《计算机网络》讲义要点

第六章 数据链路层

赵增华
天津大学智能与计算学部
2023 年春季

参考教材：

“Computer networking: a top-down approach”, by Jim Kurose, Keith Ross, Pearson, 8th Edition, 2021 年。

辅助教材：“Computer Networks”, 第 5 版英文影印版 ,A. Tanenbaum, 清华大学出版社, 2011 年。

教学目标：

通过对 Internet 经典协议的学习和剖析，让学生理解网络系统设计、网络协议设计所面临的问题和常用的解决方法。课程结束后学生能够根据工作/科研的需要设计、实现相应的网络系统和协议，并进行性能评价。授课过程中强调对问题的描述（why），然后是解决方案（how）。

学习方法：

学而不思则罔，思而不学则殆。

多读，多思，多实践。

多读：通过大量阅读理解网络、协议的基本概念，原理。阅读推荐的教材、参考书、自行在网上查找的相关内容。

多思：思考为什么。网络系统/每层（个）协议设计面临什么问题？如何解决？为什么？

多实践：1）通过网络协议分析软件（如 Wireshark）深入理解各层协议的执行过程。（WiresharkLab）

2）通过设计、实现网络协议，掌握协议的设计方法和实现技术。（Socket programming, RDT, routing protocol）

3）通过网络构建、配置，理解网络的实际部署和管理。（Lab Practice）

第六章 数据链路层

1. 理解链路层的功能。（6.1）

数据包到达网络层后，网络层根据数据包的目的 IP 地址查找转发表，找到对应的下一跳（next hop）节点的 IP 地址和输出端口（输出网卡）。把数据包转发到输出端口，传给相应数据链路层处理。

数据链路层收到网络层下发的数据包后，负责竞争到信道，以便能够把数据包传给下一跳节点。为此主要完成如下功能：

1） 链路访问（link access）：发送数据包前节点需要获得链路的访问权，即竞争使用信道。链路是相邻两个节点（点到点链路 point-to-point link）或多个节点（广播链路 broadcast link）共享的资源，需要链路访问协议来确定节点间共享链路的方式。在点到点的链路中只有两个节点共享链路，因此链路访问功能相对简单。在广播链路中，共享链路的节点通常较多，负责链路访问的是 MAC（multiple access control）协议，即“多址接入协议”。

2） 封装成帧（framing）：增加帧的头部信息，把数据包封装成数据帧（frame）。其中包括源 MAC 地址和目的 MAC 地址。

3） 差错检测（error detection）。

4） 纠错（error correction）。

5） 流量控制（flow control）。

6） 可靠传输。

上述这些功能并不是每个链路层都会提供。

数据链路层和物理层实现在网卡 NIC（Network Interface Card）上。对路由器和交换机来说，每个端口都有自己独立的数据链路层和物理层。不同的网络，数据链路层和物理层协议不同。数据链路层实现的功能也不尽相同，比如以太网 Ethernet 的数据链路层不提供可靠传输服务；而无线网络如 IEEE 802.11 WLAN 则提供一定程度的可靠传输（不是 100%可靠）。相应地有多种数据链路层协议，如 PPP，CSMA/CD，CSMA/CA 等。但是到网络层就都统一起来了，都支持 IP 协议，具有相同的数据包格式。

2. 理解多址接入协议（MAC， multiple access control）的功能及设计原则。（6.1）

MAC 协议是针对广播链路设计的多节点共享（竞争使用）链路的协议。链路是节点间共享的资源。和其它资源共享不同，网络环境下链路共享有以下特点：

（1）广播链路具有独占性。即同时只能有一个节点发送数据，否则如果两

个及以上节点同时发送数据，信号就会在信道（channel）上叠加，导致接收端无法解析出来，即发生了“碰撞/冲突（collision）”。MAC 协议的主要内容就是如何减少或者避免冲突的发生，让共享链路的节点能够协作使用信道。

（2）没有带外信道（out-of-band channel）。节点间协作共享链路需要交互的信息只能通过该链路来传输。

MAC 协议的设计原则：

1） 充分利用链路资源：当只有一个节点使用链路时，它的发送速率能达到链路带宽 R。

2） 公平性：N（N>1）个节点共享链路时，每个节点的发送速率为（1/N）R。

3） 分布式。尽量减少节点间的信息交互。

4） 简单。

3. 理解 MAC 协议的分类，每类协议的基本思想。（6.3.1，6.3.2，6.3.3，7.3）

按照信道使用的方式不同，大致分成 3 类：信道划分（channel partitioning），随机接入（random access）和轮流协议（taking turns）。每类协议都有适合的应用场景，可以满足不同的需求。因此在协议设计时要根据需求进行相应设计。

