Networking

Level 3: Student explored previously; second pathway specific course
Pathway(s): Networking Systems & Security

Description

Networking is an advanced course designed to emphasize the conceptual and practical skills necessary to design, manage, and diagnose network hardware and software. Upon completion of this course, proficient students will identify types of networks, understand the layers of the open systems interconnection (OSI) model, prevent security risks, and apply troubleshooting theory to the successful execution of networking tasks. Course content covers transmission control protocol, internet protocol, wired and wireless topologies, switching and routing, network hardware, wireless networking, and network operating systems (NOS). Upon completion of this course, proficient students will be prepared to sit for the CompTIA Network+ exam.

Student Learning Outcomes

Safety

1) Accurately read, interpret and demonstrate adherence to safety rules.
2) Identify and explain the intended sue of safety equipment available in the classroom.

Career Exploration

3) Locate and access the Computer Technology Industry Association (CompTIA) website and analyze its structure, policies, and requirements for CompTIA Network+ certification.
    a. Explain the steps required to obtain this certification.
    b. Identify methods to prepare for the exam.
4) Research networking standards organizations such as the following:
    a. American National Standards Institute
    b. Electrical Industries Alliance and Telecommunications Industry Association
    c. Institute of Electrical and Electronic Engineers
    d. International Organization for Standardization
    e. International telecommunication Union
    f. Internet Society
    g. Internet Assigned Numbers Authority
    h. Internet Corporations for Assigned Names and Numbers

Types of Networks

5) Define the term “network.”
    a. Describe the necessary features and components of a network.
    b. Differentiate between network types.
    c. Outline the features that distinguish each network from the others.
        i. Peer-to-peer networks
        ii. Client/server networks
        iii. Local area networks (LAN)
        iv. Metropolitan area networks (MAN0

v. Wide area networks (WAN)

6) Describe the functions provided by a network. Distinguish between these network services in a large office environment versus an office with a few users.
    a. File and print services
    b. Access services
    c. Communication services
    d. Internet services
    e. Management services

Open Systems Interconnection Model (OSI) Model

7) Explain the Open Systems Interconnection (OSI) Model and how data flows through it.
8) Define the functions and identify the associated hardware components of the OSI Model's following seven layers.
    a. Application
    b. Presentation
    c. Session
    d. Transport
    e. Network
    f. Data link
    g. Physical
9) Explain how each layer interacts to ensure that data arrives in the correct place without errors.

Data Transmission

10) 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 non-plenum).
    a. Compare and contrast their characteristics and proprieties.
    b. 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.
        i. Transmission speeds
        ii. Distance
        iii. Duplex
        iv. Noise immunity (e.g., security, electromagnetic inference (EMI))
        v. Frequency

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

11) Research and identify the common subprotocols associated with transmission control protocol (TCP) and internet protocol (IP). Examples include
    a. Hypertext transfer protocol (HTTP)
    b. User diagram protocol (UDP)
    c. Internet control message protocol (ICMP)
    d. Internet group management protocol (IGMP)
    e. Address resolution protocol (ARP)
    f. Domain name system (DNS)
    g. Network time protocol (NTP)

h. File transfer protocol (FTP)

i. Trivial file transfer protocol (TFTP)

12) Explain their functions and how they correlate to the layers of the open systems connection (OSI) model.

13) Describe the following address formats: IPv6, IPv4, and MAC.

Topologies

14) Define each of the following physical network topologies.

    a. Star
    b. Mesh
    c. Bus
    d. Ring
    e. Point to point
    f. Point to multipoint
    g. Hybrid

15) Give examples of the most effective applications of the above topologies.

16) Identify advantages and disadvantages of each of the above topologies.

17) Compare and contrast logical network topologies to physical network topologies.

18) Identify common logical network topologies and describe their characteristics.

Switching and Routing

19) Define switching and detail the role that it occupies in a logical network topology.

20) Describe the three types of switching (circuit, message, and packet).

21) Identify the specific details that distinguish how each method establishes paths between nodes.

22) Outline the process used to determine the most efficient path for data to flow across a network.

23) Identify and describe the variables that influence the best path, including the following most common routing protocols.

