目录

第一章 移动计算技术概述

1.1 什么是移动计算？

- 移动计算是一个全新的概念，至今没有标准的定义。

  移动计算是基于无线通信技术和便携式移动计算设备的分布式计算模式。

  A technology that allows transmission of data, via a computer, without having to be connected to a fixed physical link.

  WWW： World-Wide Web

  Web Without Wires ？!

- 移动计算 = 分布计算技术 + 移动通信 + 数据库技术

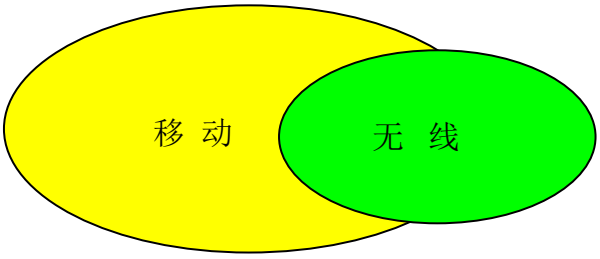
- 移动计算 = 无线计算 ？

  (Mobile Computing) (Wireless Computing)

  Wireless Computing： 无线的, 并且很可能是在线的.

  Mobile Computing： 很可能是离线的.

  虽然无线网络和移动计算通常联系在一起，但二者有区别。



- 移动计算的 Buzzwords
  - 无线计算（Wireless Computing）
  - 无限计算（Always on Computing）
  - 漫游计算（Nomadic Computing ）

- 泛化计算（Pervasive Computing Ubiquitous Computing Untethered (无范围的)）
- 嵌入计算（Embedded Computing）

- 个人移动性

  一个用户在包括固定网络和移动网络在内的整个网络系统中，移动到任何地理位置，用唯一 ID 号，使用任何终端接入网络，并得到网络业务服务的能力，该能力包括对其所使用终端的定位及相关路由、计费等。

- 终端移动性

  终端移动性是指一个终端从不同位置或从移动接入网络识别并定位该终端的能力。

1.2 移动计算基本特点

- 有限的带宽—蜂窝通信系统波特率 9.6Kbps，IMT-2000 144 Kbps 到 EDGE 300Kbps，远远低于固定网络中的铜缆或光纤通信的速率。
- 移动性—必须适应不同地点的连接请求，并且经常在移动时要求保持连接；在不同服务器覆盖范围之间移动，越区切换比较常见。
- 可靠性—由于其便携性和工作环境，可靠性更低，更容易受到干扰而出现网络故障。可能长时间地域网络断接，一些假设条件不同于传统的分布系统。移动计算装置也有一些潜在的不安全因素，如碰撞、磁场干扰、易于遗失和失窃等。
- 安全性
- 与位置相关 - 应用程序可能与位置相关，移动导致位置的不断变换。
- 有限的电源能力—通过蓄电池供电，但容量非常有限，一般只能维持 2～5 个小时，而计算密集型程序能源耗更大。
- 频繁断接性—移动计算机在移动过程中，一般不采用保持持续联网的工作方式，而是主动/被动地间歇性入网、断接和重接，甚至越区切换。

- 非对称性¯包括通信与资源安全乃至 QoS 的非对称性，访问的是地理上分布的异构节点。由于电源能力的限制，移动设备上的资源与功能有限。
- 复杂性—为支持移动性必须加入更多的功能并最终达到网络负载均衡；移动性也必然要求跨软硬件平台的兼容性。

1.3 移动计算系统组成

- 移动计算系统特征：

  1. 移动性：不同地点的连接请求, 移动时保持连接;
  2. 主动与被动的断接与重接;
  3. 网络条件的多样性;
  4. 能源限制;
  5. 通信的非对称性 （ 用户规模，安全鉴别 ）

- 移动计算环境组成

  由固定它是传统的固定网络、移动网络、无线通信、移动终端设备以及移动着的用户构成。

  网络分布计算环境利用了先进无线通信技术后的扩充。

- 移动计算环境的基本特征

  1. 大多数移动终端设备相对便宜，便携，并且易于使用;
  2. 移动计算的解决方案应该包括有线和无线两个方面;
  3. 通信服务器和后台服务器要在同一硬件平台上。

- 移动计算的硬件环境

  1. 移动终端

  便携笔记本电脑、基于笔输入的计算机、掌上电脑、PDA、寻呼机、PDA/寻呼机、PDA/电话机、移动打印机、移动传真机、移动扫描仪等。

2. Modem/无线网卡或其他数字网络接口设备

交换网络 Modem，蜂窝拨号适配器或 ISDN 拨号适配器，或特殊的无线网络接口，如 ARDIS，RAM，CDPD

目前，能适应所有无线连接形式的统一 Modem 还没有产品。

3. E-mail 服务器

4. 通信服务器和无线交换机（网关）

如 Shiva 的 NetRover 用于异步网络传输，TEKnique 的 TX-5000 用于无线网关。它们的功能包括：

异步有线会话，连接与断接服务，话路路由管理，移动标志，网络安全管理，异步无线网络连接与断接服务，协议转换（网关功能）。

5. 应用和/或数据服务器

通常通信服务器与应用/数据服务器之间以局域网相连，这种连接也可以用高速总线或者广域网中的私用线路完成。

- 移动通信系统

包括:

  - 低功率通信系统
  - 移动卫星系统
  - 无线 LAN/WAN
  - 专用移动通信系统
  - 寻呼系统
  - 数字蜂窝系统

- 掌上电脑、智能手机进入发展新阶段

  - 芯片种类更多，速度更快。

CPU 是 INTEL、TI、Motorola 三足鼎立。主频 533～100MHZ。基于 Strong ARM 架构的芯片为中低端产品采用，将陆续退出市场，基于 Xscale 机构的 PXA250 PXA255, PXA260 系列将逐渐成为主流。产品如 Dell

AximX5、iPAQ 3970，联想 XP618、SONY NX73V、NX80V。SONY 03 年 9 月推出自己 CPU（SONY Handheld Engine）的 Clie UX40 和 UX 50。

- 屏幕配置更高。

屏幕已完成从 4096 色到 65536 色（TFT LCD） 分辨率： 240×320 或 320×320。

- 操作系统更强、应用软件更全面。

预装微软 POCKET PC2003 操作系统，采用新的系统内核（新的 GUI 界面、工具软件、帮助软件和应用软件等），较 PPC2002 在 Wi-Fi 和多媒体功能上有加强。Palm 与 Clie UX40 等采用 Palm 5.0 操作系统。在智能手机方面，除常见的掌上电脑操作系统之外，还有 Symbian 和微软 Smartphone 操作系统，它们将手机功能、无线互连功能和娱乐功能有机结合起来。装有以上操作系统的智能手机如 SONY Erricson P802， DopOD 515 等。

- 外设接口更全。

目前采用较多的是 MMS/SD 或者 CF 接口。SONY 系列掌上电脑则采用了 Memory Stick。 有的机型如 ASUSA 620 则采用了 SD/CF 双接口。新的接口也层出不穷，如存储卡、USB、IEEE 1394 a/b、键盘、GPRS、GPS 等。

- 移动计算设备的电池问题

  - 锂电池连续工作时间仍然是有限的，目前大约是 3～5 小 时。而且未来 5 年这种情况将不会有大的改善。

  - 燃料电池：

在笔记本计算机燃料电池开发方面，日本和德国厂商领先。2003 年 3 约东芝公司醇燃料电池，平均输出功率为 12 瓦，最大输出功率可达 20 瓦，可以连续工作 5 个小时以上，计划于 2004 年投产。NEC 公司 2003 年 6 月也推出醇燃料电池，平均功率为 14 瓦，最大达 34 瓦，可驱动平均耗电量为 12 瓦的笔记本连续工作 5 小时，即将推出可连续工作 40 小时的醇燃料电池。德国 Masterflex 与 Smartfuel Cell 公司也计划于 2004 年推出氢燃料电池与醇燃料电池。

- 移动计算软件

（1）移动客户软件

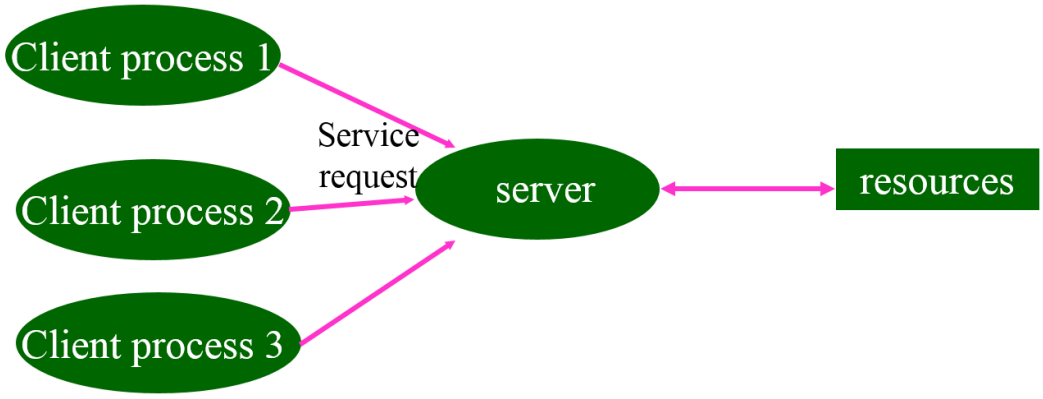
（2）移动通信服务器/交换机

（3）软件应用和/或数据服务器软件

- 移动客户软件
  - 操作系统、网络软件和各种移动终端驱动程序 (如: WinCE, PalmOS, Nokia 等开发的无线操作系统 EPOC）
  - 用户界面
  - 通信服务器软件的客户机部分
  - 传输层软件，如 TCP/IP
  - 传输层与应用层之间的中间件
  - 特殊的无线网络的驱动程序
  - 手写体与声音识别软件
- 移动通信服务器/交换机软件
  - 远程用户的连接确认
  - 通信端口管理
  - 安全验证
  - 单一逻辑信道
  - 多物理连接的多线程管理
  - 通信协议管理
  - 与后台应用服务器或数据库系统的逻辑连接
- 应用和/或数据库服务器软件
  - 基于局域网的数据库服务，如 Windows、
  - UNIX 下的 SYBASE、ORACLE、SQL 数据库。
  - 基于小型机的服务，如 AS/400
  - 基于大型机的服务

1.4 移动计算模型

- 传统分布式 Client/Server 模型



- 移动环境 Client/Server Model

  经典 Client/Server Models 必须扩充以支持断接操作，适应移动网络的弱连接性。

  - 服务器（功能）在固定网络多处复制以备不时之需；
  - 断接时，移动节点机可能需要模拟服务器的功能；
  - Client 与 Server 的信息交换： 远程过程调用（RPC） - 含异步 RPC
  - 其他优化（过滤、压缩等）技术
  - 对于轻载应用或 Client 不可靠情形，可转移部分功能到固定网络。

- Client/Agent/Server Model

  - 该模型为三层模型，将移动客户机部分功能转至固定网络的代理 Agent (亦称 Proxy)。代理将移动终端与网络服务器的相互作用一分为二。客户机提出要求之后，可进入睡眠状态，甚至断接状态。Agent 的基本功能是消息的管理，在此基础上增加与应用相关的功能 ，例如， 压缩、调整发送次序、打包等。
  - 对于轻载移动客户机比较合适；
  - 代理可作为多个移动终端的全权代表(Surrogate);

- 代理既可以作为服务器的全权代表，也可以只具备部分特定功能，这样客户机可以连接到具有连接到具有特定功能的代理，如数据库代理、Web 浏览器代理。

代理为移动用户服务，当用户激活代理后，由代理完成移动用户要求的服务，用户可以继续移动甚至断接，当代理完成任务并且重新建立连接后，代理再把结果报告给用户。

（1）使得自动通信成为可能，可以在任意时间提供信息

（2）降低了开销，因为代理工作时，用户可以关机

（3）提高了用户的工作效率

（4）利用了 C/S 和存储-转发的优点

（5）控制分解

- Client/Intercept/Server Model
  - 该模型为双代理模型，即代理成对出现。客户端代理(CSI)作为本地服务器代理运行在移动终端；而服务器端代理作为移动终端代理运行在服务器(SSI) 。
  - C/I/S 模型对于移动客户机和服务器均透明；
  - 代理主要作为 Cache 起作用，提供了断接处理的灵活性。
  - 对于重载客户（特别是计算功能强且有 Cache）比较合适；
  - 用于克服 C/A/S 模型不足，比较适合于弱连接性场合；
  - 主要不足：每一类移动网络应用都需要修改客户和服务器。
- P2P Model
  - 客户、服务器并不清晰区分，在环境中地位相同。服务器在移动状态下，亦需要经常性关机以节省能源；
  - 各种节点地位与能力相当，其间进行信息与服务的交换，分布式控制方案；
  - 在服务器一端需要设置 Agent 以适应断接与弱连接性；

- 主要任务: 强大的搜索与检索功能，对于点播类型任务而不适合于实时任务；
- 适合重载客户；
- 典型系统: Gnutella, Napster, and Morpheus.

- Mobile Agent Model

软件 Agent 技术最早可以追溯到人工智能研究初期阶段，1977 年 Hewitt 在研究 Concurrent Actor Model 时就首次提出了具有自组织性、反应机制和同步执行能力的软件模型，这就是最初的软件 Agent 思想。此后从 70 年代末到 90 年代初，科学家都将精力集中于对软件 Agent 理论的研究，并从系统的角度提出了一些基本概念。软件 Agent 的具体实践开始于 90 年代，期间人们进行了一些非常成功的尝试（如 Pleiades，ARCHON 计划等），并对软件 Agent 有了进一步的认识。

移动代理是一种能够在异构的计算机或移动网络上的结点之间自主迁移的程序。它能够自主选择何时迁往何地；在执行的任意一点将自己挂起，然后自主迁移到另一节点上，并在到达新地点之后唤醒自己继续执行；

还可以通过克隆自己或者产生子代理散布到多个节点上，每个代理均以自治，必要时以相互合作的方式共同完成更为复杂的任务。支持断接性与互操作性是其主要的优点，即使断接时，其他节点就可以从移动代理处访问到原节点的数据。

其他好处还包括减少网络延迟，支持轻载移动设备；代理执行可以独立于发送节点，其异步信息搜索与数据访问能力是其他模型所不具备的。

传统代理模型中的 Agent 可视作一个静态代理，因为它不能动态迁移到其他服务器上去。

- 移动 Agent:

■ 由于对 Agent 的定义还没有明确，所以，目前还没有一个关于移动 Agent 的确切的定义。一般认为移动 Agent 是一类能在自己控制之下从一台计算机移动到另一台计算机的自治程序，并可与其它 Agent 或资源交互的软件实体。它们能为分布式应用提供方便的、高效的和鲁棒的执行框架。

■ 上世纪 90 年代初，General Magic 公司在推出其商业系统 Telescript 时第一次提出了移动 Agent 的概念，它除了具有软件 Agent 的基本特性--自治性、

响应性、主动性和推理性外，还具有移动性，即它可以在网络上从一台主机自主地移动到另一台主机，代表用户完成指定的任务。

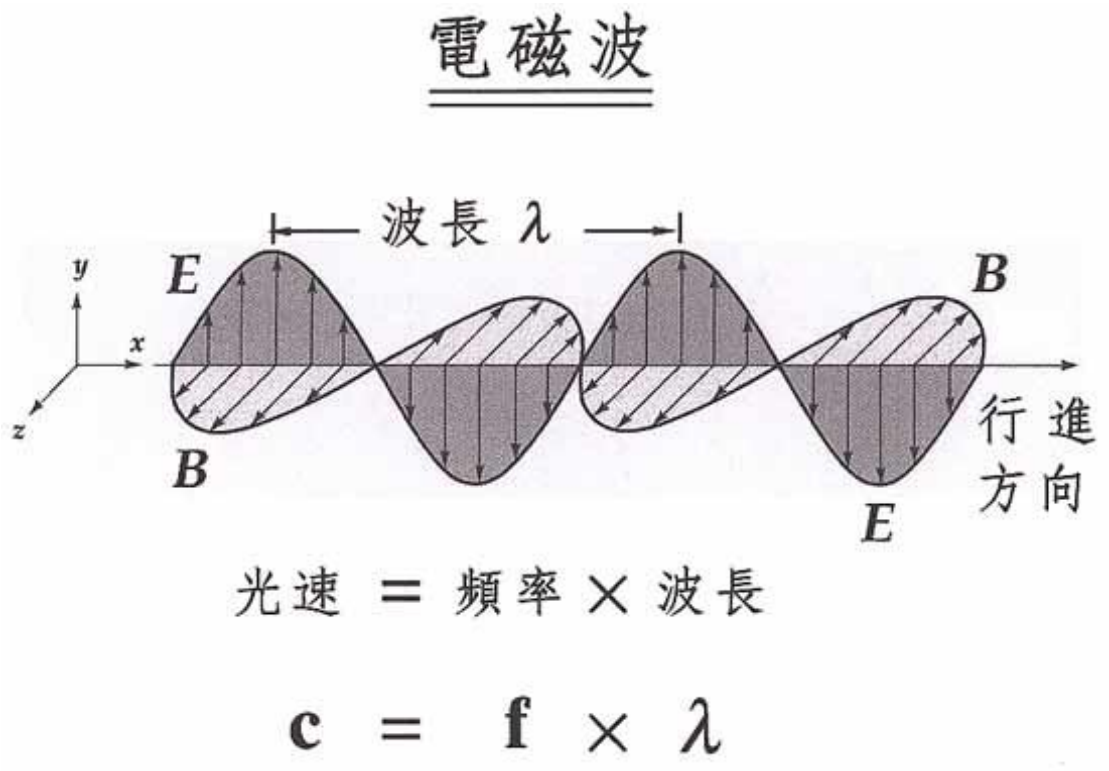
■ 目前，移动 Agent 的研究已取得了一些成就，产生了较多的移动 Agent 原型系统，如 Open Group 公司的 MOA、Stuttgart 大学的 Mole、Ochanomizu 大学的 MobileSpaces 等。

