CompTIA Network+ Certification Guide (Exam N10-009)

Unleash your full potential as a network administrator

2nd Edition

Eithne Hogan

www.bpbonline.com

Second Revised and Updated Edition 2025

First Edition 2023

Copyright © BPB Publications, India

ISBN: 978-93-65892-673

All Rights Reserved. No part of this publication may be reproduced, distributed or transmitted in any form or by any means or stored in a database or retrieval system, without the prior written permission of the publisher with the exception to the program listings which may be entered, stored and executed in a computer system, but they can not be reproduced by the means of publication, photocopy, recording, or by any electronic and mechanical means.

LIMITS OF LIABILITY AND DISCLAIMER OF WARRANTY

The information contained in this book is true and correct to the best of author's and publisher's knowledge. The author has made every effort to ensure the accuracy of these publications, but the publisher cannot be held responsible for any loss or damage arising from any information in this book.

All trademarks referred to in the book are acknowledged as properties of their respective owners but BPB Publications cannot guarantee the accuracy of this information.

To View Complete
BPB Publications Catalogue
Scan the QR Code:

www.bpbonline.com

Dedicated to

My beloved children:
Samantha**, **Patrick**, **Lesleyanne**, **Kathryn**, **Chelsea** and **Dylan
and
The best and most beautiful grandchildren:
Devin**, **Alannah**, **Frankie**, **Kara**, **Tyler** and **Joshua

About the Author

With just under 30 years of experience in education, **Eithne Hogan** has held a wide variety of roles. She currently coordinates the Datacenter Academy Program at her college, a program supported by Microsoft. Thanks to this partnership, the college boasts a fully functional three-rack mini datacenter lab, established in November 2019, to teach aspiring technicians about datacenter technologies, IT support, cybersecurity, network and server administration.

Eithne not only coordinates and instructs this program but also oversees the traineeship. Her college is an active member of the Microsoft Global Datacenter Academy Community, a community that is evolving and expanding across the globe. Eithne is a spokesperson and representative leader for her academy.

In addition to her primary role, Eithne is a part-time lecturer at other national higher education professional academies, where she teaches several CompTIA certification courses to include the A+, Network+, and Server+. She also manages the college's local Cisco Network Academy, holding certificates of recognition for Instructor Excellence and thirteen years of active service and participation. The CompTIA Academy partnership, which Eithne oversees, has been operational at the college for 25 years.

Eithne has developed nationally recognized curricula in IT, covering topics such as network infrastructure, network topologies, network administration, and switching, routing, and wireless technologies. As the digital lead for the community college, she collaborates with her colleagues to drive the transformation to digital teaching and learning practices.

About the Reviewer

Simone Bertulli is a cybersecurity professional, currently holding a senior position at the Cyber Defense Center of a leading Italian company.

He has over 15 years of experience in the IT field, with deep expertise in enterprise-class infrastructure technologies, holding certifications such as CompTIA Network+, CompTIA Security+, CompTIA Cloud+, CompTIA Storage+, CompTIA Linux+, and LPIC-3 Virtualization and High Availability.

A passionate advocate of open-source, he actively contributes to the community by writing for the Linux Professional Institute blog and delivering tech talks on FOSS-related topics, both from a technical perspective and in the field of professional training. Simone is also an official Linux Professional Institute Instructor, further strengthening his commitment to fostering open knowledge and supporting IT professionals in their career development.

Acknowledgement

I want to extend my heartfelt thanks to my family and friends for their unwavering support and encouragement throughout the writing of this book. A special mention goes to my children and grandchildren, who bring immense meaning to everything I do.

My gratitude also goes to BPB Publications for their invaluable guidance and expertise. The journey of reviewing and revising this book was long and challenging, but the collaboration with reviewers, technical experts, and editors made it a rewarding experience.

I am immensely grateful to my colleagues and the IT professionals I've had the privilege to work with over the years. Your collective wisdom, experiences, and rigorous training have been instrumental in guiding me through the rewards and challenges of this learning journey. A special mention goes to Janet Allen and Derek Haughton; your unparalleled skills and expertise in technology have been invaluable to me. Thank you.

Lastly, I want to thank all the readers who have shown interest in my book. Your support has been crucial in bringing this project to life. I hope you find the contents enriching and enjoy the learning journey as much as I have. Happy reading!

Preface

Network design and implementation are driven by organizational needs and changes. Network administrators possess a broad range of knowledge, including network planning and design, network infrastructure, network operations, security evaluation, and the ability to assess network capacity and performance. In a world where high availability and continuity of service are paramount, network administrators are the backbone of a company's assets.

The revamped Network+ exam addresses the evolving landscape of IT networking, focusing on the most sought-after skills to meet contemporary challenges, network optimization, hybrid infrastructures, and more. With Network+, candidates will gain the essential abilities needed to excel in their roles and attract potential employers. Network+ serves as the foundation for a rewarding career, making it the preferred choice for foundational networking skills across various job roles in the industry.

This book is designed to provide a comprehensive guide to the role and duties of a network administrator. While it prepares the reader for the CompTIA Network+ exam, it goes beyond that. This guide thoroughly equips readers with specific networking skills, setting them on a path toward a valuable career in technical support and IT operations. Readers will acquire the skills to install, configure, maintain, and monitor network hardware and software, and effectively use troubleshooting tools. The content also emphasizes the importance of security in network operations. This book is intended for anyone interested in pursuing a rewarding career in network administration. I hope you find it informative and helpful.

