第 5 章 移动互联网 IP 协议

IP(Internet Protocol)面向传统的互联网应用,其协议设计没有考虑设备的移动问题,因此它并不适应移动互联网应用场景。本章在介绍 IP 概念及其挑战的基础上,系统地讨论了移动 IP 的相关概念与关键技术,以及移动 IPv4 与移动 IPv6 协议实现。

5.1 移动 IP 协议的基本概念

5.1.1 IP 协议的相关内容

1. IP 协议的相关概念

IP 协议是互联网的核心协议之一。IP 网络是泛指使用 IP 协议进行通信的各种网络。IP 协议提供尽力而为(Best Effort)的传输服务。每个分组都是在 IP 网络中独立传输,并且经过的传输路径可能不同。IP 协议也不保证分组的传输可靠性,可能出现传输错误、丢失、乱序、重复等情况,依赖于上层协议(如 TCP)进行纠错。IP 协议主要包括以下重要的概念。

- IP 地址:唯一标识连接在互联网中的设备。IP 地址分为 IPv4 地址与 IPv6 地址。其中,IPv4 地址的长度为 32 位,通常采用点分十进制格式表示,例如 192.168.1.1。目前,IPv4 地址已经分配完毕。IPv6 地址的长度为 128 位,通常采用冒号分十六进制格式表示,例如 21DA:0000:0000:0000:02AA:000F:FE08:9C5A。IPv6 地址几乎可以无限扩展,解决 IPv4 地址短缺问题。IP 地址分为公有地址与私有地址。其中,公有地址通常由 ISP 分配给用户,可以在互联网上直接使用。私有地址仅在局域网内部使用,不会在互联网上直接路由。
- 分组与路由:分组(Packet)又称数据包,它是 IP 协议的基本数据单元。IP 分组包括分组头(源 IP 地址、目的 IP 地址、TTL、协议类型、分组长度等)与有效载荷(来自上层的用户数据)。路由是指分组通过 IP 网络的转发过程。路由协议主要包括 OSPF、BGP 等。路由器通过路由协议来动态更新路由表,并根据路由表选择最佳路径来转发分组。
- 子网划分:目的是提高地址利用率、减少广播流量与增强安全性。子网掩码用于标识 IP 地址的网络部分与主机部分。例如,192.168.1.0/24 表示该地址的前 24 位为网络地址,后 8 位为主机地址。这个子网可分配 254 个主机地址。
- 相关协议:网络地址转换(NAT)将私有地址映射为公有地址,解决地址不足问题。

动态主机配置协议(DHCP)为主机自动分配 IP 地址、子网掩码等信息,简化网络管理。互联网控制报文协议(ICMP)用于网络诊断,可以实现 Ping、Traceroute 等。地址解析协议(ARP)将 IP 地址解析为 MAC 地址。

2. 其他相关的网络知识

为了帮助读者更好地理解移动 IP 协议,下面以 Ethernet 为例,说明传输介质与链路、链路与网络、链路地址与网络地址之间的区别与联系。

局域网用于互联局部范围内的计算机,典型代表是 IEEE 802.3 协议的 Ethernet。IEEE 802.3 包括物理层与数据链路层协议。传统 Ethernet 是一种总线型局域网,多台计算机连接在一条共享的传输介质上。早期使用的传输介质是同轴电缆。由于多台计算机共享一条传输介质,因此在传输数据时就可能出现冲突。数据链路层(又称 MAC 层)规定了数据帧结构与 MAC 地址,以及介质访问控制的 CSMA/CD 算法。这样,MAC 层将一条物理的通信"线路"变成一条逻辑的数据"链路"。

传统 Ethernet 建立在"共享介质"的基础上,随着接入计算机的数量增多,每台计算机的传输效率降低。在这样的背景下,传统 Ethernet 发展成交换式 Ethernet,采用交换机(Switch)作为核心设备来组网。Ethernet 中传输的数据单元是 MAC 帧,其中的地址使用 MAC 地址又称物理地址,地址长度为 6B(48b)。MAC 地址通常以 12 位的十六进制数表示,例如 00:1A:2B:3C:4D:5E。MAC 地址是由网络设备生产商分配,固化在网卡的 ROM 中,并保证每个 MAC 地址在全球是唯一的。

