

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 on July 14, 2019.



Domain 1: Network Essentials	
Instructional Time: 45-55%	
STANDARD 1.0 APPLY PROBLEM-SOLVING AND CRITICAL THINKING SKILLS TO NETWORK SECURITY	
1.1 Describe methods to determine priorities in establishing and maintaining a computer network	<ul style="list-style-type: none">• Design• Document• Testing (equipment verification, connectivity)• Baseline (testing variances and limits)
1.2 Prepare a plan of work and schedule network technology tasks	<ul style="list-style-type: none">• Prioritize• Trouble tickets• Daily routine tasks (check logs, equipment, and software updates, etc.)
1.3 Apply problem-solving processes to network technology tasks (i.e., bottom-up, divide-and-conquer, top-down, etc.)	<ul style="list-style-type: none">• Scenario based - use network problem to teach:<ul style="list-style-type: none">◦ Bottom-up◦ Top-down◦ Divide-and-conquer
1.4 Prepare and present technical information for nontechnical and technical audiences in writing and verbally	<ul style="list-style-type: none">• Document and present at a technical and nontechnical level
STANDARD 5.0 DEMONSTRATE BASIC COMPUTER MATHEMATICS REQUIRED FOR NETWORK SECURITY	
5.1 Explain the function of base number systems in mathematics as it relates to network technology	<ul style="list-style-type: none">• Base 10• Base 2• Base 16
5.2 Perform decimal to binary and binary to decimal conversions	<ul style="list-style-type: none">• Decimal to binary and binary to decimal conversions
5.3 Perform decimal to hexadecimal and hexadecimal to decimal conversions	<ul style="list-style-type: none">• Decimal to hexadecimal and hexadecimal to decimal conversions

5.4 Perform hexadecimal to binary and binary to hexadecimal conversions	<ul style="list-style-type: none"> Hexadecimal to binary and binary to hexadecimal conversions
5.5 Determine the appropriate method to perform conversions (e.g., paper-pencil and electronic resources)	<ul style="list-style-type: none"> Programming calculator Subnet calculator
5.6 Apply basic Boolean logic for actions such as Google searches and scripting (e.g., “and,” “nor,” “not,” and “or”)	<ul style="list-style-type: none"> Scripting (i.e., Write batch file, etc.) Boolean logic: “and,” “nor,” “not,” and “or”
STANDARD 8.0 DESCRIBE NETWORK PROTOCOLS AND STANDARDS	
8.1 Describe the parts and use of a Media Access Control (MAC) address	<ul style="list-style-type: none"> MAC address length OUI IEEE 802
8.2 Describe the characteristics, name, and use of the seven layers of the Open Systems Interconnect (OSI) model	<ul style="list-style-type: none"> Open Systems Interconnect (OSI) model
8.3 Describe the characteristics, name, and use of the four layers of the Transmission Control Protocol/Internet Protocol (TCP/IP) model	<ul style="list-style-type: none"> Characteristics and name of the four layers of the Transmission Control Protocol/Internet Protocol (TCP/IP) model
8.4 Explain the purpose of dynamic and static routing protocols	<ul style="list-style-type: none"> Purpose of dynamic and static routing protocols
8.5 Explain the concept of ports and identify the three port ranges used in networking services and protocols [i.e., dynamic/private (49152-65535), system (0-1023), user (1024-49151), etc.]	<ul style="list-style-type: none"> Concepts of ports and identify the three port ranges used in networking services and protocols: <ul style="list-style-type: none"> Dynamic/private (49152-65535) System (0-1023) User (1024-49151)
8.6 Describe standard network ports and protocols [e.g., 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), etc.]	<ul style="list-style-type: none"> Acronyms: <ul style="list-style-type: none"> 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), etc.
8.7 Describe the applications and characteristics of Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)	<ul style="list-style-type: none"> Stateful Stateless

