IP 地址映射到物理地址的若干问题

金培权 （天津财经学院信息系 300222）

摘要：TCP/IP 协议屏蔽了网络底层的通信细节，但在物理网络上发送 IP 数据报时，最终的通信必须通过硬件提供的编址方案（物理地址）进行。本文探讨了在基于 TCP/IP 的网络/互联网络上，IP 地址映射到硬件物理地址时的若干种实现方法和相关的问题，着重讨论了 ARP 协议的实现原理和存在的问题。

关键词：TCP/IP IP 地址 物理地址 映射 ARP

一、引言

TCP/IP 协议之所以能够成为世界范围内的网络互联标准协议，其根本原因在于它屏蔽了底层不同物理网络上的通信细节，使得用户在使用 TCP/IP 进行通信时，不用去管目的节点的网络类型。TCP/IP 的这一特性使全球所有互联的网络（典型的例子是 Internet）成为一个单一的“虚拟网”。这对用户通信的好处是不言而喻的。举一个例子，一个令牌环网的用户（节点）在向一个远程以太网的用户（节点）发送数据时，它不用去管令牌环数据包如何传到以太网上以及以太网如何接收一个令牌环数据包。它只要知道目的以太网节点的 IP 地址就可以了，剩下的任务则交给 TCP/IP 协议去完成。

尽管 TCP/IP 协议使得用户通信更为方便了，但仍有许多技术上的问题值得探讨。TCP/IP 协议是通过软件来实现的，它在通信时对通信双方都隐藏物理地址，使得通信双方只需用高层 IP 地址进行通信即可。但是从通信技术上分析，使用高层的 IP 地址进行通信时，最终的物理上的通信还是必须通过硬件提供的编址方案（物理地址）来进行。这是因为实际的通信是通过底层的物理网络（如以太网、令牌环网、FDDI 等）使用各自的通信机制进行通信的。如果在一个物理网络上简简单单地不加以任何转换地发送一个 IP 数据报，那么目的节点将无法识别 IP 数据报中的信息。例如，以太网上的数据传输是通过发送和接收以太网帧来进行的。以太网帧包含源节点地址和目的节点地址，这两者都是 MAC（Media Access Control，介质访问控制）地址，MAC 地址是以太网节点的物理地址。如果将一个 IP 数据报像发送一个以太网帧一样直接地发送给一个以太网节点，那么即使该节点能够读取 IP 数据报中的地址信息，它也判断不了 32 位 IP 地址究竟代表着哪一个节点。要使得它能够判断，必须建立一种 IP 地址到 MAC 地址的映射，使得节点在使用 IP 地址发送数据时，可以根据 IP 地址找到相对应的物理地址，从而实现物理上的通信。这种地址转换问题不仅在以太网上存在，在任何一个使用 TCP/IP 协议的物理网络上都存在。这里需明确指出的是，TCP/IP 是网络层协议，而物理网络上的通信则使用数据链路层协议和物理层相关技术。例如以太网使用的是 CSMA/CD 协议，相关的物理层技术有 10－BASE5、10－BASE2 等，但它使用的网络层协议可能是 IP 协议。

实际上，基于 TCP/IP 协议的网络在通信时，是将 IP 数据报封装到物理网络帧上进行的。关于 IP 数据报发送的细节超出了本文讨论的范围，这里不加以叙述。我们关心的是：在使用 IP 地址进行通信的节点之间，它们是如何将各自的 IP 地址与各自的物理地址映射起来，从而实现物理通信的。假设 A 节点要向 B 节点发送数据，但 A 节点只知道 B 节点的 IP 地址，那么 A 节点是如何将 B 节点的 IP 地址映射到 B 节点的物理地址上的呢？假设 A、B 节点在同一物理网络上，那么情况可能稍微简单一些，但是如果 A、B 节点在不同的物理网络上，那么就出现了多级映射的问题，这又是如何解决的呢？接下将探讨 IP 地址映射成物理地址的实现问题。下面分四部分进行讨论：首先讨论实现 IP 地址映射的三种不同方法及利弊，着重探讨了 ARP 协议的有关问题；然后讨论直接映射和多级映射的有关问题。

二、静态地址映射

所谓静态地址映射，指的是在各个网络节点上都保存一张 IP 地址映射表，表中的每一项指明了一个 IP 地址与一个物理地址的对应关系。这种方法的实现思路很简单。在只有少量节点的网络上，使用这种方法实现起来也比较容易。但它的缺点也很明显。以以太网为例：(1)如果新增或删除了某个节点，那么各个节点的地址映射表都需要更新；(2)如果某个节点的网卡出了故障，因而进行了更换，那么各个节点的地址映射表也要修改相应的表项；(3)如果网络节点大量增加，那么维护地址映射表的工作也将急剧增加；(4)如果将该以太网与其他物

