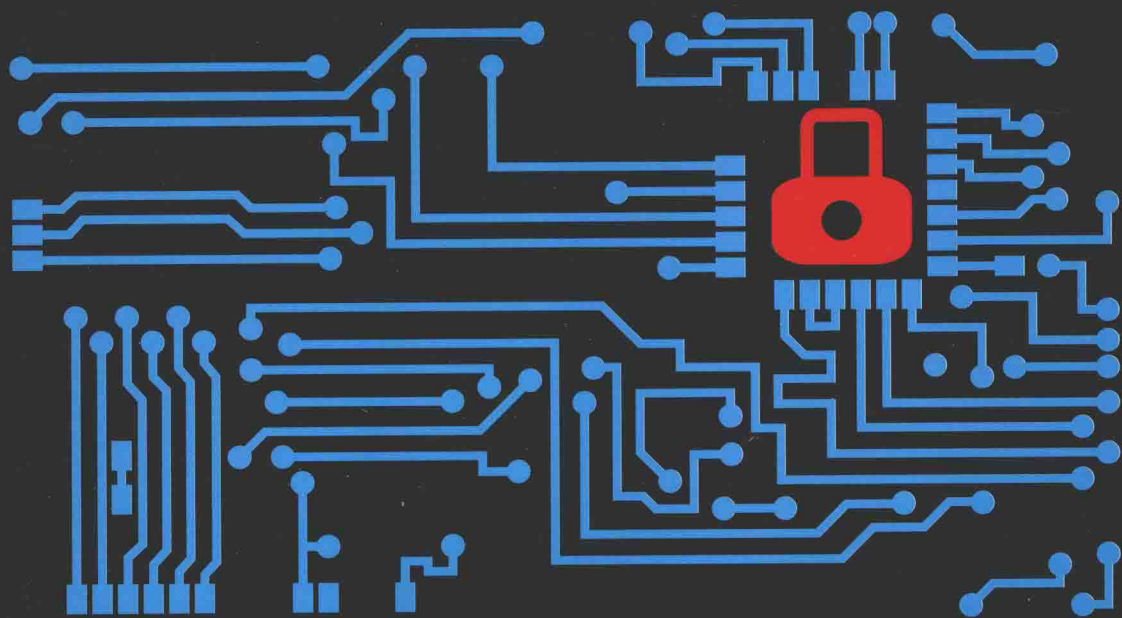


世界著名计算机教材精选

无线移动网络 安全 (第2版)

Man Young Rhee 著

葛秀慧 等译



WIRELESS MOBILE INTERNET SECURITY

Second Edition

清华大学出版社



世界著名计算机教材精选

无线移动网络安全

(第2版)

Man Young Rhee 著
葛秀慧 等译

清华大学出版社
北京

Man Young Rhee

Wireless Mobile Internet Security, Second Edition

EISBN: 978-1-118-49653-4

Copyright © 2015 by Wiley Publishing, Inc.

All Rights Reserved. This translation published under license.

Simplified Chinese translation edition is published and distributed exclusively by Tsinghua University Press under the authorization by John Wiley & Sons Inc., within the territory of the People's Republic of China only, excluding Hong Kong, Macao SAR and Taiwan. Unauthorized export of this edition is a violation of the Copyright Act. Violation of this Law is subject to Civil and Criminal Penalties.

本书中文简体字翻译版由美国 John Wiley & Sons, Inc. 公司授权清华大学出版社在中华人民共和国境内(不包括中国香港、澳门特别行政区和中国台湾)独家出版发行。未经许可之出口,视为违反著作权法,将受法律之制裁。未经出版者预先书面许可,不得以任何方式复制或抄袭本书的任何部分。

北京市版权局著作权合同登记号 图字 01-2014-3591 号

本书封面贴有 John Wiley & Sons 公司防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

图书在版编目(CIP)数据

无线移动网络安全:第2版/(韩)李迈勇著;葛秀慧等译. —北京:清华大学出版社,2016

书名原文:Wireless Mobile Internet Security, 2nd Edition

(世界著名计算机教材精选)

ISBN 978-7-302-43365-1

I. ①无… II. ①李… ②葛… III. ①无线网—移动网—安全技术—教材 IV. ①TN929.5

中国版本图书馆 CIP 数据核字(2016)第 074791 号

责任编辑:龙启铭

封面设计:傅瑞学

责任校对:梁毅

责任印制:何芊

出版发行:清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址:北京清华大学学研大厦 A 座 邮 编:100084

