WILEY Publishers Since 1807

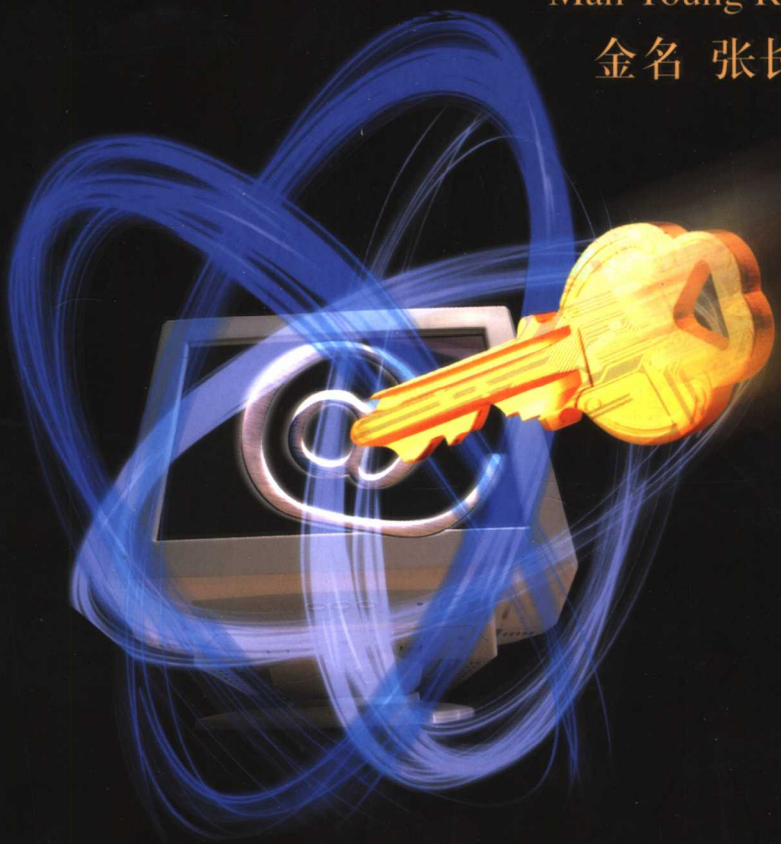
世界著名计算机教材精选

网络安全

加密原理、算法与协议

Man Young Rhee 著

金名 张长富 等译



INTERNET SECURITY

CRYPTOGRAPHIC PRINCIPLES, ALGORITHMS AND PROTOCOLS

清华大学出版社

世界著名计算机教材精选

网络安全

加密原理、算法与协议

Man Young Rhee 著
金 名 张长富 等译

清华大学出版社
北京

内 容 简 介

Man Young Rhee

Internet Security: Cryptographic Principles, algorithms, and protocols

EISBN: 0-470-85285-2

图书在版编目(CIP)数据

网络安全: 加密原理、算法与协议/(韩)李迈勇(Rhee. M. Y)著; 金名等译. —北京: 清华大学出版社,2007.7

书名原文: Internet Security

ISBN 978-7-302-15259-0

Ⅰ. 网… Ⅱ. ①李… ②金… Ⅲ. 因特网—安全技术 Ⅳ. TP393.48

中国版本图书馆 CIP 数据核字(2007)第 074186 号

责任编辑: 张 剑

责任印制: 孟凡玉

出版发行: 清华大学出版社 **地 址**: 北京清华大学学研大厦 A 座

http://www.tup.com.cn **邮 编**: 100084

c-service@tup.tsinghua.edu.cn

社 总 机: 010-62770175 **邮购热线**: 010-62786544

投稿咨询: 010-62772015 **客户服务**: 010-62776969

印 装 者: 北京国马印刷厂

经 销: 全国新华书店

开 本: 185×260 **印 张**: 20.75 **字 数**: 485 千字

版 次: 2007 年 7 月第 1 版 **印 次**: 2007 年 7 月第1 次印刷

印 数: 1~3000

定 价: 39.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题,请与清华大学出版社出版部联系调换。联系电话: (010)62770177 转 3103 **产品编号**: 023629-01

