

Fourth Edition

Javvin

Network Protocols Handbook

TCP/IP
Ethernet ATM
Frame Relay WAN LAN
MAN WLAN SS7/C7 VOIP Security
VPN SAN VLAN IEEE IETF ISO
ITU-T ANSI Novell IBM
Apple Microsoft
Cisco

Javvin Technologies, Inc.

Table of Contents

Network Communication Architecture and Protocols	1
OSI Network Architecture 7 Layers Model	2
TCP/IP Four Layers Architecture Model	4
Other Network Architecture Models: IBM SNA	5
Network Protocols: Definition and Overview	6
Protocols Guide	8
TCP/IP Protocols	8
Application Layer Protocols	10
BOOTP: Bootstrap Protocol	10
DCAP: Data Link Switching Client Access Protocol	11
DHCP: Dynamic Host Configuration Protocol	11
DNS: Domain Name System (Service) Protocol	12
Finger: User Information Protocol	13
FTP: File Transfer Protocol	14
HTTP: Hypertext Transfer Protocol	16
S-HTTP: Secure Hypertext Transfer Protocol	17
IMAP & IMAP4: Internet Message Access Protocol (version 4)	18
IRC: Internet Relay Chat Protocol	19
LDAP: Lightweight Directory Access Protocol (version 3)	20
MIME (S-MIME): Multipurpose Internet Mail Extensions and Secure MIME	21
NAT: Network Address Translation	22
NNTP: Network News Transfer Protocol	22
NTP: Network Time Protocol	23
POP and POP3: Post Office Protocol (version 3)	24
rlogin: Remote Login to Unix Systems	25
RMON: Remote Monitoring MIBs (RMON1 and RMON2)	26
SLP: Service Location Protocol	28
SMTP: Simple Mail Transfer Protocol	29
SNMP: Simple Network Management Protocol	30
SNMPv1: Simple Network Management Protocol version one	31
SNMPv2: Simple Network Management Protocol version two	32

SNMPv3: Simple Network Management Protocol version three	34
SNTP: Simple Network Time Protocol	35
Syslog Protocol	36
TELNET: Terminal Emulation Protocol of TCP/IP	37
TFTP: Trivial File Transfer Protocol	38
URL: Uniform Resource Locator	39
Whois (and RWhois): Remote Directory Access Protocol	39
XMPP: Extensible Messaging and Presence Protocol	40
X Window/X Protocol: X Window System Protocol	41
Presentation Layer Protocols	42
LPP: Lightweight Presentation Protocol	42
Session Layer Protocols	43
RPC: Remote Procedure Call Protocol	43
Transport Layer Protocols	44
ITOT: ISO Transport Service on top of TCP	44
RDP: Reliable Data Protocol	45
RUDP: Reliable User Datagram Protocol (Reliable UDP)	46
TALI: Tekelec's Transport Adapter Layer Interface	47
TCP: Transmission Control Protocol	48
UDP: User Datagram Protocol	49
Van Jacobson: Compressed TCP Protocol	50
Network Layer Protocols	51
Routing Protocols	51
BGP (BGP-4): Border Gateway Protocol	51
EGP: Exterior Gateway Protocol	51
ICMP & ICMPv6: Internet Message Control Protocol and ICMP version 6	52
IP: Internet Protocol (IPv4)	54
IPv6: Internet Protocol version 6	55
IRDP: ICMP Router Discovery Protocol	57
Mobile IP: IP Mobility Support Protocol for IPv4 & IPv6	59
NARP: NBMA Address Resolution Protocol	60
NHRP: Next Hop Resolution Protocol	61
OSPF: Open Shortest Path First Protocol	62
RIP: Routing Information Protocol (RIP2)	63
RIPng: Routing Information Protocol next generation for IPv6	64
RSVP: Resource ReSerVation Protocol	65
VRRP: Virtual Router Redundancy Protocol	66
Multicasting 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	78
MPLS: Multiprotocol Label Switching	78
GMPLS: Generalized Multiprotocol Label Switching	80
CR-LDP: Constraint-based LDP	81
LDP: Label Distribution Protocol	81
RSVP-TE: Resource Reservation Protocol - Traffic Extension	82
Data Link Layer Protocols	83
ARP and InARP: Address Resolution Protocol and Inverse ARP	83
IPCP and IPv6CP: IP Control Protocol and IPv6 Control Protocol	84
RARP: Reverse Address Resolution Protocol	85
SLIP: Serial Line IP	86
Network Security Technologies and Protocols	87
AAA Protocols	88
Kerberos: Network Authentication Protocol	88
RADIUS: Remote Authentication Dial in User Service	89
SSH: Secure Shell Protocol	90
Tunneling Protocols	91
L2F: Layer 2 Forwarding Protocol	91
L2TP: Layer 2 Tunneling Protocol	92
PPTP: Point-to-Point Tunneling Protocol	93
Secured Routing Protocols	94
DiffServ: Differentiated Service Architecture	94
GRE: Generic Routing Encapsulation	95
IPSec: Internet Protocol Security Architecture	96
IPSec AH: IPsec Authentication Header	97

IPsec ESP: IPsec Encapsulating Security Payload	98
IPsec IKE: Internet Key Exchange Protocol	99
IPsec ISAKMP: Internet Security Association and Key Management Protocol	100
SSL/TLS: Secure Socket Layer and Transport Layer Security Protocol	101
Other Security Protocols	102
SOCKS v5: Protocol for Sessions Traversal Across Firewall Securely	102
Voice over IP and VOIP Protocols	103
Signalling	105
H.323: ITU-T VOIP Protocols	105
H.225.0: Vall signalling protocols and media stream packetization for packet based multimedia communication systems	106
H.235: Security and encryption for H-series (H.323 and other H.245-based) multimediaterminals	108
H.245: Control Protocol for Multimedia Communication	109
Megaco/H.248: Media Gateway Control Protocol	110
MGCP: Media Gateway Control Protocol	111
NCS: Network-Based Call Signaling Protocol	112
RTSP: Real-Time Streaming Protocol	113
SAP: Session Announcement Protocol	114
SDP: Session Description Protocol	115
SIP: Session Initiation Protocol	116
SCCP (Skinny): Cisco Skinny Client Control Protocol	118
T.120: Multipoint Data Conferencing and Real Time Communication Protocols	119
Media/CODEC	120
G.7xx: Audio (Voice) Compression Protocols	120
H.261: Video CODEC for Low Quality Videoconferencing	122
H.263: Video CODEC for Medium Quality Videoconferencing	123
H.264 / MPEG-4: Video CODEC For High Quality Video Streaming	124
RTP: Real-Time Transport Protocol	126
RTCP: RTP Control Protocol	127
Other Protocols	128
COPS: Common Open Policy Service	128
SIGTRAN: Signaling Transport Protocol Stack	129
SCTP: Stream Control Transmission Protocol	130
TRIP: Telephony Routing over IP	132

