# Official Cert Guide

Study Planner

Review Exercises

Labs

# CCNA

## 200-301, Volume 2

**2nd Edition**

**Wendell Odom**, CCIE® No. 1624
**Jason Gooley**, CCIEx2 (RS, SP) No. 38759
**David Hucaby**, CCIE® No. 4594

ciscopress.com

# *CCNA 200-301 Official Cert Guide, Volume 2,* Second Edition

## 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**: 9780138214951.
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 **ciscopress.com/support**.

Key Topic

**Table 9-6** Comparisons Between TACACS+ and RADIUS

| Features | TACACS+ | RADIUS |
|---|---|---|
| Most often used for | Network devices | Users |
| Transport protocol | TCP | UDP |
| Authentication port number(s) | 49 | 1645, 1812 |
| Protocol encrypts the password | Yes | Yes |
| Protocol encrypts entire packet | Yes | No |
| Supports function to authorize each user to a subset of CLI commands | Yes | No |
| Defined by | Cisco | RFC 2865 |

## Developing a Security Program to Educate Users

One effective approach an enterprise can take to improve information security is to educate its user community through a corporate security program. Most users may not have an IT background, so they might not recognize vulnerabilities or realize the consequences of their own actions. For example, if corporate users receive an email message that contains a message concerning a legal warrant for their arrest or a threat to expose some supposed illegal behavior, they might be tempted to follow a link to a malicious site. Such an action might infect a user's computer and then open a back door or introduce malware or a worm that could then impact the business operations.

Key Topic

An effective security program should have the following basic elements:

- **User awareness:** All users should be made aware of the need for data confidentiality to protect corporate information, as well as their own credentials and personal information. They should also be made aware of potential threats, schemes to mislead, and proper procedures to report security incidents. Users should also be instructed to follow strict guidelines regarding data loss. For example, users should not include sensitive information in emails or attachments, should not keep or transmit that information from a smartphone, or store it on cloud services or removable storage drives.

- **User training:** All users should be required to participate in periodic formal training so that they become familiar with all corporate security policies. (This also implies that the enterprise should develop and publish formal security policies for its employees, users, and business partners to follow.)

- **Physical access control:** Infrastructure locations, such as network closets and data centers, should remain securely locked.  Badge access to sensitive locations is a scalable solution, offering an audit trail of identities and timestamps when access is granted. Administrators can control access on a granular basis and quickly remove access when an employee is dismissed.

## Chapter Review

One key to doing well on the exams is to perform repetitive spaced review sessions. Review this chapter's material using either the tools in the book or interactive tools for the same material found on the book's companion website. Refer to the "Your Study Plan" element for more details. Table 9-7 outlines the key review elements and where you can find them. To better track your study progress, record when you completed these activities in the second column.

**Table 9-7** Chapter Review Tracking

| Review Element | Review Date(s) | Resource Used |
|---|---|---|
| Review key topics | | Book, website |
| Review key terms | | Book, website |
| Answer DIKTA questions | | Book, PTP |
| Review memory tables | | Website |

## Review All the Key Topics

Key Topic

**Table 9-8** Key Topics for Chapter 9

| Key Topic Element | Description | Page Number |
|---|---|---|
| Figure 9-3 | Security terminology | 187 |
| Table 9-3 | Types of malware | 195 |
| Table 9-4 | Human security vulnerabilities | 196 |
| Paragraph | Password vulnerabilities | 196 |
| List | AAA functions | 198 |
| Table 9-6 | TACACS+ and RADIUS compared | 200 |
| List | User education | 200 |

## Key Terms You Should Know

AAA, amplification attack, brute-force attack, buffer overflow attack, denial-of-service (DoS) attack, dictionary attack, distributed denial-of-service (DDoS) attack, exploit, malware, man-in-the-middle attack, mitigation technique, multifactor authentication, password guessing, pharming, phishing, reconnaissance attack, reflection attack, social engineering, spear phishing, spoofing attack, threat, Trojan horse, virus, vulnerability, watering hole attack, whaling, worm

# CHAPTER 10

# Securing Network Devices

**This chapter covers the following exam topics:**

**1.0 Network Fundamentals**

**1.1 Explain the role and function of network components**

**1.1.c Next-generation firewalls and IPS**

**4.0 IP Services**

**4.8 Configure network devices for remote access using SSH**

**5.0 Security Fundamentals**

**5.3 Configure and verify device access control using local passwords**

All devices in the network—endpoints, servers, and infrastructure devices like routers and switches—include some methods for the devices to legitimately communicate using the network. To protect those devices, the security plan will include a wide variety of tools and mitigation techniques, with the chapters in Part III of this book discussing a large variety of those tools and techniques.