Second edition updates: The second edition includes new content reflecting changes in the exam, such as evolving use cases for modern networks, important factors of physical installations, and additional details on implementing IPv4 and IPv6 network services.

Chapter 1: OSI Model - The chapter emphasizes the importance of standards in the IT industry. It explores the origins and development of the OSI model, detailing how its seven layers decompose the essential concepts of networking functions and processes. Additionally, the chapter provides an overview and explanation of each individual layer, describing their roles in data transmission. It thoroughly explains the processes of encapsulation and decapsulation as data moves across networks. Through detailed descriptions and illustrations, the chapter guides the reader through the OSI model layers, enhancing their understanding of network fundamentals.

Chapter 2: Network Topologies - The chapter provides a comprehensive overview of network topologies, complete with illustrations for each type. It distinguishes between physical and logical topologies, explaining their differences. Additionally, the chapter delves into the functioning of virtual networks and highlights the crucial role of hypervisors. It emphasizes the importance of understanding virtualization in the modern networking landscape.

Furthermore, the chapter covers various network types, including PAN, LAN, CAN, MAN, WLAN, and WAN. This edition provides additional details on **software-defined networks** (**SDN**) and **software-defined wide area networks** (**SD-WAN**), noting that these networks are application-aware, feature zero-touch provisioning, are transport agnostic, and have central policy management.

Chapter 3: Cables and Connectors - The chapter discusses the cables and connectors utilized in Ethernet, coax, and fiber networks. It illustrates the appropriate cable types and corresponding connectors for various network applications, specifying each cable's intended use. Readers learn the distinctions between wired and wireless networks and receive step-by-step guidance on constructing straight-through or crossover cables according to proper wiring standards. Additionally, the chapter covers best practices for effective cable management.

Chapter 4: IP Addressing and Subnetting - The chapter permits the reader to learn the fundamental concepts of IP addressing. The chapter covers IPv4 and IPv6 addressing structures, the transition to IPv6 and explains how the transition is taking place. Furthermore, the reader is shown how to subnet and apply best practices in creating network subnets. The chapter includes hands-on subnetting practice. IP addressing makes devices accessible for communication. As such, the chapter includes practical examples based on real scenarios. This chapter helps the reader to solve real addressing problems and provides an easy mechanism to identify addressing schemes in networks. The chapter and second edition extends understanding on how to implement IPv4 and IPv6 network services.

Chapter 5: Ports and Protocols - The chapter educates readers on the protocols within the TCP/IP suite. As the only routable protocol, TCP/IP is essential for data transmission across all network types, both locally and globally, wherever packets need to be sent and received. The chapter details port numbers and explains their relevance to understanding functionality and security practices. It also provides guidance on which protocols might be blocked by firewalls unless specifically required.

Chapter 6: Implementing and Troubleshooting Network Services - The chapter shows core concepts of networking services. The reader is walked through a typical installation of a role-based feature in Windows Server 2019. The reader is shown how to install and configure DHCP and DNS on a server operating system. This chapter also offers a detailed description of NTP as an important network service.

Chapter 7: Data Center Technologies - The chapter provides detailed explanations and numerous illustrations on the operation of datacenter technologies. It focuses on datacenter architecture, storage solutions, and RAID. Practical examples of RAID implementations for various scenarios are covered, demonstrating the best practices for specific use cases.

Chapter 8: Cloud Concepts - The chapter is aimed to give the reader more familiarity with cloud computing, deployment models and service models. This chapter covers real-world examples of cloud provision and allows the reader to comprehend the appropriate services suited to the needs of an organization. In essence, the chapter informs the reader and permits them to identify and make good choices, when discussing or selecting online services with colleagues or other stakeholders.

Chapter 9: Managing Network Devices - The chapter is a detailed description of network devices and how they are mapped to the layers of the OSI model. The chapter is intended to demonstrate the functionality and purpose of the device in order to enable the reader to identify which device is necessary for a specific job role on the network. Furthermore, the chapter describes how the device operates and shows the reader what to watch out for to ensure the device is optimally suited for its role. The chapter emphasizes how to ensure network performance, integrity and resilience to maintain the expected service levels and maximize bandwidth.

Chapter 10: Managing Switching Protocols - The chapter takes a deeper dive into switching technologies and protocols such as STP and ARP. The chapter focuses on how switches make decisions, and how they learn and build their MAC table. The chapter permits the reader to comprehend switching functionality in order to evaluate, diagnose and troubleshoot switches on a network. Additionally, the chapter introduces the concept of VLANs, explains switch segmentation and shows the reader how to make decisions about the presence of VLANs in their companies. The chapter also shows the reader how and when to implement port security.

Chapter 11: Managing Routing Protocols - The chapter takes a deeper dive into routing technologies and protocols such as OSPF, EIGRP, and BGP. The chapter focuses on how routers make decisions, and how they learn and build their routing table. The chapter permits the reader to comprehend routing functionality in order to evaluate, diagnose and

troubleshoot routers on a network. Additionally, the chapter introduces the concept of subnets, explains router segmentation and shows the reader how to make decisions about the presence of subnets in their companies. The chapter also shows the reader how and when to implement static or dynamic routing and how to competently manage network bandwidth.

Chapter 12: Installing and Configuring Wireless Technologies - The chapter allows the reader to differentiate between IEEE 802.11 standards. The chapter provides detail on each of these standards, the frequency bands in use and configuration options per standard. Furthermore, the chapter also walks the reader through the steps to configure a SOHO router, adhering to best practices and optimum security measures.