■ 但它们还都很不成熟，存在着各种各样的缺陷。可以把目前的众多 Agent 系统看成是实验室的系统，离真正实用的产品还有很大的距离。

第二章 无线通信与网络基础

2.1 概 述

- 无线通信基础



- 多径效应

由于多径传播，造成多径信号的幅度、相位和到达时间不同，它们相互叠加会产生电平衰退(fading)和时延扩展，产生附加的调频噪声，出现接收信号失真。

- 阴影衰退

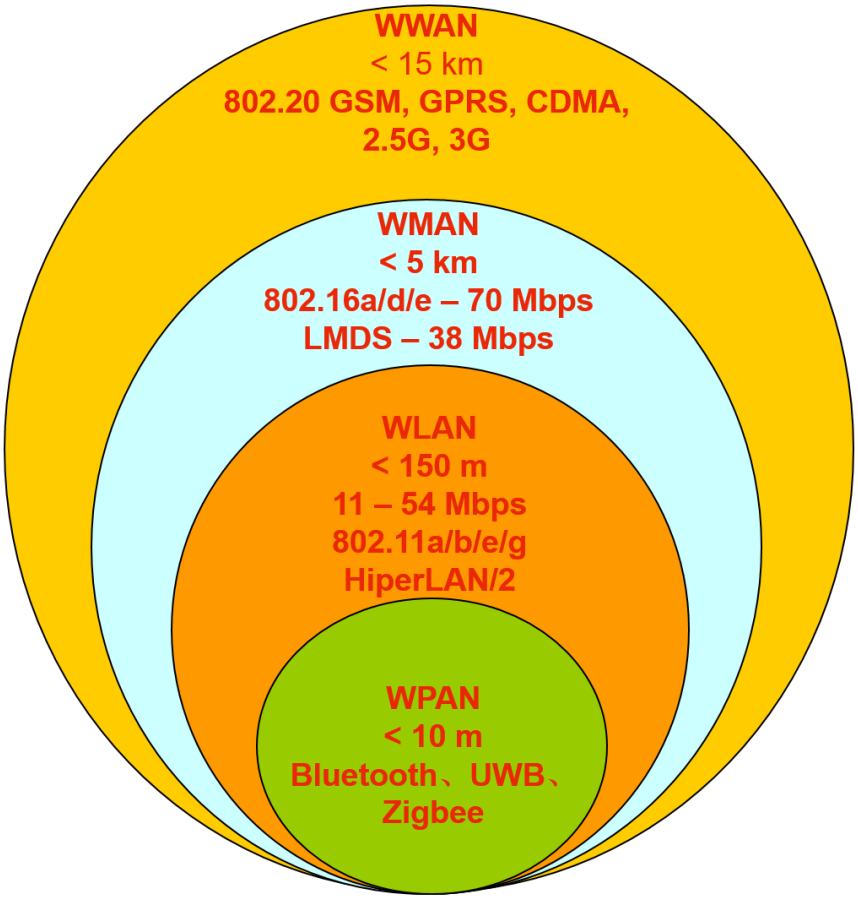
  由地形、地物、气象等原因对电磁波的遮蔽引起，由此引起的衰退为慢衰退。 接收到的信号平均功率发生变化，且是缓慢的变化。

  快衰退和慢衰退随着移动台的移动而产生变化，这二者构成移动通信接收信号不稳定的因素。

- 多普勒（Doppler）效应

  由于移动台与基站的相对运动引起接收信号的附加频率变化，距离越近，附加频率越高。

- 视距通信(LOS)
  - Line of Sight
  - 发射天线与接收端间无障碍物。
- 无线网络分类



2.2 无线局域网 WLAN

2.2.1 无线局域网的组成

- 与接入点 AP 建立关联(association)
  - 一个移动站若要加入到一个基本服务集 BSS，就必须先选择一个接入点 AP，并与此接入点建立关联。
  - 建立关联就表示这个移动站加入了选定的 AP 所属的子网，并和这个 AP 之间创建了一个虚拟线路。
  - 只有关联的 AP 才向这个移动站发送数据帧，而这个移动站也只有通过关联的 AP 才能向其他站点发送数据帧。
- 移动站与 AP 建立关联的方法

- 被动扫描，即移动站等待接收接入站周期性发出的信标帧(beacon frame)。
- 信标帧中包含有若干系统参数（如服务集标识符 SSID 以及支持的速率等）。
- 主动扫描，即移动站主动发出探测请求帧(probe request frame)，然后等待从 AP 发回的探测响应帧(probe response frame)。

- 热点(hot spot)
  - 现在许多地方，如办公室、机场、快餐店、旅馆、购物中心等都能够向公众提供有偿或无偿接入 Wi-Fi 的服务。这样的地点就叫做热点。
  - 由许多热点和 AP 连接起来的区域叫做热区(hot zone)。热点也就是公众无线入网点。
  - 现在也出现了无线因特网服务提供者 WISP (Wireless Internet Service Provider)这一名词。用户可以通过无线信道接入到 WISP，然后再经过无线信道接入到因特网。

- 移动自组网络 (ad hoc network)

自组网络是没有固定基础设施（即没有 AP）的无线局域网。这种网络由一些处于平等状态的移动站之间相互通信组成的临时网络。

- 移动自组网络的应用前景
  - 在军事领域中，携带了移动站的战士可利用临时建立的移动自组网络进行通信。
  - 这种组网方式也能够应用到作战的地面车辆群和坦克群，以及海上的舰艇群、空中的机群。
  - 当出现自然灾害时，在抢险救灾时利用移动自组网络进行及时的通信往往很有效的，

- 无线传感器网络 WSN
  - 由大量传感器结点通过无线通信技术构成的自组网络。

- 无线传感器网络的应用是进行各种数据的采集、处理和传输，一般并不需要很高的带宽，但是在大部分时间必须保持低功耗，以节省电池的消耗。
- 由于无线传感结点的存储容量受限，因此对协议栈的大小有严格的限制。
- 无线传感器网络还对网络安全性、结点自动配置、网络动态重组等方面有一定的要求。

- 无线传感器网络主要的应用领域
  - 环境监测与保护（如洪水预报、动物栖息的监控）；
  - 战争中对敌情的侦查和对兵力、装备、物资等的监控；
  - 医疗中对病房的监测和对患者的护理；
  - 在危险的工业环境（如矿井、核电站等）中的安全监测；
  - 城市交通管理、建筑内的温度/照明/安全控制等。
- 移动自组网络和移动 IP 并不相同
  - 移动 IP 技术使漫游的主机可以用多种方式连接到因特网。
  - 移动 IP 的核心网络功能仍然是基于在固定互联网中一直在使用的各种路由选择协议。
  - 移动自组网络是将移动性扩展到无线领域中的自治系统，它具有自己特定的路由选择协议，并且可以不和因特网相连。
- 几种不同的接入
  - 固定接入(fixed access)——在作为网络用户期间，用户设置的地理位置保持不变。
  - 移动接入(mobility access)——用户设置能够以车辆速度移动时进行网络通信。当发生切换时，通信仍然是连续的。
  - 便携接入(portable access)——在受限的网络覆盖面积中，用户设备能够在以步行速度移动时进行网络通信，提供有限的切换能力。

- 游牧接入(nomadic access)——用户设备的地理位置至少在进行网络通信时保持不变。如用户设备移动了位置，则再次进行通信时可能还要寻找最佳的基站

- 802.11 无线局域网
  - 80 年代，以太局域网迅猛发展，但当时无线网遵循 IEEE 802.3 标准，存在着易受其他微波噪声干扰，性能不稳定，传输速率低且不易升级，不同厂商产品不兼容等弱点。
  - 制定有利于无线网自身发展的标准。目前，WLAN 主要是 IEEE 802.11x 系列与 HiperLAN / x 系列两种标准。 1997 年 6 月，IEEE 802.11 标准通过。
  - 典型 WLAN 环境中，接入点(AP)进行数据发送和接受，一个 AP 能够在几十～上百米的范围内连接多个无线用户。在有有线和无线网络的情况下，AP 可以通过标准的 Ethernet 电缆与有线网络相连。
- IEEE WLAN 标准

IEEE 802.11 标准主要对 PH 和 MAC 层进行了规定，其中 MAC 层是重点。各厂商产品在同一物理层上可以互操作，逻辑链路控制层(LLC)是一致的，即 MAC 层以下对网络应用是透明的。

2.2.2 802.11 局域网的物理层

- 802.11 无线局域网可再细分为不同的类型。
- 现在最流行的无线局域网是 802.11b，而另外两种（802.11a 和 802.11g）的产品也广泛存在。
- 802.11 的物理层有以下几种实现方法：
  - 直接序列扩频 DSSS
  - 正交频分复用 OFDM
  - 跳频扩频 FHSS （已很少用）
  - 红外线 IR （已很少用）
- 几种常用的 802.11 无线局域网

标准	频段	数据速率	物理层	优缺点
802.11b	2.4 GHz	最高为 11 Mb/s	HR-DSSS	最高数据率较低，价格最低，信号传播距离最远，且不易受阻碍
802.11a	5 GHz	最高为 54 Mb/s	OFDM	最高数据率较高，支持更多用户同时上网，价格最高，信号传播距离较短，且易受阻碍
802.11g	2.4 GHz	最高为 54 Mb/s	OFDM	最高数据率较高，支持更多用户同时上网，信号传播距离最远，且不易受阻碍，价格比 802.11b 贵

2.2.3 802.11 局域网的 MAC 层协议

无线局域网不能简单地搬用 CSMA/CD 协议。这里主要有两个原因：

- CSMA/CD 协议要求一个站点在发送本站数据的同时，还必须不间断地检测信道，但在无线局域网的设备中要实现这种功能就花费过大。
- 即使我们能够实现碰撞检测的功能，并且当我们在发送数据时检测到信道是空闲的，在接收端仍然有可能发生碰撞。

- CSMA/CA 协议
  - 无线局域网不能使用 CSMA/CD，而只能使用改进的 CSMA 协议。
  - 改进的办法是把 CSMA 增加一个碰撞避免(Collision Avoidance)功能。
  - 802.11 就使用 CSMA/CA 协议。而在使用 CSMA/CA 的同时，还增加使用停止等待协议。
  - 下面先介绍 802.11 的 MAC 层。
- 帧间间隔 IFS
  - 所有的站在完成发送后，必须再等待一段很短的时间（继续监听）才能发送下一帧。这段时间通称是帧间间隔 IFS (InterFrame Space)。
  - 帧间间隔长度取决于该站欲发送的帧的类型。高优先级帧需要等待的时间较短，因此可优先获得发送权。

- 若低优先级帧还没来得及发送而其他站的高优先级帧已发送到媒体，则媒体变为忙态因而低优先级帧就只能再推迟发送了。这样就减少了发生碰撞的机会。

- CSMA/CA 协议的原理
  - 欲发送数据的站先检测信道。在 802.11 标准中规定了在物理层的空中接口进行物理层的载波监听。
  - 通过收到的相对信号强度是否超过一定的门限数值就可判定是否有其他的移动站在信道上发送数据。
  - 当源站发送它的第一个 MAC 帧时，若检测到信道空闲，则在等待一段时间 DIFS 后就可发送。
- 为什么信道空闲还要再等待
  - 这是考虑到可能有其他的站有高优先级的帧要发送。
  - 如有，就要让高优先级帧先发送。
- 假定没有高优先级帧要发送
  - 源站发送了自己的数据帧。
  - 目的站若正确收到此帧，则经过时间间隔 SIFS 后，向源站发送确认帧 ACK。
  - 若源站在规定时间内没有收到确认帧 ACK（由重传计时器控制这段时间），就必须重传此帧，直到收到确认为止，或者经过若干次的重传失败后放弃发送。
- 虚拟载波监听
  - 虚拟载波监听(Virtual Carrier Sense)的机制是让源站将它要占用信道的时间（包括目的站发回确认帧所需的时间）通知给所有其他站，以便使其他所有站在这一段时间都停止发送数据。
  - 这样就大大减少了碰撞的机会。
  - “虚拟载波监听”是表示其他站并没有监听信道，而是由于其他站收到了“源站的通知”才不发送数据。
- 虚拟载波监听的效果

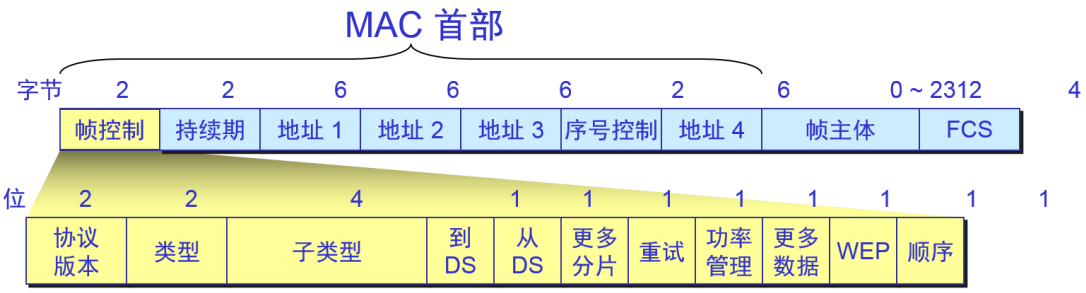
- 这种效果好像是其他站都监听了信道。
- 所谓“源站的通知”就是源站在其 MAC 帧首部中的第二个字段“持续时间”中填入了在本帧结束后还要占用信道多少时间（以微秒为单位），包括目的站发送确认帧所需的时间。

- 网络分配向量
  - 当一个站检测到正在信道中传送的 MAC 帧首部的“持续时间”字段时，就调整自己的网络分配向量 NAV (Network Allocation Vector)。
  - NAV 指出了必须经过多少时间才能完成数据帧的这次传输，才能使信道转入到空闲状态。
- 争用窗口
  - 信道从忙态变为空闲时，任何一个站要发送数据帧时，不仅都必须等待一个 DIFS 的间隔，而且还要进入争用窗口，并计算随机退避时间以便再次重新试图接入到信道。
  - 在信道从忙态转为空闲时，各站就要执行退避算法。这样做就减少了发生碰撞的概率。
  - 802.11 使用二进制指数退避算法。
- 二进制指数退避算法
  - 第 i 次退避就在 2^{2+i} 个时隙中随机地选择一个，即：
  - 第 I 次退避是在时隙 {0, 1, …, $2^{2+i}-1$} 中随机地选择一个。 。
  - 第 1 次退避是在 8 个时隙（而不是 2 个）中随机选择一个。
  - 第 2 次退避是在 16 个时隙（而不是 4 个）中随机选择一个。
- 退避计时器 (backoff timer)
  - 站点每经历一个时隙的时间就检测一次信道。这可能发生两种情况。
    - 若检测到信道空闲，退避计时器就继续倒计时。
    - 若检测到信道忙，就冻结退避计时器的剩余时间，重新等待信道变为空闲并再经过时间 DIFS 后，从剩余时间开始继续倒计时。如果退避计时器的时间减小到零时，就开始发送整个数据帧。

- 退避算法的使用情况
  - 仅在下面的情况下才不使用退避算法：检测到信道是空闲的，并且这个数据帧是要发送的第一个数据帧。
  - 除此以外的所有情况，都必须使用退避算法。即：
    - 在发送第一个帧之前检测到信道处于忙态。
    - 在每一次的重传后。
    - 在每一次的成功发送后。

2.2.4 802.11 局域网的 MAC 帧

- 802.11 帧共有三种类型，即控制帧、数据帧和管理帧。
- 下面是数据帧的主要字段。



- 802.11 数据帧的三大部分
  - MAC 首部，共 30 字节。帧的复杂性都在帧的首部。
  - 帧主体，也就是帧的数据部分，不超过 2312 字节。这个数值比以太网的最大长度长很多。不过 802.11 帧的长度通常都是小于 1500 字节。
  - 帧检验序列 FCS 是尾部，共 4 字节
- 关于 802.11 数据帧的地址

802.11 数据帧最特殊的地方就是有四个地址字段。地址 4 用于自组网络。我们在这里只讨论前三种地址。

- 序号控制字段、持续期字段和帧控制字段
  - 序号控制字段占 16 位，其中序号子字段占 12 位，分片子字段占 4 位。

- 持续期字段占 16 位。
- 帧控制字段共分为 11 个子字段。
  - 协议版本字段现在是 0。
  - 类型字段和子类型字段用来区分帧的功能。
  - 更多分片字段置为 1 时表明这个帧属于一个帧的多个分片之一。
  - 有线等效保密字段 WEP 占 1 位。若 WEP = 1，就表明采用了 WEP 加密算法。

- 802.11b 的典型解决方案
  - 对等解决方案

    一种最简单的应用方案，只要给每台 PC 安装一片无线网卡，即可相互访问。如为其中一台 PC 再安装一片有线网卡，无线网中其余 PC 即利用这台 PC 作为网关，访问有线网络或共享打印机等设备。

  - 单接入点解决方案

    接入点相当于有线网络中的集线器。无线接入点可连接周边无线终端，形成星形网络结构，同时通过 10Base-T 端口与有线网络相连，使整个无线网终端都能访问有线网络的资源，并可通过路由器访问 Internet。

  - 多接入点解决方案

    当网络规模较大，可以采用多个接入点分别与有线网络相连，从而形成以有线网络为主干的多接入点的无线网络，所有无线终端可以通过就近的接入点接入网络，访问整个网络的资源，从而突破无线网覆盖半径的限制。

