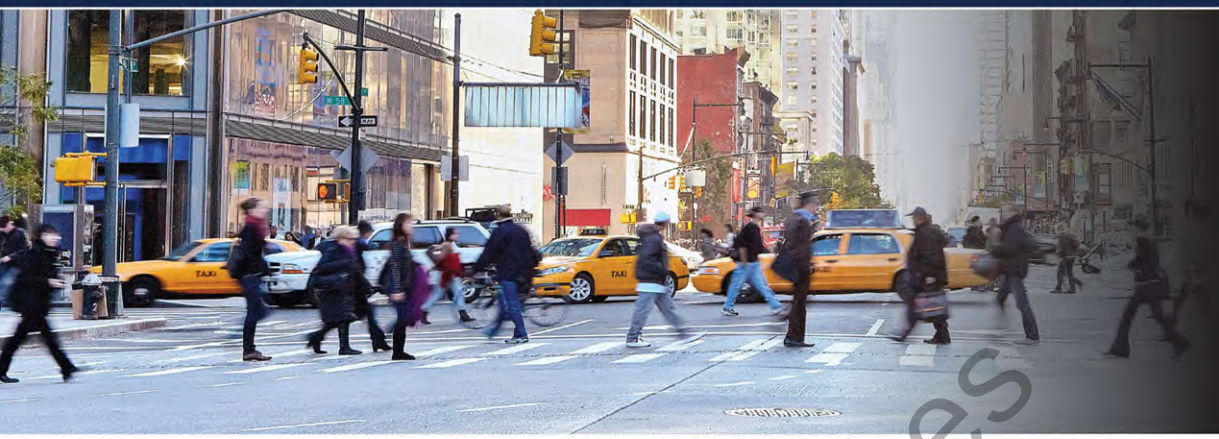
Official Cert Guide



Practice Tests

Flash Cards

Study Planner

Review Exercises

Cisco Certified Support Technician (CCST) Cybersecurity

100-160

Shane Sexton
Raymond Lacoste

ciscopress.com

Contents

CHAPTER 3

Access Management

This chapter covers the following topics:

- **Introduction to AAA:** This section introduces you to the importance of AAA.
- **Authentication:** This section focuses on the various factors of authentication, the need for MFA, as well as passwords and password policies.
- **Authorization:** This section explores the need for authorization.
- **Accounting:** This section explores the need for accounting.
- **RADIUS:** This section examines the need for RADIUS and provides some sample use cases.

To provide confidentiality, integrity, and availability, you must be able to granularly control access to all resources and ensure that the access controls are upheld at all times. If the access controls ever break down, legitimate or non-legitimate users, applications, or services will have access to resources they should not have access to.

To provide an access management solution that maintains the appropriate levels of confidentiality, integrity, and availability, you must consider the AAA framework, which outlines the best practices you need to consider when it comes to authentication, authorization, and accounting.

This chapter introduces the AAA framework. It first focuses on authentication, MFA, and password policies. It then moves on to covering authorization, followed by accounting. It wraps up by examining a AAA service known as RADIUS.

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

1.3. Explain access management principles.

"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 3-1 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 3-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Introduction to AAA	1
Authentication	2
Authorization	3
Accounting	4
RADIUS	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 correctly defines AAA?
   - **a.** A client/server protocol used for authentication, authorization, and accounting
   - **b.** The process of verifying that someone or something is in fact truly who they say they are
   - **c.** A framework that helps build the controls needed to access computing resources, enforce policies, and audit usage
   - **d.** A type of MFA that encourages three factors
2. Which of the following correctly defines authentication?
   - **a.** The process of adopting the least-privilege principle, the need-to-know principle, and the implicit-deny principle
   - **b.** The process of granting privileges and controlling what a user is able to do
   - **c.** The process of monitoring, recording, and auditing everything in an organization
   - **d.** The process of verifying that someone or something is in fact truly who they say they are
3. Which of the following correctly defines authorization?
   - **a.** The process of monitoring, recording, and auditing everything in an organization
   - **b.** The process of granting privileges and controlling what a user is able to do
   - **c.** The process of verifying that someone or something is in fact truly who they say they are
   - **d.** The process of collecting, consolidating, and correlating log files
4. Which of the following correctly defines accounting?
   - **a.** The process of using biometrics to allow access to a system
   - **b.** The process of verifying that someone or something is in fact truly who they say they are

c. The process of granting privileges and controlling what a user is able to do

d. The process of monitoring, recording, and auditing everything in an organization

5. What is RADIUS?

a. A client/server protocol used for accounting only

b. A client/server protocol used for authentication only

c. A client/server protocol used for authentication and authorization only

d. A client/server protocol used for authentication, authorization, and accounting

Foundation Topics

Introduction to AAA

Key Topic

AAA, which is pronounced "triple A" and stands for *authentication, authorization, and accounting*, is a framework. A framework is a real or conceptual structure intended to serve as a support or guide for the building of something that expands the structure into something useful. The AAA framework is a guide that helps you build the controls needed to access computing resources, enforce policies, and audit usage. AAA plays a very important role in security.

