CompTIA Network+ Certification Guide (Exam N10-008)

Unleash your full potential as a Network Administrator

Eithne Hogan

www.bpbonline.com

Copyright © 2023 BPB Online

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor BPB Online or its dealers and distributors, will be held liable for any damages caused or alleged to have been caused directly or indirectly by this book.

BPB Online has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, BPB Online cannot guarantee the accuracy of this information.

First published: 2023

Published by BPB Online
WeWork
119 Marylebone Road
London NW1 5PU

UK | UAE | INDIA | SINGAPORE

ISBN 978-93-55518-743

www.bpbonline.com

Dedicated to

My beloved six children:
Samantha, Patrick, Lesleyanne, Kathryn, Chelsea** and **Dylan
&
My beautiful six grandchildren:
***Devin, Alannah, Frankie, Kara, Tyler** and*
*'baby on the way' **Cook***

About the Author

With over 28 years' experience as an educator, **Eithne Hogan** has accomplished a wide diversity of roles. She is currently the coordinator of the Datacenter Academy Program supported by Microsoft, in the college she teaches in. With Microsoft's partnership and expertise, there is a fully functional 3 rack mini scale datacenter lab in the college, which was built in November 2019, to support the teaching and learning of datacenter technologies and server administration to aspiring technicians. Eithne is the coordinator and instructor of this program.

She is also is a part-time lecturer in other higher education universities, and delivers the content of several CompTIA certifications there. Additionally, she currently manages the college's local Cisco Network Academy, personally holding certificates of recognition in Instructor Excellence and 9 years of active service and participation. Furthermore, the CompTIA Academy partnership has been operational for 23 years in the college. Eithne oversees this affiliation.

Regarding IT, Eithne has written and developed curriculum that is nationally recognised and delivered. This curriculum includes network infrastructure, network topologies, network administration, and switching, routing and wireless technologies. She is the Digital Lead for the community college and alongside other colleagues, she collaborates and drives the transformation to the digital landscape in teaching and learning practices.

Acknowledgement

I want to express my deepest gratitude to my family and friends for their continuous support and encouragement throughout this book's writing, especially my children and my grandchildren. You all make everything I do in life meaningful beyond measure. Of that you can be sure.

I am also grateful to BPB Publications for their guidance and expertise in bringing this book to completion. It was a long journey of reviewing and revising this book, with precious participation and committed collaboration of reviewers, technical experts, and editors. But like all of these types of journeys, reaching the destined shores, makes the rocky and the calm seas all the more adventurous.

I would also like to acknowledge the colleagues and professionals I have respected during many years working in education. You have taught me so much, and given me the experience, shared stories, and taut training, that has helped me create the positives in life, and meet and outcreate the bumpier challenges.

We do not sail our ship alone.

Finally, I would like to thank all the readers who have taken an interest in my book and for their support in making this project a reality. I hope you learn much from its contents. I too share the love of opening a new book and embarking on a brand new learning journey. So I wish you the best, as you read, revise, and learn.

Enjoy!

Preface

Network administration involves managing and monitoring the functionality, quality and security of a network on a day-to-day basis. Networks are made up of a diversity of physical devices with an overlay and variety of software types, configurations and protocols. When we consider the need and range of understanding required to assimilate how hardware and software interact with each other, even in terms of a standalone PC or laptop, we can scale our thinking and visualize the sheer scope of knowledge and skills it takes to effectively manage and monitor a network. But believe me when I tell you, the challenge is worth the rewards!

Network design and implementation is based on organizational needs and changes. The breadth of knowledge administrators possess, encompasses network planning and design, network infrastructure, network operations, an ability to appraise and evaluate security, to perceive network capacity and performance, and an estimated target to be reached, in a world where high availability and continuity of service is deemed paramount. Network administrators form the backbone of a company's assets.

