

MANAGING IP NETWORKS

IEEE Press
445 Hoes Lane,
Piscataway, NJ 08854

IEEE Press Editorial Board
Stamatios V. Kartalopoulos, *Editor in Chief*

M. Akay	M. E. El-Hawary	M. Padgett
J. B. Anderson	R. J. Herrick	W. D. Reeve
R. J. Baker	D. Kirk	S. Tewksbury
J. E. Brewer	R. Leonardi	G. Zobrist
	M. S. Newman	

Kenneth Moore, *Director of IEEE Press*
Catherine Faduska, *Senior Acquisitions Editor*
Christina Kuhnen, *Associate Acquisitions Editor*

IEEE Communications Society, *Sponsor*
ComSoc Liaison to IEEE Press, Mansoor Shafi

Technical Reviewer
James Won-Ki Hong, POSTECH, Korea

Books in the IEEE Press Series on Network Management

Aidarous and Plevyak, *Telecommunications Network Management into the 21st Century*, 1995

Aidarous and Plevyak, *Telecommunications Network Management: Technology and Implementation*, 1997

Chen and Kong, *Integrated Telecommunications Management Solutions*, 1999

Raman, *Fundamentals of Telecommunications Network Management*, 1999

Rozenblit, *Security for Telecommunications Network Management*, 1999

Ahmad, *Asynchronous Transfer Mode (ATM) Technology, Networks, and Protocols*, 2002

MANAGING IP NETWORKS

Challenges and Opportunities

Edited by

SALAH AIDAROUS
THOMAS PLEVYAK

With Contributions by

JAVIER ARACIL
ANDREA FUMAGALLI
PAUL LEVINE
JOBERTO SÉRGIO BARBOSA MARTINS
MOSTAFA HASHEM SHERIF
BURKHARD STILLER
LUCA VALCARENGHI

IEEE Press Series on Network Management
Salah Aidarous and Thomans Plevyak, *Series Editors*

IEEE Communications Society, *Sponsor*



IEEE PRESS



A JOHN WILEY & SONS, INC., PUBLICATION

Copyright © 2003 by the Institute of Electrical and Electronics Engineers, Inc. All rights reserved.

Published simultaneously in Canada.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400, fax 978-750-4470, or on the web at www.copyright.com. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, e-mail: permreq@wiley.com.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representation or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services please contact our Customer Care Department within the U.S. at 877-762-2974, outside the U.S. at 317-572-3993 or fax 317-572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print, however, may not be available in electronic format.

Library of Congress Cataloging-in-Publication Data:

Managing IP networks : challenges and opportunities / edited by Salah Aidarous, Thomas Plevyak.
p. cm. — (IEEE Press series on network management)
Includes bibliographical references and index.
ISBN 0-471-39299-5 (cloth)
1. Computer networks—Management. 2. TCP/IP (Computer network protocol) I. Aidarous, Salah. II. Plevyak, Thomas. III. IEEE series on network management

TK5105.5.M3577 2003
004.6'2—dc21

2003053465

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

In memory of
Salah Aidarous
co-editor of this book
and an outstanding technical professional
in the field of communications

CONTENTS

Contributors	xv
Introduction	1
1 Current Practice and Evolution	7
Salah Aidarous	
1.1 Introduction	7
1.2 Evolution of Network Architecture	8
1.3 Technology Breakthrough	9
1.4 IP Management Challenges	10
1.5 IP/PSTN Integration	11
1.7 Summary	12
2 eCommerce	13
Paul Levine	
2.1 Introduction	13
2.2 eCommerce Requirements	14
2.2.1 Consumer Interest in eCommerce Standardization	14
2.2.2 Consumer Requirements for eCommerce	15

2.2.3	Horizontal Aspects	18
2.3	Open-edi	21
2.3.1	Open-edi Conceptual Model	21
2.3.2	Open-edi Reference Model	23
2.3.3	MoU Management Group Concerning Standardization in the Field of eBusiness	27
2.4	Business Operational View	28
2.4.1	Emphasis on Semantics	28
2.4.2	BOV Requirements	29
2.4.3	BOV Methodology	30
2.5	Semantics (Data Definition Standards)	33
2.5.1	IT-Enablement	33
2.5.2	Data Definition Standards Examples	34
2.5.3	Harvest Existing Business Information	40
2.6	Shared Semantics for Interoperability (Data Exchange Standards)	42
2.6.1	Business Process Modeling in ebXML	43
2.6.2	tML Framework	49
2.6.3	Business Application Contracts in TM Forum's New-Generation OSS	51
2.7	Summary	53
	References	54

