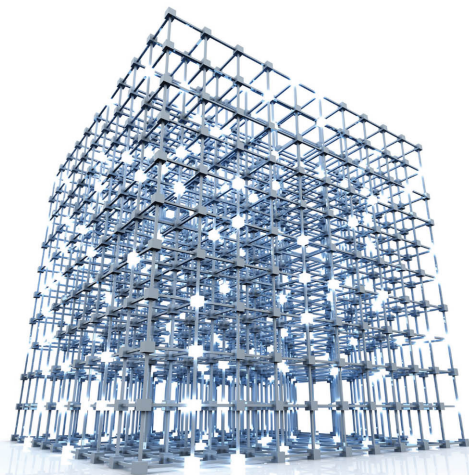




William Stallings

Foundations of Modern Networking

SDN, NFV, QoE, IoT, and Cloud



FREE SAMPLE CHAPTER



SHARE WITH OTHERS

THE WILLIAM STALLINGS BOOKS ON COMPUTER AND DATA COMMUNICATIONS TECHNOLOGY

DATA AND COMPUTER COMMUNICATIONS, TENTH EDITION

A comprehensive survey that has become the standard in the field, covering (1) data communications, including transmission, media, signal encoding, link control, and multiplexing; (2) communication networks, including circuit and packet switched, Frame Relay, ATM, and LANs; (3) the TCP/IP protocol suite, including IPv6, TCP, MIME, and HTTP, as well as a detailed treatment of network security. **Received the 2007 Text and Academic Authors Association (TAA) award for the best Computer Science and Engineering Textbook of the year.**

WIRELESS COMMUNICATION NETWORKS AND SYSTEMS (with Cory Beard)

A comprehensive, state-of-the art survey. Covers fundamental wireless communications topics, including antennas and propagation, signal encoding techniques, spread spectrum, and error-correction techniques. Examines satellite, cellular, wireless local loop networks, and wireless LANs, including Bluetooth and 802.11. Covers wireless mobile networks and applications.

COMPUTER SECURITY, THIRD EDITION (with Lawrie Brown)

A comprehensive treatment of computer security technology, including algorithms, protocols, and applications. Covers cryptography, authentication, access control, database security, cloud security, intrusion detection and prevention, malicious software, denial of service, firewalls, software security, physical security, human factors, auditing, legal and ethical aspects, and trusted systems. **Received the 2008 TAA award for the best Computer Science and Engineering Textbook of the year.**

OPERATING SYSTEMS, EIGHTH EDITION

A state-of-the art survey of operating system principles. Covers fundamental technology as well as contemporary design issues, such as threads, SMPs, multicore, real-time systems, multiprocessor scheduling, embedded OSs, distributed systems, clusters, security, and object-oriented design. **Third, fourth and sixth editions received the TAA award for the best Computer Science and Engineering Textbook of the year.**

CRYPTOGRAPHY AND NETWORK SECURITY, SIXTH EDITION

A tutorial and survey on network security technology. Each of the basic building blocks of network security, including conventional and public-key cryptography, authentication, and digital signatures, are covered. Provides a thorough mathematical background for such algorithms as AES and RSA. The book covers important network security tools and applications, including S/MIME, IP Security, Kerberos, SSL/TLS, network access control, and Wi-Fi security. In addition, methods for countering hackers and viruses are explored. **Second edition received the TAA award for the best Computer Science and Engineering Textbook of 1999.**

NETWORK SECURITY ESSENTIALS, FIFTH EDITION

A tutorial and survey on network security technology. The book covers important network security tools and applications, including S/MIME, IP security, Kerberos, SSL/TLS, network access control, and Wi-Fi security. In addition, methods for countering hackers and viruses are explored.

BUSINESS DATA COMMUNICATIONS, SEVENTH EDITION (with Tom Case)

A comprehensive presentation of data communications and telecommunications from a business perspective. Covers voice, data, image, and video communications and applications technology and includes a number of case studies. Topics covered include data communications, TCP/IP, cloud computing, Internet protocols and applications, LANs and WANs, network security, and network management.

COMPUTER ORGANIZATION AND ARCHITECTURE, TENTH EDITION

A unified view of this broad field. Covers fundamentals such as CPU, control unit, microprogramming, instruction set, I/O, and memory. Also covers advanced topics such as multicore, superscalar, and parallel organization. **Five-time winner of the TAA award for the best Computer Science and Engineering Textbook of the year.**

Foundations of Modern Networking

SDN, NFV, QoE, IoT, and Cloud

William Stallings

With contributions by:

Florence Agboma
British Sky Broadcasting

Sofiene Jelassi
Assistant Professor
University of Monastir, Tunisia

PEARSON

800 East 96th Street, Indianapolis, Indiana 46240 USA

Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud

Copyright © 2016 by Pearson Education, Inc.

All rights reserved. Printed in the United States of America. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. To obtain permission to use material from this work, please submit a written request to Pearson Education, Inc., Permissions Department, 200 Old Tappan Road, Old Tappan, New Jersey 07675, or you may fax your request to (201) 236-3290.

ISBN-13: 978-0-13-417539-3

ISBN-10: 0-13-417539-5

Library of Congress Control Number: 2015950673

Text printed in the United States on recycled paper at RR Donnelley, Crawfordsville, IN
First printing: November 2015

Trademarks

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the publisher was aware of a trademark claim, the designations have been printed with initial capital letters or in all capitals.

Warning and Disclaimer

The author and publisher have taken care in the preparation of this book, but make no expressed or implied warranty of any kind and assume no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact international@pearsoned.com.

Visit us on the Web: informit.com/aw

Associate Publisher
Dave Dusthimer

Executive Editor
Brett Bartow

Senior Development Editor
Christopher Cleveland

Managing Editor
Sandra Schroeder

Project Editor
Mandie Frank

Copy Editor
Keith Claine

Indexer
Publishing Works

Proofreader
Katie Matejka

Technical Reviewers
Wendell Odom
Tim Szigeti

Editorial Assistant
Vanessa Evans

Designer
Alan Clements

Composer
Mary Sudul

Contents at a Glance

Preface	xxi
PART I MODERN NETWORKING	3
CHAPTER 1 Elements of Modern Networking	4
CHAPTER 2 Requirements and Technology	38
PART II SOFTWARE DEFINED NETWORKS	75
CHAPTER 3 SDN: Background and Motivation	76
CHAPTER 4 SDN Data Plane and OpenFlow	92
CHAPTER 5 SDN Control Plane	112
CHAPTER 6 SDN Application Plane	144
PART III VIRTUALIATION	175
CHAPTER 7 Network Functions Virtualization: Concepts and Architecture	176
CHAPTER 8 NFV Functionality	198
CHAPTER 9 Network Virtualization	230
PART IV DEFINING AND SUPPORTING USER NEEDS	265
CHAPTER 10 Quality of Service	266
CHAPTER 11 QoE: User Quality of Experience	300
CHAPTER 12 Network Design Implications of QoS and QoE	322
PART V MODERN NETWORK ARCHITECTURE: CLOUDS AND FOG	347
CHAPTER 13 Cloud Computing	348
CHAPTER 14 The Internet of Things: Components	372
CHAPTER 15 The Internet of Things: Architecture and Implementation ..	394
PART VI RELATED TOPICS	433
CHAPTER 16 Security	434
CHAPTER 17 The Impact of the New Networking on IT Careers	466
Appendix A: References	492
Glossary	498
Index	510

Table of Contents

Preface	xxi
PART I MODERN NETWORKING	3
Chapter 1: Elements of Modern Networking	4
1.1 The Networking Ecosystem	5
1.2 Example Network Architectures	7
A Global Network Architecture	7
A Typical Network Hierarchy	9
1.3 Ethernet	11
Applications of Ethernet	11
Standards	14
Ethernet Data Rates	14
1.4 Wi-Fi	19
Applications of Wi-Fi	19
Standards	21
Wi-Fi Data Rates	21
1.5 4G/5G Cellular	23
First Generation	23
Second Generation	23
Third Generation	24
Fourth Generation	24
Fifth Generation	25
1.6 Cloud Computing	25
Cloud Computing Concepts	26
The Benefits of Cloud Computing	27
Cloud Networking	28
Cloud Storage	28

1.7	Internet of Things	28
	Things on the Internet of Things	28
	Evolution	29
	Layers of the Internet of Things	29
1.8	Network Convergence	30
1.9	Unified Communications	33
1.10	Key Terms	37
1.11	References	37
Chapter 2: Requirements and Technology		38
2.1	Types of Network and Internet Traffic	39
	Elastic Traffic	39
	Inelastic Traffic	40
	Real-Time Traffic Characteristics	43
2.2	Demand: Big Data, Cloud Computing, and Mobile Traffic	45
	Big Data	45
	Cloud Computing	48
	Mobile Traffic	51
2.3	Requirements: QoS and QoE	53
	Quality of Service	53
	Quality of Experience	54
2.4	Routing	55
	Characteristics	55
	Packet Forwarding	56
	Routing Protocols	57
	Elements of a Router	59
2.5	Congestion Control	60
	Effects of Congestion	60
	Congestion Control Techniques	64

2.6	SDN and NFV	67
	Software-Defined Networking	67
	Network Functions Virtualization	69
2.7	Modern Networking Elements	71
2.8	Key Terms	72
2.9	References	73
PART II SOFTWARE DEFINED NETWORKS		75
Chapter 3: SDN: Background and Motivation		76
3.1	Evolving Network Requirements	77
	Demand Is Increasing	77
	Supply Is Increasing	77
	Traffic Patterns Are More Complex	78
	Traditional Network Architectures are Inadequate	79
3.2	The SDN Approach	80
	Requirements	80
	SDN Architecture	81
	Characteristics of Software-Defined Networking	85
3.3	SDN- and NFV-Related Standards	85
	Standards-Developing Organizations	87
	Industry Consortia	89
	Open Development Initiatives	89
3.4	Key Terms	91
3.5	References	91
Chapter 4: SDN Data Plane and OpenFlow		92
4.1	SDN Data Plane	93
	Data Plane Functions	93
	Data Plane Protocols	95

4.2	OpenFlow Logical Network Device	95
	Flow Table Structure	98
	Flow Table Pipeline	102
	The Use of Multiple Tables	106
	Group Table	107
4.3	OpenFlow Protocol	109
4.4	Key Terms	111
Chapter 5: SDN Control Plane		112
5.1	SDN Control Plane Architecture	113
	Control Plane Functions	113
	Southbound Interface	116
	Northbound Interface	117
	Routing	119
5.2	ITU-T Model	120
5.3	OpenDaylight	122
	OpenDaylight Architecture	122
	OpenDaylight Helium	124
5.4	REST	128
	REST Constraints	128
	Example REST API	130
5.5	Cooperation and Coordination Among Controllers	133
	Centralized Versus Distributed Controllers	133
	High-Availability Clusters	134
	Federated SDN Networks	135
	Border Gateway Protocol	136
	Routing and QoS Between Domains	137
	Using BGP for QoS Management	138
	IETF SDNi	140
	OpenDaylight SNDi	141

5.6	Key Terms	143
5.7	References	143
Chapter 6: SDN Application Plane		144
6.1	SDN Application Plane Architecture	145
	Northbound Interface	146
	Network Services Abstraction Layer	146
	Network Applications	147
	User Interface	147
6.2	Network Services Abstraction Layer	147
	Abstractions in SDN	147
	Frenetic	150
6.3	Traffic Engineering	153
	PolicyCop	153
6.4	Measurement and Monitoring	157
6.5	Security	157
	OpenDaylight DDoS Application	157
6.6	Data Center Networking	162
	Big Data over SDN	163
	Cloud Networking over SDN	164
6.7	Mobility and Wireless	168
6.8	Information-Centric Networking	168
	CCNx	169
	Use of an Abstraction Layer	170
6.9	Key Terms	173
PART III VIRTUALIATION		175
Chapter 7: Network Functions Virtualization: Concepts and Architecture		176
7.1	Background and Motivation for NFV	177
7.2	Virtual Machines	178
	The Virtual Machine Monitor	179

Architectural Approaches	180
Container Virtualization	183
7.3 NFV Concepts	184
Simple Example of the Use of NFV	188
NFV Principles	189
High-Level NFV Framework	190
7.4 NFV Benefits and Requirements	191
NFV Benefits	191
NFV Requirements	192
7.5 NFV Reference Architecture	193
NFV Management and Orchestration	194
Reference Points	195
Implementation	196
7.6 Key Terms	197
7.7 References	197
Chapter 8: NFV Functionality	198
8.1 NFV Infrastructure	199
Container Interface	199
Deployment of NFVI Containers	203
Logical Structure of NFVI Domains	204
Compute Domain	205
Hypervisor Domain	208
Infrastructure Network Domain	209
8.2 Virtualized Network Functions	213
VNF Interfaces	213
VNFC to VNFC Communication	215
VNF Scaling	216
8.3 NFV Management and Orchestration	217
Virtualized Infrastructure Manager	217

Virtual Network Function Manager	218
NFV Orchestrator	219
Repositories	219
Element Management	220
OSS/BSS	220
8.4 NFV Use Cases	221
Architectural Use Cases	222
Service-Oriented Use Cases	223
8.5 SDN and NFV	225
8.6 Key Terms	228
8.7 References	229
Chapter 9: Network Virtualization	230
9.1 Virtual LANs	231
The Use of Virtual LANs	234
Defining VLANs	235
Communicating VLAN Membership	236
IEEE 802.1Q VLAN Standard	237
Nested VLANs	239
9.2 OpenFlow VLAN Support	240
9.3 Virtual Private Networks	241
IPsec VPNs	241
MPLS VPNs	243
9.4 Network Virtualization	247
A Simplified Example	248
Network Virtualization Architecture	250
Benefits of Network Virtualization	252
9.5 OpenDaylight’s Virtual Tenant Network	253
9.6 Software-Defined Infrastructure	257
Software-Defined Storage	259

SDI Architecture	261
9.7 Key Terms	263
9.8 References	263
PART IV DEFINING AND SUPPORTING USER NEEDS	265
Chapter 10: Quality of Service	266
10.1 Background	267
10.2 QoS Architectural Framework	268
Data Plane	269
Control Plane	271
Management Plane	272
10.3 Integrated Services Architecture	273
ISA Approach	273
ISA Components	274
ISA Services	276
Queuing Discipline	277
10.4 Differentiated Services	279
Services	281
DiffServ Field	282
DiffServ Configuration and Operation	284
Per-Hop Behavior	286
Default Forwarding PHB	287
10.5 Service Level Agreements	291
10.6 IP Performance Metrics	293
10.7 OpenFlow QoS Support	296
Queue Structures	296
Meters	297
10.8 Key Terms	299
10.9 References	299

Chapter 11: QoE: User Quality of Experience	300
11.1 Why QoE?	301
Online Video Content Delivery	302
11.2 Service Failures Due to Inadequate QoE Considerations	304
11.3 QoE-Related Standardization Projects	304
11.4 Definition of Quality of Experience.	305
Definition of Quality	306
Definition of Experience	306
Quality Formation Process	307
Definition of Quality of Experience.	308
11.5 QoE Strategies in Practice	308
The QoE/QoS Layered Model	308
Summarizing and Merging the QoE/QoS Layers	310
11.6 Factors Influencing QoE	311
11.7 Measurements of QoE	312
Subjective Assessment.	312
Objective Assessment	314
End-User Device Analytics	315
Summarizing the QoE Measurement Methods.	316
11.8 Applications of QoE	317
11.9 Key Terms	319
11.10 References.	320
Chapter 12: Network Design Implications of QoS and QoE	322
12.1 Classification of QoE/QoS Mapping Models	323
Black-Box Media-Based QoS/QoE Mapping Models	323
Glass-Box Parameter-Based QoS/QoE Mapping Models.	325
Gray-Box QoS/QoE Mapping Models	326
Tips for QoS/QoE Mapping Model Selection	327

12.2	IP-Oriented Parameter-Based QoS/QoE Mapping Models	327
	Network Layer QoE/QoS Mapping Models for Video Services	328
	Application Layer QoE/QoS Mapping Models for Video Services	328
12.3	Actionable QoE over IP-Based Networks	330
	The System-Oriented Actionable QoE Solution	330
	The Service-Oriented Actionable QoE Solution	331
12.4	QoE Versus QoS Service Monitoring	332
	QoS Monitoring Solutions	334
	QoE Monitoring Solutions	335
12.5	QoE-Based Network and Service Management	341
	QoE-Based Management of VoIP Calls	341
	QoE-Based Host-Centric Vertical Handover	341
	QoE-Based Network-Centric Vertical Handover	342
12.6	Key Terms	344
12.7	References	344

PART V MODERN NETWORK ARCHITECTURE: CLOUDS AND FOG 347

Chapter 13: Cloud Computing 348

13.1	Basic Concepts	349
13.2	Cloud Services	351
	Software as a Service	352
	Platform as a Service	353
	Infrastructure as a Service	354
	Other Cloud Services	355
	XaaS	357
13.3	Cloud Deployment Models	358
	Public Cloud	359
	Private Cloud	359
	Community Cloud	360
	Hybrid Cloud	360

13.4	Cloud Architecture	361
	NIST Cloud Computing Reference Architecture	361
	ITU-T Cloud Computing Reference Architecture	365
13.5	SDN and NFV	368
	Service Provider Perspective	369
	Private Cloud Perspective	369
	ITU-T Cloud Computing Functional Reference Architecture	369
13.6	Key Terms	371
Chapter 14: The Internet of Things: Components		372
14.1	The IoT Era Begins	373
14.2	The Scope of the Internet of Things	374
14.3	Components of IoT-Enabled Things	377
	Sensors	377
	Actuators	380
	Microcontrollers	381
	Transceivers	386
	RFID	387
14.4	Key Terms	393
14.5	References	393
Chapter 15: The Internet of Things: Architecture and Implementation		394
15.1	IoT Architecture	395
	ITU-T IoT Reference Model	395
	IoT World Forum Reference Model	401
15.2	IoT Implementation	409
	IoTivity	409
	Cisco IoT System	420
	ioBridge	427
15.3	Key Terms	431
15.4	References	431

PART VI RELATED TOPICS	433
Chapter 16: Security	434
16.1 Security Requirements	435
16.2 SDN Security	436
Threats to SDN	436
Software-Defined Security	440
16.3 NFV Security	441
Attack Surfaces	441
ETSI Security Perspective	444
Security Techniques	446
16.4 Cloud Security	446
Security Issues and Concerns	449
Cloud Security Risks and Countermeasures	450
Data Protection in the Cloud	452
Cloud Security as a Service	453
Addressing Cloud Computer Security Concerns	456
16.5 IoT Security	458
The Patching Vulnerability	459
IoT Security and Privacy Requirements Defined by ITU-T	459
An IoT Security Framework	462
Conclusion	465
16.6 Key Terms	465
16.7 References	465
Chapter 17: The Impact of the New Networking on IT Careers	466
17.1 The Changing Role of Network Professionals	467
Changing Responsibilities	467
Impact on Job Positions	469
Bottom Line	470

17.2	DevOps	470
	DevOps Fundamentals	471
	The Demand for DevOps	475
	DevOps for Networking	476
	DevOps Network Offerings	478
	Cisco DevNet	479
	Conclusion on the Current State of DevOps	479
17.3	Training and Certification	480
	Certification Programs	480
	IT Skills	488
17.4	Online Resources	489
17.5	References	491
	Appendix A: References	492
	Glossary	498
	Index	510

About the Author

Dr. William Stallings has made a unique contribution to understanding the broad sweep of technical developments in computer security, computer networking, and computer architecture. He has authored 18 textbooks, and, counting revised editions, a total of 70 books on various aspects of these subjects. His writings have appeared in numerous ACM and IEEE publications, including the *Proceedings of the IEEE* and *ACM Computing Reviews*. He has 13 times received the award for the best computer science textbook of the year from the Text and Academic Authors Association.



