Instructional Framework

Network Security

11.1999.00

This Instructional Framework identifies, explains, and expands the content of the standards/measurement criteria, and, as well, guides the development of multiple-choice items for the Technical Skills Assessment. This document corresponds with the Technical Standards endorsed in May 2024.

Domain 1: Network Troubleshooting **Instructional Time: 25 - 30%**	
STANDARD 10.0 PERFORM NETWORK MAINTENANCE AND RESOLVE ISSUES	
10.1 Explain the troubleshooting process (e.g., define problem, identify probable cause, test hypothesis, create action, implement action plan, verify solution, and document)	• Define problem • Identify probable cause • Test hypothesis • Create action • Implement action plan • Verify solution • Document

10.2 Prepare a work/maintenance plan and prioritize and schedule network security tasks (i.e., Cron Jobs)	• Cron Jobs
	• Prioritize
	• Trouble tickets
	• Daily routine tasks
	  ○ Check logs
	  ○ Equipment
	  ○ Software updates

10.3 Describe the purpose and benefits of network utilities [i.e., Network Statistics (netstat), Name Server Lookup (nslookup), Ping, Traceroute, etc.]	• Network Statistics (netstat) • Name Server Lookup (nsLookup) • Ping • Traceroute • Etc.

10.4 Demonstrate the use of visual indicators and diagnostic utilities (i.e., Wireshark, etc.) to interpret problems	• Wireshark

10.5 Identify connectivity issues in various node environments (i.e., smartphones, switches, tablets, Linux/UNIX, Windows, etc.)	• Connectivity issues in various environments
	  ○ Smartphones
	  ○ Switches
	  ○ Tablets
	  ○ Linux/UNIX
	  ○ Windows
	• Etc.

10.6 Identify and resolve network issues (i.e., cable failure, connection failure, environmental, misconfigurations, power failure, user error, etc.)	• Network issues
	  ○ Cable failure
	  ○ Connection failure
	  ○ Environmental
	  ○ Misconfigurations
	  ○ Power
	  ○ User error
	• Etc.

10.7 Identify common tools and methods for monitoring a network (i.e., automation, scripting, AI tools, etc.)	• Automation • Scripting • AI tools • Simple Network Management Protocol (SNMP)
10.8 Describe AI and Machine Learning-based tools for network maintenance and issue resolution [e.g., large language models (LLMs)]	• Large Language Model (LLM)
Domain 2: Networking Concepts **Instructional Time: 20 - 25%**	
STANDARD 1.0 INVESTIGATE NETWORK SECURITY AS A CAREER	
1.1 Explain network security (e.g., the protection of data that is stored on the network or which is in transit across, into, and out of the network)	• The protection of data that is stored on the network or which is in transit across, into, and out of the network • Examples

	○ Data at rest ○ Data in motion ○ Data in use
1.2 Describe the responsibilities of a network security technician (i.e., ensure the network works securely, test and configure software, provide IT support, troubleshoot the network or server, resolve infrastructure issues, etc.)	● Ensure the network works securely ● Test and configure software ● Provide IT support ● Troubleshoot the network or server ● Resolve infrastructure issues
1.3 Identify skills and ethical characteristics needed to be a successful network security technician (i.e., critical thinking, problem solving, prioritizing, reading, and interpreting network diagrams and technical schematics, preparing and presenting technical information verbally and in writing to different audiences, keeping up to date on network security, etc.)	● Critical thinking, problem solving, prioritizing ● Reading, and interpreting network diagrams and technical schematics ● Preparing and presenting technical information verbally and in writing to different audiences ● Keeping up to date on network security ● Use problem solving techniques ○ Bottom-up, ○ Top-down ○ Divide-and-conquer ● Document and present at a technical and nontechnical level
1.4 Describe education and training opportunities including industry certifications and licensures (i.e., CompTIA, CISCO, CISSP, CEH, etc.)	● CompTIA ● CISCO ○ CCT (Cisco Certified Technician) ○ CCNA (Cisco Certified Network Associate) ● CISSP ● CEH ● Network+
1.5 Identify career opportunities in network security	● Explore career opportunities ○ Job posting boards
STANDARD 2.0 MAINTAIN A SAFE, ENVIRONMENTALLY CONSCIOUS NETWORKING ENVIRONMENT	
2.1 Identify hazards and unsafe practices that can lead to serious accidents or injuries (i.e., electrostatic discharge hazards, poor ergonomic practices, etc.)	● Electrostatic discharge hazards ● Poor ergonomic practices ● Ergonomic solutions to prevent injuries ○ Carpal tunnel