译者序

今天，因特网是所有信息的基础设施，是信息传播的一种机制，是个人、政府机关、金融机构、学术团体和各种商业贸易之间进行协作和交互的媒介，而且没有地理位置的限制。

不论由于是个人还是专业使用的需要，人们已经变得越来越依赖于因特网了，如E-mail、文件传送、远程登录、Web页面访问或商业事务处理。因特网使计算和通信世界发生了革命性的变化，以开发和支持客户和服务器服务。因特网的可用性及其能提供的强大的计算和通信能力，使得形成了一种新的商业模式。由于浏览器和万维网技术的应用，允许用户很容易地访问链接到全球的信息，这更是得到了极大地促进这种商业模式。

因特网是全球范围的，但这种全球的互连网络是开放的、不安全的媒体。随着人们对因特网的不断认识和因特网的普及，因特网安全问题显现出来了。要保护用户免受基于因特网的攻击，当出现安全问题时提供恰当的解决办法，必须应用密码技术。本书介绍的就是在因特网安全中有关密码操作、原理、算法和协议的核心内容。要消除由犯罪活动产生的各种威胁，必须依靠密码技术。在培育、改进和提供因特网安全中，认证、消息完整性和加密是非常重要的。没有这种认证过程，攻击者可以模仿任何人，然后获得对网络的访问权。要求消息完整性是因为数据在因特网中传输时可能被修改。没有经过加密，信息就可能变成真正的公开了。

本书通过严谨、彻底和定性的讲述，深入地介绍了因特网安全及其实现的理论与实践知识。本书由11章组成，重点介绍了一些与因特网有关的关键的安全性问题。本书首先简要介绍了因特网的历史和TCP/IP协议族，使读者对因特网和TCP/IP协议有一个初步的了解，为后面介绍因特网安全打下基础。接着介绍了一些重要的分组加密算法和数字签名技术，并介绍了几种公钥加密系统以及因特网的公钥基础设施，然后介绍了网络层安全的IPsec协议和安全套接字层协议，这些是实现因特网安全所需的技术和手段。最后介绍了E-mail的安全性和防火墙的设计与实现，以及用于保护因特网信用卡事务处理的SET协议。

本书由金名、张长富主译，黄中敏、马静静、冯华君、宋明钧、刘守燕、杨咏梅、魏敬安、朱建波、徐志平、赵杰辉、傅祎、郭碧莲、郭洵、洪晓煜、黄宣达、江松波、柯渝、赖曲芳、廖阳、刘文红、贺军、王雷、戴军等人也参与了本书的一些工作。

本书适用于高年级本科生和研究生、专业工程师和研究人员作为因特网原理的入门教材。作为一本参考书，对计算机工程师、通信工程师和系统工程师都是很有用的。它还适用于自学。本书可以被学术和专业人士使用，还可以作为企业和研究机构的培训使用。

因特网是全球范围的，但这种全球的互连网络是开放的、不安全的媒体。因特网使计算和通信世界发生了革命性的变化，以开发和支持客户和服务器服务。因特网的可用性及其能提供的强大的计算和通信能力，使得形成了一种新的商业模式。由于浏览器和万维网技术的应用，允许用户很容易地访问链接到全球的信息，这更是得到了极大地促进这种商业模式。因特网已被证实为当今信息贸易的基础工具。

今天，因特网是所有信息的基础设施，是信息传播的一种机制，是个人、政府机关、金融机构、学术团体和各种商业贸易之间进行协作和交互的媒介，而且没有地理位置的限制。

不论由于是个人还是专业使用的需要，人们已经变得越来越依赖于因特网了，如 E-mail、文件传送、远程登录、Web 页面访问或商业事务处理。随着人们对因特网的不断认识和因特网的普及，因特网安全问题显现出来了。在不安全的媒介上进行在线事务处理，很容易诱发因特网犯罪活动。

