AP®

AP® Networking

COURSE FRAMEWORK

For Use Beginning with the
2026-2027 School Year Pilot

AP® Career Kickstart™
AP courses that build
professional career skills

What AP® Stands For

Thousands of Advanced Placement teachers have contributed to the principles articulated here. These principles are not new; they are, rather, a reminder of how AP already works in classrooms nationwide. The following principles are designed to ensure that teachers' expertise is respected, required course content is understood, and that students are academically challenged and free to make up their own minds.

1. AP stands for clarity and transparency. Teachers and students deserve clear expectations. The Advanced Placement Program makes public its course frameworks and sample assessments. Confusion about what is permitted in the classroom disrupts teachers and students as they navigate demanding work.
2. AP is an unflinching encounter with evidence. AP courses enable students to develop as independent thinkers and to draw their own conclusions. Evidence and the scientific method are the starting place for conversations in AP courses.
3. AP opposes censorship. AP is animated by a deep respect for the intellectual freedom of teachers and students alike. If a school bans required topics from their AP courses, the AP Program removes the AP designation from that course and its inclusion in the AP Course Ledger provided to colleges and universities. For example, the concepts of evolution are at the heart of college biology, and a course that neglects such concepts does not pass muster as AP Biology.
4. AP opposes indoctrination. AP students are expected to analyze different perspectives from their own, and no points on the AP Exam are awarded for agreement with any specific viewpoint. AP students are not required to feel certain ways about themselves or the course content. AP courses instead develop students' abilities to assess the credibility of sources, draw conclusions, and make up their own minds.

   As the AP English Literature course description states: "AP students are not expected or asked to subscribe to any one specific set of cultural or political values, but are expected to have the maturity to analyze perspectives different from their own and to question the meaning, purpose, or effect of such content within the literary work as a whole."
5. AP courses foster an open-minded approach to the histories and cultures of different peoples. The study of different nationalities, cultures, religions, races, and ethnicities is essential within a variety of academic disciplines. AP courses ground such studies in primary sources so that students can evaluate experiences and evidence for themselves.
6. Every AP student who engages with evidence is listened to and respected. Students are encouraged to evaluate arguments but not one another. AP classrooms respect diversity in backgrounds, experiences, and viewpoints. The perspectives and contributions of the full range of AP students are sought and considered. Respectful debate of ideas is cultivated and protected; personal attacks have no place in AP.
7. AP is a choice for parents and students. Parents and students freely choose to enroll in AP courses. Course descriptions are available online for parents and students to inform their choice. Parents do not define which college-level topics are suitable within AP courses; AP course and exam materials are crafted by committees of professors and other expert educators in each field. AP courses and exams are then further validated by the American council on Education and studies that confirm the use of AP scores for college credits by thousands of colleges and universities nationwide.

The AP Program encourages educators to review these principles with parents and students so they know what to expect in an AP course. Advanced Placement is always a choice, and it should be an informed one. AP teachers should be given the confidence and clarity that once parents have enrolled their child in an AP course, they have agreed to a classroom experience that embodies these principles.

Contents

COURSE FRAMEWORK

Acknowledgments

The Advanced Placement Program would like to acknowledge the following committee members, consultants, and reviewers for their assistance with and commitment to the development of this course. All individuals and their affiliations were current at the time of contribution.

Development Committee

Katie Cunningham, *Blackstone Valley Vocational Regional SD, Upton, MA*

Terri Johnson Akse, *University of Colorado–Colorado Springs, Colorado Springs, CO*

Ruston Pennington, *Western Hills High School, Benbrook, TX*

Nathan Pettijohn, *Midlothian ISD, Midlothian, TX*

Michael Qaissaunee, *Brookdale Community College, Lincroft, NJ*

Regina Smith, *Kearns Academy, High Point, NC*

Diego Tibaquirá, *Miami Dade College, Miami, FL*

Stephanie Wascher, *Rock Valley College, Rockford, IL*

Higher Education Advisory Committee

Dane Brown, *United States Naval Academy, Annapolis, MD*

Jun Dai, *Worcester Polytechnic Institute, Worcester, MA*

Melissa Dark, *DARK Enterprises, Inc., Lafayette, IN*

Chance Folmar, *Front Range Community College, Westminster, CO*

Tommy Gober, *Emporia State University, Emporia, KS*

Angel Hueca, *Carnegie Mellon University, Pittsburgh, PA*

Terri Johnson Akse, *University of Colorado–Colorado Spring, Colorado Springs, CO*

Kyle Jones, *Sinclair Community College, Dayton, OH*

Bekah Michael, *University of Cincinnati, Cincinnati, OH*

Michael Qaissaunee, *Brookdale Community College, Lincroft, NJ*

Diego Tibaquirá, *Miami Dade College, Miami, FL*

Anthony Tsetse, *Northern Kentucky University, Highland Heights, KY*

Industry Advisory Committee

Charles Banks, *VP & Manager of Information Security Services, U.S. Bank, Cincinnati, OH*

Charles Gardner, *EnterpriseKC, Leawood, KS*

Carol Kim, *Director of Technology, Data & AI, IBM, Armonk, NY*

Dr. Cynthia Sutherland, *CISSP Chief Information Security Officer (Former) Joint Chiefs of Staff*

High School Advisory Committee

Beth Cerrone, *Innovation Center, St. Vrain Valley School District, Longmont, CO*

Naomi Chamblee, *Shelby County Area Technology Center, Shelbyville, KY*

Jeremiah Milonas, *Red Bank Regional School District, Little Silver, NJ*

Kristi Rice, *Spotsylvania High School, Spotsylvania, VA*

Jennifer Schmerber, *Taft High School, San Antonio, TX*

Expert Consultants

Devin Canaday, *The STEMpreneur, LLC, Chester, VA*

Angel Piñeiro, Jr., *ATCA Services, New York, NY*

Thomas Walcott, *Gambrills, MD*

John R. Williamson, *Eastern Kentucky University, Richmond, KY*

College Board Staff

Moriah Walker, *Director, AP Networking Curriculum & Assessment*

James Turnage, *Director, AP Networking Curriculum & Assessment*

Ben Dougherty, *Senior Director, Manager, AP Cybersecurity Curriculum & Assessment*

Simon Glick, *Director, Content Development & Editorial, Career Kickstart*

Alesha Fox, *Executive Director, AP Instructional Services*

Ellen Gluck, *Senior Director, Career Kickstart Product Readiness*

Chad Hoge, *Senior Director, Course Product Manager*

Daniel McDonough, *Senior Director, AP Content & Assessment Publications*

Shawn Harris, *Director, AP Career Kickstart Professional Learning*

Jason VanBilliard, *Executive Director, Assessment Innovation & Department Head, AP Math, Computer Science, and Cyber Curriculum & Assessment*

Allison Thurber, *Vice President, AP Curriculum & Assessment*

Andy Tucker, *Senior Director, AP Access*

Abby Whitbeck, *Vice President, AP Program Strategy & Career Kickstart*

SPECIAL THANKS *Jocelyn Nguyen-Reed*

THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

About the AP Networking Course

AP Networking trains students in the field and aligns closely with standard first-year collegiate networking courses. Students develop problem-solving and communication skills by configuring, securing, and troubleshooting networks of increasing scale. Through hands-on activities and real-world scenarios, students are encouraged to understand, design, and manage networks that enable functionalities such as streaming and communication, workplace collaboration, and resilient public infrastructure. Developed in partnership with college faculty and industry leaders, this yearlong course aligns with the NICE Workforce Framework.

AP Career Kickstart, a Group of AP Courses

The “Career Kickstart” designation is awarded to AP courses developed not just with colleges to qualify high school students for college credit, but also with industry leaders and employers, to equip students with the skills needed for specific careers.

College Course Equivalent

The AP Networking course is designed to be the equivalent of a one-semester college introduction to networking course.

Prerequisites

There are no specific course prerequisites for AP Networking. Students should be motivated and willing to work both individually and in teams on college-level projects. AP Networking is designed to serve as a foundational course that aligns with multiple Programs of Study within Career and Technical Education (CTE) Digital Technology Pathways.

Unit Scenarios

Unit Scenarios for each unit in the AP Networking framework offer authentic networking situations and are designed to connect the knowledge and skills students gain in each unit to relevant, real-world applications. Each scenario is paired with relevant student activities. The scenarios were developed in partnership with teachers from the AP community to share ways that they approach teaching some of the topics in each unit. These scenarios are offered to support hands-on, career-connected instruction. Teachers may use their own scenarios in addition to, or in lieu of, those provided here.

Legal and Professional Norms for the Practice of Networking and Cybersecurity

By their nature, networking and cybersecurity relate to the storage, processing, and transmission of sensitive data (e.g. proprietary corporate data, financial data, health care data, educational data). To fulfill their responsibilities, networking professionals frequently have elevated permissions on devices and access to sensitive data. For this reason, there are norms for the practice of networking and cybersecurity that guide professionals in using their permission, access, and tools to secure and protect systems, data, organizations, and individuals.

Instructors should share and review with students examples of norms from professional networking and cybersecurity organizations (e.g. ISC2) and governmental organizations (e.g. The UK Cyber Security Council) so students understand why these norms exist as well as the importance of following them.

In addition to professional norms, many types of data and sectors of industry are regulated by laws. Specific legal requirements vary by country, but the United States, United Kingdom, and European Union have laws relating to collecting, storing, processing, and transmitting data:

- Personally Identifiable Information (PII) (including biometric data like voice recordings, fingerprints, and face scans)
- Protected Health Information (PHI)
- Student Education Records
- Financial Records and Transactions

The security of some types of data is mandated by industry regulation. For example, the security of credit card payment data is regulated by the Payment Card Industry Data Security Standard (PCI DSS).

Instructors are expected to introduce students to these laws, industry-specific regulations, and professional norms throughout the duration of the course, integrating them into appropriate topics.

AP NETWORKING

Course Framework

Course Framework Components

Course Units

Unit 1: Managing My Connections

Unit 2: Managing My Shared Connections

Unit 3: Managing Many Connections

Unit 4: Managing Our Global Connections

Course Framework Overview

This course framework provides a clear and detailed description of the course requirements necessary for student success. The framework specifies what students must know, be able to do, and understand to qualify for college credit and/or placement.

The course framework includes two essential components:

(1) COURSE SKILLS (P. 5)

Networking Skills, including Collaboration Skills, are critical to the deep understanding and application of networking knowledge and practice. Students should develop and use these skills throughout the course.

(2) COURSE CONTENT (P. 7)

The course content is organized into units that reflect key domains of networking knowledge and practice.

Course Skills

NETWORKING SKILLS

Skill Category 1	Skill Category 2	Skill Category 3	Skill Category 4
Connect and Configure Enable data transmission through computer networks.	**Secure** Apply protective, detective, and deterrent security controls.	**Troubleshoot** Diagnose causes of degraded performance or functionality, and test potential solutions to resolve problems.	**Collaborate** Work with others and AI to accomplish a task.
1.A Identify common device and network components, protocols, and configurations, and explain processes and relationships in computer networking	**2.A** Identify vulnerabilities and their impacts in data, devices, and networks, and explain how security controls, with and without AI integration, can mitigate vulnerabilities and monitor networks.	**3.A** Identify common device and network problems, and explain how tools, including AI, can be used to diagnose the causes of the problems.	**4.A** Develop clear, shared team objectives related to a networking task.
1.B Determine, with and without the support of AI, the appropriate configurations and settings for network devices to enable connectivity, management, and performance.	**2.B** Determine, with and without the support of AI, mitigation strategies to address device and network vulnerabilities.	**3.B** Determine, with and without the support of AI, the causes of common device and network problems and determine potential solutions to solve those problems.	**4.B** Determine clear roles and responsibilities for members of a team working to accomplish a networking task.
1.C Implement and document device and network configurations to establish and maintain connectivity.	**2.C** Implement and document security controls to address potential vulnerabilities and monitor networks.	**3.C** Implement and document a potential solution to solve a problem.	**4.C** Implement AI as a collaboration tool individually and as a group.
1.D Verify connectivity and configurations of devices and networks, and apply the troubleshooting skills to resolve any problems.	**2.D** Verify that security controls mitigate the intended vulnerability while maintaining access and availability, and apply troubleshooting skills to resolve any problems.	**3.D** Verify the success of a solution and continue applying troubleshooting skills if needed.	**4.D** Complete assigned work to accomplish a collaborative networking task.

THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

Course Content

This course framework provides a clear and detailed description of course requirements necessary for student success. The framework specifies what students should know and be able to do, with a focus on connecting, configuring, securing, and troubleshooting devices and systems across a variety of network types and sizes. The framework emphasizes the importance of critical thinking and problem-solving in the field.

Units

There are four units in AP Networking. Pacing recommendations at the unit level and on the Course at a Glance table provide suggestions for how to teach the required course content. The suggested class periods are based on a schedule in which the class meets five days a week for 45 minutes each day. While these recommendations have been made to aid in planning, adjust the pacing based on the student needs, alternate schedules (e.g., block scheduling), or individual schools' academic calendars.

Topics

Each unit is divided into teachable segments called topics. The topic pages (starting on p. 15) contain all required content for each topic. Topics in Unit 1-4 typically require [X-Y] class periods of instruction. Teachers are not obligated to teach the topics in the suggested sequence listed in each unit. However, to receive authorization to label this course "Advanced Placement," all topics must be included in the course.

Course at a Glance

Plan

The Course at a Glance provides a useful visual organization of the AP Networking components, including:

- Sequence of units.
- Progression of topics within each unit.

Teach

COURSE SKILLS

1	Connect and Configure
2	Secure
3	Troubleshoot
4	Collaborate

Assess

At the end of each topic and unit, assess students' understanding of the content and skills and provide them with actionable feedback.

