

# **Cybersecurity 1: Networking Fundamentals**

---

**PILOT COURSE GUIDE 2024–25**

## **Includes**

- Course Framework
- Exam Overview

THIS PAGE IS INTENTIONALLY LEFT BLANK.

# Contents

---

- v **Career Kickstart Pilot**
- vi **Acknowledgments**
- 1 **Career Kickstart Program**
- 2 **Why College Board is Developing Career Kickstart**
- 3 **Why Career and Technical Education**
- 5 **Career Kickstart Classroom Experience**
- 8 **About the Cybersecurity Pathway**
- 9 **About the Networking Fundamentals Course**
- 10 **Career Kickstart Course Development**

---

## COURSE FRAMEWORK

- 15 **Introduction**
- 16 **Course Framework Components**
- 17 **Networking Skills**
- 19 **Course Content**
- 20 **Course at a Glance**
- 23 **Unit Guides**
- 24 **Using the Unit Guides**
- 27 **UNIT 1:** Introduction to Cybersecurity and Networking
- 49 **UNIT 2:** Layers, Protocols, and Addressing
- 75 **UNIT 3:** Configuring a LAN
- 85 **UNIT 4:** Advanced LAN Topics
- 101 **UNIT 5:** Network Security

---

## EXAM OVERVIEW

- 118 **Sample Exam Questions**
- 121 **Answer Key and Question Alignment to Course Framework**

**Pilot Course Guide 2024–25**

Content will change in future versions

THIS PAGE IS INTENTIONALLY LEFT BLANK.

# Career Kickstart Pilot

---

The Advanced Placement® Program (AP®) is exploring the creation of a new careers-focused program, Career Kickstart (CK).

At its eventual launch, CK aspires to expand the successful AP model to the career and technical education (CTE) space by offering schools a new set of career-oriented high school courses that provide students with relevant, high-quality instruction and experiences that lead to industry-recognized credentials and college credit.

As part of our development process, CK is running a Pilot program: an opportunity to test our curricular framework for Networking Fundamentals, one of the courses within our Cybersecurity pathway, during the 2024–25 school year.

**We are developing key elements of all CK courses, and the Pilot represents part of the program's development phase. This Guide and the associated resources are in development and are NOT FINAL. These materials will be vetted by experienced high school teachers, higher education faculty, and industry experts. These materials will evolve thanks to the feedback collected over the Pilot years 2024–25 and 2025–26.**

# Acknowledgments

---

The CK Program would like to acknowledge the following advisors for their assistance and commitment to developing this course.

## Higher Education Advisory Committee Members

**Dane Brown**, U.S. Cyber Team Coach, Annapolis, MD  
**Jun Dai**, Worcester Polytechnic Institute, Worcester, MA  
**Jenny Daugherty**, DARK Enterprises, Inc., Lafayette, IN  
**Chance Folmar**, Front Range Community College, Westminster, CO  
**Charles Gardner**, Cyber Innovation Center, Bossier City, LA  
**Tommy Gober**, Infosec Institute, Mason, OH  
**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 Qaissaune**, Brookdale Community College, Lincroft, NJ  
**Diego Tibaquirá**, Miami Dade College, Miami, FL  
**Anthony Tsetse**, Northern Kentucky University, Highland Heights, KY

## Industry Advisory Committee Members

**Charles Banks**, U.S. Bank, Cincinnati, OH  
**Carol Kim**, IBM, New York, NY  
**Angel Piñeiro, Jr.**, CompTIA, Chicago, IL  
**Cynthia Sutherland**, Amazon Web Services, Seattle, WA

## High School Advisory Committee Members

**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  
**Moriah Walker**, Lakota Local Schools, Liberty Township, OH

## Expert Consultants

**Devin Canaday**, Equity and Access Consultant, The STEMpreneur, LLC, Chester, VA  
**Thomas Walcott**, Cybersecurity Consultant, Gambrills, MD  
**John R. Williamson**, Curriculum, Instruction, and Assessment Consultant, Eastern Kentucky University, Richmond, KY

## **Career Kickstart Cybersecurity Pathway Team**

**Ben Dougherty**, Director of IT Pathways, Cybersecurity, Career Kickstart

**Joe MacAdam**, Assessment Specialist, Career Kickstart

**James Turnage**, Assessment Specialist, Networking, Career Kickstart

## **Career Kickstart Program Team**

**Brandi Augenstein**, Director of Pilot Partnerships, Career Kickstart

**Alyssa Chudnofsky**, Senior Director of Partnerships and Course Adoption, Career Kickstart

**Brandon Dawes**, Director of Programmatic Operations, Career Kickstart

**Ellen Gluck**, Director of Assessment, Career Kickstart

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

**Rachel Haltom-Irwin**, General Manager, Career Kickstart

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

**Alessandra Hashemi**, Director of Employer Partnerships, Career Kickstart

**Jessica Johnson**, Director of Postsecondary and Workforce Connections, Career Kickstart

**Jason Locke**, Executive Director of Springboard and Pre-AP Program Operations

**Jocelyn Nguyen-Reed**, Director of Professional Learning, Career Kickstart

**Alexa Schlechter**, Director of Pilots, Career Kickstart

**Michael Warner**, Director of Research and Scale, Career Kickstart

**Mima Wellington**, Director of Ordering and Specialized Partnerships, Pre-AP Programs

**Natasha Vasavada**, Executive Director of New AP Course Development

**Abby Whitbeck**, Vice President of AP Program Strategy and Career Kickstart

THIS PAGE IS INTENTIONALLY LEFT BLANK.

# Career Kickstart Program

---

Career Kickstart (CK) is a new career-focused program that will lead to credentials and college credit for all students who want to prepare for a career, whether they are heading to 2- or 4-year colleges, technical schools, or the workforce. With a focus on high-demand fields like cybersecurity, CK will bring the best of AP to courses designed for career and technical education (CTE).

CK courses are powered by the AP features that educators value: robust professional learning for teachers, dedicated educator communities, free student resources, high-quality assessments, and the broadest national network of college credit policies.

CK offers two-course pathways that equip students for in-demand careers. Both industry experts and college faculty participate in defining the scope and sequence of the courses. Courses emphasize hands-on experience, teach professional and technical skills, and align to CTE standards and credentials valued by industry.

Over time CK plans to launch multiple pathways across several career clusters.

# Why College Board Is Developing Career Kickstart

---

College Board reaches more than 7 million students a year, helping them navigate the path from high school to college and career. Our not-for-profit membership organization was founded more than 120 years ago. We pioneered programs like the SAT® and AP® to expand opportunities for students and help them develop the skills they need. Our BigFuture® program helps students plan for college, pay for college, and explore careers.

To continue these pioneering efforts, College Board is building CK to strengthen and expand CTE education nationwide. Students demand more career exploration in high school to help them turn a passion into a profession, but many lack access to quality career-focused programs that lead to in-demand jobs. College Board launched Career Kickstart to provide a pathway for these students.

With a proven record of designing high-quality educational opportunities at scale, College Board is building CK in partnership with industry, higher education, and high school educators to assure national access to outstanding career education that today is only available in some communities.

College Board's aim is to clear a path for all students to own their future, saving students time and money on their educational journey. Career Kickstart is an important new program to meet that mission.

# Why Career and Technical Education

---

**Career and Technical Education (CTE)** is a powerful engine of opportunity. Effective CTE prepares young people and adults for good jobs in high-skill, in-demand careers.<sup>1</sup> CTE is expansive and a vital tool in efforts to narrow the skills gap, and it can be a portal to good jobs for millions across the United States:

- **Most students take a CTE course at some point during high school.** Ninety-two percent of public high school students engage in CTE learning in the classroom and on the job.<sup>2</sup>
- **Strong preparation for college and career.** Ninety-four percent of CTE students graduate high school, roughly 10% higher than the national average, and most enroll directly in college.<sup>3</sup>
- **Narrowing the skills gap.** CTE can help address the U.S.'s projected deficit of 6.5 million skilled workers, including workforce shortages in infrastructure, healthcare, and manufacturing.<sup>4</sup>
- **Access to good jobs.** CTE associate degrees can pay \$10,000 more per year than associate degrees in other fields – and can even pay more than bachelor's degrees – while limiting student debt.<sup>5</sup>

---

#### Sources:

1. Content and sources in this section derived from Association for Career and Technical Education, "What is Career and Technical Education?," (February, 2022), accessed May 27, 2024, [https://www.acteonline.org/wp-content/uploads/2022/03/ACTE\\_What\\_is\\_CTE\\_Infographic\\_February2022-2.pdf](https://www.acteonline.org/wp-content/uploads/2022/03/ACTE_What_is_CTE_Infographic_February2022-2.pdf)
2. U.S. Department of Education, Institute of Education Sciences, National Center for Education Statistics (NCES), High School Longitudinal Study of 2009 (HSLS:09), Base-year, 2013 Update, and High School Transcript File; U.S. Department of Education, National Center for Education Statistics, 2015–16 National Postsecondary Student Aid Study (NPSAS:16).
3. U.S. Department of Education, "Bridging the Skills Gap; Career and Technical Education in High School," (September 2019), accessed May 30, 2023, <https://www2.ed.gov/datalstory/cte/index.html>. Information on CTE graduation compared to the national average from <https://www.usnews.com/education/k12/articles/the-benefits-of-career-and-technical-education-programs-for-high-schoolers>
4. Construction Industry Resources as cited in Madeline Ngo, "Skilled workers are scarce, posing a challenge for Biden's 'infrastructure plan,'" New York Times, (September 9, 2021, updated November 6, 2021); Korn Ferry, "Future of work, The global talent crunch," (2018); Rainer Strack, Miguel Carrasco, Philipp Kolo, Nicholas Nouri, Michael Priddis, and Richard George, "The future of jobs in the era of AI," Boston Consulting Group (2021), Paul Wellener, Victor Reyes, Heather Ashton, and Chad Moutray, "Creating pathways for tomorrow's workforce today," Deloitte (2021).
5. Georgetown University Center on Education and the Workforce, "The overlooked value of certificates and associate's degrees: What students need to know before they go to college," (2020); Mark Schneider, "Higher Education Pays," CollegeMeasures.org (2013); College Board, Annual Survey of Colleges (2022); NCES, IPEDS Fall 2020 Enrollment data and IPEDS 2020 Institutional Characteristics data.

To build on these strengths, College Board aims to expand access to quality career pathways and is excited to do so in partnership with the CTE community. College Board comes to this space humbly, but with scale, expertise, and a proven track record:

- **Widespread access.** Nine out of 10 high school seniors are at a school with AP courses. 34.6% of 2022 U.S. public high school graduates took at least one AP Exam during high school.<sup>6</sup>
- **Expanding the teacher pipeline.** AP Computer Science Principles (CSP) increased the number of teachers teaching AP CSP nationally from 2,700 to 7,000 over a 5-year span (2016–22).<sup>7</sup>
- **Post-secondary success.** Completing an AP course is associated with a range of positive student outcomes including greater likelihood of enrollment and completion of college.<sup>8</sup>

---

6. College Board, "AP Program Results, Class of 2022," Accessed June 4, 2024, <https://reports.collegeboard.org/ap-program-results/class-of-2022>

7. Education Writers Association, "CTE Explainer," Accessed June 4, 2024, <https://ewa.org/issues/career-technical-education/cte-career-and-technical-education-explainer>

8. College Board, "AP Students in College: A Review of Key Research," Accessed June 4, 2024. <https://apcentral.collegeboard.org/media/pdf/ap-students-in-college.pdf>

# Career Kickstart Classroom Experience

---

CK classes are designed to offer an applied, inclusive classroom experience focused on career connections, and to provide teachers the resources they need.

## Engaging and Preparing Students

**Applied learning.** Students build the skills they need to solve problems rooted in authentic job-related scenarios.

- *Focused on problem-solving and applied learning* CK students learn by investigating and solving authentic problems and by transferring their emerging understanding to new situations. This productive struggle can increase student understanding, support students who have faced academic challenges, and increase teacher job satisfaction.<sup>1</sup>
- *Teaches Professional and Technical skills* Professional skills – such as communication, collaboration, and critical thinking – represent seven out of the ten top skills mentioned in career and technical field job postings.<sup>2</sup> CK course content is aligned to industry expectations for both professional and technical skills and students have ongoing opportunities to develop both sets of skills in tandem throughout their course experience.

**Career connections.** Students learn to understand the field and to develop the skills and interests required to be successful.

- *Relevant to workforce needs* CK is focused on developing CTE course pathways that connect to high-growth, in-demand jobs in fast-growing career clusters.<sup>3</sup> CK is co-creating courses with industry experts to ensure that students build the skills they need to succeed on the job.
- *Aligned to credentials and opportunities for college credit* To build on the increasing focus of colleges and universities on “stackable” credentials, CK courses are designed to align with industry-recognized certifications and

---

### Sources:

1. Buck Institute for Education, “Research Summary: PBL and 21st Century Competencies,” (2013), accessed May 27, 2024, [https://pblworks.org/sites/default/files/2019-01/FreeBIE\\_Research\\_Summary.pdf](https://pblworks.org/sites/default/files/2019-01/FreeBIE_Research_Summary.pdf).
2. America Succeeds, “The High Demand for Durable Skills,” (October, 2021), accessed May 27, 2024, [https://mcusercontent.com/9a1ab6cad8fd1f7312ec7cba5/files/e85c8be0-4f42-fa5a-da78-713bb4bff4ea/The\\_High\\_Demand\\_for\\_Durable\\_Skills.pdf](https://mcusercontent.com/9a1ab6cad8fd1f7312ec7cba5/files/e85c8be0-4f42-fa5a-da78-713bb4bff4ea/The_High_Demand_for_Durable_Skills.pdf) from <https://americasucceeds.org/policy-priorities/durable-skills>.
3. National Association of State Directors of Career Technical Education Consortium, “Career Technical Education and Labor Market Demand,” Career Technical Education Consortium (2011), accessed May 27, 2024, <https://www2.ed.gov/datastory/cte/index.html>.

qualify students for college credit.<sup>4</sup> (Please note that students participating in the Pilot program in 2024–25 will not have the opportunity to qualify for college credit.)

- *Embedded with Work-Based Learning (WBL) opportunities* Many employers report that typical high school and college graduates lack the right skills.<sup>5,6</sup> WBL can help decrease the skills gap by connecting students to positive relationships with professionals, expanded social capital, and authentic work experiences.<sup>7</sup> CK courses encourage students to engage with industry professionals and build relationships with industry organizations.

**Inclusive for all students.** Students can meaningfully engage with content regardless of background with appropriate context and scaffolds. Students feel welcome in their learning environments.

- *Eliminates barriers to student success* CK eliminates unnecessary prerequisites and other barriers that can otherwise prevent motivated students from succeeding. Courses are designed to support students no matter their prior content knowledge or academic skills.<sup>8</sup>
- *Support for learners, teachers, and schools everywhere* CK courses are designed to increase equitable access and success through scaffolded lessons vetted by equity experts; offer pedagogy and instructional activities that support teachers of different experience levels; and provide resources and training opportunities built to help schools implement and expand their CTE offerings.<sup>9,10</sup>

- 
4. Center for Occupational Research and Development in partnership with Social Policy Research Associates, *Introduction to Stackable Credentials*, OCTAE Program Memorandum 21-1 (January, 2021), accessed May 27, 2024, <https://s3.amazonaws.com/PCRN/file/introduction-to-stackable-credentials.pdf>.
  5. Business Roundtable, "Work in Progress: How CEOs Are Helping Close America's Skills Gap," (June 2017), accessed May 27, 2024, [https://s3.amazonaws.com/brt.org/BRT-SkillsGap201711012017\(1\).pdf](https://s3.amazonaws.com/brt.org/BRT-SkillsGap201711012017(1).pdf).
  6. National Association of Colleges and Employers, "Job Outlook 2022," (November, 2023), accessed May 27, 2024, <https://www.naceweb.org/docs/default-source/default-document-library/2023/publication/research-report/2024-nace-job-outlook.pdf>.
  7. Martha Ross, Richard Kazis, Nicole Bateman, and Laura Stateder, *Work-Based Learning Can Advance Equity and Opportunity for America's Young People*, Metropolitan Policy Program at Brookings (November, 2020), accessed May 27, 2024, [https://www.brookings.edu/wp-content/uploads/2020/11/20201120\\_BrookingsMetro\\_Work-based-learning\\_Final\\_Report.pdf](https://www.brookings.edu/wp-content/uploads/2020/11/20201120_BrookingsMetro_Work-based-learning_Final_Report.pdf).
  8. John M. Bridgeland, John J. Dilulio, Jr., and Karen Burke Morison, "The Silent Epidemic: Perspectives of High School Dropouts," Civic Enterprises in association with Peter D. Hart Research Associates for the Bill & Melinda Gates Foundation (March, 2006), accessed May 27, 2024, <https://files.eric.ed.gov/fulltext/ED513444.pdf>.
  9. Sean F. Reardon, "The Widening Academic Achievement Gap Between the Rich and the Poor: New Evidence and Possible Explanations," in Whither Opportunity? Rising Inequality, Schools, and Children's Life Chances, eds. Greg J. Duncan and Richard J. Murnane, (New York, NY: Russell Sage Foundation (2011), accessed May 27, 2024, <https://cepala.stanford.edu/sites/default/files/reardon%20whither%20opportunity%20-%20chapter%205.pdf>.
  10. Melissa S. Kearney and Phillip B. Levine, "Income inequality, social mobility, and the decision to drop out of high school" Brookings Papers on Economic Activity (March, 2016), accessed May 27, 2024, <https://www.brookings.edu/bpea-articles/income-inequality-social-mobility-and-the-decision-to-drop-out-of-high-school/>.

## Resources for Teachers

CK courses offer robust support materials for teachers including:

- Course framework outlining the essential knowledge and learning objectives for each course, with pacing suggestions, emphasizing both the technical and professional skills needed in industry.
- Sample lesson plans aligned to the course frameworks, utilizing applied and career-connected pedagogy.
- Five-day summer training on course content, lesson development, and delivery.
- Monthly professional learning opportunities during the school year.
- Online teacher community to share best practices with 150+ Cybersecurity teachers.

# About the Cybersecurity Pathway

---

Cybersecurity is a high-growth field with entry-level jobs that pay well and don't require a 4-year degree. There are currently more than 500,000 open cybersecurity jobs across the country, but less than 2% of high school students have access to cybersecurity pathways.<sup>1</sup>

The 2-year-long courses in the CK Cybersecurity Pathway – first Cybersecurity 1: Networking Fundamentals and then the Cybersecurity 2: Cybersecurity Fundamentals course – are designed to provide students with stackable credentials that can apply to entry-level jobs and to college, and to help connect them to jobs that provide good salaries in this in-demand, high-growth industry.

After demonstrating competency through CK cybersecurity coursework, students have multiple options to continue their career development:

- Go directly into the workforce or secure an apprenticeship
- Continue progress toward taking common industry certifications including CompTIA Network+, Cisco Certified Networking Associate (CCNA), Cisco Certified Support Technician (CCST): Networking, CompTIA Security+, and Cisco Certified Support Technician (CCST): Cybersecurity
- Apply college credits to a relevant community college degree or certificate program
- Apply college credits to a relevant 4-year degree

Several early-career jobs associated with the cybersecurity pathway do not require a college degree and pay median salaries in the range of \$62,000 to \$137,000, including:<sup>2</sup>

- Cloud Architect
- Cyber Crime Investigator
- Cyber Defense Incident Responder
- Cyber Ops Planner
- System Testing and Evaluation Specialist
- Systems Administrator
- Vulnerability Assessment Analyst

---

## Sources:

1. Cyberseek.org, "Cybersecurity Supply/Demand Heatmap," accessed May 27, 2024, <https://www.cyberseek.org/heatmap.html>.
2. Cyber.org, "Cyber Career Profiles," accessed May 27, 2024, <https://cyber.org/career-exploration/cyber-career-profiles>.

# About the Networking Fundamentals Course

---

## Description

The first course in the Cybersecurity Pathway, Cybersecurity 1: Networking Fundamentals is a full-year high school course that covers the fundamentals of networking. It is equivalent to a college-level Introduction to Networking course. The course interweaves essential networking concepts with relevant, hands-on problem-solving activities to maximize students' understanding of network hardware and configuration, the use of protocols to enable reliable and accurate transmission of data between different hosts around the world, and relevant security practices that secure the transmission of data both within and between computer networks.

## College Course Equivalent

CK Networking Fundamentals is designed to be the equivalent of a 3-credit course taken in the first or second year of a college cybersecurity degree or certificate program. Developed in partnership with higher education faculty, this course meets all of the requirements necessary to earn college credit. (*Please note that students participating in the Pilot program in 2024–25 will not have the opportunity to qualify for college credit.*)

## Certification

CK Networking Fundamentals is designed to help students develop understanding and skills that will contribute to their ability to pass widely recognized professional cybersecurity certifications such as CompTIA Network+, Cisco Certified Network Associate (CCNA), and Cisco Certified Support Technician (CCST): Networking.

# Career Kickstart Course Development

---

Based on best practices in industry, K-12 education, and college-level CTE programs, CK follows an intentional process to ensure that the skills and knowledge students develop in CK courses align with higher education and industry expectations. CK courses are developed through extensive consultation with faculty and industry experts.

## Cybersecurity 1: Networking Fundamentals Course Development Timeline

- **October 2023–April 2024:** Advisory boards made up of college faculty, high school educators, and industry experts help develop and refine the CK Networking Fundamentals Course Framework and other course resources.
- **May–July 2024:** Pilot Guide, end-of-year assessment, and other course resources are reviewed and further refined with college faculty, high school educators, and industry experts.
- **July 15–19, 2024:** Cybersecurity 1 Pilot teachers from approximately 120 high schools participate in CK Summer Institute and provide feedback. At the same time and location, teachers from approximately 30 high schools will participate in the Summer Institute as part of the Pilot of the second course in the pathway, Cybersecurity 2: Cybersecurity Fundamentals.
- **August 2024–May 2025:** Pilot teachers use CK resources, including the Pilot framework and select lesson plans for Networking Fundamentals, and provide feedback.
- **April–May 2025:** Assessment administration and completion of first Pilot year for both Cybersecurity courses.
- **August–September 2025:** Teachers again teach Cybersecurity 1 and Cybersecurity 2 in schools nationwide in a second Pilot year.
- **May 2026:** Assessment administration and completion of second Pilot year for both Cybersecurity courses.

## Pilot Course Overview (2024–25)

CK's Pilot program asks experienced cybersecurity teachers to sign-on as thought partners to the course development. They will put the new framework into practice in the 2024–25 school year and will provide regular feedback and data to assist in gauging the teachability and efficacy of the course and opportunities for strengthening in 2025–26.

From these experienced instructors, CK aims to answer the following questions:

- **Teacher Supports:** Do the CK course framework, CK Summer Institute professional learning and additional resources for teachers together enable effective teaching? What more is needed?
- **Student Outcomes:** Do the scope and sequence of the CK framework effectively engage students and facilitate the intended learning outcomes? What more is needed?
- **End-of-Year Assessment:** What is needed to ensure valid assessment and project-based learning at scale for the two courses in the Cybersecurity pathway so that each course provides authentic, impactful learning for students, articulates to college credit, and aligns with leading industry-recognized credentials?

During the Pilot year, participating teachers will provide feedback on which elements work, which need improvement, and what new elements should be added.

This feedback and partnership will inform a succeeding pilot of the course, which will include teachers new to the CK Networking Fundamentals content area in addition to experienced teachers.

## Equity and Access

The CK program prioritizes equitable access to high-quality CTE programming for all students. Our aim is to foster environments that empower students to bring their authentic selves to the learning process. Students bring unique perspectives gained from various lived experiences, such as ethnic, racial, socioeconomic, and learning differences; such perspectives enrich the CK classroom environment. CK courses welcome students from all backgrounds. CK seeks to remove as many barriers as possible that would otherwise limit access to high-quality CTE opportunities for students.

Throughout the Pilot year, we will collaborate with teachers, administrators, and students to understand how best to encourage and enable a wide range of students to succeed in CK courses.

THIS PAGE IS INTENTIONALLY LEFT BLANK.

**CK NETWORKING FUNDAMENTALS**

---

# Course Framework



# Introduction

---

Networking involves hardware, software, problem-solving, and systems that are the basis for so much of contemporary life. The Networking Fundamentals course strives to teach students essential skills and modes of thinking, by allowing them to develop professional skills and understanding through rewarding and challenging concepts and experiences.

Networking Fundamentals is often the first course in a high school pathway that can lead students to a

well-compensated career path in an in-demand industry. A well-designed, contemporary Networking Fundamentals course that includes opportunities for students to collaborate on real-world problems can support career readiness and help ensure equity, access, and success. Such a course can broaden participation in related industries by providing a strong and engaging introduction to the discipline.

# Course Framework Components

---

## Overview

This course framework provides a description of what students should know and be able to do to qualify for college credit or placement.

### The course framework includes two essential components:

#### **1 NETWORKING SKILLS**

These skills are central to the study and practice of Networking. Students should practice and build these skills on a regular basis over the span of the course.

#### **2 COURSE CONTENT**

The course content is organized into five units of study that provide a suggested sequence for the course. These units comprise the content and conceptual understandings that college faculty typically expect students to master to qualify for college credit and/or placement. Each unit is composed of a variety of Topics, which are further broken down into both Learning Objectives – what a student must be able to know and do after learning the topic – and Essential Knowledge statements – the content knowledge needed to demonstrate mastery of the learning objective. The course helps develop student understanding by spiraling overarching core concepts throughout the units.

## **CK NETWORKING FUNDAMENTALS**

# **Networking Skills**

---

The following table presents skills that students should develop during the Networking Fundamentals course. These skills form the basis of tasks students will encounter in the professional realm.

# CK Networking Fundamentals

## Networking Skills

| Skill 1   | Skill 2   | Skill 3   |
|---|---|---|
| <i>Explain networking and cybersecurity concepts.</i>   | <i>Design a secure network.</i>   | <i>Configure a secure network.</i>  |
| <b>1.A</b> Describe and explain concepts and processes related to data, computer networking, and cybersecurity.<br><br><b>1.B</b> Explain relationships among data, computer networking, and cybersecurity. | <b>2.A</b> Determine appropriate endpoints, network appliances, transmission media, and communication protocols to meet network requirements.<br><br><b>2.B</b> Determine security controls that address potential vulnerabilities. | <b>3.A</b> Connect and configure network components using appropriate media, communication protocols, and commands.<br><br><b>3.B</b> Test network connectivity, verify network requirements, and troubleshoot network issues.<br><br><b>3.C</b> Create technical documentation of network layouts, settings, and configurations. |

## Professional Skills

Professional skills such as communication, collaboration, and critical thinking are highly sought by employers hiring for positions within information technology related fields. **The table below includes a draft overview of professional skills for this CK course; in future versions of the framework this table will be revised and the professional skills will be integrated.**

| Skill 1  | Skill 2   | Skill 3  |
|--|---|--|
| <b>COMMUNICATION</b><br><i>Communicate technical information to both technical and non-technical audiences.</i>  | <b>PROBLEM-SOLVING</b><br><i>Use a methodology to solve complex problems.</i>   | <b>COLLABORATION</b><br><i>Effectively collaborate with a team to meet a shared goal.</i>  |
| <b>1.A</b> Identify the purpose of the communication.<br><br><b>1.B</b> Synthesize relevant information from multiple sources.<br><br><b>1.C</b> Distill, tailor, and contextualize content for a specific audience.<br><br><b>1.D</b> Share information in a form that meets the needs of a specific audience or setting (e.g., verbal, written, or presentation form). | <b>2.A</b> Identify and define the problem.<br><br><b>2.B</b> Identify and evaluate potential root cause(s).<br><br><b>2.C</b> Identify and evaluate potential solutions.<br><br><b>2.D</b> Implement and justify a best solution.<br><br><b>2.E</b> Evaluate the outcome of the solution and iterate, if necessary.<br><br><b>2.F</b> Document and reflect upon the process and outcome. | <b>3.A</b> Use strategies to build trust and rapport with members of the team.<br><br><b>3.B</b> Develop clear, shared team objectives.<br><br><b>3.C</b> Define clear roles and responsibilities for members of the team.<br><br><b>3.D</b> Use strategies to leverage the diverse opinions and individual strengths of team members.<br><br><b>3.E</b> Use strategies to resolve conflicts and differences of opinions among team members.<br><br><b>3.F</b> Follow through on agreed-upon deliverables. |

## Course Content

This course framework describes the course requirements necessary for student success, with a focus on the overarching concepts and processes of the discipline. The framework also encourages instruction that prepares students for advanced information technology coursework and its use in a wide array of fields.

The following four overarching concepts are threads that run throughout the course. They help students to create meaningful connections across units and topics and will help students to develop deeper conceptual understanding as they revisit and apply these concepts.

### HARDWARE & CONFIGURATION

The backbone of any network is the hardware that runs it. Hardware is the physical infrastructure that enables communication and data transfer between devices. Without this hardware, computers have no means of accessing a network. Network hardware includes network interface cards (NICs), hubs, switches, routers, modems, and cabling or wireless access points. Networks are set up by physically connecting hardware and configuring settings.

### OSI MODEL

The Open Systems Interconnection (OSI) model is a framework for understanding how networking communication systems work. OSI consists of seven layers: physical, data link, network, transport, session, presentation, and application. The model is important because it allows for standardization of the framework for designing and understanding communication systems. This modularity allows for easier development and maintenance of computer systems, interoperability that ensures different devices and networks can communicate with each other, and a structured approach to troubleshooting problems by isolating issues and identifying root causes.

### PROTOCOLS

Network protocols are established sets of rules built into devices' software and hardware that determine how data are transmitted between different devices. Protocols make it possible for devices to interact with each other across LANs (local area networks) and WANs (wide area networks) regardless of differences in their internal processes, structure, or design. Protocols are often created by information technology organizations to reflect industry standards.

### SECURITY

With so many everyday tasks being conducted online today, it is imperative that data are stored, sent, and received securely. Network security is the subset of cybersecurity that is concerned with keeping data secure when moving within and between networks. This may include keeping system software up-to-date, using secure passwords, or implementing a firewall on a host or in a network to prevent unauthorized access to computer networks that hold sensitive data.

# Course at a Glance

## Plan

Course at a Glance provides a useful visual organization of the CK Networking Fundamentals curricular components, including the following:

- Sequence of units, along with suggested pacing, based on 45-minute class periods, meeting five days each week for a full academic year.
- Progression of topics within each unit.

## Teach

### CYBERSECURITY SKILLS

- Explain networking and cybersecurity concepts.
- Design a secure network.
- Configure a secure network.

The individual topic pages will show all the suggested skills.

### Expected number of class periods

Total: 92–140 Class Periods

| UNIT 1                   |            | Introduction to Cybersecurity and Networking |  |
|--------------------------|------------|--|--|
| Suggested Pacing* Topics |            | 22–30 Class Periods                          |  |
| <b>1</b>                 | <b>1.1</b> | <b>Introduction to Cybersecurity</b>         |  |
| <b>1</b>                 | <b>2</b>   | <b>Personal Digital Security</b>             |  |
| <b>1</b>                 | <b>2</b>   | <b>Enterprise Security</b>                   |  |
| <b>1</b>                 | <b>1.4</b> | <b>Introduction to Computer Systems</b>      |  |
| <b>1</b>                 | <b>1.5</b> | <b>Introduction to Command Line</b>          |  |
| <b>1</b>                 | <b>1.6</b> | <b>Introduction to Networks</b>              |  |
| <b>1</b>                 | <b>2</b>   | <b>SOHO vs. Enterprise Networks</b>          |  |
| UNIT 2                   |            | Layers, Protocols, and Addressing            |  |
| Suggested Pacing* Topics |            | 18–31 Class Periods                          |  |
| <b>1</b>                 | <b>2.1</b> | <b>OSI and TCP/IP Models</b>                 |  |
| <b>1</b>                 | <b>2</b>   | <b>Introduction to Protocols and Servers</b> |  |
| <b>1</b>                 | <b>3</b>   | <b>Cabling</b>                               |  |
| <b>1</b>                 | <b>3</b>   | <b>Network Topologies</b>                    |  |
| <b>1</b>                 | <b>2.5</b> | <b>Physical Addressing</b>                   |  |
| <b>1</b>                 | <b>2.6</b> | <b>Logical Addressing</b>                    |  |
| <b>1</b>                 | <b>2</b>   | <b>IP Configuration</b>                      |  |
| <b>1</b>                 | <b>3</b>   |  |  |

**UNIT  
3****Configuring a LAN**

Suggested Pacing\* Topics

**14–21** Class Periods**1** 3.1 Switching**1** 3.2 Switch Security**1** 3.3 More on Protocols**1** 3.4 LAN Configuration and Troubleshooting**UNIT  
4****Advanced LAN Topics**

Suggested Pacing\* Topics

**21–28** Class Periods**1** 4.1 IPv4 Addressing**1** 4.2 Routing**1** 4.3 Subnetting**1** 4.4 Wireless Networks**2** 4.5 Network Troubleshooting**UNIT  
5****Network Security**

Suggested Pacing\* Topics

**17–30** Class Periods**1** 5.1 Introduction to Security Controls**1** 5.2 Physical and Administrative Controls**1** 5.3 Technical Controls: Firewalls**1** 5.4 Technical Controls: Network Segmentation**1** 5.5 Technical Controls: Network Monitoring**1** 5.6 Defense in Depth

\*Based on 45-minute class periods

THIS PAGE IS INTENTIONALLY LEFT BLANK.

## **CK NETWORKING FUNDAMENTALS**

# **Unit Guides**

---

Designed with input from the community of cybersecurity educators and industry experts, the unit guides offer teachers guidance in building students' skills and knowledge. The Pilot sequence was identified through multi-round consultation with college instructors, high school teachers, and industry experts and is intended to enhance student engagement by giving regular opportunities for authentic, hands-on experiences. Each unit also features at least one fully developed lesson plan that was written with student engagement, instructional value, and accessibility for a diverse set of learners in mind. Pilot participants will test these lessons in their classrooms and provide the CK team with feedback to improve upon the teacher resources for this course.

## Using the Unit Guides

UNIT 1 ~22-30 45-MINUTE CLASS PERIODS

### Introduction to Cybersecurity and Networking

**KEY QUESTIONS**

- Is it true that a cyber attack can disrupt my access to clean water?
- How do I protect my own personal information?
- How can photos, music and movies be represented as only 0s and 1s?

**UNIT OBJECTIVES**

By the end of this unit, students should be able to:

- Practice good cyber hygiene
- Navigate a file system using a command line interface (CLI)

**Developing Understanding**

Understanding the basic components of computer networks and digital communication is essential to making good decisions about a network's design and configuration. In this early stage, the focus is on developing networking literacy. Role-playing activities and thoughtful questioning can help students develop intuitions about the needs for specific network hardware and configurations as well as the challenges that can arise when transmitting digital information.

**Building Networking Skills**

Understanding the basic components of computer networks and digital communication is essential to making good decisions about a network's design and configuration. In this early stage, the focus is on developing networking literacy. Role-playing activities and thoughtful questioning can help students develop intuitions about the needs for specific network hardware and configurations as well as the challenges that can arise when transmitting digital information.

CK Cybersecurity 1: Networking Fundamentals      Pilot Course Guide 2024-25 | V.1 Course Framework | 29

### UNIT OPENERS

**Key Questions** motivate students and inspire inquiry.

**Unit Objectives** outline key skills and knowledge that students will gain through the content and activities of the given unit.

**Developing Understanding** provides an overview that contextualizes and situates the key content of the unit within the scope of the course.

**Building Networking Skills** describe specific sub-skills within the course skills that are appropriate to focus on in that unit.

UNIT 1 Introduction to Cybersecurity and Networking

### UNIT AT A GLANCE

| Topic                                | Learning Objectives  | Suggested Instructional Periods |                 |
|--------------------------------------|--|---------------------------------|-----------------|
|                                      |  | Teach & Labs                    | Review & Assess |
| 1.1 Introduction to Cybersecurity    | <b>1.1.A</b> Describe the impacts of cybersecurity on individuals, organizations, governments, and critical infrastructure.<br><b>1.1.B</b> Describe the foundational concepts of confidentiality, integrity, and availability in cybersecurity.   | 2-3                             | 0               |
| 1.2 Personal Digital Security        | <b>1.2.A</b> Explain how an individual can limit the risk of identity theft, credit card fraud, and stolen login credentials.<br><b>1.2.B</b> Apply password security practices that can prevent an unauthorized user from accessing an individual's online accounts.<br><b>1.2.C</b> Explain how practicing secure software behaviors can protect an individual's data. | 2-3                             | 1               |
| 1.3 Enterprise Security              | <b>1.3.A</b> Explain how personal digital security is different from enterprise security.<br><b>1.3.B</b> Explain how the state and classification of data impact the security controls an organization implements.  | 2                               | 1               |
| 1.4 Introduction to Computer Systems | <b>1.4.A</b> Explain how the hardware components of a computer system function.<br><b>1.4.B</b> Explain how key software programs allow a computer system to perform specific functions.<br><b>1.4.C</b> Describe the benefits of using virtualization in a computer system.   | 3-4                             | 1               |
| 1.5 Introduction to Command Line     | <b>1.5.A</b> Describe the characteristics of Windows and Linux file systems.<br><b>1.5.B</b> Apply appropriate commands using the command line interface (CLI) to navigate a file system.  | 3-5                             | 1               |

30 | Course Framework V.1 | Pilot Course Guide 2024-25      CK Cybersecurity 1: Networking Fundamentals

**Unit at a Glance** shows the Topics, Learning Objectives, and suggested number of instructional periods to cover each Topic in class.

**Suggested Instructional Periods** include a proposed number of classes to cover each Topic. Two numbers are given: first, a suggested range of classes reserved for direct instruction and labs; second, a suggested range of classes to allocate to review and assessment.

# Using the Unit Guides

The screenshot shows the 'Topic 1.2 Personal Digital Security' page. At the top left is the 'UNIT 1' logo. Below it, under 'SUGGESTED SKILLS:', there are two items: 'Explain relationships among data, computer networking, and cybersecurity.' and 'Determine security controls that address potential vulnerabilities.' To the right, under 'TOPIC 1.2 Personal Digital Security', is a large blue arrow pointing down to the 'LEARNING OBJECTIVE' and 'ESSENTIAL KNOWLEDGE' sections. The 'LEARNING OBJECTIVE' section contains one item: 'LO-1.2.A Explain how an individual can limit the risk of identity theft, credit card fraud, and stolen login credentials.' The 'ESSENTIAL KNOWLEDGE' section contains five items, each with a sub-item: 'EK-1.2.A.1 Individuals can reduce the risk of identity theft and unwanted tracking by limiting the sharing of personal information on public websites, such as photos, location tags, and names, and dates of special events are often used to verify identity for doing personal and sensitive business, so when adversaries (also referred to as threat actors or attackers) have this information, they may try to impersonate another individual.'; 'EK-1.2.A.2 Using secure Internet connections when sending sensitive information can help prevent negative outcomes, such as identity theft, credit card fraud, stolen login credentials; Illustrative Example: Using virtual private networks (VPNs) while on public Wi-Fi'; 'EK-1.2.A.3 Being cautious about emails and messages from unknown senders can prevent a phishing attack. Phishing attacks often involve malicious links or downloads that can contain malware (malicious software) or trick a person into sharing sensitive information such as account login credentials.'; 'EK-1.2.A.4 Applying strong passwords, such as those with adequate length and a combination of uppercase, lowercase, numeric, and symbolic characters, makes it more difficult for an adversary to crack a user's password.'; and 'EK-1.2.A.5 Using a different password for each online account prevents an adversary from being able to reuse a compromised password to access additional online accounts. Updating online passwords at regular intervals ensures that if an adversary finds an old password, it is no longer useful.' At the bottom of the page, there is a note: 'continued on next page' and 'CK Cybersecurity 1: Networking Fundamentals'.

## TOPIC PAGES

**Suggested Skills** offer one or more recommended sub-skills to pair with the topic.

**Learning Objectives** define what a student should be able to do with content knowledge.

**Essential Knowledge** statements describe the knowledge required to perform the learning objective.

The screenshot shows the 'Sample Exam Questions' page. At the top left is the 'UNIT 1' logo. Below it, under 'TOPIC 1.2 Personal Digital Security', is a large blue arrow pointing down to the 'Sample Exam Questions' section. The section title is 'Sample Exam Questions'. Below the title is a note: 'The sample exam questions that follow illustrate the relationship between the course framework and the CK Cybersecurity 1: Networking Fundamentals Exam and serve as examples of the types of questions that may appear on the Pilot Year 1 Exam (school year 2024–2025). After the sample questions, you will find a table that shows the correct answers and the learning objectives to which each question relates.' Under the note is a heading 'Multiple-Choice Questions' followed by two numbered questions. Question 1 asks about protecting credit card information during an online purchase. Question 2 asks about bypassing a network's perimeter firewall. At the bottom of the page, there is a note: '118 | Exam Overview V.1 | Pilot Course Guide 2024-25' and 'CK Cybersecurity 1: Networking Fundamentals'.

## EXAM OVERVIEW

**Sample Exam Questions** serve as examples of the types of questions that may appear on the Pilot Year 1 Exam (school year 2024–25).

THIS PAGE IS INTENTIONALLY LEFT BLANK.

## **CK NETWORKING FUNDAMENTALS**

### **UNIT 1**

# **Introduction to Cybersecurity and Networking**

THIS PAGE IS INTENTIONALLY LEFT BLANK.

# Introduction to Cybersecurity and Networking



## KEY QUESTIONS

- Is it true that a cyber attack can disrupt my access to clean water?
- How do I protect my own personal information?
- How can photos, music and movies be represented as only 0s and 1s?

## UNIT OBJECTIVES

By the end of this unit, students should be able to:

- Practice good cyber hygiene
- Navigate a file system using a command line interface (CLI)

## Developing Understanding

Unit 1 introduces students to the concept of networking and lays the foundation upon which the rest of the course rests. Students will learn the fundamentals of cybersecurity and the difference between personal and enterprise security. Students will learn about the elements of computers and how hardware and software work together to make a computer perform familiar functions. Students will be introduced to the command line interface (CLI). Students will learn what a computer network is and how scale impacts networks.

## Building Networking Skills

Understanding the basic components of computer networks and digital communication is essential to making good decisions about a network's design and configuration. In this early stage, the focus is on developing networking literacy. Role-playing activities and thoughtful questioning can help students develop intuitions about the needs for specific network hardware and configurations as well as the challenges that can arise when transmitting digital information.

**UNIT AT A GLANCE**

| <b>Topic</b>                                | <b>Learning Objectives</b>   | <b>Suggested Instructional Periods</b> |                            |
|---|--|--|----------------------------|
|   |  | <b>Teach &amp; Labs</b>                | <b>Review &amp; Assess</b> |
| <b>1.1 Introduction to Cybersecurity</b>    | <b>1.1.A</b> Describe the impacts of cybersecurity on individuals, organizations, governments, and critical infrastructure.<br><b>1.1.B</b> Describe the foundational concepts of confidentiality, integrity, and availability in cybersecurity.   | 2–3                                    | 0                          |
| <b>1.2 Personal Digital Security</b>        | <b>1.2.A</b> Explain how an individual can limit the risk of identity theft, credit card fraud, and stolen login credentials.<br><b>1.2.B</b> Apply password security practices that can prevent an unauthorized user from accessing an individual's online accounts.<br><b>1.2.C</b> Explain how practicing secure software behaviors can protect an individual's data. | 2–3                                    | 1                          |
| <b>1.3 Enterprise Security</b>              | <b>1.3.A</b> Explain how personal digital security is different from enterprise security.<br><b>1.3.B</b> Explain how the state and classification of data impact the security controls an organization implements.  | 2                                      | 1                          |
| <b>1.4 Introduction to Computer Systems</b> | <b>1.4.A</b> Explain how the hardware components of a computer system function.<br><b>1.4.B</b> Explain how key software programs allow a computer system to perform specific functions.<br><b>1.4.C</b> Describe the benefits of using virtualization in a computer system.   | 3–4                                    | 1                          |
| <b>1.5 Introduction to Command Line</b>     | <b>1.5.A</b> Describe the characteristics of Windows and Linux file systems.<br><b>1.5.B</b> Apply appropriate commands using the command line interface (CLI) to navigate a file system.  | 3–5                                    | 1                          |

## Introduction to Cybersecurity and Networking

| <b>Topic</b>                            | <b>Learning Objectives</b>   | <b>Suggested Instructional Periods</b> |                            |
|---|--|--|----------------------------|
|   |  | <b>Teach &amp; Labs</b>                | <b>Review &amp; Assess</b> |
| <b>1.6 Introduction to Networks</b>     | <b>1.6.A</b> Describe the characteristics of computer networks.<br><b>1.6.B</b> Explain how computers transmit digital communications.<br><b>1.6.C</b> Convert a number between decimal and binary.<br><b>1.6.D</b> Describe the primary types of networks defined by geographical size. | 3–4                                    | 0–1                        |
| <b>1.7 SOHO vs. Enterprise Networks</b> | <b>1.7.A</b> Explain how a SOHO (small office, home office) network functions.<br><b>1.7.B</b> Explain why SOHO and enterprise networks have different challenges and security implications.   | 3–4                                    | 0–1                        |

**SUGGESTED SKILLS:****1.B**

Explain relationships among data, computer networking, and cybersecurity.

**TOPIC 1.1**

# Introduction to Cybersecurity

**LEARNING OBJECTIVE****LO-1.1.A**

Describe the impacts of cybersecurity on individuals, organizations, governments, and critical infrastructure.

**ESSENTIAL KNOWLEDGE****EK-1.1.A.1**

Cybersecurity is the practice of preventing, detecting, and responding to adversarial attacks and natural disasters that impact computer systems, networks, and associated data to ensure confidentiality, integrity, and availability.

**EK-1.1.A.2**

Individuals use computer systems and networks to manage many aspects of their everyday lives, such as employment, personal finance, commerce, and social activities.

**EK-1.1.A.3**

Organizations use computer systems and networks to enhance productivity, store proprietary or sensitive information, and foster internal and external communication.

**EK-1.1.A.4**

Governments use computer systems and networks to provide services such as education, healthcare, transportation, and public safety.

**EK-1.1.A.5**

Critical infrastructure refers to the assets, systems, and networks that enable a nation to function (such as transportation, communication, water, and energy) and whose destruction would have debilitating impact on the health, safety, and security of a nation. Critical infrastructure uses computer systems and networks to manage information and operations.

**EK-1.1.A.6**

Cybersecurity ensures that people can reliably access necessary services in a way that maintains the privacy of their data. Breaches in security can have consequences that include exposure of sensitive data, loss of intellectual property, identity theft, financial fraud, erosion of trust in digital systems, and loss of life.

*continued on next page*

## Introduction to Cybersecurity and Networking

### LEARNING OBJECTIVE

**LO-1.1.B**

Describe the foundational concepts of confidentiality, integrity, and availability in cybersecurity.

### ESSENTIAL KNOWLEDGE

**EK-1.1.B.1**

The concepts of confidentiality, integrity, and availability are the basis of security requirements and are collectively referred to as the CIA Triad.

**EK-1.1.B.2**

Confidentiality means that data are only accessible by authorized individuals, systems, or processes. Systems not meeting the requirements of confidentiality are vulnerable to having sensitive data stolen.

**EK-1.1.B.3**

Integrity means that data are accurate and trustworthy. Integrity includes non-repudiation, which verifies the origin of data. Systems not meeting the requirements of integrity are vulnerable to adversaries impersonating entities and tampering with data.

**EK-1.1.B.4**

Availability means that data and services are accessible when required by authorized individuals. Systems not meeting the requirements of availability have unexpected periods of time when they are out of service.

**SUGGESTED SKILLS:****1.B**

Explain relationships among data, computer networking, and cybersecurity.

**2.B**

Determine security controls that address potential vulnerabilities.

**TOPIC 1.2****Personal Digital Security****LEARNING OBJECTIVE****LO-1.2.A**

Explain how an individual can limit the risk of identity theft, credit card fraud, and stolen login credentials.

**LO-1.2.B**

Apply password security practices that can prevent an unauthorized user from accessing an individual's online accounts.

**ESSENTIAL KNOWLEDGE****EK-1.2.A.1**

Individuals can reduce the risk of identity theft and unwanted tracking by limiting the sharing of personal information on public websites. Information found in photos, location tags, family member names, and dates of special events are often used to verify identity for doing personal and sensitive business, so when adversaries (also referred to as threat actors or attackers) have this information, they may use it to impersonate another individual.

**EK-1.2.A.2**

Using secure Internet connections when sending sensitive information can help prevent negative outcomes, such as identity theft, credit card fraud, stolen login credentials.

Illustrative Example: Using virtual private networks (VPNs) while on public Wi-Fi

**EK-1.2.A.3**

Being cautious about emails and messages from unknown senders can prevent a phishing attack. Phishing attacks often involve malicious links or downloads that can contain malware (malicious software) or trick a person into sharing sensitive information such as account login credentials.

**EK-1.2.B.1**

Using strong passwords, such as those with adequate length and a combination of uppercase, lowercase, numeric, and symbolic characters, makes it more difficult for an adversary to crack a user's password.

**EK-1.2.B.2**

Using a different password for each online account prevents an adversary from being able to reuse a compromised password to access additional online accounts. Updating online passwords at regular intervals ensures that if an adversary finds an old password, it is no longer useful.

**EK-1.2.B.3**

Multifactor authentication (MFA) requires an individual to provide two or more types of information to log into an account. For example, when an individual enters a password for an online account, they can be prompted to enter a verification code sent by text message to their personal phone or to use an authenticator application before they can access the account. Multi-factor authentication can prevent an adversary who successfully obtains a valid password from accessing the individual's account.

*continued on next page***CK Cybersecurity 1:** Networking Fundamentals

## Introduction to Cybersecurity and Networking

### LEARNING OBJECTIVE

**LO-1.2.C**

Explain how practicing secure software behaviors can protect an individual's data.

### ESSENTIAL KNOWLEDGE

**EK-1.2.C.1**

Maintaining up-to-date software on personal devices will ensure the latest security patches are applied to address known vulnerabilities. Vulnerabilities in software can often be exploited to gain access to the device, read or modify sensitive data, or use the device for unintended purposes.

**EK-1.2.C.2**

Installing and maintaining anti-virus software on devices can help individuals detect and prevent malicious files from being downloaded and executed on a device. Malicious files can compromise sensitive data or can allow an adversary to gain access to the device.

**EK-1.2.C.3**

Maintaining an updated backup of personal data in a safe location can help an individual recover from a cyber incident, hardware failure, or system failure with minimal data loss.

**SUGGESTED SKILLS:****1.B**

Explain relationships among data, computer networking, and cybersecurity.

**2.B**

Determine security controls that address potential vulnerabilities.

**TOPIC 1.3**

# Enterprise Security

**LEARNING OBJECTIVE****LO-1.3.A**

Explain how personal digital security is different from enterprise security.

**ESSENTIAL KNOWLEDGE****EK-1.3.A.1**

Personal digital security involves tactics and behaviors for helping an individual protect their own data. Though individuals depend on service providers for the protection of their data, personal digital security focuses on the individual's share of responsibility to protect their data.

**EK-1.3.A.2**

Enterprise security involves the protection of the data managed by an organization, which usually requires the protection of a larger set of assets and information.

**EK-1.3.A.3**

Enterprise security often must consider:

- a wider user base and its interactions with sensitive information, both on premises and remotely
- the storage and maintenance of proprietary information
- a more complex network and systems infrastructure for the organization's operations
- the adherence of the organization's policies and procedures to current laws and regulations for managing sensitive, industry-specific data
- reputational and financial impacts of security incidents
- that an enterprise is usually a higher-value target than an individual for motivated adversaries

**EK-1.3.A.4**

In enterprise security, the tactics used in personal digital security are often applied to the many individuals and devices that access the organization's network. For example, a password policy may require all users to create strong passwords and change them at regular intervals, all user devices have antivirus software installed, and device software updates and backups are completed regularly.

*continued on next page*

## Introduction to Cybersecurity and Networking

### LEARNING OBJECTIVE

#### LO-1.3.B

Explain how the state and classification of data impact the security controls an organization implements.

### ESSENTIAL KNOWLEDGE

#### EK-1.3.B.1

Security controls are measures implemented to protect the confidentiality, integrity, and availability of data used by an organization.

#### EK-1.3.B.2

Data exist on a computer system or network in one of three states:

- i. Data at rest refers to data that are not currently being used or accessed.
- ii. Data in transit, or data in motion, refers to data that are being transferred within or between computer systems.
- iii. Data in use refers to data that are being processed or accessed by a computer system.

#### EK-1.3.B.3

Protecting data at rest requires security controls that protect both physical access to the computer systems that store data as well as administrative access to the data on them.

#### EK-1.3.B.4

Protecting data in transit requires security controls that monitor and protect data while they move through network infrastructure including network devices and transmission media.

#### EK-1.3.B.5

Protecting data in use requires security controls that verify that the user accessing the data is legitimate and authorized to access the data.

#### EK-1.3.B.6

Organizations must implement security controls to protect data in each of its possible states and to the level required by its classification. Data classified as having higher levels of sensitivity generally require higher levels of security.

#### EK-1.3.B.7

Organizations establish policies and procedures for how data are handled, managed, and protected. Many of these policies are based on state laws, federal laws, and industry sector standards that establish requirements for the protection of certain types of sensitive data.

#### EK-1.3.B.8

Organizations apply a combination of security controls, each of which addresses different types of data vulnerabilities. For example, to address different threats to an organization's computer systems and networks, organizations often educate users about phishing scams, require card readers to access specific areas, and use firewalls to restrict network traffic.

**SUGGESTED SKILLS:****1.A**

Describe and explain concepts and processes related to data, computer networking, and cybersecurity.

**TOPIC 1.4**

# Introduction to Computer Systems

**LEARNING OBJECTIVE****LO-1.4.A**

Explain how the hardware components of a computer system function.

**ESSENTIAL KNOWLEDGE****EK-1.4.A.1**

A computer system is made up of hardware, software, and data that work together to perform specific functions. Hardware refers to the physical components that make up the system, while software refers to the programs executed on a computer to perform specific tasks.

**EK-1.4.A.2**

The central processing unit (CPU) is responsible for executing required arithmetic, logic, and input/output operations.

**EK-1.4.A.3**

The random access memory (RAM) temporarily holds data as it is being used for immediate operations. RAM is volatile, which means that data stored on it will be lost if the system loses power.

**EK-1.4.A.4**

Storage is used to hold data long term. It is non-volatile, which means that data persist even if the system is powered off. Typical storage devices include hard disk drives (HDD) and solid state drives (SSD).

**EK-1.4.A.5**

The motherboard is the core printed circuit board (PCB) that allows for the communication between the different electronic components of a computer system.

**EK-1.4.A.6**

Peripheral components are externally connected to a computer system to provide additional functionality to the system. For example, monitors and speakers provide ways for the computer to give output. Mice and keyboards provide ways for the computer to receive input.

**LO-1.4.B**

Explain how key software programs allow a computer system to perform specific functions.

**EK-1.4.B.1**

Firmware is software that manages hardware components, including how devices initialize and boot when powered on and how they communicate with other hardware. Security features are sometimes embedded in a device's firmware.

Illustrative Examples:

- Basic Input/Output System (BIOS)
- Unified Extensible Firmware Interface (UEFI)

*continued on next page*

## Introduction to Cybersecurity and Networking

### LEARNING OBJECTIVE

**LO-1.4.B**

Explain how key software programs allow a computer system to perform specific functions.

### ESSENTIAL KNOWLEDGE

**EK-1.4.B.2**

The operating system is software that interfaces between the user and the hardware. It is responsible for managing system resources and performing required system tasks such as launching applications. Common operating systems include Windows, macOS, Linux, Android, and iOS.

**EK-1.4.B.3**

Application software is software that performs a specific function not directly related to the computer system. Common application software includes word processors, Internet browsers, media players, and games.

**EK-1.4.B.4**

A driver is software that allows a device to communicate with a computer system's operating system. Peripheral components like printers and USB drives often require drivers to be installed before they can be used.

**LO-1.4.C**

Describe the benefits of using virtualization in a computer system.

**EK-1.4.C.1**

Virtualization is a technology that allows for the creation of multiple virtual instances or environments on a single hardware system rather than requiring each to be on its own hardware system.

**EK-1.4.C.2**

A virtual instance (or virtual machine) typically refers to an emulation of a physical computer running an operating system and applications.

Illustrative Example: A hypervisor such as VirtualBox can be used to launch an instance of Ubuntu (a Linux distribution) on a Windows machine.

**EK-1.4.C.3**

A virtual environment refers to the collection of virtual resources that may include multiple virtual instances, virtual networks, and other virtualized components.

**EK-1.4.C.4**

Virtualization can increase system efficiency and flexibility by allowing hardware resources to be pooled and allocated quickly and dynamically across different virtual instances and environments.

**EK-1.4.C.5**

Virtualization can increase security, because virtual instances and environments are isolated from one another even if they are on the same physical machine.

**SUGGESTED SKILLS:****1.A**

Describe and explain concepts and processes related to data, computer networking, and cybersecurity.

**TOPIC 1.5**

# Introduction to Command Line

**LEARNING OBJECTIVE****LO-1.5.A**

Describe the characteristics of Windows and Linux file systems.

**ESSENTIAL KNOWLEDGE****EK-1.5.A.1**

A file system is a logical structure by which files are named and stored on a computer system. A file system is determined and managed by the operating system.

**EK-1.5.A.2**

Data are often stored as files and their locations are stored in directories. Directories can hold the locations of multiple files and directories.

**EK-1.5.A.3**

A Windows file system stores information on various drives, each of which is represented with a drive letter. For example, C : represents the C drive. Each drive contains files and directories that branch out from that drive.

Illustrative Example:

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

**EK-1.5.A.4**

A Linux file system begins with the root directory, /. All files and directories branch out from the root directory.

Illustrative Example:

Linux file path: /home/user/Desktop

home is a directory in the root directory, user is a directory in home, and Desktop is a directory in user.

**LO-1.5.B**

Apply appropriate commands using the command line interface (CLI) to navigate a file system.

**EK-1.5.B.1**

Operating systems commonly allow users to interact with the computer system through a graphical user interface (GUI), which uses icons, menus, and windows, or through a command line interface (CLI), which uses a terminal window application and text-based input.

*continued on next page*

## Introduction to Cybersecurity and Networking

### LEARNING OBJECTIVE

**LO-1.5.B**

Apply appropriate commands using the command line interface (CLI) to navigate a file system.

### ESSENTIAL KNOWLEDGE

**EK-1.5.B.2**

Though GUIs are often more intuitive for users, CLIs can sometimes offer faster, more customized, and more efficient administration of networks and computer systems. Sometimes, devices can only be configured using CLI. Terminal on macOS and Linux, Command Prompt on Windows, and PowerShell on Windows are applications that allow users to access the file system and system utilities via CLI.

**EK-1.5.B.3**

The CLI prompt often begins with the username and host name and is followed by the directory of the file system currently being referenced. On Linux, the location begins with the root directory, /, followed by the names of nested directories. ~ indicates the current user's home directory. On Windows, the location begins with a drive letter, followed by the names of nested directories.

Illustrative Examples:

Linux Prompt: user@hostname ~ /home/user/Desktop \$

Linux Prompt: user@hostname ~ \$

Windows Prompt: C:\Users\user\Desktop>

**EK-1.5.B.4**

A file path is used to identify a location in a file system. An absolute path is a path that begins with the root directory (Linux) or drive letter (Windows). A relative path does not begin with the root directory or drive letter and gives a path in relation to the current working directory.

Illustrative Example:

/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.

*continued on next page*

**LEARNING OBJECTIVE****LO-1.5.B**

Apply appropriate commands using the command line interface (CLI) to navigate a file system.

**ESSENTIAL KNOWLEDGE****EK-1.5.B.5**

Entering commands in the CLI usually takes the form of command options arguments.

- The command is the name of the utility or command to be executed.
- Options are the optional parameters that can be used with this command, which are often denoted with a `-`.
- Arguments provide information passed to the command to guide its function. Arguments are sometimes required to execute a command.

**Illustrative Example:**

The command `ls` can be used in several ways on a Linux system:

- `ls`

This execution of `ls` is without options or arguments. It will display the contents of the current directory excluding hidden files.

- `ls -a`

This execution of `ls` uses the option `-a`. It will display all the contents of the current directory including any hidden files.

- `ls /etc`

This use of `ls` has no options, but uses an argument of `/etc`. It will display the contents of the `/etc` directory excluding hidden files.

- `ls -a /etc`

This use of `ls` uses both an option `-a` and an argument of `/etc`. It will display the contents of the `/etc` directory including any hidden files.

**EK-1.5.B.6**

Common commands to navigate and manipulate the file system include:

- `cd` - change the currently referenced directory
- `ls` - view the contents of the current directory (Mac / Linux)
- `dir` - view the contents of the current directory (Windows)
- `pwd` - view the current working directory (Mac / Linux)
- `cat` - concatenate and print files (Mac / Linux)
- `mkdir` - create a new directory
- `touch` - create a new file or update the timestamp of an existing file
- `mv` - move a file from one directory to another (or rename a file)
- `cp` - copy a file to a directory

## TOPIC 1.6

# Introduction to Networks

### LEARNING OBJECTIVE

**LO-1.6.A**

Describe the characteristics of computer networks.

**LO-1.6.B**

Explain how computers transmit digital communications.

### ESSENTIAL KNOWLEDGE

**EK-1.6.A.1**

Computer networks are made up of multiple devices connected for the purpose of communicating information by sending and receiving data. Data may include text, images, sound files, software, etc.

**EK-1.6.A.2**

A network node refers to any device connected to a network. A host is a type of node that actively participates in the generation or consumption of data, such as computers, servers, and printers. Network nodes that facilitate data transmission, such as switches or routers, are not considered hosts.

**EK-1.6.A.3**

Computer networks allow devices to share resources such as file storage, printers, and email.

**EK-1.6.A.4**

Computer networks need to enable authorized users to access data securely and reliably.

**EK-1.6.B.1**

Digital communication requires a sender, receiver, transmission medium, and communication protocols.

**EK-1.6.B.2**

Networking protocols, or communication protocols used in computer networks, are rules used to define how messages are exchanged between nodes of a network, including how data are sequenced and formatted.

**EK-1.6.B.3**

A network interface card (NIC) is required for a device to access a network. The NIC defines which transmission medium is used to transmit data, so different NICs are required for accessing wired networks and wireless networks.

**EK-1.6.B.4**

Computers convert data into binary, which is represented with 0s and 1s or on and off signals.

**EK-1.6.B.5**

Binary data are transmitted to other devices through transmission media in formats such as light, electricity, and electromagnetic waves.

**SUGGESTED SKILLS:****1.A**

Describe and explain concepts and processes related to data, computer networking, and cybersecurity.

continued on next page

**LEARNING OBJECTIVE****LO-1.6.C**

Convert a number between decimal and binary.

**LO-1.6.D**

Describe the primary types of networks defined by geographical size.

**ESSENTIAL KNOWLEDGE****EK-1.6.C.1**

Decimal refers to base-10 numbers and uses the digits 0–9. A decimal number has place values that are powers of 10. From right to left, the place values are worth: 1, 10, 100, 1000, etc.

**EK-1.6.C.2**

Binary refers to base-2 numbers and uses the digits 0 and 1. A binary digit is called a bit. A binary number has place values that are powers of two. From right to left, the place values are worth: 1, 2, 4, 8, etc.

**EK-1.6.C.3**

The converted decimal number in binary will have 1s in the place values that add up to that decimal number.

**EK-1.6.D.1**

A local area network (LAN) is a collection of devices connected in one physical location, such as a single office building or a home network.

**EK-1.6.D.2**

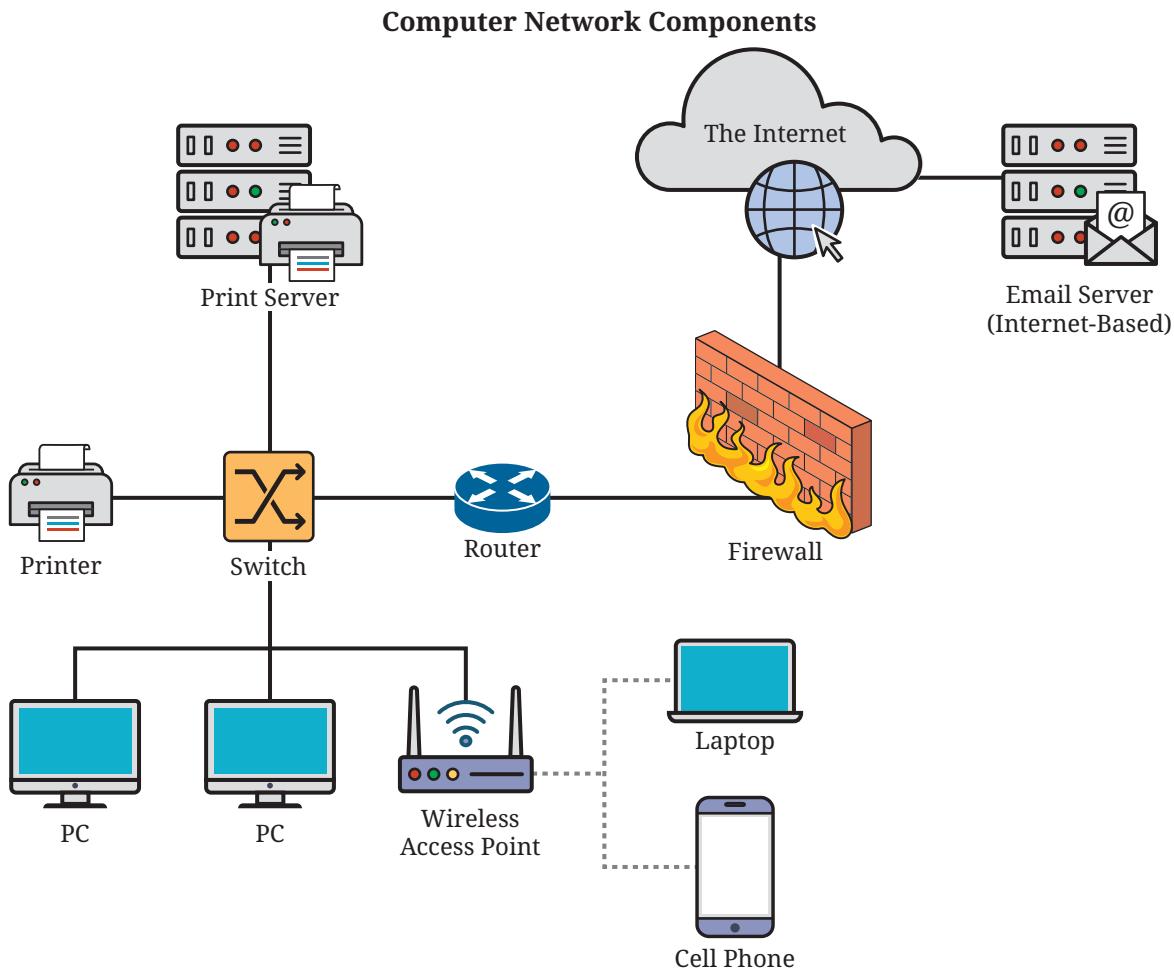
A wide area network (WAN) connects local area networks (LANs) together such as the Internet or a network for a large organization that spans multiple geographical locations.

**EK-1.6.D.3**

A personal area network (PAN) connects devices that are the closest to the user, usually via Bluetooth. This might include Bluetooth keyboards, mice, headphones, and printers.

**EK-1.6.D.4**

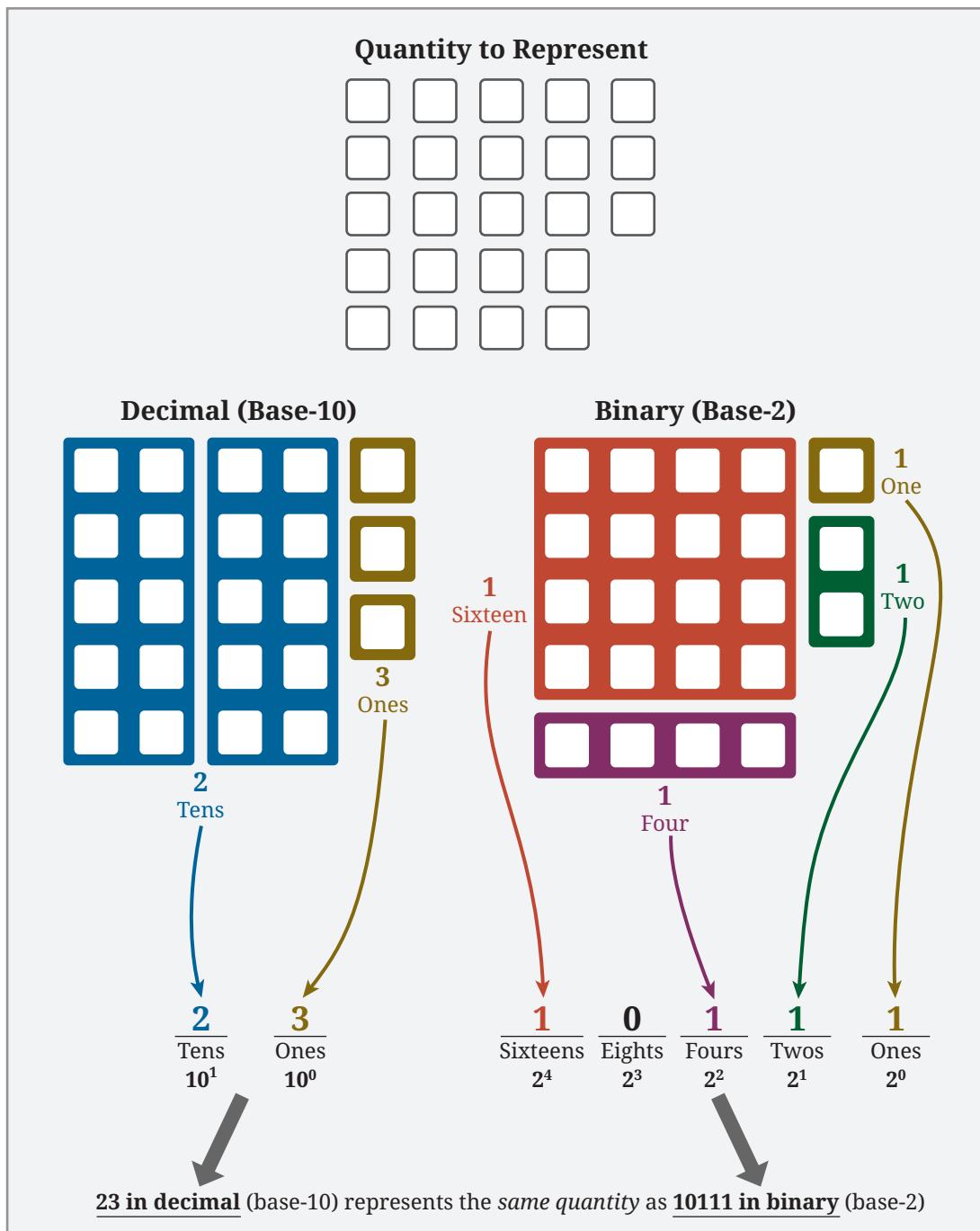
A metropolitan area network (MAN) is a private network used by an entity to communicate in a city or local geographical area and is larger than a LAN but smaller than a WAN.



On some networks, the **switch**, **router**, **firewall** and **wireless access point** are integrated into one device. In addition, many of the services used within a network (such as email and file storage for example) can be internet-based, where servers beyond the LAN (local area network) provide the functionality.

— Represents a wired connection    - - - Represents a wireless connection

**Figure 1.6a:** Computer Network Components



Representing numbers in different bases is similar to having different words for the same object or idea in different languages. (For example, cat and gato represent the same idea, but one is in English and one is in Spanish.). In this illustration, 23 in decimal (base-10) represents the same quantity as 10111 in binary (base-2). In a base-10 number, all the place values follow powers of ten (ones, tens, hundreds, etc.) while in a base-2 number, all the place values follow powers of two (ones, twos, fours, eights, etc.)

**Figure 1.6b:** Decimal to Binary

**SUGGESTED SKILLS:****1.A**

Describe and explain concepts and processes related to data, computer networking, and cybersecurity.

**2.A**

Determine appropriate endpoints, network appliances, transmission media, and communication protocols to meet network requirements.

**TOPIC 1.7**

# SOHO vs. Enterprise Networks

**LEARNING OBJECTIVE****LO-1.7.A**

Explain how a SOHO (small office, home office) network functions.

**ESSENTIAL KNOWLEDGE****EK-1.7.A.1**

A SOHO network is a network that serves a small number of users in a single LAN, typically for a small business. Common SOHO network devices include a modem, router, wireless access point, switch, firewall, and endpoints. Common endpoints include laptops, PCs, printers, and cell phones.

**EK-1.7.A.2**

The modem connects a SOHO network to an Internet service provider (ISP)'s network so the Internet is accessible to the SOHO network.

**EK-1.7.A.3**

The router connects to the modem and transmits data to and from the SOHO network.

**EK-1.7.A.4**

The wireless access point allows endpoints to connect to the SOHO network wirelessly.

**EK-1.7.A.5**

The switch allows for endpoint devices to connect to the SOHO network using physical wires. The switch is also physically connected to the router and wireless access point.

**EK-1.7.A.6**

The firewall can filter network traffic according to specific rules, which can prevent unauthorized access to the network.

**EK-1.7.A.7**

Many SOHO networks use a device that integrates the router, wireless access point, switch, and firewall. Colloquially, this is often referred to as a wireless router.

*continued on next page*

**LEARNING OBJECTIVE****LO-1.7.B**

Explain why SOHO and enterprise networks have different challenges and security implications.

**ESSENTIAL KNOWLEDGE****EK-1.7.B.1**

A SOHO network is a LAN intended to serve a small number of devices and users (typically about 1–10) in a small business setting. An enterprise network is intended to serve a large number of devices and users (hundreds or thousands) and often involves a WAN.

**EK-1.7.B.2**

SOHO networks need to support smaller volumes of network traffic and require fewer resources. Enterprise networks need to support larger volumes of network traffic, which requires the use of dedicated network devices and specific network designs to meet the needs of a large organization.

**EK-1.7.B.3**

SOHO networks are less expensive and simpler to implement and secure than enterprise networks because they do not require as much hardware. SOHO networks also do not require as many personnel to install, configure, and maintain them.

## **CK NETWORKING FUNDAMENTALS**

### **UNIT 2**

# **Layers, Protocols, and Addressing**

THIS PAGE IS INTENTIONALLY LEFT BLANK.

# Layers, Protocols, and Addressing

## KEY QUESTIONS

- How does the browser know what to show when I type in a URL?
- How do data travel across oceans?
- Will the Internet ever be overloaded if we put all the world's Internet of Things on it? (e.g. cars, toasters and toilets?)

## UNIT OBJECTIVES

By the end of this unit, students should be able to:

- Select an appropriate cable type for a given scenario
- Differentiate between physical and logical device addresses and their purposes
- Configure an IP address for a device

## Developing Understanding

Unit 2 introduces students to layers, protocols, and addressing, where network devices speak in zeroes and ones and send data through a transmission medium such as electricity along a copper wire or radio waves through the air. Students will learn about the different cables and topologies used in modern networks. Students will learn that all data they access and send through the Internet must travel physically from one device to another, no matter where those devices are located around the world. Finally, students will learn about physical and logical device addressing, and how dynamic host configuration protocol (DHCP) can be used to manage logical addresses on a network.

## Building Networking Skills

Understanding how collections of bits become useful information is one step in a student's journey to demystifying how the Internet works. The technology is not magic; it is made up of a series of discrete steps and literal physical movement of electrical signals on a wire. Network addressing is critical to ensuring that data reaches the appropriate destination. Furthermore, understanding how data travel between devices and the advantages and drawbacks of the topologies through which devices are connected in a network has strong implications for a network's design. In this stage in students' networking experience, they develop a more concrete understanding of how digital information travels physically. Hands-on experiences with cabling and topologies, and a conceptual understanding of number systems, help students build a foundation for the more complex networking concepts that come later in the course.

**UNIT AT A GLANCE**

| <b>Topic</b>                                     | <b>Learning Objectives</b>   | <b>Suggested Instructional Periods</b> |                            |
|--|--|--|----------------------------|
|  |  | <b>Teach &amp; Labs</b>                | <b>Review &amp; Assess</b> |
| <b>2.1 OSI and TCP/IP Models</b>                 | <b>2.1.A</b> Describe the purpose of the OSI and TCP/IP models in computer networking.<br><b>2.1.B</b> Describe the characteristics of the seven layers of the OSI model.<br><b>2.1.C</b> Describe how the four layers of the TCP/IP model relate to the seven layers of the OSI model.<br><b>2.1.D</b> Describe encapsulation and de-encapsulation in data transmission.<br><b>2.1.E</b> Describe the process of encapsulation in the OSI and TCP/IP models.<br><b>2.1.F</b> Describe the process of de-encapsulation in the OSI and TCP/IP models. | 3–4                                    | 1                          |
| <b>2.2 Introduction to Protocols and Servers</b> | <b>2.2.A</b> Determine whether TCP (transmission control protocol) or UDP (user datagram protocol) is appropriate for a specific situation.<br><b>2.2.B</b> Describe the relationship among servers, protocols, and logical ports on a network.  | 2–3                                    | 1–2                        |
| <b>2.3 Cabling</b>                               | <b>2.3.A</b> Describe the characteristics of the most common cable types used in computer networks.<br><b>2.3.B</b> Describe the different categories of twisted pair cabling.<br><b>2.3.C</b> Determine the appropriate cables for a given context.   | 2–3                                    | 0–1                        |
| <b>2.4 Network Topologies</b>                    | <b>2.4.A</b> Describe common network topologies.<br><b>2.4.B</b> Describe the advantages and disadvantages of common network topologies.<br><b>2.4.C</b> Describe the differences between client-server and peer-to-peer network models.   | 2–3                                    | 0–1                        |

## Layers, Protocols, and Addressing

| <b>Topic</b>                   | <b>Learning Objectives</b>  | <b>Suggested Instructional Periods</b> |                            |
|--------------------------------|---|--|----------------------------|
|                                |   | <b>Teach &amp; Labs</b>                | <b>Review &amp; Assess</b> |
| <b>2.5 Physical Addressing</b> | <b>2.5.A</b> Describe the purpose and structure of MAC addresses.<br><b>2.5.B</b> Convert between binary and hexadecimal number systems.  | 3–4                                    | 0–1                        |
| <b>2.6 Logical Addressing</b>  | <b>2.6.A</b> Describe the purpose and structure of IPv4 and IPv6 addresses.<br><b>2.6.B</b> Describe the differences between the types of addresses used in computer networks.<br><b>2.6.C</b> Determine the MAC and IP addresses on a host device. | 2–3                                    | 0–1                        |
| <b>2.7 IP Configuration</b>    | <b>2.7.A</b> Describe the purpose and function of DHCP.<br><b>2.7.B</b> Configure an IP address on a host device and use tools to verify its settings.  | 1–2                                    | 1–2                        |

**SUGGESTED SKILLS:****1.A**

Describe and explain concepts and processes related to data, computer networking, and cybersecurity.

**TOPIC 2.1****OSI and TCP/IP Models****LEARNING OBJECTIVE****LO-2.1.A**

Describe the purpose of the OSI and TCP/IP models in computer networking.

**LO-2.1.B**

Describe the characteristics of the seven layers of the OSI model.

**ESSENTIAL KNOWLEDGE****EK-2.1.A.1**

The OSI (Open Systems Interconnection) and TCP/IP (Transmission Control Protocol/Internet Protocol) networking models provide a common standard that promotes interoperability between the network hardware and software created by different manufacturers.

**EK-2.1.A.2**

The OSI and TCP/IP models define layering for computer communications to break the process down into smaller, more manageable steps where each layer uses different protocols to enclose (encapsulate) its information to be passed to the next layer. The standardization of protocols for data transmission allows for the broader adoption of specific protocols regardless of the system or medium.

**EK-2.1.B.1**

The physical layer (Layer 1) of the OSI model deals with the bits that are transmitted via the medium (cable or air waves). This layer breaks down information going out from a system into bits that can be carried out to the destination via the specific medium used.

**EK-2.1.B.2**

In the data link layer (Layer 2) of the OSI model, bits are encoded, decoded, and organized before being transferred between machines on the same network.

**EK-2.1.B.3**

The network layer (Layer 3) of the OSI model handles the transfer of data between networks.

**EK-2.1.B.4**

The transport layer (Layer 4) of the OSI model handles how data are transferred between applications including flow control, error detection, and error correction.

**EK-2.1.B.5**

The session layer (Layer 5) of the OSI model forms, manages, and ends the connections between the local and remote applications.

*continued on next page*

## Layers, Protocols, and Addressing

### LEARNING OBJECTIVE

**LO-2.1.B**

Describe the characteristics of the seven layers of the OSI model.

**LO-2.1.C**

Describe how the four layers of the TCP/IP model relate to the seven layers of the OSI model.

**LO-2.1.D**

Describe encapsulation and de-encapsulation in data transmission.

### ESSENTIAL KNOWLEDGE

**EK-2.1.B.6**

The presentation layer (Layer 6) of the OSI model prepares data for the application layer by defining how two devices should encode, encrypt, and compress data so it is received correctly on the other end.

**EK-2.1.B.7**

The application layer (Layer 7) of the OSI model ensures an application can effectively interact with other applications on different computer systems and networks.

**EK-2.1.C.1**

The network access layer of the TCP/IP model correlates with Layers 1 and 2 in the OSI model.

**EK-2.1.C.2**

The Internet layer of the TCP/IP model correlates with Layer 3 in the OSI model.

**EK-2.1.C.3**

The transport layer of the TCP/IP model correlates with Layer 4 in the OSI model.

**EK-2.1.C.4**

The session layer of the TCP/IP model correlates with Layers 5, 6, and 7 in the OSI model.

**EK-2.1.D.1**

Encapsulation, when applied to networking concepts, is the process of a sending node adding additional information (usually as headers and trailers) to the data as it travels between layers of the OSI or TCP/IP models.

NOTE: This is not to be confused with encapsulation that applies to object-oriented programming.

**EK-2.1.D.2**

A protocol data unit (PDU) is a single unit of information to be transmitted over a network. It contains the data to be transmitted and protocol information needed for the 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.

**EK-2.1.D.3**

De-encapsulation takes place on the receiving node and involves removing the headers and trailers attached during the encapsulation process.

**EK-2.1.D.4**

An error-checking process during de-encapsulation ensures the integrity and reliability of the data.

*continued on next page*

**LEARNING OBJECTIVE****LO-2.1.E**

Describe the process of encapsulation in the OSI and TCP/IP models.

**ESSENTIAL KNOWLEDGE****EK-2.1.E.1**

The upper layers of the OSI model (application, presentation, and session) or the application layer of the TCP/IP model prepare the data, or payload, to be transmitted and pass it to the transport layer where it will be encapsulated.

**EK-2.1.E.2**

The transport layer of both models encapsulates the data with a header to create a segment if TCP (transmission control protocol) is used or a datagram if UDP (user datagram protocol) is used so the data can be put back together when it reaches its destination. The header includes fields for the logical port, sequence number, and other acknowledgment components.

**EK-2.1.E.3**

The network layer of the OSI model or the Internet layer of the TCP/IP model receives the segment or datagram from the transport layer and encapsulates the data with a header to create a packet. Packets can be different sizes to accommodate the bandwidth of the network. The header contains fields for the source IP address, the destination IP address, and other information to properly route the data.

**EK-2.1.E.4**

The data link layer of the OSI model encapsulates the packet received from the network layer to create a frame. The encapsulation includes a header containing the source and destination MAC addresses along with a trailer that is used for error checking.

**EK-2.1.E.5**

The physical layer of the OSI model converts the encapsulated data it receives from the data link layer into bits to be transmitted over the medium. The TCP/IP model refers to the data link and physical layers of the OSI model as the network access layer.

*continued on next page*

## Layers, Protocols, and Addressing

### LEARNING OBJECTIVE

**LO-2.1.F**

Describe the process of de-encapsulation in the OSI and TCP/IP models.

### ESSENTIAL KNOWLEDGE

**EK-2.1.F.1**

The physical layer of the OSI model receives signals representing bits from the transmission medium and converts them into frames to give to the data link layer to de-encapsulate.

**EK-2.1.F.2**

The data link layer of the OSI model checks the assembled frames from the physical layer and uses the trailer to check for errors and confirm the integrity of the data. Any frames that arrive with errors are dropped. The data link layer of the receiving node de-encapsulates the packet by removing the header and trailer for the correctly transmitted frames. The extracted packet is then passed to the network layer. The TCP/IP model considers the actions at the data link and physical layers together.

**EK-2.1.F.3**

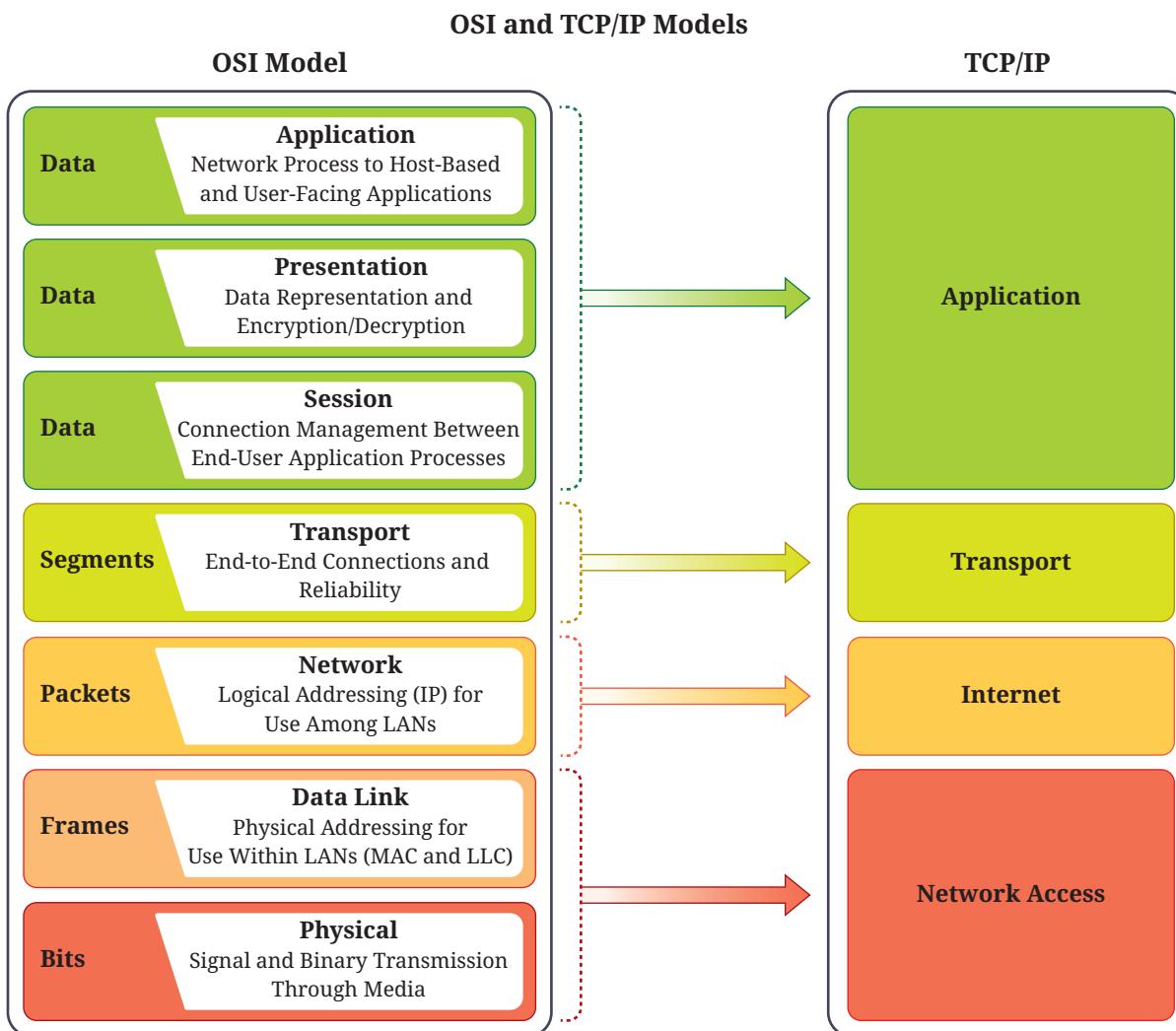
The network layer of the OSI model or the Internet layer of the TCP/IP model receives the packet from the data link layer. The network layer removes the header for the packet whose destination address matches its own and passes the resulting segment or datagram to the transport layer.

**EK-2.1.F.4**

The transport layer of both models uses information from the segment headers to ensure all information was received and arranges the segments into the correct order. Data sent using TCP that isn't received properly will be resent. When all data are received correctly, the headers are removed, and the data are reassembled into the original data stream that is passed to the upper layers of the OSI model.

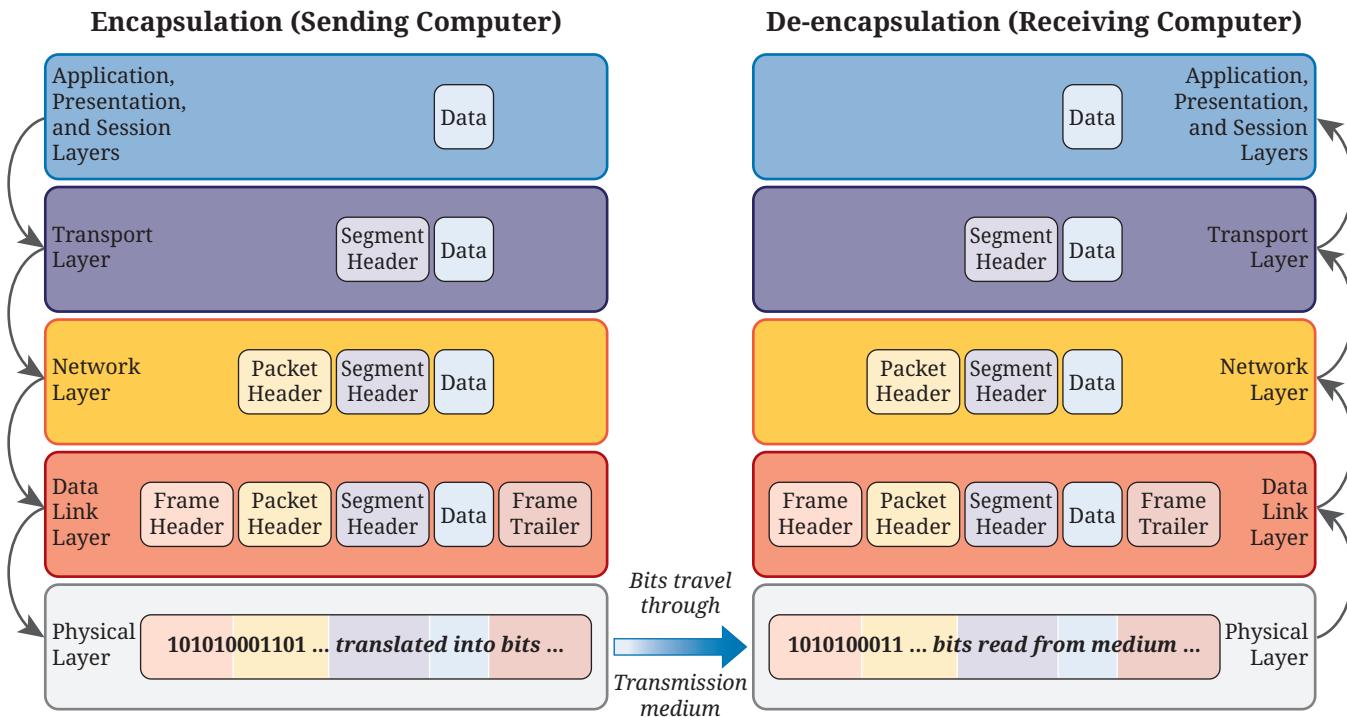
**EK-2.1.F.5**

The upper layers of the OSI model or the application layer of the TCP/IP model convert the de-encapsulated data received from the transport layer in a way that the destination application can read and visualize.



**Figure 2.1a:** OSI and TCP/IP Models

## Layers, Protocols, and Addressing



Before data is sent across a transmission medium, it is encapsulated with information to ensure it is sent to and received by the intended host device. Upon receiving the data from the transmission medium, the receiving device de-encapsulates the data.

**Figure 2.1b:** Encapsulation and De-encapsulation

**SUGGESTED SKILLS:****1.A**

Describe and explain concepts and processes related to data, computer networking, and cybersecurity.

**2.A**

Determine appropriate endpoints, network appliances, transmission media, and communication protocols to meet network requirements.

**TOPIC 2.2**

# Introduction to Protocols and Servers

**LEARNING OBJECTIVE****LO-2.2.A**

Determine whether TCP (transmission control protocol) or UDP (user datagram protocol) is appropriate for a specific situation.

**ESSENTIAL KNOWLEDGE****EK-2.2.A.1**

TCP and UDP are transport layer protocols. Which one should be used depends on whether the delivery of data packets is to be guaranteed.

**EK-2.2.A.2**

TCP is a connection-oriented protocol used to guarantee the delivery of data between applications. To guarantee delivery of data, TCP requires acknowledgment from the receiving host for each data segment being sent, which increases the amount of network traffic and communications required for all data to be delivered.

**EK-2.2.A.3**

When TCP is used, the sending host tracks the acknowledgments received by the receiving host. For any acknowledgments not received within a specific time period, the sending host will resend data segments.

**EK-2.2.A.4**

TCP should be used whenever complete and accurate data are more important than transmission speed. For example, chat, web, and email applications use TCP to ensure that messages and web content are not incorrect or scrambled.

**EK-2.2.A.5**

UDP is a connectionless protocol that enables the efficient transmission of data in packets with minimal overhead, but without guaranteed delivery or order of packets.

**EK-2.2.A.6**

UDP does not require a connection between the sending and receiving host nor the acknowledgments of any packets, so it should be used when transmission speed is more important than complete and accurate data. For example, video streaming and gaming applications often use UDP.

*continued on next page*

## Layers, Protocols, and Addressing

### LEARNING OBJECTIVE

#### LO-2.2.B

Describe the relationship among servers, protocols, and logical ports on a network.

### ESSENTIAL KNOWLEDGE

#### EK-2.2.B.1

A server is a computer with special software installed that allows it to provide a centralized resource or service to other computers in a network. For example, a web server is used to store files and respond to requests for a website.

Illustrative Examples: Printing, file storage, web pages, email, games.

#### EK-2.2.B.2

A server uses specific protocols related to its purpose. For example, web servers use HTTP (HyperText Transfer Protocol) or HTTPS (Hypertext Transfer Protocol Secure).

Illustrative Example: Web browsers send HTTP/HTTPS requests and receive responses from the appropriate web server.

#### EK-2.2.B.3

HTTP and HTTPS are standard web protocols used to exchange web data over the Internet. HTTPS is a secure version of the HTTP because it encrypts the data transmitted over the Internet. HTTP and HTTPS are application layer protocols.

#### EK-2.2.B.4

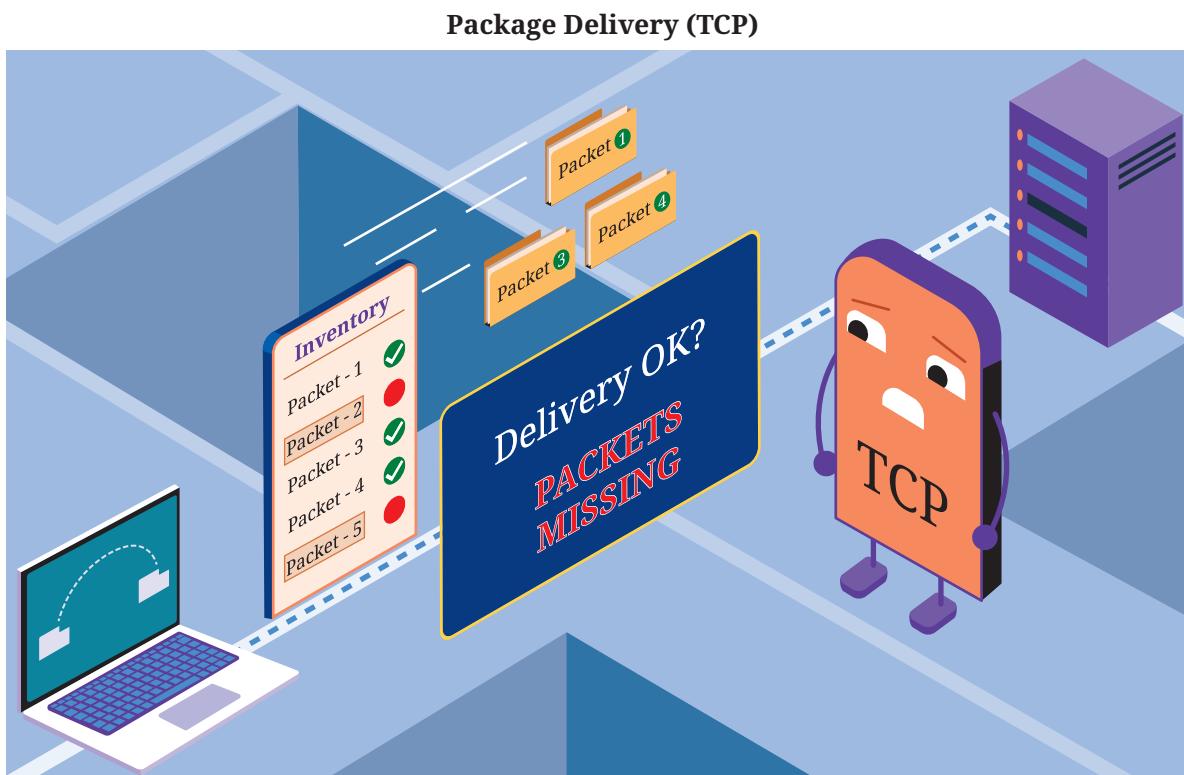
DNS (Domain Name System) is a protocol that translates human-readable domain names used in URLs (uniform resource locators) into Internet Protocol (IP) addresses, which are used to locate the specific web servers. DNS is an application layer protocol.

#### EK-2.2.B.5

Logical ports are used to identify the intended application receiving data. A server is set to communicate using specific logical ports. There are several services that have default ports for communication: HTTP (80), HTTPS (443), DNS (53).

#### EK-2.2.B.6

Clients that request resources or services from servers must use the appropriate protocols and logical ports for a server to be able to respond to the requests.



TCP (Transmission Control Protocol) provides confirmation of data delivery whereas UDP (User Datagram Protocol) does not.

**Figure 2.2:** Packet Delivery (TCP)

**SUGGESTED SKILLS:****1.B**

Explain relationships among data, computer networking, and cybersecurity.

**3.A**

Connect and configure network components using appropriate media, communication protocols, and commands.

**3.B**

Test network connectivity, verify network requirements, and troubleshoot network issues.

## TOPIC 2.3

# Cabling

**LEARNING OBJECTIVE****LO-2.3.A**

Describe the characteristics of the most common cable types used in computer networks.

**ESSENTIAL KNOWLEDGE****EK-2.3.A.1**

The three types of cabling used in modern networks are twisted pair, coaxial, and fiber optic.

**EK-2.3.A.2**

Twisted pair cables have copper conductors covered with thin insulation that are twisted around one another to cancel out electromagnetic interference (EMI) from external sources, which can disrupt the signal and corrupt data being transported.

**EK-2.3.A.3**

Coaxial cables have a single copper conductor at the center inside a layer of insulation, a braided metal shield, and an exterior plastic sheath.

**EK-2.3.A.4**

Fiber optic cables have a center glass core surrounded by multiple layers of protective and reflective materials.

**LO-2.3.B**

Describe the different categories of twisted pair cabling.

**EK-2.3.B.1**

Twisted pair cables are categorized (CAT) based on bandwidth and speed of data transmission.

**EK-2.3.B.2**

CAT5, CAT6, CAT7, and CAT8 are used in modern networks and offer faster and more efficient communication.

**EK-2.3.B.3**

CAT5 has a data rate of up to 100 Mbps and can transmit signals up to 100 meters (328 ft.). The CAT5e variation of this cable can transmit at speeds up to 1 Gbps.

**EK-2.3.B.4**

CAT6 has data rates of up to 1 Gbps over 100 meters (328 ft.). The CAT6a variation of this cable can transmit at speeds up to 10 Gbps.

*continued on next page*

**LEARNING OBJECTIVE****LO-2.3.C**

Determine the appropriate cables for a given context.

**ESSENTIAL KNOWLEDGE****EK-2.3.C.1**

Twisted pair cables are more affordable and easier to install than coaxial and fiber optic cables but are more susceptible to EMI and cannot transmit signals as far.

**EK-2.3.C.2**

Coaxial cables are more resistant to EMI and can transmit signals farther than twisted pair cables. They are more expensive and difficult to install than twisted pair cables.

**EK-2.3.C.3**

Fiber optic cables are immune to EMI and can carry signals much farther than coaxial and twisted pair cables because they transmit signals by carrying light instead of electricity. Fiber optic cables are more expensive and difficult to install than coaxial and twisted pair cables.

**EK-2.3.C.4**

Signal strength, distance, interference, speed, cost, and security are important factors to consider when choosing a cable. A NIC compatible with that cable type is also required.

## Layers, Protocols, and Addressing

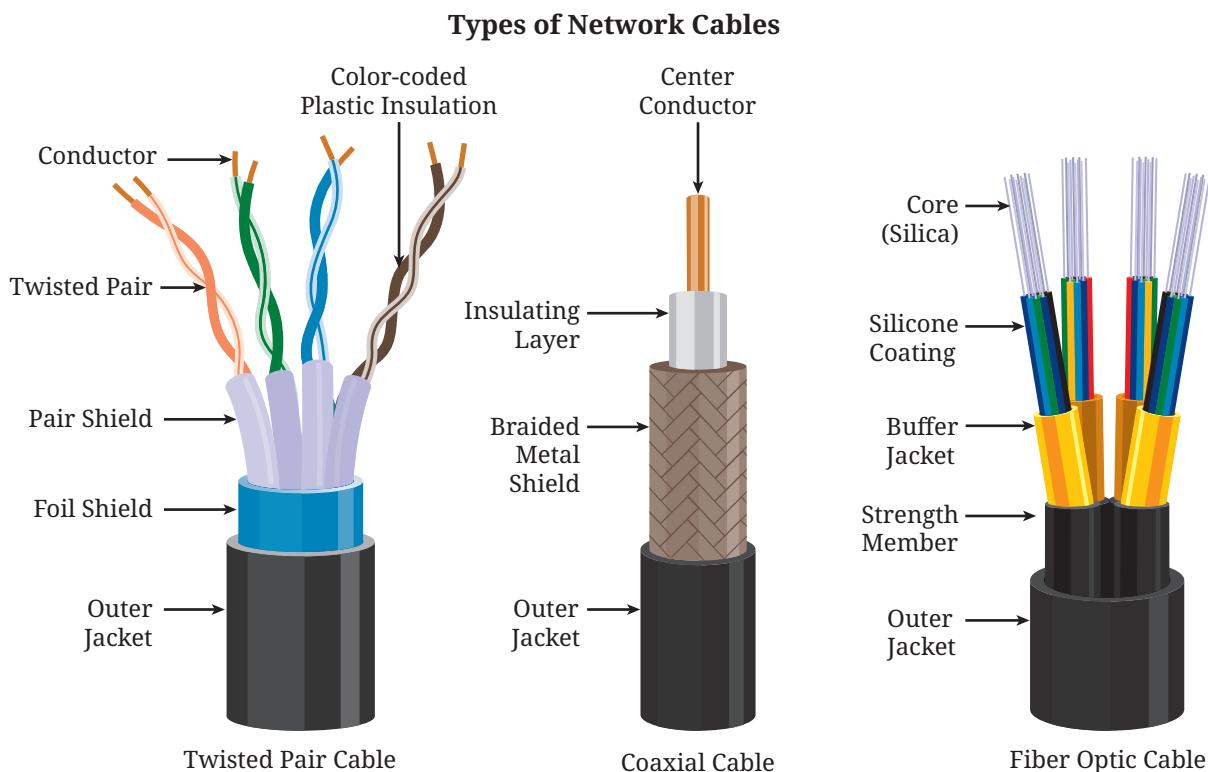


Figure 2.3: Types of Network Cables

**SUGGESTED SKILLS:****1.A**

Describe and explain concepts and processes related to data, computer networking, and cybersecurity.

**3.A**

Connect and configure network components using appropriate media, communication protocols, and commands.

**3.C**

Create technical documentation of network layouts, settings, and configurations.

**TOPIC 2.4**

# Network Topologies

**LEARNING OBJECTIVE****LO-2.4.A**

Describe common network topologies.

**LO-2.4.B**

Describe the advantages and disadvantages of common network topologies.

**ESSENTIAL KNOWLEDGE****EK-2.4.A.1**

The topology of a network refers to how its nodes are arranged. The network's physical topology refers to how its devices are physically connected while the network's logical topology refers to how data travel within it.

**EK-2.4.A.2**

In a bus topology, all the nodes are connected to a single medium that transmits data.

**EK-2.4.A.3**

In a ring topology, nodes are connected in a circular chain that loops back to the originating node.

**EK-2.4.A.4**

In a star topology, each node is connected indirectly to every other node through a central network device, typically a network switch.

**EK-2.4.A.5**

In a full mesh topology, each node is connected directly to each other.

**EK-2.4.A.6**

A hybrid topology is created when two or more network topologies are joined together.

**EK-2.4.B.1**

The bus topology is the simplest and least expensive to set up. However, it cannot handle a large number of nodes, is difficult to troubleshoot, and is less secure because all devices receive transmitted data instead of only the intended receiving device.

**EK-2.4.B.2**

The ring topology is less expensive and simpler to set up than star and mesh topologies. However, because network traffic is unidirectional, a single node may cause network failure, and data may need to travel through nodes for which they are not intended. This topology is easier to troubleshoot than bus, but not as easy as star.

*continued on next page*

## Layers, Protocols, and Addressing

### LEARNING OBJECTIVE

**LO-2.4.B**

Describe the advantages and disadvantages of common network topologies.

**LO-2.4.C**

Describe the differences between client-server and peer-to-peer network models.

### ESSENTIAL KNOWLEDGE

**EK-2.4.B.3**

The star topology is easier to scale, because adding nodes does not increase network traffic dramatically. Network traffic is easier to analyze, and troubleshooting in this topology is easier than bus, ring, and mesh. Nodes in this topology generally only receive data that are intended for them. However, this topology is more expensive to set up, and the central device can be a single point of failure.

**EK-2.4.B.4**

The mesh topology is the most resilient topology because failure of one node does not cause network failure. This topology can support high volumes of network traffic. However, this topology is expensive, complex to administer, and may contain redundant and unused connections between nodes.

**EK-2.4.C.1**

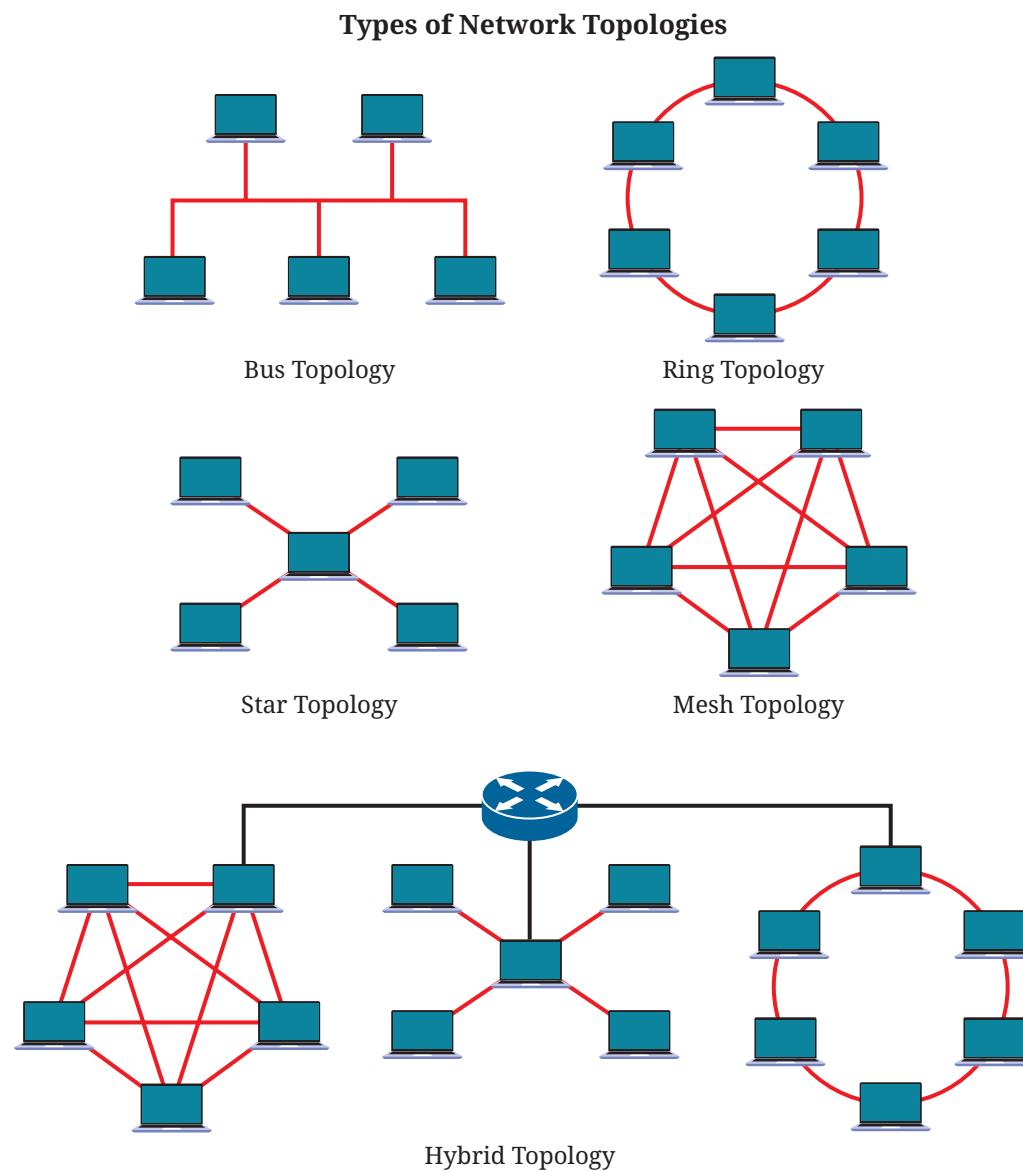
In a client-server network model, each node can either provide services or request services. In a peer-to-peer network model, each node can both provide and request services.

**EK-2.4.C.2**

A client-server network model is more efficient but is generally more expensive to set up than a peer-to-peer network model.

**EK-2.4.C.3**

Client-server networks tend to be more secure than peer-to-peer because they are centralized as opposed to decentralized. In a centralized setup, security controls are also centralized, providing more control over the security of the data. In a peer-to-peer network, each peer's security settings may be inconsistent across the network.



The topology of a network refers to how its nodes are arranged. The topology can describe how the nodes are physically connected (physical topology) or how data is sent between the nodes (logical topology).

**Figure 2.4:** Types of Network Topologies

## TOPIC 2.5

# Physical Addressing

### LEARNING OBJECTIVE

**LO-2.5.A**

Describe the purpose and structure of MAC addresses.

### ESSENTIAL KNOWLEDGE

**EK-2.5.A.1**

A MAC address is a unique 48-bit number that is used to identify a host within a local area network (LAN). Each MAC address, intended to be unique, is assigned to the NIC by the manufacturer.

**EK-2.5.A.2**

A MAC address may also be called a physical address, a hardware address, or an Ethernet address.

**EK-2.5.A.3**

MAC addresses are typically written as six pairs of hexadecimal numbers separated by hyphens or colons.

Illustrative Example: MAC addresses can be represented in three hexadecimal formats:

- 001b:6384:45e6
- 00:1b:63:84:45:e6
- 00-1B-63-84-45-E6

**EK-2.5.A.4**

A MAC address contains two parts: the first half of the address is associated with the organizational unique identifier (OUI) that identifies the manufacturer of the device, and the second half of the address identifies the device itself.

**LO-2.5.B**

Convert between binary and hexadecimal number systems.

**EK-2.5.B.1**

Hexadecimal refers to base-16 numbers and uses the digits 0–9 and A–F (where A represents the value 10, B represents the value 11, etc.). A hexadecimal number has place values that are powers of 16. From right to left, each place value is worth: 1, 16, 256, etc.

**EK-2.5.B.2**

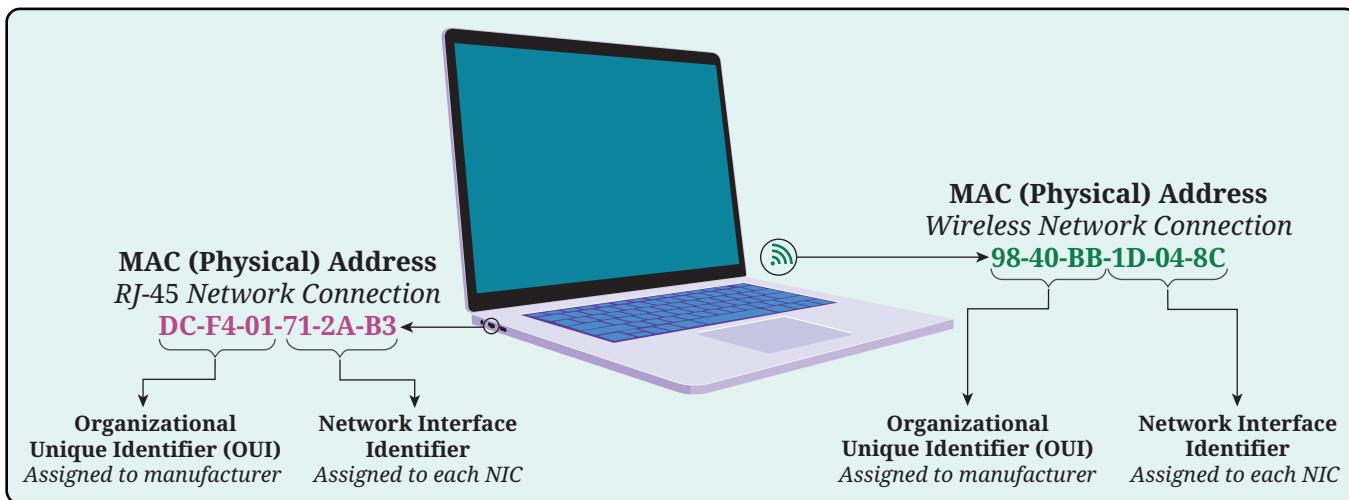
Every four bits can be represented with one hexadecimal digit. In the following series, the four digit binary is shown with its equivalent single hexadecimal digit: 0000 → 0, 0001 → 1, 0010 → 2, 0011 → 3, ... 1110 → E, 1111 → F.

**EK-2.5.B.3**

Hexadecimal numbers are used as shorthand for binary numbers, allowing humans to more easily read, write, and understand large binary numbers. For example, a MAC address is a 48-bit address written as 12 hexadecimal digits.

**SUGGESTED SKILLS:****1.A**

Describe and explain concepts and processes related to data, computer networking, and cybersecurity.

**MAC (Physical) Address**

For each way a device can connect to a network (both wired connections and wireless connections), a device must have a network interface card (NIC). Every NIC has a MAC (physical) address associated with it. The first half of the MAC address identifies the manufacturer of the NIC, while the second half identifies the NIC itself.

**Figure 2.5:** MAC (Physical) Address

## TOPIC 2.6

# Logical Addressing

### LEARNING OBJECTIVE

**LO-2.6.A**

Describe the purpose and structure of IPv4 and IPv6 addresses.

### ESSENTIAL KNOWLEDGE

**EK-2.6.A.1**

An IP address is used to identify hosts between different LANs. There are two types of IP addresses: IPv4 and IPv6.

**EK-2.6.A.2**

An IPv4 address consists of 32 bits that are typically grouped into four octets (groups of eight bits). An IPv4 address is typically written in dotted decimal format, where four decimal numbers are period-separated.

Illustrative Example: 192.168.1.1

**EK-2.6.A.3**

IPv4 addresses must be paired with subnet masks, which are commonly represented in dotted decimal format. They are used to determine whether hosts are on the same network. Common subnet masks include 255.0.0.0, 255.255.0.0, and 255.255.255.0.

**EK-2.6.A.4**

IPv6 was created in anticipation of the exhaustion of the IPv4 address space with the huge increase in the number of devices needing to connect to the Internet.

**EK-2.6.A.5**

An IPv6 address consists of 128 bits that are typically grouped as 8 hexets (groups of 16 bits) written with hexadecimal digits separated by colons. Illustrative Example: 2003:AB00:CDEF:000A:0000:0000:0001 /64

**EK-2.6.A.6**

An IPv6 address can be abbreviated with a double colon, which can be used to replace the longest string of consecutive zeros in the address. This process can only be used once in the address. Leading zeroes can also be omitted.

Illustrative Example: 2003:AB00:CDEF:000A::1 /64

**SUGGESTED SKILLS:****1.A**

Describe and explain concepts and processes related to data, computer networking, and cybersecurity.

*continued on next page*

**LEARNING OBJECTIVE****LO-2.6.B**

Describe the differences between the types of addresses used in computer networks.

**ESSENTIAL KNOWLEDGE****EK-2.6.B.1**

An address is a number that identifies a host on a network. There are two addressing schemes used in computer networks: Media Access Control (MAC) and Internet Protocol (IP).

**EK-2.6.B.2**

Every network host has both a MAC address and an IP address associated with it. Address resolution protocol (ARP) is used to map MAC addresses to IP addresses for devices on a network.

**EK-2.6.B.3**

MAC addresses are considered physical addresses because they are connected directly to the hardware. IP addresses are considered logical addresses because they are assigned based on the network a device is accessing.

**EK-2.6.B.4**

MAC addresses are portable; they stay the same even when a device goes from one network to another. IP addresses are not portable; they change when a device goes from one network to another.

**EK-2.6.B.5**

MAC addresses function at the data link layer (Layer 2) of the OSI model. IP addresses function at the network layer (Layer 3) of the OSI model.

**LO-2.6.C**

Determine the MAC and IP addresses on a host device.

**EK-2.6.C.1**

Tools such as ipconfig and ifconfig in the command line interface (CLI) and the network settings utility in the graphical user interface (GUI) can be used to identify the MAC and IP addresses on a host.

**EK-2.6.C.2**

In network setting outputs, depending on the operating system, MAC addresses might also appear under the label "Physical Address," "Hardware Address," or "Ether Address."

## TOPIC 2.7

# IP Configuration

### LEARNING OBJECTIVE

**LO-2.7.A**

Describe the purpose and function of DHCP.

**LO-2.7.B**

Configure an IP address on a host device and use tools to verify its settings.

### ESSENTIAL KNOWLEDGE

**EK-2.7.A.1**

DHCP (Dynamic Host Configuration Protocol) is a protocol used to automatically assign IPv4 addresses and configure network settings for devices in a network.

**EK-2.7.A.2**

To enable DHCP on a network, a network device must be configured as a DHCP server. Hosts on the network must be configured to request IP configuration information from the DHCP server.

**EK-2.7.B.1**

An IP address can be assigned manually by a user or automatically using DHCP. The network settings can often be changed using a graphical user interface (GUI) utility built into the operating system.

**EK-2.7.B.2**

The network configuration settings can be verified using command line tools such as `ipconfig /all` on Windows and `ifconfig` on Linux and Mac.

**SUGGESTED SKILLS:****1.A**

Describe and explain concepts and processes related to data, computer networking, and cybersecurity.

**2.A**

Determine appropriate endpoints, network appliances, transmission media, and communication protocols to meet network requirements.

**3.A**

Connect and configure network components using appropriate media, communication protocols, and commands.

THIS PAGE IS INTENTIONALLY LEFT BLANK.

## **CK NETWORKING FUNDAMENTALS**

### **UNIT 3**

# **Configuring a LAN**

THIS PAGE IS INTENTIONALLY LEFT BLANK.

# Configuring a LAN

## KEY QUESTIONS

- How can an adversary imitate someone else's device?
- If someone gains access to a network, how can we prevent them from getting to other parts of the network?
- When my Internet goes down, how can I figure out where the problem is?

## UNIT OBJECTIVES

By the end of this unit, students should be able to:

- Apply port security principles to protect a switch
- Configure a small LAN (one switch with multiple endpoints)
- Troubleshoot common network connectivity issues

## Developing Understanding

Unit 3 dives more deeply into the data link layer of the OSI model, where network switches become the conduit for creating a local area network (LAN). Students will learn how a switch uses addresses in a frame header to send data to the correct device. Students will also develop their skills in hardware configuration. Whether they use a network simulator or real physical hardware, at this point in the course students will gain experience logging into and changing configuration settings so a switch can function on a small LAN. Students will also explore how switches can be vulnerable to attack, and security measures that can mitigate those vulnerabilities.

## Building Networking Skills

At this stage, students will gain experience configuring dedicated network hardware and applying troubleshooting skills to mitigate connectivity issues as they arise. Working through various scenarios for configuring and troubleshooting networks can help students build transferable skills that they can apply in future cybersecurity courses and careers.

**UNIT AT A GLANCE**

| <b>Topic</b>                                     | <b>Learning Objectives</b>   | <b>Suggested Instructional Periods</b> |                            |
|--|--|--|----------------------------|
|  |  | <b>Teach &amp; Labs</b>                | <b>Review &amp; Assess</b> |
| <b>3.1 Switching</b>                             | <b>3.1.A</b> Explain how a switch directs traffic within a LAN.<br><b>3.1.B</b> Explain why the use of virtual local area networks (VLANs) can improve network performance and security.   | 3–4                                    | 0–1                        |
| <b>3.2 Switch Security</b>                       | <b>3.2.A</b> Explain how MAC spoofing and MAC flooding can be used to attack a network switch.<br><b>3.2.B</b> Explain how port security mitigates common risks associated with a network switch.  | 2–3                                    | 1–2                        |
| <b>3.3 More on Protocols</b>                     | <b>3.3.A</b> Describe the purpose and functions of common application layer protocols.<br><b>3.3.B</b> Determine the OSI and TCP/IP layers associated with common network protocols.   | 3–4                                    | 1                          |
| <b>3.4 LAN Configuration and Troubleshooting</b> | <b>3.4.A</b> Configure a small local area network (LAN) containing a switch and multiple endpoints.<br><b>3.4.B</b> Determine the appropriate security measures to address vulnerabilities in a local area network (LAN) containing a switch and multiple endpoints.<br><b>3.4.C</b> Troubleshoot common network problems in a LAN containing a switch and multiple endpoints. | 3–4                                    | 1–2                        |

**SUGGESTED SKILLS:****1.A**

Describe and explain concepts and processes related to data, computer networking, and cybersecurity.

**2.A**

Determine appropriate endpoints, network appliances, transmission media, and communication protocols to meet network requirements.

## TOPIC 3.1

# Switching

**LEARNING OBJECTIVE****LO-3.1.A**

Explain how a switch directs traffic within a LAN.

**ESSENTIAL KNOWLEDGE****EK-3.1.A.1**

A switch contains a content addressable memory (CAM) table to track which devices are connected to which physical ports.

**EK-3.1.A.2**

When a switch receives a frame, the source MAC address and the corresponding physical port that received the frame is stored in the switch's CAM table. A typical switch operates at the data link layer (Layer 2) of the OSI model.

**EK-3.1.A.3**

When a switch receives a frame, it will look up the destination MAC address in its CAM table and send the frame out of the corresponding physical port, or all other physical ports if the MAC address is not found.

**LO-3.1.B**

Explain why the use of virtual local area networks (VLANs) can improve network performance and security.

**EK-3.1.B.1**

VLANs allow for the segmentation of a network, through which subsets of the devices physically connected to a switch can be grouped into separate, logical LANs.

**EK-3.1.B.2**

VLANs increase network performance because network traffic is also separated into smaller logical LANs. This means that messages can reach their destinations faster because they are not competing with network traffic from other LANs.

**EK-3.1.B.3**

VLANs increase network security because any broadcast messages are limited to a specific VLAN as opposed to the larger network. This limits the number of messages a host might receive not intended for it.

**SUGGESTED SKILLS:****1.B**

Explain relationships among data, computer networking, and cybersecurity.

**2.B**

Determine security controls that address potential vulnerabilities.

**TOPIC 3.2**  
**Switch Security****LEARNING OBJECTIVE****LO-3.2.A**

Explain how MAC spoofing and MAC flooding can be used to attack a network switch.

**LO-3.2.B**

Explain how port security mitigates common risks associated with a network switch.

**ESSENTIAL KNOWLEDGE****EK-3.2.A.1**

MAC spoofing occurs when a device on a network uses software to mask the original MAC address associated with its NIC.

**EK-3.2.A.2**

MAC spoofing allows a device to mimic the MAC address of another device on a network, potentially enabling it to receive network traffic not intended for it.

**EK-3.2.A.3**

MAC flooding occurs when a switch is sent enough frames containing different source MAC addresses to overflow the CAM table, or cause the CAM table to run out of memory.

**EK-3.2.A.4**

MAC flooding can cause the switch to fall into a fail-open state, which results in all network traffic being broadcast to all nodes on the network rather than directed to the intended recipient.

**EK-3.2.B.1**

Port security applies restrictions on physical ports on a switch.

**EK-3.2.B.2**

A physical port on a switch can be set as "up" or "down." When a physical port is set to "up," a physical device connected to that port is able to send and receive network traffic through that port. When a physical port is set to "down," all network traffic on that port is dropped. Setting unused ports to down can prevent unauthorized devices – which could be used to launch a network attack – from physically connecting to the network.

**EK-3.2.B.3**

A physical port on a switch can be set to only allow a certain number of MAC addresses or a specific set of MAC addresses to use that port. Any traffic that is beyond the limit of addresses or not on the list of addresses is dropped. Limiting the number of MAC addresses associated with a physical port can prevent unauthorized devices from physically connecting to the network. It can also protect the switch's CAM table from being flooded.

**SUGGESTED SKILLS:****1.A**

Explain relationships among data, computer networking, and cybersecurity.

**2.A**

Determine appropriate endpoints, network appliances, transmission media, and communication protocols to meet network requirements.

**3.A**

Connect and configure network components using appropriate media, communication protocols, and commands.

## TOPIC 3.3

# More on Protocols

**LEARNING OBJECTIVE****LO-3.3.A**

Describe the purpose and functions of common application layer protocols.

**ESSENTIAL KNOWLEDGE****EK-3.3.A.1**

File Transfer Protocol (FTP) is a standard network protocol for transferring files between a computer client and a computer server. FTP uses default ports 20 and 21.

**EK-3.3.A.2**

SFTP (Secure File Transfer Protocol) is a secure protocol that uses encryption to transfer files between networked devices. SFTP uses default port 22.

**EK-3.3.A.3**

SMTP (Simple Mail Transfer Protocol) is a protocol used for exchanging emails between servers. SMTP uses default port 25.

**EK-3.3.A.4**

POP3 (Post Office Protocol version 3) is used to retrieve email messages from a mail server to a client. POP3 uses default port 110.

**EK-3.3.A.5**

IMAP (Internet Message Access Protocol) is used to retrieve email messages from a mail server to a client. IMAP uses default port 143.

**EK-3.3.A.6**

NTP (Network Time Protocol) is used to synchronize clocks on a network. Unsynchronized clocks can make the investigation of security incidents difficult because the timestamps of logged events may not be correct. NTP uses default port 123.

**EK-3.3.A.7**

RDP (Remote Desktop Protocol) is a proprietary protocol developed by Microsoft used to remotely access a computer on a network. RDP allows users to interact with the computer from a graphical user interface as if they were physically sitting in front of it. RDP uses default port 3389.

**EK-3.3.A.8**

Secure Shell (SSH) is a network protocol used to remotely access a device on a network. Unlike its predecessor Telnet, SSH encrypts all transmitted data and requires users to authenticate. SSH uses default port 22, and Telnet uses default port 23.

*continued on next page*

**LEARNING OBJECTIVE****LO-3.3.B**

Determine the OSI and TCP/IP layers associated with common network protocols.

**ESSENTIAL KNOWLEDGE****EK-3.3.B.1**

Each layer of the OSI and TCP/IP models uses various protocols to define how to format or interpret data as it is encapsulated or de-encapsulated as it travels through the layers. The layer a protocol belongs to depends on its function.

**EK-3.3.B.2**

Application layer protocols define the interface between applications and the underlying networking infrastructure. Software applications apply these protocols to enable users to access specific services. FTP, SFTP, SMTP, POP3, IMAP, NTP, RDP, and SSH are application layer protocols.

**EK-3.3.B.3**

Network layer protocols are used to send data from a source host to a destination host on a different network segment. IPv4 and IPv6 are network layer protocols.

**EK-3.3.B.4**

Data link layer protocols are used to send data from a source host to a destination host on the same network segment. ARP is a data link layer protocol.

**SUGGESTED SKILLS:****1.A**

Explain relationships among data, computer networking, and cybersecurity.

**2.B**

Determine security controls that address potential vulnerabilities.

**3.A**

Connect and configure network components using appropriate media, communication protocols, and commands.

**3.B**

Test network connectivity, verify network requirements, and troubleshoot network issues.

**TOPIC 3.4**

# LAN Configuration and Troubleshooting

**LEARNING OBJECTIVE****LO-3.4.A**

Configure a small local area network (LAN) containing a switch and multiple endpoints.

**ESSENTIAL KNOWLEDGE****EK-3.4.A.1**

A console cable is used to connect a computer to a switch to access the switch's management console. A physical cable is used to connect the switch to other network devices.

**EK-3.4.A.2**

Endpoints on the network must have their IP addresses and subnet masks configured to meet the requirements of the network.

**EK-3.4.A.3**

Settings on a network switch can be manually assigned using the command line interface (CLI) or the graphical user interface (GUI) of the switch's management console.  
NOTE: For this course, students may use either CLI or GUI to configure a switch.

**EK-3.4.A.4**

For the switch to be able to pass traffic in a LAN, the switch's access password, IP address, and subnet mask must be set.

**LO-3.4.B**

Determine the appropriate security measures to address vulnerabilities in a local area network (LAN) containing a switch and multiple endpoints.

**EK-3.4.B.1**

Statically setting an IP address decreases the chances of unexpected IP address conflicts or changes. This can ensure higher rates of network resource availability and can be useful for any network device or endpoint that needs to provide consistent service.

**EK-3.4.B.2**

Grouping devices into VLANs based on patterns of network traffic can increase network performance and security.

**EK-3.4.B.3**

Changing default login credentials on all network devices, requiring strong passwords for all user accounts, and limiting administrative privileges to only specific accounts prevent unauthorized users from accessing the network and its configurations.

*continued on next page*

**LEARNING OBJECTIVE****LO-3.4.B**

Determine the appropriate security measures to address vulnerabilities in a local area network (LAN) containing a switch and multiple endpoints.

**LO-3.4.C**

Troubleshoot common network problems in a LAN containing a switch and multiple endpoints.

**ESSENTIAL KNOWLEDGE****EK-3.4.B.4**

Port security on a switch can be configured to meet network requirements and minimize the risk of external access to secure data.

**EK-3.4.B.5**

Wireless networks can be configured to use the highest level of encryption enabled by the network device.

**EK-3.4.B.6**

Updating all devices to the most current firmware, operating system, and application software can increase network performance and security because software updates often include performance fixes and patches for known vulnerabilities.

**EK-3.4.C.1**

The troubleshooting process generally includes the following steps:

- i. identifying the problem
- ii. establishing a theory of probable causes
- iii. testing the theory to determine root cause
- iv. establishing a plan of action and implementing the solution
- v. verifying the solution
- vi. implementing preventative measures
- vii. documenting findings, actions, and outcomes

**EK-3.4.C.2**

ping is a network utility that can be used to test network (host-to-host) connectivity with the Internet Control Message Protocol (ICMP). By learning what hosts can and cannot communicate, a network administrator can isolate where in the network a problem might be.

**EK-3.4.C.3**

Disconnected or faulty network hardware like cables, NICs, and network devices can contribute to loss of network connectivity. Using tools like cable certifiers and replacing hardware with working spares can help to isolate and fix hardware-related network problems.

**EK-3.4.C.4**

Incorrect IP addresses, subnet masks, and other configuration settings can cause network connection problems. Checking and fixing configuration settings for network devices and hosts can restore network connectivity.

## **CK NETWORKING FUNDAMENTALS**

### **UNIT 4**

# **Advanced LAN Topics**

THIS PAGE IS INTENTIONALLY LEFT BLANK.

# Advanced LAN topics

## KEY QUESTIONS

- How does an email get from one device to another?
- What is “the Internet” anyway? Is it the same as “the cloud”?
- How does putting in the Wi-Fi password let me onto the Internet?

## UNIT OBJECTIVES

By the end of this unit, students should be able to:

- Configure a router to enable inter-LAN communication
- Apply subnetting to segment an IPv4 network
- Enable appropriate security features for a wireless LAN

## Developing Understanding

Unit 4 introduces students to the network and transport layers of the OSI model, where network routers are responsible for sending data all around the world. Students will dive deeper into internet protocol (IP) addressing and router configuration, which are fundamental to understanding how the Internet works. In this unit, students will build the understanding that a router uses IP addressing to determine whether messages should be sent outside its own network and how traffic leaving the network is moved through different routers until it reaches its intended destination. Furthermore, for some types of network traffic, recipients will send acknowledgements to the sender for received data. In this unit students will also explore how wireless networks are different from wired networks and learn how to split a network into small sub-networks (subnets).

## Building Cybersecurity Skills

When designing a network, understanding the structures of both IPv4 and IPv6 addressing is critical for determining the most appropriate addressing scheme. IP addressing concepts and their mathematical underpinnings can be challenging for any learner at first; it is common for students to struggle with applying mathematical conversions within the multi-step process of determining appropriate subnets for a network. Contextualizing these mathematical conversions can be beneficial and grounding for students. In this section, students will learn basic router configuration and should continue to practice applying troubleshooting techniques to ensure device and network connectivity.

## UNIT AT A GLANCE

| Topic                              | Learning Objectives  | Suggested Instructional Periods |                 |
|------------------------------------|--|---------------------------------|-----------------|
|                                    |  | Teach & Labs                    | Review & Assess |
| <b>4.1 IPv4 Addressing</b>         | <b>4.1.A</b> Determine whether two hosts are on the same network using their IPv4 addresses and subnet masks.<br><b>4.1.B</b> Explain how MAC addresses, IPv4 addresses, and subnet masks are used to direct network traffic in a LAN.<br><b>4.1.C</b> Describe the purposes of public and private IPv4 addresses. | 4–5                             | 1               |
| <b>4.2 Routing</b>                 | <b>4.2.A</b> Explain how a router determines where to send data it receives.<br><b>4.2.B</b> Configure a network router so that separate LANs directly connected to the router can communicate.<br><b>4.2.C</b> Explain how data travels through devices between different networks.                               | 3–4                             | 1               |
| <b>4.3 Subnetting</b>              | <b>4.3.A</b> Explain why subnetting is used in computer networks.<br><b>4.3.B</b> Apply a variable length subnet mask (VLSM) to appropriately subnet an IPv4 network.  | 3–4                             | 1–2             |
| <b>4.4 Wireless Networks</b>       | <b>4.4.A</b> Explain why a network might contain both wired and wireless segments.<br><b>4.4.B</b> Explain how encryption and changing default settings impact the security of wireless networks.  | 2–3                             | 1               |
| <b>4.5 Network Troubleshooting</b> | <b>4.5.A</b> Troubleshoot common network problems using appropriate network tools.   | 4–5                             | 1–2             |

**SUGGESTED SKILLS:****1.A**

Describe and explain concepts and processes related to data, computer networking, and cybersecurity.

**2.A**

Determine appropriate endpoints, network appliances, transmission media, and communication protocols to meet network requirements.

## TOPIC 4.1

# IPv4 Addressing

### LEARNING OBJECTIVE

**LO-4.1.A**

Determine whether two hosts are on the same network using their IPv4 addresses and subnet masks.

### ESSENTIAL KNOWLEDGE

**EK-4.1.A.1**

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.

**EK-4.1.A.2**

A subnet mask consists of 32 bits that has a string of 1 bits followed by a string of 0 bits. Subnet masks are written either as four period-separated decimal numbers or with Classless Inter-Domain Routing (CIDR) notation, which uses a forward slash followed by the number of 1 bits in the subnet mask.

Illustrative Examples:

- 255.255.248.0
- /21

**EK-4.1.A.3**

The network bits of an IPv4 address are those that positionally correspond to the 1s of the subnet mask. The host bits of an IPv4 address are those that positionally correspond to the 0s of the subnet mask. Two IPv4 addresses belong to the same network when they have matching network bits and subnet masks.

**LO-4.1.B**

Explain how MAC addresses, IPv4 addresses, and subnet masks are used to direct network traffic in a LAN.

**EK-4.1.B.1**

Since the network bits must match for any two hosts on a network, any host on that specific network must have an IP address that falls within a certain range.

**EK-4.1.B.2**

On a network, the first IP address is reserved as the network address, which identifies the network itself. The last IP address is reserved as the broadcast address, which is used when data are to be sent to all hosts on that network.

**EK-4.1.B.3**

When a host sends data to a host on a different network, the data must go through a router.

*continued on next page*

**LEARNING OBJECTIVE****LO-4.1.B**

Explain how MAC addresses, IPv4 addresses, and subnet masks are used to direct network traffic in a LAN.

**LO-4.1.C**

Describe the purposes of public and private IPv4 addresses.

**ESSENTIAL KNOWLEDGE****EK-4.1.B.4**

When addressing data to be sent, a sending host will compare its own IPv4 address and subnet mask with that of the destination host. When the destination host is on the same network, it sends the data to that host directly. Otherwise, it will send the data to the default gateway (router) so it can be sent to the appropriate network.

**EK-4.1.B.5**

When addressing data to be sent on the LAN, the host uses the MAC address of either the destination host if on the LAN or the default gateway (router) if the destination host is on the separate LAN. If the MAC address is not known, the sending host will send an Address Resolution Protocol (ARP) request to the network to learn which MAC address is associated with the target IPv4 address.

**EK-4.1.B.6**

A host will keep entries of known MAC address and IPv4 pairings in an ARP table. The host will reference this table before sending an ARP request to the network. `arp` is a command line tool that is used to view information related to a host's ARP table.

**EK-4.1.C.1**

Public addresses are addresses that can be assigned to organizations to be used externally on the Internet. Private addresses are addresses that can only be used within a LAN, as routers are programmed to drop any data addressed to a private address.

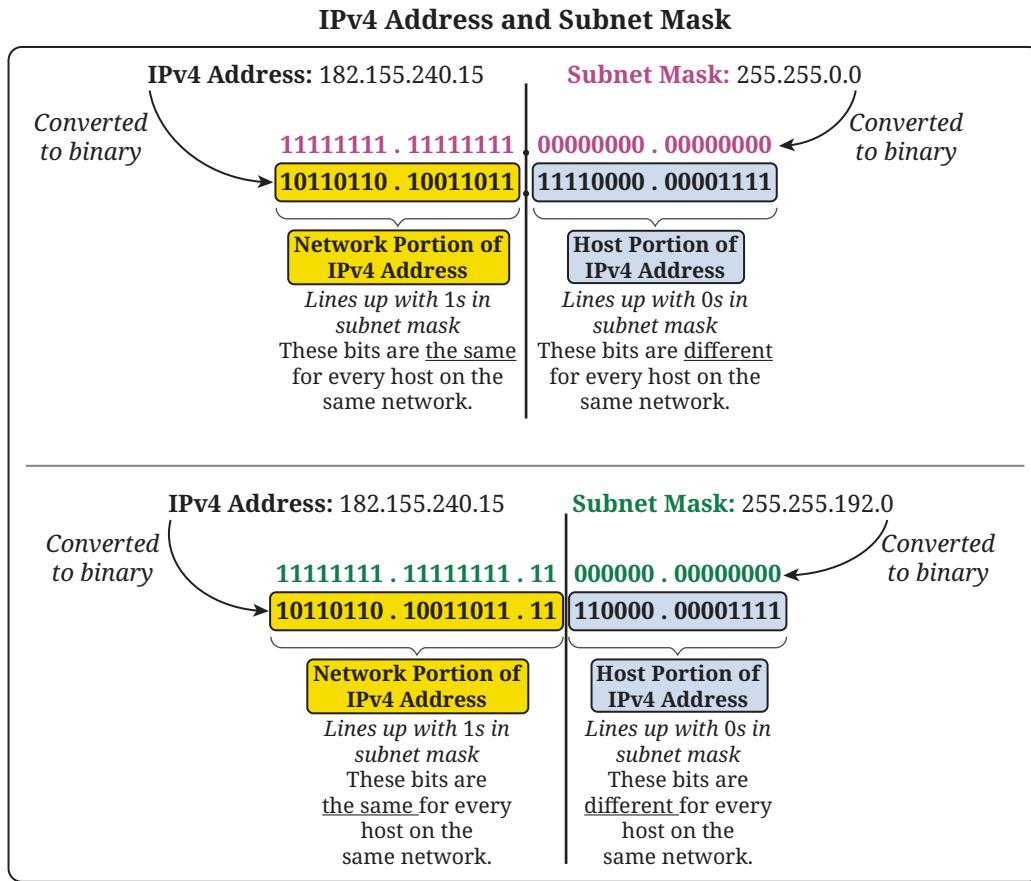
**EK-4.1.C.2**

Private addresses are often used within a LAN for network address translation (NAT), which allows a network to have an internal IP addressing scheme so all hosts within that network are associated with one external, public IP address. NAT helps conserve the use of public IP addresses.

**EK-4.1.C.3**

Private addresses are any addresses that fall in the following ranges:

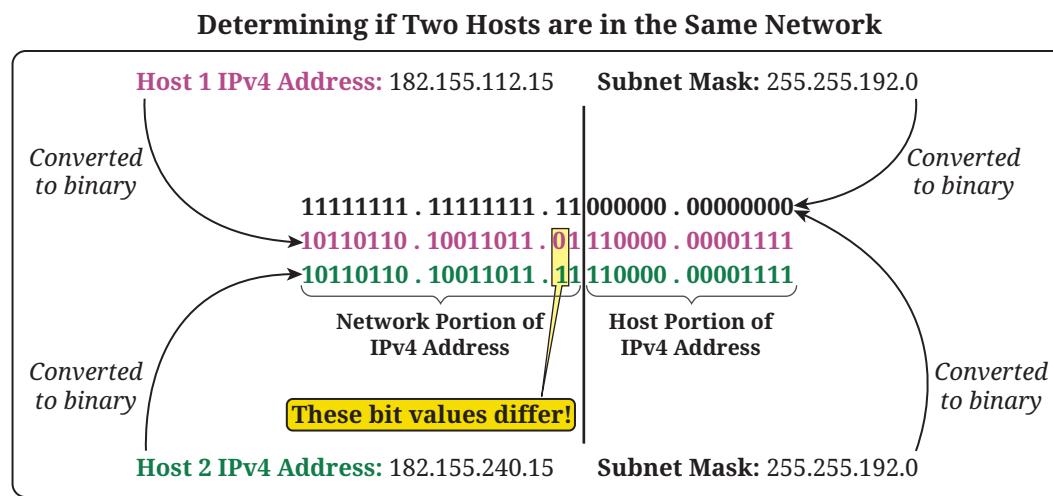
- 10.0.0.0 to 10.255.255.255
- 172.16.0.0 to 172.31.255.255
- 192.168.0.0 to 192.168.255.255



Every IPv4 address must be paired with a subnet mask. The subnet mask determines which bits of the IPv4 address identify the host's network and which bits identify the host itself within the network. The **network portion** of the IPv4 address contains the bits that positionally correspond to the 1s of the subnet mask. The **host portion** of the IPv4 address contains the bits that positionally correspond to the 0s of the subnet mask.

In this example, the IPv4 addresses are the same, but the subnet masks are different. Notice how having different subnet masks changes the **network portion** and **host portion** of each address.

**Figure 4.1a:** IPv4 Address and Subnet Mask



When two unique hosts have the same bit values in the network portion of their IPv4 addresses, they are considered to be in the same network. When two hosts have different bit values in their respective network portions, they are on different networks and require a router to talk to one another.

In this example, **Host 1** and **Host 2** have different IPv4 addresses, but the same subnet mask. Because one of the bits in their respective network portions differ, **Host 1** and **Host 2** are on *different* networks and any communications between them will need to go through a router.

**Figure 4.1b:** Determining if Two Hosts Are in the Same Network

## TOPIC 4.2

# Routing

### LEARNING OBJECTIVE

**LO-4.2.A**

Explain how a router determines where to send data it receives.

### ESSENTIAL KNOWLEDGE

**EK-4.2.A.1**

A router is a network device that connects and manages traffic among LANs using the IP addresses on data packets. The router often acts as the edge between the public network and the private (internal) network. Routers operate at Layer 3 of the OSI model.

**EK-4.2.A.2**

A router contains a routing table to track which physical interfaces are associated with other networks. When it receives data, it compares the destination IP address on the data with the entries in its routing table to determine which physical interface the data should be sent through or if the data should be dropped.

**EK-4.2.A.3**

Routes in a routing table can be set statically (manually) by a network administrator, or they can be set dynamically using a routing protocol. Routing protocols use different algorithms to share known routing information between connected routers.

Illustrative Examples: RIP, OSPF, BGP, ISIS

**EK-4.2.A.4**

A typical routing table entry will contain the following information:

- a destination network's address and subnet mask
- the address of the next hop, which is the device that is one step closer to getting the data to the intended destination
- the physical interface associated with the next hop
- the metric, which is a measure of the cost (e.g., number of hops, time, etc.) associated with the next hop

**EK-4.2.A.5**

When multiple next hops are available for the destination network, the hop with the lowest metric at that time will be chosen. The value of the metric can change over time with changing circumstances in different networks, which can result in data taking different paths at different times. How a metric is calculated can differ with different routing protocols.

**EK-4.2.A.6**

When the router prepares to send the data to the next hop, it will de-encapsulate the frame and encapsulate it with updated data link (Layer 2) information.

**SUGGESTED SKILLS:****1.A**

Describe and explain concepts and processes related to data, computer networking, and cybersecurity.

**2.A**

Determine appropriate endpoints, network appliances, transmission media, and communication protocols to meet network requirements.

**3.A**

Connect and configure network components using appropriate media, communication protocols, and commands.

*continued on next page*

**LEARNING OBJECTIVE****LO-4.2.B**

Configure a network router so that separate LANs directly connected to the router can communicate.

**LO-4.2.C**

Explain how data travels through devices between different networks.

**ESSENTIAL KNOWLEDGE****EK-4.2.B.1**

A physical cable is used to directly connect the router to each LAN.

**EK-4.2.B.2**

A router must have its password, IP address and subnet mask, and interface information set to begin routing traffic for a network. NOTE: For this course, students may use either CLI or GUI to configure a router.

**EK-4.2.B.3**

For a router to be able to communicate between two LANs, a routing table entry must exist that ensures each LAN's network address is associated with the appropriate interface.

**EK-4.2.B.4**

`route` is a common command used to review and modify the entries of a routing table. `route` is also used to modify the routing protocols used by a router.

**EK-4.2.C.1**

A path between two computing devices on a computer network is a sequence of directly connected computing devices that begins at the sender and ends at the receiver.

**EK-4.2.C.2**

Data from the sending host will find a path to its destination host through one of two ways. If the destination host is on the same LAN, the data travel through one or more switches. If the destination host is outside of the LAN, the data travel through one or more routers; when the data reach the router for the LAN of the destination host, they are sent through one or more switches on that LAN to reach the destination host.

**EK-4.2.C.3**

`traceroute` (Mac/Linux) and `tracert` (Windows) are command line tools that show a packet's path from the source network to the destination network by showing the IPv4 addresses at each hop in the path.

## TOPIC 4.3

# Subnetting

### LEARNING OBJECTIVE

**LO-4.3.A**

Explain why subnetting is used in computer networks.

### ESSENTIAL KNOWLEDGE

**EK-4.3.A.1**

Early network address architecture used classful addressing which divided the IPv4 address space into five classes of different sizes: Class A, Class B, Class C, Class D, and Class E. Class A, Class B, and Class C were assigned to organizations based on size – Class A addresses to the largest organizations, and Class C address to the smallest organizations. Class D and Class E addresses are reserved for other purposes.

**EK-4.3.A.2**

Class A, Class B, and Class C addresses are assigned specific subnet masks: 255.0.0.0, 255.255.0.0, and 255.255.255.0, respectively.

**EK-4.3.A.3**

Classful addressing assigned organizations a fixed number of addresses, resulting in many IP addresses not being used. Large organizations also experienced degraded network performance because all of the hosts were on the same network, sharing the same bandwidth of the network. In general, classful addressing is no longer used.

**EK-4.3.A.4**

Classless addressing, also known as classless inter-domain routing (CIDR), uses different subnet masks from those associated with Class A, Class B, and Class C addresses. This allows for subnetting, where a larger network is split into smaller subnetworks (also known as subnets).

**EK-4.3.A.5**

Subnetting decreases the number of nodes on a single subnet, allowing data to find its intended destination faster within a large network. It also allows for different sizes of IP address spaces to be assigned to organizations, so fewer IP addresses go unused.

**SUGGESTED SKILLS:****1.B**

Explain relationships among data, computer networking, and cybersecurity.

**2.A**

Determine appropriate endpoints, network appliances, transmission media, and communication protocols to meet network requirements.

**3.A**

Connect and configure network components using appropriate media, communication protocols, and commands.

**3.B**

Test network connectivity, verify network requirements, and troubleshoot network issues.

**3.C**

Create technical documentation of network layouts, settings, and configurations.

*continued on next page*

**LEARNING OBJECTIVE****LO-4.3.B**

Apply a variable length subnet mask (VLSM) to appropriately subnet an IPv4 network.

**ESSENTIAL KNOWLEDGE****EK-4.3.B.1**

VLSM (variable length subnet mask) allows for subnets to use custom subnet masks. This allows for different sized subnets and more efficient usage of each IP address space.

**EK-4.3.B.2**

A subnet mask paired with an IPv4 address can be used to determine the size of a network and the range of IPv4 addresses that can be assigned to hosts on that network.

**EK-4.3.B.3**

Classless addressing and custom subnet masks subdivide the host bits of the IPv4 addressing scheme into subnet bits and host bits.

**EK-4.3.B.4**

The number of hosts a network can accommodate is equal to 2 to the power of the host bits minus 2, because the first and last addresses on a network are reserved for the network address and broadcast address, respectively.

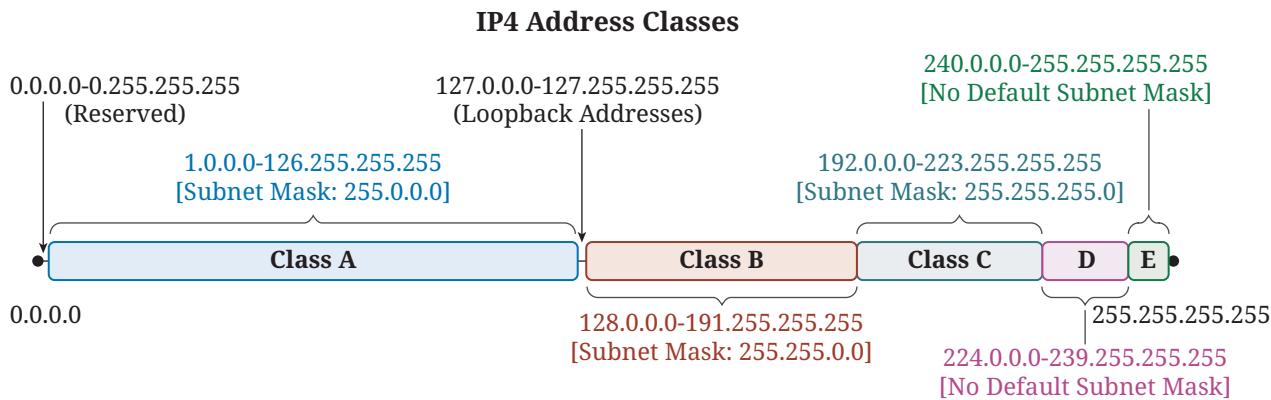
Illustrative Example: A network with 8 host bits can accommodate 254 hosts.

**EK-4.3.B.5**

The number of subnets and the size of each subnet depend on the number of bits allocated from the host portion. The number of subnets can be up to 2 to the power of the number of bits allocated.

**EK-4.3.B.6**

An appropriate subnet size is the smallest possible network size that accommodates the required number of hosts on a network.



In the first kind of network address architecture, IPv4 addresses were divided into 5 different classes with different ranges of IPv4 addresses, so they could be assigned to organizations based on the number of nodes needing an IP address in each organization. Class A, Class B and Class C addresses are the only ones commercially available.

Figure 4.3: IPv4 Address Classes

**SUGGESTED SKILLS:****1.B**

Explain relationships among data, computer networking, and cybersecurity.

**2.B**

Determine security controls that address potential vulnerabilities.

**TOPIC 4.4****Wireless Networks****LEARNING OBJECTIVE****LO-4.4.A**

Explain why a network might contain both wired and wireless segments.

**LO-4.4.B**

Explain how encryption and changing default settings impact the security of wireless networks.

**ESSENTIAL KNOWLEDGE****EK-4.4.A.1**

A wired network uses cables to connect devices, such as laptop or desktop computers, to the Internet or another network. A dedicated NIC is required for a device to access a wired network.

**EK-4.4.A.2**

A wireless network uses electromagnetic waves to communicate between devices on the network. A dedicated NIC is required for a device to access a wireless network.

Illustrative Examples: Cellular phones, wireless sensors, satellite dish receivers, laptops

**EK-4.4.A.3**

Wired networks are more secure, more stable, more reliable, and faster than wireless networks.

**EK-4.4.A.4**

Wireless networks are more convenient, allow for mobility, and are easier to set up than wired networks.

**EK-4.4.A.5**

Implementing both wired and wireless segments in a network can balance the needs of its users and the security of its data.

**EK-4.4.B.1**

Wireless transmissions can apply encryption standards such as WEP, WPA, WPA2, and WPA3. Encrypting the data before it is transmitted makes it more difficult for an adversary to capture and read the data when it is in transit.

**EK-4.4.B.2**

Some encryption standards are more secure than others. WEP and WPA are more easily broken compared to WPA2 and WPA3.

**EK-4.4.B.3**

Default login credentials for wireless networking devices should be changed to prevent unauthorized users from altering network settings and accessing protected data.

**EK-4.4.B.4**

Creating a unique SSID (service set identifier) and strong authentication measures for the wireless network prevents unauthorized users from accessing the network using password cracking methods.

## TOPIC 4.5

# Network Troubleshooting

### LEARNING OBJECTIVE

**LO-4.5.A**

Troubleshoot common network problems using appropriate network tools.

### ESSENTIAL KNOWLEDGE

**EK-4.5.A.1**

Power fluctuations can cause network issues. Tools like power quality analyzers can help monitor the electrical power being supplied to the network. Devices like an uninterruptible power supply (UPS) can also provide battery power backup and deliver a consistent power level to the network.

**EK-4.5.A.2**

Signal interference can cause network connectivity issues. Using tools like spectrum analyzers can help identify sources of interference, which may include objects emitting electromagnetic fields or objects that use common frequencies in wireless networking.

**EK-4.5.A.3**

Network congestion can cause poor network performance. Packet analysis tools, SNMP (Simple Network Management Protocol) monitoring, and flow analyzers can be used to identify the sources of network congestion.

**EK-4.5.A.4**

IP address misconfigurations, including issues with DHCP scope and server connections, as well as DNS settings, can cause network connection issues. Checking and fixing settings on network devices and hosts can help restore network connectivity.

**EK-4.5.A.5**

Application software issues can affect network performance. Ensuring that applications are compatible with operating systems and other software, updating or using correct versions of software, and checking for correct application configurations can help resolve network issues.

**SUGGESTED SKILLS:****2.B**

Determine security controls that address potential vulnerabilities.

**3.B**

Test network connectivity, verify network requirements, and troubleshoot network issues.

THIS PAGE IS INTENTIONALLY LEFT BLANK.

## **CK NETWORKING FUNDAMENTALS**

### **UNIT 5**

# **Network Security**

THIS PAGE IS INTENTIONALLY LEFT BLANK.

# Network Security

## KEY QUESTIONS

- How do some websites get blocked on a network?
- What are the ways my school district protects my personal information?
- When digital crimes are committed, how do investigators figure out what happened?

## UNIT OBJECTIVES

By the end of this unit, students should be able to:

- Enable a firewall to protect a network
- Segment a network for increased security
- Apply a suite of security controls at different layers to implement a defense-in-depth strategy

## Developing Understanding

Unit 5 focuses on network security controls. Students will learn about different categories of security controls and their purposes. Students will learn how organizations use physical and administrative controls to deter and mitigate vulnerabilities to systems and networks. Students will also learn about technical network security controls like firewalls, network segmentation, and network monitoring. Finally, students will learn about defense in depth including how security controls are layered to increase the total security of an organization.

## Building Networking Skills

Valuable information is stored on computers connected to networks, and valuable information travels across networks. This makes networks, and the devices on those networks, targets for adversaries who seek to disrupt, steal, harm, or destroy systems and networks and the data they contain. Learning about networks vulnerabilities will give students insight into how security controls can be used to mitigate vulnerabilities and protect computers, networks, and data.

**UNIT AT A GLANCE**

| <b>Topic</b>  | <b>Learning Objectives</b>  | <b>Suggested Instructional Periods</b> |                            |
|---|---|--|----------------------------|
|   |   | <b>Teach &amp; Labs</b>                | <b>Review &amp; Assess</b> |
| <b>5.1 Introduction to Security Controls</b>        | <b>5.1.A</b> Describe the types of security controls used to protect computers, networks, and data.<br><b>5.1.B</b> Explain how security controls are used to protect an organization.  | 2–3                                    | 0–1                        |
| <b>5.2 Physical and Administrative Controls</b>     | <b>5.2.A</b> Explain how physical controls are used to protect networks.<br><b>5.2.B</b> Explain how administrative controls are used to protect networks.  | 2–3                                    | 0–1                        |
| <b>5.3 Technical Controls: Firewalls</b>            | <b>5.3.A</b> Describe the different types of firewalls.<br><b>5.3.B</b> Explain how a firewall allows or denies the flow of network traffic.<br><b>5.3.C</b> Describe the impacts of allow lists and deny lists on security.  | 3–4                                    | 1–2                        |
| <b>5.4 Technical Controls: Network Segmentation</b> | <b>5.4.A</b> Describe the benefits of network segmentation.<br><b>5.4.B</b> Explain how different techniques for network segmentation increase a network's security.  | 2–4                                    | 1–2                        |
| <b>5.5 Technical Controls: Network Monitoring</b>   | <b>5.5.A</b> Describe the characteristics of an intrusion detection system (IDS) and an intrusion protection system (IPS).<br><b>5.5.B</b> Describe the security benefits of logging network events.  | 1–3                                    | 1                          |
| <b>5.6 Defense in Depth</b>                         | <b>5.6.A</b> Explain why a defense-in-depth security strategy is necessary to optimally protect an organization.<br><b>5.6.B</b> Explain how an organization selects which security controls to implement.<br><b>5.6.C</b> Determine a combination of security measures to harden a networking environment. | 3–4                                    | 1–2                        |

## TOPIC 5.1

# Introduction to Security Controls

### LEARNING OBJECTIVE

**LO-5.1.A**

Describe the types of security controls used to protect computers, networks, and data.

**LO-5.1.B**

Explain how security controls are used to protect an organization.

### ESSENTIAL KNOWLEDGE

**EK-5.1.A.1**

Security controls are measures implemented to protect the confidentiality, integrity, and availability of data used by an organization.

**EK-5.1.A.2**

Technical controls are implemented using computer hardware and software.

**EK-5.1.A.3**

Administrative controls are implemented using policies and procedures, including user education.

**EK-5.1.A.4**

Physical controls are implemented to manage physical access to computing systems and networks.

**EK-5.1.B.1**

Security controls protect an organization through preventative, detective, and corrective functions:

- i. Preventative controls seek to stop attacks from happening.
- ii. Detective controls seek to detect when attacks have occurred.
- iii. Corrective controls seek to address the impact of a security incident after it has occurred.

**SUGGESTED SKILLS:****1.B**

Explain relationships among data, computer networking, and cybersecurity.

*continued on next page*

**LEARNING OBJECTIVE****LO-5.1.B**

Explain how security controls are used to protect an organization.

**ESSENTIAL KNOWLEDGE****EK-5.1.B.2**

Security controls protect multiple facets of an organization's network:

- i. Perimeter security includes controls that focus on preventing attacks from reaching the internal network.
- ii. Network security includes controls that focus on securing network infrastructure so access to one part of the network cannot be leveraged to access another part of the network.
- iii. Host or endpoint security includes controls that focus on security of each host or endpoint device connected to the network.
- iv. Application security includes controls that focus on security of software and applications used on the network.
- v. Data security includes controls that focus on protecting sensitive data from unauthorized access, corruption, or theft.

## TOPIC 5.2

# Physical and Administrative Controls

### LEARNING OBJECTIVE

**LO-5.2.A**

Explain how physical controls are used to protect networks.

**LO-5.2.B**

Explain how administrative controls are used to protect networks.

### ESSENTIAL KNOWLEDGE

**EK-5.2.A.1**

Installing fencing, setting up cameras, and stationing security guards around the building can deter adversaries from trying to physically access an organization's network.

**EK-5.2.A.2**

Locks on doors, server cabinets, and computers can prevent network devices from being accessed or stolen.

**EK-5.2.A.3**

Card readers can be used to ensure only authorized personnel can access areas that house sensitive data.

**EK-5.2.B.1**

Implementing security awareness training teaches users to identify and report suspicious activities like phishing emails and social engineering attacks, preventing them from falling victim to an attack and compromising the network and its data.

**EK-5.2.B.2**

Creating and enforcing security policies and procedures provide a structured approach to managing and protecting an organization's data. Security policies – such as acceptable use policies (AUP), password policies, and data security policies – are documents that outline the principles and strategies an organization uses to protect its data. Procedures are the instructions that detail how to implement a policy.

**SUGGESTED SKILLS:****1.B**

Explain relationships among data, computer networking, and cybersecurity.

**2.B**

Determine security controls that address potential vulnerabilities.

**3.C**

Create technical documentation of network layouts, settings, and configurations.

**SUGGESTED SKILLS:****1.B**

Explain relationships among data, computer networking, and cybersecurity.

**2.B**

Determine security controls that address potential vulnerabilities.

**3.A**

Connect and configure network components using appropriate media, communication protocols, and commands.

**3.B**

Test network connectivity, verify network requirements, and troubleshoot network issues.

## TOPIC 5.3

# Technical Controls: Firewalls

### LEARNING OBJECTIVE

**LO-5.3.A**

Describe the different types of firewalls.

**LO-5.3.B**

Explain how a firewall allows or denies the flow of network traffic.

### ESSENTIAL KNOWLEDGE

**EK-5.3.A.1**

A firewall is used to admit or deny traffic entry into a network or host. A firewall can be a standalone physical device, or it can be software on a device such as a router or an endpoint.

**EK-5.3.A.2**

A host-based firewall permits or denies traffic into or out of a single device, while a network-based firewall permits or denies traffic into or out of a network.

**EK-5.3.A.3**

A stateless firewall filters traffic based on information in packet headers such as IP addresses, ports, and protocols, while a stateful firewall filters traffic based on the state of active connections.

**EK-5.3.A.4**

A next-generation firewall (NGFW) has both the capabilities of typical stateless and stateful firewalls and additional advanced features, such as intrusion prevention, deep packet inspection, and filtering by application type.

**EK-5.3.B.1**

Network administrators set up the rules, called access control lists (ACLs), that firewalls use to permit or deny inbound and outbound network traffic.

**EK-5.3.B.2**

ACLs are checked in order (usually top to bottom), and the first rule that matches the criteria will be executed for the specified data.

**EK-5.3.B.3**

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

*continued on next page*

**LEARNING OBJECTIVE****LO-5.3.C**

Describe the impacts of allow lists and deny lists on security.

**ESSENTIAL KNOWLEDGE****EK-5.3.C.1**

An allow list is a list of entities that are granted permission to access a particular resource. Any entity not listed on the allow list will be implicitly denied access to the resource.

**EK-5.3.C.2**

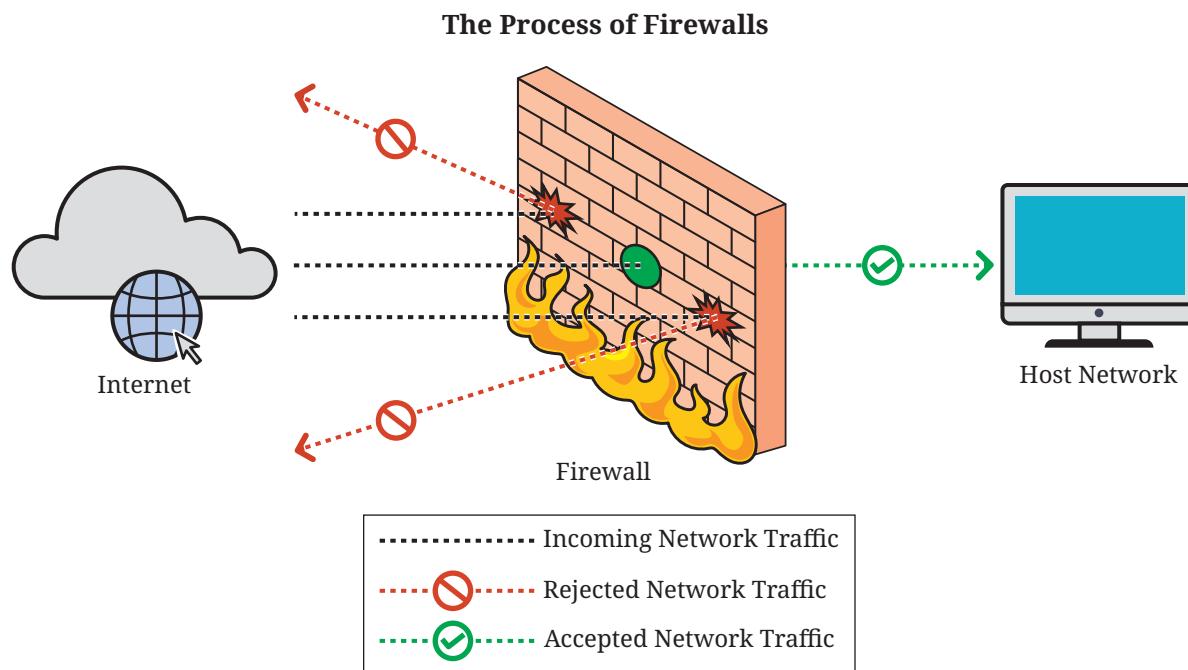
A deny list is a list of entities that are explicitly denied access to a particular resource. Any entity not on that list is implicitly allowed access to the resource.

**EK-5.3.C.3**

Generally, allow lists result in fewer entities being able to access a particular resource. This approach is more proactive, but can lead to more occurrences of legitimate entities to potentially be blocked if they have been unintentionally omitted from the list, impacting the availability of the resource.

**EK-5.3.C.4**

Generally, deny lists result in more entities being able to access a particular resource. This approach is more reactive and can lead to more occurrences of illegitimate entities being able to access the resource, potentially impacting the confidentiality of the data.



A firewall is used to admit or deny traffic entry into a network or host. Firewalls might use source IP addresses, destination IP addresses, or logical ports to filter traffic.

**Figure 5.3:** The Process of Firewalls

**TOPIC 5.4**

# Technical Controls: Network Segmentation

**LEARNING OBJECTIVE****LO-5.4.A**

Describe the benefits of network segmentation.

**ESSENTIAL KNOWLEDGE****EK-5.4.A.1**

Network segmentation refers to the process of dividing a network into smaller, isolated segments or subnetworks (subnets).

**EK-5.4.A.2**

Dividing a network into smaller subnets isolates their network traffic, which can increase the speed of communication because there is less network congestion.

**EK-5.4.A.3**

Network segmentation can prevent attacks affecting one subnet from moving laterally and thus impacting other subnets.

**EK-5.4.A.4**

Network segmentation can allow for different security policies and controls to be applied to different segments of the network, allowing for higher security zones and lower security zones.

**LO-5.4.B**

Explain how different techniques for network segmentation increase a network's security.

**EK-5.4.B.1**

Firewall zones and rules can be used to create a screened subnet (also known as a demilitarized zone, or DMZ), a network segment that sits between public, external networks like the Internet and internal, private networks. The screened subnet typically is a lower security zone than the internal, private networks. A screened subnet typically holds an organization's publicly facing resources, keeping them separated from the internal network.

**EK-5.4.B.2**

Switches can be used to create VLANs, which logically separate devices physically connected to central switches. A message traveling from one VLAN to a different VLAN must go through a Layer 3 or routing-capable device.

**EK-5.4.B.3**

Subnetting can be used to create different subnets based on IP addressing. A message traveling from one subnet to another must go through a Layer 3 or routing-capable device.

**EK-5.4.B.4**

An organization may use a combination of network segmentation techniques to best fit the needs of the organization, its users, its network, and the data it protects.

**SUGGESTED SKILLS:****1.B**

Explain relationships among data, computer networking, and cybersecurity.

**2.B**

Determine security controls that address potential vulnerabilities.

**3.B**

Test network connectivity, verify network requirements, and troubleshoot network issues.

**3.C**

Create technical documentation of network layouts, settings, and configurations.

**SUGGESTED SKILLS:****1.B**

Describe and explain concepts and processes related to data, computer networking, and cybersecurity.

**2.B**

Determine security controls that address potential vulnerabilities.

**TOPIC 5.5**

# Technical Controls: Network Monitoring

**LEARNING OBJECTIVE****LO-5.5.A**

Describe the characteristics of an intrusion detection system (IDS) and an intrusion protection system (IPS).

**LO-5.5.B**

Describe the security benefits of logging network events.

**ESSENTIAL KNOWLEDGE****EK-5.5.A.1**

Both an IDS and IPS monitor and analyze network traffic to identify suspicious behavior or patterns that indicate a security incident has occurred.

**EK-5.5.A.2**

Both an IDS and IPS generate alerts for system administrators when security incidents are detected, but an IPS will also take active measures to mitigate and respond to the security incident.

**EK-5.5.B.1**

Enabling logging of relevant events on network devices and endpoints, such as logons and system configuration changes, can provide useful information when investigating the causes and impacts of security incidents.

**EK-5.5.B.2**

Regular monitoring of log files can help uncover unusual activity on a network, which can help in early identification of security incidents.

## TOPIC 5.6

# Defense in Depth

### LEARNING OBJECTIVE

**LO-5.6.A**

Explain why a defense-in-depth security strategy is necessary to optimally protect an organization.

### ESSENTIAL KNOWLEDGE

**EK-5.6.A.1**

A defense-in-depth strategy, also referred to as layered defense, refers to the use of multiple security controls to protect sensitive data, as opposed to one security solution or product.

**EK-5.6.A.2**

A defense-in-depth strategy allows an organization to address different types of threats, each with a security control most suited to mitigate it.

**EK-5.6.A.3**

A defense-in-depth strategy allows for resilience in data protection so when one security control is bypassed by an adversary, another security control may still prevent access to the network or limit the damage done to the network and its data.

**LO-5.6.B**

Explain how an organization selects which security controls to implement.

**EK-5.6.B.1**

An organization may implement specific security controls to comply with legal requirements based on the types of data the organization uses to provide its products or services.

**EK-5.6.B.2**

To conserve financial resources and employee capacity, an organization will often favor solutions that are cost effective and easy to implement and maintain.

**EK-5.6.B.3**

Organizations typically implement controls that address high-probability security events, high-impact security events, or a combination of both.

**LO-5.6.C**

Determine a combination of security measures to harden a networking environment.

**EK-5.6.C.1**

Securing a network typically involves multiple measures and types of controls applied in combination.

**EK-5.6.C.2**

Security measures are tailored to the requirements of the network, which may include hardware requirements, software requirements, number of users served by the network, and network performance and functionality requirements.

**SUGGESTED SKILLS:****1.B**

Explain relationships among data, computer networking, and cybersecurity.

**2.B**

Determine security controls that address potential vulnerabilities.

**3.C**

Create technical documentation of network layouts, settings, and configurations.

THIS PAGE IS INTENTIONALLY LEFT BLANK.

**CK CYBERSECURITY 1: NETWORKING  
FUNDAMENTALS**

---

# Exam Overview

THIS PAGE IS INTENTIONALLY LEFT BLANK.

# Exam Overview

---

*The Career Kickstart Cybersecurity 1: Networking Fundamentals Exam assesses student understanding of the learning objectives outlined in the course framework. The end-of-course exam is 2 hours long and includes 72 multiple-choice questions representing balanced content from all five units of the framework. For Pilot Year 1, school year 2024–2025, there are no free-response questions.*

*Multiple-choice questions will be presented in two sections of equal length. Each section will include 36 questions; students will have one hour per section. All multiple-choice questions are single-select, meaning they have one correct answer. Multiple-choice questions include the following formats:*

- *Discrete, stand-alone questions*
- *Discrete, stand-alone questions with a stimulus to evaluate*
- *Set-based questions with a shared stimulus to evaluate*

*Stimuli that students may evaluate include, but are not limited to, scenarios, lists of constraints or requirements, network diagrams, command line interfaces, packet captures, tables, and file directories.*

*The exam will be delivered digitally using College Board's Bluebook platform, the same testing platform used for AP and SAT exams.*

# Sample Exam Questions

---

The sample exam questions that follow illustrate the relationship between the course framework and the *CK Cybersecurity 1: Networking Fundamentals* Exam and serve as examples of the types of questions that may appear on the Pilot Year 1 Exam (school year 2024–2025). After the sample questions, you will find a table that shows the correct answers and the learning objectives to which each question relates.

## Multiple-Choice Questions

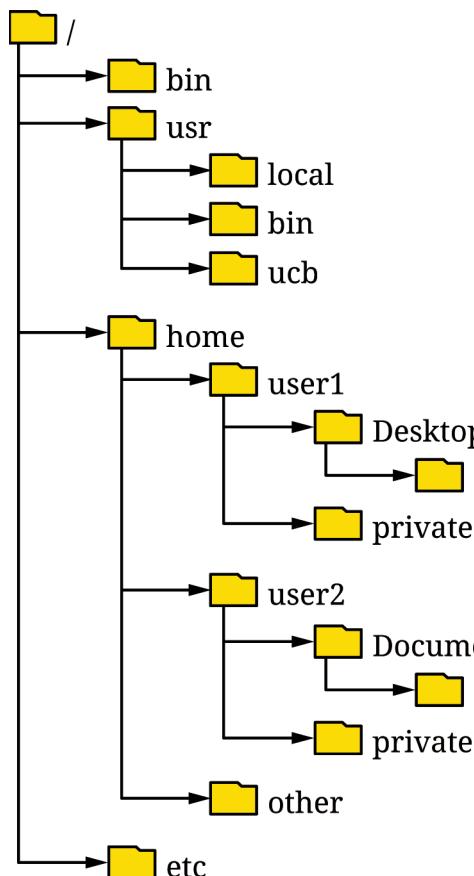
1. An individual wants to make an online purchase using a credit card while connected to public Wi-Fi. Which of the following actions can best protect their credit card information in this situation?
  - (A) Using autofill for the credit card details
  - (B) Using a secure connection to make the purchase
  - (C) Using a unique password for the online account used for making the purchase
  - (D) Using multi-factor authentication to log into the account used for making the purchase
  
2. An attacker successfully bypasses a network's perimeter firewall and gains unauthorized access to the internal network.  
Which **additional** security measure will restrict the attacker's lateral movement even after the perimeter firewall has been compromised?
  - (A) Encryption
  - (B) Network Segmentation
  - (C) Virtual Private Network (VPN)
  - (D) Intrusion Detection System (IDS)

3. Computers on a Local Area Network are configured with default gateway IP address 172.16.2.1 and subnet mask 255.255.255.0.

Which IP address and subnet mask pair belong to the LAN?

- (A) IP Address: 172.16.1.1  
Subnet Mask: 255.255.255.0
- (B) IP Address: 172.16.1.1  
Subnet Mask: 255.255.255.128
- (C) IP Address: 172.16.2.2  
Subnet Mask: 255.255.255.0
- (D) IP Address: 172.16.2.2  
Subnet Mask: 255.255.255.128

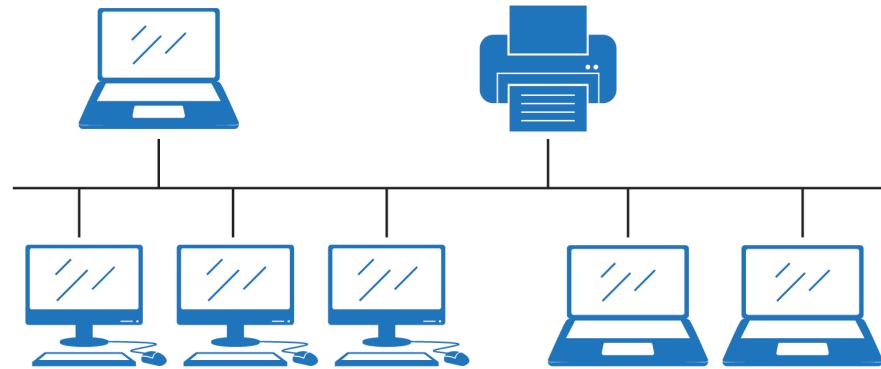
4. Review the following Linux terminal directory.



A user is working in the home directory in their Linux terminal. Which command uses an absolute path to navigate into the directory named "user1"?

- (A) cd user1  
(B) cd /user1  
(C) cd home/user1  
(D) cd /home/user1

5. Review the following network diagram.



Which network topology is represented in the diagram?

- (A) Star topology
- (B) Ring topology
- (C) Mesh topology
- (D) Bus topology

6. A user lists all of the firewall rules in a Kali Linux machine and gets the following output:

```
(kali㉿kali)-[~] $ sudo iptables -L
chain INPUT (policy ACCEPT)
target     prot opt source      destination
DROP       tcp  -- anywhere    anywhere    tcp dpt:ssh
ACCEPT     tcp  -- anywhere    anywhere    tcp dpt:http
DROP       tcp  -- anywhere    anywhere    tcp dpt:ftp
ACCEPT     tcp  -- anywhere    anywhere    tcp dpt:https
DROP       tcp  -- anywhere    anywhere    tcp dpt:ftp-data
ACCEPT     tcp  -- anywhere    anywhere    tcp dpt:ms-wbt-server
```

Which of the following ports is being blocked by the firewall?

- (A) 22
- (B) 80
- (C) 443
- (D) 3389

# **Answer Key and Question Alignment to Course Framework**

| <b>Multiple-Choice Question</b> | <b>Answer</b> | <b>Learning Objective</b> |
|---------------------------------|---------------|---------------------------|
| 1                               | B             | 1.2.A                     |
| 2                               | B             | 5.6.A                     |
| 3                               | C             | 4.1.A                     |
| 4                               | D             | 1.5.B                     |
| 5                               | D             | 2.4.A                     |
| 6                               | A             | 3.3.A                     |

THIS PAGE IS INTENTIONALLY LEFT BLANK.