（1） 信道划分（channel partitioning）

把信道分成不相交的子信道，每个节点使用一个子信道。这类协议有：TDMA，FDMA 等。

优点：没有冲突。可以保证每个节点的传输质量（带宽、延迟等）。

缺点：不能充分利用信道资源。只有一个节点使用时，也只能占用 1/N 的带宽。

应用实例：传统电话通信网络（telecommunication network）的链路。

（2） 随机接入（random access）

节点如果有数据包要发送，就随机接入信道。这类协议主要有两个系列：ALOHA；CSMA。链路利用率和协议有关。

优点：可以充分利用链路资源，一个节点使用时，可以占用整个链路。节点公平共享链路。方便分布式实现。

缺点：有冲突。

应用实例：以太网 Ethernet 的链路协议（CSMA/CD）；

IEEE 802.11 WLAN 链路协议（CSMA/CA）

（3） 轮流协议（taking turns）

是上述两种协议的折衷。既没有冲突，又能充分利用链路资源。这类协议有：polling （轮询），token ring（令牌环）等。

应用实例：Bluetooth（polling）；

FDDI (token ring)。FDDI 已经很少使用了。

4. 了解 ALOHA，Slotted ALOHA。熟练掌握 CSMA/CD，理解载波侦听后要冲突检测的原因。（6.3.2）

ALOHA：是第一个无线网络的链路访问协议，具有重要的历史地位。但是链路利用率低，已经很少使用了。

CSMA：链路利用率很高，广泛应用在局域网中。

CSMA 协议设计面临的问题：

（1） 如何检测冲突。

（2） 冲突后如何恢复。

不同的协议，由于应用的网络场景（通信介质、信道特点等）不同，解决方法各异。比如应用于 Ethernet 的 CSMA/CD；应用于 WLAN 的 CSMA/CA。

CSMA/CD：工作流程图如图 4-1 所示。能够在帧的发送过程中检测出冲突，因而采用持续帧听信道状态的方式。一旦检测到信道闲就立即发送数据。冲突恢复采用著名的二进制退避（binary backoff）算法。该算法巧妙地把冲突次数和退避时长关联起来，不需要参与的节点间交互协作信息，可以分布式实现，降低了实现成本。

