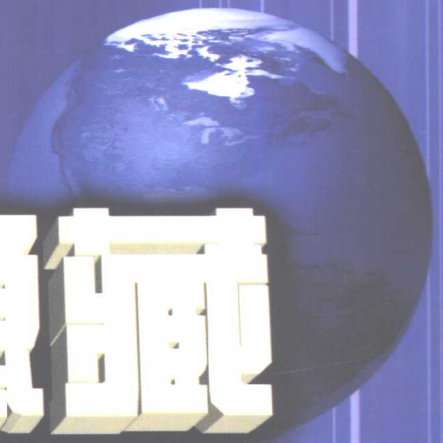
求是科技

网络与信息安全



监听与隐藏

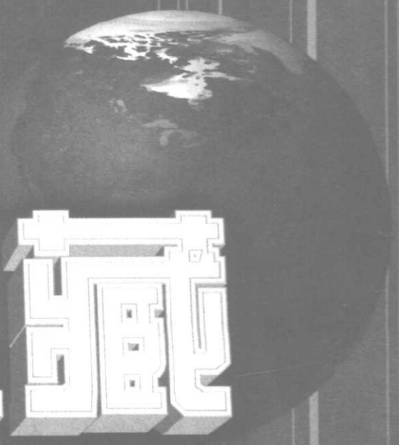
网络侦听揭密与数据保护技术

■求是科技 谭思亮 编著

人民邮电出版社
POSTS & TELECOMMUNICATIONS PRESS

是科技

网络与信息安全



监听与隐藏

网络侦听揭密与数据保护技术

■ 求是科技 谭思亮 编著

人民邮电出版社

图书在版编目(CIP)数据

监听与隐藏：网络侦听揭密与数据保护技术/谭思亮编著.—北京：人民邮电出版社，2002.8
ISBN 7-115-10418-2

I. 监… II. 谭… III. 计算机网络—安全技术 IV. TP393.08

中国版本图书馆 CIP 数据核字(2002)第 048922 号

内容提要

本书介绍了网络监听与信息安全的基本理论和关键技术，主要包含 4 部分内容：第 1 部分介绍网络体系结构、TCP/IP 协议族、局域网技术与网络编程的一些基础知识。第 2 部分介绍网络监听技术，包括包捕获、过滤、协议分析的程序设计基础和一些监听工具的介绍。第 3 部分介绍防范监听技术、保证信息安全的一些方法，包括消除网络结构隐患、检测与清除监听器和使用加密技术等。第 4 部分为实例学习，其中第 10 章介绍一些较简单实例，主要是对前面 3 部分内容的一些应用，第 11 章介绍如何设计并编程实现一个大型网络监听系统。

本书主要面向对网络监听与信息安全有兴趣的读者，全书内容丰富，讲解由浅入深，有很强的实用性和指导性。

网络与信息安全

监听与隐藏——网络侦听揭密与数据保护技术

◆ 编　　著　求是科技　谭思亮
责任编辑　张立科

◆ 人民邮电出版社出版发行　北京市崇文区夕照寺街 14 号
邮编　100061　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
读者热线　010-67180876
北京汉魂图文设计有限公司制作
北京顺义向阳胶印厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：27
字数：657 千字　　2002 年 8 月第 1 版
印数：1-5 000 册　　2002 年 8 月北京第 1 次印刷

ISBN 7-115-10418-2/TP・2958

定价：49.00 元

本书如有印装质量问题，请与本社联系　电话：(010)67129223

关于本书

Sniffer（监听）最初是提供给管理员的一类极具威力的网络工具，使用这类工具可以监视网络的状态、数据流动情况以及网络上传输的信息并利用这些信息来分析网络性能、排除网络故障。建立在监听技术基础上的网络分析仪是专业网络工程师必不可少的工具，其全球市场每年达数十亿美元。

监听工具能有效地截获网上的数据，因此它同时也成为黑客最喜爱的工具。黑客运行监听程序以暗中监视他人的网络状况、窃取明文传输的密码和各种机密数据，对网络信息安全造成极大威胁。为保护网络关键数据传输的安全，通常必须采用各种反监听措施以保证信息不被窃取。