This book is designed to provide a comprehensive guide to the job role and duties of a network administrator. It prepares the reader to sit for the CompTIA Network+ exam, but it does so much more than this. In a thorough manner, this guide enables the reader to learn specific networking skills and start their journey in a technical support and IT operational role. It enables the reader to acquire the skillset to install, configure, maintain, and monitor network hardware, software, and effectively handle troubleshooting tools. The book's content incorporates acute awareness of security as it pertains to network operations. The book is intended for anyone who wishes to understand how to have a rewarding career in network administration. I hope you will find this book informative and helpful. Here are some brief descriptions of all the chapters in the book:

Chapter 1: The OSI Model – 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 works as data traverses networks. The descriptions and illustrations walk the reader through the layers of the model, and builds their understanding of network fundamentals.

Chapter 2: Network Topologies - presents a detailed overview of network topologies, including illustrations of each topology covered. The chapter differentiates between physical and logical topologies. The chapter shows how virtual networks function, and explains the critical nature of hypervisors. The chapter also articulates how understanding of virtualization is paramount in today's networking environment.

Chapter 3: Cables and Connectors – covers the cables and connectors used in Ethernet, Coax and Fiber networks. Furthermore, the chapter demonstrates the correct cable type and matching connector(s) used in networks, to include the cable's intended purpose. Readers are shown the difference between wired and wireless networks and are given step-by-step instructions for building a straight through or crossover cable, adhering to the appropriate wiring standards. Additionally, the chapter details proper cable management procedures.

Chapter 4: IP Addressing and Subnetting – 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.

Chapter 5: Ports and Protocols – helps the reader learn the protocols of the TCP/IP suite of protocols. TCP/IP is the only routable protocol and therefore is used in data transmission across all network types, locally and globally, anywhere packets need to be sent and delivered. The chapter outlines port numbers and describes how these numbers are applicable to comprehending functionality and security practices. The chapter offers advice to the reader about protocols that might be blocked in firewalls, unless otherwise required.

Chapter 6: Implementing and Troubleshooting Network Services – 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 – explains with details and numerous illustrations, how datacenter technologies operate. The chapter is focused on datacenter architecture, storage solutions and RAID. The chapter covers practical examples of RAID implementations for given scenarios and demonstrates best use for specific implementations.

Chapter 8: Cloud Concepts – 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 – 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, in order 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 – 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 – 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 – 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 – 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 – gives special attention to the real-world practicalities of running a business or organization. The chapter focuses on documentation required, and the negotiation needed to manage a corporate network and do so effectively. Furthermore, the chapter emphasises the importance of planning, designing and reviewing policies and procedures as part of the organizations change management ethos and gives recommendations to the reader, showing them how to be positive collaborators in IT and business operations.

Chapter 15: Resilience, Fault Tolerance, and Recovery – 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 – 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: Vulnerabilities, Threats, and Attacks – 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 – covers practical techniques related to securing and hardening a network. Furthermore, the chapter also allows the reader to 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 – 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 use case 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 – 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 – 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 – 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 – 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 – 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 – 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 – 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/4ab0d8

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. The OSI Model 1

Introduction 1

Structure 2

Objectives 2

The need for standards 2

Standards versus protocols 3

The OSI model 4

Protocol data units 7

Bit 8

Frame 8

Segment 9

Packet 9

Analogy for data transmission 9

The seven layers of the OSI model 11

The physical layer 11

Modes of communication 12

The data link layer 14

The network layer 15

The transport layer 17

Scenario 18

The session layer 19

The presentation layer 20

The application layer 21

Data encapsulation and decapsulation (within the context of the OSI model) 22

Defining data encapsulation 23

Data flow and encapsulation 23

Stages of data flow 24
Decapsulation 27
Conclusion 27
Key learning 27
Key terms 28
Questions 29

2. Network Topologies 31
Introduction 31
Structure 31
Objectives 32
Physical versus logical topologies 32
Physical topologies 33
Bus topology 34
Star topology 36
Ring topology 39
Mesh topology 42
Hybrid topology 46
Tree topology 47
Logical topologies 47
Logical bus 48
Logical ring 48
Network types 49
Personal Area Network (PAN) 50
Local Area Network (LAN) 50
Campus Area Network (CAN) 51
Metropolitan Area Network (MAN) 51
Wide Area Networks (WAN) 51
WLAN 52
Virtual network concepts 53

