

Career & Technical Education | Information Technology Networking

Subject Code: 145035

Outcome & Competency Descriptions

Course Description:

Students will install, operate, maintain, and troubleshoot a network. Students will learn to manage, configure, and troubleshoot network infrastructure and media. Students will discuss common network topologies and communication protocols.

Strand 1. Business Operations/21st Century Skills

Learners apply principles of economics, business management, marketing, and employability in an entrepreneur, manager, and employee role to the leadership, planning, developing, and analyzing of business enterprises related to the career field.

Outcome: 1.4. Knowledge Management and Information Technology

Demonstrate current and emerging strategies and technologies used to collect, analyze, record, and share information in business operations.

Competencies

- 1.4.3. Verify compliance with security rules, regulations and codes (e.g., property, privacy, access, accuracy issues, client and patient record confidentiality) pertaining to technology specific to the industry pathway.

Strand 2. IT Fundamentals

Learners apply fundamental principles of IT, including the history of IT and its impact on society, common industry terms, systems theory, information storage and retrieval, database management, and computer hardware, software, and peripheral device configuration and installation. This base of knowledge and skills may be applied across the career field.

Outcome: 2.1. Security, Risks, and Safeguards

Describe the need for security and explain security risks and security safeguards.

Competencies

- 2.1.12. Describe privacy security compliance on systems (e.g., Health Insurance Portability and Accountability Act [HIPAA], Payment Card Industry [PCI], Sarbanes Oxley Act [SOX], Americans with Disabilities Act [ADA], General Data Protection Regulation [GDPR], European Union Data Protection Regulation [EUDPR]).

Outcome: 2.2. Networking Fundamentals

Apply networking fundamentals to infrastructure systems.

Competencies

- 2.2.1. Differentiate between Local Area Networks (LANs), Wide Area Networks (WANs), Wireless Local Area Networks (WLANs), Near Field Communication (NFC) and other network infrastructure.
- 2.2.2. Select the basic point-to-point (PTP) and point-to-multipoint (PTMP) network topologies (e.g., star, ring, tree, network, mesh, irregular) and broadband and baseband transmission methods.
- 2.2.3. Select network storage techniques (e.g., fiber channel, cloud, Fiber Channel over Ethernet [FCoE], Serial Attached SCSI [SAS], Network File Systems [NFS], Network Attached Storage/Server Message Blocks [NAS/SMB], Redundant Array of Inexpensive Disks [RAID]).
- 2.2.4. Differentiate between the Internet, intranets, and extranets.
- 2.2.5. Identify and apply Transmission Control Protocol and Internet Protocol (TCP/IP), Internet Protocol Version 4 (IPv4), Internet Protocol Version 6 (IPv6) applications and services (e.g., rlogin, Simple Mail Transfer Protocol [SMTP], Telecommunications Network [Telnet], File Transfer Protocol [FTP], Domain Name System [DNS], Network File System [NFS], Voice over Internet Protocol [VoIP], Internet Control Message Protocol [ICMP]).
- 2.2.6. Differentiate between cable types (e.g., fiber optic, twisted pair, coaxial) and interfaces.

- 2.2.7. Understand and interpret various elements of a fully qualified domain.
- 2.2.8. Describe the characteristics and uses of networks, network devices, and components (e.g., hubs, switches, routers, firewalls).

Strand 3. Information Security

Learners apply principles of information security to implement and maintain security compliance and network security. Learners select components and mechanisms required for a multilayer defense structure and evaluate and minimize security risks to wired and wireless networks and devices.

Outcome: 3.1. Components of Information Security

Describe the components associated with information security systems.

Competencies

- 3.1.1. Differentiate between authentication and authorization.
- 3.1.2. Compare and contrast authentication techniques (e.g., single factor, multifactor, passwords, biometrics, certificates, Radio Frequency Identification [RFID] cards).
- 3.1.3. Compare and contrast methods of achieving information assurance and integrity and confidentiality (e.g., digital signatures, digital certifications, hashing algorithms, encryption).
- 3.1.4. Describe Virtual Private Networks (VPNs) using tunneling protocols (e.g., Layer 2 Tunneling Protocol [L2TP], Secure Socket Tunneling Protocol [SSTP], Point-to-Point Tunneling Protocol [PPTP]) and encrypting techniques).
- 3.1.5. Discuss the role of certificate authorities (CAs) and Public Key Infrastructure (PKI).

