PEARSON IT CERTIFICATION

Save 10% on Exam Voucher
See Inside

Practice Tests
Video Training
Flash Cards
Review Exercises
Labs
Interactive Study Guide
Study Planner

Cert Guide

Advance your IT career with hands-on learning

CompTIA®

Network+

N10-008

ANTHONY SEQUEIRA
CCIE® NO. 15626

In addition to the wealth of content and exam preparation exercises, this edition includes a series of free hands-on exercises to help you master several real-world configuration and troubleshooting activities. These exercises can be performed on the ***CompTIA Network+ N10-008 Hands-on Lab Simulator Lite*** software, included free on the companion website that accompanies this book. This software, which simulates the experience of configuring real operating systems and network devices, contains the following 14 free lab exercises:

1. Network Topologies
2. Matching Well-Known Port Numbers
3. TCP/IP Protocols and Their Functions
4. Network Application Protocols
5. OSI Model Layer Functions
6. Contrast Virtualization Technologies and Services
7. Using ARP to Discover a MAC Address
8. IPv4 Address Types and Classes
9. Configuring a Client Network Adapter with an IPv4 Address
10. Configuring a Small Office/Residential Router—Network User Security Settings
11. Matching Wireless Standards and Terminology
12. Using ipconfig, ping, arp, tracert Together to Troubleshoot Connectivity
13. Security Appliance Terminology and Methods
14. Troubleshooting Practice

CompTIA Network+ N10-008 Hands-on Lab Simulator Minimum System Requirements:

Windows: Microsoft Windows 10, Windows 8.1; Intel Pentium III or faster; 512 MB RAM (1GB recommended); 1.5 GB hard disk space; 32-bit color depth at 1024x768 resolution

Mac: Apple macOS, 11, and 10.15; Intel Core Duo 1.83 Ghz or faster; 512 MB RAM (1 GB recommended); 1.5 GB hard disk space; 32-bit color depth at 1024x768 resolution

Other applications installed during installation: Adobe AIR 3.8; Captive JRE 6

Additional Resources

IP, ICMP, UDP, and TCP: https://www.ajsnetworking.com/udp-and-tcp/

OSI and Things That Use It Quiz: https://www.ajsnetworking.com/osi-and-things-that-use-it-quiz/

Review Questions

The answers to these review questions are in Appendix A, "Answers to Review Questions."

1. What protocol is considered the de facto standard when it comes to secure access to remote systems for management purposes?
   a. Telnet
   b. SSH
   c. IPSec
   d. IMAP

2. You are interested in dynamically assigning the IP address information in your IPv4-based network infrastructure. What protocol can you use to accomplish this?
   a. DNS
   b. TFTP
   c. FTP
   d. DHCP

3. What global hierarchical system is used to resolve names to IP addresses?
   a. TFTP
   b. DHCP
   c. NTP
   d. DNS

4. What port and protocol are used by HTTPS? (Choose two.)
   a. TCP
   b. UDP
   c. 443

d. 123
e. 8080
f. 80

5. What is the port and protocol used by Syslog? (Choose two.)
   a. TCP
   b. UDP
   c. 148
   d. 514
   e. 240

6. What protocol do ping and traceroute use in their operation?
   a. IPsec
   b. DNS
   c. ICMP
   d. DHCP

7. Which incoming email protocols are encrypted and secure because they use SSL/TLS sessions? (Choose two.)
   a. POP3 over SSL
   b. IMAPS
   c. SMTP
   d. POP

8. You need to establish an authenticated and encrypted connection between a client and a host system. What should you use?
   a. Telnet
   b. SSH
   c. LDAP
   d. LDAPS

This page intentionally left blank

This chapter covers the following topics related to Objective 1.6 (Explain the use and purpose of network services) of the CompTIA Network+ N10-008 certification exam:

- DHCP
  - Scope
  - Exclusion ranges
  - Reservation
  - Dynamic assignment
  - Static assignment
  - Lease time
  - Scope options
  - Available leases
  - DHCP relay
  - IP helper/UDP forwarding
- DNS
  - Record types
    - Address (A)
    - Canonical name (CNAME)
    - Mail exchange (MX)
    - Authentication, authorization, accounting, auditing (AAAA)
    - Start of authority (SOA)
    - Pointer (PTR)
    - Text (TXT)
    - Service (SRV)
    - Name server (NS)
  - Global hierarchy
    - Root DNS servers
    - Internal vs. external
    - Zone transfers
    - Authoritative name servers
    - Time to live (TTL)
    - DNS caching
    - Reverse DNS/reverse lookup/forward lookup
    - Recursive lookup/iterative lookup
- NTP
  - Stratum
  - Clients
  - Servers

CHAPTER 6

Network Services

While there are many network services available today, three services are so commonplace that we encounter them at every turn in the modern network: DHCP, DNS, and NTP. In this chapter, you'll learn the important basics of these critical network components.

Foundation Topics

DHCP

Statically assigning IP address information to individual networked devices can be time-consuming, error prone, and subject to scalability problems. Instead of using static IP address assignments, many corporate networks dynamically assign IP address parameters to their devices. This is typically referred to as ***dynamic address assignment***. The alternative approach is referred to as manual assignment, or ***static assignment***.

An early choice for performing automatic assignment of IP addresses was Bootstrap Protocol (BOOTP). Currently, however, the most popular approach for dynamic IP address assignment is the use of Dynamic Host Configuration Protocol (***DHCP***).

Engineers developed BOOTP as a method of assigning IP address, subnet mask, and default gateway information to diskless workstations. In the early days of Microsoft Windows (for example, Microsoft Windows 3.1), Microsoft Windows did not natively support TCP/IP. To include TCP/IP support, an add-on TCP/IP application (for example, Trumpet Winsock) could be run. Such an application would typically support BOOTP.

DHCP offers a more robust solution to IP address assignment than does BOOTP. DHCP does not require a statically configured database of MAC-address-to-IP-address mappings. Also, DHCP has a wide variety of options beyond basic IP address, subnet mask, and default gateway parameters. For example, a DHCP server can educate a DHCP client about the IP address of a TFTP server from which a configuration file could be downloaded.

Figure 6-1 illustrates the exchange of messages that occurs as a DHCP client obtains IP address information from a DHCP server. The list that follows describes these steps in further detail:

Key Topic

Step 1. When a DHCP client initially boots, it has no IP address, default gateway, or other such configuration information. Therefore, the way a DHCP client initially communicates is by sending a broadcast message (that is, a DHCPDISCOVER message to the destination address 255.255.255.255) in an attempt to discover a DHCP server.

Step 2. When a DHCP server receives a DHCPDISCOVER message, it can respond with a unicast DHCPOFFER message. Because the DHCP-DISCOVER message is sent as a broadcast, more than one DHCP server might respond to this discover request. However, the client typically