Hypervisors 54
Conclusion 56
Key learning 56
Key terms 57
Questions 58

3. Cables and Connectors 59
Introduction 59
Structure 60
Objectives 60
Copper 60
Unshielded twisted pair 61
Shielded twisted pair (STP) 64
UTP cable types 66
Maximum lengths of cable 67
Ethernet cable color code standards 69
T-568a straight-through Ethernet cable 70
Rj-45 crossover Ethernet cable 71
Ethernet cable instructions 71
Basic theory 72
UTP testing parameters 73
Coaxial cable 74
Coaxial cable types 74
Cable structure 74
Coax connector types 75
Fiber 76
Types of fiber media 77
Light sources 79
Fiber optic cable types and distance 80
Fiber connector types 81
Transceiver types 82

Conclusion 82
Key learning 83
Key terms 84
Questions 84

4. IP Addressing and Subnetting 87
Introduction 87
Structure 88
Objectives 88
IP addressing 89
The significance of IP addressing: An analogy 90
The structure of IP addresses 92
IPv4 addressing 94
Binary bit position and value 95
Subnet mask 97
Private vs public addresses 99
IPv4 reserved addresses 99
Private address space (RFC 1918) 100
Classless Inter-Domain Routing (CIDR) 103
Variable Length Subnet Masking (VLSM) 105
Sample VLSM scenario 105
Important points to remember 106
The benefits of VLSM 110
Discovering a network ID: The bitwise AND operation 111
Comparing IPv4 and IPv6 address structures 112
IPV6 addressing 113
Assigning IPv6 addresses 115
IPv4 and IPv6 coexistence: Migration techniques 116
Subnetting with IPv6 117
Conclusion 118
Key learning 118

Key terms 119
Answers to VLSM/subnetting questions *120*
Questions 121

5. Ports and Protocols 123
Introduction 123
Structure 124
Objectives 124
The TCP/IP protocol suite 125
Ports and protocols 128
Port assignment 129
Chart(s) of ports and protocols 130
Internet layer protocols 131
Transport layer protocols 132
Application layer protocols 134
Conclusion 140
Key learning 141
Questions 142

6. Implementing and Troubleshooting Network Services 143
Introduction 143
Structure 143
Objectives 144
DHCP 144
Implementing and configuring DHCP *146*
Installing the DHCP server role 147
Configuring DHCP *154*
Domain Name Service (DNS) 161
How DNS works? *162*
Network Time Protocol (NTP) 164
Conclusion 166

Key learning 167
Key terms 167
Questions 168

7. Data Center Technologies 169
Introduction 169
Structure 170
Objectives 170
Data center network architecture 170
Tiered network architecture 171
Software Defined Networking (SDN) 173
Spine and leaf 173
Traffic flows 175
Storage area networks 175
Fault tolerance—RAID 176
Conclusion 177
Key learning 178
Key terms 178
Questions 178

8. Cloud Concepts 179
Introduction 179
Structure 180
Objectives 180
Deployment models 181
Public cloud 181
Private cloud 181
Hybrid cloud 182
Community cloud 182
Service models 183
Software as a service (SaaS) 184

Infrastructure as a service (IaaS) *185*
Platform as a service (PaaS) *185*
Desktop as a service (DaaS) *186*
Service models: User-managed versus provider managed 187
Connectivity options 189
Virtual private network (VPN) *189*
Private-direct connection to the cloud provider *191*
Multitenancy *191*
Conclusion 191
Key learning 192
Key terms 192
Questions 193