社 总 机:010-62770175 邮 购:010-62786544

投稿与读者服务:010-62776969, c-service@tup.tsinghua.edu.cn

质量反馈:010-62772015, zhiliang@tup.tsinghua.edu.cn

课件下载:<http://www.tup.com.cn>, 010-62795954

印 装 者:北京密云胶印厂

经 销:全国新华书店

开 本:185mm×260mm 印 张:24.75

版 次:2016年9月第1版 字 数:610千字

印 数:1~2000

印 次:2016年9月第1次印刷

定 价:59.00元

产品编号:058684-01

目 录

第 1 章 互连网络与分层模型	1
1.1 互连技术	1
1.1.1 局域网(LAN)	2
1.1.2 广域网(WAN)	3
1.2 互连设备	4
1.2.1 交换机.....	5
1.2.2 中继器.....	5
1.2.3 网桥.....	5
1.2.4 路由器.....	6
1.2.5 网关.....	6
1.3 OSI 模型	7
1.4 TCP/IP 模型	9
1.4.1 网络访问层	10
1.4.2 网际层	10
1.4.3 传输层	11
1.4.4 应用层	11
第 2 章 TCP/IP 协议族与 Internet 栈协议	12
2.1 网络层协议.....	12
2.1.1 网际协议(IP)	12
2.1.2 地址解析协议(ARP)	22
2.1.3 反向地址解析协议(RARP)	25
2.1.4 无类别域间路由选择(CIDR).....	25
2.1.5 IP 版本 6(IPv6 或 IPng).....	26
2.1.6 Internet 控制报文协议(ICMP)	32
2.1.7 Internet 组管理协议(IGMP)	33
2.2 传输层协议.....	33
2.2.1 传输控制协议(TCP)	33
2.2.2 用户数据报协议(UDP)	35
2.3 万维网.....	38
2.3.1 超文本传输协议(HTTP)	38
2.3.2 超文本标记语言	38
2.3.3 通用网关接口	39
2.3.4 Java	39
2.4 文件传输.....	39

2.4.1	文件传输协议(FTP)	40
2.4.2	简单文件传输协议(TFTP)	40
2.4.3	网络文件系统(NFS)	40
2.5	电子邮件	40
2.5.1	简单邮件传输协议(SMTP)	41
2.5.2	邮局协议版本3(POP3)	41
2.5.3	Internet 消息访问协议(IMAP)	42
2.5.4	多用途 Internet 邮件扩展(MIME)	42
2.6	网络管理服务	42
2.7	IP 地址转换	43
2.8	路由选择协议	43
2.8.1	路由信息协议(RIP)	44
2.8.2	开放式最短路径优先(OSPF)	44
2.8.3	边界网关协议(BGP)	44
2.9	远程系统程序	45
2.9.1	TELNET	45
2.9.2	远程登录(Rlogin)	45
2.10	社交网络服务	46
2.10.1	Facebook	46
2.10.2	Twitter	46
2.10.3	Linkedin	46
2.10.4	Groupon	46
2.11	智能 IT 设备	46
2.11.1	智能手机	46
2.11.2	智能 TV	47
2.11.3	视频游戏机	47
2.12	网络安全威胁	47
2.12.1	蠕虫	47
2.12.2	病毒	47
2.12.3	DDoS	47
2.13	Internet 安全威胁	48
2.13.1	网络钓鱼	48
2.13.2	SNS 安全威胁	48
2.14	计算机安全威胁	48
2.14.1	漏洞利用	48
2.14.2	密码破解	49
2.14.3	Rootkit	49
2.14.4	特洛伊木马	49
2.14.5	键盘记录器	49

