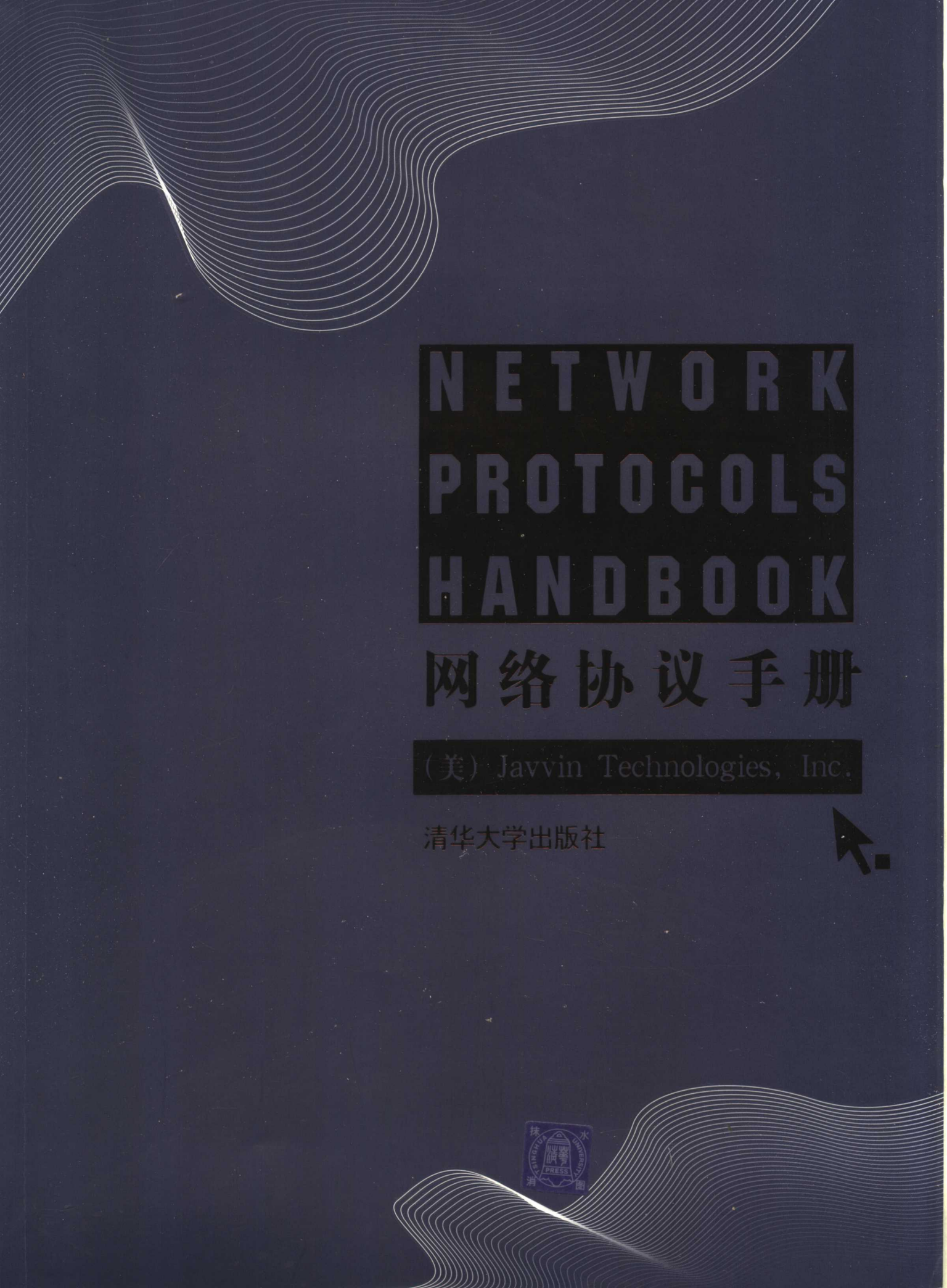




NETWORK PROTOCOLS HANDBOOK

网络协议手册

(美) Javvin Technologies, Inc.

清华大学出版社



NETWORK PROTOCOLS HANDBOOK

网络协议手册

(美) Javvin Technologies, Inc.



江苏工业学院图书馆
藏书章

清华大学出版社
北京

内 容 简 介

本书纵观网络协议,阐释和总结了所有常用网络通信协议,包括 TCP/IP, security, VoIP, WAN, LAN, MAN, SAN 等. 本书也囊括了 Cisco, Novell, IBM, Microsoft, Apple 等厂商的网络协议.

这本书可供信息技术和网络专业人员作为参考书和手册,也可供高校相关专业的学生作为参考.

版权所有,翻印必究. 举报电话: 010-62782989 13501256678 13801310933

本书封面贴有清华大学出版社防伪标签,无标签者不得销售.

本书防伪标签采用特殊防伪技术,用户可通过在图案表面涂抹清水,图案消失,水干后图案复现;或将表面膜揭下,放在白纸上用彩笔涂抹,图案在白纸上再现的方法识别真伪.

