Microsoft®

CompTIA® Network+®

Exam N10-005

Rapid Review

Craig Zacker

Rapid Review

CompTIA Network+ Exam N10-005

Assess your readiness for CompTIA Network+ Exam N10-005—and quickly identify where you need to focus and practice. This practical, streamlined guide walks you through each exam objective, providing "need to know" checklists, review questions, tips, and links to further study—all designed to help bolster your preparation

Reinforce your exam prep with a *Rapid Review* of these objectives:

- Network Concepts
- Network Installation and Configuration
- Network Media and Topologies
- Network Management
- Network Security

This book is an ideal complement to the in-depth training of the Microsoft Press® *Training Kit* and other exam-prep resources for CompTIA Network+ Exam N10-005.

CompTIA Network+®

ABOUT THE AUTHOR

Craig Zacker, an editor and educator, has written or contributed to dozens of books on networking, operating systems, and PC hardware, including *CompTIA Network+ Training Kit (Exam N10-005)* and *MCITP Self-Paced Training Kit (Exam 70-686): Windows® 7 Desktop Administrator.*

CompTIA AUTHORIZED PARTNER

CompTIA APPROVED QUALITY CONTENT

ISBN: 978-0-7356-6683-2

9 780735 666832 90000

U.S.A. $29.99
Canada $31.99
[*Recommended*]

*Certification/
CompTIA Network+*

Microsoft®

Microsoft®

CompTIA® Network+® Rapid Review (Exam N10-005)

Craig Zacker

ISBN: 978-0-7356-6683-2

1 2 3 4 5 6 7 8 9 LSI 7 6 5 4 3 2

Printed and bound in the United States of America.

Microsoft Press books are available through booksellers and distributors worldwide. If you need support related to this book, email Microsoft Press Book Support at *mspinput@microsoft.com*. Please tell us what you think of this book at *http://www.microsoft.com/learning/booksurvey*.

The example companies, organizations, products, domain names, email addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

This book expresses the author's views and opinions. The information contained in this book is provided without any express, statutory, or implied warranties. Neither the author, Microsoft Corporation, nor its resellers, or distributors
will be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

Acquisitions and Developmental Editor: Kenyon Brown

Production Editor: Rachel Steely

Editorial Production and Illustration: Diane Kohnen, S4Carlisle Publishing Services

Technical Reviewer: Brian Blum

Copyeditor: Andrew Jones

Indexer: Stephen R. Ingle

Cover Design: Best & Company Design

Cover Composition: Karen Montgomery

Contents at a Glance

Contents

Introduction

This Rapid Review is designed to assist you with studying for the CompTIA Network+ exam N10-005. The Rapid Review series is designed for exam candidates who already have a good grasp of the exam objectives through a combination of experience, skills, and study, and could use a concise review guide to help them assess their readiness for the exam.

The N10-005 exam is aimed at an IT networking professional who has:

- CompTIA A+ certification or equivalent knowledge
- A minimum of 9 to 12 months of experience in IT networking

Although this experience would preferably include foundation-level networking skills and knowledge, you might have real-world experience. Most candidates who take this exam have the knowledge and skills that are required to implement a defined network architecture with basic network security. Furthermore, a successful candidate will be able to configure, maintain, and troubleshoot network devices using appropriate network tools and understand the features and purpose of network technologies. Candidates will be able to make basic solution recommendations, analyze network traffic, and be familiar with common protocols and media types. It is important to note that you should have some real-world experience with networking prior to taking the N10-005 exam and that having practical knowledge is a key component to achieving a passing mark.

This book will review every concept described in the following exam objective domains:

- Objective 1.0: Network Concepts
- Objective 2.0: Network Installation and Configuration
- Objective 3.0: Network Media and Topologies
- Objective 4.0: Network Management
- Objective 5.0: Network Security

This is a Rapid Review and not a comprehensive guide such as the *CompTIA Network+ Training Kit*. The book covers every exam objective on the N10-005 exam, but will not necessarily cover every exam question. CompTIA regularly adds new questions to the exam, making it impossible for this (or any) book to provide every answer. Instead, this book is designed to supplement your existing independent study and real-world experience with the product.

If you encounter a topic in this book that you do not feel completely comfortable with, you can visit the links described in the text, in addition to researching the topic further using other websites, as well as consulting support forums. If you review a topic and find that you don't understand it, you should consider consulting the *CompTIA Network+ Training Kit* from Microsoft Press. You can also purchase practice exams, or use the one available with the Training Kit, to further determine if you need further study on particular topics.

NOTE **The Rapid Review is designed to assess your readiness for the N10-005 exam. It is not designed as a comprehensive exam preparation guide. If you need that level of training for any or all of the exam objectives covered in this book, we suggest the *CompTIA Network+ Training Kit* (ISBN: 9780735662759). The Training Kit provides comprehensive coverage of each N10-005 exam objective, along with exercises, review questions, and practice tests. The Training Kit also includes a discount voucher for the exam.**

CompTIA Professional Certification Program

CompTIA professional certifications cover the technical skills and knowledge needed to succeed in a specific IT career. Certification is a vendor-neutral credential. An exam is an internationally recognized validation of skills and knowledge, and is used by organizations and professionals around the globe. CompTIA certification is ISO 17024 Accredited (Personnel Certification Accreditation) and, as such, undergoes regular reviews and updates to the exam objectives. CompTIA exam objectives reflect the subject areas in an edition of an exam, and result from subject-matter expert workshops and industry-wide survey results regarding the skills and knowledge required of a professional with a number of years of experience.

MORE INFO **For a full list of CompTIA certifications, go to *http://certification.comptia.org/getCertified/certifications.aspx*.**

Support and feedback

The following sections provide information on errata, book support, feedback, and contact information.

Errata

We've made every effort to ensure the accuracy of this book and its companion content. Any errors that have been reported since this book was published are listed on our Microsoft Press site:

http://www.microsoftpressstore.com/title/9780735666832

If you find an error that is not already listed, you can report it to us through the same page.

If you need additional support, email Microsoft Press Book Support at *mspinput@microsoft.com.*

Please note that product support for Microsoft software is not offered through the addresses above.

We want to hear from you

At Microsoft Press, your satisfaction is our top priority, and your feedback our most valuable asset. Please tell us what you think of this book at:

http://www.microsoft.com/learning/booksurvey

The survey is short, and we read every one of your comments and ideas. Thanks in advance for your input!

Stay in touch

Let’s keep the conversation going! We’re on Twitter: *http://twitter.com/MicrosoftPress*.

Preparing for the exam

CompTIA certification exams are a great way to build your resume and let the world know about your level of expertise. Certification exams validate your on-the-job experience and product knowledge. Although there is no substitute for on-the-job experience, preparation through study and hands-on practice can help you prepare for the exam. We recommend that you augment your exam preparation plan by using a combination of available study materials and courses. For example, you might use the Training Kit and another training kit for your "at home" preparation, and take a CompTIA professional certification course for the classroom experience. Choose the combination that you think works best for you.

CHAPTER 1

Network Concepts

The Network Concepts domain accounts for approximately 21% of the CompTIA Network+ exam, but more than that, it covers some of the most fundamental principles of computer networking. These are concepts that you encounter repeatedly, both as you prepare for the exam and as you work in the IT field.

To excel at this objective, you must possess a good grasp of certain organizational concepts, such as the OSI reference model; an understanding of basic networking functions, such as IP addressing; and some memorized facts and figures, such as well-known port numbers.

This chapter covers the following objectives:

- Objective 1.1: Compare the layers of the OSI and TCP/IP models
- Objective 1.2: Classify how applications, devices, and protocols relate to the OSI model layers
- Objective 1.3: Explain the purpose and properties of IP addressing
- Objective 1.4: Explain the purpose and properties of routing and switching
- Objective 1.5: Identify common TCP and UDP default ports
- Objective 1.6: Explain the function of common networking protocols
- Objective 1.7: Summarize DNS concepts and components
- Objective 1.8: Given a scenario, implement proper network troubleshooting methodology
- Objective 1.9: Identify virtual network components

Objective 1.1: Compare the layers of the OSI and TCP/IP models

For this exam objective, you must know the structure of the two basic models defining the networking process: the OSI reference model and the TCP/IP model. The OSI model is designed to be independent of any specific networking implementation, and as a result, it does not conform precisely to the networking stacks in general use today. By contrast, the TCP/IP model was designed with specific protocols in mind, and is pertinent only on networks using those protocols. However, virtually all networks today use TCP/IP, so the TCP/IP model is as viable as the OSI model for demonstration, documentation, and discussion purposes.

Exam need to know

- OSI model

  For example: Do you know that the OSI reference model consists of seven layers: Layer 1 – Physical; Layer 2 – Data link; Layer 3 – Network; Layer 4 – Transport; Layer 5 – Session; Layer 6 – Presentation; and Layer 7 – Application?

- TCP/IP model

  For example: Do you know that the model of the TCP/IP protocol stack consists of four layers: the network interface layer (also known as the link layer); the internet layer; the transport layer; and the application layer?

OSI model

The Open Systems Interconnection (OSI) reference model is a theoretical example of a network protocol stack, which networking educators and administrators use to categorize and define a computer's various networking functions. The top of the model interacts with the applications running on the computer, which might at times require the services of the network. The bottom of the model connects to the network medium over which the system transmits its signals, as shown in Figure 1-1. There are different protocols operating at the various layers of the model, each of which provides functions needed to complete the network communication process.

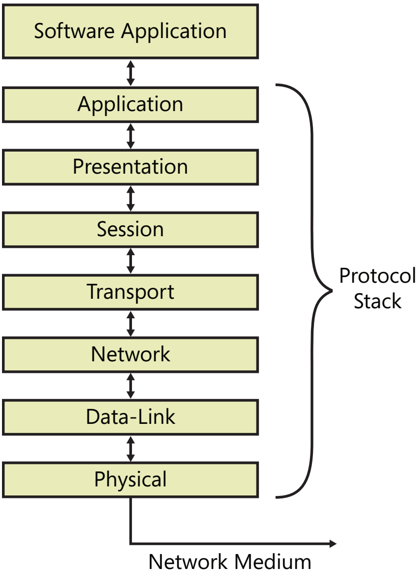

FIGURE 1-1 The seven layers of the OSI reference model.

True or false: The layers of the OSI reference model correspond to the initials of the mnemonic "All People Seem To Need Data Processing."

Answer: *True*. The layers of the OSI model, from top to bottom, are application, presentation, session, transport, network, data-link, and physical.

> ***EXAM TIP*** **While most of the mnemonics that students use to remember the OSI model layers list them from top to bottom, the OSI model layers are traditionally numbered from bottom to top, with the physical layer being Layer 1 and the application layer being Layer 7. One mnemonic for this is "Please Do Not Tell Secret Passwords Anytime."**

> ***MORE INFO*** **The upper layers of the OSI model are seldom referenced by number. The most common use for the layer numbers is in discussions of routing and switching technologies. Switches operate primarily at Layer 2, the data-link layer, and routers at Layer 3, the network layer. However, these devices can have capabilities that span to other layers, resulting in references to technologies such as Layer 3 switching. For more information, see Objectives 1.2 and 1.4.**

TCP/IP model

The development of the TCP/IP protocols began years before the documents defining the OSI reference model were published, but the protocols conform to a layered model in much the same way. Instead of the seven layers used by the OSI model, the TCP/IP model—sometimes called the Department of Defense (DoD) model—has four layers. The TCP/IP model layers, in comparison with those of the OSI model, are shown in Figure 1-2.

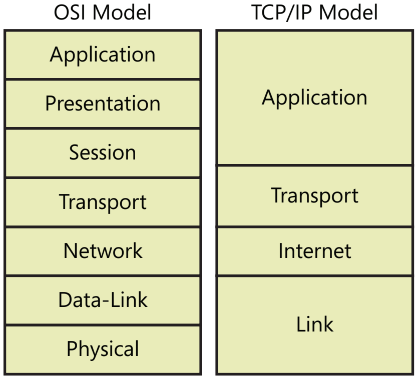

FIGURE 1-2 The four TCP/IP model layers, compared with the seven-layer OSI reference model.

The TCP/IP model layers—even those with the same names—are not exactly analogous to the OSI model layers, nor were the models created with the same intent. The OSI model is intended to be a guide for the creation of networking protocols, whereas the TCP/IP model is a representation of protocols that already exist.

True or false: The link layer of the TCP/IP protocol stack is exactly congruent to the data-link and physical layers of the OSI model.

Answer: *False*. Despite being roughly analogous to the OSI data-link layer, the TCP/IP link layer does not include physical specifications of any kind, nor does it include complex LAN protocols such as Ethernet. Therefore, on many TCP/IP networks, the protocol operating at the link layer might not be part of the TCP/IP suite.

> ***EXAM TIP*** **In the TCP/IP model, the term "internet" is a generic reference to an internetwork and uses a lowercase "i," as opposed to the public, packet-switching network known as the Internet, with an uppercase "I." Be careful not to confuse the two.**

True or false: The TCP/IP protocol stack was designed to conform to the OSI reference model.

Answer: *False*. Most of the TCP/IP protocols that make up the protocol stack were designed and developed in the 1970s, and therefore predate the OSI reference model. In fact, there is no protocol stack in common use that conforms precisely to the OSI layers. Although originally intended to be a model for an actual networking solution, OSI is now used only as an educational and organizational tool.

> ***EXAM TIP*** **The N10-005 revision of the Network+ exam objectives released in 2011 adds the TCP/IP model and specifically requires students to compare its layers with those of the OSI model. Be careful to distinguish between the two models, and familiarize yourself with the differences between the corresponding layers.**

> ***MORE INFO*** **For more information about the structure of the TCP/IP model, see RFC 1122, "Requirements for Internet Hosts – Communication Layers," available at *http://tools.ietf.org/html/rfc1122*.**

Can you answer these questions?

Find the answers to these questions at the end of this chapter.

1. What is the primary TCP/IP protocol operating at the link layer of the TCP/IP model?
2. Which of the OSI model layers do not have TCP/IP protocols directly associated with them?
3. What are the two protocols operating at the transport layer in both the OSI and TCP/IP models?
4. What organizations were responsible for publishing the original documents defining the OSI reference model and the TCP/IP model?

Objective 1.2: Classify how applications, devices, and protocols relate to the OSI model layers

One of the primary functions of the OSI model is to organize and separate the various elements of the networking process. When defining the function of a network element, such as a protocol, device, or application, it is common to begin by specifying the OSI model layer at which the element operates. This helps to categorize the function of the element and provides a basic idea of its purpose.

For example, a data-link layer device is generally understood to be involved in local network communications, while the network and transport layers are devoted to end-to-end communications that can span multiple networks. The Network+ exam requires you to understand the functions of many different applications, devices, and protocols, and classifying those elements using the OSI model is the first step to achieving that understanding.

Exam need to know

- Classify how MAC addresses relate to the OSI model layers.

  For example: At which layer of the OSI model are network nodes identified using MAC addresses?
- Classify how IP addresses relate to the OSI model layers.

