# 无线网络安全

# 无线网络简介




# 无线网络分类

## 无线网络

### 无线个域网（Wireless Personal Area Network, WPAN）

传输距离：10m左右
典型技术：
IEEE 802.15 (WPAN)
Bluetooth（蓝牙）
ZigBee
传输速率：
10Mbit/s

### 无线局域网（Wireless Local Area Network, WLAN ）

传输距离：
几十米~几千米
典型技术：
IEEE 802.11（a,b,g,i,n）
传输速率：
11~300Mbit/s

### 无线城域网（Wireless Metropolitan Area Network, WMAN）

传输距离：城市大部分地区
典型技术：
IEEE 802.16（WiMAX）

*:有的分类也将其作为3G 标准之一

### 无线广域网（Wireless Wide Area Network, WWAN）

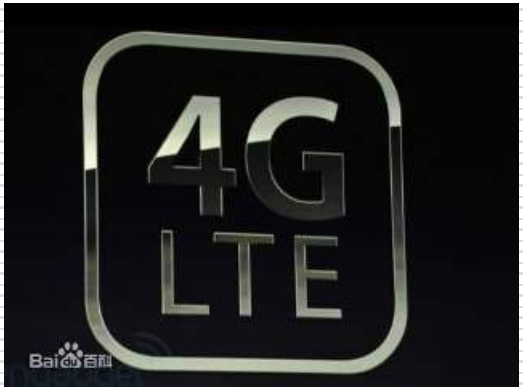
主要是通过移动通信卫星进行数据通信的网络
典型技术：
IEEE 802.20（MBWA，移动宽带无线接入系统）
3G 4G
传输速率：
2Mbit/s

# 无线网络安全

- 缺乏安全性是许多公司和用户不愿安装无线网络的重要原因之一
  - 有线网络: 数据流从电缆的一点传送到另一个点，安全是物理访问问题
  - 无线网络: 在空中发送数据，为中途拦截信号提供了机会
  - 当我们期望更宽、更广的传输范围时，这个范围经常已经超出了我们的建筑物和住宅的尺寸，而且RF信号能够穿透墙壁

# 无线网络安全

- 3G(4G)时代的到来给我们带来新的挑战
  - ✓ 手机通话内容被监听、收条短信电话簿就被盗取、下载音乐却让手机中了病毒……面对这些时常让手机用户头疼的问题，中国工程院副院长、院士邬贺铨，在第十一届中国科协年会“信息化与转型”学术研讨会上语出惊人地指出：手机安全问题正面临严峻的挑战，而且随着手机上网的普及，这一现象还将日趋严重

# 无线局域网简介

- 无线局域网络(Wireless Local Area Networks；WLAN)是相当便利的数据传输系统，它利用射频（Radio Frequency； RF）的技术，取代旧式碍手碍脚的双绞铜线（Coaxial）所构成的局域网络，使得无线局域网络能利用简单的存取架构让用户透过它，达到“信息随身化、便利走天下”的理想境界。
- WLAN标准：IEEE 802.11

# IEEE 802.11

| 标准 | 数据速率 | 调制方式 | 射频频段 | |
|---|---|---|---|---|
| 802.11 | 1Mbps | 二进制移相键控BPSK | 红外（IR）或2.4GHz | |
| 802.11 | 2Mbps | 正交移相键控QPSK | | |
| 802.11b | 5.5Mbps | QPSK | 2.4GHz | 802.11高速率/Wi-Fi（无线高保真） |
| 802.11b | 11Mbps | QPSK | | |
| 802.11a/g | 54Mbps | 正交频分复用OFDM | 5GHz(a)<br>2.4GHz(g) | 802.11g与802.11b兼容 |
| 802.11n | 300Mbps~600Mbps | MIMO（多入多出）与OFDM技术相结合 | 2.4GHz/5GHz | 兼容802.11b/g |