图书在版编目(CIP)数据

网络协议手册/美国 Javvin 技术有限公司著. —北京:清华大学出版社,2005. 10

书名原文: Network Protocols Handbook

ISBN 7-302-10959-1

I. 网… II. 美… III. 计算机网络—通信协议—技术手册 IV. TN915.04-62

中国版本图书馆 CIP 数据核字(2005)第 048117 号

出 版 者: 清华大学出版社

<http://www.tup.com.cn>

社 总 机: 010-62770175

地 址: 北京清华大学学研大厦

邮 编: 100084

客户服务: 010-62776969

责任编辑: 赵彤伟

封面设计: 常雪影

印 刷 者: 清华大学印刷厂

装 订 者: 三河市李旗庄少明装订厂

发 行 者: 新华书店总店北京发行所

开 本: 210×285 印张: 19.25 插页: 1 字数: 850 千字

版 次: 2005 年 10 月第 1 版 2005 年 10 月第 1 次印刷

书 号: ISBN 7-302-10959-1/TN·279

印 数: 1~3000

定 价: 49.00 元

Preface

We are living in the information technologies (IT) age. The IT provides us many powerful tools that have significantly changed our way of life, work and business operations. Among all the IT advancements, Internet has the most impact on our society in every aspect for the past 20 years. From Internet, people can get instant news, communicate with others, use it as a super-encyclopedia and find anything that they are interested in via search engines at their finger tips; Company can conduct business to business (B2B), business to consumer (B2C), with great efficiency; Government can announce policies, publicize regulations, and provide administrative information and services to the general public. Internet not only provides unprecedented convenience to our daily life, but also opens up new areas of disciplines and commercial opportunities that have boosted overall economy by creating many new jobs. It is reported that Internet will become a \$ 20 trillion industry in the near future.

The Internet has also made significant progress and rapid adoption in China. According to the 14th Statistical Survey Report on the Internet Development in China announced on July 20, 2004 by China Internet Network Information Center (CNNIC), there are about 87 million Internet users as counted by the end of June 2004, in mainland China, second only to the US; There are about 36 million computer hosts; The number of domain names registered under CN is 382 216; The number of "www" websites is 626 600. It should be also noted that China has started its China Next Generation Internet (CNGI) project at the beginning of 2000, right after US and Europe started the similar initiatives. China now is becoming one of the most important and influential members not only in the World Trade Organization, but also within the Internet community.

To build the Internet and many other networks, engineers and organizations around the world have created many technologies over the past 20 years, in which network protocol is one of the key technology areas. After years of development on the communication standards and generations of networking architecture, network communication protocols have become a very complex subject. Various standard organizations have defined many communication protocols and all major vendors have their own proprietary technologies. Yet, people in the industry are continuously proposing and designing new protocols to address new problems in the network communications. It has become a huge challenge for IT and network professionals at all levels to understand the overall picture of communication protocols and to keep up with the pace of its on-going evolutions.

Javvin Company, based on Silicon Valley in California, USA, is a network software provider. This book is one of its contributions to provide an overview of network protocols and to serve as a reference and handbook for IT and network professionals. The book fully explains and reviews all commonly used network communication protocols, including TCP/IP, security, VoIP, WAN, LAN, MAN, SAN and ISO protocols. It also covers Cisco, Novell, IBM, Microsoft, Apple and DEC network protocols. Hundreds of hyperlinks of references for further reading and studies are available in the book. It is an excellent reference for Internet programmers, network professionals and college students who are majoring IT and networking technology. It is also useful for individuals who want to know more details about the technologies underneath the Internet. I highly recommend this book to our readers.

Ke Yan, Ph. D.

Chief Architect of Juniper Networks
Founder of NetScreen Technologies

Table of Contents

Network Communication Architecture and Protocols	1
OSI Network Architecture 7-Layer Model	2
TCP/IP 4-Layer Architecture Model	5
Other Network Architecture Models; IBM SNA	6
Network Protocol: Definition and Overview	8
Protocols Guide	10
TCP/IP Protocols	10
Application Layer Protocols	13
BOOTP: Bootstrap Protocol	13
DCAP: Data Link Switching Client Access Protocol	14
DHCP: Dynamic Host Configuration Protocol	14
DNS: Domain Name System (Service) Protocol	15
FTP: File Transfer Protocol	16
Finger: User Information Protocol	18
HTTP: Hypertext Transfer Protocol	19
S-HTTP: Secure Hypertext Transfer Protocol	20
IMAP and IMAP4: Internet Message Access Protocol (version 4)	21
IRCP: Internet Relay Chat Protocol	22
LDAP: Lightweight Directory Access Protocol (version 3)	23
MIME (S-MIME): Multipurpose Internet Mail Extensions and Secure MIME	24
NAT: Network Address Translation	25
NNTP: Network News Transfer Protocol	26
NTP: Network Time Protocol	27
POP and POP3: Post Office Protocol (version 3)	28
rlogin: Remote Login in UNIX Systems	29
RMON: Remote Monitoring MIBs (RMON1 and RMON2)	30
SLP: Service Location Protocol	32
SMTP: Simple Mail Transfer Protocol	33
SNMP: Simple Network Management Protocol	33
SNMPv1: Simple Network Management Protocol (version 1)	34
SNMPv2: Simple Network Management Protocol (version 2)	36
SNMPv3: Simple Network Management Protocol (version 3)	37
SNTP: Simple Network Time Protocol	38
TELNET: Terminal Emulation Protocol of TCP/IP	39
TFTP: Trivial File Transfer Protocol	40
URL: Uniform Resource Locator	41
Whois (and RWhois): Remote Directory Access Protocol	42
X Window/X Protocol: X Window System Protocol	42
Presentation Layer Protocol	44
LPP: Lightweight Presentation Protocol	44
Session Layer Protocol	45
RPC: Remote Procedure Call Protocol	45