  For example: At which layer of the OSI model are network nodes identified using IP addresses?
- Classify how EUI-64 relates to the OSI model layers.

  For example: In what layer of the OSI reference model do you find an EUI-64?
- Classify how frames relate to the OSI model layers.

  For example: Which layer of the OSI model uses the term “frame” to refer to the protocol data unit generated by a networking protocol?
- Classify how packets relate to the OSI model layers.

  For example: At which layer of the OSI reference model are data structures called packets?
- Classify how switches relate to the OSI model layers.

  For example: At which layer of the OSI model do switches perform their basic functions?
- Classify how routers relate to the OSI model layers.

  For example: At which layer of the OSI model do routers perform their basic functions?
- Classify how multilayer switches relate to the OSI model layers.

  For example: At which layers of the OSI model do multilayer switches perform their functions?
- Classify how hubs relate to the OSI model layers.

  For example: At which layer of the OSI model do hubs perform their basic functions?
- Classify how encryption devices relate to the OSI model layers.

  For example: Which layer of the OSI model is responsible for encrypting data?
- Classify how cables relate to the OSI model layers.

  For example: Which layer of the OSI model defines the properties of network cables?

- Classify how NICs relate to the OSI model layers.

  For example: At which layer of the OSI model do NICs operate?
- Classify how bridges relate to the OSI model layers.

  For example: At which layer of the OSI model do bridges perform their basic functions?

MAC addresses

A media access control (MAC) address, also known as a hardware address, is a six-byte hexadecimal value that local area networking (LAN) protocols at the data-link layer use to identify systems on a shared network medium. Manufacturers of network interface adapters permanently assign a unique MAC address to each adapter, so that there can be no address duplication on any network.

True or false: Ethernet devices use MAC addresses to identify the source and the destination of each frame they transmit over the network.

Answer: *True.* The Ethernet frame format contains a six-byte Source Address field and a six-byte Destination Address field, which together function like the addresses on a postal envelope.

> ***MORE INFO*** **Data-link layer protocols are concerned only with LAN communications, so the values in the Destination Address and Source Address fields must identify systems on the local network. If a computer on the LAN is transmitting to another computer on the same LAN, then its packets contain the address of that target computer in their Destination Address fields. If a computer is transmitting to another computer on a different network, then the value in the Destination Address field must be the address of a router on the LAN.**

True or false: Internet transmissions use a MAC address to identify the final recipient of a message.

Answer: *False.* Internet transmissions use an Internet Protocol (IP) address to identify the final recipient of a message, not a MAC address. This is because MAC addresses are local. A packet might pass through multiple LANs on the way to a destination on the Internet, and have different destination MAC addresses as it does so.

> ***EXAM TIP*** **For the Network+ exam, you must be able to distinguish MAC addresses from IP addresses. A MAC address is a six-byte hexadecimal value, such as 60-EB-69-93-5E-E4. An IP version 4 address is 32 bits, generally expressed in four octets of dotted decimal notation, as in 192.168.76.3. An IP version 6 address is 128 bits long, and generally expressed in 8 groups of 16-bit hexadecimal values separated by colons, such as fe80::7441:4473:f204:ec1d.**

IP addresses

The Internet Protocol (IP) is the primary end-to-end protocol in the TCP/IP networking stack. Operating at the network layer of the OSI model (and the internet layer of the TCP/IP model), IP has its own addressing system, which it uses to identify systems on the network.

As with Ethernet, IP has header fields that contain the IP addresses of the source and destination systems involved in a network transaction. The difference between the two is that IP uses IP addresses instead of MAC addresses, and the Destination IP Address field identifies the final recipient of the transmission.

True or false: Ethernet systems on a TCP/IP network have a protocol that converts network layer IP addresses to data-link layer MAC addresses.

Answer: *True*. Address Resolution Protocol (ARP) converts IP addresses into MAC addresses by broadcasting request packets containing the IP address on the local network and waiting for the holder of that IP address to respond with a reply containing the equivalent MAC address.

> ***MORE INFO*** **IP is currently in transition from version 4 to version 6, and the two versions have different address formats. For more information, see "Objective 1.3: Explain the purpose and properties of IP addressing."**

True or false: Packets on a TCP/IP network can have two destination addresses pointing to different systems.

Answer: *True*. The IP header at the network layer has a Destination IP Address field that always specifies the ultimate destination of the packet. At the same time, the Ethernet header at the data-link layer will have a changing Destination Address field that points to the next intermediary system on the local network, until it finally reaches the ultimate destination network, at which point both addresses will point to the same ultimate destination.

EUI-64

The extended unique identifier-64 (EUI-64) is a 64-bit value that some TCP/IP systems use to form the second half of a 128-bit IPv6 address. The IPv6 address is a network layer structure, but the EUI-64 value for a system is derived from its data-link layer MAC address.

True or false: No two computers can legitimately have the same EUI-64 value in their IPv6 addresses.

Answer: *True*. The EUI-64 value that makes up the second half of some IPv6 addresses is taken from the system's MAC address, which, by definition, is unique. Therefore, no two EUI-64 values on different systems can be identical, unless an individual is making a deliberate attempt to spoof the IPv6 address.

MORE INFO **To derive the 64-bit EUI-64 value for an interface, an IPv6 implementation splits the 48-bit MAC address into two 24-bit halves, and takes the two 24-bit values and adds a 16-bit value between them: *11111111 11111110* in binary or *ff fe* in hexadecimal. Finally, it changes the seventh bit in the OUI—called the universal/local bit—from a 0 to a 1. This changes the hexadecimal value of the first byte in the address from 00 to 02. Therefore, a computer with a network adapter that has a MAC address of *00-1a-6b-3c-ba-1f* would have an IPv6 global unicast address with the following EUI-64 value: *021a:6bff:fe3c:ba1f*.**

True or false: All IPv6 addresses include the system's EUI-64 value.

Answer: *False*. Some IPv6 implementations avoid using the EUI-64 value, for fear that it might be possible to track the physical location of a computer based on its IPv6 address.

Frames

The data structures created by the protocols at the various layers of the OSI reference model have different names. At the data-link layer, the structure that a protocol creates when it encapsulates a network layer message is called a frame. The term frame is not used at any other layer.

Unlike the protocols at the upper layers, a data-link layer frame consists of both a header and a footer, which the protocol adds to the data it receives from the network layer. The resulting frame is the final element added to the data packet, which is then ready for transmission over the network.

True or false: A data-link layer frame includes an error detection mechanism.

Answer: *True*. The frame check sequence (FCS) field in the data-link layer footer contains a checksum calculated by the source computer. Once the frame reaches its destination, the receiving computer performs the same calculation and compares the results to the FCS value. If the two fail to match, then the frame has been corrupted or modified in transit.

EXAM TIP **Candidates for the Network+ exam should be familiar with the terminology used for the data units created by the various protocols in the TCP/IP stack. Data-link layer protocols create "frames." IP, at the network layer, creates "packets." Connectionless protocols such as UDP, at the transport layer, create units called "datagrams." Because IP is a connectionless protocol, the term datagram can apply to those data units as well. The TCP protocol at the transport layer creates individual messages called "segments," which are part of a "sequence."**

True or false: All data-link layer frames include source and destination MAC addresses.

Answer: *False*. Ethernet frames always include source and destination MAC addresses, but there are data-link layer protocols other than Ethernet that do not. The Point-to-Point Protocol (PPP) is designed for use on wide area network (WAN) connections between systems. Because there are only two systems involved in a WAN connection, there is no need to include addresses in every frame.

> ***EXAM TIP*** **There are several different variants of the Ethernet frame format, the selection of which depends on the version of the Ethernet standard the system is configured to use. The formats are functionally the same, but for systems on the network to communicate, they must all be using the same frame format.**

Packets

Although it is often mistakenly used to refer to the entire data structure transmitted over the network, the term packet actually refers to the unit of data carried inside a data-link layer frame. A packet is therefore a network layer structure.

On a packet-switching internetwork, such as the Internet, packets might travel through dozens of networks, with the router for each network stripping off the previous frame and applying its own frame to the data. The packet inside these many different frames remains intact, however.

True or false: Every TCP/IP packet contains a frame.

Answer: *False*. The packet is the network-layer data carried within the data-link layer frame. Therefore, every frame contains a packet.

> ***EXAM TIP*** **The Network+ exam might also refer to the network layer data unit as a datagram. Technically, a datagram is the data unit created by a connectionless protocol. This is why both IP and UDP generate datagrams. However, because there is no connection-oriented protocol at the network layer, the terms datagram and packet are synonymous in TCP/IP networking.**

True or false: Every TCP/IP packet must contain a transport layer datagram or segment.

Answer: *False*. Packets carrying transport layer data must contain a UDP datagram or a TCP segment, but there are also packets that carry Internet Control Message Protocol (ICMP) data directly within the IP datagram, which do not use UDP or TCP.

Switches

A switch is a data-link layer device that connects computers and other systems together into a LAN. Basic switches consist of a box or a rack-mounted module with one or more rows of female cable connectors. Plugging devices into the connectors enables them to communicate with each other by transmitting packets.

Unlike hubs, switches have intelligence that enables them to determine the address of the device connected to each port. When a unicast packet arrives through any of the switch's ports, the switch reads its destination addresses and forwards the packet out through the port providing access to the destination system.

True or false: Switches have almost completely replaced hubs on today's local area networks.

Answer: *True*. Switches conserve network bandwidth by delivering packets only to their intended recipients. On a hub-based network, every computer must receive and process every packet received by the hub.

> ***MORE INFO*** **In addition to functioning at the data-link layer, switches can also have network layer capabilities as well. For more information, see "Objective 1.4: Explain the purpose and properties of routing and switching," and "Objective 2.1: Given a scenario, install and configure routers and switches."**

True or false: All switched networks use a bus topology.

Answer: *False*. A switch functions as the cabling nexus for a LAN. Each computer has its own cable connecting it to the switch. Switched networks can therefore be said to use a star topology.

> ***EXAM TIP*** **The Network+ exam has, at times, referred to the relatively simple switching devices used in home and small-to-medium office networks as "basic switches." These are strictly data-link layer devices that do not have advanced features, such as VLANs.**

Routers

A router is a network layer component that connects two networks together, selectively forwarding only the traffic that is destined for the other network. Because most large networks today are switched internally, the primary function of routers is to connect LANs to WAN connections.

Routers also have tables containing information about other networks, which enable them to direct incoming packets to their ultimate destinations.

True or false: Splitting a network with a router reduces the amount of broadcast traffic on the network.

Answer: *True*. Unlike switches, hubs, and bridges, routers do not forward broadcast traffic.

> ***MORE INFO*** **For more information on routing, see "Objective 1.4: Explain the purpose and properties of routing and switching," and "Objective 2.1: Given a scenario, install and configure routers and switches."**

True or false: A router must have at least two network interfaces.

Answer: *False*. By the traditional definition, a router must be connected to two or more networks, so it must have at least two network interfaces. These interfaces can be standard LAN adapters, or any type of WAN equipment. However, with the advent of virtual LANs, there are now routers available with a single interface. Called stub routers or one-armed routers, these devices connect to a switch and route traffic between VLANs.

Multilayer switches

A multilayer switch is an advanced networking device that, in addition to functioning as a standard data-link layer switch, also supports functions associated with other OSI model layers, most particularly network layer routing.

True or false: In addition to the data-link layer, switches can also operate at the network layer.

Answer: *True*. Advanced switches have the ability to create virtual LANs (VLANs), which are subnets that exist only in the switch. To enable VLANs to communicate with each other, these switches also support virtual routing, which is a network layer process.

> ***MORE INFO*** **For more information on VLANs and advanced switching techniques, see "Objective 2.1: Given a scenario, install and configure routers and switches."**

Hubs

A hub is a cabling nexus for a LAN using a star topology. Unlike a switch, which is often similar in appearance, a hub is a purely physical layer device. The hub amplifies the signals entering through any of its ports and forwards them out through all of the other ports, creating a shared network medium.

True or false: Hubs can read the destination addresses from the frames arriving through its ports.

Answer: *False*. Hubs lack any ability to interpret incoming signals. They are electrical devices that manipulate signals at the physical level, but they cannot interpret them.

> ***EXAM TIP*** **Having been largely replaced by switches, hubs are all but obsolete in the networking world today, and are less likely to appear on the Network+ exam than they have on previous iterations of the test.**

True or false: Replacing a hub with a switch increases the efficiency of a LAN.

Answer: *True*. While a hub forwards incoming signals out through all of its ports, switches only forward signals out through the destination port. This conserves bandwidth and provides each pair of computers with what amounts to a dedicated link.

> ***NOTE*** **A repeater is a device that extends the maximum length of a network cable by amplifying the signals passing over it. Because hubs do essentially the same thing for all of their connected devices, they are sometimes referred to as multiport repeaters.**

Encryption devices

The term encryption device refers to any mechanism that employs an algorithm to cryptographically encode data. Encryption devices can be as large as a server or as small as a USB flash drive. Whatever the form of the device, however, the encryption process is carried out at the presentation layer of the OSI model.

True or false: On TCP/IP systems, encryption algorithms are standalone protocols that run at the presentation layer of the OSI model.

Answer: *False*. There are no standalone presentation layer protocols in the TCP/IP suite. Presentation layer functions, including encryption, are typically incorporated into application layer protocols.

> ***EXAM TIP*** **Unlike the other hardware components mentioned in this objective, there are no dedicated networking components called encryption devices. Encryption is a function that is incorporated into other hardware and software components. Therefore, while the Network+ exam might refer to encryption devices, this is solely for the purpose of testing your knowledge that encryption is a presentation layer process.**

Cables

Cables are the physical layer components that form the network medium on most LANs. Depending on the topology, distance, and environmental requirements for the network, LANs use one of the following three basic cable types: coaxial, twisted pair, or fiber optic.

True or false: Coaxial cables are no longer used to build new Ethernet LANs.

Answer: *True*. Coaxial Ethernet networks require a bus topology, and for various reasons, including cost and ease of installation, this type of cable is no longer used.

NICs

The network interface adapter, also known as a network interface card or NIC, is the hardware implementation of the data-link layer protocol. Virtually all of the NICs sold today are Ethernet, with models available that support various speeds, expansion buses, and cable types.

True or false: Most of the desktop computers manufactured today have an Ethernet network interface adapter integrated into the motherboard.

Answer: *True*. Ethernet network interface adapters are all but ubiquitous on the motherboards manufactured for desktop computers.

> ***EXAM TIP*** **The Network+ exam might persist in using the term NIC (pronounced as "nick"), even when referring to a network interface adapter that is not actually an expansion card.**

True or false: Every NIC has a unique MAC address permanently assigned by the manufacturer.

Answer: *True*. It is the network interface adapter that has the MAC address assigned to it by the hardware manufacturer, whether the adapter is a separate card or integrated into the motherboard.

