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 7-17 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。

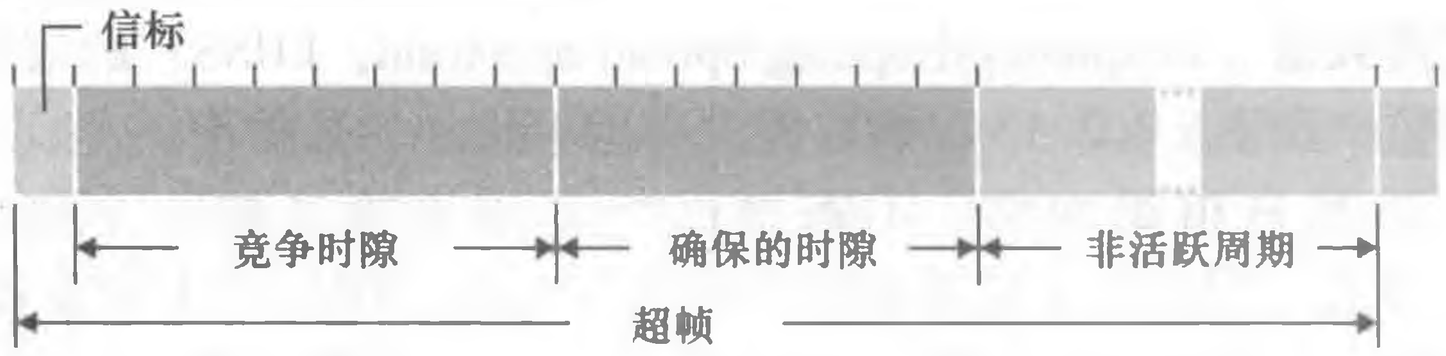

图 7-17　ZigBee 802.14.4 超帧结构

7.4　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。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 7.7 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；Palat 2009；Scourias 2012；Turner 2012；Akyildiz 2010］，以及特别优秀和详尽的参考资料［Mouly 1992；Sauter 2014］。

历史事件

4G 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4G 蜂窝移动系统。在某些国家（如韩国和日本），4G LTE 覆盖率高于90%，即几乎是无所不在。在2015 年，已部署的 LTE 系统的平均下载速率，范围从美国和印度的 10Mbps 到新西兰的接近40Mbps。这些4G 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。4G 系统以一种与现在仅蜂窝电话接入的相似方式，允许用户在移动中从遥远的户外位置接入因特网。在许多场合中，用户可以同时接入无线 LAN 和4G。对于4G 系统具有的更为受限和更为昂贵的能力，许多移动设备在两者都可用时，默认使用 WiFi 而不是使用4G。无线边缘网络接入将主要经过无线 LAN 还是经过蜂窝系统仍是一个悬而未决的问题：

- 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 和更高速率的 IEEE 802.11 无线 LAN 已经得到了广泛部署。几乎所有便携计算机、平板电脑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）也具有低功率的无线 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 语音服务与蜂窝电话网络或 IP 网络连接，因此绕过运营者的蜂窝语音和4G 数据服务。

当然，许多其他的专家相信4G 不仅将取得巨大的成功，而且也将使我们工作和生活的方式发生引人注目的革命。WiFi 和4G 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。

7.4.1 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，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% 的蜂窝用户使用 GSM。

当人们谈论蜂窝技术时，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）。3G 系统也支持语音和数据，但更为强调数据能力和更高速的无线电接入链路。今天正在部署的 4G 系统基于 LTE 技术，其特征为全 IP 核心网络，并且以几兆比特速率提供了话音和数据集成。

2G 蜂窝网体系结构：语音与电话网连接

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7-18左侧的六边形所示。如同在7.3.1节中学习的802.11WiFi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7-18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。