监听技术及其防范是本书的两大主题。全书共分 4 个部分，共 11 章，内容由浅入深。

第 1 部分包括第 1 章~第 3 章，介绍网络基础知识，主要面向对网络及网络编程不很熟悉的读者。

第 1 章讲述网络体系结构与 TCP/IP 协议族，重点在于分析各常用协议数据包格式，为以后的协议分析打下基础。

第 2 章讲述作为监听技术主要舞台的局域网技术，包括网络接口卡、局域网拓扑结构、主要的局域网类型和一些网络互连设备。

第 3 章讲述网络编程，包括 NetBIOS 标准接口和 Socket 编程。本章最后介绍的 Raw socket 是实现网络监听的一种重要技术。

第 2 部分包括第 4 章~第 6 章，讲解网络监听技术。

第 4 章讲述包捕获与过滤技术，包括包捕获、过滤和分解机制，重点介绍了 BPF 模型与 pcap 库接口以及如何使用它们进行监听。

第 5 章讲述如何设计协议分析模块进行数据包分析。数据包分析可以说是网络监听的真正目的，也是监听程序设计的难点所在。本章结合前面所学内容，实际设计并编码实现了一个协议分析模块，提供对 TCP/IP 体系结构中从链路层到传输层几种常用协议的支持。

第 6 章面向网络管理者角度讲述网络监听技术，主要包括监听的原理与实施，并介绍了几种常用的监听工具。

第 3 部分包括第 7 章~第 9 章，讲述如何防范网络监听，保证信息安全。

第 7 章介绍通用的网络和系统安全策略，包括局域网内的防范（访问控制、使用安全的网络结构等）、对外部网络的防护（防火墙、虚拟专用网等）。本章最后介绍了一些常见平台漏洞与补救方法。

第 8 章讲述如何检测网络监听程序和木马病毒的存在，并介绍了监听检测工具 anti-sniff 的使用。

第 9 章介绍了保证信息安全的一种关键技术：数据加密；内容主要包括密码学的一些基本概念、加密技术的应用、安全算法（以对称算法 DES 与非对称算法 RSA 为例）与安全协议（以 SSL 为例）的设计与实现。

第 4 部分包括第 10 章~第 11 章，主要是实例学习。

第 10 章介绍了一些较简单的实例，主要是对前面 3 部分内容的应用。

第 11 章介绍如何设计并编程实现一个较完善的网络监听系统。

本书内容除第 4 部分实例学习是建立在特定系统上之外，其余各部分均与具体操作系统无关，其内容可适用于 Windows、UNIX、Linux 等平台。

由于作者水平有限，书中难免有不足和疏忽之处，恳请读者和各位同仁批评指正。全书有关的源代码请到http://www.ucbook.com上下载。

编者

目 录

第 1 章　计算机网络体系结构

1.1　基础知识与常见术语

1.1.1　网络功能与协议

计算机网络体系结构（Network Architecture）又称为网络系统结构，它从功能的角度描述计算机网络的结构，是计算机网络层次结构模型和各层次协议的集合。

计算机网络是由独立的计算机互相连接组成可以交换信息的集合体。其基本目标在于为地理位置不同的用户提供访问通路，实现信息和资源的共享。要实现这个目标，下列功能是必需的：

- 连接源结点和目的结点的物理传输线路，可以经过中间结点。
- 每条线路两端的结点进行二进制通信。
- 无差错的信息传送。
- 多个用户共享一条物理线路。
- 按照地址信息，进行路由选择。
- 信息缓冲和流量控制。
- 会话控制。
- 满足各种用户的访问要求。

为了简化网络设计的复杂性，通常采用“功能分层”的方法来描述计算机网络，即网络按一系列层来管理，每一层都建立在前一层的基础上。

按层次划分的计算机网络功能中，最重要的功能是通信功能。这种通信功能主要涉及同一层次中通信双方的相互作用；不同计算机上进行对话的第 N 层通信各方可分别看成是一种进程，也称为对等进程；第 N 层对等进程通信时所遵守的规则称为第 N 层协议。

协议由语法（syntax）、语义（semantics）、定时关系（timing）三个部分组成。语法定义以二进制形式表示的命令和相应的结构；语义是由发出的命令请求，完成的动作和回送的响应组成的集合；定时关系是有关事件顺序的说明。

协议的相邻网络层之间有接口（Interface），它定义了下层向上层提供的原语操作和服务。对于第 N 层协议来说，它使用下层提供的服务接口，完成某种功能并为上层提供服务。任何层间服务是在接口的服务访问点（Service Access Point，简称 SAP）上进行的，每个服务访问点有唯一的识别地址，每个层间接口可以有多个服务访问点。

