使用本书
示例捕获文件
斗技基金会
与支持
章 数据包分析技术与网络基础
1.1 数据包分析与数据包嗅探器
1.1.1 评估数据包嗅探器
1.1.2 数据包嗅探器工作过程
1.2 网络通信原理
1.2.1 协议
1.2.2 七层 OSI 参考模型
1.2.3 OSI 参考模型中的数据…
1.2.4 数据封装
1.2.5 网络硬件
1.3 流量分类
1.3.1 广播流量
1.3.2 组播流量
1.3.3 单播流量
1.4 小结
章 监听网络线路
2.1 混杂模式
2.2 接网络中嗅探

1.2.2 七层 OSI 参考模型

网络协议是基于它们在行业标准 OSI 参考模型中的职能进行分层的。OSI 模型将网络通信过程分为七个不同层次，如图 1-1 所示。这个分层模使得我们更容易理解网络通信。

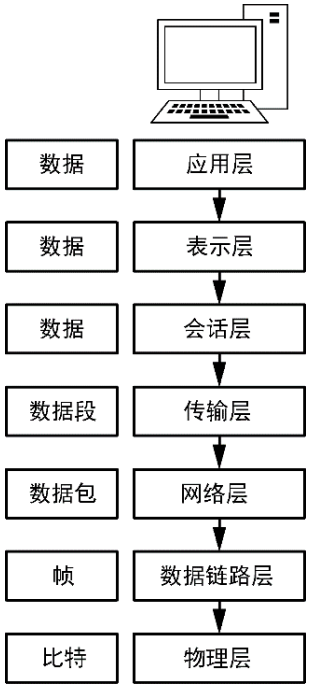

图 1-1 OSI 参考模型的七层协议视图

顶端的应用层表示用来访问网络资源的实际程序。底层则是物理层，过它来进行实际的网络数据传播。每一层次上的网络协议共同合作，来确通信数据在协议上层或下层中得到妥善处理。

> 注意
>
> OSI 参考模型最初在 1983 年由国际标准化组织出版，标准号为 ISO 7498。OSI 参考模型只一个行业建议标准，协议开发时并不需要严格地遵守它。OSI 参考模型也并不是现有唯一的网络型，例如，有些人更推崇美国国防部（DoD）的网络模型，也被称为 TCP / IP 模型。

OSI 参考模型中的每层都具有特定功能，具体如下。

应用层（Application layer，第 7 层）：OSI 参考模型的最上层，为用访问网络资源提供一种手段。这通常是唯一一层能够由最终用户看到的协议，因为它提供的接口，是最终用户所有网络活动的基础。

使用本书
示例捕获文件
科技基金会
与支持
章 数据包分析技术与网络基础
1.1 数据包分析与数据包嗅探器
1.1.1 评估数据包嗅探器
1.1.2 数据包嗅探器工作过程
1.2 网络通信原理
1.2.1 协议
1.2.2 七层 OSI 参考模型
1.2.3 OSI 参考模型中的数据…
1.2.4 数据封装
1.2.5 网络硬件
1.3 流量分类
1.3.1 广播流量
1.3.2 组播流量
1.3.3 单播流量
1.4 小结
章 监听网络线路
2.1 混杂模式
2.2 接网络中嗅探

会话层（Session layer，第 5 层）：这一层管理两台计算机之间的对话（会话），负责在所有通信设备之间建立、管理和终止会话连接。会话层还负责以全双工或者半双工的方式来创建会话连接，在通信主机间关闭连接，不是粗暴地直接丢弃。

传输层（Transport layer，第 4 层）：传输层的主要目的是为较低层提供可靠的数据传输服务。通过流量控制、分段/重组、差错控制等机制，传输层确保网络数据端到端的无差错传输。因为要确保可靠的数据传输其过极为烦琐，所以 OSI 参考模型将其作为完整的一层。传输层同时提供了面连接和无连接的网络协议。某些防火墙和代理服务器也在这一层工作。

网络层（Network layer，第 3 层）：这一层负责数据在物理网络中的由转发，是最复杂的 OSI 层之一。它除了负责网络主机的逻辑寻址（例如通过一个 IP 地址），还处理数据包分片和一些情况下的错误检测。路由器这一层上工作。

数据链路层（Data link layer，第 2 层）：这一层提供了通过物理网络输数据的方法，其主要目的是提供一个寻址方案，可用于确定物理设备如 MAC 地址）。网桥和交换机是工作在数据链路层的物理设备。

物理层（Physical layer，第 1 层）：OSI 参考模型的底层是传输网络数据的物理媒介。这一层定义了所有使用的网络硬件设备的物理和电气特性包括电压、集线器、网络适配器、中继器和线缆规范等。

物理层建立和终止连接，并提供一种共享通信资源的方法，将数字信转换成模拟信号传输，并反过来将接收模拟信号转换回数字信号。

> 注意
>
> 一个把 OSI 模型各个层次都记住的口诀是 Please Do Not Throw Sausage Pizza Away。从一层开始，每个单词的首字母依次代表着 OSI 模型中的每一层。

表 1-1 列出了 OSI 参考模型各个层次上的一些常见网络协议。

表 1-1　OSI 参考模型各个层次上的典型网络协议

层次	协议
应用层	HTTP、SMTP、FTP、Telnet

使用本书
示例捕获文件
科技基金会
与支持
章 数据包分析技术与网络基础
1.1 数据包分析与数据包嗅探器
1.1.1 评估数据包嗅探器
1.1.2 数据包嗅探器工作过程
1.2 网络通信原理
1.2.1 协议
1.2.2 七层 OSI 参考模型
1.2.3 OSI 参考模型中的数据…
1.2.4 数据封装
1.2.5 网络硬件
1.3 流量分类
1.3.1 广播流量
1.3.2 组播流量
1.3.3 单播流量
1.4 小结
章 监听网络线路
2.1 混杂模式
2.2 接网络中嗅探

表示层	ASCII、 MPEG、 JPEG、 MIDI
会话层	NetBIOS、 SAP、 SDP、 NWlink
传输层	TCP、 UDP、 SPX
网络层	IP、 IPX
数据链路层	Ethernet、 Token Ring、 FDDI、 AppleTalk

尽管 OSI 参考模型仅仅是一个建议标准，你还是应该将其牢记在心。读这本书时，你会发现，对不同层网络协议进行交互才能解决你所面对的络问题。比如遇到路由器问题，你应该快速确认这是「第 3 层上的问题」，而应用软件问题则被识别为「第 7 层上的问题」。

> 注意
>
> 在讨论我们的工作时，一位同事说他曾处理过一位用户的投诉，用户反映不能访问网络资源而实际原因是用户输入的密码不正确。我的同事将这个案例标成了「第 8 层的问题」，第 8 层是用户层的一种非官方说法，通常是由那些整天工作在数据包层次上的网络工程师们所使用。