UNIT 1

Managing My Connections

Skill		Topic
3	1.1	Fixing What's Slowing Me Down: Troubleshooting Issues on My Device
1	1.2	Getting the Most Out of My Network: Connecting and Optimizing My Device
2	1.3	What Could Go Wrong: Identifying the Security Needs of My Device
2	1.4	Locking It Down: Securing My Device

UNIT 2

Managing My Shared Connections

Skill		Topic
3	2.1	Missed Connection: Troubleshooting My SOHO Network
1	2.2	Identification Needed: Documenting My Network
1	2.3	Smart Moves: Upgrading My Network
1	2.4	Leveling Up: Advanced Features on My Network
2	2.5	Guarding My Network: Identifying Security Needs
2	2.6	Applying Defense: Securing My Network

UNIT 3

Managing Many Connections

Skill		Topic
1	3.1	Planning a Network: Choosing the Right Devices and Connections
1	3.2	Creating a Network: Switching and Topologies
1	3.3	Making It Work: Connecting, Configuring, and Verifying Access
2	3.4	Building the Boundaries: Identifying Segmentation Security
2	3.5	Controlling the Traffic: Firewalls and Filtering
3	3.6	Restored Connections: Documenting, Diagnosing, and Fixing a Segmented LAN

UNIT 4

Managing Our Global Connections

Skill		Topic
2 3	4.1	What Happens When Networks Break or Fail?
1 3	4.2	The Language of the Network: Protocols and the OSI and TCP/IP Models
1	4.3	Tools of Network Analysts: Using the CLI
1	4.4	How Data Travel the Internet: Routing, Metrics, and Paths
2	4.5	From the Inside Out: Monitoring and Defending a Large Network
1 3	4.6	Moving Forward: Designing for Reliability and Growth

THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

AP NETWORKING

UNIT 1

Managing My Connections

UNIT 1

Managing My Connections

UNIT SCENARIO

Scenarios at the start of each unit in the AP Networking framework offer authentic situations that are designed to connect the knowledge and skills students gain in the first topic to relevant, real-world applications. Each scenario is paired with relevant student activities. Teachers may use their own scenarios in addition to, or in lieu of, those provided here.

SCENARIO 1A:
The Case of the Sluggish Device

This weekend you are planning to finish a project and stream your favorite show. However, when you open your device to get started, it is not operating smoothly. The applications are slow and videos are buffering, and you need your device functionality restored quickly. You need to use a structured troubleshooting process to find the root cause, determine the best solution, and restore your device's functionality.

You will create a device recovery walkthrough that documents your investigation and troubleshooting process. Your goal is to walk an audience through your process step-by-step so they can follow it themselves. The walkthrough might be a narrated screen recording, a demonstration video, or an annotated presentation that explains the process taken to restore device functionality.

Walkthrough Suggestions:

- Initial observations and any early troubleshooting steps
- Diagnostic data such as error messages, CPU, RAM, storage, or Wi-Fi strength
- Potential solutions
- Steps taken to implement the chosen solution
- Verification of restored functionality
- Suggestions for avoiding or troubleshooting a similar issue in the future

TOPIC 1.1

Fixing What's Slowing Me Down: Troubleshooting Issues on My Device

SUGGESTED SKILLS

3.A
Identify common device and network problems, and explain how tools, including AI, can be used to diagnose the causes of the problems.

3.B
Determine, with and without the support of AI, the causes of common device and network problems and determine potential solutions to solve those problems.

Required Course Content

LEARNING OBJECTIVE

1.1.A
Explain how to troubleshoot common device and network issues.

ESSENTIAL KNOWLEDGE

1.1.A.1
Users often encounter devices and networks with performance or connectivity issues. Solutions to these issues may not be immediately evident because computers and networks involve many interconnected hardware and software layers.

1.1.A.2
The first step in the troubleshooting process is gathering information to identify an issue. This can include user reports about unexpected behavior, loss of functionality, and the circumstances under which an issue occurs. Many connectivity and performance issues can often be resolved with simple, well-known fixes, such as restarting or checking physical connections, that should be applied before launching the troubleshooting process to save time, effort, and resources.

1.1.A.3
Diagnostic tools and techniques can be used to establish a theory of probable cause for the loss of functionality in devices and networks. This can save time while troubleshooting by narrowing the potential solutions. Many devices have embedded troubleshooting tools that can check settings to identify issues.

1.1.A.4
When determining potential solutions, simple and nondisruptive options should be tested first. Solutions can be ranked by time, difficulty, and expense to implement, with priority given to simple and cost-effective solutions like closing applications and restarting devices, before moving to more complex solutions like replacing hardware and upgrading software.

1.1.A

Explain how to troubleshoot common device and network issues.

1.1.A.5

After selecting an appropriate solution, it should be implemented and then verified to confirm that the issue is resolved. Verification includes checking that the device or system is functioning normally.

1.1.A.6

If functionality is not restored after the implementation of a solution, there could be more than one issue causing a loss of functionality, or the root cause might have been misidentified. The troubleshooting process should continue by implementing other potential solutions, documenting the steps taken, and verifying results.

1.1.A.7

AI tools can assist in the troubleshooting process and enhance troubleshooting efficiency but should be used alongside traditional diagnostic methods and human judgment. Solutions suggested by an AI tool should be manually verified to ensure functionality has been restored. AI tools can be used to:

- suggest potential causes based on error messages and patterns in user-reported issues
- identify appropriate solutions by analyzing diagnostic data, error messages, and system behavior
- assist in implementing solutions for common issues by providing suggestions and verification methods based on diagnostic data

1.1.B

Identify likely root causes of a device issue using diagnostic tools and techniques.

1.1.B.1

Common issues on endpoint devices include slow or no network connectivity, delays in opening files, and applications that are slow to respond or that freeze or crash. These can often be resolved by implementing common solutions. If functionality is not restored, the troubleshooting process should continue with gathering diagnostic information. Common solutions for device issues include:

- restarting the device
- closing unnecessary applications or programs
- disconnecting and reconnecting to the network

1.1.B

Identify likely root causes of a device issue using diagnostic tools and techniques.

1.1.B.2

High processor (central processing unit, or CPU) or memory (random access memory, or RAM) usage can cause applications to become slow or unresponsive. Task manager applications can be used to check resource usage.

- Sustained CPU usage above 80–90% indicates the processor is overloaded and may cause slow or unresponsive performance.
- Sustained RAM usage above 80–90% indicates the system is using a significant amount of available short-term memory, which is needed to keep applications running smoothly.

1.1.B.3

Insufficient available storage space can lead to slow file access and degraded application performance. System storage levels below 10% indicate that the device may not have enough space to perform reliably, which can lead to slower performance and limited functionality.

1.1.B.4

A weak wireless signal or disconnection from the access point can cause applications to fail to load content or sync data. This can be identified by checking the network icon in the notification bar, which displays signal strength and network connection status.

1.1.B.5

Overheating can cause a device to slow down, shut down unexpectedly, or lose connectivity as a protective measure. Devices may overheat when ventilation is poor, the processor is overloaded for an extended period, or the device is used in a hot or sunny environment. Many devices display temperature warnings or automatically reduce performance to cool down.

1.1.C

Determine an appropriate solution to resolve a device issue.

1.1.C.1

Solutions for high CPU usage include ending high-usage or unresponsive tasks or processes.

1.1.C.2

Solutions for high RAM usage include:

- deleting temporary files
- installing more RAM if the problem is persistent

1.1.C.3

Solutions for low available storage include:

- deleting temporary and unused files and applications
- moving files to external or cloud storage
- installing additional storage if the problem is persistent

1.1.C.4

Solutions for limited or lost network connectivity include:

- verifying the network name and password
- moving closer to the wireless access point

1.1.C.5

Solutions for overheating include:

- checking for appropriate ventilation
- ending high-usage tasks or processes
- moving a device to a cooler area or out of direct sunlight

1.1.C.6

After implementing a solution, users should verify that functionality has been restored by confirming that applications respond normally or that the internet and network resources are accessible.

SUGGESTED SKILLS

1.A
Identify common device and network components, protocols, and configurations, and explain processes and relationships in computer networking.

1.B
Determine, with and without the support of AI, the appropriate configurations and settings for network devices to enable connectivity, management, and performance.

TOPIC 1.2

Getting the Most Out of My Network: Connecting and Optimizing My Device

Required Course Content

LEARNING OBJECTIVE

1.2.A
Configure a device for secure wireless connectivity to a network.

ESSENTIAL KNOWLEDGE

1.2.A.1
Before connecting to a wireless network, a device must have wireless capability enabled. This includes turning on Wi-Fi or ensuring the wireless adapter is active.

1.2.A.2
To connect to a wireless network, the user must know the network name—also called the service-set identifier (SSID)—and password if required. Available wireless networks can be viewed by opening the network settings for a device, often accessible through the notification area or settings menu. Users should connect only to trusted networks and avoid unknown or unprotected networks, which may allow unauthorized access to data or devices.

1.2.A.3
A connection to a wireless network can be initiated by selecting the desired SSID from the list of available networks. If the network is protected, the device will prompt the user to enter the password. Wireless network passwords are case-sensitive.

1.2.A.4
After connecting to a wireless network, users should verify the connection by checking the network icon for any errors and confirming that they are able to access the internet and network resources.

1.2.B

Determine strategies to improve speed, reliability, or performance based on task requirements such as working, streaming, and gaming.

1.2.B.1

Different tasks require different levels of device performance and network speed. Users can take steps to improve their device performance.

1.2.B.2

Network bandwidth is the amount of data that can move through a network at a specific time. Bandwidth is important for the speed of a network connection. Users can improve available bandwidth by:

- disconnecting other devices from the network
- pausing large updates or downloads

1.2.B.3

Network connection strength is important for reliability. Low signal strength can cause lag. Users can improve device connection strength by:

- moving a device closer to the router or wireless access point
- reducing signal interference from solid objects such as walls
- switching to a wired Ethernet connection when available

1.2.B.4

Device processing and available storage are important for device performance during high-usage tasks. Users can improve device performance by:

- closing unused applications and browser tabs
- deleting unused or temporary files and applications

SUGGESTED SKILLS

2.A
Identify vulnerabilities and their impacts in data, devices, and networks, and explain how security controls, with and without AI integration, can mitigate vulnerabilities and monitor networks.

2.B
Determine, with and without the support of AI, mitigation strategies to address device and network vulnerabilities.

TOPIC 1.3
What Could Go Wrong: Identifying the Security Needs of My Device

Required Course Content

LEARNING OBJECTIVE

1.3.A
Identify the impacts of digital and physical attacks on individual devices.

ESSENTIAL KNOWLEDGE

1.3.A.1
Digital and physical attacks are designed to gain unauthorized access to accounts, data, or devices. Unauthorized access can result in exposure of sensitive or personal information, including financial records, health data, and personally identifiable information (PII). Exposed data may be leaked or sold.

1.3.A.2
Information gathered from compromised accounts or exposed credentials can be used to commit fraud, make purchases, or apply for loans. Victims may experience credit score damage, financial debt, or long-term identity misuse.

1.3.A.3
Unauthorized access to devices and data used by a small business or organization can damage its reputation and disrupt operations. Leaked client information, unprofessional communication, or service interruptions can lead to erosion of trust, negative publicity, and loss of customers.

1.3.A.4
Malware can cause devices to behave abnormally, slow down, crash, or become unusable. Malware can allow attackers to access files, monitor activity, or take remote control of a device. Infected devices may also be used to spread malware to other systems.

1.3.B Determine appropriate security controls to limit the impacts of common device attacks.	**1.3.B.1** Security controls are implemented to mitigate vulnerabilities. Selecting an appropriate security control requires understanding specific device vulnerabilities and their potential impacts.

1.3.B.2

Security controls to mitigate weak authentication include:

- implementing strong passwords that are harder to guess
- enabling multifactor authentication (MFA) to add additional layers of security beyond passwords
- using biometric verification methods, such as fingerprint scans and facial recognition, that authenticate users based on unique physical characteristics

1.3.B.3

Phishing refers to an adversary sending deceptive communications, like spoofed emails, fake websites, or urgent messages, to mislead users into revealing credentials or downloading malware. Security controls to limit the impact of phishing can include enabling email filtering to block malicious messages and training users to detect and report phishing messages.

1.3.B.4

Shoulder surfing refers to an unauthorized individual observing or recording a user's screen or keyboard to gather information. Security controls to limit the impact of shoulder surfing can include:

- installing privacy screens that limit viewing angles, making displays visible only to users directly in front of them
- positioning screens away from high-traffic areas to reduce visibility to others

1.3.B.5

Security controls to limit the impact of malware can include:

- installing and regularly updating antivirus and antimalware software
- keeping operating systems and applications updated to patch known vulnerabilities

SUGGESTED SKILLS

2.C

Implement and document security controls to address potential vulnerabilities and monitor networks.

2.D

Verify that security controls mitigate the intended vulnerability while maintaining access and availability, and apply troubleshooting skills to resolve any problems

TOPIC 1.4

Locking It Down: Securing My Device

Required Course Content

LEARNING OBJECTIVE

1.4.A

Implement strong passwords to help prevent unauthorized access.

ESSENTIAL KNOWLEDGE

1.4.A.1

Implementing complexity in passwords includes using at least one character from each character set. Passwords with characters from each character set are significantly harder for an adversary to guess or compromise than passwords that use characters from only one or two character sets. The character sets often required are:

- uppercase letters (A–Z)
- lowercase letters (a–z)
- numeric digits (0–9)
- special characters (!"#$%&'()*+,-./:;<=>?@ [\ ] ^_ ` {|}~)

1.4.A.2

Implementing a minimum password length means that users must have at least a certain number of characters in their password. The longer and more complex a password is, the longer it will take an automated tool to find the password.

1.4.A.3

Implementing a lockout period after a certain number of invalid login attempts prevents an adversary from continuously guessing passwords. Many organizations lock a user's account after 3–5 invalid login attempts. The lockout duration varies.