Chapter 13: Managing and Monitoring a Network - The chapter outlines Windows integrated tools and free open source software, used to manage and monitor networks. The chapter's primary intention is to permit the reader to apply this knowledge in a practical way and show them how to use integrated or third-party tools to troubleshoot a system. The chapter offers examples of ways to assess network performance and provides mechanisms to narrow down relevant issues that negatively impact network operation.

Chapter 14: Policies and Procedures in Practice - The chapter emphasizes the practicalities of running a business or organization, focusing on required documentation and the negotiation needed for effective corporate network management. It highlights the importance of planning, designing, and reviewing policies and procedures as part of the organization's change management ethos. Additionally, it provides recommendations for being positive collaborators in IT and business operations.

The chapter also covers physical installations with guidance on the installation and maintenance of network equipment. It explains how to consider optimal locations (e.g., IDF, MDF), select the appropriate rack size, manage port-side exhaust/intake for cooling, organize cabling with patch and fiber distribution panels, ensure lockable components for security, and address power needs using UPS, PDU, power load, and voltage requirements. Furthermore, it details accounting for environmental factors such as temperature and humidity.

Chapter 15: Resilience, Fault Tolerance, and Recovery - The chapter offers a detailed description of backup and failover strategies and demonstrates where these strategies fit in with high availability planning and with a Disaster Recovery Plan. Furthermore, the chapter shows the reader how to implement RAID and explains which failover strategy suits a given scenario. This chapter covers practical examples of working with recovery strategies.

Chapter 16: Security Concepts - The chapter introduces the reader to common security concepts. The chapter lays the foundations for further topics covered in the upcoming chapters. Additionally, the chapter shows the user ways to safeguard users on a network and how to mitigate internal and external threats, thereby protecting the network users' privacy and data.

Chapter 17: Cybersecurity Attacks - The chapter extends on the concepts of the previous chapter and offers a detailed description of vulnerabilities, threats and attacks. This chapter shows the reader how to mitigate threats and demonstrates strategies for eliminating vulnerabilities and loopholes on the network. The chapter provides practical examples of real-world technology-based attacks and social engineering attacks and offers advice on how to counter these risks and threats.

Chapter 18: Network Hardening Techniques - The chapter covers practical techniques related to securing and hardening a network. Furthermore, the chapter also allows the reader learn and apply the strategies to manage workstations, monitor network devices, secure hardware and software, and educate users to ensure best practices while accessing the organization's network resources. The chapter covers network management policies and protocols such as password complexity, multi-factor authentication, SMNP and Syslog among others.

Chapter 19: Remote Management - The chapter shows core concepts of remote management procedures and provides practical examples and remote management connectivity options to the reader. The chapter includes practical examples and case use scenarios for diverse VPN configurations. The chapter covers remote desktop connectivity options and explains to the reader the context of their use, emphasising security implications. Additionally, this chapter provides the reader with a step-by-step guide to configuring an RDP gateway on a Windows server.

Chapter 20: Implementing Physical Security - The chapter focuses on the objectives of physical security controls and shows the reader effective security methods to be used, and how to implement these methods on networks. Furthermore, the chapter also instils in the reader the relevance of prevention measures and demonstrates proactive actions used by network administrators to optimize security procedures and protocols running on the network. These procedures includes perimeter security of the building itself and includes the concept of security zones.

Chapter 21: Network Troubleshooting - The chapter gives special attention to the network troubleshooting model. The chapter goes through the steps of the troubleshooting model and presents the reader with tips and tools for handing each step with proficiency. This chapter encourages the reader to follow this model and methodology and consequently

become equipped with the cognitive awareness required for a job role in administering networks.

Chapter 22: Troubleshooting Cable Connectivity - The chapter covers the skills and competences required to troubleshoot cable connectivity. The chapter presents bounded media as the fundamental backbone of wired networks and shows the reader how to visually inspect cables and LEDs in Ethernet and fiber networks. Furthermore, the chapter shows the reader how to use hardware tools to diagnose and troubleshoot defective or incorrectly chosen cabling.

Chapter 23: Network Utilities - The chapter covers network software tools as used in command line interface and Cisco's IOS. The chapter offers real-world examples of problems that occur on networks where these tools are invaluable. Furthermore, the reader is shown how to use a wide variety of tools and is given practical case uses for each tool presented. The chapter demonstrates a range of third-party software tools and CLI commands, and explains how to use each tool and identify the correct purpose of its use.

Chapter 24: Troubleshooting Wireless Networks - The chapter presents a detailed overview of the infrastructure of wireless networks. Additionally, the chapter focuses on wireless deployments, standards and limitations, common issues and solutions and other common checks and tests. The chapter encourages the reader to follow troubleshooting methods to work through and resolve the issues that arise in wireless networks and at all times incorporate the learning of network models, such as the OSI model and the network troubleshooting model.

Chapter 25 Troubleshooting General Networking Issues - The chapter covers the common considerations applicable to general networking issues. The chapter provides the reader with comprehensive detail on common issues and shows the reader how to incorporate knowledge of the OSI model, when resolving network issues. Furthermore, the chapter also maps network problems to the relevant layer of the OSI model and offers the reader ways to manage problem-solving. This chapter brings the learning full cycle and permits the reader to apply the OSI model in a practical way, using it as a tool and guide in network repair.

