Save 10% on Exam Voucher

See Inside

CompTIA® Network+ N10-006

Flash Cards and Exam Practice Pack

More than 700 flash cards, practice questions, and quick reference sheets for the CompTIA Network+ N10-006 exam

PEARSON IT CERTIFICATION

ANTHONY SEQUEIRA, CCIE NO. 15626

CompTIA® Network+ N10-006

Flash Cards and Exam Practice Pack

Anthony Sequeira, CCIE No. 15626

Pearson
800 East 96th Street
Indianapolis, IN 46240 USA

CompTIA Network+ N10-006 Flash Cards and Exam Practice Pack

Anthony Sequeira

Printed in the United States of America

First Printing August 2015

Library of Congress Control Number: 2015942715

ISBN-13: 978-0-7897-5464-6

ISBN-10: 0-7897-5464-9

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson IT Certification cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

This book is designed to provide information about the CompTIA Network+ N10-006 exam. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information provided is on an “as is” basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the CD or programs accompanying it.

Special Sales

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

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

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

Publisher: Paul Boger

Associate Publisher: Dave Dusthimer

Executive Editor: Brett Bartow

Managing Editor: Sandra Schroeder

Development Editor: Marianne Bartow

Senior Project Editor: Tonya Simpson

Copy Editor: Cheri Clark

Technical Editor: Sean Wilkins

Editorial Assistant: Vanessa Evans

Cover Designer: Mark Shirar

Composition: Mary Sudul

Proofreader: Chuck Hutchinson

Contents at a Glance

About the Author

Anthony Sequeira, CCIE No. 15626, began his IT career in 1994 with IBM in Tampa, Florida. He quickly formed his own computer consultancy, Computer Solutions, and then discovered his true passion: teaching and writing about Microsoft and Cisco technologies. Anthony has lectured to massive audiences around the world while working for Mastering Computers. Anthony has never been happier in his career than he is now as a trainer for CBT Nuggets. He is an avid tennis player, a private pilot, and a semi-professional poker player, and he enjoys getting beaten up by women and children at the martial arts school he attends with his daughter.

About the Technical Reviewer

Sean Wilkins (@Sean_R_Wilkins) is an accomplished networking consultant and writer for infoDispersion (www.infodispersion.com) who has been in the IT field for more than 20 years, working with several large enterprises. Sean holds certifications with Cisco (CCNP/CCDP), Microsoft (MCSE), and CompTIA (A+ and Network+). His educational accomplishments include a Master of Science degree in information technology with a focus in network architecture and design, a Master of Science in organizational management, a Master certificate in network security, a Bachelor of Science in computer networking, and an Associate of Applied Science in computer information systems. Sean spends most of his time writing articles and books for various clients, including Cisco Press, Pearson, Tom's IT Pro, and PluralSight.

Dedications

This book is dedicated to my extended family at CBT Nuggets. Watch, learn, conquer!

Acknowledgments

Thanks so much, as always, to my friend Brett Bartow for this awesome opportunity. Thanks also to his beautiful wife, Marianne, for putting up with me.

This book would not have been possible without my dear friends Kevin Wallace and Keith Barker. Kevin, I am so proud of you and your amazing new venture. Keith, working with you every day at CBT Nuggets is a dream come true.

Thanks to Juliana, Jane, Ken, and all my friends at Slyce in Indian Rocks Beach who tolerated me night after night as I wrote this book. It sure is more fun than the local library—and open much later! Not to mention all the yummy Kentucky Bourbon Ale. And if you love pizza, it is THE place!

Thank you so much to my beautiful wife and daughter, Jo and Bella. Watching me sit in front of a computer is pretty drab, but helping people around the world realize better lives sure is worth the sacrifice. At least I hope you believe that.

Finally, thanks to Sean Wilkins for a killer technical edit. He is wicked smart.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@pearsonitcertification.com

Mail: Pearson IT Certification
ATTN: Reader Feedback
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Visit our website and register this book at www.pearsonitcertification.com/register for convenient access to any updates, downloads, or errata that might be available for this book.

Introduction

Networking technologies are progressing at a breakneck pace and are becoming more crucial to corporations all the time. As such, the Network+ exam is more important than ever. As this text was written, much care was taken to follow the latest Network+ exam blueprint letter for letter. It was also written with the current and future state of networking in mind.

This text was designed to assist you very directly with your Network+ exam. The primary tool here is the Flash Cards, which were created to ensure your quick recall of the many facts and rich vocabulary of modern networking.

