Tennessee CTE

Networking

Safety

1 **Accurately read, interpret, and demonstrate adherence to safety rules, including but not limited to rules published by the National Science Teachers Association (NSTA), rules pertaining to electrical safety, Internet safety, Occupational Safety and Health Administration (OSHA) guidelines, and state and national code requirements. Be able to distinguish between rules and explain why certain rules apply. Complete safety test with 100 percent accuracy.** 1

2 **Identify and explain the intended use of safety equipment available in the classroom. For example, demonstrate how to properly inspect, use, and maintain safe operating procedures with tools and equipment.** 2

Career Exploration

3 **Locate and access the Computer Technology Industry Association (CompTIA) website and analyze its structure, policies, and requirements for CompTIA Network+ certification. Explain what steps are required to obtain the certification, methods to prepare for the examination, and how it can be a stepping stone to more advanced certifications.** 3

4 **Research the following networking standards organizations and write an informative paper explaining the industry standards that are managed by each. Describe why these standards are important and how they influence the work of a network administrator or other IT professional.** 4

- a American National Standards Institute 4.A
- b Electronic Industries Alliance and Telecommunications Industry Association 4.B
- c Institute of Electrical and Electronics Engineers 4.C
- d International Organization for Standardization 4.D
- e International Telecommunication Union 4.E
- f Internet Society 4.F
- g Internet Assigned Numbers Authority 4.G
- h Internet Corporation for Assigned Names and Numbers 4.H

Types of Networks

5 Define the term "network," define and describe the necessary features and components of a network, and differentiate between different network types. Using graphic illustrations, or other diagrams, identify and describe the following types of networks, outlining the features that distinguish each network from the others and effectively diagraming the flow of information in each. 5

- a Peer-to-peer networks 5.A
- b Client/server networks 5.B
- c Local area networks (LAN) 5.C
- d Metropolitan area networks (MAN) 5.D
- e Wide area networks (WAN) 5.E

6 Describe the following functions provided by a network. Distinguish between these network services in a large office versus an office with few users, providing specific examples. 6

- a File and print services 6.A
- b Access services 6.B
- c Communication services 6.C
- d Internet services 6.D
- e Management services 6.E

Open Systems Interconnection Model (OSI) Model

7 Create and use diagrams to explain the Open Systems Interconnection (OSI) Model and the flow of data through it. Define the functions and identify the associated hardware components of the OSI Model's following seven layers. For example, explain how each layer interacts to ensure that data arrives in the correct place without errors. 7

- a Application 7.A
- b Presentation 7.B
- c Session 7.C
- d Transport 7.D
- e Network 7.E
- f Data Link 7.F
- g Physical 7.G

Data Transmission

8 Identify and describe a range of standard cable types (e.g., coaxial cable, shielded twisted pair, unshielded twisted pair, single-mode fiber, multimode fiber, serial, plenum, and nonplenum), comparing and contrasting their characteristics and properties and differentiating between them accurately. Explain why it is necessary to consider the following properties when selecting and installing the appropriate cables for a networking task, and why these decisions must conform to industry standards. For a given task and environment, make a recommendation about an appropriate cable type and defend the recommendation with specific evidence and reasoning. 8

- a Transmission speeds 8.A
- b Distance 8.B
- c Duplex 8.C
- d Noise immunity (e.g., security, electromagnetic interference (EMI)) 8.D
- e Frequency 8.E

Transmission Control Protocol (TCP)/Internet Protocol (IP)

9 Research and identify the common subprotocols associated with transmission control protocol (TCP) and internet protocol. Using a combination of text and graphic illustrations, explain their functions and how they correlate to the layers of the open systems connection (OSI) model. Examples of subprotocols include, but are not limited to: hypertext transfer protocol (HTTP), user diagram protocol (UDP), internet control message protocol (ICMP), internet group management protocol (IGMP), address resolution protocol (ARP), domain name system (DNS), network time protocol (NTP), file transfer protocol (FTP), and trivial file transfer protocol (TFTP). 9

---

10 Describe the following address formats: IPv6, IPv4, and MAC. Using the advantages and disadvantages as supporting evidence, identify and explain the application of each format. 10