<p>8.8 Differentiate IPv4/IPv6 addresses and their corresponding subnet masks [i.e., classful networks, Classless Interdomain Routing (CIDR), private vs public IP]</p>	<ul style="list-style-type: none"> • Classful networks • Classless Interdomain Routing (CIDR) • Private IP • Public IP
<p>8.9 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., Asynchronous Transfer Mode (ATM), frame relay, Multiprotocol Label Switching (MPLS), etc.]</p>	<ul style="list-style-type: none"> • Basic characteristics and protocols <ul style="list-style-type: none"> ○ Metropolitan Area Network (MAN) ○ Software-Defined Wide Area Network (SD-WAN) ○ Wide Area Network (WAN) technologies ○ Asynchronous Transfer Mode (ATM) ○ Frame relay ○ Multiprotocol Label Switching (MPLS)
<p>8.10 Describe remote access protocols and services</p>	<ul style="list-style-type: none"> • Remote access protocols and services
<p>8.11 Describe the function and purpose of security protocols [i.e., Hypertext Transfer Protocol Secure (HTTPS), Secure File Transfer Protocol (SFTP), tunneling, Virtual Private Network (VPN), etc.]</p>	<ul style="list-style-type: none"> • Function and purpose of security protocol <ul style="list-style-type: none"> ○ Hypertext Transfer Protocol Secure (HTTPS) ○ Secure File Transfer Protocol (SFTP) ○ Tunneling ○ Virtual Private Network (VPN), etc.
<p>8.12 Explain the importance of proper documentation in accordance with industry standards</p>	<ul style="list-style-type: none"> • Physical topology • Logical topology • End-user agreement documentation
<p>STANDARD 9.0 CONFIGURE A BASIC NETWORK</p>	
<p>9.1 Design a network map with virtual and physical segments</p>	<ul style="list-style-type: none"> • VLAN
<p>9.2 Construct dynamic and static routes</p>	<ul style="list-style-type: none"> • Dynamic and static routes
<p>9.3 Explain proper labeling in accordance with industry standards (i.e., cable, device, rack, wall plates, etc.)</p>	<ul style="list-style-type: none"> • Proper labeling in accordance with industry standards <ul style="list-style-type: none"> ○ Cable ○ Device ○ Rack ○ Wall plates, etc.
<p>9.4 Describe the components needed and purpose to build fault tolerance into a network</p>	<ul style="list-style-type: none"> • Fault tolerance and redundancy <ul style="list-style-type: none"> ○ Mesh ○ Failover ○ Port forwarding

9.5 Describe the purpose of a disaster recovery plan for a network	<ul style="list-style-type: none"> • Offsite storage • Documentation
9.6 Install and configure a physical and/or virtual networked system (i.e., Linux/UNIX, Windows, etc.)	<ul style="list-style-type: none"> • VMware • VirtualBox (free software)
9.7 Configure network cards, network settings, and operating system	<ul style="list-style-type: none"> • Configure <ul style="list-style-type: none"> ◦ Network cards ◦ Network settings ◦ Operating system
9.8 Configure and connect devices to the network (i.e., computers, printers, routers, switches, etc.)	<ul style="list-style-type: none"> • Configure and connect devices to the network <ul style="list-style-type: none"> ◦ Computers ◦ Printers ◦ Routers ◦ Switches
9.9 Identify the appropriate tools to use for diagnostic tasks or network repair (i.e., execute Traceroute, ipconfig, Ping, etc.)	<ul style="list-style-type: none"> • Appropriate tools to use for diagnostic tasks or network repair <ul style="list-style-type: none"> ◦ Traceroute ◦ Ipconfig ◦ Ping
STANDARD 11.0 PERFORM NETWORK MAINTENANCE AND RESOLVE ISSUES	
11.1 Identify maintenance tasks and create a schedule	<ul style="list-style-type: none"> • Prioritize • Trouble tickets • Daily routine tasks (check logs, equipment, and software updates, etc.)
11.2 Describe the purpose and benefits of network utilities [i.e., Network Statistics (Netstat), Name Server Lookup (Nslookup), Ping, Traceroute, etc.]	<ul style="list-style-type: none"> • Network utilities <ul style="list-style-type: none"> ◦ Network Statistics (Netstat) ◦ Name Server Lookup (Nslookup) ◦ Ping ◦ Traceroute, etc.
11.3 Demonstrate the use of visual indicators (i.e., indicator lights on devices, etc.) and diagnostic utilities (i.e., Wireshark, etc.) to interpret problems	<ul style="list-style-type: none"> • Network utilities <ul style="list-style-type: none"> ◦ Network Statistics (Netstat) ◦ Name Server Lookup (Nslookup) ◦ Ping ◦ Traceroute, etc.