2.14.6	欺骗攻击	49
2.14.7	数据包嗅探器	50
2.14.8	会话劫持	50
第3章	移动无线技术的总趋势	51
3.1	1G 蜂窝技术	51
3.1.1	高级移动电话系统(AMPS)	51
3.1.2	北欧移动电话(NMT)	51
3.1.3	全接入通信系统(TACS)	51
3.2	2G 移动无线技术	51
3.2.1	蜂窝数字分组数据(CDPD),北美协议	52
3.2.2	全球移动通信系统(GSM)	53
3.2.3	TDMA-136 或 IS-54	54
3.2.4	集成数字增强型网络(iDEN)	54
3.2.5	cdmaOne IS-95A	54
3.2.6	个人数字蜂窝(PDC)	54
3.2.7	i-mode	54
3.2.8	无线应用协议(WAP)	54
3.3	2.5G 移动无线技术	55
3.3.1	增强型电路交换数据(ECSD)	56
3.3.2	高速电路交换数据(HSCSD)	56
3.3.3	通用分组无线服务(GPRS)	56
3.3.4	增强型数据速率 GSM 演进(EDGE)	56
3.3.5	cdmaOne IS-95B	56
3.4	3G 移动无线技术(3G 的形势与地位)	57
3.4.1	通用移动通信系统(UMTS)	59
3.4.2	高速下行分组接入(HSDPA)	60
3.4.3	CDMA2000 1x	60
3.4.4	CDMA2000 1xEV(1x 演进)	60
3.4.5	CDMA2000 1xEV-DO(1x 演进,只是数据)	60
3.4.6	CDMA2000 1xEV-DV(1x 演进,数据和声音)	60
3.5	与 UMTS 安全相关的加密算法	61
第4章	对称分组密码	66
4.1	数据加密标准(DES)	66
4.1.1	算法描述	67
4.1.2	密钥调度	68
4.1.3	DES 加密	70
4.1.4	DES 解密	75
4.1.5	三重 DES	78
4.1.6	使用初始向量的 DES-CBC 密码算法	79

4.2	国际数据加密算法(IDEA)	81
4.2.1	子密钥生成与分配	82
4.2.2	IDEA 加密	84
4.2.3	IDEA 解密	87
4.3	RC5 算法	90
4.3.1	RC5 算法描述	90
4.3.2	密钥扩展	90
4.3.3	加密	95
4.3.4	解密	96
4.4	RC6 算法	101
4.4.1	RC6 描述	101
4.4.2	密钥调度	101
4.4.3	加密	102
4.4.4	解密	105
4.5	AES(Rijndael)算法	112
4.5.1	符号约定	112
4.5.2	数学运算	113
4.5.3	AES 算法规约	115
第 5 章	散列函数、消息摘要与消息认证码	132
5.1	DMDC 算法	132
5.1.1	密钥调度	132
5.1.2	消息摘要计算	136
5.2	高级 DMDC 算法	139
5.2.1	密钥调度	139
5.2.2	计算消息摘要	142
5.3	MD5 消息摘要算法	144
5.3.1	追加填充位	144
5.3.2	追加长度	144
5.3.3	初始化 MD 缓冲区	145
5.3.4	定义 4 个辅助函数(F、G、H 和 I)	145
5.3.5	第 1、2、3、4 轮的 FF、GG、HH 和 II 变换	145
5.3.6	四轮计算(64 步)	146
5.4	安全散列函数	154
5.4.1	消息填充	154
5.4.2	初始化 160 位缓冲区	155
5.4.3	使用的函数	155
5.4.4	使用的常量	156
5.4.5	计算消息摘要	156
5.5	密钥散列消息认证码(HMAC)	160

第 6 章 非对称公钥密码系统	166
6.1 Diffie-Hellman 指数密钥交换	166
6.2 RSA 公钥密码系统	169
6.2.1 RSA 加密算法	169
6.2.2 RSA 签名方案	173
6.3 ElGamal 公钥加密系统	174
6.3.1 ElGamal 加密	175
6.3.2 ElGamal 签名	176
6.3.3 ElGamal 认证方案	178
6.4 Schnorr 公钥加密系统	180
6.4.1 Schnorr 认证方案	180
6.4.2 Schnorr 签名算法	181
6.5 数字签名算法	184
6.6 椭圆曲线加密系统	186
6.6.1 椭圆曲线	186
6.6.2 应用 ElGamal 算法的椭圆曲线密码系统	193
6.6.3 椭圆曲线数字签名算法	194
6.6.4 ECDSA 签名计算	197
第 7 章 公钥基础设施	200
7.1 作为标准的 Internet 出版物	200
7.2 数字签名技术	202
7.3 PKI 实体的功能角色	206
7.3.1 策略审批机构	207
7.3.2 策略证书机构	207
7.3.3 认证中心	209
7.3.4 组织注册机构	209
7.4 PKI 操作的要素	210
7.4.1 分层的树形结构	210
7.4.2 策略制定机构	211
7.4.3 交叉认证	212
7.4.4 X.500 识别名	214
7.4.5 安全密钥的产生与分配	215
7.5 X.509 证书格式	216
7.5.1 X.509 v1 证书格式	216
7.5.2 X.509 v2 证书格式	217
7.5.3 X.509 v3 证书格式	218
7.6 证书吊销列表	223
7.6.1 CRL 字段	223
7.6.2 CRL 扩展	225