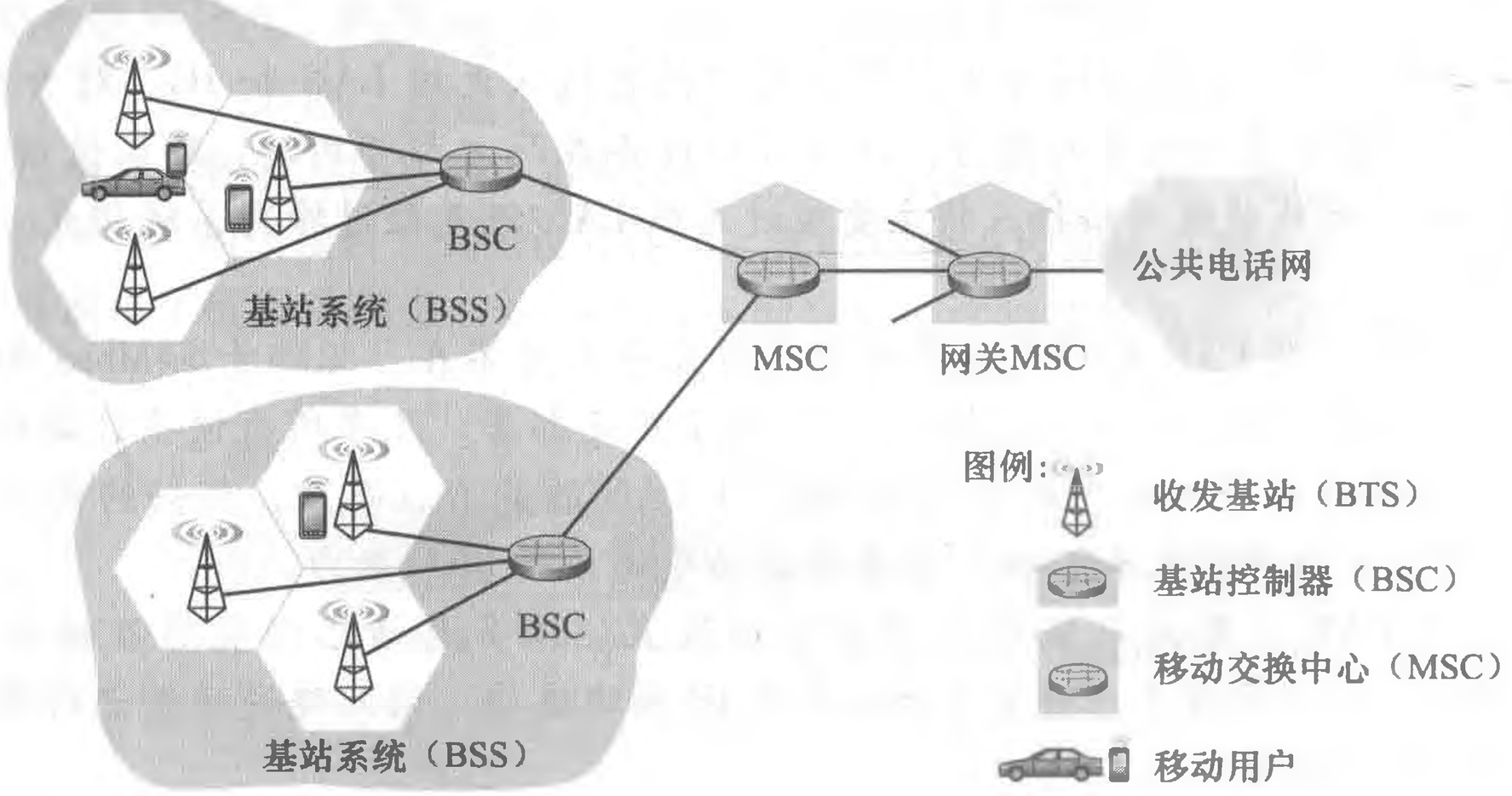

图7-18　GSM 2G蜂窝网体系结构的组件

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6.3.4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7.7.2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7.7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。

7.4.2　3G蜂窝数据网：将因特网扩展到蜂窝用户

我们在7.4.1节中的讨论关注了蜂窝语音用户连接到公共电话网。但当我们开始这样

干时，当然也乐意读电子邮件、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），并能够经过蜂窝数据网连接进入因特网。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，蜂窝数据网的主题是一个相当令人眼花缭乱的竞争和不断演化的标准集合，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 技术提出要求，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 和 4G 标准［3GPP 2016］。

我们自上而下地查看一下显示在图 7-19 中的 3G 蜂窝数据网体系结构。

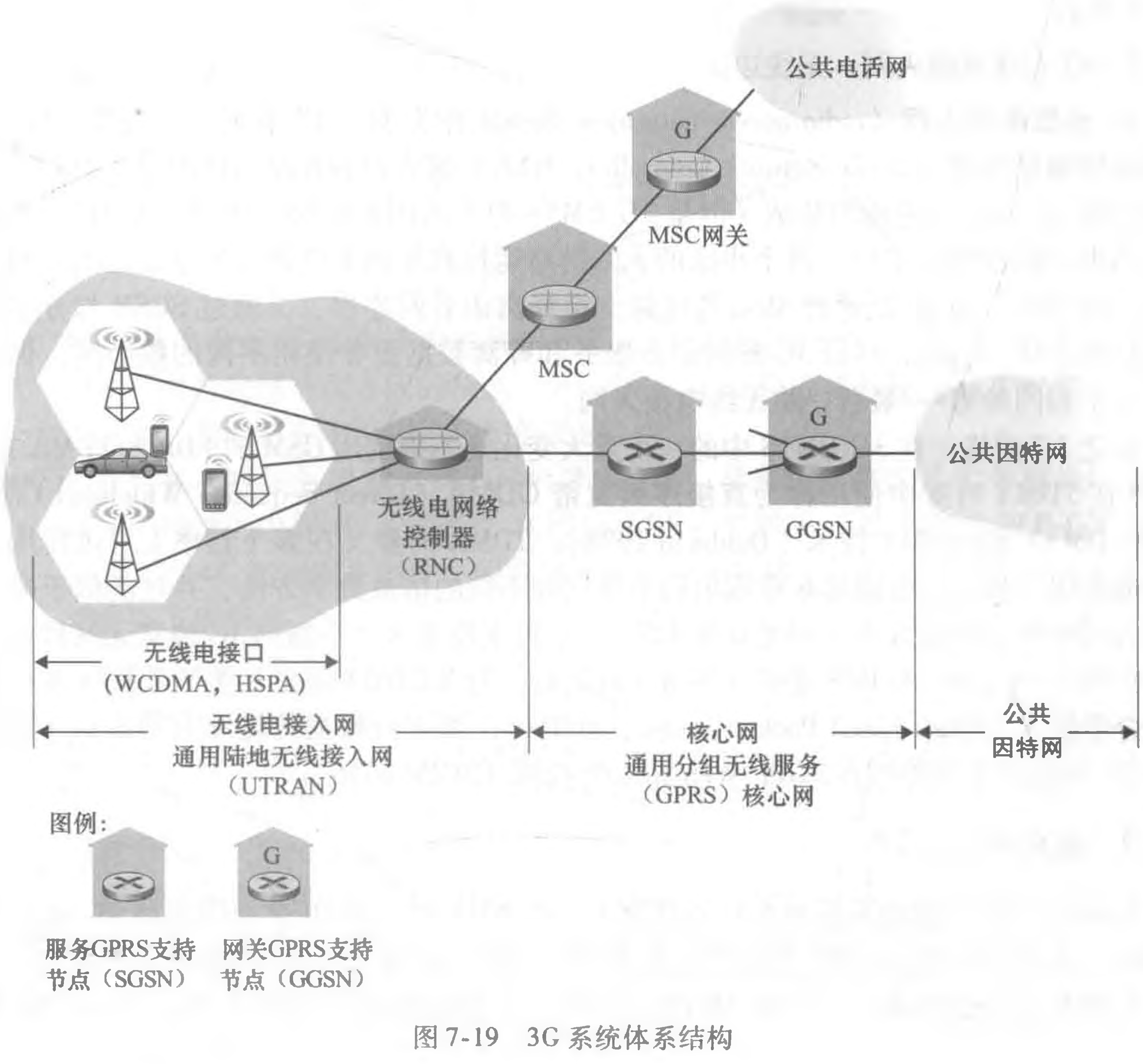

图 7-19　3G 系统体系结构

1. 3G 核心网

3G 核心蜂窝数据网将无线电接入网连接到公共因特网。核心网与我们前面在图 7-18 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 数据服务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 4.3 节中遇到过的挑战——在前面我们讨论了在因特网中新的（IPv6）和旧的（IPv4）集成的技术。

在3G核心网中有两类节点：**服务通用分组无线服务支持节点**（Serving Generalized packet radio service Support Node，SGSN）和**网关GPRS支持节点**（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节点交付（或从移动节点获取）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，维护活跃移动节点的位置（小区）信息，执行位于无线接入网中的移动节点和GGSN之间的数据报转发。GGSN起着网关的作用，将多个SGSN连接到更大的因特网。GGSN因此是源于移动节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。对外部而言，GGSN看起来像任何其他网络路由器，从外面看来，GGSN网络中3G节点的移动性隐藏在GGSN背后。

