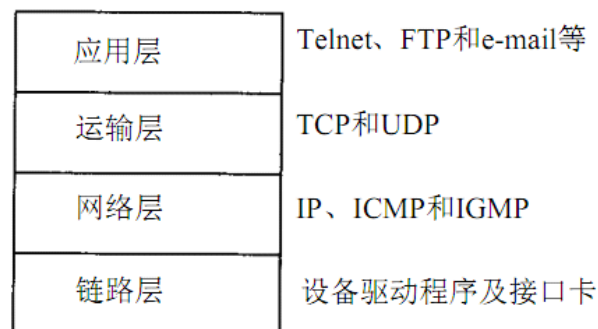


## TCP/IP 学习笔记之概述

### 1、分层

网络协议通常分不同层次进行开发，每一层分别负责不同的通信功能。一个协议族，比如 TCP/IP，是一组不同层次上的多个协议的组合。TCP/IP 通常被认为是一个四层协议系统，其示意图如下：



（图 1）TCP/IP 协议族的四个层次

每一层负责不同的功能：

- 1) 链路层：有时也称作数据链路层或网络接口层，通常包括操作系统中的设备驱动程序和计算机中对应的网络接口卡。它们一起处理与电缆（或其他任何传输媒介）的物理接口细节。
- 2) 网络层：有时也称作互联网层，处理分组在网络中的活动，例如分组的选路。在 TCP/IP 协议族中，网络层协议包括 IP 协议（网际协议），ICMP 协议（Internet 互联网控制报文协议），以及 IGMP 协议（Internet 组管理协议）。
- 3) 运输层：主要为两台主机上的应用程序提供端到端的通信。在 TCP/IP 协议族中，有两个互不相同的传输协议：TCP（传输控制协议）和 UDP（用户数据报协议）。

TCP 为两台主机提供高可靠性的数据通信。它所做的工作包括把应用程序交给它的数据分成合适的小块交给下面的网络层，确认接收到的分组，设置发送最后确认分组的超时时钟等。由于运输层提供了高可靠性的端到端的通信，因此应用层可以忽略所有这些细节。

而另一方面，UDP 则为应用层提供一种非常简单的服务。它只是把称作数据报的分组从一台主机发送到另一台主机，但并不保证该数据报能到达另一端。

任何必需的可靠性必须由应用层来提供。

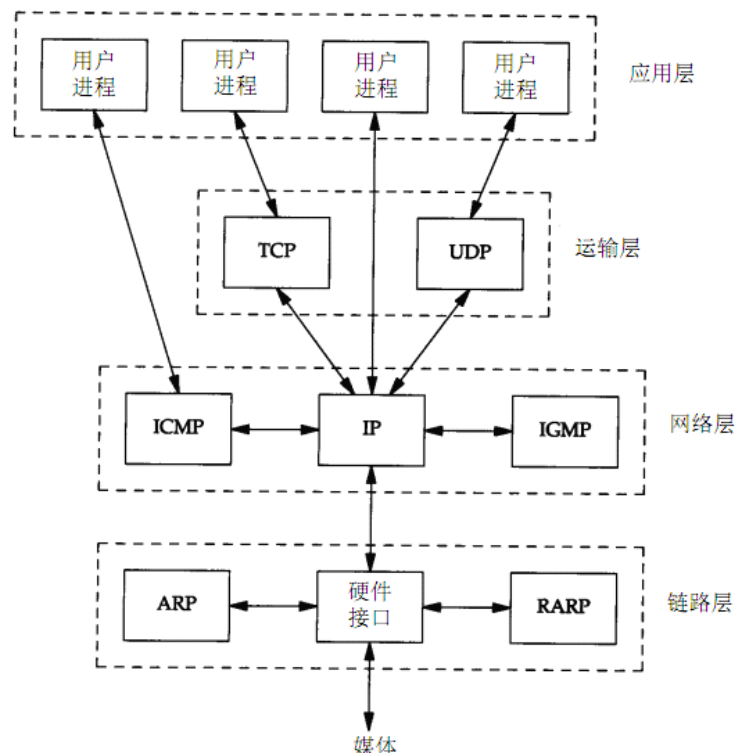
注：这两种运输层协议分别在不同的应用程序中有不同的用途。

4) 应用层：负责处理特定的应用程序细节。几乎各种不同的 T C P / I P 实现都会提供下面这些通用的应用程序：

- Telnet、FTP 和 e-mail 等
- FTP 文件传输协议。
- SMTP 简单邮件传送协议。
- SNMP 简单网络管理协议。
- ...