Wide Area Network and Wan Protocols	133
ATM Protocols	134
ATM: Asynchronous Transfer Mode Reference Model and Protocols	134
ATM Layer: Asynchronous Transfer Mode Layer	136
AAL: ATM Adaptation Layers (AAL1, AAL2, AAL3/4, AAL5)	137
ATM UNI: ATM Signaling User-to-Network Interface	140
LANE NNI: ATM LAN Emulation NNI	142
LANE UNI: ATM LAN Emulation UNI	144
MPOA: Multi-Protocol Over ATM	146
ATM PNNI: ATM Private Network-to-Network Interface	147
Q.2931: ATM Signaling for B-ISDN	148
SONET/SDH: Synchronous Optical Network and Synchronous Digital Hierarchy	150
EoS: Ethernet over SONET/SDH	151
Broadband Access Protocols	153
BISDN: Broadband Integrated Services Digital Network (Broadband ISDN)	153
ISDN: Integrated Services Digital Network	154
LAP-D: ISDN Link Access Protocol-Channel D	155
Q.931: ISDN Network Layer Protocol for Signaling	156
DOCSIS: Data Over Cable Service Interface Specification	157
xDSL: Digital Subscriber Line Technologies (DSL, IDSL, ADSL, HDSL, SDSL,VDSL,G.Lite) ...	158
PPP Protocols	159
PPP: Point-to-Point Protocols	159
BAP: PPP Bandwidth Allocation Protocol and BACP: Bandwidth Allocation Control Protocol	160
BCP: PPP Briding Control Protocol	161
EAP: PPP Extensible Authentication Protocol	162
CHAP: Challenge Handshake Authentication Protocol	163
LCP: PPP Link Control Protocol	164
MP: MultiLink Point to Point Protocol (MultiPPP)	165
PPP NCP: Point to Point Protocol Network Control Protocols	166
PAP: Password Authentication Protocol	167
PoS: Packet over SONET/SDH	168
PPPoA: PPP over ATM AAL5	169
PPPoE: PPP over Ethernet	170
Other WAN Protocols	171
Frame Relay: WAN Protocol for Internetworking	171
LAPF: Link Access Procedure for Frame Mode Services	173
HDLC: High Level Data Link Control	174

LAPB: Link Access Procedure, Balanced	175
X.25: ISO/ITU-T Protocol for WAN Communications	176
Local Area Network and LAN Protocols	178
Ethernet Protocols	179
Ethernet: IEEE 802.3 Local Area Network Protocols	179
Fast Ethernet: 100Mbps Ethernet (IEEE 802.3u)	181
Gigabit (1000 Mbps) Ethernet: IEEE 802.3z (1000Base-X) and 802.3ab (1000 Base-T) ..	182
10-Gigabit Ethernet: The Ethernet Protocol IEEE 802.3ae for LAN, WAN and MAN	183
Virtual LAN Protocols	185
VLAN: Virtual Local Area Network and the IEEE 802.1Q	185
IEEE 802.1P: LAN Layer 2 QoS/CoS Protocol for Traffic Prioritization	186
GARP: Generic Attribute Registration Protocol	187
GMRP: GARP Multicast Registration Protocol	188
GVRP: GARP VLAN Registration Protocol	189
Wireless LAN Protocols	190
WLAN: Wireless LAN by IEEE 802.11 Protocols	190
IEEE 802.11i: WLAN Security Standard	191
IEEE 802.1X: EAP over LAN (EAPOL) for LAN/WLAN Authentication and Key Management ...	193
WPAN: Wireless Personal Area Network Communication Protocols	194
IEEE 802.15.1 and the Bluetooth for WPAN Communications	196
Other Protocols	197
FDDI: Fiber Distributed Data Interface	197
Token Ring: IEEE 802.5 LAN Protocol	198
LLC: Logic Link Control (IEEE 802.2)	199
SNAP: SubNetwork Access Protocol	200
STP: Spanning Tree Protocol (IEEE 802.1D)	201
Metropolitan Area Network and MAN Protocol	202
DQDB: Distributed Queue Dual Bus (Defined in IEEE 802.6)	203
SMDS: Switched Multimegabit Data Service	204
WiMAX: Broadband Wireless MAN Standard defined in IEEE802.16	205
Storage Area Network and SAN Protocols	207
FC & FCP: Fibre Channel and Fibre Channel Protocol	208
FCIP: Fibre Channel over TCP/IP	209
iFCP: Internet Fibre Channel Protocol	211