Bridges

A bridge is a data-link layer device that splits a LAN in half and selectively forwards traffic based on its destination address. When a packet arrives through one of the bridge's interfaces, the bridge reads the destination hardware address from the Ethernet header. If the packet is destined for a computer on the other side of the bridge, it forwards the packet out through its other interface. If the packet is destined for a computer on the same side of the bridge from which it was received, the bridge simply discards the packet.

True or false: Installing a bridge on a LAN splits the network into two separate broadcast domains.

Answer: *False*. Bridges forward all broadcasts to the other side of the network. The address-based filtering they perform is limited to unicast transmissions.

EXAM TIP **The Network+ exam objectives still mention bridges, even though the devices are rarely used on today's networks.**

NOTE **Bridges possess a degree of intelligence similar to that of switches. A basic switch is, in essence, nothing more than a multiport bridge.**

Can you answer these questions?

Find the answers to these questions at the end of this chapter.

1. Only one of the items listed in this objective is associated with an OSI model layer other than the physical, data-link, or network. Which is it?
2. You can build a simple Ethernet LAN with nothing more than a NIC for each computer, a switch, and some cables. Which of those components are associated exclusively with the physical layer of the OSI model?
3. A multilayer switch functions primarily at which two layers of the OSI reference model?
4. Which of the devices listed in this objective can split a network into two broadcast domains?
5. Which layer of the OSI model uses addresses that can be 32 or 128 bits long?

Objective 1.3: Explain the purpose and properties of IP addressing

IP addressing is one of the fundamental functions of the TCP/IP protocol suite and the network layer IP. Every device on an internetwork must have a unique IP address, so that IP can address packets specifically to it. IP addresses specify both the network on which the device is located and the device itself, called a host, on that particular network. Routers use the network identifier to forward packets to the correct network, and the router on the destination network uses the host identifier to forward the packets to the correct device.

Exam need to know

- Explain the intended purpose and properties of now-obsolete IP address classes**.**

  For example: Which IP address class provided the largest number of hosts per subnet?
- Explain the purpose and properties of Classless Inter-Domain Routing (CIDR).

  For example: How many bits are allocated for the host identifier in the 10.0.54.0/24 network address?
- Explain the purpose and properties of IPv4 and IPv6 formatting.

  For example: What is the largest possible value for each of the four decimal numbers in an IPv4 address?
- Explain the purpose and properties of the MAC address format.

  For example: What is the term used for the first three bytes of a MAC address?
- Explain the purpose and properties of subnetting.

  For example: How many hosts can you create on a subnet with the mask 255.255.255.240?
- Explain the purpose and properties of multicasts, unicasts, and broadcasts.

  For example: What is the standard MAC address value used for a broadcast transmission?
- Explain the purpose and properties of APIPA.

  For example: What is the IPv4 network used by default for Automatic Private IP Addressing?

IP address classes

IPv4 addresses contain both a network identifier and a host identifier, which means that some of the 32 bits in the address specify the network on which the host is located and the rest of the bits identify the specific host on that network. However, the division between the network identifier bits and the host identifier bits is not always in the same place. The original IP standard defined three primary classes of

IP addresses: A, B, and C, which provided support for networks of different sizes, as shown in Figure 1-3.

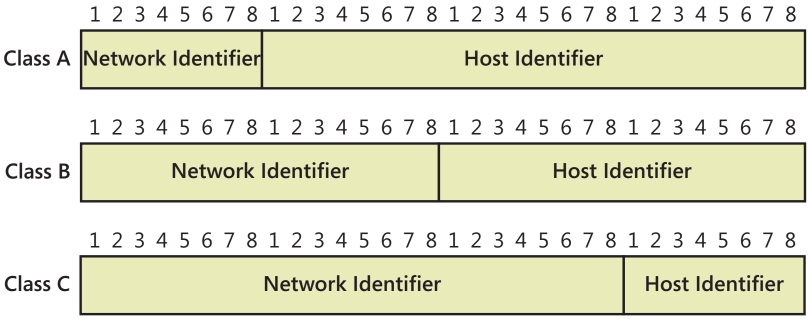

FIGURE 1-3 The three primary classes of IPv4 addresses.

The characteristics of these three address classes are listed in Table 1-1.

TABLE 1-1 IPv4 address classes.

IP ADDRESS CLASS	CLASS A	CLASS B	CLASS C
First bit values (binary)	0	10	110
First byte value (decimal)	0 -127	128-191	192-223
Number of network identifier bits	8	16	24
Number of host identifier bits	24	16	8
Number of possible networks	126	16,384	2,097,152
Number of possible hosts	16,777,214	65,534	254

The “First bit values” row in the table specifies the values that the first one, two, or three bits of an address in each class must have. Early TCP/IP implementations used these bit values to determine the class of an address.

For web servers and other computers to be accessible by clients on the Internet, they must have public IP addresses, that is, addresses registered with an authority, such as an Internet service provider (ISP). For workstations and other computers that do not require an Internet presence, administrators typically use private IP addresses, which are freely available for use on any network and are not registered as belonging to any particular organization.

The private address ranges for each class are as follows:

- **Class A** 10.0.0.0 through 10.255.255.255
- **Class B** 172.16.0.0 through 172.31.255.255
- **Class C** 192.168.0.0 through 192.168.255.255

True or false: You cannot assign all of the possible values in a given address class to network devices.

Answer: *True*. The host identifier values in each address class consisting of all zeroes and all ones are reserved; you cannot assign them to hosts. The all zeroes address identifies the network itself and the all ones address is the broadcast address for the network.

> ***NOTE*** **In addition to classes A, B, and C, the IP standard defines two additional address classes: Class D, which is used for multicast addresses; and Class E, which is experimental. Class D addresses begin with the bit values 1110, and Class E addresses begin with the values 11110.**

> ***EXAM TIP*** **The Network+ objectives refer to public and private addresses, but they are also sometimes known as registered and unregistered addresses. Candidates should be familiar with both sets of terms.**

True or false: A web server must have a public IP address to be accessible by clients on the Internet.

Answer: *True*. Public, or registered, IP addresses are assigned to particular organization and reserved for use by one host on the Internet.

> ***EXAM TIP*** **Although classful addressing is no longer used on the Internet, CompTIA continues to include it in the Network+ objectives and on the exam, for historical context.**

Classless inter-domain routing (CIDR)

There are many networks that have more than the 254 hosts provided by a Class C address, and there are none that have the 16 million provided by a Class A. The classful IP addressing system, therefore, proved to be wasteful as the IP address space grew crowded. CIDR is a subnetting method that enables administrators to place the division between the network bits and the host bits anywhere in the address, not just between octets. This makes it possible to create networks of almost any size.

CIDR also introduced a new notation for network addresses. A standard IPv4 network address is followed by a forward slash and a numeral specifying the size of the network identifier. For example, 192.168.43.0/24 represents an address that uses a 24-bit network identifier, leaving the other 8 bits for up to 254 host identifiers, which would formerly be known as a Class C address.

True or false: Classless IP addresses use the first few binary bits of the network identifier to specify the size of the network.

Answer: *False*. In a classless address, the size of the network is indicated by the suffix, or by the use of a subnet mask.

EXAM TIP **The CIDR notation is the most commonly used form of network address used on the Network+ exam. Candidates must know that the number following the slash specifies the size of the network identifier, and that the remaining bits identify the host.**

True or false: In the classless address 192.168.76.0/24, the number 24 specifies how many hosts you can create on the network.

Answer: *False*. The number 24 indicates the number of bits in the network identifier. There are therefore 8 host bits, allowing a maximum of 254 hosts on the network.

IPv4 and IPv6 address formatting

The original IP protocol standard calls for 32-bit IP addresses, but the depletion of the IPv4 address space led to the development of IPv6, which uses 128-bit addresses. The IP addresses used in networks around the world are currently in the midst of a lengthy conversion from IPv4 to IPv6.

An IPv4 address is a 32-bit value that contains both a network identifier and a host identifier. The address is notated by using four decimal numbers ranging from 0 to 255, separated by periods, as in 192.168.1.44. This is known as dotted decimal notation.

IPv6 addresses use a notation called colon-hexadecimal format, which consists of eight 16-bit hexadecimal numbers, separated by colons, as in the following example:

```
21cd:0053:0000:0000:e8bb:04f2:003c:c394
```

When an IPv6 address has two or more consecutive 8-bit blocks of 0s, you can replace them with a double colon. You can also remove the leading 0s in any block where they appear, as follows:

```
21cd:53::e8bb:4f2:3c:c394
```

True or false: The hexadecimal value 21cd:53::e8bb::3c:c394 is a valid IPv6 address.

Answer: *False*. A valid IPv6 address can only have one double colon in it.

EXAM TIP **Network+ candidates must be familiar with the rules for contracting IPv6 addresses.**

MORE INFO **For more information on the formation of IPv6 addresses, see the "EIU-64" section in "Objective 1.2: Classify how applications, devices, and protocols relate to the OSI model layers."**

MAC address formatting

The first three bytes of a MAC address, called the organizationally unique identifier (OUI), consist of a value assigned to the hardware manufacturer by the Institute of Electrical and Electronics Engineers (IEEE). The second three bytes consist of a unique value assigned by the manufacturer to each individual device.

True or false: Two computers can have the same OUI.

Answer: *True*. The OUI is a value assigned to a manufacturer of network interface adapters, and all of the adapters produced by that manufacturer will have MAC addresses with identical OUIs. Only the second three bytes of the MAC address on every adapter must be unique.

> ***EXAM TIP*** **Network+ candidates must be able to differentiate MAC addresses and IPv6 addresses, both of which use hexadecimal (base sixteen) notation.**

True or false: The Ipconfig.exe program on a Windows computer displays the MAC address assigned to the network interface adapter.

Answer: *True*. In addition to TCP/IP configuration settings, Ipconfig.exe identifies each of the network interface adapters in the computer and displays their MAC addresses, as in the third line of the following display.

```
Connection-specific DNS Suffix  . : zacker.local
Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
Physical Address. . . . . . . . . : 60-EB-69-93-5E-E5
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::7441:4473:f204:ec1d%10(Preferred)
IPv4 Address. . . . . . . . . . . : 192.168.2.9(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Lease Obtained. . . . . . . . . . : Sunday, April 15, 2012 1:11:50 PM
Lease Expires . . . . . . . . . . : Friday, April 27, 2012 1:11:48 PM
Default Gateway . . . . . . . . . : 192.168.2.99
DHCP Server . . . . . . . . . . . : 192.168.2.1
DHCPv6 IAID . . . . . . . . . . . : 241232745
DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-14-81-CC-39-60-EB-69-93-5E-E5
DNS Servers . . . . . . . . . . . : 192.168.2.1
Primary WINS Server . . . . . . . : 192.168.2.1
NetBIOS over Tcpip. . . . . . . . : Enabled
```

> ***MORE INFO*** **For more information on the formation of IPv6 addresses, see the "MAC Address" section in "Objective 1.2: Classify how applications, devices, and protocols relate to the OSI model layers."**

IP address subnetting

When the wastefulness of classful IP addressing was recognized, the designers of the IP protocol developed a system for subdividing network addresses by creating subnets within them. A subnet is simply a subdivision of a network address that administrators can use to represent a part of a larger network, such as one LAN on an internetwork or the client of an ISP. Thus, a large ISP might have a Class A address registered to it, and it might allocate sections of that network address to its clients in the form of subnets.

To understand the process of creating subnets, you must understand the function of the subnet mask. TCP/IP systems at one time recognized the class of an address simply by examining the values of its first three bits. Today, when you configure the TCP/IP client on a computer, you assign it an IPv4 address and a subnet mask. The subnet mask is a 32-bit value that specifies which bits of the IP address are the network identifier and which bits are the host identifier. For example, the subnet mask 255.255.255.0, in binary form, is 24 ones and eight zeroes. The ones are the network identifier bits and the zeroes are the host identifier bits.

True or false: To create eight-bit subnets on a Class A network address, you would use a subnet mask value of 255.255.0.0.

Answer: *True*. The subnet mask for a Class A address is 255.0.0.0. Borrowing eight bits from the host identifier to create subnets gives you a 16-bit network identifier. The subnet mask, therefore, consists of 16 ones and 16 zeroes, in binary form, or 255.255.0.0 in decimal form.

> ***EXAM TIP*** **Candidates for the Network+ exam should be capable of calculating a subnet mask by converting a 32-bit string of ones and zeroes into a dotted decimal value.**

True or false: The boundary between the network identifier and the host identifier in a subnetted IPv4 address must fall between bytes.

Answer: *False*. Subnets can be any size, so the boundary between the network and host identifiers can theoretically fall between any two bits.

Multicasts, unicasts, and broadcasts

IPv4 supports three basic types of addresses, as follows:

- **Unicast** A one-to-one transmission sent to an IP address with a specific host identifier, anywhere on the internetwork.
- **Broadcast** A one-to-many transmission sent to an IP address with a host identifier that consists of all 1s. Broadcast transmissions are received and processed by all of the hosts on the local network.
- **Multicast** A one-to-many transmission sent to a specially-allocated multicast IP address. Multicast addresses are targeted at specific groups of hosts, which can be scattered around the internetwork.

True or false: Registration of hosts in multicast groups is handled by the Internet Control Message Protocol (ICMP).

Answer: *False*. The protocol that hosts use to register themselves in multicast groups is called the Internet Group Management Protocol (IGMP).

> ***EXAM TIP*** **Network+ exam candidates should be able to recognize a broadcast address, and be familiar with the term "broadcast domain," which refers to the group of network devices that will receive a broadcast transmission generated by a particular computer. The boundaries between broadcast domains are typically set by routers. Switches, bridges, and hubs all forward broadcasts.**

True or false: Both MAC addresses and IPv4 addresses support broadcast transmissions, but IPv6 addresses do not.

Answer: *True*. MAC addresses and IPv4 addresses consisting of all ones (ffffffffffff or 255.255.255.255, respectively) cause a transmission to be sent to all of the local network devices. IPv6, however, has no broadcast addresses; it uses multicasts and a new type of transmission called an anycast, instead.

Automatic private IP addressing

Automatic Private IP Addressing (APIPA) is a DHCP failover mechanism used by all of the current Windows operating systems. When a device fails to locate a DHCP server on the network, APIPA takes over and automatically assigns an address on the 169.254.0.0/16 network to the computer. The system then uses the Address Resolution Protocol (ARP) to ensure that no other computer on the local network is using the same address.

For a small network that consists of only a single, unrouted LAN, APIPA is a simple and effective alternative to installing a DHCP server, as it creates and assigns addresses that are all on the same subnet.

True or false: Two computers on the same network that assign themselves addresses using APIPA cannot communicate with each other.

Answer: *False*. APIPA assigns addresses that are all on the same IP subnet, and the systems use ARP to confirm that their addresses are unique. Therefore, two systems on the same network with APIPA addresses can communicate with each other.

> ***EXAM TIP*** **Network+ exam candidates should be able to recognize an IPv4 address assigned by APIPA.**

True or false: APIPA is capable of assigning both IPv4 and IPv6 addresses.

Answer: *False*. APIPA can only assign IPv4 addresses. IPv6 has its own mechanism for self-assigning addresses, called stateless address autoconfiguration.