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。**无线电网络控制器**（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“节点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节点和收发基站之间，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6章指出的全部三种不同的信道共享方法，并且类似于有线电缆接入网中所采用的方法（参见6.3.4节）。这种变化要求一个新的3G蜂窝无线接入网与显示在图7-19中的2G BSS无线电网络并行运行。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 2016］。

7.4.3　走向4G：LTE

第四代（4G）蜂窝系统正在广泛部署中。在2015年，有50多个国家的4G覆盖率超过50%。由3GPP提出的4G长期演进互联网（LTE）标准［Sauter 2014］，较之3G系统而言有两个重要的创新：一个全IP核心网和一个加强的无线电接入网。下面对此进行讨论。

1. 4G系统体系结构：一个全IP核心网

图7-20显示了总体的4G网络体系结构，它（不幸地）又引入另一个（相当难以理解的）新词汇以及一些网络组件的首字母缩写词。但我们不要被这些首字母缩写词搞晕！有关4G体系结构，有两个重要的高层次观察。

- 一种统一的、全IP网络体系结构。与图7-19显示的3G网络不同，3G网络对于语音和数据流量具有分离的网络组件和路径，显示在图7-20中的4G体系结构是“全IP的”，即语音和数据都承载在IP数据报中，来自/去往无线设备（用户设

备，4G 的术语为 UE），到分组网关（P-GW）——该 P-GW 将 4G 边缘网络连接到网络的其他部分。使用了 4G，蜂窝网络来源于电话的最后痕迹已经荡然无存，让位给统一的 IP 服务了！

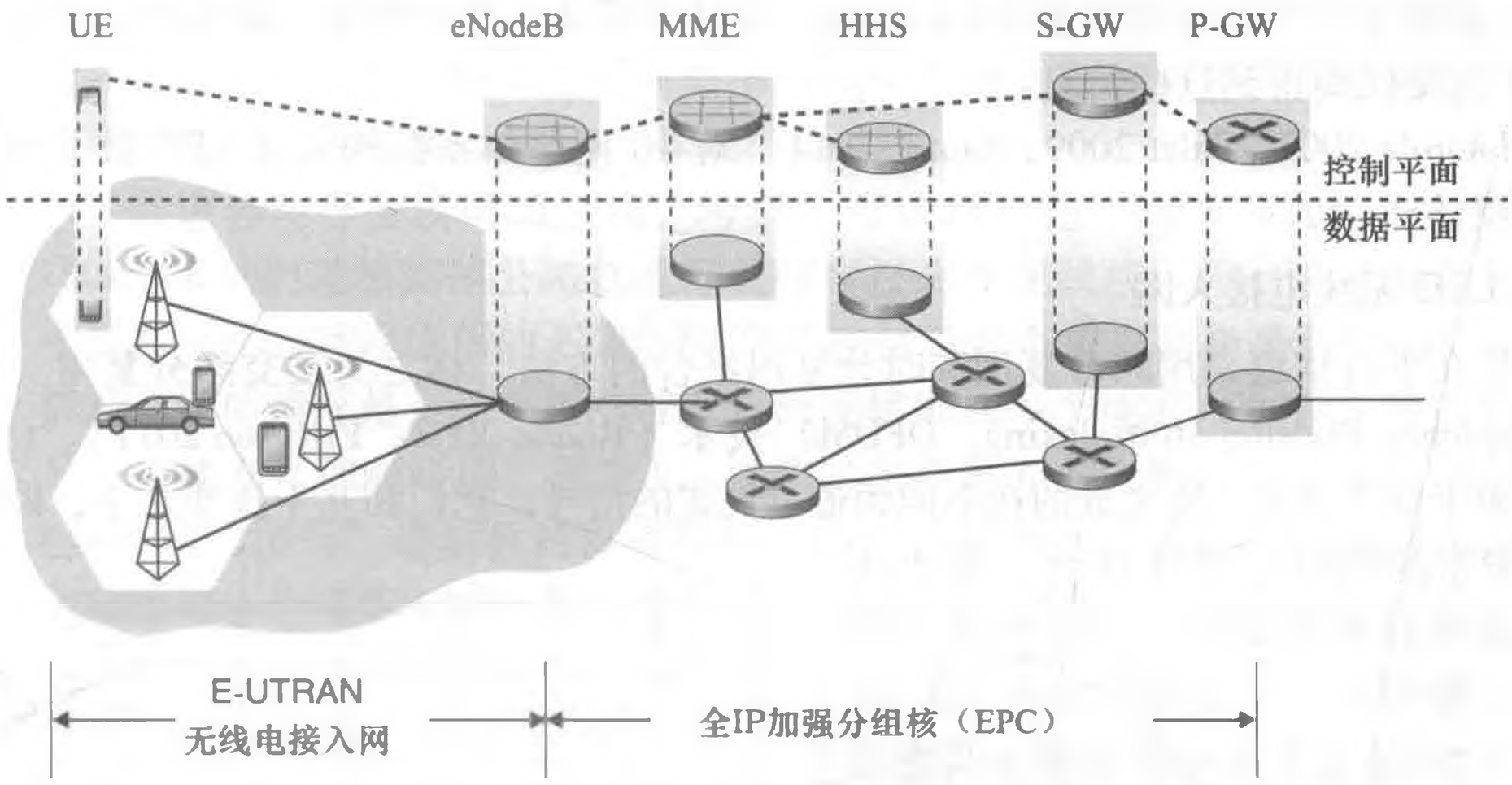

图 7-20　4G 网络体系结构

- 4G 数据平面与 4G 控制平面的清晰分离。分别对照第 4 章和第 5 章中 IP 网络层的数据平面与控制平面之间的特征，4G 网络体系结构也清晰地分离了数据平面和控制平面。我们将在下面讨论它们的功能。
- 无线电接入网与全 IP 核心网之间的清晰分离。承载用户数据的 IP 数据报经过通往外部因特网的内部 4G IP 网络，在用户（UE）和网关（图 7-20 中的 P-GW）之间转发。在 4G 控制服务组件之间经过相同的内部网络交换控制分组，这些组件的作用将在下面描述。