1.4.A.4

Strong passwords should not include common or easily guessed words or personal information like birthdates, pet names, or usernames.

1.4.A

Implement strong passwords to help prevent unauthorized access.

1.4.A.5

Implementing a passphrase involves using a sequence of words or a sentence that is easy for the user to remember but difficult for an adversary to guess. Passphrases are typically longer than passwords, increasing the total number of possible combinations and making them more resistant to automated attacks.

1.4.B

Implement device- and account-level security practices to prevent phishing, credential compromise, and data loss.

1.4.B.1

To prevent phishing-based account compromise, users should verify message sources and use caution before interacting with emails or messages, especially those requesting sensitive information. Users should:

- verify the sender’s email address
- hover over links to inspect their destination before clicking
- contact organizations directly through official websites or phone numbers

1.4.B.2

To reduce the risk of credential or data exposure over untrusted networks, users should use secure connections when accessing sensitive data. Users should:

- connect through secure networks, such as a virtual private network (VPN)
- avoid using unknown public networks
- ensure websites use the HTTPS protocol, which encrypts traffic

1.4.B.3

To prevent exploitation of known vulnerabilities that can lead to device compromise or data loss, users should keep all software and firmware current. Software refers to applications and operating systems, while firmware is embedded software that controls hardware components. Users should enable automatic updates to maintain the latest patches.

1.4.B.4

To prevent unauthorized account access through credential reuse or guessing, users should use strong, unique passwords for each account to prevent access if any single set of credentials is compromised.

1.4.B

Implement device- and account-level security practices to prevent phishing, credential compromise, and data loss.

1.4.B.5

To prevent unauthorized access through known default credentials on devices, users should update login information during initial setup. Users should:

- change default usernames and passwords on devices like routers and cameras
- recognize that Internet of Things (IoT) devices, such as smart speakers and thermostats, often have insecure default settings that should be changed

1.4.B.6

To protect devices and accounts from unauthorized access, users should configure strong security settings. Users should:

- enable MFA
- enable screen lock with a strong PIN, password, or biometric authentication
- disable automatic connection to open or public wireless networks
- disable application permissions when not in use to limit data exposure

1.4.C

Configure wireless network security features.

1.4.C.1

Wireless networks are convenient but vulnerable to security attacks involving unauthorized access and data interception.

1.4.C.2

Encrypting data before transmission makes it more difficult for an adversary to read captured data. Wireless networks should be configured to use the highest level of encryption available in the router or wireless access point settings. WPA3 is recommended; WPA2 is the minimum requirement. WEP and WPA are insecure and should not be used. Wi-Fi Protected Setup (WPS) should be disabled.

1.4.C.3

Creating a unique service set identifier (SSID) and strong authentication measures for a wireless network prevents unauthorized users from accessing the network by compromising passwords.

1.4.C.4

Password-protected networks should be configured with long, complex, and unique passwords.

AP NETWORKING

UNIT 2

Managing My Shared Connections

Managing My Shared Connections

UNIT SCENARIO

Scenarios at the start of each unit in the AP Networking framework offer authentic situations that are designed to connect the knowledge and skills students gain in the first topic to relevant, real-world applications. Each scenario is paired with relevant student activities. Teachers may use their own scenarios in addition to, or in lieu of, those provided here.

SCENARIO 2A:
Computer Lab Disconnected

You are a member of the school technology support team and multiple issues with the network arise during the computer science class, from a computer screen going black to several computers losing connectivity. As a member of the school technology support team, you have been asked to investigate some of the problems to restore connectivity. You will use your skills to troubleshoot and restore functionality as quickly as possible.

You will deliver an incident report on the root cause of the issues and the steps taken to address each issue.

Network Troubleshooting Incident Report Suggestion:

- User descriptions of functionality losses and affected devices
- Diagnostic data gathered with explanations such as indicator lights, ping results, and IP configurations
- Probable causes and potential solutions
- Verification of restored functionality
- Recommendations to avoid similar issues in the future

SUGGESTED SKILLS

3.A

Identify common device and network problems, and explain how tools, including AI, can be used to diagnose the causes of the problems.

3.B

Determine, with and without the support of AI, the causes of common device and network problems and determine potential solutions to solve those problems.

TOPIC 2.1

Missed Connection: Troubleshooting My SOHO Network

Required Course Content

LEARNING OBJECTIVE

2.1.A

Identify likely root causes of a SOHO network issue using diagnostic tools and techniques.

ESSENTIAL KNOWLEDGE

2.1.A.1

Slow or no network connectivity is a common issue in a small office/home office (SOHO) network. Networks contain multiple devices and physical connections, any of which can be the source of connectivity issues. Many issues can be resolved by implementing common solutions. If functionality is not restored, troubleshooting should continue by gathering diagnostic information. Common solutions for SOHO network connectivity include:

- restarting the network router or wireless access point
- reseating, or removing and reinserting, a loose or unplugged cable
- replacing damaged cables or connectors

2.1.A.2

A hardware failure or disconnection can prevent a device from accessing a network. This can be identified by observing the indicator lights on the router or access point. The device manual or label should be referenced to interpret the indicator lights.

- Steady or flashing green lights typically indicate normal operation.
- Red or orange lights may indicate a hardware issue or connection failure.
- Unlit indicator lights may indicate a faulty port or cable, or an unplugged cable.

2.1.A

Identify likely root causes of a SOHO network issue using diagnostic tools and techniques.

2.1.A.3

Network congestion or hardware failures can cause slow or failed connectivity to applications, websites, and services. This can be identified using the command-line interface (CLI) tool `ping` to check network connectivity and response times. The command `ping 8.8.8.8` can be used to test external connectivity by sending a connection request to one of Google's public servers.

- High response times over 100ms or lost packets may indicate network congestion or hardware issues.
- No response or 100% packet loss may indicate a local disconnection or failure.

2.1.A.4

Incorrect IP configuration can prevent a device from communicating on a network. This can be identified using the CLI command `ipconfig` (Windows) or `ifconfig` (Linux) to check a device's configuration and troubleshoot local network issues.

- IP addresses in the 169.254.0.0–169.254.255.255 range are Automatic Private IP Addressing (APIPA) addresses, indicating there was a problem assigning the device address.
- A loopback address of 127.0.0.1 indicates the device may not be connected to any network and can only send data to itself.

2.1.B

Determine an appropriate solution to resolve a SOHO network issue.

2.1.B.1

Solutions for a network hardware issue or connection failure indicated by red, orange, or unlit lights on a router or switch include:

- using a different Ethernet cable
- plugging the cable into a different port

2.1.B.2

Solutions for poor network performance or congestion indicated by ping results that show response times over 100ms, or more than 1–2% packet loss include:

- changing a wireless connection to a wired connection
- pausing large downloads
- moving a device closer to a wireless access point

2.1.B

Determine an appropriate solution to resolve a SOHO network issue.

2.1.B.3

Solutions for a device that is not connected to a network and displays an APIPA address include:

- disconnecting and reconnecting to the network
- releasing and renewing the IP address with the commands `ipconfig /release` and `ipconfig /renew`

2.1.B.4

Solutions for a device that is not connected to a network and displays only a loopback address include:

- ensuring the device Wi-Fi and network adapter are enabled
- restarting the device

2.1.B.5

To verify that network connectivity has been restored, users should confirm that the devices can successfully access the internet or network resources like shared drives, printers, or servers and that websites and network services load without delay. If network access or response times have not improved, users should gather new diagnostic information and implement additional solutions.

TOPIC 2.2

Identification Needed: Documenting My Network

Required Course Content

LEARNING OBJECTIVE

2.2.A
Explain how MAC addresses are structured and used to identify devices.

ESSENTIAL KNOWLEDGE

2.2.A.1
A network node is any device connected to a network, while a host is a type of node that sends or receives data on the network, such as a computer or printer. Hosts are often referred to as endpoints. Network devices such as switches, routers, and access points are not considered hosts.

2.2.A.2
A device needs a network interface card (NIC) to connect to a network. Media access control (MAC) addresses, also known as physical or hardware addresses, are assigned directly to a NIC. A MAC address identifies the device with the associated NIC. MAC addresses are hardcoded into a NIC and remain the same even if a device switches to a different network.

2.2.A.3
Each MAC address is a 48-bit identifier. The first half of the address, called the Organizationally Unique Identifier (OUI), identifies the manufacturer, and the second half identifies the specific device. MAC addresses can be represented in three hexadecimal formats:

- 6F72696F6E2A
- 6F:72:69:6F:6E:2A
- 6F-72-69-6F-6E-2A

SUGGESTED SKILLS

1.A
Identify common device and network components, protocols, and configurations, and explain processes and relationships in computer networking.

1.C
Implement and document device and network configurations to establish and maintain connectivity.

2.2.A

Explain how MAC addresses are structured and used to identify devices.

2.2.A.4

Hexadecimal refers to base-16 numbers and uses the characters 0–9 and A–F. Hexadecimal is more compact than binary, allowing humans to more easily read, write, and understand large binary numbers.

ILLUSTRATIVE EXAMPLE

To convert a number from decimal to hexadecimal, divide the number by 16 and find the quotient. Use the remainder for the hex digit and divide the quotient by 16 again. Repeat the steps until the quotient is equal to 0. For example, the decimal number 79 is represented in hexadecimal as 4F:

1. 79/16 = 4, remainder 15
2. 15 → F
3. 4/16 = 0, remainder 4
4. 4 → 4
5. 79 = 4F

2.2.A.5

MAC addresses of the devices physically connected to a network switch are stored in the content addressable memory (CAM) table of the switch. The CAM table allows the switch to direct data to the correct device instead of broadcasting to all ports.

ILLUSTRATIVE EXAMPLE

A network switch shows the following entries in the CAM table:

- `Device A: 6D:6F:72:69:61:68 --> port 1`
- `Device B: 4F:72:69:6F:6E:2A --> port 2`
- `Device C: 70:6F:6C:61:72:24 --> port 3`

When device A sends data to device B, the switch uses the CAM table to forward the data only to port 2, instead of broadcasting the data to all ports.

2.2.B

Explain how IP addresses are structured and used to identify devices.

2.2.B.1

An Internet Protocol (IP) address is a logical address assigned to a device on a specific network. When a device switches networks, its IP address typically changes.

2.2.B

Explain how IP addresses are structured and used to identify devices.

2.2.B.2

An IPv4 address is a 32-bit number divided into four 8-bit sections called octets. IPv4 addresses are typically written in dotted decimal format, where each octet is expressed as a decimal number from 0 to 255, and octets are separated by a period. IPv4 addresses consist of a network ID, shared by all devices on a local network, and a host ID, which uniquely identifies each device.

ILLUSTRATIVE EXAMPLE

The dotted decimal notation of an IPv4 address condenses its 32-bit binary representation into a more readable format. Each group of 8 bits, or octet, is converted to a decimal value between 0 and 255. The binary IPv4 address 10001110.11111010.10111111.01001110 is written in dotted decimal notation as 142.250.191.78.

2.2.B.3

The network ID of an IPv4 address may be 1–3 octets depending on the class of the network. The size of the host ID indicates the number of unique host addresses available on a network.

2.2.B.4

Classful addressing divides the IPv4 address space into five classes.

- Class A allows around 17 million possible hosts.
- Class B allows around 65,000 hosts.
- Class C allows around 254 hosts.
- Class D and Class E are reserved for other purposes.

2.2.B.5

IPv4 addresses must be paired with subnet masks, which are commonly represented in dotted decimal format. The subnet mask is used to determine the network bits and the host bits. Common subnet masks include:

- 255.0.0.0 Class A to indicate the first octet is the network ID
- 255.255.0.0 Class B to indicate the first two octets are the network ID
- 255.255.255.0 Class C to indicate the first three octets are the network ID

ILLUSTRATIVE EXAMPLES

- With a subnet mask of 255.255.0.0, the first two octets of an IP address are network bits and the second two are host bits.
- With a subnet mask of 255.255.255.0, the first three octets are network bits and the fourth octet is the space available for host addresses.

2.2.B
Explain how IP addresses are structured and used to identify devices.

2.2.B.6
The Address Resolution Protocol (ARP) maps a device's IP address to its MAC address, ensuring that data are delivered to the correct destination. When a device needs to send data to another device on the same local network, an ARP request containing the known destination IP address is sent to all devices on the network. The device with the corresponding IP address sends an ARP reply that contains its MAC address.

2.2.C
Identify different types of IPv4 addresses.

2.2.C.1
Public addresses are addresses that can be assigned to organizations to be used externally. A public IP address is unique and assigned by the ISP to identify devices that are directly reachable from the internet. This address is used to communicate on the internet and to other networks.

2.2.C.2
Private addresses are used within a local area network (LAN) only; routers drop any data addressed to private IP addresses. Private addresses add a layer of security, as privately addressed devices cannot be directly accessed from an external source. Private IP addresses fall into these ranges:

- Class A: 10.0.0.0–10.255.255.255
- Class B: 172.16.0.0–172.31.255.255
- Class C: 192.168.0.0–192.168.255.255

2.2.C.3
APIPA can be used to automatically address hosts if the Dynamic Host Configuration Protocol (DHCP) server, which automates IP assignment and configuration, is unavailable or misconfigured. When APIPA is used, hosts will have an IP address in the range 169.254.0.0–169.254.255.255.

2.2.C.4
Loopback addresses are used by a device to send data for testing purposes. The most common loopback address is 127.0.0.1, which refers to the local machine.

2.2.D

Document an existing network including devices, addresses, and connections.

2.2.D.1

Network diagrams can be created to plan a network configuration and document a network after setup is complete. Network maps and diagrams create visual representations of the equipment that exists in a network, including routers, switches, access points, servers, and endpoints, with solid lines for wired connections and dashed lines for wireless connections. Device MAC and IP addresses should be included in the diagram to assist in troubleshooting and expansion.