7.6.3	CRL 项扩展	226
7.7	证书路径验证	227
7.7.1	基本路径验证	227
7.7.2	扩展路径验证	228
第 8 章	网络层安全	230
8.1	IPSec 协议	230
8.1.1	IPSec 协议文档	231
8.1.2	安全关联(SA)	232
8.1.3	散列消息认证码	233
8.2	IP 认证首部	236
8.2.1	认证首部格式	236
8.2.2	认证首部位置	237
8.3	IP 封装安全有效载荷	239
8.3.1	ESP 数据包格式	239
8.3.2	ESP 首部位置	240
8.3.3	加密与认证算法	242
8.4	IPSec 的密钥管理协议	243
8.4.1	Oakley 密钥确定协议	244
8.4.2	ISAKMP	244
第 9 章	传输层安全: SSLv3 与 TLSv1	256
9.1	SSL 协议	256
9.1.1	会话与连接状态	256
9.1.2	SSL 记录协议	257
9.1.3	SSL 更改密码规范协议	260
9.1.4	SSL 警报协议	260
9.1.5	SSL 握手协议	261
9.2	密码计算	266
9.2.1	计算主密钥	266
9.2.2	将主密钥转换成密码参数	267
9.3	TLS 协议	268
9.3.1	HMAC 算法	268
9.3.2	伪随机函数	271
9.3.3	错误警报	275
9.3.4	证书验证消息	276
9.3.5	已完成消息	276
9.3.6	TLS 密码计算	276
第 10 章	电子邮件安全: PGP 与 S/MIME	278
10.1	PGP	278
10.1.1	通过加密获得机密性	278

10.1.2	通过数字签名进行认证	279
10.1.3	压缩	280
10.1.4	Radix-64 转换	281
10.1.5	数据包首部	285
10.1.6	PGP 数据包结构	287
10.1.7	密钥信息数据包	289
10.1.8	PGP 5.x 的算法	293
10.2	S/MIME	294
10.2.1	MIME	295
10.2.2	S/MIME	300
10.2.3	S/MIME 增强安全服务	303
第 11 章	可信系统的 Internet 防火墙	306
11.1	防火墙的角色	306
11.2	防火墙相关术语	307
11.2.1	堡垒主机	307
11.2.2	代理服务器	308
11.2.3	SOCKS	308
11.2.4	阻止点	309
11.2.5	隔离区(DMZ)	309
11.2.6	日志与报警	309
11.2.7	VPN	309
11.3	防火墙类型	310
11.3.1	包过滤	310
11.3.2	电路级网关	314
11.3.3	应用级网关	314
11.4	防火墙设计	315
11.4.1	屏蔽主机防火墙(单宿主堡垒主机)	315
11.4.2	屏蔽主机防火墙(双宿主堡垒主机)	316
11.4.3	屏蔽子网防火墙	317
11.5	针对网络攻击的 IDS	317
11.5.1	Internet 蠕虫检测	318
11.5.2	计算机病毒	318
11.5.3	特殊的病毒	319
11.6	入侵检测系统	319
11.6.1	基于网络的入侵检测系统(NIDS)	320
11.6.2	无线入侵检测系统(WIDS)	321
11.6.3	网络行为分析系统(NBAS)	322
11.6.4	基于主机的入侵检测系统(HIDS)	323
11.6.5	基于特征的系统	324
11.6.6	基于异常的系统	325

11.6.7	IDS系统的隐遁技术	326
第12章	电子商务交易的SET	328
12.1	对SET的商务需求	328
12.2	SET系统的参与者	329
12.3	加密操作原则	332
12.4	双签名与签名验证	332
12.5	身份验证与消息完整性	335
12.6	支付处理	339
12.6.1	持卡人注册	339
12.6.2	商家注册	342
12.6.3	购买请求	343
12.6.4	支付授权	344
12.6.5	支付兑现	346
第13章	4G无线Internet通信技术	348
13.1	移动WiMAX	348
13.1.1	移动WiMAX网络架构	349
13.1.2	WiMAX网络参考模型(NRM)的参考点	351
13.1.3	关键支持技术	352
13.1.4	移动WiMAX网络与蜂窝无线网络间的比较	354
13.2	WiBro(无线宽带)	355
13.2.1	WiBro网络架构	355
13.2.2	WiBro系统配置的关键要素	356
13.2.3	HSDPA与WiBro间的系统对比	357
13.2.4	WiBro操作的关键特征	358
13.3	超级移动宽带(UMB)	359
13.3.1	UMB的设计目标	359
13.3.2	可用的UMB关键技术	360
13.3.3	基于IP网络架构的UMB	361
13.3.4	结论性评论	362
13.4	长期演进(LTE)	362
13.4.1	LTE特性与功能	363
13.4.2	LTE帧结构	363
13.4.3	用于下行的LTE时频结构	363
13.4.4	上行的LTE SC-FDMA	364
13.4.5	LTE网络架构	366
13.4.6	支持LTE设计的关键组件	367
13.4.7	结论	369

