

移动 IP:支持移动计算的 IP 协议

张 腾 宋茂强 (北京邮电大学 293 信箱 100876)

摘要: 现今 Internet 上的网络层协议 IPv4 的路由算法不支持主机漫游, 为此 IETF 提出了一种新的基于现有 IP 协议的移动 IP 协议, 现在移动 IP 协议是被提议的 Internet 标准。本文首先简要讲述了该协议的要求、目标和原理, 然后对移动 IP 的应用进行了初步的探讨。

关键词: 移动 IP 移动计算网络 TCP/IP

1 前言

移动计算网络使得人们接入和使用网络变得非常方便, 但现今 Internet 上的网络层协议 (IPv4) 的路由算法不支持主机漫游。因为在 IPv4 中, 主机在网络中的位置是由其 IP 地址唯一确定的, 主机必须在网络中处于由其 IP 地址标识的地方才可以接收数据, 这种要求显然不适合移动计算网络中主机可随时随地漫游的情况, 所以有必要另外设计一种基于现有 IP 协议的能支持主机漫游的网络层协议, IETF 的 IP Routing for Wireless/Mobile Hosts 工作组对几个解决方案的优缺点进行分析后提出了一种新的协议—— Mobile IP (移动 IP) 协议, 现在移动 IP 协议是被提议的 Internet 标准。主机漫游软件的研发在国际上也是一个热点课题, 许多国际著名的研究机构都在进行这方面的研究。本文简述该协议的要求、目标和原理, 并对移动 IP 的应用进行了探讨。

2 移动 IP 协议

2.1 协议要求

移动 IP 协议的设计有如下要求:

- (1) 移动节点在改变其网络的链路层接入点后, 应可以在保持其 IP 地址不变的前提下, 继续和网络上的其他节点通信;
- (2) 移动节点必须只用其永久 IP 地址和其他节点通信, 而不管其当前在网络上的链路层接入点;
- (3) 移动节点必须能与其他没有移动功能的计算机通信;
- (4) 为防止远程重定向攻击, 对于那些改变移动节点当前位置记录的信息应进行认证。

2.2 协议目标

路由协议 (包括移动 IP) 在实现时需要在网络中的不

同节点之间发送路由更新信息。移动节点与网络的链接通常是无线链路, 无线链路与有线网相比是一个低带宽高误码率的链路, 为使移动 IP 适应大范围的无线链路环境, 在设计时就必须做到使这样的路由更新信息尽可能地少。还有另外一个设计目标是在移动节点上运行的软件要尽可能简单, 因为除了功能齐全的笔记本电脑用户, 对那些使用内存、处理器受限的设备诸如寻呼机、智能蜂窝电话、PDA 等的用户而言, 这一点非常重要。

2.3 协议原理

2.3.1 移动 IP 功能实体及其相互之间的关系

IETF 移动 IP 体系结构定义了三个功能实体: 本地代理、外地代理和移动主机。它们协调工作使得移动主机在移动时无须改变 IP 地址就可以接入网络。移动代理指的是具有本地代理或外地代理或两者功能的主机。如果一个网络安装有移动代理设备, 那么这个网络是支持主机移动的。移动 IP 功能实体及其相互之间的关系如图 1 所示。

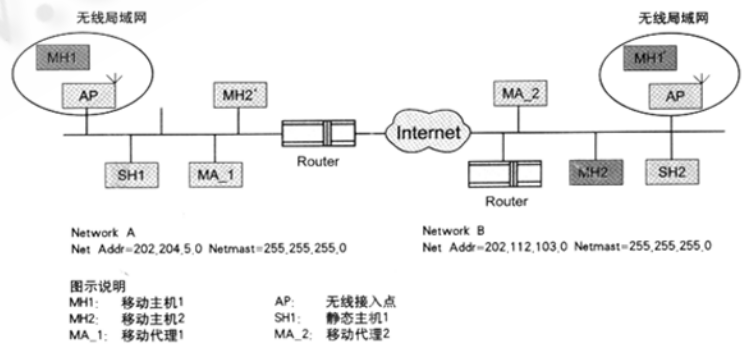


图 1 移动 IP 的功能实体及其相互之间的关系

图中, 移动主机 MH1 的本地网络是网络 A 的无线局域网, 当其漫游到网络 B (图中 MH1') 时, MA_1 充当

它的本地代理, MA_2 充当它的外地代理。同样, 移动主机 MH2 的本地网络是网络 B, 当其漫游到网络 A (图中 MH2') 时, MA_2 充当它的本地代理, MA_1 充当它的外地代理。

2.3.2 移动 IP 工作原理

在介绍移动 IP 的工作原理之前, 先引入几个专业名词。

永久地址 (Home Address): 是静态分配给移动主机 MH 的 IP 地址, 如同每台静态主机或路由器一样。当 MH 漫游到别的网络时, 永久地址不变, MH 用这个地址和其他主机通信。