因特网访问经常会产生一个安全缺陷。要保护用户免受基于因特网的攻击，当出现安全问题时提供恰当的解决办法，必须应用密码技术。本书介绍的就是在因特网安全中有关密码操作、原理、算法和协议的核心内容。要消除由犯罪活动产生的各种威胁，必须依靠密码技术。在培育、改进和提供因特网安全中，认证、消息完整性和加密是非常重要的。没有这种认证过程，攻击者可以模仿任何人，然后获得对网络的访问权。要求消息完整性是因为数据在因特网中传输时可能被修改。没有经过加密，信息就可能变成真正的公开了。

本书通过严谨、彻底和定性的讲述，深入地介绍了因特网安全及其实现的理论与实践知识。本书适用于高年级本科生和研究生、专业工程师和研究人员作为因特网原理的入门教材。本书由 11 章组成，重点介绍了一些与因特网有关的关键的安全性问题。下面是每章内容的概述。

第 1 章开始介绍了因特网的简要历史，内容包括：(1) 网络技术基础，如 LAN (Ethernet、令牌环、FDDI)，WAN(帧中继、X.25、PPP)和 ATM；(2) 连接设备，如电路交换和包交换、转发器、网桥、路由器和网关；(3) OSI 模型，它说明了其七层的功能；最后(4)五层的 TCP/IP 协议族，它提供了由物理标准、网络接口和互连网络组成的分层协议。

第 2 章介绍了 TCP/IP 协议族，内容包括：(1) TCP/IP 网络层协议，如 ICMP、与 IP 包格式有关的 IPv4 和 IPv6，寻址(包括 ARP、RARP 和 CIDR)和路由；(2) 传输层协议，如 TCP 和 UDP；(3) 用于万维网的 HTTP；(4) 用于文件传递的 FTP、TFTP 和 NFS 协议；(5) 用于E-mail 的 SMTP、POP3、IMAP 和 MIME；(6) 用于网络管理的 SNMP 协议。

第 3 章介绍了现代一些重要的分组加密算法，这些算法是近年来开发的，重点介绍了使用最广泛的加密技术，如数据加密标准(Data Encryption Standard，DES)国际数据加密算

法(International Data Encryption Algorithm，IDEA)，RC5 和 RC6 加密算法，以及高级加密标准(Advanced Encryption Standard，AES)。AES 指的是经 FIPS 认可的 Rijndael 算法(2001)，它可以处理 128 位的数据分组，使用的密钥长度为 128、192 和 256 位。DES 不是新东西，但它已经经受了 20 多年的强度密码分析。本章还全面分析了 CBC 模式的三重 DES-EDE、用于 E-mail 的 Pretty Good Privacy (PGP)，用于常规分组加密的文件存储实用工具 IDEA，以及用于公钥加密的 RSA 和用于哈希编码的 MD5。RC5 和 RC6 都是大小可变、轮数可变、密钥长度可变的参数化分组算法。它们在性能和安全级别上都有很大的灵活性。

第 4 章介绍了基于数字签名的不同认证技术。通常，通信双方需要验证对方的身份。这样做的一个实用方法是使用密码认证协议，该协议应用了一个单向的哈希函数。本章介绍了几种现代的哈希函数(例如 DMDC、MD5 和 SHA-1)，用于计算消息摘要或哈希代码，为认证提供对称方法。本章还扩展讨论了因特网标准 HMAC，它是受保护数据的一种安全摘要。HMAC 使用了不同的哈希算法，包括 MD5 和 SHA-1。传输层安全(Transport Layer Security，TLS)也使用了 HMAC 算法。

第 5 章在介绍了常规加密后，还介绍了几种公钥加密系统。本章重点介绍了用于公钥加密、数字签名和认证的技术。本章还详细介绍了广泛使用的 Diffie-Hellman 密钥交换技术(1976)、RSA (Rivest-Schamir-Adleman)算法(1978)、ElGamal 算法(1985)、Schnorr 算法(1990)、数字签名算法(DSA，1991)和椭圆曲线加密系统(ECC，1985)与椭圆曲线数字签名算法 (ECDSA，1999)。