In over 30 years in the field, he has been a technical contributor, technical manager, and an executive with several high-technology firms. He has designed and implemented both TCP/IP-based and OSI-based protocol suites on a variety of computers and operating systems, ranging from microcomputers to mainframes. Currently, he is an independent consultant whose clients have included computer and networking manufacturers and customers, software development firms, and leading-edge government research institutions.

He created and maintains the Computer Science Student Resource Site at ComputerScienceStudent.com/. This site provides documents and links on a variety of subjects of general interest to computer science students (and professionals). He is a member of the editorial board of *Cryptologia*, a scholarly journal devoted to all aspects of cryptology.

Dr. Stallings holds a Ph.D. from M.I.T. in Computer Science and a B.S. from Notre Dame in electrical engineering.

About the Contributing Authors

Florence Agboma currently works as a Technology Analyst at British Sky Broadcasting (BSkyB), London. Her work includes streaming video quality improvements for different video platforms such as linear OTT, VoD, and broadcast. She is a member of the Video Quality Experts Group (VQEG). Dr. Agboma holds a Ph.D. from the University of Essex, United Kingdom, and her research focused on quality of experience for mobile content delivery systems.



Dr. Agboma has published a number of peer-reviewed articles in journal papers, book chapters, and international conference proceedings. Her interests include video quality assessments, psychophysical methods, pay TV analytics, quality of experience management, and emerging broadcast TV technologies such as high dynamic range and ultra HD.

Sofiene Jelassi received a Bachelor of Science and a Master of Science from the University of Monastir, Tunisia, in June 2003 and December 2005, respectively. He obtained a Ph.D. in Computer Science from the University of Pierre and Marie Curie, Paris, France, in February 2010. His doctoral thesis was titled *Adaptive Quality Control of Packetized Voice Conversations over Mobile Ad-Hoc Networks*. From June 2010 to December 2013, he worked as an R&D engineer at Inria within DIONYSOS research group. From January to December 2014, he worked as a post-doctoral fellow at GTA/UFRJ in Rio de Janeiro, Brazil. Since January 2015, he has been working as Assistant Professor at University of Monastir, Tunisia.

His research includes wired and wireless software-defined networks (SDNs), server and network virtualization, network monitoring, content-oriented management of mobile networks and services, mobile virtual network operators (MVNO), customized voice and video systems, quality of user experience (QoE) measurement and modeling, in-lab and in-field usability testing, crowdsourcing, user profiling, context sensing, service gamification, and social-driven emergency services. Dr. Jelassi has more than 20 papers published in international journals and conferences.



Dedication

To Tricia, my loving wife, the kindest and gentlest person.

Acknowledgments

This book has benefited from review by a number of people who gave generously of their time and expertise. I especially thank Wendell Odom (Certskills, LLC) and Tim Szigeti (Cisco Systems), who each devoted an enormous amount of time to a detailed review of the entire manuscript.

Thanks also to the many people who provided detailed technical reviews of one or more chapters: Christian Adell (Corporació Catalana de Mitjans Audiovisuals), Eduard Dulharu (AT&T Germany), Cemal Duman (Ericsson), David L. Foote (NFV Forum (ATIS)), Harold Fritts, Scott Hogg (Global Technology Resources), Justin Kang (Accenture), Sergey Katsev (Fortinet), Raymond Kelly (Telecoms Now Ltd), Faisal Khan (Mobily Saudi Arabia), Epameinondas Kontothanasis (Unifys), Sashi Kumar (Intel), Hongwei Li (Hewlett-Packard), Cynthia Lopes (Maya Technologies), Simone Mangiante (EMC), Roberto Fuentes Martinez (Tecnocom), Mali Naghavi (Ericsson), Fatih Eyup Nar (Ericsson USA), Jimmy Ng (Huawei Technologies), Mark Noble (Salix Technology Services), Luke Reid (Sytyel Reply UK), David Schuckman (State Farm Insurance), Vivek Srivastava (Zscaler), Istvan Teglas (Cisco Systems), and Paul Zanna (Northbound Networks).

Finally, I want to thank the many people at Pearson responsible for the publication of the book. This includes the staff at Pearson, particularly Senior Development Editor Chris Cleveland; Executive Editor Brett Bartow, and his assistant Vanessa Evans; and Project Editor Mandie Frank. Thanks also to the marketing and sales staffs at Pearson, without whose efforts this book would not be in front of you.

With all this assistance, little remains for which I can take full credit. However, I am proud to say that, with no help whatsoever, I selected all the quotations.

Preface

There is the book, Inspector. I leave it with you, and you cannot doubt that it contains a full explanation.

—*The Adventure of the Lion's Mane*, Sir Arthur Conan Doyle

Background

A host of factors have converged to produce the latest revolution in computer and communications networking:

- **Demand:** Enterprises are faced with a surge of demands that focus their attention on the need to design, evaluate, manage, and maintain sophisticated network infrastructures. These trends include the following:
 - **Big data:** Enterprises large and small increasingly rely on processing and analyzing massive amounts of data. To process large quantities of data within tolerable time periods, big data may need distributed file systems, distributed databases, cloud computing platforms, Internet storage, and other scalable storage technologies.
 - **Cloud computing:** There is an increasingly prominent trend in many organizations to move a substantial portion or even all information technology (IT) operations to an Internet-connected infrastructure known as enterprise cloud computing. This drastic shift in IT data processing is accompanied by an equally drastic shift in networking requirements.
 - **Internet of Things (IoT):** The IoT involves large numbers of objects that use standard communications architectures to provide services to end users. Billions of such devices will be interconnected in industrial, business, and government networks, providing new interactions between the physical world and computing, digital content, analysis, applications, and services. IoT provides unprecedented opportunities for users, manufacturers, and service providers in a wide variety of sectors. Areas that will benefit from IoT data collection, analysis, and automation capabilities include health and fitness, healthcare, home monitoring and automation, energy savings and smart grid, farming, transportation, environmental monitoring, inventory and product management, security, surveillance, education, and many others.
 - **Mobile devices:** Mobile devices are now an indispensable part of every enterprise IT infrastructure, including employer supplied and bring your own device (BYOD). The large population of mobile devices generates unique new demands on network planning and management.
- **Capacity:** Two interlocking trends have generated new and urgent requirements for intelligent and efficient network design and management:

- **Gigabit data rate networks:** Ethernet offerings have reached 100 Gbps with further increases in the works. Wi-Fi products at almost 7 Gbps are available. And 4G and 5G networks bring gigabit speeds to cellular networks.
- **High-speed, high-capacity servers:** Massive blade servers and other high-performance servers have evolved to meet the increasing multimedia and data processing requirements of enterprises, calling for a need for efficiently designed and managed networks.
- **Complexity:** Network designers and managers operate in a complex, dynamic environment, in which a range of requirements, most especially quality of service (QoS) and quality of experience (QoE) require flexible, manageable networking hardware and services.
- **Security:** With increasing reliance on networked resources, an increasing need emerges for networks that provide a range of security services.

With the development of new network technologies in response to these factors, it is imperative for system engineers, system analysts, IT managers, network designers, and product marketing specialists to have a firm grasp on modern networking. These professionals need to understand the implications of the factors listed above and how network designers have responded. Dominating this landscape are (1) two complementary technologies that are rapidly being developed and deployed (software-defined networking [SDN] and network functions virtualization [NFV]) and (2) the need to satisfy QoS and QoE requirements.

This book provides the reader with a thorough understanding of SDN and NFV and their practical deployment and use in today's enterprises. In addition, the book provides clear explanations of QoS/QoE and the whole range of related issues, such as cloud networking and IoT. This is a technical book, intended for readers with some technical background, but is sufficiently self-contained to be a valuable resource for IT managers and product marketing personnel, in addition to system engineers, network maintenance personnel, and network and protocol designers.

Organization of the Book

The book consists of six parts:

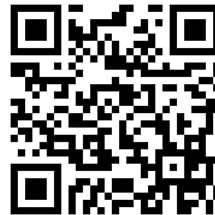
- **Modern Networking:** Provides an overview of modern networking and a context for the remainder of the book. Chapter 1 is a survey of the elements that make up the networking ecosystem, including network technologies, network architecture, services, and applications. Chapter 2 examines the requirements that have evolved for the current networking environment and provides a preview of key technologies for modern networking.
- **Software-Defined Networks:** Devoted to a broad and thorough presentation of SDN concepts, technology, and applications. Chapter 3 begins the discussion by laying out what the SDN approach is and why it is needed, and provides an overview of the SDN architecture. This chapter also looks at the organizations that are issuing specifications and standards for SDN. Chapter 4 is a detailed look at the SDN data plane, including the key components, how they

interact, and how they are managed. Much of the chapter is devoted to OpenFlow, a vital data plane technology and an interface to the control plane. The chapter explains why OpenFlow is needed and then proceeds to provide a detailed technical explanation. Chapter 5 is devoted to the SDN control plane. It includes a discussion of OpenDaylight, an important open source implementation of the control plane. Chapter 6 covers the SDN application plane. In addition to examining the general SDN application plane architecture, the chapter discusses six major application areas that can be supported by SDN and provides a number of examples of SDN applications.

- **Virtualization:** Devoted to a broad and thorough presentation of network functions virtualization (NFV) concepts, technology, and applications, as well as a discussion of network virtualization. Chapter 7 introduces the concept of virtual machine, and then looks at the use of virtual machine technology to develop NFV-based networking environments. Chapter 8 provides a detailed discussion of NFV functionality. Chapter 9 looks at traditional concepts of virtual networks, then at the more modern approach to network virtualization, and finally introduces the concept of software defined infrastructure.
- **Defining and Supporting User Needs:** Equally as significant as the emergence of the SDN and NFV is the evolution of quality of service (QoS) and quality of experience (QoE) to determine customer needs and network design responses to those needs. Chapter 10 provides an overview of QoS concepts and standards. Recently QoS has been augmented with the concept of QoE, which is particularly relevant to interactive video and multimedia network traffic. Chapter 11 provides an overview of QoE and discusses a number of practical aspects of implementing QoE mechanisms. Chapter 12 looks further into the network design implications of the combined use of QoS and QoE.
- **Modern Network Architecture: Clouds and Fog:** The two dominant modern network architectures are cloud computing and the Internet of things (IoT), sometimes referred to as fog computing. The technologies and applications discussed in the preceding parts all provide a foundation for cloud computing and IoT. Chapter 13 is a survey of cloud computing. The chapter begins with a definition of basic concepts, and then covers cloud services, deployment models, and architecture. The chapter then discusses the relationship between cloud computing and SDN and NFV. Chapter 14 introduces IoT and provides a detailed look at the key components of IoT-enabled devices. Chapter 15 looks at several model IoT architectures and then describes three example IoT implementations.
- **Related Topics:** Discusses two additional topics that, although important, do not conveniently fit into the other Parts. Chapter 16 provides an analysis of security issues that have emerged with the evolution of modern networking. Separate sections deal with SDN, NFV, cloud, and IoT security, respectively. Chapter 17 discusses career-related issues, including the changing role of various network-related jobs, new skill requirements, and how the reader can continue his or her education to prepare for a career in modern networking.

Supporting Websites

I maintain a companion website at WilliamStallings.com/Network that includes a list of relevant links organized by chapter and an errata sheet for the book.



Companion website

I also maintain the Computer Science Student Resource Site, at ComputerScienceStudent.com. The purpose of this site is to provide documents, information, and links for computer science students and professionals. Links and documents are organized into seven categories:



Computer Science
Student Resource
Site

- **Math:** Includes a basic math refresher, a queuing analysis primer, a number system primer, and links to numerous math sites.
- **How-to:** Advice and guidance for solving homework problems, writing technical reports, and preparing technical presentations.
- **Research resources:** Links to important collections of papers, technical reports, and bibliographies.
- **Other useful:** A variety of other useful documents and links.
- **Computer science careers:** Useful links and documents for those considering a career in computer science.
- **Writing help:** Help in becoming a clearer, more effective writer.
- **Miscellaneous topics and humor:** You have to take your mind off your work once in a while.

This page intentionally left blank

Chapter 3

SDN: Background and Motivation

The requirements for a future all-digital-data distributed network which provides common user service for a wide range of users having different requirements is considered. The use of a standard format message block permits building relatively simple switching mechanisms using an adaptive store-and-forward routing policy to handle all forms of digital data including “real-time” voice. This network rapidly responds to changes in network status.

—On Distributed Communications: Introduction to Distributed Communications Networks, Rand Report RM-3420-PR, Paul Baran, August 1964

Chapter Objectives

After studying this chapter, you should be able to

- Make a presentation justifying the position that traditional network architectures are inadequate for modern networking needs.
- List and explain the key requirements for an SDN architecture.
- Present an overview of an SDN architecture, to include explaining the significance of northbound and southbound APIs.
- Summarize the work being done on SDN and NFV standardization by various organizations.

This chapter begins the discussion of software-defined networks (SDNs) by providing some background and motivation for the SDN approach.

3.1 Evolving Network Requirements

A number of trends are driving network providers and users to reevaluate traditional approaches to network architecture. These trends can be grouped under the categories of demand, supply, and traffic patterns.

Demand Is Increasing

As was described in Chapter 2, “Requirements and Technology,” a number of trends are increasing the load on enterprise networks, the Internet, and other internets. Of particular note are the following:

- **Cloud computing:** There has been a dramatic shift by enterprises to both public and private cloud services.
- **Big data:** The processing of huge data sets requires massive parallel processing on thousands of servers, all of which require a degree of inter-connection to each other. Therefore, there is a large and constantly growing demand for network capacity within the data center.
- **Mobile traffic:** Employees are increasingly accessing enterprise network resources via mobile personal devices, such as smartphones, tablets, and notebooks. These devices support sophisticated apps that can consume and generate image and video traffic, placing new burdens on the enterprise network.
- **The Internet of Things (IoT):** Most “things” in the IoT generate modest traffic, although there are exceptions, such as surveillance video cameras. But the sheer number of such devices for some enterprises results in a significant load on the enterprise network.

Supply Is Increasing

As the demand on networks is rising, so is the capacity of network technologies to absorb rising loads. In terms of transmission technology, Chapter 1, “Elements of Modern Networking,” established that the key enterprise wired and wireless network technologies, Ethernet and Wi-Fi respectively, are well into the gigabits per second (Gbps) range. Similarly, 4G and 5G cellular networks provide greater capacity for mobile devices from remote employees who access the enterprise network via cellular networks rather than Wi-Fi.

The increase in the capacity of the network transmission technologies has been matched by an increase in the performance of network devices, such as LAN switches, routers, firewalls, intrusion detection system/intrusion prevention systems (IDS/IPS),

and network monitoring and management systems. Year by year, these devices have larger, faster memories, enabling greater buffer capacity and faster buffer access, as well as faster processor speeds.

Traffic Patterns Are More Complex

If it were simply a matter of supply and demand, it would appear that today's networks should be able to cope with today's data traffic. But as traffic patterns have changed and become more complex, traditional enterprise network architectures are increasingly ill suited to the demand.

Until recently, and still common today, the typical enterprise network architecture consisted of a local or campus-wide tree structure of Ethernet switches with routers connecting large Ethernet LANs and connecting to the Internet and WAN facilities. This architecture is well suited to the client/server computing model that was at one time dominant in the enterprise environment. With this model, interaction, and therefore traffic, was mostly between one client and one server. In such an environment, networks could be laid out and configured with relatively static client and server locations and relatively predictable traffic volumes between clients and servers.

A number of developments have resulted in far more dynamic and complex traffic patterns within the enterprise data center, local and regional enterprise networks, and carrier networks. These include the following:

- Client/server applications typically access multiple databases and servers that must communicate with each other, generating “horizontal” traffic between servers as well as “vertical” traffic between servers and clients.
- Network convergence of voice, data, and video traffic creates unpredictable traffic patterns, often of large multimedia data transfers.
- Unified communications (UC) strategies involve heavy use of applications that trigger access to multiple servers.
- The heavy use of mobile devices, including personal bring your own device (BYOD) policies, results in user access to corporate content and applications from any device anywhere any time. As illustrated previously in Figure 2.6 in Chapter 2, this mobile traffic is becoming an increasingly significant fraction of enterprise network traffic.
- The widespread use of public clouds has shifted a significant amount of what previously had been local traffic onto WANs for many enterprises, resulting in increased and often very unpredictable loads on enterprise routers.
- The now-common practice of application and database server virtualization has significantly increased the number of hosts requiring high-volume network access and results in every-changing physical location of server resources.