接口数据单元（Interface Data Unit，简称 IDU）是通过 SAP 进行传送的层间信息单元，由上层的服务数据单元（Service Data Unit，简称 SDU）和接口控制信息（Interface Control

Information，简称 ICI）组成。协议数据单元（Protocol Data Unit，简称 PDU）是第 *N* 层实体通过网络传送给它的对等实体的信息单元，由上层的服务数据单元 SDU 或其分段和协议控制信息（Protocol Control Information，简称 PCI）组成。

上述概念具体关系可见图 1-1。

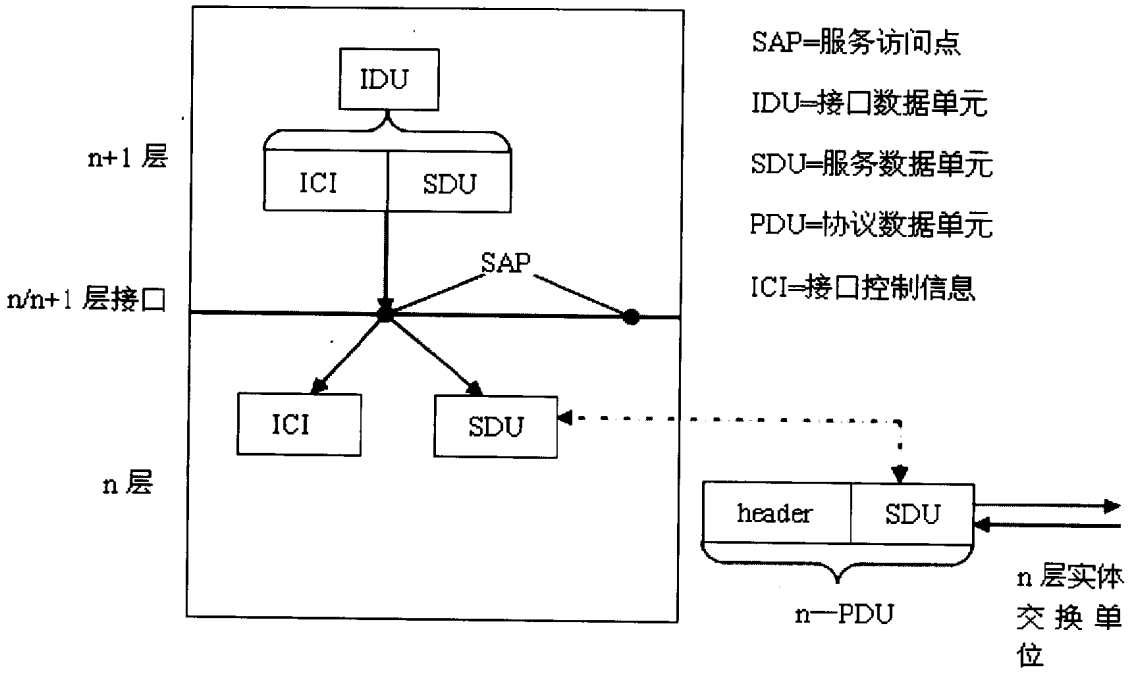


图 1-1　相邻两层间的接口

1.1.2　包与帧

1. 包

大多数计算机网络都不能连续传输任意数量的数据。事实上，为了保证所有共享网络资源的计算机能公平、迅速地使用网络，网络通常把数据分割成若干小块单独发送，这种小块称作包（Packet）。计算机在共享网络上按次序发送包。因为每个包都很小，所以计算机在使用时不需经历长时间的等待。

2. 帧

术语包指的是小数据块的一般概念，事实上并没有确切的包内容和格式的定义。相反，每种硬件技术都定义了能在该硬件上传输的数据块（包）的细节。为了帮助区分一般概念的包与特定硬件技术所使用的包，我们用术语帧（Frame）来定义用在特定网络类型中的包。

3. 帧定界与填充

在考虑数据传输时，一个显而易见的问题是如何指明每一帧的开始和结束以让发送和接收的双方能保持一致。

如果帧中数据不使用所有可能值，那么网络系统可以选择两个不用的值来标记每帧的开始与结束。如在一个只传输可打印文本文件的网络中，可以使用 ASCII 码中的 soh（十六进制数 1）和 eot（十六进制数 4）来标记数据帧的开始和结束。如图 1-2 所示。