This chapter focuses on two particular security needs in an enterprise network. First, access to the CLI of the network devices needs to be protected. The network engineering team needs to be able to access the devices remotely, so the devices need to allow remote SSH (and possibly Telnet) access. The first half of this chapter discusses how to configure passwords to keep them safe and how to filter login attempts at the devices themselves.

The second half of the chapter turns to two different security functions most often implemented with purpose-built appliances: firewalls and IPSs. These devices together monitor traffic in transit to determine if the traffic is legitimate or if it might be part of some exploit. If considered to be part of an exploit, or if contrary to the rules defined by the devices, they can discard the messages, stopping any attack before it gets started.

## "Do I Know This Already?" Quiz

Take the quiz (either here or use the PTP software) if you want to use the score to help you decide how much time to spend on this chapter. The letter answers are listed at the bottom of the page following the quiz. Appendix C, found both at the end of the book as well as on the companion website, includes both the answers and explanations. You can also find both answers and explanations in the PTP testing software.

**Table 10-1** “Do I Know This Already?” Foundation Topics Section-to-Question Mapping

| Foundation Topics Section | Questions |
|---|---|
| Securing IOS Passwords | 1–4 |
| Firewalls and Intrusion Prevention Systems | 5, 6 |

1. Imagine that you have configured the **enable secret** command, followed by the **enable password** command, from the console. You log out of the switch and log back in at the console. Which command defines the password that you had to enter to access privileged mode?
   - a. **enable password**
   - b. **enable secret**
   - c. Neither
   - d. The **password** command, if it’s configured
2. Some IOS commands store passwords as clear text, but you can then encrypt the passwords with the **service password-encryption** global command. By comparison, other commands store a computed hash of the password instead of storing the password. Comparing the two options, which one answer is the *most accurate* about why one method is better than the other?
   - a. Using hashes is preferred because encrypted IOS passwords can be easily decrypted.
   - b. Using hashes is preferred because of the large CPU effort required for encryption.
   - c. Using encryption is preferred because it provides stronger password protection.
   - d. Using encryption is preferred because of the large CPU effort required for hashes.
3. A network engineer issues a **show running-config** command and sees only one line of output that mentions the **enable secret** command, as follows:

   ```
   enable secret 5 $1$ZGMA$e8cmvkz4UjiJhVp7.maLE1
   ```

   Which of the following is true about users of this router?
   - a. A user must type **$1$ZGMA$e8cmvkz4UjiJhVp7.maLE1** to reach enable mode.
   - b. The router will hash the clear-text password that the user types to compare to the hashed password.
   - c. A **no service password-encryption** configuration command would decrypt this password.
   - d. The router will decrypt the password in the configuration to compare to the clear-text password typed by the user.
4. The **show running-config** command output on a router includes the following line: **username test05 secret 8 $8$rTJqzmkwdI20WU$.mktApC8shjjwgABbQp7UjOmttmJaiIDfvBBJOpcns6**. Which answer best describes the command the network engineer used to configure this **username** command with its clear-text password?
   - a. **username test05 algorithm-type scrypt secret cisco**
   - b. **username test05 algorithm-type sha256 secret cisco**

- **c.** **username test05 algorithm-type md5 secret cisco**
- **d.** **username test05 secret cisco**

**5.** A next-generation firewall sits at the edge of a company's connection to the Internet. It has been configured to prevent Telnet clients residing in the Internet from accessing Telnet servers inside the company. Which of the following might a next-generation firewall use that a traditional firewall would not?