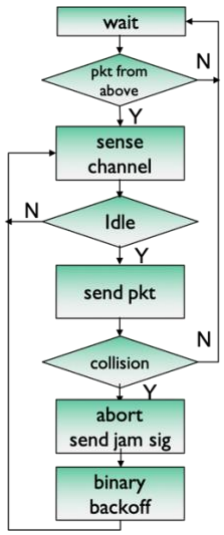


图 4-1 CSMA/CD 工作流程图

5. 理解 Ethernet。（6.4）

（1） 熟练掌握 CSMA/CD，深入理解冲突检测和二进制指数退避机制。

（2） Ethernet 中设备的互联。

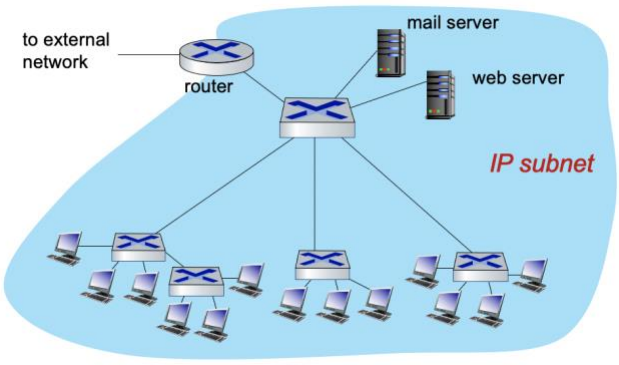


图 4-2 Ethernet 中设备的互联方式示意图

Ethernet 中设备的互联方式如图 4-2 所示。路由器的一个接口连接一个子网，交换机用于扩展路由器的接口。交换机也可以级联，进一步增加可接入的主机数量。

如图 4-3 所示，路由器是三层互联设备，交换机是二层互联设备。

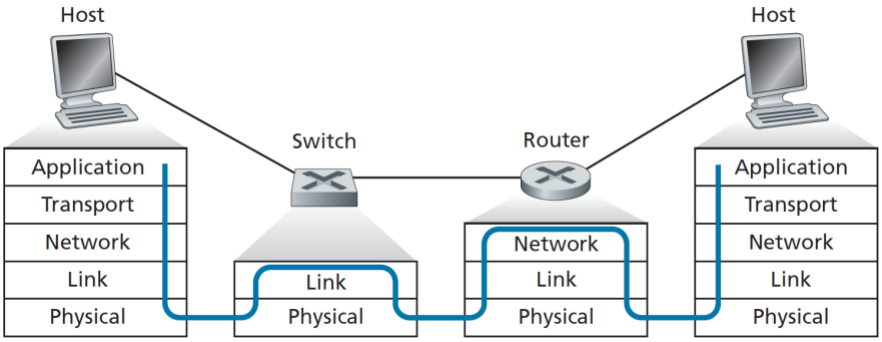


图 4-3 Router 和 Switch 对数据包的处理过程

（3） 掌握 ARP 的工作机制。

1) ARP 解决的问题

ARP 实现 IP 地址到 MAC 地址到转换。这里的 IP 地址是下一跳节点（next hop）的 IP 地址。如图 5-1 所示，该 IP 地址是网络层根据收到的数据包的目的 IP 地址，通过查找转发表所给出的。链路层把数据包封装成帧则需要知道链路层目的节点（下一跳节点）的 MAC 地址，因此 ARP 协议需要把下一跳节点的 IP 地址转换成 MAC 地址。

2) 熟悉 ARP 的工作过程，如图 5-1 所示。体会如何做到即插即用（plug-and-play）。

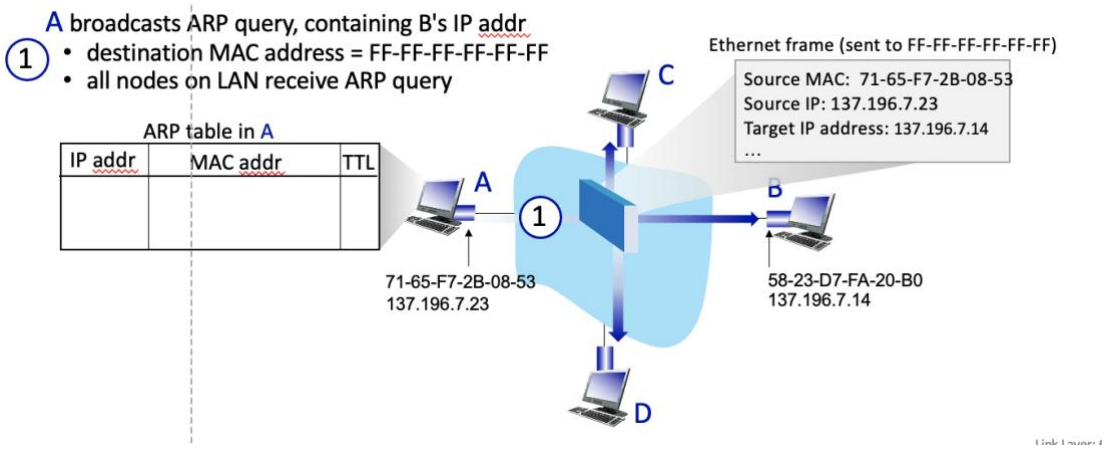


图 5-1 ARP 协议工作原理示意图

3) 协议设计小技巧：ARP 表中的 TTL。

ARP 表中的 TTL 用于保持 IP 地址-MAC 地址映射的时效性。IP 地址可能会随时间发生改变，比如使用笔记本电脑在教室上网所分配到的 IP 地址为 IP1，下课后回到宿舍，在宿舍上网所分配到的 IP 地址为 IP2，则 IP1 和 IP2 可能会不同（二者所在的子网可能不同）。但是笔记本电脑的 MAC 地址通常是固定的。有了 TTL 就可以把一段时间内没有使用过的表项删除掉，以保持映射的时效性。