3 Quality of Service in IP Networks

57

Joberto Sérgio Barbosa Martins

	Introduction	57
3.1	IP Context and Quality of Service	58
3.1.1	IP Network Context and Perspectives	59
3.1.2	Switched Networks, IP Networks, and Applications	59
3.1.3	IP and Quality of Service: Basic Issues	61
3.2	Quality of Service	64
3.2.1	Quality of Service: Trying a Definition	64
3.2.2	Quality of Service: How to Proceed?	64
3.2.3	Application's Taxonomy: Quality of Service	65
3.2.4	Quality of Service Parameters	67
3.3	Quality of Service: Approaches and Initiatives for IP Networks	74
3.3.1	Quality of Service: Some Basic Definitions	75
3.3.2	IP Quality of Service: How to Handle It?	78
3.3.3	Do We Need Quality of Service Control?	78

3.4	Packet Conditioning, Queue Scheduling, and Congestion Control in Routers	80
3.4.1	Packet Conditioning	81
3.4.2	Queue Scheduling	84
3.4.3	Congestion Control	89
3.5	Integrated Services Architecture	95
3.5.1	IETF Quality of Service Strategies and Initiatives	95
3.5.2	Goals and Basics	95
3.5.3	Integrated Service Architecture: Characteristics and Services	96
3.5.4	Services	97
3.5.5	Resource Reservation Protocol	100
3.5.6	RSVP: Final Considerations	108
3.6	Differentiated Services Architecture	110
3.6.1	Goals and Basics	110
3.6.2	The Differentiated Services Architecture	111
3.6.3	Service-Level Specifications and Traffic Conditioning	113
3.6.4	Diff-Serv Functionalities	115
3.6.5	Differentiated Services and Per-Hop Behaviors	118
3.6.6	Expedited Forwarding	119
3.6.7	Assured Forwarding	121
3.6.8	Differentiated Services: Final Considerations	124
3.7	Multiprotocol Label Switching	124
3.7.1	Identifying Routing and Switching Basics and Possible Variations	125
3.7.2	Goals and Basics	126
3.7.3	MPLS Operation	126
3.7.4	MPLS Domain	127
3.7.5	Forward Equivalence Class and MPLS Labels	128
3.7.6	Label Switched Path	129
3.7.7	Packet-to-FEC Assignment	131
3.7.8	Label Distribution	132
3.7.9	Label Distribution Protocols	136
3.7.10	Constraint-Based Routing Label Distribution Protocol	138
3.7.11	MPLS and ATM	140
3.7.12	MPLS and GMPLS: Final Considerations	141
3.8	Summary	141
	References	142

4 A Survey of Charging Internet Services**143**

Burkhard Stiller

- 4.1 Introduction 143
 - 4.1.1 Outline 146
- 4.2 Motivation and Terminology 146
 - 4.2.1 Scenario 148
 - 4.2.2 Viewpoints 148
 - 4.2.3 Fairness and Utility 151
 - 4.2.4 Charging Tasks and Terms 153
 - 4.2.5 Definitions of Terminology 159
 - 4.2.6 Networking Terms 161
- 4.3 Related Work 161
 - 4.3.1 Charging Projects 162
 - 4.3.2 Metering, Accounting, and Mediation Technology 165
 - 4.3.3 Traditional Telecommunication Billing 166
- 4.4 Internet Services and Technology Choices 167
 - 4.4.1 Quality of Service Methods 168
 - 4.4.2 Service Differentiation Methods 168
 - 4.4.3 Internet Technology Choices 169
 - 4.4.4 Interprovider Agreements 171
 - 4.4.5 Standardized Data Formats 173
 - 4.4.6 Electronic Payment Systems 175
- 4.5 Pricing Models 175
 - 4.5.1 Pricing Model Constituents 175
 - 4.5.2 General Characteristics of Pricing Models 176
 - 4.5.3 Static and Dynamic Pricing Models 182
 - 4.5.4 Pricing Model Classification Approaches 185
- 4.6 ISP Cost Models 187
- 4.7 Charging Support Systems 188
 - 4.7.1 CSS Components 189
 - 4.7.2 CSS Dimensions 190
 - 4.7.3 Basic CSS Tasks 191
 - 4.7.4 CSS Architecture 192
- 4.8 Business Model Aspects 196
 - 4.8.1 Market-managed Three-tiered Model 192
 - 4.8.2 Internet Service Provider Segmentation 197
 - 4.8.3 Application Service Provider 198
 - 4.8.4 Charging Content 200