Can you answer these questions?

Find the answers to these questions at the end of this chapter.

1. Which IP address class provides the largest number of hosts per subnet?
2. What subnet mask must you use for a network with the address 172.16.132.0/21?
3. What subnet does APIPA use when assigning IP addresses?
4. The link local unicast addresses generated by the IPv6 stateless address autoconfiguration process use the network address `fe80:0000:0000:0000/64`. What is the most compact allowable form of this address?
5. What is the OUI in the following MAC address: 60-EB-69-86-3A-C7?

Objective 1.4: Explain the purpose and properties of routing and switching

Routers and switches are the two basic connectivity devices used to join individual LANs into internetworks. Routing is the process of forwarding data packets from one network to another, until they reach their final destinations. A switch is a multiport bridging device in which each port forms a separate network segment. Similar in appearance to a hub, a switch receives incoming traffic through any of its ports and forwards the traffic out to the single port needed to reach the destination.

Both routing and switching are complex processes that require the additional functionality of many other specialized TCP/IP processes and protocols. This objective covers a good many of these processes and protocols, knowledge of which is essential for the Network+ exam.

Exam need to know

- Explain the purpose and properties of routing tables.

  For example: Why does every TCP/IP system need a routing table?
- Explain the differences between static and dynamic routing.

  For example: What tools do you use for static routing?
- Explain the function of routing metrics.

  For example: Where do routing metric values come from?
- Explain the meaning of next hop routing.

  For example: What is a hop and what is its significance to the routing process?
- Explain the differences between link state, distance vector, and hybrid routing protocols.

  For example: How does a link state protocol measure route efficiency?
- Explain the purpose and properties of RIP.

  For example: What is the difference between RIPv1 and RIPv2?
- Explain the purpose and properties of EIGRP.

  For example: How does EIGRP evaluate the efficiency of routes?
- Explain the purpose and properties of OSPF.

  For example: How does OSPF offer an improvement over RIP?
- Explain the meaning of convergence.

  For example: Why is a network's convergence state significant?
- Explain the purpose of the Spanning-Tree Protocol.

  For example: What switching problem does the Spanning Tree Protocol address?
- Explain the purpose and properties of 802.1q VLANs.

  For example: Why are VLANs needed on switched networks?

- Explain the purpose of port mirroring.

  For example: Why do administrators need mirrored ports?
- Explain the differences between broadcast domains and collision domains.

  For example: What effect do switches have on collision domains?
- Explain the differences between IGP and EGP.

  For example: What exterior gateway protocol is in common use today?

Routing tables

Every host on a TCP/IP network has a routing table that holds the information the system uses to send packets to their proper destinations. On a LAN, routing is essentially the process of determining what data-link layer protocol address the system should use to reach a particular IP address. In the case of an Ethernet LAN, IP must determine what MAC address the system should use in its Ethernet frames.

If a computer wants to transmit a packet to a destination on the local network, for example, the routing table instructs it to address the packet directly to that system. This is called a direct route. If a packet's destination is on another network, the routing table supplies the address of the router that the system should use to reach that destination.

Remember that data-link layer protocols such as Ethernet can only send frames to the local network. Because the final destination of the packet is on a distant network, the Ethernet destination on the local network must be a router. This is called an indirect route.

True or false: On a TCP/IP network, every router and computer has its own routing table.

Answer: *True*. Every host on a TCP/IP network must have a routing table to determine where to send its packets. This includes routers and computers.

> ***EXAM TIP*** **The Network+ exam typically associates the routing process and routing tables with IP, which runs at the network layer of the OSI model. Dynamic routing protocols, however, which are responsible for populating the routing table, operate at the application layer.**

True or false: The default gateway is usually the first entry in a computer's routing table.

Answer: *True*. The default gateway is the router that a system uses for all packets with destinations not listed in the routing table.

> ***MORE INFO*** **For more information on working with routing tables, see "Objective 2.1: Given a Scenario, install and configure routers and switches."**

Static vs. dynamic routing

There are two techniques for updating a routing table: static routing and dynamic routing. In static routing, a network administrator manually creates routing table entries, using a program designed for this purpose. In dynamic routing, routers use specialized protocols to create routing table entries automatically.

True or false: Static routing is suitable only for relatively small networks.

Answer: *True*. Static routing requires administrators to type the information for each route, often using a command line program with a cryptic syntax. Therefore, it is a time-consuming process that is prone to errors.

> ***EXAM TIP*** **Network+ exam candidates should be familiar with the software tools used for static routing and the protocols used for dynamic routing.**

Routing metrics

Each entry in a routing table contains a metric, which is a value that specifies the efficiency of the route. Metric values are relative; a lower value indicates a more efficient route than a higher value. When a routing table contains multiple routes to the same destination, the system always uses the table entry with the lower metric value.

The term hop count refers to the distance between two networks, based on the number of routers that packets must pass through on the way from the source to the destination. Distance vector routing protocols use hop counts to create metric values in routing table entries. A route with fewer hops is considered to be more efficient than one with more hops.

The size of IP packets depends on the data-link layer protocol the network is using. The transmitting system uses the maximum transmission unit (MTU) of the connected network to determine how large each datagram should be. The MTU is the largest possible frame supported by the data-link layer protocol. Using the largest frame conserves bandwidth by eliminating the overhead involved in transmitting multiple packets instead of one. If, during the journey from source to destination, a packet encounters a network with a smaller MTU, the router for that network fragments the packet into smaller pieces and transmits each one individually.

One of the criteria that link state protocols use to evaluate routes is the route cost. The route cost is a metric assigned by the network administrator used to rate the relative usability of a route. The cost can refer to the literal financial expense incurred by the link, or any other pertinent factor. By using criteria such as this, link state protocols reflect the latency of network routes more precisely. Latency is the time required for data to travel from one location to another.

True or false: The metric values in a routing table must be 15 or less.

Answer: *False*. The Routing Information Protocol (RIP) uses metric values that can be no larger than 15, but that is a limitation of the protocol, not of the routing table.

True or false: On a network that uses static routing, administrators can use any values they wish for the routing table metrics.

Answer: *True*. In static routing, the metric values are relative, and have no statistical meaning. All that matters when there are two routes to the same network is which has the lower metric value.

True or false: IPv4 and IPv6 routers both fragment packets when necessary.

Answer: *False*. In IPv6, intermediate routers do not fragment packets. Instead, end systems use Path MTU Discovery to determine the MTU for an entire route from source to destination.

> ***EXAM TIP*** **Network+ exam candidates should understand the concept of the path MTU and Path MTU Discovery, and how they affect the fragmentation process in IP.**

Next hop

The term next hop refers to the next router on a packet's path through an internetwork to its destination. Routing table entries specify only the next hop that a packet should take, not the entire route. RIPv2 routes have a Next Hop field that contains the address of the next router, which in a Windows routing table goes in the Gateway field.

True or false: In distance vector routing, a hop between two LANs in the same building carries the same weight as a transoceanic hop between networks on different continents.

Answer: *True*. The fundamental flaw of distance vector routing is its reliance on hop counts that do not consider the distance or relative speed of the links between routers.

> ***EXAM TIP*** **Network+ exam candidates should associate hop counts with both distance vector routing and the Routing Information Protocol (RIP).**

Link state vs. distance vector routing

A routing protocol that uses metrics based on the number of hops to the destination is called a distance vector protocol**.** The metric value included with each route determines the efficiency of the route, based on the number of hops required to reach the destination. In a distance vector routing protocol, every router on the network advertises its routing table to its neighboring routers. Each router then examines the information supplied by the other routers, chooses the best route to each destination network, and adds it to its own routing table.

Distance vector routing has a fundamental flaw: it bases its routing metrics solely on the number of hops between two networks, which is not always efficient. When an internetwork consists of multiple LANs in the same location, all connected using the same data-link layer protocol, the hop count is a valid indicator. However, when WAN links are involved, a single hop can refer to anything from a high-speed leased line to a dial-up modem connection. It is therefore possible for traffic moving over a route with fewer hops to take longer than one with more hops.

The alternative to distance vector routing is called link state routing**.** A link state routing protocol works by flooding the network with messages called link state advertisements. Each router receiving such a message propagates it to its neighbors, incrementing a sequence number value for each entry that indicates its distance from the source. Using these advertisements, each router compiles a map of the network and uses it to construct its own routing table.

True or false: Link state routing protocols are preferable on an internetwork with links running at different speeds.

Answer: *True*. Link state routing evaluates the efficiency of a route based on actual transport times, not hop counts.

> ***EXAM TIP*** **Network+ exam candidates should be able to explain the differences between distance vector and link state routing protocol and provide examples of each.**

True or false: Distance vector routing protocols impose a greater processing burden on routers than link state protocols.

Answer: *False*. Link state routing is more complex than RIP and requires more processing by the router.

RIP

The Routing Information Protocol (RIP) is a popular interior gateway protocol in the TCP/IP suite. When a RIP router starts, it generates a RIP request and transmits it as a broadcast over all of its network interfaces. Upon receiving the broadcast, every other router on any network that supports RIP generates a reply message that contains its routing table information. A reply message can contain up to 25 routes. When the router that sent the request receives the replies, it integrates the routing information in the reply messages into its own routing table.

The metric value included with each RIP route determines the efficiency of the route, based on the number of hops required to reach the destination. When routers receive routing table entries from other routers using RIP, they increment the value of the metric for each route to reflect the additional hop required to reach the destination.

RIP version 1 is widely criticized for the large amount of broadcast traffic it produces, and for its lack of a subnet mask field. Version 2 of the protocol adds a subnet mask field and support for the use of multicast transmissions instead of broadcasts.

True or false: Because it lacks a subnet mask field, RIPv1 can only be employed on networks that use classful IP addressing.

Answer: *True*. Without a subnet mask, the only way a router receiving RIPv1 data can identify the size of the network identifier in an address is to read the class from its first few bits. For subnetted classes, or for classless addressing, each RIP route must include a subnet mask.

EXAM TIP **Network+ exam candidates should know the differences between the RIP versions, and be aware that RIPv2 is the predominant dynamic routing protocol used on LANs today.**

True or false: RIPv1 is a distance vector routing protocol, but RIPv2 is a link state protocol.

Answer: *False*. RIP is a distance vector protocol in both versions, which uses hop counts to generate its metrics.

EIGRP

The Enhanced Interior Gateway Routing Protocol (EIGRP) is a hybrid between a distance vector and a link state protocol, relying on six vector metrics to compare the value of entries in a computer's routing table. These vector metrics are as follows:

- **Bandwidth** The bandwidth of the link between the router and the destination network
- **Load** The relative traffic saturation of the link between the router and the destination network
- **Delay** The total transmission delay between the router and the destination network
- **Reliability** The relative reliability of the link between the router and the destination network
- **MTU** The path maximum transfer unit (MTU) value of the link between the router and the destination network
- **Hop count** The number of intermediate systems between the router and the destination network

True or false: EIGRP was conceived after RIP and before Open Shortest Path First (OSPF).

Answer: *True*. Before OSPF became available, the outcry against RIP grew so loud that Cisco Systems came out with the Interior Gateway Routing Protocol (IGRP), and eventually EIGRP.

EXAM TIP **Network+ exam candidates should be able to identify EIGRP as a hybrid routing protocol, combining elements of link state and distance vector protocols.**

OSPF

OSPF is a link state routing protocol that, unlike RIP and most other TCP/IP protocols, uses messages that are encapsulated directly in IP datagrams, not in TCP segments or UDP datagrams. Link state routing, as implemented in OSPF, uses a formula called the Dijkstra algorithm to judge the efficiency of a route based on criteria such as the following:

- **Hop count** Though link state routing protocols still use the hop count to judge a route's efficiency, it is only part of the equation.
- **Transmission speed** The speed at which the various links operate is an important part of a route's efficiency. Faster links obviously take precedence over slow ones.
- **Congestion delays** Link state routing protocols consider the network congestion caused by the current traffic pattern when evaluating a route, and bypass links that are overly congested.
- **Route cost** The route cost is a metric assigned by the network administrator used to rate the relative usability of various routes. The cost can refer to the literal financial expense incurred by the link, or any other pertinent factor.

True or false: OSPF evaluates routes by counting the number of hops between the source and the destination.

Answer: *False*. OSPF is a link state protocol, which relies on a combination of factors to evaluate routes, rather than counting hops.

> ***EXAM TIP*** **Network+ exam candidates must be conscious of which routing protocols are distance vector protocols which are link state protocols, and which are those they call hybrids.**

True or false: OSPF is a more suitable routing protocol than RIP for an internetwork spanning multiple sites with WAN links running at different speeds.

Answer: *True*. Because OSPF uses actual performance criteria to evaluate routes, rather than hop counts, it is a better choice than RIP for internetworks with links running at various speeds.

Convergence

Convergence is the process of updating the routing tables on all of a network's routers in response to a change in the network, such as the failure or addition of a router. Distance vector protocols such as RIP have a rather slow convergence rate because updates are generated by each router asynchronously, that is, without synchronization or acknowledgment. Link state routing protocols judge the relative efficiency of routes more precisely and have a better convergence rate than RIP.

True or false: The convergence rate of a network is based in part on the routing protocols it uses.

Answer: *True*. Link state routing protocols generally provide a better convergence rate than distance vector protocols, but there are other factors that affect convergence as well, such as the presence of relatively slow WAN links..

> ***EXAM TIP*** **The Network+ exam generally requires candidates to understand nothing more than the meaning of the term convergence, as it applies to dynamic routing.**

True or false: Convergence rates are only an issue with networks that use dynamic routing.

Answer: *True*. On a network that uses static routing, there are no dynamic routing protocols, so convergence is only a reflection of how long it takes the administrator to update all of the routing tables on the network.

Spanning Tree Protocol

Installing multiple switches on a network can provide fault tolerance if a switch fails. However, it is also possible for the switches to begin forwarding traffic in an endless cycle, a condition called a switching loop (or a bridge loop, because it can also occur with bridges).

To address the problem of bridge looping, switches (and bridges) use a technique called the Spanning Tree Protocol (STP). STP is a data-link layer protocol that selects a non-redundant subset of switches to form the spanning tree, deactivating the others. Data circulating throughout the network uses only the switches in the tree unless a switch fails, in which case the protocol activates one of the inactive switches to replace it.

True or false: The Spanning Tree Protocol is only needed on networks with multiple switches per segment.

Answer: *True*. Switching loops only occur when there are multiple switches forwarding packets back and forth to each other.

EXAM TIP **Network+ exam candidates should be familiar with the purpose of the Spanning Tree Protocol, but they do not need to know the particulars of how it works.**

Virtual LANs

A virtual LAN or VLAN is a group of systems on a switched network that functions as a logical network segment. The systems on a VLAN can communicate locally with each other, but not with systems on other VLANs. The physical network is still switched, however; the VLANs exist as a logical overlay to the switching fabric, as shown in Figure 1-4.