IP 地址用于在互联网中标识主机与网络设备。在互联网应用的通信流程中,同时涉及 IP 地址与 MAC 地址的处理。这里,IP 地址工作在网络层,而 MAC 地址工作在数据链路层。如果互联网中的一台主机需要发送数据,相应的分组中包含目的节点的 IP 地址。在互联网环境中,路由器根据目的 IP 地址对分组进行路由选择;在局域网环境中,交换机根据目的 MAC 地址对数据帧进行转发。地址解析协议(ARP)用于将 IP 地址解析为对应的 MAC 地址,以便路由器、交换机之间能够进行交互。

3. IP 协议在移动互联网中的问题

IP 协议要求互联网中的每台主机具有一个 IP 地址,用于标识这台主机在网络中的位置。图 5-1 给出了手机漫游与 IP 地址的关系。用户 A 的手机 A 在网络 A 中完成注册,该网络为手机 A 分配了一个 IP 地址(200.1.1.10);用户 B 的手机 B 也在同一网络中完成注册,该网络为手机 B 分配了一个 IP 地址(200.1.1.80)。如果手机 A 需要向手机 B 发送数据,Wi-Fi 路由器在其路由表中查找 200.1.1.80,发现 200.1.1.10 与 200.1.1.80 位于同一 DS 中,则两台手机之间就能够传输数据。

如果与手机 B 进行数据传输的过程中,用户 A 携带手机移动到另一幢办公楼,当前所在网络 B 的 IP 地址为 195.1.2.0/24,那么手机 A 能否通过 200.1.1.10 与用户 B 继续通信?这时显然存在问题。对于网络 B 中的路由器,其路由表中仅有源地址为 195.1.2.0/24 的节点到其他节点的路由信息,无法为 IP 地址不属于 195.1.2.0/24 的手机提供路由。这是移动节点在漫游过程中必然会遇到的问题。为了保证移动节点在漫游过程中仍能保持已有通信,这就需要研究支持移动互联网的 IP 协议。

在不改变现有 IP 协议的条件下,解决这个问题仅有两种可能的方案:第一种方案是主机在每次改变接入点时改变 IP 地址;第二种方案是主机在改变接入点时不改变 IP 地址,而

是在整个互联网中加入针对该主机的特定主机路由。这两种方案时都存在重大的缺陷。第一种方案的缺点是不能保持通信连续性，由于移动主机的 IP 地址不断变化，导致移动主机无法与其他主机通信。第二种方案的缺点是路由器对每个分组都进行路由选择，路由表将急剧膨胀，路由器处理特定路由的负荷加重，不能满足大型网络要求。因此，IETF 成立了专门的工作组 IP Routing for Wireless/Mobile Hosts，并从 1992 年开始制定移动 IP 相关标准。

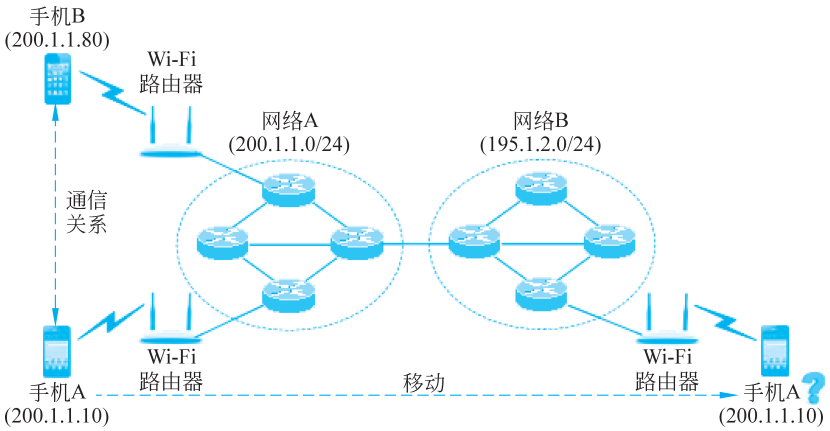

图 5-1　手机漫游与 IP 地址的关系

5.1.2　移动 IP 技术发展过程

针对 IP 协议在移动互联网中遇到的问题，由于最初改进是针对当时的 IPv4 协议，因此，初期的移动 IP 协议被称为移动 IPv4(Mobile IPv4，MIPv4)。1996 年，IETF 发布了第一个移动 IPv4 标准(RFC 2002 文档)，定义了移动 IPv4 的基本框架。2002 年，RFC 2002 被更新为 RFC 3344，进一步完善了移动 IPv4 核心机制，包括代理发现、注册过程、分组转发等。RFC 3344 还定义了移动节点(MN)、归属代理(HA)与外地代理(FA)的角色，以及通过隧道技术实现分组透明转发的方案。