Authentication is about verifying the identity of those who access your systems and data. Therefore, without authentication, you can't control access to your data, and so you can't protect confidentiality, integrity, and availability (CIA). Authorization is about controlling what can be done to your systems and data. Therefore, without authorization, you can't control what can be done with your data, and so you can't protect CIA. Accounting is about recording everything that is happening to your systems and data. Therefore, without accounting, you can't keep track of the who, what, where, when, why, and how of your data, and so you can't protect CIA.

As you can see, without AAA, it is impossible to meet the CIA needs of your organization.

Authentication

Key Topic

Authentication is about proving the identity of someone or something, or verifying that someone or something is in fact truly who they say they are. Why do I say "someone or something"? Well, *someone* refers to a person, and *something* refers to anything else that needs to be authenticated. Keep in mind that systems, devices, tools, applications, and so on need to be authenticated. If you are only focused on people, you are leaving your organization vulnerable to attack.

There are a multitude of factors that people, systems, devices, applications, and tools can use to authenticate. Table 3-2 explores these factors and provides examples.

Key Topic

Table 3-2 Authentication Factors

Factor	Description	Examples
Something you know	This is authentication based on knowledge.	A username, a password, a personal identification number (PIN) you have memorized, a passphrase you have memorized, CAPTCHA test, personal verification questions

Factor	Description	Examples
Something you have	This is authentication based on possession.	A security token that can provide you with a random PIN A random PIN, passphrase, or notification from your smartphone that you can accept or reject A swipe card, tap card, or passkey
Something you are	This is authentication based on unique aspects of yourself and relies on biometrics.	Your fingerprint, your facial geometry, your retina, your palm print
Somewhere you are	This is authentication based on location.	You are allowed or denied based on your connection to the corporate Wi-Fi versus coffee shop Wi-Fi versus airport Wi-Fi versus home Wi-Fi. You are allowed or denied based on your connection in the United States versus Canada versus any other country.
Something you do	This is authentication based on habits and characteristics.	The way you walk, the way you write, the way you talk, the path you take to work, the places you eat lunch, the sports you play and when
Time	This is authentication based on the time of day and/or day of the week.	You are allowed on the Internet between 9 a.m. and 5 p.m. and are not allowed on the Internet between 5 p.m. and 9 a.m. You are allowed to connect to the VPN Monday through Friday, 7 a.m. to 9 p.m. local time

Multifactor Authentication (MFA)

Using a single factor of authentication is no longer advisable. For example, relying on a username and password (a single factor: something you know) will not protect you as it once did. Cybercriminals have developed very creative ways to figure out your username and password (such as via a convincing phishing email), and once they know them, they will be able to access anything you can access with them. The same thing is true with PINs or passphrases that you have created and memorized. Once a cybercriminal has that information, they will have access to systems and data you don't want them to have access to.

Key Topic

One of the best ways to protect yourself today is with **multifactor authentication (MFA)**. MFA involves using two or more of the factors mentioned previously, in combination, to successfully authenticate (for example, combining something you know with something you have or combining something you have with something you are or combining something you have with somewhere you are). As of this writing, MFA is becoming closer to being the norm for every application and service that exists.

Now please note that MFA does not protect you from becoming the victim of a phishing attack that is designed to steal your credentials—or any other type of attack for that matter. It does, however, help prevent the cybercriminal from gaining access to your systems

and data based only on the credentials they stole in the phishing attack. How so? Well, even though they may have stolen your username and password, they do not have the second factor that is needed to successfully authenticate to the systems and access the data. For example, let's say your first factor is a username and password. Regardless of how strong the password is, it could be stolen/captured during a phishing attack or a data breach targeting your authentication database. If you have a second factor that is required, like a one-time PIN generated by an application installed on your cell phone that is valid for only 30 seconds, the cybercriminal will not be able to access your systems and data because they do not have your cell phone and can't get the one-time PIN—and they also can't guess it or brute force it because it changes every 30 seconds.