The standard that defines the use of virtual LANs on an Ethernet network is IEEE 802.1q. Network administrators create VLANs by using a web-based configuration utility built into the switch. With this utility, administrators can specify the MAC addresses or switch ports of the systems that are to be part of each VLAN. Because VLANs are independent of the physical network, their members can be located anywhere, and a single system can even be a member of more than one VLAN. For systems in different VLANs to communicate, the switch must use routers, either physical or virtual.

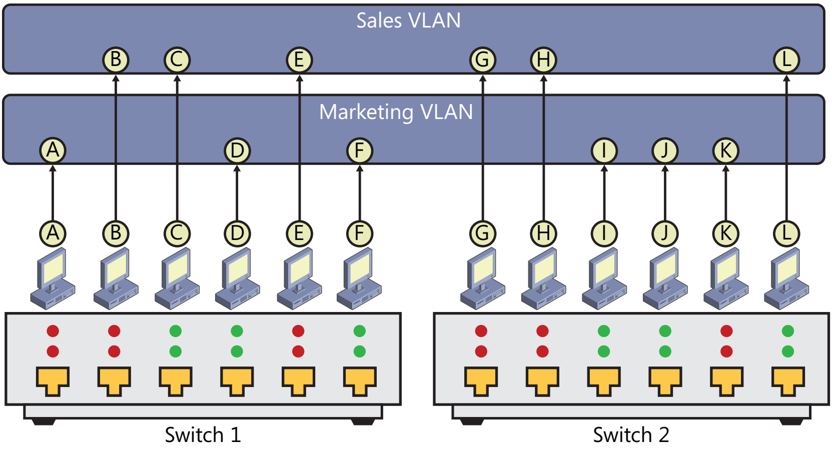

FIGURE 1-4 VLANs on a switched network.

True or false: VLANs are only necessary on networks that use switches instead of routers.

Answer: *True*. On a routed internetwork, the routers create the subnets that divide the network, so there is no need for VLANs.

> ***EXAM TIP*** **Network+ exam candidates must understand the need for VLANs and how they exist solely within switches.**

True or false: Virtual LANs cannot communicate with physical LANs.

Answer: *False*. Using routers, VLANs can communicate with each other and with physical LANs.

> ***MORE INFO*** **For more information on VLANs, see “Objective 2.1: Given a scenario, install and configure routers and switches.”**

Port mirroring

On a switched network, capturing traffic for monitoring and analysis is difficult, because switches forward incoming unicast traffic only to its intended recipient. A protocol analyzer connected to a standard switch port therefore has access only to one computer’s incoming and outgoing traffic, plus any broadcasts transmitted over the local network segment.

To monitor or capture all of the traffic transmitted on the network, you must plug the computer running the protocol analyzer into a switch that supports port mirroring. Switches that support port mirroring have a special port to which they send all incoming traffic.

True or false: You must employ switches that support port mirroring if you want to connect switches together to create a single network.

Answer: *False*. Port mirroring is only required if you want to use a protocol analyzer or other device to monitor or capture all of the traffic transmitted over the network.

Broadcast domains and collision domains

A broadcast domain is the group of computers that will receive a broadcast message transmitted by any one of its members. A LAN typically forms a single broadcast domain, because hubs, switches, and bridges all propagate broadcast transmissions to every system connected to them. Routers do not propagate broadcasts, however, so connecting two segments with a router creates two broadcast domains.

A collision domain is a group of network devices connected in such a way that if two devices transmit at the same time, a collision occurs. Ethernet LANs that use a shared network medium, such as bus networks or hub-based star networks, form a single collision domain, as do wireless LANs based on IEEE 802.11. Most Ethernet LANs today, however, use switches, which either create a separate collision domain for each pair of devices, in the case of a half-duplex connection; or eliminate collisions entirely, in the case of a full-duplex connection.

True or false: Splitting a hub-based Ethernet network in two by adding a bridge creates two separate collision domains.

Answer: *True*. Bridges wait until they receive an entire packet before they forward it out through the other port. Therefore, if computers on opposite sides of the bridge transmit at once, the packets will be delayed and will not collide.

EXAM TIP **Network+ exam candidates must know the difference between a broadcast domain and a collision domain, and how the standard network connectivity devices affect them.**

True or false: Switches create a separate broadcast domain for each pair of devices connected to them.

Answer: *False*. Switches forward broadcast packets out through all of their ports, just like hubs, so they maintain a single broadcast domain for all of their connected systems.

IGP vs. EGP

Routing protocols are generally divided into two categories: interior gateway protocols (IGPs) and exterior gateway protocols (EGPs)**.** On the Internet, a collection of networks that fall within the same administrative domain is called an autonomous system (AS)**.** Autonomous systems are the largest and highest-level administrative units on the Internet. Autonomous systems have unique identifiers called autonomous system numbers (ASNs), consisting of two 16-bit decimal numbers, separated by a period.

The routers within an AS use an IGP, such as the RIP or the OSPF protocol, to exchange routing information among themselves. At the edges of an AS are routers that communicate with the other ASes on the Internet, using an exterior gateway protocol (as shown in Figure 1-5) such as the Border Gateway Protocol (BGP) or the Exterior Gateway Protocol (EGP).

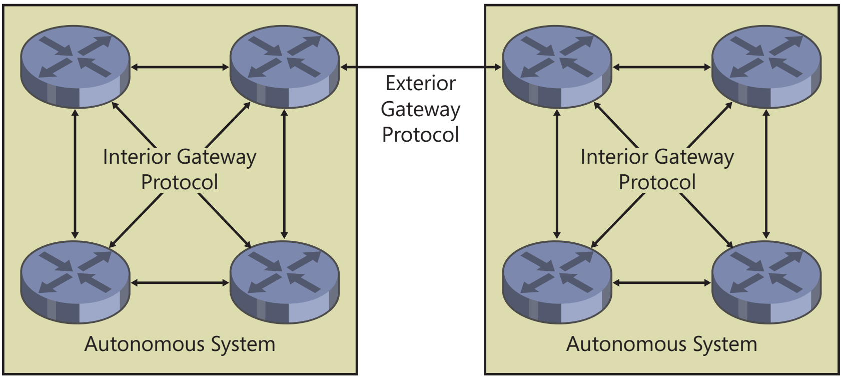
Exterior Gateway Protocol
Interior Gateway Protocol
Autonomous System
Interior Gateway Protocol
Autonomous System

FIGURE 1-5 IGPs and EGPs within and between autonomous systems.

True or false: Link state routing protocols are used for exterior gateway routing, and distance vector protocols are used for interior gateway routing.

Answer: *False*. Both link state and distance vector protocols are used for interior gateway routing.

> ***EXAM TIP*** **The term "exterior gateway protocol" is both a generic name for the routing protocols used between autonomous systems and the name of a specific protocol used between ASes. In the latter, the phrase is capitalized, in the former it is not. The Network+ exam objectives refer to IGP and EGP using only the acronyms, so candidates should be familiar with both usages.**

Can you answer these questions?

Find the answers to these questions at the end of this chapter.

1. What is one of the advantages of creating VLANs on a large switched network?
2. How can switching from RIPv1 to RIPv2 help to conserve bandwidth on a LAN?
3. How does the Spanning Tree Protocol prevent switching loops?
4. What are the main differences between RIPv1 and RIPv2?
5. Why is convergence an important factor in the routing process?

Objective 1.5: Identify common TCP and UDP default ports

One of the important functions of a transport layer protocol is to identify the protocol or process that generated the data it carries so that the receiving system can deliver the data to the correct application. Both TCP and UDP do this by specifying the number of a port that has been assigned to a particular process by the Internet Assigned Numbers Authority (IANA).

When a TCP/IP packet arrives at its destination, the transport layer protocol receiving the IP datagram from the network layer reads the value in the Destination Port field and delivers the information in the Data field to the program or protocol associated with that port.

All of the common Internet applications have particular port numbers associated with them, called well-known ports. The IANA has designated all of the port numbers less than 1024 as well-known ports, but not all of them are assigned to applications. TCP and UDP both maintain their own separate lists of well-known port numbers.

Exam need to know

- SMTP – 25

  For example: What well-known port number does SMTP use?
- HTTP – 80

  For example: What well-known port number does HTTP use?
- HTTPS – 443

  For example: What well-known port number does HTTPS use?
- FTP – 20, 21

  For example: What well-known port number does FTP use?
- TELNET – 23

  For example: What well-known port number does TELNET use?
- IMAP – 143

  For example: What well-known port number does IMAP use?
- RDP – 3389

  For example: What well-known port number does RDP use?
- SSH – 22

  For example: What well-known port number does SSH use?
- DNS – 53

  For example: What well-known port number does DNS use?
- DHCP – 67, 68

  For example: What well-known port numbers does DHCP use?

Ports

The well-known port numbers associated with some of the major application layer protocols in the TCP/IP suite are listed in Table 1-2.

TABLE 1-2 Well-known port numbers.

PROTOCOL	ACRONYM	TRANSPORT LAYER PROTOCOL	PORT NUMBER
Simple Mail Transfer Protocol	SMTP	TCP	25
Hypertext Transfer Protocol	HTTP	TCP	80
Hypertext Transfer Protocol Secure	HTTPS	TCP	443
File Transfer Protocol	FTP	TCP	20 (Data), 21 (Control)
TELNET	TELNET	TCP	23
Internet Mail Access Protocol	IMAP	TCP	143
Remote Desktop Protocol	RDP	TCP	3389
Secure Shell	SSH	TCP, UDP	22
Domain Name System	DNS	UDP, TCP	53
Dynamic Host Configuration Protocol	DHCP	UDP. TCP	67 (Server), 68 (Client)

True or false: FTP is an unusual protocol in that it uses two different port numbers on the server for a single transaction.

Answer: *True*. FTP servers use port 21 for control traffic, and port 20 for data. When a client sends a request for a file, it sends it to port 21. The server then opens port 20 and uses it to actually transmit the file.

> ***EXAM TIP*** **This is one of the few Network+ objectives that requires rote memorization. You must know the port numbers associated with the listed protocols for the exam.**

True or false: HTTP servers use port 80, but HTTP clients can select their own port numbers.

Answer: *True*. HTTP and many other protocols require clients to select a port number, called an ephemeral port number, for their side of the transaction.

Can you answer these questions?

Find the answers to these questions at the end of this chapter.

1. Which of the protocols listed in this objective uses well-known ports for both the server and the client?
2. When configuring an email client that will use IMAP and SMTP, what port numbers would you use for incoming and outgoing traffic?
3. What port does a client browser use when establishing an encrypted connection to a web server?
4. What is the number of well-known ports the IANA designates at this time?

Objective 1.6: Explain the function of common networking protocols

Objective 1.6 requires Network+ exam candidates to know the basic functions of the most important protocols in the TCP/IP suite. These protocols are scattered throughout the layers of the OSI model, and many of them are covered in greater detail in other objectives. For those protocols that are not covered elsewhere, you should be familiar with their functions and where they fit into the OSI model, but there is no need to go too deeply into their intricacies.

Exam need to know

- TCP/IP suite

  For example: What are the primary protocols of the TCP/IP suite at the network and transport layers?
- TCP

  For example: What services does TCP provide that UDP does not?
- UDP

  For example: What types of transactions is UDP generally used for?
- DHCP

  For example: What is the purpose of DHCP?
- FTP

  For example: How does FTP differ from TELNET?
- TFTP

  For example: What type of file is TFTP typically used to download?
- DNS

  For example: Where does DNS store its information about names and addresses?
- HTTP

  For example: What command does an HTTP client use to request a file from a web server?

- HTTPS

  For example: How does HTTPS increase the security of web transactions?
- ARP

  For example: How does ARP resolve IP addresses into MAC addresses?
- SIP (VoIP)

  For example: Why is it necessary for a system to use SIP to establish a session before it sends VoIP data?
- RTP (VoIP)

  For example: What function does RIP provide in a Voice over IP session?
- TELNET

  For example: What functions can you perform on a remote computer using TELNET?
- SSH

  For example: Why is SSH preferable to TELNET?
- NTP

  For example: Why is it necessary for servers on a network to synchronize their clocks?
- POP3

  For example: What is the primary difference between the POP3 and IMAP protocols?
- IMAP4

  For example: Where do IMAP clients store their message data?
- SMTP

  For example: How does SMTP determine where to send email message traffic?
- SNMP2/3

  For example: A network management console uses SNMP to gather information from what client components?
- ICMP

  For example: What TCP/IP utilities use the ICMP protocol?
- IGMP

  For example: Why is multicasting a critical function of IPv6?
- TLS

  For example: Which protocol does TLS replace?

TCP/IP suite

The TCP/IP suite is a collection of protocols that span layers 2 through 7 of the OSI reference model. Together, the protocols provide a complete networking solution, with the exception of a physical layer implementation. The TCP/IP protocols are defined in documents called Requests for Comments (RFCs), published by the Internet Engineering Task Force. Some of the most important protocols in the TCP/IP suite are listed in Table 1-3.

TABLE 1-3 TCP/IP protocols.

ACRONYM	PROTOCOL	FUNCTION	OSI LAYER
ARP	Address Resolution Protocol	Resolves IP address into MAC addresses	Data-link
FTP	File Transfer Protocol	Transfers files to and from a remote host	Application
HTTP	Hypertext Transfer Protocol	Requests and receives files from web servers	Application
ICMP	Internet Control Message Protocol	Provides error messaging, diagnostic, and routing functions for IP	Network
IGMP	Internet Group Management Protocol	Provides multicast group registration services	Network
IMAP	Internet Message Access Protocol	Retrieves mail from a server and stores it permanently for client access	Application
IP	Internet Protocol	Provides connectionless network services, including addressing, routing, and fragmentation	Network
POP3	Post Office Protocol, version 3	Retrieves mail from a server and stores it temporarily for client download	Application
SMTP	Simple Mail Transfer Protocol	Provides mail transport service	Application
SNMP	Simple Network Management Protocol	Carries operational status information from agents to network management consoles	Application
TCP	Transmission Control Protocol	Provides connection-oriented services, including guaranteed delivery, error correction, and flow control	Transport
UDP	User Datagram Protocol	Provides connectionless transport service	Transport

EXAM TIP The Network+ exam might refer to TCP/IP as a protocol suite or a protocol stack; the two expressions are synonymous.

True or false: A network can conceivably run using only protocols from the TCP/IP suite.

Answer: *False*. The TCP/IP suite does not include physical layer implementations. Therefore a network cannot run without a protocol that provides the physical layer, such as Ethernet.

> ***EXAM TIP*** **The TCP/IP suite includes hundreds of different protocols and specifications, only a few of which are covered on the Network+ exam.**

TCP

The TCP/IP suite uses two protocols at the transport layer to provide different levels of service for applications: the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP). Both TCP and UDP generate protocol data units (PDUs) that are carried inside IP datagrams. TCP is a connection-oriented protocol that provides reliable service with guaranteed delivery, packet acknowledgment, flow control, and error correction and detection.

TCP is designed for transmitting data that requires perfect bit accuracy, such as program and data files. Not surprisingly, TCP generates much more control traffic than UDP does, because it provides so many services.