Transport Layer Protocols	47
ITOT: ISO Transport Service on Top of TCP	47
RDP: Reliable Data Protocol	47
RUDP: Reliable User Datagram Protocol (Reliable UDP)	49
TALI: Tekelec's Transport Adapter Layer Interface	50
TCP: Transmission Control Protocol	50
UDP: User Datagram Protocol	52
Van Jacobson: Compressed TCP Protocol	52
Network Layer Protocols	54
Routing Protocols	54
BGP(BGP-4): Border Gateway Protocol	54
EGP: Exterior Gateway Protocol	54
IPv4: Internet Protocol (version 4)	55
IPv6: Internet Protocol (version 6)	56
ICMP and ICMPv6: Internet Control Message Protocol and ICMP(version 6)	57
IRDP: ICMP Router Discovery Protocol	58
Mobile IP: IP Mobility Support Protocol for IPv4 and IPv6	60
NARP: NBMA Address Resolution Protocol	61
NHRP: Next Hop Resolution Protocol	62
OSPF: Open Shortest Path First Protocol (version 2)	63
RIP: Routing Information Protocol (RIP2)	64
RIPng: Routing Information Protocol Next Generation for IPv6	65
RSVP: Resource ReSerVation Protocol	65
VRRP: Virtual Router Redundancy Protocol	66
Multicast Protocols	67
BGMP: Border Gateway Multicast Protocol	67
DVMRP: Distance Vector Multicast Routing Protocol	68
IGMP: Internet Group Management Protocol	69
MARS: Multicast Address Resolution Server	70
MBGP: Multiprotocol BGP	71
MOSPF: Multicast Extensions to OSPF	72
MSDP: Multicast Source Discovery Protocol	73
MZAP: Multicast-Scope Zone Announcement Protocol	74
PGM: Pragmatic General Multicast Protocol	75
PIM-DM: Protocol Independent Multicast-Dense Mode	76
PIM-SM: Protocol Independent Multicast-Sparse Mode	77
MPLS Protocols	77
MPLS: Multiprotocol Label Switching	77
CR-LDP: Constraint-Based Label Distribution Protocol	79
LDP: Label Distribution Protocol	79
RSVP-TE: Resource ReSerVation Protocol-Traffic Engineering	80
Data Link Layer Protocols	82
ARP and InARP: Address Resolution Protocol and Inverse ARP	82
IPCP and IPv6CP: IP Control Protocol and IPv6 Control Protocol	82
RARP: Reverse Address Resolution Protocol	83
SLIP: Serial Line IP	84
Network Security Technologies and Protocols	86
AAA Protocols	87
Kerberos: Network Authentication Protocol	87

RADIUS: Remote Authentication Dial In User Service	87
SSH: Secure Shell Protocol	88
Tunnelling Protocols	90
L2F: Layer 2 Forwarding Protocol	90
L2TP: Layer 2 Tunnelling Protocol	90
PPTP: Point-to-Point Tunnelling Protocol	92
Secured Routing Protocols	94
DiffServ: Differentiated Service	94
GRE: Generic Routing Encapsulation	94
IPSec: Security Architecture for IP	95
IPSec AH: IPSec Authentication Header	96
IPSec ESP: IPSec Encapsulating Security Payload	97
IPSec IKE: Internet Key Exchange Protocol	98
IPSec ISAKMP: Internet Security Association and Key Management Protocol	98
TLS: Transport Layer Security Protocol	99
Other Security Protocol	101
SOCKSv5: Protocol for Sessions Traversal Across Firewall Securely	101
Voice over IP and VoIP Protocols	102
Signalling	104
H. 323: VoIP Protocols	104
H. 225.0: Call Signalling Protocols and Media Stream Packetization for Packet-Based Multimedia Communication Systems	105
H. 235: Security and Encryption for H-Series (H. 323 and Other H. 245-Based) Multimedia Terminals	106
H. 245: Control Protocol for Multimedia Communication	107
Megaco/H. 248: Media Gateway Control Protocol	109
MGCP: Media Gateway Control Protocol	110
RTSP: Real-Time Streaming Protocol	111
SAP: Session Announcement Protocol	112
SDP: Session Description Protocol	114
SIP: Session Initiation Protocol	115
SCCP (Skinny): Cisco Skinny Client Control Protocol	116
T. 120: Multipoint Data Conferencing and Real-Time Communication Protocols	117
Media/CODEC	119
G. 7xx: Audio (Voice) Compression Protocols	119
H. 261: Video Coding and Decoding (CODEC)	120
H. 263: Video Coding and Decoding (CODEC)	121
RTP: Real-Time Transport Protocol	123
RTCP: RTP Control Protocol	124
Other VoIP Protocols	126
COPS: Common Open Policy Service	126
SCTP: Stream Control Transmission Protocol	126
TRIP: Telephony Routing over IP	127
Wide Area Network and WAN Protocols	129
ATM Protocols	130
ATM: Asynchronous Transfer Mode Reference Model	130
ATM Layer: Asynchronous Transfer Mode Layer	131
AAL: ATM Adaptation Layer (AAL0, AAL2, AAL3/4, and AAL5)	132
ATM UNI: ATM Signalling User-to-Network Interface	134