2002 年，IETF 开始对移动 IPv4 的部署问题进行优化与扩展。2004 年，RFC 3846 文档扩展了支持认证、授权与计费(AAA)服务。2006 年，RFC 4433 文档定义了动态归属代理分配机制。2007 年，RFC 4881 文档定义了移动节点的低延时切换机制。2008 年，RFC 5177 文档扩展了家庭网络前缀动态分配。2008 年，RFC 5265 文档定义了 IPsec VPN 网关的穿越机制。2009 年，RFC 5266 文档扩展了 MOBIKE 协议支持。2009 年，RFC 5454 文档扩展了支持双协议栈(IPv4 与 IPv6)。2010 年，IETF 继续推进 MIPv4 协议标准化，包括 RADIUS 扩展与管理信息库(MIB)更新。

综上所述，移动 IPv4 发展经历了早期研究、核心协议标准化、扩展与优化、兼容性与多隧道机制，以及与其他技术融合的多个阶段。随着移动互联网发展及应用需求变化，移动 IPv4 不断演进以面对实际部署中的挑战。

5.1.3　移动 IP 的设计目标

移动 IP 协议的设计目标是：移动主机在改变接入点时，无论是在不同网络之间或不同

链路之间移动时，都不必改变它的 IP 地址，可保持已有通信的连续性。因此，移动 IP 研究解决移动主机支持分组转发的网络层协议问题。

移动 IP 研究主要解决两个问题：

- 移动主机可通过一个永久的 IP 地址连接到任何链路上。
- 当移动主机切换到一个新的链路时，仍然能保持与对方的正常通信。

作为网络层的一种协议，移动 IP 协议应具备以下特征。

- 移动 IP 协议要与现有的互联网协议兼容。
- 移动 IP 协议与底层采用的 MAC 层与物理层协议无关。
- 移动 IP 协议对传输层及以上的高层协议是透明的。
- 考虑到移动节点通常采用无线方式接入，涉及无线信道带宽、误码率、电池供电等因素，移动 IP 协议应尽量简化，减少协议开销。
- 移动 IP 协议应具有良好的可扩展性、可靠性和安全性。

5.1.4 移动 IP 的基本术语

1. 移动 IP 系统结构

图 5-2 给出了移动 IP 的系统结构。其中，涉及构成移动 IP 系统的主要功能实体（包括节点、代理、通信对端等），以及工作过程涉及的主要术语（包括地址、网络、链路、移动绑定、隧道等）。

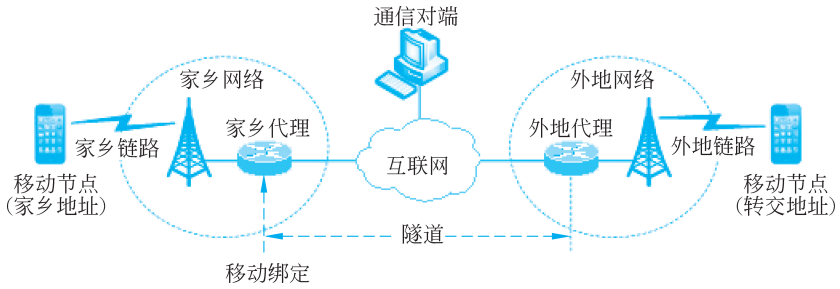

图 5-2 移动 IP 的系统结构

在讨论移动 IP 的工作原理时，涉及构成移动 IP 系统的以下 4 个实体。

- 移动节点（Mobile Node，MN）：从一个网络移动到另一个网络的笔记本计算机、平板计算机、手机或路由器。移动节点改变网络接入点之后，可以不改变自身的 IP 地址，继续与其他节点通信。
- 家乡代理（Home Agent，HA）：位于移动节点所属的家乡网络中提供服务的路由器，负责维护移动节点的家乡地址与当前转交地址的绑定，并通过隧道技术将分组转发给移动节点。家乡代理与外地代理统称为移动代理。
- 外地代理（Foreign Agent，FA）：移动节点所访问的外地网络中提供服务的路由器，负责向移动到这个网络的移动节点提供服务，包括分配转交地址、转发注册信息、分组路由等。当移动节点的家乡代理通过隧道发送分组时，外地代理接收并将分组转发给移动节点。
- 通信对端（Correspondent Node，CN）：与移动节点在移动过程中进行通信的节点，它