4）ARP 协议是数据链路层的协议，只在邻居节点间（同一个子网内）广播控制包，这些控制包不会传到子网外面。即 ARP 的作用范围：一个子网内部。

（4） 理解教材图 6.19 Two subnets interconnected by a router 的例子，要能独自分析数据包的传输过程。（6.4.1）

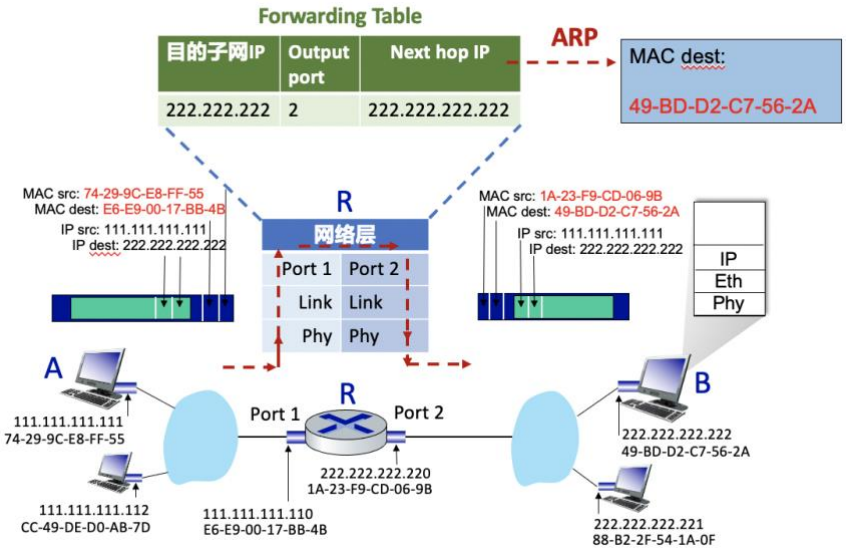


图 5-2 数据包跨子网传输过程中，在路由器的处理过程示意图

数据包跨子网传输过程中，在路由器的处理过程如图 5-2 所示。数据包到达路由器 R 的端口 1 后，从端口 1 经由物理层、数据链路层上传到网络层。网络层根据数据包目的 IP 地址查找转发表，获取其下一跳（next hop）IP 地址 222.222.222.222 和端口号 2。把数据包转发到端口 2，传入端口 2 的数据链路层。数据链路层调用 ARP 协议获得下一跳 IP 地址所对应的 MAC 地址 49-BD-D2-C7-56-2A；封装数据包成帧（frame）；执行 MAC 协议竞争到信道；把数据帧下传到物理层；物理层把数字信号转换成模拟信号发送到链路上。

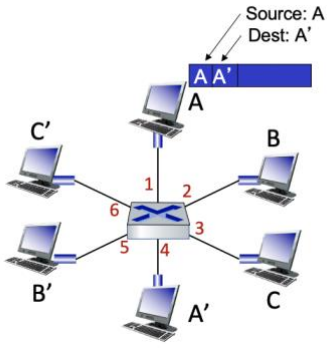
注意：

1）IP 地址是属于网络层的。数据包产生时就携带了源 IP 地址和目的 IP 地址，这两个地址在数据包传输过程中是不改变的。路由器需要根据数据包的目的 IP 地址为其选路。

2）MAC 地址是属于数据链路层的。数据包在不同链路中传输，链路两端的设备具有不同的 MAC 地址。数据包在跨子网传输过程中会经过不同的链路，从链路的一端（源）传到另一端（目的）。因此目的 MAC 地址和源 MAC 地址是不断变化的。

（5） 理解并掌握交换机的交换表自学习机制。（6.4.3）

这里的交换机指二层交换机，即工作在数据链路层的交换机。区别于市面上的三层交换机。



MAC addr	interface	TTL
A	*1*	*60*

图 5-3 交换机的交换表自学习机制示意图

交换表的自学习机制：

交换机有个交换表，用于保存端口和设备的映射关系，即哪个设备（用 MAC 地址标识）接插在哪个端口上。交换机用自学习的方式维护交换表，非常巧妙地实现了即插即用。基本思想是只要设备发送数据包，交换机就能在其所连接