LANE NNI; ATM LAN Emulation NNI	136
LANE UNI; ATM LAN Emulation UNI	138
MPOA; Multi-Protocol Over ATM	140
ATM PNNI; ATM Private Network-to-Network Interface	142
Q. 2931; ATM Signalling for B-ISDN	143
SONET/SDH; Synchronous Optical Network and Synchronous Digital Hierarchy	144
Broadband Access Protocols	147
BISDN; Broadband Integrated Service Digital Network (Broadband ISDN)	147
ISDN; Integrated Service Digital Network	148
LAP-D; ISDN Link Access Protocol-Channel D	149
Q. 931; ISDN Network Layer Protocol for Signalling	151
DOCSIS; Data Over Cable Service Interface Specification	152
xDSL; Digital Subscriber Line Technologies (DSL, IDSL, ADSL, HDSL, SDSL, VDSL, and G. Lite)	152
Point-to-Point Protocols	154
PPP; Point-to-Point Protocols	154
BAP; PPP Bandwidth Allocation Protocol	155
BACP; PPP Bandwidth Allocation Control Protocol	155
BCP; PPP Bridging Control Protocol	155
EAP; PPP Extensible Authentication Protocol	156
CHAP; Challenge Handshake Authentication Protocol	157
LCP; PPP Link Control Protocol	158
MPPP; MultiLink Point-to-Point Protocol (MultiPPP)	159
PPP NCP; Point-to-Point Protocol Network Control Protocol	160
PAP; Password Authentication Protocol	161
PPPoA; PPP over ATM AAL5	162
PPPoE; PPP over Ethernet	162
Other WAN Protocols	164
Frame Relay; WAN Protocol for Internetworking	164
LAPF; Link Access Procedure for Frame Mode Services	165
HDLC; High Level Data Link Control	166
LAPB; Link Access Procedure, Balanced	167
X. 25; ISO/ITU-T Protocol for WAN Communications	168
Local Area Network and LAN Protocols	170
Ethernet Protocols	171
Ethernet; IEEE 802.3 Local Area Network Protocols	171
Fast Ethernet; 100 Mb/s Ethernet (IEEE 802.3u)	172
Gigabit (1000 Mb/s) Ethernet; IEEE 802.3z(1000Base-X) and 802.3ab(1000Base-T) and GBIC	174
10-Gigabit Ethernet; The Ethernet Protocol IEEE 802.3ae for LAN, WAN and MAN	175
Virtual LAN Protocols	177
VLAN; Virtual Local Area Network and the IEEE 802.1Q	177
IEEE 802.1P; LAN Layer 2 QoS/CoS Protocol for Traffic Prioritization	178
GARP; Generic Attribute Registration Protocol	179
GMRP; GARP Multicast Registration Protocol	180
GVRP; GARP VLAN Registration Protocol	181
Wireless LAN Protocols	183
WLAN; Wireless LAN Defined by IEEE 802.11	183

IEEE 802.1X; EAP over LAN (EAPOL) for LAN/WLAN Authentication and Key Management	184
IEEE 802.15 and Bluetooth; WPAN Communications	185
Other Protocols	187
FDDI; Fibre Distributed Data Interface	187
Token Ring; IEEE 802.5 LAN Protocol	188
LLC; Logic Link Control (IEEE 802.2)	189
SNAP; SubNetwork Access Protocol	190
STP; Spanning Tree Protocol (IEEE 802.1D)	190
Metropolitan Area Network and MAN Protocols	193
DQDB; Distributed Queue Dual Bus (Defined in IEEE 802.6)	193
SMDS; Switched Multimegabit Data Service	194
IEEE 802.16; Broadband Wireless MAN Standard (WiMAX)	196
Storage Area Network and SAN Protocols	198
FC and FCP; Fibre Channel and Fibre Channel Protocol	198
FCIP; Fibre Channel over TCP/IP	199
iFCP; Internet Fibre Channel Protocol	201
iSCSI; Internet Small Computer System Interface (SCSI)	202
iSNS and iSNSP; Internet Storage Name Service and iSNS Protocol	203
NDMP; Network Data Management Protocol	205
SCSI; Small Computer System Interface	206
ISO Protocols in OSI 7-Layer Reference Model	208
Application Layer	210
ISO ACSE; Association Control Service Element	210
ISO CMIP; Common Management Information Protocol	211
CMOT; CMIP Over TCP/IP	212
ISO FTAM; File Transfer Access and Management Protocol	213
ISO ROSE; Remote Operations Service Element Protocol	214
ISO RTSE; Reliable Transfer Service Element Protocol	216
ISO VTP; ISO Virtual Terminal (VT) Protocol	217
X.400; Message Handling Service Protocol	217
X.500; Directory Access Protocol (DAP)	219
ISO-PP; OSI Presentation Layer Protocol	220
ISO-SP; OSI Session Layer Protocol	221
ISO-TP; OSI Transport Layer Protocols: TP0, TP1, TP2, TP3, and TP4	222
Network Layer	225
CLNP; Connectionless Network Protocol	225
ISO-CONP; Connection-Oriented Network Protocol	226
ES-IS; End System to Intermediate System Routing Exchange Protocol	227
IDRP; Inter-Domain Routing Protocol	228
IS-IS; Intermediate System to Intermediate System Routing Protocol	229
Cisco Protocols	231
CDP; Cisco Discovery Protocol	231
CGMP; Cisco Group Management Protocol	232
DTP; Cisco Dynamic Trunking Protocol	233
EIGRP; Enhanced Interior Gateway Routing Protocol	234
HSRP; Hot Standby Router Protocol	235
IGRP; Interior Gateway Routing Protocol	236
ISL and DISL; Cisco Inter-Switch Link Protocol and Dynamic ISL Protocol	236