  - 无线中继解决方案

    无线接入器还有另外一种用途，即充当有线网络的延伸。比如信息点的分布范围超出了单个接入点的覆盖半径，我们可以采用两个接入点实现无线中继，以扩大无线网络的覆盖范围

  - 无线冗余解决方案

对于网络可靠性要求较高的应用环境，接入点一旦失效，整个无线网络会瘫痪。因此，可以将两个接入点放置在同一位置，从而实现无线冗余备份的方案。

- 多蜂窝漫游工作方式

在一个大楼中或者在很大的平面里面部署无线网络时，可以布置多个接入点构成一套微蜂窝系统，这与移动电话的微蜂窝系统十分相似。微蜂窝系统允许一个用户在不同的接入点覆盖区域内任意漫游，随着位置的变换，信号会由一个接入点自动切换到另外一个接入点。

2.3 无线个人区域网 WPAN

- WPAN 的核心思想：用无线电（RF）或红外线代替传统的有线电缆，以个人为中心实现个人使用的电子设备的互联，组建个人化自组信息网络。不需要使用接入点 AP。
- 整个网络的范围大约在 10 m 左右。
- 从计算机网络的角度来看，WPAN 是一个局域网；从电信网络的角度来看，WPAN 是一个接入网，称为电信网络“最后一米”的解决方案。
- 无线个人区域网 WPAN 和个人区域网 PAN (Personal Area Network)并不完全等同，因为 PAN 不一定都是使用无线连接的。

WPAN 和 WLAN 并不一样

- WPAN 是以个人为中心来使用的无线人个区域网，它实际上就是一个低功率、小范围、低速率和低价格的电缆替代技术。WPAN 都工作在 2.4 GHz 的 ISM 频段。
- 但 WLAN 却是同时为许多用户服务的无线局域网，它是一个大功率、中等范围、高速率的局域网。

1. 蓝牙系统(Bluetooth)

- 是一种点对点、点对多点短距离无线通信技术，联网移动通信设备和电脑设备，并能无线上网。
- 实际应用范围还可以拓展到各种家电、消费电子和汽车等产品。

- 发明和最早使用的 WPAN 是 1994 年爱立信公司推出的蓝牙系统，其标准是 IEEE 802.15.1 。
- 蓝牙以公元 10 世纪一位纳维亚国王的名字命名。1998 年 5 月，爱立信、诺基亚、东芝、IBM 和英特尔五家公司联合成立了蓝牙共同利益集团（Bluetooth SIG）。 99 年 7 月发布 Bluetooth 1.0 标准。至今加盟蓝牙 SIG 的公司已达到 2 千多。

- 皮可网(piconet)
  - Piconet 直译就是“微微网”，表示这种无线网络的覆盖面积非常小。
  - 蓝牙的数据率为 720 kb/s，通信范围在 10 米左右。使用 TDM 方式和扩频跳频 FHSS 技术组成不用基站的皮可网(piconet)。
  - 每一个皮可网有一个主设备(Master)和最多 7 个工作的从设备(Slave)。
  - 通过共享主设备或从设备，可以把多个皮可网链接起来，形成一个范围更大的扩散网(scatternet)。
  - 这种主从工作方式的个人区域网实现起来价格就会比较便宜。
- 蓝牙（Bluetooth）技术
  - 蓝牙包括核心协议(Core) 和简档（Profile）两个部分。
  - 协议主要定义蓝牙的技术细节（如串口仿真协议、逻辑链路控制和适配协议等），而简档定义相应的实现协议栈，这样即可为全球兼容性奠定基础。
  - 蓝牙标准主要定义底层协议，也定义一些高层协议和相关接口。整个协议体系结构分为 4 层 .
- 蓝牙协议体系结构
  - (1) 核心协议层（链路管理协议 LMP、蓝牙逻辑链路控制与适配协议 L2CAP、服务检测协议 SDP）
  - (2) 线缆替代协议层 （RFCOMM）
  - (3) 电话控制协议层（TCB, BIN/AT）
  - (4) 其它协议层（与 Internet 应用相关的高层协议，如 PPP、UDP/TCP/IP、OBEX/vCard/vCal、IrMC、E-mail、WAP 等)

- 蓝牙安全性：
  - 物理层：蓝牙跳频速度达 1600 跳/s，属快速跳频，加上通信的短距离的特性，提供一定程度的物理层的安全特性。
  - 链路层：蓝牙链路级的安全特性在 L2CAP 协议中完成。基于链路密钥的概念，密钥为 128 比特长的随和序列。蓝牙设备在每次建链时都要核对密钥，通信时该密钥将用于鉴权和加密。
  - 业务级：采用了安全管理器的概念，安全管理器可以对每一个设备和服务指定信任等级和访问极限，满足蓝牙设备和服务的安全接入。
- 蓝牙应用：
  - 话音/数据的接入。它是将一台计算设备通过安全的无线链路连接到一个通信设备，完成与广域通信网络互联。
  - 外围设备互联是指将各种外设通过蓝牙链路连接到主机。
- 蓝牙技术 vs Wi-Fi 技术
  - 蓝牙技术主要面向近距离信息设备如手机、电器设备、数码相机以及 PC 等的连接，1Mbps 的速率使其可以方便、快速地传送较广泛一类数据，如数码相片、email、话音、文件等。
  - Wi-Fi 技术是无线 Ethernet。通过在 PC 内插入 PCI MCA 卡，无线传送速率可达到 11Mbps，并通过 Access Point 接入网络，并可将多个用户连上宽带 DSL。
  - 蓝牙的最高速率为 2Mbps，和现有的无线 LAN 相同。另一个缺点是：它们的传输距离只有几米～几十米远，而无线 LAN 最远可达 100 米。
  - 无线 LAN 技术可以实现在有限空间内的移动连网。在其性能已提升至和有线 LAN 同等后，家庭用户将更乐于接受它。对家庭用户而言,不需要电缆连接是无线 LAN 最好的一个优点。

2. 红外线无线网络 (Infrared Data Association)
   - 红外线辐射波长范围: 700～1300nm
   - 红外线无线网络组成：
     - 红外发射器（红外 LED 器件）

- 传输信道
- 红外接收器

- 红外线通信特点
  - 发射与接收设备体积小，重量轻，成本低;
  - 支持各种速率的点到点话音和数据业务;
  - 主要应用在嵌入式系统和设备中;
  - 红外频带宽，不干扰现有射频系统性能，干扰低;
  - 红外 LOS，不能穿透墙，保密性强;
  - 红外数据传输率高，>1Mb/s（0.96～4Mbps）；
  - IrDA 主要应用：设备互联、信息网关
    - 设备互联后可完成不同设备内文件与信息的交换,信息网关负责连接信息终端和互联网
- 红外线无线网络结构
  - IrDA 协议栈分成两部分：核心协议和可选协议。
  - IrDA 的核心协议包括：物理层协议、链路接入协议、链路管理协议和服务发现协议。
  - 核心协议完成对物理传输媒介的监测与控制，发现设备，可靠的数据链路的建立与维持，高层数据包的适配，不同协议数据的复用与流量控制。

3. 低速 WPAN
   - 低速 WPAN 主要用于工业监控组网、办公自动化与控制等领域，其速率是 2 ~ 250 kb/s。
   - 低速 WPAN 的标准是 IEEE 802.15.4。最近新修订的标准是 IEEE 802.15.4-2006。
   - 低速 WPAN 中最重要的就是 ZigBee。是一种新兴的低复杂度、低功耗、低数据速率、低成本的无线网络通信技术。

- ZigBee 技术主要用于各种电子设备（固定的、便携的或移动的）之间的无线通信，其主要特点是通信距离短（10 ~ 80 m），传输数据速率低，并且成本低廉。

- ZigBee 的特点
  - 功耗非常低。在工作时，信号的收发时间很短；而在非工作时，ZigBee 结点处于休眠状态。对于某些工作时间和总时间之比小于 1% 的情况，电池的寿命甚至可以超过 10 年。
  - 网络容量大。一个 ZigBee 网络最多有 255 个结点，其中一个是主设备，其余则是从设备。若是通过网络协调器，最多可支持超过 64000 个结点。
  - 速率低 - 基本速率是 250 kb/s；当降低到 28kb/s 时，传输范围可扩大到 134 米，并获得更高的可靠性；
  - 有效覆盖范围 10～75 米之间，具体依据实际发射功率大小和各种不同应用模式而定，能够覆盖普通家庭或办公室环境。
  - 成本低—数据传输速率低，协议简单，又无专利费；
  - 安全性—Zigbee 提供了数据完整性检查和鉴权功能，加密算法采用 AES-128；
  - ZigBee 适合于承载数据流量较小的业务，如遥控、传感器等，满足工业控制、消费性电子设备、汽车、农业和医用设备控制等领域的特定需求。例如，在无线传感器环境中众多传感器之间相互协调实现通信，只需要很少的能量，以接力的方式将数据从一个传感器传到另一个传感器。

- ZigBee 的标准
  - 在 IEEE 802.15.4 标准基础上发展而来的。
  - 所有 ZigBee 产品也是 802.15.4 产品。
  - IEEE 802.15.4 只是定义了 ZigBee 协议栈的最低的两层（物理层和 MAC 层），而上面的两层（网络层和应用层）则是由 ZigBee 联盟定义的。

- ZigBee 的协议栈

- ZigBee 的组网方式可采用星形和网状拓扑，或两者的组合
  - 有一个全功能设备 FFD 充当网络的协调器。
  - ZigBee 网络中数量最多的端设备是精简功能设备 RFD 结点。

4. 高速 WPAN
   - 高速 WPAN 用于在便携式多媒体装置之间传送数据，支持 11 ~ 55 Mb/s 的数据率，标准是 802.15.3 。
   - IEEE 802.15.3a 工作组还提出了更高数据率的物理层标准的超高速 WPAN，它使用超宽带 UWB 技术。
   - UWB 技术工作在 3.1 ~ 10.6 GHz 微波频段，有非常高的信道带宽。超宽带信号的带宽应超过信号中心频率的 25% 以上，或信号的绝对带宽超过 500 MHz。
   - 超宽带技术使用了瞬间高速脉冲，可支持 100 ~ 400 Mb/s 的数据率，可用于小范围内高速传送图像或 DVD 质量的多媒体视频文件。

5. 超宽带（UWB）技术

UWB 技术又被称为脉冲无线电发射技术。根据美国联邦通信委员会（FCC）的定义，是指在 3.1G-10.6G 频段内占用 10dB/带宽大于 500MHz 的无线发射方案。

- UWB 吞吐量
  - High speed at short range
    - 480 Mb/s at ~3m
    - Does not penetrate walls

- UWB 概 述
  - UWB 无线技术基于共用频段思想，打破短距离无线通信频率资源供不应求及不兼容的现状，为频谱管理和无线系统工程中存在的诸多问题提供有效的解决方案；
  - UWB 能为无线个域网接入技术提供低功耗、高带宽且易于实现的底层技术支撑，实现便携设备和固定设备、个人电脑和娱乐设备的空中接口，建立可兼容的全 IP 网络；
  - UWB 系统能在短距离内支持高达 400Mb/s 的信息传输率，并可通过减小传输速率来增加传输距离，实现精确的定位跟踪；
  - 同时，UWB 设备具有能支持有效多次反射路由机制的精确位置跟踪功能，更有利于在动态节点的自组织网（ad hoc）中实现定位。
  - UWB 信号的宽频带、低功率谱密度的特性，决定了 UWB 有以下优势：
    - 易于与现有的窄带系统，如 GPS、蜂窝通信系统、地面电视等共用频段，大大提高了频谱利用率；
    - 易于实现多用户的短距离高速数据通信；
    - 对多径衰落具有鲁棒性。
  - 适合 UWB 技术的实际应用包括：
    - 高速无线个域网；
    - 无线以太接口链路；
    - 智能无线局域网；
    - 户外对等网络；
    - 传感、定位和识别网络

2.4 无线城域网 WMAN

- 2002 年 4 月通过了 802.16 无线城域网的标准。欧洲的 ETSI 也制订类似的无线城域网标准 HiperMAN。

- 2003 年，Intel、Nokia、Fujitsu 等制造商创立 WiMax（Wireless Interoperability Microwave Acess， 将共同支持 IEEE 802.16 标准的无线 MAN 产品开发。
- IEEE 802.16 工作的频段是无需授权频段，范围在 2～66GHz 之间，在 20MHz 带宽时，支持高达 100Mbps 的共享数据传输速率。
- WMAN 可提供“最后一英里”的宽带无线接入（固定的、移动的和便携的）。
- 在许多情况下，无线城域网可用来代替现有的有线宽带接入，因此它有时又称为无线本地环路。

WiMAX(Worldwide Interoperability for Microwave Access)

- WiMAX 常用来表示无线城域网 WMAN，这与 Wi-Fi 常用来表示无线局域网 WLAN 相似。
- IEEE 的 802.16 工作组是无线城域网标准的制订者，而 WiMAX 论坛则是 802.16 技术的推动者。
- 两个正式标准
    - 802.16d（它的正式名字是 802.16-2004），是固定宽带无线接入空中接口标准（2 ~ 66 GHz 频段）。
    - 802.16 的增强版本，即 802.16e，是支持移动性的宽带无线接入空中接口标准（2 ~ 6 GHz 频段），它向下兼容 802.16-2004。
- WiMax 作为城域网接入手段，最大覆盖范围 50 公里。是一种定位于宽带 IP 城域网的无线接入技术。主要用于固定无线宽带接入（ FBWA ）、地理位置分散的信息热点回程传输，或大业务量用户的接入。
- WiMax 采用了多种技术来应对建筑物阻挡情况下的非视距（ NLOS ）和阻挡视距（ OLOS ）的传播条件，因此其可以实现非视距传输。
- WiMax 是解决“最后一公里”的通信接入问题。特别是对于偏远地区没有 Cable 和 DSL 服务，通过 WiMax 的布建将能助于最后一公里的无线宽带布建。
- 链路层技术

  适应 TCP/IP 协议对信道传输质量的要求，在链路层加入了 ARQ 机制，减少到达网络层的信息差错，提高系业务吞吐量。同时 采用天

线阵、天线极化方式等天线分集技术来应对 OLOS 和 NLOS 造成的深衰落。

- QoS 性能

  可以向用户提供具有 QoS 性能的数据、视频、话音（ VoIP ）业务。三种等级服务： 固定带宽、 承诺带宽、 尽力而为。

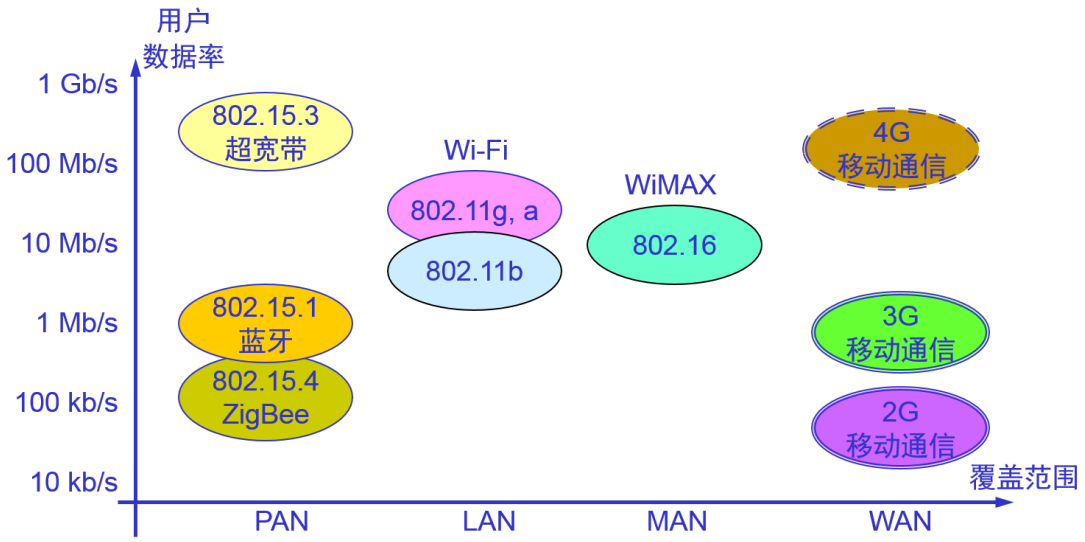
- WiMax 面临的问题：技术复杂、成本较高

  WiMax 传播距离较远，环境复杂，导致其技术复杂。WiMax 基站台费用约是 2 万美元。据 IEEE 估计，只有当每单位用户数所负担的平均成本下降至 300 美元以下，且基站台降至 1 万美元以下，则宽带无线才将有可能成为最后一公里服务。

- WiMax 可以作为 802.11x 网络的延伸架构，不是取代 IEEE 802.11x ，而是与 802.11x 整合。

- WiMax 也面临 IEEE802.20 的考验。IEEE 802.20 标准是移动宽带无线接入系统（ MBWA ， Mobile Broadband Wireless Access ），其目标趋近于 4G 的设想。移动性是 802.20 的突出性能， 它所适应的移动速度高达 250 km/h ，其小区半径为 1km 。这些性能则是 WiMax 所无法比拟的。