第 6 章因特网的公钥基础设施(public-key infrastructure，PKI)。PKI 通过公钥证书自动地管理公钥。策略认可机构(Policy Approval Authority，PAA)是证书管理基础设施的根。该机构对 PKI 整个级别上的所有项都是已知的，为所有用户生成指导说明，CA 和下级的策略制定机构必须遵守。策略认证机构(Policy Certificate Authorities，PCA)由该基础设施中第二级的所有项组成。PCA 必须发布安全策略、过程、合法性问题、费用以及其他认为有必要的内容。认证机构(Certification Authorities，CA)形成了 PCA 的下一级。PKI 由很多的 CA 组成，CA 不负责策略的制定。CA 由用户和它认证的 RA 组成。CA 的基本功能是生成和管理公钥证书，它把用户的身份与用户的公钥捆绑在一起。注册机构(Registration Authority，RA)是用户与 CA 之间的接口。RA 的基本功能是从 CA 的角度进行用户的身份确认和认证。它还给终端用户发放 CA 证书。X.500 描述的是目录服务。X.509 使用 X.500 目录描述了认证服务。X.509 证书经历了三个版本：1998 年的版本 1，1993 年的版本 2 和 1996 年的版本 3。现在的 X.509 v3 是基于大量产品和因特网标准而形成的。这三个版本将依次介绍。最后，证书注销列表(Certificate Revocation Lists，CRL)用于列举那些已注销的未到期的证书。CRL 可能是从例程管理注销到私钥生成条件等多种原因被重新激活。本章还介绍了因特网 PKI 的证书路径合法认证过程和 PKI 证书管理基础设施的体系结构。

第 7 章介绍了网络层安全的 IPsec 协议。IPsec 提供了在因特网或公用 WAN 上的 LAN 和虚拟专用网(virtual private network，VPN)进行安全通信的能力。IPsec 的使用使得商业活动可以极大地依赖因特网。IPsec 协议是由 IETF 开发的一组安全扩展，使用密码算法和协议在 IP 层提供保密和认证服务。要保护 IP 数据包(datagram)的内容，有两种主要的转换类型：认证头(Authentication Header，AH)和封装安全负载(Encapsulating

Security Payload，ESP)。这些是提供无连接完整性、数据原始认证、保密性和反重放服务的协议。安全关联(Security Association，SA)是IPsec的基础。AH和ESP都使用了SA。SA是发送方与接收方之间的一个简单连接，为其中进行的数据流量提供安全服务。本章还介绍了OAKLEY密钥确认协议和ISAKMP。

第8章讨论了安全套接字层协议版本3(Secure Socket Layer version 3，SSLv3)和传输层安全协议版本1(Transport Layer Security version 1，TLSv1)。TLSv1协议本身是基于SSLv3协议的。很多与算法有关的数据结构和规则都非常类似，因此TLSv1和SSLv3之间的差别不大。TLSv1协议为因特网上的通信双方提供通信保密与数据完整。这两种协议都允许客户/服务器应用程序以这样一种方式进行通信：防止偷听、篡改或消息伪造。SSL或TLS协议由两层组成：记录协议与握手协议。记录协议携带要传递的高层应用消息，把数据分割成易管理的分组，还可以压缩数据，应用MAC，进行加密，添加头部，并把结果传递给TCP。被接收的数据经解密后给更高级的客户。握手协议是在记录层之上进行操作的，是SSL或TLS最重要的部分。握手协议由客户与服务器交换的消息系列组成。该协议在服务器与客户之间提供了三种服务。握手协议允许客户/服务器达成一个协议版本，通过组成一个MAC来进行相互认证，在传递应用程序协议或接收数据的第一个字节之前，协商一个加密算法和密钥，用于保护以SSL记录形式发送的数据。受密钥保护的哈希消息认证码(hashing message authentication code，HMAC)是一些受保护数据的安全摘要。没有MAC秘密的知识，无法伪造HMAC。HMAC可以与多种不同的哈希算法一起使用：MD5和SHA-1，这可以表示为HMAC-MD5 (secret，data)和SHA-1 (secret，data)。SSLv3方案与TLS MAC方案有两个不同：TSL使用的是定义在RFC 2104中的HMAC算法，TLS的主秘密计算也与SSLv3的不同。

