TCP-IP 学习笔记之 ARP(地址解析协议)

一、引言

当一台主机把以太网数据帧发送到位于同一局域网上的另一台主机时，是根据 48 bit 的以太网地址来确定目的接口的（即物理地址）。设备驱动程序从不检查 I P 数据报中的目的 I P 地址。

地址解析为这两种不同的地址形式提供映射： 32 bit 的 I P 地址和数据链路层使用的任何类型的地址。

ARP 与 RARP 的区别：

ARP 为 IP 地址到对应的硬件地址之间提供动态映射。此过程是自动完成的，一般应用程序用户或系统管理员不必关心。

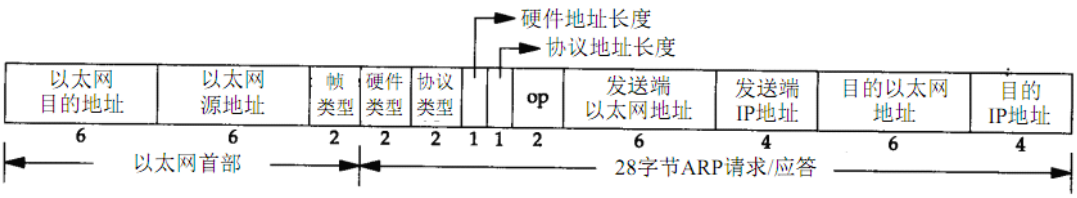
RARP 是被那些没有磁盘驱动器的系统使用（一般是无盘工作站或 X 终端），它需要系统管理员进行手工设置。

注：在 ARP 背后有一个基本概念，那就是网络接口有一个硬件地址（一个 48 bit 的值，标识不同的以太网或令牌环网络接口）。在硬件层次上进行的数据帧交换必须有正确的接口地址。但是，TCP/IP 有自己的地址：32 bit 的 IP 地址。知道主机的 IP 地址并不能让内核发送一帧数据给主机。内核（如以太网驱动程序）必须知道目的端的硬件地址才能发送数据。ARP 的功能是在 32 bit 的 IP 地址和采用不同网络技术的硬件地址之间提供动态映射。

点对点链路不使用 ARP。当设置这些链路时（一般在引导过程进行），必须告知内核链路每一端的 IP 地址。像以太网地址这样的硬件地址并不涉及。

二、ARP 的分组格式

在以太网上解析 IP 地址时，ARP 请求和应答分组的格式如图 1 所示（ARP 可以用于其他类型的网络，可以解析 IP 地址以外的地址。紧跟着帧类型字段的前四个字段指定了最后四个字段的类型和长度）。



(图 1)用于以太网的 ARP 请求或应答分组格式

①以太网目的地址

占 6 字节，目的地址为全 1 的特殊地址是广播地址。电缆上的所有以太网接口都要接收广播的数据帧。

②以太网源地址

占 6 字节，为发送端的物理地址

③帧类型

占 2 字节，表示后面数据的类型。对于 ARP 请求或应答来说，该字段的值为 0x0806。

④硬件类型

占 2 字节，硬件类型字段表示硬件地址的类型。它的值为 1 即表示以太网地址。

⑤协议类型

占 2 字节，协议类型字段表示要映射的协议地址类型。它的值为 0x0800 即表示 IP 地址。它的值与包含 IP 数据报的以太网数据帧中的类型字段的值相同。

⑥硬件地址长度

占 1 字节，指出硬件地址的长度，以字节为单位，对于以太网上 IP 地址的 ARP 请求或应答来说，它们的值为 6。

⑦协议地址长度

占 1 字节，指出协议地址的长度，以字节为单位，对于以太网上 IP 地址的 ARP 请求或应答来说，它们的值为 4。

⑧op 操作字段

占 1 字节，操作字段指出四种操作类型，它们是 ARP 请求（值为 1）、ARP 应答（值为 2）、RARP 请求（值为 3）和 RARP 应答（值为 4）。注：这个字段必需的，因为 ARP 请求和 ARP 应答的帧类型字段值是相同的。

⑨发送端以太网地址

占 6 字节，与以太网源地址一致。

⑩发送端 IP 地址

占 4 字节。

⑾目的以太网地址

占 6 字节。

⑿目的 IP 地址

占 4 字节。

备注：

①在以太网的数据帧报头中和 ARP 请求数据帧中都有发送端的硬件地址。

②对于一个 ARP 请求来说，除目的端硬件地址外的所有其他的字段都有填充值。当系统收到一份目的端为本机的 ARP 请求报文后，它就把硬件地址填进去，然后用两个目的端地址分别替换两个发送端地址，并把操作字段置为 2，最后把它发送回去。

③由于 ARP 请求或回答的数据帧长都是 42 字节（28 字节的 ARP 数据，14 字节的以太网帧头），因此，每一帧都必须加入填充字符以达到以太网的最小长度要求：60 字节。

这个最小长度 60 字节包含 14 字节的以太网帧头，但是不包括 4 个字节的以太网帧尾。有一些书把最小长度定为 64 字节，它包括以太网的帧尾。

作者：tdyizhen1314

(现从事 LED 行业，专注于户外大型 LED 显示屏控制系统的研发，希望与大家一起交流，共同进步)

邮箱：495567585@qq.com

td.logic@hotmail.com