2.2.D.2

A SOHO network serves a small number of users on a single LAN, typically in a home or small business. SOHO networks commonly include routers, switches, access points, endpoints, firewalls, and cabling.

2.2.D.3

A router directs data between the local network and other networks. It is often combined with a modem in a single device to provide access to the internet through an internet service provider (ISP).

2.2.D.4

A switch connects wired devices and manages network traffic within a LAN.

2.2.D.5

A wireless access point (WAP) enables wireless connectivity by connecting to a router or switch. Many SOHO networks use a wireless gateway, which is a single device that combines the functionality of a modem, router, switch, and WAP.

2.2.D.6

Endpoints are devices that connect to a network to send and receive data, such as laptops, PCs, printers, network attached storage (NAS), servers, 3D printers, voice over IP (VoIP) phones, IoT devices, and mobile phones.

2.2.D.7

Common cable types used in a SOHO network include twisted pair (Ethernet), coaxial, and fiber optic, with twisted pair being the most common for internal wired connections. Coaxial and fiber optic cables are often used by ISPs to externally connect to the SOHO router.

SUGGESTED SKILLS

1.A

Identify common device and network components, protocols, and configurations, and explain processes and relationships in computer networking.

1.B

Determine, with and without the support of AI, the appropriate configurations and settings for network devices to enable connectivity, management, and performance.

TOPIC 2.3 Smart Moves: Upgrading My Network

Required Course Content

LEARNING OBJECTIVE

2.3.A

Determine appropriate endpoint devices to meet user needs in a SOHO network.

ESSENTIAL KNOWLEDGE

2.3.A.1

Computers, including desktops, laptops, and servers, are ideal for tasks that require high interactivity, multitasking, or processing power, such as content creation, software development, and data analysis.

2.3.A.2

Internet of Things (IoT) devices are common items, such as thermostats, appliances, smart TVs, security systems, and wearable technology like fitness trackers and medical monitors, that are capable of connecting to other devices and the internet. These devices are ideal for automating tasks, monitoring environments, streaming media, or enabling remote control in SOHO networks.

2.3.A.3

Mobile devices, including smartphones, handheld gaming devices, and tablets, are small and lightweight network endpoints that connect wirelessly to networks. These are ideal for flexible, on-the-go communication, quick data entry, and mobile access to applications.

2.3.A.4

Organizations and small businesses use specialized endpoint devices for specific needs. Specialized endpoint devices include:

- printers and scanners for handling documents
- voice over IP (VoIP) phones that enable voice calls over an internet connection
- point-of-sale (POS) terminals for transaction processing and inventory management

2.3.B

Determine appropriate data transmission media to meet specified user needs.

2.3.B.1

When determining the most appropriate transmission medium for a LAN, users should consider factors such as device location, performance needs, susceptibility to interference, ease of installation, and cost. The best option balances performance, reliability, and budget based on user needs.

2.3.B.2

Twisted pair cabling can come in shielded (STP) or unshielded (UTP), with shielded offering more protection against interference. Twisted pair is suitable for devices that need a faster and more stable connection than wireless, such as desktop computers, printers, or NAS devices. Considerations for using twisted pair include:

- Cost: affordable
- Ease of installation: easy
- Connection speed: supports high-speed connections of up to 10Gbps, up to 100 meters
- Susceptibility to interference: STP should be used in environments with high EMI, such as near HVAC equipment, fluorescent lighting, or other electronic devices that emit radio signals, while UTP is sufficient for most standard installations

2.3.B.3

Wireless connections, such as Wi-Fi, are ideal for devices that need mobile access like smartphones, tablets, laptops, and IoT devices. Considerations for using wireless connections include:

- Cost: affordable
- Ease of installation: easy, especially in environments where installing cables would be difficult
- Connection speed: varies with signal strength but can support 500Mbps–1Gbps
- Susceptibility to interference: more susceptible than wired connections to interference and signal degradation due to walls, other devices, or network congestion

2.3.B

Determine appropriate data transmission media to meet specified user needs.

2.3.B.4

Coaxial cable may be used when upgrading or maintaining existing networks that already use coaxial connectors. Coaxial cable is less common in modern LANs but may be used in older buildings for cable-based internet connections. Considerations for using coaxial include:

- Cost: moderate, typically more expensive than twisted pair but cheaper than fiber optic cabling
- Ease of installation: more rigid and harder to install than twisted pair
- Connection speed: supports high-speed connections of up to 1Gbps, with significant signal loss over 450 meters
- Susceptibility to interference: offers better shielding from interference than twisted pair

2.3.B.5

Fiber optic cable should be used when there is a need for ultra-high bandwidth, complete EMI resistance, or maximum connection stability and speed. Fiber optic cable is not commonly used inside SOHO LANs. Considerations for using fiber include:

- Cost: more expensive than wireless, coaxial, or twisted pair
- Ease of installation: fragile and requires special tools for installation
- Connection speed: supports high-speed connections of up to 1–100Gbps, with transmission distances of up to 100 km
- Susceptibility to interference: immune to EMI because the signal is carried by light instead of electrical pulses

2.3.C

Explain why dynamic or static IP addressing should be used in a given scenario.

2.3.C.1

IP addresses can be configured as dynamic or static to meet the needs of users or organizations. Dynamic IP addresses are assigned automatically and may change when a device reconnects to the network or after a set period. Static IP addresses remain constant.

2.3.C

Explain why dynamic or static IP addressing should be used in a given scenario.

2.3.C.2

Dynamic addressing is preferred for networks that require flexibility and efficient use of IP addressing space. Dynamic Host Configuration Protocol (DHCP) automates IP assignment and configuration, assigning addresses only to devices that are currently connected to the network.

2.3.C.3

Static addressing is appropriate for devices that need a consistent address on a network, such as servers, printers, remote services, or security systems. Dynamic addressing is better suited for mobile or temporary devices like tablets, laptops, or guest devices.

2.3.C.4

Dynamic addressing is easier to manage on networks with limited administrative support; it is common in homes and small offices. Static addressing may be preferred when precise control is needed, but it requires manual setup and careful tracking to prevent IP address conflicts.

SUGGESTED SKILLS

1.B
Determine, with and without the support of AI, the appropriate configurations and settings for network devices to enable connectivity, management, and performance.

1.C
Implement and document device and network configurations to establish and maintain connectivity.

TOPIC 2.4

Leveling Up: Advanced Features on My Network

Required Course Content

LEARNING OBJECTIVE	ESSENTIAL KNOWLEDGE
2.4.A Evaluate an AI-generated network design, configuration, or troubleshooting suggestion.	**2.4.A.1** AI tools can be used to generate suggestions for SOHO network design, configuration, or troubleshooting. Effective prompts should include details such as the number of users, types of devices, internet usage patterns, and budget constraints. Vague prompts may lead to impractical or overly complex recommendations.
	2.4.A.2 Suggestions generated by AI may include unrealistic device recommendations, overcomplicated setups, and incorrect IP addressing schemes. Some suggestions might be technically accurate but inappropriate for a specific network.
	2.4.A.3 When evaluating AI-generated SOHO network suggestions, consider whether the design meets requirements for performance, ease of setup, wireless coverage, and cost-effectiveness. Recommendations should align with the simplicity and manageability expected in a small or home office environment and should be realistic, secure, and user-friendly.
2.4.B Configure a media server for local file storage, gaming, or streaming.	**2.4.B.1** A media server is a device on a network that can be used to stream content to other devices, store shared files, and host multiplayer games. Hosting a local media server provides more control, faster access, and higher privacy than utilizing a cloud-based or subscription media service; it is often more cost effective.

2.4.B

Configure a media server for local file storage, gaming, or streaming.

2.4.B.2

When configuring a media server on a network, a host device such as a computer, gaming console, or NAS must be selected. The host device will store, process, and share data with other devices on the network. The host device needs enough processing power, storage, and memory to handle the requests from devices on the network. This device must be connected to the network; a wired connection is recommended for speed and reliability.

2.4.B.3

To allow other devices in a network to access shared data on a media server, file-sharing software must be installed or enabled. This may include applications for media streaming, game hosting, or file sharing, depending on how the server will be used.

2.4.B.4

To enable the media server to access media, game files, or shared documents, these files must be stored on the host device. Folders should be organized and stored where the server software or file-sharing service is configured to share them with other devices on the network.

2.4.B.5

A static IP address or hostname can be configured for a media server to ensure it can be consistently located on the network by other devices.

2.4.B.6

Verification of successful configuration of a media server involves connecting to the server from another device and confirming access to shared files, media, or games.

SUGGESTED SKILLS

2.A
Identify vulnerabilities and their impacts in data, devices, and networks, and explain how security controls, with and without AI integration, can mitigate vulnerabilities and monitor networks.

2.B
Determine, with and without the support of AI, mitigation strategies to address device and network vulnerabilities.

TOPIC 2.5

Guarding My Network: Identifying Security Needs

Required Course Content

LEARNING OBJECTIVE

2.5.A
Identify impacts of potential security vulnerabilities in a SOHO network.

ESSENTIAL KNOWLEDGE

2.5.A.1
Unauthorized access, exposure or loss of sensitive data, and disruption of services such as internet, file sharing, or printing can occur when a SOHO network lacks proper security controls. Common vulnerabilities such as weak passwords, default configurations, or unmonitored devices increase the risk of these impacts.

2.5.A.2
Unauthorized access to a network can allow an adversary to change network configurations or disable security controls. This can occur when routers and access points use default usernames, passwords, or settings that are widely known or easily guessed.

2.5.A.3
Data loss, device compromise, or malware infection can result when network devices are not updated or secured. These impacts may occur due to outdated firmware or the connection of untrusted devices with known vulnerabilities.

2.5.A.4
Unauthorized access to additional systems or devices can occur when an adversary moves laterally through a network. This often occurs through insecure IoT devices or unknown guest devices with weak credentials or unmonitored access.

2.5.B

Determine appropriate security controls to mitigate vulnerabilities in a SOHO network.

2.5.B.1

Security controls can be implemented to mitigate vulnerabilities in SOHO networks, which often stem from misconfigurations, outdated software, or insecure devices. To determine an appropriate control, users must first identify the vulnerability and consider how it could affect data, devices, or services.

2.5.B.2

Security controls to mitigate the risk of default configurations on routers and access points include:

- changing default login credentials on routers and access points
- enabling WPA2 or WPA3 wireless encryption
- disabling WPS

2.5.B.3

Security controls to mitigate firmware vulnerabilities include regularly installing firmware updates to apply security patches and enabling automatic updates if available to ensure devices have the latest firmware version.

2.5.B.4

Security controls to mitigate the risk of IoT vulnerabilities include:

- changing default login credentials on IoT devices
- applying firmware and software patches regularly
- isolating IoT devices on a network segment separate from critical devices and data to limit lateral movement

2.5.B.5

Security controls to mitigate the risk of unknown devices include establishing a guest network that is separate from the main network; this allows visitors to access the internet while isolating internal devices and data.

SUGGESTED SKILLS

2.A

Identify vulnerabilities and their impacts in data, devices, and networks, and explain how security controls, with and without AI integration, can mitigate vulnerabilities and monitor networks.

2.C

Implement and document security controls to address potential vulnerabilities and monitor networks.

TOPIC 2.6

Applying Defense: Securing My Network

Required Course Content

LEARNING OBJECTIVE	ESSENTIAL KNOWLEDGE
2.6.A Explain how firewalls and network segmentation can be used to improve network security.	**2.6.A.1** Technical controls like firewalls and network segmentation are important security strategies that limit unauthorized access by restricting traffic flow through a network. **2.6.A.2** Firewalls and network segmentation can be used to create different zones of security in a network, such as separating guest traffic from internal systems, which helps prevent malware or adversaries from moving laterally through a network. **2.6.A.3** Firewalls can be used to limit the traffic allowed in or out of a network by applying rules that evaluate information such as IP addresses, ports, and protocols. By limiting the allowed traffic, firewalls reduce the risk of data exposure. **2.6.A.4** Network segmentation can be used to divide a network into smaller segments, isolating sensitive or high-risk devices and data, reducing unnecessary traffic, and creating distinct security zones.
2.6.B Determine appropriate device grouping for network segmentation to improve performance and security.	**2.6.B.1** Network segmentation allows devices to be grouped into zones based on shared roles, security risk levels, or performance needs. When determining device groups for segmentation, consideration should be given to the function of a device, the potential security risks, and the performance requirements.

2.6.B

Determine appropriate device grouping for network segmentation to improve performance and security.

2.6.B.2

Devices can be grouped by their roles to simplify troubleshooting and expansion. Device groups based on roles could include:

- security camera systems
- media devices, including game consoles and streaming servers
- family devices, such as laptops, tablets, and phones

2.6.B.3

Devices can be grouped by their risk level to isolate vulnerable or untrusted devices and prevent threats from spreading across the network. Device groups based on risk levels could include:

- office computers and servers that need high security
- IoT devices, such as thermostats, speakers, and smart TVs, which are often vulnerable
- guest devices placed on a separate wireless segment to limit access to internal resources

2.6.B.4

Devices can be grouped by their performance needs to prioritize the traffic of high-bandwidth or low-latency tasks. Device groups based on performance needs could include:

- gaming consoles and computers used for online play
- media servers used for streaming
- devices used for high-demand remote video editing or rendering

2.6.B.5

Devices can be grouped by the type of user to reduce unnecessary traffic and simplify access control to data and network resources. Device groups based on user types could include:

- office departments, such as sales and accounting
- education users, such as teachers, students, and technicians

THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

AP NETWORKING

UNIT 3

Managing Many Connections

UNIT
3

Managing Many Connections

UNIT SCENARIO

Scenarios at the start of each unit in the AP Networking framework offer authentic situations that are designed to connect the knowledge and skills students gain in the first topic to relevant, real-world applications. Each scenario is paired with relevant student activities. Teachers may use their own scenarios in addition to, or in lieu of, those provided here.