9. Managing Network Devices 195
Introduction 195
Structure 196
Objectives 196
Network segments *197*
Repeater *198*
Hub *199*
Network interface card *200*
Layer 2 switch *200*
Bridge *202*
Access point *203*
Router *203*
Layer 3 capable switch/multilayer switch *204*
Firewall *205*
Voice gateway *206*
Load balancer *206*
Media converter *207*
Wireless LAN controller *207*

Cable modem *207*
DSL modem *208*
Other (security-related) network devices *208*
Networked devices 209
Internet of Things (IoT) *209*
Conclusion 210
Key learning 210
Key terms 210
Questions 211

10. Managing Switching Protocols 213
Introduction 213
Structure 214
Objectives 214
How a switch works? 214
VLANs 216
Access ports and trunk ports *218*
Voice VLANs *220*
The benefits of using VLANs *221*
Port security 222
Secure MAC address types *222*
Port violation *223*
Other protocols 223
Link aggregation *223*
Spanning tree protocol 225
Other STP considerations *227*
Address resolution protocol *228*
Conclusion 229
Key learning 230
Key terms 230
Questions 230

11. Managing Routing Protocols 231
Introduction 231
Structure 232
Objectives 232
The primary functions and features of a router 233
Router interfaces 233
The routing table 235
Interconnecting networks 238
Static and dynamic routing 241
Static routes 241
The benefits of static routing 242
The drawbacks and limitations of static routing 242
Dynamic routes 244
Routing Information Protocol (RIP) 244
IGRP 245
Open Shortest Pathway First (OSPF) 245
Intermediate System to Intermediate System (IS-IS) 247
Border Gateway Protocol (BGP) 247
Administrative Distance (AD) 247
The benefits of dynamic routing 248
The drawbacks and limitations of dynamic routing 249
Bandwidth management 249
Key terms 249
Conclusion 250
Questions 251

12. Installing and Configuring Wireless Technologies 253
Introduction 253
Structure 255
Objectives 255
Benefits of wireless technologies 255

Wireless standards....256
Channels and frequency bands....257
Historical context....258
The 2.4 GHz frequency band....261
The 5 GHz frequency band....262
Channel bonding....263
Modulation techniques....263
Examples of wireless deployments....265
Autonomous AP versus central switching....268
Benefits of a WLC....269
Wireless topology modes....270
Antenna types....270
Wireless identification....272
Cellular technologies....273
Multiple-input and multiple-output (MIMO)....273
Configuring a SOHO router....274
Conclusion....281
Key learning....281
Key terms....282
Questions....282

13. Managing and Monitoring a Network....283
Introduction....283
Structure....284
Objectives....284
Performance metrics and sensors....284
Performance monitor on a Windows 10 System....286
Network availability monitoring....289
Open-source network monitoring tools....291
Simple network management protocol....291
Network device logs....293

System logs 295
Syslog *297*
Open-source Syslog servers *297*
Environmental factors and sensors *301*
NetFlow data *302*
Conclusion 303
Key learning 304
Key terms 304
Questions 305

14. Policies and Procedures in Practice 307
Introduction 307
Structure 308
Objectives 308
Plans and procedures 308
Change management 309
Incident response plan 310
Disaster recovery plan 312
Business continuity plan 314
System lifecycle *315*
Standard operating procedures 316
Policy compliance 317
Hardening and security policies *317*
Common documentation 319
Common agreements (partner integration) *320*
Non-disclosure agreement (NDA) *320*
Service-level agreement (SLA) *321*
Memorandum of Understanding (MOU) *321*
Conclusion 321
Key learning 322
Key terms 322

Questions 323

15. Resilience, Fault Tolerance, and Recovery 325

Introduction 325

Structure 326

Objectives 326

Redundancy: hardware and software strategies 326

Load balancing 327

Multipathing 329

Network interface card (NIC) teaming 331

Implementations of RAID 332

Redundant hardware/clusters 338

Facilities and infrastructure support 338

Redundancy and high availability (HA) concepts 339

Network device backup/restore 340

Conclusion 341

Key learning 342

Key terms 342

Questions 343

16. Security Concepts 345

Introduction 345

Structure 346

Objectives 346

Confidentiality, integrity, and availability (CIA) 347

Threats 348

Common vulnerabilities and exposures (CVE) 349

The principle of least privilege (PoLP) 350

The Zero Trust model 352

Zero Trust through network segmentation 352

Zero day 353

Defense in Depth 354
Authentication methods 356
Two-factor (2FA)/multifactor authentication 357
Risk management 358
Security information and event management (SIEM) 359
Conclusion 359
Key learning 360
Key terms 361
Questions 363