Chapter 26: Network+ Practice Exams - The chapter provides the reader with practice multiple choice questions. The questions are aligned with the domains of the Network+, as outlined in CompTIA's official exam objectives.

Coloured Images

Please follow the link to download the
Coloured Images of the book:

https://rebrand.ly/kviekfn

We have code bundles from our rich catalogue of books and videos available at **https://github.com/bpbpublications**. Check them out!

Errata

We take immense pride in our work at BPB Publications and follow best practices to ensure the accuracy of our content to provide with an indulging reading experience to our subscribers. Our readers are our mirrors, and we use their inputs to reflect and improve upon human errors, if any, that may have occurred during the publishing processes involved. To let us maintain the quality and help us reach out to any readers who might be having difficulties due to any unforeseen errors, please write to us at :

errata@bpbonline.com

Your support, suggestions and feedbacks are highly appreciated by the BPB Publications' Family.

Did you know that BPB offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at www.bpbonline.com and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at :

business@bpbonline.com for more details.

At **www.bpbonline.com**, you can also read a collection of free technical articles, sign up for a range of free newsletters, and receive exclusive discounts and offers on BPB books and eBooks.

Piracy

If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at **business@bpbonline.com** with a link to the material.

If you are interested in becoming an author

If there is a topic that you have expertise in, and you are interested in either writing or contributing to a book, please visit **www.bpbonline.com**. We have worked with thousands of developers and tech professionals, just like you, to help them share their insights with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions. We at BPB can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about BPB, please visit **www.bpbonline.com**.

Join our book's Discord space

Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

https://discord.bpbonline.com

Table of Contents

1. OSI Model 1
Introduction 1
Structure 1
Objectives 2
Need for standards 2
Standards versus protocols 2
Evolution of the OSI model 3
Protocol data units 5
Bit 6
Frame 7
Packet 8
Segment 8
Analogy for data transmission 8
Seven layers of the OSI model 9
Physical layer 9
Modes of communication 10
Data link layer 12
Network layer 13
Transport layer 15
Scenario 15
Session layer 16
Presentation layer 17
Application layer 18
Data encapsulation and decapsulation 19
Defining data encapsulation 20
Data flow and encapsulation 20
Stages of data flow 21
Decapsulation 23
Conclusion 24
Points to remember 24

Key terms 25
Questions 26

2. Network Topologies 27
Introduction 27
Structure 27
Objectives 28
Physical versus logical topologies 28
Physical topologies 29
Bus topology 29
Star topology 31
Ring topology 34
Mesh topology 36
Hybrid topology 39
Tree topology 40
Logical topologies 41
Logical bus 41
Logical ring 41
Network types 42
Personal area network 42
Local area network 43
Campus area network 43
Metropolitan area network 43
Wide area networks 44
WLAN 44
Virtual network concepts 45
Hypervisors 46
Conclusion 47
Points to remember 48
Key terms 49
Questions 49

3. Cables and Connectors 51
Introduction 51
Structure 52
Objectives 52
Copper 52
Unshielded twisted pair 52
Shielded twisted pair 55
UTP cable types 57
Maximum lengths of cable 58
Ethernet cable color code standards 60
T-568a straight-through Ethernet cable 60
Rj-45 crossover Ethernet cable 61
Ethernet cable instructions 62
Basic theory 63
UTP testing parameters 63
Coaxial cable 64
Coaxial cable types 64
Cable structure 64
Coax connector types 65
Fiber 66
Types of fiber media 67
Light sources 68
Fiber optic cable types and distance 69
Fiber connector types 70
Transceiver types 71
Conclusion 71
Points to remember 72
Key terms 72
Questions 74

4. IP Addressing and Subnetting 75
Introduction 75
Structure 76
Objectives 76
IP addressing 77
Understanding the significance of IP addressing through an analogy 78
Structure of IP addresses 80
IPv4 addressing 82
Binary bit position and value 82
Subnet mask 84
Private vs. public addresses 85
IPv4 reserved addresses 86
Private address space 87
Classless inter-domain routing 90
Variable Length Subnet Masking 92
Sample VLSM scenario 92
Benefits of VLSM 97
Discovering a network ID using the bitwise AND operation 98
Comparing IPv4 and IPv6 address structures 99
IPV6 addressing 99
Assigning IPv6 addresses 101
IPv4 and IPv6 coexistence and migration techniques 102
Subnetting with IPv6 103
Conclusion 104
Points to remember 104
Key terms 104
Answers to VLSM/subnetting questions 105
Questions 106

5. Ports and Protocols 107
Introduction 107
Structure 108
Objectives 108

TCP/IP protocol suite 108
Ports and protocols 111
Port assignment 112
Charts of ports and protocols 112
Internet layer protocols 113
Transport layer protocols 115
Application layer protocols 116
Conclusion 120
Points to remember 121
Key terms 121
Questions 122

6. Implementing and Troubleshooting Network Services 123
Introduction 123
Structure 124
Objectives 124
Dynamic Host Configuration Protocol 124
Implementing and configuring DHCP 126
Installing the DHCP server role 127
Configuring DHCP 133
Domain Name Service 139
Working of DNS 139
Network Time Protocol 142
Stratum 142
Conclusion 143
Points to remember 144
Key terms 144
Questions 145