<p>11.4 Identify connectivity issues in various node environments (i.e., smart phones, switches, tablets, Linux/UNIX, Windows, etc.)</p>	<ul style="list-style-type: none"> • Connectivity issues in various environments <ul style="list-style-type: none"> ○ Smart phones ○ Switches ○ Tablets ○ Linux/UNIX ○ Windows, etc.
<p>11.5 Identify and resolve network issues (i.e., cable failure, connection failure, environmental, misconfigurations, power, user error, etc.)</p>	<ul style="list-style-type: none"> • Network issues <ul style="list-style-type: none"> ○ Cable failure ○ Connection failure ○ Environmental ○ Misconfigurations ○ Power ○ User error, etc.
<p>11.6 Identify common tools and methods of monitoring a network</p>	<ul style="list-style-type: none"> • Monitoring a network <ul style="list-style-type: none"> ○ Tools and methods ○ SolarWinds, etc.

<p>Domain 2: Devices and Framework Instructional Time: 25-35%</p>	
<p>STANDARD 7.0 DEMONSTRATE NETWORK MEDIA AND TOPOLOGIES</p>	
<p>7.1 Specify the characteristics and main features of various networking topologies (e.g., bus, mesh, ring, and star)</p>	<ul style="list-style-type: none"> • Bus • Mesh • Ring • Star
<p>7.2 Compare and contrast proper physical network topology</p>	<ul style="list-style-type: none"> • Physical network topology <ul style="list-style-type: none"> ○ Bus ○ Ring ○ Star ○ Hybrid
<p>7.3 Identify appropriate connectors, media types, and uses for various networks</p>	<ul style="list-style-type: none"> • RJ45 Female • RJ45 Male 8P8C (8 Position, 8 Contact)

7.4 Compare and contrast physical and virtual networks [i.e., Software-Defined Wide-Area Network (SD-WAN), Virtual Local Area Network (VLAN), etc.]	<ul style="list-style-type: none"> • Software-Defined Wide-Area Network (SD-WAN) • Virtual Local Area Network (VLAN)
7.5 Specify the characteristics of physical network technologies including cable types, length, speed, and topology	<ul style="list-style-type: none"> • CAT3 • CAT5 • CAT6A • CAT4 • CAT5 • CAT6 • 10BASE5 (100) • 100BASE5 (10) • FIBER
7.6 Specify the characteristics of wireless network technologies including frequency, speed, topology, and transmission (i.e., local area, metropolitan area, wide area networks, etc.)	<ul style="list-style-type: none"> • 02.11
7.7 Describe the structure of the internet (network of networks)	<ul style="list-style-type: none"> • Hierarchy <ul style="list-style-type: none"> ◦ LAN to WAN
7.8 Identify the features, functions, and purpose of commonly used network components [i.e., routers, modem, switches, bridges, hubs, NIC (network interface card), etc.]	<ul style="list-style-type: none"> • Bottom-up • NIC • Computer • Switch • Router

Domain 3: Network Security

Instructional Time: 15-25%

STANDARD 3.0 SPECIFY NETWORK SECURITY BEST PRACTICES, RISKS, AND THREATS

3.1 Perform risk management activities (e.g., define risk, determine risk level, and identify methods to address risk)	<ul style="list-style-type: none"> • Define risk • Determine risk level • Identify methods to address risk (mitigation)
3.2 Define policies to manage system and data availability, confidentiality, and integrity	<ul style="list-style-type: none"> • End-user agreements • Physical security • ACLs • Group policies