第 1 章 互连网络与分层模型

现在,Internet 是广泛应用的信息基础设施,但本质上,Internet 是一种不安全的发送信息的信道。当从一个 Web 站点向另一个站点发送消息(或数据包)时,在消息中的数据到达目的地之前,要路由通过多个中间站点。Internet 能兼容各种异构平台,从而使得使用不同计算机与操作系统的人们可以互相通信。Internet 的历史比较复杂,主要体现在技术、组织和社区等方方面面的复杂性。随着电子商务、信息获取与社区交互的发展,Internet 也迈上了一个新的台阶。

早期的 ARPANET 研究人员完成了包交换技术的最初示范。在 20 世纪 70 年代后期,Internet 的发展被认可,随后,随着对协调机制需求的增长,感兴趣的研究社区规模也在扩大。美国国防高级研究计划局(Defense Advanced Research Projects Agency,DARPA)成立了国际合作委员会(International Cooperation Board,ICB),以配合一些专注于数据包卫星研究的欧洲国家的活动,而 **Internet 配置控制委员会**(Internet Configuration Control Board,ICCB)协助 DARPA 管理 Internet 活动。1983 年,DARPA 意识到,Internet 社区的持续增长需要重组协调机制。ICCB 被解散,取而代之的是,根据任务组的主席职位,成立了 **Internet 活动委员会**(Internet Activities Board,IAB)。IAB 使 **Internet 工程任务组**(Internet Engineering Task Force,IETF)有了转机,成为 IAB 成员。到 1985 年,出现了越来越多更实用的 Internet 工程。这种增长导致工作组形式的 IETF 子结构的诞生。DARPA 不再是 Internet 资金的主要来源。从那时起,DARPA 在 Internet 活动中的作用越来越小。IAB 意识到 IETF 越来越重要,重组并确认 **Internet 工程指导小组**(Internet Engineering Steering Group,IESG)作为主要标准的审查机构。除 IETF 之外,IAB 重组成立了 **Internet 研究任务组**(Internet Research Task Force,IRTF)。

最初,Internet 主要用于科学研究,但 20 世纪 80 年代初,Internet 的发展已超出了最初的研究初衷,出现了大量的用户群体,且增加了商业活动。这种增长使商业部门越来越关注相关的标准进程。随着关注越来越多,事情得到进展,最终于 1991 年成立了 **Internet 协会**(Internet Society,IS)。1992 年,重组了 **Internet 活动委员会**(Internet Activities Board,IAB),更名为 **Internet 架构委员会**(Internet Architecture Board,IAB),在 Internet 协会主持下运作。新的 IAB、IESG 与 IETF 间的相互支持关系使之能更好地执行标准的批准、制定服务及一些措施,这些都有利于 IETF 工作的开展。

1.1 互连技术

数据信号通过一种或多种传输介质(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。网络互连技术包括**局域网**(Local Area Networks,LAN)到**广域网**(Wide Area Networks,WAN)。局域网是指有限地理区域内(如单个建筑、

公寓或校园)的网络;广域网是指跨越较大地理区域(如一个国家、一个洲甚至是全世界)的网络。

1.1.1 局域网(LAN)

LAN 是一种通信系统,它允许有限地理区域内(如单独的办公楼、仓库或校园)的多个独立设备之间进行直接的相互通信。LAN 有三种标准化的体系结构:以太网(Ethernet)、令牌环(token ring)和光纤分布式数据接口(Fiber Distributed Data Interface,FDDI)。

以太网

以太网是一种 LAN 的标准,最初由 Xerox 公司开发,后来由 DEC、Intel 公司和 Xerox 公司联合开发并扩展。以太网使用的访问机制是带冲突检测的载波侦听多路访问(Carrier Sense Multiple Access with Collision Detection,CSMA/CD)。在 CSMA / CD 中,在一个基站传输数据之前,它必须侦听介质,以确定是否有其他基站正在使用该介质。如果没有其他基站在传输数据,则这个基站可以发送它自己的数据。如果两个或多个基站同时发送数据,就会产生冲突。因此,所有基站都必须不断地监听介质,检测可能产生的任何冲突。如果发生冲突,所有基站会忽略所接收的数据。发送基站需要等待一段时间后,再发送数据。为了减少产生第二次冲突的可能性,发送基站会分别产生随机数,以确定该基站需要等待多久才能重新发送数据。