Traditional Network Architectures are Inadequate

Even with the greater capacity of transmission schemes and the greater performance of network devices, traditional network architectures are increasingly inadequate in the face of the growing complexity, variability, and high volume of the imposed load. In addition, as quality of service (QoS) and quality of experience (QoE) requirements imposed on the network are expanded as a result of the variety of applications, the traffic load must be handled in an increasingly sophisticated and agile fashion.

The traditional internetworking approach is based on the **TCP/IP protocol architecture**. Three noteworthy characteristics of this approach are as follows:

- Two-level end system addressing
- Routing based on destination
- Distributed, autonomous control

Let's look at each of these characteristics in turn.

The traditional architecture relies heavily on the network interface identity. At the physical layer of the TCP/IP model, devices attached to networks are identified by hardware-based identifiers, such as Ethernet MAC addresses. At the internetworking level, including both the Internet and private internets, the architecture is a network of networks. Each attached device has a physical layer identifier recognized within its immediate network and a logical network identifier, its IP address, which provides global visibility.

The design of TCP/IP uses this addressing scheme to support the networking of autonomous networks, with distributed control. This architecture provides a high level of resilience and scales well in terms of adding new networks. Using IP and distributed routing protocols, routes can be discovered and used throughout an internet. Using transport-level protocols such as TCP, distributed and decentralized algorithms can be implemented to respond to congestion.

Traditionally, routing was based on each packet's destination address. In this **datagram** approach, successive packets between a source and destination may follow different routes through the internet, as routers constantly seek to find the minimum-delay path for each individual **packet**. More recently, to satisfy QoS requirements, packets are often treated in terms of **flows** of packets. Packets associated with a given flow have defined QoS characteristics, which affect the routing for the entire flow.

However, this distributed, autonomous approach developed when networks were predominantly static and end systems predominantly of fixed location. Based on these characteristics, the Open Networking Foundation (ONF) cites four general limitations of traditional network architectures [ONF12]:

TCP/IP protocol architecture

The protocol architecture built around the TCP and IP protocols, consisting of five layers: physical, data link, network/Internet (usually IP), transport (usually TCP or UDP), and application.

packet

A unit of data sent across a network. A packet is a group of bits that includes data plus protocol control information. The term generally applies to protocol data units at the network layer.

packet switching

A method of transmitting messages through a communications network, in which long messages are subdivided into short packets. Each packet is passed from source to destination through intermediate nodes. At each node, the entire message is received, stored briefly, and then forwarded to the next node.

Datagram

A packet that is treated independently of other packets for packet switching. A datagram carries information sufficient for routing from the source to the destination without the necessity of establishing a logical connection between the endpoints.

flow

A sequence of packets between a source and destination that are recognized by the network as related and are treated in a uniform fashion.

- **Static, complex architecture:** To respond for demands such as differing levels of QoS, high and fluctuating traffic volumes, and security requirements, networking technology has grown more complex and difficult to manage. This has resulted in a number of independently defined protocols each of which addresses a portion of networking requirements. An example of the difficulty this presents is when devices are added or moved. The network management staff must use device-level management tools to make changes to configuration parameters in multiple switches, routers, firewalls, web authentication portals, and so on. The updates include changes to access control lists (ACLs), virtual LAN settings, QoS settings in numerous devices, and other protocol-related adjustments. Another example is the adjustment of QoS parameters to meet changing user requirements and traffic patterns. Manual procedures must be used to configure each vendor's equipment on a per-application and even per-session basis.
- **Inconsistent policies:** To implement a network-wide security policy, staff may have to make configuration changes to thousands of devices and mechanisms. In a large network, when a new virtual machine is activated, it can take hours or even days to reconfigure ACLs across the entire network.
- **Inability to scale:** Demands on networks are growing rapidly, both in volume and variety. Adding more switches and transmission capacity, involving multiple vendor equipment, is difficult because of the complex, static nature of the network. One strategy enterprises have used is to oversubscribe network links based on predicted traffic patterns. But with the increased use of virtualization and the increasing variety of multimedia applications, traffic patterns are unpredictable.
- **Vendor dependence:** Given the nature of today's traffic demands on networks, enterprises and carriers need to deploy new capabilities and services rapidly in response to changing business needs and user demands. A lack of open interfaces for network functions leaves the enterprises limited by the relatively slow product cycles of vendor equipment.

3.2 The SDN Approach

This section provides an overview of SDN and shows how it is designed to meet evolving network requirements.

Requirements

Based on the narrative of Section 3.1, we are now in a position to detail the principal requirements for a modern networking approach. The Open Data Center Alliance (ODCA) provides a useful, concise list of requirements, which include the following [ODCA14]:

- **Adaptability:** Networks must adjust and respond dynamically, based on application needs, business policy, and network conditions.
- **Automation:** Policy changes must be automatically propagated so that manual work and errors can be reduced.
- **Maintainability.** Introduction of new features and capabilities (software upgrades, patches) must be seamless with minimal disruption of operations.
- **Model management:** Network management software must allow management of the network at a model level, rather than implementing conceptual changes by reconfiguring individual network elements.
- **Mobility:** Control functionality must accommodate mobility, including mobile user devices and virtual servers.
- **Integrated security:** Network applications must integrate seamless security as a core service instead of as an add-on solution.
- **On-demand scaling:** Implementations must have the ability to scale up or scale down the network and its services to support on-demand requests.

SDN Architecture

An analogy can be drawn between the way in which computing evolved from closed, vertically integrated, proprietary systems into an open approach to computing and the evolution coming with SDN (see Figure 3.1). In the early decades of computing, vendors such as IBM and DEC provided a fully integrated product, with a proprietary processor hardware, unique assembly language, unique operating system (OS), and the bulk if not all of the application software. In this environment, customers, especially large customers, tended to be locked in to one vendor, dependent primarily on the applications offered by that vendor. Migration to another vendor's hardware platform resulted in major upheaval at the application level.

Today, the computing environment is characterized by extreme openness and great customer flexibility. The bulk of computing hardware consists of x86 and x86-compatible processors for standalone systems and ARM processors for embedded systems. This makes it easy to port operating systems implemented in C, C++, Java, and the like. Even proprietary hardware architectures, such as IBM's zEnterprise line, provide standardized compilers and programming environments and so can easily run open sources operating systems such as Linux. Therefore, applications written for Linux or other open operating systems can easily be moved from one vendor platform to another. Even proprietary systems such as Windows and Mac OS provide programming environments to make porting of applications an easy matter. It also enables the development of virtual machines that can be moved from one server to another across hardware platforms and operating systems.

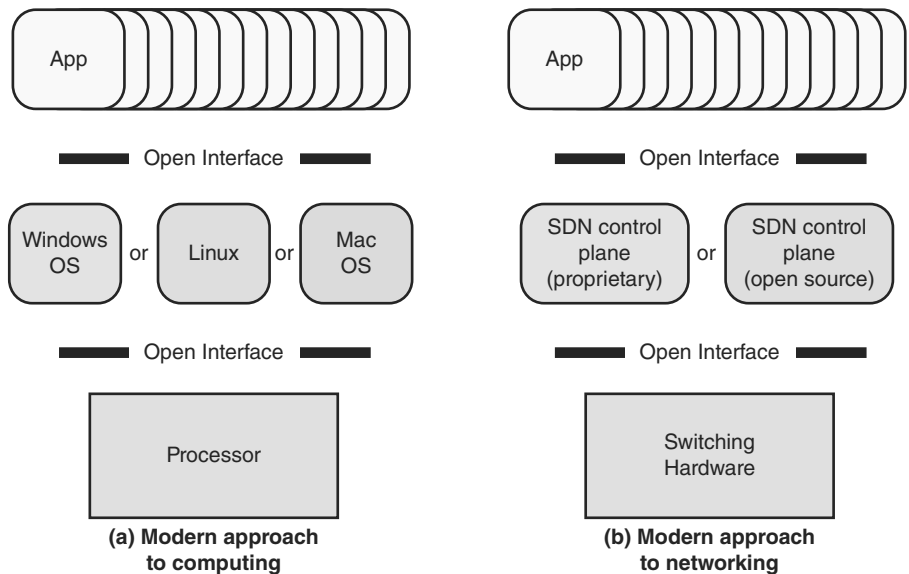


FIGURE 3.1 The Modern Approach to Computing and Networking

The networking environment today faces some of the same limitations faced in the pre-open era of computing. Here the issue is not developing applications that can run on multiple platforms. Rather, the difficulty is the lack of integration between applications and network infrastructure. As demonstrated in the preceding section, traditional network architectures are inadequate to meet the demands of the growing volume and variety of traffic.

The central concept behind SDN is to enable developers and network managers to have the same type of control over network equipment that they have had over x86 servers. As discussed in Section 2.6 in Chapter 2, the SDN approach splits the switching function between a data plane and a control plane that are on separate devices (see Figure 3.2). The data plane is simply responsible for forwarding packets, whereas the control plane provides the “intelligence” in designing routes, setting priority and routing policy parameters to meet QoS and QoE requirements and to cope with the shifting traffic patterns. Open interfaces are defined so that the switching hardware presents a uniform interface regardless of the details of internal implementation. Similarly, open interfaces are defined to enable networking applications to communicate with the SDN controllers.

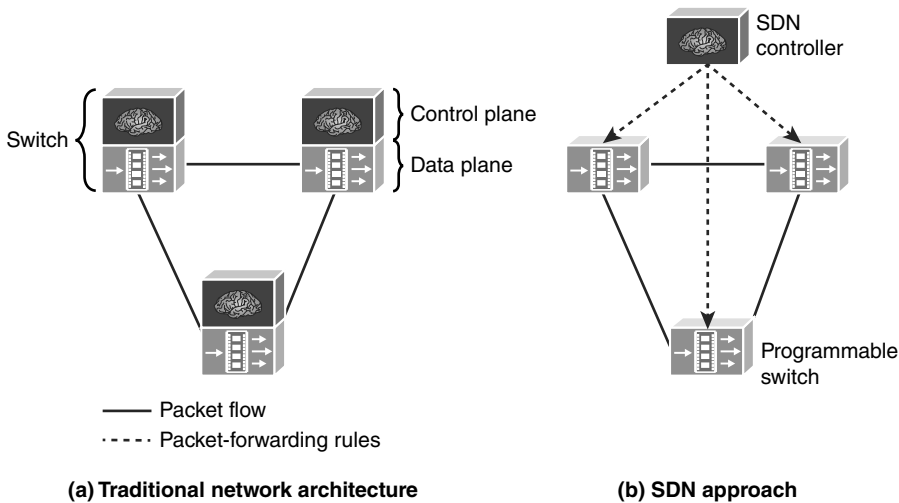


FIGURE 3.2 Control and Data Planes

Figure 3.3 elaborates on the structure shown in Figure 2.15, showing more detail of the SDN approach. The data plane consists of physical switches and virtual switches. In both cases, the switches are responsible for forwarding packets. The internal implementation of buffers, priority parameters, and other data structures related to forwarding can be vendor dependent. However, each switch must implement a model, or abstraction, of packet forwarding that is uniform and open to the SDN controllers. This model is defined in terms of an open **application programming interface (API)** between the control plane and the data plane (southbound API). The most prominent example of such an open API is OpenFlow, discussed in Chapter 4, “SDN Data Plane and OpenFlow.” As Chapter 4 explains, the OpenFlow specification defines both a protocol between the control and data planes and an API by which the control plane can invoke the OpenFlow protocol.

← See Figure 2.15, *Software Defined Networking*

application programming interface (API)

A language and message format used by an application program to communicate with the operating system or some other control program such as a database management system (DBMS) or communications protocol. APIs are implemented by writing function calls in the program, which provide the linkage to the required subroutine for execution. An open or standardized API can ensure the portability of the application code and the vendor independence of the called service.

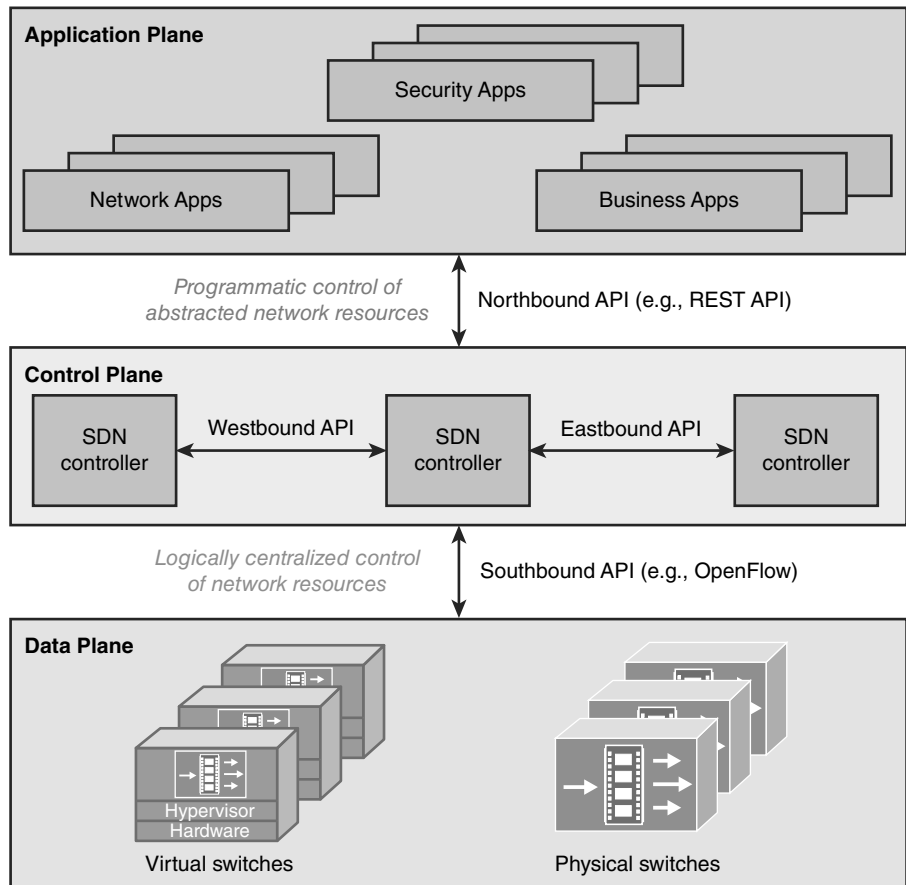


FIGURE 3.3 Software-Defined Architecture

→ See Chapter 5, “SDN Control Plane”

SDN controllers can be implemented directly on a server or on a virtual server. OpenFlow or some other open API is used to control the switches in the data plane. In addition, controllers use information about capacity and demand obtained from the networking equipment through which the traffic flows. SDN controllers also expose northbound APIs, which allow developers and network managers to deploy a wide range of off-the-shelf and custom-built network applications, many of which were not feasible before the advent of SDN. As yet there is no standardized northbound API nor a consensus on an open northbound API. A number of vendors offer a Representational State Transfer (REST)-based API to provide a programmable interface to their SDN controller.

Also envisioned but not yet defined are horizontal APIs (east/westbound), which would enable communication and cooperation among groups or federations of controllers to synchronize state for high availability.

At the application plane are a variety of applications that interact with SDN controllers. SDN applications are programs that may use an abstract view of the network for their decision-making goals. These applications convey their network requirements and desired network behavior to the SDN controller via a northbound API. Examples of applications are energy-efficient networking, security monitoring, access control, and network management.

Characteristics of Software-Defined Networking

Putting it all together, the key characteristics of SDN are as follows:

- The control plane is separated from the data plane. Data plane devices become simple packet-forwarding devices (refer back to Figure 3.2).
- The control plane is implemented in a centralized controller or set of coordinated centralized controllers. The SDN controller has a centralized view of the network or networks under its control. The controller is portable software that can run on commodity servers and is capable of programming the forwarding devices based on a centralized view of the network.
- Open interfaces are defined between the devices in the control plane (controllers) and those in the data plane.
- The network is programmable by applications running on top of the SDN controllers. The SDN controllers present an abstract view of network resources to the applications.

standards

Documents that provide requirements, specifications, guidelines, or characteristics that can be used consistently to ensure that materials, products, processes, and services are fit for their purpose. Standards are established by consensus among those participating in a standards-making organization and are approved by a generally recognized body.

3.3 SDN- and NFV-Related Standards

Unlike some technology areas, such as Wi-Fi, there is no single standards body responsible for developing open **standards** for SDN and NFV. Rather, there is a large and evolving collection of standards-developing organizations (SDOs), industrial consortia, and open development initiatives involved in creating standards and guidelines for SDN and NFV. Table 3.1 lists the main SDOs and other organizations involved in the effort and the main outcomes so far produced. This section covers some of the most prominent efforts.

open standard

A standard that is developed on the basis of an open decision-making procedure available to all interested parties, is available for implementation to all on a royalty-free basis, and is intended to promote interoperability among products from multiple vendors.

TABLE 3.1 SDN and NFV Open Standards Activities

Organization	Mission	SDN- and NFV-Related Effort
Open Networking Foundation (ONF)	An industry consortium dedicated to the promotion and adoption of SDN through open standard development.	OpenFlow
Internet Engineering Task Force (IETF)	The Internet's technical standards body. Produces RFCs and Internet standards.	Interface to routing systems (I2RS) Service function chaining
European Telecommunications Standards Institute (ETSI)	An EU-sponsored standards organization that produces globally applicable standards for information and communications technologies.	NFV architecture
OpenDaylight	A collaborative project under the auspices of the Linux Foundation.	OpenDaylight
International Telecommunication Union—Telecommunication Standardization Sector (ITU-T)	United Nations agency that produces Recommendations with a view to standardizing telecommunications on a worldwide basis.	SDN functional requirements and architecture
Internet Research Task Force (IRTF) Software Defined Networking Research Group (SDNRG)	Research group within IRTF. Produces SDN-related RFCs.	SDN architecture
Broadband Forum (BBF)	Industry consortium developing broadband packet networking specifications.	Requirements and framework for SDN in telecommunications broadband networks
Metro Ethernet Forum (MEF)	Industry consortium that promotes the use of Ethernet for metropolitan and wide-area applications.	Defining APIs for service orchestration over SDN and NFV
IEEE 802	An IEEE committee responsible for developing standards for LANs.	Standardize SDN capabilities on access networks.
Optical Internetworking Forum (OIF)	Industry consortium promoting development and deployment of interoperable networking solutions and services for optical networking products.	Requirements on transport networks in SDN architectures

Organization	Mission	SDN- and NFV-Related Effort
Open Data Center Alliance (ODCA)	Consortium of leading IT organizations developing interoperable solutions and services for cloud computing.	SDN usage model
Alliance for Telecommunications Industry Solutions (ATIS)	A standards organization that develops standards for the unified communications (UC) industry.	Operational opportunities and challenges of SDN/NFV programmable infrastructure
Open Platform for NFV (OPNFV)	An open source project focused on accelerating the evolution of NFV.	NFV infrastructure

Standards-Developing Organizations

The Internet Society, ITU-T, and ETSI are all making key contributions to the standardization of SDN and NFV.