SCENARIO 3A:
Game Day Network Design

Your school is hosting a regional gaming tournament with a live audience and an online livestream. Players, coaches, staff, judges, and spectators will all be connected to the network. As part of the event team, your job is to plan a network that can support every device and user type. Slow or dropped connections could disrupt the livestream, delay matches, or even change the outcome of the competition.

You'll be given details about the event space, user groups, and performance needs. Using this information, you must determine the endpoint devices, network connections, and network segments required for a flawless tournament setup.

Event Network Document Suggestions:

- Device list by user role
- Device connection type, wired or wireless
- Network segmentation diagram to separate user types
- Number of switches, ports, and wireless access points needed
- Justification for device and connection assignments

SUGGESTED SKILLS

1.A
Identify common device and network components, protocols, and configurations, and explain processes and relationships in computer networking.

1.B
Determine, with and without the support of AI, the appropriate configurations and settings for network devices to enable connectivity, management, and performance.

TOPIC 3.1

Planning a Network: Choosing the Right Devices and Connections

Required Course Content

LEARNING OBJECTIVE

3.1.A
Determine the endpoint devices required for a given scenario.

ESSENTIAL KNOWLEDGE

3.1.A.1
The devices needed for a segmented network can vary based on the user role and performance required. Several different types of devices are often needed.

3.1.A.2
Laptops are preferred for users that need to interact with multiple browser-based platforms, type frequently, or multitask across applications.

3.1.A.3
Tablets and smartphones are suitable for mobile access to forms or dashboards to view and update data quickly.

3.1.A.4
Gaming consoles, desktops, or high-performance laptops are necessary for environments where high frame rates and low input latency are required, such as in esports or cybersecurity competitions, video editing and rendering, and large data analysis.

3.1.A.5
Desktops or high-performance laptops with wired Ethernet ports should be used for management workstations or local servers to provide reliability and consistent access to administrative tools such as file hosting and streaming.

3.1.B

Determine the number and type of network connections required for a given scenario.

3.1.B.1

The device connections needed for a segmented network can vary based on the primary function and performance required.

3.1.B.2

Wireless networks can provide scalable access for many devices. Wireless networks should be used to create:

- guest networks for visitors that need basic internet access but should not access internal resources
- internal networks for standard users with access to tools and platforms
- administrator networks for secure, mobile access to administrative tools and data

3.1.B.3

One wireless access point (WAP) can typically support 30–50 mobile devices or up to 20 computers or laptops. Because wireless signal strength decreases with distance and obstacles such as walls or EMI, large or irregular spaces may require multiple WAPs to maintain reliable connectivity for all users.

3.1.B.4

Wired connections should be used for devices that require high-reliability, low-latency, or large data transfers, including:

- high-performance or gaming computers on an internal user network
- management workstations, servers, and livestreaming equipment on an internal staff network

3.1.B.5

Each wired connection requires a port on a network switch. To properly equip a network, consideration should be given to:

- the total number of wired devices
- the available ports on each switch
- the number and length of cables needed
- the number of switches needed

3.1.B.6

Routers connect different network segments together and direct data between them based on IP addresses. Each device in a segmented network must be assigned a default gateway, the router, so that it can send data to devices in other segments or to the internet.

TOPIC 3.2

Creating a Network: Switching and Topologies

SUGGESTED SKILLS

1.A
Identify common device and network components, protocols, and configurations, and explain processes and relationships in computer networking.

1.B
Determine, with and without the support of AI, the appropriate configurations and settings for network devices to enable connectivity, management, and performance.

Required Course Content

LEARNING OBJECTIVE

3.2.A
Explain how data travel through a segmented network.

ESSENTIAL KNOWLEDGE

3.2.A.1
A segmented network divides devices into groups to improve performance, management, and security. Each segment has its own range of IP addresses and is typically used to separate user types, functions, or resources. Networks can be segmented physically with network hardware or logically with software configurations.

3.2.A.2
When preparing data to be sent, a packet is created with a header that contains fields for the source IP address, the destination IP address, and other information to properly route the data. A sending host will compare its own IPv4 address and subnet mask with the destination address.

- If the destination is on the same network segment, the data are sent directly to the destination MAC address through a switch.
- If the destination IP address is on a different network or segment, the data are sent to the default gateway, or router, to be directed to the correct network.

3.2.A.3
A router contains a routing table that shows possible routes that packets can travel. When a router receives data, the destination IP address is compared to the routing table entries to determine the segment the data should be sent to, and the router forwards the packet to a switch on the correct segment to be delivered to the destination device.

3.2.B

Determine appropriate network segmentation methods for a given scenario.

3.2.B.1

Devices, applications, and services should be grouped based on their sensitivity, access requirements, and traffic needs. Segmenting guest access, IoT devices, user workstations, and internal services reduces congestion from broadcast messages and limits an adversary's ability to move laterally.

3.2.B.2

Physical segmentation should be used when maximum isolation and security are needed, such as in restricted zones or separate departments. Physical segmentation uses separate switches, routers, or cabling to build isolated subnetworks. It increases complexity and cost but provides strong separation.

ILLUSTRATIVE EXAMPLE

A university computer science department designed a testing lab that is connected to its own switch and router, separate from the switches and routers used by the university's classrooms and offices. Because the lab uses separate network hardware, traffic is physically isolated from the rest of the network.

3.2.B.3

Virtual local area networks (VLANs) should be used to provide a flexible way to separate network traffic and devices without requiring extra physical hardware. VLANs allow flexible grouping of devices connected to the same switch, making them ideal for separating departments, device types, or user roles on shared hardware.

ILLUSTRATIVE EXAMPLE

An office connects employee computers, VoIP phones, and printers to the same managed switch, while their switch ports are assigned to different VLANs. So all devices share the same physical switch, but the VLAN assignments keep employee data traffic, voice traffic, and printing traffic logically separated.

3.2.B.4

Subnetting should be used to organize devices by IP range and support routing, access control, or efficient address allocation. Subnetting is well suited for environments that require firewall enforcement between IP groups or broadcast control across multiple segments. Subnetting divides a large network into smaller, logically separated address ranges.

3.2.B

Determine appropriate network segmentation methods for a given scenario.

3.2.B.5

Wireless segmentation using multiple SSIDs should be used when different user groups need separate wireless access, such as staff and guests. These SSIDs can be assigned to separate VLANs or subnets, providing both traffic isolation and access control.

3.2.C

Explain why a specific wired network topology would be selected in a given scenario.

3.2.C.1

Network topologies are selected based on the specific needs of a network, including reliability, cost, and ease of maintenance. These factors influence how devices are connected and how traffic flows across the network. Modern networks typically use star, mesh, and hybrid, while topologies like bus and ring are generally avoided due to their limited fault tolerance and scalability.

3.2.C.2

In a star topology, each node is connected indirectly to every other node through a central network device, typically a network switch. All data pass through this central point, making the network easy to scale and troubleshoot.

3.2.C.3

In a mesh topology, each node is connected directly to every other node, providing multiple paths for data to travel. This topology has a high fault tolerance but requires more cabling, devices, and management.

3.2.C.4

Hybrid topologies are often used in larger networks to combine elements of star and mesh to balance performance, reliability, and cost. They are commonly used in large LANs where different segments of the network have different needs or constraints.

3.2.C.5

Reliability is a key factor in networks where uptime is essential.

- Star topology is reliable because all nodes are independently connected, but the central switch is a single point of failure.
- Mesh topology is more reliable and offers higher fault tolerance because multiple data paths exist, allowing communication to continue even if one connection fails.

3.2.C

Explain why a specific wired network topology would be selected in a given scenario.

3.2.C.6

Cost to install and maintain often influences topology choice.

- Star topology is relatively cost-effective due to the minimal cabling and hardware requirements.
- Mesh topology is more expensive and complex due to the number of connections and cabling required.

3.2.C.7

Ease of setup and maintenance is important for long-term network management.

- Star topology is easy to install, scale, and troubleshoot, as each device connects independently; this is ideal for networks with limited resources.
- Mesh topology is more complex to install, scale, and maintain due to redundant connections; this is ideal for networks with dedicated support.

3.2.D

Evaluate an AI-generated network configuration for a LAN with multiple segments.

3.2.D.1

AI tools can be used to generate suggestions for topologies, segmentation strategies, and devices needed for a segmented LAN. Prompts should clearly define technical requirements such as traffic flow, security policies, redundancy needs, and physical layout constraints. Incomplete prompts may result in flawed or partial designs.

3.2.D.2

Suggestions generated by AI may include missing or incomplete segments, suggestions that only address some of the identified requirements, and devices or connections that are not the best solution. Suggestions can be technically accurate while adding unnecessary complexity or cost.

3.2.D.3

AI tools are valuable for generating ideas and identifying potential areas of concern or opportunities for improvement, but any AI output should be evaluated and verified before being implemented to ensure it aligns with the needs, goals, and constraints of the network.

SUGGESTED SKILLS

1.C
Implement and document device and network configurations to establish and maintain connectivity.

1.D
Verify connectivity and configurations of devices and networks, and apply the troubleshooting skills to resolve any problems.

TOPIC 3.3

Making It Work: Connecting, Configuring, and Verifying Access

Required Course Content

LEARNING OBJECTIVE

3.3.A
Configure an IP address on a device and verify the settings.

ESSENTIAL KNOWLEDGE

3.3.A.1
A static IP address is assigned manually, while dynamic addresses are leased by a DHCP server that manages a pool of available IP addresses.

3.3.A.2
A static IP address can be configured on a host device by accessing the network settings and manually entering the IP address, subnet mask, and default gateway. Every IP address in a LAN must be unique and within the IP address range of the network.

3.3.A.3
The DHCP server, typically built into a router or switch, manages and automatically assigns hosts a range of IP addresses from the DHCP pool. To configure a DHCP pool users:

- access the web interface or CLI of the network device
- define the IP address range of the DHCP pool
- set the subnet mask, default gateway, and network address
- specify the IP address renewal frequency, often referred to as a lease

3.3.A.4
DHCP can be enabled on a host device by selecting the option to obtain IP addresses automatically in the network settings.

3.3.A

Configure an IP address on a device and verify the settings.

3.3.A.5

Verify that the IP configuration, subnet mask, default gateway, and MAC address match intended settings using `ipconfig`, `ifconfig`, or network settings. MAC addresses may appear as “Physical Address,” “Hardware Address,” or “Ether Address.”

3.3.B

Determine whether two devices are on the same network based on their IP addresses and subnet masks.

3.3.B.1

IPv4 address and subnet mask notation simplifies binary notation for ease of human use; each octet is a set of eight bits, or binary digits. In dotted decimal format, each octet is converted into a decimal number between 0 and 255.

3.3.B.2

The 32 bits of an IPv4 address are divided into two sections: network bits and host bits. The subnet mask paired with the IPv4 address is used to determine the network and host bits of the IPv4 address. A subnet mask is a sequence of ones (1) followed by a sequence of zeros (0). The ones designate the network bits, while the trailing sequence of zeros designates the host bits.

3.3.B.3

Classless Inter-Domain Routing (CIDR) notation uses a forward slash followed by the number of 1 bits in the subnet mask.

ILLUSTRATIVE EXAMPLES

- /24 = 11111111.11111111.11111111.00000000 = 255.255.255.0
- /16 = 11111111.11111111.00000000.00000000 = 255.255.0.0
- /26 = 11111111.11111111.11111111.11000000 = 255.255.255.192

3.3.B

Determine whether two devices are on the same network based on their IP addresses and subnet masks.

3.3.B.4

Two IPv4 addresses belong to the same network when they have matching network bits and subnet masks. To determine this, the network portion of each address should be compared using the subnet mask. If the network portions are the same, the devices are on the same network.

ILLUSTRATIVE EXAMPLE

With a subnet mask 255.255.255.0, the first three octets are the network bits and the last octet consists of the host bits. For example:

- IP Address 1: 192.168.1.10
- IP Address 2: 192.168.1.20
- IP Address 3: 192.168.2.30

The network bits match on the first two IP addresses as they are on the same network, but the third address is on a different network.

3.3.C

Configure a local area network (LAN).

3.3.C.1

To physically connect and configure a LAN, a variety of tools and devices are needed, including:

- appropriate cabling to connect devices
- cable stripper or wire stripper to remove insulation jackets from cables
- connectors, such as RJ45, to connect Ethernet cables to devices
- crimping tool to attach connectors to cables
- cable management and labeling tools to organize and secure cables and power cords
- network devices and endpoints
- personal safety equipment like safety glasses and gloves

3.3.C.2

When connecting and configuring a LAN, the devices, cabling, and network needs must be identified to determine the appropriate topologies and settings. Network design should be completed before connecting and configuring devices.

3.3.C.3

Settings on a network switch like the password, IP address, and subnet mask can be manually assigned using the CLI or the graphical user interface (GUI) of the switch's management console. The management console can be accessed by connecting through a console cable.

3.3.C Configure a local area network (LAN).	**3.3.C.4** A router or gateway is required to provide access to external networks, including the internet. The router must be configured with an IP address and subnet mask to act as the default gateway for devices on the local network. **3.3.C.5** Wireless connectivity can be added to a LAN by installing a wireless access point or enabling wireless features on a wireless router. The WAP should be configured with an SSID, wireless security settings, an IP address, and a subnet mask. **3.3.C.6** Endpoints on the network must have their IP addresses and subnet masks configured to meet the requirements of the network. IP addresses can be assigned individually using static addressing or automatically using DHCP. **3.3.C.7** To verify connectivity of devices on a network, `ping` can be used to send Internet Control Message Protocol (ICMP) packets to a specific IP address. If successfully connected, the target device will respond to the ICMP request. For example, `ping 192.168.1.127` will send ICMP packets to the device with the IP address 192.168.1.127.
3.3.D Configure a wireless access point to support a guest network and an internal network.	**3.3.D.1** Most wireless access points allow a guest network to be created to provide internet access without access to the internal network. This provides a level of protection for the main network. **3.3.D.2** An internal wireless network should be configured first to ensure the settings are correct and the internal devices and resources can communicate. This includes creating an SSID with a strong password, enabling WPA2 or WPA3 encryption, and disabling WPS. **3.3.D.3** A guest network can be enabled through the router or access point settings. The settings can typically be accessed by entering the IP address of the router or access point in a web browser and logging in with the administrator credentials.