7. Data Center Technologies 147
Introduction 147
Structure 148
Objectives 148
Data center network architecture 148

Tiered network architecture *149*
Software-defined networking 151
Spine and leaf *151*
Traffic flows *152*
Storage area networks 153
Fault tolerance and redundancy 154
Conclusion 154
Points to remember 155
Key terms 155
Questions 155

8. Cloud Concepts 157
Introduction 157
Structure 158
Objectives 158
Deployment models 158
Public cloud *159*
Private cloud *159*
Hybrid cloud *160*
Community cloud *160*
Service models 161
Software as a service *161*
Infrastructure as a service *162*
Platform as a service *163*
Desktop as a service *164*
User-managed vs. provider-managed service models *165*
Connectivity options 166
Virtual private network *166*
Private-direct connection to the cloud provider *167*
Multitenancy *167*
Use cases for modern network environments 168
Software-defined wide area network *168*
Software-defined wide area network in practice *169*

Infrastructure as code *170*
Branching strategies *171*
Conclusion 172
Points to remember 172
Key terms 173
Questions 174

9. Managing Network Devices 175
Introduction 175
Structure 176
Objectives 176
Networking devices 176
Network segments *177*
Repeater *178*
Hub *178*
Network interface card *179*
Layer 2 switch *179*
Bridge *181*
Access point *181*
Router *182*
Layer 3 capable switch/multilayer switch *183*
Firewall *184*
Voice gateway *184*
Load balancer *185*
Media converter *185*
Wireless LAN controller *186*
Cable modem *186*
Digital subscriber line modem *186*
Other network devices *187*
Networked devices 187
Internet of Things *187*
Conclusion 188
Points to remember 188

Key terms 189
Questions 189

10. Managing Switching Protocols 191
Introduction 191
Structure 192
Objectives 192
Operations and functions of a switch 192
Virtual local area networks 193
Access ports and trunk ports 196
Voice VLANs 197
Port security 199
Secure MAC address types 199
Port violation 200
Other protocols 200
Link aggregation 200
Spanning tree protocol 202
Other STP considerations 204
Address resolution protocol 204
Conclusion 206
Points to remember 206
Key terms 207
Questions 207

11. Managing Routing Protocols 209
Introduction 209
Structure 210
Objectives 210
Primary functions and features of a router 210
Router interfaces 211
Routing table 212
Interconnecting networks 215
Static and dynamic routing 217
Static routes 217

Benefits of static routing *217*
Drawbacks and limitations of static routing *218*
Dynamic routes *219*
Routing Information Protocol *219*
Interior Gateway Routing Protocol *220*
Open Shortest Pathway First *220*
Intermediate System to Intermediate System *222*
Border Gateway Protocol *222*
Administrative distance *222*
Benefits of dynamic routing *223*
Drawbacks and limitations of dynamic routing *223*
Bandwidth management 224
Conclusion 224
Points to remember 225
Key terms 225
Questions 226

12. Installing and Configuring Wireless Technologies 227
Introduction 227
Structure 228
Objectives 228
Benefits of wireless technologies 228
Wireless standards 229
Channels and frequency bands 230
Historical context *231*
2.4 GHz frequency band *233*
5 GHz frequency band *234*
Channel bonding *235*
Modulation techniques *235*
Examples of wireless deployments *237*
Autonomous AP vs. central switching *239*
Wireless topology modes *241*
Antenna types *241*

Wireless identification *243*
Cellular technologies *243*
Multiple-Input and Multiple-Output *244*
Configuring a SOHO router 244
Conclusion 250
Points to remember 251
Key terms 252
Questions 252

13. Managing and Monitoring a Network 253
Introduction 253
Structure 254
Objectives 254
Performance metrics and sensors 254
Performance Monitor on a Windows 10 System *255*
Network availability monitoring *259*
Open-source network monitoring tools 260
Simple network management protocol *261*
Network device logs *263*
System logs 264
Syslog *265*
Open-source Syslog Servers *266*
Environmental factors and sensors *269*
NetFlow data *270*
Conclusion 271
Points to remember 272
Key terms 273
Questions 273

14. Policies and Procedures in Practice 275
Introduction 275
Structure 276
Objectives 276
Plans and procedures 276

Change management 277
Incident response plan 278
Disaster recovery plan 280
Business continuity plan 281
System lifecycle *283*
Standard operating procedures 284
Policy compliance 285
Hardening and security policies *285*
Common documentation 286
Important factors of physical installations 287
Hot Aisle/Cold Aisle layout 288
Main distribution frame vs. intermediate distribution frame 288
Sensors 289
Common agreements *289*
Non-disclosure agreement *289*
Service-level agreement *290*
Memorandum of understanding *290*
Conclusion 291
Points to remember 291
Key terms 292
Questions 292

15. Resilience, Fault Tolerance, and Recovery 293
Introduction 293
Structure 294
Objectives 294
Redundancy of hardware and software strategies 294
Load balancing *295*
Multipathing *296*
Network interface card teaming *298*
Implementations of RAID 299
Redundant hardware/clusters *304*
Facilities and infrastructure support *304*

Redundancy and high availability concepts *305*
Network device backup/restore *306*
Conclusion 307
Points to remember 308
Key terms 308
Questions 309

16. Security Concepts 311
Introduction 311
Structure 312
Objectives 312
Confidentiality, integrity, and availability 312
Threats 313
Common vulnerabilities and exposures *315*
Principle of least privilege 316
Zero Trust model 317
Zero Trust through network segmentation *317*
Zero-day *318*
Defense in depth 319
Authentication methods 321
Two-factor (2FA)/multifactor authentication *321*
Risk management 322
Security information and event management 323
Conclusion 323
Points to remember 324
Key terms 324
Questions 326