Using Flash Cards

Flash Cards have been a proven method of learning everything from anatomy for medical students to learning a new language.

Because many compare mastering Network+ to learning a new language, these tools are perfect to assist you in your journey to conquering the Network+ exam.

Care was taken to construct the Flash Cards in a manner most conducive to your learning. A brief query is composed on the front of the card, and then a verified correct answer is on the back of the card. Some Flash Cards could have more than one correct response. In that case, we provided as many examples of correct answers as possible.

We organized the Flash Cards to coordinate with the Network+ study blueprint to maximize their effectiveness. So, for example, if you are feeling weak in the area of wireless LANs, you can go directly to that section of the Flash Cards.

Review the cards as many times as necessary to feel confident in each area of study. It is recommended that you review all cards one final time before the actual test.

Using the Quick Reference Sheets

Another excellent tool is the Quick Reference Sheets. These not only will serve to refresh you in key exam blueprint areas, but also will serve as a quick reference when you are working in or designing modern networks. You can use the Flash Card section to help determine areas where you might need additional review.

Although the Quick Reference Sheets are not meant to provide exhaustive coverage of the material in each blueprint section, they are guaranteed to review *every* topic mentioned. This ensures that there are no unpleasant surprises in your Network+ exam.

You should consider further research in areas where you might need additional assistance or in areas that you are interested in. Let these Quick Reference Sheets provide you with a strong foundation of knowledge in these topics that you can easily build on using resources such as Safari Books Online or Wikipedia.

What's On the CD-ROM?

The CD-ROM that accompanies this book is also very valuable. When you are ready to test your knowledge, the disc contains hundreds of multiple-choice questions for practice, as well as dozens of performance-based questions that mimic those found in the actual exam. These exercises should prove to be very challenging.

It is critical that you study with these resources before your exam. Although the Flash Cards and Quick Reference Sheets are incredibly important study tools, they are not presented in the format you will encounter on the exam. Working with the resources on the CD-ROM will not only further your understanding of what you truly do not know, but also help you to feel confident with the format of questions in your actual exam.

Chapter 1

Network Devices and Services

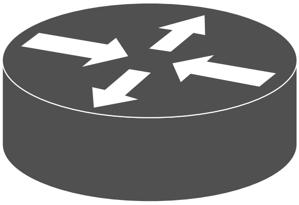
As today's networks increase in complexity and importance, more and more networking devices and networking services are available. This chapter ensures that you can compare and contrast these various components. Combined with the Flash Cards and practice questions of this text, you can confidently answer the many potential questions regarding these devices and service technologies.

Network Devices

You might encounter more than this list of network devices in your real-world experiences, but this list in the Quick Reference Sheets shows the devices you must know to be successful on the Network+ exam.

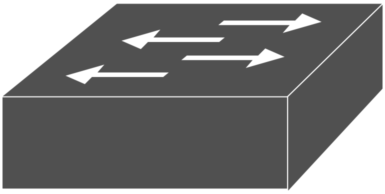
Routers—Perhaps one of the most famous of the network devices, the router operates primarily at Layer 3 of the OSI model. This means it must maintain a database of IPv4 and/or IPv6 prefixes that it can reach. This database is termed the routing table. It can be populated automatically, statically, and dynamically using many different available routing protocols. Most routers can perform many other functions, making them a key workhorse of the network. These additional functions include various security mechanisms, Quality of Service (QoS), and Network Address Translation (NAT), just to name a few. The interfaces of routers create separate collision domains as well as separate broadcast domains. Figure 1-1 shows how Cisco likes to represent routers in network diagrams.

Figure 1-1 *A Router as Represented by Cisco Systems*



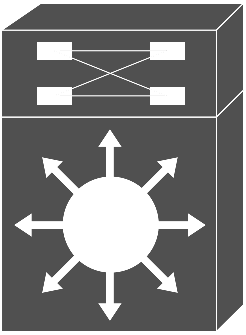
Switches—Whereas a router possesses just a couple of ports (typically), the switch has many. Some larger enterprise switches have literally hundreds. The switch operates primarily at Layer 2 of the OSI model and, as such, it is largely concerned with MAC addresses. Each port of the switch creates its own collision domain, but by default, each port does not create its own broadcast domain. Whereas routers are obsessed with moving packets between subnets, switches are concerned with switching frames as blindingly fast as possible within the subnet. Figure 1-2 shows how Cisco represents a Layer 2 switch, also termed a *workgroup switch*.