Table 3-3 provides examples of MFA.

Key Topic

Table 3-3 Examples of MFA

Factor 1	Factor 2	Description
Your bank card	A memorized PIN	Your bank card is one factor (something you have), and the PIN is the other factor (something you know).
A swipe card	A retinal scan	The swipe card is one factor (something you have), and the retinal scan is the other factor (something you are).
A username and a password	A notification sent to your phone that asks you to click yes or no	The username/password is one factor (something you know), and your phone with the notification is the other factor (something you have).
A fingerprint scan	A PIN	The fingerprint scan is one factor (something you are), and the PIN is the other factor (something you know).
A username and a password	Your location	Your username/password is one factor (something you know), and your location is the other factor (somewhere you are).

Please be aware that true multifactor authentication requires two or more different factors, as shown in Table 3-3. So, having a username/password and a memorized PIN is not MFA as they are both something you know—and so count as only one factor. A retinal scan and a fingerprint scan are not MFA as they are also the same factor (something you are). Having your phone that generates a PIN that you enter and then an app on your phone that gives you a one-time password is not MFA as these are, again, the same factor (something you have). These are all examples of **two-step authentication** because two steps are needed for authentication, but only a single factor is being used. What I want you to realize from this is that if you implement MFA poorly, you might not be as protected as you think you are, and you would do better with other combinations. For example, what would you consider to be stronger?

Option 1. A username/password and a six-digit one-time PIN generated at the time it is needed

Or

Option 2. A USB authentication key that needs to be entered into the system and then a notification displayed on your phone that needs to be accepted or rejected

So, option 1 is an example of MFA as there are two different factors in use, and option 2 is an example of two-step authentication because the same factor is used twice. In this case, it is clear that it would be much harder for the cybercriminal to access your system with two-step authentication (the USB key and your phone) as they would need physical access to both those devices and the system they are accessing. Although option 1 is a great option and highly recommended, you can see that strength comes from the combinations and not necessarily from just different factors being used. So, for the CCST Cybersecurity exam, be clear about the difference between MFA and two-step authentication in case you have to pick them out of a lineup.

Key Topic

Passwords and Password Policies

The most common way to authenticate today is with a username and password. Regardless of whether they are used as the only factor or as part of MFA or as part of two-step authentication, usernames and passwords are not going away anytime soon. Therefore, it is important to ensure that passwords meet certain requirements so that they are less apt to be easily guessed or determined using brute-force techniques and then reused by cybercriminals. In addition, they should be stored securely (hashed) in a database so that if the database is compromised, the likelihood of a cybercriminal being able to use any of the passwords in the database is significantly reduced.

So, what should a password be? It should be:

- Something that is not guessable
- Something that can't be brute forced
- Something that the user can remember without having to write it down
- Something that can be used for a long period of time

We used to encourage complexity by forcing users to include lowercase letters, uppercase letters, a digit, and special characters, but users would do the minimum to meet the requirements instead of creating complex passwords. For example, the password "password" would simply become "Password1!" which is not complex at all. We wanted them to use something like "Yt56R34w" but got "Password1!" instead. So, complexity requirements really haven't worked out as they were intended to and still result in passwords being guessable, brute forced, and written down.

Now we encourage length. The longer a password is, the harder it is to guess, and the harder it is to brute force. Users can now use passphrases or sentences for their passwords, which they can remember with ease without writing them down. For example, the password "We_Love_Oranges_And_Orange_Marmalade" is not easy to guess, it is impossible to brute force,

and the user will not have to write it down. In addition, it will not have to be changed for a long time.

So, what would be a good password policy today? A good password policy would

- Encourage length (12 characters minimum with no maximum).
- Encourage the use of passphrases or sentences (something easy to remember but really long).
- Force the use of an uppercase letter, a special character, and a number and allow the rest to be all lowercase.
- Increase the number of days between password changes to a year or more.

Now a user can create a password such as "B3ing_A_CCST_Cybersecurity_Is_Awesome!" which would meet all the requirements of the password policy and more while being impossible to guess or brute forced, and the user will not have to write it down. If they don't want to use the special character _, then it would still be acceptable to use "B3ingACCSTCybersecurityIsAwesome!". You could even omit the special character ! or the number, and this would still be a very safe password.

In addition, because of the length requirement, a user could use their password for a longer period of time. Instead of forcing users to change their passwords every 30 to 90 days, you could let them change it every year or even every few years. According to the website How Secure Is My Password, at https://www.security.org/how-secure-is-my-password/, it would take a computer about 1 hundred tredecillion years to crack (brute force) the password "B3ingACCSTCybersecurityIsAwesome!". So using this password for a few years without changing it should be fine.