---

11 Define each of the following physical network topologies, and draw diagrams to distinguish among the layouts. Include examples of the most effective applications, as well as identify the advantages and disadvantages of each topology. 11

- a Star 11.A
- b Mesh 11.B
- c Bus 11.C
- d Ring 11.D
- e Point to point 11.E
- f Point to multipoint 11.F
- g Hybrid 11.G

12 **Compare and contrast logical network topologies to physical network topologies. Explain how these two types of topologies differ. Identify the common logical network topologies and describe their characteristics. Provide examples demonstrating how logical network topologies are useful in troubleshooting.** 12

13 **Define switching and detail the role that it occupies in a logical network topology. Describe the three types of switching (circuit, message, and packet) and identify the specific details that distinguish how each method establishes paths between nodes.** 13

14 **Define routing and explain why a router is protocol dependent. Identify and list the properties of a router and describe its basic functions, citing examples found in informational texts.** 14

15 **Write descriptive text that outlines the process used to determine the most efficient path (e.g., route) for data to flow across a network. Identify and describe that variables the influence the best path, including the following most common routing protocols.** 15

- a Link-state: open shortest path first (OSPF), intermediate system to intermediate system (IS-IS) 15.A
- b Distance-vector: routing information protocol (RIP), routing information protocol version 2 (RIPv2), border gateway protocol (BGP) 15.B
- c Hybrid: enhanced interior gateway routing protocol (EIGRP) 15.C

Network Hardware

16 **Research the following types of network interface cards (NICs). Create a table or other graphic organizer that lists examples and characteristics of NICs, as well as steps to selecting the appropriate NIC. Demonstrate proper installation and configuration of each device, attending to appropriate measurements and units. Summarize the multistep procedure to install and configure the various NICs.** 16

- a Internally attached (internal bus standards) 16.A
- b Externally attached (peripheral bus standards) 16.B
- c On-board 16.C
- d Wireless 16.D

17 **Define a repeater and explain its limitations. Describe the characteristics of a hub; explain how it is a type of repeater, yet it still differs from the repeater. Install and configure the following types of hubs and identify their distinguishing characteristics.** 17

- a Passive 17.A
- b Intelligent 17.B
- c Managed 17.C
- d Stand-alone 17.D
- e Workgroup 17.E

18 **Compare and contrast bridges with repeaters and hubs, identifying examples of advantages that bridges have over these devices. Provide supporting evidence to justify each example.** 18

19 **Create and execute a plan to first install multiple nodes to a small switch, and then to connect the switch to another connectivity device. Verbally describe the steps of the procedure as they are being demonstrated.** 19

20 **Identify common gateway devices and explain how they are different from connectivity devices. Further, explain why the gateways must operate on multiple layers of the open systems interconnection (OSI) model.** 20

Wireless Networking

21 **Demonstrate understanding of wireless transmission technology. Use a combination of graphic illustrations and text to describe how a wireless signal originates from an electrical current and travels along a conductor. Include definitions and functions of the following concepts.** 21

- a Antenna 21.A
- b Signal propagation 21.B
- c Signal degradation 21.C
- d Frequency ranges 21.D
- e Narrowband, broadband, and spread spectrum signals 21.E
- f Fixed vs. mobile 21.F

22 **Compare and contrast wireless local area network (WLAN) infrastructure to that of wired network topologies. Identify and explain the differences between the two layout types.** 22

23 **Locate and access the 802.11 standards (wireless fidelity or Wi-Fi) developed by the Institute for Electrical and Electronics Engineers (IEEE). Explain the purpose of these standards, as well as how IT professionals should apply them to networking systems.** 23

24 **Explore Bluetooth technology, differentiating between purposes of, and standards that govern, Bluetooth and other technologies (such as those governed by IEEE 802.111).** 24

25 **Given specifications to install and configure a basic wireless network in a home or small office, write and execute a plan that includes, but is not limited to, the following:** 25

- a Install the client 25.A
- b Locate and place the access point 25.B
- c Install the access point 25.C
- d Verify installation 25.D

Provide details of the multistep procedure and justify the recommendations in the plan by providing supporting evidence that conforms to industry standards (e.g., Institute for Electrical and Electronics Engineers (IEEE) 802.11, Bluetooth).