Figure 1-2 *A Switch as Represented by Cisco Systems*



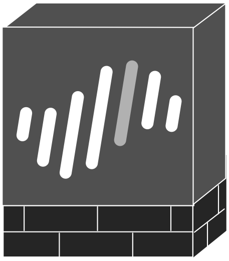
Multilayer Switches—A real beast of a system, the multilayer switch performs the functions of routing and switching in one device. These devices set the speed records when it comes to moving packets as quickly as possible between subnets and within subnets. Figure 1-3 shows a Cisco multilayer switch.

Figure 1-3 *A Multilayer Switch as Represented by Cisco Systems*



Firewalls—When it comes to securing your network, the firewall is a lead actor. These devices specialize in ensuring that bad people stay out and trusted people are enabled to access the devices and services they need from within the network. Keep in mind that firewalls also come in software varieties, so they are not always a separate physical device. For example, there is a software-based firewall built in to the Windows client operating system. The most popular hardware-based firewalls today are termed *stateful firewalls*. They dynamically permit traffic out of a protected network, and then allow the appropriate return traffic back in. Like routers, firewalls operate on Layer 3 and above of the OSI model. Figure 1-4 shows a firewall as represented by Palo Alto Networks, a very popular maker of firewall software and appliances.

Figure 1-4 *A Firewall as Represented by Palo Alto Networks*



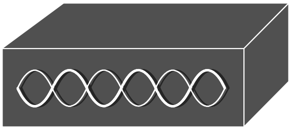
HIDS/HIPS—The Host Intrusion Detection System (HIDS) was one of the first security mechanisms designed for computing devices. Originally intended for the mainframe, its job remains the same today. It examines the packets entering the computer and the processes that are running on the system and alerts users or IT staff regarding activities that are suspicious.

But what if mere detection is not enough? What if you want to prevent the attacks on the host system entirely? HIPS is an installed software package that monitors a single host for suspicious activity by analyzing events occurring within that host and then prevents the attack attempt.

IDS/IPS—Also known as *Network Intrusion Detection Systems* or *Network Intrusion Prevention Systems*, these device seek to alert administrators (detection) about malicious packets attempting to enter the network, or they try to stop (prevention) these packets. There are many styles of IDS and IPS. These include signature-based, in which you load predefined templates that identify bad traffic, and policy-based, which define “normal” traffic for your enterprise. An interesting approach is called a *honey pot*, in which the IDS/IPS device tries to lure attackers by pretending to be an unprotected server system or network device.

Access Point—Access points come in all shapes and sizes. Some are completely wireless, and these usually extend the wireless signal from another access point that is typically connected with a wire to the more traditionally connected network. The access points that connect with one or more wires to the local area network (LAN) are often called *wired access points*. Some access points also include routing capabilities in addition to the switching port. These devices are often called *wireless routers*. Figure 1-5 shows a Cisco wireless access point.

Figure 1-5 *An Access Point as Represented by Cisco Systems*

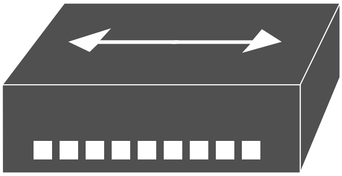


Content Filter—Want to protect your corporate network and keep your employees out of trouble while at work? A content filter seeks to accomplish these goals by blocking the capability to reach certain sites, download specific files, read certain e-mails, or various other controls. Content filtering is accomplished by using a wide variety of software and hardware solutions. For example, many firewalls can also act as content filters in addition to various standalone software packages.

Load Balancer—Another network device that comes in many shapes and sizes is the load balancer. The idea here is software and/or hardware that takes requests and distributes them across many identical resources. Perhaps you have a key database that needs to be checked frequently. You can replicate identical copies of this database, and then have a load balance distribute the requests among these multiple copies. There are many instances in which load balancing is very useful in an IT organization.

Hub—Hubs in the LAN have become legacy devices, being replaced by the faster and more efficient switches. A hub is a Layer 1 device, taking in bits, perhaps trying to strengthen their signal, and then sending these bits out all remaining ports on the device. When traffic is not filtered properly by using Layer 2 addressing, hubs create a large collision domain as well as a single broadcast domain. This large single collision domain increases network collisions. Figure 1-6 shows Cisco's preferred method for representing hubs.