17. Cybersecurity Attacks 327
Introduction 327
Structure 327
Objectives 328
Technology-based attacks 328
OSI model and cyber-attack examples *328*

Layer 1: The physical layer *329*
Layer 2: The datalink layer *330*
Layer 3: The network layer *331*
Layer 4: The transport layer *333*
Layers 5, 6, and 7: The session, presentation, and application layers *334*
Cyber-attacks *334*
Man-in-the-Middle attack *335*
Malware *335*
Social engineering 336
Case studies 338
Questions *339*
Conclusion 341
Points to remember 341
Key terms 341
Questions 343

18. Network Hardening Techniques 345
Introduction 345
Structure 346
Objectives 346
Securing a workstation 346
Techniques to secure a network 348
Access control lists *348*
Example of ACLs *349*
Router advertisement guard *350*
ARP inspection *351*
Dynamic ARP Inspection best practice *351*
DHCP snooping *352*
VLAN security considerations *352*
Secure SNMP *354*
Wireless security *358*
Wireless encryption protocols *359*
Plan, Plan, Plan *362*

Wireless access point security measures *363*
Best practices of WLAN attack countermeasures 363
Wireless intrusion detection/prevention systems *363*
Penetration testing *364*
Vulnerability scanning *365*
Internet of Things security considerations 365
IoT weaknesses *366*
Best security practices of IoT *366*
Conclusion 368
Points to remember 368
Key terms 369
Questions 369

19. Remote Management 371
Introduction 371
Structure 372
Objectives 372
Virtual private network 372
Site-to-site VPN *374*
Client-to-site VPN *375*
Clientless VPN *376*
Split tunnel and full tunnel configuration *378*
Split tunneling case use an example *378*
Remote desktop connection 379
Remote desktop protocol *381*
RDP: Security considerations *382*
Remote Desktop Gateway 383
Configuring an RDP Gateway on a Windows server *383*
Configuration of remote desktop gateway *384*
Configuring remote desktop gateway servers/settings *386*
Creating computer groups *388*
Virtual network computing 390
Virtual desktop *390*

Authentication and authorization considerations 391
Remote Authentication Dial-In User Service *391*
Terminal Access Controller Access-Control System Plus *393*
In-band vs. out-of-band management 394
Telnet/Secure Shell *396*
Conclusion 396
Points to remember 396
Key terms 397
Questions 397

20. Implementing Physical Security 399
Introduction 399
Structure 400
Objectives 400
Physical security controls 400
Deter *401*
Detect *402*
Delay *403*
Respond *404*
Recover *405*
Detection methods 405
Asset tags *405*
Alarms *406*
Configuration management 406
Prevention methods 407
Biometrics *407*
Locking racks *408*
Security zones *409*
Employee training *409*
Asset disposal *410*
Sanitize devices for disposal *411*
Factory reset/wipe configuration *412*
Conclusion 413

Points to remember 414
Key terms 414
Questions 414

21. Network Troubleshooting 415
Introduction 415
Structure 416
Objectives 416
Stages of troubleshooting 416
First step 417
Gather information about the problem 417
Question the users: The value of effective questioning 418
Second step 420
Third step 422
Fourth step 423
Fifth step 424
Sixth step 424
Seventh step 425
Working through the stages of troubleshooting 426
Conclusion 426
Points to remember 426
Key terms 427
Questions 427

22. Troubleshooting Cable Connectivity 429
Introduction 429
Structure 430
Objectives 430
Common cable connectivity issues 430
Link status troubleshooting 431
Meeting cabling standards 432
Basic cable tests 433
Cable management 434
Cable faults 434

Common network tools 436
Cable crimper *436*
Punch down tool *437*
Tone generator *438*
Loopback adapter *438*
Optical Time-Domain Reflectometer *439*
Multimeter *439*
Cable tester *440*
Wire map *440*
Network tap *441*
Fusion splicers *442*
Spectrum analyzers *442*
Cable strippers/snips/cutters *443*
Fiber light meter *443*
Conclusion 444
Points to remember 444
Key terms 444
Questions 445

23. Network Utilities 447
Introduction 447
Structure 449
Objectives 449
Network software tools 449
Wi-Fi analyzer *449*
Protocol analyzer/packet capture *450*
Bandwidth speed tester *451*
iPerf *452*
Port scanner *453*
NetFlow analyzers *454*
Trivial file transfer protocol server *455*
Terminal emulator *455*
IP scanner *456*

Command line tools ... 456
PING ... *457*
Process ... *457*
Troubleshooting examples ... *458*
Sample output ... *459*
IPCONFIG/IFCONFIG/IP ... *460*
Troubleshooting examples ... *460*
Sample output ... *461*
NSLOOKUP ... *463*
Troubleshooting examples ... *463*
Sample output ... *464*
Traceroute/Tracert ... *464*
Troubleshooting examples ... *465*
Sample output ... *465*
Address Resolution Protocol ... *466*
Troubleshooting examples ... *467*
Sample output ... *467*
NETSTAT ... *468*
Troubleshooting examples ... *468*
Sample output ... *469*
HOSTNAME ... *469*
Sample output ... *469*
ROUTE ... *469*
Sample output ... *469*
TELNET ... *470*
Options ... *470*
Sample output ... *471*
TCPDUMP ... *471*
Sample output ... *471*
NMAP ... *471*
Basic network platform commands ... 472
Examples of commands in the IOS ... *473*
User EXEC mode ... *473*