When it comes to storing passwords in a database, it is imperative that you use hashing and salting. Hashing is done so that the password is stored as a hash instead of plaintext. This way, if the database is ever exfiltrated, the cybercriminal will get all the hashes but will have a very difficult time converting the hashes back into the plaintext passwords. (We cover hashing in Chapter 4, "Cryptography.") Salting is a way to ensure uniqueness when storing a password as a hash and reduce the chances of a rainbow table being successful. Without salting, if two people have exactly the same plaintext password, the hash that is stored in the database will be exactly the same. However, if a salt is added (for example, four or more extra random characters) during the hashing process, then those two plaintext passwords would produce two different hashes that would be stored in the database. These extra random characters make it impossible for a cybercriminal to obtain the passwords by using a rainbow table.

Don't forget that a lengthy password does not eliminate the need for MFA. If by chance a cybercriminal tricks you into giving them your password via a phishing attack, MFA will save you, and then once you discover that you have given up your password, you can change the password and sleep better knowing that the cybercriminal did not get into your account.

Authorization

Authorization is the process of granting and controlling what an authenticated user is able to do. It is focused on permissions. When it comes to permissions, you should adopt three principles:

- The **least-privilege principle**, which is about giving users only the minimum permissions they need to accomplish their objectives
- The **need-to-know principle**, which is about only giving users access to what they absolutely need to do their jobs and perform their roles
- The **implicit-deny principle**, which means everyone is prevented from doing everything unless they are explicitly allowed

If you are careless with authorization, your users could do something they should not (by accident or on purpose), resulting in risks associated with CIA. A cybercriminal could gain control of an account with more privileges than they should have and move vertically (within a system) or laterally (between systems) and exfiltrate data, which would compromise CIA. Therefore, it is imperative that you control exactly what each user can access by establishing policies and rules and adopting the least-privilege principle (only giving users minimum permissions they need to do their job), the need-to-know principle (only giving users access to what they need to know to do their job), and the implicit-deny principle (denying by default unless explicitly allowed).

Accounting

Accounting is about keeping track of who, what, where, when, why, and how. It is the process of monitoring, recording, and auditing everything in your organization. By keeping track of who accessed what data, where and when they accessed it, why they accessed it, and how they accessed it, you will be more aware and in tune with what is happening (good or bad) in and around your organization. For a security professional, this is one of the most important A's of AAA, yet many fail to implement an appropriate level of accounting, or if they do, they are overwhelmed by it and fail to continually follow up on what needs to be done with the collected information. Accounting generates a lot of logs, and the logs will be your window into the happenings within and around your network and resources. So, having a **security information and event management (SIEM)** solution as well as a **security orchestration, automation, and response (SOAR)** tool will definitely help you stay in the loop and focused on continually monitoring and protecting your network. A SIEM solution helps you collect logs, consolidate logs, correlate logs, and get notified about abnormalities/threats in logs that are in breach of established policies. A SOAR tool helps you automate responses and reduce the amount of human intervention when an abnormality/threat has been detected.

For example, say that your SIEM solution collects logs, consolidates logs, correlates logs, and notifies you, but you have to manually react and respond. So from the moment of notification to the successful completion of the response, there may be a significant amount of time lost. With the help of a SOAR tool, you might have scripts or the help of artificial intelligence (AI) and machine learning (ML) to immediately respond to the notifications and threats without human intervention.

RADIUS

Key Topic

Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol originally designed to give remote users the ability to access services via dial-up connections. (If you don't know what dial-up is, it is because you are too young. Back in my early days, we did not have always-on broadband or fiber connections to the Internet; we had to use our telephone landlines to dial in to the Internet.) RADIUS was a service used for remote authentication with dial-up network access. Because of its flexibility, over time RADIUS has evolved and been adopted and adapted for other scenarios as well. Today it is a protocol we use with AAA for authentication, authorization, and accounting purposes.

The best way to learn about RADIUS is through an example of its use. Refer to Figure 3-1 as we go through the following example.

Key Topic

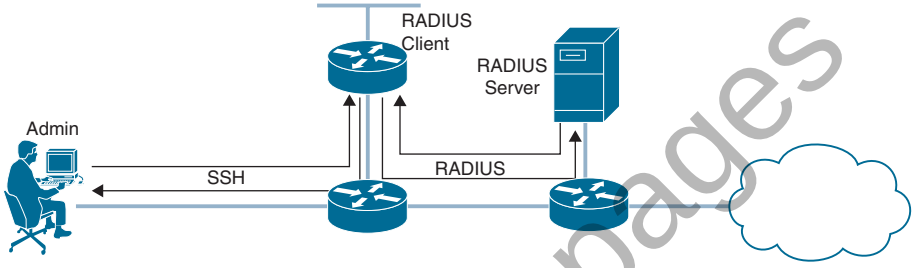


Figure 3-1 *Admin Using SSH to Manage a Router and Router Authenticating the Admin Using RADIUS*

On the right side of this figure is a RADIUS server. It is a server that contains a database of usernames and passwords, and it can communicate using the RADIUS protocol. You can implement RADIUS servers with several different options; in this example, we use Cisco Identity Services Engine (ISE). This is the server part of the client/server protocol.

In the middle of the figure is a router. This router is configured to communicate with the RADIUS server using the RADIUS protocol any time authentication needs to be performed. This is the client part of the client/server protocol.

Now focus on the left side of the figure, where you see the administrator of the router. The admin opens the SSH client and makes a connection to the router using SSH (port 22) for management purposes. They then need to provide their username and password to authenticate. When the router receives the username and password, it contacts the RADIUS server by using the RADIUS protocol so that the RADIUS server can determine if the admin is authenticated or not, based on the credentials provided. If the admin provided a username and password listed in the database, the RADIUS server tells the router to grant the admin access. If they did not provide a username and password listed in the database, the RADIUS server tells the router to deny the admin access.

With RADIUS, authentication and authorization happen at the same time. So, when the admin is being authenticated by the RADIUS server, the server can also be configured to tell the client (the router in Figure 3-1) what the user (the admin in Figure 3-1) is allowed and not allowed to do, based on a database of permissions that has been defined on the RADIUS

server. For example, in Figure 3-1, once the user authenticates, they may only be authorized to configure, verify, and troubleshoot routing protocols on the router. Or maybe they are authorized to only perform verification tasks and no configuration tasks.

As mentioned earlier, because of its flexibility, RADIUS can be used in many different scenarios. For example, Figure 3-2 shows a wireless user, a wireless access point, and the RADIUS server.

Key Topic

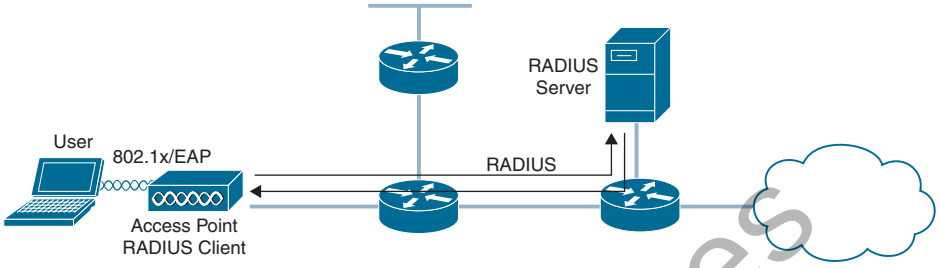


Figure 3-2 *Wireless User Authenticating to the Wireless Network Using 802.1x, EAP, and RADIUS*

For this scenario, the wireless user needs access to the network. When connecting, they provide their username and password to the wireless AP, using 802.1x and Extensible Authentication Protocol (EAP) messages. The wireless AP (RADIUS client) then sends those credentials to the RADIUS server, using the RADIUS protocol. The RADIUS server compares the username and password to those listed in the database. If the username and password are correct, the RADIUS server notifies the wireless AP that the user is authenticated and authorized, and the wireless AP can provide the user access to the network. If the username and password are not correct, the RADIUS server notifies the wireless AP that the user is not authenticated or authorized, and the wireless AP can prevent the user from accessing the network.

In addition to configuring authentication and authorization, you can also configure accounting with RADIUS. This gives you a centralized way of keeping track of who has been authenticated and who has not, when they were authenticated, and when they were not authenticated. This is important from a security standpoint as it gives you the ability to keep track of all successful and unsuccessful authentication and authorization sessions.

RADIUS uses UDP as its transport protocol. Traditionally, UDP port 1645 was used for authentication and authorization, and UDP port 1646 was used for accounting. However, today we typically see UDP port 1812 for authentication and authorization and UDP port 1813 for accounting. Why is this important? Many Cisco devices default to using 1645 and 1646 as the port numbers, but the RADIUS servers default to using 1812 and 1813 as the port numbers. So, when setting up RADIUS on many Cisco devices, you have to change the port numbers on those devices to 1812 and 1813.