17. Vulnerabilities, Threats, and Attacks 365
Introduction 365
Structure 366
Objectives 366
Technology-based attacks 366
The OSI model and cyber-attack examples 367
Layer 1: The physical layer 368
Layer 2: The datalink layer 369
Layer 3: The network layer 370
Layer 4: The transport layer 372
Layers 5, 6, and 7: The session, presentation, and application layers 373
Cyber-attacks 373
Man in the Middle (MitM) attack 374
Malware 375
Social engineering 376
Conclusion 378
Key learning 379
Key terms 379
Questions 381

18. Network Hardening Techniques....383
Introduction....383
Structure....384
Objectives....384
Securing a workstation....384
Techniques to secure a network....386
Access control lists....386
Example of ACLs....388
Router advertisement guard....389
ARP inspection....389
Dynamic ARP Inspection (DAI) Best Practice....390
DHCP snooping....391
VLAN security considerations....392
Secure SNMP....393
Wireless security....398
Wireless encryption protocols....399
Plan, Plan, Plan....401
Wireless access point security measures....402
Best practice: WLAN attack countermeasures....403
Wireless intrusion detection systems (WIDS)/wireless intrusion prevention systems (WIPS)....403
Penetration testing (pen-testing)....404
Vulnerability scanning....405
Internet of Things security considerations....405
IoT weaknesses....406
Best security practices: IoT....406
Conclusion....408
Key learning....409
Key terms....409
Questions....409

19. Remote Management 411
Introduction 411
Structure 412
Objectives 412
Virtual private network (VPN) 412
Site-to-site VPN 414
Client-to-site VPN 415
Clientless VPN 416
Split tunnel and full tunnel configuration 418
Split tunneling case use an example 419
Remote desktop connection 420
Remote desktop protocol 422
RDP: Security considerations 424
Remote Desktop Gateway (RDP) 424
Configuring an RDP gateway on a Windows server 424
Configuration of remote desktop gateway 426
Configuring remote desktop gateway servers/settings 427
Create computer groups 429
Virtual network computing (VNC) 432
Virtual desktop 433
Authentication and authorization considerations 434
Remote Authentication Dial-In User Service (RADIUS) 434
Terminal Access Controller Access-Control System Plus (TACACS+) 436
In-band versus out-of-band management 437
Telnet/Secure Shell (SSH) 439
Conclusion 439
Key learning 440
Key terms 440
Questions 440

20. Implementing Physical Security 441
Introduction 441
Structure 442
Objectives 442
Physical security controls 442
Deter *443*
Detect *444*
Delay *445*
Respond *447*
Recover *447*
Detection methods 448
Asset tags *448*
Alarms: Tamper detection or chassis intrusion *449*
Configuration management 449
Prevention methods 450
Biometrics *450*
Locking racks *451*
Security zones *452*
Employee training *453*
Asset disposal *454*
Sanitize devices for disposal *454*
Factory reset/wipe configuration *455*
Conclusion 457
Key learning 457
Key terms 458
Questions 458

21. Network Troubleshooting 459
Introduction 459
Structure 460
Objectives 460

The stages of troubleshooting 460
Step 1: Identify the problem *461*
Gather information about the problem *462*
Question the users: The value of effective questioning *462*
Step 2: Establish a theory of probable cause *465*
Step 3: Test the theory *467*
Step 4: Establish a plan of action *468*
Step 5: Implement the solution *469*
Step 6: Verify full system functionality *469*
Step 7: Document findings, actions, and outcomes *470*
Working through the stages of troubleshooting 471
Conclusion 471
Key learning 471
Key terms 472
Questions 472