Internet Society

A number of **standards-developing organizations (SDOs)** are looking at various aspects of SDN. Perhaps the most active are two groups within the Internet Society (ISOC): IETF and IRTF. ISOC is the coordinating committee for Internet design, engineering, and management. Areas covered include the operation of the Internet itself and the standardization of protocols used by end systems on the Internet for interoperability. Various organizations under the ISOC are responsible for the actual work of standards development and publication.

The Internet Engineering Task Force (IETF) has working groups developing SDN-related specifications in the following areas:

- **Interface to routing systems (I2RS):** Develop capabilities to interact with routers and routing protocols to apply routing policies.
- **Service function chaining:** Develop an architecture and capabilities for controllers to direct subsets of traffic across the network in such a way that each virtual service platform sees only the traffic it must work with.

The Internet Research Task Force (IRTF) has published *Software-Defined Networking (SDN): Layers and Architecture Terminology* (RFC 7426, January 2015). The document provides a concise reference that reflects current approaches regarding the SDN layer architecture. The **Request For Comments (RFC)** also provides a useful discussion of the southbound API (Figure 3.3) and describes some specific APIs, such as for I2RS.

standards-developing organization (SDO)

An official national, regional, or international standards body that develops standards and coordinates the standard activities of a specific country, region or the world. Some SDOs facilitate the development of standards through support of technical committee activities, and some may be directly involved in standards development.

Request For Comments (RFC)

A document in the archival series that is the official channel for publications of the Internet Society, including IETF and IRTF publications. An RFC may be informational, best practice, draft standard, or an official Internet standard.

IRTF also sponsors the Software Defined Networking Research Group (SDNRG). This group investigates SDN from various perspectives with the goal of identifying the approaches that can be defined, deployed, and used in the near term and identifying future research challenges.

ITU-T

The International Telecommunication Union—Telecommunication Standardization Sector (ITU-T) is a UN agency that issues standards, called recommendations, in the telecommunications area. So far, their only published contribution to SDN is Recommendation Y.3300 (*Framework of Software-Defined Networking*, June 2014). The document addresses definitions, objectives, high-level capabilities, requirements, and high-level architecture of SDN. It provides a valuable framework for standards development.

ITU-T has established a Joint Coordination Activity on Software-Defined Networking (JCA-SDN) and begun work on developing SDN-related standards.

Four ITU-T study groups (SGs) are involved in SDN-related activities:

- **SG 13 (Future networks, including cloud computing, mobile, and next-generation networks):** This is the lead study group of SDN in ITU-T and developed Y.3300. This group is studying SDN and virtualization aspects for next-generation networks (NGNs).
- **SG 11 (Signaling requirements, protocols, and test specifications):** This group is studying the framework for SDN signaling and how to apply SDN technologies for IPv6.
- **SG 15 (Transport, access, and home):** This group looks at optical transport networks, access networks, and home networks. The group is investigating transport aspects of SDN, aligned with the Open Network Foundation's SDN architecture.
- **SG 16 (Multimedia):** This group is evaluating OpenFlow as a protocol to control multimedia packet flows, and is studying virtual content delivery networks.

European Telecommunications Standards Institute

ETSI is recognized by the European Union as a European Standards Organization. However, this not-for-profit SDO has member organizations worldwide and its standards have international impact.

ETSI has taken the lead role in defining standards for NFV. ETSI's Network Functions Virtualisation (NFV) Industry Specification Group (ISG) began work in January 2013 and produced a first set of specifications in January 2015. The 11 specifications

include an NFV's architecture, infrastructure, service quality metrics, management and orchestration, resiliency requirements, and security guidance.

Industry Consortia

Consortia for open standards began to appear in the late 1980s. There was a growing feeling within private-sector multinational companies that the SDOs acted too slowly to provide useful standards in the fast-paced world of technology. Recently, a number of consortia have become involved in the development of SDN and NFV standards. We mention here three of the most significant efforts.

By far the most important **consortium** involved in SDN standardization is the Open Networking Foundation (ONF). ONF is an industry consortium dedicated to the promotion and adoption of SDN through open standards development. Its most important contribution to date is the OpenFlow protocol and API. The OpenFlow protocol is the first standard interface specifically designed for SDN and is already being deployed in a variety of networks and networking products, both hardware based and software based. The standard enables networks to evolve by giving logically centralized control software the power to modify the behavior of network devices through a well-defined “forwarding instruction set.” Chapter 4 is devoted to this protocol.

The Open Data Center Alliance (ODCA) is a consortium of leading global IT organizations dedicated to accelerating adoption of interoperable solutions and services for cloud computing. Through the development of usage models for SDN and NFV, ODCA is defining requirements for SDN and NFV cloud deployment.

The Alliance for Telecommunications Industry Solutions (ATIS) is a membership organization that provides the tools necessary for the industry to identify standards, guidelines, and operating procedures that make the interoperability of existing and emerging telecommunications products and services possible. Although ATIS is accredited by ANSI, it is best viewed as a consortium rather than an SDO. So far, ATIS has issued a document that identifies operational issues and opportunities associated with increasing programmability of the infrastructure using SDN and NFV.

Open Development Initiatives

There are a number of other organizations that are not specifically created by industry members and are not official bodies such as SDOs. Generally, these organizations are user created and driven and have a particular focus, always with the goal of developing open standards or open source software. A number of such groups have become

→ See Chapter 4, “SDN Data Plane and OpenFlow”

consortium

A group of independent organizations joined by common interests. In the area of standards development, a consortium typically consists of individual corporations and trade groups concerned with a specific area of technology.

active in SDN and NFV standardization. This section lists three of the most significant efforts.

OpenDaylight

→ *See Section 5.3, “OpenDaylight”*

OpenDaylight is an open source software activity under the auspices of the Linux foundation. Its member companies provide resources to develop an SDN controller for a wide range of applications. Although the core membership consists of companies, individual developers and users can also participate, so OpenDaylight is more in the nature of an open development initiative than a consortium. ODL also supports network programmability via southbound protocols, a bunch of programmable network services, a collection of northbound APIs, and a set of applications.

OpenDaylight is composed of about 30 projects, and releases their outputs in simultaneous manner. After its first release, Hydrogen, in February 2014, it successfully delivered the second one, Helium, at the end of September 2014.

Open Platform for NFV

→ *See Section 7.4, “NFV Benefits and Requirements”*

Open Platform for NFV is an open source project dedicated to acceleration the adoption of standardized NFV elements. OPNFV will establish a carrier-grade, integrated, open source reference platform that industry peers will build together to advance the evolution of NFV and to ensure consistency, performance, and interoperability among multiple open source components. Because multiple open source NFV building blocks already exist, OPNFV will work with upstream projects to coordinate continuous integration and testing while filling development gaps.

OpenStack

OpenStack is an open source software project that aims to produce an open source cloud operating system. It provides multitenant Infrastructure as a Service (IaaS), and aims to meet the needs of public and private clouds regardless of size, by being simple to implement and massively scalable. SDN technology is expected to contribute to its networking part, and to make the cloud operating system more efficient, flexible, and reliable.

OpenStack is composed of a number of projects. One of them, Neutron, is dedicated for networking. It provides Network as a Service (NaaS) to other OpenStack services. Almost all SDN controllers have provided plug-ins for Neutron, and through them services on OpenStack and other OpenStack services can build rich networking topologies and can configure advanced network policies in the cloud.

3.4 Key Terms

After completing this chapter, you should be able to define the following terms.

application programming interface (API)	REpresentational State Transfer (REST)
consortium	Request For Comments (RFC)
datagram	service function chaining
flow	southbound API
IEEE 802	standard
northbound API	standards-developing organization (SDO)
open standard	TCP/IP protocol architecture
packet switching	

3.5 References

ODCA14: Open Data Center Alliance. *Open Data Center Alliance Master Usage Model: Software-Defined Networking Rev. 2.0*. White Paper. 2014.

ONF12: Open Networking Foundation. *Software-Defined Networking: The New Norm for Networks*. ONF White Paper, April 13, 2012.

This page intentionally left blank

Symbols

1-Gbps Ethernet, 15-16
1G (first generation) cellular networks, 23
2G (second generation) cellular networks, 23
2.5-Gbps Ethernet, 19
3G (third generation) cellular networks, 24
4G (fourth generation) cellular networks, 24
5-Gbps Ethernet, 19
5G (fifth generation) cellular networks, 25
10-Gbps Ethernet, 16-17
25-Gbps Ethernet, 18
50-Gbps Ethernet, 18
100-Gbps Ethernet, 17
400-Gbps Ethernet, 19

A

AAA (authentication, authorization, and accounting), 126-127
ABAP, 488
abstractions
 defined, 147
 ICN, 170-173
 SDN, 146-149
 abstractions, 147-149
 Frenetic, 150-152
abuse security threats, 450
access, 10
 big data concerns, 48
 control RFID technology, 388
 facilities, 6
 management
 cloud security, 448
 SecaaS, 455
accountability, 436
accounts, hijacking, 451
accuracy (sensors), 379
ACM Career Resources website, 489
ACs (attachment circuits), 244
action buckets, 108

actionable QoE, 330-331
actions
 defined, 101
 flow tables, 101-102
 VTN flow filter, 256
active measurement techniques, 295
actuating devices (IoT), 396
actuators, 29, 380-381
addresses
 broadcast, 231
 unicast, 231
admission control
 ISA, 275
 traffic, 271
Adobe Experience Manager, 489
AF (assured forwarding) PHB, 288-289
agents
 IoT, 399
 management, 275
 QoE, 337-339
aggregation routers, 8
agile software development, 471
agility
 cloud computing, 50
 NV, 253
algorithms, routing, 273
Alliance for Telecommunications Industry Solutions (ATIS), 89
all type group type, 108
ALM (application lifecycle management), 473
Amazon Web Services (AWS), 482
analytics
 big data, 46
 Cisco IoT system, 424-425
 defined, 46
 IoT, 30
Ansible, 489
anti-counterfeiting RFID technology, 388
Apache Kafka, 489
APIs (application programming interfaces), 83
 cloud security, 450
 Defined, 83

- QoE monitoring layers, 337
- REST, 130-132
- SDN, 83
- SDN northbound controller, 117
- application level (IWF IoT reference model), 407**
- applications**
 - convergence, 30
 - development, 471
 - elastic, 39
 - enablement platform component (Cisco IoT system), 426
 - lifecycle management (ALM), 473
 - processors, 383
 - programming interfaces. *See* APIs
 - providers, 6
 - QoE/QoS video services mapping models, 328-329
 - real-time, 43
 - RFID, 387-389
 - SDI, 258
 - SDN, 85, 145-147
 - applications, 147
 - data center networking, 162-168
 - ICN, 168-173
 - measurement, 157
 - mobility/wireless, 168
 - monitoring, 157
 - network services abstraction layer, 146-152
 - northbound interface, 146
 - security, 157-159, 162
 - traffic engineering, 153-156
 - user interfaces, 147
 - service class characteristics, 41
 - service providers, 7
- architectures**
 - cloud computing
 - ITU-T cloud computing reference, 365-368
 - NIST cloud computing reference, 361-365
 - CloudNaaS, 167
 - cloud security, 448
 - Defense4All, 160-162
 - DevOps, 472
 - enterprise LAN, 12
 - evolving trends
 - complex traffic patterns, 78
 - demand increases, 77
 - inadequate architectures, 79-80
 - supply increases, 77
 - global, 7-8
 - hierarchy, 9
 - access, 10
 - core, 11
 - distribution, 10
 - inadequate, 79
 - IoT
 - benefits, 395
 - ITU-T reference model, 395-401
 - IWF reference model, 401-408
 - MANO, 217
 - NFV reference, 193-194
 - implementation, 196
 - management/orchestration, 194
 - reference points, 195
 - NV, 250-252
 - OpenDaylight, 122
 - base network service functions, 124
 - control plane/application plane functionality, 123
 - flexibility, 123
 - Helium, 124
 - layers, 122
 - modules, 125-127
 - SAL, 123
 - SDNi, 141-142
 - PolicyCop application, 154
 - QoS, 268
 - control plane, 271-272
 - data plane, 269-271
 - management plane, 272
 - REST
 - API example, 130-132
 - constraints, 128-130
 - defined, 128
 - URIs, 129
 - SDI, 261-262
 - SDN high-level (ITU-T Y.3300), 120-121
 - SDS, 259
 - SLAs, 292
 - TCP/IP, 79
 - traditional, 79-80
 - UC
 - audio conferencing, 34
 - benefits, 36
 - convergence, 35
 - defined, 33
 - elements, 33-35
 - instant messaging, 34
 - IP enabling contact centers, 35
 - mobility, 35
 - presence, 35
 - RTC dashboard, 33
 - unified messaging, 34
 - video conferencing, 34
 - web conferencing, 34
 - use cases (NFV), 222-223
 - VMs, 180-183
 - VTN, 257
- ARP opcode field (flow table match fields), 100**
- AS (autonomous systems), 58**
- assured forwarding (AF) PHB, 288-289**
- asynchronous messages, 109**
- ATIS (Alliance for Telecommunications Industry Solutions), 89**
- attachment circuits (ACs), 244**

attack surfaces

- NFV, 441-444
- SDN, 437

audio conferencing, 34**authentication, 438****authentication, authorization, and accounting (AAA), 126-127****authenticity, 435****autonomous systems (AS), 58****availability**

- cloud security, 448-449
- security requirement, 435
- SLAs, 292

AWS (Amazon Web Services) certification programs, 482**B****backbone networks. See core networks****backpressure, 64****bandwidth**

- 3G cellular networks, 24
- cross-section, 163

“Bandwidth Needs in Core and Aggregation Nodes in the Optical Transport Network” website, 37**Beacon, 115****behavior aggregates, 280****benefits**

- cloud computing, 27
- convergence, 32
- elastic traffic, 40
- NFV, 191-192
- NV, 252
- UC, 36

best effort delivery service, 267**BGP (Border Gateway Protocol), 136**

- defined, 136
- functions, 136
- neighbor acquisitions/reachability, 136
- network reachability, 137
- OpenDaylight, 126
- SDN, 138-140

big data, 45

- analytics, 46
- applications (SDN), 163-164
- areas of concern, 48
- defined, 45
- ecosystem example, 46-48
- infrastructures, 46
- three V's, 48

binary explicit congestion signaling, 66**black-box media-based QoE/QoS mapping models, 323-325****blade servers, 14****Border Gateway Protocol (BGP), 136****boundary nodes (DiffServ), 280****broadcast addresses, 231****broadcast domains, 231****Brocade**

- Mobile Analytics DevOps related products, 479
- NFV certification, 481

buildings IoT services, 377**bulk transfer capacity metric, 294****business continuity, 456****business-driven convergence, 31****C****CaaS (Communications as a Service), 355-357****cache constraint (REST), 129****caching, 170****CapEx (capital expenditure), 191****capital cost savings, 253****capital expenditure (CapEx), 191****CAPM (Certified Associate in Project Management), 485****careers (IT)**

- certification programs, 480-487
 - cloud computing, 482-483
 - IT security, 487
 - networking, 484
 - project management, 485
 - SDN, 481
 - systems engineer, 486
 - virtualization, 481-483
- emerging roles, 467
 - responsibilities, 467-469
 - SDN/NFV impacts, 469-470
- online resources, 489-490
- overview website, 490
- skills in demand, 488-489

carrier Ethernet, 14**Cassandra, 488****CBWFQ (class-based WFQ), 279****CCA-V (Citrix Certified Associate - Virtualization), 484****CCE-V (Citrix Certified Expert - Virtualization), 484****CCNx, 169-170****CCP-V (Citrix Certified Professional - Virtualization), 484****CDNs (Content Delivery Networks), 224****CE (customer edge), 244****cellular networks, 23**

- 1G (first generation), 23
- 2G (second generation), 23
- 3G (third generation), 24
- 4G (fourth generation), 24
- 5G (fifth generation), 25

centralized controllers, 133**centralized server farms, 16**

certification programs, 480-487

- cloud computing, 482-483
- IT security, 487
- networking, 484
- project management, 485
- SDN, 481
- systems engineer, 486
- virtualization, 481-483

Certified Associate in Project Management (CAPM), 485**channels**

- 1G/2G cellular networks, 23
- OpenFlow, 96

Chef, 488**chips, 384-385****choke packets, 65****Cisco**

- DevNet, 479
- networking certifications, 484
- IoT system, 420
 - application enablement platform, 426
 - data analytics, 424-425
 - fog computing, 424
 - management and automation, 426
 - network connectivity, 423-424
 - security, 425-426
 - six pillars, 421
- Performance Routing (PfR), 272
- Systems Internetworking Technology Handbook website, 299
- virtualization certification programs, 481

CISM (Certified Information Security Manager), 487**Citrix Certified Associate - Virtualization (CCA-V), 484****Citrix Certified Expert - Virtualization (CCE-V), 484****Citrix Certified Professional - Virtualization (CCP-V), 484****class-based WFQ (CBWFQ), 279****class selector PHB, 289-291****classes (RFID tags), 392****classifiers**

- DiffServ, 280
- traffic, 285

client-server constraint (REST), 128**cloud computing, 350**

- agility, 50
- architecture
 - ITU-T cloud computing reference, 365-368
 - NIST cloud computing reference, 361-365
- auditors, 363
- benefits, 27, 349
- brokers, 363
- carriers, 363
- certification programs, 482-483
- CloudNaaS, 164-168
 - architecture, 167
 - framework, 165