If you are interested in reading more about RADIUS, you can check out RFC 2865, which covers authentication and authorization for RADIUS, and RFC 2866, which covers accounting for RADIUS.

Summary

To provide an access management solution that maintains the levels of confidentiality, integrity, and availability you need, consider the AAA framework, which includes authentication, authorization, and accounting:

- **Authentication** is about proving the identity of someone or something.
  - **Something you know** is authentication based on knowledge.
  - **Something you have** is authentication based on possession.
  - **Something you are** is authentication based on unique aspects of yourself and relies on biometrics.
  - **Somewhere you are** is authentication based on location.
  - **Something you do** is authentication based on habits and characteristics.
  - **Time** is authentication based on the time of day and/or day of the week.
  - **MFA** is about using two or more factors for authentication.
- **Authorization** is the process of granting and controlling what an authenticated user is able to do.
  - The **least-privilege principle** says to give users the minimum permissions they need to accomplish their objectives.
  - The **need-to-know principle** says to give users access only to what they absolutely need to do their jobs and perform their roles.
  - The **implicit-deny principle** says to ensure that everyone is prevented from doing everything unless explicitly allowed.
- **Accounting** is about keeping track of who, what, where, when, why, and how. It is the process of monitoring, recording, and auditing everything in an organization.
  - A **SIEM** solution helps you collect logs, consolidate logs, correlate logs, and get notified about abnormalities/threats in logs that are in breach of established policies.
  - A **SOAR** tool helps you automate responses and reduce the amount of human intervention required when an abnormality/threat has been detected.
- **Remote Authentication Dial-In User Service (RADIUS)** is a client/server protocol used with authentication, authorization, and accounting.

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 3-4 lists these key topics and the page number on which each is found.

Key Topic

Table 3-4 Key Topics for Chapter 3

Key Topic Element	Description	Page Number
Paragraph	The AAA framework	36
Paragraph	Authentication	36
Table 3-2	Authentication Factors	36
Paragraph	MFA	37
Table 3-3	Examples of MFA	38
Section	Passwords and password policies	39
Section	Authorization	41
Section	Accounting	41
Paragraph	RADIUS	42
Figure 3-1	Admin Using SSH to Manage a Router and Router Authenticating the Admin Using RADIUS	42
Figure 3-2	Wireless User Authenticating to the Wireless Network Using 802.1x, EAP, and RADIUS	43

Define Key Terms

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

AAA; authentication; something you know; something you have; something you are; somewhere you are; something you do; multifactor authentication (MFA); two-step authentication; authorization; least-privilege principle; need-to-know principle; implicit-deny principle; accounting; security information and event management (SIEM); security orchestration, automation, and response (SOAR); Remote Access Dial-In User Service (RADIUS)

Complete Tables and Lists from Memory

Print a copy of Appendix B, "Memory Tables," found on the companion website, or at least the section for this chapter, and complete the tables and lists from memory. Appendix C, "Memory Tables Answer Key," includes completed tables and lists you can use to check your work.

Review Questions

1. What does AAA stand for?
   - **a.** Authentication, accessibility, and availability
   - **b.** Availability, authentication, and authorization
   - **c.** Authentication, authorization, and accounting
   - **d.** Authentication, availability, and accounting
2. Which of the following are examples of MFA? (Choose two.)
   - **a.** A USB authentication key that needs to be connected to the USB port on the system and a notification displayed on your phone that needs to be accepted or rejected
   - **b.** A bank card and a memorized PIN
   - **c.** A fingerprint scan followed by a facial scan
   - **d.** A username/password and a four-digit PIN that you have memorized
   - **e.** A username/password and a notification sent to your phone that requires you to click yes or no
3. Which of the following are authorization principles? (Choose three.)
   - **a.** Enable MFA
   - **b.** Least privilege
   - **c.** Need to know
   - **d.** Implicit deny
   - **e.** Record all activity
4. Which of the following is a system that can help you collect logs, consolidate logs, correlate logs, and get notified about abnormalities and threats in logs that are in breach of established policies.
   - **a.** SIEM
   - **b.** SOAR
   - **c.** RADIUS
   - **d.** MFA
5. What port numbers are typically used with RADIUS?
   - **a.** 20 and 21
   - **b.** 22 and 23
   - **c.** 1812 and 1813
   - **d.** 3388 and 3389