## 2、TCP/IP 的分层

在 T C P / I P 协议族中，有很多种协议。



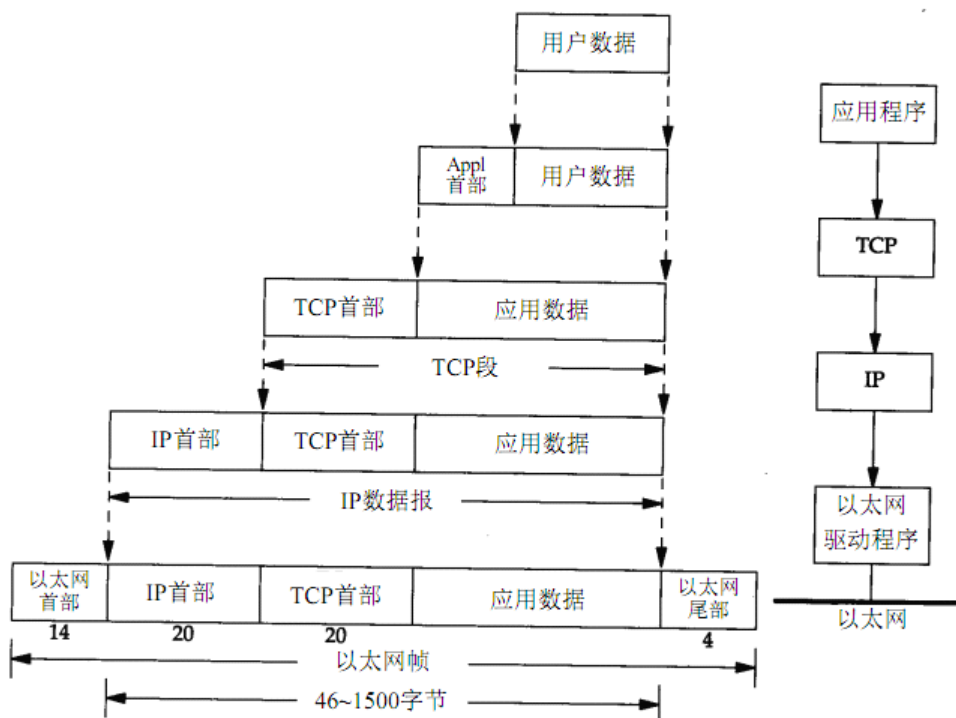
(图 2) TCP/IP 协议族中不同层次的协议

## 3、数据的封装

当应用程序用 T C P 传送数据时，数据被送入协议栈中，然后逐个通过每一层直到被当作一串比特流送入网络。其中每一层对收到的数据都要增加一些首部信息（有时还要增

加尾部信息），该过程如图 3 所示。TCP 传给 IP 的数据单元称作 TCP 报文段或简称为 TCP 段（TCP segment）。IP 传给网络接口层的数据单元称作 IP 数据报（IP datagram）。通过以太网传输的比特流称作帧（Frame）。

以太网数据帧的物理特性是其长度必须在 46~1500 字节之间。分组既可以是一个 IP 数据报，也可以是 IP 数据报的一个片（fragment）。



（图 3）数据进入协议栈时的封装过程

UDP 数据与 TCP 数据基本一致。唯一的不同的是 UDP 传给 IP 的信息单元称作 UDP 数据报（UDP datagram），而且 UDP 的首部长为 8 字节。