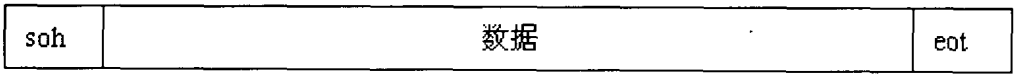


图 1-2　一般帧格式

但事实上大多数网络允许帧中传输任意数据，特定的帧开始和帧结束标志可能在数据中重复出现，因此，简单地在帧的数据部分中传输这些字符会引起问题。通常，为了区分传输的数据与控制信息，例如帧的定界符，网络系统会要求发送方在发送之前稍微修改一下数据，然后要求接收方在把数据传输给应用之前恢复原来的数据。这样，不管网络上的应用要求帧中传输何种数据，网络系统也不会把它们与控制信息混淆。

网络系统通常以插入多余的位或字符的手段来修改传输的数据，这种技术被称为数据充填（Data Stuffing）。字符充填（Character Stuffing）与字节充填（Byte Stuffing）是指使用面向字符硬件的数据充填，而更常用的位充填（Bit Stuffing）是指使用面向位硬件的数据充填。下面我们将以字符填充为例说明。

我们仍使用 soh 与 eot 作为帧定界符，所以这两个字符不能在帧数据中出现。在字节填充技术中使用标志字符来标志数据中特殊字符（帧定界符与标识字符本身）的出现。如选择 ASCII 码中的 esc（十六进制的 1B）作为标志字符，当特殊字符出现时，发送方计算机就插入 esc 与一普通字符来代替该特殊字符（例如：用 esc+a 代替 soh，用 esc+b 代替 eot，用 esc+c 代替 esc 本身），接收方遇到标志字符（esc）后将其后跟随的普通字符（a，b，c）转化为特殊字符（soh，eot，esc）。图 1-3 表示了这种映射关系。

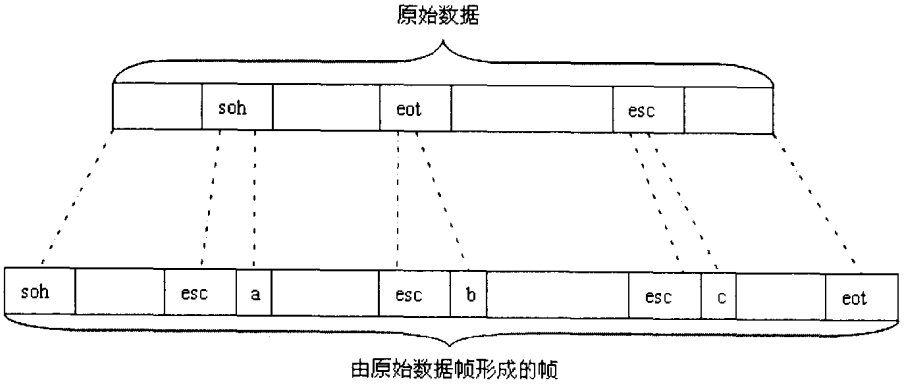


图 1-3　数据填充与成帧

位填充技术通常使用六个连续的 1 作为帧定界符。为了确保 6 个连续的 1 不会出现在数据中，发送方在每 5 个连续的 1 后面插入一个附加的 0。接收方在接收比特流时，如果发现

连续的 5 个 1 后面是 0，则这个 0 必须被删除或忽略；如果在 5 个连续的 1 后面还是 1，这就标志着数据包的开始或者结束。

1.1.3 网络规模分类

网络从传输规模上可以分为：局域网、城域网与广域网。

1. 局域网

局域网（Local Area Networks，简称 LAN）将距离很近的计算机连接起来，它传输地域小，延迟时间短，可以应用多种拓扑结构，允许多台计算机共享通信介质，大多数局域网采用广播通信方式。由于以上特点，监听主要发生在局域网中，在第二章中对局域网技术有详细分析。

2. 广域网

与局域网对应的是广域网（Wide Area Networks，简称 WAN），广域网是局域网之间的连接，它范围广，通常是全球性的网络，运行 TCP/IP 协议，一般使用点到点通道技术。最著名的广域网就是因特网（Internet）。

3. 城域网

城域网（Metropolitan Area Network，简称 MAN）是介于局域网与广域网之间的一种网络，它的范围比局域网大得多，比城域网又小得多。现在对网络规模分类时，基本划分为局域网和广域网两大类，已经很少涉及城域网。