4.9	Summary and Conclusions	202
	Acknowledgments	203
	References	204

5 IP Security **211**

Mostafa Hashem Sherif

5.1	Introduction	211
5.2	Security of Telecommunications Services	211
5.3	Security Objectives	213
5.4	OSI Model for Cryptographic Security	214
	5.4.1 Security Services at the Link Layer	217
	5.4.2 Security Services at the Network Layer	217
	5.4.3 Application Security	220
5.5	Message Confidentiality	220
	5.5.1 Symmetric Cryptography	221
	5.5.2 Public Key Cryptography	222
5.6	Data Integrity	223
	5.6.1 Verification of the Integrity with a One-Way Hash Function	224
	5.6.2 Verification of the Integrity with Public Key Cryptography	226
	5.6.3 Blind Signature	226
	5.6.4 Verification of the Integrity with Symmetric Cryptography	228
5.7	Identification of Participants	230
	5.7.1 Biometric Identification	231
	5.7.2 Summary and Evaluation	233
5.8	Authentication of Participants	234
5.9	Access Control	235
	5.9.1 Denial-of-Service	237
5.10	Nonrepudiation	239
	5.10.1 Time-stamping and Sequence Numbers	240
5.11	Secure Management of Cryptographic Keys	240
	5.11.1 Production and Storage	241
	5.11.2 Distribution	241
	5.11.3 Utilization, Withdrawal, and Replacement	242
	5.11.4 Key Revocation	242
	5.11.5 Deletion, Backup, and Archiving	242

- 5.11.6 Comparison Between Symmetric and Public Key Cryptography 242
- 5.12 Exchange of Secret Keys: Kerberos 243
 - 5.12.1 Public Key Kerberos 246
- 5.13 Exchange of Public Keys 247
 - 5.13.1 Diffe–Hellman Exchange 247
 - 5.13.2 Internet Security Association and Key Management Protocol 248
 - 5.13.3 Simple Key Management for Internet Protocols 249
 - 5.13.4 Key Exchange Algorithm 250
- 5.14 Certificate Management 250
 - 5.14.1 Basic Operation 253
 - 5.14.2 Description of an X.509 Certificate 253
 - 5.14.3 Certification Path 255
 - 5.14.4 Process of Strong Authentication 259
 - 5.14.5 Certificate Revocation 261
 - 5.14.6 Attribute Certificates 261
- 5.15 Applications for Network Management 263
- 5.16 Encryption Cracks 264
- 5.17 Summary 266
- Appendix I: Areas Related to Security Policies 267
- Appendix II: Principles of Symmetric Encryption 267
 - AII.1 Modes of Algorithm Utilization for Block Encryption 267
 - AII.2 Examples of Symmetric Block Encryption Algorithms 273
- Appendix III: Principles of Public Key Encryption 275
 - AIII.1 RSA 275
 - AIII.2 Public Key Cryptography Standards 276
 - AIII.3 Pretty Good Privacy 277
 - AIII.4 Elliptic Curve Cryptography 278
- Appendix IV: Principles of the Digital Signature Algorithm 279
 - References 280

6 The Future Optical Internet: Integration of Optical and IP Technologies 287

Andrea Fumagalli, Javier Aracil, and Luca Valcarenghi

- 6.1 Introduction 287
- 6.2 Optical Network Technologies 288
 - 6.2.1 Optical Components 289
 - 6.2.2 The Optical Layer 292