由于 TCP、UDP、ICMP 和 IGMP 都要向 IP 传送数据，因此 IP 必须在生成的 IP 首部中加入某种标识，以表明数据属于哪一层。为此，**IP 在首部中存入一个长度为 8 bit 的数值，称作协议域。**1 表示为 ICMP 协议，2 表示为 IGMP 协议，6 表示为 TCP 协议，17 表示为 UDP 协议。

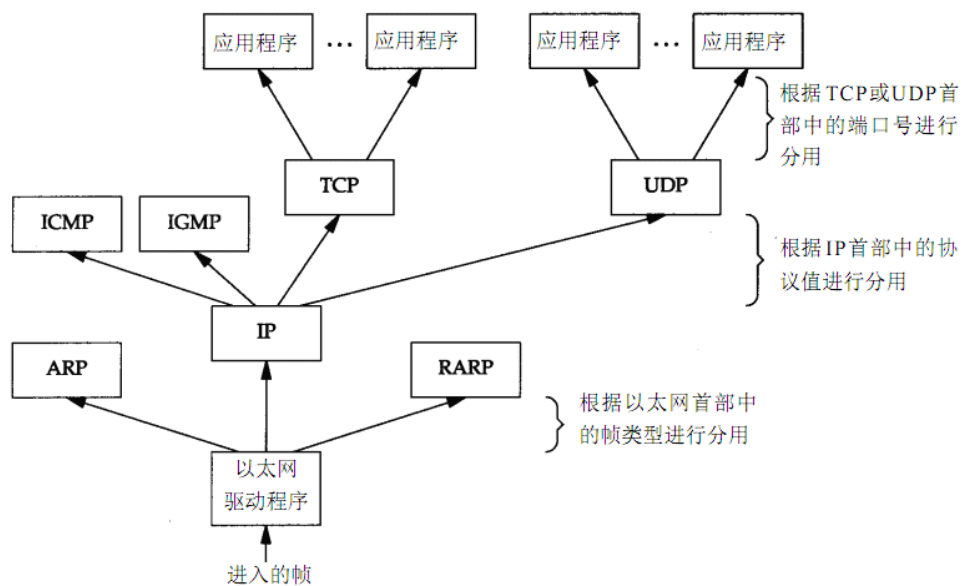
类似地，许多应用程序都可以使用 TCP 或 UDP 来传送数据。运输层协议在生成报文首部时要存入一个应用程序的标识符。**TCP 和 UDP 都用一个 16 bit 的端口号来表**

示不同的应用程序。**TCP** 和 **UDP** 把源端口号和目的端口号分别存入报文首部中。

网络接口分别要发送和接收 IP、ARP 和 RARP 数据，因此也必须在以太网的帧首部中加入应用程序某种形式的标识，以指明生成数据的网络层协议。为此，以太网的帧首部也有一个 16 bit 的帧类型域。

#### 4、以太网数据帧的分用

当目的主机收到一个以太网数据帧时，数据就开始从协议栈中由底向上升，同时去掉各层协议加上的报文首部。每层协议盒都要去检查报文首部中的协议标识，以确定接收数据的上层协议。这个过程称作分用（Demultiplexing），图 4 显示了该过程是如何发生的。



（图 4） 以太网数据帧的分用过程

为协议 ICMP 和 IGMP 定位一直是一件很棘手的事情。在(图 2)中，把它们与 IP 放在同一层上，那是因为事实上它们是 IP 的附属协议。但是在这里，我们又把它们放在 IP 层的上面，这是因为 ICMP 和 IGMP 报文都被封装在 IP 数据报中。

对于 ARP 和 RARP，在这里把它们放在以太网设备驱动程序的上方，这是因为它们和 IP 数据报一样，都有各自的以太网数据帧类型。但是有时又把 ARP 作为以太网设备驱动程序的一部分，放在 IP 层的下面，其原因在逻辑上是合理的。

对于解包 T C P 时，是通过目的端口号、源 I P 地址和源端口号进行解包。

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](mailto:495567585@qq.com)

[td.logic@hotmail.com](mailto:td.logic@hotmail.com)