令牌环

令牌环是一种 LAN 标准,最初由 IBM 公司开发,它使用逻辑环形拓扑结构。CSMA/CDP 所用的访问方法可能会产生冲突。因为,基站在捕获完美的传输链路之前,可能尝试多次发送数据。如果数据流量很大,这种冗余会产生不确定长度的延迟。因此,CSMA/CD 没有办法预测冲突发生,也没有办法预测由多个基站试图同时捕获链路所产生的延迟。而令牌环通过让基站轮流发送数据来解决 CSMA / CD 存在的这种不确定性问题。

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,直到它遇到需要发送数据的基站为止。要发送数据的基站都必须等待令牌。当一个基站捕获令牌后,就能发送自己的数据帧。这个数据帧绕着环继续前行,每个基站都重新生成该数据帧。中间的每个基站都检查目的地地址,如果发现这个数据帧是对另一个基站寻址,就将它中继到其相邻的基站。预定接收的基站识别自身的地址,复制该消息、进行差错校验,并修改数据帧中最后一个字节的四位,表示该地址已被确认,且复制了数据帧。然后,完整的数据包继续在环中前行,直到返回发送它的基站。

光纤分布式数据接口

光纤分布式数据接口(FDDI)是一种由美国国家标准协会(American National Standards Institute,ANSI)和 ITU-T 提出的标准化 LAN 协议。它支持 100 Mbps 的数据速率,并提供了替代以太网和令牌环的高速网络。当设计 FDDI 时,需要使用光纤电缆以支持 100 Mbps 的数据速率。

FDDI 的访问方法也称为令牌传递(token passing)。在令牌环网络中,基站每次捕获令牌时,只能发送一个帧。在 FDDI 中,令牌传递机制略有不同,其访问是定时的。每个基站

维护一个计时器,来显示令牌必须离开基站的时间。如果基站接收令牌的时间早于预定时间,则它可以持有令牌并发送数据,直到预定的离开时间为止。另一方面,如果基站在预定时间或更晚的时间接收到令牌,则它必须将令牌传递给下一个基站,并等待令牌的下一轮到来。

FDDI 的实现是一个双环。在大多数情况下,数据传输都使用主环。主环发生故障的情况下才使用备用环。当主环出现问题时,将激活备用环来完成数据传输和维护服务。

1.1.2 广域网(WAN)

WAN 提供跨越广阔地理区域的数据、语音、图像与视频信息的远距离传输,其跨越的地理区域可能是一个国家、一个洲乃至全世界。相比之下,局域网依靠自己的硬件进行传输,而广域网则利用公共的、租赁的或专用通信设备进行传输,且往往混合使用这些通信设备。

PPP

点对点协议(Point-to-Point Protocol,PPP)设计用于处理使用异步调制解调器链路或高速同步租赁线路的数据传输。PPP 帧使用如下的格式:

- 标志字段(Flag field): 每个帧以一个字节的标志作为开始,其值是 7E(01111110)。该标志用于在位级上同步发送方与接收方。
- 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): 这是两个字节的字段,其值为 0021(0000 0000 0010 0001),表示传输控制协议/网际协议(Transmission Control Protocol/Internet Protocol,TCP/IP)。
- 数据字段(Data field): 数据字段多达 1500 个字节。
- CRC: 这是两个字节的循环冗余校验(Cyclic Redundancy Check,CRC)。CRC 在物理层实现,但用于数据链路层。在数据单元末尾附加冗余位(CRC)序列,使所得的数据单元能被预定的二进制数整除。在其目的地,输入数据单元除以相同的数。如果没有余数,就接收这个数据单元。如果有余数存在,那么这个数据单元在传输中已被破坏,因此必须拒绝接收这个数据单元。

X.25

X.25 是广泛用于 WAN 的包交换协议。在 1976 年,ITU-T 开发了 X.25。X.25 是数据终端设备与数据电路终端设备之间的接口,用于数据包模式下公共数据网络的终端操作。

X.25 定义了数据包模式终端如何连接到数据包网络以进行数据交换。它描述了建立连接、数据交换、确认、流控制和数据控制所需的过程。

帧中继

帧中继是一种 WAN 协议,其设计目标是弥补 X.25 的缺陷。X.25 提供了扩展的差错校验和流控制。在数据包路由经过的每个基站,都要对数据包进行准确性校验。每个基站都保留原始帧的一个副本,直到它收到下一个基站的确认,证实该帧已完好无缺地到达为