- IaaS, 166
- VMs, 166
- context, 27
- core, 50
- defined, 26, 349
- deployment models, 359-360
- DevOps, 477
- flexibility, 50
- fog computing, compared, 405
- history, 25
- networking, 28
- NFV, 368-371
- NIST characteristics, 26
- OSS, 50
- performance, 50
- requirements, 50
- scalability, 50
- SDN, 368-371
- security, 446
 - architecture, 448
 - auditability, 449
 - availability, 448-449
 - compliance, 447
 - controls, 457
 - data protection, 448-453
 - governance, 447
 - identity/access management, 448
 - incident response, 448
 - Security as a Service, 453-456
 - sharing vendor resources, 449
 - software isolation, 448
 - subscriber protection, 450
 - threats, 449-452
 - trust, 447
- services
 - CaaS, 355
 - cloud capability types, 356
 - CompaaS, 356
 - DSaaS, 356
 - emerging, 357
 - IaaS, 354-355
 - NaaS, 356
 - PaaS, 353
 - SaaS, 352-353
 - XaaS, 357-358
- storage, 28, 350
- traffic flow, 48
 - intercloud, 50
 - intracloud, 49
 - OSS, 50

Cloudera Impala, 488-489**CloudNaaS (Cloud Network as a Service), 164-168**

- architecture, 167
- framework, 165
- IaaS, 166
- VMs, 166

Cloud Security Alliance, 453

Cloud Security as a Service. See SecaaS

cloud service management, 364

CloudShell DevOps related products, 479

CM (Control Manager), 417-420

CoAP (constrained application protocol), 411-414

code-on-demand constraint (REST), 130

codepoints, 280

cognitive processing, 307

collaboration, 474

collaboration/processes level (IWF IoT reference model), 407

commercial off-the-shelf (COTS), 184

Communication object, 338

communications

IoT devices, 399

networks (IoT), 396

unified

audio conferencing, 34

benefits, 36

convergence, 35

defined, 33

elements, 33-35

instant messaging, 34

IP enabling contact centers, 35

mobility, 35

presence, 35

RTC dashboard, 33

unified messaging, 34

video conferencing, 34

web conferencing, 34

VLAN membership, 236

VNFC to VNFC, 215-216

Communications as a Service (CaaS), 355-357

community cloud infrastructure, 360

CompaaS (Compute as a Service), 356

components (IoT-enabled things), 377

actuators, 380-381

microcontrollers, 381-386

RFID technology, 387-392

sensors, 377-379

transceivers, 386

Compute as a Service (CompaaS), 356

compute domain

defined, 199

elements, 205-208

eswitch, 205

NFV, 187

NFVI nodes, 206-208

compute nodes, 206

Computer Jobs website, 490

Computer Science Student Resources website, 490

ComputerWorld IT Topic Center website, 490

conditioning traffic (DiffServ), 281, 285

conferencing, 34

confidentiality

security requirement, 435

TLS, 438

configuring

DiffServ, 284

LANs, 231

NFV, 188-189

QoE monitoring, 335

VLANs, 234

congestion

avoidance, 270

controlling, 64

backpressure, 64

choke packets, 65

explicit signaling, 66-67

implicit signaling, 65

ISA, 273

TCP, 267

effects, 60

ideal performance, 61-63

practical performance, 63-64

connections

access facilities, 6

application providers, 6-7

content providers, 7

global architectures, 8

IoT, 30, 423-424

IP performance metric, 294

network providers, 6

connectivity level (IWF IoT reference model), 403

constrained application protocol (CoAP), 411-414

constrained devices, 409

constraints (REST), 128-130

cache, 129

client-server, 128

code-on-demand, 130

layered system, 130

stateless, 128

uniform interface, 129

consumer and home IoT services, 376

containers

defined, 183

interface, 199-202

NFVI, 203

virtualization, 183

content

Delivery Networks (CDNs), 224

packets, 169

providers, 7

contextual definition, 303

continuous data sources, 44

control layers, 121

Control Manager, 417-420

control plane (SDN), 68, 82, 113

centralized controllers, 133

controller implementation initiatives, 115

- distributed controllers, 134
 - federation, 135
 - functions, 113-114
 - HA clusters, 134
 - northbound interfaces, 117-119
 - OpenDaylight architecture, 122
 - base network service functions, 124
 - control plane/application plane functionality, 123
 - flexibility, 123
 - Helium, 124
 - layers, 122
 - modules, 125-127
 - SAL, 123
 - PolicyCop application, 155
 - QoS
 - architecture, 271-272
 - management, 138-140
 - REST
 - API example, 130-132
 - constraints, 128-130
 - defined, 128
 - routing, 119-120, 137-138
 - SDNi
 - IETF, 140-141
 - OpenDaylight, 141-142
 - southbound interfaces, 116-117
 - controlled load services, 277**
 - Controller object, 338**
 - controllers**
 - cloud security, 457
 - congestion, 64
 - backpressure, 64
 - choke packets, 65
 - congestion effects, 60
 - explicit signaling, 66-67
 - ideal performance, 61-63
 - implicit signaling, 65
 - practical performance, 63-64
 - data flow, 271-272
 - SDN, 68
 - centralized, 133
 - distributed, 134
 - federation, 135
 - functions, 113-114
 - HA clusters, 134
 - IETF SDNi, 140-141
 - implementation initiatives, 115
 - implementing, 84
 - northbound interfaces, 117-119
 - OpenDaylight, 122-127
 - OpenDaylight SDNi, 141-142
 - PolicyCop application, 155
 - privacy, 134
 - QoS management, 138-140
 - reliability, 133
 - REST. *See* REST
 - routing, 119-120
 - routing between domains, 137-138
 - scalability, 133
 - security threats, 439
 - southbound interfaces, 116-117
 - switch messages, 109
 - VTN, 127
 - convergence**
 - applications, 30
 - benefits, 32
 - business-driven, 31
 - defined, 30
 - enterprise services, 30
 - infrastructure, 31
 - UC architecture, 35
 - cookie entry (flow tables), 99**
 - core networks**
 - cloud computing, 50
 - defined, 11
 - high-speed local, 16
 - core routers, 8**
 - COTS (commercial off-the-shelf), 184**
 - counters**
 - flow tables, 98
 - group tables, 107
 - CPE (customer premises equipment), 224**
 - CQ (custom queuing), 278**
 - credibility (DevOps), 478**
 - credit based explicit congestion signaling, 67**
 - cross-section bandwidth, 163**
 - current and voltage devices, 379**
 - customer edge (CE), 244**
 - customer premises equipment (CPE), 224**
 - custom queuing (CQ), 278**
-
- ## D
- data**
 - abstraction level (IWF IoT reference model), 407
 - accumulation level (IWF IoT reference model), 406-407
 - analytics, 30, 424-425
 - big, 45
 - analytics, 46
 - areas of concern, 48
 - defined, 45
 - ecosystem example, 46-48
 - infrastructures, 46
 - three V's, 48
 - capturing devices (IoT), 396
 - carriers (IoT), 396-397
 - centers
 - defined, 7
 - Ethernet, 13

- Ethernet data rates, 17
 - SDN applications, 162-168
- deduplication, 258
- loss/leakage, 451
- loss prevention (DLP), 455
- management servers, 46
- motion, 406
- packet inspection, 184
- processing systems, 46
- protection, 448, 452-453
- rates
 - 3G cellular networks, 24
 - Ethernet, 14-19
 - Wi-Fi, 21-22
- sources, 44
- warehouses, 46
- Data-Acquisition object, 338**
- Data Over Cable Service Interface Specification (DOCSIS), 126**
- data plane**
 - QoS architecture, 269-271
 - SDN, 68, 82
 - functions, 93-94
 - protocols, 95
 - security threats, 437-439
- Data Storage as a Service (DSaaS), 356**
- datagrams, 80**
- DDoS (distributed denial-of-service), 127**
 - OpenDaylight, 127
 - OpenDaylight Defense4All application, 157-159, 162
 - architecture, 160-162
 - context, 158
 - detected attacks, mitigating, 159
 - protection techniques, 158
- dedicated processors, 383**
- deeply embedded systems, 386**
- default forwarding PHB, 287**
- Defense4All application, 157-159, 162**
 - architecture, 160-162
 - context, 158
 - detected attacks, mitigating, 159
 - protection techniques, 158
- delays**
 - big data, 48
 - elastic traffic, 39
 - inelastic traffic, 40
 - jitters, 40
 - real-time traffic, 43
 - SLAs, 292
- delivery, 302-303**
- demand**
 - big data, 45
 - analytics, 46
 - areas of concern, 48
 - defined, 45
 - ecosystem example, 46-48
 - infrastructures, 46
 - three V's, 48
 - cloud computing, 48
 - core, 50
 - intercloud, 50
 - intracloud, 49
 - OSS, 50
 - requirements, 50
 - virtual machines, 49
 - evolving requirements, 77
 - mobile traffic, 51
 - categories, 52
 - growth, 52
 - projections, 52
 - wireless users, 52
 - world total, calculating, 51
- deployment**
 - applications lifecycle, 471
 - cloud computing, 359-360
 - Internet, 29
 - IoT, 409
 - Cisco IoT system, 420-426
 - ioBridge, 427-430
 - IoTivity. *See* IoTivity
 - NFV, 443
 - NFVI containers, 203
 - SDN
 - domains, 134
 - driving factors, 68-69
- destination addresses field (flow table match fields), 99**
- development. *See* DevOps**
- devices**
 - constrained, 409
 - discovery, 419
 - IoT, 396
 - actuating, 396
 - communication, 399
 - data-capturing, 396
 - data-carrying, 396-397
 - galvanic driving, 398
 - gateways, 398
 - general, 396-398
 - infrared, 397
 - interaction technologies, 397
 - optical, 398
 - RFID, 397
 - sensing, 396
 - manager, 114
 - unconstrained, 410
- DevNet, 479**
- DevOps (development operations), 471**
 - ALM, 473
 - architecture, 472
 - automation, 475
 - Cisco DevNet, 479
 - cloud computing, 477

- collaboration, 474
- credibility, 478
- current state, 479
- defined, 471
- demand, 475
- development/testing, 473
- fundamentals, 471-475
- monitoring/optimizing, 473
- network infrastructure, 476-478
- planning and measuring, 473
- programmability, 477
- releasing/deploying, 473
- related products, 478
- scripting, 477
- version control systems, 477

Dice rankings of IT skills in demand, 488-489

DICE website, 490

differentiated services codepoint (DSCP), 256

DiffServ (differentiated services), 279

- behavior aggregates, 280
- boundary nodes, 280
- characteristics, 279
- classifiers, 280
- codepoints, 280-282
- configuration, 284
- domains, 280-281
- dropping, 280
- DSField, 280-282
- interior nodes, 280
- marking, 281
- metering, 281
- node, 280
- PHB, 281-286
 - assured forwarding, 288-289
 - class selector, 289-291
 - default forwarding, 287
 - expedited forwarding, 287
- service examples, 282
- SLAs, 281
- TCA, 281
- terminology, 280
- traffic conditioning, 281-285

digital traffic channels, 23

direct packet through pipeline instructions, 102

disaster recovery, 456

discarding packets, 273

discovery

- devices, 419
- link, 120

distributed denial-of-service. See DDoS

distribution

- abstraction, 149
- controllers, 134
- networks, 10

DLP (data loss prevention), 455

DLUX UI, 127

DOCSIS (Data Over Cable Service Interface Specification), 126

domains

- broadcast, 231
- compute, 187
- DiffServ, 280-281
- infrastructure network, 187
- NFV, 190
- NFVI, 199
 - compute, 205-208
 - hypervisor, 208-209
 - IND, 209-213
 - logical structure, 204
- SDN, 133, 137-138

double-sided quality models, 323

droppers

- DiffServ, 280
- packets, 285

DSaaS (Data Storage as a Service), 356

DSCP (differentiated services codepoint), 256

DSField, 280-282

E

ecosystem

- application providers, 6-7
- connections, 6
- content providers, 7
- data centers, 7
- fog networking, 7
- IoT (Internet of Things), 7
- network providers, 6
- users, 5

edge computing level (IWF IoT reference model), 403-404

edge routers, 8

EF (expedited forwarding) PHB, 287

EGP (exterior gateway protocol), 59

egress port field (flow table match fields), 99

egress processing, 103-105

elastic traffic

- applications, 39
- benefits, 40
- defined, 39
- delays, 39
- QoS, 40
- requirements, 39
- total elapsed time, 40

electric actuators, 381

electronic product codes (EPCs), 387

EM (element management), 220

e-mail security, 455

embedded systems, 381-383

E-Model, 325

encapsulated packets, 111

encryption

- 1G/2G cellular networks, 23
- cloud security, 456

end users. See users**energy IoT services, 377****enterprise networks**

- Ethernet, 13
- LANs
 - architecture, 12
 - Ethernet data rates, 17
- services, 30
- Wi-Fi, 20

entries

- flow tables, 98
- group tables, 107

EPCs (electronic produce codes), 387**equipment consolidation, 253****ERPs (exterior router protocols), 59, 136****error detection/correction, 23****eswitches, 205****Ethernet**

- carrier, 14
- data centers, 13
- data rates, 14
 - 1-Gbps, 15-16
 - 2.5/5-Gbps, 19
 - 10-Gbps, 16-17
 - 25/50-Gbps, 18
 - 100-Gbps, 17
 - 400-Gbps, 19
- defined, 11
- enterprise, 13
- homes, 12
- LAN connections, 8
- metro, 14
- offices, 12
- source port field (flow table match fields), 99
- standards, 14
- type field (flow table match fields), 99
- WANs, 14
- Wi-Fi combination, 12

The Ethernet Alliance, 14**ETSI (European Telecommunications Standards Institute), 88, 444-446****Eureka Celtic, 304****event-based messages, 111****events, 308****expedited forwarding (EF) PHB, 287****explicit congestion signaling, 66-67****exterior gateway protocol (EGP), 59****exterior router protocols (ERPs), 59, 136****F****faces, 170****fair queuing, 279****fast failover group type, 109****FEC (forwarding equivalence class), 244****federation, 135****FIFO (first-in, first-out), 277****fifth generation (5G) cellular networks, 25****first generation (1G) cellular networks, 23****fixed access network functions, 225****flags entry (flow tables), 99****flexibility**

- cloud computing, 50
- NV, 253
- OpenDaylight architecture, 123

Floodlight, 115**flows**

- congestion avoidance, 270
- controlling, 271-272
- ISA, 273
- metering, 272
- OpenFlow, 97-98
- packets
 - defined, 80
 - marking, 270
- queue management, 270
- recording, 272
- restoration, 272
- statistics, 111
- tables
 - action sets, 102
 - entries, 98
 - instructions component, 101-102
 - match fields, 99-101
 - nesting, 106-107
 - pipeline, 102-105
 - structure, 98
- traffic
 - classification, 269
 - policing, 270
 - shaping, 270
 - VTN, 256
 - WFQ, 279

Flume, 488**fog computing**

- Cisco IoT system, 424
- cloud computing, compared, 405
- defined, 404

fog networking, 7**ForCES (Forwarding and Control Element Separation), 117****forwarding**

- abstraction, 148
- equivalence class (FEC), 244

packets, 56-57, 275

paths, 187

PHB, 287-289

rules manager, 124

shortest path, 114

fourth generation (4G) cellular networks, 24

frame tagging, 236

frameworks

high-level, 190-191

IoT security, 462-464

Frenetic, 150-152

full-reference quality models, 323

functional block interface, 200

functionalities (RFID), 391-392

functions

fixed access, 225

network, 187

VNF, 213

interfaces, 213-214

potential functions, 213

scaling, 216

VNFC to VNFC communication, 215-216

G

galvanic driving devices, 398

gateways

IoT, 396-398

nodes, 206

GBP (Group Based Policy), 126

general devices (IoT), 396-398

GET message type, 131

GIAC (Global Information Assurance Certification)