Outcome: 3.2. General Security Compliance

Implement and maintain general security compliance.

Competencies

- 3.2.2. Perform backup, restore, and verification procedures.
- 3.2.3. Describe and assign permissions (e.g., read-only, read-write).
- 3.2.4. Provide user authentication (e.g., assign and reset user accounts and passwords).
- 3.2.5. Install, test, implement, and update virus and malware detection and protection software.
- 3.2.6. Identify sources of virus and malware infection and remove viruses and malware.
- 3.2.7. Provide documentation, training, and support to users on established security procedures.
- 3.2.8. Identify the need for disaster recovery policies and procedures (e.g., business continuity plans, scenario testing).

Outcome: 3.3. Network Security

Implement and maintain network security.

Competencies

- 3.3.1. Describe network security policies (e.g., acceptable use policy, VLAN management, firewall rules).
- 3.3.2. Identify security appliances and tools (e.g., virtual private network gateways, IPS, firewalls, unified threat management, network access controls) and describe the role of each in a networked environment.
- 3.3.3. Devise account administration functions to support network security.
- 3.3.4. Describe Access Control Lists (ACLs) and explain why they are used.
- 3.3.5. Assess risk levels based on vulnerability of the organization, likelihood of risk, and impact on the organization.
- 3.3.6. Describe the relationships among change, vulnerability, configuration, and patch management to protect systems and applications.
- 3.3.7. Train users in network security procedures.

Outcome: 3.4. Multilayer Defense Structure

Explain information technology mechanisms as they apply to a multilayer defense structure.

Competencies

- 3.4.1. Describe available systems for intrusion prevention, detection, and mitigation.
- 3.4.2. Analyze system log files to identify security events.
- 3.4.3. Compare and contrast network analysis software (e.g., network analyzer) and hardware tools to identify security risks and vulnerabilities.

Outcome: 3.5. Wireless Security

Implement secure wireless networks.

Competencies

- 3.5.1. Describe wireless security risks (e.g., unauthorized access) and how to mitigate them.

- 3.5.2. Compare methods of increasing the security of wireless networks and devices (e.g., Media Access Control [MAC] address filtering, Wi-Fi Protected Access [WPA], 802.1x, Remote Authentication Dial In User Service [RADIUS]).
- 3.5.3. Research security standards provided by Institute of Electrical and Electronics Engineers (IEEE).
- 3.5.4. Describe practices and policies for preventing and detecting installation of rogue networks.
- 3.5.5. Describe security practices and policies for personal devices.
- 3.5.6. Implement and test the security of a wireless network.

Strand 4. Infrastructure Systems

Learners apply principles of networking and infrastructure related to the installation, administration, and maintenance of computer networks and components. Knowledge and skills may be applied to network connectivity, cabling, protocols, architecture, classification, topologies, operating systems, Open Systems Interconnection (OSI) standards, data encoding, Quality of Service (QoS), Internet Protocol (IP) addressing, and wide area network (WAN) design.

Outcome: 4.1. Network Infrastructure Build a multinode network.

Competencies

- 4.1.1. Determine the basic point-to-point (PTP) and point-to-multipoint (PTMP) network topologies (e.g., star, ring, tree, mesh, hybrid) and identify broadband and baseband (e.g., Ethernet) transmission methods and standards.
- 4.1.2. Explain packet-switching techniques.
- 4.1.3. Compare the characteristics of connection-oriented and connectionless protocols and select protocols based on given criteria.
- 4.1.4. Identify standard and emerging network technologies (e.g., broadband, satellite, optic, cellular, Local-Area Network (LAN) and WiFi).
- 4.1.5. Describe how Unified Communication (UC) integrates voice, data, and video communications.
- 4.1.6. Configure and build a network.

Outcome: 4.2. Open Systems Interconnection Describe the Open Systems Interconnection (OSI) standard (International Organization for Standardization [ISO] Standard 7498).

Competencies

- 4.2.1. Identify the benefits of using a layered network model.
- 4.2.2. Compare Open Systems Interconnection layer positions and their relationships to one another.
- 4.2.3. Compare the seven layers of the Open Systems Interconnection stack to the four layers of the Transmission Control Protocol/Internet Protocol (TCP/IP) stack.
- 4.2.4. Compare the basics of Transmission Control Protocol/Internet layers, components, and functions.
- 4.2.5. Describe actions to be performed at each of the Open Systems Interconnection physical layers.
- 4.2.6. Explain how the Open Systems Interconnection layers relate to the elements of network communication.

