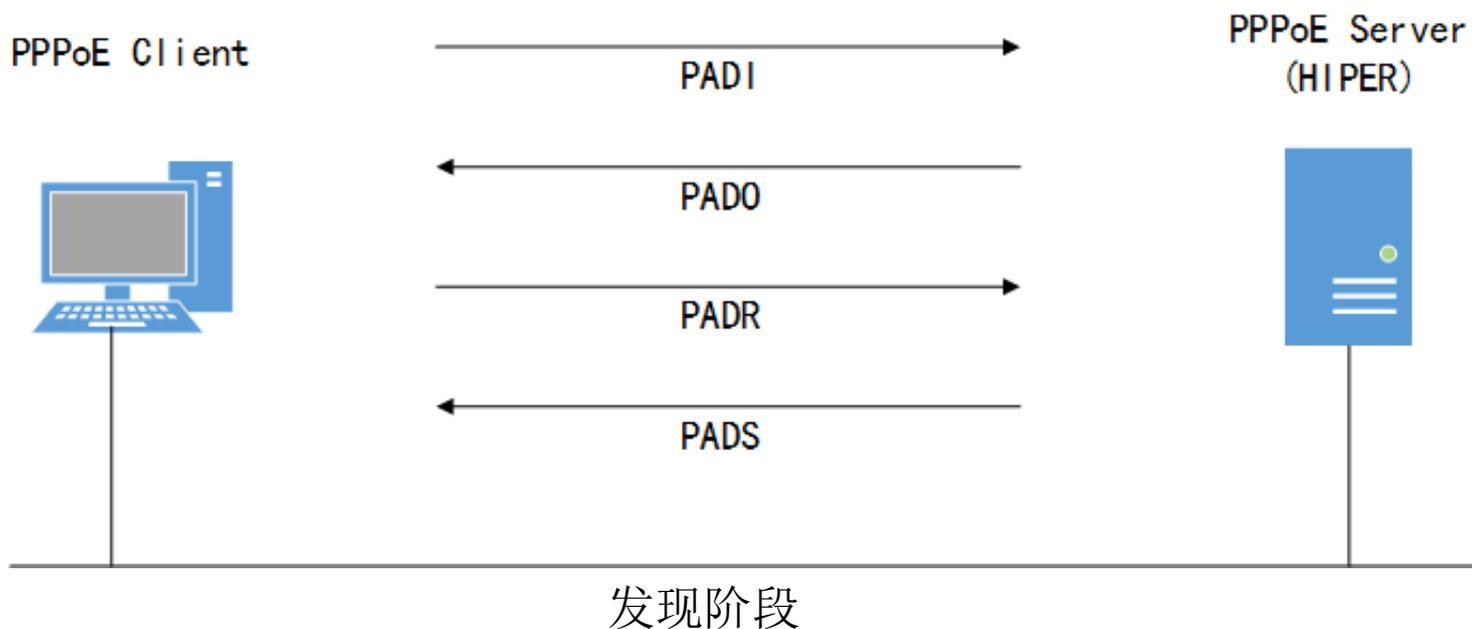
- PPPoE，即以太网上的点对点协议，它可以使以太网上的主机通过一个简单的接入设备连接到Internet上，并对接入的用户进行控制、计费管理。
- PPPoE协议采用Client/Server（客户端/服务器）方式，它将PPP报文封装在以太网帧内，在以太网上提供点对点的连接。