Privileged EXEC mode ... *474*
Sample output ... *474*
Putting commands into action ... 476
TCP three-way handshake ... *476*
Three-way handshake ... *477*
Conclusion ... 479
Points to remember ... 479
Key terms ... 479
Questions ... 479

24. Troubleshooting Wireless Networks ... 481
Introduction ... 481
Structure ... 482
Objectives ... 482
Wireless deployments ... 482
Standards and limitations ... 483
Received signal strength indication and dBm ... *485*
RSSI ... *485*
dBm ... *485*
Effective Isotropic Radiated Power/Power settings ... *487*
Measuring transmission ... *487*
Wireless considerations ... *487*
Antenna placement ... *487*
Coverage overlap ... *488*
Polarization ... *489*
AP association time ... *489*
Channel utilization ... *490*
Site survey ... *490*
Common issues and solutions ... 492
Misconfigured devices ... *492*
Signaling and coverage ... *493*
Interference ... *493*
Channel interference or overlap ... *494*

Captive portal issues *495*
Client disassociation issues *496*
Disassociation attack *496*
Other checks and tests 497
Conclusion 497
Points to remember 497
Key terms 498
Questions 498

25. Troubleshooting General Networking Issues 499
Introduction 499
Structure 500
Objectives 500
General considerations 500
Establishing a network baseline *501*
Using the OSI model in troubleshooting *501*
Common issues 502
Physical layer *503*
Data-link layer *503*
Switching loops *504*
Remote access *506*
Troubleshooting VLAN assignment issues *506*
Network layer *506*
Issues with routing tables *507*
Static and dynamic routes *507*
Routing loops *508*
Troubleshooting DNS settings *509*
Transport layer *509*
Session layer *510*
Application layer *510*
Business operations/operational procedures 511
Conclusion 512
Points to remember 512

Key terms 512
Questions 513

26. Network+ Practice Exams 515
Exam 1 515
Networking fundamentals 515
Networking implementations 519
Network operations 521
Network security 523
Network troubleshooting 525
Exam 2 528
Networking fundamentals 528
Networking implementations 531
Network operations 534
Network security 536
Network troubleshooting 538
Exam 1 answers 541
Exam 2 answers 543

APPENDIX: Network+ (N10-009) Certification Exam Objectives 547
1.0 Networking concepts 547
2.0 Network implementation 547
3.0 Network operations 548
4.0 Network security 548
5.0 Network troubleshooting 548

Index 549-560

Chapter 1
OSI Model

Introduction

This chapter outlines the need for standards in the IT industry. The chapter describes the origins and evolution of the OSI model and how the seven layers of the OSI model break down the core concepts of networking functions and processes. Furthermore, the chapter also gives the reader an overview and explanation of each discrete layer and describes how the layer operates in data transmission. It explains in detail how encapsulation and decapsulation work as data traverses networks. The descriptions and illustrations walk the reader through the layers of the model and build their understanding of network fundamentals.

Structure

This chapter will cover the following topics:

- Need for standards
- Evolution of the OSI model
- Seven layers of the OSI model
- Data encapsulation and decapsulation

Objectives

After reading this chapter, you will be able to explain concepts related to the **Open Systems Interconnection** (**OSI**) reference model. You will also be able to understand protocol architectures and appreciate the need for standards and protocols, breaking down the overall functionality of data transmission into its constituent parts.

Need for standards

When new systems of communication emerge and evolve, the way they grow and develop is not necessarily evenly distributed. This occurs especially in the case of a global system, where changes are not limited to local or even regional factors. The way global systems spread, and scale is not geographically, logistically, or uniformly measured over time. Technology and networking are not immune to this *disruptive* but initially *fragmented* means of growth. When we go back to the inception, evolution, and proliferation of networks and observe how these networks and networking technologies have expanded throughout the world, especially from the early 80s, the need for organizational standards and guidelines is apparent. When you have technology as a diverse, globally distributed phenomenon, it is even more apparent that there must be guiding principles to keep everything intact, orderly, flowing smoothly, and operating in a somewhat cohesive, reliable fashion. Three words will stand you through the test of time in expressing the critical nature of having standards in place to fasten the growth and expansion of networking. These words are interoperability, compatibility, and scalability. Unless one considers all of these three areas and what they signify in physical or logical internetworking operations, what one manufactures, designs, innovates, or implements may not work in the landscape of a global operation or, indeed, within the network infrastructure itself. In real-world operations, organizing principles and standards are a must. When discussing networking, the OSI model (and other models such as TCP/IP) could be identified as the universal language for exchanging and discussing ideas about networking functionality and computer network operation and design.

Standards versus protocols

When one considers what is meant by standards, we usually qualify the word with *low*, *poor*, *high,* or *excellent* as a descriptor. In essence, standards are sought as a level of quality, achievement, and so on that is considered acceptable or desirable. In the narrative of networking, this is what occurred when multiple organizations were brought together to put shape and order to networks as they were expanding in the early decades of growth. Participants and experts hailed from many disciplines. Without proper growth management, this expansion of networking could have been an outright chaotic catastrophe. The gathering of minds and expertise met the challenges and problems posed. Regarding standards, one could ask, is there a difference between standards and protocols

when discussing networking fundamentals? If there is, why is it good to mentally sharpen this distinction? As we move through the chapters, you will see why fine-tuning your definitions and spotting differences optimizes your understanding of networking concepts and practices.