可以是互联网中的服务器或其他移动终端。因此，通信对端可以是一个固定节点，也可以是一个移动节点。

2. 移动 IP 基本术语

在讨论移动 IP 的工作原理时，涉及以下基本术语。

- 家乡地址(Home Address，HoA)：家乡网络为移动节点分配的一个永久 IP 地址。无论移动节点在家乡网络或外地网络，它的家乡地址始终不改变。因此，有些文献将它称为归属地址，可作为移动节点的身份标识。
- 转交地址(Care-of Address，CoA)：移动节点接入一个外地网络时，被分配的一个临时 IP 地址。转交地址是移动节点与家乡代理的隧道出口。
- 家乡网络(Home Network，HN)：移动节点分配家乡地址的网络。
- 外地网络(Foreign Network，FN)：移动节点分配转交地址的网络。
- 家乡链路(Home Link，HL)：移动节点在家乡网络时接入的链路。家乡链路所在网络与移动节点的家乡地址具有相同的网络前缀。
- 外地链路(Foreign Link，FL)：移动节点在外地网络时接入的链路。家乡链路、外地链路能够精确描述移动节点的接入位置。
- 移动绑定(Mobility Binding，MB)：家乡网络维护的移动节点的家乡地址与转发地址之间的关联。
- 隧道(Tunnel)：家乡代理向移动节点转发分组所用的逻辑链路。隧道的一端通常是家乡代理，另一端是外地代理或移动节点。

5.2 移动 IPv4 协议

5.2.1 移动 IPv4 代理发现

RFC 3344 文档定义了移动 IPv4 系统的核心架构。移动 IPv4 的设计目标是笔记本计算机、手机等移动设备在切换网络时，无须更换 IP 地址，保持正在进行的通信，并且该过程对上层应用与通信对端屏蔽了移动过程的实现细节。移动 IPv4 的工作流程主要涉及代理发现、移动节点注册、数据传输等。当移动节点到达某个网络时，需要判断自己是在家乡网络，还是进入了一个新的网络，这个过程称为代理发现(Agent Discovery)。移动 IPv4 的代理发现是通过扩展 ICMP 路由发现机制来实现的。

1. 代理通告

移动代理使用了一种扩展的 ICMP 代理发现协议。文档 RFC 1256 定义了这种路由发现机制的扩展方案。外地代理或本地代理将会周期性地向其连接的链路上广播一个代理通告(Agent Advertisement)报文。图 5-3 给出了 ICMP 代理通告报文结构。其中，通用头部的类型字段值为 9，代码字段值为 0，表示该报文的基本类型为路由器通告；扩展头部的类型字段值为 16，表示该报文的细分类型为代理通告。每个代理通告报文可以携带多个供移动节点使用的转交地址。

当移动节点接收到代理通告报文时，可根据该报文确定自己接入的网络。如果代理通告报文的信息字段的(Home，H)标记为 1，表示该报文的发送方是家乡代理，则移动节点已

回到家乡网络，此时无须使用移动 IP 服务。如果代理通告报文的信息字段的(Foreign，F)标记为 1，表示该报文的发送方是外地代理，则移动节点已接入一个外地网络，此时需要外地代理提供的转交地址。另外，如果一个网络支持动态配置功能，移动节点也可通过 DHCP 直接获取配置转交地址(无须外地代理参与)。