RGMP; Cisco Router Port Group Management Protocol	237
TACACS (and TACACS +) ; Terminal Access Controller Access Control System	238
VTP; Cisco VLAN Trunking Protocol	239
XOT; X.25 over TCP Protocol by Cisco	241
Novell NetWare and Protocols	242
IPX; Internetwork Packet Exchange Protocol	243
NCP; NetWare Core Protocol	244
NLSP; NetWare Link Services Protocol	245
SPX; Sequenced Packet Exchange Protocol	246
IBM Systems Network Architecture (SNA) and Protocols	248
IBM SMB; Server Message Block Protocol	249
APPC; Advanced Program-to-Program Communications (SNA LU 6.2)	250
SNA NAU; Network Accessible Units (PU, LU and CP)	251
NetBIOS; Network Basic Input Output System	252
NetBEUI; NetBIOS Extended User Interface	253
APPN; Advanced Peer-to-Peer Networking	254
DLSw; Data-Link Switching Protocol	256
QLLC; Qualified Logic Link Control	257
SDLC; Synchronous Data Link Control	257
AppleTalk; Apple Computer Protocols Suite	259
DECnet and Protocols	261
SS7/C7 Protocol Suite; Signalling System #7 for Telephony Signalling	263
BISUP; Broadband ISDN User Part	264
DUP; Data User Part	265
ISUP; ISDN User Part	265
MAP; Mobile Application Part	267
MTP2 and MTP3; Message Transfer Part level 2 and level 3	268
SCCP; Signalling Connection Control Part of SS7	269
TCAP; Transaction Capabilities Application Part	270
TUP; Telephone User Part	271
Other Protocols	273
Microsoft CIFS; Common Internet File System	273
Microsoft SOAP; Simple Object Access Protocol	273
Xerox IDP; Internet Datagram Protocol	275
Toshiba FANP; Flow Attribute Notification Protocol	276
Network Protocols Dictionary: From A to Z and 0 to 9	278
Major Networking and Telecom Standard Organizations	293

Figures

Figure 1-1	Communication between computers in a network	3
Figure 1-2	Data encapsulation at each layer	3
Figure 1-3	Data communication between peer layers	4
Figure 1-4	TCP/IP protocol stack 4-layer model	5
Figure 1-5	SNA vs. OSI model	6
Figure 1-6	SNA network topology	6
Figure 1-7	Communications between TPs and LUs in SNA	7
Figure 2-1	RMON monitoring layers	30
Figure 2-2	Remote procedure call flow	45
Figure 2-3	Mobile IP functional flow chart	60
Figure 2-4	MPLS protocol stack architecture	78
Figure 2-5	IPSec protocol stack structure	96
Figure 2-6	H. 323 protocol stack structure	105
Figure 2-7	H. 235 – Encryption of media	107
Figure 2-8	H. 235 – Decryption of media	107
Figure 2-9	T. 120 data conferencing protocol structure	118
Figure 2-10	ATM reference model	147
Figure 2-11	Gigabit Ethernet protocol stack	174
Figure 2-12	Packet bursting mode in Gigabit Ethernet	175
Figure 2-13	10-Gigabit Ethernet architecture	175
Figure 2-14	IEEE 802. 15 (Bluetooth) protocol stack	186
Figure 2-15	DQDB architecture	194
Figure 2-16	IEEE 802. 16 (WiMax) functional flow chart	196
Figure 2-17	IEEE 802. 16 (WiMax) protocol stack	197
Figure 2-18	Storage area network architecture	198
Figure 2-19	Fibre Channel Protocol	199
Figure 2-20	NDMP functional components	205
Figure 2-21	SCSI protocol stack structure	207
Figure 2-22	Novell NetWare protocol stack architecture	242
Figure 2-23	IBM SNA vs. OSI model	248
Figure 2-24	IBM APPN network illustration	255
Figure 2-25	QLLC network architecture	257
Figure 2-26	AppleTalk protocol stack architecture	259
Figure 2-27	DECnet protocol suite architecture	261
Figure 2-28	SS7/C7 protocol suite architecture	263
Figure 2-29	SCCP protocol structure	269
Figure 2-30	TCAP protocol structure	271
Figure 2-31	Microsoft CIFS flow chart	274

Network Communication Architecture and Protocols

A network architecture is a blueprint of the complete computer communication network, which provides a framework and technology foundation for designing, building and managing a communication network. It typically has a layered structure. Layering is a modern network design principle which divides the communication tasks into a number of smaller parts, each part accomplishing a particular sub-task and interacting with the other parts in a small number of well-defined ways. Layering allows the parts of a communication to be designed and tested without a combinatorial explosion of cases, keeping each design relatively simple.