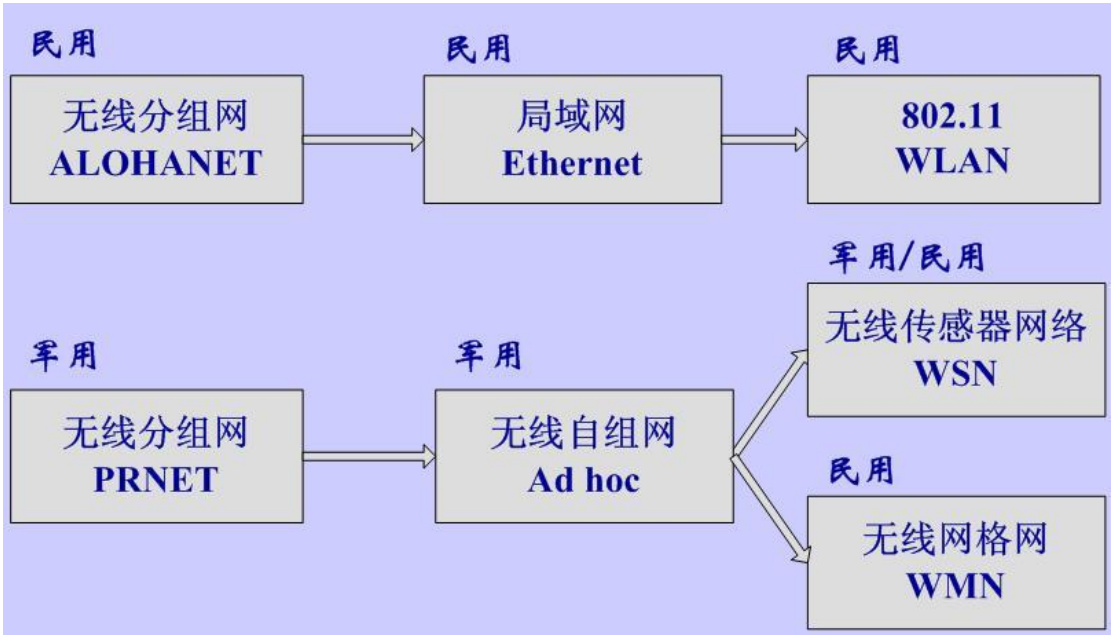
- 几种无线网络的比较



第三章 无线 Ad hoc 网络

3.1 Ad hoc 网络的基本概述

- 网络技术发展的主线



- Ad hoc 术语的来源
  - Ad hoc 来源于拉丁语—本意是“向这个”
  - 英文名称：Ad hoc network Self-organizing network Infrastructureless network Multi-hop network
  - Ad hoc 在英语中的含义是： “for the specific purpose only” —“为某个特定目的、临时的、事先未准备的”
  - 1991 年 5 月：IEEE 正式采用“Ad hoc 网络” — 一种特殊的自组织、对等式、多跳、无线移动网络
- Ad hoc 网络的发展历史
  - 早在 1972 年，美国 DARPA 就启动了分组无线网项目 PRNET（Packet Radio NETwork），研究在战场环境下利用分组无线网进行数据通信，但是不能支持大型网络环境的需要。

- 1983 年，启动了高残存性自适应网络项目 SURAN（SURvivable Adaptive Network）
- SURAN 项目研究任务：
  - 如何将无线分组网技术用于支持更大规模的网络
  - 开发了能够适应战场快速变化的自适应网络协议
- SURAN 计划的三个具体的目标：
  - 开发出符合分组无线网络协议的产品
  - 开发并验证适合上万个结点的组网方法
  - 开发并验证存在复杂电子干扰条件下可生存的分组无线网络技术
- GloMo 计划
  - 1994 年： DARPA 又启动了全球移动信息系统 GloMo（Globle Mobile Information Systems）计划项目，并一直研究至今。
  - 1996 年—2000 年 WINGs 研究项目
    - ✓ 无线自适应移动信息系统 WAMIS—多跳、移动环境下支持实时多媒体业务的高速分组无线网络
    - ✓ 主要目标：如何将无线移动自组网与 Internet 无缝地连接起来
- 成立于 1991 年的 IEEE 802.11 标准委员会采用了“Ad hoc 网络”一词来描叙这种网络，自组织、对等式、多跳无线移动通信网络，Ad hoc 网络就此诞生。
- Internet 工作组：
  - IETF1997 年成立 MANET 工作组（mobile ad hoc network）
  - 利用多跳无线网构造基于 IP 的移动互联网
  - IETF 在 2003 成立了 ANS 研究组（Ad Hoc Networks Scalability）

移动 ad hoc 网络（MANET）

- 移动 Ad hoc 网络/多跳无线网络
  - 由一组带有无线通信收发装置的移动终端节点组成
  - 网络中每个移动终端自由移动
  - 网络中所有移动终端地位相等
  - 可以在任何时候、任何地点快速构建
  - 不需要现有信息基础网络设施的支持
  - 是一个多跳、临时、无中心网络。

多跳无线网、自组织网络、无固定设施的网络、对等网络

- MANET 网络的特点
  - 具备移动通信网络和计算机网络的特点
    - 移动通信和计算机网络相结合
      - ✓ 报文交换采用分组交换机制
      - ✓ 移动终端是配有无线收发设备的移动便携式终端
    - 移动终端兼备双重角色
      - ✓ 作为主机要运行面向用户的应用程序
      - ✓ 作为路由器要运行相应的路由协议
    - 终端之间路由通过多个中间节点转发完成
  - 网络拓扑动态变化
    - 用户终端随意移动
    - 移动节点的开机/关机
    - 无线电发送功率变化
    - 无线信道间互相干扰
    - 地形等综合因素影响
  - 无中心网络的自组性

- 无控制中心
- 每个节点地位平等
- 节点随时加入/离开网络
- 任何节点故障不会影响整个网络
- 具有更强鲁棒性和抗毁性

- 多跳组网方式
  - 接收端和发送端可使用比两者直接通信小得多的功率进行通信→大大节约能量的消耗
  - 中间节点参与分组转发→能有效降低对无线传输设备的设计难度和成本，同时扩大自组网络覆盖范围。
- 有限的无线传输带宽
  - 无线信道能提供的网络带宽比有线信道要低很多
  - 竞争共享无线信道产生的碰撞
  - 信号衰落、噪声干扰以及信道之间干扰等
- 移动终端的自主性
  - 自组网络的移动终端之间存在某种协同工作关系
  - 每个终端都将承担为其它终端进行分组转发的义务
- 安全性差
  - 无线链路使网络容易受到链路层的攻击
  - 节点漫游时缺乏物理保护
  - 移动性使节点之间的信任关系经常变化
- 网络的可扩展性不强
  - 节点之间的相互干扰造成网络容量下降
  - 各节点吞吐量随网络节点总数的增加而下降
- 存在单向的无线信道

- 无线终端发射功率的不同以及地形环境的影响

- 生存时间短

- MANET 与其他无线网络
  - 与分组无线网、无线局域网、红外网络比较
    - 单跳与多跳
    - 研究重点不同
    - 通信模式不同
- Ad hoc 网络的应用
  - 军事应用：主要应用领域。因其特有的无需架设网络设施、快速、抗毁性强等特点，已经成为战术互联网的核心技术。美军研制了大量的无线自组织网络设备，用于单兵、车载、指挥所等不同的场合，并大量装备部队。
  - 紧急和突发场合：在发生了地震、水灾、火灾灾难后，能够在这些恶劣和特殊的环境下提供通信支持。
  - 偏远野外地区：无法依赖固定或预设的网络设施进行通信。
  - 临时场合：Ad hoc 网络的快速、简单组网能力使得它可以用于临时场合的通信。比如会议、庆典、展览等场合，可以免去布线和部署网络设备的工作。
  - 动态场合和分布式系统：通过无线连接远端的设备、传感节点和激励器，可方便用于分布式控制，特别适合于调度和协调远端设备的工作，自动高速公路系统（AHS）中协调和控制车辆，对工业处理过程进行远程控制等。
  - 个人局域网（PAN）：用于实现 PDA、手机、掌上电脑等个人电子通信设备之间的通信，并可以构建虚拟教室和讨论组等崭新的移动对等应用（MP2P）。
  - 传感器网络：应用的另一大领域。具有非常广阔的应用前景。
  - 商业应用：组建家庭无线网络、无线数据网络、移动医疗监护系统和无线设备网络，开展移动和可携带计算以及无所不在的通信业务等。

- 其它应用：比如它可以用来扩展现有蜂窝移动通信系统的覆盖范围，实现地铁和隧道等场合的无线覆盖，实现汽车和飞机等交通工具之间的通信，用于辅助教学和构建未来的移动无线城域网和自组织广域网等。
- Ad hoc 网络如何接入现有的 Internet 也是近年研究的一个热点。

3.2 Ad hoc 网络的体系结构

- 节点结构
  - MANET 节点结构
    - 主机：面向移动用户，完成数据处理等功能。
    - 路由器：负责路由选择、转发用户数据报功能。
    - 无线收发装置：完成数据传输功能。
  - MANET 网络结构
    - 平面结构（完全分布式）
      - ✓ 所有节点的地位平等
    - 层次结构（分层分布式）
      - ✓ 网络被划分为簇（cluster）
      - ✓ 每个簇由一个簇头和多个簇成员组成
      - ✓ 簇头可形成更高一级的网络
- 分级结构
  - 单频分级
    - 系统使用一个频率
    - 簇头和网关形成虚拟主干
    - 簇头的选举和维护较复杂
  - 多频分级

- 每一级使用一个频率
- 高级结点的功率大，带宽较宽
- 簇头要有两套协议栈

- 平面结构的优缺点
  - 优点
    - 简单
      - ✓ 所有节点能力相同
    - 健壮
      - ✓ 只要存在多条路径就能通信
    - 相对安全
      - ✓ 节点覆盖范围较小
  - 缺点
    - 路由开销大
    - 可扩充性差
- 层次结构的优缺点
  - 优点
    - Cluster 成员功能简单
    - 路由信息局部化
    - 节点定位简单
    - 可扩展性好
    - 抗毁性好
  - 缺点
    - Cluster 头需要选择
    - 所有传输都通过头

- Closter 头是瓶颈

- 移动 Ad hoc 的协议栈
  - 一般协议栈
    - 基于 TCP/IP
    - 传输层协议要修改
    - 路由协议和组网方式要修改
    - 与 Internet 互联
- MANET 面临的问题
  - 特殊的信道共享方式
    - 共享信道
    - “隐藏终端”/“暴露终端”
  - 动态变化网络拓扑
    - 常规路由协议花较高代价（带宽、能源、CPU 等）获得的路由信息可能已经陈旧
  - 有限的无线传输带宽
    - 减少节点之间交换的信息量
    - 减少控制信息带来的附加开销
  - 节能问题
    - 功率控制
    - 电池供电
  - 安全问题
    - 无线信道更容易受到各种攻击
    - 缺乏物理保护使得攻击可能来自内部
    - 移动性使得节点之间的信任关系不断变化

- 安全策略应具有可扩展性

- 网络管理
  - 拓扑管理
    - ✓ 确定一种将一组节点组织成网络的机制
  - 移动性管理
    - ✓ 跟踪网络内移动节点的位置
  - 服务质量保证
    - ✓ 多跳拓扑动态变化的 MANET 服务质量保证仍然是个问题
  - 地址自动配置
  - 其他问题

- 影响 ad hoc 网络的主要因素
  - 无线通信技术
    - 受限于底层无线通信技术的性能（传输率、延迟、吞吐量）
  - 节点密度
    - 密度越高传输路径的跳数越多，受网络拓扑变化的影响就越明显。
  - 节点移动速度
    - 速度越高节点间的拓扑结构的稳定性越差，路由计算和交换负载越大。
  - 通信负荷和通信模式
    - 流量特性和分布将直接影响到网络的吞吐性能。

- 实现 MANET 的关键技术
  - 路由协议
  - 服务质量
  - 功率控制

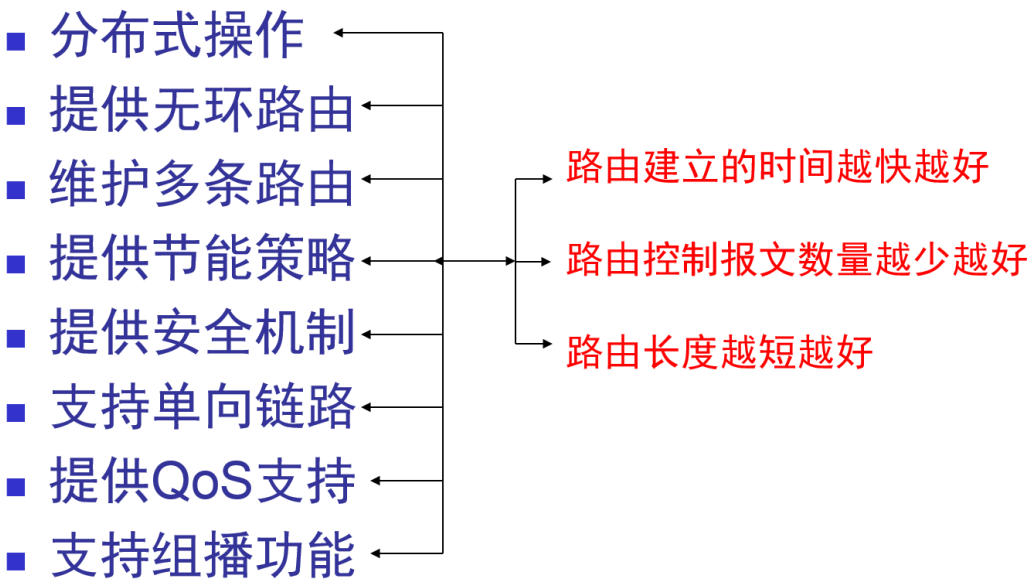
- 安全问题
- Ad hoc 网络的互联
- Ad hoc 网络的资源管理
- 传输层服务的性能

3.3 Ad hoc 网络路由技术

- MANET 路由概述
  - 通信两点可能不在相互的无线传输范围内
  - 需要其他节点承担路由器的转发工作
  - 节点移动要发现新路由
  - 多条链路组成路径
  - 移动导致路径变化
- MANET 路由面临的困难
  - 路由信息不易获得
    - 定期交换路由信息或者按需搜索路由的开销大
    - 网络资源有限，并且必须被所有节点共享
    - 节点资源（电池、CPU 等）也是有限
    - 也许不可能收集齐所有的路由信息
  - 路由信息不完整
    - 移动和分区很难将信息分发到一个没有固定成员网络的所有节点
  - 路由信息可能过期
    - 不可能连续地或者立即地交换信息
    - 节点随时移动

- 无线传播变化很大

- 为什么需要新的路由协议？
  - 传统的路由解决方案(如在 Internet 和蜂窝网中的一些方案)都是假定网络拓扑结构是相对稳定的；
  - 传统的路由方案依赖于保存在某些网络节点或特定管理节点中的分布式路由数据库，而 Ad Hoc 网络节点不可能永久存储路由信息，而且它们存储的信息也并不是一直真实可靠的；
  - 常规路由协议不是为高移动性和低带宽网络设计的；
  - DV 算法存在“无穷计算”问题和慢收敛；
  - 采用泛洪技术的（链路状态）协议造成额外的通信和控制开销；
  - 常规路由协议周期性地路由更新消耗大量的网络带宽和节点能源；
  - 当网络节点失效和网络分区时形成路由回路；
  - 无线终端功率的差异以及无线信道的干扰导致单向信道的存在；
- Ad hoc 网络对路由协议的要求



- Ad hoc 路由协议分类
  - 平面路由

- 无需建立具有特殊 cluster 头功能节点的层次结构；
- 不划分区域以及所谓的区内/外不同路由
- 所有的节点在路由机制中地位平等
- 寻址方式是平面的

- 层次路由
  - 节点功能不同
  - 寻址方式是分层进行的
- 地理信息辅助路由
  - 利用地理信息进行路由选择

- 表驱动（table driven）路由
  - 先应式（proactive ）路由
    - 传统的分布式最短路径路由协议
      - ✓ 链路状态或者距离向量
      - ✓ 所有节点连续更新"可达"信息
    - 每个节点维护到网络中所有节点的路由
    - 所有路由都已经存在并且随时可用
    - 路由请求的延迟低
    - 路由开销高
- 表驱动路由协议特点
  - 初期，主要是修改有线网络路由协议以适应 *Ad hoc* 网络环境，大多属于表驱动路由协议。
  - 表驱动路由协议的路由查找策略与传统路由协议类似，节点通过周期性广播路由信息报文，交换路由信息，主动发现路由；同时，节点须维护去往网络中所有节点路由。

- 优点：当节点需要发送数据报文时，只要去往目标节点的路由存在，所需的延时很小；缺点：需要花费较大开销，尽可能使得路由更新能够紧随当前拓扑结构的变化。然而，动态变化拓扑结构可能使得路由更新变成过时信息，路由协议始终处于不收敛状态。
- 主要的表驱动路由协议：DBF (Distributed Bellman-Ford)、DSDV (Destination-Sequenced Distance-Vector Routing)、WRP (Wireless Routing Protocol)。

- 按需（on-demand）路由协议
  - 反应式（reactive）路由
    - 在源端需要时候通过路由发现过程来确定路由
      - ✓ 控制信息采用泛洪（flooding）方式
      - ✓ 路由请求延迟高
      - ✓ 路由开销低
    - 两种实现技术
      - ✓ 源路由（报文头携带完整的路由信息）
      - ✓ 逐跳路由（类似于现在的 Internet 路由）

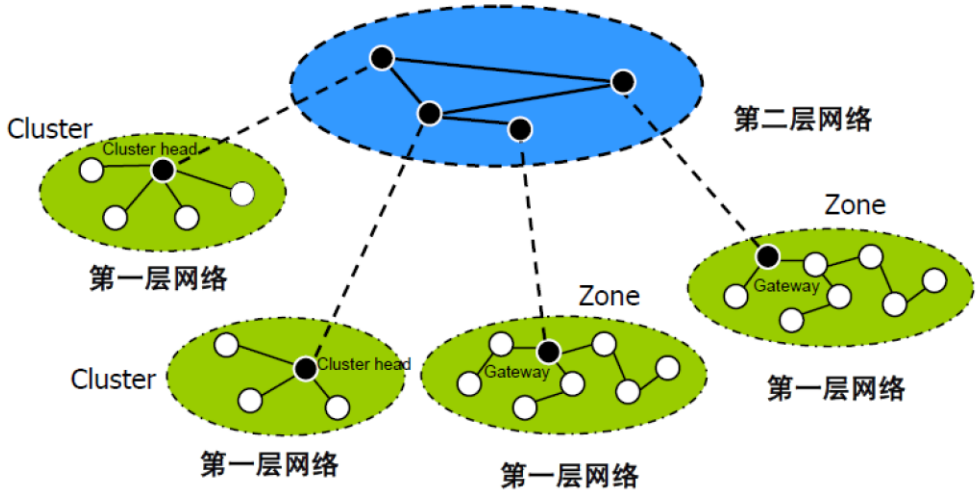
- 按需路由协议的特点
  - 根据发送节点的需求进行路由发现过程，网络拓扑结构和路由表内容也按需建立（只是整个网络拓扑结构的一部分）。
  - 优点：不需周期性广播路由信息，节省网络资源。
  - 缺点：发送分组时，必须临时启动路由发现过程来寻找路由，因而延迟大
  - 主要路由协议：
    - DSR (Dynamic Source Routing)
    - AODV (Ad Hoc on Demand Distance Vector Routing)
    - TORA (Temporally Ordered Routing Algorithm)

- 两种路由机制的权衡

- 路由发现的延迟
  - 主动协议因全程维护所有的路由而具备低延迟
  - 按需协议因只在需要时才发现所需路由而导致高延迟
- 路由发现/维护的开销
  - 按需协议因只在需要时才维护路由而具备低开销
  - 主动协议因连续更新路由可能导致（不一定）高开销
- 哪种途径表现更好取决于流量和移动模式

- 分级路由协议
  - 层次式（hierarchical）路由
    - 一些节点组成一个 cluster 或者 zone
    - 这些 cluster 或者 zone 可组成较大的 supercluster 或者 superzone
  - Cluster 和 zone 的不同
    - cluster 内所有节点都与 cluster head 直接通信，cluster 内节点间的通信一般是两跳。
    - zone 的大小没有限制，zone 内节点的通信可多跳。
  - ZRP

- 二级路由协议概念描述



- 分级路由协议的优缺点
  - 优点
    - 网络拓扑结构的细节通过节点的层层聚合被隐藏起来，由此大大降低大型网络的存储要求。
    - 路由信息分层传播，需要在全局传播的路由信息较少。
    - 有限的链路状态维护
    - 按需建立路由
  - 缺点
    - 分级路由协议的移动管理比较复杂
    - 某些节点（cluster head/ gateway）比其他节点承担更多的通信和计算负载。
- 评价 MANET 路由协议的指标
  - 端-端的数据吞吐量和延迟
    - 反映了数据报的传输质量
  - 路由请求的时间
    - 有数据需要发送到发送出去的时间
  - 路由协议的效率
    - 路由控制信息与数据信息的比率
- 主要的表驱动路由协议
  - DSDV (Destination-Sequenced Distance-Vector Routing) 目标序列距离向量路由
  - DSR (Dynamic Source Routing) 动态源路由
  - AODV (Ad hoc on-demand Distance-Vector Routing) 按需距离向量路由
- 表驱动路由协议--DSDV

- 每个终端维护一张到网中每一个目标终端的路由信息：
  - 下一跳终端, 到目标终端的跳数；
  - 目标终端指定（生成）的序列号；
- 每个终端周期性的向相邻节点发送路由表；
  - 每个终端所能到达的目标终端、到目标终端的跳数、序列号（保持最大的，即最新的）；
  - 每个终端广播时单调递增序列号
- 接收路由更新包时，终端将该包报文与当前路由表比较，旧的（较小的）序列号路径将被删除。
- 当接收器随后公布路由信息时，将它在广播报文中收到的路由信息一起公布。公布之前，接收器给距离增加一个增量，其原因是收到的报文需经过多跳才能到达目的节点（即从转发器到接收器）。
- 无线网络由于单向链路的普遍存在而产生不对称性，从其邻居节点接收到一个报文时，不能说明它们之间一定存在一条单跳数据链路。为了避免单向链路引起的问题，每个移动节点不能插入从其邻居节点接收的路由信息，除非邻居节点显示也能接收该结点报文。
- 在本算法中，只考虑双向链的情况。
- 要选择的最重要的一个参数是广播路由信息报文间的时间；当移动节点收到实际已修改过或新的路由信息时，立即将其转发出去。这要求本算法能尽可能快地收敛。

DSDV 协议特点

- 1、DSDV 路由协议需要每个节点向其邻居公告路由 表，随着时间的流逝，路由记录常常会发生改变，因此这种对路由表的公告必须可靠地反映移动节点的位置。
- 2、每个节点必须根据需要同意向其它节点转发数据报文。
- 3、任意时刻不会产生环路。
- 4、周期性或触发式更新路由信息可能引起过大的通信负载。
- 5、不支持多路径的路由。

- DSDV 协议路由表记录结构
  - 每个移动节点广播数据包含其新的序列号以及下列新的路由信息：
    - 1.目标节点地址
    - 2.到达目标节点的跳数
    - 3.收到的有关目标节点的信息序列号—该序列号原先被目标节点做了标记。
  - 在报文头中传送的路由表中包含硬件地址和网络地址。路由表同样包含由发送者产生的序列号，更新的序列号的路由是作为报文转发的基础，但不必公布。对于序列号相同的路径，选距离最小者。
- 对拓扑变化的响应
  - 节点移动时可能引起链路中断，这种情况可能由第二层协议检测到，也可能由于暂时没有从以前的邻居节点接收到广播的报文而推断出来。我们称中断。
  - 链路的距离为∞，当到下一跳链路中断时，经过下一跳的任何路由的距离都被设置为∞并且被重新分配一个序列号（这种修改立即反映在广播路由信息的报文中）。任何移动节点（不包括目的节点）产生序列号，说明必须建立信息来描述中断链路的产生。
  - 为了减少传输路由报文的信息量，定义下列两个概念：

    1、完全转贮报文：包含全部有效路由信息的报文。

    2、增量报文：只包含与上次路由相比改变部分的报文。
- 路由选择标准
  - 当移动节点收到新（与上次收到的路由信息相比）的路由信息（通常是增量报文）时，选择的标准是：选择带有最新序列号的路由，去掉带旧序列号的路由。
  - 带有序列号的路由意味选择了一条距离更短的路由。
  - 选择不同节点间的时间偏差也是路由选择的一个标准。

移动节点的路由信息广播是异步的。采用上述路由选择的标准可能引起波动，可能导致移动节点收到某种形式的新路由信息时，老是改变下一跳到另一跳的路由，甚至当目的节点没有移动时也如此。

- 选择新的路由有两种方式：1、更新的序列号。2、更短的距离。

- 按需路由协议

  - 表驱动路由协议的路由查找策略与传统路由协议类似，节点通过周期性广播路由信息报文，交换路由信息，主动发现路由；同时，节点须维护去往网络中所有节点路由。

  - 当节点需要发送数据报文时，只要去往目标节点的路由存在，所需的延时很小；但需要花费较大开销，尽可能使得路由更新能够紧随当前拓扑结构的变化。

  - 按需路由协议根据发送节点的需求进行路由发现过程，网络拓扑结构和路由表内容也按需建立。

  - 不需周期性广播路由信息，节省网络资源。但发送分组时，必须临时启动路由发现过程来寻找路由，因而延迟大。

  - DSR (Dynamic Source Routing)动态源路由

    由路由查找和路由维护两个过程组成：

  - 当源终端发现没有去往目标终端的路由时，触发路由查找过程。

  - 源终端 A 在网络中广播路由请求报文(RREQ) ，相邻终端 B 和 C 收到路由请求报文后，记录报文经过了该终端，然后继续转发，直到到达了目标终端 D。

  - 终端 D 将会收到来自多条不同路径的路由请求报文，每个路由请求报文中包含有相应的路径信息。节点 D 根据一定的选择原则选取一条从源终端到目标终端的最优路径，并将该信息附在向源终端 A 发送的路由响应报文中，作为对路由请求的响应。

  - 源终端 A 根据收到的路由响应报文更新路由信息，从而获得去往目标终端 D 的路由。

  - 当拓扑结构发生变化时，通过路由维护过程删除失效路由，重新发起路由请求过程。

- 路由维护通常依靠底层提供的链路失效检测机制进行触发。如果某个终端不能到达下一跳终端，如图中终端 B 在它的通信范围内不能到达终端 C，那么在路由查找过程后建立的路由信息就需要更新。
- 一般地，链路断开的上行终端会发起一个路由错误报文，将链路失效信息发送到源终端，源终端再对目标终端的路由进行重新查找。

- Dynamic Source Routing (DSR)
  - 在进行路由查找的过程中，源终端将一个 RREQ（路由请求）报文泛洪整个 Ad hoc 网络；
  - 每个 RREQ 报文拥有唯一的 ID 号和一个初始值为空的列表，当终端接收到 RREQ 报文的时候，如果该终端已经见到过这个报文的 ID，或者列表中包含该终端，那么终端丢弃该报文并停止泛洪；否则，终端将自身添加到列表的末端，并且将 RREQ 报文继续广播给相邻终端。
  - 目标终端需要进行选择。根据最短路径原则，当路由回复报文（RREP）到达源终端 N1 后，路由查找过程结束。

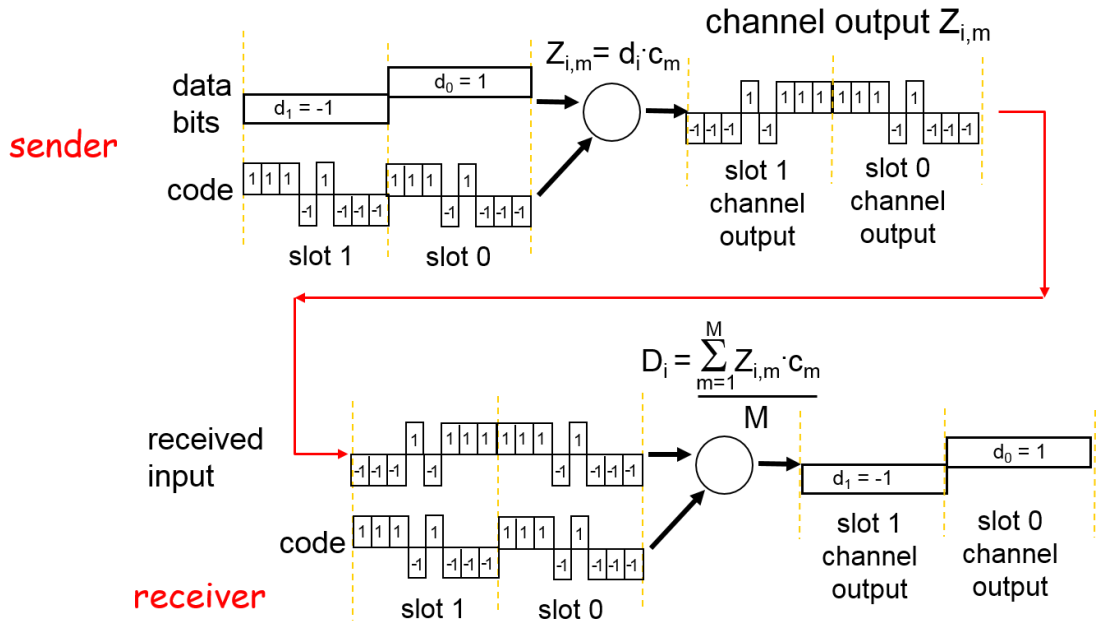
- 按需路由协议 AODV
  - 只需有相互通信的两个终端才进行路由查找与维护
  - AODV 使用广播机制进行路由查找，每个节点仅保持前驱终端的信息，而 DSR 存储所经过终端的源路由信息（导致网络负载过大）。
  - RREQ 报文包含信息: <源地址，源序列号， 广播 ID 号，目标地址号，目标序列号，跳数>
  - <源地址，广播 ID 号>唯一的 RREQ，广播 ID 号在终端每次发起一个新的 RREQ 时递增。每个相邻转发将跳数增 1。如果中间终端收到一个 RREQ 中的源地址，广播 ID 号相同时，认为冗余，弃掉。
  - 源序列号，目标序列号作用是维护路由最新（比较 RREQ 和路由表项）。

第四章 无线广域网

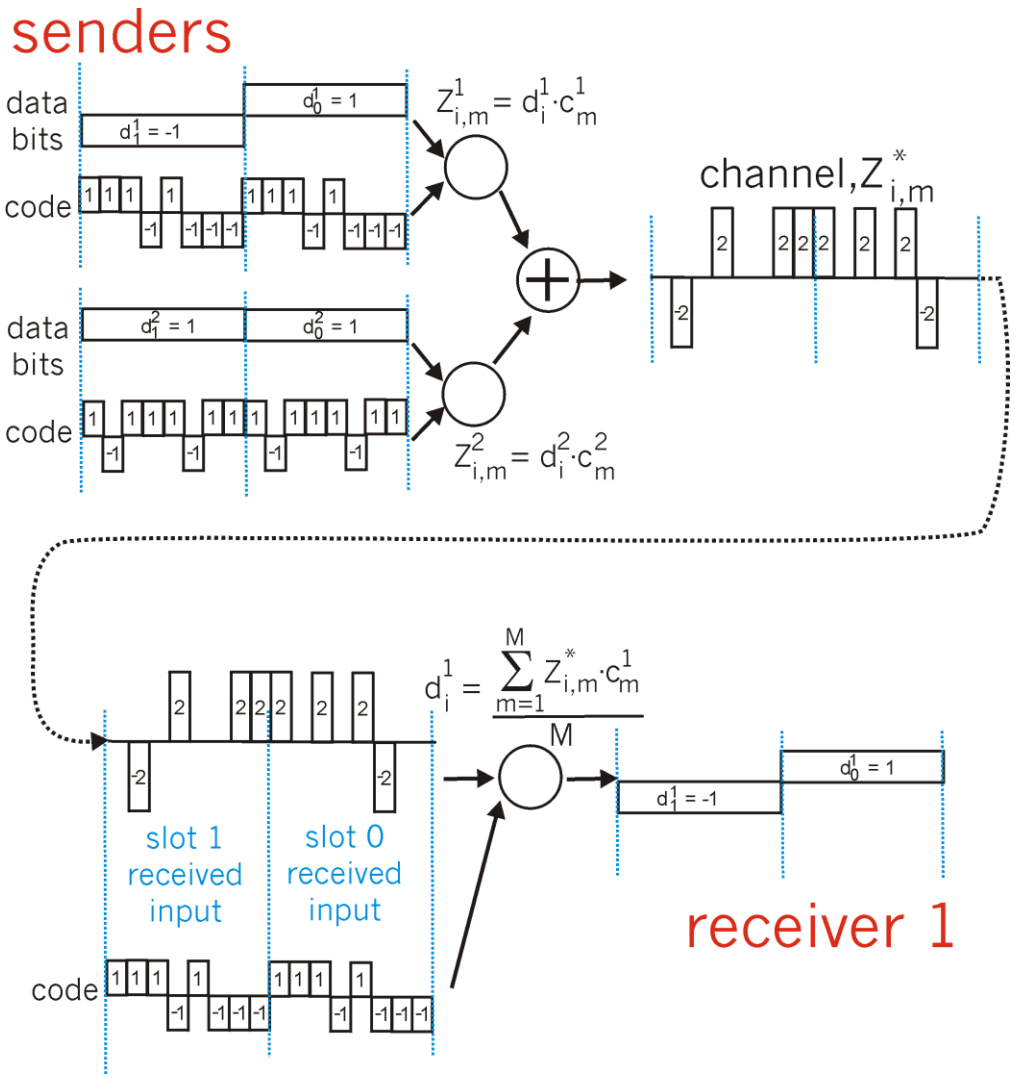
4.6 CDMA 的特点

- 高容量 (约为 FDMA 的 10 倍, 比 TDMA 大 3 倍),
- 固有的高保密性
- 开放式蜂窝结构（C-ONA）
- 高频率利用 (每个用户享有整个频率资源)
- 话音质量提高, 多媒体与综合业务
- 和现有系统基本兼容，易于过渡
- 合理的成本
- CDMA 需要精确的定时和定位，因此需要 GPS

- CDMA Encode/Decode



- CDMA: two-sender interference



4.7 GPRS

- GPRS--第 2.5 代移动通信
  - 通用分组无线业务（GPRS - General Packet Radio Service）是在现有 GSM 网络上开通的一种新型分组数据传输业务，它是利用分组交换（Packet-Switched）概念所发展出的一套无线传输方式。利用该技术将高速分组数据业务引入到现有的蜂窝移动通信网，使现有的移动通信网和数据网结合起来。具体地，话音业务仍然使用 GSM 的电路交换技术，数据业务使用新的分组交换技术。
  - GPRS 网络并不是一种全新的通信网络系统，只是在原有 GSM 基础上增加一些重要节点，可以与 GSM 中的 MSC 集成在一起，保留了 GSM 网络的所有特点。

- GPRS 对 IP、X.25 协议提供完全透明的支持。
- 第 2 代到第 3 代的过渡技术。 GPRS 发展的第二步是通过增强数据速率改进(EDGE)将每个信道的速率提高到 48Kbps.
- 可完成自动图像传送, 文件下载

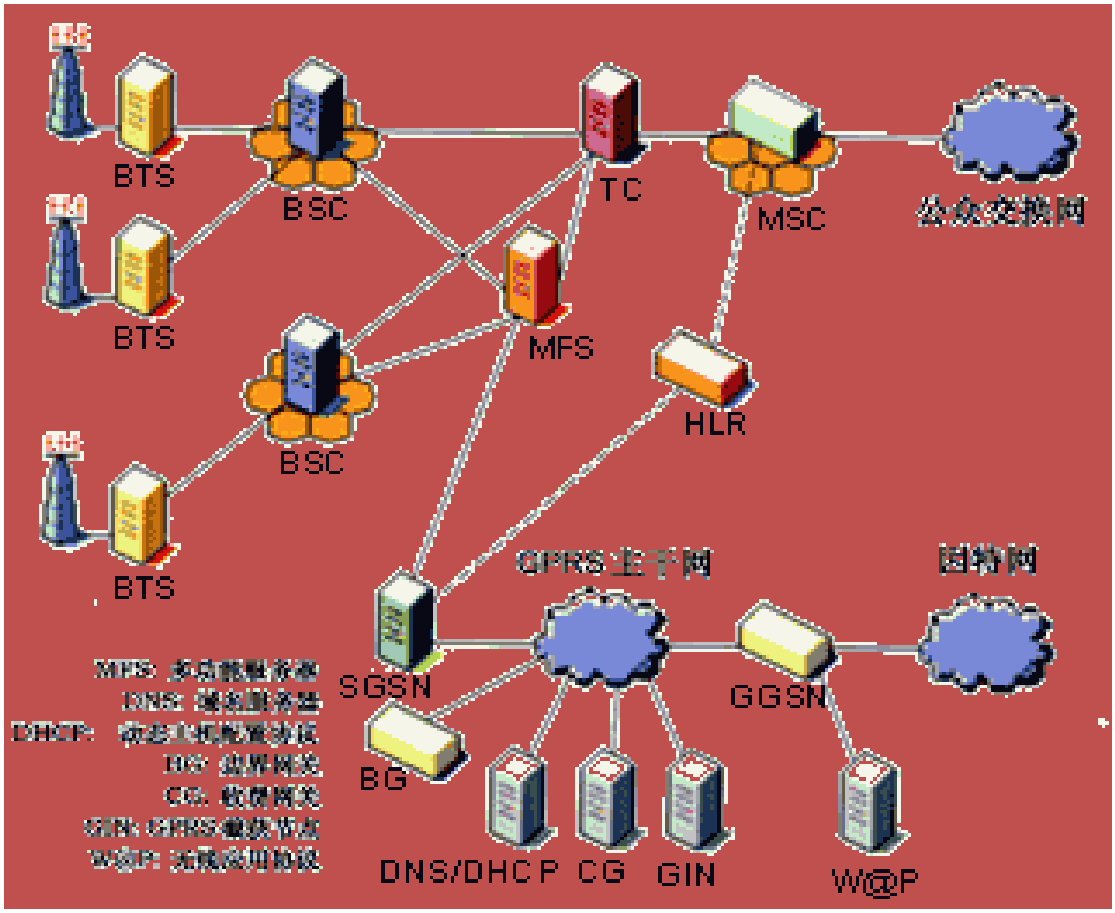
传输速率: 室外 <30km/h 384kb/s

室内 <3km/s 2Mb/s

- 欧洲：直接扩频 美国：多载波

- GPRS 系统结构

GGSN: Gateway GPRS Supported Node
SGSN: Serving GPRS Support Node



- GPRS

- 通信过程：

所有与路由数据传输有关的信息存储在 HLR 中。对用户 A 到用户 B 的数据业务，源 SGSN-S 把它从 BTS 发送到 BSC，BSC 接受后对它进行封装，

然后路由到 GGSN，在检查分组的目的地址后通过现有的分组交换网络送到目的 GGSN，再送到目的 SGSN-D，在 SGSN 进行解封装，再利用 GSM 系统的基站传送到目的移动终端。

- 网关支持节点 GGSN（Gateway GSN）

主要作用：网关，亦称作 GPRS 路由器。与外部网络的逻辑接口，可和多种不同数据网络连接，如 ISDN、PSPDN 和 LAN 等，如把 GSM 网中的 GPRS 分组数据包进行协议转换，从而将其传送到远端的 TCP/IP 或 X.25 网络。

- 服务支持节点 SGSN（Serving GSN）- GPRS 网络中最重要的网络节点。

主要作用：记录移动台的当前位置信息，并且在移动台和 GGSN 之间完成移动分组数据的发送和接收，完成数据传送和格式转换。SGSN 负责认证管理。

- GPRS 可让多个用户共享某些固定的信道资源。如果把空中接口上的 TDMA 帧中的 8 个时隙都用来传送数据，那么数据速率最高可达 164kb/s.
- GSM 空中接口的信道资源既可以被话音占用，也可以被 GPRS 数据业务占用。在信道充足的条件下，可以把一些信道定义为 GPRS 专用信道。GPRS 能让通信永远在线，GPRS 可使重要数据均可在语音呼叫之外一个独立信道自由进出而不影响正常通话。
- GPRS 网络的传输速度最快将达到 115K，其上网速度比 PC 使用的 56.6kbps Modem 上网速率还要快；其收费方式是以流量的多少计算费用，用户只需按实际传送的数据量付费。

- 国内 2.5G 移动通信技术对比状况：
  - 中国移动 GPRS 网络已覆盖全国 200 多个城市。
    - 通过 GPRS 接上 Internet ，面向便携机的基于 PCM CIA 或 USB 卡的无线上网服务，“随 e 行” 。用户一次性交纳 2400 元，就获得一块 GPRS 网卡、一张专用数据 SIM 卡以及不限时，不限流量的上网服务。理论峰值 171.2Kbps，标称 30～40Kbps，实际上平均传输率 4.02Kbps。稳定性好些，覆盖范围大。
    - 最近，“随 e 行”进行了升级，提供“双模”卡，内置 GPRS 和 WLAN 双功能，这样就可以在热点地区使用 WLAN 上网。

- 中国联通 CDMA 1X 只在全国省会城市开通，速度快些。
    - “掌中宽带”比中国移动时间上晚一年， 网卡价格 2000 元左右，资费标准：每月资费 50 元，每月流量 100MB，超过部分资费每 KB0.005 元；每月资费 200 元，每月流量 500MB，超过部分资费每 KB0.005 元；每月资费 300 元，每月流量 2000MB，超过部分资费每 KB0.005 元。标准理论峰值 1531.6Kbps，平均传输率 7.11Kbps

4.8 第三代移动通信技术

- UMTS（Universal Mobile Telecommunications System）
    - 3GM 关键技术：
        - 初始同步技术，RAKE 接收技术，高效通路编码技术，功率控制技术
    - 支持宽带多媒体业务
        - 高质量话音， 分组数据业务，实时的视频传输，开创无线通信，因特网与多媒体融合的新时代
    - 3GM 与中国
        - 2GM 我国错过机会， TD-SCDMA 是我国提交的 3GM 标准，已获多方认同
- IMT 2000（International Mobile Telecommunications 2000）
    - 1. 第一个采用全球统一标准的移动通信系统，用户可以在全球范围内实现漫游；
    - 2. 一个针对宽带数据通信设计的系统，工作在 **2GHz** 频段，提供 **2Mbps** 的传输速率和 **5MHz** 以上的带宽，不仅进行话音通信，更可以进行移动的多媒体通信；
    - 3. 将把固定网、卫星网和地面移动网结合成一个综合的整体网络。将使电信网和计算机网络更加紧密的结合，消除传统话音通信和数据通信之间的界限。

- 3G 的目标
  - 全球统一频段、统一标准，全球无缝覆盖
  - 高效的频谱效率
  - 高服务质量、高保密性能
  - 易于 2G 系统演进过渡
  - 提供多媒体业务
    - 车速环境：144kbps
    - 步行环境：384kbps
    - 室内环境：2048kbps
- 3G 的历史
  - 1985：FPLMTS，1996 更名为 IMT-2000
  - 1992：WRC'92（世界无线电大会）分配频 230MHz
  - 1999.3：完成 IMT-2000 RTT 关键参数
  - 1999.11：完成 IMT-2000 RTT 技术规范
  - 2000：完成 IMT2000 全部网络标准
- 3G 标准化组织及其标准
  - 国际电信联盟(ITU)通过的 3G 标准有三个：
    - 1. W-CDMA: 以欧洲、日本 27 家公司为主提出。
    - 2. CDMA 2000: 以北美高通公司提出。
    - 3. TD-SCDMA: 以我国大唐电信牵头、西门子联合提出并最终由中国无线通信标准组织（CWTS）提出。

      FDD 频段： W-CDMA，CDMA 2000

      TDD 频段： TD-SCDMA
- 两大协调组织

- 3GPP（Third Generation Partnership Projects），负责协调 WCDMA。TD-SCDMA。其成员：ETSI、（日）ARIB、（韩）TTA、（美） TIA 及（中国）CCSA
- 3GPP2（Third Generation Partnership Projects 2），负责协调 CDMA 2000。 其成员有：TIA、ARIB、TTA 及 CCSA（中国通信标准化协会）

- 中国 3G 频谱分配（2002 年 11 月）
  - IMT 2000、欧洲的频率划分和中国一致
  - 北美的频率划分与中国的核心频段冲突
  - 第三代公众移动通信系统的工作频段为：
    - （一）主要工作频段：
      - ✓ 频分双工（FDD）方式：1920 - 1980MHz / 2110 - 2170MHz；
      - ✓ 时分双工（TDD）方式：1880 - 1920MHz、2010 - 2025MHz。
    - （二）补充工作频率：
      - ✓ 频分双工（FDD）方式：1755 - 1785MHz / 1850 - 1880MHz；
      - ✓ 时分双工（TDD）方式：2300 - 2400MHz，与无线电定位业务共用，均为主要业务，共用标准另行制定。
    - （三）卫星移动通信系统工作频段：
      - ✓ 1980 - 2010MHz / 2170 - 2200MHz。

第五章 移动 IP 原理

5.1 移动 IP 概述

- 传统 IP 工作原理及局限性

- IP 地址有两个部分：
  - 网络前缀部分
  - 主机部分网络
- 网络前缀看成是用来标识一条链路的，而主机部分是用来标识连接在链路上的一台特定主机或路由器的。
- 前缀长度指明了一个 IP 地址网络前缀部分的比特数
- 另一种 IP 地址及其前缀长度的简写方式为：地址/前缀长度，　例：129.61.18.26/24
- 对于一个节点来说,有两类 IP 包:
  - 一类是包的目的端点就是这个节点本身;
  - 另一类包的目的端点为其它节点。
- 节点通过比较自己的 IP 地址和 IP 包中的目的地址,判断自己是否是目的端点。
  - 如不是，转发
  - 转发决策依据——IP 路由表
  - 如是，根据 IP 报头中的协议类型域送交相应的高层协议处理。

传统 IP 的局限性

当主机 2 切换到主机 B 与路由器 B 相连的那条链路上时，从分支节点到旧链路，沿途所有节点内的特定主机路由必须删除；从分支节点到新链路，沿途所有节点必须加入特定主机路由。

传统 IP（特定主机路由）能否解决移动问题？

- 必须至少向从移动节点的家乡链路至外地链路沿途的所有节点传送特定主机路由；
- 每次节点切换路由时，上面那些路由中的一部分（最坏的情况下是全部）必须进行更新；
- 在以后的几年，互联网上可能有几百万个移动节点，因此，为全面解决互联网的移动性，上面 2 条所说的数目都得乘上几百万；

- 存在严重的安全问题，需要认证机制和复杂的地址管理协议。

- 改变 IP 地址能否解决移动问题？
  - 节点的 TCP 连接由以下 4 个值唯一确定：源 IP 地址、目的 IP 地址、源 TCP 端口号、目的 TCP 端口号。
  - 这 4 个值在一个 TCP 连接的整个过程中是保持不变，当目标节点的 IP 地址发生变化时，这个约定将断开连接。
  - 特定主机路由方案存在着严重的可扩展性、可靠性和安全性问题，因此，用这种方案解决全球互联网上节点的可移动性是不可行的。
- 移动计算网络
  - 移动计算网络应具备如下特征：
    - 主机可在网中自由移动；
    - 当网中某处的主机移动至另一处时，用户无须进行任何操作仍能象在原处一样保持与网络的连接。
    - 移动对上层应用是透明的，或者说上层应用意识不到主机的移动。
    - 用动态地址自动配置的方式接入网络不是移动 IP
  - 各部分功能
    - MH （移动主机）：可在小区内或整个 Internet 范围内移动的设备。
    - AP（无线接入点）：MH 接入 Internet 所需的设备
    - MA（移动代理）实现 MH 的网间漫游管理；
    - 其它设备均为现在 Internet 上的通用设备。
  - 在移动计算网络环境下，存在这样两种不同层次的移动：
    - 链路层移动：指移动主机在同一 IP 子网内移动
    - 网络层移动：指移动主机在跨子网的移动

- 在链路层的移动仅涉及到移动主机、移动前的无线接入站及移动后的无线接入站。我们把这种移动称为散步（Walking）。
- 在网络层的移动指移动主机在不同 IP 子网之间的移动，除了涉及到有关的移动主机及无线接入站以外，还涉及到移动管理路由器，该路由器完成网际间的漫游管理和用户身份认证等处理。我们把这种移动称为漫游（Roaming）。
- 主机的移动透明性包含两方面的含义：
  - 一是操作透明性，指主机的移动并不引起应用软件的重新配置、重新启动等操作。
  - 二是性能透明性，指应用软件的性能并不由于主机的移动而大幅度劣化。
- 移动透明性是实现移动计算网络的重要指标。如果移动透明性得以保证，则使用 MH 的用户无须顾及自己是否在移动。
- 移动 IP 主要关心的是跨子网的网络层漫游，并保证移动的透明性。

移动 IP 的发展过程

- 第一个移动主机协议称作 Mobile *IP,由哥伦比亚大学的 John Ioannidis 设计。它的主要思想是使用虚拟移动子网和 IPIP(IP in IP)打包。
- 几乎与此同时，Sony 公司的 Fumio Terqoka 设计了另一种移动主机协议，虚拟 IP（VIP）。VIP 协议使用了特殊的路由器来记忆移动主机的位置，并定义了新的 IP 头选项来传递数据。

移动 IP 协议的发展

- 不久后 IBM 的 C. Perking 和 Y.Reckter 也设计了一种移动主机协议,这种协议利用了现有 IP 协议中的可选功能——松散源选径（Loose Source routing)来支持主机的移动。
- 1994 年 A. Myles 和 C. Perking 分析了前三种移动主机协议的优缺点，重新设计了一种协议：MIP，并将它提交给互联网学会下属的工程技术委员会(IETF)。MIP 后来发展成了下面我们将要详细讨论的 Mobile IP 协议。

- 移动 IP 是一种在全球互联网上提供移动功能的方案，具有可扩展性较高、可靠边性较强和安全性较高等特点，并使节点在切换链路时仍可保持正在进行的通信。
- 值得特别注意的是，移动 IP 提供了一种 IP 路由机制，使移动节点可以用一个永久的 IP 地址连接在任何链路上。
- 移动 IP 是在互联网中提供移动功能的网络层方案，与运行在什么媒介上无关（与底层的链路特性无关）。
- 蜂窝式数字分组数据和 802.11 只提供同质移动功能，不能在不同媒介的网络间提供移动功能。移动 IP 同时具有同质移动和异质移动功能，这是独一无二的。
- 同一年中，卡耐基.梅隆大学（CMU）的 D.B.Johnson 设计了 MHRP 协议，它的思想很类似于松散源选径。不同之处是源选径是利用 IP 头的选项，而 MHRP 重新定义了一种打包协议来代替源选径。
- 不管是 MHRP 还是 MIP 在安全性上都存在严重的问题。因此，A. Myles、C. Perking 和 D.B.Johnson 共同制定了 IMHP，IMHP 引入了一种新的安全机制并提出了简单认证的概念，后来这一概念被 IPv6 所借鉴。

- IETF 移动 IP 协议体系
  - IETF 的网间漫游工作小组一直致力于在 Internet 上提供主机可移动性的标准。该工作组已提出了在现存的 IP 协议之上实现网间漫游的基本框架。
  - 主机漫游软件的研发在国际上也是个热点课题，CMU、纽约大学、瑞典皇家学院、FTP Softeare、IBM、Motorola、Nokia、SUN、Telxon 等的研究机构都在进行这方面的研究。
  - 由于现在因特网协议为 IPv4，所以移动 IP(Mobile IP)系统 也表示采用因特网协议版本 4 的节点构成。
  - 随着因特网的发展，出现了支持更多节点数目、更加适合移动的因特网新版本，称为 IPv6，对应的漫游协议为移动 IPv6。
  - 移动 IP 对应的主要文献为 RFC2002 和 RFC2003 (RFC: Request For Comments)

- 获取方法：ftp://ds.internic.net/rfc/rfcNNNN.txt NNNN 表示想要的 RFC 的文件号
- 所有已发表的 RFC 文件的"索引"：ftp://ds.internic.net/rfc/rfc-index.txt

5.2 移动 IP 的组成

- 在 IETF 的 Mobile IP 的草案中涉及到漫游的实体有：
  - MH(Mobile Host:移动主机)
  - HA(Home Agent:家代理)
  - FA(Foreign Agent:外地代理)
- HA 和 FA 可统称为 MA(Mobile Agent:移动代理)

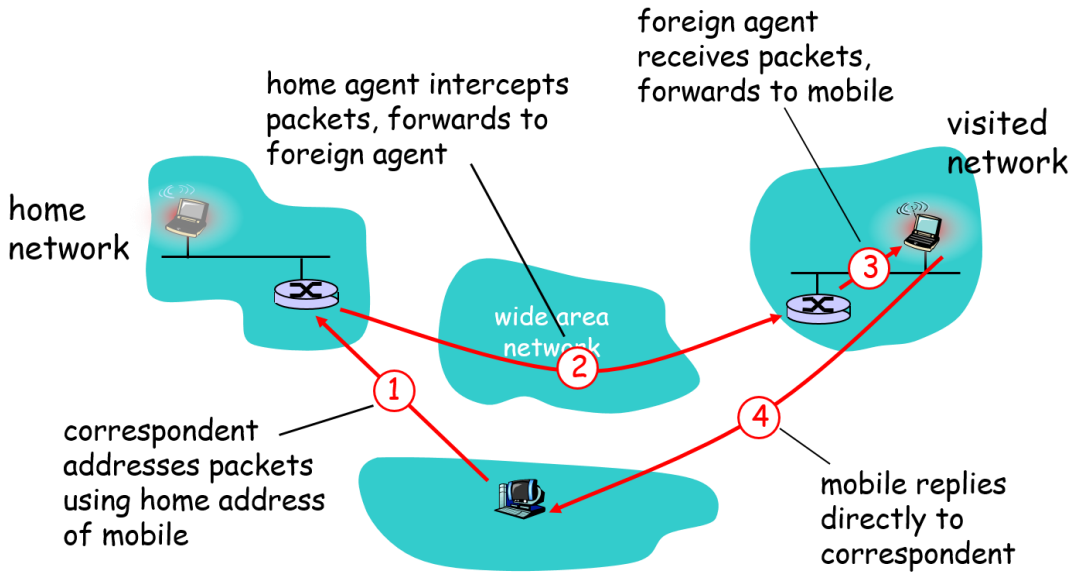
- 转交地址（Care of address）
  - 当 MH 漫游到外地网时，它从外地代理 FA 处获得一个转交地址并通知其家代理 HA。
  - 分为外地代理转交地址和共处转交地址（DHCP 获得）
  - MH 的 HA 将把发给该 MH 原来地址的 IP 包接收下来并重新打包后发送到 MH 的转交地址（通常是 FA 的 IP 地址），再由其转交至 MH。
  - 使用转交地址而不是临时借用外地网的 IP 地址的主要原因是为了克服现在 IP 地址不足的困难。
- 隧道(Tunnel)
  - 当 MH 漫游到外地网时，由于其它主机并不知道它已漫游，故发给它的 IP 包仍然送至其家网。
  - MH 的 HA 将把这些 IP 包接收下来并重新打包后发送到 MH 的 FA。
  - 所谓 MH 的隧道，指由 HA 至 FA 的用来传送这些重新打包后的 IP 包的通道。在隧道的发送端，HA 依据隧道协议把需传送的 IP 包重新打包，在接收端 FA 完成拆包。
- 代理搜寻(Agent discovery)

- MH 开机后，确定自己是在家网还是在外地网的过程称为代理搜寻。
- 代理搜寻的方法有两种：由代理（FA 或 HA）发送代理公告（Agent advertisement）报文的方法和由 MH 发送代理请求(Agent solicitation)报文的方法。
- 前者由代理定期地发送代理公告广播报文，MH 接收到该报文后判断自己处在何处。后者由 MH 主动发送代理请求广播报文，依据 HA 或 FA 的应答报文 MH 判断自己处在何处。

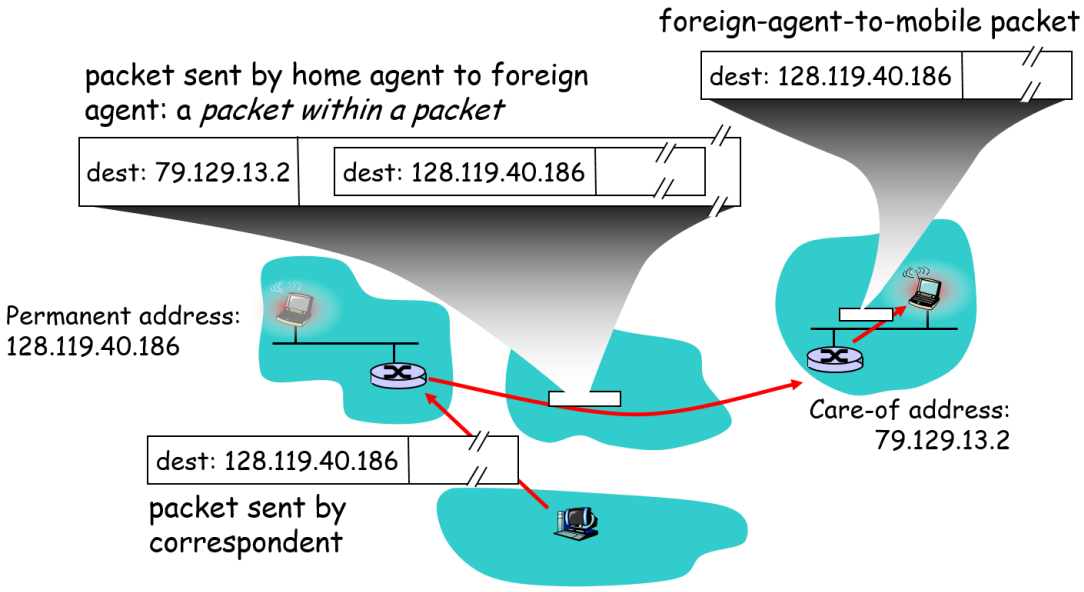
- 登录或注册(Registration)
  - 当 MH 获得转交地址后，通知其 HA 并设置好其隧道的过程称做登录或注册。
  - 由 MH 通过 FA 或直接向其 HA 发出注册请求(Registration request)报文。前者在使用转交地址情况，后者是用共处转交地址。
  - HA 修改 MH 的位置信息并设置好隧道后，向 MH 返回注册应答(Registration reply)报文。

5.3 移动 IP 的基本步骤

- Mobility via Indirect Routing



- Mobile IP: indirect routing



- 移动 IP 的工作过程
  - MH 利用代理搜寻功能检测自己已处于漫游状态，并获得转交地址；
  - MH 向 HA 注册；
  - HA 收集发给 MH 的 IP 包，并利用其隧道发给 MH；
  - 不论 MH 是否漫游，它使用现在的 IP（版本 4.0）协议发送 IP 包。
  - 如图，假设 MH1 由子网 A 漫游至子网 B。这时，MH1 检测到自己的移动后首先从外地代理 FA2 获得转交地址，然后向家代理 HA1 注册。
  - 子网 C 中的固定主机 SH 向 MH1 发送 IP 包。由于 SH 向 MH1 发送 IP 包时仍然使用 MH1 原来的 IP 地址，故发出的包将到达子网 A。HA1 把这些 IP 包接收下来后，并利用 HA1 至 FA2 的隧道把它们转送给 FA2。最后由 FA2 把从这些包转交给 MH1。
- 移动 IP 实体及相互关系

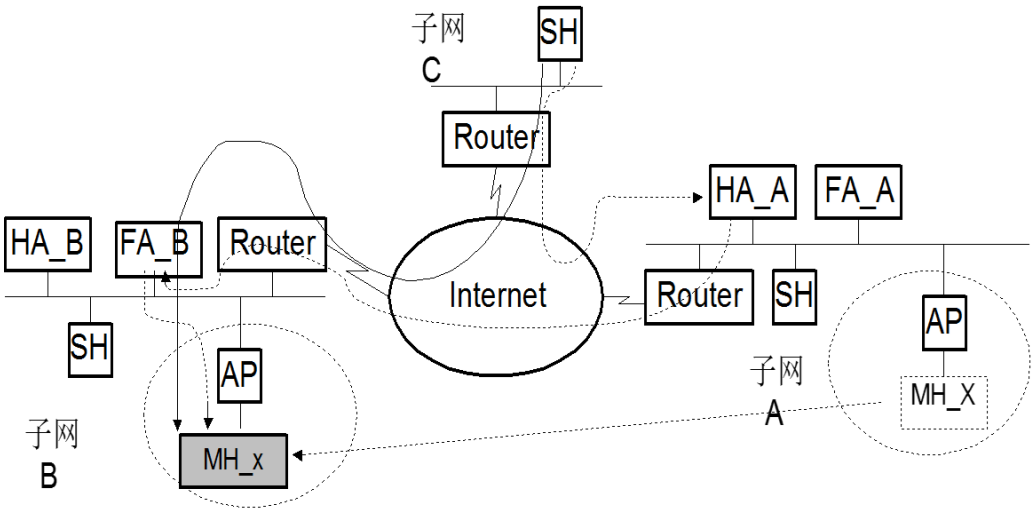
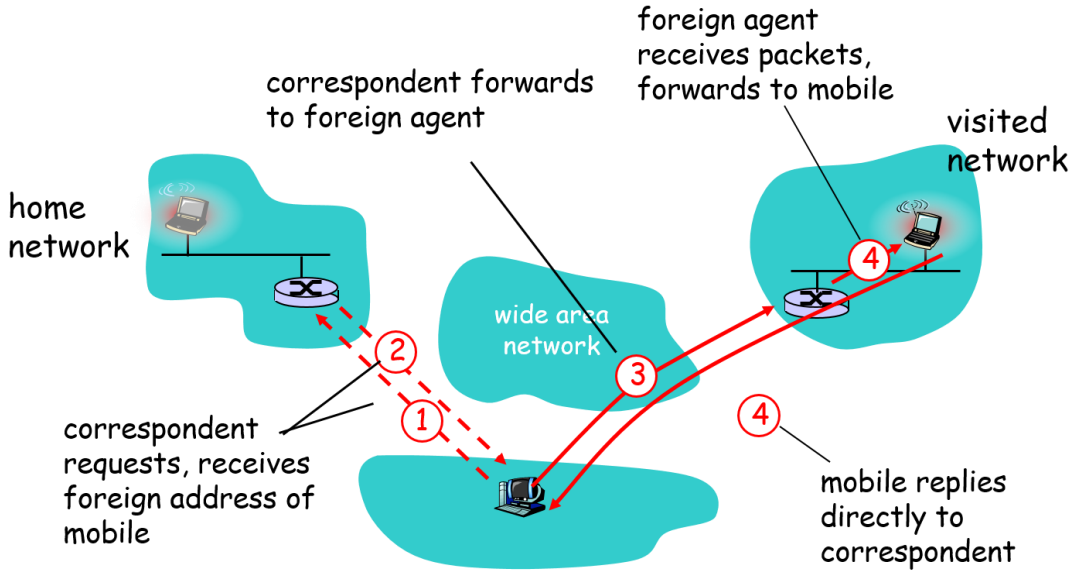


图 移动IP实体及相互关系

- 移动 IP 的工作过程
  - 图中的虚线示出了 IP 包的路经。我们可以看到这并非最佳路由，这将导致效率的严重下降，上层网络应用程序的传输速率将降低一半左右。
  - 图中的实线是经过路由优化后的 IP 数据报的路径。它可以达到或接近最佳路由。
- Mobility via Direct Routing



- 移动 IP 的工作过程
  - 路由优化的原理

- 移动主机的家代理将移动主机的转交地址通知与移动主机通信的节点，此节点将移动节点当前的转交地址存储起来
- 用隧道将它们自己的数据直接送到移动节点的当前位置。
- 当移动主机漫游到新的子网时，会搜寻一新的外地代理，并注册、得到新的转交地址。
- 移动主机将会通知原外地代理它已漫游到新的子网中。
- 移动主机的家代理也将通知与移动主机通信的节点更新其存储的移动主机的转交地址。

- 可以把路由优化总结成漫游处理的第五步：
  - 移动主机和其家代理分别通知其它相应节点自己的移动，其它节点根据这一信息进行路由优化。

第七章 无线网络安全

7.1 网络安全及其基本属性

- 计算机网络与信息安全的性能指标
  - 保密性(confidentiality)：就是保证信息不泄漏给未经授权的人。信息的保密性包括传输过程中的保密性和存储时的保密性。
  - 完整性(integrity)：就是防止信息被未经授权地篡改，即防止信息在传输和存储过程中被非法修改、破坏或丢失，并且能够判断出信息是否已经被修改；目的是要保证信息在传输和存储过程中的一致性。
  - 可用性(availability)：就是保证信息及信息系统确实为授权使用者所用，即系统要保证合法用户在需要时可以随时访问系统资源。
  - 可控性(controllability)：就是指网络应具有可管理性，能够根据授权对网络及信息系统实施安全监控，使得管理者能够有效地控制网络用户的行为和网上信息的传输。

- 不可否认性(non-repudiation)：也称为不可抵赖性。即通过记录参与网络通信活动的双方的身份认证、交易过程和通信过程等，使得任何一方无法否认其过去所从事的活动。

- 网络的安全威胁
  - 黑客攻击
    - 非授权访问
    - 对信息完整性的攻击
  - 拒绝服务攻击
    - 异常型
    - 资源耗尽型
  - 恶意代码
    - 计算机病毒
    - 特洛伊木马
    - 计算机蠕虫
- 网络信息安全技术
  - 数据加密技术
  - 防病毒技术
  - 防火墙技术
  - 身份认证技术
  - 访问控制技术
  - 漏洞扫描技术
  - 黑客跟踪技术
  - 入侵检测技术
  - VPN 技术
  - 安全审计

- 数据备份
- 安全管理技术

- 密码学与数据加密

  密码理论与技术的分类

  - 基于数学的密码理论与技术
    - 对称密钥密码体制、非对称密钥密码体制、认证码、Hash 函数、身份认证、数字签名、密钥分配与管理、PKI 技术
  - 基于非数学的密码理论与技术
    - 信息隐藏与数字水印、量子密码、基于生物特征的识别理论与技术、混沌密码、热流密码

- 对称密钥密码体制
  - 对称密钥密码体制 ←→ 私钥密码体制
  - 特点：
    - 加密和解密使用相同的密钥，故称为对称密钥。
    - 使用的密钥只有加密者和解密者知道，对外不能公开，否则就起不到加密的作用，故称为私有密钥，简称私钥。
    - 加密依赖于加密密钥的安全性。
  - 分组密码
    - 以多个数据位形成的分组为单位进行加密
  - 序列密码
    - 以位为单位进行加密
  - 典型的对称密钥加密算法：DES、IDEA、AES 等

- 非对称密钥密码体制
  - 非对称密钥：加密过程和解密过程使用不同的密钥

- 注意：解密密钥是保密的，而加密密钥是公开的，所以这种加密体制又称公开密钥密码体制
- 优点：
  - 密钥分发方便，可以以公开的方式分配加密密钥。
  - 密钥保管量少。网络中的数据发送方可以共用同一个公开加密密钥，从而减少密钥的数量。
- 常用算法：RSA 体制、ELGamal 体制、椭圆曲线密码体制

- 混合密码体制
  - 原理：利用公钥密码体制加密私钥密码体制的密钥，消息的收发双方共用这个密钥，然后按照私钥密码体制的方法进行加密和解密运算。
  - 混合密码体制的加密过程
    - ①用对称密钥将要发送的消息加密
    - ②用接收方的公开密钥将对称密钥加密，形成数字信封
    - ③封装成数据包
    - ④用自己的私钥解密其中的数字信封，得到发送方加密信息的对称密钥
    - ⑤用获得的对称密钥解密数据包中的加密信息
- 常见的密码算法
  - 流行的密码算法：DES、AES、RSA、IDEA、DSA
- 消息认证
  - 消息认证（message authentication）也称为消息鉴别或者报文鉴别，它用来验证用户的身份，对访问的请求、消息的内容等进行识别，确定消息是否被篡改。常采用由消息生成验证码的方法对消息进行认证。
  - 消息认证方法
    - 消息加密
    - 消息验证码

- 杂凑码

- 数字签名
  - 数字签名是手写签名的电子模拟，是通过信息处理技术产生的一段特殊数字消息，该消息具有手写签名的一切特点，是可信、不可伪造、不可抵赖和不可修改的。与手写签名一样具有同等的法律效力。
  - 数字签名至少应满足的三个条件
    - 签名者事后不得否认自己的签名
    - 接收者能够验证签名，而任何其他人都不能伪造签名
    - 当双方就签名的真伪发生争执时第三方能够进行仲裁
  - 数字签名方案的组成
    - 签名算法: 签名算法的密钥是秘密的，只有签名人掌握
    - 验证算法: 验证算法则是公开的，以便他人进行验证
  - 签名和加密的区别
    - 加密：保护信息不被非授权用户访问
    - 签名：让接收者确认消息的发送者是谁，以及消息是否被篡改
- 采用公钥加密 RSA 体制进行数字签名的基本流程

发送前Tom对电子合同进行签名

① 使用杂凑函数处理电子合同，生成一个消息摘要

② 使用自己的私钥加密消息摘要，形成一个数字签名

③ 将电子合同和数字签名一起发送给 Bob

Bob对Tom发送来的报文进行鉴别

① 使用与 Tom 相同的杂凑函数计算出接收到的电子合同的消息摘要

② 使用 Tom 的公钥解密来自 Tom 的消息摘要，恢复 Tom 原来的消息摘要

③ 将自己生成的消息摘要与 Tom 原来的消息摘要进行比较；若两者相同，则表明电子合同确实来自于 Tom；若两者不同，则表明电子合同或者不是来自于 Tom，或者电子合同的内容已被篡改。

- 公开秘钥基础设施
  - PKI（Public Key Infrastructure）
  - 功能：
    - 密钥的产生、存储、分发、撤消和管理等，为网络应用提供密钥和证书的管理、证书的认证、数据加密、数字签名等服务，是国家信息化基础设施的重要组成部分。
    - PKI 采用证书管理公开密钥，通过第三方可信任的认证中心，把用户的公开密钥和其它用户标识信息捆绑在一起，在网上实现密钥的自动管理和用户身份的认证，它为电子商务、电子政务等网上业务的开展提供一整套安全基础设施。
- 数字证书
  - 数字证书：是由权威机构 CA（Certificate Autority）发行的一种电子文档，是网络环境下的一种身份证，用于标识用户的身份及其公开密钥的合法性。
  - 数字证书的特点：
    - 证书中包含用户的身份信息，因此可以用于证明用户的身份。
    - 证书中包含非对称密钥，不但可以用于数据加密，还可以用于数字签名，以保证通信过程的安全性和不可抵赖性。

- 由于证书是由权威机构颁布的，因而具有很高的公信度。

- 数字证书的原理：是基于公开密钥密码体制，每个用户均拥有两个密钥：公钥和私钥；其中私钥用于解密和签名，而公钥则是提供给其它用户使用，用于数据的加密和验证签名。

- 数字证书的分类

  - 系统证书
  - 用户证书
    - ✓ 个人数字证书
    - ✓ 机构数字证书
    - ✓ 个人签名证书
    - ✓ 机构签名证书

7.2 无线网络安全分析

- 无线网络安全威胁：

  - 1、无线链路上的威胁
    - 非授权访问数据
    - 完整性威胁
    - 拒绝服务攻击
  - 2、服务网络的威胁
    - 非授权的访问数据
    - 完整性的威胁
    - 拒绝服务攻击
    - 非授权的访问
    - 否认

- 3、终端威胁
  - 与访问控制相关
  - 与数据完整性相关
  - 复制 SIM 卡
  - 与病毒相关

- GSM 网络安全分析

  目前，GSM 网络安全主要针对语音业务保护，主要包括：

  - （1）通过鉴权防止未授权的用户，维护运营商和用户利益。
  - （2）通过无线信道传输的加密，保护用户的隐私。
  - （3）以独立于终端的设备（SIM 卡）管理用户信息。
  - （4）以一个临时代码代替用户标志，使第三方无法在无线信道上跟踪用户。

- GSM 系统的认证机制

  - GSM 系统认证基于私钥体制。在手机 SIM 卡中存储用户国际移动用户标志(IMSI)和用户私钥(Ki)，在服务网认证中心数据库存储了用户标志(IMSI)和用户的私钥(Ki)。
  - 当移动终端(MS)需要呼叫或更新位置时，则需要网络认证。认证中心根据 IMSI 找到用户 Ki，然后产生认证三元组 TRIPLE：

    （RAND，XRES，Kc）

    RAND：128 位随机数

    XRES：期望响应数（认证码），由 A3 算法产生

    Kc：会话加密密钥, 由 A8 算法产生
  - 认证中心将这个三元组发给移动交换机服务区 MSC/VLR，然后 MSC/VLR 将其中的 RAND 发给 MS，MS 的 SIM 卡根据接收到 RAND 和存在卡中的 Ki，利用 A3 和 A8 算法分别计算出用于认证的响应 XRES 和加密密钥(Kc)，并通过无线接口将 XRES 和 KC 送回 MSC/VLR。

- 在 MSC/VLR 中，会比较两个 RES，如果不同，则认证失败。如果相同，则认证成功 .
- 用户可以使用网络服务并且在后面的通信过程中用户和基站之间通过无线线路的通信 用各自计算出来的 Kc 作为密钥加密。

- GSM 数据加密过程
  - 加密方法：在无线链路上的数据流是通过用户的数据流和密钥流逐比特相加来获得的。将明文组织成 114 位的数据块。
  - 利用 A5 算法产生密钥流，

    输入为：64 位 Kc 与 22 位 TDMA 帧号逐位相加；

    输出为：密钥流 S1 114 位，密钥流 S2 114 位。
  - 将明文的 114 位数据与输出的密钥流逐位相异或产生密文
  - 接受端用同样的方法与密文逐位相异或得到明文
  - 在 MS 中，加密用 S2，解密用 S1；在网络中，反之。
- 用户身份保护
  - 方法：用 TMSI(临时移动身份)隐藏 IMSI （移动用户标志），其中访位置寄存器 VLR 负责管理 TMSI 和 IMSI 的对应。
  - GSM 加密范围：移动台(MS)和基站(BSC)分别采用 A5 算法加密，即只对无线部分进行加密。
- GSM 系统的安全缺陷

  1、单向身份认证，无法防止伪造的网络设备的攻击。

  2、加密密钥及认证数据使用明文传输，易造成密钥泄露。

  3、加密功能只用在空中接口，没有延伸到核心网络，如基站和基站控制器的传输链路中用户信息和信令信息都是以明文传输。

  4、用户身份认证密钥不可变，无法抵挡重放攻击。

  5、用户漫游时，服务网络与归属网络间缺乏有效联系。

6、无第三方仲裁机构，当各网络实体出现纠纷，无法提交 给第三方仲裁机构

7、缺乏安全升级能力与安全可见性，不提示是否在加密。

8、加密和认证算法不公开，密钥匙太短。

7.3 无线局域网安全问题分析

- WLAN 安全
  - 由于无线电波没有物理边界的特性，而且无线 LAN 的接入非常简单，就存在恶意使用的危险。所以比其他网络技术更需要一种对无线节点接入认证和授权的机制。
  - WLAN 安全性集中在：认证、加密、数据完整性
    - 认证是对用户身份的检测，阻塞非法使用
    - 加密是保证数据在传输过程中不被窃取和篡改
  - WLAN 安全解决方案可从软硬件两方面着手：透过内建软件安全关卡或在硬件上进行加密处理。软件方案增加 CPU 负担，成本较低，硬件方式则正好相反。
- IEEE 802.11 安全机制
  - IEEE 802.11 物理层安全
  - IEEE 802.11 链路层安全
  - IEEE 802.11 网络层安全
- 无线局域网物理层安全
  - 直接序列扩频
  - 跳频技术
- 直接扩频序列的缺陷

直接扩频系统（DSSS）使用一个众所周知的 11 位扩频序列，并能调制该标准中规定的 14 个信道中的一个。

不过，由于使用的序列事先知道，且系统载频又是固定的，而且可能的频率数目也是有限，所以，黑客可以容易地收到 DSSS 传送的信号。

- 无线局域网链路层安全
  - 有线等效保密协议
    - WEP-Wired Equivalent Protocol
  - WEP 的三个预期目标
    - 机密性
    - 访问控制
    - 完整性
- WLAN 安全

WEP 手动设置接入密码，当 AP 中设定 WEP 加密认证后，就可将不知道密码的用户排除在外。但密码在所有终端上都相同，很容易被窃取。

WEP 应用于物理层和数据链路层，采用 64 位(或 128 位)共享密钥和 RC4 流密码加密算法，用来保护无线传输过程中的链路级数据的协议。

Almost permanent key, very week security, able to crack by collecting statistic.

Current security level for 99.9% products on the market.

- WEP 共享密钥认证

在进行实际的数据通信之前,无线网络客户端必须与 AP 建立起通信关联。只有在客户与 AP 间关联后,客户间才能交换数据。关联过程有两步，涉及三种状态。

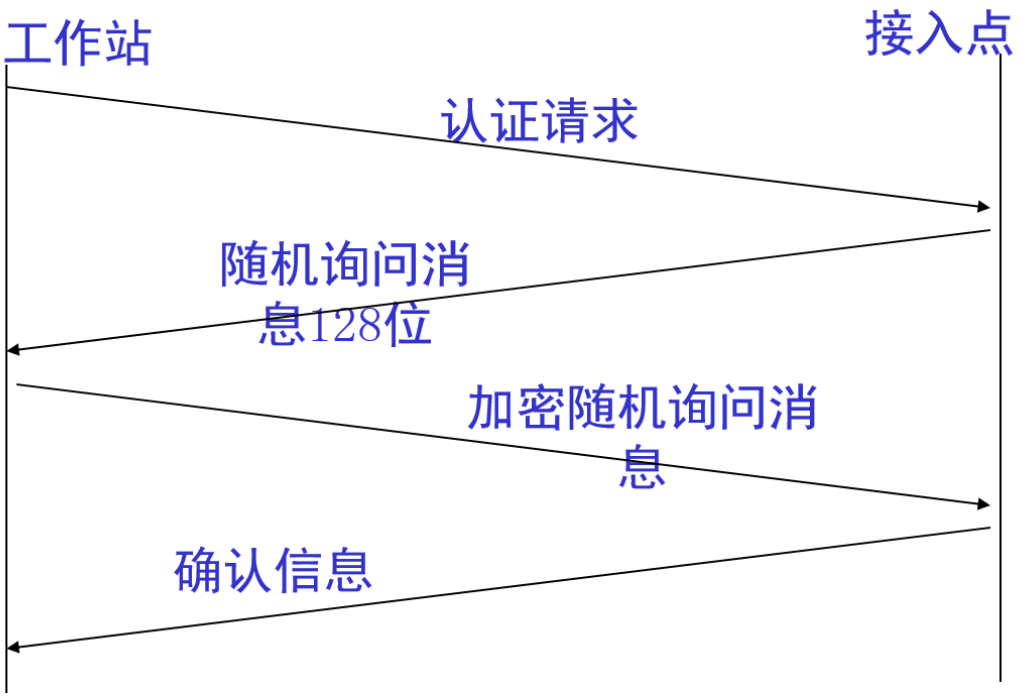
① 未认证，未关联；

② 通过认证，未关联；

③ 通过认证，关联成功。

为了从一个状态转换到另一个状态，通信双方必须交换被称为管理帧的信息报文。通过认证、关联成功后,客户端便成为无线网络中的一个实体，就可以在网络上进行数据传输了。

- 共享密钥认证过程



- WEP 加密原理
  - 1、对数据帧求校验和(使用 CRC-32 算法) 以获得 C(M)，其中 M 是消息。合并 M 和 C(M) 以获得明文 P = (M, C(M))；
  - 2、发送端随机选择一个 24 位初始向量 **IV**(Initiation Vector) 将之和 40 位共享密钥（ Secret Key ）连接在一起，输入 RC4 伪随机序列发生器（ PRNG SEUDORANDOM NUMBER GENERATOR ）产生伪随机序列，表示为 RC4(V,K)；
  - 3、发送端将明文 P = (M, C(M))和伪随机序列进行异或运算，产生加密数据；
  - 4、发送端初始向量 **IV** 放在密文前面，产生实际传输的数据流。

  解密只是与加密相反，接收方重新生成密钥流，并将它与密文进行 XOR 来恢复明文。该消息 P 被分成两个部分：M 和 C， 计算 C(M)并将它与接收到的校验和 C 进行比较。

  如果不匹配，那么消息主体在传输期间已经以某一方式更改过。

- WEP 的缺陷
  - WEP 算法的安全性在数学上取决于其密钥不易被发现。

- Nikita Borisov, 等人在 2001 年 1 月国际微波会议上的一篇论文指出了 IEEE 802.11 体系结构性安全弱点：如果用相同的初始向量 IV 和密钥加密两条消息，那么流密码(如 RC4) 容易受到攻击。 如果一起对密文进行 XOR 运算，那么密钥流将互相抵消且两个明文 XOR 将保留。
- 由于 WEP 中各安全要素以一种不安全的方式结合在一起，导致了其诸多的安全漏洞。
- 表现在：密钥管理、数据保密性、数据完整性、 认证的安全缺陷

- 密钥管理缺陷
  - 在 IEEE 802.11 标准中，缺少一种有效的密钥管理和分发机制。
  - 一般情况下，WEP 密钥被静态地分配给客户机，密钥或存储在客户机的磁盘存储器中，或存储在客户机的无线适配器的内存中。
  - 当客户机丢失后，非正常用户就具有了访问网络的权限，而管理员并不能检测到这种对网络安全的破坏。
  - 当接到机主的的报告后，管理员必须对与丢失客户机密钥相同的其他客户机的静态密钥重新编码。
- 数据保密性的缺陷
  - RC4 是一个序列密码加密算法，发送者用一个密钥序列和明文异或产生密文，接收者用相同的密钥序列与密文异或以恢复出明文。
  - 该加密方式要求不能用相同的密钥序列加密两个不同的消息，否则攻击者将可得到两条明文的异或值，如果攻击者知道一条明文的某些部分，那么另一条明文的对应部分就可被恢复出来(一般情况下，得到两条明文的异或值已足够恢复出其明文)。
- 数据完整性的缺陷

在 WEP 中，CRC-32 算法和 RC4 算法具有线性特性。这暗示了有一些控制校验和的方法，使协议可以接受它，但与消息内容无关。

另外，只要知道一部分信息包内容，就可以执行这类攻击。攻击者只要相应地调整校验和，就可以使被篡改的消息变为合法的消息。

- 认证的安全缺陷

- 在 IEEE 802.11b 中采用了两种认证方式：
  - 开放系统认证
  - 共享密钥认证
- 认证的目的是阻止非法的用户介入特定的无线局域网络共享密钥认证协议：通过窃听能够很容易蒙骗和利用现在的共享密钥认证协议, 协议固定的结构和 WEP 的缺陷是实现攻击的关键。

WLAN 安全

- TKIP（Temporal Key Integrity Protocol）-- 临时密钥完整性协议
  - WEP 改进，与现有硬件兼容(通过固件/驱动程序升级）
  - 仍然使用 RC4 算法，临时密钥为 128bit
  - 每传送 10000 个包改变临时密钥，且临时密钥与顺序号以及地址有关。
  - 过渡时期的方案。作为 Wi-Fi 联盟的 Wi-Fi 保护接入（WPA）主要内容，2003 年以后作为 Wi-Fi 的认证。
- 基于 AES(Advanced Encryption Standard)数据封装
  - 具有更高安全级别的加密，强度更大（特别是防止黑客帧插入有明显效果）
  - 需要硬件支持以及更强大的引擎
  - 构成坚固安全网（RSN）一种可选的功能
- 现有认证机制
  - ESS-ID

    AP 将客户使用的扩展服务集合标识（ESS-ID）与自己的进行比较，相同则开放通信信道。
  - MAC 地址过滤

    利用各个无线网卡具有不同的 MAC 地址，指示 AP 实施分组过滤，仅仅通过指定源 MAC 地址的数据。

- IEEE 802.1x 认证
  - 基于端口的网络接入控制，具体绑定了可扩展认证协议（EAP ）作为用户身份认证机制。
  - IEEE 802.1x 包括：STA 和 AP 上的端口接入实体 PAE、LAN 上的 EAP 封装和 RADIUS 认证服务器

- 无线局域网网络层安全
  - 服务配置标识符 SSID
  - 身份认证
  - 虚拟局域网 VPN
  - 访问控制列表
  - 端口访问控制技术（IEEE 802.1x）

- 服务配置标识符 SSID

在每一个接入点，写入一个服务区域认证 ID (WLAN ESSID)。

每当端点要连上接入，接入点会检查其 SSID 是否与其相同。如果不符，就拒绝给予服务。

- 虚拟局域网 VPN

VPN 是指在一个公共 IP 网络平台上通过隧道以及加密技术保证专用数据的网络安全性，它不属于 IEEE 802.11 标准定义。

但是，用户可以借助 VPN 来抵抗无线网络的不安全因素，同时还可以提供基于 Radius 的用户认证以及计费。

- 访问控制列表

将无线局域网络设定为只给特定的接入点使用，因为每一张无线网卡都有一个惟一的 MAC Address，只要将其分别输入接入点即可。

相反，如果有网卡被偷或发觉有存取行为异样，可以将这些 MAC Address 输入，禁止其再次使用。

利用这个存取控制，如果外来不速之客得知网络的 WLAN ESSID，它一样会被拒之于外。

- 端口访问控制技术（IEEE 802.1x）

  该技术也是用于无线局域网的一种增强性网络安全解决方案。

  当无线工作站与 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 为用户打开这个逻辑端口，否则不允许用户上网。

  IEEE 802.1x 除提供端口访问控制能力之外，还提供基于用户的认证系统及计费，特别适合于公共无线接入解决方案。

7.4 IEEE 802.11i 安全机制

- Wi-Fi 保护接入（WPA）
- 强健的安全网络 （RSN）
- WAPI (WLAN Authentication and Privacy Infrastructure)，即无线局域网鉴别与保密基础结构

- WAPI 介绍

  WAPI (无线局域网鉴别与保密基础结构)。

  WAPI 是针对 IEEE 802.11 中 WEP 协议安全问题，经多方参加，反复论证，充分考虑各种应用模式，由中国提出的 WLAN 安全解决方案-（属中国国家标准 GB15629.11)。

- WAPI 方案

  - 系统有移动终端、AP 和认证服务器 AS 组成；其中，认证服务器 AS 的主要功能是负责证书的发放、验证与吊销等；移动终端与 AP 上都安装有 AS 发放的公钥证书，作为自己的数字身份凭证。
  - 当移动终端登录至无线接入点 AP 时，在访问网络之前必须通过 AS 进行双向身份验证。根据验证的结果，只有持有合法证书的移动终端才能接入持有合法证书的无线接入点 AP。
  - WAPI 不仅可以防止非法移动终端接入 AP 而访问网络并占用网络资源，且还可防止移动终端登录至非法 AP 而造成信息泄漏。

- WAPI 工作原理

- 认证激活：当移动终端登录至 AP 时，由 AP 向移动终端发送认证激活以启动整个认证过程。
- 接入认证请求：移动终端向 AP 发出接入认证请求，即将移动终端证书与移动终端的当前系统时间发往 AP，其中，系统时间称为接入认证请求时间。
- 证书认证请求：AP 收到移动终端接入认证请求后，向 AS 发出证书认证请求，即将移动终端证书、接入认证请求时间、AP 证书并利用 AP 的私钥对它们签名构成证书认证请求报文发送给 AS。
- 证书认证响应：AS 收到 AP 的证书认证请求后，验证 AP 的签名及 AP 和移动终端证书的合法性。完毕后，AS 将移动终端证书认证结果(包括移动终端证书、认证结果及 AS 对其签名)、AP 证书认证结果(包括 AP 证书、认证结果、接入认证请求时间及 AS 对其签名)构成证书认证响应报文发回给 AP。
- 接入认证响应：AP 对 AS 返回的证书认证响应进行签名验证，得到移动终端证书的认证结果。AP 将移动终端证书认证结果、AP 证书认证结果以及 AP 对它们的签名组成接入认证响应报文回送至移动终端。由其验证 AS 的签名后，得到 AP 证书的认证结果并根据该认证结果决定是否接入该 AP。
- 私钥验证请求：AP 和 MT 都需要确认对方是否是证书的合法持有者，私钥验证请求包含实时产生的随机数，请求对方对其签名，以验证对方是否拥有该证书的私钥。该请求可由 AP 或移动终端发起。
- 私钥验证响应：包含对私钥验证请求中随即数据的签名，提供自己是证书合法持有者的证明。移动终端与 AP 之间完成了证书认证过程。若认证成功，则 AP 允许移动终端接入，否则解除其登录。
- 在证书双向认证结束后，若 AP 和移动终端可以利用合法证书的公钥进行会话密钥的协商，上述的私钥验证过程也可省略，实现密钥的集中、安全管理。