	○ Repetitive action, etc. ● Grounding and bonding ● Generators ○ Fluorescent light ballasts ○ Microwaves
2.2 Describe OSHA and other state and national regulations designed to reduce safety risks and workplace injuries	● Occupational Safety and Health Administration (OSHA) regulations
2.3 Explain environmental considerations when disposing of computer/network components (i.e., disposing of batteries, devices with lithium batteries, etc.)	● Disposing of batteries ● Devices with lithium batteries ● EPA (Environmental Protection Agency) regulations ● E-Waste recycling
2.4 Use techniques to manage power consumption in the networked environment (i.e., test wattage usage, power control, explore green methods such as climate batteries and energy efficiency methods, cloud-based software, etc.)	● Test wattage usage ● Power control ● Explore green methods such as climate batteries and energy efficiency methods ● Cloud ○ Public ○ Private ○ Hybrid ● Power management settings ● Smart Home ○ IoT (Internet of Things)
2.5 Identify energy efficiencies and suggest ways to improve consumption (i.e., office environment AC units, thermostats, computer power settings, etc.)	● Office environment AC units ● Thermostats ● Computer power settings ● Power management settings ● Wake-on- Lan
2.6 Use, maintain, and store tools and equipment according to manufacturer's standards	● Crimper ● Cable tester ● Punch down tool ● PPE (Personal Protection Equipment) ● ESD strap ● Wire cutters

	• User Manuals • Etc.
STANDARD 3.0 DEMONSTRATE BASIC MATHEMATICS FOR NETWORK SECURITY	

3.1 Define the number base systems in mathematics related to network technology	• Number base systems
	  ○ Base 2
	  ○ Base 10
	  ○ Base 16

3.2 Perform decimal to binary and binary to decimal conversions (e.g., dotted decimal IPv4)	• Decimal to binary and binary to decimal conversions • Dotted decimal IPv4
3.3 Perform decimal to hexadecimal and hexadecimal to decimal conversions	• Decimal to hexadecimal and hexadecimal to decimal conversions
3.4 Perform hexadecimal to binary and binary to hexadecimal conversions	• Hexadecimal to binary and binary to hexadecimal conversions

3.5 Determine the appropriate method to perform conversions (e.g., paper-pencil and electronic resources)	• Paper-pencil and electronic resources
	• Calculator
	  ○ Programming
	  ○ Scientific
	  ○ Windows

3.6 Use basic Boolean logic for actions such as Google searches and scripting (e.g., and, not, and or)	• Boolean logic
	  ○ And, not, and or
	• Scripting
	  ○ Write batch file
	  ○ Etc.

Domain 3: Network Security **Instructional Time: 15 - 20%**	
STANDARD 5.0 UTILIZE BEST PRACTICES FOR COMPUTER AND NETWORK RISKS AND THREATS	

5.1 Explain the risk management process (i.e., define risk, determine risk level, identify methods to address risk, identify inventory assets that may be compromised, identify functionalities, etc.)	● Define risk ● Determine risk level ● Identify methods to address risk ○ Mitigation ● Identify inventory assets that may be compromised ● Identify functionalities ● Etc.
5.2 Define network threats to data availability, confidentiality, and integrity	● End-user agreements ● Physical security ● ACLs (Access Control Lists) ● Group policies ● File sharing
5.3 Discuss and give examples of the severity of data loss to an individual and to an organization	● Identity theft ● Financial impact ● Intellectual property ● Personal data loss ● Prioritize the severity of data lost ● Loss of Work and Productivity

