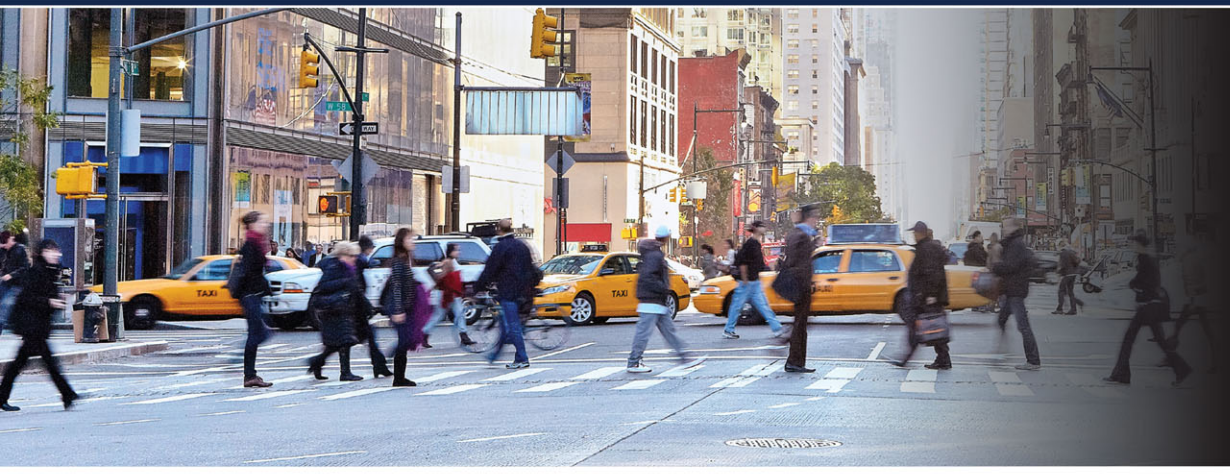
Official Cert Guide



Practice Tests

Flash Cards

Study Planner

Review Exercises

Cisco Certified Support Technician (CCST) Cybersecurity

100-160

Shane Sexton
Raymond Lacoste

ciscopress.com

Cisco Certified Support Technician (CCST) Cybersecurity 100-160 Official Cert Guide

Companion Website and Pearson Test Prep Access Code

Access interactive study tools on this book's companion website, including practice test software, review exercises, Key Term flash card application, a study planner, and more!

To access the companion website, simply follow these steps:

1. Go to www.ciscopress.com/register.
2. Enter the **print book ISBN:** 9780138203924.
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the **Registered Products** tab.
6. Under the book listing, click on the **Access Bonus Content** link.

When you register your book, your Pearson Test Prep practice test access code will automatically be populated with the book listing under the Registered Products tab. You will need this code to access the practice test that comes with this book. You can redeem the code at **PearsonTestPrep.com**. Simply choose Pearson IT Certification as your product group and log into the site with the same credentials you used to register your book. Click the **Activate New Product** button and enter the access code. More detailed instructions on how to redeem your access code for both the online and desktop versions can be found on the companion website.

If you have any issues accessing the companion website or obtaining your Pearson Test Prep practice test access code, you can contact our support team by going to **pearsonitp.echelp.org**.