4G 体系结构的主要组件如下：

- eNodeB 是 2G 基站和 3G 无线电网络控制器（又称为节点 B）的逻辑后代，并且此时还起着关键作用。它的数据平面作用是在 UE 和 P-GW 之间（经过 LTE 无线电接入网）转发数据报。UE 数据报在 eNodeB 被封装，并且通过 4G 网络的全 IP 强化分组核（EPC）以隧道形式传输到 P-GW。eNodeB 与 P-GW 之间的隧道类似于我们在 4.3 节中看到的 IPv6 数据报隧道，这些分组在两个 IPv6 端点之间通过一个使用 IPv4 路由器的网络传输。这些隧道可能与保证服务质量（QoS）相关。例如，4G 网络可能确保语音流量在 UE 和 P-GW 之间历经不超过 100ms 时延，分组丢失率小于 1%；TCP 流量也许能够确保 300ms 时延以及小于 0.0001% 的分组丢失率［Palat 2009］。我们将在第 9 章涉及 QoS。在控制平面中，eNodeB 代表 UE 来处理注册和移动性信令流量。
- **分组数据网络网关**（Packet Data Network Gateway，P-GW）给 UE 分配 IP 地址，并且保证 QoS 实施。作为隧道端点，当向或从 UE 转发数据报时，它也执行数据报封装/解封装。
- **服务网关**（S-GW）是数据平面移动性锚点，即所有 UE 流量将通过 S-GW 传递。该 S-GW 也执行收费/记账功能以及法定的流量拦截。
- **移动性管理实体**（Mobility Management Entity，MME）代表位于它所控制单元中的

UE，执行连接和移动性管理。它从 HHS 接收 UE 订购信息。我们在 7.7 节中详细讨论蜂窝网络中的移动性。

- **归属用户服务**（Home Subscriber Server，HSS）包含了包括漫游接入能力、服务质量配置文件和鉴别信息的 UE 信息。如我们在 7.7 节中所见，该 HSS 从 UE 归属蜂窝提供商得到这些信息。

［Motorola 2007；Palat 2009；Sauter 2014］对 4G 网络体系结构及其 EPC 做了可读性很强的介绍。

2. LTE 无线电接入网

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，每个活跃的移动节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 7-21 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），移动节点能够获取越来越高的传输速率。在移动节点之间进行时隙（重）分配的频度为每毫秒一次。不同的调制方案也能用于改变传输速率，参见我们前面对图 7-3 的讨论以及 WiFi 网络中调制方案的动态选择。

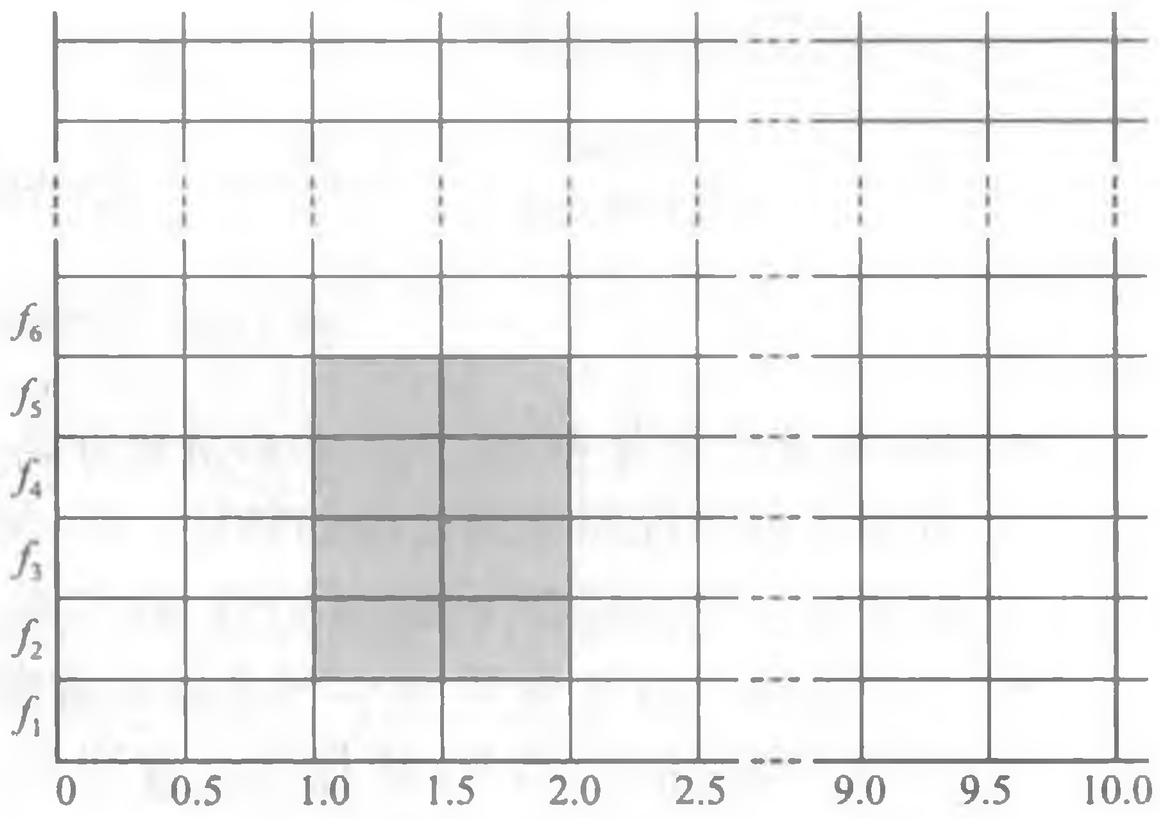

图 7-21　在每个频率上，20 个 0.5ms 的时隙组成 10ms 帧。阴影显示了一个 8 时隙分配

LTE 标准并未对向移动节点特殊分配时隙进行强制要求。相反，允许哪个移动节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，使无线电网络控制器能够最大限度地利用无线媒体。此外，能够使用用户优先权和服务的契约等级（如银、金或铂金）调度下行分组传输。除了上面描述的 LTE 能力，高级 LTE 通过向移动节点分配聚合信道提供了数百兆下行带宽［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。WiMAX 目前还没有得到 LTE 那样的广泛部署，它的详细讨论能够在本书的 Web 站点上找到。

7.5　移动管理：原理

学习了无线网络中通信链路的无线特性后，现在我们将注意力转向这些无线链路带来的移动性。宽泛地讲，移动节点是随时间改变它与网络连接位置的节点。因为移动性这一术语在计算机界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 7-22 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 7.3.4 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或特斯拉轿车内以 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 7-22 从网络层角度阐明了用户移动性的程度谱。