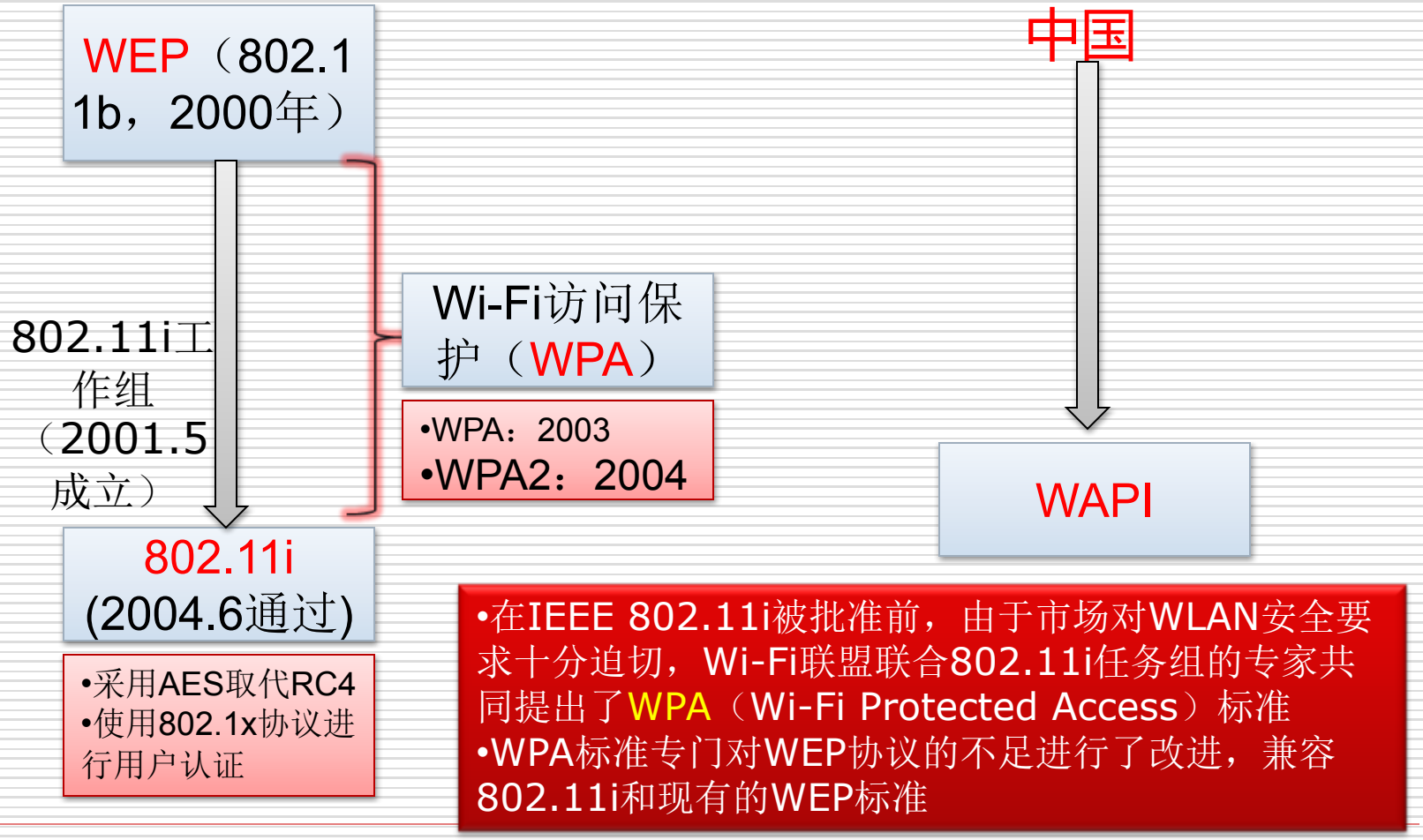
# 802.11网络的两个基本构件

- 无线局域网网络有两个基本构件——站和无线接入点

- 站（Station，STA）
- 站是无线网的端头设备，例如笔记本、掌上电脑等。通常是通过计算机加一块无线网卡构成的。

- 无线接入点（Access Point，AP）
- AP将STA与DS相连，典型的DS是某单位的有线网络，AP也可在不访问DS情况下将多个STA相连。

# 802.11安全体系


WEP（802.11b，2000年）
802.11i工作组（2001.5成立）
802.11i
(2004.6通过)
•采用AES取代RC4
•使用802.1x协议进行用户认证
Wi-Fi访问保护（WPA）
•WPA：2003
•WPA2：2004
中国
WAPI
•在IEEE 802.11i被批准前，由于市场对WLAN安全要求十分迫切，Wi-Fi联盟联合802.11i任务组的专家共同提出了WPA（Wi-Fi Protected Access）标准
•WPA标准专门对WEP协议的不足进行了改进，兼容802.11i和现有的WEP标准