22. Troubleshooting Cable Connectivity 473
Introduction 473
Structure 474
Objectives 474
Common cable connectivity issues 474
Link status troubleshooting *475*
Meeting cabling standards *476*
Basic cable tests *478*
Cable management *479*
Cable faults *479*
Common network tools 481
Cable crimper *482*
Punch Down Tool *483*
Tone generator *483*
Loopback adapter *484*

Optical Time-Domain Reflectometer (OTDR) *485*
Multimeter *485*
Cable tester *486*
Wire map *487*
Network tap *487*
Fusion splicers *488*
Spectrum analyzers *489*
Cable strippers/snips/cutters *489*
Fiber light meter *490*
Conclusion 490
Key learning 491
Key terms 491
Questions 492

23. Network Utilities 493
Introduction 493
Structure 495
Objectives 495
Network software tools 495
Wi-Fi analyzer (InSSIDer) *496*
Protocol analyzer/packet capture (Wireshark) *496*
Bandwidth speed tester (speed test master) *498*
iPerf *499*
Port scanner (Nmap) *499*
Netflow analyzers (Solar Winds) *501*
Trivial file transfer protocol (TFTP) server (Windows server) *502*
Terminal emulator (Putty) *503*
IP scanner *504*
Command line tools 504
PING *505*
Process *505*

Troubleshooting examples *506*
Sample output *507*
IPCONFIG/IFCONFIG/IP *508*
Troubleshooting examples *509*
Sample output *510*
NSLOOKUP *512*
Troubleshooting examples *512*
Sample output *513*
Traceroute/Tracert *514*
Troubleshooting examples *514*
Sample output *515*
ARP *516*
Troubleshooting examples *517*
Sample output *517*
NETSTAT *518*
Troubleshooting examples *518*
Sample output *519*
HOSTNAME *520*
Sample output *520*
ROUTE *520*
Sample output *520*
TELNET *521*
Options *521*
Sample output *522*
TCPDUMP *522*
Sample output *522*
NMAP *523*
Basic network platform commands 523
Examples of commands in the IOS *524*
User Exec mode (read-only) *525*

Privileged EXEC mode *525*
Sample output *525*
Putting commands into action 527
TCP: three-way handshake *528*
Three-way handshake (as captured in Wireshark) *530*
Conclusion 531
Key learning 531
Key terms 531
Questions 531

24. Troubleshooting Wireless Networks 533
Introduction 533
Structure 534
Objectives 534
Wireless deployments 535
Standards and limitations 536
Received signal strength indication (RSSI) and dBm *538*
RSSI *538*
dBm *538*
Effective isotropic radiated power (EIRP)/power settings *540*
Measuring transmission *540*
Wireless considerations *541*
Antenna placement *541*
Coverage overlap *542*
Polarization *543*
AP association time *543*
Channel utilization *543*
Site survey *544*
Common issues and solutions 546
Misconfigured devices *546*
Signaling and coverage *547*

Interference *547*
Channel interference or overlap *548*
Captive portal issues *550*
Client disassociation issues *550*
Disassociation attack *551*
Other common checks and tests 551
Conclusion 552
Key learning 552
Key terms 552
Questions 553

25. Troubleshooting General Networking Issues 555
Introduction 555
Structure 556
Objectives 557
General considerations 557
Establishing a network baseline *558*
Using the OSI model in troubleshooting *559*
Common issues 560
The physical layer *560*
The data-link layer *561*
Switching loops *562*
Remote access *564*
Troubleshooting VLAN assignment issues *564*
The network layer *565*
Issues with routing tables *566*
Static and dynamic routes *566*
Routing loops *567*
Troubleshooting DNS settings *567*
The transport layer *568*
The session layer, presentation layer *569*

The application layer *569*
Business operations/operational procedures 570
Conclusion 571
Key learning 571
Key terms 572
Questions 572