If a network architecture is open, no single vendor owns the technology and controls its definition and development. Anyone is free to design hardware and software based on the network architecture. The TCP/IP network architecture, which the Internet is based on, is such a open network architecture and it is adopted as a worldwide network standard and widely deployed in local area network (LAN), wide area network (WAN), small and large enterprises, and last but not the least, the Internet.

Open Systems Interconnection (OSI) network architecture, developed by International Organization

for Standardization (ISO), is an open standard for communication in the network across different equipment and applications by different vendors. Though not widely deployed, the OSI 7-layer model is considered the primary network architectural model for inter-computing and inter-networking communications.

In addition to the OSI network architecture model, there exist other network architecture models by many vendors, such as IBM Systems Network Architecture (SNA), Digital Equipment Corporation's (DEC; now part of HP) Digital Network Architecture (DNA), Apple Computer's AppleTalk, and Novell's NetWare. Actually, the TCP/IP architecture does not exactly match the OSI model. Unfortunately, there is no universal agreement regarding how to describe TCP/IP with a layered model. It is generally agreed that TCP/IP has fewer levels (from three to five layers) than the seven layers of the OSI model.

Network architecture provides only a conceptual framework for communications between computers. The model itself does not provide specific methods of communication. Actual communication is defined by various communication protocols.

OSI Network Architecture 7-Layer Model

Open Systems Interconnection (OSI) model is a reference model developed by ISO in 1984, as a conceptual framework of standards for communication in the network across different equipment and applications by different vendors. It is now considered the primary architectural model for inter-computing and inter-networking communications. Most of the network communication protocols used today have a structure based on the OSI model. The OSI model defines the communications process into 7 layers, dividing the tasks involved with moving information between networked computers into seven smaller, more manageable task groups. A task or group of tasks is then assigned to each of the seven OSI layers. Each layer is reasonably self-contained, so that the tasks assigned to each layer can be implemented independently. This enables the solutions offered by one layer to be updated without adversely affecting the other layers.

The OSI 7-layer model has clear characteristics at each layer. Basically, layers 7 through 4 deal with end to end communications between data source and destinations, while layers 3 to 1 deal with communications between network devices. On the other hand, the seven layers of the OSI model can be divided into two groups: upper layers (layers 7, 6 and 5) and lower layers (layers 4, 3, 2, and 1). The upper layers of the OSI model deal with application issues and generally are implemented only in software. The highest layer, the application layer, is closest to the end user. The lower layers of the OSI model handle data transport issues. The physical layer and the data link layer are implemented in hardware and software. The lowest layer, the physical layer, is closest to the physical network medium (the wires, for example) and is responsible for placing data on the medium.

The specific description for each layer is as follows:

Layer 7: Application Layer

- Defines interface-to-user processes for communication and data transfer in network
- Provides standardized services such as virtual terminal, file and job transfer and operations

Layer 6: Presentation Layer

- Masks the differences of data formats between dissimilar systems
- Specifies architecture-independent data transfer format
- Encodes and decodes data; encrypts and decrypts data; compresses and decompresses data

Layer 5: Session Layer

- Manages user sessions and dialogues
- Controls establishment and termination of logic links between users
- Reports upper layer errors

Layer 4: Transport Layer

- Manages end-to-end message delivery in network
- Provides reliable and sequential packet delivery through error recovery and flow control mechanisms
- Provides connectionless oriented packet delivery

Layer 3: Network Layer

- Determines how data are transferred between network devices
- Routes packets according to unique network device addresses
- Provides flow and congestion control to prevent network resource depletion

Layer 2: Data Link Layer

- Defines procedures for operating the communication links
- Frames packets
- Detects and corrects packets transmit errors

Layer 1: Physical Layer

- Defines physical means of sending data over network devices
- Interfaces between network medium and devices
- Defines optical, electrical and mechanical characteristics

Information being transferred from a software application in one computer to an application in another proceeds through the OSI layers. For example, if a software application in computer A has informa-

tion to pass to a software application in computer B, the application program in computer A needs to pass the information to the application layer (layer 7) of computer A, which then passes the information to the presentation layer (layer 6), which relays the data to the session layer (layer 5), and so on all the way down to the physical layer (layer 1). At the physical layer, the data is placed on the physical network medium and is sent across the medium to computer B. The physical layer of computer B receives the data from the physical medium, and then its physical layer passes the information up to the data link layer (layer 2), which relays it to the network layer (layer 3), and so on, until it reaches the application layer (layer 7) of computer B. Finally, the application layer of computer B passes the information to the recipient application program to complete the communication process. The Figure 1-1 illustrated this process.

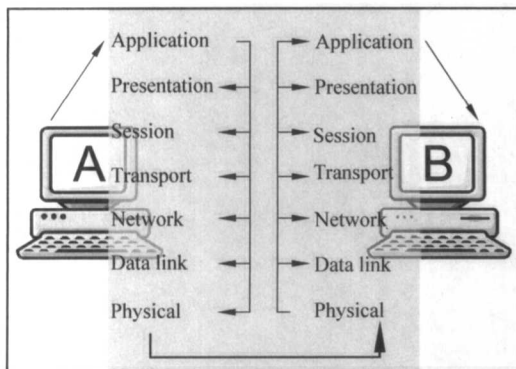


Figure 1-1 Communication between computers in a network

The seven OSI layers use various forms of control information to communicate with their peer layers in other computer systems. This control information consists of specific requests and instructions that are exchanged between peer OSI layers. Headers and trailers of data at each layer are the two basic forms to carry the control information.