GSEC (Security Essentials), 487

Git, 477

glass-box parameter-based QoE/QoS mapping models, 325-326

global architectures, 7-8

Google cloud computing certification programs, 483

governance, 447

gray-box QoE/QoS mapping models, 326-327

Group Based Policy (GBP), 126

group tables

action buckets, 108

entries, 107

group types, 108-109

OpenFlow, 97, 107-109

groups, 108-109

guaranteed services, 276

H

HA (high-availability) clusters, 134

Hadoop, 488

hardware virtualization, 178

Hbase, 488

healthcare IoT services, 376

Helium (OpenDaylight), 124

hierarchy, 9

access, 10

core, 11

distribution, 10

high-level frameworks, 190-191

high-level SDN architecture (ITU-T Y.3300), 120-121

high-speed local core networks, 16

hijacking accounts/services, 451

homes

Ethernet, 12

NFV, 224

Wi-Fi, 20

host-centric vertical handover QoE-based network management, 341-342

host trackers, 124

HP ASE - SDN Application Developer certification, 481

hybrid cloud infrastructure, 360

hydraulic actuators, 380

hypervisor domain, 199, 208-209

hypervisor introspection, 446

I

IaaS (Infrastructure as a Service), 166, 354

CloudNaaS, 166

defined, 166, 354

examples, 354

separation of responsibilities, 355

IAM (Identity and access management), 455

IBM

cloud computing certification programs, 482

study "Every Day We Create 2.5 Quintillion Bytes of Data" website, 73

ICMP type/code fields (flow table match fields), 100

ICMPv6 type/code fields (flow table match fields), 100

ICN (Information-Centric Networking), 168-173

identification RFID technology, 387

identifiers

group, 107

URIs, 129

identity

access management (IAM), 455

cloud security, 448

SecaaS, 455

IEEE (Institute of Electrical and Electronics Engineers), 14

802.1, 237

802.1Q standard, 237-238

802.3, 237

802.11 standards, 21

802, 14, 237

- Computer Society Build Your Career website, 490
- Job Site website, 490
- Resume Lab website, 490
- Standards Association (IEEE-SA), 305
- IETF (Internet Engineering Task Force), 87, 140-141**
- IGP (interior gateway protocol), 59**
- image, camera devices, 379**
- IM (instant messaging), 34**
- implementing**
 - NFV, 196
 - SDN controllers, 84, 115
- implicit congestion signaling, 65**
- incident response, 448**
- IND (infrastructure network domain), 199, 209-213**
 - L2 versus L3 virtual networks, 210-211
 - NFV, 187
 - reference points, 209
 - virtualization, 210
 - virtual network alternatives, 211
- indirect group type, 109**
- industrial IoT services, 376**
- inelastic traffic**
 - defined, 40
 - delays, 40
 - internet requirements, 42
 - packet loss, 41
 - QoS requirements, 42
 - requirements, 40
 - service class characteristics, 41
 - throughput, 40
- inertial devices, 378**
- Information-Centric Networking (ICN), 168-173**
- Information Technology. See IT**
- infrared devices, 397**
- infrastructures**
 - as a Service. *See* IaaS
 - based VN, 212
 - big data, 46
 - convergence, 31
 - network domain. *See* IND
 - NFV, 199
 - compute domain, 205-208
 - container deployment, 203
 - domains, 199, 204
 - hypervisor domain, 208-209
 - IND, 209-213
 - nodes, 206-208
 - virtual network alternatives, 211
 - virtualized manager (VIM), 217-218
- ingress port field (flow table match fields), 99**
- ingress processing, 102-104**
- inspecting packets, 184**
- instant messaging (IM), 34**
- Institute of Electrical and Electronics Engineers. See IEEE**
- instructions component, 102**
- instructions entry (flow tables), 98**
- integrated circuits, 384**
- Integrated Services Architecture. See ISA**
- integrity**
 - security requirement, 435
 - TLS, 438
- Inter-SDN Controller Communication: Using Border Gateway Protocol website, 143**
- interactive QoE, 55**
- intercloud networks, 50**
- intercommunicating smart objects, 374**
- Interest packets, 169**
- interfaces**
 - cloud security, 450
 - container, 199-202
 - functional block, 200
 - SDN controllers
 - northbound, 117-119, 146
 - southbound, 116-117
 - sensors, 377
 - uniform, 129
 - user, 147
 - VNF, 213-214
- interior gateway protocol (IGP), 59**
- interior nodes, 280**
- interior router protocols (IRPs), 58, 119**
- International Information System Security Certification Consortium (ISC)2 Certified Information Systems Security Professional (CISSP), 487**
- International Telecommunication Union—Telecommunication Standardization Sector. See ITU-T**
- Internet**
 - defined, 39
 - deployment generations, 29
 - Engineering Task Force (IETF), 87, 140-141
 - exchanges, 17
 - media providers, 17
 - wireless, 52
- Internet of Things. See IoT**
- Internet Research Task Force (IRTF), 87**
- Internet Society (ISOC), 87**
- internets, 39, 42**
- intracloud networks, 49**
- intrusion management, 456**
- ioBridge**
 - platform, 427
 - RealTime.io, 430
 - ThingSpeak, 428-429
 - website, 427
- I/O ports, 59**
- IoT (Internet of Things), 7**
 - actuators, 380-381
 - agents, 399

- architecture, 395
 - benefits, 373
 - Cisco IoT system, 420
 - application enablement platform, 426
 - data analytics, 424-425
 - fog computing, 424
 - management and automation, 426
 - network connectivity, 423-424
 - security, 425-426
 - six pillars, 421
 - components, 377, 389
 - defined, 28
 - deploying, 409
 - embedded devices, 28
 - equation, 374
 - intercommunicating smart objects, 374
 - Internet deployment evolution, 29
 - ioBridge
 - platform, 427
 - RealTime.io, 430
 - ThingSpeak, 428-429
 - website, 427
 - IoTivity, 409
 - base, 410
 - Base, 415-417
 - Base services, 417-420
 - CoAP, 411-414
 - constrained devices, 409
 - Linux Foundation, 409
 - OIC, 409
 - unconstrained devices, 410
 - ITU-T reference model, 395, 400-401
 - actuating devices, 396
 - communication networks, 396
 - data-capturing devices, 396
 - data carriers, 396
 - devices, 396-399
 - gateway, 396
 - general devices, 396
 - sensing devices, 396
 - terminology, 395-396
 - things, 396
 - IWF reference model, 401-403
 - application, 407
 - collaboration/processes, 407
 - connectivity, 403
 - data abstraction, 407
 - data accumulation, 406-407
 - edge computing, 403-404
 - physical devices/controllers, 403
 - summary, 408
 - layers, 29-30
 - microcontrollers, 381
 - application processors, 383
 - chips, 385
 - dedicated processors, 383
 - deeply embedded systems, 386
 - embedded systems, 381-383
 - microprocessors, 383-384
 - RFID technology, 387
 - access control, 388
 - anti-counterfeiting tool, 388
 - applications, 387-388
 - functionalities, 391-392
 - operating frequencies, 391
 - payment/stored value systems, 387
 - readers, 390
 - tags, 389-390
 - tracking/identification, 387
 - scope, 374-377
 - security, 458-459
 - framework, 462-464
 - patching vulnerabilities, 459
 - requirements, 459-461
 - sensors, 377
 - accuracy, 379
 - precision, 379
 - resolution, 380
 - types, 377-379
 - service sectors
 - buildings, 377
 - consumer and home, 376
 - energy, 377
 - healthcare/life science, 376
 - industrial, 376
 - IT/networks, 375
 - retail, 376
 - security/public safety, 375
 - transportation, 376
 - tags, 375
 - technology development, 373
 - transceivers, 386
 - World Forum. *See* IWF
- iotas, 427**
- IoTivity, 409**
- base, 410
 - Base, 415
 - resources, querying, 416-417
 - services, 415-420
 - clients, 419
 - CoAP, 411-414
 - formats, 412
 - message exchange example, 414
 - message method, 413
 - messages, 412
 - constrained devices, 409
 - Linux Foundation, 409
 - OIC, 409
 - servers, 419
 - unconstrained devices, 410
 - website, 409

IP

- backbone, 8
- enabling contact centers, 35
- field (flow table match fields component), 99
- mobility, 35
- Performance Metrics Working Group. *See* IPPM
- security (IPsec), 241-243

IP-oriented parameter-based QoE/QoS mapping models, 327-329**IPPM (IP Performance Metrics Working Group), 293-296**

- benefits, 293
- measurement techniques, 295
- metrics, listing of, 293
- need, 293
- pdv, 295
- sample metrics, 295
- stages, 294
- statistical metrics, 295

IPsec, 241-243**IPv4 (flow table match fields), 100****IPv6 (flow table match fields), 100-101****IRPs (interior router protocols), 58, 119****IRTF (Internet Research Task Force), 87****ISA (Integrated Services Architecture), 273**

- components, 274-275
- design, 273-274
- flows, 273
- QoS, 273
- services, 276-279

ISACA Certified Information Security Manager (CISM), 487**ISC2 (International Information System Security Certification Consortium) CISSP (Certified Information Systems Security Professional), 487****ISC2 Systems Security Certified Practitioner (SSCP), 487****ISG NFV (Network Functions Virtualization Industry Standards Group), 186**

- container interface, 199-202
- NFV standards, 186

ISOC (Internet Society), 87**ISP**

- connections, 8
- core routing, 17

IT (information technology), 29, 407

- defined, 407
- IoT services, 375
- professionals, 467
 - certification programs, 480-487
 - online resources, 489-490
 - responsibilities, 467-469
 - SDN/NFV impacts, 469-470
 - skills in demand, 488-489

ITU-T (International Telecommunication Union—Telecommunication Standardization Sector), 88, 304

- cloud computing reference architecture, 365-371
 - actors, 365
 - layers, 366-368
- IoT reference model (Y.2060), 395, 400-401
 - actuating devices, 396
 - communication networks, 396
 - data-capturing devices, 396
 - data carriers, 396
 - devices, 396-399
 - gateway, 396
 - general devices, 396
 - sensing devices, 396
 - terminology, 395-396
 - things, 396
- SDN/NFV standards, 88
- Y.2060 Overview of the Internet of Things, 374
- Y.2066 security and privacy, 459-461
- Y.3300 SDN high-level architecture, 120-121
- Y.3500
 - cloud capabilities types, 356
 - cloud service categories, 355
 - emerging cloud service categories, 357

IWF (IoT World Forum), 401-403

- application level, 407
- collaboration/processes level, 407
- connectivity level, 403
- data abstraction level, 407
- data accumulation level, 406-407
- edge computing level, 403-404
- physical devices/controllers level, 403
- summary, 408

J-K

JCA-SDN (Joint Coordination Activity on Software-Defined Networking), 88**Juniper networking certifications, 485****Kemp Technologies blog “SDN is from Mars, NFV is from Venus” website, 229**

L

L2Switch, 127**L2VPN (Layer 2 VPN), 244-246****L2/L3 virtual networks, 210-211****L3VPN (Layer 3 VPN), 244-246****label-switched paths (LSPs), 244****label-switching routers (LSRs), 244****LANs**

- configuration, 231
- enterprise, 17
- partitioned, 233
- switches, 231

Laravel, 489

latency. *See* **delays**

Layer 3 switches, 10

layered system constraint (REST), 130

Layer object, 338

layers

- abstraction, 146-152
- control, 121
- IoT, 29-30
- ITU-T cloud computing reference architecture, 366-368
- OpenDaylight architecture, 122
- QoE/QoS, 308-310
- resource, 121

legacy switches, 238

LE (lower than best effort) traffic, 268

life science IoT services, 376

link discovery, 120

Linux Foundation, 409

LISP (Location/Identifier Separation Protocol), 126-127

logical ports, 96

logical resources, 247

logical switches (OpenFlow), 97

- flow table. *See* **flows**, **tables**
- group tables, 107-109

lower than best effort (LE) traffic, 268

LSPs (label-switched paths), 244

LSRs (label-switching routers), 244

M

MACs (media access control) frames, 231

magnetic devices, 379

malicious insider threats, 451

management

- agents, 275
- automation component (Cisco IoT system), 426
- cloud service, 364
- device, 114
- forwarding rules, 124
- NFV management and orchestration. *See* **MANO**
- notification, 114
- QoS architecture, 272
- servers, 46
- statistics
 - OpenDaylight, 124
 - SDN controllers, 114
- switch
 - OpenDaylight, 124
 - retrieving statistics, 131
 - updating statistics, 132
- topology
 - OpenDaylight, 124
 - SDN controllers, 114, 120
- virtualized infrastructure (VIM), 217-218
- VNF, 218

MANO (NFV management and orchestration), 217

- architecture, 217
- element management, 220
- NFVO, 219
- OSS/BSS, 220
- repositories, 219
- VIM, 217-218
- VNF, 218

MANs (metropolitan-area networks), 14, 17

mapping models (QoE/QoS), 323

- black-box media-based, 323-325
- choosing, 327
- glass-box parameter-based, 325-326
- gray-box, 326-327
- IP-oriented parameter-based, 327-329

MapReduce, 488

marking

- DiffServ, 281
- packets, 270
- traffic, 285

master QoE agents, 339

match fields entry (flow tables), 98-101

mean opinion score (MOS), 316

measurement

- applications, 157
- QoE, 312
 - end-user device analytics, 315
 - MOS (mean opinion score), 316-317
 - objective assessment, 314-315
 - subjective assessment, 312-314

mechanical actuators, 381

media

- access control frames (MACs), 231
- devices, 379
- Internet providers, 17
- video on demand, 17

membership (VLANs)

- communicating, 236
- defining, 235

messages

- CoAP, 412-414
- GET, 131
- instant, 34
- OpenFlow, 109-111
- POST, 132
- SDNi, 141
- unified, 34

metadata field (flow table match fields), 100

meters

- DiffServ, 281
- OpenFlow QoS support, 297-298
- tables, 97
- traffic, 272, 285

metrics

- IP performance, 293
 - benefits, 293
 - listing of, 293

- measurement techniques, 295
- need, 293
- pdv, 295
- sample metrics, 295
- stages, 294
- statistical metrics, 295
- QoE
 - mapping models, 323-329
 - networks/services management, 341-344
 - service monitoring, 335-340
 - service-oriented actionable, 331
 - system-oriented actionable, 330
- QoS
 - mapping models, 323-329
 - service monitoring, 334-335
- metro Ethernet, 14**
- metropolitan-area networks (MANs), 14**
- microcontrollers, 381**
 - application processors, 383
 - chips, 385
 - dedicated processors, 383
 - deeply embedded systems, 386
 - embedded systems, 381-383
 - microprocessors, 383-384
- microprocessors, 383-384**
- Microsoft**
 - cloud computing certification programs, 482
 - systems engineer certifications, 486
- mobile cellular networks, 223**
- mobile traffic, 51-52**
- mobility**
 - SDN
 - applications, 168
 - driving factor, 69
 - UC architecture, 35
- models**
 - cloud deployment
 - community, 360
 - hybrid, 360
 - private, 359
 - public, 359
 - QoE/QoS mapping, 323
 - black-box media-based, 323-325
 - choosing, 327
 - glass-box parameter-based, 325-326
 - gray-box, 326-327
 - IP-oriented parameter-based, 327-329
- modern networking**
 - elements, 71
 - requirements, 80
- modules**
 - OpenDaylight, 125
 - controller, 126
 - network applications, orchestration, and services, 127
 - southbound interfaces/protocol plug-ins, 125
 - PolicyCop application, 155

- monitoring**
 - applications, 157
 - categories, 332
 - on-demand, 333
 - probes, 333
 - QoE, 335-340
 - agent objects, 338
 - API layers, 337
 - configurations, 335
 - QoS, 334-335
 - virtual machines (VMMs), 179-180, 183
- MOS (mean opinion score), 316-317**
- motherboards, 383**
- MPLS (Multiprotocol Label Switching), 9**
 - label value/traffic class/BoS fields (flow table match fields), 100
 - LSRs, 244
 - VPNs, 243-247
 - Layer 2, 245-246
 - Layer 3, 246
- multicore processors, 384**
- multimedia, 301**

N

- NaaS (Network as a Service), 356**
- National Institute of Standards and Technology.**
See NIST
- neighbors, 136**
- nesting**
 - flow tables, 106-107
 - VLANs, 239
- NETCONF, 125**
- network-centric vertical handover QoE-based network management, 342-344**
- network layer QoE/QoS video services mapping models, 328**
- networks**
 - capacity, 48
 - certification programs, 484
 - cloud, 350
 - connectivity, 423-424
 - functions (NFs), 187
 - Functions Virtualization Industry Standards Group.
See ISG NFV
 - Functions virtualization infrastructure. *See NFVI*
 - Functions virtualization. *See NFV*
 - interface cards (NICs), 205
 - nodes, 207
 - operating system (NOS), 114
 - OSS, 50
 - point of presence (N-PoP), 187
 - providers, 6
 - QoE-based management
 - host-centric vertical handover, 341-342
 - network-centric vertical handover, 342-344
 - VoIP calls, 341

services

catalog, 219

NFV, 187

virtualization. *See* NV

NFs (network functions), 187

NFV (network functions virtualization), 70, 184

background, 177-178

benefits, 191-192

cloud computing, 368-371

compute domains, 187

configuration example, 188-189

container interface, 199-202

COTS, 184

data packet inspection, 184

defined, 70, 187

deployment, 443

forwarding paths, 187

functions, 187

high-level framework, 190-191

infrastructure, 199

compute domain, 205-208

container deployment, 203

domains, 187, 199, 204

hypervisor domain, 208-209

IND, 209-213

nodes, 206-208

virtual network alternatives, 211

instances, 220

IT/network job position impact, 469-470

MANO, 217

architecture, 217

element management, 220

NFVO, 219

OSS/BSS, 220

repositories, 219

VIM, 217-218

VNFM, 218

modern networking schema, 72

NFVI, 187

NFVI-Node, 187

NFVI-PoP, 187

N-PoP, 187

orchestrator (NFVO), 219

PNF, 187

principles, 189

reference architecture, 193-194

implementation, 196

management/orchestration, 194

reference points, 195

requirements, 192-193

services, 187

SDI, enabling, 258

SDN

relationship, 225-228

similarities, 70

security, 441

attack surfaces, 441-444

ETSI security perspective, 444-446

techniques, 446

standards, 85-87, 186

industry consortiums, 89

open development initiatives, 90

SDOs, 87-89

use cases, 221

architectural, 222-223

service-oriented, 223-225

virtual networks, 187, 210

vision, 185

VNF, 187, 213

FG, 187

interfaces, 213-214

potential functions, 213

scaling, 216

sets, 187

VNFC to VNFC communication, 215-216

NFVI (network functions virtualization infrastructure), 187, 199

container deployment, 203

domains, 199

compute, 205-208

hypervisor, 208-209

IND, 209-213

logical structure, 204

nodes, 187, 206-208

PoP, 187, 207

resources, 220

virtual network alternatives, 211

NFVlaaS (NFVI as a Service), 222

NFVO (NFV orchestrator), 219

NICs (network interface cards), 205

NIST (National Institute of Standards and Technology), cloud computing, 26

characteristics, 26

reference architecture, 361-365

nodes

DiffServ, 280

NFVI, 187, 206-208

no-reference quality models, 324

northbound interfaces, 117-119, 146

NOS (network operating system), 114

notification manager, 114, 419

N-PoP (network point of presence), 187

NV (network virtualization)

agility, 253

architecture, 250-252

benefits, 252

capital cost savings, 253

defined, 247

equipment consolidation, 253

example, 248-249

flexibility, 253

function manager, 218

infrastructure-based, 212

- L2 versus L3, 210-211
- levels of abstraction, 248
- logical resources, 247
- NFV, 187
- NFVI alternatives, 211
- operational cost savings, 253
- physical resources, 247
- rapid service provisioning, 253
- scalability, 253
- virtual overlay, 212
- virtual resources, 247