- **MAC (Media Access Control) addresses** are unique identifiers assigned to network interface cards (NICs) at the data link layer. Vulnerabilities include MAC address spoofing, MAC flooding, and ARP (Address Resolution Protocol) spoofing.
- **ARP (Address Resolution Protocol)** is used to map IP addresses to MAC addresses in a local network. Vulnerabilities include ARP spoofing and ARP cache poisoning.
- **HTTP (Hypertext Transfer Protocol)** is an application-layer protocol used for transmitting and receiving web-based content. Vulnerabilities include on-path attacks, cross-site scripting (XSS), SQL injection, and cross-site request forgery (CSRF).
- **ICMP (Internet Control Message Protocol)** is primarily used for diagnostics and error reporting in IP networks. Vulnerabilities include ICMP flood attacks and ICMP redirect attacks.
- **DHCP (Dynamic Host Configuration Protocol)** is used for dynamically assigning IP addresses and network configuration parameters to devices on a network. Vulnerabilities include DHCP spoofing and DHCP starvation attacks.
- **DNS (Domain Name System)** translates domain names (such as www.example.com) into IP addresses (such as 203.0.113.10), facilitating the use of easy-to-remember names when referring to resources. It is an application layer protocol. Vulnerabilities include DNS spoofing and DNS amplification attacks.
- **FTP (File Transfer Protocol)** is used to facilitate the transfer of files between computers on a network. Vulnerabilities include lack of encryption, weak authentication, and data tampering.
- **Telnet** establishes a remote terminal connection between a client and a server over a network. Vulnerabilities include lack of encryption, weak authentication, and on-path attacks.
- **SSH (Secure Shell)** is used to provide secure encrypted communication and secure remote administration of network devices and systems. Vulnerabilities include weak authentication, vulnerabilities in SSH implementations, and misconfigured access controls.

- **CIDR** notation allows for efficient allocation and utilization of IP addresses. CIDR notation enables network administrators to define and enforce network segmentation.
- **Network segmentation** helps improve network performance, enhance security, and simplify network management because it makes it possible to ensure that what happens in a subnet stays in a subnet or what happens in a subnet does not affect another subnet.
- **Public IP addresses** are used on the Internet.
- **Private IP addresses** are used everywhere else.
- **NAT** takes a private RFC 1918 address that is only routable on a private network and converts it into a public IP address that is routable on the Internet.

- **MAC (Media Access Control) addresses** operate at the data link layer of the OSI model and are primarily used for communication between devices in the same subnet/VLAN/broadcast domain.

Exam Preparation Tasks

As mentioned in the Introduction, you can customize your strategy for exam preparation. Suggested tasks include the exercises here, Chapter 16, "Final Preparation," and the exam simulation questions on the companion website.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 5-3 lists these key topics and the page number on which each is found.

Key Topic

Table 5-3 Key Topics for Chapter 5

Key Topic Element	Description	Page Number
List	TCP/IP stack application layer	80
List	TCP/IP stack transport layer	80
List	TCP/IP stack Internet layer	80
List	TCP/IP stack link layer	80
Section	Transmission Control Protocol (TCP)	81
Section	User Datagram Protocol (UDP)	81
Section	Internet Protocol version 4 (IPv4)	82
Section	Internet Protocol version 6 (IPv6)	83
Section	Media Access Control (MAC)	83
Section	Address Resolution Protocol (ARP)	84
Section	Hypertext Transfer Protocol (HTTP)	84
Section	Internet Control Message Protocol (ICMP)	85
Section	Dynamic Host Configuration Protocol (DHCP)	85
Section	Domain Name System (DNS)	86
Section	File Transfer Protocol (FTP)	86
Section	Telnet	87
Section	Secure Shell (SSH)	87
Paragraph	How CIDR notation impacts security	89
Paragraph	How network segmentation impacts security	90
Table 5-2	Characteristics of Public and Private Networks	91
Paragraph	The impact of NAT on security	93
List	Security considerations of MAC addressing	94

Complete Tables and Lists from Memory

There are no memory tables for this chapter.

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

TCP/IP stack, OSI (Open Systems Interconnection) reference model, application layer, presentation layer, session layer, transport layer, network layer, data link layer, physical layer, Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Protocol version 4 (IPv4), Internet Protocol version 6 (IPv6), Media Access Control (MAC) address, Address Resolution Protocol (ARP), Hypertext Transfer Protocol (HTTP), Internet Control Message Protocol (ICMP), Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), File Transfer Protocol (FTP), Telnet, Secure Shell (SSH), CIDR (classless interdomain routing), Network Address Translation (NAT)