1.1.4 网络类型与网络操作系统

1. 网络类型

按网络中的计算机相互间的地位而言，有对等网络（Peer to Peer Networks）和基于服务器的网络（Server Based Networks）之分。

在对等网中所有计算机地位平等，没有从属关系，没有特定的服务器，用户数少，网络较大时不易管理；在这种网络中安全性检验通常在本地进行。

在基于服务器的网络中有专门响应用户请求的计算机作为服务器，服务采用客户机/服务器（Client/Server）模式：客户机向服务器发出请求，服务器相应请求，完成相关工作，再将结果返回给客户机。在这种模式中服务器端通常有专用服务器程序完成工作并进行应答；客户端可用客户程序或浏览器进行请求。

2. 网络操作系统

常见的网络操作系统通常有以下几种：Windows 9x/NT/2000，Unix，Linux，Netware。Windows 9x 操作系统主要作为客户机使用，其余几种通常作为服务器使用。Netware 操作系统主要运行 IPX/SPX 协议族；Windows NT/2K、Unix/Linux 主要运行 TCP/IP 协议族。

1.2　开放系统互连参考模型

开放系统互连（Open System Interconnection，简称 OSI）参考模型是一个多层的通信协议，最初由国际标准化组织（International Standard Organization，简称 ISO）开发，1983 年正式成为国际标准。

所谓开放系统是指允许任意两个具有不同基本体系结构的系统进行通信的一套协议集。ISO 一直致力于允许多种设备相互通信的研究，并制定了开放系统互连模型。如果发展完善的话，OSI 将允许任意两台连接的计算机实现通信。

OSI 模型将网络划分为七层模型，分别用以在各层上实现不同的功能，这七层从上至下分别是：应用层（Application Layer）、表示层（Presentation Layer）、会话层（Session Layer）、传输层（Transport Layer）、网络层（Network Layer）、数据链路层（Data Link Layer）及物理层（Physical Layer），其通信模型如图 1-4 所示。