5.4 Identify security threats related to computer data, hardware, and software (i.e., denial of service, eavesdropping, intrusion, unauthorized access, unauthorized use, spoofing, tampering, repudiation, information disclosure, elevation of privilege, etc.)	● Security Threats
	  ○ Ransomware
	  ○ Denial of service
	  ○ Eavesdropping
	  ○ Intrusion
	  ○ Unauthorized access
	  ○ Unauthorized use
	● Spoofing
	● Tampering
	● Repudiation
	● Information disclosure
	● Elevation of privilege
	● Etc.

5.5 Explain the importance of physical security of computer and network hardware following best practices (e.g., cameras, locks, USB port blocking, encryption, bit-locker for Windows, and LBM for Linux)	● Physical security
	  ○ Cameras
	  ○ Locks
	  ○ USB port blocking

	○ Encryption ○ Bit-locker for Windows ○ LBM for Linux (Linux Block Mode) ○ Kensington lock ○ Etc.
5.6 Describe network threats (i.e., denial of service, email spoofing, hacking/cracking, intrusion, malware, phishing, social engineering, spamming, system vulnerabilities, website defacement, tampering, repudiation, information disclosure, elevation of privilege, etc.)	● Denial of service ● Email spoofing ● Hacking/cracking ● Intrusion ● Malware ● Phishing ● Social engineering ● Spamming ● System vulnerabilities ● Website defacement ● Tampering ● Repudiation ● Information disclosure ● Elevation of privilege ● Etc.
5.7 Describe best practices to protect against network threats of data at rest, data in transit, and data during processing (i.e., access control, antivirus software, awareness and training, encryption, firewalls, incident detection systems/tools, intrusion detection prevention, network segmentation, port/service blocking, software updates/patches, etc.)	● Access control ● Antivirus software ● Awareness and training ● Encryption ● Firewalls ● Incident detection systems/tools ● Intrusion detection prevention ● Network segmentation ● Port/service blocking ● Software updates/patches
5.8 Describe password best practices [i.e., authentication, authorization, and accountability (AAA), passphrases, physical keys, password managers, age, complexity, history, length, lockout, etc.]	● Authentication, Authorization, and Accountability (AAA) ● Passphrases ● Physical keys ● Password managers ● Age

	• Complexity • History • Length • Lockout • Etc.
5.9 Analyze authentication methods used to secure access to the network [i.e., biometrics, key cards, multi-factor authentication (MFA), passwords, single sign-on (SSO), two-factor authentication (2FA), etc.]	• Biometrics • Key cards • Multi-factor authentication (MFA) • Passwords • Single sign-on (SSO) • Two-factor authentication (2FA)

5.10 Identify best practices for access control (i.e., changing default passwords, disabling unused accounts, least privileges, privileged account management, role-based access control, etc.) and legal liability of collecting biometric data (e.g., identification of medical information, inadvertently collecting privacy information, and compromising a situation)	• Access control
	  ○ Changing default passwords
	  ○ Disabling unused accounts
	  ○ Least privileges
	  ○ Privileged account management
	  ○ Role-based access control
	• Legal liability of collecting biometric data
	  ○ Identification of medical information
	  ○ Inadvertently collecting privacy information
	  ○ Compromising a situation