转交地址 (Care-of Address): 当 MH 漫游到别的网络时, 它从外地代理 FA 处得到一个临时转交地址并通知其本地代理 HA。HA 把所有发给 MH 永久地址的数据报转发到 MH 的转交地址, 再由 FA 转发给 MH。

本地代理 (Home Agent): 是一个路由器, 周期性地发布代理广告。当 MH 漫游到别的网络时, HA 把所有发给 MH 永久地址的数据报截获下来重新打包后发到 MH 的转交地址。

外地代理 (Foreign Agent): 是一个路由器, 周期性地发布代理广告。向漫游过来的 MH 提供转交地址, 并转发由本地代理发来的数据报给 MH。同时外地代理也是 MH 发送数据报的缺省路由器。

代理搜寻 (Agent discovery): MH 确定自己是在本地网络还是外地网络的过程称为代理搜寻。实现代理搜寻有两种方法: 由移动代理发送代理广告 (Agent Advertisement) 的方法和由 MH 发送代理索求 (Agent Solicitation) 的方法。前者由移动代理周期性地发布代理广告, MH 收到该报文后判断自己的位置。后者由 MH 主动发布代理索求, 根据移动代理的响应报文判断自己的位置。

注册 (Registration): MH 获得转交地址后, 通知其 HA 并建立 HA 到 FA 隧道的过程叫注册。MH 通过 FA 向 HA 发送注册请求 (Registration request), HA 接收注册请求, 建立隧道, 向 MH 回复注册响应 (Registration reply)。

隧道 (Tunneling): 发给 MH 的数据报被 HA 截获并封装 (encapsulated) 后发给 FA。封装是指把源 IP 包用一个新的 IP 头重新打包, 源 IP 包作为新 IP 包的数据域, 不做任何改动。外层 IP 头的源和目的地址分别对应 HA 和 FA。这一工作机制称为隧道技术 (tunneling), 因为里层 IP 包对中间路由器来说是不可知的。

移动 IP 的工作过程可概括如下:

(1) 移动代理周期性地组播或广播代理广告;

(2) 移动节点监听这些代理广告并检查它们的内容判断当前链接的是本地链路还是外地链路。如果是本地链路, MH 将象其他静态节点一样对代理广告不作任何处理, 否则 MH 从代理广告中获取一个转交地址;

(3) MH 向本地代理注册其转交地址, 从安全上考虑, 注册信息要被认证;

(4) 本地代理截获发往 MH 的数据报并通过隧道转发到 MH 的转交地址;

(5) 外地代理从隧道中取出数据报并转发给 MH, 同时作为 MH 发送数据报的缺省路由器;

下面结合图 1 举例说明移动 IP 工作原理。

在图中, 移动主机 MH2 的本地网络是网络 B。当它接入到网络 A 后, 成为 A 的访问主机 MH2', 此时 MA_2 充当 MH2 的本地代理, MA_1 充当 MH2 的外地代理。MH2' 监听 MA_1 周期性发布的代理广告, 判断自己不在本地网络, 从代理广告中获得一转交地址。MH2' 通过 MA_1 向 MA_2 注册其转交地址, MA_2 告知 MH2' 注册成功。当网络 B 中的静态主机 SH2 向 MH2' 发送数据时, MA_2 通过代理 ARP (Proxy-ARP) 截获这个数据报, 重新封装 (encapsulated) 后发给 MA_1, MA_1 接收这个数据报解封装 (decapsulated) 后转发给 MH2'。当 MH2' 向 SH2 发送数据时, MA_1 充当其缺省路由器, 把数据报转到网络 B。

2.3.3 移动 IP 的协议数据格式

移动 IP 定义的协议数据都是由一个固定长度的信息部分外加一个或多个扩展 (extension) 构成。这些扩展部分可以让现存的协议携带许多有用的信息, 这为以后设计新的移动 IP 应用提供了一个框架, 非常便于扩展。移动 IP 的扩展部分具有相同的格式, 它们都是由三个部分组成: Type、Length 和 Data。

· Type 域表识本扩展的类别, 比如 Type=16 是移动代理广告扩展;

· Length 域是 Data 域的字节数;

· Data 域是协议信息内容。

这种格式通常被称为 TLD 编码 (Type-Length-Data), 在许多 Internet 协议和标准中普遍使用。

移动 IP 的代理搜寻过程建立在现存的标准协议 RFC1256.9 路由器广告 (Router Advertisement) 之上。代理搜寻没有修改 ICMP 路由器广告的报文内容, 只是增加了和移动功能有关的扩展。这样带有转交地址扩展的路由器广告就成为了代理广告。代理索求和 RFC1256 路由器索求 (Router Solicitations) 完全相同 (除了 TTL)。

移动IP的注册过程由两条消息组成:注册请求和注册响应,用UDP作为传输方式.为保护注册信息不被修改和伪造,在进行注册时,移动节点和本地代理必须共享一个安全协商(Security association),并使用128位密钥的MD5(RFC1321)加密算法.注册报文有以下几种扩展:移动节点-本地代理认证扩展、移动节点-外地代理认证扩展、本地代理-外地代理认证扩展.这些扩展字段的目的是在注册交互过程中保证注册信息不被修改和伪造.