3.3.D Configure a wireless access point to support a guest network and an internal network.	**3.3.D.4** When the guest network feature is enabled on a router or access point, the guest network configuration is available and is similar to configuring a standard wireless network. A separate SSID must be created with a strong password and WPA2 or WPA3 encryption enabled. **3.3.D.5** Additional measures that can be implemented on a guest network include: ▪ limiting the number of devices ▪ disabling access to the internal network ▪ setting access hours or session time limits ▪ enabling a captive portal that requires users to log in and agree to terms of use **3.3.D.6** Correct configuration of a guest wireless network can be verified by connecting a device to the network. The device should have access to the internet without access to internal network resources.

TOPIC 3.4

Building the Boundaries: Identifying Segmentation Security

SUGGESTED SKILLS

2.B
Determine, with and without the support of AI, mitigation strategies to address device and network vulnerabilities.

2.C
Implement and document security controls to address potential vulnerabilities and monitor networks.

Required Course Content

LEARNING OBJECTIVE

3.4.A
Identify the impacts of common threats and vulnerabilities in a segmented LAN.

ESSENTIAL KNOWLEDGE

3.4.A.1
Unauthorized access, unverified device connections, and data exposure are common impacts in segmented networks with multiple user types and devices. These risks highlight the need for appropriate access controls to ensure confidentiality, integrity, and availability of data.

3.4.A.2
Unauthorized access to administrative systems or confidential data can occur when user groups, devices, or resources are not properly separated by access controls. This lack of segmentation may also lead to interference with shared resources or user productivity.

3.4.A.3
Sensitive data and network resources may be accessed by unauthorized users when wireless networks use weak security methods, such as simple passwords, outdated encryption like WEP, or no encryption at all.

3.4.A.4
Sensitive systems and internal data may be compromised if unknown or unverified devices are allowed to connect to the network. These devices may intercept traffic, spread malware, or bypass internal security controls.

3.4.A.5
An adversary may move laterally across a network and gain access to multiple systems or segments where firewall rules are weak or misconfigured.

3.4.B

Determine appropriate security controls to limit the impacts of common threats and vulnerabilities in a segmented LAN.

3.4.B.1

Segmented networks use security controls to reduce the impact of unauthorized access. Security controls should be implemented to follow the principle of least privilege, allowing users and devices only the minimum access necessary to perform their tasks.

3.4.B.2

Security controls to limit unauthorized access include:

- creating isolated guest wireless networks
- assigning distinct IP address ranges or DHCP pools for device groups
- segmenting devices physically with separate network hardware

3.4.B.3

Security controls to limit the impact of weak wireless network security include:

- configuring the wireless segment with a unique SSID
- strong password protection
- WPA2 or WPA3 encryption

3.4.B.4

Security controls to limit connections from unknown or unverified devices can include:

- enabling MAC address filtering to allow only approved devices
- setting unused ports to down
- using DHCP reservations to limit address leasing to only known devices

3.4.B.5

Security controls to limit lateral movement or unintended communication between segments can include:

- allowing only essential services, such as printing, to communicate across segments
- deny-by-default firewall or access policies that block traffic between subnets

3.4.C

Configure subnetting to appropriately segment a network.

3.4.C.1

Subnetting is a method of network segmentation that divides a network into smaller sections called subnets. Subnetting can help with network congestion, security, and management.

3.4.C

Configure subnetting to appropriately segment a network.

3.4.C.2

A subnet mask is used to determine the network and host bits. In the process of subnetting, host bits are re-assigned as network bits, reducing the number of available host addresses and creating the range of subnet addresses.

ILLUSTRATIVE EXAMPLE

In a network with IP address 192.168.1.0, with a subnet mask 255.255.255.0, there are 256 total addresses in one network with 254 usable host addresses in the last octet. To create two subnets in this network to improve performance or create segments, the subnet mask can be changed to 255.255.255.128, creating two subnets:

- Subnet 1: 192.168.1.0- 192.168.1.127
- Subnet 2: 192.168.1.128- 192.168.1.255

3.4.C.3

The number of hosts a network can accommodate is 2^n-2 where n is the number of host bits. The first and last addresses on a network are reserved for the network address and broadcast address, respectively, and cannot be assigned to hosts.

- The network address is the first address in a subnet; it's used to identify the subnet.
- The broadcast address is the last address in a subnet; it's used to send messages to all devices in that subnet.
- The usable host range includes the IP addresses between the network and broadcast addresses that can be assigned to devices.

ILLUSTRATIVE EXAMPLES

- A network with 8 host bits has $2^8 = 256$ total addresses. The first address is the network address and the last is the broadcast address, leaving 254 usable host addresses.
- A network with 5 host bits has $2^5 = 32$ total addresses. After reserving the network and broadcast addresses, 30 addresses can be assigned to hosts.

3.4.C

Configure subnetting to appropriately segment a network.

3.4.C.4

An appropriate subnet size is the smallest possible network size that accommodates the required number of hosts on a network. IP address blocks should be large enough to fit all hosts plus two reserved addresses.

ILLUSTRATIVE EXAMPLES

- Subnet A has 27 hosts, which will require 29 addresses, and the next power of 2 is 32, requiring 5 host bits.
- Subnet B has 12 hosts, which will require 14 addresses, and the next power or 2 is 16, requiring 4 host bits.

3.4.C.5

Once subnets have been created, they can be assigned to different VLANs or segments to isolate traffic and create zones of security. Each subnet should have a nonoverlapping IP address range and subnet mask. Subnet blocks are configured on routers or switches through the CLI or network settings.

3.4.C.6

After subnets have been assigned, connectivity between devices on the same subnet should be verified to ensure the configuration is correct.

TOPIC 3.5

Controlling the Traffic: Firewalls and Filtering

SUGGESTED SKILLS

2.B
Determine, with and without the support of AI, mitigation strategies to address device and network vulnerabilities.

2.C
Implement and document security controls to address potential vulnerabilities and monitor networks.

Required Course Content

LEARNING OBJECTIVE	ESSENTIAL KNOWLEDGE
3.5.A Explain how MAC filtering can increase security.	**3.5.A.1** MAC filtering restricts access by allowing only approved MAC addresses. A switch port can be configured to permit a limited or specific set of MAC addresses; all others are denied. **3.5.A.2** Limiting the number and range of MAC addresses associated with a physical switch port can prevent unauthorized devices from physically connecting to the network. **3.5.A.3** MAC filtering can be used to prevent MAC flooding. MAC flooding occurs when a switch receives many unique MAC addresses and overflows the CAM table, causing the CAM table to run out of memory. MAC flooding can force the switch into a fail-open state, which broadcasts all network traffic to all nodes. This can lead to network congestion and interception of data intended for other devices.
3.5.B Determine an appropriate firewall for a scenario.	**3.5.B.1** Firewalls are used to create areas of different access levels in a network and prevent unauthorized access or movement between zones. When determining which firewall to use considerations include: ▪ the level of traffic inspection needed, such as simple filtering or deep packet inspection ▪ whether the firewall protects a device, a zone, or an entire organization ▪ whether the network is exposed to the internet, contains sensitive data, or involves untrusted users or devices

3.5.B
Determine an appropriate firewall for a scenario.

3.5.B.2
Firewalls can be chosen based on their level of filtering.

- A stateless firewall filters traffic based on fixed rules, like IP addresses, ports, or protocols, but does not log or track connections. It is appropriate for simple or low-risk network segments.
- A stateful firewall tracks active connections and can track and log suspicious traffic. This is ideal for zones that need connection awareness and logging.
- A next-generation firewall (NGFW) includes advanced features like intrusion prevention and application-based filtering. NGFWs are suitable for high-risk zones or where detailed traffic inspection is needed.

3.5.B.3
A perimeter firewall protects the boundary between internal and external networks and serves as the first line of defense against external threats. It handles high traffic volumes and applies broad security policies to all incoming and outgoing traffic.

3.5.B.4
An internal firewall is deployed within a network to isolate sensitive devices or departments and prevent lateral movement. Internal firewalls can be used to create a screened subnet (also known as a demilitarized zone, or DMZ) between public networks and internal resources. Screened subnets are lower-security zones that are used to host public-facing services.

3.5.B.5
A host-based firewall is software installed on individual devices to add more security and customization. These are typically used to secure endpoints that move between networks or require tailored security settings.

3.5.C
Configure firewall rules for different network segments.

3.5.C.1
Firewalls use rules to permit or deny inbound and outbound network traffic. Lists of firewall rules are known as access control lists (ACLs). ACLs are checked in order, top to bottom, and the first rule that matches the criteria will be executed for the specified data.

3.5.C

Configure firewall rules for different network segments.

3.5.C.2

A typical ACL will specify the direction of traffic on an interface (inbound or outbound), the criterion to filter by (IP addresses, logical port, service, or application), and action (permit or deny). Different firewalls will use different criteria to filter traffic. Common ports and protocols used in ACLs include:

- Hypertext Transfer Protocol Secure (HTTPS) port 443 – secure web traffic
- Domain Name System (DNS) port 53 – domain name resolution
- Secure Shell (SSH) port 22 – secure remote CLI access
- Secure File Transfer Protocol (SFTP) port 22 – secure file transfer over SSH

3.5.C.3

ACLs should be created to limit opportunities for malicious traffic, closing unused and vulnerable ports whenever possible while prioritizing services needed. Vulnerable ports and protocols include:

- Hypertext Transfer Protocol (HTTP) port 80 – unencrypted web traffic
- Telnet port 23 – unencrypted remote CLI access
- File Transfer Protocol (FTP) port 21 – unencrypted file transfer

ILLUSTRATIVE EXAMPLE

The following rule configuration prioritizes necessary services (ports 443, 22, and 53) while closing unused and vulnerable ports (ports 80 and 23):

- `101 ALLOW inbound TCP port 443 from ALL;`
- `102 ALLOW inbound TCP port 22 from ALL;`
- `103 DENY inbound TCP port 80 from ALL;`
- `104 DENY inbound TCP port 23 from ALL;`
- `105 ALLOW inbound UDP port 53 from ALL;`

3.5.C

Configure firewall rules for different network segments.

3.5.C.4

Firewall rules are implemented in order, and changing the order of a set of rules can change which traffic is allowed or denied. Consideration must be given to filtering priorities when establishing the order of rules. More specific rules should be placed above broad, general rules.

ILLUSTRATIVE EXAMPLE

The following rule configuration would allow SSH traffic and deny all other inbound TCP traffic:

- `101 ALLOW inbound TCP port 22 from ALL;`
- `102 DENY inbound TCP ALL from ALL;`

Reversing the order of those rules would deny all inbound TCP traffic, including SSH traffic.

3.5.C.5

After configuring firewall rules, users should verify that the intended access is allowed and that unauthorized access is blocked. Verification can include using `ping` to access other segments and ensure continued access to network resources.

TOPIC 3.6

Restored Connections: Documenting, Diagnosing, and Fixing a Segmented LAN

Required Course Content

LEARNING OBJECTIVE

3.6.A
Document the network design, including IP configuration, devices, and connections.

ESSENTIAL KNOWLEDGE

3.6.A.1
Documentation of a network enables efficient network management and troubleshooting. Complete and clear documentation should be provided for all users, including updates whenever changes occur.

3.6.A.2
Network topologies, including physical and logical segmentation, can be represented in a visual diagram with labeled devices and wired and wireless connections.

3.6.A.3
Devices should be labeled with consistent and clear names and roles to support identification and troubleshooting.

3.6.A.4
IP addressing schemes should be recorded, with any statically addressed devices identified.

3.6.A.5
To ensure appropriate security is applied, segments with specific firewall rules or access control requirements should be noted.

SUGGESTED SKILLS

3.A
Identify common device and network problems, and explain how tools, including AI, can be used to diagnose the causes of the problems.

3.B
Determine, with and without the support of AI, the causes of common device and network problems and determine potential solutions to solve those problems.

3.6.B

Identify likely root causes of an issue in a LAN with multiple segments using diagnostic tools and techniques.

3.6.B.1

Common issues in a LAN with multiple segments include devices failing to connect, limited access to internal resources, or slow performance. Many connectivity and performance issues in a large network can be resolved by implementing common solutions. If functionality is not restored, gathering diagnostic information facilitates the troubleshooting process. Common solutions for segmented LAN connectivity include:

- restarting the network router, switch, or wireless access point
- restarting affected devices
- disconnecting and reconnecting to the network
- ensuring the device is connected to the correct SSID and the password is correct

3.6.B.2

An unavailable DHCP server or exhausted DHCP pool can cause devices to be assigned APIPA addresses, which prevent communication outside of the local network. This can be identified by checking the IP address configuration.

3.6.B.3

A missing or incorrect gateway or subnet mask will prevent network access. Properly configured devices will have an IP address, subnet mask, and default gateway that matches the network settings. This can be identified by comparing the network settings to the IP configuration

3.6.B.4

Firewall rules or restrictions can block internal and external device communication. This can be identified using the `ping` command to test internal and external reachability.

3.6.B.5

Weak wireless signal strength or high interference can cause degraded wireless performance. This can be identified using wireless signal analyzer tools, available as mobile apps or standalone devices.

- Weak signal strength (below –70 dBm) may indicate that the WAP is too far or is being obstructed by walls or objects.
- High noise or interference may indicate EMI from other devices.

3.6.B

Identify likely root causes of an issue in a LAN with multiple segments using diagnostic tools and techniques.