STANDARD 9.0 HARDEN A NETWORK	
9.1 Explain how to harden the network against unauthorized access and abuse	• Strong password • Device Hardening • MFA (Multi-factor Authentication) • Encryption • Network Access control • Security Rules • Zones • Implement Firewalls • Patch Management • Etc.
9.2 Explain the difference among hardening, patching, and types of vulnerabilities (i.e., social, cognitive, environmental, emotional, military,	• Social • Cognitive

etc.)	• Environmental • Emotional • Military
9.3 Identify common network threats (i.e., denial of service, eavesdropping, intrusion, probing, unauthorized access, 2.4v5G, Wi-Fi attack vectors, etc.)	• Denial of service • Eavesdropping • Intrusion • Probing • Unauthorized access • 2.4v5G • Wi-Fi attack vectors
9.4 Identify physical network threats [i.e., disrupting media (cutting fiber), environmental/power disruption, unauthorized access to devices, Farraday Cage, etc.]	• Disrupting media ○ Like cutting fiber • Environmental/power disruption • Unauthorized access to devices • Faraday Cage • Etc.
9.5 Describe the benefits of enabling and disabling ports and networks (i.e., VLAN, DMZ, etc.)	• VLAN (Virtual Local Area Network) • Demilitarized Zone (DMZ) • IP subnetting VLSM (Variable Length Subnet Mask) • Etc.
9.6 Describe the benefits of enabling and disabling ports and network services	• Authorized access • MAC address filtering • Hypertext Transfer Protocol (HTTP) vs. Secure Hypertext Transfer Protocol (HTTPS) • File Transfer Protocol (FTP) vs. Secure File Transfer Protocol (SFTP)
9.7 Describe the techniques to secure a Wi-Fi network [i.e., Wi-Fi Protected Access (WPA), Wi-Fi Protected Access 3 (WPA3), IoT device security, etc.]	• Wi-Fi Protected Access (WPA)/ 2 (WPA2) / 3 (WPA3) • IoT (Internet of Things) device security • SSID • Default password • Default IP address • WEP

9.8 Explain the principles of firewall rules and their importance in network hardening (i.e., application, packet filtering, stateful, etc.)	• Application • Packet Filtering • Stateful • Access Control List (ACL) • Hardware and software firewalls

9.9 Describe the benefits, disadvantages, and purposes of using a proxy service	• Proxy Service
	  ○ Advantages/Disadvantages
	  ○ Purposes

9.10 Describe the benefits, disadvantages, and purposes of using network intrusion detection/prevention systems [i.e., Intrusion Detection System/Intrusion Prevention System (IDS/IPS), Security information and event management (SIEM), etc.]	• Intrusion Detection System / Intrusion Prevention System (IDS/IPS) • Security information and event management (SIEM) • Etc.
STANDARD 11.0 INVESTIGATE LEGAL AND ETHICAL ISSUES RELATED TO NETWORK SECURITY	
11.1 Research issues regarding intellectual property rights including software licensing and software duplication [e.g., Business Software Alliance, Creative Commons, Digital Right Management (DRM), Electronic Freedom Foundation (EFF), and Intellectual Property Watch]	• Business Software Alliance • Creative Commons • Digital Right Management (DRM) • Electronic Freedom Foundation (EFF) • Intellectual Property Watch • Copyright laws
11.2 Differentiate among freeware, open source, proprietary, and shareware software relative to legal and ethical issues	• Open source • Closed source
11.3 Identify issues, laws, and trends affecting data and privacy [e.g., Certified Network Professional (CNP); General Data Protection Regulation (GDPR); Health Insurance Portability and Accountability Act (HIPAA); Payment Card Industry Data Security Standard (PCI-DSS); Sarbanes-Oxley Act (SOX); Federal Communications System (FCC); and Family Education Rights and Privacy Act (FERPA)]	• Certified Network Professional (CNP) • General Data Protection Regulation (GDPR) • Health Insurance Portability and Accountability Act (HIPAA) • Payment Card Industry Data Security Standard (PCI-DSS) • Sarbanes-Oxley Act (SOX) • Federal Communications System (FCC) • Family Education Rights and Privacy Act (FERPA) • Torrenting
11.4 Describe acceptable use of industry-related data, private and public networks, and social networking	• Acceptable use of: ○ Industry-related data