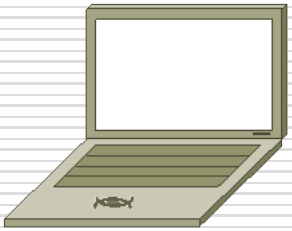
# 802. 11的认证机制

- IEEE 802.11定义了两种认证方式：

- 开放系统认证(Open System Authentication)
  - 默认的认证机制
  - 认证以明文形式进行
  - 适合安全要求较低的场所
- 共享密钥认证(Shared Key Authentication)
  - 可选的认证机制
  - 必须能执行WEP

# 开放系统认证

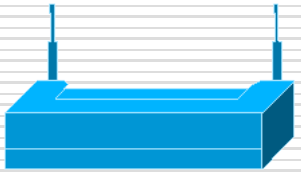
- 一般而言，凡使用开放系统认证的工作站都能被成功认证（空认证）
- 认证过程只有两步：
  - 认证请求
  - 认证响应



请求帧

•验证算法标识=“开放系统”

•验证处理序列号=1



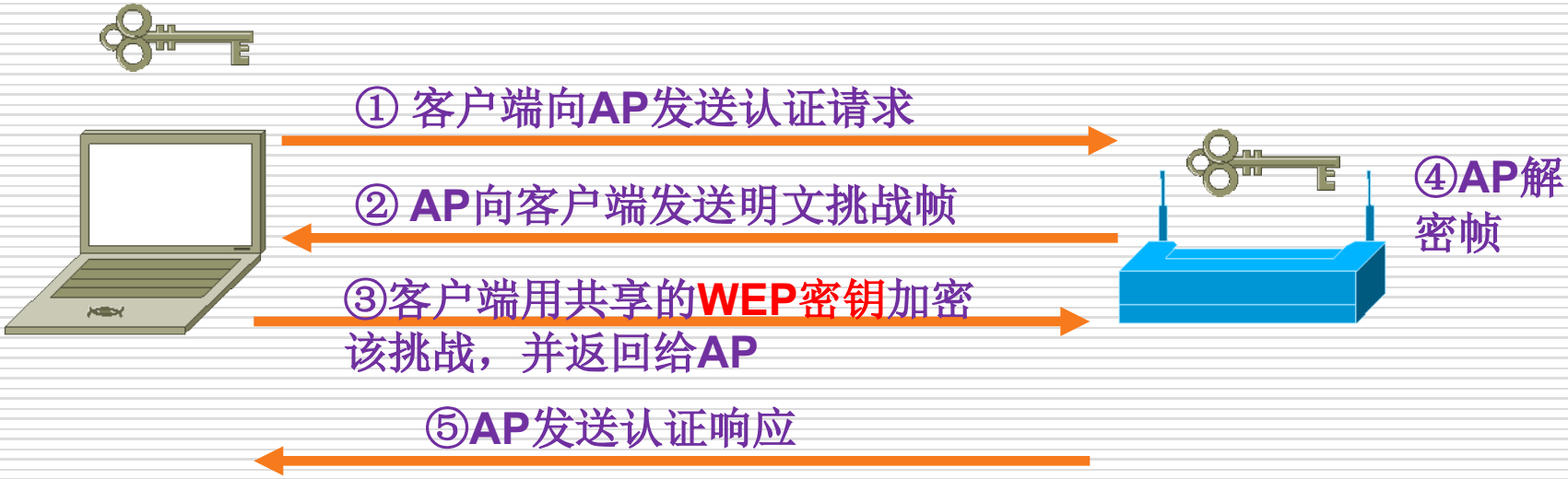
验证帧

•验证算法标识=“开放系统”

•验证处理序列号=2

•验证请求的结果

# 共享密钥认证




- 802.11提供的是单向认证：
  - 只认证工作站的合法性
  - 没有认证AP的合法性