Figure 1-6 *A Hub as Represented by Cisco Systems*



Analog Modem—Another device that is becoming more legacy is the analog modem. It connects to the public switched telephone network (PSTN) to communicate digital signals from the computer over long distances. This technology is slower and less reliable compared to more modern techniques. It is amazing to think that this technology was the main method of accessing the Internet at one time.

Packet Shaper—Whereas a firewall seeks to stop certain forms of traffic from entering your private network, the packet shaper attempts to control the amount of traffic that is permitted. Packet shapers try to enforce your limits on the volume of traffic based on various parameters. Perhaps you want voice and video traffic to have preference over web pages and e-mail. The packet shaping devices can help enforce this policy.

VPN Concentrator—The virtual private network (VPN) has exploded in popularity with increased Internet speeds. The VPN concentrator is typically a hardware device that simultaneously connects as many VPN users as possible. These devices are often located at a corporate headquarters, where many users and branch offices usually make the VPN connection.

Network Services and Applications

Services and applications used for networking purposes are just as important as devices. This section quickly references these for you.

VPNs—The virtual private network seeks to make network users believe they are connected to a system or another network directly, even though this connection might be made across the globe. The public Internet often serves as the connection medium. Strong network security is typically used to keep the transfer of information truly "private." VPNs include the following:

- **Site to site**—This provides convenience and cost-effectiveness for a branch-office type of environment. One device, such as a router, makes a VPN connection to another site. Then all of the end systems at the local site can connect over the VPN using the router's connection. This eliminates the responsibility for each client system to obtain the appropriate VPN software and its proper configuration.
- **Host to site**—If a client system installs software to connect to a remote site over a VPN, this is called a *host to site connection*.
- **Host to host**—As you might guess, in a host to host connection two clients install appropriate software to make a VPN connection with each other. Note that this might be a client and a server operating system as well. The main difference is that there is not an entire site (network) participating in the connection.

Protocols—There are various protocols and configuration options for VPNs today. This is due to their extreme explosion in popularity, and a consistent drive to improve their security and reliability. The following are some protocols you need to be familiar with:

- **IPsec**—IP Security (IPsec) is a suite of protocols that provides a wide variety of security protections to a VPN. For example, in lower-security environments, IPsec can feature Message Digest Authentication (MD5) for authentication and Data Encryption Standard (DES) for encryption. In a higher-security environment, Secure Hash Algorithm (SHA-1) can be used along with the Advanced Encryption Standard (AES). Tunnel mode can protect the entire packet, or transport mode can focus on protecting just the payload. IPsec support was optional in IPv4, but in IPv6, the node must support IPsec.
- **GRE**—Generic Routing Encapsulation can be a real workhorse in your network. It is useful in a wide variety of circumstances. One example is if you have traffic that cannot be protected by IPsec. First encapsulate the traffic in GRE, and then compress the GRE traffic within IPsec. It is important to note that GRE by itself does not provide security mechanisms.

- **SSL VPN**—The Secure Sockets Layer VPN enables you to create a VPN connection using your standard web browser as the client software.
- **PTP/PPTP**—The Point-to-Point Tunneling Protocol (PPTP) uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets. The PPTP specification does not describe encryption or authentication features and relies on the Point-to-Point Protocol being tunneled to implement security functionality. However, the most common PPTP implementation shipping with the Microsoft Windows product families allows for various levels of authentication and encryption natively as standard features of the Windows PPTP stack.

TACACS/RADIUS—In today's corporate networks there are many devices for which users need to log in. TACACS and RADIUS are security protocols that communicate from a network device to a database of user and group accounts. Often, TACACS and RADIUS are used in a AAA environment. AAA provides accounting, authentication, and authorization services. TACACS is often considered more secure than RADIUS because it protects the entire packet and not just the password as RADIUS does.

RAS—Remote Access Services enable a client to access a server system over a network as vast as the Internet.

Web Services—Many devices today provide HTTP and HTTPS services so that web pages can be accessed from the device. For example, a Cisco router might run the HTTPS service so that administrators can access a web page hosted on the router that provides configuration options for the device.

Unified Voice Services—For years, only data was sent through the network. Now, more voice traffic finds its way on the data network as well. Various devices help make this possible, from sophisticated software packages that replace the traditional PBX system, to digital phones with which end users place calls. Figure 1-7 shows a Cisco representation of an IP phone.

Figure 1-7 *A Voice over IP Phone as Represented by Cisco Systems*

Network Controllers—Network controllers exist on network interface cards (NICs) and permit various types of network devices to connect to the network. On many devices, such as personal computers, the network controller is modular and can easily be swapped for another model or type.