EXAM CRAM

CompTIA® Network+ N10-008

Cram Sheet

Flash Cards

Practice Tests

EMMETT DULANEY

EXAM CRAM

CompTIA® Network+ N10-008 Exam Cram

Emmett Dulaney

Pearson

CompTIA® Network+ N10-008 Exam Cram

ISBN-13: 978-0-13-737576-9

ISBN-10: 0-13-737576-X

ScoutAutomatedPrintCode

Trademarks

Warning and Disclaimer

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.

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 intlcs@pearson.com.

Editor-in-Chief
Mark Taub

Director ITP Production Management
Brett Bartow

Executive Editor
Nancy Davis

Development Editor
Ellie Bru

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Copy Editor
Chuck Hutchinson

Indexer
Timothy Wright

Proofreader
Abigail Manheim

Technical Editor
Chris Crayton

Publishing Coordinator
Cindy Teeters

Cover Designer
Chuti Prasertsith

Compositor
codeMantra

Contents at a Glance

Table of Contents

About the Author

Emmett Dulaney (CompTIA Network+, Cloud+, Security+, A+, and others) has been the author of several books on certifications and operating systems over the past 20 years. He is a columnist for *Certification Magazine* and a professor at a small university in Indiana. He is currently the editor of a journal devoted to business education (and the business of education).

Dedication

For Elijah, Wolfgang, Teresa, and Harrison: the second round
—Emmett Dulaney

Acknowledgments

Thanks are due to Eleanor (Ellie) Bru for working on this title once more and making it as strong as it can be. An enormous amount of credit for this book goes to Chris Crayton, without whom this edition would be only a shadow of what it is. It was an honor to work with him again, and I owe him enormous gratitude. Thanks continue to be due to Mike Harwood, who wrote the first few editions, and to the team of talented individuals at Pearson who work behind the scenes and make each title the best it can be.

About the Technical Reviewer

Chris Crayton is a technical consultant, trainer, author, and industry-leading technical editor. He has worked as a computer technology and networking instructor, information security director, network administrator, network engineer, and PC specialist. Chris has authored several print and online books on PC repair, CompTIA A+, CompTIA Security+, and Microsoft Windows. He has also served as technical editor and content contributor on numerous technical titles for several leading publishing companies. He holds numerous industry certifications, has been recognized with many professional and teaching awards, and has served as a state-level SkillsUSA final competition judge.

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: community@informit.com

Introduction

Welcome to *CompTIA Network+ N10-008 Exam Cram*. This book is designed to prepare you to take—and pass—the CompTIA Network+ exam. The Network+ exam has become the leading introductory-level network certification available today. It is recognized by both employers and industry giants as providing candidates with a solid foundation of networking concepts, terminology, and skills. The Network+ exam covers a broad range of networking concepts to prepare candidates for the technologies they are likely to work with in today's network environments.

About Network+ Exam Cram

Exam Crams are designed to give you the information you need to know to prepare for a certification exam. They cut through the extra information, focusing on the areas you need to get through the exam. With this in mind, the elements within the Exam Cram titles are aimed at providing the exam information you need in the most succinct and accessible manner.

In this light, this book is organized to closely follow the actual CompTIA objectives for exam N10-008. As such, it is easy to find the information required for each of the specified CompTIA Network+ objectives. The objective focus design used by this Exam Cram is an important feature because the information you need to know is easily identifiable and accessible. To see what we mean, compare the CompTIA objectives to the book's layout, and you can see that the facts are right where you would expect them to be.

Within the chapters, potential exam hotspots are clearly highlighted with Exam Alerts. They have been carefully placed to let you know that the surrounding discussion is an important area for the exam. To further help you prepare for the exam, a Cram Sheet is included that you can use in the final stages of test preparation. Be sure to pay close attention to the bulleted points on the Cram Sheet because they pinpoint the technologies and facts you probably will encounter on the test.

Finally, great effort has gone into the questions that appear throughout the chapter and the practice tests to ensure that they accurately represent the look and feel of the ones you will see on the real Network+ exam. Be sure, before taking the exam, that you are comfortable with both the format and content of the questions provided in this book.

About the Network+ Exam

The Network+ (N10-008 Edition) exam is the newest iteration of several versions of the exam. The new Network+ objectives are aimed toward those who have at least nine months of experience in network support or administration. CompTIA believes that new Network+ candidates should have A+ certification (or its equivalent), but it is not required, and this should not discourage those who do not.

You will have a maximum of 90 minutes to answer the 90 questions on the exam. The allotted time is quite generous, so when you finish, you probably will have time to double-check a few of the answers you were unsure of.

By the time the dust settles, you need a minimum score of 720 to pass the Network+ exam. This is on a scale of 100 to 900. For more information on the specifics of the Network+ exam, refer to CompTIA's main website at http://certification.comptia.org/.

CompTIA Network+ Exam Topics

Table I-1 lists general exam topics (that is, objectives) and specific topics under each general topic (that is, subobjectives) for the CompTIA Network+ N10-008 exam. This table also lists the chapter in which each exam topic is covered.

TABLE I-1 **CompTIA Network+ Exam Topics**

Chapter	N10-008 Exam Objective	N10-008 Exam Subobjective
1 (Network Technologies, Topologies, and Types)	1.0 Networking Fundamentals	1.2 Explain the characteristics of network topologies and network types.
2 (Models, Ports, Protocols, and Network Services)	1.0 Networking Fundamentals	1.1 Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts. 1.5 Explain common ports and protocols, their application, and encrypted alternatives. 1.6 Explain the use and purpose of network services.
3 (Addressing, Routing, and Switching)	1.0 Networking Fundamentals	1.4 Given a scenario, configure a subnet and use appropriate IP addressing schemes.
	2.0 Network Implementations	2.2 Compare and contrast routing technologies and bandwidth management concepts. 2.3 Given a scenario, configure and deploy common Ethernet switching features.

Chapter	N10-008 Exam Objective	N10-008 Exam Subobjective
4 (Network Implementations)	1.0 Networking Fundamentals 2.0 Network Implementations	1.7 Explain basic corporate and datacenter network architecture. 2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.
5 (Cabling Solutions and Issues)	1.0 Networking Fundamentals 5.0 Network Troubleshooting	1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution. 5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tool.
6 (Wireless Solutions and Issues)	2.0 Network Implementations 5.0 Network Troubleshooting	2.4 Given a scenario, install and configure the appropriate wireless standards and technologies. 5.4 Given a scenario, troubleshoot common wireless connectivity issues.
7 (Cloud Computing Concepts and Options)	1.0 Networking Fundamentals	1.8 Summarize cloud concepts and connectivity options.
8 (Network Operations)	3.0 Network Operations	3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability. 3.2 Explain the purpose of organizational documents and policies. 3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.
9 (Network Security)	4.0 Network Security	4.1 Explain common security concepts. 4.2 Compare and contrast common types of attacks. 4.3 Given a scenario, apply network hardening techniques. 4.4 Compare and contrast remote access methods and security implications. 4.5 Explain the importance of physical security.
10 (Network Troubleshooting)	5.0 Network Troubleshooting	5.1 Explain the network troubleshooting methodology. 5.3 Given a scenario, use the appropriate network software tools and commands. 5.5 Given a scenario, troubleshoot general networking issues.

Booking and Taking the Network+ Certification Exam

Unfortunately, testing is not free. You're charged for each test you take, whether you pass or fail. In the United States and Canada, tests are administered by Pearson VUE testing services. To access the VUE contact information and book an exam, refer to the website at http://www.pearsonvue.com or call 1-877-551-7587. When booking an exam, you need to provide the following information:

- Your name as you would like it to appear on your certificate.
- Your Social Security or Social Insurance number.
- Contact phone numbers (to be called in case of a problem).
- Mailing address, which identifies the address to which you want your certificate mailed.
- Exam number and title.
- Email address for contact purposes. This often is the fastest and most effective means to contact you. Test vendors require it for registration.
- Credit card information so that you can pay online. You can redeem vouchers by calling the respective testing center.

What to Expect from the Exam

If you haven't taken a certification test, the process can be a little unnerving. Even if you've taken numerous tests, it is not much better. Mastering the inner mental game often can be as much of a battle as knowing the material. Knowing what to expect before heading in can make the process a little more comfortable.

Certification tests are administered on a computer system at a VUE authorized testing center. The format of the exams is straightforward: each question has several possible answers to choose from. The questions in this book provide a good example of the types of questions you can expect on the exam. If you are comfortable with them, the test should hold few surprises. Many of the questions vary in length. Some of them are longer scenario questions, whereas others are short and to the point. Carefully read the questions; the longer questions often have a key point that will lead you to the correct answer.

Most of the questions on the Network+ exam require you to choose a single correct answer, but a few require multiple answers. When there are multiple correct answers, a message at the bottom of the screen prompts you to "Choose all that apply." Be sure to read these messages.

A Few Exam-Day Details

It is recommended that you arrive at the examination room at least 15 minutes early, although a few minutes earlier certainly would not hurt. This will give you time to prepare and will give the test administrator time to answer any questions you might have before the test begins. Many people suggest that you review the most critical information about the test you're taking just before the test. (Exam Cram books provide a reference—the Cram Sheet, located inside the front of this book—that lists the essential information from the book in distilled form.) Arriving a few minutes early will give you some time to compose yourself and mentally review this critical information.

You will be asked to provide two forms of ID, one of which must be a photo ID. Both of the identifications you choose should have a signature. You also might need to sign in when you arrive and sign out when you leave.

Be warned: The rules are clear about what you can and cannot take into the examination room. Books, laptops, note sheets, and so on are not allowed in the examination room. The test administrator will hold these items, to be returned after you complete the exam. You might receive either a wipe board or a pen and a single piece of paper for making notes during the exam. The test administrator will ensure that no paper is removed from the examination room.

After the Test

Whether you want it or not, as soon as you finish your test, your score displays on the computer screen. In addition to the results appearing on the computer screen, a hard copy of the report prints for you. Like the onscreen report, the hard copy displays the results of your exam and provides a summary of how you did on each section and on each technology. If you were unsuccessful, this summary can help you determine the areas you need to brush up on.

When you pass the Network+ exam, you will have earned the Network+ certification, and your certificate will be mailed to you within a few weeks. Should you not receive your certificate and information packet within five weeks of passing your exam, contact CompTIA at fulfillment@comptia.org, or call 1-630-678-8300 and ask for the fulfillment department.

Last-Minute Exam Tips

Studying for a certification exam is no different than studying for any other exam, but a few hints and tips can give you the edge on exam day:

- **Read all the material:** CompTIA has been known to include material not expressly specified in the objectives. This book has included additional information not reflected in the objectives to give you the best possible preparation for the examination.
- **Watch for the Exam Tips and Notes:** The Network+ objectives include a wide range of technologies. Exam Tips and Notes found throughout each chapter are designed to pull out exam-related hotspots. These can be your best friends when preparing for the exam.
- **Use the questions to assess your knowledge:** Don't just read the chapter content; use the exam questions to find out what you know and what you don't. If you struggle, study some more, review, and then assess your knowledge again.
- **Review the exam objectives:** Develop your own questions and examples for each topic listed. If you can develop and answer several questions for each topic, you should not find it difficult to pass the exam.

Good luck!

Companion Website

Register this book to get access to the Pearson Test Prep practice test software and other study materials plus additional bonus content. Check this site regularly for new and updated postings written by the author that provide further insight into the more troublesome topics on the exams. Be sure to check the box that you would like to hear from us to receive updates and exclusive discounts on future editions of this product or related products.

To access this companion website, follow these steps:

1. Go to www.pearsonITcertification.com/register and log in or create a new account.
2. Enter the ISBN: 9780137375769.
3. Answer the challenge question as proof of purchase.
4. Click the **Access Bonus Content** link in the Registered Products section of your account page, to be taken to the page where your downloadable content is available.

Please note that many of our companion content files can be very large, especially image and video files.

If you are unable to locate the files for this title by following these steps, please visit www.pearsonITcertification.com/contact and select the Site Problems/ Comments option. Our customer service representatives will assist you.

Pearson Test Prep Practice Test Software

As noted previously, the print book comes with the Pearson Test Prep practice test software containing two full exams. (The ebook edition of the *CompTIA Network+ N10-008 Exam Cram* does not include access to the Pearson Test Prep practice exams that come with the print edition.) These practice tests are available to you either online or as an offline Windows application. To access the practice exams that were developed with this book, please see the instructions in the card inserted in the sleeve in the back of the book. This card includes a unique access code that enables you to activate your exams in the Pearson Test Prep practice test software.

Note

The cardboard sleeve in the back of this book includes a piece of paper. The paper lists the activation code for the practice exams associated with this book. Do not lose the activation code. On the opposite side of the paper from the activation code is a unique, one-time-use coupon code for the purchase of the Premium Edition eBook and Practice Test.

Accessing the Pearson Test Prep Software Online

The online version of this software can be used on any device with a browser and connectivity to the Internet, including desktop machines, tablets, and smartphones. To start using your practice exams online, follow these steps:

1. Go to www.PearsonTestPrep.com.
2. Select **Pearson IT Certification** as your product group.
3. Enter your email/password for your account. If you don't have an account on PearsonITCertification.com, you will need to establish one by going to PearsonITCertification.com/join.

4. In the My Products tab, click the **Activate New Product** button.
5. Enter the access code printed on the insert card in the back of your book to activate your product.
6. The product will now be listed in your My Products page. Click the **Exams** button to launch the exam settings screen and start your exam.

Accessing the Pearson Test Prep Software Offline

If you want to study offline, you can download and install the Windows version of the Pearson Test Prep software. There is a download link for this software on the book's companion website, or you can enter the following link in your browser:

www.pearsonitcertification.com/content/downloads/pcpt/engine.zip

To access the book's companion website and the software, follow these steps:

1. Register your book by going to PearsonITCertification.com/register and entering the ISBN: 9780137375769.
2. Respond to the challenge questions.
3. Go to your account page and select the **Registered Products** tab.
4. Click the **Access Bonus Content** link under the product listing.
5. Click the **Install Pearson Test Prep Desktop Version** link under the Practice Exams section of the page to download the software.
6. After the software downloads, unzip all the files on your computer.
7. Double-click the application file to start the installation, and follow the onscreen instructions to complete the registration.
8. When the installation is complete, launch the application and select the **Activate Exam** button on the My Products tab.
9. Click the **Activate a Product** button in the Activate Product Wizard.
10. Enter the unique access code found on the card in the sleeve in the back of your book, and click the **Activate** button.
11. Click **Next** and then **Finish** to download the exam data to your application.
12. You can now start using the practice exams by selecting the product and clicking the **Open Exam** button to open the exam settings screen.

Note that the offline and online versions will sync together, so saved exams and grade results recorded on one version will be available to you on the other as well.

Customizing Your Exams

After you are in the exam settings screen, you can choose to take exams in one of three modes:

- Study Mode
- Practice Exam Mode
- Flash Card Mode

Study Mode enables you to fully customize your exams and review answers as you are taking the exam. This is typically the mode you would use first to assess your knowledge and identify information gaps. Practice Exam Mode locks certain customization options because it is presenting a realistic exam experience. Use this mode when you are preparing to test your exam readiness. Flash Card Mode strips out the answers and presents you with only the question stem. This mode is great for late-stage preparation when you really want to challenge yourself to provide answers without the benefit of seeing multiple-choice options. This mode will not provide the detailed score reports that the other two modes will, so it should not be used if you are trying to identify knowledge gaps.

In addition to these three modes, you will be able to select the source of your questions. You can choose to take exams that cover all the chapters, or you can narrow your selection to a single chapter or the chapters that make up specific parts in the book. All chapters are selected by default. If you want to narrow your focus to individual chapters, first deselect all the chapters; then select only those on which you want to focus in the Objectives area.

You can also select the exam banks on which to focus. Each exam bank comes complete with a full exam of questions that cover topics in every chapter. The two exams printed in the book are available to you as well as two additional exams of unique questions. You can have the test engine serve up exams from all four banks or just from one individual bank by selecting the desired banks in the exam bank area.

You can make several other customizations to your exam from the exam settings screen, such as the time of the exam, the number of questions, whether to randomize questions and answers, whether to show the number of correct answers for multiple answer questions, or whether to serve up only specific types of questions. You can also create custom test banks by selecting only questions that you have marked or questions on which you have added notes.

Updating Your Exams

If you are using the online version of the Pearson Test Prep software, you should always have access to the latest version of the software as well as the exam data. If you are using the Windows desktop version, every time you launch the software, it will check to see if there are any updates to your exam data and automatically download any changes that were made since the last time you used the software. This requires that you are connected to the Internet at the time you launch the software.

Sometimes, due to many factors, the exam data may not fully download when you activate your exam. If you find that figures or exhibits are missing, you may need to manually update your exams.

To update a particular exam you have already activated and downloaded, select the **Tools** tab and then click the **Update Products** button. Again, this is an issue only with the desktop Windows application.

If you want to check for updates to the Pearson Test Prep exam engine software, Windows desktop version, select the **Tools** tab and click the **Update Application** button. This will ensure that you are running the latest version of the software engine.

Assessing Exam Readiness

Exam candidates never really know whether they are adequately prepared for the exam until they have completed about 30 percent of the questions. At that point, if you are not prepared, it is too late. The best way to determine your readiness is to work through the CramSaver quizzes at the beginning of each chapter and review the exam objectives and Exam Alerts presented in each chapter. It is best to work your way through the entire book unless you can complete each subject without having to do any research or look up any answers.

Premium Edition eBook and Practice Tests

The print book also includes an exclusive offer for 80 percent off the Premium Edition eBook and Practice Tests edition of this title. Please see the coupon code included with the cardboard sleeve for information on how to purchase the Premium Edition.

CHAPTER 4

Network Implementations

This chapter covers the following official Network+ objectives:

- Explain basic corporate and datacenter network architecture.
- Compare and contrast various devices, their features, and their appropriate placement on the network.

This chapter covers CompTIA Network+ objectives 1.7 and 2.1. For more information on the official Network+ exam topics, see the “About the Network+ Exam” section in the Introduction.

All but the most basic of networks require devices to provide connectivity and functionality. Understanding how these networking devices operate and identifying the functions they perform are essential skills for any network administrator and are requirements for a Network+ candidate.

This chapter introduces commonly used networking devices, and that is followed by a discussion of basic corporate and datacenter network architecture later in the chapter. You are not likely to encounter all the devices mentioned in this chapter on the exam, but you can expect to work with at least some of them.

Common Networking Devices

- ▶ **Compare and contrast various devices, their features, and their appropriate placement on a network.**

CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section.

1. What is the difference between an active and a passive hub?
2. What is the major difference between a hub and a switch?
3. What are the types of ports found on hubs and switches?
4. What can distribute incoming data to specific application servers and help distribute the load?
5. True or false: A multilayer switch operates as both a router and a switch.
6. Your company is looking to add a hardware device to the network that can increase redundancy and data availability as it increases performance by distributing the workload. What use case might this sample technology apply to?

Answers

1. Hubs can be either active or passive. Hubs are considered active when they regenerate a signal before forwarding it to all the ports on the device.
2. Rather than forwarding data to all the connected ports, a switch forwards data only to the port on which the destination system is connected.
3. Hubs and switches have two types of ports: *medium-dependent interface (MDI)* and *medium-dependent interface crossed (MDI-X)*.
4. A content switch can distribute incoming data to specific application servers and help distribute the load.
5. True. A multilayer switch operates as both a router and a switch.
6. A load balancer can be either a software or hardware component, and it increases redundancy and data availability as it increases performance by distributing the workload.

The best way to think about this chapter is as a catalog of networking devices. The first half looks at devices that you can commonly find in a network of any substantial size. The devices are discussed in objective order to simplify study and include everything from simple access points to VPN concentrators.

ExamAlert

Remember this objective begins with "Compare and contrast various devices." This means that you need to be able to distinguish one networking or networked device from another and know its appropriate placement on the network. What does it do? Where does it belong?

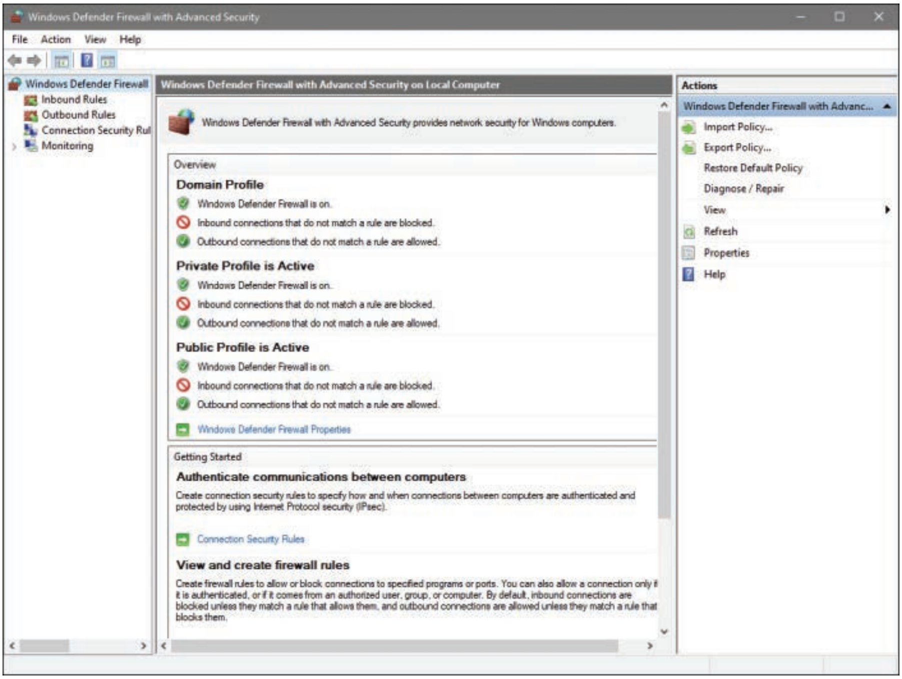
Firewall

A *firewall* is a networking device, either hardware or software based, that controls access to your organization's network. This controlled access is designed to protect data and resources from an outside threat. To provide this protection, firewalls typically are placed at a network's entry/exit points—for example, between an internal network and the Internet. After it is in place, a firewall can control access into and out of that point.

Although firewalls typically protect internal networks from public networks, they are also used to control access between specific network segments within a network. An example is placing a firewall between the Accounts and Sales departments.

As mentioned, firewalls can be implemented through software or through a dedicated hardware device. Organizations implement software firewalls through *network operating systems (NOSs)* such as Linux/UNIX, Windows servers, and macOS servers. The firewall is configured on the server to allow or block certain types of network traffic. In small offices and for regular home use, a firewall is commonly installed on the local system and is configured to control traffic. Many third-party firewalls are available.

Hardware firewalls are used in networks of all sizes today. Hardware firewalls are often dedicated network devices that can be implemented with little configuration. They protect all systems behind the firewall from outside sources. Hardware firewalls are readily available and often are combined with other devices today. For example, many broadband routers and wireless access points have firewall functionality built in. In such a case, the router or AP might have a number of ports available to plug systems into. Figure 4.1 shows Windows Defender Firewall and the configured inbound and outbound rules.



Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Private Profile is Active

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Public Profile is Active

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Windows Defender Firewall Properties

Getting Started

Authenticate communications between computers

Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

Connection Security Rules

View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rule that blocks them.

FIGURE 4.1 **Configuration of Windows Defender Firewall**

> **ExamAlert**
>
> Remember that a firewall uses inbound and outbound rules and can protect internal networks from public networks and control access between specific network segments.

IDS/IPS

An *intrusion detection system (IDS)* is a passive detection system. The IDS can detect the presence of an attack and then log that information. It also can alert an administrator to the potential threat. The administrator then analyzes the situation and takes corrective measures if needed.

A variation on the IDS is the *intrusion prevention system (IPS)*, which is an active detection system. With IPS, the device continually scans the network, looking for inappropriate activity. It can shut down any potential threats. The IPS looks for any known signatures of common attacks and automatically tries to prevent those attacks. An IPS is considered an active/reactive security measure because it actively monitors and can take steps to correct a potential security threat.

Following are several variations on IDSs/IPSs:

- **Behavior based:** A *behavior-based system* looks for variations in behavior such as unusually high traffic, policy violations, and so on. By looking for deviations in behavior, it can recognize potential threats and quickly respond.
- **Signature based:** A signature-based system, also commonly known as *misuse-detection system (MD-IDS/MD-IPS)*, is primarily focused on evaluating attacks based on attack signatures and audit trails. Attack signatures describe a generally established method of attacking a system. For example, a TCP flood attack begins with a large number of incomplete TCP sessions. If the MD-IDS knows what a TCP flood attack looks like, it can make an appropriate report or response to thwart the attack. This IDS uses an extensive database to determine the signature of the traffic.
- **Network-based intrusion detection/prevention system (NIDS or NIPS):** The system examines all network traffic to and from network systems. If it is software, it is installed on servers or other systems that can monitor inbound traffic. If it is hardware, it may be connected to a hub or switch to monitor traffic.
- **Host-based intrusion detection/prevention system (HIDS or HIPS):** These applications are spyware or virus applications that are installed on individual network systems. The system monitors and creates logs on the local system.

ExamAlert

An intrusion detection system (IDS) can detect malicious activity and send alerting messages, but it does not prevent attacks. An intrusion prevention system (IPS) protects hosts and prevents against malicious attacks from the network layer up through the application layer.

Router

In a common configuration, routers create larger networks by joining two network segments. A *small office/home office (SOHO)* router connects a user to the Internet. A SOHO router typically serves 1 to 10 users on the system. A router can be a dedicated hardware device or a computer system with more than one network interface and the appropriate routing software. All modern network operating systems include the functionality to act as a router.

Note

Routers normally create, add, or divide networks or network segments at the network layer of the OSI reference model because they normally are IP-based devices. Chapter 2, “Models, Ports, Protocols, and Network Services,” covers the OSI reference model in greater detail.

A router derives its name from the fact that it can route data it receives from one network to another. When a router receives a packet of data, it reads the packet’s header to determine the destination address. After the router has determined the address, it looks in its routing table to determine whether it knows how to reach the destination; if it does, it forwards the packet to the next hop on the route. The next hop might be the final destination, or it might be another router. Figure 4.2 shows, in basic terms, how a router works.

Note

You can find more information on network routing in Chapter 3, “Addressing, Routing, and Switching.”

A router works at Layer 3 (the network layer) of the OSI model.

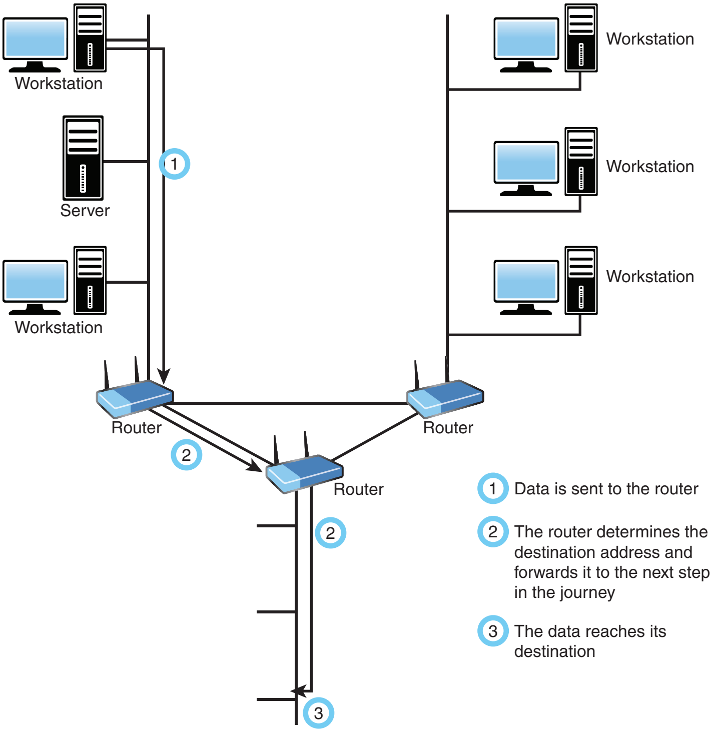

Workstation
Server
Workstation
1
Workstation
Workstation
Workstation
Router
Router
2
Router
2
3
1 Data is sent to the router
2 The router determines the destination address and forwards it to the next step in the journey
3 The data reaches its destination

FIGURE 4.2 **How a router works**

Switch

Like hubs, *switches* are the connectivity points of an Ethernet network. Devices connect to switches via twisted-pair cabling, one cable for each device. The difference between hubs and switches is in how the devices deal with the data they receive. Whereas a hub forwards the data it receives to all the ports on the device, a switch forwards it to only the port that connects to the destination device. It does this by the MAC address of the devices attached to it and then by matching the destination MAC address in the data it receives. Figure 4.3 shows how a switch works. In this case, it has learned the MAC addresses of the devices attached to it; when the workstation sends a message intended for another workstation, it forwards the message on and ignores all the other workstations.

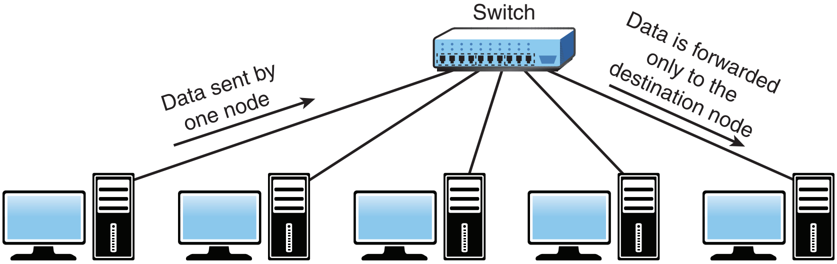


FIGURE 4.3 **How a switch works**

By forwarding data to only the connection that should receive it, the switch can greatly improve network performance. By creating a direct path between two devices and controlling their communication, the switch can greatly reduce the traffic on the network and therefore the number of collisions. As you might recall, collisions occur on Ethernet networks when two devices attempt to transmit at the same time. In addition, the lack of collisions enables switches to communicate with devices in full-duplex mode. In a full-duplex configuration, devices can send data to and receive data from the switch at the same time. Contrast this with half-duplex communication, in which communication can occur in only one direction at a time. Full-duplex transmission speeds are double that of a standard half-duplex connection. So, a 100 Mbps connection becomes 200 Mbps, and a 1000 Mbps connection becomes 2000 Mbps, and so on.

The net result of these measures is that switches can offer significant performance improvements over hub-based networks, particularly when network use is high.

Irrespective of whether a connection is at full or half duplex, the method of switching dictates how the switch deals with the data it receives. The following is a brief explanation of each method:

- **Cut-through:** In a cut-through switching environment, the packet begins to be forwarded as soon as it is received. This method is fast, but it creates the possibility of errors being propagated through the network because no error checking occurs.
- **Store-and-forward:** Unlike cut-through, in a store-and-forward switching environment, the entire packet is received and error-checked before being forwarded. The upside of this method is that errors are not propagated through the network. The downside is that the error-checking process takes a relatively long time, and store-and-forward switching is considerably slower as a result.
- **Fragment-free:** To take advantage of the error checking of store-and-forward switching, but still offer performance levels nearing that of cut-through switching, fragment-free switching can be used. In a fragment-free switching environment, enough of the packet is read so that the switch can determine whether the packet has been involved in a collision. As soon as the collision status has been determined, the packet is forwarded.

Hub and Switch Cabling

In addition to acting as a connection point for network devices, hubs and switches can be connected to create larger networks. This connection can be achieved through standard ports with a special cable or by using special ports with a standard cable.

As you learned in Chapter 3, the ports on a hub, switch, or router to which computer systems are attached are called *medium-dependent interface crossed (MDI-X)*. The crossed designation is derived from the fact that two of the wires within the connection are crossed so that the send signal wire on one device becomes the receive signal of the other. Because the ports are crossed internally, a standard or straight-through cable can be used to connect devices.

Another type of port, called a *medium-dependent interface (MDI)* port, is often included on a hub or switch to facilitate the connection of two switches or hubs. Because the hubs or switches are designed to see each other as an extension of the network, there is no need for the signal to be crossed. If a hub or switch does not have an MDI port, hubs or switches can be connected by using a cable between two MDI-X ports. The crossover cable uncrosses the internal crossing. Auto MDI-X ports on more modern network device interfaces can detect whether the connection would require a crossover, and automatically choose the MDI or MDI-X configuration to properly match the other end of the link.

ExamAlert

In a crossover cable, wires 1 and 3 and wires 2 and 6 are crossed.

A switch can work at either Layer 2 (the data link layer) or Layer 3 (the network layer) of the OSI model. When it filters traffic based on the MAC address, it is called a Layer 2 switch since MAC addresses exist at Layer 2 of the OSI model (if it operated only with IP traffic, it would be a Layer 3 switch).

Multilayer Switch

It used to be that networking devices and the functions they performed were separate. Bridges, routers, hubs, and more existed but were separate devices. Over time, the functions of some individual network devices became integrated into a single device. This is true of *multilayer switches*.

A multilayer switch is one that can operate at both Layer 2 and Layer 3 of the OSI model, which means that the multilayer device can operate as both a switch and a router (by operating at more than one layer, it is living up to the name of being “multilayer”). Also called a Layer 3 switch, the multilayer switch is a high-performance device that supports the same routing protocols that routers do. It is a regular switch directing traffic within the LAN; in addition, it can forward packets between subnets.

ExamAlert

A multilayer switch operates as both a router (Layer 3 capable device) and a switch (Layer 2 switch).

A content switch is another specialized device. A content switch is not as common on today’s networks, mostly due to cost. A content switch examines the network data it receives, decides where the content is intended to go, and forwards it. The content switch can identify the application that data is targeted for by associating it with a port. For example, if data uses the Simple Mail Transfer Protocol (SMTP) port, it could be forwarded to an SMTP server.

Content servers can help with load balancing because they can distribute requests across servers and target data to only the servers that need it, or distribute data between application servers. For example, if multiple mail servers are used, the content switch can distribute requests between the servers, thereby sharing the load evenly. This is why the content switch is sometimes called a load-balancing switch.

ExamAlert

A content switch can distribute incoming data to specific application servers and help distribute the load.

Hub

At the bottom of the networking devices food chain, so to speak, are hubs. Hubs are used in networks that use Ethernet twisted-pair cabling to connect devices. Hubs also can be joined to create larger networks. *Hubs* are simple devices that direct data packets to all devices connected to the hub, regardless of whether the data package is destined for the device. This makes them inefficient devices and can create a performance bottleneck on busy networks.

In its most basic form, a hub does nothing except provide a pathway for the electrical signals to travel along. Such a device is called a *passive* hub. Far more common nowadays is an *active* hub, which, as well as providing a path for the data signals, regenerates the signal before it forwards it to all the connected devices. In addition, an active hub can buffer data before forwarding it. However, a hub does not perform any processing on the data it forwards, nor does it perform any error checking.

Hubs come in a variety of shapes and sizes. Small hubs with five or eight connection ports are commonly called *workgroup hubs*. Others can accommodate larger numbers of devices (normally up to 32). These are called *high-density devices*.

ExamAlert

Because hubs don't perform any processing, they do little except enable communication between connected devices. For today's high-demand network applications, something with a little more intelligence is required. That's where switches come in.

A basic hub works at Layer 1 (the physical layer) of the OSI model.

Bridge

A *bridge*, as the name implies, connects two networks. Bridging is done at the first two layers (physical and data link layer) of the OSI model and differs from routing in its simplicity. With routing, a packet is sent to where it is intended to go, whereas with bridging, it is sent away from this network. In other words, if a packet does not belong on this network, it is sent across the bridge with the assumption that it belongs there rather than here.

If one or more segments of the bridged network are wireless, the device is known as a *wireless bridge*.

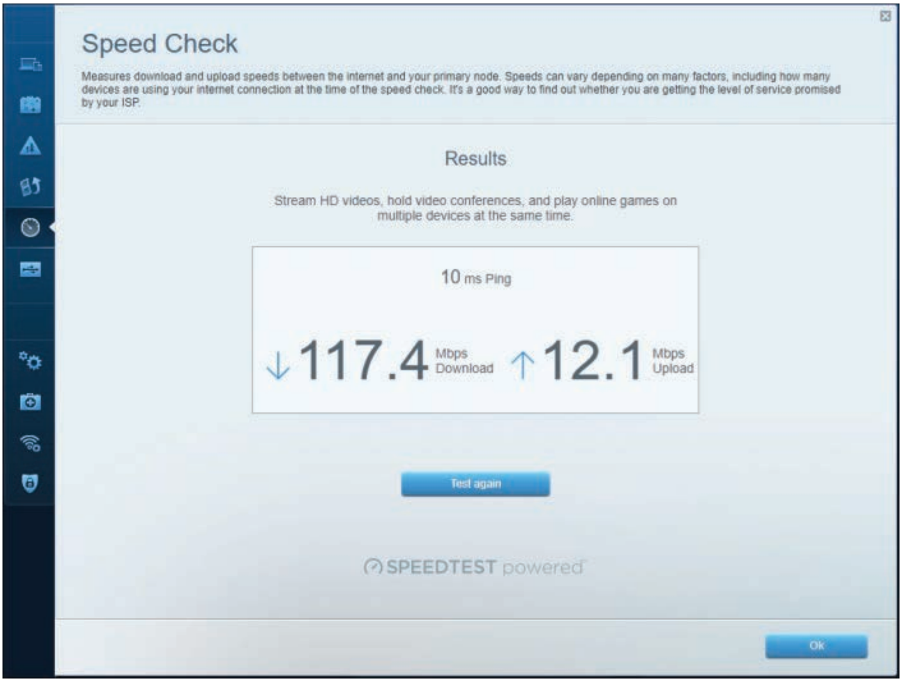
DSL and Cable Modems

A traditional modem (short for modulator/demodulator) is a device that converts the digital signals generated by a computer into analog signals that can travel over conventional phone lines. The modem at the receiving end converts the signal back into a format that the computer can understand. While modems can be used as a means to connect to an ISP or as a mechanism for dialing up a LAN, they have faded in use in recent years in favor of faster technologies.

Modems can be internal add-in expansion cards or integrated with the motherboard, external devices that connect to a system's serial or USB port, or proprietary devices designed for use on other devices, such as portables and handhelds.

A *DSL modem* makes it possible for telephone lines to be used for high-speed Internet connections. Much faster than the old dial-up modems, DSL modems use the subscriber (dedicated) lines and send the data back and forth across them—translating them into signals the devices can use.

Similarly, a *cable modem* has a coaxial connection for connecting to the provider's outlet and an *unshielded twisted-pair (UTP)* connection for connecting directly to a system or to a hub, switch, or router. Cable providers often supply the cable modem, with a monthly rental agreement. Many cable providers offer free or low-cost installation of cable Internet service, which includes installing a network card in a PC. Some providers also do not charge for the network card. Figure 4.4 shows the results of a speed test from a cable modem.



Speed Check

Measures download and upload speeds between the internet and your primary node. Speeds can vary depending on many factors, including how many devices are using your internet connection at the time of the speed check. It's a good way to find out whether you are getting the level of service promised by your ISP.

Results

Stream HD videos, hold video conferences, and play online games on multiple devices at the same time.

10 ms Ping

↓117.4 Mbps Download ↑12.1 Mbps Upload

FIGURE 4.4 **Speed test results**

Most cable modems offer the capability to support a higher-speed Ethernet connection for the home LAN than is achieved. The actual speed of the connection can vary somewhat, depending on the utilization of the shared cable line in your area.

Access Point

The term *access point (AP)* can technically be used for either a wired or wireless connection, but in reality it is almost always associated only with a wireless-enabling device. A *wireless access point (WAP)* is a transmitter and receiver (transceiver) device used to create a *wireless LAN (WLAN)*. WAPs typically are separate network devices with a built-in antenna, transmitter, and adapter. WAPs use the wireless infrastructure network mode to provide a connection point between WLANs and a wired Ethernet LAN. WAPs also usually have several ports, giving you a way to expand the network to support additional clients.

Depending on the size of the network, one or more WAPs might be required. Additional WAPs are used to allow access to more wireless clients and to expand the range of the wireless network. Each WAP is limited by a transmission range—the distance a client can be from a WAP and still obtain a usable signal. The actual distance depends on the wireless standard used and the obstructions and environmental conditions between the client and the WAP.

ExamAlert

An AP or WAP can operate as a bridge connecting a standard wired network to wireless devices or as a router passing data transmissions from one access point to another.

Saying that a WAP is used to extend a wired LAN to wireless clients does not give you the complete picture. A wireless AP today can provide different services in addition to just an access point. Today, the APs might provide many ports that can be used to easily increase the network's size. Systems can be added to and removed from the network with no effect on other systems on the network. Also, many APs provide firewall capabilities and *Dynamic Host Configuration Protocol (DHCP)* service. When they are hooked up, they give client systems a private IP address and then prevent Internet traffic from accessing those systems. So, in effect, the AP is a switch, DHCP server, router, and firewall.

APs come in all shapes and sizes. Many are cheaper and are designed strictly for home or small office use. Such APs have low-powered antennas and limited expansion ports. Higher-end APs used for commercial purposes have high-powered antennas, enabling them to extend how far the wireless signal can travel.

Note

APs are used to create a wireless LAN and to extend a wired network. APs are used in the infrastructure wireless topology.

An AP works at Layer 2 (the data link layer) of the OSI model.

Media Converter

When you have two dissimilar types of network media, a *media converter* is used to allow them to connect. They are sometimes referred to as couplers. Depending on the conversion being done, the converter can be a small device, barely larger than the connectors themselves, or a large device within a sizable chassis.

Reasons for not using the same media throughout the network, and thus reasons for needing a converter, can range from cost (gradually moving from coax to fiber), disparate segments (connecting the office to the factory), or the need to run particular media in a setting (the need for fiber to reduce EMI problems in a small part of the building).

Figure 4.5 shows an example of a media converter. The one shown converts between 10/100/1000TX and 1000LX (with an SC-type connector).

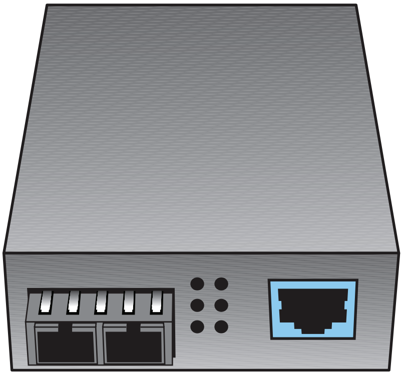


FIGURE 4.5 A common media converter

The following converters are commonly implemented and are ones that CompTIA has previously included on the Network+ exam.

ExamAlert

Make sure you know that the possibilities listed here exist:

- Single mode fiber to Ethernet
- Single mode to multimode fiber
- Multimode fiber to Ethernet
- Fiber to coaxial

Voice Gateway

When telephone technology is married with information technology, the result is called telephony. There has been a massive move from landlines to *voice over IP (VoIP)* for companies to save money. One of the biggest issues with the administration of this is security. When both data and VoIP are on the same line, they are both vulnerable in the case of an attack. Standard telephone systems should be replaced with a securable *PBX*.

A *VoIP gateway*, also sometimes called a PBX gateway, can be used to convert between the legacy telephony connection and a VoIP connection using Session Initiation Protocol (SIP). This is referred to as a "digital gateway" because the voice media are converted in the process.

ExamAlert

Be sure that you know that by having both data and VoIP on the same line, they are both vulnerable in the case of an attack.

Repeater

A *repeater* (also called a booster or wireless range extender) can amplify a wireless signal to make it stronger. This increases the distance that the client system can be placed from the access point and still be on the network. The extender needs to be set to the same channel as the AP for the repeater to take the transmission and repeat it. This is an effective strategy to increase wireless transmission distances.

ExamAlert

Carefully read troubleshooting question scenarios to be sure the transmission from the AP is getting to the repeater first, and then the repeater is duplicating the signal and passing it on.

Wireless LAN Controller

Wireless LAN controllers are often used with branch/remote office deployments for wireless authentication. When an AP boots, it authenticates with a controller before it can start working as an AP. This is often used with *VLAN pooling*, in which multiple interfaces are treated as a single entity (usually for load balancing).

Load Balancer

Network servers are the workhorses of the network. They are relied on to hold and distribute data, maintain backups, secure network communications, and more. The load of servers is often a lot for a single server to maintain. This is where load balancing comes into play. *Load balancing* is a technique in which the workload is distributed among several servers. This feature can take networks to the next level; it increases network performance, reliability, and availability.

ExamAlert

Remember that load balancing increases redundancy and therefore data availability. Also, load balancing increases performance by distributing the workload.

A load balancer can be either a hardware device or software specially configured to balance the load.

Note

Multilayer switches and DNS servers can serve as load balancers.

Proxy Server

Proxy servers typically are part of a firewall system. They have become so integrated with firewalls that the distinction between the two can sometimes be lost.

However, proxy servers perform a unique role in the network environment—a role that is separate from that of a firewall. For the purposes of this book, a proxy server is defined as a server that sits between a client computer and the Internet and looks at the web page requests the client sends. For example, if a client computer wants to access a web page, the request is sent to the proxy server rather than directly to the Internet. The proxy server first determines whether the request is intended for the Internet or for a web server locally. If the request is intended for the Internet, the proxy server sends the request *as if it originated the request*. When the Internet web server returns the information, the proxy server returns the information to the client. Although a delay might be induced by the extra step of going through the proxy server, the process is largely transparent to the client that originated the request. Because each request a client sends to the Internet is channeled through the proxy server, the proxy server can provide certain functionality over and above just forwarding requests.

One of the most notable extra features is that proxy servers can greatly improve network performance through a process called *caching*. When a caching proxy server answers a request for a web page, the server makes a copy of all or part of that page in its cache. Then, when the page is requested again, the proxy server answers the request from the cache rather than going back to the Internet. For example, if a client on a network requests the web page www.comptia.org, the proxy server can cache the contents of that web page. When a second client computer on the network attempts to access the same site, that client can grab it from the proxy server cache, and accessing the Internet is unnecessary. This greatly increases the response time to the client and can significantly reduce the bandwidth needed to fulfill client requests.

Nowadays, speed is everything, and the capability to quickly access information from the Internet is a crucial concern for some organizations. Proxy servers and their capability to cache web content accommodate this need for speed.

An example of this speed might be found in a classroom. If a teacher asks 30 students to access a specific *Uniform Resource Locator (URL)* without a proxy server, all 30 requests would be sent into cyberspace and subjected to delays or other issues that could arise. The classroom scene with a proxy server is quite different. Only one request of the 30 finds its way to the Internet; the other 29 are filled by the proxy server's cache. Web page retrieval can be almost instantaneous.

However, this caching has a potential drawback. When you log on to the Internet, you get the latest information, but this is not always so when information is retrieved from a cache. For some web pages, it is necessary to go directly to the Internet to ensure that the information is up to date. Some proxy servers can update and renew web pages, but they are always one step behind.

The second key feature of proxy servers is allowing network administrators to filter client requests. If a server administrator wants to block access to certain websites, a proxy server enables this control, making it easy to completely disallow access to some websites. This is okay, but what if it were necessary to block numerous websites? In this case, maintaining proxy servers gets a bit more complicated.

Determining which websites users can or cannot access is usually done through something called an *access control list (ACL)*. Chapter 3 discussed how an ACL can be used to provide rules for which port numbers or IP addresses are allowed access. An ACL can also be a list of allowed or nonallowed websites; as you might imagine, compiling such a list can be a monumental task. Given that millions of websites exist, and new ones are created daily, how can you target and disallow access to the "questionable" ones? One approach is to reverse the situation and deny access to all pages except those that appear in an "allowed" list. This approach has high administrative overhead and can greatly limit the productive benefits available from Internet access.

Understandably, it is impossible to maintain a list that contains the locations of all sites with questionable content. In fairness, that is not what proxy servers were designed to do. However, by maintaining a list, proxy servers can better provide a greater level of control than an open system. Along the way, proxy servers can make the retrieval of web pages far more efficient.

A *reverse proxy server* is one that resides near the web servers and responds to requests. These are often used for load-balancing purposes because each proxy can cache information from a number of servers.

VPN Concentrators and Headends

A *VPN concentrator* can be used to increase remote-access security. This device can establish a secure connection (tunnel) between the sending and receiving network devices. VPN concentrators add an additional level to VPN security. They not only can create the tunnel but also can authenticate users, encrypt the data, regulate the data transfer, and control traffic.

The concentrator sits between the VPN client and the VPN server, creates the tunnel, authenticates users using the tunnel, and encrypts data traveling through the tunnel. When the VPN concentrator is in place, it can establish a secure connection (tunnel) between the sending and receiving network devices.

VPN concentrators add an additional level to VPN security. Depending on the exact concentrator, they can do the following:

- Create the tunnel.
- Authenticate users who want to use the tunnel.
- Encrypt and decrypt data.
- Regulate and monitor data transfer across the tunnel.
- Control inbound and outbound traffic as a tunnel endpoint or router.

The VPN concentrator invokes various standard protocols to accomplish these functions.

A *VPN headend* (or *head-end*) is a server that receives the incoming signal and then decodes/encodes it and sends it on.

Networked Devices

One of the fastest areas of growth in networking isn't necessarily in adding more users, but in adding more devices. Each "smart" device has the ability to monitor or perform some task and report the status of the data it has collected, or itself, back. Most of these devices require IP addresses and function like normal nodes, but some network only through Bluetooth or NFC. Table 4.1 lists some of the devices commonly being added to the network today.

TABLE 4.1 **Commonly Networked Devices**

Device	Description	Key Points
Telephones	Utilizing voice over IP (VoIP), the cost of traditional telephone service is reduced to a fraction of its old cost.	In the world of voice over IP (VoIP), an *endpoint* is any final destination for a voice call.
Printer	The printer was one of the first devices to be networked. Connecting the printer to the network makes it possible to share with all authorized users.	Networked printers need to be monitored for security concerns. Many high-speed printers spool print jobs, and the spooler can be a weakness for some unauthorized person looking for sensitive information.
Physical access control devices	These devices include door locks, gates, and other similar devices.	They greatly reduce the cost of manual labor, such as guards at every location.
Cameras	Cameras allow for monitoring areas remotely.	The capability to pan, tilt, and zoom (PTZ) is important in camera selection.
HVAC sensors	These devices provide heating, ventilation, and air conditioning.	Smart sensors for HVAC can work in conjunction with other sensors. For example, a smoke detector can go off and notify the furnace to immediately shut off the fan to prevent spreading smoke throughout the building.
IoT	Internet of Things (IoT) includes such devices as refrigerators, smart speakers, smart thermostats, and smart doorbells.	The acceptance—and adoption—of these items in the home market is predicted to grow so quickly that the number of sensors in use will outnumber the number of users within the next decade.
ICS/SCADA	Industrial Control Systems (ICS) is a catchall term for sensors and controls used in industry. A subset of this is SCADA (supervisory control and data acquisition), which refers to equipment often used to manage automated factory equipment, dams, power generators, and similar equipment.	When it comes to sensors and controls, an emerging area of growth is that of in-vehicle computing systems. Automobiles tend to have sophisticated systems, such as computers complete with hard drives and GPS devices. Similar devices to those always sensing the status of the vehicle are used in industrial environments for automation, safety, and efficiency.

ExamAlert

You will be expected to know the devices mentioned in this chapter. Review Table 4.1, and make sure that you understand each device and how and why it is used on the network.

Cram Quiz

1. Users are complaining that the network's performance is unsatisfactory. It takes a long time to pull files from the server, and, under heavy loads, workstations can become disconnected from the server. The network is heavily used, and a new videoconferencing application is about to be installed. The network is a 1000BASE-T system created with Ethernet hubs. Which device are you most likely to install to alleviate the performance problems?

   ❍ **A.** Switch

   ❍ **B.** Router

   ❍ **C.** Media converter

   ❍ **D.** Firewall

2. Which of the following devices forwards data packets to all connected ports?

   ❍ **A.** Router

   ❍ **B.** Switch

   ❍ **C.** Content filter

   ❍ **D.** Hub

3. Which of the following devices passes data based on the MAC address?

   ❍ **A.** Hub

   ❍ **B.** Switch

   ❍ **C.** MSAU

   ❍ **D.** Router

4. Which of the following can serve as load balancers?

   ❍ **A.** IDS and DNS servers

   ❍ **B.** Multilayer switches and IPS

   ❍ **C.** Multilayer switches and DNS servers

   ❍ **D.** VoIP PBXs and UTM appliances

5. Which of the following is the best answer for a device that continually scans the network, looking for inappropriate activity?

   ❍ **A.** IPS

   ❍ **B.** NGFW

   ❍ **C.** VCPN

   ❍ **D.** AAA

Cram Quiz Answers

1. **A.** Replacing Ethernet hubs with switches can yield significant performance improvements. Of the devices listed, switches are also the only ones that can be substituted for hubs. A router is used to separate networks, not as a connectivity point for workstations. A media converter is used to connect two dissimilar types of network media. A firewall is not a solution to the problem presented.
2. **D.** Hubs are inefficient devices that send data packets to all connected devices. Switches pass data packets to the specific destination device. This method significantly increases network performance.
3. **B.** When determining the destination for a data packet, the switch learns the MAC address of all devices attached to it and then matches the destination MAC address in the data it receives. None of the other devices listed passes data based solely on the MAC address.
4. **C.** Multilayer switches and DNS servers can serve as load balancers.
5. **A.** An intrusion prevention system (IPS) is a device that continually scans the network, looking for inappropriate activity.

Networking Architecture

- **Explain basic corporate and datacenter network architecture.**

CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then complete the Cram Quiz at the end of the section.

1. What is the term for the network architecture design in which servers, appliances, and other switches located within the same rack are connected to an in-rack network switch?
2. True or false: Traffic flows entering and leaving a datacenter are known as East-West traffic.
3. True or false: In the three-tiered architecture, the access/edge layer ensures data is delivered to edge/end devices.

Answers

1. This is known as top-of-rack (ToR) switching.
2. False. Traffic flows entering and leaving a datacenter are known as North-South traffic.
3. True. The access/edge layer is the place where switches connect to and ensure data is delivered to edge/end devices.

The networking devices discussed previously in this chapter are used to build networks. For this particular objective, CompTIA wants you to be aware of some of the architecture and design elements of the network. Whether you're putting together a datacenter or a corporate office, planning should be involved, and no network should be allowed to haphazardly sprout without management and oversight.

Three-Tiered Architecture

To improve system performance, as well as to improve security, it is possible to implement a *tiered* systems model. This is often referred to as an *n*-tiered model because the *n*- can be one of several different numbers.

If we were looking at database, for example, with a one-tier model, or single-tier environment, the database and the application exist on a single system. This is common on desktop systems running a standalone database. Early UNIX implementations also worked in this manner; each user would sign on to a terminal and run a dedicated application that accessed the data. With two-tier architecture, the client workstation or system runs an application that communicates with the database that is running on a different server. This common implementation works well for many applications. With *three-tiered architecture*, security is enhanced. In this model, the end user is effectively isolated from the database by the introduction of a middle-tier server. This server accepts requests from clients, evaluates them, and then sends them on to the database server for processing. The database server sends the data back to the middle-tier server, which then sends the data to the client system. Becoming common in business today, this approach adds both capability and complexity.

While the examples are of database tiering, this same approach can be taken with devices such as routers, switches, and other servers. In a three-tiered model of routing and switching, the three tiers would be the core, the distribution/aggregation layer, and the access/edge. We walk through each of the layers present in this scenario.

Core Layer

The *core* layer is the backbone: the place where switching and routing meet (switching ends, routing begins). It provides high-speed, highly redundant forwarding services to move packets between distribution-layer devices in different regions of the network. The core switches and routers would be the most powerful in the enterprise (in terms of their raw forwarding power,) and would be used to manage the highest-speed connections (such as 100 Gigabit Ethernet). Core switches also incorporate internal firewall capability as part of their features, helping with segmentation and control of traffic moving from one part of the network to another.

Distribution/Aggregation Layer

The *distribution layer*, or *aggregation layer* (sometimes called the workgroup layer), is the layer in which management takes place. This is the place where QoS policies are managed, filtering is done, and routing takes place. Distribution layer devices can be used to manage individual branch-office WAN connections, and this is considered to be smart (usually offering a larger feature set than switches used at the access/edge layer). Lower latency and larger MAC address table sizes are important features for switches used at this level because they aggregate traffic from thousands of users rather than hundreds (as access/edge switches do).

Access/Edge Layer

Switches that allow end users and servers to connect to the enterprise are called access switches or edge switches, and the layer where they operate in the three-tiered model is known as the *access layer*, or *edge layer*. Devices at this layer may or may not provide Layer 3 switching services; the traditional focus is on minimizing the cost of each provisioned Ethernet port (known as "cost-per-port") and providing high port density. Because the focus is on connecting client nodes, such as workstations to the network, this is sometimes called the desktop layer.

ExamAlert

Remember: The core layer is the backbone of the network (where the fastest routers and switches operate to manage separate networks), whereas the distribution/aggregation layer (between the access/edge and core layers) is the "boundary" layer where ACLs and Layer 3 switches operate to properly manage data between VLANs and subnetworks. The access/edge layer is the place where switches connect to and ensure data is delivered to edge/end devices, such as computers and servers.

Software-Defined Networking

Software-defined networking (SDN) is a dynamic approach to computer networking intended to allow administrators to get around the static limitations of physical architecture associated with traditional networks. They can do so through the implementation of technologies such as the Cisco Systems Open Network Environment.

The goal of SDN is not only to add dynamic capabilities to the network but also to reduce IT costs through implementation of cloud architectures. SDN combines network and application services into centralized platforms that can automate provisioning and configuration of the entire infrastructure.

The SDN architecture, from the top down, consists of the application layer, control layer, and infrastructure layer. CompTIA also adds the management plane as an objective, and a discussion of each of these components follows.

Application Layer

The *application layer* is the top of the SDN stack, and this is where load balancers, firewalls, intrusion detection, and other standard network applications are located. While a standard (non-SDN) network would use a specialized appliance for each of these functions, with an SDN network, an application is used in place of a physical appliance.

Control Layer

The *control layer* is the place where the SDN controller resides; the controller is software that manages policies and the flow of traffic throughout the network. This controller can be thought of as the brains behind SDN, making it all possible. Applications communicate with the controller through a northbound interface, and the controller communicates with switching using southbound interfaces.

Infrastructure Layer

The physical switch devices themselves reside at the *infrastructure layer*. This is also known as the control plane when breaking the architecture into "planes" because this is the component that defines the traffic routing and network topology.

Management Plane

With SDN, the management plane allows administrators to see their devices and traffic flows and react as needed to manage data plane behavior. This can be done automatically through configuration apps that can, for example, add more bandwidth if it looks as if edge components are getting congested. The management plane manages and monitors processes across all layers of the network stack.

> **ExamAlert**
>
> A major benefit of SDN is that it replaces traditional dedicated hardware/services with virtual.

Spine and Leaf

In an earlier section, we discussed the possibility of tiered models. A two-tier model that Cisco promotes for switches is the *spine and leaf* model. In this model, the spine is the *backbone* of the network, just as it would be in a skeleton and is responsible for interconnecting all the leaf switches in a full-mesh topology. Thanks to the mesh, every leaf is connected to every spine, and the path is randomly chosen so that the traffic load is evenly distributed among the top-tier switches. If one of the switches at the top tier were to fail, there would only be a slight degradation in performance throughout the datacenter.

Because of the design of this model, no matter which leaf switch is connected to a server, the traffic always has to cross the same number of devices to get to another server. This keeps latency at a steady level.

When *top-of-rack (ToR) switching* is incorporated into the network architecture, switches located within the same rack are connected to an in-rack network switch, which is connected to aggregation switches (usually via fiber cabling). The big advantage of this setup is that the switches within each rack can be connected with cheaper copper cabling and the cables to each rack are all that need be fiber.

ExamAlert

Remember that in a spine and leaf model the spine is the backbone of the network and is responsible for interconnecting all the leaf switches in a full-mesh topology.

Traffic Flows

Traffic flows within a datacenter typically occur within the framework of one of two models: East-West or North-South. The names may not be the most intuitive, but the East-West traffic model means that data is flowing among devices within a specific datacenter while North-South means that data is flowing into the datacenter (from a system physically outside the datacenter) or out of it (to a system physically outside the datacenter).

The naming convention comes from the way diagrams are drawn: data staying within the datacenter is traditionally drawn on the same horizontal line (East-to-West), while data leaving or entering is typically drawn on a vertical line (North-to-South). With the increase in virtualization being implemented at so many levels, the East-West traffic has increased in recent years.

ExamAlert

East-West traffic is a concept referring to network traffic flow within a datacenter between servers. North-South refers to data transfers between the datacenter and that outside of the network.

Datacenter Location Types

One of the biggest questions a network administrator today can face is where to store the data. At one point in time, this question was a no-brainer: servers were kept close at hand so they could be rebooted and serviced regularly. Today, however, that choice is not such an easy one. The cloud, virtualization, software-defined networking, and many other factors have combined to offer several options in which cost often becomes one of the biggest components.

An *on-premises datacenter* can be thought of as the old, traditional approach: the data and the servers are kept in house. One alternative to this is to share a *colocation*. In this arrangement, several companies put their "servers" in a shared space. The advantage to this approach is that by renting space in a third-party facility, it is often possible to gain advantages associated with connectivity speed, and possibly technical support. When describing this approach, we placed "servers" in quotation marks because the provider will often offer virtual servers rather than dedicated machines for each client, thus enabling companies to grow without a reliance on physical hardware.

Incidentally, any remote and autonomous office, regardless of the number of users who may work from it, is known as a *branch office*. This point is important because it may be an easy decision to keep the datacenter on-premises at headquarters, but network administrators need to factor in how to best support branch offices as well. The situation could easily be that while on-premises works best at headquarters, all branch offices are supported by colocation sites.

Storage-Area Networks

When it comes to data storage in the cloud, encryption is one of the best ways to protect it (keeping it from being of value to unauthorized parties), and VPN routing and forwarding can help. Backups should be performed regularly (and encrypted and stored in safe locations), and access control should be a priority.

The consumer retains the ultimate responsibility for compliance. Per NIST SP 800-144,

> The main issue centers on the risks associated with moving important applications or data from within the confines of the organization's computing center to that of another organization (i.e., a public cloud), which is readily available for use by the general public. The responsibilities of both the organization and the cloud provider vary depending on the service model. Reducing cost and increasing efficiency are primary motivations for moving towards a public cloud, but relinquishing responsibility for security should not be. Ultimately, the organization is accountable for the choice of public cloud and the security and privacy of the outsourced service.

For more information, see http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf.

Shared storage can be done on *storage-area networks (SANs)*, *network-attached storage (NAS)*, and so on; the virtual machine sees only a "physical disk." With clustered storage, you can use multiple devices to increase performance. A handful of technologies exist in this realm, and the following are those that you need to know for the Network+ exam.

> **Tip**
>
> Look to CompTIA's Cloud+ certification for more specialization in cloud and virtualization technologies.

iSCSI

The *Small Computer Systems Interface (SCSI)* standard has long been the language of storage. *Internet Small Computer Systems Interface (iSCSI)* expands this through Ethernet, allowing IP to be used to send SCSI commands.

Logical unit numbers (LUNs) came from the SCSI world and carry over, acting as unique identifiers for devices. Both NAS and SAN use "targets" that hold up to eight devices.

Using iSCSI for a virtual environment gives users the benefits of a file system without the difficulty of setting up Fibre Channel. Because iSCSI works both at the hypervisor level and in the guest operating system, the rules that govern the size of the partition in the OS are used rather than those of the virtual OS (which are usually more restrictive).

The disadvantage of iSCSI is that users can run into IP-related problems if configuration is not carefully monitored.

Fibre Channel and FCoE

Instead of using an older technology and trying to adhere to legacy standards, Fibre Channel (FC) is an option providing a higher level of performance than anything else. It utilizes FCP, the Fiber Channel Protocol, to do what needs to be done, and *Fibre Channel over Ethernet (FCoE)* can be used in high-speed (10 GB and higher) implementations.

The big advantage of Fibre Channel is its scalability. FCoE encapsulates FC over the Ethernet portions of connectivity, making it easy to add into an existing network. As such, FCoE is an extension to FC intended to extend the scalability and efficiency associated with Fibre Channel.

ExamAlert

Know that FCoE allows Fibre Channel to use 10 Gigabit Ethernet (or even higher) networks. This solves the problem of enterprises having to run parallel infrastructures for both LANs and SANs.

Network-Attached Storage

Storage is always a big issue, and the best answer is always a storage-area network. Unfortunately, a SAN can be costly and difficult to implement and maintain. That is where *network-attached storage (NAS)* comes in. NAS is easier than SAN and uses TCP/IP. It offers file-level access, and a client sees the shared storage as a file server.

Note

On a VLAN, multipathing creates multiple paths to the storage resources and can be used to increase availability *and* add fault tolerance.

ExamAlert

For the exam, you should know the difference between NAS and SAN technologies and how to apply them.

Cram Quiz

1. Logical unit numbers (LUNs) came from the SCSI world and use “targets” that hold up to how many devices?

○ **A.** 4

○ **B.** 6

○ **C.** 8

○ **D.** 128

2. What is the network architecture in which the database and the application exist on a single system?

○ **A.** *N*-tiered

○ **B.** One-tiered

○ **C.** Two-tiered

○ **D.** Three-tiered

3. On a VLAN, what creates multiple paths to the storage resources and can be used to increase availability and add fault tolerance?

   ❍ **A.** FCoE

   ❍ **B.** Adding a management plane

   ❍ **C.** Colocating

   ❍ **D.** Multipathing

4. What traffic pattern refers to data that travels outside the datacenter or enterprise?

   ❍ **A.** East-to-West

   ❍ **B.** North-to-South

   ❍ **C.** On-premises

   ❍ **D.** West-to-South

5. What layer in three-tiered network architecture is considered the backbone of a network?

   ❍ **A.** Core layer

   ❍ **B.** Distribution/aggregation layer

   ❍ **C.** Access/edge layer

   ❍ **D.** Application layer

Cram Quiz Answers

1. **C.** LUNs came from the SCSI world and carry over, acting as unique identifiers for devices. Both NAS and SAN use “targets” that hold up to eight devices.
2. **B.** The network architecture in which the database and the application exist on a single system is called a one-tiered model.
3. **D**. On a VLAN, multipathing creates multiple paths to the storage resources and can be used to increase availability and add fault tolerance.
4. **B.** North-South refers to data transfers between the datacenter and that outside of the network. East-West traffic is a concept referring to network traffic flow within a datacenter between servers. On-premises can be thought of as the old, traditional approach: the data and the servers are kept in house. Although West-to-South is a direction, it is not a valid specified data path.
5. **A.** The core layer is the backbone of the network where the fastest routers and switches operate to manage separate networks. The distribution/aggregation layer is between the access/edge and core layers. This is the “boundary” layer where ACLs and Layer 3 switches operate. The access/edge layer is the place where switches connect to and ensure data is delivered to edge/end devices. The application layer is the seventh and top layer of the OSI reference model.

What’s Next?

For the Network+ exam, and for routinely working with an existing network or implementing a new one, you need to identify the characteristics of network media and their associated cabling. Chapter 5, “Cabling Solutions and Issues,” focuses on the media and connectors used in today’s networks and what you are likely to find in wiring closets.

Index