Outcome: 4.3. Network Media

Select, assemble, terminate, and test media.

Competencies

- 4.3.1. Identify the criteria used in selecting media (e.g., physical properties, transmission technologies, transmission span, bandwidth, topology, security, noise immunity, installation considerations, cost).
- 4.3.2. Differentiate between media types (e.g., coaxial, twisted pair, fiber optic) and interfaces.
- 4.3.3. Compare media categories (e.g., fiber (single mode vs. multimode), CAT5, CAT5E, CAT6+).
- 4.3.4. Describe types of media connectors (e.g., Bayonet Neill-Concelman [BNC], RJ-11, RJ-45, LC, ST, SC, Duplex Multimode LC) and grounding and bonding techniques.
- 4.3.5. Identify media standards (e.g., American National Standards Institute [ANSI], Electronic Industries Alliance/Telecommunications Industry Association [EIA/TIA]-568, EIA/TIA-568A and 568B).
- 4.3.6. Identify the advantages and disadvantages of cabling systems.
- 4.3.7. Describe typical problems associated with cable installation.
- 4.3.8. Assemble and test Ethernet cable (e.g., straight-through, crossover, loopback).

Outcome: 4.4. Wireless Communications

Explain wireless communications.

Competencies

- 4.4.1. Compare wireless standards in common use (e.g., Institute of Electrical and Electronics Engineers [IEEE] 802.11, Cellular, Bluetooth, Worldwide Interoperability

- for Microwave Access [WiMAX], Radio Frequency Identification [RFID], Near Field Communication [NFC]).
- 4.4.2. Compare characteristics of wireless signals (e.g., reflection, diffraction, scattering, fading).
- 4.4.3. Differentiate media access methods used by wireless.
- 4.4.4. Describe appropriate applications of wireless technologies to specific communication scenarios.
- 4.4.5. Compare Radio Frequency (RF) functions and principles.

Outcome: 4.5. Wireless Network Solutions

Design and implement wireless network solutions.

Competencies

- 4.5.1. Compare secure wireless solutions operating in ad-hoc, infrastructure, or mesh modes.
- 4.5.2. Describe the frequency ranges and associated rules in the wireless spectrum as managed by the Federal Communication Commission (FCC).
- 4.5.3. Describe the Service Set Identifier (SSID) as used in wireless communications.
- 4.5.4. Select and install access points, wireless Network Interface Cards (NICs), antennas, and other hardware and software components to provide a wireless networking solution as determined by a site and customer survey.
- 4.5.5. Troubleshoot Wireless Local Area Networks (WLANs) using system logs, vendor-provided utilities, and diagnostic tools.
- 4.5.6. Secure the wireless network.
- 4.5.7. Configure a wireless mesh network with non-overlapping channels.

Outcome: 4.6. Network Protocols

Compare network protocols.

Competencies

- 4.6.1. Explain network protocols (e.g., Transmission Control Protocol/Internet Protocol [TCP/IP], User Datagram Protocol [UDP], Internet Protocol Version 4 [IPv4], Internet Protocol Version 6 [IPv6]).
- 4.6.2. Identify the advantages of protocols (e.g., Domain Name System [DNS], File Transfer Protocol [FTP], Hypertext Transfer Protocol [HTTP], Telecommunications Network [Telnet], Remote Desktop Protocol [RDP], Secure Shell [SSH]) and associated port numbers.
- 4.6.3. Explain the purposes of encapsulation and decapsulation (or de-encapsulation) and their relationship to the Open Systems Interconnection (OSI) model.
- 4.6.4. Explain the difference between User Datagram Protocol (UDP) and Transmission Control Protocol (TCP).
- 4.6.5. Identify Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) conventional ports (e.g., Simple Mail Transfer Protocol [SMTP], Telnet, Hypertext Transfer Protocol [HTTP], File Transfer Protocol [FTP]).
- 4.6.6. Explain Transmission Control Protocol/Internet Protocol (TCP/IP) protocol details (e.g., Internet addresses, Address Resolution Protocol [ARP], Reverse Address Resolution Protocol [RARP], IP datagram format, routing IP datagrams, TCP segment format, IPv4, IPv6).
- 4.6.7. Describe a Virtual Private Network (VPN) and identify associated protocols (e.g., Layer 2 Tunneling Protocol [L2TP], Point-to-Point Tunneling Protocol [PPTP]).
- 4.6.8. Capture and compare wired and wireless packets.