True or false: Before a system can transmit data using TCP, it must exchange connection establishment messages with the destination system.

Answer: *True*. TCP performs a connection establishment procedure called a three-way handshake before sending application data.

> ***EXAM TIP*** **Network+ exam candidates should be familiar with the differences between the TCP and UDP protocols at the transport layer, including the services they provide and the application layer protocols that use them.**

UDP

UDP is a connectionless transport layer protocol that provides unreliable service with a minimum of overhead. Many applications use UDP for short transactions that consist only of a single request and reply; others use it for data transmissions that can survive the loss of a few bits, such as audio and video streams.

True or false: The PDUs that UDP and IP create are both called datagrams.

Answer: *True*. The term datagram is used for the PDUs created by any connectionless protocol. UDP and IP are both connectionless, so they can both utilize that term.

DHCP

Dynamic Host Configuration Protocol (DHCP) is a service that automatically configures the TCP/IP client computers on a network by assigning them unique IP addresses and other parameters. Unlike its predecessor, the Bootstrap Protocol

(BOOTP), DHCP leases addresses to clients for a given period of time and reclaims them when they are no longer in use.

> ***MORE INFO*** **For more information on DHCP, see "Objective 2.3: Explain the purpose and properties of DHCP."**

True or false: DHCP can permanently assign IP addresses to clients.

Answer: *True*. DHCP servers can assign specific addresses manually, assign permanent addresses from a pool, and assign addresses dynamically, on a leased basis.

> ***EXAM TIP*** **The Network+ exam nearly always has one or more questions on DHCP, typically involving implementation details, such as the creation of scopes and relay agents.**

FTP

FTP, the **File Transfer Protocol**, is an application layer TCP/IP protocol that is used by an authenticated client to connect to a server and transfer files to and from its drives. Using FTP is not the same as sharing a drive with another system on the network, nor is it a terminal emulator like TELNET. Access is limited to a few basic file management commands, and the primary function of the protocol is to copy files to a local system, not to access them in place on the server.

True or false: To use FTP, you must purchase an FTP client application.

Answer: *False*. Virtually all operating systems include a character-based FTP client, so there is no need to purchase one. Most web browsers are also capable of functioning as FTP clients.

> ***EXAM TIP*** **In some cases, the Network+ exam requires candidates to be familiar with basic FTP commands, such as get, for downloading a file from the remote system, and put, for uploading a file to the remote system.**

TFTP

The Trivial File Transfer Protocol (TFTP) is a minimized, low-overhead version of FTP that can transfer files across a network. TFTP uses UDP at the transport layer instead of TCP and does not include FTP's authentication and user interface features. TFTP was originally designed for use on diskless workstations that have to download an executable system file from a network server in order to boot.

True or false: TFTP can work together with DHCP to provide all the services needed to start a diskless workstation.

Answer: *True*. A diskless workstation can retrieve an IP address and other TCP/IP configuration settings from a DHCP server and then download a boot file using TFTP.

EXAM TIP **Network+ exam candidates should know that TFTP uses the connectionless service provided by UDP at the transport layer, while FTP uses the connection-oriented TCP service.**

DNS

The Domain Name System (DNS) is a distributed database that contains name and IP address information about the systems on a network. TCP/IP computers can use DNS servers to resolve host names into IP addresses before they initiate communication.

MORE INFO **For more information on DNS, see "Objective 1.7: Summarize DNS concepts and its components."**

True or false: Each DNS server contains information about all of the hosts on the network.

Answer: *False*. Each DNS server can only contain information about a part of the network. The system is designed to distribute authoritative data among many servers and forward requests to provide access to any data a client needs.

EXAM TIP **DNS is a critical element of TCP/IP communications, both on the Internet and on private networks. The Network+ exam nearly always includes questions that require an understanding of DNS and its operations.**

HTTP

Communication between web servers and their browser clients is largely dependent on an application layer protocol called the Hypertext Transfer Protocol (HTTP). HTTP is a relatively simple protocol that takes advantage of the services provided by the TCP protocol at the transport layer to transfer files from servers to clients. When a client connects to a web server by typing a URL in a browser or clicking a hyperlink, the client generates an HTTP request message and transmits it to the server. HTTP consists of only two message types: requests and responses. As with many other application layer protocols, HTTP messages take the form of text commands.

True or false: Displaying a single webpage on a browser can require many HTTP request/response transactions.

Answer: *True*. Each HTTP request and response can retrieve a single file from the web server, but a single webpage can require many text and media files, which the browser must request separately.

EXAM TIP **Network+ exam candidates should be aware that HTTP relies on the connection-oriented service provided at the transport layer by TCP.**

HTTPS

Hypertext Transfer Protocol Secure (HTTPS) is a variant of HTTP that uses the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) security protocols to provide data encryption and server identification services. HTTPS is the accepted standard for secured Internet transactions such as online banking and e-commerce. An HTTPS connection uses the *https://* prefix in its URL and connects by default to port 443, instead of port 80, which is used by HTTP.

True or false: All websites have support for HTTPS connections. All you have to do is change the prefix in the URL.

Answer: *False*. HTTPS is not an automatic feature provided by all web servers. An administrator must enable and configure it for users to establish an encrypted connection.

ARP

The function of Address Resolution Protocol (ARP) is to reconcile the IP addresses used to identify systems at the upper layers of the protocol stack with the MAC addresses at the data-link layer. When a TCP/IP application requests network resources, it supplies the destination IP address used in the IP protocol header. ARP converts the IP address into the MAC address used in the data-link layer protocol header by broadcasting a request containing the IP address on the local network and waiting for the holder of that IP address to respond with a reply containing the equivalent MAC address.

True or false: ARP can only resolve IP addresses for systems on the local network into MAC addresses.

Answer: *True*. Because it relies on broadcast transmissions, which are limited to the local network, ARP can only resolve local IP addresses into MAC addresses.

> ***EXAM TIP*** **Network+ exam candidates should be careful not to confuse ARP, which resolves IP addresses into MAC addresses, with DNS, which resolves names into addresses.**

SIP

The Session Initiation Protocol (SIP) is an application layer request/response protocol that Voice over IP (VoIP) uses to establish a session between two network nodes and terminate the session when the data exchange is completed. SIP does not carry the actual voice traffic; it simply sets up the call between the two parties in preparation for the data exchange.

True or false: Voice over IP relies on TCP to establish a communications session between two callers.

Answer: *False*. VoIP uses a specialized application layer protocol called SIP to establish sessions between callers. At the transport layer, SIP can use either TCP or UDP.

RTP

In a VoIP call, after the SIP protocol establishes a session, the two callers use the Real-Time Transport Protocol (RTP) to transmit the actual audio stream across the network. At the same time, the systems use the RTP Control Protocol (RTCP) to manage and monitor the transmissions.

True or false: VoIP uses application layer protocols to manage call sessions and transmit media streams.

Answer: *True*. RTP and RTCP (and the other protocols that VoIP uses) are all application layer protocols.

> ***EXAM TIP*** **The inclusion of SIP and RTP in this objective is the only mention of Voice over IP in the Network+ exam objectives. While candidates should be familiar with the basic functions of these protocols, there is no need for an in-depth study of VoIP for this exam.**

TELNET

TELNET is a terminal emulation program that provides users with access to a text-based interface on a remote system. Unlike FTP, which is designed for file transfers and has only a limited set of file management commands that you can execute on the server, TELNET enables the remote user to execute programs and configure operating system components. As a result, TELNET and FTP tend to complement each other; together, they are known as the DARPA commands and can provide reasonably comprehensive access to a UNIX or Linux system.

True or false: TELNET and FTP provide roughly the same access to a remote system.

Answer: *False*. TELNET provide access to the command line on the remote system, while FTP provides a limited command set used for file management and transfers.

> ***EXAM TIP*** **Because of its lack of security, administrators today typically use a program like SSH rather than TELNET, but it still remains part of the Network+ exam objectives.**

SSH

Secure Shell (SSH) is a protocol that provides encrypted command line access to another computer on the network. Used primarily by UNIX/Linux systems, SSH is an improvement over TELNET, which transmits passwords and other data over the network in clear text (that is, unencrypted) form.

True or false: SSH requires that the communicating systems have a client program and a server program.

Answer: *True*. As with TELNET, one of the computers involved in an SSH session must be running a client program and one must be running a server. Most UNIX and Linux distributions include both.

NTP

The Network Time Protocol (NTP) is an application layer protocol designed to synchronize the clocks of computers on packet-switching networks with varying degrees of latency. Because transmissions on a packet-switching network are not precisely predictable, there is no way of knowing exactly how long it will take for a packet to travel from its source to its destination. Therefore, any attempt to transmit a time signal over the network with precise accuracy is likely to be futile. NTP is designed to overcome that network latency and enable systems to synchronize their clocks with a great deal of precision.

True or false: Active Directory requires all of the domain controllers on a network to have synchronized clocks.

Answer: *True*. Because administrators can modify the Active Directory database from any domain controller, properly calibrated time stamps are necessary to ensure that changes are applied in the proper order.

POP3

The Post Office Protocol, version 3 (POP3) is designed to provide mailbox services for client computers that are themselves not capable of performing transactions with SMTP servers. Most of the clients that require a mailbox service are not continuously connected to the Internet and are therefore not capable of receiving messages any time a remote SMTP server wants to send them. A POP3 server is continuously connected and is always available to receive messages for offline users. The server then retains the messages in an electronic mailbox until the user connects to the server and requests them.

POP3 is similar to SMTP in that it communicates with clients using text-based commands and responses. As with SMTP, the client transmits commands to the server, but in POP3, there are only two possible response codes, +OK, indicating the successful completion of the command, and –ERR, indicating that an error has occurred to prevent the command from being executed. In the case of POP3, the server also sends the requested email message data to the client, rather than the client sending outgoing messages to the server as in SMTP.

True or false: POP3 servers must remain connected to the Internet at all times to receive messages destined for clients.

Answer: *True*. SMTP servers forward email traffic based on the MX resource records supplied by DNS servers. The MX records specify the address of the mail server that must be ready to receive message traffic at any time. If the server is offline, mail messages sent to it will bounce.

> ***EXAM TIP*** **The Network+ exam requires candidates to know the various protocols used for email messaging, the ports they use, and the differences between them.**

IMAP4

Internet Message Access Protocol (IMAP) version 4 is a mailbox service that is designed to improve upon POP3's capabilities. IMAP functions similarly to POP3 in that it uses text-based commands and responses, but the IMAP server provides considerably more functionality than a POP3 server. The biggest difference between IMAP and POP3 is that IMAP is designed to store email messages on the server permanently and provides a wider selection of commands that enable clients to access and manipulate their messages. Storing the mail on the server enables users to easily access their mail from any computer.

True or false: IMAP clients store email messages in encrypted form on the client computer.

Answer: *False*. IMAP clients permanently store all email messages on the server.

> ***EXAM TIP*** **Network+ exam candidates should know that clients can use email protocols such as IMAP and POP3 to download messages from a mail server, but they cannot use them to send messages. For that, they must use SMTP.**

SMTP

Simple Mail Transfer Protocol (SMTP) is an application layer messaging protocol that is responsible for most of the server-to-server mail traffic on the Internet. Like HTTP and FTP messages, SMTP messages are based on text commands. SMTP communications can take place between email clients and servers or between pairs of servers. In each case, the basic communication model is the same. One computer, called the sender-SMTP, initiates communication with the other, the receiver-SMTP, by establishing a TCP connection using the standard three-way handshake.

True or false: Email clients connect to SMTP servers to download their incoming email messages.

Answer: *False*. Email clients use SMTP servers for their outgoing messages, but to download their incoming messages, they must connect to a POP3 or IMAP server.

SNMP2/3

The Simple Network Monitoring Protocol (SNMP) is a TCP/IP application layer protocol and query language that specially equipped networking devices use to communicate with a central console. Many of the networking hardware and software products on the market, including routers, switches, network adapters, operating systems, and applications, are equipped with SNMP agents.

An SNMP agent is a software module that is responsible for gathering information about a device and delivering it to a computer that has been designated as the network management console. The agents gather specific information about the network devices and store them as managed objects in a management information base (MIB). At regular intervals, the agents transmit their MIBs to the console by using SNMP messages, which are carried inside UDP datagrams.

True or false: All versions of SNMP secure the data being collected from agents.

Answer: *False*. SNMPv1 has no security protection other than a community string, which functions as a password, and which systems transmit in clear text. SNMPv2 added a new security system that many people criticized as being overly complex. An interim version, called SNMPv2c, consisted of SNMPv2 without the new security system, and with the old version 1 community string instead. SNMP version 3 has standard security services, including authentication, message integrity, and encryption.

> ***EXAM TIP*** **For the purposes of the Network+ exam, SNMP versions 1 and 2 should be considered as unsecure protocols, while SNMP version 3 is secure.**

ICMP

The Internet Control Message Protocol (ICMP) is a network layer protocol that does not carry user data, although its messages are encapsulated in IP datagrams. ICMP fills two roles in the TCP/IP suite; it provides error reporting functions, informing the sending system when a transmission cannot reach its destination, for example, and it carries query and response messages for diagnostic programs. The Ping utility, for instance, which is included in every TCP/IP implementation, uses ICMP echo messages to determine if another system on the network is able to receive and send data.

True or false: ICMP messages are encapsulated in UDP datagrams.

Answer: *False*. Unlike most TCP/IP protocols, ICMP does not use the transport services provided by TCP or UDP. Instead, its messages are carried directly within IP datagrams, with no intervening header.

> ***EXAM TIP*** **ICMP, apart from appearing in the Network+ objectives, is also the basis for some of the most essential TCP/IP troubleshooting tools, including Ping and Traceroute. Candidates for the exam should be familiar with these, as well as other functions of ICMP.**

IGMP

Class D IP addresses ranging from 224.0.1.0 to 238.255.255.255 are reserved for multicasting purposes. A multicast transmission is simply a packet transmitted to one of those Class D addresses. However, determining which systems are part of the multicast group that recognizes that address and receives the packets is a process that involves the use of the Internet Group Management Protocol (IGMP).

True or false: Multicasts are preferable to broadcasts because they can be transmitted to systems on other networks.

Answer: *True*. Broadcast transmissions are limited to the local network because routers do not propagate them. However, routers do propagate multicasts, so they can address systems on other networks.

EXAM TIP **Network+ exam candidates should be aware that multicasts are a crucial part of IPv6 communications, because IPv6 does not support broadcast transmissions.**

TLS

Transport Layer Security (TLS) is the successor to Secure Sockets Layer (SSL) and is now the standard cryptographic protocol for web communications. Virtually all current web servers and browsers support TLS, as do many other Internet applications.

True or false: HTTPS is a combination of HTTP and the TLS security protocol.

Answer: *True*. When you access a secure website on the Internet by using the *https://* prefix on a URL, the web server uses TLS to secure the data it would normally deliver using only HTTP.

EXAM TIP **TLS and SSL both are available in several versions providing successively greater degrees of security. However, for the Network+ exam, you need only know that these are both encryption protocols used for web traffic and that TLS is more secure than SSL.**

Can you answer these questions?