3.6.B.6

Fluctuating or unstable power supply can cause network devices to reboot unexpectedly or lose connectivity. Frequent short outages, less than 5 seconds, may not trigger software alerts but can disrupt routing tables or DHCP leases. This can be identified using a power analyzer that logs voltage levels and interruptions.

- Voltage levels below 110V or above 125V (in a 120V system) may cause network devices to restart or malfunction.
- Power logs that show multiple brief dropouts across devices may indicate a shared electrical issue or overloaded power source.

3.6.C

Determine an appropriate solution to resolve an issue in a LAN with multiple segments.

3.6.C.1

Solutions for an unavailable DHCP server or exhausted DHCP pool include:

- restarting the DHCP server
- expanding the IP address range of the DHCP pool to support more addresses
- limiting the lease time to force IP assignments to recycle more quickly

3.6.C.2

Solutions for devices with missing or incorrect default gateway or subnet mask include:

- assigning the correct default gateway and subnet mask
- ensuring the DHCP server settings include network information

3.6.C.3

Solutions for improperly configured access control rules or firewall restrictions include:

- reordering ACL rules to place allow rules before broad deny rules
- checking deny rules to avoid unintentionally blocking necessary traffic
- ensuring the ACL rules are correct regarding direction, ports, and protocols
- changing firewall rules to allow necessary outbound traffic to external networks

3.6.C

Determine an appropriate solution to resolve an issue in a LAN with multiple segments.

3.6.C.4

Solutions for weak wireless signal strength or high interference include:

- moving the access point to improve the coverage radius
- reducing physical obstructions between the access point and devices
- relocating the access point away from sources of EMI like microwaves and Bluetooth devices

3.6.C.5

Solutions for voltage drops or power delivery problems include:

- replacing or relocating devices to a different power circuit
- installing an uninterruptible power supply (UPS)

3.6.C.6

To verify that functionality has been restored, users should confirm that devices can maintain a stable connection to the network and reach both internal and external resources as needed.

AP NETWORKING

UNIT 4

Managing Our Global Connections

UNIT 4

Managing Our Global Connections

UNIT SCENARIO

Scenarios at the start of each unit in the AP Networking framework offer authentic situations that are designed to connect the knowledge and skills students gain in the first topic to relevant, real-world applications. Each scenario is paired with relevant student activities. Teachers may use their own scenarios in addition to, or in lieu of, those provided here.

SCENARIO 4A:
Grocery Store Downtime

You are an IT support intern for a local grocery store. It is a busy Saturday morning with many customers preparing for upcoming events. Suddenly prices on items are incorrect, the inventory system shows products on the shelves as out of stock, and payment processing becomes unreliable. The store manager fears there may be a security incident impacting confidentiality, integrity, and availability all at once.

Your job is to investigate what happened, identify which parts of the CIA Triad were compromised, and determine the potential short- and long-term impacts on the store and its customers. You will compile your findings into an incident evidence and impact report for store management.

Incident Evidence and Impact Report Suggestions:

- Incident summary
  - What happened, when it occurred, and which systems or services were affected.
- CIA Triad analysis and evidence
  - Confidentiality: What sensitive data may have been accessed or exposed? What evidence supports this?
  - Integrity: Were files, records, or systems altered without authorization? What is the proof?
  - Availability: Were services down or degraded? What symptoms were observed?
- Impact assessment
  - Short-term disruptions – Immediate effects on customers, employees, and operations.
  - Long-term impacts – Possible consequences for sales, reputation, and customer trust.

SUGGESTED SKILLS

2.A
Identify vulnerabilities and their impacts in data, devices, and networks, and explain how security controls, with and without AI integration, can mitigate vulnerabilities and monitor networks.

3.A
Identify common device and network problems, and explain how tools, including AI, can be used to diagnose the causes of the problems.

TOPIC 4.1
What Happens When Networks Break or Fail?

Required Course Content

LEARNING OBJECTIVE

4.1.A
Identify evidence of compromised confidentiality, integrity, or availability.

ESSENTIAL KNOWLEDGE

4.1.A.1
Confidentiality, integrity, and availability are the basis of secure and reliable network communication and are collectively referred to as the CIA triad.

- Confidentiality means that only authorized individuals, systems, or processes access data.
- Integrity means that data are accurate, trustworthy, and have not been altered.
- Availability means that data and services are accessible to authorized entities.

4.1.A.2
Violations of the CIA triad often occur together, resulting in greater impact. Understanding the full scope of an incident requires investigating what happened, who was affected, and how data or services were impacted. Incident investigation involves reviewing:

- access logs
- alerts from firewalls or network monitoring tools
- error reports
- missing or corrupted files
- network outages or slowdowns

4.1.A

Identify evidence of compromised confidentiality, integrity, or availability.

4.1.A.3

When confidentiality is compromised, systems are vulnerable to having sensitive data exposed or stolen. A breach of confidentiality can be identified by:

- unauthorized access
- network traffic showing exfiltration of sensitive data
- exposed credentials
- unusual activity on sensitive data

4.1.A.4

When integrity is compromised, systems may contain false or inaccurate data. A breach of integrity can be identified by:

- unauthorized data changes
- inconsistencies in logs
- unauthorized software installations
- corruption of data

4.1.A.5

When availability is compromised, systems have unexpected periods of time when they are out of service. A breach of availability can be identified by:

- an inability to access systems, networks, or resources
- slow or dropped connections
- unexpected high volume of network traffic
- frequent error messages

4.1.B

Explain how unreliable connectivity impacts organizations.

4.1.B.1

Network connectivity supports essential tasks such as communication, data access, and service delivery. When connectivity is unreliable, users or employees may lose access to essential systems, which can lead to delays, errors, or lost productivity.

4.1.B.2

The impacts of a loss of connectivity vary based on the timing of the disruption and the type of system affected. Outages during peak activity cause greater impacts than those occurring during low-usage periods. There can be severe consequences when critical infrastructure systems, such as emergency response, power, or water, are disrupted at any time.

4.1.B Explain how unreliable connectivity impacts organizations.	**4.1.B.3** In some sectors, such as the food supply chain, healthcare, and the military, connectivity disruptions can cause serious functional or public safety consequences. **4.1.B.4** Extended or repeated network outages can cause long-term consequences, including: ▪ financial loss from missed transactions or reduced productivity ▪ reputational damage that discourages customers or investors ▪ erosion of public trust, especially for public institutions or critical services

TOPIC 4.2

The Language of the Network: Protocols and the OSI and TCP/IP Models

Required Course Content

LEARNING OBJECTIVE

4.2.A

Describe the purpose of common network protocols.

ESSENTIAL KNOWLEDGE

4.2.A.1

Network protocols define rules that ensure data are recognized and properly handled during transmission.

4.2.A.2

Network protocols are used for identifying devices and networks to ensure data are directed to the correct destination.

- MAC addresses and ARP are used to identify devices on a local network.
- IP addresses identify local and remote devices.
- DHCP automatically assigns IP addresses to devices.
- DNS translates domain names into IP addresses.

ILLUSTRATIVE EXAMPLE

Entering the URL google.com uses the DNS protocol to translate into one of Google's public IP addresses, such as 172.253.63.100. This translation allows for simplified communication and resolution of web requests.

SUGGESTED SKILLS

1.A

Identify common device and network components, protocols, and configurations, and explain processes and relationships in computer networking.

3.B

Determine, with and without the support of AI, the causes of common device and network problems and determine potential solutions to solve those problems.

4.2.A

Describe the purpose of common network protocols.

4.2.A.3

Network protocols are used to define how data are packaged and verified.

- ICMP reports transmission time and errors during data transmission; ICMP is used in tools like `ping` and `traceroute`.
- Transmission Control Protocol (TCP) is a connection-oriented protocol that tracks acknowledgements and resends missing data; TCP is used when complete and accurate transmission is essential.
- User Datagram Protocol (UDP) is a connectionless protocol that is used when transmission speed is more important than accuracy, such as in streaming or online gaming.

4.2.A.4

Network protocols allow users to interact with content or services by defining how data are requested, sent, and received.

- FTP and SFTP are used to transfer files between devices.
- HTTP and HTTPS are used to load webpages.
- Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP3), and Internet Message Access Protocol (IMAP) are used in email communications.

4.2.B

Describe the purpose and organization of the OSI and TCP/IP models.

4.2.B.1

The Open Systems Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) networking models describe how computers communicate on a network and allow for a common language around network devices, protocols, and data.

4.2.B

Describe the purpose and organization of the OSI and TCP/IP models.

4.2.B.2

A protocol data unit (PDU) is a single unit of information transmitted over a network. It contains the data and protocol information needed for transmission. The PDU at each layer of the OSI and TCP/IP model changes as it is encapsulated with more information to assist with the transmission of the data.

Protocol data units at each OSI model layer:

- layer 1– physical layer: bits
- layer 2 – data link layer: frames
- layer 3 – network layer: packets
- layer 4 – transport layer: segments
- layer 5 – session layer: data
- layer 6 – presentation layer: data
- layer 7 – application layer: data

Protocol data units at each TCP/IP model layer:

- network access layer: bits and frames
- internet layer: packets
- transport layer: segments
- application layer: data

4.2.B.3

The OSI model has seven layers that correspond to the four layers of the TCP/IP model.

- OSI layers 1–2 correlate with the TCP/IP network access layer.
- OSI layer 3 correlates with the TCP/IP internet layer.
- OSI layer 4 correlates with the TCP/IP transport layer.
- OSI layers 5–7 are often collectively referred to as the upper layers and correlate with the TCP/IP application layer.

4.2.B.4

The OSI model organizes network protocols into layers based on their functions, defining how data are formatted, transmitted, and interpreted at each stage. This includes:

- layer 1 physical: bits and physical transmission media
- layer 2 data link: Ethernet, MAC addresses
- layer 3 network: IP addresses, ICMP
- layer 4 transport: TCP, UDP
- layers 5–7 upper layers: application layer protocols, such as DNS and HTTPS

4.2.C

Explain how to use the OSI and TCP/IP models when troubleshooting.

4.2.C.1

The OSI and TCP/IP model layers can be used to structure the troubleshooting process. Using the model helps isolate issues to a specific layer, such as identifying a cable problem at the physical layer or a firewall issue at the transport layer. A layered approach helps organize where to begin and what to check next.

- The physical layer includes cables, connectors, and wireless transmitters.
- The data link layer includes NICs, MAC addresses, and layer-2 switches.
- The network layer includes routers, IP addresses, and layer-3 capable switches.
- The transport layer includes gateways and firewalls.
- The upper layers include software, operating systems, and endpoint devices.

4.2.C.2

Troubleshooting can follow different structured approaches depending on the symptoms.

- A bottom-up approach starts with physical connection checks.
- A top-down approach begins with applications.
- A middle-out approach may begin in the middle with the network settings and move up or down.

TOPIC 4.3

Tools of Network Analysts: Using the CLI

SUGGESTED SKILLS

1.C

Implement and document device and network configurations to establish and maintain connectivity.

1.D

Verify connectivity and configurations of devices and networks, and apply the troubleshooting skills to resolve any problems.

Required Course Content

LEARNING OBJECTIVE

4.3.A

Apply appropriate commands using a CLI to navigate computer systems.

ESSENTIAL KNOWLEDGE

4.3.A.1

While GUIs can be more intuitive for users, CLIs allow for simplified automation and repetition of tasks or commands. Many devices only have a CLI, because CLIs take up less space than GUIs and CLIs use less processing power than GUIs, leaving more storage and processing available to the user for tasks, applications, and storage.

4.3.A.2

In Linux-based operating systems, the location often begins with the root directory, `/`, followed by the names of nested directories. Many modern CLI shells use a dollar sign, `$`, to indicate the prompt for user entry. The tilde, `~`, indicates the current user's home directory.

ILLUSTRATIVE EXAMPLES

- In Linux file path `/home/user/Desktop`, `home` is a directory in the root directory, `user` is a directory in `home`, `Desktop` is a directory in `user`.
- The Linux prompt `user@hostname /home/user/Desktop $` represents that the command line interface is ready for input in the `Desktop` directory.
- The Linux prompt `user@hostname ~ $` represents that the command line interface is ready for input in the user's home directory.

4.3.A

Apply appropriate commands using a CLI to navigate computer systems.

4.3.A.3

Command Prompt is a proprietary Windows CLI, and it lists the working directory starting with a drive letter followed by the names of nested directories. The system is ready to accept a command when it displays the right-angle bracket, `>`, at the end of the directory path.

ILLUSTRATIVE EXAMPLES

- In Windows file path `C:\Users\username\Desktop`, `Users` is a directory in `C:`, `username` is a directory in `Users`, and `Desktop` is a directory in `username`.
- In Windows prompt `C:\Users\user\Desktop`, `/home/user/Desktop` is an absolute path, whereas `Desktop` is a relative path. If the current working directory is `/home/user`, then referencing the relative path `Desktop` will assume to look for `Desktop` in `/home/user`.

4.3.A.4

CLI commands follow a standard syntax pattern: command, options, arguments.

- Commands are the name of the program to be executed, such as `cd` or `ls`.
- Options are optional parameters that modify how the command operates or the output of the command. Options are often denoted with a dash, `–`, and are also referred to as switches or flags.
- Arguments provide specific information the command needs to operate such as a file or path. Some commands require arguments, while others can run with no additional input.

To illustrate this structure, the command `ls` can be used in several ways on a Linux system.

- `ls` This execution of `ls` is without options or arguments. When no argument is provided, the working directory is the default argument. It will list or display the contents of the working directory excluding hidden files.
- `ls –a` This execution of `ls` specifies the option `–a`. This option displays all content in the working directory, including hidden files and directories.
- `ls user1` This use of `ls` has no options but specifies an argument of `user1`. It will display the contents of the `user1` directory excluding hidden files.
- `ls –a user1` This use of `ls` specifies both an option of `–a` and an argument of `user1`. It will display the contents of the `user1` directory including any hidden files.