Headers are prepended to data that has been passed down from upper layers. Trailers are appended to data that has been passed down from upper layers. An OSI layer is not required to attach a header or a trailer to data from upper layers.

Each layer may add a header and a trailer to its data, which consists of the upper layer's header, trailer and data as it proceeds through the layers.

The headers contain information that specifically addresses layer-to-layer communication. Headers, trailers and data are relative concepts, depending on the layer that analyzes the information unit. For example, the transport header (TH) contains information that only the transport layer sees. All other layers below the transport layer pass the transport header as part of their data. At the network layer, an information unit consists of a layer 3 header and data.

At the data link layer, however, all the information passed down by the network layer (the layer 3 header and the data) is treated as data. In other words, the data portion of an information unit at a given OSI layer potentially can contain headers, trailers, and data from all the higher layers. This is known as encapsulation (see Fig. 1-2).

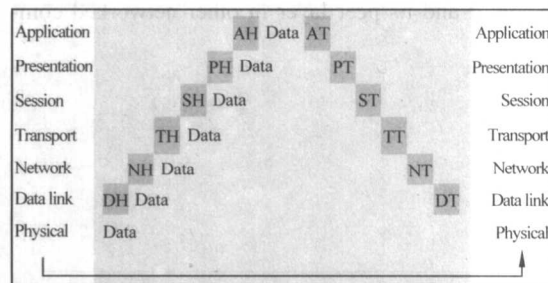


Figure 1-2 Data encapsulation at each layer

For example, if computer A has data from a software application to send to computer B, the data is passed to the application layer. The application layer in computer A then communicates any control information required by the application layer in computer B by prepending a header to the data. The resulting message unit, which includes a header, the data and maybe a trailer, is passed to the presentation layer, which prepends its own header containing control information intended for the presentation layer in computer B. The message unit grows in size as each layer prepends its own header and trailer containing control information to be used by its peer layer in computer B. At the physical layer, the entire information unit is transmitted through the network medium.

The physical layer in computer B receives the information unit and passes it to the data link layer. The data link layer in computer B then reads the control information contained in the header prepended by the data link layer in computer A. The header

and the trailer are then removed, and the remainder of the information unit is passed to the network layer. Each layer performs the same actions; The layer reads the header and trailer from its peer layer, strips it off, and passes the remaining information unit to the next higher layer. After the application layer performs these actions, the data is passed to the recipient software application in computer B, in exactly the form in which it was transmitted by the application in computer A.

One OSI layer communicates with another layer to make use of the services provided by the second layer. The services provided by adjacent layers help a given OSI layer communicate with its peer layer in other computer systems. A given layer in the OSI model generally communicates with three other OSI layers; the layer directly above it, the layer directly below it and its peer layer in other networked com-

puter systems. The data link layer in computer A, for example, communicates with the network layer of computer A, the physical layer of computer A and the data link layer in computer B. The Figure 1-3 illustrates this example.

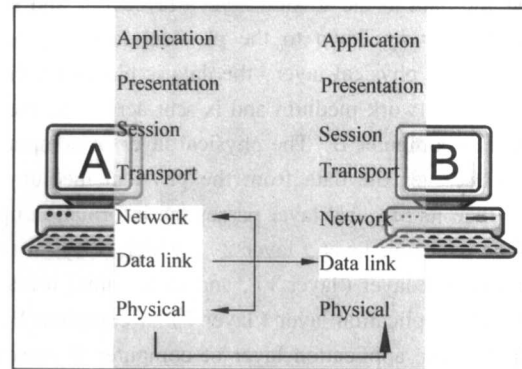


Figure 1-3 Data communication between peer layers

TCP/IP 4-Layer Architecture Model

TCP/IP architecture does not exactly follow the OSI model. Unfortunately, there is no universal agreement regarding how to describe TCP/IP with a layered model. It is generally agreed that TCP/IP has fewer levels (from three to five layers) than the seven layers of the OSI model. We adopt a 4-layer model for the TCP/IP architecture (see Fig. 1-4).

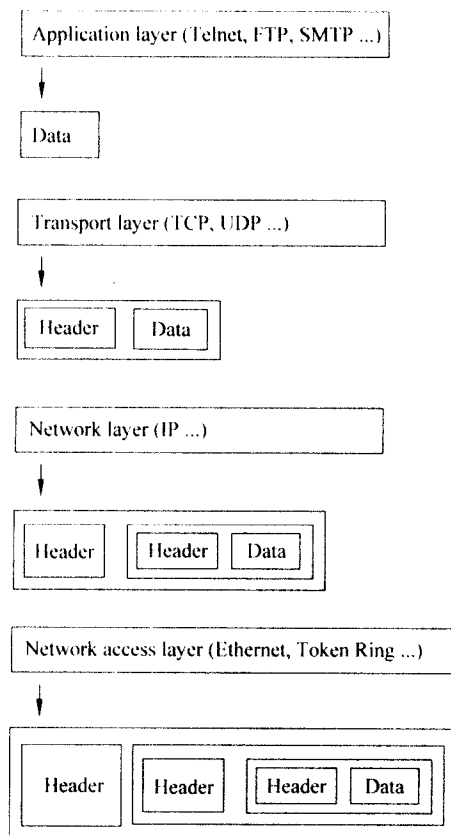


Figure 1-4 TCP/IP protocol stack 4-layer model

TCP/IP architecture omits some features found under the OSI model, combines the features of some adjacent OSI layers and splits other layers apart. The 4-layer structure of TCP/IP is built as information is passed down from applications to the physical network layer. When data is sent, each layer treats all of the information it receives from the upper layer as data, adds control information (header) to the front of that data and then passes it

to the lower layer. When data is received, the opposite procedure takes place as each layer processes and removes its header before passing the data to the upper layer.