7.无线局域网的接入认证

□ PPPoE接入认证

■ PPPoE连接

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



7.无线局域网的接入认证

□ Web接入认证

- 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。

8. 无线通信常见的加密

8.无线通信加密

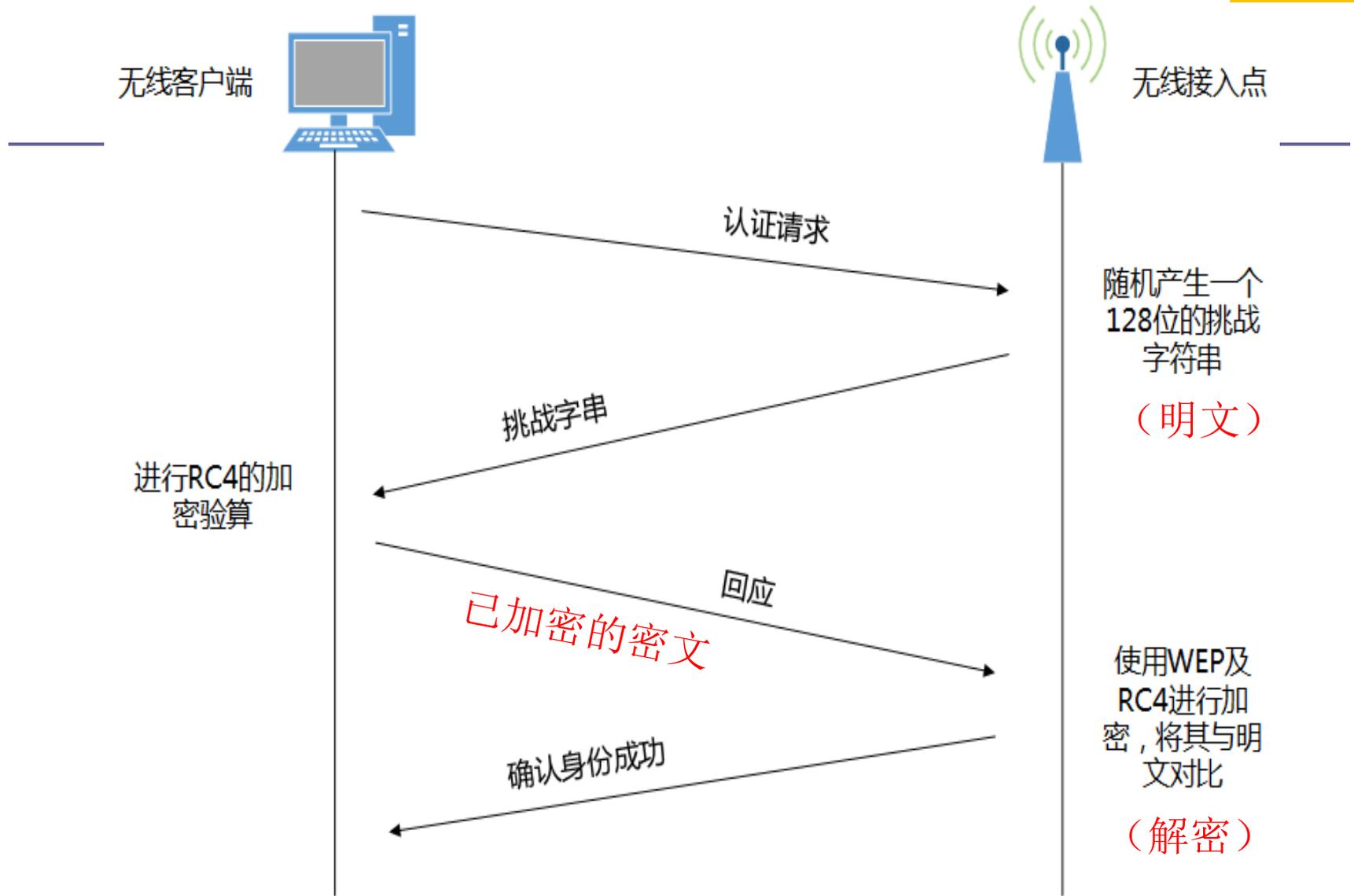
8.1 WEP

- 无线通信常见的加密技术有WEP、AES、WPA-PSK/WPA2-PSK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。

8.无线通信加密

8.1 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拓展到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

8.无线通信加密

8.2 WPA/WPA2

□ 802.11i对802.11安全性的改进

- 由于802.11标准存在公认的安全漏洞，严重威胁到无线局域网的进一步应用。2003年，IEEE又制定了IEEE802.11i标准，以增强IEEE802.11的媒体接入控制功能，改进无线局域网的安全性。
- 802.11i是围绕IEEE 802.1X用户端口身份验证和设备验证制定的，主要包括两项内容：
 - Wi-Fi保护存取（简称 WPA）技术
 - 强健安全网络（简称 RSN）

8.无线通信加密

8.2 WPA/WPA2

- 由于WEP加密技术在安全方面存在缺陷，于是出现了新的WLAN加密技术WPA（Wi-Fi Protected Access，Wi-Fi保护访问）和WPA2。
- WPA/WPA2主要解决WEP在共享密钥上的漏洞，添加了数据完整性检查和用户级的认证措施。