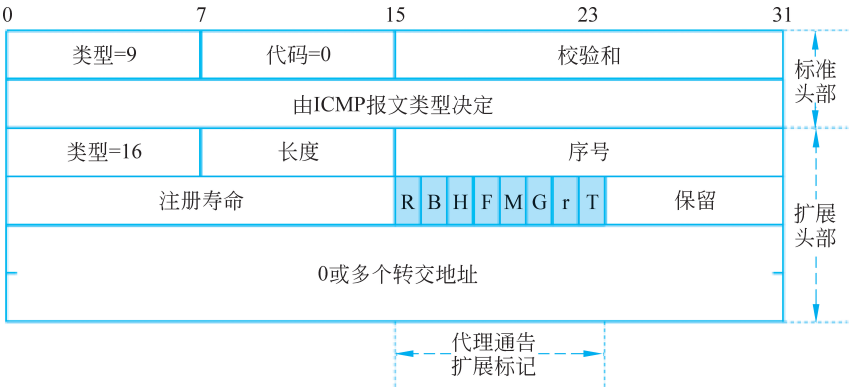

图 5-3　ICMP 代理通告报文结构

2. 代理请求

当移动节点进入一个网络时，如果没有接收到代理通告报文，为了减少移动节点的等待时间，它将向其连接的链路上广播一个代理请求(Agent Solicitation)报文，以便快速发现该网络中的代理。在代理请求报文中，通用头部的类型字段值为 10，代码字段值为 0，表示基本类型为路由器请求；扩展头部的类型字段值为 16，表示细分类型为代理请求。当外地代理或本地代理接收到代理请求报文时，将会立即返回一个代理通告报文。代理请求更适用于移动节点频繁切换网络的应用场景。

5.2.2　移动节点注册

移动节点接入一个外地网络之后，首先从外地代理获得一个转交地址，然后将这个转交地址向家乡代理进行注册，以建立家乡地址与转交地址的移动绑定，这个过程称为“移动节点注册”。此后，家乡代理就能将通信对端发送给移动主机的分组，通过移动绑定建立的隧道转发给在外地漫游的移动主机。文档 RFC 3344 定义了移动 IPv4 的注册功能，它使用了两种注册报文：注册请求与注册应答。注册报文都作为载荷封装在 UDP 的数据部分，UDP 报文使用的目的端口号为 434。

移动节点的注册流程可分为以下 4 步。

① 注册请求发送：移动节点向家乡代理发送一个注册请求，其中包含必要信息(包括家乡地址、转交地址、注册有效期等)。如果转交地址是通过外地代理来获得，则注册请求需要经过外地代理的转发，外地代理可能添加附加信息(如自身地址)。两种注册报文需要通过认证机制(如共享密钥)验证合法性，防止伪造注册请求的拒绝服务攻击。

② 注册请求处理：家乡代理接收到注册请求之后，验证移动节点身份及注册信息的有效性。如果验证通过，家乡代理将移动节点的转交地址与家乡地址绑定，并在本地维护绑定缓存表，以记录移动节点的当前位置。家乡代理根据自身策略判断需要与外地代理建立隧道，还是直接更新自身的路由表。

③ 注册响应与隧道建立：家乡代理向移动节点发送一个注册确认报文，通知对方注册成功还是失败。如果注册确认经外地代理转发至移动节点，则外地代理需同时更新本地路由表以支持后续的数据转发。接下来，家乡代理与外地代理之间建立隧道，将发往移动节点的分组封装后通过隧道发送到外地代理，然后由外地代理拆封后通过本地链路交付给移动节点。

④ 注册维护与更新：在注册有效期到期之前，移动节点需要重新发起注册以更新有效期。如果移动节点切换至新外地网络，则需要重复上述流程以更新移动绑定。

5.2.3 移动节点的数据传输

隧道技术是移动 IP 实现跨网络通信的核心机制，通过封装与拆封机制保障移动节点在外地网络的通信连续性。当移动节点在外地网络中，家乡代理将发送给移动节点的分组转发给已注册的外地代理。这时，家乡代理利用隧道技术将原始分组作为载荷封装在转发分组中，从而使原始分组原封不动地到达隧道终点。外地代理将转发分组拆封后获得原始分组，并将原始分组转发到移动节点。当移动节点使用配置转交地址时，移动节点本身就是隧道终点，它将转发分组拆封后获得原始分组。

移动 IPv4 主要有两种隧道模式：完整封装与最小封装。其中，RFC 2003 文档定义了完整封装(IP in IP)模式，原始分组被完整封装在外层分组中，外层分组头的目的地址为移动节点的转交地址，源地址为家乡代理的地址。这种模式的优点是适应场景广泛；缺点是封装效率低(新增 20 字节开销)。RFC 2004 文档定义了最小封装(Minimal Encapsulation)模式，原始分组被部分封装在外层分组中，仅保留必要的封装信息(如原始分组的源地址与目的地址)。这种模式的优点是封装效率高(仅增加 8～12 字节)，适用于带宽敏感的应用场景；缺点是通信双方必须都支持该协议。

