

# CONTENTS

---

<b>Contributors</b>	<b>xv</b>
<b>Introduction</b>	<b>1</b>
<b>1 Current Practice and Evolution</b>	<b>7</b>
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
<b>2 eCommerce</b>	<b>13</b>
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

**viii** CONTENTS

- 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

**x** CONTENTS**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

**xii** CONTENTS

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 Diffie–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
<b>6 The Future Optical Internet: Integration of Optical and IP Technologies</b>	<b>287</b>
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

<b>Acronyms</b>	<b>335</b>
-----------------	------------

<b>Index</b>	<b>345</b>
--------------	------------