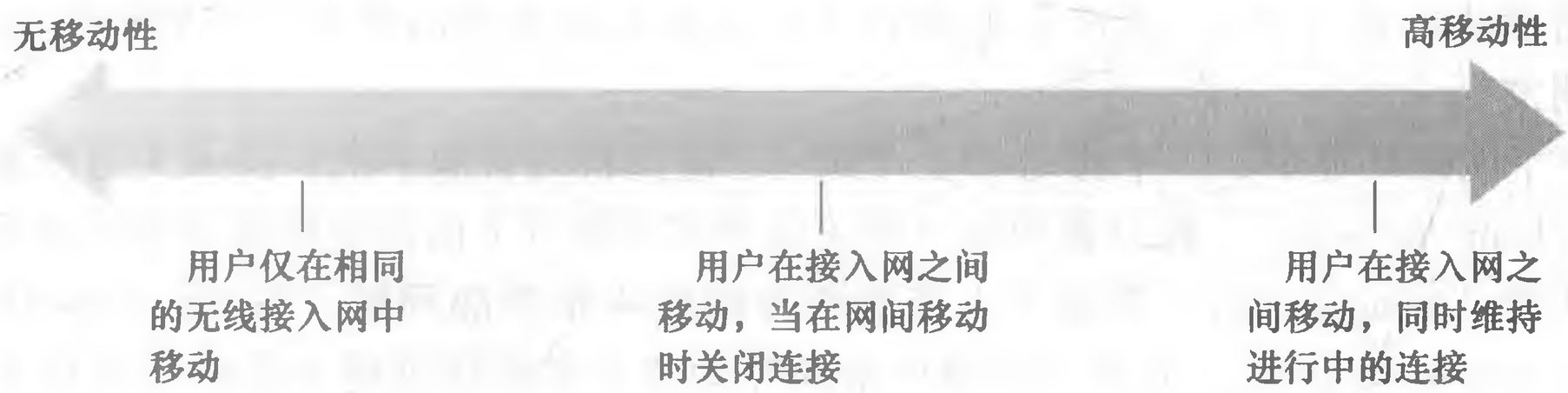

图 7-22　从网络层观点来看各种程度的移动性

- 移动节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（本质上是你电话的网络层地址）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 连接的宝马或特斯拉司机而言，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，它允许移动节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 4.3 节中看到的 DHCP 提供了这种功能。
- 支持有线基础设施的东西有哪些可用？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 2016］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，一个移动节点（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节点执行下面讨论的移动管理功能的实体叫**归属代理**（home agent）。移动节点当前所在网络叫作**外部网络**（foreign network）或**被访网络**（visited network），在外部网络中帮助移动节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）就是希望与该移动节点通信的实体。图 7-23 阐述了这些概念，也说明了下面考虑的编址概念。在图 7-23 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。

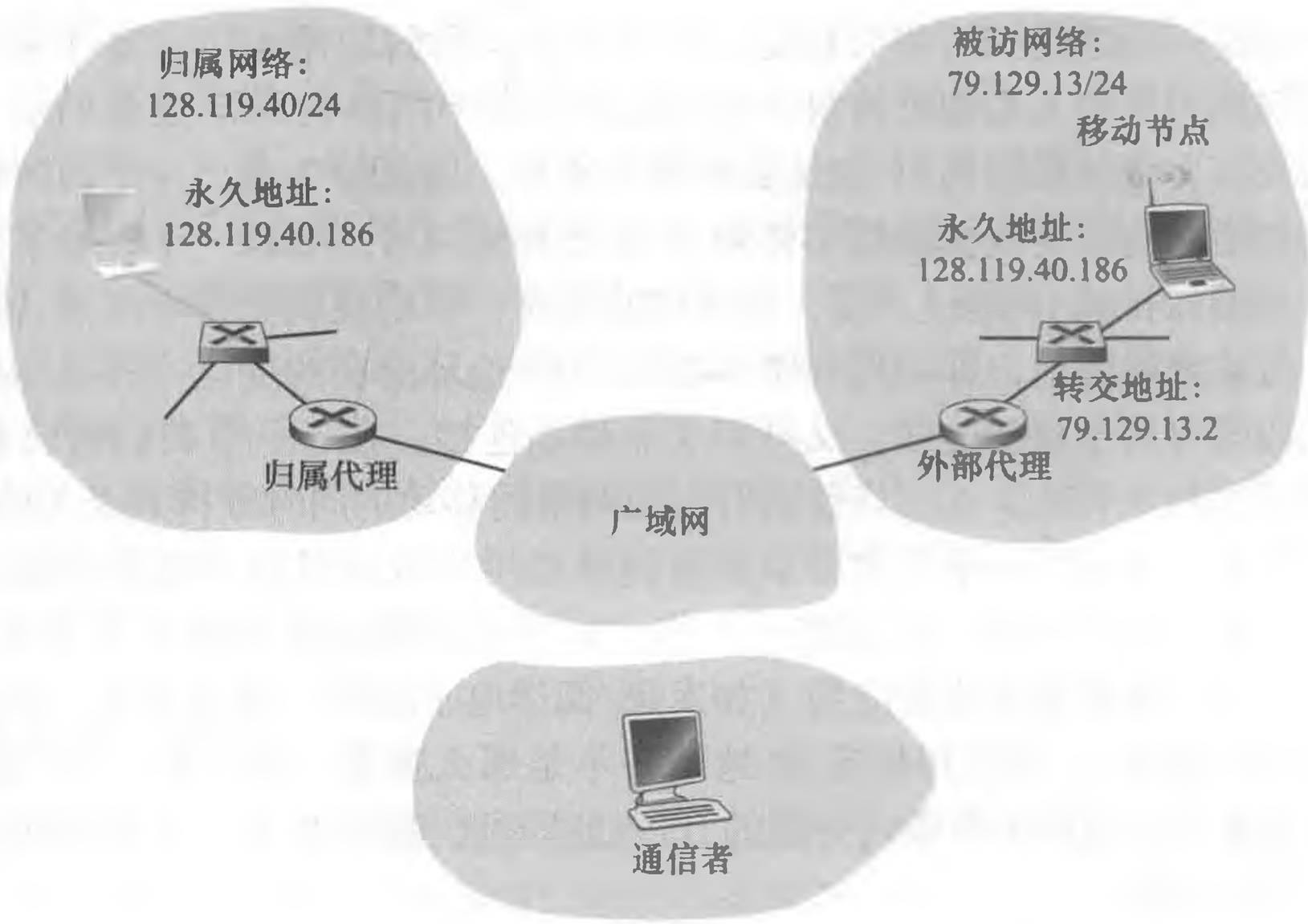

图 7-23　移动网络体系结构中的初始要素

7.5.1　寻址

我们前面提到为了使用户移动性对网络应用透明，希望一个移动节点在从一个网络移动到另一个网络时保持其地址不变。当某移动节点位于一个外部网络时，所有指向此节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，告诉它们该移动节点正在它的网络中。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节点的固定地址，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节点的固定地址（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节点的永久地址的正确路径；参见4.3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。当移动节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节点的特别路由，旧的外部网络将撤销其与该移动节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节点的位置，很容易将数据报路由到该移动节点，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节点的转发表表项。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节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，在移动节点的归属网络中的归属代理也能跟踪该移动节点所在的外部网络。这当然需要一个移动节点（或一个代表该移动节点的外部代理）与归属代理之间的协议来更新移动节点的位置。