26 **Given specifications to install and configure a wireless network in a large office, conduct a site survey to assess requirements of the clients, facility characteristics, and coverage area. Using the survey results, write and execute a plan that includes, but is not limited to, the following:** 26

- a Wireless access point placement 26.A
- b Antenna types 26.B
- c Interference 26.C
- d Frequencies 26.D
- e Channels 26.E
- f Wireless standards 26.F
- g Service set identifier (SSID) (e.g., enable/disable) 26.G

Provide details of the multistep procedure and justify the plan by providing supporting evidence that conforms to the Institute for Electrical and Electronics Engineers (IEEE) 802.11 standards.

Network Operating Systems

27 In teams, research various types of network operating systems (NOS) (e.g., Microsoft Windows server, Linux enterprise server, UNIX, etc.). Identify the basic functions of a NOS, and synthesize the findings to write an explanatory text that includes, but is not limited to, the following: 27

- a Guiding questions to determine the optimal software requirements 27.A
- b Client support features 27.B
- c Organization of network elements 27.C
- d Sharing applications 27.D
- e Managing system resources (e.g., memory, multitasking, multiprocessing) 27.E
- f Why it is important to consider future needs 27.F

Present the paper to other teams and revise it based on constructive feedback from peers.

Security

28 Develop a plan for a regularly scheduled audit to examine a network's security risks. The plan should include, but is not limited to, the following: 28

- a How often and when the audit will be conducted 28.A
- b Security threats to be examined 28.B
- c Rating system to assess the security threats 28.C
- d Security policy goals and content 28.D
- e How security breaches will be addressed 28.E

Implement the security plan for the duration of the course, revising as necessary.

29 Research and describe the most common security risks associated with people; data transmission and hardware; protocols and software; and internet access. Investigate and distinguish among the following common prevention methods to secure a network system. 29

- a Physical security 29.A
- b Security in network design 29.B
- c Network operating system security 29.C
- d Encryption 29.D
- e Authentication protocols 29.E
- f Wireless network security 29.F

Given various scenarios, identify the most applicable best practices to secure a network. Implement these practices and write a justification for each scenario solution. Provide supporting evidence drawing on industry standards.

30 **Explore the application of firewalls to secure networks. Describe their features and functions while distinguishing between the types (e.g., software and hardware). Install and configure a basic firewall. Verbally explain each step of the implementation process as it is executed. Cite any applicable industry standards.** `30`

31 **Define fault tolerance, distinguishing between failures and faults in a network. Write a paper describing the following aspects that should be monitored and managed to sustain fault tolerance.** `31`

- a Environment `31.A`
- b Power `31.B`
- c Topology and connectivity `31.C`
- d Servers `31.D`
- e Storage `31.E`

Identify those aspects that are most influential on fault tolerance and justify the claim with supporting evidence. Demonstrate the application of these practices and compare the changes (if any) in the tolerance to results generated by other classmates.

Troubleshooting

32 **For each network system problem given, apply the following general troubleshooting theory.** `32`

- a Gather information from users or the system, back up data, and document findings `32.A`
- b Verify the problem exists and how many users are affected `32.B`
- c Isolate the cause of the problem and generate alternative solutions `32.C`
- d Determine whether escalation is necessary `32.D`
- e Plan a solution and resolve the problem `32.E`
- f Verify that the problem was resolved and prevent a future occurrence `32.F`
- g Document findings, resolution, and preventative maintenance plan `32.G`

Following the steps of the general troubleshooting theory, select a problem to present to classmates as a case study.

33 **For a given assignment related to the following common problems, follow the troubleshooting theory using appropriate hardware and software tools (e.g., cable tester, butt set, multimeter, protocol analyzer, throughput testers, connectivity software, etc.).** 33

a Wireless problems (e.g., interference, signal strength, configurations, latency) 33.A

b Router and switch problems (e.g., switching loop, bad cables, port configuration) 33.B

c Physical connectivity problems (e.g., connectors, wiring, split cables, cable placement) 33.C

Identify the problem(s) and document the findings and resolution. Include an explanation of the common symptoms, diagnostic procedures, and specific tools used that led to the problem resolution.