Find the answers to these questions at the end of this chapter.

1. Which of the protocols covered by this objective are considered to be transport protocols?
2. Which of the application layer protocols covered by this objective are used by Voice over IP?
3. Which protocols covered by this objective carry email messages?
4. Which transport layer protocol does DNS use for most of its transmissions?
5. Which of the protocols covered in this objective is the only one that operates at the data-link layer?

Objective 1.7: Summarize DNS concepts and its components

Computers are designed to work with numbers, whereas humans are more comfortable working with words. This fundamental dichotomy is the reason why the Domain Name System came to be. Very simply, the DNS is a database service that converts computer names to IP addresses and addresses back into names.

DNS servers are a ubiquitous part of most TCP/IP networks, even if users aren’t aware of them. TCP/IP communications are based solely on IP addresses. Before one system can communicate with another, it must know the other system’s IP address. Often, the user supplies to a client application a friendly name for a desired server. The application must then resolve that server name into an IP address before it can transmit a message to it. If the name resolution mechanism fails to function, no communication with the server is possible.

Exam need to know

- Summarize the concept of DNS servers

  For example: How many DNS servers contain the entire Internet domain namespace?
- Summarize the concept of DNS records

  For example: Which resource record type contains name-to-address mappings for IPv6 addresses?
- Summarize the concept of Dynamic DNS

  For example: What network service has made it necessary to develop a mechanism for dynamically updating DNS resource records?

DNS servers

If you connect to the Internet, you use a DNS server each time you enter a server name or URL into a web browser or other application to resolve the name of the system you specified into an IP address. When a standalone computer connects to an Internet Service Provider (ISP), the ISP's server usually supplies the addresses of the DNS servers that the system will use. On a TCP/IP network, administrators configure clients with the addresses of the DNS servers they will use. This can be a manual process performed for each workstation or part of an automated DHCP configuration process.

DNS is a distributed database service; thousands of servers all over the Internet function as the authority for a small piece of the DNS namespace. By forwarding name resolution requests from server to server, it is possible to resolve any DNS name into its equivalent IP address, no matter where on the Internet the authoritative information for that name is stored.

In addition to resolving names into addresses, DNS servers can also resolve addresses into names, when necessary. This is called reverse name lookup. The DNS also plays an essential role in Active Directory Domain Services (AD DS), the Windows directory service.

True or false: Every DNS server contains a small piece of the DNS namespace.

Answer: *False*. Some DNS servers exist only to provide name resolution services to clients. They do not host any part of the DNS namespace. These are called caching-only servers.

> ***EXAM TIP*** **Network+ exam candidates should be familiar with the DNS domain namespace and with the messaging sequence that DNS servers use to resolve a name on the Internet.**

True or false: A forwarder is a DNS server that accepts name resolution queries from other DNS servers.

Answer: *False*. All DNS servers accept name resolution queries from other DNS servers. A forwarder is a DNS server that accepts a certain type of query. When a server receives a **recursive query,** it is responsible for trying to resolve the requested name and for transmitting a reply back to the requester. If the server does not possess the required information, it must send its own queries to other DNS servers until it obtains the requested information. The resolvers in client systems nearly always send recursive queries to DNS servers.

When a server receives an iterative query, it can either respond with information from its own database or refer the requester to another DNS server. The recipient of the iterative query responds with the best answer it currently possesses, but it is not responsible for searching for the information, as with a recursive query. DNS servers processing a recursive query from a client typically use iterative queries to request information from other servers. A forwarder is a server that is configured to receive recursive queries from other servers.

DNS records

DNS servers are essentially database servers that store information about the hosts and subdomains for which they are responsible in resource records (RRs)**.** When you run your own DNS server, you create a resource record for the name of each host that you want the rest of the network to be able to access. There are several different types of resource records used by DNS servers, the most important of which are:

- **A (32-bit Address)** Provides a name-to-address mapping that supplies an IPv4 address for a specific DNS name. This record type performs the primary function of the DNS, converting names to addresses.
- **AAAA (128-bit Address)** Provides a name-to-address mapping that supplies an IPv6 address for a specific DNS name. This record type performs the primary function of the DNS, converting names to addresses.
- **MX (Mail Exchanger)** Identifies a system that will direct email traffic sent to an address in the domain to the individual recipient, a mail gateway, or another mail server.
- **CNAME (Canonical Name)** Creates an alias that points to the canonical name (that is, the “real” name) of a host identified by an A or AAAA record. Administrators use CNAME records to provide alternative names by which systems can be identified.
- **PTR (Pointer)** Provides an address-to-name mapping that supplies a DNS name for a specific address in the in-addr.arpa domain. This is the functional opposite of an A record, used for reverse lookups only.

In addition to functioning as the authority for a small section of the DNS namespace, servers process client name resolution requests by either consulting their own resource records or forwarding the requests to another DNS server on the network. The process of forwarding a request is called a referral, and this is how all of the DNS servers on the Internet work together to provide a unified information resource for the entire domain namespace.

True or false: An MX record identifies a mail server that is ready to accept messages sent to recipients in a particular domain.

Answer: *True*. When an SMTP server receives an outgoing message from an email client, it does a DNS MX lookup of the domain in the destination email address, and sends the message to the server specified in the MX record.

> ***EXAM TIP*** **Network+ exam candidates must know the functions of the resource records listed in this objective.**

True or false: The standard name resolution process for an Internet web server consists of DNS queries requesting AAAA records from a DNS server.

Answer: *False*. Because the Internet still uses IPv4, the standard name resolution process for an Internet name requests an A record from the server.

True or false: It is possible for a single computer to have multiple names in the DNS.

Answer: *True*. To assign multiple names to a single computer, you can create multiple A or AAAA records, or you can create a single A or AAAA record and one or more CNAME records.

Dynamic DNS

The process of adding resource records to a DNS server is called name registration. Administrators originally registered DNS names manually, by adding resource records to a text file. However, as networks grow larger and more complex, the biggest problem arising from manual name registration stems from the increasing use of DHCP servers to dynamically assign IP addresses to network workstations. Dynamic assignment of IP addresses means that workstations can have different addresses from one day to the next, and the original DNS standard has no way of keeping up with the changes.

To make the use of DNS practical for technologies that require regular updates to resource records, such as AD DS, the IETF published a document that defines a new DNS message type, called an Update, that systems like domain controllers and DHCP servers can generate and transmit to a DNS server. These Update messages can modify or delete existing resource records or create new ones, based on prerequisites specified by the administrator.

True or false: Dynamic updates enable DNS servers to connect to the systems in their resource records and query them for address changes.

Answer: *False*. Dynamic updates originate with DHCP servers and AD DS domain controllers, not with the systems specified in the resource records

> ***EXAM TIP*** **The IETF standard that defines the Update message refers to the technology as Dynamic Updates, while the Network+ exam objectives refer to Dynamic DNS. There are also Internet-based services that call themselves Dynamic DNS, which enable computers with DHCP-assigned IP addresses to update a DNS**

resource record on a public server whenever their addresses change. This enables a user on the Internet to access a remote computer on a home or office network, even when its address changes regularly.

Can you answer these questions?

Find the answers to these questions at the end of this chapter.

1. Which DNS resource record type can administrators use to create aliases for computers on the network?
2. A DNS client performing a reverse name resolution receives which type of resource record from the DNS server?
3. Apart from name resolution, what other critical function does DNS perform on AD DS networks?
4. In DNS terminology, what is a resolver?
5. Which type of query does a DNS server typically use when querying other DNS servers?

Objective 1.8: Given a scenario, implement the following network troubleshooting methodology

One of the key elements of troubleshooting a network problem is having a plan of action. Many troubleshooting calls are from users who are improperly using software, and these can often be cleared up immediately with some remedial training. When you are faced with what appears to be a real problem, however, you should follow a set troubleshooting procedure, which consists of a series of steps similar to those in this objective.

Exam need to know

- Identify the problem

  For example: What questions should the troubleshooter ask the user?
- Establish a theory of probable cause

  For example: What are all of the possible causes of the problem?
- Test the theory to determine cause

  For example: What can you do to determine whether your theory is correct?
- Establish a plan of action to resolve the problem and identify potential effects

  For example: What needs to be done to resolve the problem fully?
- Implement the solution or escalate as necessary

  For example: Under what conditions must the problem be escalated?
- Verify full system functionality and if applicable implement preventative measures

  For example: Is there anything that can be done to prevent the problem from reoccurring?

- Document findings, actions, and outcomes

  For example: What mechanisms does the organization have in place to maintain a history of the problem and its solution?

Identify the problem

The first step in troubleshooting a network problem is to determine exactly what is going wrong and to note how the problem affects the network so that you can assign it a priority. It is sometimes difficult to determine the exact nature of the problem from the description given by a relatively inexperienced user, but part of the process of narrowing down the cause of a problem involves obtaining accurate information about what has occurred. Users are often vague about what they were doing when they experienced the problem, or even what the indications of the problem were.

Begin by asking the user questions like the following:

- What exactly were you doing when the problem occurred?
- Have you had any other problems with your computer lately?
- Was the computer behaving normally just before the problem occurred?
- Has any hardware or software been installed, removed, or reconfigured recently?
- Did you or anyone else do anything to try to resolve the problem?

When a computer or other network component that used to work properly now does not, it stands to reason that some change has occurred. When a user reports a problem, it is important to determine how the computing environment changed immediately before the malfunction. Unfortunately, getting this information from the user can often be difficult. On a network with properly established maintenance and documentation procedures, you should be able to determine whether the user's computer has been upgraded or modified recently.

Major changes, such as the installation of new hardware or software, are obvious possible causes of the problem, but you must be conscious of causes evidenced in more subtle changes as well. For example, an increase in network traffic levels, as disclosed by a protocol analyzer, can contribute to a reduction in network performance.

True or false: The priority you assign to a problem report should, in most cases, be based primarily on the number of users the problem affects.

Answer: *True*. Although there can be political and economic factors that affect your decision, the general rule is that the more users who are affected, the higher the priority of the problem.

Establish a theory of probable cause

After gathering all the information you can, make a list of all the possible problems that fit the circumstances, from the mundane to the extreme. A user's inability to access a website could be caused by a problem in the user's computer, a problem in the web server, or anywhere in between. When you first begin the troubleshooting process, your list of possibilities might include everything from an unplugged network cable to solar flares. As you gather more information, you should be able to rule out a lot of the possible causes on your list and work your way down to a manageable few.

The final step of this phase is to select the item from your list that seems to be the most probable cause of the problem. Don't be afraid to question the obvious. There's an old doctors' axiom that says, "When you hear hoofbeats, think horses, not zebras." In the context of network troubleshooting, this means that when you look for the probable cause of a problem, start with the obvious cause first.

True or false: The most obvious cause of a problem is usually the correct one.

Answer: *False*. IT troubleshooting is rarely well-guided by simplistic axioms such as these. A problem's cause can be just as easily obvious as obscure.

> ***EXAM TIP*** **Troubleshooting questions on the Network+ exam are often scenario-based, and can contain information that is there only to distract you from the correct answer. Be prepared to use the troubleshooting procedure to eliminate the wrong answers, leaving you with the correct ones.**

Test the theory to determine the cause

When you have established your theory of the probable cause of the problem, the next step is to test that theory. If you have isolated the problem to a particular piece of equipment, try to determine whether hardware or software is the culprit. If it is a hardware problem, you might replace the unit that is at fault or use an alternative that you know is functioning properly.

In some cases, the only way to test your theory involves resolving the problem. For example, if you suspect that a computer's inability to access the network is due to a bad patch cable, the only way to test your theory is to replace the patch cable with one you know is good. If that works, then your theory is confirmed.

Confirming your theory might actually resolve the problem, but that is not always so. If the problem affects multiple computers, each of which will require modifications, then you might be able to confirm your theory by modifying one, to see if your procedure works.

If your test concludes that your theory is incorrect, then you have to go back to your list of possible causes and decide which of the remaining ones is the next most probable. Then the whole testing process begins again. It is not unusual for a troubleshooter to disprove several theories before arriving at the correct one.

Depending on the size of your organization and the chain of command, you might have to escalate the problem by bringing it to someone with greater responsibility than yours, someone who can determine when or if you can safely test your theory.

True or false: The easiest way to test if a hardware component has malfunctioned is to replace it with one that you know is working properly.

Answer: *True*. Replacing the suspected component is a sure way of testing it, but it is not always the most practical or most economical way. A component that is vital to the company's operation or extremely expensive might not be easily replaceable, in which case you must find another solution.

> ***EXAM TIP*** **When taking the Network+ exam, do not eliminate answers because you think they are too simple. CompTIA sometimes couches simple concepts in complex language to distract you.**

Establish a plan of action to resolve the problem and identify potential effects

If your theory is proven correct and your solution needs to be implemented on a larger scale, the next step of the process is to create a complete plan of what needs to be done to fully resolve the issue. The plan should include all service interruptions that will be needed and all potential effects on the rest of the network. If the plan includes taking critical network components offline, then it should include the ramifications of that downtime and scheduling recommendations for work during off hours.

It is important, throughout the troubleshooting process, to keep an eye on the big network picture and not become too involved in the problems experienced by one user (or application or LAN). While resolving one problem, you could inadvertently create another that is more severe or that affects more users.

True or false: Server troubleshooting takes precedence over user productivity.

Answer: *False*. This is almost never true, especially when user productivity is directly equated with generation of revenue. Server outages should be planned for off hours and coordinated with all of the management personnel involved.

> ***EXAM TIP*** **Network+ exam questions on this objective can be concerned as much with the political realities of network troubleshooting as with the technical challenges.**

Implement the solution or escalate as necessary

When you have a solution to the problem mapped out and ready, it is time to implement it. If the solution falls within your area of responsibility, you can go ahead and do what is needed. However, if the solution involves other areas, or if special permission is required for the expenditures needed to execute your plan, then this is the time to escalate the issue to someone higher up in your organization's chain of command.

True or false: Escalation of a problem only occurs when a troubleshooter is unable to arrive at a satisfactory solution.

Answer: *False*. A well-organized IT department has a chain of command that specifies who is responsible for each area of the network. Escalation of a troubleshooting issue should occur whenever it falls under a superior's area of responsibility.

EXAM TIP **The Network+ exam questions do not assume the existence of a particular organizational model to which a troubleshooting process must conform. The exam objectives can apply to small, informal businesses as easily as large, enterprise networks.**

Verify full system functionality and, if applicable, implement preventative measures

Even if you have already performed small-scale tests to confirm your theory, after your solution is completely implemented, you must test again to confirm its success. To fully test whether the problem is resolved, you should return to the very beginning of the process and repeat the task that originally brought it to light. If the problem no longer occurs, you should test any other functions related to the changes you made, to ensure that fixing one problem has not created another.