O

objective assessment (QoE), 314-315

ODCA (Open Data Center Alliance), 80, 89

office Ethernet, 12

off-path caching, 170

OIC (Open Interconnect Consortium), 409

OnCue, 489

on-demand monitoring, 333

one-sided quality models, 324

one-way delay metric, 294

one-way loss metric, 294

one-way loss pattern metric, 294

ONF (Open Networking Foundation), 79

- Certified SDN Associate certification, 481

- Certified SDN Engineer certification, 481

- defined, 89

- traditional network architecture limitations, 79-80

Onix, 115

ONOS (Open Network Operating System), 115

on-path caching, 170

Open Data Center Alliance (ODCA), 80, 89

open development initiatives, 90

Open Interconnect Consortium (OIC), 409

Open Networking Foundation. See ONF

Open Network Operating System (ONOS), 115

Open Platform, 90

Open Platform for NFV (OPNFV), 196

Open Service Gateway Initiative (OSGi), 123

open standards, 85-87

- industry consortiums, 89

- open development initiatives, 90

- SDOs, 87-89

Open vSwitch Database Management Protocol (OVSDB), 116

OpenCrowd example SaaS services survey, 352-353

OpenDaylight, 90, 115, 122

- architecture, 122

- base network service functions, 124

- control plane/application plane functionality, 123

- flexibility, 123

- Helium, 124

- layers, 122

- modules, 125-127

- SAL, 123

Defense4All DDoS application, 157-159, 162

- architecture, 160-162

- context, 158

- detected attacks, mitigating, 159

- protection techniques, 158

SDNi, 141-142

VTN, 253-257

- architecture, 257

- Coordinator, 254

- elements, 254

- flows, 256

- Manager, 254

- mapping, 255

OpenFlow, 89

- channels, 96

- defined, 95

- encapsulated packets, 111

- event-based messages, 111

- flow, 98, 111

- flow tables

- actions, 101

- action sets, 102

- entries, 98

- instructions component, 102

- match fields, 99-101

- nesting, 106-107

- pipeline, 102-105

- structure, 98

- group tables, 107-109

- action buckets, 108

- entries, 107

- group types, 108-109

- messages, 109-111

- ports, 96

- QoS, 296-298

- switches, 96-97

- VLAN support, 240

OpenStack, 90, 126-127

operating frequencies (RFID), 391

operations

- cost savings, 253

- expenditure (OpEx), 191

- support system (OSS), 50

- technology (OT), 29, 407

OpEx (operational expenditure), 191

OPNFV (Open Platform for NFV), 196

optical devices, 379-398

OSGi (Open Service Gateway Initiative), 123

OSS (operations support system), 50

OSS/BSS (NFV MANO), 220

OT (operational technology), 29, 407

OVSDB (Open vSwitch Database Management Protocol), 116, 125-127

P

PaaS (Platform as a Service), 353, 488

PAAAs (Policy Adaptation Actions), 156

Packet Cable MultiMedia, 125

packet-switched networks (PSNs), 244

packets

choke, 65

Content, 169

defined, 79

delaying, 285

delay variation (pdv), 294-295

discarding, 273

dropping, 285

encapsulated, 111

faces, 170

flows, 80, 97

forwarding, 56-57

ISA router implementation, 275

SDN, 83

inspection, 184

Interest, 169

loss, 41

marking, 270

queue management, 270

real-time transmission, 44

scheduling, 275

switching, 79

variable-length, 44

partitioning

LANs, 233

virtual, 212

Pascal, 489

passive measurement techniques, 295

patching vulnerabilities (IoT), 459

payment RFID technology, 387

PCEP (Path Computation Element Communication Protocol), 126

PCMM (Packet Cable MultiMedia), 125

pdv (packet delay variation), 294-295

peering, 11

perception, 306

perceptual QoE, 54

perform action on packet instructions, 102

performance

cloud computing, 50

congestion

ideal, 61-63

practical, 63-64

IP performance metrics, 293-296

benefits, 293

listing of, 293

measurement techniques, 295

need, 293

pdv, 295

sample metrics, 295

stages, 294

statistical metrics, 295

QoE

categories, 54

challenges, 55

defined, 54

QoS, compared, 54

SLAs, 281

Persistent-Data object, 339

personal technology, 29

PfMP (Portfolio Management Professional), 486

PfR (Cisco Performance Routing), 272

PgMP (Program Management Professional), 486

PHB (per-hop behavior), 286

assured forwarding, 288-289

class selector, 289-291

default forwarding, 287

DiffServ, 281

expedited forwarding, 287

physical devices/controllers level (IWF IoT reference model), 403

physical network function (PNF), 187

physical port field (flow table match fields), 100

physical ports, 96

physical resources, 247

Pig, 488

pipelines (flow tables), 102-105

egress processing, 105

ingress processing, 104

processing, 102-103

Platform as a Service (PaaS), 353, 488

platforms (ioBridge), 427

RealTime.io, 430

ThingSpeak, 428-429

PLC (powerline carrier), 12

Plugin2OC, 126-127

PMI-ACP (PMI Agile Certified Practitioner), 485

PMI-PBA (PMI Professional in Business

Analysis), 486

PMP (Project Management Professional), 486

pneumatic actuators, 381

PNF (physical network function), 187

PoE (Power over Ethernet), 12

POF (Protocol Oblivious Forwarding), 117

points of presence (PoPs), 17, 187

policing traffic, 270

Policy Adaption Actions (PAAs), 156

PolicyCop, 153-156

architecture, 154

control rules, 155

features, 154

modules, 155

PAAs, 156

workflow, 156

PoPs (points of presence), 17, 187

Portfolio Management Professional (PfMP), 486

ports, 96, 100

position measuring devices, 378

POST message type, 132

Power over Ethernet (PoE), 12

power workgroups, 16

powerline carrier (PLC), 12

POX, 115

PQ (priority queuing), 278

pressure/force sensors, 378

printed circuit boards, 383

priority entry (flow tables), 98

privacy

cloud

infrastructure, 359

perspective, 369

SDN controllers, 134

probes, 333

processing

big data, 48

flow table pipelines, 102-103

egress, 105

ingress, 104

processors

application, 383

dedicated, 383

micro, 383-384

multicore, 384

PROD (production), 471

professionals

certification programs, 480-487

cloud computing, 482-483

IT security, 487

networking, 484

project management, 485

SDN, 481

systems engineer, 486

virtualization, 481-483

emerging roles, 467

responsibilities, 467-469

SDN/NFV impacts, 469-470

online resources, 489-490

skills in demand, 488-489

Program Management Professional (PgMP), 486

programmability (DevOps), 477

project management, 485

Project Management Professional (PMP), 486

protection. See also security

cloud data, 452-453

DDoS attacks, 157-159, 162

protocols

BGP

defined, 136

functions, 136

routing between SDN domains, 138

SDN QoS management, 138-140

CoAP, 411-414

formats, 412

message exchange example, 414

message method, 413

messages, 412

EGP, 59

ERP, 136

IGP, 59

IP. *See* IP

LISP, 126

MPLS, 9

neighbor acquisitions./reachability 136

network reachability, 137

Oblivious Forwarding (POF), 117

OpenFlow. *See* OpenFlow

PCEP, 126

Plugin Manager, 417

reservation, 275

routing, 57

ERPs, 59

IRPs, 58

ISA, 275

SDN data plane, 95

SNMP, 126

TCP

congestion control, 267

flags field (flow table match fields), 101

source/destination ports (flow table match fields), 100

TCP/IP, 79

providers

application, 6-7

architectural components (cloud), 364

bridge traffic ISID field (flow table match fields), 100

content, 7

Internet media, 17

network, 6

proximity motion sensors, 378

PSN (packet-switched networks), 244

psychological QoE, 54

public

cloud infrastructure, 359

safety IoT services, 375

Wi-Fi, 20

Q

QoE (Quality of Experience), 54, 266

actionable, 330-331

agents, 337

APIs, 337

master, 339

objects, 338

slave, 339

- applications, 317
 - categories, 54
 - challenges, 55
 - definitions, 306-308
 - influences, 311-312
 - layered model, 308-310
 - mapping models, 323
 - black-box media-based, 323-325
 - choosing, 327
 - glass-box parameter-based, 325-326
 - gray-box, 326-327
 - IP-oriented parameter-based, 327-329
 - measurement, 312
 - end-user device analytics, 315
 - MOS (mean opinion score), 316-317
 - objective assessment, 314-315
 - subjective assessment, 312-314
 - monitoring, 335-340
 - agent objects, 338
 - API layers, 337
 - configurations, 335
 - motivations, 301
 - networks and services management, 318
 - host-centric vertical handover, 341-342
 - network-centric vertical handover, 342-344
 - VoIP calls, 341
 - online video content delivery, 302-303
 - QoS, compared, 54
 - service
 - failures, 304
 - monitoring, 317
 - standardization projects, 304-305
 - QoS (quality of service), 40, 266**
 - architecture, 268
 - control plane, 271-272
 - data plane, 269-271
 - management plane, 272
 - background, 267-268
 - defined, 53, 266
 - DiffServ. *See* DiffServ
 - elastic traffic, 40
 - IPPM, 293-296
 - benefits, 293
 - measurement techniques, 295
 - metrics, listing of, 293
 - need, 293
 - pdv, 295
 - sample metrics, 295
 - stages, 294
 - statistical metrics, 295
 - ISA
 - components, 274-275
 - defined, 273
 - design, 273-274
 - flows, 273
 - services, 276-279
 - layered model, 308-310
 - mapping models, 323
 - black-box media-based, 323-325
 - choosing, 327
 - glass-box parameter-based, 325-326
 - gray-box, 326-327
 - IP-oriented parameter-based, 327-329
 - modern networking schema, 72
 - monitoring, 334-335
 - online video content delivery, 303
 - OpenFlow, 296-298
 - policies, 272
 - PolicyCopy application, 153-156
 - architecture, 154
 - control rules, 155
 - features, 154
 - modules, 155
 - PAAAs, 156
 - workflow, 156
 - properties, 53
 - QoE, compared, 54
 - routing, 272
 - SDN
 - managing with BGP, 138-140
 - routing between domains, 137-138
 - SLAs
 - architecture, 292
 - availability, 292
 - features, 291
 - latency, 292
 - reliability, 293
 - QUALINET, 304-308**
 - quality**
 - formation process, 307-308
 - QoE definition, 306
 - Quality of Experience. *See* QoE**
 - Quality of Service. *See* QoS**
 - QuEEN (Quality of Experience Estimators in Networks), 305**
 - querying resources, 416-417**
 - queues**
 - custom, 278
 - data flows, 270
 - disciplines, 277-279
 - fair queuing, 279
 - FIFO, 277
 - management, 270
 - OpenFlow QoS support, 296
 - priorities, 278
-
- ## R
- radio-frequency identification. *See* RFID**
 - random early detection (RED), 271**
 - RAN (radio access network), 224**
 - rapid service provisioning, 253**
 - rate based explicit congestion signaling, 67**

RBAC (role-based access control), 463**read range (RFID tags), 390****real-time, 43, 430**

- communications (RTC), 33

- traffic

- continuous data sources, 44

- defined, 43

- delays, 43

- illustration, 43

- on/off sources, 44

- packet transmission, 44

- variable-length packets, 44

recording traffic, 272**Red Hat**

- Certified Engineer (RHCE), 487

- Certified Systems Administrator (RHCSA), 487

- Enterprise Linux Atomic Host DevOps related products, 479

RED (random early detection), 271**reference points**

- IND, 209

- NFV, 195

references

- “Bandwidth Needs in Core and Aggregation Nodes in the Optical Transport Network” website, 37

- Cisco Systems Internetworking Technology

- Handbook website, 299

- IBM Study “Every Day We Create 2.5 Quintillion

- Bytes of Data” website, 73

- Inter-SDN Controller Communication: Using Border Gateway Protocol, 143

- IoT World Forum website, 431

- Kemp Technologies blog “SDN is from Mars, NFV is from Venus” website, 229

- “SDI Wars: WTF Is Software Defined Center Infrastructure?” website, 263

- Telecom Lighthouse, 229

reliability

- SDN controllers, 133

- SLAs, 293

repositories, 219**REpresentational State Transfer. See REST****Request For Comments (RFC), 87****requirements**

- cloud computing, 50

- elastic traffic, 39

- evolving

- complex traffic patterns, 78

- demand increases, 77

- inadequate architectures, 79-80

- supply increases, 77

- inelastic traffic, 40-42

- IoT security, 459-461

- modern networks, 80

- NFV, 192-193

- security, 435-436

reservation protocols, 275**reserving**

- ports, 97

- resources, 272

residential. See homes**resolution, 380****resources**

- layers, 121

- NFVI, 220

- querying, 416-417

- reserving, 272

responsibilities

- IT/network professionals, 467-469

- NIST cloud computing reference architecture, 361, 364

REST (REpresentational State Transfer), 128

- API example, 130-132

- constraints, 128-130

- cache, 129

- client-server, 128

- code-on-demand, 130

- layered system, 130

- stateless, 128

- uniform interface, 129

- defined, 128

- resource request/response handlers, 419

- URIs, 129

restoring traffic, 272**retail IoT, 376****RFC (Request For Comments), 87****RFC 4594 (Configuration Guidelines for DiffServ Service Classes), 41****RFID (radio-frequency identification), 387**

- access control, 388

- anti-counterfeiting tool, 388

- applications, 387-389

- devices, 397

- functionalities, 391-392

- operating frequencies, 391

- payment/stored value systems, 387

- readers, 390

- tags, 389-390

- functionalities, 391-392

- operating frequencies, 391

- readers, 390

- types, 390

- tracking/identification, 387

RHCE (Red Hat Certified Engineer), 487**RHCSA (Red Hat Certified Systems Administrator), 487****roles**

- based access control (RBAC), 463

- IT professionals, 467

- responsibilities, 467-469

- SDN/NFV impacts, 469-470

- NIST cloud computing reference architecture, 361-364

round-trip delay metric, 294

routing

- aggregation, 8
- algorithms, 273
- characteristics, 55-56
- core, 8
- elements, 59-60
- packet forwarding, 56-57
- peering, 11
- protocols, 57
 - ERPs, 59
 - IRPs, 58
- QoS, 272
- queuing disciplines, 277-279
- router elements, 59-60
- SDN
 - controllers, 119-120
 - domains, 137-138

RStudio, 489**RTC (real-time communications) dashboard, 33****Ryu, 115****S****SaaS (Software as a Service), 352**

- defined, 352
- OpenCrowd example SaaS services survey, 352-353
- subscribers, 352

SAL (service abstraction layer), 123**Salesforce cloud computing certification programs, 482****sample metrics, 295****satellite TV end-to-end delivery chain, 301****scalability, 216**

- cloud computing, 50
- NV, 253
- SDN controllers, 133

scheduling

- data flows, 270
- packets, 275

scripting (DevOps), 477**SCTP (Stream Control Transmission Protocol), 100, 342****“SDI Wars: WTF Is Software Defined Center Infrastructure?” website, 263****SDI (software-defined infrastructure), 257**

- applications, 258
- architecture, 261-262
- defined, 257
- features, 258-259
- NFV, 258
- SDN, 258
- SDS, 259-260

SDK API (CM), 419**SDN (software-defined networking), 67**

- API, 83

applications, 85, 145

- applications, 147
- data center networking, 162-168
- ICN, 168-173
- measurement, 157
- mobility/wireless, 168
- monitoring, 157
- network services abstraction layer, 146-152
- northbound interface, 146
- security, 157-162
- traffic engineering, 153-156
- user interface, 147

certification programs, 481

characteristics, 85

cloud computing, 368-371

controllers, 68

- application threats, 439

centralized, 133

distributed, 134

federation, 135

functions, 113-114

HA clusters, 134

IETF SDNi, 140-141

implementing, 84, 115

northbound interfaces, 117-119

OpenDaylight modules, 126

OpenDaylight SDNi, 141-142

PolicyCop application, 155

privacy, 134

QoS management, 138-140

reliability, 133

routing, 119-120

routing between domains, 137-138

scalability, 133

security threats, 439

southbound interfaces, 116-117

control plane, 68, 82, 113

data plane, 68, 82

functions, 93-94

protocols, 95

security threats, 437-439

defined, 67

deployment driving factors, 68-69

domains, 133

functionality, 67

IT/network job position impact, 469-470

ITU-T Y.3300 high-level architecture, 120-121

mobility driving factor, 69

modern networking schema, 72

NFV

relationship, 225-228

similarities, 70

NOS, 114

OpenDaylight architecture, 122

base network service functions, 124

control plane/application plane functionality, 123

flexibility, 123

- Helium, 124
- layers, 122
- modules, 125-127
- SAL, 123
- OpenFlow. *See* OpenFlow
- packet forwarding, 83
- REST
 - API example, 130-132
 - constraints, 128-130
 - defined, 128
- SDI, enabling, 258
- security
 - controllers, 114
 - goals, 157
 - OpenDaylight Defense4All DDoS application, 157-162
 - software-defined, 440
 - threats, 436, 439
- server virtualization, 68
- standards, 85-87
 - industry consortiums, 89
 - open development initiatives, 90
 - SDOs, 87-89
- SDNi (Software-Defined Networking interface), 127**
 - aggregator, 127
 - IETF, 140-141
 - messages, 141
 - OpenDaylight, 141-142
 - wrappers, 127
- SDOs (standards-developing organizations), 87-89**
- SDS (software-defined storage), 259-260**
- SecaaS (Cloud Security as a Service), 453-456**
 - business continuity/disaster recovery, 456
 - data loss prevention, 455
 - encryption, 456
 - IAM, 455
 - intrusion management, 456
 - network security, 456
 - security assessments, 455
 - SIEM, 456
 - Web security, 455
- second generation (2G) cellular networks, 23**
- Secure Network Bootstrapping Infrastructure (SNBi), 125**
- security**
 - AAA
 - authentication filter, 127
 - OpenDaylight, 126
 - big data concerns, 48
 - certification programs, 487
 - Cisco IoT system, 425-426
 - cloud computing, 446
 - architecture, 448
 - auditability, 449
 - availability, 448-449
 - compliance, 447
 - controls, 457
 - data protection, 448, 452-453
 - governance, 447
 - identity/access management, 448
 - incident response, 448
 - Security as a Service, 453-456
 - sharing vendor resources, 449
 - software isolation, 448
 - subscriber protection, 450
 - threats, 449-452
 - trust, 447
 - DDoS
 - Defense4All application, 157-159, 162
 - OpenDaylight, 127
 - e-mail, 455
 - encryption, 23
 - information and event management (SIEM), 456
 - IoT, 458-459
 - framework, 462-464
 - patching vulnerabilities, 459
 - requirements, 459-461
 - services, 375
 - IP (IPsec), 241-243
 - network, 456
 - NFV, 441
 - attack surfaces, 441-444
 - ETSI security perspective, 444-446
 - techniques, 446
 - privacy
 - cloud, 359, 369
 - SDN controllers, 134
 - requirements, 435-436
 - SDN
 - controllers, 114
 - goals, 157
 - OpenDaylight Defense4All DDoS application, 157-162
 - software-defined, 440
 - threats, 436, 439
 - TLS, 438
 - Web, 455
- select group type, 109**
- sensing devices (IoT), 396**
- sensors, 377**
 - accuracy, 379
 - defined, 377
 - interfaces, 377
 - IoT, 29
 - precision, 379
 - resolution, 380
 - technology, 29
 - types, 378-379
- servers**
 - blade, 14
 - centralized farms, 16
 - data management, 46
 - Iotivity, 419

