

表 6-1 IEEE 802.11 标准小结

标准	频率范围	数据率
802.11b	2.4~2.4835GHz	最高为 11Mbps
802.11a	5.1~5.8GHz	最高为 54Mbps
802.11g	2.4~2.485GHz	最高为 54Mbps

这 3 个 802.11 标准具有许多共同特征。它们都使用相同的媒体访问协议 CSMA/CA，我们稍后将对其进行讨论。这 3 个标准都对它们的链路层帧使用相同的帧格式，它们都具有降低传输速率以到达更远距离的能力。并且这 3 个标准都允许“基础设施模式”和“自组织模式”两种模式。然而，如表 6-1 所示，这 3 个标准在物理层有一些重要的区别。

802.11b 无线 LAN 具有 11Mbps 的数据率，工作在非许可证的 2.4~2.4835GHz 的无线频谱上，与 2.4GHz 电话和微波炉争用频谱。802.11a 无线 LAN 可以以高得多的比特率工作，但它在更高的频率上运行。然而，由于运行的频率更高，802.11a LAN 对于给定的功率级别传输距离较短，并且它受多径传播的影响更大。802.11g LAN 与 802.11b LAN 工作在同样的较低频段上，并且与 802.11b 向后兼容（这样你能够逐步地升级 802.11b 的客户），而且与 802.11a 有相同的高传输速率，使得用户能够更好地享受网络服务。

一个相对新的 WiFi 标准 802.11n [IEEE 802.11n 2012]，使用多输入多输出（MIMO）天线；即在发送侧的两个或多个天线和在接收侧的两个或多个天线之间发送/接收不同的信号 [Diggavi 2004]。根据所使用的调制方案，每秒几百兆比特的传输率对于 802.11n 是可能的。

6.3.1 802.11 体系结构

图 6-7 显示了 802.11 无线 LAN 体系结构的基本构件。802.11 体系结构的基本构件模块是基本服务集（Basic Service Set, BSS）。一个 BSS 包含一个或多个无线站点和一个在 802.11 术语中称为接入点（Access Point, AP）的中央基站（base station）。图 6-7 展示了两个 BSS 中的 AP，它们连接到一个互联设备上（如交换机或者路由器），互联设备又连接到因特网中。在一个典型的家庭网络中，有一个 AP 和一台将该 BSS 连接到因特网中的路由器（通常综合成为一个单元）。

与以太网设备类似，每个 802.11 无线站点都具有一个 6 字节的 MAC 地址，该地址存储在该站适配器（即 802.11 网络接口卡）的固件中。每个 AP 的无线接口也具有一个 MAC 地址。与以太网类似，这些 MAC 地址由 IEEE 管理，理论上是全球唯一的。

如 6.1 节所述，配置 AP 的无线 LAN 经常被称作基础设施无线 LAN（infrastructure wireless LAN），其中的“基础设施”是指 AP 连同互联 AP 和一台路由器的有线以太网。图 6-8 显示了 IEEE 802.11 站点也能将它们自己组合在一起形成一个自组织网络，即一个无中心控制和与“外部世界”无连接的网络。这里，该网络是由彼此已经发现相互接近且有通信需求的移动设备“动态”形成，并且在它们所处环境中没有预先存在的网络基础设施。当携带便携机的人们聚集在一起时（例如，在一个会议室、一列火车或者一辆汽车中），并且要在没有中央化的 AP 的情况下交换数据，一个自组织网络就可能形成了。随着要通信的便携设备的继续激增，人们对自组织网络产生巨大的兴趣。然而在本节中，我们只关注基础设施无线 LAN。

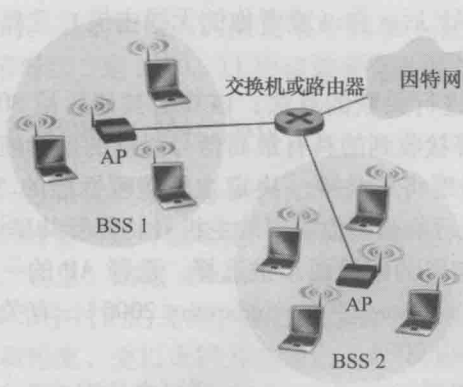


图 6-7 IEEE 802.11 LAN 体系结构

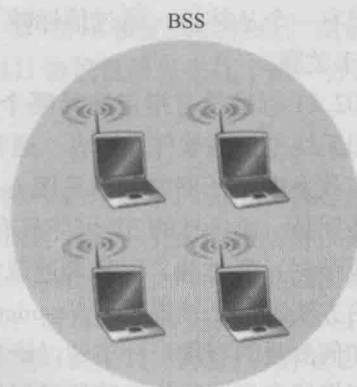


图 6-8 IEEE 802.11 自组织网络

信道与关联

在 802.11 中，每个无线站点在能够发送或者接收网络层数据之前，必须与一个 AP 相关联。尽管所有 802.11 标准都使用了关联，但我们将专门在 IEEE 802.11b/g 环境中讨论这一主题。

当网络管理员安装一个 AP 时，管理员为该接入点分配一个单字或双字的服务集标识符（Service Set Identifier, SSID）。（例如，当你在 Microsoft Windows XP 中“查看可用网络时”，将显示某范围内每个 AP 的 SSID。）管理员还必须为该 AP 分配一个信道号。为了理解信道号，回想前面讲过的 802.11 运行在 2.4~2.4835GHz 的频段中。在这 85MHz 的频段内，802.11 定义了 11 个部分重叠的信道。当且仅当两个信道由 4 个或更多信道隔开时它们才无重叠。特别是信道 1、6 和 11 的集合是唯一的 3 个非重叠信道的集合。这意味着管理员可以在同一个物理网络中安装 3 个 802.11b AP，为这些 AP 分配信道 1、6 和 11，然后将每个 AP 都连接到一台交换机上。

既然已经对 802.11 信道有了基本了解，我们则可以描述一个有趣（且并非完全不寻常）的情况，即有关 WiFi 丛林。WiFi 丛林（WiFi jungle）是一个任意物理位置，在这里无线站点能从两个或多个 AP 中收到很强的信号。例如，在纽约城的许多咖啡馆中，无线站点可以从附近许多 AP 中选取一个信号。其中一个 AP 可能由该咖啡馆管理，而其他 AP 可能位于咖啡馆附近的住宅区内。这些 AP 中的每一个都可能位于不同的子网中，并被独立分配一个信道。

现在假定你带着自己的便携机进入这样一个 WiFi 丛林，寻求无线因特网接入和一个蓝莓松饼。设在这个丛林中有 5 个 AP。为了获得因特网接入，你的无线站点需要加入其中一个子网并因此需要与其中的一个 AP 相关联（associate）。关联意味着这一无线站点在自身和该 AP 之间创建一个虚拟线路。特别是，仅有关联的 AP 才向你的无线站点发送数据帧，并且你的无线站点也仅仅通过该关联 AP 向因特网发送数据帧。然而，你的无线站点是如何与某个特定的 AP 相关联的？更为根本的问题是，你的无线站点是如何知道哪个 AP 位于丛林中的呢？

802.11 标准要求每个 AP 周期性地发送信标帧（beacon frame），每个信标帧包括该 AP 的 SSID 和 MAC 地址。你的无线站点为了得知正在发送信标帧的 AP，扫描 11 个信道，找出来自可能位于该区域的 AP 所发出的信标帧（其中一些 AP 可能在相同的信道中传输，

即这里有一个丛林!)。通过信标帧了解到可用 AP 后,你(或者你的无线主机)选择一个 AP 用于关联。

802.11 标准没有指定选择哪个可用的 AP 进行关联的算法;该算法被遗留给 802.11 固件和无线主机的软件设计者。通常,主机选择接收到的具有最高信号强度的信标帧。虽然高信号强度好(例如可参见图 6-3),信号强度将不是唯一决定主机接收性能的 AP 特性。特别是,所选择的 AP 可能具有强信号,但可能被其他附属的主机(将需要共享该 AP 的无线带宽)所过载,而某未过载的 AP 由于稍弱的信号而未被选择。选择 AP 的一些可替代的方法近来已被提出 [Vasudevan 2005; Nicholson 2006; Sudaresan 2006]。有关信号强度如何测量的有趣而朴实的讨论参见 [Bardwell 2004]。

扫描信道和监听信标帧的过程被称为**被动扫描**(passive scanning)(参见图 6-9a)。无线主机也能够执行**主动扫描**(active scanning),这是通过向位于无线主机范围内的所有 AP 广播探测帧完成的,如图 6-9b 所示。AP 用一个探测响应帧应答探测请求帧。无线主机则能够在响应的 AP 中选择某 AP 与之相关联。

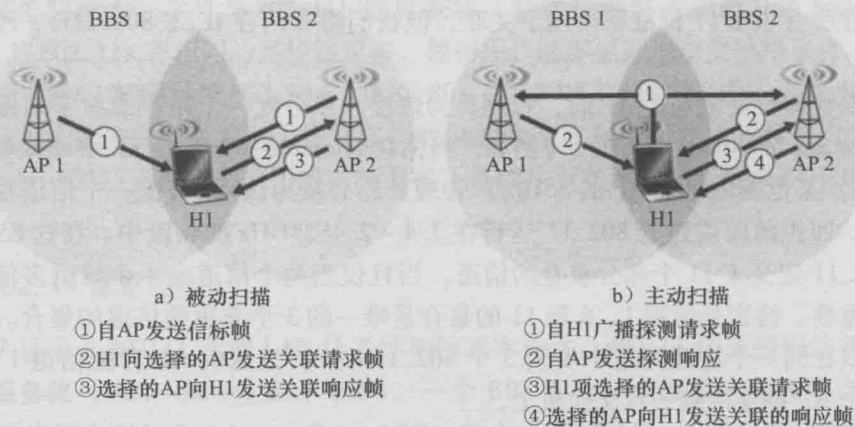


图 6-9 对接入点的主动和被动扫描

选定与之关联的 AP 后,无线主机向 AP 发送一个关联请求帧,并且该 AP 以一个关联响应帧进行响应。注意到对于主动扫描需要这种第二次请求/响应握手,因为一个对初始探测请求帧进行响应的 AP 并不知道主机选择哪个(可能多个)响应的 AP 进行关联,这与 DHCP 客户能够从多个 DHCP 服务器进行选择有诸多相同之处(参见图 4-21)。一旦与一个 AP 关联,该主机希望加入该 AP 所属的子网中(以 4.4.2 节中的 IP 寻址的意义)。因此,该主机通常将通过关联的 AP 向该子网发送一个 DHCP 发现报文(参见图 4-21),以获取在该 AP 子网中的一个 IP 地址。一旦获得地址,网络的其他部分将直接视你的主机为该子网中的另一台主机。

为了与特定的 AP 创建一个关联,某无线站点可能要向该 AP 鉴别它自身。802.11 无线 LAN 提供了几种不同的鉴别和接入方法。一种被许多公司采用的方法是,基于一个站点的 MAC 地址允许其接入一个无线网络。第二种被许多因特网咖啡屋采用的方法是,应用用户名和口令。在两种情况下,AP 通常与一个鉴别服务器进行通信,使用一种诸如 RADIUS [RFC 2865] 或 DIAMETER [RFC 3588] 的协议,在无线终端站和鉴别服务器之间中继信息。分离鉴别服务器和 AP,使得一个鉴别服务器可以服务于多个 AP,将(经常是

敏感的) 鉴别和接入的决定集中到单一服务器中, 使 AP 费用和复杂性较低。我们将在 8.8 节看到, 定义 802.11 协议族安全性的新 IEEE 802.11i 协议就恰好采用了这一方法。

6.3.2 802.11 MAC 协议

一旦某无线站点与一个 AP 相关联, 它就可以经该接入点开始发送和接收数据帧。然而因为许多站点可能希望同时经相同信道传输数据帧, 因此需要一个多路访问协议来协调传输。这里, 站点 (station) 可以是一个无线站点, 或者是一个 AP。正如在第 5 章和 6.2.1 节中讨论的那样, 宽泛地讲有三类多路访问协议: 信道划分 (包括 CDMA)、随机访问和轮流。受以太网及其随机访问协议巨大成功的鼓舞, 802.11 的设计者为 802.11 无线 LAN 选择了一种随机访问协议。这个随机访问协议称作带碰撞避免的 CSMA (CSMA with collision avoidance), 或简称为 CSMA/CA。与以太网的 CSMA/CD 相似, CSMA/CA 中的“CSMA”代表“载波侦听多路访问”, 意味着每个站点在传输之前侦听信道, 并且一旦侦听到该信道忙则抑制传输。尽管以太网和 802.11 都使用载波侦听随机接入, 但这两种 MAC 协议有重要的区别。首先, 802.11 使用碰撞避免而非碰撞检测; 其次, 由于无线信道相对较高的误比特率, 802.11 (不同于以太网) 使用链路层确认/重传 (ARQ) 方案。我们将在下面讨论 802.11 的碰撞避免和链路层确认机制。

在 5.3.2 节和 5.4.2 节曾讲过, 使用以太网的碰撞检测算法, 以太网结点在发送过程中监听信道。在发送过程中如果检测到另一结点也在发送, 则放弃自己的发送, 并且在等待一个小的随机时间后再次发送。与 802.3 以太网协议不同, 802.11 MAC 协议并未实现碰撞检测。这主要由两个原因所致:

- 检测碰撞的能力要求站点具有同时发送 (站点自己的信号) 和接收 (检测其他站点是否也在发送) 的能力。因为在 802.11 适配器上, 接收信号的强度通常远远小于发送信号的强度, 制造具有检测碰撞能力的硬件代价较大。
- 更重要的是, 即使适配器可以同时发送和监听信号 (并且假设它一旦侦听到信道忙就放弃发送), 适配器也会由于隐藏终端问题和衰减问题而无法检测到所有的碰撞, 参见 6.2 节的讨论。

由于 802.11 无线局域网不使用碰撞检测, 一旦站点开始发送一个帧, 它就完全地发送该帧; 也就是说, 一旦站点开始发送, 就不会返回。正如人们可能猜想的那样, 碰撞存在时仍发送整个数据帧 (尤其是长数据帧) 将严重降低多路访问协议的性能。为了降低碰撞的可能性, 802.11 采用几种碰撞避免技术, 我们稍后讨论它们。

然而, 在考虑碰撞避免之前, 我们首先需要分析 802.11 的链路层确认 (link-layer acknowledgment) 方案。6.2 节讲过, 当无线 LAN 中某站点发送一个帧时, 该帧会由于多种原因不能无损地到达目的站点。为了处理这种不可忽视的故障情况, 802.11 MAC 使用链路层确认。如图 6-10 所示, 目的站点收到一个通过 CRC 校验的帧后, 它等待一个被称作短帧间间隔 (Short Inter-Frame Spacing, SIFS) 的一小段时间, 然后发回一个确认帧。如果发送站点在给定的时间内未收到确认帧, 它假定出现了错误并重传该帧, 使用 CSMA/CA 协议访问该信道。如果在若干固定次重传后仍未收到确认, 发送站点将放弃发送并丢弃该帧。

讨论过 802.11 如何使用链路层确认后, 我们可以描述 802.11 的 CSMA/CA 协议了。假设一个站点 (无线站点或者 AP) 有一个帧要发送。

1) 如果初始时某站点监听到信道空闲, 它将在一个被称作分布式帧间间隔 (Distributed Inter-Frame Space, DIFS) 的短时间段后发送该帧, 如图 6-10 所示。

2) 否则, 该站点选取一个随机回退值 (如我们在 5.3.2 节中遇到的那样) 并且在侦听信道空闲时递减该值。当侦听到信道忙时, 计数值保持不变。

3) 当计数值减为 0 时 (注意到这只可能发生在信道被侦听为空闲时), 该站点发送整个数据帧并等待确认。

4) 如果收到确认, 发送站点知道它的帧已被目的站正确接收了。如果该站点要发送另一帧, 它将从第二步开始 CSMA/CA 协议。如果未收到确认, 发送站点将重新进入第二步中的回退阶段, 并从一个更大的范围内选取随机值。

前面讲过, 在以太网的 CSMA/CD 的多路访问协议 (5.3.2 节) 下, 一旦侦听到信道空闲, 站点开始发送。然而, 使用 CSMA/CA, 该站点在倒计时时抑制传输, 即使它侦听到该信道空闲也是如此。为什么 CSMA/CD 和 CSMA/CA 采用了不同的方法呢?

为了回答这一问题, 我们首先考虑这样一种情形: 两个站点分别有一个数据帧要发送, 但是, 由于

侦听到第三个站点已经在传输, 双方都未立即发送。使用以太网的 CSMA/CD 协议中, 两个站点将会在检测到第三方发送完毕后立即开始发送。这将导致一个碰撞, 在 CSMA/CD 协议中碰撞并非是一个严重的问题, 因为两个站点检测到碰撞后都会放弃它们的发送, 从而避免了由于碰撞而造成的该帧剩余部分的无用发送。而在 802.11 中情况却十分不同, 因为 802.11 并不检测碰撞和放弃发送, 遭受碰撞的帧仍将被完全传输。因此 802.11 的目标是无论如何尽可能避免碰撞。在 802.11 中, 如果两个站点侦听到信道忙, 它们都将立即进入随机回退, 希望选择一个不同的回退值。如果这些值的确不同, 一旦信道空闲, 其中的一个站点将在另一个之前发送, 并且 (如果两个站点均未对对方隐藏) “失败站点”将会听到“胜利站点”的信号, 冻结它的计数器, 并在胜利站点完成传输之前一直抑制传输。通过这种方式, 避免了高代价的碰撞。当然, 在以下情况下使用 802.11 仍可能出现碰撞: 两个站点可能互相是隐藏的, 或者两者可能选择了非常靠近的随机回退值, 使来自先开始站点的传输也必须到达第二个站点。回想前面我们在图 5-12 的环境中讨论随机访问算法时遇到过这个问题。

1. 处理隐藏终端: RTS 和 CTS

802.11 MAC 协议也包括了一个极好 (但为可选) 的预约方案, 以帮助在出现隐藏终端的情况下避免碰撞。我们在图 6-11 的环境下研究这种方案, 其中显示了两个无线站点和一个接入点。这两个无

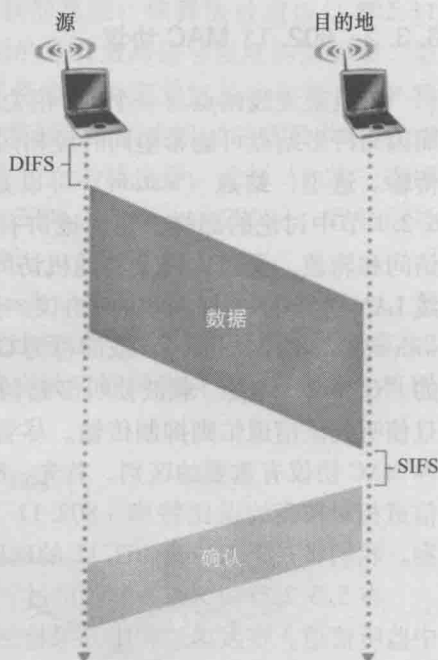


图 6-10 802.11 使用链路层确认

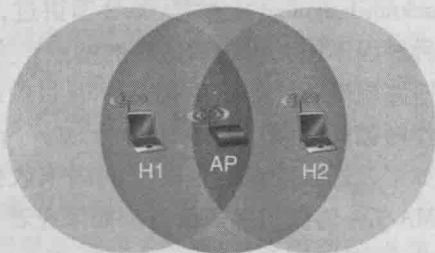


图 6-11 隐藏终端的例子: H1 和 H2 彼此互相隐藏

线站点都在该 AP 的覆盖范围内（其覆盖范围显示为阴影圆环），并且两者都与该 AP 相关联。然而，由于衰减，无线结点的信号范围局限在图 6-11 所示的阴影圆环内部。因此，尽管每个无线站点对 AP 都不隐藏，两者彼此却是隐藏的。

现在我们考虑为什么隐藏终端会导致出现问题。假设站点 H1 正在传输一个帧，并且在 H1 传输的中途，站点 H2 要向 AP 发送一个帧。由于 H2 未听到来自 H1 的传输，它将首先等待一个 DIFS 间隔，然后发送该帧，导致产生了一个碰撞。从而在 H1 和 H2 的整个发送阶段，信道都被浪费了。

为了避免这一问题，IEEE 802.11 协议允许站点使用一个短请求发送（Request to Send, RTS）控制帧和一个短允许发送（Clear to Send, CTS）控制帧来预约对信道的访问。当发送方要发送一个 DATA 帧时，它能够首先向 AP 发送一个 RTS 帧，指示传输 DATA 帧和确认（ACK）帧需要的总时间。当 AP 收到 RTS 帧后，它广播一个 CTS 帧作为响应。该 CTS 帧有两个目的：给发送方明确的发送许可，也指示其他站点在预约期内不要发送。

因此，在图 6-12 中，在传输 DATA 帧前，H1 首先广播一个 RTS 帧，该帧能被其范围内包括 AP 在内的所有站点听到。AP 然后用一个 CTS 帧响应，该帧也被其范围内包括 H1 和 H2 在内的所有站点听到。站点 H2 听到 CTS 后，在 CTS 帧中指定的时间内将抑制发送。RTS、CTS、DATA 和 ACK 帧如图 6-12 所示。

RTS 和 CTS 帧的使用能够在两个重要方面提高性能：

- 隐藏终端问题被缓解了，因为长 DATA 帧只有在信道预约后才被传输。
- 因为 RTS 和 CTS 帧较短，涉及 RTS 和 CTS 帧的碰撞将仅持续短 RTS 和 CTS 帧的持续期。一旦 RTS 和 CTS 帧被正确传输，后续的 DATA 和 ACK 帧应当能无碰撞地发送。