At this point, the time you spend documenting the troubleshooting process becomes worthwhile. Repeat the procedures used to duplicate the problem exactly to ensure that the trouble the user originally experienced has been completely eliminated, and not just temporarily masked. If the problem was intermittent to begin with, it might take some time to ascertain whether the solution has been effective. It might be necessary to check with the user several times to make sure that the problem is not recurring.

If the problem ended up being the result of some network condition, or the action of a user administrator, you should consider at this point what must be done to prevent the problem from occurring again. This might involve a change to existing company policy or the creation of a new one.

True or false: Testing a solution to a troubleshooting issue involves recreating the original problem, if possible.

Answer: *True*. Recreate the original steps that caused the problem to appear, or have the original user do so, to determine whether your solution has been successful.

Document findings, actions, and outcomes

Although it is presented here as a separate step, the process of documenting all of the actions you perform should begin as soon as the user calls for help. A well-organized network support organization should have a system in place in which each problem call is registered as a trouble ticket that will eventually contain a complete record of the problem and the steps taken to isolate and resolve it.

The final phase of the troubleshooting process is to explain to the user what happened and why. Of course, the average network user is probably not interested in hearing all the technical details, but it is a good idea to let users know whether their actions caused the problem, exacerbated it, or made it more difficult to resolve. Educating users can lead to a quicker resolution next time or can even prevent a problem from occurring altogether.

True or false: Documentation of a troubleshooting effort should begin as soon as the problem is resolved.

Answer: *False*. Documentation should begin as soon as the problem is reported and continue throughout the troubleshooting process.

> ***EXAM TIP*** **The order of the troubleshooting steps provided in the Network+ exam objective is important. Candidates should be familiar with each step and be able to list them in the proper order.**

Can you answer these questions?

Find the answers to these questions at the end of this chapter.

1. A user reports a problem to the help desk; after making a concerted troubleshooting effort for several hours, you are unable to resolve the issue. What should you do next?
2. It is a busy morning at the help desk, and you are currently handling three calls. One appears to be a hard drive failure in a user's workstation, one is a user unable to access a particular website, and the third consists of several calls reporting that the company email server is unavailable. Which should you handle first?
3. A user calls the help desk and reports an inability to access any network resources, whether internally or on the Internet. What should you do to determine the scope of the problem?
4. How do you test whether a network access problem is limited to a single workstation?

Objective 1.9: Identify virtual network components

In networking, virtualization is a process that adds a layer of abstraction between actual, physical hardware and the system making use of it. Virtualization is a relatively recent philosophy in network management. Although virtualization was originally a tool primarily employed for lab testing and pre-production work, administrators are now using virtual components throughout their networks, taking advantage of the flexibility that virtualization provides.

Exam need to know

- Identify the function of a virtual desktop

  For example: For what applications are virtual desktop products suitable?
- Identify the function of a virtual server

  For example: What are the advantages of virtual servers over physical servers?
- Identify the function of a virtual switch

  For example: How is a virtual switch different from a physical switch?
- Identify the function of a virtual PBX

For example: Can a virtual PBX provide the same service as a standard telephone system?

- Identify the difference between onsite vs. offsite virtualization

  For example: Why would you want to have virtual machines stored offsite?
- Identify the function of Network as a Service (NaaS)

  For example: Is NaaS more cost effective that hosting your own virtual machines?

Virtual desktops

Administrators typically use Type I virtualization products, such as Hyper-V, for server virtualization. This type of virtualization can provide the performance levels needed to run high-volume production servers. Type II virtualization provides an excellent platform for education, laboratory testing, and software evaluation. It also enables desktop users to run an instance of another operating system on a single computer, without the complications of dual booting.

In this practice, often called *desktop virtualization,* a user can run applications that are not compatible with his or her primary operating system. For example, there are several products that enable Apple Macintosh users to run an instance of Windows. Other products run on Windows 7 and enable users to install an earlier version of Windows, allowing them to run an application that has not been updated.

Windows 7 even includes a feature called Windows XP Mode, which is a fully licensed version of Windows XP that you can install on a computer running Windows 7 with Microsoft Windows Virtual PC.

True or false: Desktop virtualization is a low-cost way of deploying multiple production servers as virtual machines on a single workstation.

Answer: *False*. Type II virtualization provides a suitable platform for virtual workstations or for servers in a laboratory or classroom, but not for a production environment.

> ***EXAM TIP*** **Generally speaking, Network+ questions concerning desktop virtualization are referring to Type II hypervisors, while virtual servers are referring to Type I virtualization.**

True or false: Hardware virtualization support is required to run any type of hypervisor product.

Answer: *False*. There are hypervisor implementations that do not require hardware virtualization support.

Virtual servers

A virtual server is a separate instance of an installed operating system running on a physical computer. Instead of having the server access the computer's hardware directly, an intervening component called a hypervisor creates a virtual machine (VM) environment, and the server operating system runs in that environment.

The hypervisor is responsible for handling all of the hardware calls that the virtual machine makes and passing them along to the correct physical hardware. When you create a virtual machine, you specify what (virtual) hardware should be in it.

The advantage of this capability is that the hypervisor can create multiple virtual machines on a single computer, sharing the physical hardware among them. Each virtual machine can then have a separate operating system instance installed on it. The instances appear to the network as separate computers, each with its own hardware, its own addresses, and its own applications. If one virtual machine suffers a software malfunction and crashes, the other virtual machines on the same computer are in most cases unaffected.

True or false: Virtual servers enable administrators to run multiple roles on a single computer without them interfering with each other.

Answer: *True*. Multiple applications running on a single operating system instance can interfere with each other, causing the whole system to crash. By running the applications on separate virtual machines, one can crash without affecting the others.

> ***EXAM TIP*** **Questions about Hyper-V on the Network+ exam refer to virtual servers.**

True or false: Virtual servers in a production environment typically run on a Type I hypervisor.

Answer: *True*. A Type I hypervisor provides better virtual machine performance than a Type II hypervisor, so production servers usually run in a Type I environment.

Virtual switches

One of the problems that any server or desktop virtualization solution has to solve is that of network access. A physical computer usually has only one network adapter in it, but if there are multiple VMs running on that computer, each one has its own virtual adapter that needs access to the network. One way that a hypervisor can accomplish this is to use virtual switching**.**

To keep communication within the hypervisor, most virtualization products can create a virtual switch that enables all of the VMs on a computer to communicate with each other, just as if their network adapters were connected to a physical switch. For Type I virtualization solutions, there are also third-party virtual switch products available. These are essentially software switches that provide additional security, management, and wide area networking (WAN) services.

True or false: Virtual switches can enable virtual machines to participate in a physical network.

Answer: *True*. Virtual switches can provide virtual machines with access to the physical network through the physical network adapter in the host computer.

> ***EXAM TIP*** **There are several virtual switch implementations available, both as commercial and open source products. However, any questions on virtual switching on the Network+ exam will be generic, and will not involve the properties or features of any specific product.**

Virtual PBX

A private branch exchange (PBX) is essentially a telephone exchange, that is, a switchboard, wholly owned and operated by a business or other private entity, rather than by a telephone company. As its core functionality, the PBX routes incoming calls to the proper extensions and provides outgoing callers with automatic access to a line. The original alternative to a PBX for a business was a key system, which required callers to push buttons to select their own lines.

Deciding on the correct telephone solution was always difficult for relatively small businesses lacking the knowledgeable staff required to maintain a PBX. This eventually led to the appearance of hosted PBX services, sometimes called virtual PBXs, in which a telephone company provided the PBX services to a customer but maintained the actual hardware at their own facility.

Another option is a software-based solution, running on a computer at the customer's site, which provides the same services as a hardware-based PBX.

The recent emphasis on cloud computing has led to the development of several hosted PBX solutions that use VoIP to provide services to customers over the Internet. Because of their decentralized nature, the actual company telephones connected by the virtual PBX service can be located anywhere, whereas a traditional PBX was limited to extensions located in the same facility.

True or false: A virtual PBX provides the same PSTN-based telephone functionality as a physical PBX.

Answer: *False*. A virtual PBX provides telephony services based on VoIP, not the Public Switched Telephone Network (PSTN).

> ***EXAM TIP*** **The Network+ objectives use the term "virtual PBX," which is actually the trademark of a company providing cloud-based VoIP services. However, the term can actually refer to a software-based telephony solution run on a customer's computer, or to PBX services delivered over the Internet.**

Onsite vs. offsite

Because virtual machines all interface with the same hypervisor, you can easily copy or move a virtual machine from one physical computer to another. This enables administrators to easily maintain offline copies of virtual machines, so that if a physical computer fails, duplicates of its virtual servers are immediately available. Administrators can also maintain copies offsite, for backups in the event of theft or natural disaster. Some organizations maintain their entire data centers offsite, in a facility belonging to a hosting service that is responsible for its security and environmental maintenance.

True or false: Offsite datacenter hosting can be more economical than hosting the systems yourself.

Answer: *True*. In an area where office space comes at a premium, hosting virtual machines offsite can be cheaper than leasing space locally.

Network as a Service (NaaS)

Some service providers are in the business of selling access to offsite networks of virtual machines to customers; for a monthly fee, you can create a server or a network of servers at another location that runs any applications you need, just as if you were hosting them onsite. Sometimes called Network as a Service (NaaS)**,** this concept is a progenitor of cloud computing.

True or false: NaaS eliminates some of the traditional concerns of the network administrator, such as bandwidth, fault tolerance, and environmental services.

Answer: *True*. NaaS is a pay-as-you-go arrangement that enables you to select the services you want and upgrade them as needed. Part of the arrangement is an agreed quality of service that covers fault tolerance and allowable downtime.

Can you answer these questions?

Find the answers to these questions at the end of this chapter.

1. How does a Type I hypervisor differ from a Type II hypervisor?
2. What relatively new telephony service has made the virtual PBX possible?
3. How do virtual servers provide network administrators with fault tolerance?

Answers

This section contains the answers to the “Can you answer these questions?” sections in this chapter.

Objective 1.1: Compare the layers of the OSI and TCP/IP models

1. The Point-to-Point Protocol (PPP) is the primary TCP/IP protocol operating at the link layer. PPP is designed for use with modems and other direct connections in which there is no need for media access control, as with Ethernet. Because it connects only two systems, PPP is called a point-to-point or end-to-end protocol. On a system using PPP, the TCP/IP protocols define the workings of the entire protocol stack, except for the physical layer itself, which relies on a hardware standard.
2. The presentation and the session layers of the OSI model do not have TCP/IP protocols dedicated exclusively to them. In most cases, application layer protocols include the session and presentation layer functions.
3. At the transport layer, the Transmission Control Protocol (TCP) provides connection-oriented service and the User Datagram Protocol (UDP) provides connectionless service.
4. The OSI reference model is defined in a document published by the International Organization for Standardization (ISO), and the TCP/IP model is defined in a Request For Comments document published by the Internet Engineering Task Force (IETF).

Objective 1.2: Classify how applications, devices, and protocols relate to the OSI model layers

1. Encryption devices function as the presentation layer of the OSI model. All of the other listed components are physical, data-link, or network layer devices.
2. The cables are the only component listed that is exclusively associated with the physical layer; the switch and the NICs are associate with the data-link layer.
3. The data-link layer and the network layer. The basic function of a switch is a data-link layer process, but to accommodate advanced features, such as VLANs, network layer capabilities are required.
4. Routers do not forward broadcast traffic; therefore they split a network into separate broadcast domains.
5. The addresses associated with the Internet Protocol (IP), running at the network layer, are 32 bits long in version 4 and 128 bits long in version 5.

Objective 1.3: Explain the purpose and properties of IP addressing

1. Class A subnets provide over 16 million hosts.
2. The subnet mask for a network with a /21 suffix is, in binary notation: 11111111 11111111 11111000 00000000; or in decimal notation: 255.255.248.0.
3. APIPA uses the 169.254.0.0/16 subnet when assigning IP addresses.
4. The last twelve zeroes in the network address can be compacted as follows: fe80::/64.
5. The OUI in the MAC address is the first three bytes: 60-EB-69.

Objective 1.4: Explain the purpose and properties of routing and switching

1. A large network connected by switches forms a single broadcast domain that can generate a huge amount of traffic. Splitting the network into VLANs enables you to create multiple, smaller broadcast domains.
2. RIPv2 supports the use of multicasts instead of broadcasts. By reducing the amount of broadcast traffic on the network, bandwidth is conserved.
3. On network segments with redundant switches, the Spanning Tree Protocol selects one of the switches to be operative, and leaves the others dormant until they are needed. This prevents the switches from forwarding packets back and forth to each other.
4. RIPv2 includes a subnet mask field that enables the protocol to support networks that use classless addressing. RIPv2 also supports multicasting, which can help to reduce the broadcast traffic on the network.

5. For an internetwork to function efficiently, the routing tables on all of its systems must be current and correct. Convergence is the process by which changes are propagated to all of the routing tables on the network.

Objective 1.5: Identify common TCP and UDP default ports

1. DHCP uses well-known ports for both client and server. This is because DHCP transactions begin before the TCP/IP settings on the client computer are configured.
2. An email client using IMAP and SMTP would use port 25 for outgoing traffic and port 143 for incoming.
3. The client browser connects with the HTTPS protocol, which uses port 443.
4. The port numbers below 1024 are reserved for use as well-known ports, so there are 1023 available.

Objective 1.6: Explain the function of common networking protocols

1. TCP and UDP are transport protocols.
2. SIP and RTP are application layer protocols used by VoIP.
3. SMTP, IMAP, and POP3 are all protocols that carry email messages.
4. DNS typically uses UDP at the transport layer.
5. The ARP protocol operates at the data-link layer.

Objective 1.7: Summarize DNS concepts and its components

1. Administrators can create aliases by using CNAME resource records.
2. A reverse name resolution request causes a DNS server to supply a PTR resource record containing an address-to-name mapping.
3. DNS enables clients to locate AD DS domain controllers on the network.
4. A resolver is a DNS client.
5. DNS servers typically send iterative queries to other servers.

Objective 1.8: Given a scenario, implement the following network troubleshooting methodology

1. The next step would be to escalate the problem to a senior administrator.
2. The email server issue appears to have the potential to affect the most people, so you should address that problem first.
3. To determine the scope of the problem, try to ascertain whether anyone else is having the same experience.
4. You can test whether a problem is limited to a single workstation by trying to reproduce the problem on another workstation.

Objective 1.9: Identify virtual network components

1. A Type I hypervisor addresses the hardware directly, while a Type II runs on top of a host operating system.
2. Voice over IP is the telephony service that has made the virtual PBX possible.
3. By creating identical virtual machines on different host computers, you can leave one VM as an offline backup to the operational one.

Index

About the author

Craig Zacker is the author or co-author of dozens of books on operating systems, networking topics, and PC hardware, including *Windows Small Business Server 2011 Administrator's Pocket Consultant* and *MCITP Self-Paced Training Kit for Exam 70-686: Windows 7 Desktop Administrator*, both for Microsoft Learning. He has also been an English professor, a network administrator, a webmaster, a corporate trainer, a darkroom technician, a library clerk, a student, and a newspaper boy. He lives in the Susquehanna Valley with his wife and a neurotic cat.