第9章介绍了E-mail的安全性。由Philip Zimmermann发明的Pretty Good Privacy (PGP)，在全球计算机社区的多种平台上，被广泛地用在了个人和商业版本中。PGP组合使用了对称密钥和非对称公钥加密，为E-mail和数据文件提供安全服务。PGP使用数字签名、加密、压缩(ZIP)和radix-64转换(ASCII Armor)为消息和数据文件提供数据完整性服务。随着人们对E-mail和文件存储依赖的不断加深，认证和保密服务变得越来越重要了。多用途因特网邮件扩展(Multipurpose Internet Mail Extension，MIME)是RFC 822框架的扩展，它定义了使用E-mail发送文本消息的格式。MIME真正的目的是解决使用SMTP的某些问题和限制。S/MIME提高了MIME因特网E-mail格式标准的安全，它基于来自RSA数据安全的技术。尽管PGP和S/MIME走的都是IETF标准之路，但看起来PGP为很多用户保持了对个人E-mail安全性的选择，而S/MIME是作为商业和企业使用的工业标准出现的。PGP和S/MIME方案都在本章进行了介绍。

第10章讨论了防火墙主题。防火墙是一种用于防止内部系统免受因特网安全威胁的有效方法。防火墙是一个安全的网关，它控制了在公用因特网与专用内部网(或企业网)之间的访问。防火墙是一种代理，它以某种方式监视网络流量，阻止它认为是不恰当或危险的流量。在现实中，因特网访问为单个用户、政府机关和大多数组织带来了好处。但这种访问也产生了安全威胁。在双向处理SMTP和HTTP连接中，防火墙起到了一个中间服务器的作用。防火墙还要求使用访问协商和诸如SOCKS之类的封装协议，以获得对因特网和内部网的访问。很多防火墙支持三重宿主，允许使用DMZ网络。要设计和配置防火墙，需

要熟悉堡垒主机(bastion host)代理服务器、SOCKS、节流点(choke point)、DMZ、日志与警告、VPN 等。防火墙可以划分为三大类：包过滤器、电路层网关和应用程序网关。本章将依次介绍每种防火墙。最后，本章将介绍遮挡式主机(screened host)防火墙以及如何实现防火墙策略。要实现一定级别的安全，可以考虑三种基本的防火墙设计：单宿主堡垒主机(single-homed bastion host)、双宿主堡垒主机(dual-homed bastion host)和遮挡式子网防火墙。

第 11 章介绍了用于保护因特网信用卡事务处理的 SET 协议。近年来电子商务的快速发展，为消费者、零售商和金融机构提供了巨大的机会。SET 协议依靠密码和 X.509 v3 数字证书来确保消息保密、支付完整性和身份认证。使用 SET 协议，通过保证支付信息是安全的，只能被既定的接收者访问，保护了消费者和经销商。SET 协议通过确保信息在任何时候都是经安全加密的，使用数字签名验证那些访问支付信息的人的身份，防止传输信息在传送时被修改。SET 是唯一的因特网事务处理协议，通过认证来提供安全性。消息数据使用随机对称密钥进行加密，而该随机对称密钥又使用接收者的公钥进行了加密。已加密消息与数字信封一起发送到接收者。接收者用私钥把数字信封解密，然后使用对称密钥还原原始消息。SET 协议通过使用数字签名和数字证书验证信用卡持卡人与经销商之间的金融关系，解决了因特网购物的匿名问题。本章还全面地探讨了如何确保因特网的安全信用卡事务处理。

本书适用于高年级本科生或研究生一或两学期课程的教材。作为一本参考书，对计算机工程师、通信工程师和系统工程师都是很有用的。它还适用于自学。本书可以被学术和专业人士使用，还可以作为企业和研究机构的培训使用。在本书的最后，有一个常用的缩写语列表和参考书目。

第 1 章

互连网络与分层模型

今天，因特网是一个分布广泛的信息基础设施，但它因此也是一个不安全的消息发送通道。当一个消息（或数据包）从一个 Web 站点发送到另一个站点时，含有数据的消息在到达目的地之前，需要路由过多个中间站点。因特网被设计为可以容纳各种异构平台，从而人们可以使用不同的计算机和操作系统进行通信。因特网的历史很复杂，涉及了很多方面，如技术方面、组成方面和社区方面等。因特网的概念朝着电子商务、信息获取和社区交互迈出了一大步。