The TCP/IP 4-layer model and the key functions of each layer are described below:

Application layer

The application layer in TCP/IP groups the functions of OSI application, presentation layer and session layer. Therefore, any process above the transport layer is called an application in the TCP/IP architecture. In TCP/IP socket and port are used to describe the path over which applications communicate. Most application level protocols are associated with one or more port number.

Transport layer

In TCP/IP architecture, there are two transport layer protocols. The Transmission Control Protocol (TCP) guarantees information transmission. The User Datagram Protocol (UDP) transports datagram without end-to-end reliability checking. Both protocols are useful for different applications.

Network layer

The Internet Protocol (IP) is the primary protocol in the TCP/IP network layer. All upper and lower layer communications must travel through IP as they are passed through the TCP/IP protocol stack. In addition, there are many supporting protocols in the network layer, such as ICMP, to facilitate and manage the routing process.

Network access layer

In the TCP/IP architecture, the data link layer and physical layer are normally grouped together to become the network access layer. TCP/IP makes use of existing data link and physical layer standards rather than defining its own. Many RFCs describe how IP utilizes and interfaces with the existing data link protocols such as Ethernet, Token Ring, FDDI, HSSI, and ATM. The physical layer, which defines the hardware communication properties, is not often directly interfaced with the TCP/IP protocols in the network layer and above.

Other Network Architecture Models: IBM SNA

In addition to the open architectural models such as the OSI 7-layer model and the TCP/IP architecture model, there exist a few popular vendor specific network communication models, such as IBM Systems Network Architecture (SNA), Digital Equipment Corporation's (DEC, now part of HP) Digital Network Architecture (DNA). We will only provide details on the IBM SNA here.

Although it is now considered a legacy networking architecture, the IBM SNA is still widely deployed. SNA was designed around the host-to-terminal communication model that IBM's mainframes use. IBM expanded the SNA protocol to support peer-to-peer networking. This expansion was deemed Advanced Peer-to-Peer Networking (APPN) and Advanced Program-to-Program Communication (APPC). APPN represents IBM's second-generation SNA. In creating APPN, IBM moved SNA from a hierarchical, mainframe-centric environment to a peer-based networking environment. The heart of APPN is an IBM architecture that supports peer-based communications, directory services, and routing between two or more APPC systems that are not directly attached.

SNA has many similarities with the OSI 7-layer reference model. However, the SNA model has only six layers and it does not define specific protocols for its physical control layer. The physical control layer is assumed to be implemented via other standards. The functions of each SNA component are described as follows:

- Data Link Control (DLC) – defines several protocols, including the Synchronous Data Link Control (SDLC) protocol for hierarchical communication, and the token ring network communication protocol for LAN communication between peers. SDLC provided a foundation for ISO HDLC and IEEE 802.2.
- Path control – performs many OSI network layer functions, including routing and data-gram segmentation and reassembly (SAR).
- Transmission control – provides a reliable end-to-end connection service (similar to TCP), as well as encrypting and decrypting services.
- Data flow control – manages request and response processing, determines whose turn it is

to communicate, groups messages and interrupts data flow on request.

- Presentation services – specifies data-transformation algorithms that translate data from one format to another, coordinate resource sharing and synchronize transaction operations.
- Transaction services – provides application services in the form of programs that implement distributed processing or management services.

The Figure 1-5 illustrates how the IBM SNA model maps to the ISO OSI reference model.

SNA	OSI
Transaction services	Application
Presentation services	Presentation
Data flow control	Session
Transmission control	Transport
Path control	Network
Data link control	Data link
Physical	Physical

Figure 1-5 SNA vs. OSI model

The Figure 1-6 gives a typical SNA network topology.

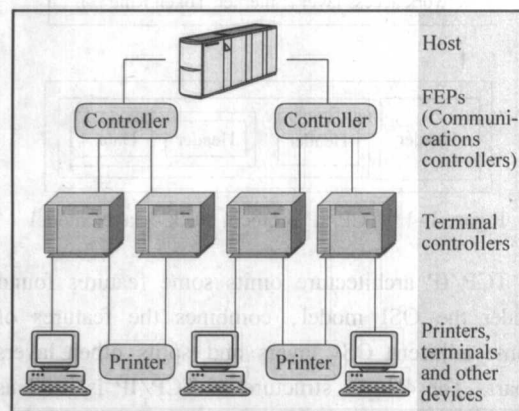


Figure 1-6 SNA network topology

SNA supports the following types of networks:

- A subarea network is a hierarchically organized network consisting of subarea nodes and peripheral nodes. Subarea nodes, such as hosts and communication controllers, handle general network routing. Peripheral nodes,