图 5-4 给出了移动节点通过隧道转发分组的过程。如果主机 A(通信对端)向主机 B(移动节点)发送一个分组，则原始分组的源地址是主机 A 的 IP 地址，目的地址是主机 B 的 IP 地址。当该分组发送到主机 B 的家乡代理时，主机 B 已漫游到外地网络。家乡代理接收到该分组之后，通过移动绑定查找主机 B 的转交地址。家乡代理为该分组加上外层分组头，源地址为隧道入口(家乡代理)地址，目的地址为隧道出口(外地代理)地址。分组的隧道传输过程经过多个路由器的转发，但是它们看不到主机 B 的家乡地址。外地代理将分组拆封后获得原始分组，并将其转发给主机 B。

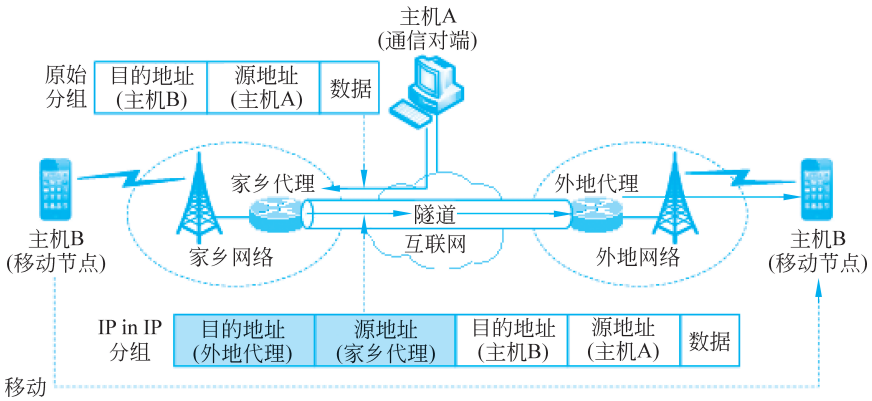

图 5-4 移动节点通过隧道转发分组的过程

5.2.4 MAC 地址解析

MAC 地址是数据链路层唯一的标识符，用于局域网中的设备之间的直接通信。在移动 IPv4 的应用场景中，当家乡代理或外部代理向移动节点转发数据，或者家乡代理通过隧道向外部代理转发数据时，需要解析目的设备的 MAC 地址以完成最终交付。家乡代理响应移动节点家乡地址的 ARP 请求，维护移动节点的 IP 地址与 MAC 地址绑定关系，确保发送到其家乡地址的分组能够被截获。外地代理通过代理 ARP 响应移动节点的转交地址相关请求，将分组拆封后基于 MAC 地址转发到移动节点。

MAC 解析在移动 IP 中具有以下特殊性。

- 地址绑定的动态性：移动节点在切换网络之后，其转交地址对应的 MAC 地址可能发生变化。当移动节点使用外地代理提供的转交地址时，数据链路层的目的地址为外地代理的 MAC 地址，外地代理基于移动节点的注册信息（如移动标识符）来转发数据。当移动节点直接使用配置转交地址时，需要通过本地 ARP 协议获取其当前的 MAC 地址。
- 跨网络通信的局限性：传统 ARP 仅适用于同一子网的 MAC 地址解析，移动 IP 要通过代理 ARP 或隧道封装实现跨子网的 MAC 地址解析。NAT 设备修改网络层的 IP 地址与传输层的端口号，可能导致 MAC 地址解析失效（如隧道分组外层地址被改写），需依赖 UPnP 或 STUN 协议穿透。

MAC 解析在典型场景中的工作流程如下。

① 移动节点注册：移动节点通过外地代理向家乡代理注册转交地址，建立 IP 地址与 MAC 地址的绑定关系。外地代理记录移动节点的 MAC 地址，并维护本地 ARP 缓存表（移动节点的转交地址与 MAC 地址的映射关系）。

② 分组投递：家乡代理截获发送给移动节点的分组，利用隧道技术将原始分组封装为隧道分组，外层分组头的目的地址为外地代理的地址或移动节点的转交地址。外地代理通过 ARP 解析外层分组头 IP 地址对应的 MAC 地址（外地代理的 MAC 地址或移动节点的当前 MAC 地址），完成数据链路层投递。

③ 本地拆封与转发：外地代理或移动节点拆封隧道分组，基于原始分组头的目的地址（移动节点的家乡地址）查找本地 MAC 地址表，最终交付至移动节点。

5.2.5 路由优化

移动 IPv4 方案中存在“三角路由”问题。在移动节点离开家乡网络之后，当通信对端向移动节点发送数据时，需要经过移动节点的家乡代理转发，而移动节点向通信对端发送数据时可以直接发送，导致了双向的传输路径不一致，形成了类似三角形的路径关系，这种现象称为“三角路由”。移动 IPv4 要求所有发往移动节点的数据必须通过家乡代理进行隧道封装与转发，而移动节点发出的数据可采用标准 IP 路由直接发送至通信对端，无须经过家乡代理，这是产生“三角路由”问题的根本原因。

“三角路由”问题主要缺点：

- 这种路由通常不是最优的，容易出现“绕路”现象，增加数据传输延时。
- 家乡代理可能因负荷太重而成为通信的瓶颈。

- 当移动节点移动到较远的地方时，节点注册的开销将会增大。

“三角路由”问题主要有以下两种解决方案。

- 路由优化机制：当家乡代理接收到通信对端发往移动节点的数据时，向通信对端发送绑定更新(Binding Update)，向其通知移动节点的转交地址。此后，通信对端将数据直接封装并发送至移动节点，避免绕行家乡代理。这种方案可减少路径跳数与延时，提升传输效率。
- 反向隧道技术：强制要求移动节点发往通信对端的数据也通过家乡代理转发。这种方案虽然保持了双向路径的对称性，但是增加了移动节点到家乡代理的传输开销。这种方案适用于有防火墙或 NAT 穿透的场景。

5.2.6 移动 IPv4 的工作过程

在讨论了移动 IPv4 基本内容的基础上，下面通过一个应用场景分析移动 IPv4 协议的工作过程。

1. 基本分析

在移动 IPv4 的应用场景中，两位用户使用手机通过办公室 Wi-Fi 网络进行通信，其中一位用户(手机 A)有事离开办公室，手机 A 从 Wi-Fi 网络切换到 5G 网络。这里，手机 A 是移动节点，手机 B 是通信对端，Wi-Fi 网络是家乡网络，5G 网络是外地网络。移动 IPv4 的工作过程涉及以下 4 个节点。

- 移动节点(MN)：手机 A，家乡地址(HoA)为 202.1.1.10，在外地网络中的转交地址(CoA)为 10.0.0.2。
- 通信对端(CN)：手机 B，IP 地址为 202.1.1.16。
- 家乡代理(HA)：位于家乡网络 202.1.1.0/24，IP 地址为 202.1.1.1。
- 外地代理(FA)：位于 5G 网络 10.0.0.0/24，IP 地址为 10.0.0.1。

移动节点(手机 A)从 Wi-Fi 网络移动到 5G 网络时，仍然与通信对端(手机 B)保持通信关系。移动 IPv4 协议在用户透明的情况下，完成了代理发现、注册与地址绑定，以及两台手机之间的数据传输。图 5-5 给出了移动 IPv4 的工作过程。

移动 IPv4 的工作过程可以分为以下几步。

(1) MN 获取新的 CoA。

MN 在家乡网络时，MN 与 CN 之间直接通信，家乡代理不干预数据传输过程。MN 在移动过程中发现 Wi-Fi 信号逐渐减弱，触发移动检测机制，开始扫描新网络，发现 5G 基站信号。MN 接入 5G 网络之后，通过两种方式获取 CoA：MN 提取 FA 的 IP 地址作为自己的 FA-CoA；如果 5G 网络中未部署外地代理，MN 可通过 DHCP 或静态配置直接获得临时 IP 地址(如 10.0.0.1)作为 Co-located CoA(Co-CoA)。