	<ul style="list-style-type: none"> • File sharing • Other topics as needed
3.3 Classify data according to its sensitivity and criticality (i.e., mission critical, protect cafeteria menu vs. personal, financial and health information, trade secrets, etc.)	<ul style="list-style-type: none"> • Prioritize the severity of data lost
3.4 Identify security threats related to computer data, hardware, and software (i.e., denial of service, eavesdropping, intrusion, unauthorized access, unauthorized use, etc.)	<ul style="list-style-type: none"> • Security threats <ul style="list-style-type: none"> ◦ Denial of service ◦ Eavesdropping ◦ Intrusion ◦ Unauthorized access ◦ Unauthorized use
3.5 Explain the importance of physical security of computer and network hardware following best practices (i.e., cameras, locks, USB port blocking, etc.)	<ul style="list-style-type: none"> • Physical security
3.6 Describe network threats (i.e., denial of service, email spoofing, hacking/cracking, intrusion, malware, phishing, social engineering, spamming, system vulnerabilities, website defacement, etc.)	<ul style="list-style-type: none"> • Social engineering
3.7 Describe best practices to protect against network threats (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.)	<ul style="list-style-type: none"> • 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.
3.8 Define best practices to protect data at rest, data in transit, and data during processing	<ul style="list-style-type: none"> • Encryption • Tunneling
3.9 Describe password best practices (i.e., age, complexity, history, length, lockout, etc.)	<ul style="list-style-type: none"> • Password best practices <ul style="list-style-type: none"> ◦ Age ◦ Complexity ◦ History ◦ Length ◦ Lockout

<p>3.10 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.]</p>	<ul style="list-style-type: none"> • Authentication methods to secure access to the network <ul style="list-style-type: none"> ○ Biometrics ○ Key cards ○ Multi-factor authentication (MFA) ○ Passwords, single sign-on (SSO) ○ Two-factor authentication (2FA)
<p>3.11 Identify best practices for access control (i.e., changing default passwords, disabling unused accounts, least privileges, privileged account management, role-based access control, etc.)</p>	<ul style="list-style-type: none"> • Access control best practices <ul style="list-style-type: none"> ○ Changing default passwords ○ Disabling unused accounts ○ Least privileges ○ Privileged account management ○ Role-based access control
<p>STANDARD 4.0 INVESTIGATE LEGAL AND ETHICAL ISSUES RELATED TO NETWORK SECURITY</p>	
<p>4.1 Explore issues regarding intellectual property rights including software licensing and software duplication [i.e., Business Software Alliance, Creative Commons, Digital Right Management (DRM), https://www.ip-watch.org/about/, https://www.eff.org/, etc.]</p>	<ul style="list-style-type: none"> • Copyright laws
<p>4.2 Differentiate among freeware, open source, proprietary, and shareware software relative to legal and ethical issues</p>	<ul style="list-style-type: none"> • Open source • Closed source
<p>4.3 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), and Sarbanes-Oxley Act (SOX)]</p>	<ul style="list-style-type: none"> • Torrenting • HIPAA
<p>4.4 Describe acceptable use of industry-related data, private and public networks, and social networking</p>	<ul style="list-style-type: none"> • Acceptable use of: <ul style="list-style-type: none"> ○ Industry-related data ○ Private networks ○ Public networks ○ Social networking
<p>STANDARD 6.0 DESCRIBE THE DEVELOPMENT AND EVOLUTION OF COMPUTERS AND NETWORK SECURITY</p>	
<p>6.1 Describe a computer and its components and function</p>	<ul style="list-style-type: none"> • Computer components and functions
<p>6.2 Explain the historical evolution of the computer and computer networks</p>	<ul style="list-style-type: none"> • ARPAnet • Computer and network timeline

6.3 Explain how the development of computers has impacted modern life	<ul style="list-style-type: none"> • Development of computers has impacted modern life <ul style="list-style-type: none"> ◦ FOMO (Fear of Missing Out) ◦ Cell phone withdrawal, etc.
6.4 Identify the components and structure of an information system [e.g., applications, media (cables, fiber, and wireless), network devices (router, switches, etc.), operating systems, and servers]	<ul style="list-style-type: none"> • Components and structure of an information system <ul style="list-style-type: none"> ◦ Applications ◦ Media (cables, fiber, and wireless) ◦ Network devices (router, switches, etc.) ◦ Operating systems and servers
6.5 Discuss future trends and societal impacts in digital devices and network technology [i.e., Internet of Things (IoT), privacy, etc.]	<ul style="list-style-type: none"> • Internet of Things (IoT)