1.1 网络技术

数据信号通过一种或多种传输媒介（双绞线、同轴线和光纤等），从一个设备传输到另一个设备。要传输的消息是网络通信的基本单元。一个消息可能由一个或多个单元、帧或包组成，而这些都是网络通信的基本单位。网络技术包括**局域网**（local area networks，LAN）到**广域网**（wide area networks，WAN），其中，局域网指的是有限地理区域内（如单个建筑物、公寓或校园）的网络，而广域网指的是较大地理区域（它可以指一个国家、一个洲甚至是整个世界）的网络。

1.1.1 局域网

局域网（local area network，LAN）就是一个通信系统，它允许在有限地理区域内（如单个办公建筑物、仓库或校园）的多个各自独立的设备相互之间直接进行通信。标准化的局域网有三种体系结构：**以太网**（Ethernet）、**令牌环**（token ring）和**光纤分布式数据接口**（fibre distributed data interface，FDDI）。

1.1.1.1 以太网

以太网是一种最初由 Xerox 公司开发的 LAN 标准，后来由 DEC、Intel 公司和 Xerox 公司联合开发。在以太网中使用的访问机制称为**带有冲突检测的载波侦听多路存取**（Carrier Sense Multiple Access with Collision Detection，CSMA/CD）。在 CSMA/CD 中，某个基站在传输数据之前，必须检查是否有其他基站正在使用这种媒介。如果没有其他的基站在传输数据，那么该基站就可以发送它的数据了。如果有两个或多个基站同时发送数

据，就可能会产生冲突。因此，所有基站都必须不断地检查传输媒介以检测是否有任何冲突。如果发生冲突，所有基站都将忽略所接收的数据。发送基站在等待一定的时间后再重新发送数据。为了减少第二次冲突的可能性，发送基站分别生成一个随机数，以确定该基站要等待多久才能重新发送数据。

1.1.1.2 令牌环

令牌环是最初由 IBM 开发的一种 LAN 标准，它使用一个逻辑环拓扑。由 CSMA/CD 使用的访问方法可能产生冲突。因此，基站在捕捉到一个好的链路之前，可能会进行多次的数据发送。如果数据流量大，这种冗余会产生不定长的延时。没有办法能预测冲突的发生，也没有办法能预测由多个基站同时试图捕捉链路所产生的延时。令牌环通过让基站依次发送数据，解决了这种不确定性。

作为一种访问方法，令牌按顺序从一个基站传递到另一个基站，直到它遇到一个有数据要发送的基站。要发送数据的基站等待令牌的到来。基站捕捉到令牌后就发送其数据帧。该数据帧沿着这个环前进，每个基站都重新生成该帧。每个中间基站都检查该帧的目标地址，如果发现该帧是指向其他的基站，就把它发送给相邻的基站。要接收该帧的基站识别出它自己的地址后，复制该消息，进行错误检查，并修改该帧最后一个字节中的 4 个位，以表示该地址已经被识别，并且已经复制了该帧。然后，整个数据包继续在环中前进，直到返回到发送它的基站。

1.1.1.3 光纤分布式数据接口

光纤分布式数据接口(Fiber Distributed Data Interface，FDDI)是由 ANSI 和 ITU－T 进行标准化的一种 LAN 协议。它支持 100 Mbps 的数据率，是替代以太网和令牌环的一种高速网络。当设计 FDDI，100 Mbps 的数据率需要光纤光缆。

FDDI 的访问方法称为**令牌传递**(token passing)。在令牌环网络中，当一个基站捕获到一个令牌后，每次只能发送一个帧。在 FDDI 中，令牌传递方法的不同在于访问是由时间来限制的。每个基站有一个计时器，由它显示该令牌何时离开这个基站。如果某个基站接收的令牌比预定的时间早，那么它就保留这个令牌，并进行数据发送，直到既定的离开时间为止。相反，如果某个基站在预定或更晚的时间接收到令牌，它必须把令牌传递给下一个基站，然后等待令牌的下一次到来。