	○ Private networks ○ Public networks ○ Social networking
11.5 Research how data privacy laws and regulations influence network security business practices	● Acceptable Use Policy ● End User License Agreement
11.6 Discuss the responsibilities of network security professionals (i.e., protecting organizational assets, and maintaining consistent and equitable cyber practices, etc.), and explore consequences of unethical behavior to include personal legal liability (i.e., Cyberwire.com/caveat, etc.)	● Protecting organizational assets ● Maintaining consistent and equitable cyber practices ● Consequences of unethical behavior to include personal legal liability ○ thecyberwire.com ○ Etc.
Domain 4: Networking Implementation **Instructional Time: 15 - 20%**	
STANDARD 6.0 ANALYZE NETWORK MEDIA AND NETWORK TECHNOLOGIES	
6.1 Explain the purpose of and types of network media (i.e., fiber optic cable, coaxial cable, ethernet, etc.)	● Fiber optic cable ● Coaxial cable ● Ethernet
6.2 Explain the purpose and types of topologies (i.e., bus, ring, tree, star, mesh, etc.)	● Bus ● Ring ● Tree ● Star ● Mesh
6.3 Compare proper physical network topology	● Physical network topology ○ Bus ○ Ring ○ Star ○ Mesh ● Hybrid

6.4 Identify appropriate connectors, media types, and uses for various networks	● Connectors ○ RJ45 Female ○ RJ45 Male 8P8C (8 Position, 8 Contact) ○ RS232 ● Cable Types ○ Straight-Through ○ Crossover ○ Rollover ● Fiber ○ Single Mode ○ Multi-Mode ● STP/UTP (Shielded Twisted Pair/Unshielded Twisted Pair) ○ LAN/WAN/MAN
6.5 Compare physical and virtual networks [i.e., Software-Defined Wide-Area Network (SD-WAN), Virtual Local Area Network (VLAN), etc.]	● Software-Defined Wide-Area Network (SD-WAN) ● Virtual Local Area Network (VLAN)
6.6 Specify the characteristics of physical network technologies including cable types, length, speed, and topology	● STP/UTP (Shielded Twisted Pair/Unshielded Twisted Pair) ● FIBER ● Coaxial
6.7 Specify the characteristics of wireless network technologies including frequency, speed, topology, and transmission [i.e., local area, metropolitan area, wide area networks, 5G cellular, Bluetooth, IoT, satellite, Citizens Broadband Radio Service (CBRS), Unlicensed spectrum, etc.]	● 802.11 ○ Local area ○ Metropolitan area ○ Wide area networks ○ 5G cellular ● 802.15 ○ Bluetooth ○ IoT ● Satellite ● Citizens Broadband Radio Service (CBRS) ● Unlicensed spectrum

6.8 Describe the structure of the internet (network of networks)	• Hierarchy ○ PAN (Personal Area Network) to WAN (Wide Area Network) • ISP (Internet Service Provider)
6.9 Identify the features, functions, and purpose of commonly used network components [i.e., routers, modems, switches, bridges, network interface card (NIC), etc.]	• Routers • Modems • Switches • Bridges • NIC (Network Interface Cards) • Intermediary Devices • End Devices • Wireless Devices • Media
STANDARD 8.0 CONFIGURE A BASIC NETWORK	
8.1 Design a network map with virtual and physical segments, (e.g., logical network map)	• Logical network map • VLAN (Virtual Local Area Network)
8.2 Construct dynamic and static routes	• Dynamic Routes • Static Routes

8.3 Explain labeling according to industry standards (i.e., cable, device, rack, wall plates, etc.)	• Proper labeling in accordance with industry standards
	  ○ Cable
	  ○ Device
	  ○ Rack
	  ○ Wall plates
	  ○ Etc.