26. Network + Practice Exams 573
Exam 1 573
Networking fundamentals *573*
Networking implementations *575*
Network operations *577*
Network security *578*
Network troubleshooting *579*
Exam 2 581
Networking fundamentals *581*
Networking implementations *584*
Network operations *585*
Network security *587*
Network troubleshooting *588*
Exam 1 Answers 590
Exam 2 Answers 592

Index 597-614

Chapter 1
The OSI Model

Introduction

Cast the Net Wide

One of the things we do when learning new subjects, enhancing existing learning, or when aiming to apply our practical understanding, occurs in the act of casting out the net. In a way, we are the potential *fisher people* exploring new knowledge to feed our minds and serve us well our food. So, we cast out our personal learning net in times of seeking and searching and a strong desire to be productive. With a firm sense of purpose and focus on our intended goals driven by our willingness to learn, we can haul in our perfect catch and observe and investigate what we have processed, experienced, and encountered. Reaching through the spaces of learning, we need to know our net is cast as wide as what we wish to know so that we cover the spaces competently and comprehensively. While spreading out our net, we need to include as many people, as much data and as many things and processes as they pertain to the subject field being studied in order to differentiate data and align understanding—and this inclusion of materials then gives us our options and solutions.

This is the world of networking

If your purpose in learning about networking is to become a network administrator, prepare to take the CompTIA Network+ exam or enhance your existing knowledge

and practical skills, then this book is for you. It serves as a practical guide to learning about networks and as an aid to consult during and after learning. Merriam-Webster dictionary defines a network as "a system of computers and peripherals that are able to communicate with each other". This system and these interconnections cover diverse geographical spaces, ranging from the smallest area within a room or home to a campus on a university, buildings in a city, networks between countries, or internetworks interwoven across the span of oceans. Yes, we are truly globally connected, and it is through the nature and spaces of these interconnecting systems we cast out our net and grow in personal skill and aptitude.

CompTIA's Network+ covers precise knowledge and skills in networking technologies. The skills we will learn throughout the following chapters encompass networking fundamentals, network implementations, network operations, network security, and network troubleshooting. Our map is the CompTIA Network+ objectives. Our guide is in the learning material and subject matter. Our purpose is to cast the net of learning and consolidate our reach and aim. Our mission is to cast the net of learning wide!

Structure

This chapter will cover the following topics:

- The need for standards
- The OSI model
- The seven layers of the OSI model
- Data encapsulation and decapsulation (within the context of the OSI model)

Objectives

After reading this chapter, you will be able to compare and contrast the layers of the OSI 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.

The need for standards

Often 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 copper 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 you manufacture, design, innovate, or implement 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 handling of growth, 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 then well ask, is there a difference between standards and protocols in 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. So, let us begin. 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 relates 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. 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, 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.

The OSI model

The **Open Systems Interconnection** (**OSI**) model was developed in the 1970s by the **International Organization for Standardization** (**ISO**) and adopted as an international standard in 1984. We might always remember the impact a tongue twister has when we look at these two acronyms—where ISO created the OSI model. Plus, there may be a double impact when the organization *as* ISO is actually stated in a different order to the organization's first letters and to top it off, the organization cites that it was never intended to be an acronym to begin with. Such is the mental confusion at times. One thing you will learn as an individual in the world of technology is, that it is a lavish mental landscape populated and lush with acronyms. You may even have been greeted with a smile and nod of *welcome to the acronym land* on a new course of networking study. And what a truism! To counter acronym overload, we will manage the acronyms, non-acronyms, and *backronyms* as we move through the chapter content.

The OSI model 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 the field of 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 like the architect who successfully adheres to the blueprint is guaranteed to achieve an appropriate mapping of the structure he is designing; a network engineer, electrician, hardware manufacturer, or software developer is able to achieve success when following the guidelines and adhering to the rules of the OSI model. Think of it like a big-picture puzzle or jigsaw. Although one piece is independent in its own right, it still holds