iSCSI: Internet Small Computer System Interface (SCSI)	212
iSNS and iSNSP: Internet Storage Name Service and iSNS Protocol	213
NDMP: Network Data Management Protocol	214
SCSI: Small Computer System Interface	215
ISO Protocols in OSI 7 Layers Model	217
Application Layer	219
ISO ACSE: Association Control Service Element	219
ISO CMIP: Common Management Information Protocol	220
CMOT: CMIP over TCP/IP	222
ISO FTAM: File Transfer Access and Management Protocol	223
ISO ROSE: Remote Operations Service Element Protocol	224
ISO RTSE: Reliable Transfer Service Element Protocol	226
ISO VTP: ISO Virtual Terminal (VT) Protocol	227
X.400: Message Handling Service Protocol	227
X.500: Directory Access Protocol (DAP)	229
ASN.1: Abstract Syntax Notation One	230
Presentation Layer	231
ISO-PP: OSI Presentation Protocol	231
Session Layer	232
ISO-SP: OSI Session Protocol	232
Transport Layer	233
ISO-TP: OSI Transport Layer Protocols TP0, TP1, TP2, TP3, TP4	233
Network Layer	235
CLNP: Connectionless Network Protocol (ISO-IP)	235
ISO CONP: Connection-Oriented Network Protocol	236
ES-IS: End System to Intermediate System Routing Exchange Protocol	237
IDRP: Inter-Domain Routing Protocol	238
IS-IS: Intermediate System to Intermediate System Routing Protocol	239
Cisco Protocols	240
CDP: Cisco Discovery Protocol	241
CGMP: Cisco Group Management Protocol	242
DTP: Cisco Dynamic Trunking Protocol	243
EIGRP: Enhanced Interior Gateway Routing Protocol	244
HSRP: Hot Standby Router Protocol	245
IGRP: Interior Gateway Routing Protocol	246

ISL & DISL: Cisco Inter-Switch Link Protocol and Dynamic ISL Protocol	247
NetFlow: Cisco Network Traffic Monitoring and Management Protocol	248
RGMP: Cisco Router Port Group Management Protocol	249
TACACS (and TACACS+): Terminal Access Controller Access Control System	250
VTP: Cisco VLAN Trunking Protocol	251
XOT: X.25 over TCP Protocol by Cisco	253
Novell NetWare and Protocols	254
IPX: Internetwork Packet Exchange Protocol	255
NCP: NetWare Core Protocol	256
NLSP: NetWare Link Services Protocol	257
SPX: Sequenced Packet Exchange Protocol	259
IBM Systems Network Architecture (SNA) and Protocols	260
IBM SMB: Server Message Block Protocol	261
APPC: Advanced Program to Program Communications (SNA LU6.2)	262
SNA NAU: Network Accessible Units (PU, LU and CP)	263
NetBIOS: Network Basic Input Output System	265
NetBEUI: NetBIOS Extended User Interface	266
APPN: Advanced Peer-to-Peer Networking	267
DLSw: Data-Link Switching Protocol	268
QLLC: Qualified Logic Link Control	269
SDLC: Synchronous Data Link Control	270
AppleTalk: Apple Computer Protocols Suite	272
DECnet and Protocols	274
SS7/C7 Protocols: Signalling System #7 for Telephony	276
BISUP: Broadband ISDN User Part	278
DUP: Data User Part	278
ISUP: ISDN User Part	279
MAP: Mobile Application Part	281
MTP2 and MTP3: Message Transfer Part level 2 and level 3	282
SCCP: Signalling Connection Control Part of SS7	283
TCAP: Transaction Capabilities Application Part	284

TUP: Telephone User Part	285
Other Protocols	286
Microsoft CIFS: Common Internet File System	286
Microsoft SOAP: Simple Object Access Protocol	287
NFS: Network File System	288
Xerox IDP: Internet Datagram Protocol	290
Toshiba FANP: Flow Attribute Notification Protocol	291
Appendices	293
Appendix A: TCP and UDP Port Numbers	293
Appendix B: Major Networking and Telecom Standard Organizations	295
Appendix C: Network Protocols Dictionary: From A to Z and 0 to 9	296
Network Protocols Map	362

Table of Figures

Figure 1-1: Communication between computers in a network	2
Figure 1-2: Data encapsulation at each layer	3
Figure 1-3: Data communication between peer layers	3
Figure 1-4: TCP/IP Protocol Stack 4 Layer Model	4
Figure 1-5: SNA vs. OSI model	5
Figure 1-6: SNA Network Topology	5
Figure 1-7: Communication between TP and LU in SNA	6
Figure 2-1: RMON Monitoring Layers	27
Figure 2-2: Simple Network Management Protocol (SNMP) Architecture	30
Figure 2-3: Sample Syslog Architecture	36
Figure 2-4: Remote Procedure Call Flow	43
Figure 2-5: Mobile IP Functional Flow Chart	59
Figure 2-6: MPLS protocol stack	79
Figure 2-7: GMPLS Protocol Stack Diagram	80
Figure 2-8: IPsec Protocol Stack Structure	97
Figure 2-9: H.323 Protocol Stack Structure	106
Figure 2-10: H.235 - Encryption of media	108
Figure 2-11: H.235 - Decryption of media	108
Figure 2-12: The relations between MGCP/NCS and other VOIP standards	112
Figure 2-13: T.120 Data Conferencing Protocol Structure	119
Figure 2-14: SIGTRAN Architecute	129
Figure 2-15: SIGTRAN Protocol Stack	129
Figure 2-16: ATMAsynchronous Transfer Mode	134
Figure 2-17: EoS Protocol Structure	152
Figure 2-18: ATM Reference Model	153
Figure 2-19: Packet over SONET/SDH	169
Figure 2-20: Encapsulating IP into a SONET/SDH frame	169
Figure 2-21: Ethernet protocols	179
Figure 2-22: Gigabit Ethernet Protocol Stack	182
Figure 2-23: Packet Bursting Mode in Gigabit Ethernet	182
Figure 2-24: 10 Gigabit Ethernet Architecture	183
Figure 2-25: IEEE 802.1Q Tagged Frame for Ethernet	185
Figure 2-26: IEEE 802.11 WLAN Protocols Stack	190
Figure 2-27: IEEE 802.11i Components	192
Figure 2-28: CCMP MPDU Format	192