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

Network Hardware

24) Research the following types of network interface cards (NICs).

    a. Internally attached (internal bus standards)
    b. Externally attached (peripheral bus standards)
    c. On-board
    d. Wireless

25) Outline the steps to selecting the appropriate NIC.

26) Demonstrate proper installation and configuration of each device, attending to appropriate measurements and units.

27) Summarize the multistep procedure to install and configure the various NICs.

28) Define a repeater and explain its limitations.

29) Describe the characteristics of a hub; explain how it is a type of repeater, yet still differs from the repeater.
30) Install and configure the following types of hubs and identify their distinguishing characteristics.
    a. Passive
    b. Intelligent
    c. Managed
    d. Stand-alone
    e. Workgroup
31) Compare and contrast bridges with repeaters and hubs.
32) Create and execute a plan to first install multiple nodes to a small switch, and then to connect the switch to another connectivity device.
33) Identify common gateway devices and explain how they are different from connectivity devices.

Wireless Networking

34) Demonstrate understanding of wireless transmission technology.
35) Describe how a wireless signal originates from an electrical current and travels along a conductor.
36) Define and describe the functions of the following:
    a. Antenna
    b. Signal propagation
    c. Signal degradation
    d. Frequency ranges
    e. Narrowband, broadband, and spread spectrum signals
    f. Fixed vs. mobile.
37) Compare and contrast wireless local area network (WLAN) infrastructure to that of the wired network topologies.
38) Locate and access the 802.11 standards (wireless fidelity or Wi-Fi) developed by the Institute for Electrical and Electronics Engineers (IEEE).
39) Explain how IT professional should apply them to networking systems.
40) Explore Bluetooth technology.
41) Given specifications to install and configure a basic wireless network in a home or small office, execute a plan that includes the following:
    a. Install the client
    b. Locate and place the access point
    c. Install the access point
    d. Verify installation
42) Given specifications to install and configure a wireless network in a large office, conduct a site survey to assess requirements of the client, facility characteristics, and coverage area.
43) Using the survey results, write and execute a plan that includes the following:
    a. Wireless access point placement
    b. Antenna types
    c. Interference
    d. Frequencies
    e. Channels
    f. Wireless standards

g. Service set identifier (SSID) (e.g., enable/disable)

Network Operating Systems

44) Research various types of network operating systems (NOS) (e.g., Microsoft Windows server, Linux enterprise server, UNIX, etc.).
45) Identify the basic functions of a NOS.

Security

46) Develop a plan for a regularly scheduled audit to examine a network's security risks. The plan should include the following:
    a. How often and when the audit will be conducted
    b. Security threats to be examined
    c. Rating system to assess the security threats
    d. Security policy goals and content
    e. How security breaches will be addressed
47) Research and describe the most common security risks associated with people, data transmission, and hardware, protocols and software, and internet access.
48) Investigate and distinguish among the following common prevention methods to secure a network system.
    a. Physical security
    b. Security in network design
    c. Network operating system security
    d. Encryption
    e. Authentication protocols
    f. Wireless network security
49) Given various scenarios, identify the most applicable best practices to secure a network.
50) Explore the application of firewalls to security networks.
51) Install and configure a basic firewall.
52) Define fault tolerance, distinguishing between failures and faults in a network.
53) Describe the following aspects that should be monitored and managed to sustain fault tolerance.
    a. Environment
    b. Power
    c. Topology and connectivity
    d. Servers
    e. Storage

Troubleshooting

54) For each network system problem given, apply the following general troubleshooting theory.
    a. Gather information from users or the system, back up data, and document findings
    b. Verify the problem exists and how many users are affected
    c. Isolate the cause of the problem and generate alternative solutions
    d. Determine whether escalation is necessary
    e. Plan a solution and resolve the problem
    f. Verify the problem was resolved and prevent a future occurrence

g. Document findings, resolution, and preventative maintenance plan.

55) Troubleshoot various common problems using appropriate hardware and software tools (e.g., cable tester, butt set, multimeter, protocol analyzer, throughput testers, connectivity software, etc.) Examples include:

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

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

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