- network management, 47
- virtualization, 68
- services**
 - abstraction layer (SAL), 123
 - actionable QoE, 331
 - class characteristics (traffic), 41
 - cloud
 - CaaS, 355
 - cloud capability types, 356
 - CompaaS, 356
 - DSaaS, 356
 - emerging, 357
 - IaaS, 354-355
 - NaaS, 356
 - PaaS, 353
 - SaaS, 352-353
 - XaaS, 357-358
 - Cloud Security as a Service, 453-456
 - business continuity/disaster recovery, 456
 - data loss prevention, 455
 - encryption, 456
 - IAM, 455
 - intrusion management, 456
 - network security, 456
 - security assessments, 455
 - SIEM, 456
 - Web security, 455
 - differentiated. *See* DiffServ
 - enterprise, 30
 - function chaining (SFC), 126
 - GBP, 126
 - hijacking, 451
 - IoTivity Base, 415-420
 - ISA, 276
 - controlled load, 277
 - guaranteed, 276
 - queuing disciplines, 277-279
 - LISP, 127
 - monitoring
 - categories, 332
 - on-demand, 333
 - probes, 333
 - QoE, 317
 - network
 - NFV, 187
 - SDN application plane abstraction layer, 146-152
 - OpenStack, 126
 - PaaS, 488
 - provider perspective (cloud computing), 369
 - QoE-based management
 - host-centric vertical handover, 341-342
 - network-centric vertical handover, 342-344
 - VoIP calls, 341
 - sectors (IoT)
 - buildings, 377
 - consumer and home, 376
 - energy, 377
 - healthcare/life science, 376
 - industrial, 376
 - IT/networks, 375
 - retail services, 376
 - security/public safety, 375
 - transportation, 376
 - SNBi, 127
 - use cases (NFV), 223-225
 - CDNs, 224
 - fixed access network functions, 225
 - home environments, 224
 - mobile cellular networks, 223
 - RAN equipment, 224
- SFC (service function chaining), 126**
- shaping**
 - DiffServ, 281
 - traffic, 270, 285
- sharing**
 - technology threats, 451
 - vendor resources, 449
- shortest path forwarding, 114**
- SIEM (security information and event management), 456**
- Simple Network Management Protocol (SNMP), 126**
- singleton metrics, 294**
- SIT (system integration testing), 471**
- skills in demand, 488-489**
- SLAs (service level agreements), 272**
 - architecture, 292
 - availability, 292
 - DiffServ, 281
 - features, 291
 - latency, 292
 - reliability, 293
- slave QoE agents, 339**
- smart home data models (CM), 419**
- Smashwords.com, 263**
- SNBi (Secure Network Bootstrapping Infrastructure), 125-127**
- SNMP (Simple Network Management Protocol), 126**
- Soft Sensor Manager, 417**
- software**
 - as a Service. *See* SaaS
 - defined networking. *See* SDN
 - Defined Networking interface. *See* SDNi
 - isolation, 448
 - security, 440
 - storage (SDS), 259-260
- source/target IPv4 addresses in ARP payload field (flow table match fields), 100**
- southbound interfaces, 116-117**
- specialized sensors, 379**
- specification abstraction, 149**
- SSCP (Systems Security Certified Practitioner), 487**

standards

- defined, 85
- developing organizations (SDOs), 87-89
- Ethernet, 14
- IEEE 802.1Q, 237-238
- NFV, 85-87, 186
 - industry consortiums, 89
 - open development initiatives, 90
 - SDOs, 87-89
- open, 85
- QoE projects, 304-305
- QoS. *See* ISA
- SDN, 85-87
 - industry consortiums, 89
 - open development initiatives, 90
 - SDOs, 87-89
- Wi-Fi, 21

stateless constraint (REST), 128**statistics**

- manager
 - OpenDaylight, 124
 - SDN controllers, 114
- metrics, 295
- switch
 - retrieving, 131
 - updating, 132

storage

- big data, 48
- cloud, 350
- IoT, 30
- nodes, 206

stored value systems RFID technology, 387**Stream Control Transmission Protocol (SCTP), 100, 342****subjective assessment (QoE), 312-314****subscriptions**

- manager, 419
- protecting, 450

SuperCloud DevOps related products, 479**switches**

- eswitch, 205
- LAN, 231
- Layer 3, 10
- legacy, 238
- OpenDaylight, 124
- OpenFlow, 96-97
- statistics
 - retrieving, 131
 - updating, 132
- ToR, 17

symmetric messages, 110**system integration testing (SIT), 471****system-oriented actionable QoE, 330****systems engineer certification programs, 486****T****tables****flow**

- actions, 101
- action sets, 102
- entries, 98
- instructions component, 102
- match fields, 99-101
- nesting, 106-107
- pipeline, 102-105
- structure, 98
- group
 - action buckets, 108
 - entries, 107
 - group types, 108-109
 - OpenFlow, 107-109
 - OpenFlow logical switch, 97
 - flow, 106-107
 - group, 107-109

tags (RFID), 389-390

- functionalities, 391-392
- operating frequencies, 391
- readers, 390
- read range, 390
- types, 390

tail drop technique, 271**Taylor & Francis Online website, 431****TCAs (traffic conditioning agreements), 281****TCP**

- congestion control, 267
- flags field (flow table match fields), 101
- source/destination ports (flow table match fields), 100

TCP/IP

- characteristics, 79
- defined, 79

technology development, 373**Telecom Lighthouse website, 229****temperature sensors, 379****templates, 181****things (IoT), 396****Things Manager, 417****ThingSpeak, 428-429****third generation (3G) cellular networks, 24****threats**

- cloud security, 449
 - abuse/nefarious use, 450-452
 - account/service hijacking, 451
 - data loss/leakage, 451
 - malicious insiders, 451
 - shared technology issues, 451
 - unknown risk profiles, 452
 - unsecure interfaces/APIs, 450

- SDN security, 436, 439
 - application plane, 439
 - control plane, 439
 - data plane, 437-439
- three V's (volume, velocity, variability), 48**
- throughput, 40**
- timeouts entry (flow tables), 98**
- Timer object, 339**
- TLS (Transport Layer Security), 437**
 - phases, 438
 - security, 438
 - TCP/IP architecture, 437
- token buckets, 285**
- topology manager**
 - OpenDaylight, 124
 - SDN controllers, 114, 120
- ToR (top-of-rack) switches, 17**
- total elapsed time, 40**
- tracking RFID technology, 387**
- traditional architectures, 79-80**
- traffic**
 - best effort, 267
 - big data, 45
 - analytics, 46
 - areas of concern, 48
 - defined, 45
 - ecosystem example, 46-48
 - infrastructures, 46
 - three V's, 48
 - classification, 269, 285
 - cloud computing, 48
 - core, 50
 - intercloud, 50
 - intracloud, 49
 - OSS, 50
 - requirements, 50
 - virtual machines, 49
 - complex patterns, 78
 - conditioning
 - agreements, 281
 - DiffServ, 281-285
 - congestion. *See* congestion
 - controlling, 271-272
 - droppers, 285
 - engineering, 153-156
 - elastic
 - applications, 39
 - benefits, 40
 - defined, 39
 - delays, 39
 - QoS, 40
 - requirements, 39
 - total elapsed time, 40
 - flows
 - classification, 269
 - policing, 270
 - shaping, 270
 - VTN, 256
- inelastic
 - defined, 40
 - delays, 40
 - internet requirements, 42
 - packet loss, 41
 - QoS requirements, 42
 - requirements, 40
 - service class characteristics, 41
 - throughput, 40
- lower than best effort, 268
- markers, 285
- metering, 272, 285
- mobile, 51
 - categories, 52
 - growth, 52
 - projections, 52
 - wireless users, 52
 - world total, calculating, 51
- packet marking, 270
- policing, 270
- queuing and scheduling, 270
- real-time
 - continuous data sources, 44
 - defined, 43
 - delays, 43
 - illustration, 43
 - on/off sources, 44
 - packet transmission, 44
 - variable-length packets, 44
- recording, 272
- restoration, 272
- shaping, 270, 285
- specification (TSpec), 276
- TCP congestion control, 267
- transceivers, 386**
- transmission technologies, 11**
 - cellular
 - 1G (first generation), 23
 - 2G (second generation), 23
 - 3G (third generation), 24
 - 4G (fourth generation), 24
 - 5G (fifth generation), 25
 - defined, 23
 - Ethernet
 - carrier, 14
 - data centers, 13
 - data rates, 14-19
 - defined, 11
 - enterprise, 13
 - homes, 12
 - metro, 14
 - offices, 12
 - standards, 14
 - WANs, 14
 - Wi-Fi combination, 12

Wi-Fi

- data rates, 21-22
- defined, 19
- enterprise, 20
- homes, 20
- public, 20
- standards, 21

transportation IoT services, 376

Transport Layer Security (TLS), 437-438

trick mode, 302

trust, 447

TSpec (traffic specification), 276

Tunnel IDs field (flow table match fields), 100

tunnels, 245

Type 1/Type 2 hypervisors, 183

U

UAT (user acceptance testing), 471

UC (unified communications), 33

- audio conferencing, 34
- benefits, 36
- convergence, 35
- defined, 33
- elements, 33-35
- instant messaging, 34
- IP enabling contact centers, 35
- mobility, 35
- presence, 35
- RTC dashboard, 33
- unified messaging, 34
- video conferencing, 34
- web conferencing, 34

UDP source/destination ports (flow table match fields), 100

unconstrained devices, 410

unicast addressing, 231

Unified Functional Testing, 489

unified messaging, 34

uniform interfaces, 129

uniform resource identifiers (URIs), 129

unknown risk profiles, 452

update action set instructions, 102

update metadata instructions, 102

updating switch statistics, 132

URIs (uniform resource identifiers), 129

use cases (NFV), 221

- architectural, 222-223
- service-oriented, 223-225
 - CDNs, 224
 - fixed access network functions, 225
 - home environments, 224
 - mobile cellular networks, 223
 - RAN equipment, 224

user acceptance testing (UAT), 471

users

- defined, 5
- experience. *See* QoE
- interface, 147
- wireless, 52

V

variability, 48

variable-length packets, 44

VCA-DCV (VMware Certified Associate—Data Center Virtualization), 483

VCAP5-DCA (VMware Certified Advanced Professional 5—Data Center Administration), 483

VCAP5-DCD (VMware Certified Advanced Professional 5—Data Center Design), 484

VCDX5-DCV (VMware Certified Design Expert 5—Data Center Virtualization), 484

VCP5-DCV (VMware Certified Professional 5—Data Center Virtualization), 483

VCP-NV (VMware Certified Professional—Network Virtualization) certification, 481

VCs (virtual channels), 245

velocity, 48

version control systems, 477

video

- conferencing, 34
- content delivery
 - online, 302-303
 - satellite TV end-to-end delivery chain, 301
- on demand, 17
- Quality Experts Group (VQEG), 305
- services QoE/QoS mapping models, 327-329

VIDs (VLAN identifiers), 237

VIM (virtualized infrastructure management), 217-218

virtual channels (VCs), 245

virtual local-area networks. *See* VLANs

virtual machine monitors (VMMs), 179-180, 183

virtual machines. *See* VMs

virtual network platform as a service (VNPaaS), 223

virtual private networks. *See* VPNs

Virtual Tenant Network. *See* VTN

virtualization

- background, 178
- CDNs, 224
- certification programs, 481-483
- container, 183
- defined, 177
- fixed access network functions, 225
- hardware, 178
- home environments, 224
- IND, 210
- infrastructure management, 217-218
- network
 - agility, 253
 - architecture, 250-252

- benefits, 252
- capital cost savings, 253
- defined, 247
- equipment consolidation, 253
- example, 248-249
- flexibility, 253
- function manager, 218
- infrastructure-based, 212
- L2 versus L3, 210-211
- levels of abstraction, 248
- logical resources, 247
- NFV, 187
- NFVI alternatives, 211
- operational cost savings, 253
- physical resources, 247
- rapid service provisioning, 253
- scalability, 253
- virtual overlay, 212
- virtual resources, 247
- NFV. *See* NFV
- partitioning, 212
- resources, 247
- SDI
 - applications, 258
 - architecture, 261-262
 - defined, 257
 - features, 258-259
 - NFV, 258
 - SDN, 258
 - SDS, 259-260
- servers, 68
- VLANs
 - configuration, 234
 - defined, 234
 - IEEE 802.1Q standard, 237-238
 - membership, 235-236
 - nesting, 239
 - OpenFlow support, 240
- VMs
 - architectures, 180-183
 - CloudNaaS, 166
 - container virtualization, 183
 - defined, 178, 187
 - files, 181
 - templates, 181
 - Type 1/Type 2 hypervisors, 183
 - VMMs, 179-180
- VNFs, 187, 213
 - catalog, 219
 - components (VNFCs), 213-216
 - forwarding graphs, 187, 223
 - interfaces, 213-214
 - manager (VNFM), 218
 - potential functions, 213
 - scaling, 216
 - sets, 187
 - VNFC to VNFC communication, 215-216
- VPNs, 241
 - defined, 241
 - IPsec, 241-243
 - MPLS, 243-247
- VTN, 127, 253-257
 - architecture, 257
 - controllers, 127
 - Coordinator, 254
 - elements, 254
 - flows, 256
 - Manager, 254
 - mapping, 255
- virtualized network function. *See* VNFs**
- VLANs (virtual local-area networks), 234**
 - configuration, 234
 - defined, 234
 - ID/VLAN user priority fields (flow table match fields), 100
 - identifiers (VIDs), 237
 - IEEE 802.1Q standard, 237-238
 - membership,
 - communicating, 236
 - defining, 235
 - nesting, 239
 - OpenFlow support, 240
- VMMs (virtual machine monitors), 179-180, 183**
- VMs (virtual machines), 178**
 - architectures, 180-183
 - CloudNaaS, 166
 - container virtualization, 183
 - defined, 49, 178, 187
 - files, 181
 - templates, 181
 - Type 1/Type 2 hypervisors, 183
 - VMMs, 179-180
- VMware Certified Advanced Professional 5—Data Center Administration (VCAP5-DCA), 483**
- VMware Certified Advanced Professional — Data Center Design (VCAP5-DCD), 484**
- VMware Certified Associate—Data Center Virtualization (VCA-DCV), 483**
- VMware Certified Design Expert 5—Data Center Virtualization (VCDX5-DCV), 484**
- VMware Certified Professional 5—Data Center Virtualization (VCP5-DCV), 483**
- VMware Certified Professional—Network Virtualization (VCP-NV) certification, 481**
- VNF (virtualized network functions), 187, 213**
 - catalog, 219
 - components, 213-216
 - forwarding graphs, 223
 - interfaces, 213-214
 - manager (VNFM), 218
 - potential functions, 213
 - scaling, 216
 - sets, 187
 - VNFC to VNFC communication, 215-216

VNF FG (VNF forwarding graph), 187, 223
VNFaaS (VNF as a Service), 222
VNFCs (VNF components), 213-216
VNFM (virtual network function manager), 218
VNFPaaS (virtual network platform as a service), 223
VoIP calls, 341
VPNs (virtual private networks), 241
 defined, 241
 IPsec, 241, 243
 MPLS, 243-247
 Layer 2, 245-246
 Layer 3, 246
VQEG (Video Quality Experts Group), 305
VTN (Virtual Tenant Network), 127, 253-257
 architecture, 257
 controllers, 127
 Coordinator, 254
 elements, 254
 flows, 256
 Manager, 254
 mapping, 255

W

WANs (wide-area networks), 14
waterfall development, 471
WDM (wavelength-division multiplexing), 8
web
 conferencing, 34
 security, 455
websites
 ACM Career Resources, 489
 “Bandwidth Needs in Core and Aggregation Nodes
 in the Optical Transport Network,” 37
 Career Overview, 490
 Cisco Systems Internetworking Technology Hand-
 book, 299
 CoAP, 411
 Computer Jobs, 490
 Computer Science Student Resources, 490
 ComputerWorld IT Topic Center, 490
 DICE, 490
 IBM Study “Every Day We Create 2.5 Quintillion
 Bytes of Data” website, 73

IEEE, 490
 Inter-SDN Controller Communication: Using Border
 Gateway Protocol, 143
 ioBridge, 427
 IoTivity, 409
 IoT World Forum, 401, 431
 IT career resources, 489-490
 Kemp Technologies blog “SDN is from Mars, NFV
 is from Venus,” 229
 Linux Foundation, 409
 OIC, 409
 OpenCrowd example SaaS services survey, 352-353
 RealTime.io, 430
 “SDI Wars: WTF Is Software Defined Center
 Infrastructure?,” 263
 Smashwords.com, 263
 Taylor & Francis Online, 431
 Telecom Lighthouse, 229
 ThingSpeak, 428
weighted RED (WRED), 271
WFQ (weighted fair queuing), 279
wide-area networks (WANs), 14
Wi-Fi

 data rates, 21-22
 defined, 19
 enterprise, 20
 Ethernet combination, 12
 homes, 20
 mobile traffic, 52
 public, 20
 SDN applications, 168
 standards, 21

Wi-Fi Alliance, 21
workstations, 46
world total mobile traffic, 51
wrappers
 ICN, 171
 OpenDaylight SDNi, 142
WRED (weighted RED), 271

X – Z

XaaS (X as a Service), 357-358
Xamarin, 489