Figure 2-29: CCMP CBC-MAC IV	192
Figure 2-30: CCMP CTR	192
Figure 2-31: TKIP MPDU Format	192
Figure 2-32: Bluetooth/IEEE802.15.1 Protocol Stack	195
Figure 2-33: ZigBee/IEEE 802.15.4 Protocol Stack	195
Figure 2-34: UWB/IEEE 802.15.3 Protocol Stack	195
Figure 2-35: IEEE 802.15 (Bluetooth) Protocol Stack	196
Figure 2-36: DQDB Architecture	203
Figure 2-37: DQDB Cell Format	203
Figure 2-38: DQDB cell header	203
Figure 2-39: WiMax Protocol Stack	206
Figure 2-40: Storage Area Network Architecture	207
Figure 2-41: Fibre Channel Protocol	208
Figure 2-42: NDMP Functional Components	214
Figure 2-43: SCSI Protocol Stack Structure	216
Figure 2-44: ISO Protocols in OSI 7 Layers Reference Model	217
Figure 2-45: Network Management Based on the CMIP/CMIS	220
Figure 2-46: Cisco IOS NetFlow Architecture	248
Figure 2-47: NetFlow Seven Flow Fields and the Cache	248
Figure 2-48: Novell Netware Protocol Stack Architecture	255
Figure 2-49: IBM SNA vs. OSI Model	260
Figure 2-50: IBM APPN Network Illustration	267
Figure 2-51: QLLC Network Architecture	269
Figure 2-52: AppleTalk Protocol Stack Architecture	273
Figure 2-53: DECnet Protocol Suite Architecture	275
Figure 2-54: SS7/C7 Protocol Suite Architecture	276
Figure 2-55: SCCP Protocol Structure	283
Figure 2-56: TCAP Protocol Structure	284
Figure 2-57: Microsoft CIFS Flow Chart	287
Figure 3-1: TCP/UDP Port Numbers	293

TCP/IP Four Layers 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 four layers model for the TCP/IP architecture.

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 pass 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 is 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.

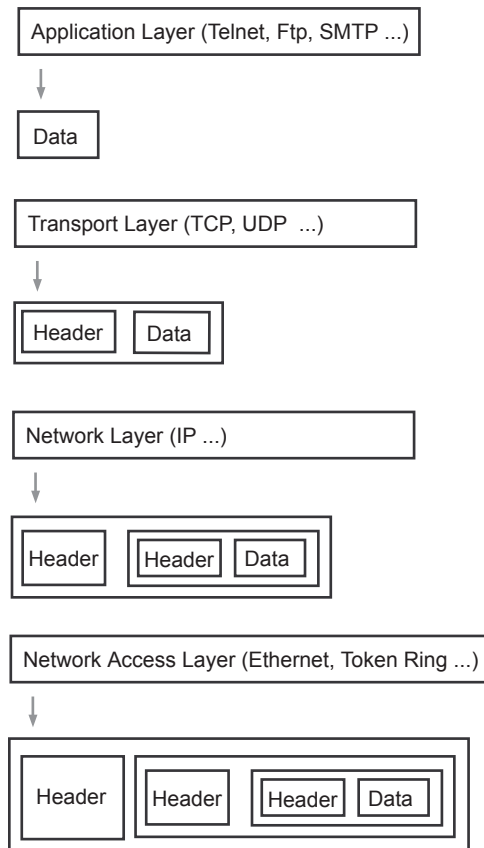


Figure 1-4: TCP/IP Protocol Stack 4 Layer Model

In this book, however, we present TCP/IP protocols into the OSI 7 layers structure for comparison purpose.

SNMP: Simple Network Management Protocol

Protocol Description

Simple Network Management Protocol (SNMP) is the standard protocol developed to manage nodes (servers, workstations, routers, switches and hubs, etc.) on an IP network. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Network management systems learn of problems by receiving traps or change notices from network devices implementing SNMP.

An SNMP managed network consists of three key components:

managed devices, agents, and network-management systems (NMSs). A managed device is a network node that contains an SNMP agent and that resides on a managed network. Managed devices collect and store management information and make this information available to NMSs using SNMP. Managed devices, sometimes called network elements, can be routers and access servers, switches and bridges, hubs, computer hosts, or printers. An agent is a network management software module that resides in a managed device. An agent has local knowledge of management information and translates that information into a form compatible with SNMP. An NMS executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs must exist on any managed network. The following picture illustrates the SNMP architecture:

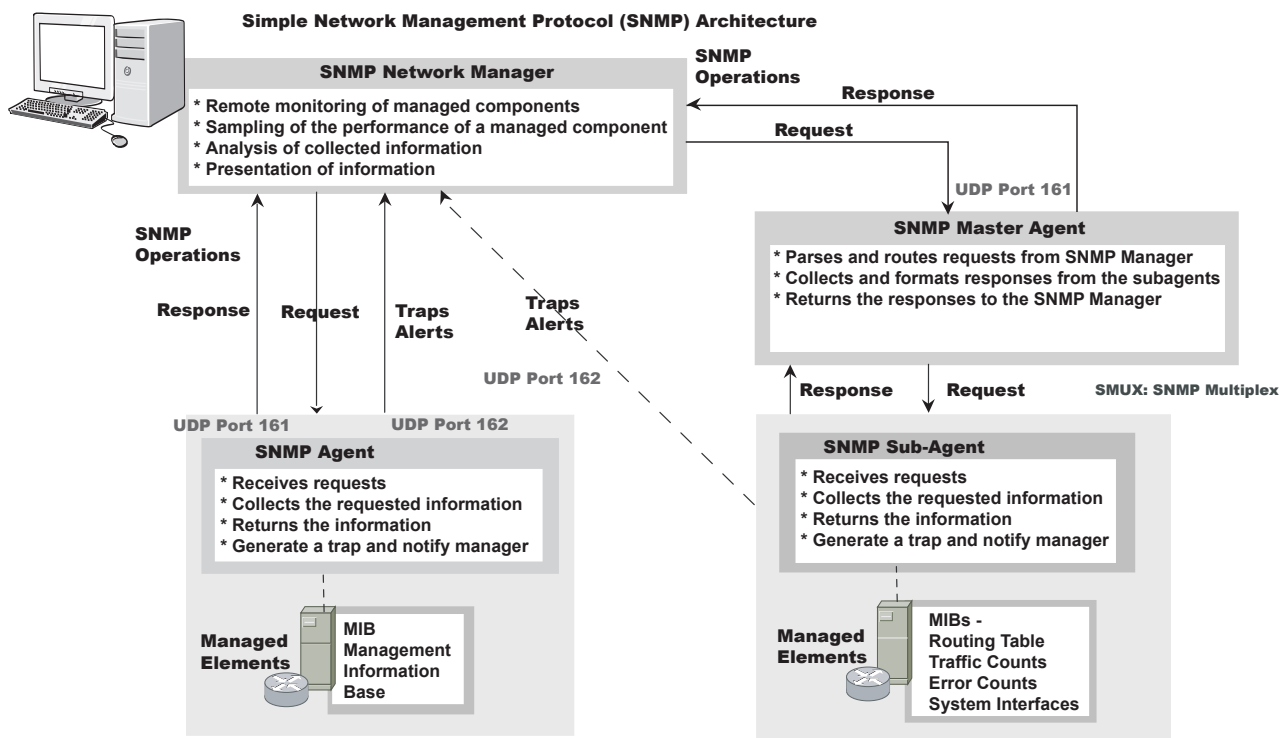


Figure 2-2: Simple Network Management Protocol (SNMP) Architecture

Currently, there are three versions of Simple Network Management Protocols defined: SNMP v1, SNMP v2 and SNMP v3. The following table provides the summary of the operations and features of the different versions of SNMP:

SNMP v1	Basic Operations and Features
Get	Used by the NMS to retrieve the value of one or more object instances from an agent
GetNext	Used by the NMS to retrieve the value of the next object instance in a table or a list within an agent
Set	Used by the NMS to set the values of object instances within an agent.
Trap	Used by agents to asynchronously inform the NMS of a significant event.
SNMP v2	Additional Operations and Features

GetBulk	Used by the NMS to efficiently retrieve large blocks of data.
Inform	Allows one NMS to send trap information to another NMS and to then receive a response.
SNMP v3	Security Enhancement
	User-based Security Model (USM) for SNMP message security.
	View-based Access Control Model (VACM) for access control.
	Dynamically configure the SNMP agents using SNMP SET commands.

To solve the incompatible issues among different versions of SNMP, RFC 3584 defines the coexistence strategies. SNMP also includes a group of extensions as defined by RMON, RMON 2, MIB, MIB2, SMI, OIDs, and Enterprise

OIDs.

Protocol Structure

SNMP is an application protocol, which is encapsulated in UDP. The general SNMP message format for all versions is shown below:

Version	Community	PDU
---------	-----------	-----

- Version -- SNMP version number. Both the manager and agent must use the same version of SNMP. Messages containing different version numbers are discarded without further processing.
- Community -- Community name used for authenticating the manager before allowing access to the agent.
- PDU (Protocol Data Unit) -- The PDU types and formats for SNMPv1, v2 and v3 will be explained in the corresponding sections.

Related Protocols

SNMPv1, SNMPv2, SNMPv3, UDP, RMON, SMI, OIDs

Sponsor Source

SNMP is defined by IETF (<http://www.ietf.org>) with a group of RFCs shown in the reference links.

Reference

- <http://www.javvin.com/protocol/rfc1155.pdf>
Structure and Identification of Management Information for TCP/IP based internets
- <http://www.javvin.com/protocol/rfc1156.pdf>
Management Information Base Network
- <http://www.javvin.com/protocol/rfc1157.pdf>
A Simple Network Management Protocol
- <http://www.javvin.com/protocol/rfc1441.pdf>
Introduction to SNMPv2
- <http://www.javvin.com/protocol/rfc2579.pdf>
Textual Conventions for SNMPv2
- <http://www.javvin.com/protocol/rfc2580.pdf>
Conformance Statements for SNMPv2
- <http://www.javvin.com/protocol/rfc2578.pdf>
Structure of Management Information for SNMPv2
- <http://www.javvin.com/protocol/rfc3416.pdf>
Protocol Operations for SNMPv2
- <http://www.javvin.com/protocol/rfc3417.pdf>
Transport Mappings for SNMPv2
- <http://www.javvin.com/protocol/rfc3418.pdf>
Management Information Base for SNMPv2
- <http://www.javvin.com/protocol/rfc3410.pdf>
Introduction and Applicability Statements for Internet Standard Management Framework
- <http://www.javvin.com/protocol/rfc3411.pdf>
Architecture for Describing SNMP Frameworks
- <http://www.javvin.com/protocol/rfc3412.pdf>
Message Processing and Dispatching for the SNMP
- <http://www.javvin.com/protocol/rfc3413.pdf>
SNMP Applications
- <http://www.javvin.com/protocol/rfc3414.pdf>
User-based Security Model (USM) for SNMPv3
- <http://www.javvin.com/protocol/rfc3415.pdf>
View-based Access Control Model for the SNMP
- <http://www.javvin.com/protocol/rfc3584.pdf>
Coexistence between SNMP v1, v2 and v3

SNMPv1: Simple Network Management Protocol version one

Protocol Description

Simple Network Management Protocol (SNMP) is the protocol developed to manage nodes (servers, workstations, routers, switches and hubs etc.) on an IP network. SNMP enables network administrators to manage network performance, find and solve network problems and plan for network growth. Network management systems learn of problems by receiving traps or change notices from network devices implementing SNMP.

Currently, there are three versions of SNMP defined: SNMP v1, SNMP v2 and SNMP v3. In this document, we provide information primarily on the SNMPv1. SNMPv1 is a simple request/response protocol. The network-management system issues a request, and managed devices return responses. This behavior is implemented by using one of four protocol operations: Get, GetNext, Set, and Trap. The Get operation is used by the NMS to retrieve the value of one or more object instances from an agent. If the agent responding to the Get operation cannot provide values for all the object instances in a list, it does not provide any values. The GetNext operation is used by the NMS to retrieve the value of the next object instance in a table or a list within an agent. The Set operation is used by the NMS to set the values of object instances within an agent. The trap operation is used by agents to asynchronously inform the NMS of a significant event.

For information on the SNMP overview, SNMPv2 and SNMPv3, please check the corresponding pages.

Protocol Structure

SNMP is an application protocol, which is encapsulated in UDP. The general SNMP message format for all versions is shown below:

Version	Community	PDU
---------	-----------	-----

- Version -- SNMP version number. Both the manager and agent must use the same version of SNMP. Messages containing different version numbers are discarded without further processing.
- Community -- Community name used for authenticating the manager before allowing access to the agent.
- PDU for SNMPv1 -- There are five different PDU types: Get-Request, GetNextRequest, GetResponse, SetRequest, and Trap. A general description of each of these is given in the next section.

The format for GetRequest, GetNext Request, GetResponse and SetRequest PDUs is shown here.

PDU type	Request ID	Error status	Error index	Object 1, value 1	Object 2, value 2	...
----------	------------	--------------	-------------	-------------------	-------------------	-----

- Payload length -- 6-bit field that indicates which of the 44 octets in the Segmentation Unit contain actual data. BOM and COM segments always indicate 44 octets. EOM segments indicate between 4 and 44 octets, in multiples of 4 octets. SSM segments indicate between 28 and 44 octets, in multiples of 4 octets.
- Payload CRC -- 10-bit field that performs error detection on the Segment Type, Sequence Number, Message Identifier, Segmentation Unit, Payload Length and Payload CRC fields.
- Once assembled, SIP Level 2 PDUs are passed to the PLCP and physical functions within SIP Level 1 for transmission.

Related Protocols

IEEE 802.6 (DQDB), ATM, SMDS

Sponsor Source

SMDS is defined by Bellcore (Telcordia) (<http://www.telcordia.com>).

Reference

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/smds.htm

Switched Multimegabit Data Service

WiMAX: Broadband Wireless MAN Standard defined in IEEE802.16

Protocol Description

The IEEE 802.16 defines the wireless metropolitan area network (MAN) technology which is branded as WiMAX. The 802.16 includes two sets of standards, 802.16-2004 (802.16d) for fixed WiMAX and 802.16-2005(802.16e) for mobile WiMAX. In addition to provide the missing link for the “last mile” connection in metropolitan area networks where DSL, T1/T3 and Cable and other broadband access methods are not available or too expensive, WiMAX also offers an alternative to satellite Internet services for rural areas and allows mobility of the customer equipment.

IEEE 802.16 standards are concerned with the air interface between a subscriber’s transceiver station and a base transceiver station. The fixed WiMax standard IEEE 802.16-2004 (also known as 802.16d) is approved by the IEEE in June 2004, which provides fixed, point-to-multi point broadband wireless access service and its product profile utilizes the OFDM 256-FFT (Fast Fourier Transform) system profile. The fixed WiMAX 802.16-2004 standard supports both time division duplex (TDD) and frequency division duplex (FDD) services - the latter of which delivers full duplex transmission on the same signal if desired. In Dec. 2005, IEEE approved the mobile WiMax standard, the 802.16-2005 (also known as 802.16e). IEEE 802.16e, based on the early WiMax standard 802.16a, adds mobility features to WiMAX in the 2 to 11 GHz licensed bands. 802.16e allows for fixed wireless and mobile Non Line of Sight (NLOS) applications primarily by enhancing the OFDMA (Orthogonal Frequency Division Multiple Access).

IEEE 802.16 WiMAX is designed as a complementary technology to other wireless communication technologies such as Wi-Fi (WLAN) and Bluetooth (WPAN). The following table provides a quick comparison of 802.16 with 802.11 and the Bluetooth (802.15):

Parameters	IEEE802.16d / 802.16-2004 (Fixed WiMAX)	IEEE802.16e / 802.16-2005 (Mobile WiMAX)	802.11 (WLAN)	802.15.1 (Bluetooth)
Frequency Band	2-66GHz	2 - 11GHz	2.4 – 5.8GHz	2.4GHz
Range	~31 miles	~31 miles	~100 meters	~10meters
Maximum Data rate	~134 Mbps	~15 Mbps	~55 Mbps	~3Mbps
Number of users	Thousands	Thousands	Dozens	Dozens

Protocol Structure

IEEE 802.16 Protocol Architecture has 4 layers: Convergence, MAC, Transmission and physical, which can be mapped to two OSI lowest layers: the physical and data link layer. The WiMax protocol stack is displayed below:

WiMAX Protocol Stack

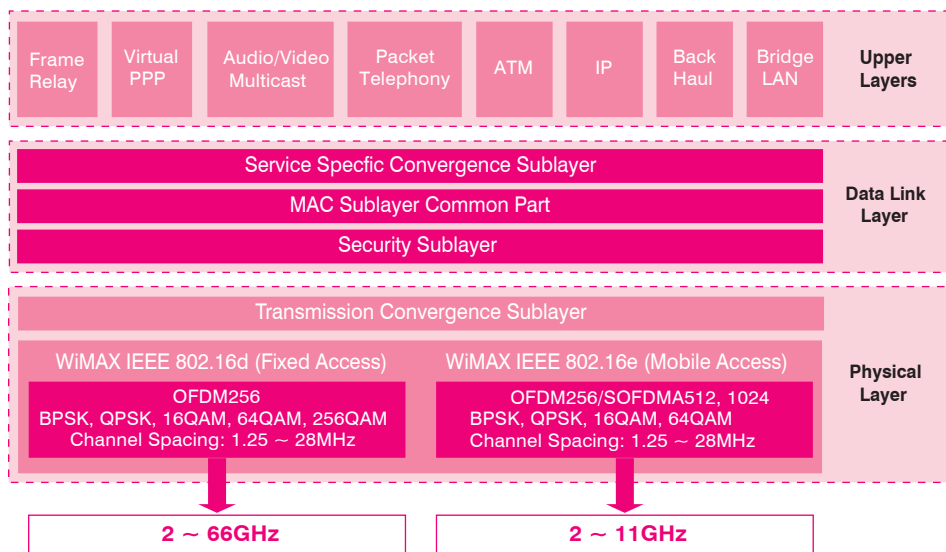


Figure 2-39: WiMax Protocol Stack

Related Protocols

IEEE 802.11, WLAN, Bluetooth, IEEE 802.15, WPAN, WiMAX, WMAN, IEEE802.16d, IEEE802.16-2004, IEEE802.16e, IEEE802.16-2005

Sponsor Source

The WiMAX wireless MAN standards are defined by the IEEE 802.16 working group.

Reference

<http://grouper.ieee.org/groups/802/16/published.html>

Published 802.16 standards

http://www.intel.com/ebusiness/pdf/wireless/intel/80216_wimax.pdf

IEEE 802.16 and WiMAX

Network Protocols Dictionary: From A to Z and 0 to 9

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z Numbers

A

AAL: ATM Adaptation Layer 137

The ATM Adaptation Layer (AAL) relays ATM cells between the ATM Layer and higher layers. When relaying information received from the higher layers, it segments the data into ATM cells. When relaying information received from the ATM Layer, it must reassemble the payloads into a format the higher layers can understand. This operation, which is called Segmentation and Reassembly (SAR), is the main task of AAL. Different AALs (AAL0, AAL1, AAL2, AAL3/4 and AAL5) were defined in supporting different traffic or services expected to be used.

ATM Forum and ITU-T Specification: ITU-T I.366

AAL0: ATM Adaptation Layer Type 0

ATM Adaptation Layer Type 0 (AAL0) refers to raw ATM cells. AAL0 payload consists of 48 bytes without a special field.

ATM Forum and ITU-T Specification: ITU-T I.366.2

AAL1: ATM Adaptation Layer Type 1 137

ATM Adaptation Layer Type 1 (AAL1) supports constant bit rates, time-dependent traffic such as voice and video. AAL1 is used for connection-oriented, delay-sensitive services requiring constant bit rates (CBR), such as video and voice traffic.

ATM Forum and ITU-T Specification: ITU-T I.366.2

AAL2: ATM Adaptation Layer Type 2 137

ATM Adaptation Layer Type 2 (AAL2) is designed for variable bit rate video transfer. AAL2 is perfect for low-rate voice traffic, with compression, silent and idle channel suppression. AAL type 2 is subdivided into the Common Part Sublayer (CPS) and the Service Specific Convergence Sublayer (SSCS).

ATM Forum and ITU-T Specification: ITU-T I.366.2

AAL3/4: ATM Adaptation Layer Type 3/4 137

ATM Adaptation Layer Type 3/4 (AAL3/4) is designed for variable bit rate, delay-tolerant data traffic requiring some sequencing and/or error detection support. AAL 3/4 supports both connectionless and connection-oriented links, but is primarily used for the transmission of SMDS packets over ATM networks.

ATM Forum and ITU-T Specification: ITU-T I.366.2

AAL5: ATM Adaptation Layer Type 5 137

ATM Adaptation Layer Type 5 (AAL5) is designed for variable bit rate, delay-tolerant connection-oriented data traffic requiring minimal sequencing or error detection support. AAL5 supports connection-oriented, VBR services. AAL5 is used predominantly for the transfer of classic IP over ATM and LANE traffic. AAL5 uses SEAL and is the least complex of the current AAL recommendations. AAL5 has no per-cell length or per-cell CRC fields, and offers low bandwidth overhead and simpler processing requirements in exchange for reduced bandwidth capacity and error-recovery capability.

ATM Forum and ITU-T Specification: ITU-T I.366.2

AARP: AppleTalk Address Resolution Protocol 272

AppleTalk Address Resolution Protocol (AARP), similar to the Address Resolution Protocol (ARP), maps AppleTalk nodes

addresses at the network layer to the physical layer (usually MAC) addresses. The AARP table allows for management of the Address Mapping Table on the managed device.

Apple Protocol

ACSE: Association Control Service Element 219

Association Control Service Element (ACSE), an application layer protocol in the OSI model defined by ISO, is designed to establish and release an application-association between two AEs and to determine the application context of that association. The ACSE supports two modes of communication: connection-oriented and connectionless. For the connection-oriented mode, the application association is established and released by the reference of ACSE connection-oriented services. For the connectionless mode, the application association exists during the invocation of the single ACSE connectionless mode service, a UNIT-DATA.

ISO / ITU-T Specification: ISO 8650 / X.227

ADCCP: Advanced Data Communications Control Protocol

Advanced Data Communications Control Protocol (ADCCP) is a bit-oriented data link control protocol that places data on a network and ensures proper delivery to a destination. ADCCP is based on the IBM's SDLC (Synchronous Data Link Control) protocol. The HDLC (High Level Data Link Control) by ISO and the LAPB (Link Access Protocol-Balanced) by ITU/CCITT are based on the ADCCP.

ANSI Specification: ANSI X3.66

ADSL Lite 152

ADSL Lite, also known as universal ADSL, splitterless ADSL or G.lite, is one of the Digital Subscriber Line technologies that allows broadband data access over normal phone lines (twisted pair cables, also called POTS). ADSL Lite offers a maximum of 1.5 Mbit/s downstream and 512 kbit/s upstream and does not require the use of phone line splitters.

ANSI/ITU-T Protocol

ADSL: Asynchronous Digital Subscriber Line 152

Asynchronous Digital Subscriber Line (ADSL) is one of the Digital Subscriber Line technologies that allows broadband data access over normal phone lines (twisted pair cables, also called POTS). ADSL allows higher speed for data downstream than upstream, and this is why the word "Asynchronous" is there. For conventional ADSL, downstream rates start at 256 kbit/s and typically reach 8 Mbit/s within 1.5 km (5000 ft) of the DSLAM-equipped central office or remote terminal. Upstream rates start at 64 kbit/s and typically reach 256 kbit/s but can go as high as 1024 kbit/s. The name ADSL Lite is sometimes used for the slower versions.

ANSI/ITU-T Protocols

ADSP: AppleTalk Data Stream Protocol 272

AppleTalk Data Stream Protocol (ADSP) is a session-level protocol that provides symmetric, connection-oriented, full-duplex communication between two sockets on the AppleTalk network. In addition, it handles flow-control and reliability and provides a data channel for the hosts, which is a simple trans-

port method for data across a network. ADSP is a connection-oriented protocol that guarantees in-sequence data delivery with flow control.

Apple Protocol

AEP: AppleTalk Echo Protocol 272

AppleTalk Echo Protocol (AEP) is a transport layer protocol in the AppleTalk protocol suite designed to test the reachability of network nodes. AEP generates packets to be sent to the network node and is identified in the Type field of a packet as an AEP packet. The packet is first passed to the source DDP. After it is identified as an AEP packet, it is forwarded to the node where the packet is examined by the DDP at the destination. After the packet is identified as an AEP packet, the packet is then copied and a field in the packet is altered to create an AEP reply packet, and is then returned to the source node.

Apple Protocol

AES: Advanced Encryption Standard

The Advanced Encryption Standard (AES), also known as Rijndael, is a block cipher adopted as an encryption standard developed by NIST. AES is intended to specify an unclassified, publicly-disclosed, symmetric encryption algorithm. AES has a fixed block size of 128 bits and a key size of 128, 192 or 256 bits.

NIST Specification: Federal Information Processing Standards Publication 197

AES-CMAC

AES-CMAC, abbreviation of Advanced Encryption Standard-Cipher-based Message Authentication Code, is an authentication algorithm based on CMAC with the 128-bit Advanced Encryption Standard (AES). AES-CMAC achieves a security goal similar to that of HMAC. Since AES-CMAC is based on a symmetric key block cipher, AES, and HMAC is based on a hash function, such as SHA-1, AES-CMAC is appropriate for information systems in which AES is more readily available than a hash function.

IETF Specification: RFC 4493

AES-CMAC-PRF-128

AES-CMAC-PRF-128, abbreviation of Advanced Encryption Standard-Cipher-based Message Authentication Code-Pseudo-Random Function-128, is an authentication algorithm based on AES-CMAC. AES-CMAC-PRF-128 is identical to AES-CMAC except that the 128-bit key length restriction is removed.

IETF Specification: RFC 4615

AFP: Apple Filing Protocol 272

Apple Filing Protocol (AFP), formerly AppleTalk Filing Protocol, is the protocol for communicating with AppleShare file servers. Built on top of ASP, it provided services for authenticating users (extensible to different authentication methods including two-way random-number exchange) and for performing operations specific to the Macintosh HFS filesystem.

Apple Protocol

AFP: AppleTalk Filing Protocol 272

AppleTalk Filing Protocol (AFP), renamed to Apple Filing Protocol now, is the protocol for communicating with AppleShare file servers. Built on top of ASP, it provided services for authenticating users (extensible to different authentication methods including two-way random-number exchange) and for performing operations specific to the Macintosh HFS file system.

Apple Protocol

AH: Authentication Header 97

Authentication Header, a protocol in the IPsec (Internet Security) suite, is used to provide connectionless integrity and data origin authentication for IP datagrams, and to provide protection against replays. This protection service against replay is an optional service to be selected by the receiver when a Security Association is established. AH provides authentication for as much of the IP header as possible, as well as for upper level protocol data. However, some IP header fields may change in transit and the value of these fields, when the packet arrives at the receiver, may not be predictable by the sender. The values of such fields cannot be protected by AH. Thus the protection provided to the IP header by AH is only partial in some cases.

IETF Specification: RFC 2402

Airline protocol

Airline protocol refers to the airline reservation system data and the protocols, such as P1024B (ALC), P1024C (UTS), and MATIP, that transport the data between the mainframe and the Agent Set Control Unit (ASCU).

AKE: Augmented Key Exchange

Augmented Key Exchange (AKE) is a key exchange protocol for public key cryptography systems.

IETF Protocol

ALC: Airline Control Protocol

Airline Control Protocol (ALC) is a data link layer polled protocol that runs in full-duplex mode over synchronous serial (V.24) lines and uses the binary-coded decimal (BCD) character set.

ANDNA: Abnormal Netsukuku Domain Name

Anarchy Abnormal Netsukuku Domain Name Anarchy (ANDNA), similar to the Domain Name System (DNS), is the distributed, non-hierarchical and decentralised system of hostname management in Netsukuku. The ANDNA database is scattered inside all the Netsukuku and works in the following way: in order to resolve a hostname, we just have to calculate its hash. The hash is nothing more than a number (IP), and the node related to that IP is called `andna_hash_node`. The `hash_node` will keep a small database, which associates all the hostnames related to it with the IP of the node, which has registered the same hostnames.

APON: ATM Passive Optical Network

ATM Passive Optical Network (APON), or ATM PON, is the initial PON specification defined by the FSAN (Full Service Access Network) group using ATM as their layer 2 signaling protocol. Use of the term APON led users to believe that only ATM services could be provided to end-users, so the FSAN decided to broaden the name to Broadband PON (BPON). BPON systems offer numerous broadband services including Ethernet access and video distribution.

FSAN Group Protocol

APPC: Advanced Program-to-Program Communications 262

Advanced Program-to-Program Communications (APPC), a protocol roughly in the OSI presentation and session layers, is a programming interface standard in the IBM SNA system that allows interconnected systems to communicate and share the processing of programs. Originally developed by IBM as a remote transaction processing tool between Logic Units (LUs), APPC is now used to provide distributed services within a heterogeneous computing environment. APPC establishes and

Network Protocols Handbook

“This book is an excellent reference for Internet programmers, network professionals and college students who are majoring IT and networking technologies. It is also useful for any individuals who want to know more details about Internet technologies. I highly recommend this book to our readers.”

Dr. Ke Yan
Chief Architect of Juniper Networks
Founder of NetScreen Technologies

Fully explains and illustrates all commonly used network communication protocols, including TCP/IP, WAN, LAN technologies

Covers the latest and emerging technologies such as VOIP, SAN, MAN, VPN/Security, WLAN, VLAN and more

Addresses vendor-specific technologies: Cisco, IBM, Novell, Sun, HP, Microsoft, Apple, etc.

Reviews the ISO networking architecture and protocols

Covers SS7 protocols

Hundreds of illustrations of protocol formats and header structures

Hundreds of references for further reading and studies

Comprehensive networking technology and protocol dictionary

“Must-Have” for IT/Networking professionals and students

The logo for Javvin Technologies, Inc. features the word "Javvin" in a stylized, cursive script. The letters are a light brown or tan color with a subtle gradient and a slight shadow effect, giving it a three-dimensional appearance. The 'J' is particularly large and loops around the 'a'.

Javvin Technologies, Inc.

13485 Old Oak Way
Saratoga CA 95070 USA
www.javvin.com