Organizational standards mainly apply to people: what they create, manufacture, design, engineer, and build. Bodies that control these standards essentially seek uniformity in terms of quality in processes, methods, high quality, efficiency, and workability in tactical policies and procedures. But it would not be amiss to say that standards and the use of standards indicate or relate to the production and labor of people. Protocols, when one pursues networking, relate specifically to data. A network protocol is a set of rules for formatting and processing data. And there we have the difference. It is true to say that protocols are made and implemented by people, but when one speaks of protocols, one is directly considering what the function of the protocol is, the way the data is formatted or presented, why a given rule is required for data transmission, the impact of the protocol on data, and its role in networking as a practical thing. In short, when we think of standards, we associate organizational standards with people, but when we think about protocols, we associate protocols with data. As networking evolved over the decades, organizational standards helped to make worldwide networking a viable venture. Protocols make networking functions possible.

Evolution of the OSI model

The OSI model was developed in the 1970s by the **International Organization for Standardization** (**ISO**) and adopted as an international standard in 1984.

It was originally developed as a universal standard for creating networks. It provides us with a great teaching tool to understand networking fundamentals. The ISO model is a conceptual framework akin to a blueprint an architect may be given on a house or larger structure. It is a reference guide for all kinds of specialisms in networking practice. The OSI model is used to describe the functions of a networking system. When referred to as a guide, it assists us in understanding the flow of data as it travels across the network and between networks and explains what happens to the data along the way. The model is broken down into seven layers. Each layer handles the functions and tasks in hardware and software to promote error-free data transmission. Just as an architect who follows a blueprint aims to map out a structure accurately, professionals like network engineers, electricians, hardware manufacturers, and software developers strive for success by adhering to the OSI model's guidelines and rules. However, though absolute success is not guaranteed, successes are increased with careful adherence to these networking standards. Think of it like a *big-picture puzzle* or *jigsaw*. Although one piece is independent in its own right, it still holds integrity to the overall design and to the overall functionality in practice and in the interdependencies of the layers. The OSI model holds the pieces of the picture of networking functionality together. It does so by synthesizing and breaking down the

overall picture and practice into seven layers that divide and distinguish the parts from the whole. If you ask yourself what a network needs to do to be fully operational, the OSI model will assist you with an answer.

This book focuses on explaining the OSI model, and describing how it is structured and used in networking. The book's intention is not to argue the legitimacy or relevance of the OSI model in modern networking. However, understanding the theory behind the OSI model offers several potential benefits for technicians and administrators. By exploring these theories and models, we can better grasp their practical applications and abstractions. Viewing these concepts from a problem-solving, solutions-focused perspective allows us to address questions like *if it works—then how? and apply what we learn to our daily tasks*. This approach enhances our ability to troubleshoot, design, and optimize network systems effectively. Consequently, our purpose in this chapter is to view the seven layers as IT practitioners and focus on the *actions* indicative of each layer.

We will focus on the following questions regarding the OSI model in this section:

- What is happening on this layer?
- How does it work?
- Moreover, how would you apply this understanding in practice in your day-to-day duties?
- Could knowing something about this specific area, assist you in your job role, perhaps as a network trouble-shooter or network administrator?

In summary, the OSI model presents us with a marvelous means of visualizing networking interactions and getting our teeth into the mechanics of what the model embraces.

The OSI model has seven layers, from layers 1–7: the physical layer, the data link layer, the network layer, the transport layer, the session layer, the presentation layer, and the application layer.

Note: Mnemonics are used to remember the seven layers. From layers 1–7, it is Please Do Not Tell Secret Passwords Anytime; from layers 7–1, it is All People Seem To Need Data Processing.

The model is usually presented in stack formation because this graphical representation demonstrates the concepts of data flow and protocols best as we *move up and down* through the stack.

Figure 1.1 outlines the seven layers and shows the protocol data units associated with each layer:

***Figure 1.1**: OSI model layers*

In *Figure 1.2*, the primary functions of each layer are outlined. Note the focus is not on the protocols or mechanisms that implement the functions, just the functions themselves:

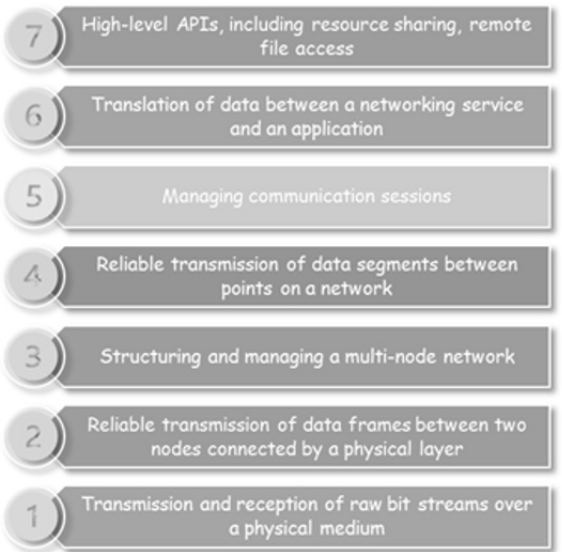

***Figure 1.2**: The functionality at each layer*

Protocol data units

A protocol data unit is an OSI term that refers to a group of information added or removed by a layer of the OSI model. **Protocol data units** (**PDU**) is a significant term related to