理网络互联，那么想在每个节点上都保存和维护一张地址映射表是荒谬的。

所以静态地址映射充其量也只能适合只有少量节点的局域网。在大型网络或进行网际互联时，这种方法是不可行的。

三、函数式地址映射

这种方法的思路是在 IP 地址和物理地址之间建立一种函数关系，知道了 IP 地址后，就可以根据这种函数关系计算出相应的物理地址。比如在一个 C 类的 IP 网络上，就可以提取 IP 地址中的主机地址，并根据主机地址确定物理地址。可以举一个例子，Pronet 是一种令牌环技术，这种技术允许用户自己选择节点的物理地址，而不是像以太网那样由厂商分配。在 Pronet 网卡上有 8 个跳线，根据跳线设置可选择 0 到 255 的一个物理地址。那么在 Pronet 上建立 C 类网络时，可以建立这样的函数关系：节点的物理地址 = 节点 IP 地址中的主机地址。例如 IP 地址为 174.52.6.1 的节点，它的物理地址就等于 1。在其他物理网络上，也可以设计一个函数，使得 IP 地址能映射到物理地址上。这种方法在理论上似乎是可行的，但是实际中：首先是选择这样一个函数本身就是一件十分困难的事情；另一个是在一些物理网络上，节点的物理地址是一个有限的集合，比如一个 30 个节点的以太网只有 30 个物理地址，而 IP 地址的集合则可能比物理地址的集合大得多；又因为 IP 地址是用户自己分配的（网络部分除外），所以要在随意分配的 IP 地址与有限的物理地址之间建立函数映射存在很大的困难，况且还要考虑网络节点的增删以及网络互联等复杂情况；第三方面是在一些物理地址位数比 IP 地址位数小的物理网络中（如 Pronet），根据 IP 地址计算物理地址相对容易，而在物理地址位数大于 IP 地址位数的物理网络中（如以太网 MAC 地址为 48bit），要从 32 位的 IP 地址中计算出 48 位的物理地址是无法实现的。

函数式地址映射的优点是方便和高效。另外，选定一个好的函数后，在增加节点时也不需要改变已有的 IP 地址分配或重新编译代码。

四、ARP 动态映射

由于前两种方法或多或少都存在着难以避免的缺点，因此最终都被 ARP 取代了。ARP（Address Resolution Protocol，地址解析协议或地址转换协议）已成为 TCP/IP 协议族中的重要一员。现在运行的 Internet 上的节点都使用 ARP 进行地址映射。ARP 可看成是一种动态地址映射方法。它允许节点在只知道同一物理网络上的目的节点的 IP 地址的情况下，找到目的节点的物理地址。

1. ARP 的工作原理

ARP 的动态思路可如下所述：当发送节点 A 要转换目的节点 B 的 IP 地址 IB 时，它就广播一个特殊的分组，要求 IP 地址为 IB 的节点用它的物理地址 PB 响应它。包括 B 在内的所有节点都收到了这个请求，但只有 B 识别出它的 IP 地址并且发回一个包括它自己物理地址的应答。当 A 收到应答后，就可以使用 B 的物理地址将数据发送给 B 了。

实际当中，并非每个节点在发送分组之前都要发送一个广播。如果真是这样，那么通信的费用就太昂贵了。实际上，每一个 ARP 的节点都保留了 ARP 高速缓存，用于保存最近获得的 IP 地址与物理地址对。这样，在每次发送分组之前，节点都先去查询自己的 ARP 高速缓存，如果找到了所需的 IP 地址与物理地址的映射，就不需发送广播了。由于网络通信倾向于成对的节点之间的通信，所以 ARP 高速缓存免去了许多 ARP 请求。

2. ARP 报文的封装和标识

ARP 请求和应答都是通过发送 ARP 报文来实现的。当发送一个 ARP 报文时，如前所述，也必须通过物理网络来进行传递。这时的做法是 ARP 报文作为物理网络帧数据封装到物理网络帧当中去，如下图所示：

为了识别携带有 ARP 报文的帧，发送节点给带有 ARP 报文的帧的帧首部的类型字段分配一个特殊的值，当帧到达某个节点时，该节点根据帧类型确定该帧是否携带有 ARP 报文，并据以处理。例如，在以太网中，带有 ARP 报文的帧类型字段为 080616，这个值在所有以太网帧中都是统一使用的。

3. ARP 的实现过程

ARP 的实现过程分为 IP 地址映射和 ARP 报文处理两个过程。

（1）IP 地址映射。发送节点在发送 ARP 报文（请求/应答）之前，先根据目的节点的 IP 地址查询自己的 ARP 高速缓存，若找到了 IP 地址相应的的物理地址，就提取该物理地址并和数据一起放入帧中，然后发送；若没找到，则发送一个 ARP 请求，并等待应答。

（2）ARP 报文的处理。当一个 ARP 报文到达时，节点首先提取发送节点的 IP 地址与物理地址对，然后检查本地 ARP 高速缓存中是否有该发送方的地址对，若有，