8.4 Describe the components needed and purpose to build fault tolerance into a network	• Fault tolerance and redundancy
	  ○ Mesh
	  ○ Failover
	  ○ Port forwarding
	  ○ Spanning Tree Protocol (STP)

8.5 Describe the purpose of a disaster recovery plan for a network	• Offsite storage • Cloud storage • Documentation

8.6 Install and configure a physical and/or virtual networking system [e.g., Linux/UNIX (3-layer model: kernel, shell, utilities), pipes, and Windows]	• Linux/UNIX
	  ○ 3-layer model
	  ○ Kernel, shell, utilities
	• Pipes
	• Windows
	• VMware
	• VirtualBox (free software)

8.7 Configure network cards, network settings, and an operating system that provides common services for computer programs	• Configure:
	  ○ Network cards
	  ○ Network settings
	  ○ Operating system

8.8 Configure and connect devices to the network (i.e., computers, printers, routers, switches, etc.)	• Configure and connect devices to the network:
	  ○ Computers
	  ○ Printers
	  ○ Routers
	  ○ Switches
	  ○ Wireless Access Point (WAP)

8.9 Identify and use tools for diagnostic tasks or network repair (i.e., execute Traceroute, ipconfig, Ping, etc.)	• Tools to use for diagnostic tasks or network repair
	  ○ Traceroute
	  ○ Ipconfig
	  ○ Ping
	  ○ Etc.

Domain 5: Network Operations **Instructional Time: 10 - 15%**	
STANDARD 4.0 DESCRIBE THE DEVELOPMENT AND EVOLUTION OF COMPUTERS AND NETWORKING	
4.1 Define a computer and describe its components and their basic functions (i.e., OSI Model and TCP/IP Model; Input Unit, Output Unit, and Central Processing Unit; displaying data, coding, transferring and processing data, programming programs, etc.)	• OSI Model and TCP/IP Model • Input Unit, Output Unit and Central Processing Unit • Displaying data, coding, transferring and processing data • Programming programs • RAID (Redundant Array of Independent Disks) Array

4.2 Discuss the evolution of computers and future trends in computer networking [i.e., Advanced Research Projects Agency Network (ARPANET), Internet of Things (IoT), privacy, etc.] and societal impacts	• Advanced Research Projects Agency Network (ARPANET) • Internet of Things (IoT) • Privacy • Computer and Network speed development timeline
4.3 Discuss issues and controversies pertaining to the evolution of mobile computing and the dissemination and centralization of data and its societal impacts (i.e., IoT, Microsoft, Google, anti-competitive practices, privacy, etc.)	• Internet of Things (IoT) • Google • Anticompetitive processes • Privacy

4.4 Explain an information system's structure and components [e.g., applications; media (copper cables, fiber, and wireless); network devices (i.e., router, switches, etc.); operating systems; and servers]	• Applications
	• Media
	  ○ Copper cables, fiber, and wireless
	• Network devices
	  ○ Router
	  ○ Switches
	  ○ Firewall
	  ○ WAP (Wireless Access Point)
	• Operating systems
	  ○ System Software
	  ○ Application Software
	• Servers

4.5 Discuss recent advancements in cybersecurity technologies, threats, and the basics of artificial intelligence (AI) concerning network security	• ISE (Identity Services Engine) • IDS (Intrusion Detection System) • IPS (Intrusion Prevention System) • Threat Detection/Threat Monitoring • Etc.
4.6 Discuss emerging problem-solving methodologies such as Zero Trust principles and AI-driven threat detection	• Zero Trust principles • AI-driven threat detection
STANDARD 7.0 ANALYZE NETWORK PROTOCOLS AND STANDARDS	
7.1 Define a network protocol and explain how it works (e.g., internal and external routing protocol)	• Basic definition of a protocol • Basic explanation of a protocol

7.2 Describe the characteristics, name, and use of the four-layer model of the Transmission Control Protocol/Internet Protocol (TCP/IP) [(e.g., Media Access Control (MAC)]	• Media Access Control (MAC) • MAC address length • OUI (Organizational Unique Identifier) • Characteristics and name of the four layers of the Transmission Control Protocol/Internet Protocol (TCP/IP) model
7.3 Describe the characteristics, name, and use of the seven layers of the Open Systems Interconnect (OSI) model	• Open Systems Interconnect (OSI) model • Seven layers