的端口收到，记录下该设备和端口的映射关系。如图 5-3 所示，节点 A 发送数据包给节点 A’。交换机在端口 1 上收到了 A 的数据包，因此知道 A 接插在端口 1 上，在交换表中记录这一条目。交换表中没有 A’的端口信息，因此采用洪泛（flooding）方法把该数据包发给所有其他节点。A’收到该数据包后回复 A，于是交换机在端口 4 收到 A’的数据包，把这一映射信息记录到交换表中。

交换表中 TTL 的作用：

交换机上接插的设备或许会更换，比如把设备从一个接口换到另一个接口；新的设备接入到交换机，或者已有的接入设备被拆除了。因此，交换机需要不断维护交换表中的条目，以确保其有效性。交换表中每个条目都有一个 TTL 域，用于记录该条目的更新时长。新增加的条目 TTL 设置为最大值，根据在端口上接收到的数据包情况不断更新 TTL。当某条目的 TTL 为 0 时，表明对应端口长时间没有收到所接插设备的数据包，就将该条目删除，以确保交换表的时效性。

ARP 协议和交换机自学习机制的比较：

交换机用自学习的方式维护交换表，ARP 用广播的方式维护 ARP 表。交换机的自学习方式是被动的获取映射关系，而 ARP 是主动的获取映射关系。要理解它们的不同实现方式，并体会其实现的巧妙之处。

（6） 了解 VLANs 的工作原理。（6.4.4）

6. 理解 WLAN （7.3.1-7.3.3）

（1） 掌握 CSMA/CA 协议的基本工作原理。

WLAN 使用 CA（Collision Avoidance）的原因：

无线介质检测冲突很难实现。

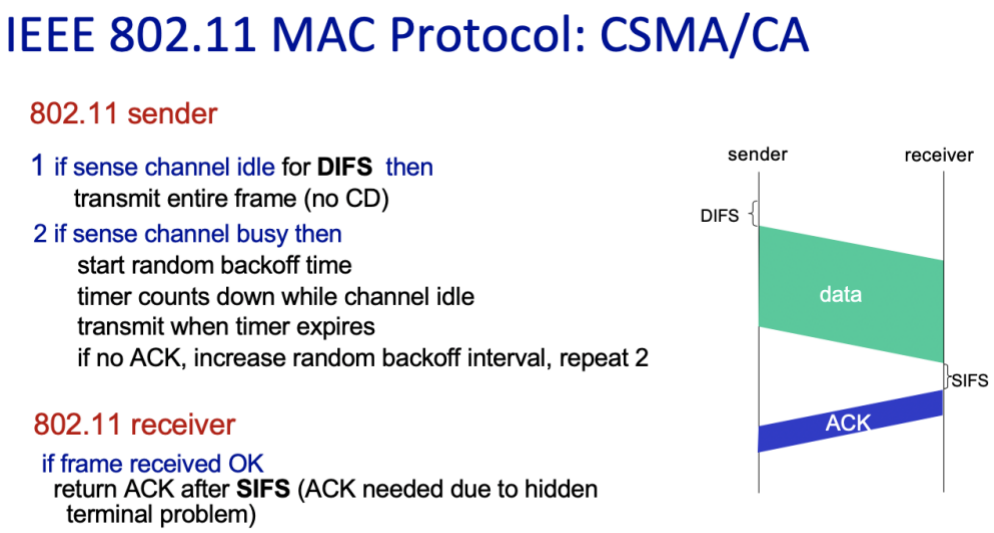


图 6-1 CSMA/CA 的基本原理

CA：

1）如果发送节点侦听到信道空闲，要持续侦听一段时间 DIFS，在这段时间内信道都是空闲的才发数据帧。因此，如果有其它节点发送数据帧，在这段时间内信号传播过来就可以被发送节点侦听到，从而避免冲突。

2）如果发送节点侦听到信道忙，则随机退避一段时间。退避后如果信道空闲，则发送数据帧，如果没有收到应答帧（ACK），则增加随机退避间隔。继续侦听信道。这种侦听到信道忙就退避的方式能有效避免冲突。例如，如果有两个以上节点同时侦听到信道忙，则都随机退避一段时间。由于随机退避的时长可能不同，当一个节点 A 侦听信道时另一个节点 B 可能已经发送数据帧了，如果 A 能侦听到 B 的信号就能避免冲突。