3 移动IP的应用

下面举两个例子来说明移动IP的应用.

第一个是有线以太网的例子,这个例子有一定的代表性,适合把校园网、大公司内网升级为支持主机移动的移动计算网络(如图2).在图中,每个部门的局域网都留有接入端口,这样别的部门的机器就可以直接接入到网络中而不需要更改IP地址.比如在一个会议室,参加会议的相关人员可以直接把笔记本电脑接入到网络中.网络管理员要做的工作是:

- (1) 把移动节点软件安装在笔记本电脑上;
- (2) 在路由器上安装本地代理和外地代理软件,也可以安装在每个子网的PC机或工作站上;
- (3) 为每个移动节点和本地代理之间配置一个共享密钥,以便在注册过程中对注册信息进行认证.

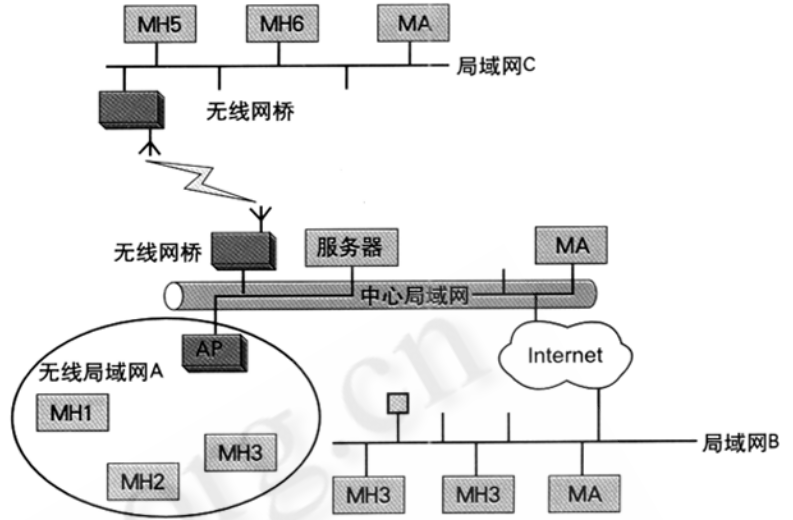


图3 移动IP应用举例2

图中无线局域网A中的移动主机通过无线接入点AP接入到中心局域网中.这些移动主机(MH1、MH2、MH3)都安装有无线网卡,通过无线上网.局域网B在地理上可以和中心局域网相距很远,移动代理MA支持连接在中心局域网上的主机漫游过来而不改变IP地址.局域网C和中心局域网通过无线网桥以无线的方式相连,无线网桥间的传输速率可达11Mbps.安装有移动节点软件的移动主机MH可以在局域网A、B、C中随意接入.■

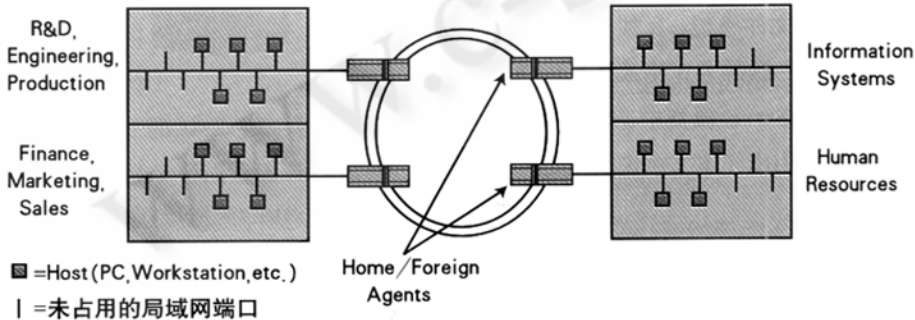


图2 移动IP应用举例1

下面再举例说明一个无线局域网的例子,这个例子适合组建临时性网络,如野外作业、临时流动会议等,同样它也适合组建无线校园网,这样学生手持一台便携式,在校园范围内,无论在教室、宿舍都能连上学校的主网(图3).

参考文献

- 1 "IP Mobility Support", C.Perkins, ed., RFC 2002, Oct.1996
- 2 "IP Encapsulation Within IP", C. Perkins, RFC 2003, May 1996
- 3 "Mobile IP The Internet Unplugged", James D.Solomon, Prentice Hall PTR, 1998
- 4 "Mobile Networking Through Mobile IP", C.Perkins, Sun Microsystems, 1998