Domain 4: Infrastructure Security Instructional Time: 5-15%	
STANDARD 2.0 MAINTAIN A SAFE AND ENVIRONMENTALLY CONSCIOUS WORK ENVIRONMENT	
2.1 Identify personal responsibility for developing and maintaining a safe and healthy work environment	<ul style="list-style-type: none"> • OSHA • AZ Professional Skills
2.2 Use equipment, materials, and tools commonly used in the field of network security correctly and safely	<ul style="list-style-type: none"> • Crimper • Cable tester • Punch down tool • PPE (Personal Protection Equipment) • ESD strap • Wire cutters
2.3 Identify ergonomic solutions to prevent injuries common to network security tasks	<ul style="list-style-type: none"> • Ergonomic solutions to prevent injuries <ul style="list-style-type: none"> ◦ Carpal tunnel ◦ Repetitive action, etc.
2.4 Determine safe working practices to avoid or eliminate electrical hazards and physical injuries	<ul style="list-style-type: none"> • Grounding and bonding
2.5 Identify techniques used to manage power consumption in the networked environment (i.e., cloud-based, software defined, etc.)	<ul style="list-style-type: none"> • Cloud-based • Software defined • Power management settings

2.6 Explain environmental considerations when disposing of computer/network components	<ul style="list-style-type: none"> • EPA (Environmental Protection Agency)
2.7 Describe and resolve most common electrostatic discharge (ESD) hazards in a network environment	<ul style="list-style-type: none"> • Generators • Fluorescent light ballasts • Microwaves, etc.
STANDARD 10.0 HARDEN A NETWORK	
10.1 Identify common network threats (i.e., denial of service, eavesdropping, intrusion, probing, unauthorized access, etc.)	<ul style="list-style-type: none"> • Denial of service • Eavesdropping • Intrusion • Probing • Unauthorized access
10.2 Identify physical network threats [i.e., disrupting media (like cutting fiber), environmental/power disruption, unauthorized access to devices, etc.]	<ul style="list-style-type: none"> • Disrupting media (similar to cutting fiber) • Environmental/power disruption • Unauthorized access to devices, etc.
10.3 Describe the benefits and purpose of segmenting networks	<ul style="list-style-type: none"> • VLAN • IP subnetting (VLSM)
10.4 Describe the benefits of disabling ports and network services	<ul style="list-style-type: none"> • Authorized access • MAC address filtering • HTTP vs. HTTPS • FTP vs. STP
10.5 Describe the techniques to secure a Wi-Fi network [i.e., Extensible Authentication Protocol (EAP), Wi-Fi Protected Access (WPA), Wi-Fi Protected Access 2 (WPA2), etc.]	<ul style="list-style-type: none"> • SSID • Default password • Default IP address • WPA • WEP • WEP2
10.6 Compare and contrast the various types of firewalls and their uses (i.e., application, packet filtering, stateful, etc.)	<ul style="list-style-type: none"> • Application, packet filtering, stateful • Hardware and software firewalls
10.7 Describe the benefits, disadvantages, and purpose of using a proxy service	<ul style="list-style-type: none"> • Benefits, disadvantages • Purpose of using a proxy service

10.8 Describe the benefits, disadvantages, and purpose of using network intrusion detection/prevention systems [i.e., Intrusion Detection System / Intrusion Prevention System (IDS/IPS), etc.]	<ul style="list-style-type: none">• Intrusion Detection System/Intrusion Prevention System (IDS/IPS), etc.
10.9 Modify an existing network diagram with appropriate network hardening devices or systems	<ul style="list-style-type: none">• “Harden” network<ul style="list-style-type: none">○ Proxy server○ VPN○ Firewall○ ACLs○ Intrusion Protection