6.2.3	All-Optical Network Architecture	294
6.3	Protocol Architectures, Signaling and Framing Techniques for the Optical Internet	303
6.3.1	The First-Generation Optical Internet: IP over First-Generation Optical Networks	305
6.3.2	The Second-Generation Optical Internet: IP over Second-Generation Optical Network	309
6.4	Traffic Engineering in the Optical Internet	315
6.4.1	Self-similarity	315
6.4.2	Flow Level Analysis	321
6.4.3	Impact on Optical Internet Traffic Engineering	323
6.5	Open Challenges	325
6.5.1	Traffic Engineering in the Optical Internet	325
6.5.2	Resilience in IP over WDM Networks	326
6.5.3	Outlook	328
	Acknowledgments	328
	References	328

Acronyms	335
-----------------	------------

Index	345
--------------	------------

CONTRIBUTORS

The late **Salah Aidarous** worked in the Network Management Division, NEC America, on the planning and development of integrated network management systems. Before his employment at NEC, he was with Nortel Technology (formerly BNR) working on a broad range of assignments in telecommunications networks and services planning and development. Dr. Aidarous received a B.S. and an M.S. in Electrical Engineering from Ain Shams University, Cairo, and a Ph.D. in Electrical Engineering from Louvain University, Belgium.

Thomas Plevyak is a past president of the IEEE Communications Society (ComSoc). He served as ComSoc President in 1998 and 1999. Mr. Plevyak is a past director of publications of ComSoc and a former editor-in-chief of *IEEE Communications Magazine*. He retired after 28 years with Bell Laboratories and AT&T Network Systems (now Lucent Technologies) and is now a Distinguished Member of Technical Staff with Verizon in Arlington, Virginia, responsible for operations and network management standards. He is also an IEEE Fellow. Mr. Plevyak is the former vice chairman of the Inter-American Telecommunications Commission (CITEL), Permanent Consultative Committee 1 (PCC.1), a unit of the Organization of American States (OAS). He is a member of the United States ITU Association (USITUA) Board of Directors. He is co-editor and an author of *Telecommunications Network Management Into the 21st Century: Techniques, Standards, Technologies, and Applications* and is co-editor of the series on network management, which includes this book.

Javier Aracil received the MSc. and Ph.D. degrees (Honors) from Technical University of Madrid in 1993 and 1995, both in Telecommunications Engineering. In 1995, he was awarded a Fulbright scholarship and appointed a postdoctoral researcher of the Department of Electrical Engineering and Computer Sciences, University of California, Berkeley. In 1998, he was a research scholar at the Center for Advanced Telecommunications,

Systems and Services of The University of Texas at Dallas. He is currently a tenured associate professor at Public University of Navarra, Spain. Dr. Aracil's research interests are in IP over WDM networks, Internet services analysis, and performance evaluation of communication networks. Dr. Aracil is a member of the editorial board of *SPIE/Kluwer Optical Networks Magazine*.

Andrea Fumagalli holds a Ph.D. in Electrical Engineering (1992) and a Laurea Degree in Electronics Engineering (1987) from the Politecnico di Torino, Italy. Since 1997, he has been an associate professor of Electrical Engineering at the University of Texas at Dallas and became the head of the Optical Networking Advanced Research (OpNeAR) Lab in 1000. His research interests include high speed and optical networking, survivable networks, and sensor networks. He serves on the editorial boards of ACM/IEEE Transactions on Networking and the Elsevier *Journal of Computer Networks*.

Paul Levine has held leadership roles in many standards bodies and information/communications industry forums with the objective of converging standardization initiatives to common approaches for B2B interoperability. Mr. Levine has enjoyed a 34-year career with Bell Laboratories, Bellcore, and Telcordia Technologies, in various positions dealing with design and administration of shared information. Most recently he held the position of Standards Development Director, COMMON LANGUAGE® Products,* the Telcordia business unit which provides a data administration service essential for operability within and interoperability among telecommunications service providers. He holds BME and MSME degrees from Rensselaer Polytechnic Institute, Troy, NY.