8.无线通信加密

□ WPA加密认证方式

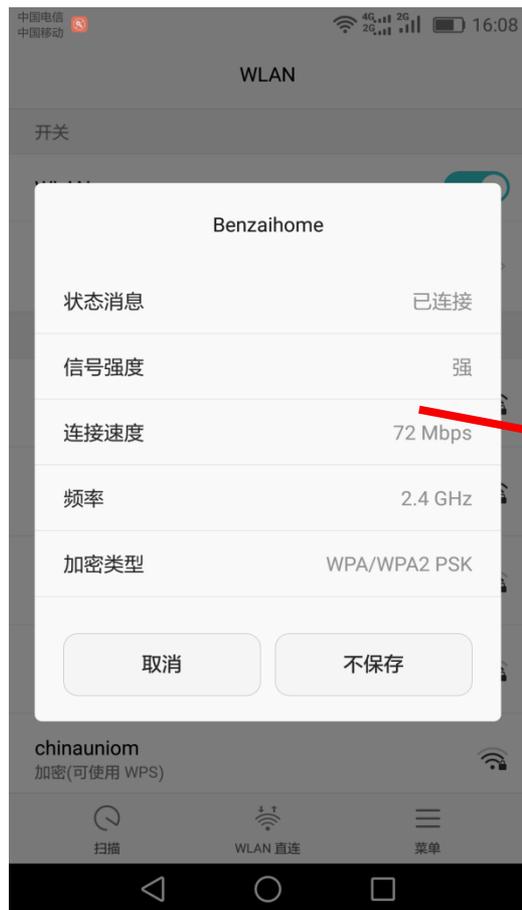
- Wi-Fi联盟给出的WPA定义为： $WPA = 802.1x + EAP + TKIP + MIC$ 。其中：
- 802.1x是指IEEE的802.1x身份认证标准；EAP（Extensible Authentication Protocol，扩展身份认证协议）是一种扩展身份认证协议。这两者就是新添加的用户级身份认证方案。
- TKIP（Temporal Key Integrity Protocol，临时密钥完整性协议）是一种密钥管理协议，即一种加密算法；
- MIC（Message Integrity Code，消息完整性编码）是用来对消息进行完整性检查的，用来防止攻击者拦截、篡改甚至重发数据封包。
- **由此可见**，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。

8.无线通信加密

□ WPA加密认证方式

- WPA2是WPA的后续版本，支持“AES”加密方式。除此之外，与过去的 WPA 相比在功能方面没有大的区别。
- 在WPA的设计中要用到一个 802.1X 认证服务器来散布不同的钥匙给各个用户；不过它也可以用在较不保险的“pre-shared key” (PSK) 模式，让每个用户都用同一个密语。Wi-Fi联盟把这个使用 pre-shared key的版本叫做WPA个人版或**WPA2 个人版**，用802.1X认证的版本叫做WPA 企业版或WPA2 企业版。