建议读者去查看本书配套网站上的 802.11 Java 小程序。这个交互小程序演示了 CSMA/CA 协议，包括 RTS/CTS 交换序列。

尽管 RTS/CTS 交换有助于降低碰撞，但它同样引入了时延以及消耗了信道资源。因此，RTS/CTS 交换仅仅用于为长数据帧预约信道。在实际中，每个无线站点可以设置一个 RTS 门限值，仅当帧长超过门限值时，才使用 RTS/CTS 序列。对许多无线站点而言，默认的 RTS 门限值大于最大帧长值，因此对所有发送的 DATA 帧，RTS/CTS 序列都被跳过。

2. 使用 802.11 作为一个点对点链路

到目前为止我们的讨论关注在多路访问环境中使用 802.11。应该指出，如果两个结点

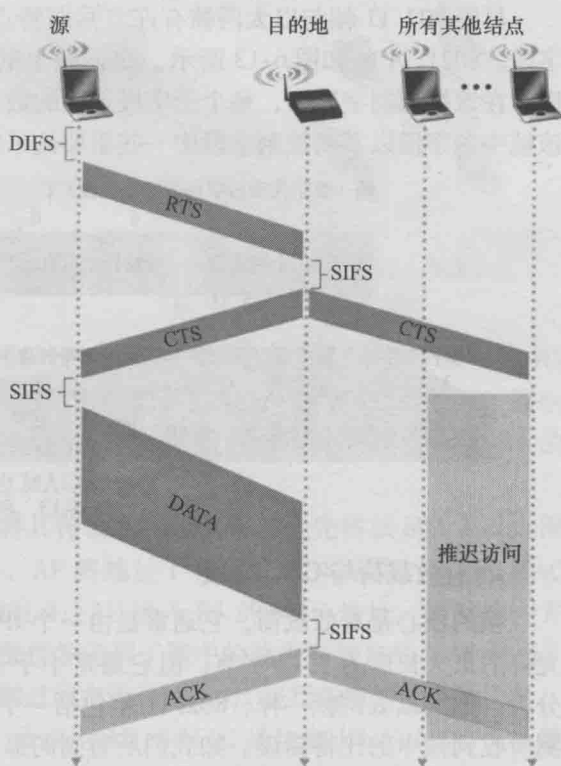


图 6-12 使用 RTS 和 CTS 帧的碰撞避免

每个都具有一个定向天线，它们可以将其定向天线指向对方，并基本上是在一个点对点的链路上运行 802.11 协议。如果商用 802.11 硬件产品价格低廉，那么使用定向天线以及增加传输功率使得 802.11 成为一个在数十公里距离中提供无线点对点连接的廉价手段。[Raman 2007] 描述了这样一个运行于印度恒河郊区平原上的多跳无线网络，其中包含了点对点 802.11 链路。

6.3.3 IEEE 802.11 帧

尽管 802.11 帧与以太网帧有许多共同特点，但它也包括了许多特定用于无线链路的字段。802.11 帧如图 6-13 所示，在该帧上的每个字段上面的数字代表该字段的字节长度；在该帧控制字段中，每个子字段上面的数字代表该子字段的比特长度。现在我们查看该帧中各字段以及帧控制字段中一些重要的子字段。

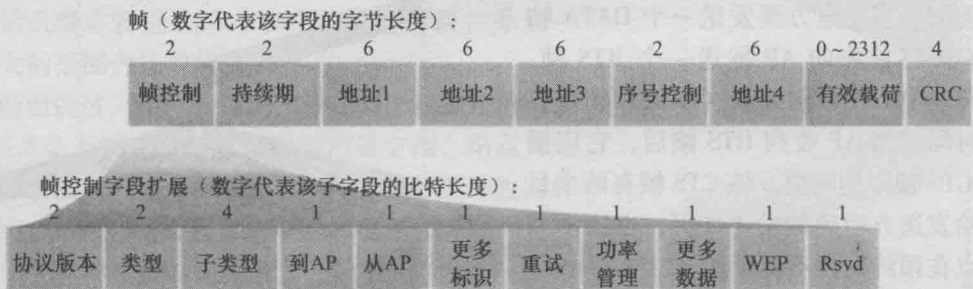


图 6-13 802.11 帧

1. 有效载荷与 CRC 字段

帧的核心是有效载荷，它通常是由一个 IP 数据报或者 ARP 分组组成。尽管这一字段允许的最大长度为 2312 字节，但它通常小于 1500 字节，放置一个 IP 数据报或一个 ARP 分组。如同以太网帧一样，802.11 帧包括一个循环冗余校验（CRC），从而接收方可以检测所收到帧中的比特错误。如我们所看到的那样，比特错误在无线局域网中比在有线局域网中更加普遍，因此 CRC 在这里更加有用。

2. 地址字段

也许 802.11 帧中最引人注意的不同之处是它具有 4 个地址字段，其中每个都可以包含一个 6 字节的 MAC 地址。但为什么要 4 个地址字段呢？如以太网中那样，一个源 MAC 地址字段和一个目的 MAC 地址字段不就足够了？事实表明，出于互联目的需要 3 个地址字段，特别是将网络层数据报从一个无线站点通过一个 AP 送到一台路由器接口。当 AP 在自组织模式中互相转发时使用第四个地址。由于我们这里仅仅考虑基础设施网络，所以只关注前 3 个地址字段。802.11 标准定义这些字段如下：

- 地址 2 是传输该帧的站点的 MAC 地址。因此，如果一个无线站点传输该帧，该站点的 MAC 地址就被插入在地址 2 字段中。类似地，如果一个 AP 传输该帧，该 AP 的 MAC 地址也被插入在地址 2 字段中。
- 地址 1 是要接收该帧的无线站点的 MAC 地址。因此，如果一个移动无线站点传输该帧，地址 1 包含了该目的 AP 的 MAC 地址。类似地，如果一个 AP 传输该帧，地址 1 包含该目的无线站点的 MAC 地址。

• 为了理解地址 3，回想 BSS（由 AP 和无线站点组成）是一个子网的一部分，并且这个子网经一些路由器接口与其他子网相连。地址 3 包含这个路由器接口的 MAC 地址。

为了对地址 3 的目的有更深入的理解，我们观察在图 6-14 环境中的网络互联的例子。在这幅图中，有两个 AP，每个 AP 负责一些无线站点。每个 AP 到路由器有一个直接连接，路由器依次又连接到全球因特网。我们应当记住 AP 是链路层设备，它既不能“说”IP 又不理解 IP 地址。现在考虑将一个数据报从路由器接口 R1 移到无线站点 H1。路由器并不清楚在它和 H1 之间有一个 AP；从路由器的观点来说，H1 仅仅是路由器所连接的子网中的一台主机。

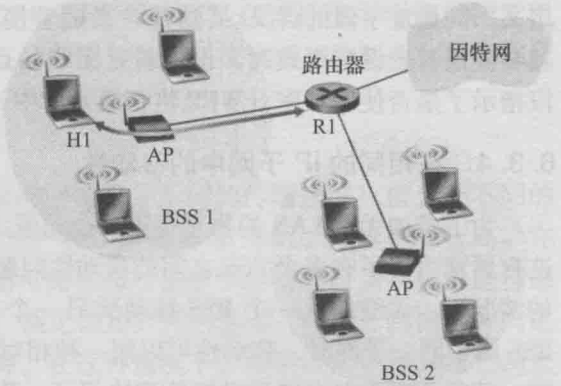


图 6-14 在 802.11 帧中使用地址字段：
在 H1 和 R1 之间发送帧

- 路由器知道 H1 的 IP 地址（从数据报的目的地址中得到），它使用 ARP 来确定 H1 的 MAC 地址，这与在普通的以太网 LAN 中相同。获取 H1 的 MAC 地址后，路由器接口 R1 将该数据报封装在一个以太网帧中。该帧的源地址字段包含了 R1 的 MAC 地址，目的地址字段包含 H1 的 MAC 地址。
- 当该以太网帧到达 AP 后，该 AP 在将其传输到无线信道前，先将该 802.3 以太网帧转换为一个 802.11 帧。如前所述，AP 将地址 1 和地址 2 分别填上 H1 的 MAC 地址和其自身的 MAC 地址。对于地址 3，AP 插入 R1 的 MAC 地址。通过这一方式，H1 可以确定（从地址 3）将数据报发送到子网中的路由器接口的 MAC 地址。现在考虑在从 H1 移动一个数据报到 R1 的过程中无线站点 H1 进行响应时发生的情况。
- H1 生成一个 802.11 帧，如上所述，分别用 AP 的 MAC 地址和 H1 的 MAC 地址填充地址 1 和地址 2 字段。对于地址 3，H1 插入 R1 的 MAC 地址。
- 当 AP 接收该 802.11 帧后，将其转换为以太网帧。该帧的源地址字段是 H1 的 MAC 地址，目的地址字段是 R1 的 MAC 地址。因此，地址 3 允许 AP 在构建以太网帧时能够确定目的 MAC 地址。

总之，地址 3 在 BSS 和有线局域网互联中起着关键作用。

3. 序号、持续期和帧控制字段

前面讲过在 802.11 网络中，无论何时一个站点正确地收到一个来自于其他站点的帧，它就回发一个确认。因为确认可能会丢失，发送站点可能会发送一个给定帧的多个副本。正如我们在 rdt2.1 协议讨论中所见（3.4.1 节），使用序号可以使接收方区分新传输的帧和以前帧的重传。因此在 802.11 帧中的序号字段在链路层与在第 3 章中运输层中的该字段有着完全相同的目的。

前面讲过 802.11 协议允许传输结点预约信道一段时间，包括传输其数据帧的时间和传输确认的时间。这个持续期值被包括在该帧的持续期字段中（在数据帧和 RTS 及 CTS 帧中均存在）。

如图 6-13 所示，帧控制字段包括许多子字段，我们将提一下其中比较重要的子字段，更加完整的讨论请参见 802.11 规范 [Held 2001; Crow 1997; IEEE 802.11 1999]。类型和子类型字段用于区分关联、RTS、CTS、ACK 和数据帧。To（到）和 From（从）字段用于定义不同地址字段的含义。（这些含义随着使用自组织模式或者基础设施模式而改变，而且在使用基础设施模式时，也随着是无线站点还是 AP 在发送帧而变化。）最后，WEP 字段指示了是否使用加密（WEP 将在第 8 章中讨论。）

6.3.4 在相同的 IP 子网中的移动性

为了增加无线 LAN 的物理范围，公司或大学经常会在同一个 IP 子网中部署多个 BSS。这自然就引出了在多个 BSS 之间的移动性问题，即无线站点如何在维持进行中的 TCP 会话的情况下，无缝地从一个 BSS 移动到另一个 BSS？正如我们将在本小节中所见，当这些 BSS 属于同一子网时，移动性可以用一种相对直接的方式解决。当站点在不同子网间移动时，就需要更为复杂的移动性管理协议了，我们将在 6.5 节和 6.6 节中学习这些协议。

我们现在看一个同一子网中的不同 BSS 之间的移动性的特定例子。图 6-15 显示了具有一台主机 H1 的两个互联的 BSS，该主机从 BSS1 移动到 BSS2。因为在这个例子中连接两个 BSS 的互联设备不是一台路由器，故在两个 BSS 中的所有站点（包括 AP）都属于同一个 IP 子网。因此，当 H1 从 BSS1 移动到 BSS2 时，它可以保持自己的 IP 地址和所有正在进行的 TCP 连接。如果互联设备是一台路由器，则 H1 必须在它移动进入的子网中获得一个新地址。这种地址的变化将打断（并且最终终止）在 H1 的任何进行中的 TCP 连接。在 6.6 节中，我们将能看到一种网络层移动性协议如移动 IP 能被用于避免该问题。

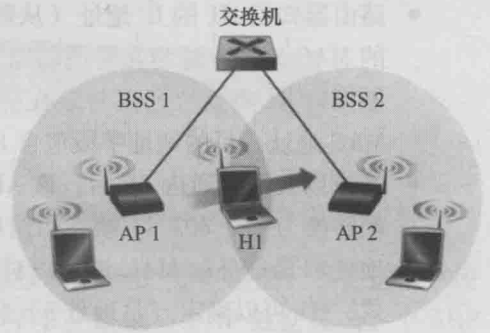


图 6-15 同一子网中的移动性

但是 H1 从 BSS1 移动到 BSS2 时具体会发生哪些事呢？随着 H1 逐步远离 AP1，H1 检测到来自 AP1 的信号逐渐减弱并开始扫描一个更强的信号。H1 收到来自 AP2 的信标帧（在许多公司和大学的设置中它与 AP1 有相同的 SSID）。H1 然后与 AP1 解除关联，并与 AP2 关联起来，同时保持其 IP 地址和维持正在进行的 TCP 会话。

从主机和 AP 的角度，这就处理了切换问题。但对图 6-15 中的交换机又会发生什么样的情况呢？交换机如何知道主机已经从一个 AP 移动到另一个 AP 呢？回想第 5 章所述，交换机是“自学习”的，并且自动构建它们的转发表。这种自学习的特征很好地处理了偶尔的移动（例如，一个雇员从一个部门调到另一个部门）。然而，交换机没有被设计用来支持用户在不同 BSS 间高度移动，同时又希望保持 TCP 连接。为理解这一问题，回想在移动之前，交换机在其转发表中有一个表项，对应 H1 的 MAC 地址与到达 H1 所通过的出交换机端口。如果 H1 初始在 BSS1 中，则发往 H1 的数据报将经 AP1 导向 H1。然而，一旦 H1 与 BSS2 关联，它的帧应当被导向 AP2。一种解决方法（真有点不规范）是在新的关联形成后，让 AP2 以 H1 的源地址向交换机发送一以太网广播帧。当交换机收到该帧后，更新其转发表，使得 H1 可以通过 AP2 到达。802.11f 标准小组正在开发一个 AP 间的协议来处理这些以及相关的问题。

6.3.5 802.11 中的高级特色

我们将简要地讨论 802.11 网络中具有两种高级能力以丰富对 802.11 的讨论内容。如我们所见, 这些能力并不是完全特定于 802.11 标准的, 而是在该标准中可能由特定机制产生的。这使得不同的厂商可使用他们自己 (专用) 的方法来实现这些能力, 这也许能让他们增强竞争能力。

1. 802.11 速率适应

我们在前面图 6-3 中看到, 不同的调制技术 (提供了不同的传输速率) 适合于不同的 SNR 情况。考虑这样一个例子, 一个 802.11 用户最初离基站 20 米远, 这里信噪比高。在此高信噪比的情况下, 该用户能够与基站使用可提供高传输速率的物理层调制技术进行通信, 同时维持低 BER。这个用户多么幸福啊! 假定该用户开始移动, 向离开基站的方向走去, 随着与基站距离的增加, SNR 一直在下降。在这种情况下, 如果在用户和基站之间运行的 802.11 协议所使用的调制技术没有改变的话, 随着 SNR 减小, BER 将高得不可接受, 最终, 传输的帧将不能正确收到。

由于这个原因, 某些 802.11 实现具有一种速率自适应能力, 该能力自适应地根据当前和近期信道特点来选择下面的物理层调制技术。如果一个结点连续发送两个帧而没有收到确认 (信道上一个比特差错的隐式指示), 该传输速率降低到前一个较低的速率。如果 10 个帧连续得到确认, 或如果用来跟踪自上次降速以来时间的定时器超时, 该传输速率提高到上一个较高的速率。这种速率适应机制与 TCP 的拥塞控制机制具有相同的“探测”原理, 即当条件好时 (反映为收到 ACK), 增加传输速率, 除非某个“坏事”发生了 (ACK 没有收到); 当某个“坏事”发生了, 减小传输速率。因此, 802.11 的速率适应和 TCP 的拥塞控制类似于年幼的孩子, 他们不断地向父母要求越来越多 (如幼儿要糖果, 青少年要求推迟睡觉), 直到父母最后说“够了!”, 孩子们不再要求了 (仅当以后情况已经变好了才会再次尝试)。已经提出了一些其他方案以改善这个基本的自动速率调整方案 [Kamerman 1997; Holland 2001; Lacage 2004]。

2. 功率管理

功率是移动设备的宝贵资源, 因此 802.11 标准提供了功率管理能力, 以使 802.11 结点的侦听、传输和接收功能以及其他需要“打开”电路的时间量最小化。802.11 功率管理按下列方式运行。一个结点能够明显地在睡眠和唤醒状态之间交替 (像在课堂上睡觉的学生!)。通过将 802.11 帧首部的功率管理比特设置为 1, 某结点向接入点指示它将打算睡眠。设置结点中的一个定时器, 使得正好在 AP 计划发送它的信标帧前唤醒结点 (前面讲过 AP 通常每 100ms 发送一个信标帧)。因为 AP 从设置的功率传输比特知道哪个结点打算睡眠, 所以该 AP 知道它不应当向这个结点发送任何帧, 先缓存目的地为睡眠主机的任何帧, 待以后再传输。

在 AP 发送信标帧前, 恰好唤醒结点, 并迅速进入全面活动状态 (与睡觉的学生不同, 这种唤醒仅需要 $250\mu\text{s}$ [Kamerman 1997]!)。由 AP 发送的信标帧包含了帧被缓存在 AP 中的结点的列表。如果某结点没有缓存的帧, 它能够返回睡眠状态。否则, 该结点能够通过向 AP 发送一个探测报文明确地请求发送缓存的帧。对于信标之间的 100ms 时间来说, $250\mu\text{s}$ 的唤醒时间以及类似的接收信标帧及检查以确保不存在缓存帧的短小时间, 没

有帧要发送和接收的结点能够睡眠 99% 的时间，从而大大节省了能源。

6.3.6 802.11 以外的标准：蓝牙和 ZigBee

如图 6-2 所示，IEEE 802.11 WiFi 标准主要针对相距多达 100m 的设备间的通信（当使用 802.11 具有定向天线的点对点配置时除外）。两个其他的 IEEE 802 协议——蓝牙和 ZigBee（定义在 IEEE 802.15.1 和 IEEE 802.15.4 标准中 [IEEE 802.15 2012]），以及 WiMAX（定义在 IEEE 802.16 标准中 [IEEE 802.16d 2004; IEEE 802.16e 2005]），它们分别是用于短距离和长距离通信的标准。当我们在 6.4 节中讨论蜂窝数据网络时，将简要接触 WiMAX，因此这里将关注用于短距离通信的网络。

1. 蓝牙

IEEE 802.15.1 网络以小范围、低功率和低成本运行。它本质上是一个低功率、小范围、低速率的“电缆替代”技术，用于互联笔记本、串行设备、蜂窝电话和智能手机，而 802.11 是一个大功率、中等范围、高速率的“接入”技术。为此，802.15.1 网络有时被称为无线个人区域网络（Wireless Personal Area Network, WPAN）标准。802.15.1 的链路层和物理层基于早期用于个人区域网络的蓝牙（Bluetooth）规范 [Held 2001, Bisdikian 2001]。802.15.1 网络以 TDM 方式工作于无需许可证的 2.4GHz 无线电波段，每个时隙长度为 625 μ s。在每个时隙内，发送方利用 79 个信道中的一个进行传输，同时从时隙到时隙以一个已知的伪随机方式变更信道。这种被称作跳频扩展频谱（Frequency-Hopping Spread Spectrum, FHSS）的信道跳动的形式将传输及时扩展到整个频谱。802.15.1 能够提供高达 4Mbps 的数据率。

802.15.1 网络是自组织网络：不需要网络基础设施（如一个接入点）来互连 802.15.1 设备。因此，802.15.1 设备必须自己进行组织。802.15.1 设备首先组织成一个多达 8 个活动设备的皮可网（piconet），如图 6-16 所示。这些设备之一被指定为主设备，其余充当从设备。主结点真正控制皮可网，即它的时钟确定了皮可网中的时间，它可以在每个奇数时隙中发送，而从设备仅当主设备在前一时隙与其通信后才可以发送，并且只能发送给主设备。除了从设备，网络中还可以有多达 255 个的寄放（parked）设备。这些设备仅当其状态被主结点从寄放转换为活动之后才可以进行通信。

希望了解更多有关 802.15.1 WPAN 信息的读者可以查阅蓝牙参考资料 [Held 2001, Bisdikian 2001]，或者 IEEE 802.15 Web 网站 [IEEE 802.15 2012]。

2. ZigBee

IEEE 的第二个个人区域网络标准是 802.15.4 [IEEE 802.15 2012]，它被称为 ZigBee。虽然蓝牙网络提供了一种“电缆替代”的超过每秒兆比特的数据率，但 ZigBee 较之蓝牙仍是以低功率、低数据率、低工作周期应用为目标。尽管我们可能倾向于认为“更大和更快就更好”，但是并非所有的网络应用都需要高带宽和随之而来的高成本（经济和功率方面）。例如，家庭温度和光线传感器、安全设备和墙上安装的开关都是非常简单、低功率、低工作周期、低成本设备。ZigBee 因此是非常适合于这些设备的。ZigBee 定义了 20kbps、