则用提取的物理地址覆盖 ARP 高速缓存中原先的物理地址；若无，则生成一个新的表项。然后：

·若到达的是一个 ARP 请求，则判断是否为自己请求的目标（通过比较 IP 地址）。若是，则用本地的物理地址形成应答，并发送给请求节点；若不是，则忽略该报文；

·如果到达的是一个 ARP 应答，则首先看自己是否曾发出 ARP 请求，若没有，则忽略；若有，则如果到达的 ARP 应答是自己所要的应答，就提取应答中的物理地址，并和数据一起放入帧中进行发送；若不是自己想要的应答，则忽略。

4. ARP 存在的问题

（1）由于 ARP 缓存不可能太大，因此在有大量节点和节点间通信的网络上，ARP 报文的发送和接收将十分繁忙，造成整个网络通信效率的降低。

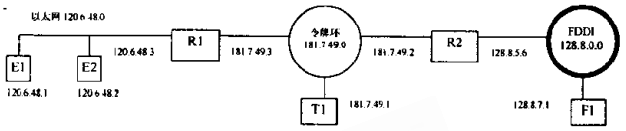
（2）由于任何节点都可以广播 ARP 请求，因此 A 节点可能会使用 B 节点的 IP 地址和自己的物理地址作为 ARP 请求中的源地址进行发送，这个 ARP 请求广播后，所有其它节点都会认为是 B 的物理地址更改了，因此都会以 A 的物理地址去覆盖 ARP 高速缓存中的 B 的物理地址。这样，在 B 发送下一个 ARP 报文之前，所有发送给 B 的分组实际上都会被 A 截取。所以，ARP 是网络安全性的一个弱点。

（3）在节点向一个不存在的 IP 地址发送数据时，尤其是向像以太网这样不能处理广播数据包的网络发送时，将会造成大量的无效的广播。例如，假设 127.5.46.1 到 127.5.46.10 是十个节点组成的一个以太网 E，如果远程的一个节点向 127.5.46.11 发送数据，那么路由器在路由时会根据此地址的网络部分将数据路由 E 中，由于 E 中不存在 127.5.46.11 这个节点，因此 E 会向自己网络中的所有节点都广播该数据包，这种广播造成了 E 中的额外的通信占用。

五、直接映射和多级映射

当通信双方节点 A、B 在同一个物理网络上时，发送节点 A 可以使用 ARP 直接请求 B 的物理地址，然后再直接发送。而当 A、B 不在同一个物理网络上时，A 不能直接向 B 发送数据，必须借助于若干个路由器才能发送，此时，A 首先要请求与自己相连的最近的路由器的物理地址，然后将数据发往该路由器，再由该路由器去完成后面的路由和继续发送工作。那么，在前者中，A 直接请求目的节点 B 的物理地址，称为直接映射；而后者，A 要向 B 发送数据，必须经过多级路由器与节点、路由器与路由器之间的地址映射，这称为多级映射。看下面的例子：

E1、E2 节点连入一个以太网，组成一个 C 类网络；T1 连入一个令牌环网，组成一个 C 类网络；F1 连入一个 FDDI，组成一个 B 类网络；路由器 R1 连接以太网和令牌环网；R2 连接令牌环网和 FDDI。



（1）若 E1 要向 E2 发送数据，则可直接发送 ARP 请求，寻找 E2 的物理地址，E2 应答后，E1 即可直接向 E2 发送，这属于直接映射；

（2）若 E1 要向 F1 发送 IP 数据报，则首先需进行 ARP 请求，请求最近 R1 的物理地址，然后将 IP 数据报封装到以太网帧中发送给 R1，R1 接收数据后，将 IP 数据报从以太网帧中提取出来，然后进行路由，确定下一个路由器为 R2，于是请求 R2 的物理地址，收到应答后，再将 IP 数据报封装到令牌环帧中发送给 R2，R2 接收数据后，提取出 IP 数据报，发现已与目的节点 F1 处于同一物理网络上，于是进行直接映射。这就是多级映射的例子。

发送节点在确定是否与目的节点同在一个物理网络上时，只需提取各目的 IP 地址中的网络部分进行比较即可。这也是 IP 地址的一大优点。

六、结束语

以上是作者对 IP 地址向物理地址映射问题的一些见解。深入掌握 IP 地址向物理地址映射的技术原理，对于理解基于 TCP/IP 的网络或网际互联具有十分重要的意义。IP 地址映射问题是 TCP/IP 研究中的核心问题之一，作者也希望以后能进一步地就相关问题进行有价值的探讨。

参考文献

[1] Douglas. E. Comer，林瑶等译，用 TCP/IP 进行网际互联－－第一卷：原理、协议和体系结构（第三版），电子工业出版社，1998/4

[2] Robert Breyer, Sean Riley 著，肖文贵等译，新版交换式以太网和快速型以太网，电子工业出版社，1997/9

[3] Novell 著，网络基础教程，电子工业出版社，1996/10

[4] 胡道元，计算机局域网（第二版），清华大学出版社，1996/12

（来稿时间：1998 年 11 月）