我们现在更详细地思考外部代理。如图7-23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节点创建一个所谓的**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。因此一个移动节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7-23中的例子中，移动节点的固定地址是128.119.40.186。当被访网络为79.129.13/24时，该移动节点具有的COA为79.129.13.2。外部代理的第二个作用就是告诉归属代理，该移动节点在它的（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”到移动节点。

虽然我们已将移动节点与外部代理的功能分开，但是应当注意到移动节点也能承担外部代理的责任。例如，某移动节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。

7.5.2　路由选择到移动节点

我们现在已看到一个移动节点是如何得到一个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

节点呢？因为只有归属代理（而不是全网的路由器）知道该移动节点的位置，故如果只是将一个数据报寻址到移动节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. 移动节点的间接路由选择

我们先考虑一个想给移动节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节点的固定地址，并将数据报发送到网络中去，完全不知道移动节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节点的归属网络。这用图7-24中的步骤1加以说明。

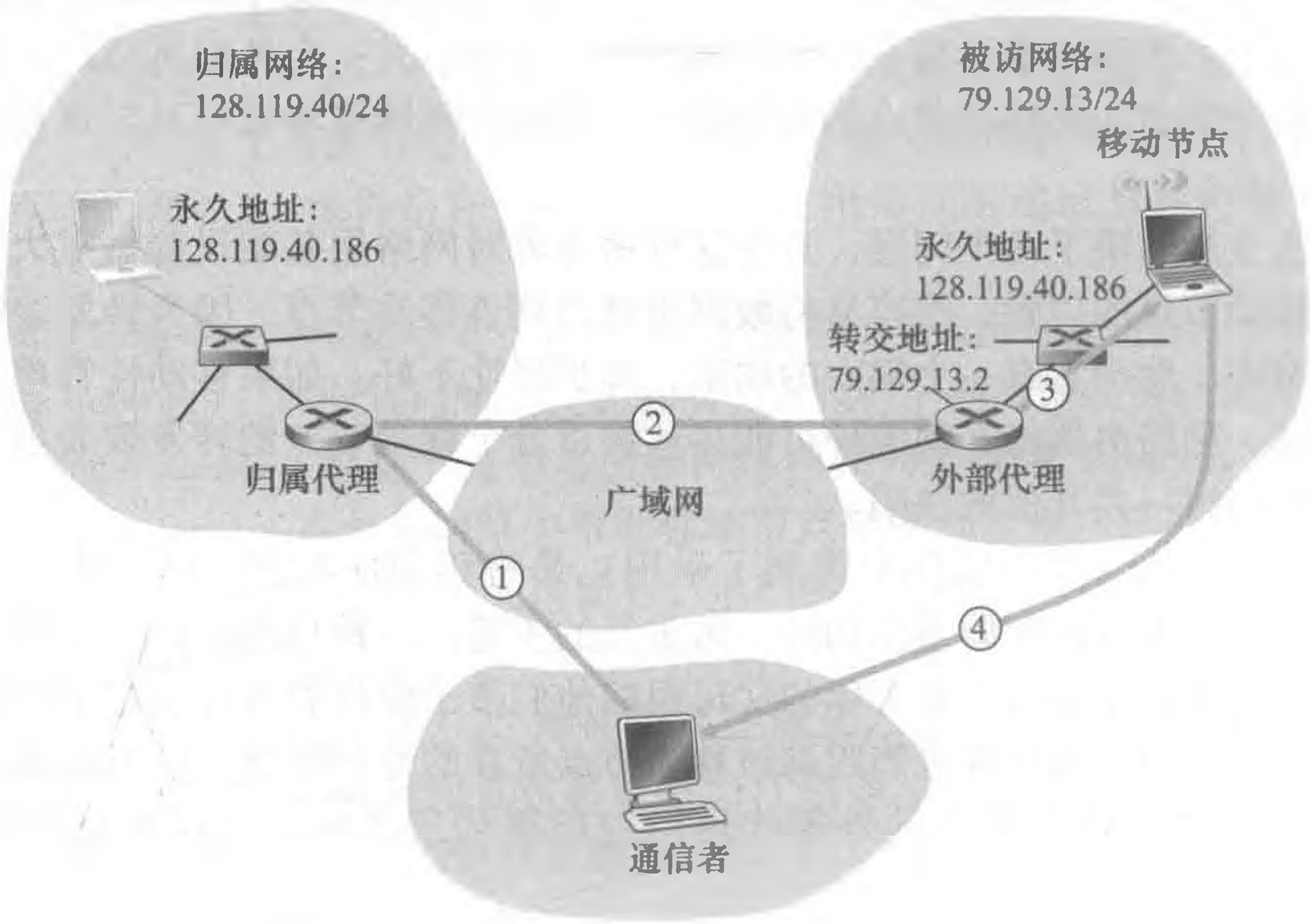

图7-24　对移动节点的间接路由选择

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节点的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，这些数据报寻址的节点的归属网络与该归属代理所在网络相同，但这些节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。通过使用移动节点的COA，该数据报先转发给外部代理（图7-24中的步骤2），然后再从外部代理转发给移动节点（图7-24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节点的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节点的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，然后再向移动节点转发该原始数据报（图7-24中的步骤3）。图7-25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；以及向移动节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 4.3 节讨论 IP 多播与 IPv6 时涉及的。