FDDI 实现的是一个双环。在大多数情况下，数据传输使用的是主环，主环发生故障的情况下才使用备用环。当主环发生故障时，就将激活备用环来完成数据传输和维持服务。

1.1.2 广域网

广域网(Wide Area Networks，WAN)提供了在较大地理区域内数据、语音、图像和视频信息的长距离传输，这种地理区域可能是一个国家、一个洲甚至是全世界。与 LAN(它依靠的是自己的硬件进行数据传输)相反，WAN 可以使用公用、租借或专用的通信设备，而且往往还是这三者的组合使用。

1.1.2.1 PPP

点对点协议(Point-to-Point Protocol，PPP)用于通过异步调制解调链路或高速同步租

借线路的数据传输。PPP 帧使用以下格式。

- **标志字段**(Flag field)：每个帧以一个字节的标志开头，这个标志的值为 7E(0111 1110)。该标志用于在发送方和接收方的位级上实现同步化。
- **地址字段**(Address field)：该字段的值为 FF(1111 1111)。
- **控制字段**(Control field)：该字段的值为 03(0000 0011)。
- **协议字段**(Protocol field)：这是一个两字节的字段，如果其值为 0021(0000 0000 0010 0001)，表示的是 TCP/IP。
- **数据字段**(Data field)：数据字段可以多达 1500 个字节。
- **循环冗余校验**(Cyclic redundancy check，CRC)：它含有两字节。CRC 是在物理层实现的，使用在数据链路层中。在数据单元的末尾附加了一个冗余位序列，从而使所得的数据单元可以被预先确定的二进制数字整除。在目的地，输入数据单元除以相同的数字。如果没有余数，就接收这个数据单元。如果有余数，那么这个数据单元在传输中被破坏了，因此必须拒绝接收。

1.1.2.2 X.25

X.25 作为在 WAN 中使用的数据包交换协议被广泛使用。它是由 ITU-T 于 1976 年开发的。X.25 是**数据终端设备**(data terminal equipment，DTE)和**数据电路终端设备**(data circuit terminating equipment，DCE)之间的接口，用于在公用数据网络上的数据包模式下的终端操作。X.25 定义了一个数据包模式终端如何连接到数据包网络中进行数据交换。它描述了创建连接、数据交换、确认、数据流控制以及数据控制所需的过程。

1.1.2.3 帧中继

帧中继是一种 WAN 协议，它弥补 X.25 的不足。X.25 提供了扩展的差错检测和流控制。在路由的每个基站，都对数据包进行正确性进行检测。每个基站保留了原始帧的一个拷贝，直到它接收到从下一个基站发送来的确认信息，表明该帧已完整地到达了下一个基站。这种基站对基站的检测是在 OSI 模式的数据链路层中实现的，但 X.25 只是在网络层上的发送方与接收方之间进行差错检测。发送方保留了原始数据包的一个拷贝，直到它接收到来自最终目的地的确认信息。X.25 上的很多流量都用于了差错检测，以确保服务的可靠性。帧中继不提供差错检测，在数据链路层也不要求进行确认。所有差错检测工作都留给了使用帧中继服务的网络层和传输层上的协议。帧中继只在物理层和数据链路层进行操作。

1.1.2.4 异步传输模式

异步传输模式(Asynchronous Transfer Mode，ATM)是对数据通信基础设施进行重构的革命性想法。它用于在高速率传输媒介(光纤光缆)上进行数据、语音和视频的传输。ATM 是一种进行信元传输的协议。一个信元(cell)即使一个 53 字节长的小的数据单元，由 5 字节的头部和 48 字节的**载荷**(payload)组成。头部含有一个**虚拟路径标志符**(virtual path identifier，VPI)和**虚拟信道标志符**(virtual channel identifier，VCI)。这两个标志符用于把信元通过网络路由到最终目的地。

ATM 网络是一个面向连接的信元交换网络。这意味着，数据单元不是像数据包交换网络中那样的数据包，也不是帧中继中那样的帧，而是一个信元。但是，ATM 与 X.25 和帧