Review Questions

1. Which of the following TCP/IP stack layers is responsible for the addressing of frames?
   - **a.** Application
   - **b.** Transport
   - **c.** Internet
   - **d.** Link
2. How would you mitigate an HTTP on-path attack?
   - **a.** By employing input validation and output encoding techniques
   - **b.** By applying rate limiting or filtering mechanisms
   - **c.** By enforcing strong passwords and implementing two-factor authentication (2FA)
   - **d.** By implementing secure HTTP (HTTPS) with Transport Layer Security (TLS)
   - **e.** By ensuring that software and systems are up to date with the latest security patches
3. Which of the following is a form of network segmentation that allows you to divide up a physical local area network into multiple virtual local area networks?
   - **a.** IPv4 and IPv6
   - **b.** CIDR
   - **c.** DHCP
   - **d.** NAT
   - **e.** VLAN
   - **f.** ACL
   - **g.** Screened subnet

This page intentionally left blank

CHAPTER 6

Network Infrastructure

This chapter covers the following topics:

- **The Network Security Architecture:** This section introduces the Cisco SAFE Security Reference Architecture.
- **Screened Subnets, Virtualization, and the Cloud:** This section describes the benefits of using a screened subnet, explains the benefits of virtualization, and introduces various security considerations for the cloud.
- **Proxy servers:** This section discusses forward and reverse proxy servers as well as the Cisco WSA.
- **Honeypots:** This section discusses how honeypots can be used to attract and deceive attackers.
- **Intrusion Detection/Prevention Systems:** This section discusses host- and network-based intrusion detection systems and intrusion prevention systems.

Networks are designed to move data from one location to another. Networks can be wired as well as wireless, and it is imperative that a network be designed with a security-first mindset. When security is an afterthought, the likelihood of a security breach is significant. However, when security is first and foremost, it significantly reduces the risk a of security breach that jeopardizes confidentiality, integrity, and availability of your data.

This chapter introduces the Cisco SAFE (Security Access for Everyone) Security Reference Architecture, which can guide you as you create layered defenses and enforce security policies to safeguard your network infrastructure and data from potential risks. SAFE focuses on security domains and places in your network (PINs). In addition, this chapter discusses the benefits of using a screened subnet, the several security benefits that virtualization offers, and various security considerations for the cloud.

This chapter also focuses on proxy servers. It describes the differences between a forward proxy and a reverse proxy. It also talks about Cisco's very own proxy server, Cisco WSA (Web Security Appliance). This chapter covers honeypots, which you can use to attract and deceive attackers in order to gain better insights into their tactics and techniques. This chapter wraps up by exploring host-based and network-based intrusion detection and prevention systems.

This chapter covers information related to the following Cisco Certified Support Technician (CCST) Cybersecurity exam objective:

2.3. Describe network infrastructure and technologies (network security architecture, DMZ, virtualization, cloud, honeypot, proxy server, IDS, IPS).

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows you to assess whether you should read this entire chapter thoroughly or jump to the "Exam Preparation Tasks" section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 6-1 lists the major headings in this chapter and their corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes and Review Questions."

Table 6-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
The Network Security Architecture	1
Screened Subnets, Virtualization, and the Cloud	2
Proxy Servers	3
Honeypots	4
Intrusion Detection/Prevention Systems	5

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question incorrect for purposes of self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Which of the following are PINs in relation to the Cisco SAFE Security Reference Architecture? (Choose four.)
   - **a.** Secure services
   - **b.** Internet edge
   - **c.** Security intelligence
   - **d.** WAN
   - **e.** Campus
   - **f.** Segmentation
   - **g.** Data center
2. Which of the following correctly describes a screened subnet?
   - **a.** A hardware or virtual appliance offered by Cisco Systems that provides web security and content filtering capabilities.
   - **b.** A security mechanism used to detect, deflect, or study unauthorized access attempts or malicious activity within a network or system.
   - **c.** A separate network segment that acts as a buffer zone between an internal trusted network and an external untrusted network, such as the Internet.
   - **d.** A security technology designed to monitor network traffic, detect malicious activities or potential security breaches, and take appropriate actions to protect the network.