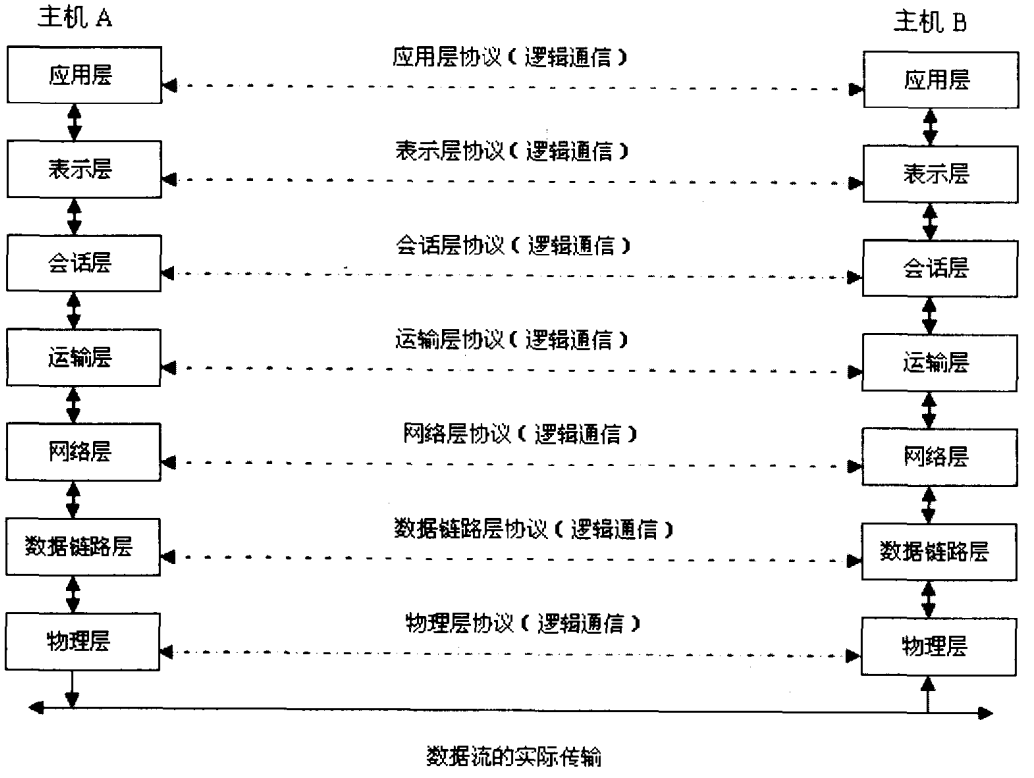


图 1-4　OSI 七层通信模型

OSI 模型中每一层只与其上下两层直接通信。高层协议偏重于处理用户服务和各种应用请求，低层协议偏重于处理实际的信息传输。分层的目的在于把各种特定的功能分离开来，并使其实现对其他层次来说是透明的。这种分层结构使各个层次的设计和测试相对独立。第 n 层为 $n+1$ 层提供服务，第 $n+1$ 层不必理会下层服务是如何实现的，因此，第 n 层实现方式的改变将不会影响第 $n+1$ 层。

1.2.1 物理层

物理层提供了一个基本机制：对二进制数据（比特）进行编码（发送到物理介质）和解码（从物理介质接收），例如 10Mbit/s（bit/s 指比特每秒）以太网的曼彻斯特编码、光纤分布式数据接口（Fiber Distributed Data Interface，简称 FDDI）的 4B/5B 编码；物理层也负责通知第二层（数据链路层）何时访问介质，比如以太网的载波监听功能。物理层以比特流的方式传送来自数据链路层的数据，而不理会数据的含义或格式；同样，它接收数据后，不加分析直接传给数据链路层。

物理层也定义与介质的物理连接机制，但不是介质本身。按照参考模型的原理，实际的物理介质在物理层之下。总之，比特流应该独立于物理介质，能够在双绞线、同轴电缆、光纤、卫星、微波和无线电波上传输。此外，在某种程度上物理层也包括连接策略，物理层上的连接策略共有三种：电路交换、报文交换和分组交换。

1.2.2 数据链路层

数据链路层也称为链路控制层（Data Link Control Layer，简称 DLC 层）负责管理数据格式。数据通常被组合成帧加以传输，帧由包含了起始标志的报头或报头位、寻址信息、数据和（对于局域网）32 位的循环冗余码（Cyclic Redundancy Check，简称 CRC）组成，循环冗余码用来在信息穿过物理介质时保证数据的完整性：在接受帧时，接收者计算循环冗余码，如果计算出的结果与该帧结尾的循环冗余码不一致，则数据链路层丢弃该帧。此外数据链路层用唯一的比特组合对将要发送的每一帧的开始和结束进行标示，对接收进来的每一帧进行判断，然后把无错的帧送往上一层，即网络层。

数据链路层提供了对链路的管理。对以太网，设备通过侦听总线来避免冲突：总线忙，设备就暂时不传输；若电路检测出总线空闲，设备就立刻传输；如果两台设备都检测到总线空闲，并同时开始传送数据，就会发生冲突；这种解决竞争的方法称为带冲突检测的载波侦听多路访问，它有效地减少了冲突的次数。在令牌网中采取令牌传递的竞争机制来防止冲突，一串循环通过所有网络节点的特定比特流称为令牌。当节点要进行传输时，它必须等待令牌的到来，并把令牌附加到要发送的报文末端；它还得改变令牌的控制位，以指示出该令牌已被占用；接着报文被送到目标节点，于是目标节点得到了令牌。根据不同的协议，目标节点可以获取令牌并进行传输（如果它有报文要发送的话），也可以把令牌传给下一节点。

数据链路层还负责监督相邻网络节点的信息流动，它使用检错或纠错技术来确保正确的传输；当数据链路检测到错误时，它请求重发，或是根据情况纠正。此外数据链路层还要解决流量控制的问题。

读者应该注意的是电气和电子工程师协会（Institute of Electrical and Electronic Engineers，简称 IEEE）对数据链路层定义略有不同。IEEE 定义的数据链路层实际上由逻辑链路控制（Logical Link Control Layer，简称 LLC 层）和介质访问层（Media Access Control Layer，简称 MAC 层）组成。MAC 层基本对应于传统的数据链路层，附加的 LLC 层主要提供了面向连接与无连接两种服务：LLC 类型 1 提供无连接的数据报服务，LLC 类型 2 提供的是可靠的面向连接的服务；ISO 在这之上定义了两种网络层服务，与 LLC 类型 1 对应的是无连接的网络服务，与 LLC 类型 2 对应的是面向连接的网络服务。