Joberto Sérgio Barbosa Martens received his Ph.D. in Computer Science, Université Paris VI, France, 1986; M.Sc. in Electronic Engineering, PII, Eindhoven, Netherlands, 1979 and B.S. in Electronic Engineering, UFPb, Brazil, 1977. Dr. Martens has also worked as visiting scientist at ICSI, Berkeley University at Berkeley, California in 1995 and worked as full professor at UFPb from 1977 to 2000. Currently, he develops activities as full professor and director of Research Activities of the Computer Networks Group (NUPERC) at University Salvador (UNIFACS), Brazil. Dr. Martens' main areas of research and activities include Quality of Service, Multimedia over IP, Telecommunications Systems, High-Speed Networks and Mobile Agents. He is a project manager, expert consultant, and course instructor in these areas for various institutions, international congresses, and enterprises. Additional information about his professional activities can be found in www.jsmnet.com.

Mostafa Hashem Sherif is a principal member of the Technical Staff at AT&T. He received a B.Sc. in Electronics and Communications and an M.Sc. in Electrical Engineering from Cairo University, Egypt in 1972 and 1975, respectively, and a Ph.D. in Engineering from the University of California, Los Angeles in 1980. In 1996, he obtained a Masters of Science in the Management of Technology from Stevens Institute of Technology, Hoboken, NJ. He is a senior member of the IEEE, a standards editor for the *IEEE Communication Magazine* and the author of *Secure Protocols for Electronic Commerce* published by CRC Press, 2002. The French version, co-authored with Professor A. Sehrouchni from the ENST of Paris, is published by Eyrolles under the title *La monnaie électronique*. Dr.

*COMMON LANGUAGE® is a registered trademark of Telcordia Technologies, Inc.

Sherif is a certified project manager from the Project Management Institute. He has participated in standardization activities in the International Telecommunication Union (ITU), T1A1, and the ATM Forum. He is a founding member of the series of conferences on management of technology sponsored by the International Association for the Management of Technology (IAMOT) and of the IEEE International Symposium on Computers and Communications (ISCC). He is a core member of the Awards and Recognition working committee of the AT&T Project Management Council and a member of the evaluation committee for the Commission on Science and Technology, State of New Jersey.

Professor Dr. Burkhard Stiller received his diploma degree in computer science and his doctoral degree from the University of Karlsruhe, Germany in October 1990 and February 1994, respectively while being a Research Assistant at the Institute of Telematics, University of Karlsruhe. After working as a research fellow at the University of California, Irvine and the University of Cambridge, Computer Laboratory, England, he joined the Computer Engineering and Networks Laboratory TIK, Swiss Federal Institute of Technology ETH Zurich, Switzerland. Currently, Dr. Stiller is a full professor at the University of Federal Armed Forces Munich, German, in charge of the Information Systems Laboratory IIS, and an assistant professor at ETH Zurich, TIK. His primary research interests include Internet communications, Quality-of-Service models, charging and accounting for packet-based services, pricing schemes, mobility and AAA architectures, and peer-to-peer systems. He published more than 50 papers and headed a number of national and international projects in areas such as CATI, Mac/MicPay, M3I, MMAPPS, or MobyDick. Professor Stiller is member of the editorial board of the Kluwer's Netmonics journal on economic research and electronic networking, the ACM, and the German Society for Computer Science GI.

Luca Valcarenghi earned a Laurea degree in Electronics Engineering in 1997 from the Politecnico di Torino, Italy, a M.S. degree in Electrical Engineering in 1999 and a Ph.D. in Electrical Engineering-Telecommunications in 2001, from the University of Texas at Dallas. In January 2002, he was appointed as research associate of the Optical Networking Advanced Research (OpNeAR) Lab of the University of Texas at Dallas Erik Jonsson School of EE/CS. He is currently assistant professor at the Scuola Superiore Sant'Anna of University Studies and Doctoral Research of Pisa, Italy. Dr. Valcarenghi co-authored more than a dozen papers published in international journals and presented in leading international conferences. He is a member of the IEEE, feature editor of the SPIE/Kluwer *Optical Networks Magazine*, and has been part of the Organizing Committee and Technical Program Committee of international conferences, such as OptiComm2000 and Optical Networking and Systems Symposium at IEEE Globecom 2003. His main research interests are optical networks design, analysis, and optimization; artificial intelligence optimization techniques; communication networks reliability and IP over WDM Networking.