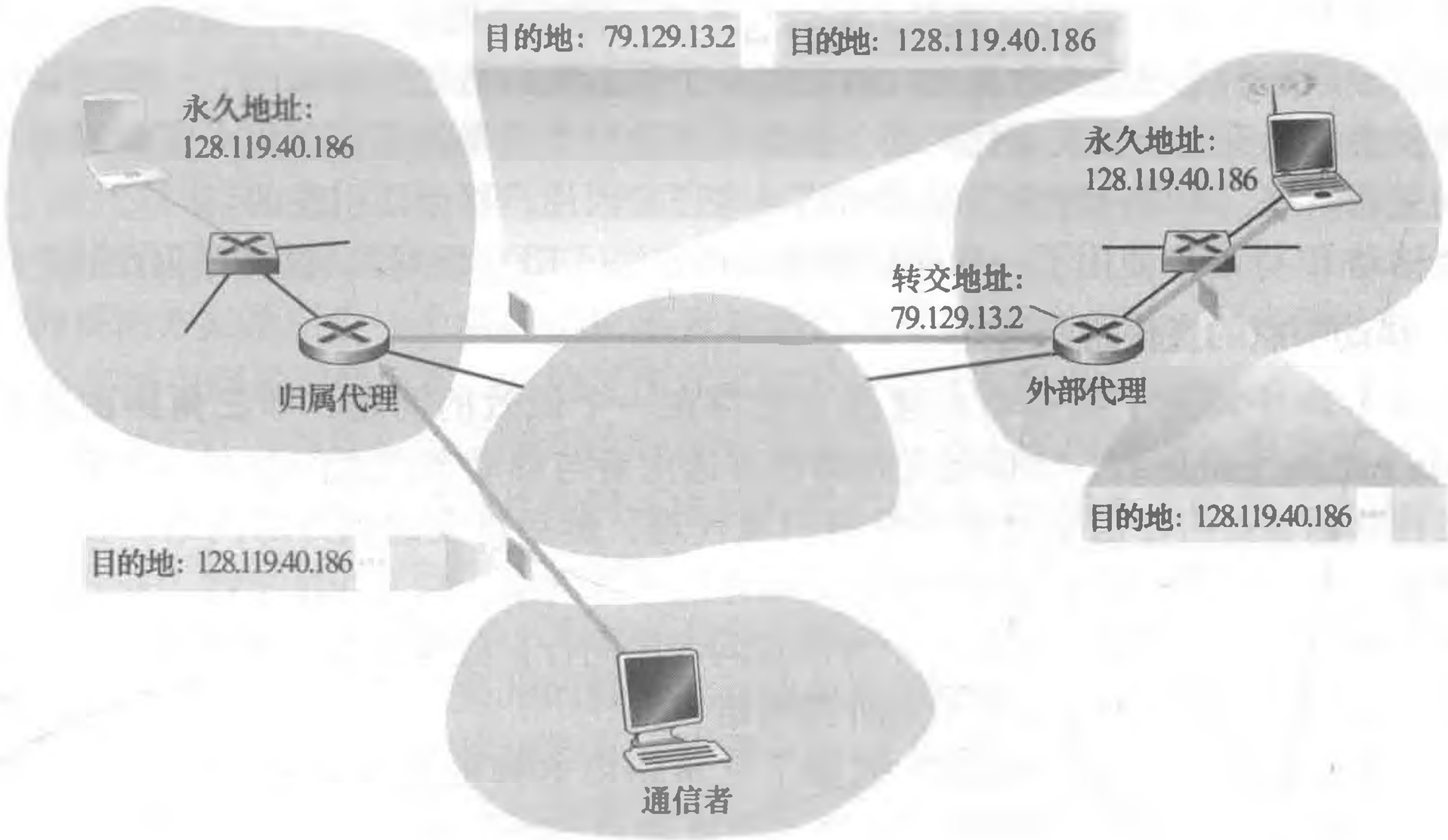

图 7-25 封装与拆封

接下来我们考虑某移动节点如何向一个通信者发送数据报。这相当简单，因为移动节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）。因为移动节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 7-24 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。

- 移动节点到外部代理的协议。当移动节点连接到外部网络时，它向外部代理注册。类似地，当一个移动节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节点的 COA。当某移动节点离开其网络时，外部代理不需要显式地注销 COA，因为当移动节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节点。

上述讨论提供了一个移动节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。假设某移动节点连到外部网络 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。该移动节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，外部代理将该移动节点的新 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。但当移动节点在网络之间移动时，它会看到数据报流中断吗？只要移动节点与网络 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。因而当一个节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 7.6 节中讨论。

2. 移动节点的直接路由选择

在图 7-24 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节点之间存在一条更有效的路由，发往移动节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）先知道该移动节点的 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，移动节点具有一个在归属代理注册过的最新的 COA。与移动节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 7-26 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节点的 COA，这与归属代理使用的隧道技术相类似，参见图 7-26 的步骤 3 和步骤 4。