需要注意的是，MN 通过 FA 周期性广播的代理通告报文获取的 CoA，不一定是内网的私有 IP 地址，这要看外地网络的配置。FA 可以是公网地址，也可以是私有地址。私有地址 10.0.0.1 不能用于公网，当它作为隧道端点的 IP 地址时，必须采用 VPN 或 NAT 技术，确保跨越公网的可达性。如果 5G 网络运营商为 MN 分配的 FA-CoA 或 Co-CoA 是公网地址，则问题得到简化。

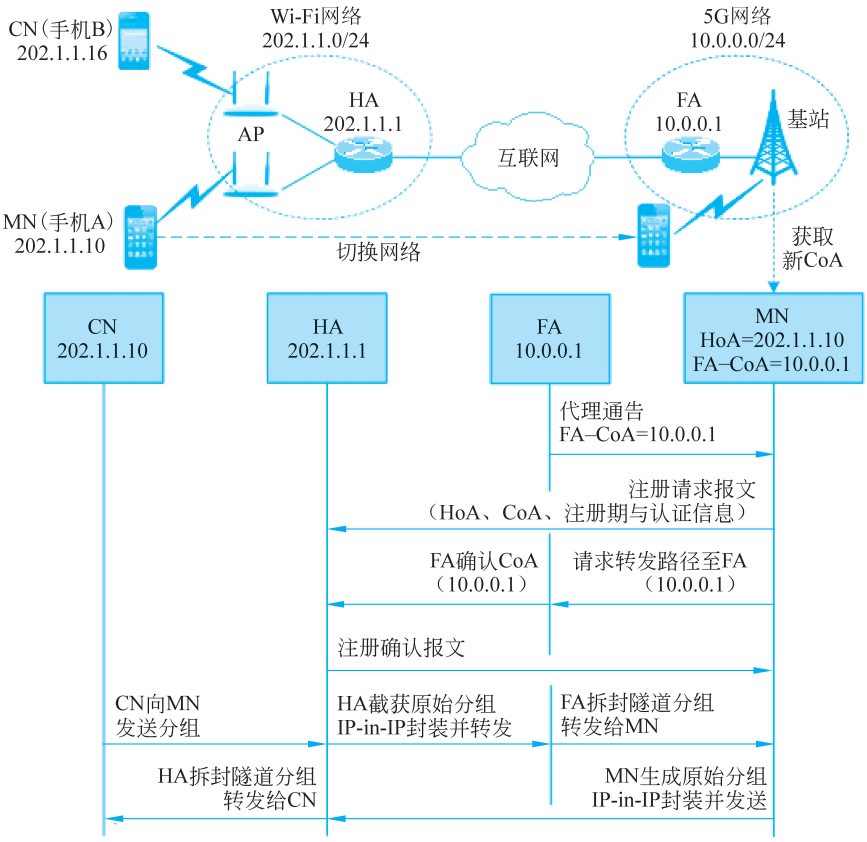

图 5-5　移动 IPv4 的工作过程

（2）MN 向 HA 注册 CoA。

首先，MN 生成注册请求报文，内容包括以下关键字段：HoA（202.1.1.10）、CoA（10.0.0.1）、注册有效期（如 3600s）及认证信息（如 MN-HA 共享的安全密钥）。然后，MN 通过 5G 网络将注册请求发送给 HA（202.1.1.1）。

（3）HA 处理注册请求。

首先，HA 验证注册请求的合法性，检查 MN 的认证码是否匹配。然后，MN 向 FA 发送请求转发路径到 10.0.0.1，FA 确认后将转发路径到 10.0.0.1 转发给 MA，确认 CoA 可达。接下来，HA 更新绑定表（Binding Cache），将 HoA（202.1.1.10）映射到新 CoA（10.0.0.1）。最后，HA 向 MN 发送注册应答报文，确认注册成功。注册 CoA 的过程约为几毫秒至几秒，可能导致短暂的通信中断。

（4）数据传输过程。

① CN 发送数据至 MN。

- CN 向 MN 发送原始分组，源地址 202.1.1.16，目的地址为 202.1.1.10。
- HA 拦截并采用 IP-in-IP 隧道封装原始分组，外层分组头的源地址＝202.1.1.1（HA），目的地址＝10.0.0.1（CoA）；内层分组头为原始分组（源地址＝202.1.1.16，目的地址＝202.1.1.10）。
- FA 收到隧道传送的分组之后，拆除外层分组头，将原始分组发送至 MN。