止。这种基站到基站的校验是在**开放系统互连**(Open Systems Interconnect, OSI)模型的数据链路层实现,但 X.25 只在网络层对发送方与接收方进行差错校验。发送方一直保留源数据包的副本,直到它接收到来自最终目的地的确认为止。X.25 网络中的大部分流量都专用于差错校验,以确保服务的可靠性。帧中继在数据链路层不提供差错校验或进行确认。相反,所有差错校验都留给使用帧中继服务的网络层和传输层协议。帧中继只工作于物理层和数据链路层。

异步传输模式

异步传输模式(Asynchronous Transfer Mode, ATM)是一种具有创新性的重构数据通信基础设施的想法。它旨在支持数据、语音和视频能在高数据率传输媒介(光纤电缆)上传输。ATM 是一种信元传输协议。信元是一个长度为 53 字节的小数据单元,由 5 个字节的报首部和 48 个字节的**有效载荷**组成。报首部包含一个**虚拟路径识别符**(Virtual Path Identifier, VPI)和**虚拟信道识别符**(Virtual Channel Identifier, VCI)。根据这两个标识符,路由器将信元路由到网络的最终目的地。

ATM 网络是面向连接的信元交换网络。这意味着,数据单元既不是包交换网络的数据包,也不是帧中继的帧,而是信元。但是,ATM 与 X.25 和帧中继一样,也是一种面向连接的网络,也就是说,在两个系统进行通信之前,必须先建立连接。为了启动连接,系统使用 20 字节的地址。在建立连接之后,VPI/VCI 的组合可以将信元从其源端引导到最终目的地。

1.2 互连设备

互连设备用于将各个网段连接起来或将网络连接成互连网络。这些设备分为五类:交换机、中继器、网桥、路由器和网关。除了交换机之外,其余设备都与 OSI 模型中不同层的协议进行交互。

中继器转发所有电信号且只工作于物理层。网桥存储和转发完整的数据包,并影响着单个局域网的流量控制。网桥工作于物理层和数据链路层。路由器为两个独立局域网之间提供链路,它工作于物理层、数据链路层和网络层。最后,网关为不兼容的局域网或应用之间提供转换服务,它工作于所有层。

互连设备与 OSI 模型不同层的协议进行交互的示意图如图 1.1 所示。

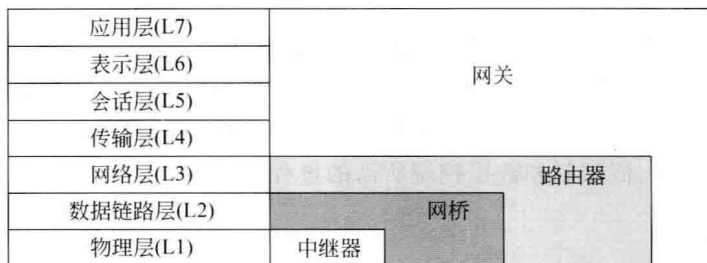


图 1.1 互连设备

1.2.1 交换机

交换网络由一系列互连的交换机组成。交换机是一种硬件/软件设备,能够在两个或多个与交换机相连的设备之间建立临时连接,但不是建立交换机之间的连接。交换机制一般分为三种方法:电路交换、数据包交换和消息交换。

- 电路交换:电路交换是在两个设备(如电话或计算机)之间建立直接的物理连接。一旦两个系统之间建立了连接,电路交换就在两个终端用户之间建立了专用路径。只要终端用户需要,就可以一直使用这条路径。
- 数据包交换:数据包交换为数据传输提供了一种更为合理的解决方案。在数据包交换网络中,数据以离散的、长度可变的分组(称为数据包)为单元进行传输。每个数据包不仅包含数据,还包含含有控制信息的首部。数据包被发送到网络,从一个节点传输到另一个节点。在每个节点,在根据数据包的首部信息对数据包进行发送之前,都会对数据包进行临时存储。

在数据包交换的数据报方法中,对每个数据包都进行单独处理,就像它单独存在一样。在数据包交换的虚电路方法中,如果在会话开始时,发送方与接收方只选择了一条线路,则所有数据包都沿着这条线路逐个传输。虽然电路交换和虚电路方法看似相同,但两者之间存在着本质区别。在电路交换中,两个终端用户之间的路径只有一个信道。在虚电路中,线路并非是两个用户专用。线路被分为多个信道,每个信道只是使用了线路中的一个信道。

- 消息交换:消息交换被称为存储与转发方法(store and forwarding method)。在这种方法中,计算机(或节点)接收消息时,一直会存储消息,在合适的线路空闲之后,再把消息发送出去。现在,这种方法已被淘汰。