查看手机连接WLAN的加密认证方式



8.无线通信加密

8.2 WPA/WPA2加密认证

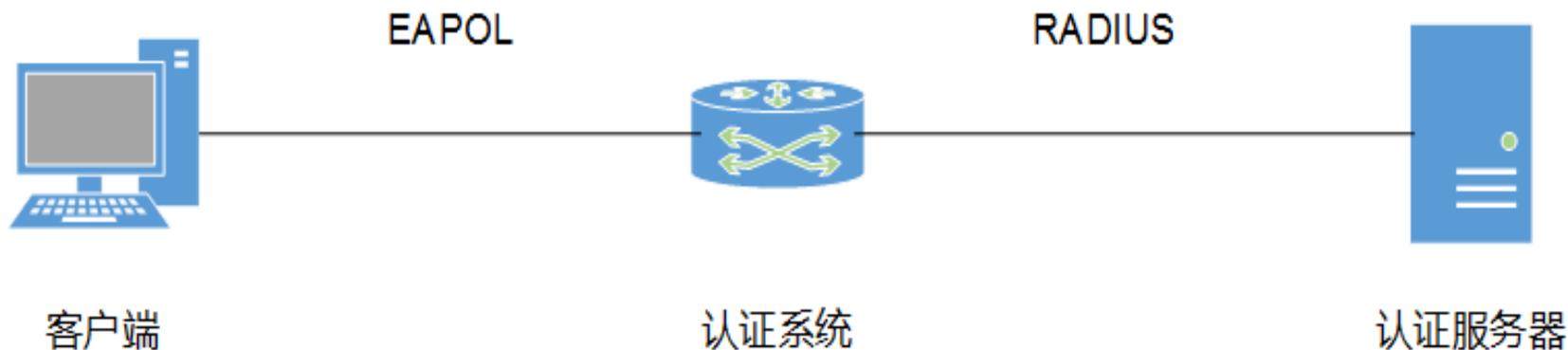
□ WPA/WPA2中的IEEE 802.1x身份认证系统

- 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。

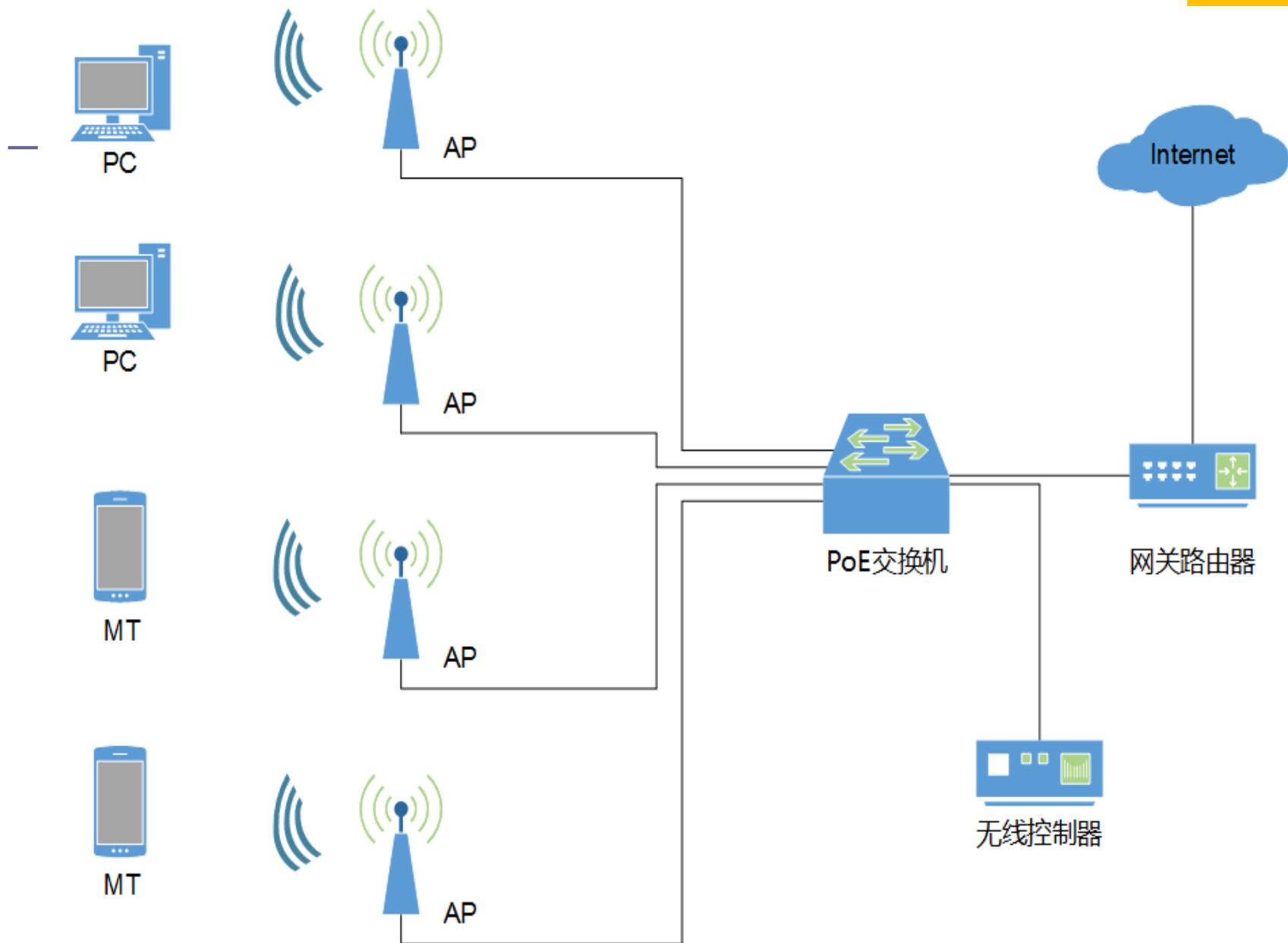
8. 无线通信加密

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)



8.实践：企业无线局域网的实现



8.实践：企业无线局域网的实现

□ 思考几个问题

- 为什么需要使用PoE交换机？
- 为什么需要使用无线控制器？
- 为什么要采用多AP模式？
- 每个AP中设置的SSID和密码是否需要一样？
- 本实验中，接入AP时采用的加密认证方式是什么？
- 每个AP采用的信道一样吗？
- 描述一下一部手机接入WLAN的过程。

第9讲 无线局域网

完