CSMA/CA 使用 stop-and-wait 方式 RDT 的原因：

a）无线信道传输丢包率较高，多种因素会导致丢包，如信道冲突、外部干扰等。

b）WLAN 的传播延迟很短（bandwidth×delay 和数据包长度相当），使用 stop-and-wait 也能获得较高的信道利用率。

CSMA/CA 中 RDT 不会确保可靠传输（100%可靠）的原因：

a）stop-and-wait 是用延迟换可靠，如果确保可靠，可能会导致链路延迟太大。

b)有的网络应用对延迟敏感，却可以容忍一定程度的丢包，如实时多媒体传输业务。如果在链路层确保可靠，对这类业务会有很大影响。

c)对可靠传输有需求的业务，可以在上层采用 RDT 确保数据传输的可靠性，比如使用 TCP 协议。

（2） 深入理解隐藏终端（hidden terminal）问题和其解决方法。

隐藏终端问题：

如下图所示，B 在 A 和 C 的通信范围内，但是 A 和 C 不在彼此的通信范围内（A 和 C 不能听到对方），A 和 C 会同时向 B 发送数据导致在 B 处冲突。A 和 C 互为隐藏终端。

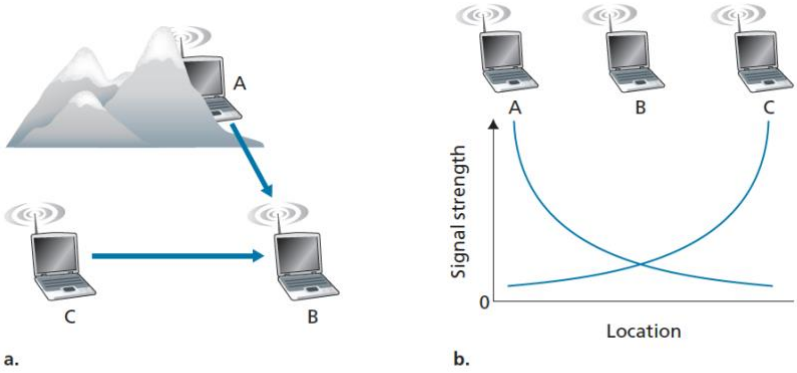
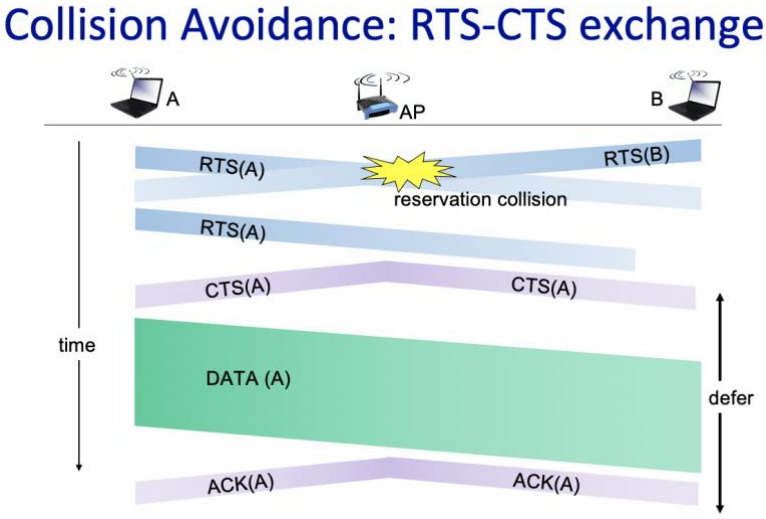


Figure 7.4 ♦ Hidden terminal problem caused by obstacle (a) and fading (b)

隐藏终端问题产生的原因：由于多径衰落，受干扰、遮挡等原因，无线信号在传输过程中信号强度会衰减。

可能的解决方法：802.11 采用的 RTS/CTS。基本思想：使用短包预约信道，减少冲突的代价。需要注意：802.11 标准中 RTS/CTS 是可选的，不要求必须使用。主要原因是代价高（预约时间）。另外，不使用 RTS/CTS 也能在一定程度上解决隐藏终端问题。假设 A 和 B 互为隐藏终端。如果 A 和 B 发送数据在 AP 处冲突，则 A 和 B 就不能收到 ACK，于是两个节点随机退避。退避之后再发送数据就有可能发送成功。



7. 深刻理解教材 6.7 节。（6.7）

这是对网络软件体系结构（TCP/IP 协议栈）工作过程的总结。