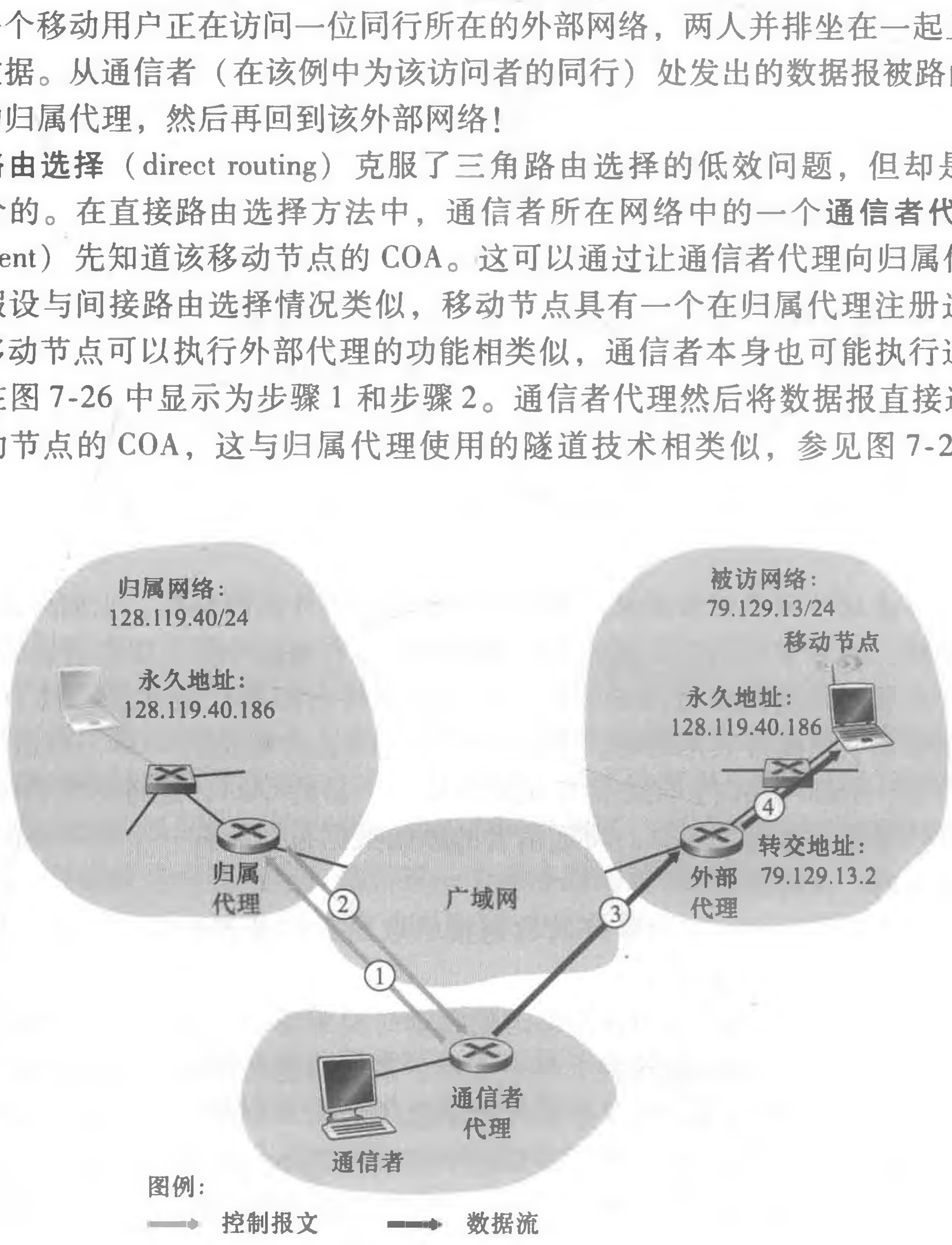

图 7-26　到某移动用户的直接路由选择

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节点的 COA（图 7-26 中的步骤 1 和步骤 2）。
- 当移动节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节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节点，并且在会话刚开始时该移动节点就位于该网络中（图 7-27 中的步骤 1）。我们将首次发现移动节点的外部网络中的外部代理标识为**锚外部代理**（anchor foreign agent）。当移动节点到达一个新外部网络后（图 7-27 中的步骤 2），移动节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节点的新 COA（步骤 4）。当锚外部代理收到一个发往已经离开的移动节点的封装数据报后，它可以使用新的 COA 重新封装数据报并将其转发给该移动节点（步骤 5）。如果移动节点其后又移到另一个外部网络中，在该被访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。

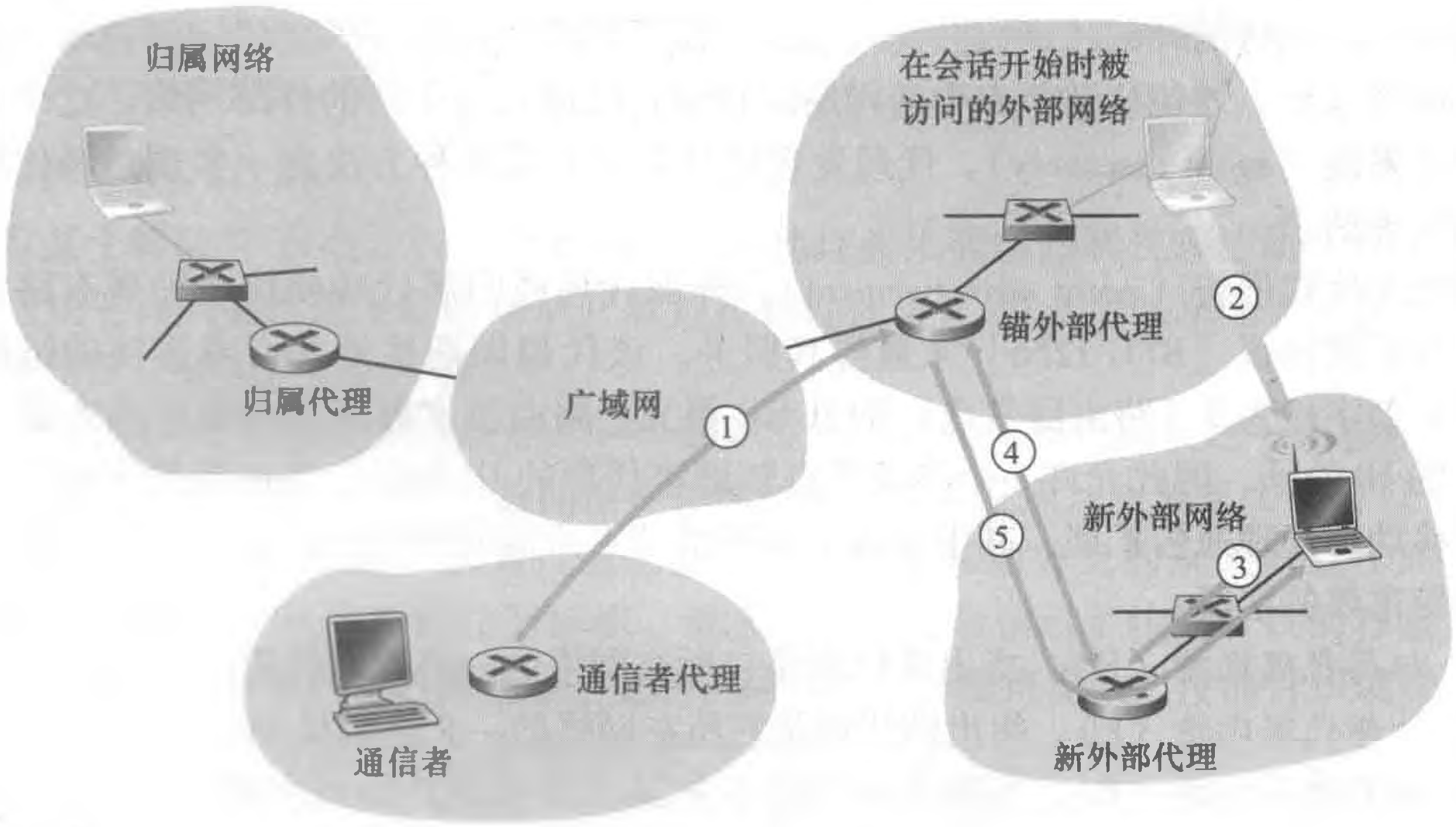

图 7-27　在网络间使用直接路由选择的移动转移

7.6　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），代理与移动节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］规定到移动节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节点通告其服务的协议，以及移动节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 定义了移动节点和/或外部代理向一个移动节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节点的方式，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节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 节点，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，才使移动节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。该代理周期性地在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，因此允许一个移动节点知道该代理的 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，其中包含了该移动节点所需的附加信息。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部网络（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，无须向外部代理注册。
- 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节点。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 7-28 说明了在代理通告报文中的某些关键字段。