1.2.2 中继器

中继器是一种电子设备,它只工作于 OSI 模型的物理层。中继器将来自一个网段的传输信号放大,再继续将信号转发到另一个网段。因此,中继器可以扩展网络的物理距离。由于噪声及数据信号的衰减,携带信息的信号在网络中只能传输有限的距离。中继器就是在信号失真之前,接收信号,重新生成信号的原始的比特模式,并在链路中对再生的信号副本进行转发。

1.2.3 网桥

网桥工作在 OSI 模型的物理层和数据链路层。单个网桥就能将不同类型的网络连接在一起,并提升网络间的互连性。网桥将大型网络划分成较小的网段。与中继器不同,网桥包含逻辑,从而使每个网段都保持独立的流量。网桥有足够的智能,能将数据帧转发给预定的接收者,还能过滤流量。事实上,这种过滤操作使网桥功能增加,能控制拥塞、隔离有问题的链路,并且通过这种对流量的分割,提升网络的安全性。

网桥可以访问与之相连的所有基站的物理地址。当一个数据帧到达网桥时,网桥不仅再生信号,还会检查目的地址,并将新副本转发到该地址所属的网段。当网桥遇到数据包

时,它读取数据帧所包含的地址,并把该地址与和它相连的两个网段中所有基站表进行比较。当找到匹配的基站,它会找到基站所属的网段,并只将数据包转发到这个网段。

1.2.4 路由器

路由器工作在 OSI 模型的物理层、数据链路层和网络层。路由器所连接的各种网络形成了 Internet。数据报从源端到目的地的过程中,在到达附属于目的网络的路由器之前,会经过多个路由器。路由器决定数据包所经由的路径。路由器在多个互连的网络中转发数据包,特别是 IP 路由器在与之相连的网络中转发 IP 数据报的情况。路由器使用数据报的地址来选择转发数据报的下一跳。数据包要从一个网络的基站发送到相邻网络的另一个基站,先要经过两个网络共有的路由器,该路由器会将数据包交换到目的网络。事实上,构造 Internet 的最简单方法就是用路由器连接两个或多个网络。路由器能连接多种不同类型的物理网络:以太网、令牌环、点对点链路和 FDDI 等。

- 路由模块接收来自处理模块的 IP 数据包。如果数据包将被转发,则它必须将 IP 数据包传递给路由模块。它先在要转发的数据包中找到下一个基站的 IP 地址和接口号。然后,将含有信息的数据包发送给拆分模块。拆分模块参照 MTU 表,找到特定端口号的最大传输单元(Maximum Transfer Unit,MTU)。
- 路由模块使用路由表来确定数据包的下一跳地址。每个路由器都维护一个路由表,该表的每一项都对应一个目的地网络。每个表项包括目的地网络的 IP 地址、到达目的地的最短距离(以跳数计)和数据包要到达最终目的地必须经过的下一个路由器(下一跳)。跳数是数据包从源端到最终目的地所经过的网络数。当路由器准备转发数据包时,它必须有路由表作为参考。路由表应当指定数据包的最佳路径。路由表可以是静态的,也可以是动态的。静态路由表是不经常改变的。当 Internet 的某处发生变化时,动态路由表会自动更新。现在,Internet 所需的是动态路由表。
- 路由开销:路由开销是通过网络的成本。特定路由器的总开销等于包含了该路由器的所有网络的开销总和。路由器选择最小开销(最小值)的路径。分配给每个网络的路由开销取决于协议的类型。路由信息协议(Routing Information Protocol,RIP)将每个网络看作一跳。因此,如果数据包经过 10 个网络到达目的地,则总成本为 10 跳。开放式最短路径优先(Open Shortest Path First,OSPF)协议允许管理员根据网络所需服务类型,为所经过的网络分配成本。这样,通过网络的路由有不同的成本。OSPF 允许路由器根据所需服务的类型拥有几种路由表。边界网关协议(Border Gateway Protocol,BGP)定义的路由开销完全不同。在 BGP 中,策略标准由管理员设置。这个策略定义了应选择的路径。

1.2.5 网关

网关工作于 OSI 模型的所有层中。传统上,将 Internet 上所有的路由设备都称为网关(gateway)。网关是一个协议转换器,它连接两个或多个异构系统,并负责这些系统之间的转换。因此,网关是指设备间执行协议转换的设备。网关接收一个协议格式的数据包,并在转发数据包之前,将其转换为另一个协议格式的数据包。网关知道连接到路由器的每个网