7.4 Explain the concept of ports and identify the port ranges used in networking services and protocols [i.e., dynamic/private (49152-65535); system (0-1023); user (1024-49151); Internet Control Message Protocol (ICMP); Address Resolution Protocol (ARP); etc.]	• Concepts of ports and identify the three port ranges used in networking services and protocols:
	  ○ Dynamic/private (49152-65535)
	  ○ System (0-1023)
	  ○ User (1024-49151)
	• Internet Control Message Protocol (ICMP)
	• Address Resolution Protocol (ARP)

7.5 Explain the purpose of dynamic and static routing protocols	• Purpose of dynamic and static routing protocols
7.6 Describe standard network ports and protocols [i.e., Domain Name System (DNS); Dynamic Host Configuration Protocol (DHCP); File Transfer Protocol (FTP); Hypertext Transfer Protocol (HTTP); Post Office Protocol (POP); Simple Mail Transfer Protocol (SMTP); Hypertext Transfer Protocol Secure (HTTPS); Secure File Transfer Protocol (SFTP); Virtual Private Network (VPN); Secure Shell (SSH); ICMP/ARP; etc.]	• Domain Name System (DNS) • Dynamic Host Configuration Protocol (DHCP) • File Transfer Protocol (FTP) • Hypertext Transfer Protocol (HTTP) • Point-of-Presence (POP) • Simple Mail Transfer Protocol (SMTP) • Hypertext Transfer Protocol Secure (HTTPS) • Secure File Transfer Protocol • Virtual Private Network (VPN) • SFTP Point-of-Presence (POP) • Secure Shell (SSH) • ICMP/ARP (Internet Control Message Protocol/Address Resolution Protocol)
7.7 Describe the applications and characteristics of Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)	• Stateful • Stateless • Error checking (Transmission Control Protocol - TCP)

	• Connectionless (User Datagram Protocol - UDP)
7.8 Differentiate IPv4/IPv6 addresses and their corresponding subnet masks [i.e., classful networks, Classless Interdomain Routing (CIDR), private vs public IP, etc.]	• Classful networks • Classless Interdomain Routing (CIDR) • Private vs public IP

7.9 Summarize the basic characteristics and protocols of Metropolitan Area Network (MAN), Software-Defined Wide Area Network (SD-WAN), and Wide Area Network (WAN) technologies (i.e., frame relay, etc.)	• Basic characteristics and protocols
	  ○ Metropolitan Area Network (MAN)
	  ○ Software-Defined Wide Area Network (SD-WAN)
	  ○ Wide Area Network (WAN) technologies
	  ○ Frame relay

7.10 Describe remote access protocols and services [i.e., remote desktop protocols (RDP), terminal emulator, etc.]	• Remote desktop protocols [RDP] • Terminal emulator • Etc.

7.11 Describe the function and purpose of security protocols [i.e., Hypertext Transfer Protocol Secure (HTTPS); Secure File Transfer Protocol (SFTP); Virtual Private Network (VPN); Point-to-Point Tunneling Protocol (PPTP); etc.]	• Function and purpose of security protocols
	  ○ Hypertext Transfer Protocol Secure (HTTPS)
	  ○ Secure File Transfer Protocol (SFTP)
	  ○ Virtual Private Network (VPN)
	  ○ Point-to-Point Tunneling Protocol (PPTP)
	  ○ Etc.

7.12 Explain the importance of proper documentation according to industry standards	• Physical topology • Logical topology • End-user agreement documentation
7.13 Discuss where RFCs (standards) are developed (i.e., IETF, IEEE, 3GPP, etc.)	• RFCs (Requests for Comments) • Internet Engineering Task Force (IETF) • Institute of Electrical and Electronics Engineers (IEEE) • 3rd Generation Partnership Project (3GPP) • Telecommunications Industry Association (TIA) • Etc.
7.14 Describe methods to determine priorities in establishing and maintaining a computer network	• Design • Document • Testing ○ Equipment verification

	○ Connectivity ● Baseline ○ Testing variances and limits