- **a.** Match message destination well-known port 23
- **b.** Match message application data
- **c.** Match message IP protocol 23
- **d.** Match message source TCP ports greater than 49152

**6.** Which actions show a behavior typically supported by a Cisco next-generation IPS (NGIPS) beyond the capabilities of a traditional IPS? (Choose two answers.)

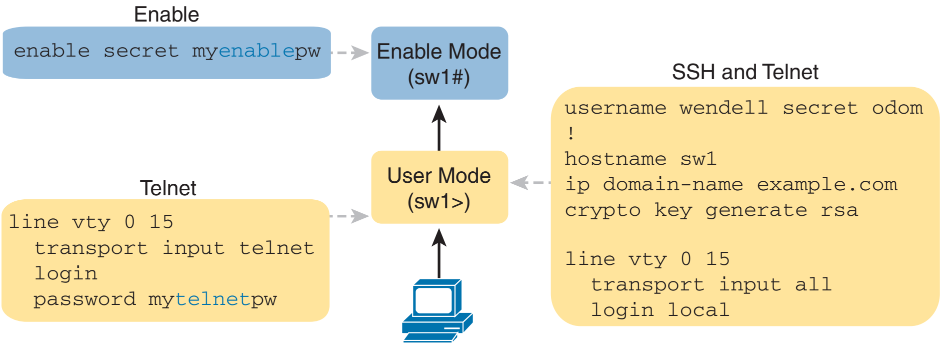
- **a.** Gather and use host-based information for context
- **b.** Comparisons between messages and a database of exploit signatures
- **c.** Logging events for later review by the security team
- **d.** Filter URIs using reputation scores

# Foundation Topics

## Securing IOS Passwords

The ultimate way to protect passwords in Cisco IOS devices is to not store passwords in IOS devices. That is, for any functions that can use an external authentication, authorization, and accounting (AAA) server, use it. However, it is common to store some passwords in a router or switch configuration, and this first section of the chapter discusses some of the ways to protect those passwords.

As a brief review, Figure 10-1 summarizes some typical login security configuration on a router or switch. On the lower left, you see Telnet support configured, with the use of a password only (no username required). On the right, the configuration adds support for login with both username and password, supporting both Telnet and SSH users. The upper left shows the one command required to define an enable password in a secure manner.



```
enable secret myenablepw
```

```
line vty 0 15
  transport input telnet
  login
  password mytelnetpw
```

```
username wendell secret odom
!
hostname sw1
ip domain-name example.com
crypto key generate rsa

line vty 0 15
  transport input all
  login local
```

**Figure 10-1** *Sample Login Security Configuration*

**NOTE** The configuration on the far right of the figure supports both SSH and Telnet, but consider allowing SSH only by instead using the **transport input ssh** command. The Telnet protocol sends all data unencrypted, so any attacker who copies the message with a Telnet login will have a copy of the password.

The rest of this first section discusses how to make these passwords secure. In particular, this section looks at ways to avoid keeping clear-text passwords in the configuration and storing the passwords in ways that make it difficult for attackers to learn the password.

## Encrypting Older IOS Passwords with service password-encryption

Some older-style IOS passwords create a security exposure because the passwords exist in the configuration file as clear text. These clear-text passwords might be seen in printed versions of the configuration files, in a backup copy of the configuration file stored on a server, or as displayed on a network engineer's display.

Cisco attempted to solve this clear-text problem by adding a command to encrypt those passwords: the **service password-encryption** global configuration command. This command encrypts passwords that are normally held as clear text, specifically the passwords for these commands:

Key Topic

**password** *password* (console or vty mode)

**username** *name* **password** *password* (global)

**enable password** *password* (global)

To see how it works, Example 10-1 shows how the **service password-encryption** command encrypts the clear-text console password. The example uses the **show running-config | section line con 0** command both before and after the encryption; this command lists only the section of the configuration about the console.

**Example 10-1** *Encryption and the* **service password-encryption** *Command*

```
Switch3# show running-config | section line con 0
line con 0
 password cisco
 login

Switch3# configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
Switch3(config)# service password-encryption
Switch3(config)# ^Z

Switch3# show running-config | section line con 0
line con 0
 password 7 070C285F4D06
 login
```

A close examination of the before and after **show running-config** command output reveals both the obvious effect and a new concept. The encryption process now hides the original