Outcome: 4.7. Transmission Control Protocol/Internet Protocol (TCP/IP)

Describe IP addressing schemes and create subnet masks.

Competencies

- 4.7.1. Explain Fully Qualified Domain Names (FQDNs) and how they are used.
- 4.7.2. Explain the IP addressing scheme and how it is used.
- 4.7.3. Identify Class A, B, and C reserved (i.e., private) address ranges and why they are used.
- 4.7.4. Identify the class of network to which a given address belongs.
- 4.7.5. Differentiate between default subnet masks and custom subnet masks.
- 4.7.6. Explain the relationship between an IP address and its associated subnet mask.
- 4.7.7. Identify the differences between classful and classless addressing schemes.
- 4.7.8. Identify multicasting addresses and explain why they are used.
- 4.7.9. Create custom subnet masks to meet network design requirements.
- 4.7.10. Compare Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6).

Outcome: 4.8. Network Operating Systems and Architecture

Describe and install networking operating systems and architecture.

Competencies

- 4.8.1. Describe media-access protocols (e.g., Carrier Sense Multiple Access with Collision Detection [CSMA/CD], Carrier Sense Multiple Access with Collision Avoidance [CSMA/CA]).
- 4.8.2. Identify the components and relationships within the Institute of Electrical and Electronics Engineers (IEEE) 802 standards.
- 4.8.3. Identify Local Area Network (LAN) performance factors (e.g., signal attenuation, signal propagation delay).
- 4.8.4. Explain the role of the Internet Engineering Task Force (IETF) in facilitating protocol development.
- 4.8.5. Implement and maintain Virtual Local Area Networks (VLANs).
- 4.8.6. Explain how the components of a network operating system (i.e., server platform, network services software, network redirection software, communications software) and all support network operations.
- 4.8.7. Identify licensing requirements.
- 4.8.8. Describe the characteristics of the tiered model (e.g., peer-to-peer, thin client, thick client, cloud).
- 4.8.9. Analyze the advantages and disadvantages of the client/server model.
- 4.8.10. Select network, desktop, and mobile Operating Systems.
- 4.8.11. Install, test, and patch network operating systems manually and using automation.
- 4.8.12. Log in to a network device (e.g., router, Secure File Transfer Protocol [SFTP] server, directory server).
- 4.8.13. Evaluate the performance of the network operating system.

Outcome: 4.9. Network Administration

Administer network operating systems and services.

Competencies

- 4.9.1. Select physical and logical topology.
- 4.9.2. Connect devices to network systems.
- 4.9.10. Troubleshoot network performance connectivity (e.g., performance monitor, command line utilities).
- 4.9.11. Explain the fundamentals of Quality of Service (QoS).
- 4.9.13. Establish a secure remote connection to manage network resources.

Outcome: 4.10. Cloud Computing

Implement a hypervisor.

Competencies

- 4.10.1. Differentiate between public, private, community and hybrid clouds and describe the fundamental cloud components (e.g., shared or dedicated processing, storage, memory, networking, hypervisor).
- 4.10.2. Provision cloud services (e.g., Software as a Service [SaaS], Platform as a Service [PaaS], Infrastructure as a Service [IaaS], Security as a Service [SECaaS], and Everything as a Service [XaaS]).

Outcome: 4.11. Wide Area Network

Design a wide area network (WAN).

Competencies

- 4.11.1. Select WAN connections (e.g., satellite, Synchronous Optical Network [SONET], T1, T3, E1, E3, Digital Subscriber Line [DSL], cable [DOCSIS], Worldwide Interoperability for Microwave Access [WiMAX], Multiprotocol Label Switching [MPLS], frame relay).
- 4.11.2. Describe point-to-point (PTP) and point-to-multipoint (PTMP) interconnection.
- 4.11.3. Evaluate and select basic telecommunications services (e.g., satellite, circuit switching, wireless, packet switching) and carriers for WAN requirements.
- 4.11.7. Determine the subnets needed on the WAN (e.g., Variable Length Subnet Masking [VLSM]).
- 4.11.8. Evaluate and select transmission options.
- 4.11.9. Evaluate and select routing protocols (e.g., Border Gateway Routing Protocol [BGRP], Open Shortest Path First [OSPF], Routing Information Protocol Version 2 [RIPv2]).