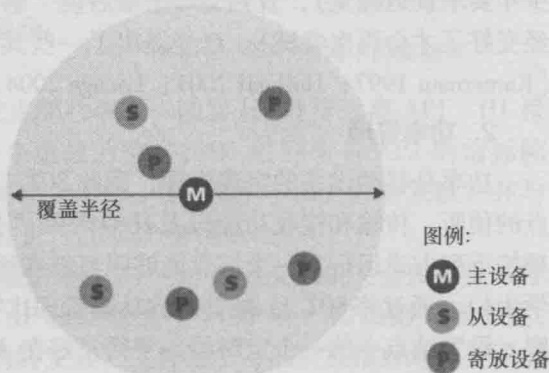


图 6-16 蓝牙皮可网

40kbps、100kbps 和 250kbps 的信道速率，这取决于信道的频率。

ZigBee 网络中的结点具有两个特色。多个所谓“简化功能设备”在单个“全功能设备”控制下作为从设备运行，与蓝牙从设备非常相似。一个全功能设备能够作为一个主设备运行，就像在蓝牙中控制多个从设备那样，并且多个全功能设备还能够配置为一个网状（mesh）网络，其中全功能设备在它们之间发送帧。ZigBee 可以共享许多我们已经在其他链路层协议中遇到的协议机制：信标帧和链路层确认（类似于 802.11），具有二进制回退的载波侦听随机访问协议（类似于 802.11 和以太网），以及时隙的固定、确保的分配（类似于 DOCSIS）。

ZigBee 网络能够配置为许多不同的方式。我们考虑一种简单的场合，其中单一的全功能设备使用信标帧以一种时隙方式控制多个简化功能设备。图 6-17 显示了这种情况，其中 ZigBee 网络将时间划分为反复出现的超帧，每个超帧以一个信标帧开始。每个信标帧将超帧划分为一个活跃周期（在这个周期内设备可以传输）和一个非活跃周期（在这个周期内所有设备包括控制器能够睡眠进而保存能量）。活跃周期由 16 个时隙组成，其中一些由采用 CSMA/CA 随机接入方式的设备使用，其中一些由控制器分配给特定的设备，因而为那些设备提供了确保的信道。有关 ZigBee 网络的更多细节能够在 [Baronti 2007, IEEE 802.15.4 2012] 中找到。

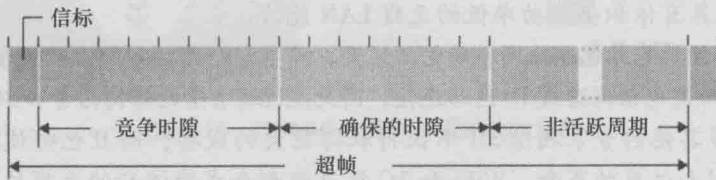


图 6-17 ZigBee 802.15.4 超帧结构

6.4 蜂窝因特网接入

在前一节中，我们考察了一台因特网主机当位于 WiFi 热区中时，即当它位于一个 802.11 接入点附近时，是如何接入因特网的。然而大多数 WiFi 热区只有一个直径为 10 ~ 100m 的小规模覆盖范围。当我们十分需要无线因特网接入但同时又无法访问 WiFi 热区时，该怎么办呢？

鉴于蜂窝电话目前在全球许多区域已经是无处不在了，一个很自然的策略就是扩展蜂窝网络，使它们不仅支持语音电话，同时也支持无线因特网接入。理想情况下，这种因特网接入将会有相当高的速率，并且可以提供无缝的移动性，允许用户在旅行过程中（如在汽车或火车上）保持其 TCP 会话。使用足够高的上行和下行比特速率，用户甚至可以在移动中维持视频会议。这种情况并非遥不可及。在 2012 年，美国的许多蜂窝电话提供商以低于 50 美元/月的价格，为用户提供数百 kbps 的上行和下行比特速率的蜂窝因特网接入。随着那些我们将在这里涉及的宽带数据服务的更广泛部署，每秒几兆比特的数据速率正变得可行。

在本节中，我们对当前和即将出现的蜂窝因特网接入技术进行简要概述。我们这里仍然重点关注无线第一跳以及将无线第一跳连接进更大的电话网和因特网的网络；在 6.7 节中，我们将考虑如何把呼叫路由选择到在不同基站间移动的用户。我们的简要讨论只是对蜂窝技术进行一个简单、宏观描述。当然，现代蜂窝通信有更大的广度和深度，有许多大学提供关于这一主题的许多课程。希望对此做更深入了解的读者可参阅 [Goodman 1997; Kaaranen 2001; Lin 2001; Korhonen 2003; Schiller 2003; Scourias 2012; Turner 2012;

Akyildiz 2010], 以及特别优秀和详尽的参考资料 [Mouly 1992]。

历史事件

3G 蜂窝移动与无线 LAN 的比较

许多蜂窝移动电话的运营者正在部署 3G 蜂窝移动系统, 它的户内数据速率为 2Mbps, 户外数据速率为 384kbps, 或者速率更高。这些 3G 系统部署在需要许可证的无线频带中, 运营者向政府支付可观的费用来获得使用频谱的许可证。3G 系统以一种与现在蜂窝电话相似的接入方式, 允许用户在活动中从遥远的户外接入因特网。例如, 3G 技术允许用户在开车的时候访问行车地图信息, 或者在海滩进行日光浴时访问电影院的信息。无论如何, 考虑到 3G 的费用和用户经常同时接入无线 LAN 和 3G 的事实, 人们可能会质疑 3G 系统使用的程度:

- 新兴的无线 LAN 基础设施将可能变得几乎无所不在。工作于 54Mbps 的 IEEE 802.11 无线 LAN 已经得到了广泛部署。几乎所有便携计算机和智能手机出厂时都配有 802.11 LAN 的能力。而且, 新兴的因特网装置 (例如无线照相机和相框) 也具有体积小、功率低的无线 LAN 能力。
- 无线 LAN 的基站也能处理移动电话装置。许多电话已经能够直接或使用类 Skype IP 语音与蜂窝电话网络或 IP 网络连接, 因此绕过运营者的蜂窝语音和 3G 数据服务。

当然, 许多其他的专家相信 3G 不仅将取得巨大的成功, 而且也将使我们工作和生活方式发生引人注目的革命。WiFi 和 3G 很可能都会成为流行的无线技术, 让漫游无线设备自动选择在其当前所处物理位置提供最好服务的接入技术。

6.4.1 蜂窝网体系结构概述

在本节描述蜂窝网体系结构时, 我们将采用全球移动通信系统 (GSM) 标准的术语。从历史的角度看, 首字母缩写词 GSM 源于术语 “Groupe Spécial Mobile”, 后来才采用了更为英文化的名字, 不过这使最初的首字母缩写词得以保留。到了 20 世纪 80 年代, 欧洲人认识到需要一个泛欧洲的数字蜂窝电话系统, 以代替多个不兼容的模拟蜂窝电话系统, 从而导致了 GSM 标准的出现 [Mouly 1992]。欧洲人在 20 世纪 90 年代初就成功地部署了 GSM 技术, 自此后 GSM 成长为移动电话领域的庞然大物, 全世界有超过 80% 以上的蜂窝用户使用 GSM。

当人们谈论蜂窝技术时, 他们经常将该技术分类为几 “代” 之一。最早一代的设计主要用于语音通信。第一代 (1G) 系统是模拟 FDMA 系统, 其专门用于语音通信。这些 1G 系统目前几乎绝迹, 它们被数字 2G 系统所替代。初始的 2G 系统也是为语音而设计, 但后来除了语音服务外还扩展了对数据 (即因特网) 的支持 (2.5G)。当前正在部署的 3G 系统也支持语音和数据, 但越来越强调其数据能力和更高速的无线接入链路。

2G 蜂窝网体系结构: 与电话网的语音连接

术语蜂窝 (cellular) 是指这样的事实, 即由一个蜂窝网覆盖的区域被分成许多称作小区 (cell) 的地理覆盖区域, 小区如图 6-18 左侧的六边形所示。如同在 6.3.1 节中学习的 802.11 WiFi 标准一样, GSM 有自己的特殊命名法。每个小区包含一个收发基站 (Base

Transceiver Station, BTS), 负责向位于其小区内的移动站点发送或接收信号。一个小区的覆盖区域取决于许多因素, 包括 BTS 的发射功率、用户设备的传输功率、小区中的障碍建筑物以及基站天线的高度。尽管图 6-18 中显示的是每个小区包含一个位于该小区中间的收发基站, 但今天的许多系统将 BTS 放置在 3 个小区的交叉处, 使得具有有向天线的单个 BTS 能够为三个小区提供服务。

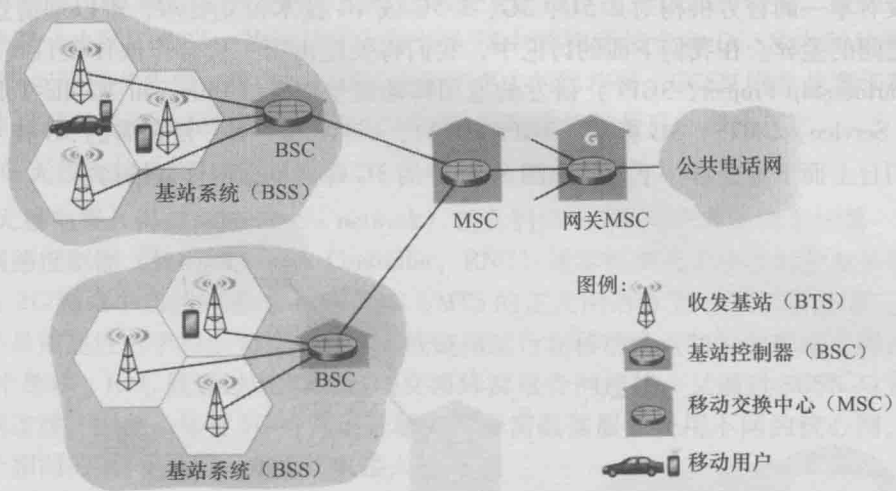


图 6-18 GSM 2G 蜂窝网体系结构的组件

2G 蜂窝系统的 GSM 标准对空中接口使用了组合的 FDM/TDM (无线电)。第 1 章中讲过, 使用纯 FDM, 信道被划分成许多频段, 每个呼叫分配一个频段。第 1 章也讲过, 使用纯 TDM, 时间被划分为帧, 每个帧又被进一步划分为时隙, 每个呼叫在循环的帧中被分配使用特定的时隙。在组合的 FDM/TDM 系统中, 信道被划分为若干频率子带; 对于每个子带, 时间又被划分为帧和时隙。因此, 对于一个组合的 FDM/TDM 系统, 如果信道被划分为 F 个子带, 并且时间被划分为 T 个时隙, 那么该信道将能够支持 $F \cdot T$ 个并发的呼叫。我们在 5.3.4 节中看到, 电缆接入网也使用了组合的 FDM/TDM 方法。GSM 系统由多个 200kHz 的频带组成, 每个频带支持 8 个 TDM 呼叫。GSM 以 13kbps 和 12.2kbps 的速率编码。

一个 GSM 网络的**基站控制器** (Base Station Controller, BSC) 通常服务于几十个收发基站。BSC 的责任是为移动用户分配 BTS 无线信道, 执行寻呼 (paging) (找出某移动用户所在的小区), 执行移动用户的切换 (切换是我们将在 6.7.2 节中涉及的主题)。基站控制器及其控制的收发基站共同构成了 GSM **基站系统** (Base Station System, BSS)。

我们将在 6.7 节中看到, 在用户鉴别和账户管理 (决定是否允许某个移动设备与蜂窝网络连接) 以及呼叫建立和切换中, **移动交换中心** (Mobile Switching Center, MSC) 起着决定性的作用。单个 MSC 通常将包含多达 5 个 BSC, 因此每个 MSC 有大约 200 000 个用户。一个蜂窝提供商的网络将有若干 MSC, 使用称为网关 MSC 的特殊 MSC 将提供商的蜂窝网络与更大的公共电话网相连。

6.4.2 3G 蜂窝数据网: 将因特网扩展到蜂窝用户

我们在 6.4.1 节中的讨论关注了蜂窝语音用户连接到公共电话网。当然, 当我们开始

这样干时，也乐意读电子邮件、访问 Web、获取位置相关的服务（例如地图和餐馆推荐），或许甚至观看流式视频。为此，我们的智能手机需要运行完整的 TCP/IP 协议栈（包括物理层、链路层、网络层、运输层和应用层），并能够经过蜂窝网与因特网连接。随着一代（和半代）继承一代，以及引入许多具有新首字母缩略词的新技术和服务，蜂窝数据网的主题也就是讨论一系列相互竞争和不断演化的标准，这个标准集合相当令人迷惑。更糟糕的是，没有单一的官方机构对 2.5G、3G、3.5G 或 4G 技术设立要求，难以理清这些竞争性标准之间的差异。在我们下面的讨论中，我们将关注由第三代合作伙伴项目（3rd Generation Partnership Project, 3GPP）研发的通用移动通信服务（Universal Mobile Telecommunications Service, UMTS）3G 标准 [3GPP 2012]，UMTS 是一种广泛部署的 3G 技术。

我们自上而下地查看一下显示在图 6-19 中的 3G 蜂窝数据网体系结构。

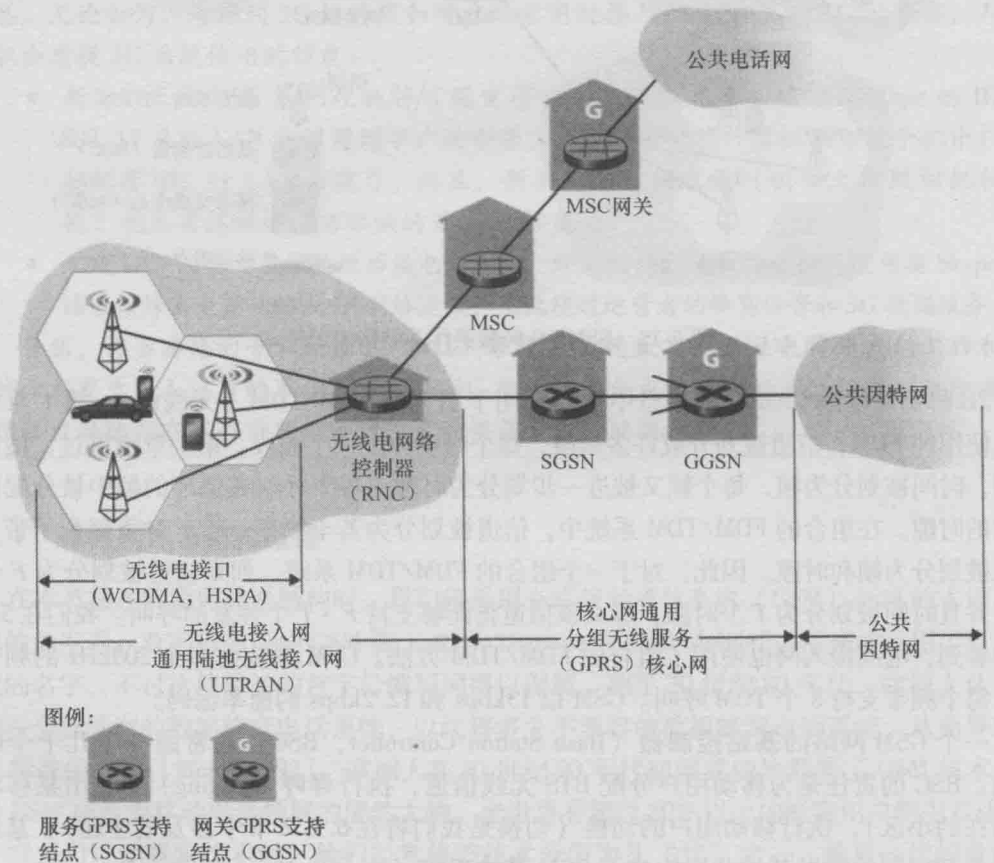


图 6-19 3G 系统体系结构

1. 3G 核心网

3G 核心蜂窝数据网将无线接入网连接到公共因特网。核心网与我们前面在图 6-18 中遇到过的现有蜂窝语音网（特别是 MSC）的组件协作。由于在现有的蜂窝语音网中具有大量的现有基础设施（有利可图的服务！），3G 的设计者们所采取的方法非常清楚：不去触动现有核心 GSM 蜂窝语音网，增加与现有蜂窝语音网平行的附加蜂窝数据功能。如果将新的数据服务直接增加到现有的蜂窝语音网上，这种方法同样会引发 4.4.4 节中遇到的挑战——在前面我们讨论了在因特网中综合新的 (IPv6) 和遗产 (IPv4) 技术。

在3G核心网中有两类结点：服务通用分组无线服务支持结点（Serving Generalized packet radio service Support Node, SGSN）和网关GPRS支持结点（Gateway GPRS Support Node, GGSN）。（GPRS（General Packet Radio Service）表示通用分组无线服务，这是一种在2G网络中的早期蜂窝数据服务；这里我们讨论的是在3G网络中的GPRS的演化版本。）一个SGSN负责向位于其连接的无线电接入网中的移动结点交付（或从移动结点获取）数据报。SGSN与该区域蜂窝语音网的MSC进行交互，提供用户认证和切换，维护活跃移动结点的位置（小区）信息，执行位于无线电接入网中的移动结点和GGSN之间的数据报转发。GGSN起到网关作用，将多个SGSN连接到更大的因特网。GGSN因此是源于移动结点的一个数据报在进入更大因特网之前遇到的3G基础设施的最后一部分。

2. 3G 无线电接入网：无线边缘

3G无线电接入网（radio access network）是我们作为3G用户看见的无线第一跳网络。无线网络控制器（Radio Network Controller, RNC）通常控制几个小区的收发基站，类似于我们在2G网络中遇到的基站（但是3G UMTS的正式用语称为一个“结点B”，这是一个相当不具描述性名字！）。每个小区的无线链路运行在移动结点和收发基站之间，就像在2G网络中那样。RNC既通过MSC与电路交换蜂窝语音网连接，又通过SGSN与分组交换的因特网连接。因此，尽管3G蜂窝语音服务和蜂窝数据服务使用不同的核心网，但它们共享一个相同的第一/最后一跳无线电接入网。

较之2G网络，在3G UMTS中的一个重大变化是不再使用GSM的FDMA/TDMA方案，UMTS在TDMA时隙中使用称为直接序列宽带CDMA（Direct Sequence Wideband CDMA, DS-WCDMA）的CDMA技术 [Dahlman 1998]。TDMA时隙又在多个频率上可供使用，即有趣地使用了我们在前面第5章指出的全部三种不同的信道共享方法，并且类似于有线电视接入网中所采用的方法（参见5.3.4节）。这种变化要求一个新的3G蜂窝无线接入网与显示在图6-19中的2G BSS无线网络并行运行。与WCDMA规范相关的数据服务被称为高速分组接入（High Speed Packet Access, HSPA），其下行数据传输率有望高达14Mbps。有关3G网络的细节能够在3GPP Web站点上找到 [3GPP 2012]。

6.4.3 走向4G：LTE

随着现在3G系统的全球部署，4G系统的到来还远吗？当然不会！4G系统的设计、早期测试和初始部署的确已经在进行中了。由3GPP提出的4G长期演化（4G Long-Term Evolution, LTE）标准，与3G相比有两项重要创新：

- 演化的分组核（Evolved Packet Core, EPC） [3GPP Network Architecture 2012]。EPC是一个简化的全IP核心网络，该网络将分离的电路交换蜂窝语音网与图6-19中显示的分组交换蜂窝数据网统一起来。它是一个“全IP”网络，是指语音和数据将在IP数据报中承载。如我们在第4章中已经看到和将在第7章中更为详细地学习的那样，IP的“尽力而为”服务模型本质上并不非常适合IP语音（VoIP）流量的严格的性能要求，除非精心管理网络资源避免（并非作出反应）拥塞。因此，EPC的关键任务是管理网络资源以提供这种高质量的服务。EPC也对网络控制和用户数据平面做出了明确划分，因为我们将在6.7节中学习的许多移动性支持功能将在控制平面中实现。EPC允许多种类型的无线电接入网（包括遗留的2G和3G无线电接入网）与核心网连接。对EPC的两个可读性很强的概述见

[Motorola 2007; Alcatel-Lucent 2009]。

- **LTE 无线电接入网 (LTE Radio Access Network)**。LTE 在下行信道采用频分复用和时分复用结合的方法，称之为正交频分复用 (Orthogonal Frequency Division Multiplexing, OFDM) 技术 [Rohde 2008; Ericsson 2011]。(“正交”一词来源于如下事实，所生成的在不同频道上发送的信号，它们相互干扰非常小，即使当信道频率紧密排列时)。在 LTE 中，每个活跃的移动结点都可以在一个或更多个信道频率上被分配一个或更多个 0.5ms 时隙。图 6-20 显示了在 4 个频率上分配 8 个时隙的情况。通过分配越来越多的时隙 (无论是用相同的频率还是用不同的频率)，移动结点能够获取越来越高的传输速率。在移动结点之间进行时隙 (重) 分配的频度为每毫秒一次。不同的调制方案也能被用于改变传输速率；参见我们前面对图 6-3 的讨论以及 WiFi 网络中调制方案的动态选择。LTE 无线网络中的另一项创新是使用复杂的多输入多输出 (MIMO) 天线。当使用 20MHz 无线频谱时，一个 LTE 用户的最大数据率能够达到下行方向 100Mbps 和上行方向 50Mbps。

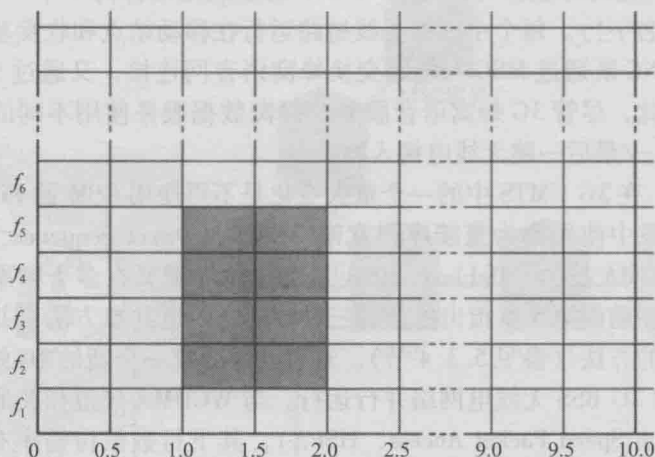


图 6-20 在每个频率上，20 个 0.5ms 的时隙组成 10ms 帧。阴影显示了一个 8 个时隙分配

LTE 标准并未对移动结点的时隙特殊分配进行强制要求。相反，允许哪个移动结点在某个给定的时隙在给定的频率下传输，这个决定由 LTE 设备商和/或网络运营商提供的调度算法来做出。使用机会调度 [Bender 2000; Kolding 2003; Kulkarni 2005]，将物理层协议与发送方和接收方之间的信道条件相匹配，基于信道条件选择分组将发往的接收方，使无线网络控制器能够最大限度地利用无线媒体。此外，用户优先权和服务的契约等级 (如银、金或铂金) 能够在下行分组传输的调度中使用。除了上面描述的 LTE 能力，高级的 LTE 通过分配聚合信道给移动结点允许数百兆下行带宽 [Akyildiz 2010]。

另一种 4G 无线技术是 WiMAX (全球微波接入互操作)，它是一个 IEEE 802.16 标准协议簇，与 LTE 有着重大差异。究竟是 LTE 还是 WiMAX 将成为 4G 技术的选择仍然有待观察，但是在本书写作的时候 (2012 年春)，LTE 看起来具有更强劲的动力。WiMAX 的详细讨论能够在本书的 Web 网站上找到。

6.5 移动管理：原理

学习了无线网络中通信链路的无线特性后，现在我们转向这些无线链路带来的移动性。

宽泛地讲，移动结点是随时间改变它与网络连接位置的结点。因为移动性这一术语在计算机和电话界有许多含义，所以先更为详细地讨论一下移动性的各个方面将对我们很有帮助。

- 从网络层的角度看，用户如何移动？一个物理上移动的用户将对网络层提出一系列不同寻常的挑战，这取决于他（她）在网络连接点之间如何移动。在图 6-21 中的移动程度谱的一端，用户也许带着一台装有无线网络接口卡的便携机在一座建筑物内走动。如我们在 6.3.4 节中所见，从网络层的角度来看，该用户并没有移动。而且，如果该用户不论在何处都与同一个接入点相关联，从链路层角度来看该用户甚至也没有移动。

在该移动程度谱的另一端，考虑一下该用户在一辆“宝马”轿车内以 150km/h 的时速沿高速公路急速行驶时穿过多个无线接入网，并希望在整个旅程中保持一个与远程应用的不间断的 TCP 连接。这个用户无疑是移动的！在这两种极端之间的情况是，一个用户带着一台便携机从一个地方（如办公室或宿舍）到另一个地方（如咖啡店、教室），并且想在新地方连入网络。该用户也是移动的（虽然比“宝马”驾驶员的移动性差一些！），只不过不需要在网络接入点之间移动时维持一个不间断的连接。图 6-21 从网络层角度阐明了用户移动性的程度谱。

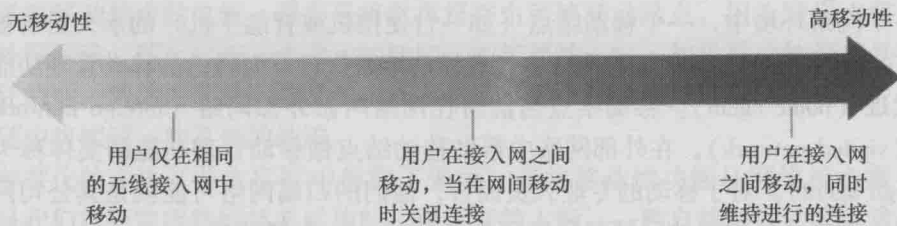


图 6-21 从网络层观点来看各种程度的移动性

- 移动结点的地址始终保持不变有多么重要？对移动电话而言，当你从一个提供商移动电话网络到另一个的过程中，你的电话号码（本质上是你的网络层地址）始终保持不变。类似地，便携机在 IP 网络之间移动时是否也必须维持相同的 IP 地址呢？

对这一问题的回答很大程度上取决于所运行的应用程序。对于那个在高速公路上飞驰，同时又希望维持对一个远程应用的不间断的 TCP 连接的宝马司机而言，维持相同的 IP 地址将会带来便利。回想第 3 章，一个因特网应用程序需要知道它与之通信的远端实体的 IP 地址和端口号。如果一个移动实体在移动过程中能够保持其 IP 地址不变，从应用的角度，移动性就变得不可见。这种透明性有十分重要的价值，即应用程序不必关心 IP 地址潜在的变化，并且同样的应用程序代码既可用于移动连接，又可用于非移动连接。在下一节我们将会看到移动 IP 提供了这种透明性，它允许移动结点在网络间移动的同时维持其永久的 IP 地址。

在另一方面，一个不太喜欢新潮的移动用户也许只想关闭办公室便携机，将其带回家，然后开机，再在家中工作。如果该便携机在家时只是作为一个客户，使用客户-服务器方式的应用（如发送/阅读电子邮件、浏览 Web、通过 Telnet 与远程主机相连），则使用特定 IP 地址并不是那么重要。特别是，用户能够得到一个由服务于家庭的 ISP 临时分配的 IP 地址即可。我们在 4.4 节中看到的 DHCP 提供了这种功能。

• 有哪些可用的有线基础设施的支持？在所有上述情形中，我们都隐含地假设存在一个固定的基础设施让移动用户连接，例如家庭的 ISP 网络、办公室的无线接入网，或者沿高速公路的无线接入网。如果这样的基础设施不存在会怎么样？如果两个用户位于彼此的通信范围内，他们能否在没有其他网络基础设施存在的情况下建立一个网络连接？自组织网络正好提供了这些能力。这一飞速发展的领域位于移动网络研究的前沿，超出了本书的范围。[Perkins 2000] 和 IETF 移动自组织网络 (manet) 工作组主页 [manet 2012] 提供了有关这一主题的详尽讨论。

为了阐述允许移动用户在不同网络间移动过程中维持正在进行的连接所涉及的问题，我们考虑一个人类的类比例子。一位 20 岁左右的青年从家里搬出，成为流动的人，在一些宿舍或公寓居住，并经常改换住址。如果一个老朋友想与他联系，这位朋友怎样才能找到这个流动的朋友呢？一种常用的方法是与他的家庭取得联系，因为一位流动的青年通常会将其目前的地址告诉家里（即使没有其他原因，哪怕只是为了让父母寄钱来帮他付房租）。其家庭由于有一个永久地址，因此成为其他想与该流动青年联系的人可采用的第一步。这些朋友后来与他的通信也许是间接的（如先将邮件发送到其父母家，再转发给该流动的青年），也许是直接的（如该朋友用得到的地址直接将邮件发送给其流动的朋友）。

在一个网络环境中，一个移动结点（如一台便携机或智能手机）的永久居所被称为归属网络 (home network)，在归属网络中代表移动结点执行下面讨论的移动管理功能的实体叫归属代理 (home agent)。移动结点当前所在网络叫做外部网络 (foreign network) 或被访网络 (visited network)，在外部网络中帮助移动结点做移动管理功能的实体称为外部代理 (foreign agent)。对于移动的专业人员而言，他们的归属网络可能就是其公司网络，而被访网络也许就是他们正访问的某同行所在的网络。一个通信者 (correspondent) 就是希望与该移动结点通信的实体。图 6-22 阐述了这些概念，也说明了下面考虑的编址概念。在图 6-22 中，我们注意到代理被配置在路由器上（例如，作为在路由器上运行的进程），但它们也能在网络中其他主机或服务器上执行。

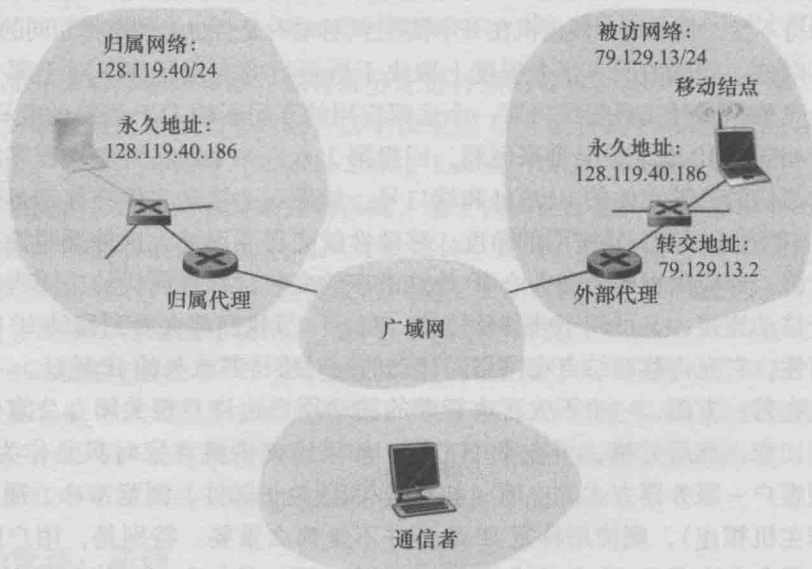


图 6-22 移动网络体系结构中的初始要素

6.5.1 寻址

我们前面提到为了使用户移动性对网络应用透明，希望一个移动结点在从一个网络移动到另一个网络时保持其地址不变。当某移动结点位于一个外部网络时，所有指向此结点固定地址的流量需要导向外部网络。怎样才能做到这一点呢？外部网络可用的一种方法就是向所有其他网络发通告，告诉它们该移动结点正在它的网络中。这通常可通过交换域内与域间路由选择信息来实现，而且只需对现有路由选择基础设施做很少的改动即可。外部网络只需通告其邻居它有一条非常特别的路由能到达该移动结点的固定地址，即告诉其他网络它有一条正确的路径可将数据报导向该移动结点的固定地址（即基本上是通知其他网络，它有一条可将数据报路由选择到该移动结点的永久地址的正确路径；参见 4.4 节）。这些邻居将在全网传播该路由选择信息，而且是当作更新路由选择信息和转发表的正常过程的一部分来做。当移动结点离开一个外部网络后又加入另一个外部网络时，新的外部网络会通告一条新的通向该移动结点的特别路由，旧的外部网络将撤销其与该移动结点有关的路由选择信息。

这种方法立刻解决了两个问题，且它这样做不需对网络层基础设施做重大改动。其他网络知道该移动结点的位置，很容易将数据报路由到该移动结点，因为转发表将这些数据报导向外部网络。然而它有一个很大的缺陷，即扩展性不好。如果移动性管理是网络路由器的责任的话，则路由器将必须维护可能多达数百万个移动结点的转发表表项。在本章后面的习题中将探讨一些其他的缺陷。

一种替代的方法（并在实际中得到了采用）是将移动性功能从网络核心搬到网络边缘，这是我们在研究因特网体系结构时一再重复的主题。一种自然的做法是由该移动结点的归属网络来实现。与那个流动青年的父母跟踪他们孩子的位置有许多相似之处，在移动结点的归属网络中的归属代理也能跟踪该移动结点所在的外部网络。这当然需要一个移动结点（或一个代表该移动结点的外部代理）与归属代理之间的协议来更新移动结点的位置。

我们现在更详细地来思考外部代理。如图 6-22 所示，概念上最简单的方法是将外部代理放置在外部网络的边缘路由器上。外部代理的作用之一就是为移动结点创建一个所谓的**转交地址**（Care-Of Address, COA），该 COA 的网络部分与外部网络的网络部分相匹配。因此一个移动结点可与两个地址相关联，即其**永久地址**（permanent address）（类比于流动青年的家庭地址）与其 COA，该 COA 有时又称为**外部地址**（foreign address）（类比于流动青年当前居住的房屋地址）。在图 6-22 中的例子中，移动结点的固定地址是 128.119.40.186。当被访网络为 79.129.13/24 时，该移动结点具有的 COA 为 79.129.13.2。外部代理的第二个作用就是告诉归属代理，该移动结点在它的（外部代理的）网络中且具有给定的 COA。我们很快就会看到，该 COA 将用于将数据报通过外部代理“重新路由选择”到移动结点。

虽然我们已将移动结点与外部代理的功能分开，但是应当注意到移动结点也能承担外部代理的责任。例如，某移动结点可在外部网络中得到一个 COA（使用一个诸如 DHCP 之类的协议），且由它自己把其 COA 通告给归属代理。

6.5.2 路由选择到移动结点

我们现在已看到一个移动结点是如何得到一个 COA 的，归属代理又是如何被告知该地址的。但让归属代理知道该 COA 仅能解决部分问题。数据报应怎样寻址并转发给移动

结点呢？因为只有归属代理（而不是全网的路由器）知道该移动结点的位置，故如果只是将一个数据报寻址到移动结点的永久地址并将其发送到网络层基础结构中，这样做已不再满足需要了。还有更多的事情要做。目前有两种不同的方法，我们将称其为间接路由选择与直接路由选择。

1. 移动结点的间接路由选择

我们先考虑一个想给移动结点发送数据报的通信者。在间接路由选择（indirect routing）方法中，通信者只是将数据报寻址到移动结点的固定地址，并将数据报发送到网络中去，完全不知道移动结点是在归属网络中还是正在访问某个外部网络，因此移动性对于通信者来说是完全透明的。这些数据报就像平常一样首先导向移动结点的归属网络。这用图 6-23 中的步骤 1 加以说明。

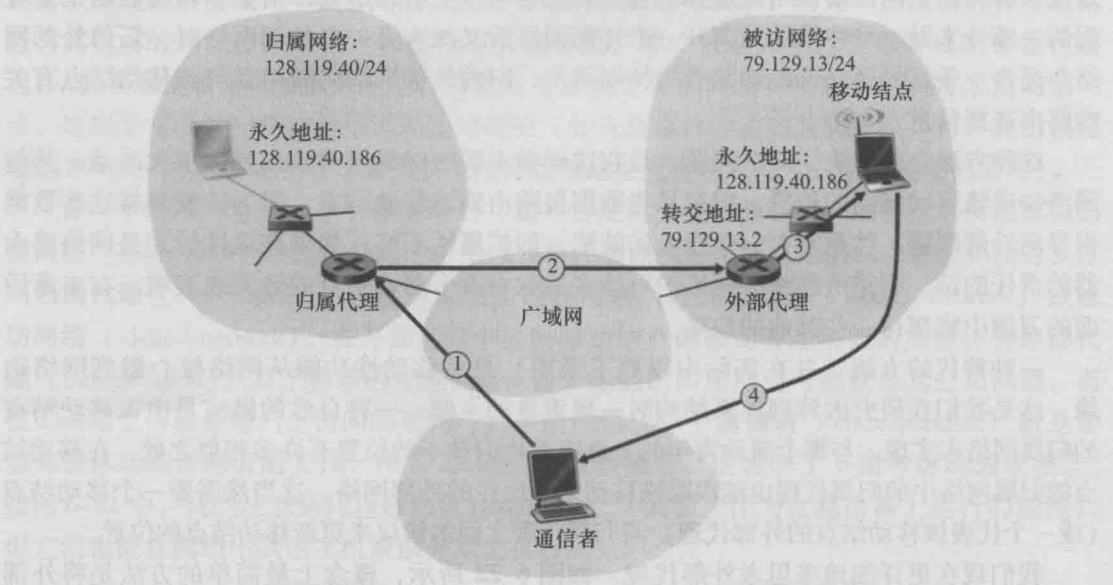


图 6-23 对移动结点的间接路由选择

我们现在将注意力转向归属代理。除了负责与外部代理交互以跟踪移动结点的 COA 外，归属代理还有另一项很重要的功能。它的第二项工作就是监视到达的数据报，这些数据报寻址的结点的归属网络与该归属代理所在网络相同，但这些结点当前却在某个外部网络中。归属代理截获这些数据报，然后按一个两步骤的过程转发它们。通过使用移动结点的 COA，该数据报先转发给外部代理（图 6-23 中的步骤 2），然后再从外部代理转发给移动结点（图 6-23 中的步骤 3）。

仔细地思考这种重新路由选择过程是有益的。归属代理需要用该移动结点的 COA 来设置数据报地址，以便网络层将数据报路由选择到外部网络。在另一方面，需要保持通信者数据报的原样，因为接收该数据报的应用程序应该不知道该数据报是经由归属代理转发而来的。让归属代理将通信者的原始完整数据报封装（encapsulate）在一个新的（较大的）数据报中，这两个目标都可以得到满足。这个较大的数据报被导向并交付到移动结点的 COA。“拥有”该 COA 的外部代理将接收并拆封该数据报，即从较大的封装数据报中取出通信者的原始数据报，然后再向移动结点转发该原始数据报（图 6-23 中的步骤 3）。

图 6-24 显示了如下过程：一个通信者向归属网络发送原始数据报；向外部代理发送一个封装的数据报；以及向移动结点交付最初的数据报。思维敏锐的读者将会注意到，这里描述的封装/拆封概念等同于隧道的概念，隧道是在第 4 章中讨论 IP 多播与 IPv6 时涉及的。

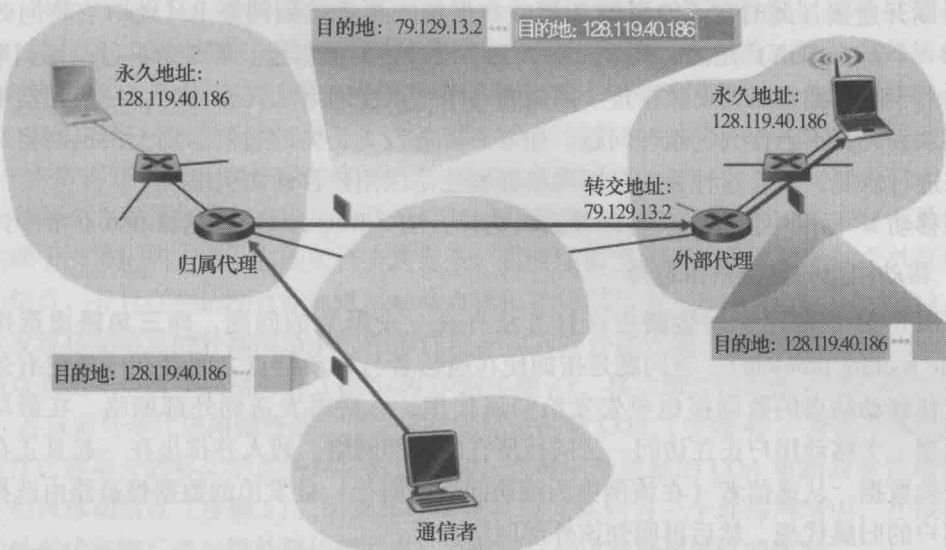


图 6-24 封装与拆封

接下来我们考虑某移动结点如何向一个通信者发送数据报。这相当简单，因为移动结点可直接将其数据报寻址到通信者（使用自己的永久地址作为源地址，通信者的地址作为目的地址）。因为移动结点知道通信者的地址，所以没有必要通过归属代理迂回传送数据报。这就是显示在图 6-23 中的步骤 4。

下面通过列出支持移动性所需要的网络层新功能，我们小结一下对有关间接路由选择的讨论。

- 移动结点到外部代理的协议。当移动结点连接到外部网络时，它向外部代理注册。类似地，当一个移动结点离开该外部网络时，它将向外部代理取消注册。
- 外部代理到归属代理的注册协议。外部代理将向归属代理注册移动结点的 COA。当某移动结点离开其网络时，外部代理不需要显式地注销 COA，因为当移动结点移动到一个新网络时，随之而来就要注册一个新的 COA，这将完成了注销。
- 归属代理数据报封装协议。将通信者的原始数据报封装在一个目的地址为 COA 的数据报内，并转发之。
- 外部代理拆封协议。从封装好的数据报中取出通信者的原始数据报，然后再将该原始数据报转发给移动结点。

上述讨论提供了一个移动结点在网络之间移动时要维持一个不间断的连接所需的各部分：外部代理、归属代理和间接转发。举一个例子来说明这些部分是如何协同工作的。假设某移动结点连到外部网络 A，向其归属代理注册了网络 A 中的一个 COA，并且正在接收通过归属代理间接路由而来的数据报。该移动结点现在移动到外部网络 B 中，并向网络 B 中的外部代理注册，外部代理将该移动结点的新 COA 告诉了其归属代理。此后，归属代理将数据报重路由到网络 B。就一个通信者关心的东西而言，移动性是透明的，即在移动

前后，数据报都是由相同的归属代理进行路由选择。就归属代理关心的东西而言，数据报流没有中断，即到达的数据报先是转发到外部网络 A；改变 COA 后，则数据报转发到外部网络 B。但当移动结点在网络之间移动时，它会看到数据报流中断吗？只要移动结点与网络 A 断开连接（此时它不能再经 A 接收数据报）再连接到网络 B（此时它将向归属代理注册一个新的 COA）用的时间少，那么几乎没有丢失数据报。第 3 章讲过，端到端连接可能会由于网络拥塞而丢失数据报。因而当一个结点在网络之间移动时，一条连接中的数据报偶尔丢失算不上什么灾难性问题。如果需要进行无丢失的通信，则上层机制将对数据报丢失进行恢复，不管这种丢失是因网络拥塞还是因用户移动而引发的。

在移动 IP 标准中使用了一种间接路由选择方法 [RFC 5944]，这将在 6.6 节中讨论。

2. 移动结点的直接路由选择

在图 6-23 中阐述了间接路由选择方法存在一个低效的问题，即三角路由选择问题 (triangle routing problem)。该问题是指即使在通信者与移动结点之间存在一条更有效的路由，发往移动结点的数据报也要先发给归属代理，然后再发送到外部网络。在最坏情况下，设想一个移动用户正在访问一位同行所在的外部网络，两人并排坐在一起且正在通过网络交换数据。从通信者（在该例中为该访问者的同行）处发出的数据报被路由选择到该移动用户的归属代理，然后再回到该外部网络！

直接路由选择 (direct routing) 克服了三角路由选择的低效问题，但却是以增加复杂性为代价的。在直接路由选择方法中，通信者所在网络中的一个通信者代理 (correspondent agent) 先知道该移动结点的 COA。这可以通过让通信者代理向归属代理询问得知，这里假设与间接路由选择情况类似，移动结点具有一个在归属代理注册过的最新的 COA。与移动结点可以执行外部代理的功能相类似，通信者本身也可能执行通信者代理的功能。在图 6-25 中显示为步骤 1 和步骤 2。通信者代理然后将数据报直接通过隧道技术发往移动结点的 COA，这与归属代理使用的隧道技术相类似，参见图 6-25 的步骤 3 和步骤 4。

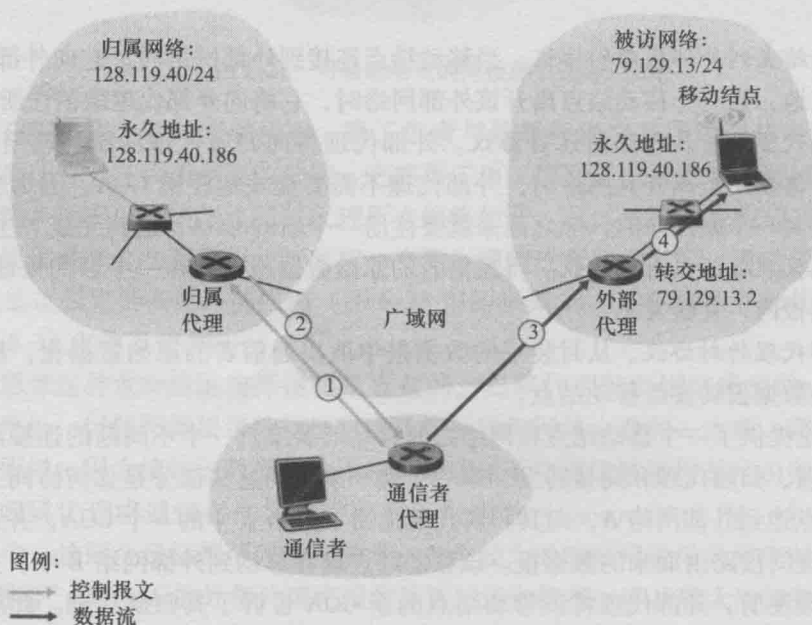


图 6-25 到某移动用户的直接路由选择

尽管直接路由选择克服了三角路由选择问题，但它引入了两个重要的其他挑战：

- 需要一个**移动用户定位协议**（mobile-user location protocol），以便通信者代理向归属代理查询获得移动结点的 COA（图 6-25 中的步骤 1 和步骤 2）。
- 当移动结点从一个外部网络移到另一个外部网络时，如何将数据报转发到新的外部网络？在间接路由选择的情况下，这个问题可以容易地通过更新由归属代理维持的 COA 来解决。然而，使用直接路由选择时，归属代理仅在会话开始时被通信者代理询问一次 COA。因此，当必要时在归属代理中更新 COA，这并不足以解决将数据路由选择到移动结点新的外部网络的问题。

一种解决方案是创建一个新的协议来告知通信者变化后的 COA。另一种方案也是在 GSM 网络实践中所采用的方案，它的工作方式如下。假设数据当前正转发给位于某个外部网络中的移动结点，并且在会话刚开始时该移动结点就位于该网络中（图 6-26 中的步骤 1）。我们将首次发现移动结点的外部网络中的外部代理标识为**锚外部代理**（anchor foreign agent）。当移动结点到达一个新外部网络后（图 6-26 中的步骤 2），移动结点向新的外部代理注册（步骤 3），并且新外部代理向锚外部代理提供移动结点的新 COA（步骤 4）。当锚外部代理收到一个发往已经离开的移动结点的封装数据报后，它可以使使用新的 COA 重新封装数据报并将其转发给该移动结点（步骤 5）。如果移动结点其后又移到另一个外部网络中，在该被访问网络中的外部代理随后将与锚外部代理联系，以便建立到该新外部网络的转发。

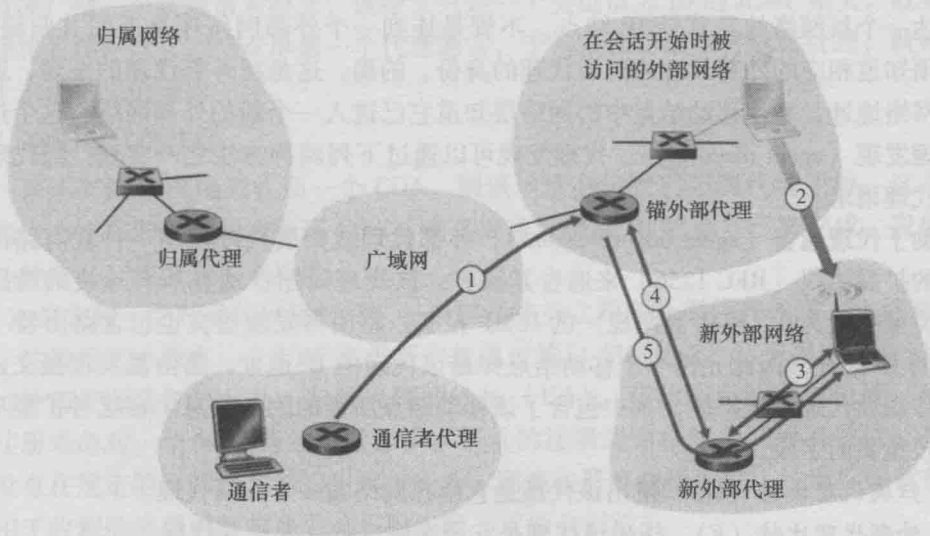


图 6-26 在网络间使用直接路由选择的移动转移

6.6 移动 IP

支持移动性的因特网体系结构与协议合起来称为移动 IP，对 IPv4 主要由 RFC 5944 定义。移动 IP 是一个灵活的标准，支持许多不同的运行模式（例如，具有或不具有外部代理的运行），代理与移动结点相互发现的多种方式，使用单个或多个 COA，以及多种形式的封装。同样，移动 IP 是一个复杂的标准，需要用整本书才能详细描述；的确有这样一本书 [Perkins 1998b]。这里，我们最基本的目标是对移动 IP 最重要的部分进行概述，并

说明它在一些常见情形中的使用。

移动 IP 体系结构包含了许多我们前面考虑过的要素，包括归属代理、外部代理、转交地址和封装/拆封等概念。当前的标准 [RFC 5944] 规定到移动结点使用间接路由选择的方法。

移动 IP 标准由三部分组成：

- 代理发现。移动 IP 定义了一个归属代理或外部代理用来向移动结点通告其服务的协议，以及移动结点请求一个外部代理或归属代理的服务所使用的协议。
- 向归属代理注册。移动 IP 定义了移动结点和/或外部代理向一个移动结点的归属代理注册或注销 COA 所使用的协议。
- 数据报的间接路由选择。该标准也定义了数据报被一个归属代理转发给移动结点的方式，包括转发数据报使用的规则、处理差错情况的规则和几种不同的封装形式 [RFC 2003; RFC 2004]。

在整个移动 IP 标准中安全性的考虑是很重要的。例如，显然需要对一个移动结点进行鉴别以确保一个恶意用户不能向归属代理注册一个伪造的转交地址，伪造地址将导致所有发给某个 IP 地址的数据报被重定向到恶意用户。移动 IP 使用许多机制来实现安全性，我们将在第 8 章考察这些机制，在以下的讨论中将不考虑安全性问题。

1. 代理发现

到达一个新网络的某移动 IP 结点，不管是连到一个外部网络还是返回其归属网络，它都必须知道相应的外部代理或归属代理的身份。的确，这是新外部代理的发现，通过一个新的网络地址，才使移动结点中的网络层知道它已进入一个新的外部网络。这个过程被称为代理发现 (agent discovery)。代理发现可以通过下列两种方法之一实现：经代理通告或者经代理请求。

借助于代理通告 (agent advertisement)，外部代理或归属代理使用一种现有路由器发现协议的扩展协议 [RFC 1256] 来通告其服务。该代理周期性地所有连接的链路上广播一个类型字段为 9 (路由器发现) 的 ICMP 报文。路由器发现报文也包含路由器 (即该代理) 的 IP 地址，因此允许一个移动结点知道该代理的 IP 地址。路由器发现报文还包括了一个移动性代理通告扩展，其中包含了该移动结点所需的附加信息。在这种扩展中有如下一些较重要的字段：

- 归属代理比特 (H)。指出该代理是它所在网络的一个归属代理。
- 外部代理比特 (F)。指出该代理是它所在网络的一个外部代理。
- 注册要求比特 (R)。指出在该网络中的某个移动用户必须向某个外部代理注册。特别是，一个移动用户不能在外网 (如使用 DHCP) 中获得一个转交地址，并假定由它自己承担外部代理的功能，无需向外网代理注册。
- M、G 封装比特。指出除了“IP 中的 IP” (IP-in-IP) 封装形式外，是否还要用其他的封装形式。
- 转交地址 (COA) 字段。由外部代理提供的一个或多个转交地址的列表。在下面的例子中，COA 将与外部代理关联，外部代理将接收发给该 COA 的数据报，然后再转发到适当的移动结点。移动用户在向其归属代理注册时将选择这些地址中的一个作为其 COA。

图 6-27 说明了在代理通告报文中的某些关键字段。

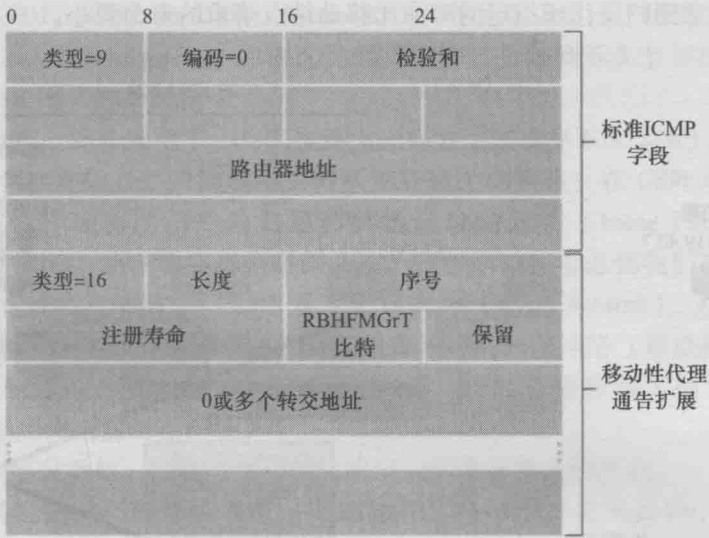


图 6-27 具有移动性代理通告扩展的 ICMP 路由器发现报文

使用**代理请求** (agent solicitation)，一个想知道代理的移动结点不必等待接收代理通告，就能广播一个代理请求报文，该报文只是一个类型值为 10 的 ICMP 报文。收到该请求的代理将直接向该移动结点单播一个代理通告，于是该移动结点将继续处理，就好像刚收到一个未经请求的通告一样。

2. 向归属代理注册

一旦某个移动 IP 结点收到一个 COA，则该地址必须要向归属代理注册。这可通过外部代理（由它向归属代理注册该 COA）或直接通过移动 IP 结点自己来完成。我们下面考虑前一种情况，共涉及 4 个步骤。

1) 当收到一个外部代理通告后，一个移动结点立即向外部代理发送一个移动 IP 注册报文。注册报文承载在一个 UDP 数据报中并通过端口 434 发送。注册报文携带以下内容：一个由外部代理通告的 COA、归属代理的地址 (HA)、移动结点的永久地址 (MA)、请求的注册寿命和一个 64 比特的注册标识。请求的注册寿命指示了注册有效的秒数。如果注册没有在规定的时间内在归属代理上更新，则该注册将变得无效。注册标识就像一个序号，用于收到的注册回答与注册请求的匹配（下面会讨论）。

2) 外部代理收到注册报文并记录移动结点的永久 IP 地址。外部代理知道现在它应该查找这样的数据报，即它封装的数据报的目的地址与该移动结点的永久地址相匹配。外部代理然后向归属代理的 434 端口发送一个移动 IP 注册报文（同样封装在 UDP 数据报中）。这一报文包括 COA、HA、MA、封装格式要求、请求的注册寿命以及注册标识。

3) 归属代理接收注册请求并检查真实性和正确性。归属代理把移动结点的永久 IP 地址与 COA 绑定在一起。以后，到达该归属代理的数据报与发往移动结点的数据报将被封装并以隧道方式给 COA。归属代理发送一个移动 IP 注册回答，该响应报文中包含有 HA、MA、实际注册寿命和被认可的请求报文注册标识。

4) 外部代理接收注册响应，然后将其转发给移动结点。

到此，注册便完成了，移动结点就能接收发送到其永久地址的数据报。图 6-28 说明了这些步骤。注意到归属代理指定的寿命比移动结点请求的寿命要小。

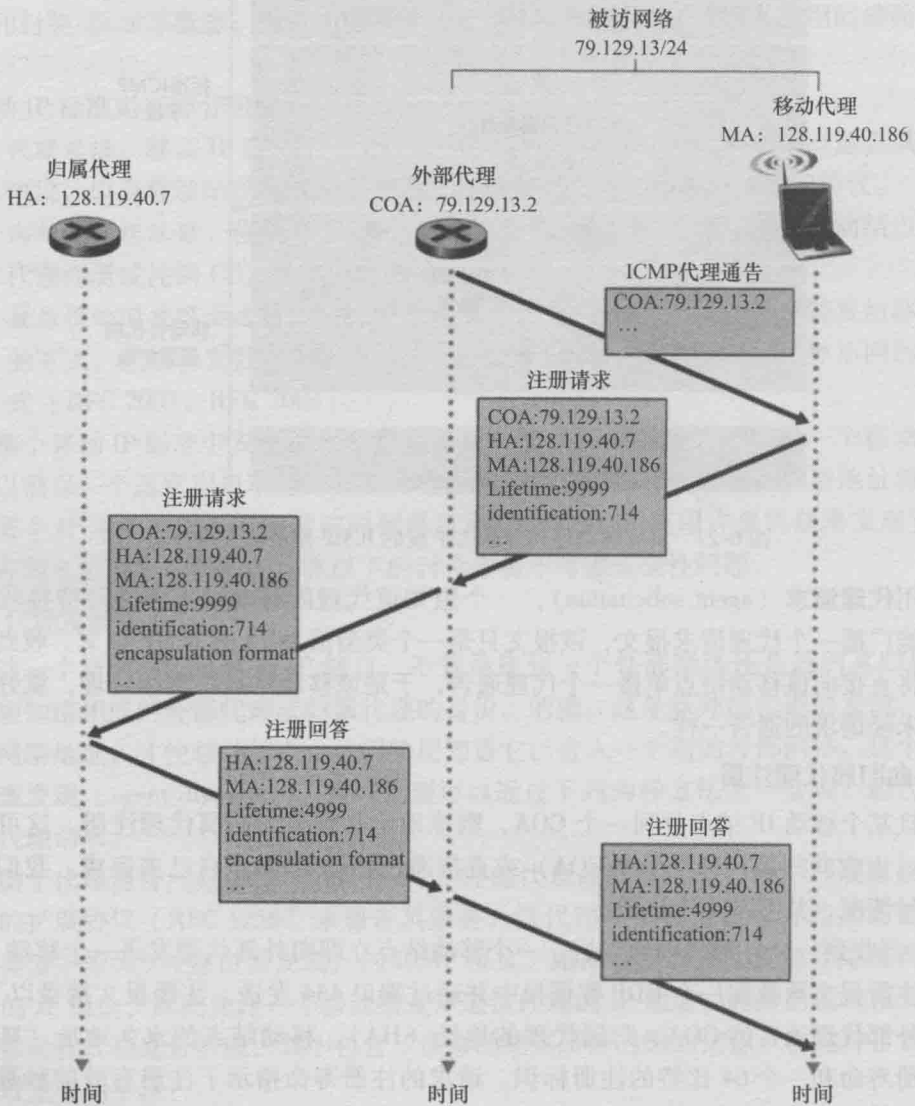


图 6-28 代理通告与移动 IP 注册

当某个移动结点离开其网络时，外部代理无需显式地取消某个 COA 的注册。当移动结点移动到一个新网（不管是另一个外部网络还是其归属网络）并注册一个新 COA 时，上述情况将自动发生。

除了上面所描述的情况，移动 IP 标准还允许许多另外的情形和功能，有兴趣的读者可以参阅 [Perkins 1998b; RFC 5944]。

6.7 蜂窝网中的移动性管理

分析了 IP 网络中的移动性管理以后，我们现将注意力转向对移动性支持有更长历史的网络，即蜂窝电话网络。尽管在 6.4 节中我们关注过蜂窝网中的第一跳无线链路，但这

里我们关注移动性，并以 GSM 蜂窝网络体系结构 [Goodman 1997; Mouly 1992; Scourias 2012; Kaaranen 2001; Korhonen 2003; Turner 2012] 作为学习案例，因为它是一个成熟并被广泛部署的技术。与在移动 IP 中的情况类似，我们将会看到 6.5 节指出的许多基本原理都被包含在 GSM 网络体系结构中。

与移动 IP 类似，GSM 采用了一种间接路由选择方法（参见 6.5.2 节），首先将通信者的呼叫路由选择到移动节点的归属网络，再从那里到达被访网络。在 GSM 术语中，移动用户的归属网络被称作该移动用户的归属公共地域移动网络（home Public Land Mobile Network, home PLMN）。由于首字母缩略词 PLMN 有些拗口，考虑到我们避免缩略词字母表的要求，我们直接将 GSM 归属 PLMN 称为归属网络（home network）。移动用户向某个蜂窝网提供商订购了服务，该蜂窝网就成为了这些用户的归属网络（即该提供商就按月提供的蜂窝服务收取用户的费用）。被访问的 PLMN，我们直接称其为被访网络（visited network），是移动用户当前所在网络。

与移动 IP 中情况类似，归属网络和被访网络的职责有很大的差别。

- 归属网络维护一个称作归属位置注册器（Home Location Register, HLR）的数据库，其中包括它每个用户的永久蜂窝电话号码以及用户个人概要信息。重要的是，HLR 也包括这些用户当前的位置信息。这就是说，如果一个移动用户当前漫游到另一个提供商的蜂窝网络中，HLR 中将包含足够多的信息来获取（通过一个我们即将描述的过程）被访网络中对移动用户的呼叫应该路由选择到的地址。我们将会看到，当一个呼叫定位到一个移动用户后，通信者将与归属网络中一个被称作网关移动服务交换中心（Gateway Mobile services Switching Center, GMSC）的特殊交换机联系。同样，为避免拗口的缩略词，我们这里用一个更具描述性的术语来称呼 GMSC，即归属 MSC（home MSC）。
- 被访网络维护一个称作访问者位置注册（Visitor Location Register, VLR）的数据库。VLR 为每一个当前在其服务网络中的移动用户包含一个表项，VLR 表项因此随着移动用户进入和离开网络而出现或消失。VLR 通常与移动交换中心（MSC）在一起，该中心协调到达或离开被访网络的呼叫建立。

在实践中，一个服务商的蜂窝网络将为其用户提供归属网络服务，同时为在其他蜂窝服务商订购服务的移动用户提供被访网络服务。

6.7.1 对移动用户呼叫的路由选择

现在我们描述一个呼叫如何定位到被访网络中的一个移动 GSM 用户。我们首先考虑下面一个简单的例子，更复杂的例子在 [Mouly 1992] 中有描述。如图 6-29 所示，这些步骤如下：

1) 通信者拨打移动用户的电话号码。该号码本身并不涉及一个特定的电话线路或位置（毕竟电话号码是固定的，而用户是移动的！），号码中的前几位数字足以全局地判别移动用户的归属网络。呼叫从通信者通过公共交换电话网到达移动用户归属网络中的归属 MSC。这是呼叫的第一步。

2) 归属 MSC 收到该呼叫并查询 HLR 来确定移动用户的位置。在最简单的情况下，HLR 返回移动站点漫游号码（Mobile Station Roaming Number, MSRN），我们称其为漫游号码（roaming number）。注意到这个号码与移动用户的永久电话号码不同，后者是与移动用

户的归属网络相关联的，而漫游号码是短暂的：当移动用户进入一个被访网络后，会给移动用户临时分配一个漫游号码。漫游号码的作用就相当于移动 IP 中转交地址的作用。并且，与 COA 类似，它也是对通信者和移动用户不可见的。如果 HLR 不具有该漫游号码，它返回被访网络中 VLR 的地址。在这种情况下（未在图 6-29 中显示出来），归属 MSC 需要查询 VLR 以便获取移动节点的漫游号码。但是 HLR 是如何首先得到漫游号码或 VLR 地址的呢？移动用户到另一个被访网络后这些值将发生怎样的变化？我们将很快考虑这些重要问题。

3) 给定一个漫游号码，归属 MSC 通过网络到达被访网络的 MSC 建立呼叫的第二步。至此，该呼叫已经完成，从通信者到达归属 MSC，再从归属 MSC 到达被访 MSC，然后到达为移动用户提供服务的基站。

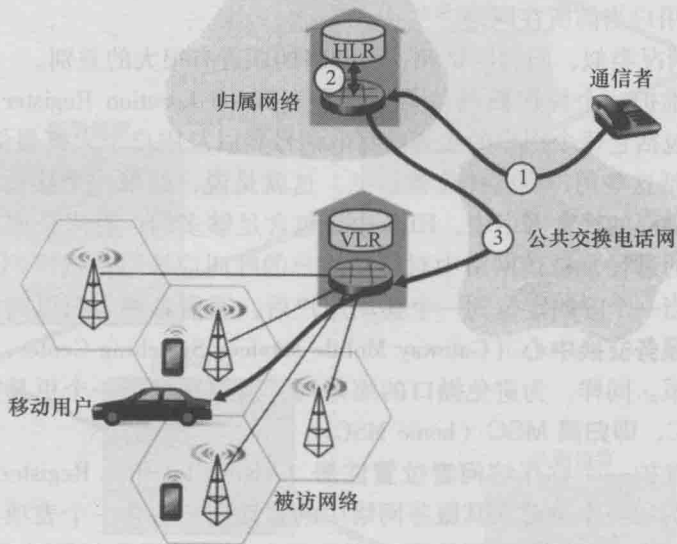


图 6-29 将呼叫定位到一个移动用户：间接路由选择

在第二步中，一个未解决的问题是 HLR 如何获得有关移动用户位置的信息。当一个移动电话切换或进入一个由新的 VLR 所覆盖的被访网络中以后，移动用户必须向被访网络注册，这是通过在移动用户和 VLR 之间交换信令报文来实现的。被访 VLR 随后又向移动用户的 HLR 发送一个位置更新请求报文。这一报文告知 HLR 可以用来联系移动用户的漫游号码，或者 VLR 地址（它可以用来随后查询以获取移动号码）。作为这个交换的一部分，VLR 同样从 HLR 那里获取移动用户的信息，以及确定被访网络应该给予移动用户什么样的服务。

6.7.2 GSM 中的切换

在一个呼叫过程中，移动站点将其关联从一个基站改变到另一个基站时出现切换（hand-off）。如图 6-30 所示，移动用户的呼叫初始时

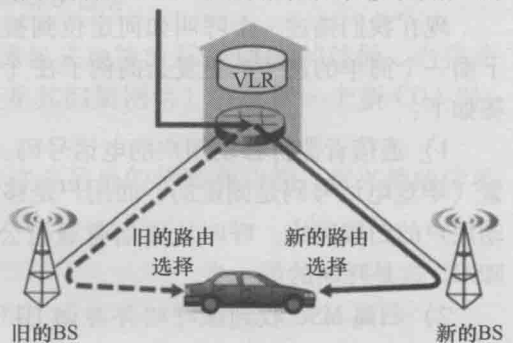


图 6-30 具有一个公共 MSC 的基站间的切换情况

(在切换前)通过一个基站(我们称其为旧基站)路由选择到该移动用户,而在切换以后它经过另一个基站(我们称其为新基站)路由选择到移动用户。注意到基站之间的切换不仅导致移动用户向/从一个新的基站传输/接收信号,而且导致正在进行的呼叫从网络中的一个交换点到新基站的重路由选择。我们首先假设新旧基站共享同一个 MSC,并且重路由选择发生在这个 MSC。

有几种原因导致切换的发生,包括:①当前基站和移动用户之间的信号减弱,使得该呼叫有被中断的危险;②一个蜂窝处理的呼叫太多,变得过载。可以通过将一些移动用户切换到邻近不太拥塞的蜂窝中,使这个拥塞得到缓解。

在与一个基站相关联期间,移动用户周期性地测量来自其当前基站和临近它的可以“听得到”的基站的信标信号强度。这些测量以每秒 1~2 次的频率报告给移动用户的当前基站。根据这些测量值、临近蜂窝的移动用户的当前负载以及其他因素,GSM 中的切换由旧的基站发起 [Mouly 1992]。GSM 标准并未明确规定基站在确定是否进行切换时所采用的具体算法。

图 6-31 显示了一个基站决定切换一个移动用户时所包括的步骤:

1) 旧基站 (BS) 通知被访问 MSC 即将要进行一个切换,通知移动用户将要切换到 (或可能的 BS 集)。

2) 被访问 MSC 发起建立到新 BS 的路径,分配承载重路由选择的呼叫所需的资源,以及用信令告知新 BS 一个切换即将出现。

3) 新 BS 分配并激活一个无线信道供移动用户使用。

4) 新 BS 发出信令返回被访问 MSC 和旧 BS,即已经建立了被访问 MSC 到新 BS 的路径并且移动用户应当被告知即将发生的切换。新 BS 提供移动用户与新的 BS 相关联所需要的所有信息。

5) 移动用户被告知它应当进行一个切换。注意到此时为止,移动用户完全不知网络已经为切换做好所有底层工作(如在新 BS 中分配一个信道,分配一条从被访问 MSC 到新 BS 的路径)。

6) 移动用户和新 BS 交换一个或多个报文,以完全激活新 BS 中新的信道。

7) 移动用户向新 BS 发送一个切换完成报文,该报文随后向上转发给被访问 MSC。该被访问 MSC 然后重路由选择到移动用户的正在进行的呼叫,使其经过新 BS。

8) 沿着到旧 BS 的路径分配的资源随后被释放。

通过考虑如下情况来总结我们对切换的讨论:当移动用户移动到一个不同于旧 BS 的、与不同的 MSC 关联的 BS 中时,并且当这种 MSC 之间的切换多次发生时,考虑这些情况下将发生什么。如图 6-32 所示,GSM 定义了锚 MSC (anchor MSC) 的概念。锚 MSC 是呼叫首次开始时移动用户所访问的 MSC,它因此在整个呼叫持续过程中保持不变。在整个呼叫持续期间,不论移动用户进行了多少次 MSC 间转换,呼叫总是从归属 MSC 路由选择到锚 MSC,然后再到移动用户当前所在的被访问 MSC。当移动用户从一个 MSC 覆盖区到达另一个 MSC 覆盖区后,正在进行的呼叫被重路由选择,从锚 MSC 到包含新基站的新被访问

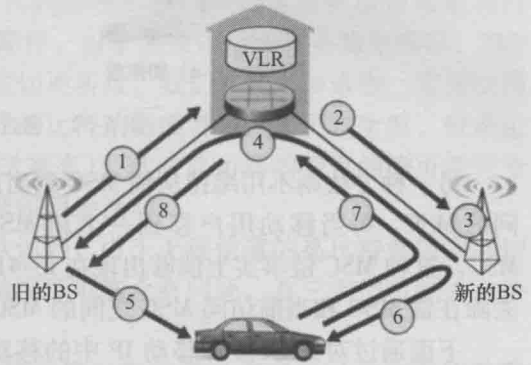


图 6-31 具有一个公共 MSC 的基站间完成一个切换的步骤

MSC。因此，在任何情况下，通信者和移动用户之间至多有 3 个 MSC（归属 MSC、锚 MSC 以及被访问 MSC）。图 6-32 图示了在移动用户所访问的 MSC 之间的一个呼叫的路由选择。

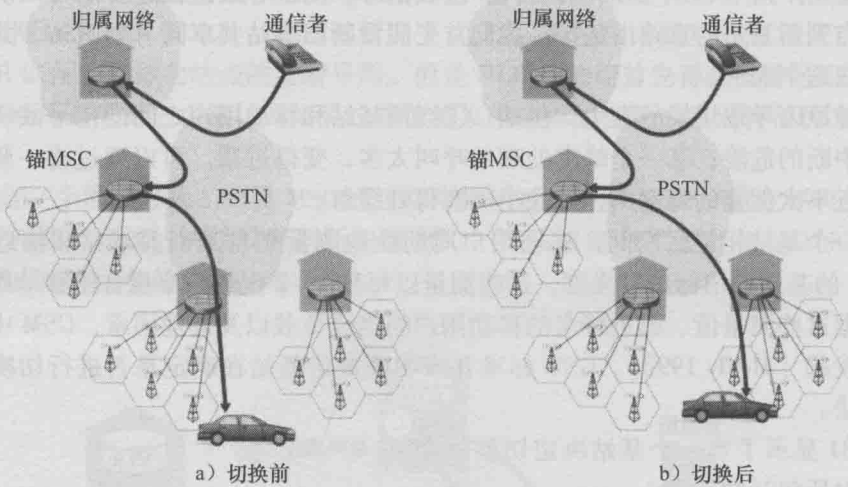


图 6-32 通过锚 MSC 重路由选择

另一种方法则不用维持从锚 MSC 到当前 MSC 的单一 MSC 跳，将直接链接移动用户访问的 MSC。每当移动用户移到一个新 MSC 后，让旧 MSC 将正在进行的呼叫转发给新 MSC。这种 MSC 链事实上能够出现在 IS-41 蜂窝网络中，通过使用最少步骤的可选路径来去除在锚 MSC 和当前访问 MSC 之间的 MSC [Lin 2001]。

下面通过对比 GSM 和移动 IP 中的移动性管理，来完成我们对 GSM 移动性管理的讨论。表 6-2 中的对比指出了尽管 IP 和蜂窝网络在很多方面有很大的区别，但它们共享数量惊人的公共功能要素和处理移动性的总体方法。

表 6-2 移动 IP 和 GSM 移动性之间的共性

GSM 要素	对 GSM 要素的解释	移动 IP 要素
归属系统	移动用户永久电话号码所归属的网络	归属网络
网关移动（服务）交换中心或简称归属 MSC，归属位置寄存器（HLR）	归属 MSC：获取移动用户路由地址的联系点。HLR：归属系统中包含移动用户永久电话号码、个人信息、当前位置和订购信息的数据库	归属代理
被访问系统	移动用户当前所在的非归属系统网络	被访网络
被访问移动（服务）交换中心或简称被访问 MSC，访问者定位记录（VLR）	被访问 MSC：负责建立与 MSC 相关联的发射区中到/从移动结点的呼叫。VLR：访问系统中的临时数据库项，包含每个访问移动用户的订购信息	外部代理
移动站点漫游号码（MSRN），或漫游号码	用于归属 MSC 和被访问 MSC 之间电话呼叫的路由地址，对移动用户和通信者均不可见	转交地址

6.8 无线和移动性：对高层协议的影响

在本章中，我们已经看到了无线网络在链路层（由于无线信道的诸如衰减、多径、隐终端等特性）和网络层（由于移动用户改变与网络的连接点）与有线网络的对应物有重

大的区别。但在运输层和应用层是否也有重大差别呢？我们很容易认为这些差别是很小的，因为在有线和无线网络中的网络层均为上层提供了同样的尽力而为服务模式。类似地，如果在有线和无线网络中都是使用诸如 TCP 和 UDP 的协议提供运输层服务，那么应用层也应该保持不变。在某个方面我们的直觉是对的，即 TCP 和 UDP 可以（也确实）运行在具有无线链路的网络中。在另一方面，运输层协议（特别是 TCP）通常在有线和无线网络中有时会有完全不同的性能。这里，在性能方面区别是明显的，我们来研究一下其中的原因。

前面讲过，在发送方和接收方之间的路径上，一个报文段不论是丢失还是出错，TCP 都将重传它。在移动用户情况下，丢失可能源于网络拥塞（路由器缓存溢出）或者切换（例如，由于重路由选择报文段到移动用户新的网络接入点引入的时延）。在所有情况下，TCP 的接收方到发送方的 ACK 都仅仅表明未能收到一个完整的报文段，发送方并不知道报文段是由于拥塞，或在切换过程中，还是由于检测到比特差错而被丢弃的。在所有情况下，发送方的反应都一样，即重传该报文段。TCP 的拥塞控制响应在所有场合也是相同的，即 TCP 减小其拥塞窗口，如 3.7 节讨论的那样。由于无条件地降低其拥塞窗口，TCP 隐含地假设报文段丢失是由于拥塞而非出错或者切换所致。我们在 6.2 节看到，在无线网络中比特错误比在有线网络中普遍得多。当这样的比特差错或者切换丢失发生时，没理由让 TCP 发送方降低其拥塞窗口（并因此降低发送速率）。此时路由器的缓存的确可能完全是空的，分组可以在端到端链路中丝毫不受拥塞阻碍地流动。

研究人员在 20 世纪 90 年代早期到中期就认识到，由于无线信道的高比特差错率和切换丢失的可能性，TCP 的拥塞控制反应在无线情况下可能会有问题。有三大类可能的方法用于处理这一问题：

- 本地恢复。本地恢复方法的目标是在比特差错出现的当时和当地（如在无线链路中）将其恢复。如在 6.3 节学习的 802.11 ARQ 协议，或者使用 ARQ 和 FEC 的更为复杂的方法 [Ayanoglu 1995]。
- TCP 发送方知晓无线链路。在本地恢复方法中，TCP 发送方完全不清楚其报文段跨越一段无线链路。另一种方法是让 TCP 发送方和接收方知道无线链路的存在，从而将在有线网络中发生的拥塞性丢包和在无线网络中发生的差错/丢包区分开，并且仅对有线网络中的拥塞性丢包采用拥塞控制。在假设端系统能够做出这种区分的情况下，[Balakrishnan 1997] 详细研究了多种类型的 TCP。[Liu 2003] 研究了在一个端到端路径中区分有线部分丢包和无线部分丢包的技术。
- 分离连接方法。在分离连接方法中 [Bakre 1995]，移动用户和其他端点之间的端到端连接被打断为两个运输层连接：一个从移动主机到无线接入点，一个从无线接入点到其他通信端点（我们假定它是有线的主机）。该端到端连接因此是由一个无线部分和一个有线部分级连形成的。经无线段的运输层能够是一个标准的 TCP 连接 [Bakre 1995]，或是一个特别定制运行在 UDP 上的差错恢复协议。[Yavatkar 1994] 研究了经无线连接使用运输层选择性重传协议。在 [Wei 2006] 中的测量报告指出了分离 TCP 连接广泛用于蜂窝数据网络中，通过使用分离 TCP 连接，上述问题的确能够有很大改进。

我们这里有关无线链路上的 TCP 的讨论是十分简要的。在无线网络中有关 TCP 挑战和解决方案的深入展望能够在 [Hanabali 2005; Leung 2006] 中找到。我们鼓励读者去查

阅这些文献以了解这个正在进行的研究领域的详情。

考虑过运输层协议后，我们接下来考虑无线和移动性对应用层协议的影响。这里一个重要的考虑是无线链路经常具有相对较低的带宽，如我们在图 6-2 中所见。因此，运行在无线链路尤其是蜂窝无线链路上的应用程序，必须将带宽作为稀有物品对待。例如，一个为在 3G 电话上运行的 Web 浏览器提供服务的 Web 服务器，就不能像为运行在有线连接的浏览器那样提供含有大量图片的内容。尽管无线链路的确为应用层提出一些挑战，它们具有的移动性同样使得一大批位置知晓和环境知晓应用成为可能 [Chen 2000; Baldauf 2007]。更一般地，无线和移动网络将在未来的泛在计算环境实现中起着重要作用 [Weiser 1991]。显然，在谈及无线和移动网络对网络应用及其协议的影响时，公平而论我们仅看到了冰山一角！

6.9 小结

无线网络和移动网络使电话发生了革命性变化，同时也对计算机网络界产生了日益深远的影响。伴随着它们对全球网络基础设施的随时、随地、无缝地接入，它们不仅使网络接入变得更加无所不在，而且催生了一组新的、令人兴奋的位置相关服务。考虑到无线网络和移动网络不断增长的重要性，本章关注用于支持无线和移动通信的原理、通用链路技术以及网络体系结构。

本章以对无线网络和移动网络的介绍开始，描述了由这种网络中通信链路的无线特性所引发的挑战和由这些无线链路带来的移动性之间的重要区别。这使我们能够更好地区分、识别和掌握每个领域中的关键概念。我们首先关注无线通信，在 6.2 节中考虑了无线链路的特征。在 6.3 节和 6.4 节中，我们研究了 IEEE 802.11 (WiFi) 无线 LAN 标准、两个 IEEE 802.15 个人区域网络 (蓝牙和 ZigBee)，以及 3G 和 4G 蜂窝因特网接入。然后将注意力转向移动性问题。在 6.5 节中我们区分了多种形式的移动性，不同的移动性面临不同的挑战，并且看到了不同的解决方案。我们考虑了移动结点的定位和路由选择问题，以及对那些动态地从一个网络接入点移到另一个网络接入点的移动用户的切换问题。在 6.6 节和 6.7 节中，我们分别考察了这些问题在移动 IP 标准和 GSM 中是如何处理的。最后，我们在 6.8 节中考虑了无线链路和移动性对运输层协议和网络应用的影响。

尽管我们用了整整一章来学习无线网络和移动网络，但全面探索这个令人兴奋和快速扩展的领域需要一整本书或更多书的篇幅。我们鼓励读者通过查阅在本章中提供的许多参考资料，对这一领域进行更深入的研究。

课后习题和问题



复习题

6.1 节

- R1. 一个无线网络运行在“基础设施模式”下是什么含义？如果某网络没有运行在基础设施模式下，那么它运行在什么模式下？这种运行模式与基础设施模式之间有什么不同？
- R2. 在 6.1 节的分类法中，所确定的四种无线网络类型各是什么？你已经使用的是这些无线网络类型中的哪一种？

6.2 节

- R3. 下列类型的无线信道损伤之间有什么区别：路径损耗、多径传播、来自其他源的干扰？
- R4. 随着移动结点离开基站越来越远，为了保证传送帧的丢失概率不增加，基站能够采取的两种措施是什么？

6.3~6.4 节

- R5. 描述 802.11 中信标帧的作用。
- R6. 是非判断：802.11 站在传输一个数据帧前，必须首先发送一个 RTS 帧并收到一个对应的 CTS 帧。
- R7. 为什么 802.11 中使用了确认，而有线以太网中却未使用？
- R8. 是非判断：以太网和 802.11 使用相同的帧格式。
- R9. 描述 RTS 门限值的工作过程。
- R10. 假设 IEEE 802.11 RTS 和 CTS 帧与标准的 DATA 和 ACK 帧一样长，使用 CTS 和 RTS 帧还会有好处吗？为什么？
- R11. 6.3.4 节讨论了 802.11 移动性，其中无线站点从一个 BSS 到同一子网中的另一个 BSS。当 AP 是通过交换机互连时，为了让交换机能适当地转发帧，一个 AP 可能需要发送一个带有哄骗的 MAC 地址的帧，为什么？
- R12. 在某蓝牙网络中的一个主设备和在 802.11 网络中的一个基站之间有什么不同？
- R13. 在 802.15.4 ZigBee 标准中超级帧的含义是什么？
- R14. 在 3G 蜂窝数据体系结构中，“核心网”的作用是什么？
- R15. 在 3G 蜂窝数据体系结构中，RNC 的作用是什么？在蜂窝语音网中 RNC 起什么作用？

6.5~6.6 节

- R16. 如果某结点与因特网具有无线连接，则该结点必定是移动的吗？试解释之。假设一个使用膝上型电脑的用户携带电脑绕着她的住所散步，并且总是通过相同的接入点接入因特网。从网络的角度看，这是移动用户吗？试解释之。
- R17. 永久地址与转交地址之间的区别是什么？谁指派转交地址？
- R18. 考虑经移动 IP 的一条 TCP 连接。是非判断：在通信者和移动主机之间的 TCP 连接阶段经过该移动用户的归属网络，但数据传输阶段直接通过该通信者和移动主机，绕开了归属网络。

6.7 节

- R19. 在 GSM 网络中，HLR 和 VLR 的目的是什么？移动 IP 的什么要素类似于 HLR 和 VLR？
- R20. 在 GSM 网络中，锚 MSC 的作用是什么？

6.8 节

- R21. 为了避免单一无线链路降低一条端到端运输层 TCP 连接的性能，能够采取的三种方法是什么？



习题

- P1. 考虑在图 6-5 中单一发送方的 CDMA 例子。如果发送方的 CDMA 码是 $(1, -1, 1, -1, 1, -1, 1, -1)$ ，那么其输出（对于所显示的两个数据比特）是什么？
- P2. 考虑图 6-6 中的发送方 2，发送方对信道 $Z_{i,m}^2$ 的输出是什么（在它被加到来自发送方 1 的信号前）？
- P3. 假设在图 6-6 中的接收方希望接收由发送方 2 发送的数据。说明通过使用发送方 2 的代码，（经计算）接收方的确能够将发送方 2 的数据从聚合信道信号中恢复出来。
- P4. 在两个发送方、两个接收方的场合，给出一个包括 1 和 -1 值的两个 CDMA 编码的例子，不允许两个接收方从两个 CDMA 发送方提取出初始传输的比特。
- P5. 假设有两个 ISP 在一个特定的咖啡馆内提供 WiFi 接入，并且每个 ISP 有其自己的 AP 和 IP 地址块。
- a. 进一步假设，两个 ISP 都意外地将其 AP 配置运行在信道 11。在这种情况下，802.11 协议是否将完全崩溃？讨论一下当两个各自与不同 ISP 相关联的站点试图同时传输时，将会发生什么情况。

- b. 现在假设一个 AP 运行在信道 1，而另一个运行在信道 11。你的答案将会有什么变化？
- P6. 在 CSMA/CA 协议的第 4 步，一个成功传输一个帧的站点在第 2 步（而非第 1 步）开始 CSMA/CA 协议。通过不让这样一个站点立即传输第 2 个帧（即使侦听到信道空闲），CSMA/CA 的设计者是基于怎样的基本原理来考虑的呢？
- P7. 假设一个 802.11b 站点被配置为始终使用 RTS/CTS 序列预约信道。假设该结点突然要发送 1000 字节的数据，并且所有其他站点此时都是空闲的。作为 SIFS 和 DIFS 的函数，并忽略传播时延，假设无比特差错，计算发送该帧和收到确认需要的时间。
- P8. 考虑在图 6-33 中显示的情形，其中有四个无线结点 A、B、C 和 D。这四个结点的无线电覆盖范围显示为其中的椭圆型阴影；所有结点共享相同的频率。当 A 传输时，仅有 B 能听到/接收到；当 B 传输时，A 和 C 能听到/接收到；当 C 传输时，B 和 D 能听到/接收到；当 D 传输时，仅有 C 能听到/接收到。

假定现在每个结点都有无限多的报文要向每个其他结点发送。如果一个报文的目的地不是近邻，则该报文必须要中继。例如，如果 A 要向 D 发送，来自 A 的报文必须首先发往 B，B 再将该报文发送给 C，C 则再将其发向 D。时间是分隙的，报文所用的传输时间正好是一个时隙，如在时隙 Aloha 中的情况一样。在一个时隙中，结点能够做下列工作之一：(i) 发送一个报文（如果它有报文向 D 转发）；(ii) 接收一个报文（如果正好一个报文要向它发送）；(iii) 保持静默。如同通常情况那样，如果一个结点听到了两个或更多的结点同时发送，出现冲突，并且重传的报文没有一个能成功收到。你这时能够假定没有比特级的差错，因此如果正好只有一个报文在发送，它将被位于发送方传输半径之内的站点正确收到。

- a. 现在假定一个无所不知的控制器（即一个知道在网络中每个结点状态的控制器）能够命令每个结点去做它（无所不知的控制器）希望做的事情，例如发送报文，接收报文，或保持静默。给定这种无所不知的控制器，数据报文能够从 C 到 A 传输的最大速率是什么，假定在任何其他源/目的地对之间没有其他报文？
- b. 现在假定 A 向 B 发送报文，并且 D 向 C 发送报文。数据报文能够从 A 到 B 且从 D 到 C 流动的组合最大速率是多少？
- c. 现在假定 A 向 B 发送报文且 C 向 D 发送报文。数据报文能够从 A 到 B 且从 C 到 D 流动的组合最大速率是多少？
- d. 现在假定无线链路由有线链路代替。在此情况下，重复问题 (a) ~ (c)。
- e. 现在假定我们又在无线状态下，对于从源到目的地的每个数据报文，目的地将向源回送一个 ACK 报文（例如，如同在 TCP 中）。对这种情况重复问题 (a) ~ (c)。

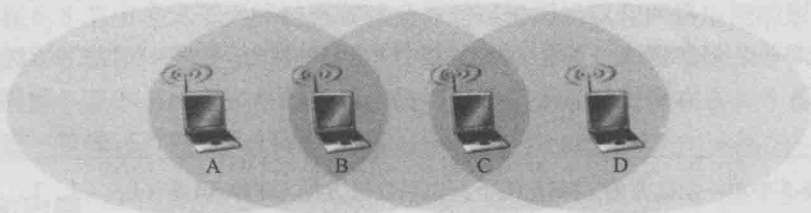


图 6-33 习题 P8 的情形

- P9. 描述 802.15.1 蓝牙帧的格式。你必须要阅读某些课外读物来获取这些信息。在帧格式中有哪些因素本质上会限制 802.15.1 网络中主动结点数量为 8 呢？试解释之。
- P10. 考虑下列理想化的 LTE 情形。下行信道（参见图 6-20）划分为时隙，使用了 F 个频率。有 4 个结点 A、B、C 和 D 分别以 10Mbps、5Mbps、2.5Mbps 和 1Mbps 速率在下行信道上可到达基站。这些速率假定基本在所有 F 个频率上能够利用所有时隙只向一个站点进行发送。基站具有无限量的数据向每个结点发送，并且在下行子帧中的任何时隙期间使用 F 个频率中的任何之一能够向这 4 个站点之一发送。

- a. 假定基站在每个时隙期间能够向它选择的任何结点发送, 它能向结点发送的最大速率是多少? 你的解决方案公平吗? 解释并定义你所指“公平”的含义。
- b. 如果有公平要求, 即每个站点在每秒期间必须收到等量的数据, 在下行子帧期间基站(向所有结点)的平均传输速率是多少?
- c. 假定该公平性准则是在子帧期间任何结点至多能够接收任何其他结点两倍多的数据。在下行子帧期间基站(向所有结点)的平均传输速率是多少? 解释你是如何得到答案的。
- P11. 在 6.5 节, 一种允许移动用户在外部网络间移动过程中保持其 IP 地址不变的建议方案是, 让外部网络通告一个到该移动用户高度特定的路由, 并使用现有的路由选择基础设施在整个网络中传播这一信息。我们将扩展性作为一种关注因素。假设移动用户从一个网络移动到另一个网络后, 新的外部网络通告一个到移动用户的特定路由, 旧的外部网络丢弃其路由。考虑路由信息如何在一个距离向量算法中传播(尤其是对于跨越全球的网络间的域间路由选择情况)。
- a. 一旦外部网络开始通告其路由, 其他路由器能否立刻将数据报路由选择到新的外部网络呢?
- b. 不同的路由器有可能认为移动用户位于不同的外部网络中吗?
- c. 讨论网络中其他路由器最终知道到达移动用户的路径所用的时间范围。
- P12. 假设图 6-22 中通信者是移动的。概述为了将数据报从初始移动用户路由选择到(现在移动的)通信者所需要的额外的网络层基础设施。如图 6-23 中那样, 显示在初始移动用户和(现在移动的)通信者之间数据报的结构。
- P13. 在移动 IP 中, 移动性将对数据报在源和目的地间的端到端时延有怎样的影响?
- P14. 考虑 6.7.2 节最后讨论的链的例子。假设一个移动用户访问外部网络 A、B 和 C, 当通信者在外部网络 A 中时, 它开始一条与移动用户的连接。列出在外部代理之间和外部代理与归属代理之间, 当移动用户从网络 A 到网络 B 再到网络 C 的过程中的报文序列。然后, 假设未执行链接, 并且通信者(以及归属代理)必须被显式地告知移动用户转交地址的改变。列出在第二种情况下需要交换的报文序列。
- P15. 考虑在一个具有外部代理的外部网络中的两个移动结点。在移动 IP 中, 这两个移动结点是否可能使用相同的转交地址? 解释你的答案。
- P16. 在我们对 VLR 如何用移动用户当前位置信息更新 HLR 的讨论中, 与 VLR 地址对 HLR 相比, 提供 MSRN 所具有的优缺点各是什么?



Wireshark 实验

在本书的配套 Web 站点上 (<http://www.awl.com/kurose-ross>), 你将会找到有关本章的一个 Wireshark 实验, 该实验用于捕获和学习在无线便携机和接入点之间交换的 802.11 帧。

人物专访

Deborah Estrin 是加州大学洛杉矶分校的计算机科学教授, 计算机网络的 Jon Postel 主席, 嵌入式网络感知中心 (CENS) 的主任以及非营利组织 openmhealth.org 的联合奠基人。她从 MIT 获得了计算机科学博士学位 (1985 年), 从加州大学伯克利分校获得硕士学位 (1980 年)。Estrin 的早期研究集中在包括多播和域间路由选择等在内的网络协议的设计。在 2002 年, Estrin 创建了美国国家自然科学基金资助的科学技术中心 CENS (<http://cens.ucla.edu>), 以研发和探索环境监视技术和应用。当前 Estrin 及其同事正在研发供人分享感知 (participatory sensing) 系统, 促进移动电话的可编程能力、邻近性和泛在性的发展; 基本部署环境是移动健康 (<http://openmhealth.org>)、社区数据收集和 STEM 教育 (<http://mobilizingcs.org>)。Estrin 教授是美国艺术和科学研究院



Deborah Estrin

(2007年)和国家工程院(2009年)的当选成员。她是IEEE、ACM和AAAS的会士。她被选为首名ACM-W雅典娜讲师(2006年),获得Anita Borg学院的妇女远见创新奖(2007年),被引入WITI名人纪念馆(2008年)和获得来自EPFL(2008年)和Uppsala大学(2011年)的Honoris Causa博士。

- 请描述在您的职业生涯中从事的几件最为令人兴奋的项目?

20世纪90年代中期当我在USC和ISI的时候,非常荣幸地与像Steve Deering、Mark Handley和Van Jacobson这样的人物在一起工作,设计多播路由选择协议(特别是PIM)。我试图将多播体系结构设计中的许多经验教训借鉴到生态监视阵列中,这是我首次真正开始全身心地应用和多学科的研究。那让我对社会和技术领域中的创新感兴趣,它们激发我对近期的研究领域——移动健康的研究兴趣。这些项目中的挑战随问题领域不同而不同,但它们的共同之处是需要睁大我们的眼睛,当我们在设计、部署、制作原型和试用之间重复时关注对问题的定义是否正确。没有一个问题能够借助于模拟或者构造的实验室实验加以分析解决。面对凌乱的问题和环境要保持清晰的体系结构,它们都对我们的能力提出挑战,并且它们都需要广泛的协作。

- 未来在无线网络和移动性方面您预见将会发生什么变化和创新?

我从来对预测未来不具太多信心,但是随着智能手机变得越来越强大和因特网基本接入点增多,我预言我们可能看到特色电话(即那些不可编程和仅能用于语音和文本信息的电话)的终结。我还认为我们将看到嵌入式SIM的继续迅速增长,各种设备通过嵌入式SIM具有经过蜂窝网络以低数据率通信的能力。

- 您预见网络和因特网的未来向何处发展?

在命名数据和软件定义网络方面的努力将出现成果,产生更可管理、可演化和更丰富的基础设施,以及更一般地表现为推动体系结构的责任向协议栈较高层发展。在因特网开始时,体系结构包括第四层及以下,位于顶端的应用程序更为竖井式/独块式的。现在则是数据和分析支配着传输。

- 什么人对于您的职业生涯给予了激励?

有三个人出现在我的脑海中。第一个人是Dave Clark,他是因特网界的秘方和无名英雄。早期我有幸在他的左右,看到他在IAB的“组织规范”和因特网管理方法方面所起的作用,即大致共识和运行编码的引导者。第二个人是Scott Shenker,他的智慧才华、正直和坚持令我印象深刻。我努力但很难像他那样清晰地定义问题和给出解决方案。无论问题大和小,我发电子邮件征求建议,他总是第一个回复的人。第三个人是我的姐姐Judy Estrin,她将创造性和勇气投入到她的职业,将想法和概念带入市场。没有Judy这类人,因特网技术将不会改变我们的生活。

- 对于希望从事计算机科学和网络职业的学生,您有什么推荐?

首先,在你的学术工作中构建一个坚实的基础,与你能够得到的任何、每个现实世界的工作经验相权衡。当你寻找一个工作环境时,在你真正关心的问题领域寻找机会,并且参与到你能够从中学到的思维敏捷的团队中。

多媒体网络

位于世界各个角落的人们当前正使用因特网来按需观看电影和电视节目。因特网电影和电视分发公司（如北美的 Netflix 和 Hulu、中国的“优酷”（Youku）和“看看”（Kankan））实际上已经成为家喻户晓的名称。而人们不仅观看因特网视频，他们也使用诸如 YouTube 这样的站点来上传和分发用户自己生成的内容，不仅成为因特网视频的消费者，也成为视频的生产者。此外，网络应用如 Skype、Google Talk 和 QQ（在中国十分流行），不仅允许人们经过因特网打“电话”，而且可以用视频和多方会议来强化该电话。事实上，我们能够确定地预测：到当前年代末，几乎所有的视频分发和语音会话都将在因特网的端到端发生，通常出现在经 4G 和 WiFi 接入网与因特网连接的无线终端上。

本章以 7.1 节中的多媒体应用的分类方法开始。我们将看到多媒体应用能够分为流式存储音频/视频、会话式 IP 音频/视频或流式实况音频/视频等几类。我们将看到这些应用类型中的每一类都有自己独特的服务需求，这些需求与传统的弹性应用如电子邮件、Web 浏览和远程注册的需求差异很大。在 7.2 节中，我们较为详细地研究流式视频。我们将探讨支撑流式视频的许多基础原则，包括客户缓存、预取和对可用带宽的适应性视频质量。我们也将研究内容分发网（Content Distribution Network, CDN），CDN 是今天广泛使用的最有影响的流式视频系统。在 7.3 节中，我们研究会话式语音和视频。它们不同于弹性应用，对端到端时延高度敏感，但能够容忍偶尔的数据丢失。此时我们将研究诸如适应性播放、前向纠错和差错掩盖等技术是如何减缓网络引入的丢包和时延的。我们还将考察 Skype 作为学习案例。在 7.4 节中，我们将学习 RTP 和 SIP，这是两个用于实时会话式语音和视频应用的协议。在 7.5 节中，我们将研究网络内部的一些机制，这些机制能用于区分一类流量（如会话式语音这样的时延敏感应用）和其他类型流量（如浏览 Web 网页这样的弹性应用），并且在多类流量中提供区分服务。

7.1 多媒体网络应用

我们将多媒体网络应用定义为任何应用音频或视频的网络应用。本小节中，我们将提供多媒体应用的分类法。我们将看到在该分类法中的每类应用都具有自己独特的服务要求和设计问题集合。但在深入讨论因特网多媒体应用前，考虑音频和视频媒体自身的内在特点是有用的。

7.1.1 视频的性质

视频最为显著的特点或许是它的高比特率（high bit rate）。经因特网分发的视频的典型传输速率从用于低质量视频会议的 100kbps 到用于流式高分辨率电影的 3Mbps。为了比较视频带宽需求与其他因特网应用的带宽需求的不同，我们简要地考虑三个不同的用户，他们每人使用了一种不同的因特网应用。第一位用户 Frank，他打算迅速将照片张贴到他的朋友的脸谱（Facebook）页面上。我们假设 Frank 每 10 秒钟查找一次新照片，并且这些

照片的平均大小是 200KB。(与以前一样,我们在整个讨论中都简单地假定 1KB = 8000 比特。)第二位用户 Martha 正从因特网(“云中”)向她的智能手机流式传输音乐。我们假定 Martha 正在听许多 MP3 歌曲,一首接着一首,都以 128kbps 速率进行编码。第三位用户 Victor 则正在观看以 2Mbps 编码的视频。最后,我们假设所有三位用户的会话长度是 4000 秒(大约 67 分钟)。表 7-1 比较了这三位用户的比特率和传输的总字节。我们看到这时流式视频消耗了最多的带宽,其比特率比脸谱和流式音乐应用的带宽大 10 倍。因此,当设计网络视频应用时,我们心中必须记住的第一件事是视频的高比特率需求。鉴于视频的流行性及其高比特率,也许不会对思科公司以下的预测感到惊讶 [Cisco 2011]:到了 2015 年,流式视频和存储视频将大约占全球因特网流量消费的 90%。

表 7-1 三种因特网应用的比特率需求的比较

	比特率	67 分钟传输的字节
Frank 脸谱	160kbps	80MB
Martha 音乐	128kbps	64MB
Victor 视频	2Mbps	1GB

视频的另一种重要特点是它被压缩,因而要在视频质量与比特率间进行折中。视频是一个图像序列,图像通常以恒定的速率显示,例如每秒 24 幅或 30 幅图像。一个没有压缩、数字编码的图像由像素阵列组成,每个像素被编码为一定数量的比特来表示亮度和颜色。在视频中有两种类型的冗余,它们都可以用来进行视频压缩(video compression)。空间冗余是给定图像的内部冗余。从直觉上讲,一个主要由空白组成的图像具有高度的冗余,能够有效地压缩而不会明显降低图像质量。时域冗余反映一幅图像和后续图像的重复程度。例如,如果一幅图像和后续图像完全一致,没有理由对后续图像再进行编码;相反,在编码过程中直接指出后续图像是完全一样的则更为有效。今天商用的压缩算法能够将视频压缩为所希望的任何基本比特率。当然,比特率越高,图像质量越好,总体用户视觉体验也越好。

我们也能够使用压缩来生成相同视频的多重版本(multiple version),每个版本有不同的质量等级。例如,我们能够使用压缩生成相同视频的三个版本,速率分别为 300kbps、1Mbps 和 3Mbps。用户则能够根据他们的当前可用带宽来决定要观看哪个版本。具有高速因特网连接的用户可以选择 3Mbps 的版本;使用 3G 智能手机观看视频的用户可以选择 300kbps 的版本。类似地,在视频会议应用中的视频能被“动态”(on-the-fly)地压缩,以在会话用户之间给定的可用端到端带宽上提供最好的视频质量。

7.1.2 音频的性质

数字音频(包括数字化语音和音乐)的带宽需求比视频低得多。然而,数字音频具有自己独特的性质,当设计多媒体应用时必须考虑这些性质。为了理解这些性质,我们首先考虑模拟音频(由人和乐器所产生)是如何转换为数字信号的:

- 模拟音频信号首先以某种固定速率采样,例如每秒 8000 个样本。每个采样值是一个任意的实数。
- 然后每个采样值被“四舍五入”为有限个数值中的一个。这种操作被称为量化(quantization)。这些有限个数值(称为量化值)通常是 2 的幂,例如 256 个量化值。
- 每个量化值由固定数量的比特表示。例如,如果有 256 个量化值,那么每个值(因此每个音频采样)用一个字节来表示。所有样本的比特表示级联在一起就形成了该信号的数字表示。举例来说,如果一个模拟信号以每秒 8000 个样值采样,而且每个样本被量化并用 8 比特表示,则得到的数字信号的速率就为每秒 64 000 比

特。通过音频扬声器播放，这个数字信号则能够转换回来（也就是解码），形成一个模拟信号。然而，解码后的模拟信号仅是初始信号的近似，并且声音质量也许有明显的下降（例如，高频的声音可能在解码信号中丢失了）。通过增加采样速率和量化值的数量，解码信号能够更好地接近初始的模拟信号。因此（与视频一样），在解码信号的质量和比特率与数字信号存储空间之间存在一种折中。

我们刚才描述的基本编码技术称为脉冲编码调制（Pulse Code Modulation, PCM）。语音编码通常采用 PCM，采样速率为每秒 8000 个样本，每个样本用 8 比特表示，得到 64kbps 的速率。音频光盘（CD）也使用 PCM，采样速率为每秒 44 100 个样本，每个样本用 16 比特表示；这样使得单声道速率为 705.6kbps，立体声速率为 1.411Mbps。

然而，PCM 编码的语音和音乐很少在因特网中使用。与视频一样，取而代之的是使用压缩技术来减小流的比特速率。人类语音能被压缩到小于 10kbps 并仍然可懂。一种接近 CD 质量立体声音乐的流行压缩技术是 MPEG 1 第 3 层，更通常的叫法是 MP3。MP3 编码器通常能够压缩为许多不同的速率；128kbps 是最常用的编码速率，并且能够产生非常小的声音失真。一种相关的标准是高级音频编码（Advanced Audio Coding, AAC），该标准已经随苹果公司而流行起来。与视频一样，能够以不同的比特率生成多重版本的预先录制的音频流。

尽管音频比特率通常比视频的比特率小得多，但用户通常对音频的小失误比视频的小失误更为敏感。例如，考虑在因特网上举行的视频会议。如果视频信号时不时地丢失几秒，该视频会议很可能继续进行而没有太多的用户抱怨。然而，如果音频信号经常丢失，用户就可能不得不中止该会话。

7.1.3 多媒体网络应用的类型

因特网能够支持各种各样有用的和娱乐性的多媒体应用。在本小节中，我们将多媒体应用分为三个大类：①流式存储音频/视频；②会话式 IP 语音/视频；③流式实况音频/视频。如我们很快将看到的那样，这些应用类型中的每种都有自己的服务需求和设计问题的集合。

1. 流式存储音频和视频

为使讨论具体化，我们这里聚焦流式存储视频，它通常结合了视频和音频组件。流式存储音频（例如流式音乐）非常类似于流式存储视频，尽管它的比特率通常要低得多。

在这类应用中，依赖的媒体是预先录制的视频（如电影、电视节目）预先录制的体育赛事或预先录制的用户生成的视频（如常在 YouTube 上看到的那些）。这些预先录制的视频放置在服务器上，用户向服务器发送请求按需观看视频。许多因特网公司今天提供流式视频，包括 YouTube（谷歌）、Netflix 和 Hulu。据估计，在今天的因特网接入网中流式存储视频构成了超过 50% 的下载流量 [Cisco 2011]。流式存储视频具有三个关键的不同特色。

- 流。在流式存储视频应用中，客户开始从服务器接收文件几秒之后，通常就开始播放视频。这意味着当客户正在从视频的一个位置开始播放时，与此同时正在从服务器接收该视频的后续部分。这种技术被称为流（streaming），它避免了在开始播放之前必须下载整个视频（并且引起一个潜在的长时延）。
- 相互作用。因为媒体是预先录制的，用户可以对多媒体内容进行暂停、重新配置前进、重新配置倒退、快进等操作。从一个客户提出这种请求到该动作在客户端表现出来，可接受的响应时间应该小于几秒。

- 连续播放。一旦视频开始播放，它应该根据初始记录的时序进行。因此，为了在客户端播放，必须从服务器中及时接收数据；否则，用户经历视频帧停滞（这时客户等待延迟的帧）或帧跳过（这时客户漏掉延迟的帧）。

到目前为止，对流式视频最重要的性能测量是平均吞吐量。为了提供连续的播放，网络为流式应用提供的平均吞吐量必须至少与该流视频本身的比特率一样大。如我们将在7.2节所见，通过使用缓存和预取，即使在吞吐量波动的时候，提供连续播放也是可能的，只要平均吞吐量（在5~10秒区间平均）保持在视频速率之上 [Wang 2008]。

对于许多流式视频应用，预先录制的视频被存储起来，并且从CDN而非从单一的数据中心流式播放。也有许多P2P视频流式应用，其中视频被存储在用户主机（对等方）上，不同视频块从可能分布在全球的不同对等方到达。在得知了因特网流式视频的性能后，我们将在7.2节更加深入地研究流式视频，特别关注客户缓存、预取、对可用带宽的适应性质量和CDN分发。

2. 会话式IP语音和视频

在因特网上的实时会话式语音通常称为**因特网电话** (Internet telephony)，因为从用户的角度看，它类似于传统的电路交换电话服务。它也常被称为**IP语音** (Voice-over-IP, VoIP)。会话式视频与之类似，除了它包括参与者的语音以及视频外。今天的大多数语音和视频会话式系统允许用户生成具有三个或更多个参与者的会议。会话式语音和视频广泛地应用于今天的因特网中，因特网公司Skype、QQ和Google Talk自称每天都有数亿用户。

在第2章有关应用服务需求的讨论中（图2-4），我们确定了一些轴，服务需求可以根据它们分类。其中的两个轴（即定时考虑和数据丢失容忍度）对会话式语音和视频应用尤其重要。定时考虑是很重要的，因为音频和视频会话式应用是高度**时延敏感** (delay-sensitive) 的。对于具有两个或更多个交互讲话者的会话来说，从用户讲话或移动开始到该动作显现在其他端的时延应当小于几百毫秒。对于语音，小于150ms的时延不会被人类听者觉察到，150~400ms的时延能够被接受，当时延超过400ms时，即使不会使对话变得完全无法理解，也会使语音会话变得令人沮丧。

另一个方面，会话式多媒体应用**容忍丢包** (loss-tolerant)，即偶尔的丢失只会在音频/视频回放时偶尔出现干扰信号，而且这些丢失经常可以部分或者全部地隐藏。这些时延敏感但容忍丢包的特性明显不同于那些弹性数据应用（如Web浏览、电子邮件、社交网络和远程注册等）的特性。对于这些弹性应用，长时延令人恼火，但并不是特别有害，然而传输数据的完全和完整性是首要的。我们将在7.3节中更加深入地探讨会话式语音和视频，特别关注适应性播放、前向纠错和差错掩盖是如何减缓网络引入的分组丢失和时延的。

3. 流式实况音频和视频

这种第三类应用类似于传统的电台广播和电视，只是它通过因特网来传输而已。这些应用允许用户接收从世界上任何角落发出的实况无线电广播和电视传输。今天有数以千计、遍及全球的无线电台和电视台正在因特网上广播内容。

实况是类似于广播的应用，它们经常有很多接收相同音频/视频节目的客户。尽管通过使用4.7节中描述的IP多播技术，能够有效地完成向多个接收方分发实况音频/视频，但是多播分发今天更多的是通过应用层多播（使用P2P网络或CDN）或通过多个独立的单播流来实现。由于使用流式存储多媒体，网络必须为每个实况多媒体流提供大于该视频

消耗速率的平均吞吐量。因为事件是直播的，尽管定时限制没有会话式语音那么严格，但时延也可能成为问题。从用户选择观看一个实况传输到播放开始，能够容忍的时延最多为 10 秒。我们在本书中将不涉及流式实况媒体，因为用于流式实况媒体的许多技术（如初始缓存时延、适应性带宽使用和 CDN 分发）都类似于流式存储媒体所使用的技术。

7.2 流式存储视频

对于流式视频应用，预先录制的视频放置在服务器上，用户向这些服务器发送请求按需观看这些视频。用户可能从开始到结束都在观看视频而没有中断它，也可能在视频结束前停止观看它，或者通过暂停、重新定位到后面或前面镜头来与视频交互。流式视频系统可分为三种类型：UDP 流（UDP streaming）、HTTP 流（HTTP streaming）和适应性 HTTP 流（adaptive HTTP streaming）。尽管在实践中所有这三种系统都在使用，但绝大多数今天的系统应用了 HTTP 流和适应性 HTTP 流。

所有这三种形式的视频流的共同特点是广泛使用了客户端应用缓存，以此来缓解变化的端到端时延和变化的服务器和客户之间可用带宽量的影响。对于流式视频（存储的和实况的），用户通常能够容忍在客户请求某视频与该流视频在客户端播放之间有几秒钟的初始小时延。所以，当视频开始到达客户时，客户不必立即开始播放，反而能够在应用程序缓存中建立该视频的储备。一旦该客户建立起几秒钟的“已缓存但尚未播放”的视频储备，客户就可以开始视频播放了。这种客户缓存（client buffering）具有两种重要的优点。第一，客户端缓存能够吸收服务器到客户时延中的波动。如果某特殊部分的视频数据延迟了，只要它在“接收到但尚未播放”的视频耗尽之前到达，这个长时延将不会被注意到。第二，如果服务器到客户带宽暂时低于视频消耗速率，用户能够继续享受连续的播放，只要客户应用缓存仍没有完全排尽。

图 7-1 显示了客户端的缓存。在这个例子中，假定视频以固定的比特率编码，因此每个视频块包含了能在相同固定时间量 Δ 区间播放的视频帧。服务器在 t_0 传输第一个视频块，在 $t_0 + \Delta$ 传输第二个视频块，在 $t_0 + 2\Delta$ 传输第三个视频块等等。一旦客户开始播放，为了重新产生初始录制视频的定时，每个块应当在前一个块之后播放 Δ 时间单元。第一个视频块于 t_1 时刻到达，第二个视频块于 t_2 时刻到达。第 i 块的网络时延是服务器传输该块

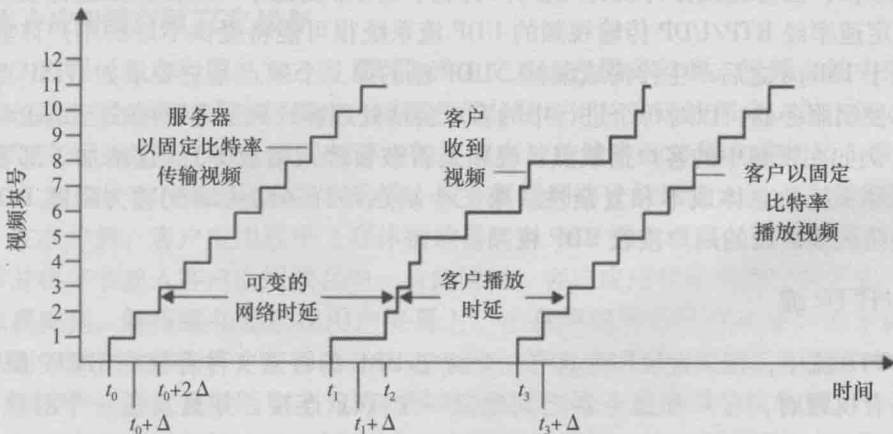


图 7-1 视频流中的客户播放时延

的时间与客户收到该块的时间之间的水平距离；注意到网络时延随视频块不同而变化。在此例子中，如果客户准备当第一块在 t_1 时刻一到达就开始播放，那么第二块将不能在 $t_1 + \Delta$ 时刻及时到达进行播放。在这种情况下，视频播放或将停止运行（等待第二块的到达）或可能漏掉第二块，即这两种情况都将导致不希望的播放损伤。相反，如果客户将播放延迟到 t_3 时刻开始，这时第一块到第六块都已经到达，所有已经收到的块在它们的播放时间前都能够进行周期性的播放。

7.2.1 UDP 流

我们这里仅简要讨论 UDP 流，在适当时候向读者更为深入地介绍这些系统背后隐含的协议。使用 UDP 流，服务器通过 UDP 以一种稳定的速率记录下视频块，用与客户的视频消耗速率相匹配的速率传输视频。例如，如果视频消耗率是 2Mbps，每个 UDP 分组承载 8000 比特视频，则服务器将每隔 $(8000 \text{ 比特}) / (2 \text{ Mbps}) = 4 \text{ ms}$ 向其套接字发送一个 UDP 分组。如我们在第 3 章所知，因为 UDP 未采用某种拥塞控制机制，所以服务器能够以视频的消耗速率将分组推进网络中，而无 TCP 的速率控制的限制。UDP 流通常使用很小的客户端缓存，空间维持小于 1 秒视频就足够了。

在将视频块传递给 UDP 之前，服务器将视频块封装在运输分组中，该运输分组是专门为传输音频和视频而设计的，使用了实时传输协议（Real-Time Transport Protocol, RTP）[RFC 3550] 或某种类似（可能是专用）的方案。我们将在 7.3 节再讨论 RTP，那时我们将在会话式语音和视频系统环境中讨论 RTP。

UDP 流的另一种不同的性质是，除了服务器到客户的视频流外，两者间还并行地维护一个单独的控制连接，通过该连接，客户可发送有关会话状态变化的命令（如暂停、重新开始、重定位等）。这种控制连接在许多方面类似于我们在第 2 章中学习的 FTP 控制连接。在本书配套 Web 网站上更为详细地解释了实时流协议（Real-Time Streaming Protocol, RTSP）[RFC 2326]，它是一种用于这样的控制连接的流行开放协议。

尽管 UDP 流已经在多个开源系统和专用产品中得到应用，但它有三个重大不足。首先，由于服务器和控制之间的可用带宽无法预测并且是变化的，恒定速率 UDP 流不能够提供连续的播放。例如考虑以下场景：视频消耗速率为 1Mbps，服务器到客户可用带宽通常超过 1Mbps，但每过几分钟就有几秒钟时间其可用带宽低于 1Mbps。在这种场景下，以 1Mbps 恒定速率经 RTP/UDP 传输视频的 UDP 流系统很可能将提供不好的用户体验，在可用带宽低于 1Mbps 之后产生停滞或漏帧。UDP 流的第二个缺点是它要求如 RTSP 服务器这样的媒体控制服务器，以对每个进行中的客户会话处理客户到服务器的交互请求和跟踪客户状态（例如在视频中的客户播放点，视频是否被暂停或播放等）。这增加了部署大规模的按需视频系统的总体成本和复杂性。第三个缺点是许多防火墙配置为阻塞 UDP 流量，防止这些防火墙后面的用户接收 UDP 视频。

7.2.2 HTTP 流

在 HTTP 流中，视频直接作为具有一个特定 URL 的普通文件存储在 HTTP 服务器上。当用户要看视频时，客户和服务器之间建立一个 TCP 连接，并且发送一个对该 URL 的 HTTP GET 请求。服务器则尽可能快地在 HTTP 响应报文中发送该视频文件，这就是说，以 TCP 拥塞控制和流控制允许的尽可能快的速率进行处理。在客户端上，字节收集在一个

客户应用缓存中。一旦在缓存中字节数量超过了预先设定的阈值，该客户应用程序开始播放，具体而言，它周期性地从客户应用缓存中抓取视频帧，对帧解压缩并在用户屏幕上显示它们。

我们在第3章学习过，当通过 TCP 传输一个文件时，由于 TCP 的拥塞控制机制，服务器到客户的传输速率可能变化很大。特别是，传输速率以与 TCP 拥塞控制相关联的“锯齿”形（例如，图 3-53）变化并非罕见。此外，分组也能由于重传机制而被大大延迟。因为 TCP 的这些特点，在 20 世纪 90 年代大多数人关于会话式的看法是流式视频将不可能在 TCP 上很好地工作。然而，随着时间的推移，流式视频系统的设计者知道了当使用了客户缓存和预取（在下面讨论）技术时，TCP 的拥塞控制和可靠数据传输机制并不一定会妨碍连续播放。

在 TCP 上使用 HTTP 也使得视频穿越防火墙和 NAT（它们常常被配置为阻挡 UDP 流量但允许大部分 HTTP 流量通过）更为容易。HTTP 流消除了因需要媒体控制服务器（如 RTSP 服务器）带来的不便，减少了在因特网上大规模部署的成本。由于所有这些优点，今天的大多数流式视频应用（包括 YouTube 和 Netflix）都使用 HTTP 流（在 TCP 上）作为它的底层流式协议。

1. 预取视频

我们刚才学习了客户端缓存可用于缓解变化的端到端时延和变化的可用带宽的影响。在前面图 7-1 的例子中，服务器以视频播放的速率传输。然而，对于流式存储视频，客户能够尝试以高于消耗速率的速率下载视频，因此预取（prefetching）将来会被消耗的视频帧。该预取的视频当然存储在客户应用缓存中。这样的预取自然伴随 TCP 流出现，因为 TCP 拥塞避免机制将试图使用服务器和客户之间的所有可用带宽。

为了深入洞察预取技术，我们来举个简单的例子。假设视频消耗速率是 1Mbps，而网络从服务器到客户能够以恒定的 1.5Mbps 速率交付视频。客户则不仅能够以非常小的播放时延播放该视频，而且还能够以每秒 500Kb 的量增加缓存的视频数据。以这种方式，如果后来该客户在一段短暂时间内以小于 1Mbps 的速率接收数据，该客户由于在其缓存中的储备将能够继续提供连续的播放。[Wang 2008] 显示了当平均 TCP 吞吐量大致为媒体比速率的两倍时，TCP 流导致最小的饥饿和低缓存时延。

2. 客户应用缓存和 TCP 缓存

图 7-2 说明了客户和服务器之间 HTTP 流的交互。在服务器侧，视频文件中的白色部分已经通过服务器的套接字进行发送，而黑色部分是留下待发送的部分。在“通过套接字的门传送”之后，放置在 TCP 发送缓存中的字节在被传输进因特网之前如第 3 章所描述。在图 7-2 中，因为 TCP 发送缓存显示为满，服务器瞬间防止从视频文件发送更多的字节到套接字。在客户侧，客户应用程序（媒体播放器）从 TCP 接收缓存（通过其客户套接字）读出字节并将字节放入客户应用缓存中。与此同时，客户应用程序周期性地从客户应用缓存中抓取视频帧，解压缩并显示在用户屏幕上。注意到如果客户应用缓存大于该视频文件，则从服务器存储器到客户应用缓存移动字节的整个过程等价于普通文件经 HTTP 的下载过程，即客户直接将视频用 TCP 允许的尽可能快的速率从服务器中拉出来。

现在考虑在流播放期间当用户暂停视频时将发生的现象。在暂停期间，比特未从客户应用缓存中删除，甚至比特继续从服务器进入缓存。如果客户应用缓存是有限的，它可能

最终会变满，这将反过来引起对服务器的“反向压力”。具体而言，一旦客户应用缓存变满，字节不再从客户 TCP 接收缓存中删除，因此它也会变满。一旦客户 TCP 接收缓存变满，字节不再从服务器 TCP 发送缓存删除，因此它也变满。一旦客户 TCP 发送缓存变满，服务器不能向套接字中发送任何更多的字节。因此，如果用户暂停视频，服务器可能被迫停止传输，在这种情况下服务器被阻塞，直到用户恢复该视频。

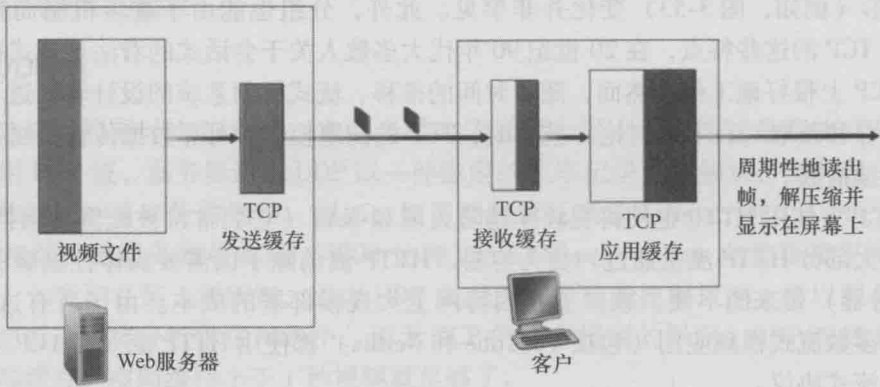


图 7-2 经 HTTP/TCP 的流式存储视频

事实上，甚至在常规的播放过程中（即没有暂停），如果客户应用缓存变满，反向压力将引起 TCP 缓存变满，这将迫使服务器降低其速率。为了决定其产生的速率，注意到当客户缓存删除 f 比特，它在客户应用缓存中产生了 f 比特的空间，这依次允许服务器发送额外的 f 比特。因此，服务器发送速率不能比客户端视频消耗速率更高。因此，当使用 HTTP 流时，一个满的客户应用缓存间接地对服务器到客户能够发送的视频速率施加了限制。

3. 流式视频的分析

某些简单的建模将有助于洞察由于应用缓存消耗所产生的初始播放时延和停滞。如图 7-3 所示， B 表示客户应用缓存的长度（以比特计）， Q 表示在客户应用缓存开始播放之前必须被缓存的比特数量。（当然， $Q < B$ 。） r 表示视频消耗速率，即客户在播放期间从客户应用缓存提取比特的速率。在此情况下，举例来说，如果视频的帧速率是 30 帧/秒，每（压缩）帧是 100 000 比特，则 $r = 3\text{Mbps}$ 。为了从细节看整体，我们将忽略 TCP 的发送和接收缓存。

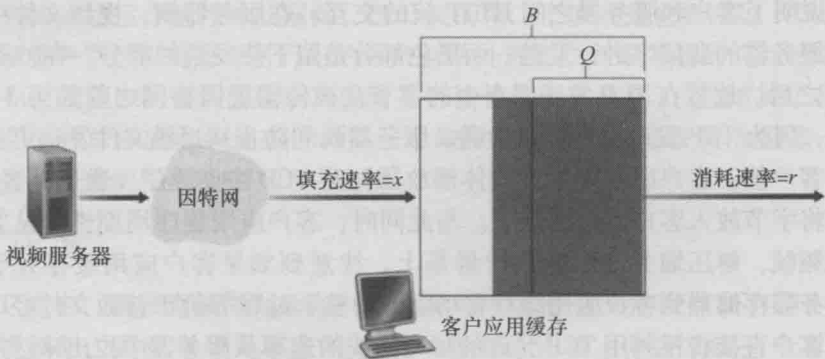


图 7-3 用户流式视频的客户端缓存的分析

我们假设无论何时客户缓存为非空时，服务器以一种恒定速率 x 发送比特。（这是一种显而易见的简化，因为 TCP 的发送速率由于拥塞控制而变化；在本章后面的习题中我们将考察更为真实的与时间相关的速率 $x(t)$ 。）假设在时刻 $t=0$ ，应用缓存为空，视频开始到达客户应用缓存。我们现在问，在什么时刻 $t=t_p$ 开始播放呢？并且在播放过程中，什么时刻 $t=t_f$ 客户应用缓存变满呢？

首先，我们来确定 t_p ，此时 Q 比特已经进入应用缓存并且开始播放。前面讲过比特以速率 x 到达客户应用缓存，并且在开始播放之前没有比特从其缓存中删除。所以，建立 Q 比特所需的时间（初始缓存时延）是 $t_p = Q/x$ 。

我们现在来决定 t_f ，这是客户应用缓存变满的时刻。我们先观察，如果 $x < r$ （即如果服务器发送速率小于视频消耗速率），则客户缓存将决不会满！的确，时刻 t_p 开始，缓存将以速率 r 排空并且仅以速率 $x < r$ 填充。最终客户缓存将完全排空，此时当客户缓存等待另一个 t_p 秒来建起 Q 比特的视频时，视频将在屏幕上停滞。所以，当网络中可用速率小于视频速率时，播放将在连续播放期和停滞播放期之间进行变动。在课后习题中，将请你决定每个连续播放期和停滞期的长度，它们都作为 Q 、 r 和 x 的函数。当 $x > r$ 时，现在我们来决定 t_f 。在这种情况下，在时刻 t_p 开始，缓存以 $x - r$ 的速率从 Q 增加到 B ，因为比特以速率 r 消耗但以速率 x 到达，如图 7-3 所示。有了这些提示，在课后习题中将请你决定 t_f ，即客户缓存变满的时刻。注意到当网络中的可用速率大于视频速率时，在初始缓存时延后，用户将享受连续的播放直到视频结束。

4. 视频的早期中止和重定位

HTTP 流系统经常利用 HTTP GET 请求报文中的 HTTP 字节范围首部（HTTP byte-range header），该首部指示了客户当前要从所希望的视频中获取的字节范围。当用户要在视频中及时重定位（即跳跃）到未来点时，这特别有用。当用户重定位到一个新位置时，客户发送一个新 HTTP 请求，用字节范围首部指出服务器应当从文件的哪个字节起发送数据。当服务器接收到该新的 HTTP 请求时，它能够忘记任何较早的请求，而是由字节范围请求中指示的字节开始发送。

在我们讨论重定位主题的时候，我们简要地提及当某用户重定位到视频中的某个未来点或提前终止视频时，某些由服务器发送的已预取但尚未观看的数据将不会被观看，即导致了网络带宽和服务器资源的浪费。例如，假设在视频中的某时刻 t_0 客户缓存充满 B 比特，在此时用户重定位到视频中的某个瞬间 $t > t_0 + B/r$ ，然后从这点起观察视频直到结束。在这种情况下，缓存中的所有 B 比特将未被观看，用于传输这 B 比特的带宽和服务器资源完全被浪费掉了。在因特网中，有大量的带宽因提前终止而浪费，这些成本可能相当大，特别是对于无线链路 [Ihm 2011]。由于这个原因，许多流系统仅使用了长度适当的客户应用缓存，或者将限制在 HTTP 请求中使用字节范围首部预取的视频数量 [Rao 2011]。

重定位和提前终止可以与下列做法类比：烹调了很多肉，仅吃了一部分，并将其他都扔掉，因而浪费了食物。因此，下次你因为没有吃完所有晚餐而被父母批评浪费食物时，你能够迅速反驳：当他们在因特网上观看电影并进行带宽重定位时，他们浪费了带宽和服务器资源！但是，别人错了不等于你对了，食物和带宽都不应被浪费！

7.2.3 适应性流和 DASH

尽管如前一小节所述，HTTP 流在实践中已经得到广泛部署（例如，YouTube 自发展