4.3.A

Apply appropriate commands using a CLI to navigate computer systems.

4.3.A.5

In a CLI users need to move between directories, view directory contents, and determine their current location within the file system. Commands to perform these actions include:

- `cd` – change the working directory
- `ls` – list the contents of a directory (Mac/Linux)
- `dir` – view the contents of a directory (Windows)
- `pwd` – view the current working directory (Mac/Linux)

4.3.A.6

The `cd` command is a useful tool for changing directories in a file system. Usage of the `cd` command includes:

- `cd subdirectory_name` – change to a subdirectory in your current location
- `cd ..` – move toward the root directory
- `cd ~` – move to the home directory
- `cd /` – move to the root directory

4.3.A.7

The `help` or `man` commands can be used to gain information about other commands. `help` is useful for providing an overview of a command, while `man` provides detailed documentation about options and usage.

4.3.B

Apply CLI commands to securely transfer files.

4.3.B.1

The CLI allows users to perform tasks efficiently, including system management and file transfers. Secure Shell (SSH) is a protocol used in CLI environments to securely connect to remote systems. It encrypts all data exchanged between the user and the remote device.

4.3.B.2

Secure File Transfer Protocol (SFTP) can be used to transfer data between devices. SFTP uses SSH to establish a secure connection ensuring that all data, including login credentials, are encrypted during the transfer. SSH and SFTP both use port 22.

4.3.B

Apply CLI commands to securely transfer files.

4.3.B.3

An SFTP session is established by connecting to a remote host or target device by entering the command `sftp <remote_username>@<remote_hostname_or_IP_address>`.

ILLUSTRATIVE EXAMPLE

To access user `panda` on location `192.168.1.15`, the command would be `sftp panda@192.168.1.15`.

To complete the SFTP connection, the user must enter the credentials. As a security feature, nothing will be displayed while typing the password.

4.3.B.4

Within an SFTP session the remote device can be navigated using CLI commands including:

- `ls` – list the contents of the current remote directory
- `cd` – change the remote directory
- `pwd` – view the current remote working directory

4.3.B.5

CLI commands to transfer files within an SFTP session include:

- `get filename` – downloads a file from the remote device to the local device
- `put filename` – uploads a file from the local device to the remote device

TOPIC 4.4

How Data Travel the Internet: Routing, Metrics, and Paths

SUGGESTED SKILLS

1.A
Identify common device and network components, protocols, and configurations, and explain processes and relationships in computer networking.

1.C
Implement and document device and network configurations to establish and maintain connectivity.

Required Course Content

LEARNING OBJECTIVE	ESSENTIAL KNOWLEDGE
4.4.A Explain how data travel between different networks.	**4.4.A.1** When addressing data to be sent, a sending host will compare its own IPv4 address and subnet mask with that of the destination host. If the destination is on a different network, the data are sent to the default gateway and must travel through one or more routers. **4.4.A.2** Network address translation (NAT) is used to allow traffic from internal devices with private IP addresses to send and receive data to and from external devices. NAT helps conserve public IP addresses and adds a layer of security. When using NAT, the default gateway replaces the source IP address in outgoing packets with the gateway's single external IP address. This allows multiple devices to share a single public IP address. **ILLUSTRATIVE EXAMPLE** A device on a local network has the private IP address 192.168.1.25 and sends data to a web server on the internet. ▪ Internal device source IP: 192.168.1.25 ▪ Router public IP: 203.0.113.10 When traffic leaves the local network, the router replaces 192.168.1.25 with 203.0.113.10. Return traffic from the web server is addressed to 203.0.113.10, and the router translates the destination back to 192.168.1.25 to deliver data to the correct device.

4.4.A

Explain how data travel between different networks.

4.4.A.3

Routers and routing-capable switches use a routing table to determine where to send packets. The table lists known networks and the best path to reach each one.

4.4.A.4

A hop occurs each time a packet is forwarded from one router to another. The first hop goes through the gateway, while additional hops pass through routers often operated by ISPs.

4.4.A.5

Once a packet reaches the destination network, the router forwards it directly to the destination device using the device's private IP address.

4.4.B

Explain how routing protocols and metrics influence the path of data.

4.4.B.1

A typical routing table entry will contain the following information:

- address and subnet mask of the destination network
- the address of the next hop
- the physical interface associated with the next hop
- the metric, which is a measure of the cost such as number of hops or time associated with the route to the next hop

4.4.B.2

Routes can be set statically, or they can be set dynamically using a routing protocol. Routing protocols determine how routers communicate and select paths for data to travel.

4.4.B.3

Dynamic routing protocols use different algorithms to choose the best path based on metrics. Metric values reflect network conditions such as distance, speed, or bandwidth. Lower metrics indicate more efficient routes.

- Routing Information Protocol (RIP) uses hop count to choose the path with the fewest routers, or hops, between the source and destination.
- Open Shortest Path First (OSPF) uses link speed and bandwidth and reroutes as needed to use the shortest path.
- Border Gateway Protocol (BGP) routes packets between large sections of the internet operated by ISPs.
- Intermediate System to Intermediate System (IS-IS) uses link state to calculate the most reliable path for data to travel.

4.4.B Explain how routing protocols and metrics influence the path of data.	4.4.B.4 When multiple next hops are available, the route with the lowest metric is chosen. Metrics can change over time based on network conditions such as congestion, device failure, or changes in link speed, which may cause data to take different paths. Different routing protocols calculate metrics in different ways.
4.4.C Determine the path of data using a routing tool.	4.4.C.1 `traceroute` (Mac/Linux) and `tracert` (Windows) are command line tools that display a packet's path from the source network to the destination network by showing the IPv4 addresses of each hop in the path. 4.4.C.2 Each line of `traceroute/tracert` output shows a hop and includes the IP address or domain name of the hop and the response time to that hop. 4.4.C.3 The output of `traceroute/tracert` can be used to count hops and identify delays and points of failure. This can help diagnose network issues and understand routing paths.

SUGGESTED SKILLS

2.B
Determine, with and without the support of AI, mitigation strategies to address device and network vulnerabilities.

2.C
Implement and document security controls to address potential vulnerabilities and monitor networks.

TOPIC 4.5

From the Inside Out: Monitoring and Defending a Large Network

Required Course Content

LEARNING OBJECTIVE	ESSENTIAL KNOWLEDGE
4.5.A Identify the impacts of common threats and vulnerabilities in a managed network.	**4.5.A.1** Unauthorized access, data exposure, or disruption of services can result from accidental or intentional misuse of systems by users. These impacts may occur when individuals access resources beyond their role, mishandle data, or fail to follow secure procedures. **4.5.A.2** Direct access to network-connected devices, data theft, or equipment tampering may occur when an unauthorized individual gains physical access to secure areas. Tactics such as tailgating, piggybacking, or theft of laptops and servers bypass physical access controls and increase the risk of internal compromise. **4.5.A.3** Widespread data compromise, service outages, or loss of administrative control can occur when an adversary or malicious software moves laterally across a network. These impacts are more likely in segmented or large networks that lack internal monitoring, access control boundaries, or containment strategies.

4.5.B

Determine appropriate security controls to limit the impacts of common threats and vulnerabilities in a managed network.

4.5.B.1

Organizations apply a combination of security controls to reduce the impact of different types of vulnerabilities. To determine appropriate security controls, administrators evaluate the likelihood and impact of specific threats and select controls that are cost-effective, scalable, and appropriate for the managed environment.

4.5.B.2

Security policies and procedures help reduce user-related vulnerabilities by defining acceptable behaviors and standardizing how systems and data are used. These controls can reduce misconfiguration, mishandling, or improper access. Common policies include:

- acceptable use policies (AUPs) that define how network resources may be used
- password and access control policies that establish strong authentication and user permission levels
- data handling guidelines for the storage, transmission, and deletion of sensitive data

4.5.B.3

Physical security controls to reduce the impact of direct access to network-connected devices include:

- installing fencing, cameras, and on-site security to deter unauthorized access
- using card readers and access control vestibules to control physical access
- locking devices in secure rooms or server cabinets
- using cable locks to secure desktop and laptop equipment
- training staff to recognize and respond to social engineering tactics

4.5.B.4

Security controls to limit the impact of unauthorized access include:

- enforcing strong password policies and account lockout settings
- applying the principle of least privilege
- implementing segmentation to restrict access between device groups and limit lateral movement
- using firewalls to block unauthorized traffic from accessing protected systems
- enabling network monitoring to detect and create alerts about suspicious activity

4.5.C

Identify indicators in intrusion detection system (IDS) or intrusion prevention system (IPS) logs that may suggest potential threats or network issues.

4.5.C.1

Regular review of IDS and IPS logs helps identify unusual or suspicious activity early, allowing for faster response to potential threats. Reviewing these logs also supports refining security policies and reducing false alerts.

4.5.C.2

IDS and IPS tools monitor and analyze network traffic for signs of suspicious or malicious behavior. IDSs monitor traffic and generate alerts if a threat is detected. IPSs inspect traffic and can take immediate action to block suspicious traffic.

4.5.C.3

IDS and IPS logs and alerts can be reviewed for indicators of security threats that suggest potential unauthorized access or malicious activity. These can include:

- repeated failed login attempts
- access attempts outside of business hours
- connections to known malicious IP addresses
- alerts for malware signatures or suspicious files
- unauthorized network scans

4.5.C.4

IDS and IPS logs and alerts can be reviewed for indicators of network performance or configuration issues. These suggest technical problems or service disruptions, not necessarily caused by an adversary, that can impact system availability and reliability. These can include:

- sudden increases in traffic volume or packet rates
- frequent packet drops or timeout errors
- misuse of protocols or unexpected service behavior
- repeated failed connections or service disruptions

4.5.D

Explain how to configure a VLAN.

4.5.D.1

VLANs improve network security and performance by logically separating devices into isolated groups, such as departments, user roles, or device types. Devices in different VLANs cannot communicate unless routing is enabled. VLANs limit broadcast traffic, reduce network congestion, and help restrict access to sensitive systems.

4.5.D

Explain how to configure a VLAN.

4.5.D.2

VLAN implementation starts with a segmentation plan that groups users or devices based on function or security level. Each VLAN is assigned a unique VLAN ID and can be named for clear identification. Devices are assigned to VLANs by connecting them to designated switch ports that are configured with the corresponding VLAN ID.

ILLUSTRATIVE EXAMPLE

A home network includes many devices and uses VLANs to segment traffic for security and performance. Devices are grouped by function, and switch ports are configured with VLAN IDs to control network access:

- VLAN 10 (ports 1–2): Home office devices, including work computers and printers
- VLAN 20 (ports 3–4): Smart and IoT devices, including thermostats, cameras, and televisions
- VLAN 30 (ports 5–6): Media devices, including game systems and a media server
- VLAN 40 (ports 7–10): Family devices, including laptops, tablets, and phones

4.5.D.3

Switch ports are configured as either access ports, which connect individual devices to a single VLAN, or trunk ports, which carry traffic from multiple VLANs between switches or routers.

4.5.D.4

VLANs are configured on a switch by creating the VLAN and assigning switch ports through the CLI or GUI. Devices connected to those ports automatically become part of the VLAN. Basic configuration of VLANs includes creating the VLAN, assigning the VLAN ID, and assigning the ports.

4.5.D.5

Devices on the same VLAN should be able to communicate; devices on different VLANs should be able to communicate only if routing is configured. Correct configuration of VLANs can be verified using tools like:

- `ping` and `traceroute` to test communication between devices
- `show vlan brief` to verify VLAN creation and port assignments

SUGGESTED SKILLS

1.A
Identify common device and network components, protocols, and configurations, and explain processes and relationships in computer networking.

3.B
Determine, with and without the support of AI, the causes of common device and network problems and determine potential solutions to solve those problems.

TOPIC 4.6

Moving Forward: Designing for Reliability and Growth

Required Course Content

LEARNING OBJECTIVE

4.6.A
Explain how IPv6 addresses support modern networks.

ESSENTIAL KNOWLEDGE

4.6.A.1
IPv6 was created to support the rapid increase in the number of internet-connected devices and to address the anticipated exhaustion of the IPv4 address space.

4.6.A.2
An IPv6 address consists of 128 bits, typically grouped as 8 hextets (groups of 16 bits) written with hexadecimal digits separated by colons. The IPv6 address space allows for 2^{128} possible addresses, allowing every device to have a globally unique and routable IP address.

ILLUSTRATIVE EXAMPLES
IPv6 addresses can be written in full or compressed formats. In the compressed format, leading zeros are removed and sequences of all-zero hextets are replaced with two colons, `::`. For example:

- 2003:AB00:CDEF:000A:0000:0000:0000:0001 → 2003:AB00:CDEF:A::1
- 2001:0DB8:0000:0000:0000:0000:0000:1234 → 2001:DB8::1234
- FE80:0000:0000:0000:01FF:FE23:4567:890A → FE80::1FF:FE23:4567:890A

4.6.A.3
IPv6 enables more efficient transmission of data than IPv4 because of simplified headers and routing processes.

4.6.B

Identify ways to improve the reliability and availability of networked systems.

4.6.B.1

Redundancy improves network reliability by ensuring backup solutions are available if a primary system fails. Common redundancy strategies include:

- implementing backup power through generators or UPS
- connecting secondary routers and switches
- deploying mobile or satellite internet during primary ISP outages
- backing up critical data regularly

4.6.B.2

Monitoring and alerting tools help ensure availability by enabling rapid detection of failures or suspicious activity.

4.6.B.3

Security controls such as firewalls, intrusion prevention systems (IPS), and access controls can reduce the risk of outages caused by attacks or misconfigurations.

4.6.B.4

Applying and documenting software updates and patches reduces the risk of failure and reduces recovery time if an outage occurs.

THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK