TestOut

TestOut Network Pro – English 6.0.x

Objective Mappings:

TestOut Network Pro
CompTIA N10-008

Revised: 2021-11-16

Powered by LABSIM

Contents

This document contains four objective mappings. Click on a mapping to view its contents.

Objective Mapping: LabSim Section to TestOut Network Pro Objectives 3

Objective Mapping: TestOut Network Pro Objectives to LabSim Section 14

Objective Mapping: LabSim Section to CompTIA N10-008 Objectives 18

Objective Mapping: CompTIA N10-008 Objectives to TestOut Section 65

Objective Mapping: LabSim Section to TestOut Network Pro Objectives

The TestOut Network Pro course covers the following TestOut Network Pro exam objectives:

Section	Title	TestOut Network Pro Objectives
1.0	**Introduction**	
1.1	Network Pro Introduction	
1.2	Use the Simulator	1.1 Implement Components and Cabling solutions • 1.1.1 - Connect and reconnect Ethernet networks 1.2 Implement Wired and Wireless devices • 1.2.5 - Connect network components
2.0	**Networking Basics**	
2.1	Networking Overview	
2.2	OSI Model and Data Encapsulation	
2.3	Data Encapsulation	
2.4	Network Protocols	
3.0	**Network Cabling and Hardware Devices**	
3.1	Copper Cables and Connectors	1.1 Implement Components and Cabling solutions • 1.1.1 - Connect and reconnect Ethernet networks 1.2 Implement Wired and Wireless devices • 1.2.5 - Connect network components

3.2	Fiber Optic Cables and Connectors	1.1 Implement Components and Cabling solutions • 1.1.1 - Connect and reconnect Ethernet networks
3.3	Wiring Implementation	1.2 Implement Wired and Wireless devices • 1.2.4 - Connect patch panel cables
3.4	Troubleshoot Network Media	
3.5	Network Adapters	1.1 Implement Components and Cabling solutions • 1.1.4 - Connect computer and network components 1.2 Implement Wired and Wireless devices • 1.2.5 - Connect network components
3.6	Networking Devices	1.2 Implement Wired and Wireless devices • 1.2.3 - Create a home wireless network • 1.2.5 - Connect network components 2.2 Configure routers and switches • 2.2.1 - Configure switches
4.0	**Network Addressing and Services**	
4.1	IP Addressing	2.1 Configure IP addressing • 2.1.1 - Configure IP addresses 2.3 Configure wireless and VoIP • 2.3.2 - Connect mobile devices

4.2	APIPA and Alternate Addressing	2.1 Configure IP addressing • 2.1.1 - Configure IP addresses
4.3	DHCP	3.1 Manage DHCP services • 3.1.1 - Implement a DHCP server • 3.1.2 - Configure DHCP options
4.4	DHCP Relay	3.1 Manage DHCP services • 3.1.1 - Implement a DHCP server • 3.1.2 - Configure DHCP options
4.5	DNS	3.2 Manage DNS services • 3.2.1 - Configure DNS addresses • 3.2.2 - Create standard DNS zones 5.1 Troubleshoot configuration and services • 5.1.3 - Troubleshoot DNS records
4.6	NTP	2.3 Configure wireless and VoIP • 2.3.5 - Configure NTP
4.7	IP Version 6	2.1 Configure IP addressing • 2.1.2 - Configure an IPv6 address
4.8	Multicast	
4.9	Troubleshoot IP Configuration Issues	5.1 Troubleshoot configuration and services • 5.1.2 - Troubleshoot IP configuration • 5.1.3 - Troubleshoot DNS records

4.10	Troubleshoot IP Communications	2.1 Configure IP addressing • 2.1.1 - Configure IP addresses
4.11	Troubleshoot DNS	3.2 Manage DNS services • 3.2.3 - Explore nslookup
5.0	**Ethernet**	
5.1	Ethernet	1.1 Implement Components and Cabling solutions • 1.1.1 - Connect and reconnect Ethernet networks
5.2	Connect Network Devices	1.1 Implement Components and Cabling solutions • 1.1.4 - Connect computer and network components
5.3	Troubleshoot Physical Connectivity	2.2 Configure routers and switches • 2.2.5 - Configure routers 5.2 Troubleshoot wired and wireless connectivity • 5.2.1 - Explore physical connectivity • 5.2.2 - Troubleshoot physical connectivity
6.0	**Firewalls and Intrusion Detection**	
6.1	Firewalls	4.1 Secure firewalls and security appliances • 4.1.1 - Configure a host firewall
6.2	Firewall Design and Implementation	4.1 Secure firewalls and security appliances • 4.1.2 - Configure a perimeter firewall • 4.1.4 - Configure a security appliance

6.3	Screened Subnets (DMZ)	4.1 Secure firewalls and security appliances • 4.1.3 - Configure a screened subnet
6.4	Intrusion Detection and Prevention	4.5 Secure network exploits • 4.5.1 - Implement an intrusion prevention system (IPS)
7.0	**Switching and Routing**	
7.1	Switching	4.2 Secure switches and wireless networks • 4.2.1 - Secure switches
7.2	Basic Switch Configuration	2.2 Configure routers and switches • 2.2.1 - Configure switches 3.3 Manage device discovery and VLANs • 3.3.3 - Create and configure VLANs
7.3	Switch Ports	1.2 Implement Wired and Wireless devices • 1.2.3 - Create a home wireless network 2.2 Configure routers and switches • 2.2.2 - Configure ports 2.3 Configure wireless and VoIP • 2.3.4 - Configure trunking
7.4	Switch Security	2.2 Configure routers and switches • 2.2.1 - Configure switches

		4.2 Secure switches and wireless networks • 4.2.1 - Secure switches • 4.2.2 - Disable switch ports
7.5	Routing	2.2 Configure routers and switches • 2.2.4 - Implement QoS
7.6	Network Address Translation	2.1 Configure IP addressing • 2.1.3 - Deploy NAT
7.7	Switching and Routing Troubleshooting	5.1 Troubleshoot configuration and services • 5.1.1 - Explore IP configuration • 5.1.2 - Troubleshoot IP configuration • 5.1.3 - Troubleshoot DNS records
8.0	**Specialized Networks**	
8.1	Corporate and Datacenter Networks	1.1 Implement Components and Cabling solutions • 1.1.3 - Configure an iSCSI initiator and target
8.2	Voice over IP (VoIP)	2.3 Configure wireless and VoIP • 2.3.3 - Configure VoIP
8.3	Virtualization	
8.4	Virtual Networking	
8.5	Cloud Concepts and Connectivity	
8.6	Internet of Things (IoT)	2.3 Configure wireless and VoIP • 2.3.1 - Connect smart devices

		3.3 Manage device discovery and VLANs • 3.3.1 - Scan for IoT devices
9.0	**Wireless Networking**	
9.1	Wireless Concepts and Standards	
9.2	Wireless Configuration	1.2 Implement Wired and Wireless devices • 1.2.3 - Create a home wireless network 2.3 Configure wireless and VoIP • 2.3.2 - Connect mobile devices 4.2 Secure switches and wireless networks • 4.2.4 - Secure a home wireless network
9.3	Wireless Network Design	1.2 Implement Wired and Wireless devices • 1.2.1 - Design indoor and outdoor wireless networks
9.4	Wireless Network Implementation	1.2 Implement Wired and Wireless devices • 1.2.2 - Implement an enterprise wireless network
9.5	Wireless Security	2.3 Configure wireless and VoIP • 2.3.2 - Connect mobile devices 4.1 Secure firewalls and security appliances • 4.1.3 - Configure a screened subnet

		4.2 Secure switches and wireless networks • 4.2.3 - Secure an enterprise wireless network • 4.2.5 - Secure email accounts on mobile devices
9.6	Wireless Troubleshooting	4.2 Secure switches and wireless networks • 4.2.3 - Secure an enterprise wireless network 5.2 Troubleshoot wired and wireless connectivity • 5.2.3 - Troubleshoot wireless network problems
10.0	**Wide Area Networks (WANs)**	
10.1	WAN Concepts	
10.2	Internet Connectivity	1.1 Implement Components and Cabling solutions • 1.1.4 - Connect computer and network components
10.3	Remote Access	4.4 Secure remote connections and VPNs • 4.4.2 - Configure a remote access VPN
10.4	Virtual Private Networks	4.4 Secure remote connections and VPNs • 4.4.2 - Configure a remote access VPN • 4.4.3 - Configure a mobile device VPN connection
11.0	**Network Operations and Management**	
11.1	Performance Metrics	
11.2	Network Management with SNMP	
11.3	Log File Management	4.1 Secure firewalls and security appliances

		• 4.1.3 - Configure a screened subnet 4.2 Secure switches and wireless networks • 4.2.2 - Disable switch ports
11.4	Monitoring	
11.5	Organization Policies	
11.6	Redundancy and High Availability	1.1 Implement Components and Cabling solutions • 1.1.6 - Configure a load balancing server 1.2 Implement Wired and Wireless devices • 1.2.6 - Configure NIC teaming
11.7	Data Backup and Storage	3.4 Manage backup and restore tasks • 3.4.1 - Back up files with File History • 3.4.2 - Recover a file from File History
11.8	Remote Management	4.4 Secure remote connections and VPNs • 4.4.1 - Allow remote desktop connections
12.0	**Network Security**	
12.1	Security Concepts	
12.2	Risk Management	
12.3	Physical Security	1.1 Implement Components and Cabling solutions • 1.1.2 - Implement physical security
12.4	Social Engineering	4.5 Secure network exploits

		• 4.5.2 - Respond to social engineering exploits
12.5	Network Threats and Attacks	4.5 Secure network exploits • 4.5.4 - Crack a password
12.6	Spoofing Attacks	3.1 Manage DHCP services • 3.1.3 - Configure DHCP snooping 4.5 Secure network exploits • 4.5.3 - Perform on-path attacks • 4.5.5 - Identify poisoning attacks
13.0	**Hardening and Update Management**	
13.1	Network Hardening	4.1 Secure firewalls and security appliances • 4.1.3 - Configure a screened subnet 4.3 Secure services and passwords • 4.3.2 - Enable and disable Linux services
13.2	Authentication	
13.3	Hardening Authentication	4.3 Secure services and passwords • 4.3.3 - Configure account password policies • 4.3.4 - Change Linux passwords
13.4	Update Management	1.1 Implement Components and Cabling solutions • 1.1.5 - Update firmware
14.0	**Network Optimization and Troubleshooting**	
14.1	Optimization	

14.2	General Network Issues	
14.3	Troubleshooting Utilities	5.1 Troubleshoot configuration and services • 5.1.4 - Troubleshoot with a network protocol analyzer
A.0	**TestOut Network Pro - Practice Exams**	
A.1	Prepare for TestOut Network Pro Certification	
A.2	TestOut Network Pro Domain Review	
B.0	**CompTIA Network+ N10-008 Practice Exams**	
B.1	Prepare for Certification	
B.2	CompTIA Network+ N10-008 Practice Exams (20 Questions)	
B.3	CompTIA Network+ N10-008 Practice Exams (All Questions)	

Objective Mapping: TestOut Network Pro Objectives to LabSim Section

The TestOut Network Pro course and certification exam cover the following TestOut Network Pro objectives:

#	Domain	Module.Section
1.0	**Hardware**	
1.1	Implement Components and Cabling solutions 1.1.1 - Connect and reconnect Ethernet networks 1.1.2 - Implement physical security 1.1.3 - Configure an iSCSI initiator and target 1.1.4 - Connect computer and network components 1.1.5 - Update firmware 1.1.6 - Configure a load balancing server	1.2 3.1, 3.2, 3.5 5.1, 5.2 8.1 10.2 11.6 12.3 13.4
1.2	Implement Wired and Wireless devices 1.2.1 - Design indoor and outdoor wireless networks 1.2.2 - Implement an enterprise wireless network 1.2.3 - Create a home wireless network 1.2.4 - Connect patch panel cables 1.2.5 - Connect network components 1.2.6 - Configure NIC teaming	1.2 3.1, 3.3, 3.5, 3.6 7.3 9.2, 9.3, 9.4 11.6
2.0	**Configuration**	
2.1	Configure IP addressing 2.1.1 - Configure IP addresses 2.1.2 - Configure an IPv6 address 2.1.3 - Deploy NAT	4.1, 4.2, 4.7, 4.10 7.6

2.2	Configure routers and switches 2.2.1 - Configure switches 2.2.2 - Configure ports 2.2.3 - Implement Spanning Tree 2.2.4 - Implement QoS 2.2.5 - Configure routers	3.6 5.3 7.2, 7.3, 7.4, 7.5
2.3	Configure wireless and VoIP 2.3.1 - Connect smart devices 2.3.2 - Connect mobile devices 2.3.3 - Configure VoIP 2.3.4 - Configure trunking 2.3.5 - Configure NTP	4.1, 4.6 7.3 8.2, 8.6 9.2, 9.5
3.0	**Management**	
3.1	Manage DHCP services 3.1.1 - Implement a DHCP server 3.1.2 - Configure DHCP options 3.1.3 - Configure DHCP snooping 3.1.4 - Configure a DHCP relay agent	4.3, 4.4 12.6
3.2	Manage DNS services 3.2.1 - Configure DNS addresses 3.2.2 - Create standard DNS zones 3.2.3 - Explore nslookup	4.5, 4.11
3.3	Manage device discovery and VLANs 3.3.1 - Scan for IoT devices	7.2 8.6

	3.3.2 - Scan networks 3.3.3 - Create and configure VLANs	
3.4	Manage backup and restore tasks 3.4.1 - Back up files with File History 3.4.2 - Recover a file from File History	11.7
4.0	**Security**	
4.1	Secure firewalls and security appliances 4.1.1 - Configure a host firewall 4.1.2 - Configure a perimeter firewall 4.1.3 - Configure a screened subnet 4.1.4 - Configure a security appliance	6.1, 6.2, 6.3 9.5 11.3 13.1
4.2	Secure switches and wireless networks 4.2.1 - Secure switches 4.2.2 - Disable switch ports 4.2.3 - Secure an enterprise wireless network 4.2.4 - Secure a home wireless network 4.2.5 - Secure email accounts on mobile devices	7.1, 7.4 9.2, 9.5, 9.6 11.3
4.3	Secure services and passwords 4.3.1 - Disable network service 4.3.2 - Enable and disable Linux services 4.3.3 - Configure account password policies 4.3.4 - Change Linux passwords	13.1, 13.3
4.4	Secure remote connections and VPNs	10.3, 10.4 11.8

	4.4.1 - Allow remote desktop connections 4.4.2 - Configure a remote access VPN 4.4.3 - Configure a mobile device VPN connection	
4.5	Secure network exploits 4.5.1 - Implement an intrusion prevention system (IPS) 4.5.2 - Respond to social engineering exploits 4.5.3 - Perform on-path attacks 4.5.4 - Crack a password 4.5.5 - Identify poisoning attacks	6.4 12.4, 12.5, 12.6
5.0	**Troubleshooting**	
5.1	Troubleshoot configuration and services 5.1.1 - Explore IP configuration 5.1.2 - Troubleshoot IP configuration 5.1.3 - Troubleshoot DNS records 5.1.4 - Troubleshoot with a network protocol analyzer	4.5, 4.9 7.7 14.3
5.2	Troubleshoot wired and wireless connectivity 5.2.1 - Explore physical connectivity 5.2.2 - Troubleshoot physical connectivity 5.2.3 - Troubleshoot wireless network problems	5.3 9.6

Objective Mapping: LabSim Section to CompTIA N10-008 Objectives

Section	Title	Objectives
1.0	**Introduction**	
1.1	Network Pro Introduction	
1.2	Use the Simulator	
2.0	**Networking Basics**	
2.1	Networking Overview	1.1 Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts. • 1.1.1 - OSI model 1.2 Explain the characteristics of network topologies and network types. • 1.2.1 - Mesh • 1.2.2 - Star/hub-and-spoke • 1.2.3 - Bus • 1.2.4 - Ring • 1.2.5 - Hybrid • 1.2.6 - Network types and characteristics 1.2.6.1 - Peer-to-peer 1.2.6.2 - Client-server 1.2.6.3 - Local area network (LAN) 1.2.6.4 - Metropolitan area network (MAN) 1.2.6.5 - Wide area network (WAN) 1.2.6.6 - Wireless local area network (WLAN) 1.2.6.7 - Personal area network (PAN) 1.2.6.8 - Campus area network (CAN) 1.2.6.9 - Storage area network (SAN)

		1.2.6.10 - Software-defined wide area network (SDWAN) 1.2.6.11 - Multiprotocol label switching (MPLS) 1.2.6.12 - Multipoint generic routing encapsulation (mGRE) • 1.2.9 - Provider links 1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution. • 1.3.1 - Copper 1.3.1.1 - Twisted pair • 1.3.2 - Fiber • 1.3.3 - Connector types 1.3.3.3 - RJ45 1.4 Given a scenario, configure a subnet and use appropriate IP addressing schemes. • 1.4.1 - Public vs. private • 1.4.2 - IPv4 vs. IPv6 • 1.4.3 - IPv4 subnetting 2.1 Compare and contrast various devices, their features, and their appropriate placement on the network. • 2.1.1 - Networking devices 2.1.1.3 - Router 3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution. • 3.3.7 - Network device backup/restore

2.2	OSI Model and Data Encapsulation	1.1 Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts. • 1.1.1 - OSI model 1.1.1.1 - Layer 1 – Physical 1.1.1.2 - Layer 2 – Data link 1.1.1.3 - Layer 3 – Network 1.1.1.4 - Layer 4 – Transport 1.1.1.5 - Layer 5 – Session 1.1.1.6 - Layer 6 – Presentation 1.1.1.7 - Layer 7 – Application
2.3	Data Encapsulation	1.1 Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts. • 1.1.2 - Data encapsulation and decapsulation within the OSI model context 1.1.2.1 - Ethernet header 1.1.2.2 - Internet Protocol (IP) header 1.1.2.3 - Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) headers 1.1.2.4 - TCP flags 1.1.2.5 - Payload 1.1.2.6 - Maximum transmission unit (MTU) 2.3 Given a scenario, configure and deploy common Ethernet switching features. • 2.3.8 - Address Resolution Protocol (ARP)
2.4	Network Protocols	1.5 Explain common ports and protocols, their application, and encrypted alternatives. • 1.5.1 - File Transfer Protocol (FTP) Ports 20/21 • 1.5.2 - Secure Shell (SSH) Port 22 • 1.5.3 - Secure File Transfer Protocol (SFTP) Port 22 • 1.5.4 - Telnet Port 23

		• 1.5.5 - Simple Mail Transfer Protocol (SMTP) Port 25 • 1.5.6 - Domain Name System (DNS) Port 53 • 1.5.7 - Dynamic Host Configuration Protocol (DHCP) Ports 67/68 • 1.5.8 - Trivial File Transfer Protocol (TFTP) Port 69 • 1.5.9 - Hypertext Transfer Protocol (HTTP) Port 80 • 1.5.10 - Post Office Protocol v3 (POP3) Port 110 • 1.5.11 - Network Time Protocol (NTP) Port 123 • 1.5.12 - Internet Message Access Protocol (IMAP) Port 143 • 1.5.13 - Simple Network Management Protocol (SNMP) Ports 161/162 • 1.5.14 - Lightweight Directory Access Protocol (LDAP) Port 389 • 1.5.15 - Hypertext Transfer Protocol Secure (HTTPS) [Secure Sockets Layer (SSL)] Port 443 • 1.5.16 - HTTPS [Transport Layer Security (TLS)] Port 443 • 1.5.17 - Server Message Block (SMB) Port 445 • 1.5.18 - Syslog Port 514 • 1.5.19 - SMTP TLS Port 587 • 1.5.20 - Lightweight Directory Access Protocol (over SSL) (LDAPS) Port 636 • 1.5.21 - IMAP over SSL Port993 • 1.5.22 - POP3 over SSL Port 995 • 1.5.23 - Structured Query Language (SQL) Server Port 1433 • 1.5.24 - SQLnet Port 1521 • 1.5.25 - MySQL Port 3306 • 1.5.26 - Remote Desktop Protocol (RDP) Port 3389 • 1.5.27 - Session Initiation Protocol (SIP) Ports 5060/5061 • 1.5.28 - IP protocol types 1.5.28.1 - Internet Control Message Protocol (ICMP) 1.5.28.2 - TCP 1.5.28.3 - UDP 1.5.28.4 - Generic Routing Encapsulation (GRE) 1.5.28.5 - Internet Protocol Security (IPSec) 1.5.28.5.1 - Internet Protocol Security (IPSec) - Authentication Header (AH)/Encapsulating Security Payload (ESP) • 1.5.29 - Connectionless vs. connection-oriented
3.0	**Network Cabling and Hardware Devices**	

3.1	Copper Cables and Connectors	1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution. • 1.3.1 - Copper 1.3.1.1 - Twisted pair 1.3.1.1.1 - Twisted pair - Cat 5 1.3.1.1.2 - Twisted pair - Cat 5e 1.3.1.1.3 - Twisted pair - Cat 6 1.3.1.1.4 - Twisted pair - Cat 6a 1.3.1.1.5 - Twisted pair - Cat 7 1.3.1.1.6 - Twisted pair - Cat 8 1.3.1.2 - Coaxial/RG-6 1.3.1.3 - Twinaxial 1.3.1.4 - Termination standards 1.3.1.4.1 - Termination standards - TIA/EIA-568A 1.3.1.4.2 - Termination standards - TIA/EIA-568B • 1.3.2 - Fiber • 1.3.3 - Connector types 1.3.3.2 - RJ11 1.3.3.3 - RJ45 1.3.3.4 - F-type connector 5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools. • 5.2.1 - Specifications and limitations 5.2.1.1 - Throughput 5.2.1.2 - Speed 5.2.1.3 - Distance • 5.2.2 - Cable considerations 5.2.2.1 - Shielded and unshielded

		5.2.2.2 - Plenum and riser-rated • 5.2.5 - Common tools 5.2.5.1 - Cable crimper
3.2	Fiber Optic Cables and Connectors	1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution. • 1.3.2 - Fiber 1.3.2.1 - Single-mode 1.3.2.2 - Multimode • 1.3.3 - Connector types 1.3.3.1 - Local connector (LC), straight tip (ST), subscriber connector (SC), mechanical transfer (MT), registered jack (RJ) 1.3.3.1.1 - Local connector (LC), straight tip (ST), subscriber connector (SC), mechanical transfer (MT), registered jack (RJ) - Angled physical contact (APC) 1.3.3.1.2 - Local connector (LC), straight tip (ST), subscriber connector (SC), mechanical transfer (MT), registered jack (RJ) - Ultra-physical contact (UPC) 1.3.3.5 - Transceivers/media converters 1.3.3.6 - Transceiver type 1.3.3.6.1 - Transceiver type - Small form-factor pluggable (SFP) 1.3.3.6.2 - Transceiver type - Enhanced form-factor pluggable (SFP+) 1.3.3.6.3 - Transceiver type - Quad small form-factor pluggable (QSFP) 1.3.3.6.4 - Transceiver type - Enhanced quad small form-factor pluggable (QSFP+)
3.3	Wiring Implementation	1.2 Explain the characteristics of network topologies and network types. • 1.2.7 - Service-related entry point 1.2.7.1 - Demarcation point

		1.2.7.2 - Smartjack 1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution. • 1.3.1 - Copper 1.3.1.1 - Twisted pair 1.3.1.1.1 - Twisted pair - Cat 5 1.3.1.1.2 - Twisted pair - Cat 5e 1.3.1.1.3 - Twisted pair - Cat 6 1.3.1.1.4 - Twisted pair - Cat 6a 1.3.1.1.5 - Twisted pair - Cat 7 1.3.1.1.6 - Twisted pair - Cat 8 1.3.1.4 - Termination standards 1.3.1.4.1 - Termination standards - TIA/EIA-568A 1.3.1.4.2 - Termination standards - TIA/EIA-568B • 1.3.3 - Connector types 1.3.3.3 - RJ45 • 1.3.4 - Cable management 1.3.4.1 - Patch panel/patch bay 1.3.4.2 - Punchdown block 1.3.4.2.1 - Punchdown block - 66 1.3.4.2.2 - Punchdown block - 110 1.3.4.2.3 - Punchdown block - Krone 1.3.4.2.4 - Punchdown block - Bix 5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools. • 5.2.3 - Cable application

		5.2.3.3 - Power over Ethernet • 5.2.5 - Common tools 5.2.5.1 - Cable crimper 5.2.5.7 - Cable tester
3.4	Troubleshoot Network Media	1.2 Explain the characteristics of network topologies and network types. • 1.2.7 - Service-related entry point 1.2.7.2 - Smartjack 1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution. • 1.3.2 - Fiber • 1.3.3 - Connector types 1.3.3.1 - Local connector (LC), straight tip (ST), subscriber connector (SC), mechanical transfer (MT), registered jack (RJ) 5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools. • 5.2.1 - Specifications and limitations 5.2.1.1 - Throughput 5.2.1.2 - Speed 5.2.1.3 - Distance • 5.2.2 - Cable considerations 5.2.2.1 - Shielded and unshielded

		5.2.2.2 - Plenum and riser-rated • 5.2.3 - Cable application 5.2.3.1 - Rollover cable/console cable 5.2.3.2 - Crossover cable 5.2.3.3 - Power over Ethernet • 5.2.4 - Common issues 5.2.4.1 - Attenuation 5.2.4.2 - Interference 5.2.4.3 - Decibel (dB) loss 5.2.4.4 - Incorrect pinout 5.2.4.5 - Bad ports 5.2.4.6 - Open/short 5.2.4.7 - Light-emitting diode (LED) status indicators 5.2.4.8 - Incorrect transceivers 5.2.4.9 - Duplexing issues 5.2.4.10 - Transmit and receive (TX/RX) reversed 5.2.4.11 - Dirty optical cables • 5.2.5 - Common tools 5.2.5.1 - Cable crimper 5.2.5.2 - Punchdown tool 5.2.5.3 - Tone generator 5.2.5.4 - Loopback adapter 5.2.5.5 - Optical time-domain reflectometer (OTDR) 5.2.5.6 - Multimeter 5.2.5.7 - Cable tester 5.2.5.8 - Wire map 5.2.5.9 - Tap 5.2.5.10 - Fusion splicers 5.2.5.11 - Spectrum analyzers 5.2.5.12 - Snips/cutters 5.2.5.13 - Cable stripper

		5.2.5.14 - Fiber light meter
3.5	Network Adapters	1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution. • 1.3.3 - Connector types 1.3.3.5 - Transceivers/media converters 1.3.3.6 - Transceiver type 1.3.3.6.1 - Transceiver type - Small form-factor pluggable (SFP) 1.3.3.6.2 - Transceiver type - Enhanced form-factor pluggable (SFP+) 1.3.3.6.3 - Transceiver type - Quad small form-factor pluggable (QSFP) 1.3.3.6.4 - Transceiver type - Enhanced quad small form-factor pluggable (QSFP+) 2.1 Compare and contrast various devices, their features, and their appropriate placement on the network. • 2.1.1 - Networking devices 2.1.1.14 - Media Converter 2.3 Given a scenario, configure and deploy common Ethernet switching features. • 2.3.8 - Address Resolution Protocol (ARP)
3.6	Networking Devices	2.1 Compare and contrast various devices, their features, and their appropriate placement on the network. • 2.1.1 - Networking devices 2.1.1.1 - Layer 2 switch 2.1.1.2 - Layer 3 capable switch 2.1.1.3 - Router 2.1.1.4 - Hub 2.1.1.5 - Access point

		2.1.1.6 - Bridge 2.1.1.7 - Wireless LAN controller 2.1.1.16 - Firewall 3.2 Explain the purpose of organizational documents and policies. • 3.2.3 - Common documentation 3.2.3.1 - Physical network diagram 3.2.3.1.1 - Physical network diagram - Floor plan 3.2.3.1.2 - Physical network diagram - Rack diagram 3.2.3.1.3 - Physical network diagram - Intermediate distribution frame (IDF)/main distribution frame (MDF) documentation 3.2.3.2 - Logical network diagram 3.2.3.3 - Wiring diagram
4.0	**Network Addressing and Services**	
4.1	IP Addressing	1.4 Given a scenario, configure a subnet and use appropriate IP addressing schemes. • 1.4.1 - Public vs. private 1.4.1.1 - RFC1918 • 1.4.2 - IPv4 vs. IPv6 1.4.2.1 - Automatic Private IP Addressing (APIPA) 1.4.2.9 - Default gateway • 1.4.3 - IPv4 subnetting 1.4.3.1 - Classless (variable-length subnet mask) 1.4.3.2 - Classful 1.4.3.2.1 - Classful - A 1.4.3.2.2 - Classful - B

		1.4.3.2.3 - Classful - C 1.4.3.2.4 - Classful - D 1.4.3.2.5 - Classful - E 1.4.3.3 - Classless Inter-Domain Routing (CIDR) notation
4.2	APIPA and Alternate Addressing	1.4 Given a scenario, configure a subnet and use appropriate IP addressing schemes. • 1.4.2 - IPv4 vs. IPv6 1.4.2.1 - Automatic Private IP Addressing (APIPA)
4.3	DHCP	1.6 Explain the use and purpose of network services. • 1.6.1 - DHCP 1.6.1.1 - Scope 1.6.1.2 - Exclusion ranges 1.6.1.3 - Reservation 1.6.1.4 - Dynamic assignment 1.6.1.5 - Static assignment 1.6.1.6 - Lease time 1.6.1.7 - Scope options 1.6.1.8 - Available leases 1.6.1.9 - DHCP relay 1.6.1.10 - IP helper/UDP forwarding
4.4	DHCP Relay	1.6 Explain the use and purpose of network services. • 1.6.1 - DHCP 1.6.1.9 - DHCP relay 1.6.1.10 - IP helper/UDP forwarding

4.5	DNS	1.6 Explain the use and purpose of network services. • 1.6.2 - DNS 1.6.2.1 - Record types 1.6.2.1.1 - Record types - Address (A) 1.6.2.1.2 - Record types - Canonical name (CNAME) 1.6.2.1.3 - Record types - Mail exchange (MX) 1.6.2.1.4 - Record types - Authentication, authorization, accounting, auditing (AAAA 1.6.2.1.5 - Record types - Start of authority (SOA) 1.6.2.1.6 - Record types - Pointer (PTR) 1.6.2.1.7 - Record types - Text (TXT) 1.6.2.1.8 - Record types - Service (SRV) 1.6.2.1.9 - Record types - Name server (NS) 1.6.2.2 - Global hierarchy 1.6.2.2.1 - Global hierarchy - Root DNS servers 1.6.2.2.2 - Global hierarchy - Internal vs. external 1.6.2.2.3 - Global hierarchy - Zone transfers 1.6.2.2.4 - Global hierarchy - Authoritative name servers 1.6.2.2.5 - Global hierarchy - Time to live (TTL) 1.6.2.2.6 - Global hierarchy - DNS caching 1.6.2.2.7 - Global hierarchy - Reverse DNS/reverse lookup/forward lookup 1.6.2.2.8 - Global hierarchy - Recursive lookup/iterative lookup
4.6	NTP	1.6 Explain the use and purpose of network services. • 1.6.3 - NTP 1.6.3.1 - Stratum 1.6.3.2 - Clients 1.6.3.4 - Servers
4.7	IP Version 6	1.4 Given a scenario, configure a subnet and use appropriate IP addressing schemes. • 1.4.2 - IPv4 vs. IPv6

		1.4.2.1 - Automatic Private IP Addressing (APIPA) 1.4.2.2 - Extended unique identifier (EUI-64) 1.4.2.3 - Multicast 1.4.2.4 - Unicast 1.4.2.5 - Anycast 1.4.2.6 - Broadcast 1.4.2.7 - Link local 1.4.2.8 - Loopback 1.4.2.9 - Default gateway • 1.4.4 - IPv6 concepts 1.4.4.1 - Tunneling 1.4.4.2 - Dual stack 1.4.4.3 - Shorthand notation 1.4.4.4 - Router advertisement 1.4.4.5 - Stateless address autoconfiguration (SLAAC)
4.8	Multicast	1.4 Given a scenario, configure a subnet and use appropriate IP addressing schemes. • 1.4.2 - IPv4 vs. IPv6 1.4.2.3 - Multicast 1.4.2.4 - Unicast 1.4.2.5 - Anycast 1.4.2.6 - Broadcast
4.9	Troubleshoot IP Configuration Issues	5.3 Given a scenario, use the appropriate network software tools and commands. • 5.3.2 - Command line tool 5.3.2.1 - ping 5.3.2.2 - ipconfig/ifconfig/ip

		5.5 Given a scenario, troubleshoot general networking issues. • 5.5.2 - Common issues 5.5.2.3 - Duplicate MAC address
4.10	Troubleshoot IP Communications	5.3 Given a scenario, use the appropriate network software tools and commands. • 5.3.2 - Command line tool 5.3.2.1 - ping 5.3.2.2 - ipconfig/ifconfig/ip 5.3.2.4 - traceroute/tracert 5.3.2.5 - arp 5.3.2.6 - netstat
4.11	Troubleshoot DNS	5.3 Given a scenario, use the appropriate network software tools and commands. • 5.3.2 - Command line tool 5.3.2.1 - ping 5.3.2.2 - ipconfig/ifconfig/ip 5.3.2.3 - nslookup/dig 5.3.2.4 - traceroute/tracert 5.3.2.7 - hostname 5.5 Given a scenario, troubleshoot general networking issues. • 5.5.2 - Common issues 5.5.2.19 - DNS issues
5.0	**Ethernet**	

5.1	Ethernet	1.2 Explain the characteristics of network topologies and network types. • 1.2.2 - Star/hub-and-spoke • 1.2.3 - Bus 1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution. • 1.3.5 - Ethernet standards 1.3.5.1 - Copper 1.3.5.1.1 - Copper - 10BASE-T 1.3.5.1.2 - Copper - 100BASE-TX 1.3.5.1.3 - Copper - 1000BASE-T 1.3.5.1.4 - Copper - 10GBASE-T 1.3.5.1.5 - Copper - 40GBASE-T 1.3.5.2 - Fiber 1.3.5.2.1 - 100BASE-FX 1.3.5.2.2 - 100BASE-SX 1.3.5.2.3 - 1000BASE-SX 1.3.5.2.4 - 1000BASE-LX 1.3.5.2.5 - 10GBASE-SR 1.3.5.2.6 - 10GBASE-LR 1.3.5.2.7 - Coarse wavelength division multiplexing (CWDM) 1.3.5.2.8 - Dense wavelength division multiplexing (DWDM) 1.3.5.2.8 - Bidirectional wavelength division multiplexing (WDM) 2.3 Given a scenario, configure and deploy common Ethernet switching features. • 2.3.7 - Carrier-sense multiple access with collision detection (CSMA/CD)
5.2	Connect Network Devices	5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools. • 5.2.3 - Cable application 5.2.3.1 - Rollover cable/console cable

		5.2.3.2 - Crossover cable
5.3	Troubleshoot Physical Connectivity	1.2 Explain the characteristics of network topologies and network types. • 1.2.1 - Mesh • 1.2.2 - Star/hub-and-spoke • 1.2.3 - Bus • 1.2.4 - Ring • 1.2.5 - Hybrid 5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools. • 5.2.2 - Cable considerations
6.0	**Firewalls and Intrusion Detection**	
6.1	Firewalls	4.3 Given a scenario, apply network hardening techniques. • 4.3.1 - Best practices 4.3.1.14 - Access control list 4.3.1.15 - Role-based access 4.3.1.16 - Firewall rules 4.3.1.16.1 - Firewall rules - Explicit deny 4.3.1.16.2 - Firewall rules - Implicit deny
6.2	Firewall Design and Implementation	2.1 Compare and contrast various devices, their features, and their appropriate placement on the network. • 2.1.1 - Networking devices 2.1.1.9 - Proxy server 2.1.1.15 - Intrusion prevention system (IPS)/intrusion detection system (IDS) device

		2.1.1.16 - Firewall 4.1 Explain common security concepts. • 4.1.8 - Defense in depth 4.1.8.2 - Screened subnet [previously known as demilitarized zone (DMZ)] 4.3 Given a scenario, apply network hardening techniques. • 4.3.1 - Best practices 4.3.1.14 - Access control list 4.3.1.15 - Role-based access 4.3.1.16 - Firewall rules 4.3.1.16.1 - Firewall rules - Explicit deny 4.3.1.16.2 - Firewall rules - Implicit deny 5.5 Given a scenario, troubleshoot general networking issues. • 5.5.2 - Common issues 5.5.2.16 - Host-based/network-based firewall settings
6.3	Screened Subnets (DMZ)	4.1 Explain common security concepts. • 4.1.8 - Defense in depth 4.1.8.2 - Screened subnet [previously known as demilitarized zone (DMZ)]
6.4	Intrusion Detection and Prevention	2.1 Compare and contrast various devices, their features, and their appropriate placement on the network. • 2.1.1 - Networking devices

		2.1.1.15 - Intrusion prevention system (IPS)/intrusion detection system (IDS) device
7.0	**Switching and Routing**	
7.1	Switching	2.1 Compare and contrast various devices, their features, and their appropriate placement on the network. • 2.1.1 - Networking devices 2.1.1.1 - Layer 2 switch 2.1.1.2 - Layer 3 capable switch 2.1.1.3 - Router 4.4 Compare and contrast remote access methods and security implications. • 4.4.9 - In-band vs. out-of-band management
7.2	Basic Switch Configuration	2.1 Compare and contrast various devices, their features, and their appropriate placement on the network. • 2.1.1 - Networking devices 2.1.1.1 - Layer 2 switch 2.1.1.2 - Layer 3 capable switch 2.1.1.3 - Router 2.3 Given a scenario, configure and deploy common Ethernet switching features. • 2.3.1 - Data virtual local area network (VLAN) • 2.3.2 - Voice VLAN • 2.3.3 - Port configurations 2.3.3.9 - Auto-medium-dependent interface crossover (MDI-X) • 2.3.4 - Media access control (MAC) address tables

		• 2.3.7 - Carrier-sense multiple access with collision detection (CSMA/CD) • 2.3.8 - Address Resolution Protocol (ARP) • 2.3.9 - Neighbor Discovery Protocol 4.4 Compare and contrast remote access methods and security implications. • 4.4.9 - In-band vs. out-of-band management
7.3	Switch Ports	2.1 Compare and contrast various devices, their features, and their appropriate placement on the network. • 2.1.1 - Networking devices 2.1.1.1 - Layer 2 switch 2.1.1.2 - Layer 3 capable switch 2.3 Given a scenario, configure and deploy common Ethernet switching features. • 2.3.1 - Data virtual local area network (VLAN) • 2.3.3 - Port configurations 2.3.3.1 - Port tagging/802.1Q 2.3.3.2 - Port aggregation 2.3.3.2.1 -Port aggregation - Link Aggregation Control Protocl (LACP) 2.3.3.6 - Port mirroring 2.3.3.8 - Jumbo frames • 2.3.5 - Power over Ethernet (PoE)/Power over Ethernet plus (PoE+) • 2.3.6 - Spanning Tree Protocol
7.4	Switch Security	2.1 Compare and contrast various devices, their features, and their appropriate placement on the network. • 2.1.1 - Networking devices 2.1.1.1 - Layer 2 switch 2.1.1.2 - Layer 3 capable switch

		2.1.1.3 - Router 2.3 Given a scenario, configure and deploy common Ethernet switching features. • 2.3.1 - Data virtual local area network (VLAN) • 2.3.2 - Voice VLAN • 2.3.3 - Port configurations 2.3.3.7 - Port security 4.1 Explain common security concepts. • 4.1.9 - Authentication methods 4.1.9.8 - 802.1X 4.2 Compare and contrast common types of attacks. • 4.2.1 - Technology-based 4.2.1.4 - VLAN hopping 4.2.1.5 - ARP spoofing 4.2.1.11 - MAC spoofing 4.3 Given a scenario, apply network hardening techniques. • 4.3.2 - Wireless security 4.3.2.1 - MAC filtering
7.5	Routing	1.4 Given a scenario, configure a subnet and use appropriate IP addressing schemes. • 1.4.5 - Virtual IP (VIP) • 1.4.6 - Subinterfaces

		2.2 Compare and contrast routing technologies and bandwidth management concepts. • 2.2.1 - Routing 2.2.1.1 - Dynamic routing 2.2.1.1.1 - Dynamic routing - Protocols [Routing Internet Protocol (RIP), Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol 2.2.1.1.2 - Dynamic routing - Link state vs. distance vector vs. hybrid 2.2.1.2 - Static routing 2.2.1.3 - Default route 2.2.1.4 - Administrative distance 2.2.1.5 - Exterior vs. interior 2.2.1.6 - Time to live • 2.2.2 - Bandwidth management 2.2.2.1 - Traffic shaping 2.2.2.2 - Quality of service (QoS) 2.3 Given a scenario, configure and deploy common Ethernet switching features. • 2.3.3 - Port configurations 2.3.3.1 - Port tagging/802.1Q 3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution. • 3.3.6 - Redundancy and high availability (HA) concepts 3.3.6.5.2 - Active-active vs. active-passive - Virtual Router Redundancy Protocol (VRRP)/First Hop Redundancy Protocol (FHRP)

7.6	Network Address Translation	1.4 Given a scenario, configure a subnet and use appropriate IP addressing schemes. • 1.4.1 - Public vs. private 1.4.1.2 - Network address translation (NAT) 1.4.1.3 - Port address translation (PAT)
7.7	Switching and Routing Troubleshooting	5.5 Given a scenario, troubleshoot general networking issues. • 5.5.1 - Considerations 5.5.1.1 - Device configuration review 5.5.1.2 - Routing tables 5.5.1.3 - Interface status 5.5.1.4 - VLAN assignment 5.5.1.5 - Network performance baselines • 5.5.2 - Common issues 5.5.2.1 - Collisions 5.5.2.2 - Broadcast storm 5.5.2.3 - Duplicate MAC address 5.5.2.4 - Duplicate IP address 5.5.2.5 - Multicast flooding 5.5.2.6 - Asymmetrical routing 5.5.2.7 - Switching loops 5.5.2.8 - Routing loops 5.5.2.9 - Rogue DHCP server 5.5.2.10 - DHCP scope exhaustion 5.5.2.11 - IP setting issues 5.5.2.11.1 - IP setting issues - Incorrect gateway 5.5.2.11.2 - IP setting issues - Incorect subnet mask 5.5.2.11.3 - IP setting issues - Incorrect IP address 5.5.2.11.4 - IP setting issues - Incorrect DNS 5.5.2.12 - Missing route

8.0	Specialized Networks	
8.1	Corporate and Datacenter Networks	1.7 Explain basic corporate and datacenter network architecture. • 1.7.2 - Software-defined networking 1.7.2.1 - Application layer 1.7.2.2 - Control layer 1.7.2.3 - Infrastructure layer 1.7.2.4 - Management plane • 1.7.5 - Storage area networks 1.7.5.1 - Connection types 1.7.5.1.1 - Connection types - Fibre Channel over Ethernet (FCoE) 1.7.5.1.2 - Connection types - Fibre Channel 1.7.5.1.3 - Connection types - Internet Small Computer Systems Interface (iSCSI)
8.2	Voice over IP (VoIP)	2.1 Compare and contrast various devices, their features, and their appropriate placement on the network. • 2.1.1 - Networking devices 2.1.1.13 - Voice gateway • 2.1.2 - Networked devices 2.1.2.1 - Voice over Internet Protocol (VoIP) phone 2.2 Compare and contrast routing technologies and bandwidth management concepts. • 2.2.2 - Bandwidth management

		2.2.2.2 - Quality of service (QoS)
8.3	Virtualization	1.2 Explain the characteristics of network topologies and network types. • 1.2.8 - Virtual network concepts 1.2.8.1 - vSwitch 1.2.8.2 - Virtual network interface card (vNIC) 1.2.8.3 - Network function virtualization (NFV) 1.2.8.4 - Hypervisor 4.4 Compare and contrast remote access methods and security implications. • 4.4.7 - Virtual desktop
8.4	Virtual Networking	1.2 Explain the characteristics of network topologies and network types. • 1.2.8 - Virtual network concepts 1.2.8.1 - vSwitch 1.2.8.2 - Virtual network interface card (vNIC) 1.2.8.3 - Network function virtualization (NFV) 1.2.8.4 - Hypervisor
8.5	Cloud Concepts and Connectivity	1.8 Summarize cloud concepts and connectivity options. • 1.8.1 - Deployment models 1.8.1.1 - Public 18.1.2 - Private 1.8.1.3 - Hybrid 1.8.1.4 - Community • 1.8.2 - Service models

		1.8.2.1 - Software as a service (SaaS) 1.8.2.2 - Infrastructure as a service (IaaS) 1.8.2.3 - Platform as a service (PaaS) 1.8.2.4 - Desktop as a service (DaaS) • 1.8.4 - Connectivity options 1.8.4.1 - Virtual private network (VPN) 1.8.4.2 - Private-direct connection to cloud provider • 1.8.5 - Multitenancy • 1.8.6 - Elasticity • 1.8.7 - Scalability • 1.8.8 - Security implications
8.6	Internet of Things (IoT)	2.1 Compare and contrast various devices, their features, and their appropriate placement on the network. • 2.1.2 - Networked devices 2.1.2.6 - Internet of Things (IoT) 2.1.2.6.1 - Internet of Things (IoT) - Refrigerator 2.1.2.6.2 - Internet of Things (IoT) - Smart speakers 2.1.2.6.3 - Internet of Things (IoT) - Smart thermostats 2.1.2.6.4 - Internet of Things (IoT) - Smart doorbells 2.1.2.7 - Industrial control systems/supervisory control and data acquisition (SCADA)
9.0	**Wireless Networking**	
9.1	Wireless Concepts and Standards	2.4 Given a scenario, install and configure the appropriate wireless standards and technologies. • 2.4.1 - 802.11 standards 2.4.1.1 - a

		2.4.1.2 - b 2.4.1.3 - g 2.4.1.4 - n (WiFi 4) 2.4.1.5 - ac (WiFi 5) 2.4.1.6 - ax (WiFi 6) • 2.4.2 - Frequencies and range 2.4.2.1 - 2.4GHz 2.4.2.2 - 5GHz • 2.4.3 - Channels 2.4.3.1 - Regulatory impacts • 2.4.4 - Channel bonding • 2.4.5 - Service set identifier (SSID) 2.4.5.1 - Basic service set 2.4.5.2 - Extended service set 2.4.5.3 - Independent basic service set (Ad-hoc) 2.4.5.4 - Roaming • 2.4.9 - Multiple input, multiple output (MIMO) and multi-user MIMO (MU-MIMO)
9.2	Wireless Configuration	2.4 Given a scenario, install and configure the appropriate wireless standards and technologies. • 2.4.5 - Service set identifier (SSID) 2.4.5.1 - Basic service set • 2.4.7 - Encryption standards 2.4.7.1 - WiFi Protected Access (WPA)/WPA2 Personal [Advanced Encryption Standard (AES)/Temporal Key Integrity Protocol (TKIP)]

		2.4.7.2 - WPA/WPA2 Enterprise (AES/TKIP)
9.3	Wireless Network Design	2.4 Given a scenario, install and configure the appropriate wireless standards and technologies. • 2.4.6 - Antenna types 2.4.6.1 - Omni 2.4.6.2 - Directional 5.4 Given a scenario, troubleshoot common wireless connectivity issues. • 5.4.1 - Specifications and limitations 5.4.1.1 - Throughput 5.4.1.2 - Speed 5.4.1.3 - Distance 5.4.1.4 - Received signal strength indication (RSSI) signal strength 5.4.1.5 - Effective isotropic radiated power (EIRP)/power settings • 5.4.2 - Considerations 5.4.2.1 - Antennas 5.4.2.1.1 - Antennas - Placement 5.4.2.1.2 - Antennas - Type 5.4.2.1.3 - Antennas - Polarization 5.4.2.2 - Channel utilization 5.4.2.3 - AP association time 5.4.2.4 - Site survey
9.4	Wireless Network Implementation	2.4 Given a scenario, install and configure the appropriate wireless standards and technologies. • 2.4.5 - Service set identifier (SSID) 2.4.5.1 - Basic service set 2.4.5.2 - Extended service set

		2.4.5.3 - Independent basic service set (Ad-hoc) 2.4.5.4 - Roaming • 2.4.7 - Encryption standards 2.4.7.1 - WiFi Protected Access (WPA)/WPA2 Personal [Advanced Encryption Standard (AES)/Temporal Key Integrity Protocol (TKIP)] 2.4.7.2 - WPA/WPA2 Enterprise (AES/TKIP)
9.5	Wireless Security	4.2 Compare and contrast common types of attacks. • 4.2.1 - Technology-based 4.2.1.7 - Rogue access point (AP) 4.2.1.8 - Evil twin 4.2.1.13 - Deauthentication 4.3 Given a scenario, apply network hardening techniques. • 4.3.2 - Wireless security 4.3.2.1 - MAC filtering 4.3.2.2 - Antenna placement 4.3.2.3 - Power levels 4.3.2.4 - Wireless client isolation 4.3.2.5 - Guest network isolation 4.3.2.6 - Preshared keys (PSKs) 4.3.2.7 - EAP 4.3.2.8 - Geofencing 4.3.2.9 - Captive portal 5.5 Given a scenario, troubleshoot general networking issues. • 5.5.2 - Common issues

		5.5.2.21 - BYOD challenges
9.6	Wireless Troubleshooting	5.4 Given a scenario, troubleshoot common wireless connectivity issues. • 5.4.1 - Specifications and limitations 5.4.1.1 - Throughput 5.4.1.2 - Speed 5.4.1.3 - Distance 5.4.1.4 - Received signal strength indication (RSSI) signal strength 5.4.1.5 - Effective isotropic radiated power (EIRP)/power settings • 5.4.2 - Considerations 5.4.2.1 - Antennas 5.4.2.1.1 - Antennas - Placement 5.4.2.1.2 - Antennas - Type 5.4.2.1.3 - Antennas - Polarization 5.4.2.2 - Channel utilization 5.4.2.3 - AP association time 5.4.2.4 - Site survey • 5.4.3 - Common issues 5.4.3.1 - Interference 5.4.3.1.1 - Interference - Channel overlap 5.4.3.2 - Antenna cable attenuation/signal loss 5.4.3.3 - RF attenuation/signal loss 5.4.3.4 - Wrong SSID 5.4.3.5 - Incorrect passphrase 5.4.3.6 - Encryption protocol mismatch 5.4.3.7 - Insufficient wireless coverage 5.4.3.8 - Captive portal issues 5.4.3.9 - Client disassociation issues

10.0	Wide Area Networks (WANs)	
10.1	WAN Concepts	1.2 Explain the characteristics of network topologies and network types. • 1.2.6 - Network types and characteristics 1.2.6.11 - Multiprotocol label switching (MPLS) • 1.2.9 - Provider links 1.2.9.1 - Satellite 1.2.9.2 - Digital subscriber line (DSL) 1.2.9.3 - Cable 1.2.9.4 - Leased line 1.2.9.5 - Metro-optical 1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution. • 1.3.5 - Ethernet standards 1.3.5.2.7 - Coarse wavelength division multiplexing (CWDM) 1.3.5.2.8 - Dense wavelength division multiplexing (DWDM) 1.3.5.2.8 - Bidirectional wavelength division multiplexing (WDM)
10.2	Internet Connectivity	1.2 Explain the characteristics of network topologies and network types. • 1.2.9 - Provider links 1.2.9.1 - Satellite 1.2.9.2 - Digital subscriber line (DSL) 1.2.9.3 - Cable 1.2.9.4 - Leased line 1.2.9.5 - Metro-optical

		2.4 Given a scenario, install and configure the appropriate wireless standards and technologies. • 2.4.8 - Cellular technologies 2.4.8.1 - Code-division multiple access (CDMA) 2.4.8.2 - Global System for Mobile Communications (GSM) 2.4.8.3 - Long-Term Evolution (LTE) 2.4.8.4 - 3G, 4G, 5G
10.3	Remote Access	3.2 Explain the purpose of organizational documents and policies. • 3.2.2 - Hardening and security policies 3.2.2.4 - Remote access policy 4.1 Explain common security concepts. • 4.1.9 - Authentication methods 4.1.9.2 - Terminal Access Controller Access-Control System Plus (TACACS+) 4.1.9.4 - Remote Authentication Dial-in User Service (RADIUS
10.4	Virtual Private Networks	4.4 Compare and contrast remote access methods and security implications. • 4.4.1 - Site-to-site VPN • 4.4.2 - Client-to-site VPN 4.4.2.1 - Clientless VPN 4.4.2.2 - Split tunnel vs. full tunnel • 4.4.8 - Authentication and authorization considerations
11.0	**Network Operations and Management**	

11.1	Performance Metrics	3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability. • 3.1.1 - Performance metrics/sensors 3.1.1.1 - Device/chassis 3.1.1.1.1 - Device/chassis - Temperature 3.1.1.1.2 - Device/chassis - Central processing unit (CPU) usage 3.1.1.1.3 - Device/chassis - Memory 3.1.1.2 - Network metrics 3.1.1.2.1 - Network metrics - Bandwidth 3.1.1.2.2 - Network metrics - Latency 3.1.1.2.3 - Network metrics - Jitter • 3.1.7 - Baselines
11.2	Network Management with SNMP	3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability. • 3.1.2 - SNMP 3.1.2.1 - Traps 3.1.2.2 - Object identifiers (OIDs) 3.1.2.3 - Management information bases (MIBs)
11.3	Log File Management	3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability. • 3.1.3 - Network device logs 3.1.3.1 - Log reviews 3.1.3.1.1 - Log reviews - Traffic logs 3.1.3.1.2 - Log reviews - Audit logs 3.1.3.1.3 - Log reviews - Syslog 3.1.3.2 - Logging levels/severity levels
11.4	Monitoring	3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.

		• 3.1.3 - Network device logs 3.1.3.1 - Log reviews 3.1.3.1.1 - Log reviews - Traffic logs 3.1.3.1.2 - Log reviews - Audit logs 3.1.3.1.3 - Log reviews - Syslog • 3.1.4 - Interface statistics/status 3.1.4.1 - Link state (up/down) 3.1.4.2 - Speed/duplex 3.1.4.3 - Send/receive traffic 3.1.4.4 - Cyclic redundancy checks (CRCs) 3.1.4.5 - Protocol packet and byte counts • 3.1.5 - Interface errors or alerts 3.1.5.1 - CRC errors 3.1.5.2 - Giants 3.1.5.3 - Runts 3.1.5.4 - Encapsulation errors • 3.1.6 - Environmental factors and sensors 3.1.6.1 - Temperature 3.1.6.2 - Humidity 3.1.6.3 - Electrical 3.1.6.4 - Flooding • 3.1.7 - Baselines • 3.1.8 - NetFlow data • 3.1.9 - Uptime/downtime 5.3 Given a scenario, use the appropriate network software tools and commands. • 5.3.1 - Software tools

		5.3.1.2 - Protocol analyzer/packet capture 5.3.1.3 - Bandwidth speed tester 5.3.1.4 - Port scanner 5.3.1.5 - iperf 5.3.1.6 - NetFlow analyzers 5.3.1.9 - IP scanner
11.5	Organization Policies	3.2 Explain the purpose of organizational documents and policies. • 3.2.1 - Plans and procedures 3.2.1.1 - Change management 3.2.1.2 - Incident response plan 3.2.1.3 - Disaster recovery plan 3.2.1.4 - Business continuity plan 3.2.1.5 - System life cycle 3.2.1.6 - Standard operating procedures • 3.2.2 - Hardening and security policies 3.2.2.1 - Password policy 3.2.2.2 - Acceptable use policy 3.2.2.3 - Bring your own device (BYOD) policy 3.2.2.4 - Remote access policy 3.2.2.5 - Onboarding and offboarding policy 3.2.2.6 - Security policy 3.2.2.4 - Data loss prevention • 3.2.3 - Common documentation 3.2.3.1 - Physical network diagram 3.2.3.1.1 - Physical network diagram - Floor plan 3.2.3.1.2 - Physical network diagram - Rack diagram 3.2.3.1.3 - Physical network diagram - Intermediate distribution frame (IDF)/main distribution frame (MDF) documentation

		3.2.3.2 - Logical network diagram 3.2.3.3 - Wiring diagram 3.2.3.4 - Site survey report 3.2.3.5 - Audit and assessment report 3.2.3.6 - Baseline configurations • 3.2.4 - Common agreements 3.2.4.1 - Non-disclosure agreement (NDA) 3.2.4.2 - Service-level agreement (SLA)
11.6	Redundancy and High Availability	3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution. • 3.3.1 - Load balancing • 3.3.2 - Multipathing • 3.3.3 - Network interface card (NIC) teaming • 3.3.4 - Redundant hardware/clusters 3.3.4.1 - Switches 3.3.4.2 - Routers 3.3.4.3 - Firewalls • 3.3.5 - Facilities and infrastructure support 3.3.5.1 - Uninterruptible power supply (UPS) 3.3.5.2 - Power distribution units (PDUs) 3.3.5.3 - Generatos 3.3.5.4 - HVAC 3.3.5.5 - Fire suppression • 3.3.6 - Redundancy and high availability (HA) concepts 3.3.6.1 - Cold site 3.3.6.2 - Warm site 3.3.6.3 - Hot site

		3.3.6.4 - Cloud site 3.3.6.5 - Active-active vs. active-passive 3.3.6.5.1 - Active-active vs. active-passive - Multiple Internet service providers (ISPs)/diverse paths 3.3.6.5.2 - Active-active vs. active-passive - Virtual Router Redundancy Protocol (VRRP)/First Hop Redundancy Protocol (FHRP) 3.3.6.6 - Mean time to repair (MTTR) 3.3.6.7 - Mean time between failure (MTBF) 3.3.6.8 - Recovery time objective (RTO) 3.3.6.9 - Recovery point objective (RPO) • 3.3.7 - Network device backup/restore 3.3.7.1 - State 3.3.7.2 - Configuration
11.7	Data Backup and Storage	3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution. • 3.3.7 - Network device backup/restore 3.3.7.1 - State 3.3.7.2 - Configuration
11.8	Remote Management	4.4 Compare and contrast remote access methods and security implications. • 4.4.3 - Remote desktop connection • 4.4.4 - Remote desktop gateway • 4.4.5 - SSH • 4.4.6 - Virtual network computing (VNC)
12.0	**Network Security**	
12.1	Security Concepts	4.1 Explain common security concepts. • 4.1.1 - Confidentiality, integrity, availability (CIA)

		• 4.1.2 - Threats 4.1.2.1 - Internal 4.1.2.2 - External • 4.1.3 - Vulnerabilities 4.1.3.1 - Common vulnerabilities and exposures (CVE) 4.1.3.2 - Zero-day • 4.1.4 - Exploits • 4.1.5 - Least privilege • 4.1.6 - Role-based access • 4.1.7 - Zero Trust • 4.1.8 - Defense in depth 4.1.8.1 - Network segmentation enforcement 4.1.8.2 - Screened subnet [previously known as demilitarized zone (DMZ)] 4.1.8.3 - Separation of duties 4.1.8.4 - Network access control 4.1.8.5 - Honeypot • 4.1.9 - Authentication methods 4.1.9.1 - Multifactor 4.1.9.2 - Terminal Access Controller Access-Control System Plus (TACACS+) 4.1.9.3 - Single sign-on (SSO) 4.1.9.4 - Remote Authentication Dial-in User Service (RADIUS 4.1.9.5 - LDAP 4.1.9.6 - Kerberos 4.1.9.7 - Local authentication 4.1.9.8 - 802.1X 4.1.9.9 - Extensible Authentication Protocol (EAP)
12.2	Risk Management	4.1 Explain common security concepts.

		• 4.1.10 - Risk Management 4.1.10.1 - Security risk assessments 4.1.10.1.1 - Security risk assessments - Threat assessment 4.1.10.1.2 - Security risk assessments - Vulnerability assessment 4.1.10.1.3 - Security risk assessments - Penetration testing 4.1.10.1.4 - Security risk assessments - Posture assessment 4.1.10.2 - Business risk assessments 4.1.10.2.1 - Business risk assessments - Process assessment 4.1.10.2.2 - Business risk assessments - Vendor assessment • 4.1.11 - Security information and event management (SIEM) 4.5 Explain the importance of physical security. • 4.5.3 - Asset disposal 4.5.3.1 - Factory reset/wipe configuration 4.5.3.2 - Sanitize devices for disposal
12.3	Physical Security	4.5 Explain the importance of physical security. • 4.5.1 - Detection methods 4.5.1.1 - Camera 4.5.1.2 - Motion detection 4.5.1.3 - Asset tags 4.5.1.4 - Tamper detection • 4.5.2 - Prevention methods 4.5.2.1 - Employee training 4.5.2.2 - Access control hardware 4.5.2.2.1 - Access control hardware - Badge readers 4.5.2.2.2 - Access control hardware - Biometrics 4.5.2.3 - Locking racks

		4.5.2.4 - Locking cabinets 4.5.2.5 - Access control vestibule (previously known as a mantrap) 4.5.2.6 - Smart lockers
12.4	Social Engineering	4.2 Compare and contrast common types of attacks. • 4.2.2 - Human and environmental 4.2.2.1 - Social engineering 4.2.2.1.1 - Social engineering - Phishing 4.2.2.1.2 - Social engineering - Tailgating 4.2.2.1.3 - Social engineering - Piggybacking 4.2.2.1.4 - Social engineering - Shoulder surfing
12.5	Network Threats and Attacks	4.2 Compare and contrast common types of attacks. • 4.2.1 - Technology-based 4.2.1.1 - Denial-of-service (DoS)/distributed denial-of-service (DDoS) 4.2.1.1.1 - Denial-of-service (DoS)/distributed denial-of-service (DDoS) - Botnet/command and control 4.2.1.3 - DNS poisoning 4.2.1.9 - Ransomware 4.2.1.10 - Password attacks 4.2.1.10.1 - Password attacks - Brute-force 4.2.1.10.2 - Password attacks - Dictionary 4.2.1.14 - Malware
12.6	Spoofing Attacks	2.1 Compare and contrast various devices, their features, and their appropriate placement on the network. • 2.1.1 - Networking devices 2.1.1.15 - Intrusion prevention system (IPS)/intrusion detection system (IDS) device

		2.1.1.16 - Firewall 4.2 Compare and contrast common types of attacks. • 4.2.1 - Technology-based 4.2.1.2 - On-path attack (previously known as man-in-the-middle attack) 4.2.1.3 - DNS poisoning 4.2.1.5 - ARP spoofing 4.2.1.6 - Rogue DHCP 4.2.1.11 - MAC spoofing 4.2.1.12 - IP spoofing 4.3 Given a scenario, apply network hardening techniques. • 4.3.1 - Best practices 4.3.1.11 - Enable DHCP snooping
13.0	**Hardening and Update Management**	
13.1	Network Hardening	4.3 Given a scenario, apply network hardening techniques. • 4.3.1 - Best practices 4.3.1.1 - Secure SNMP 4.3.1.2 - Router Advertisement (RA) Guard 4.3.1.3 - Port security 4.3.1.4 - Dynamic ARP inspection 4.3.1.5 - Control plane policing 4.3.1.6 - Private VLANs 4.3.1.7 - Disable unneeded switchports 4.3.1.8 - Disable unneeded network services 4.3.1.9 - Change default passwords 4.3.1.10 - Password complexity/length

		4.3.1.11 - Enable DHCP snooping 4.3.1.12 - Change default VLAN 4.3.1.13 - Patch and firmware management 4.3.1.14 - Access control list 4.3.1.15 - Role-based access 4.3.1.16 - Firewall rules 4.3.1.16.1 - Firewall rules - Explicit deny 4.3.1.16.2 - Firewall rules - Implicit deny
13.2	Authentication	3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability. • 3.1.3 - Network device logs 3.1.3.1 - Log reviews 3.1.3.1.2 - Log reviews - Audit logs 4.1 Explain common security concepts. • 4.1.9 - Authentication methods 4.1.9.1 - Multifactor 4.1.9.3 - Single sign-on (SSO) 4.1.9.4 - Remote Authentication Dial-in User Service (RADIUS 4.1.9.6 - Kerberos 4.1.9.7 - Local authentication 4.1.9.8 - 802.1X 4.1.9.9 - Extensible Authentication Protocol (EAP) 4.4 Compare and contrast remote access methods and security implications. • 4.4.8 - Authentication and authorization considerations 4.5 Explain the importance of physical security. • 4.5.2 - Prevention methods

		4.5.2.2.2 - Access control hardware - Biometrics 5.5 Given a scenario, troubleshoot general networking issues. • 5.5.2 - Common issues 5.5.2.14 - Certificate issues
13.3	Hardening Authentication	3.2 Explain the purpose of organizational documents and policies. • 3.2.2 - Hardening and security policies 3.2.2.1 - Password policy 4.1 Explain common security concepts. • 4.1.9 - Authentication methods 4.1.9.1 - Multifactor 4.1.9.3 - Single sign-on (SSO) 4.3 Given a scenario, apply network hardening techniques. • 4.3.1 - Best practices 4.3.1.9 - Change default passwords
13.4	Update Management	3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution. • 3.3.7 - Network device backup/restore 3.3.7.1 - State

		3.3.7.2 - Configuration 4.3 Given a scenario, apply network hardening techniques. • 4.3.1 - Best practices 4.3.1.13 - Patch and firmware management
14.0	**Network Optimization and Troubleshooting**	
14.1	Optimization	2.1 Compare and contrast various devices, their features, and their appropriate placement on the network. • 2.1.1 - Networking devices 2.1.1.1 - Layer 2 switch 2.1.1.2 - Layer 3 capable switch 2.1.1.3 - Router 2.1.1.4 - Hub 2.3 Given a scenario, configure and deploy common Ethernet switching features. • 2.3.7 - Carrier-sense multiple access with collision detection (CSMA/CD) 4.2 Compare and contrast common types of attacks. • 4.2.1 - Technology-based 4.2.1.2 - On-path attack (previously known as man-in-the-middle attack) 5.5 Given a scenario, troubleshoot general networking issues. • 5.5.2 - Common issues

		5.5.2.23 - Network performance issues
14.2	General Network Issues	5.1 Explain the network troubleshooting methodology. • 5.1.1 - Identify the problem 5.1.1.1 - Gather information 5.1.1.2 - Question users 5.1.1.3 - Identify symptoms 5.1.1.4 - Determine if anything has changed 5.1.1.5 - Duplicate the problem, if possible 5.1.1.6 - Approach multiple problems individually • 5.1.2 - Establish a theory of probable cause 5.1.2.1 - Question the obvious 5.1.2.2 - Consider multiple approaches 5.1.2.2.1 - Consider multiple approaches - Top-to-bottom/bottom-to-top OSI model 5.1.2.2.2 - Consider multiple approaches -Divide and conquer • 5.1.3 - Test the theory to determine the cause 5.1.3.1 - If the theory is confirmed, determine the next steps to resolve the problem 5.1.3.2 - If the theory is not confirmed, reestablish a new theory or escalate • 5.1.4 - Establish a plan of action to resolve the problem and identify potential effects • 5.1.5 - Implement the solution or escalate as necessary • 5.1.6 - Verify full system functionality and, if applicable, implement preventive measure • 5.1.7 - Document findings, actions, outcomes, and lessons learned 5.5 Given a scenario, troubleshoot general networking issues. • 5.5.2 - Common issues

		5.5.2.7 - Switching loops 5.5.2.8 - Routing loops 5.5.2.9 - Rogue DHCP server 5.5.2.10 - DHCP scope exhaustion 5.5.2.13 - Low optical link budget 5.5.2.14 - Certificate issues 5.5.2.15 - Hardware failure 5.5.2.16 - Host-based/network-based firewall settings 5.5.2.17 - Blocked services, ports, or addresses 5.5.2.18 - Incorrect VLAN 5.5.2.19 - DNS issues 5.5.2.20 - NTP issues 5.5.2.21 - BYOD challenges 5.5.2.22 - Licensed feature issues 5.5.2.23 - Network performance issues
14.3	Troubleshooting Utilities	5.3 Given a scenario, use the appropriate network software tools and commands. • 5.3.1 - Software tools 5.3.1.1 - WiFi analyzer 5.3.1.2 - Protocol analyzer/packet capture 5.3.1.3 - Bandwidth speed tester 5.3.1.4 - Port scanner 5.3.1.5 - iperf 5.3.1.6 - NetFlow analyzers 5.3.1.7 - Trivial File Transfer Protocol (TFTP) server 5.3.1.8 - Terminal emulator 5.3.1.9 - IP scanner • 5.3.2 - Command line tool 5.3.2.1 - ping 5.3.2.2 - ipconfig/ifconfig/ip 5.3.2.3 - nslookup/dig 5.3.2.4 - traceroute/tracert

		5.3.2.5 - arp 5.3.2.6 - netstat 5.3.2.7 - hostname 5.3.2.8 - route 5.3.2.9 - telnet 5.3.2.10 - tcpdump 5.3.2.11 - nmap
A.0	**TestOut Network Pro - Practice Exams**	
A.1	Prepare for TestOut Network Pro Certification	
A.2	TestOut Network Pro Domain Review	
B.0	**CompTIA Network+ N10-008 Practice Exams**	
B.1	Prepare for Certification	
B.2	CompTIA Network+ N10-008 Practice Exams (20 Questions)	
B.3	CompTIA Network+ N10-008 Practice Exams (All Questions)	

Objective Mapping: CompTIA N10-008 Objectives to TestOut Section

#	Domain	TestOut Section
1.0	**Networking Fundamentals**	
1.1	Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts. 1.1.1 - OSI model ○ 1.1.1.1 - Layer 1 – Physical ○ 1.1.1.2 - Layer 2 – Data link ○ 1.1.1.3 - Layer 3 – Network ○ 1.1.1.4 - Layer 4 – Transport ○ 1.1.1.5 - Layer 5 – Session ○ 1.1.1.6 - Layer 6 – Presentation ○ 1.1.1.7 - Layer 7 – Application 1.1.2 - Data encapsulation and decapsulation within the OSI model context ○ 1.1.2.1 - Ethernet header ○ 1.1.2.2 - Internet Protocol (IP) header ○ 1.1.2.3 - Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) headers ○ 1.1.2.4 - TCP flags ○ 1.1.2.5 - Payload ○ 1.1.2.6 - Maximum transmission unit (MTU)	2.1, 2.2, 2.3
1.2	Explain the characteristics of network topologies and network types. 1.2.1 - Mesh 1.2.2 - Star/hub-and-spoke 1.2.3 - Bus 1.2.4 - Ring 1.2.5 - Hybrid 1.2.6 - Network types and characteristics ○ 1.2.6.1 - Peer-to-peer ○ 1.2.6.2 - Client-server	2.1 3.3, 3.4 5.1, 5.3 8.3, 8.4 10.1, 10.2

	○ 1.2.6.3 - Local area network (LAN) ○ 1.2.6.4 - Metropolitan area network (MAN) ○ 1.2.6.5 - Wide area network (WAN) ○ 1.2.6.6 - Wireless local area network (WLAN) ○ 1.2.6.7 - Personal area network (PAN) ○ 1.2.6.8 - Campus area network (CAN) ○ 1.2.6.9 - Storage area network (SAN) ○ 1.2.6.10 - Software-defined wide area network (SDWAN) ○ 1.2.6.11 - Multiprotocol label switching (MPLS) ○ 1.2.6.12 - Multipoint generic routing encapsulation (mGRE) 1.2.7 - Service-related entry point ○ 1.2.7.1 - Demarcation point ○ 1.2.7.2 - Smartjack 1.2.8 - Virtual network concepts ○ 1.2.8.1 - vSwitch ○ 1.2.8.2 - Virtual network interface card (vNIC) ○ 1.2.8.3 - Network function virtualization (NFV) ○ 1.2.8.4 - Hypervisor 1.2.9 - Provider links ○ 1.2.9.1 - Satellite ○ 1.2.9.2 - Digital subscriber line (DSL) ○ 1.2.9.3 - Cable ○ 1.2.9.4 - Leased line ○ 1.2.9.5 - Metro-optical	
1.3	Summarize the types of cables and connectors and explain which is the appropriate type for a solution. 1.3.1 - Copper ○ 1.3.1.1 - Twisted pair ○ 1.3.1.1.1 - Twisted pair - Cat 5 ○ 1.3.1.1.2 - Twisted pair - Cat 5e ○ 1.3.1.1.3 - Twisted pair - Cat 6 ○ 1.3.1.1.4 - Twisted pair - Cat 6a ○ 1.3.1.1.5 - Twisted pair - Cat 7 ○ 1.3.1.1.6 - Twisted pair - Cat 8 ○ 1.3.1.2 - Coaxial/RG-6 ○ 1.3.1.3 - Twinaxial ○ 1.3.1.4 - Termination standards	2.1 3.1, 3.2, 3.3, 3.4, 3.5 5.1 10.1

	○ 1.3.1.4.1 - Termination standards - TIA/EIA-568A ○ 1.3.1.4.2 - Termination standards - TIA/EIA-568B 1.3.2 - Fiber ○ 1.3.2.1 - Single-mode ○ 1.3.2.2 - Multimode 1.3.3 - Connector types ○ 1.3.3.1 - Local connector (LC), straight tip (ST), subscriber connector (SC), mechanical transfer (MT), registered jack (RJ) ○ 1.3.3.1.1 - Local connector (LC), straight tip (ST), subscriber connector (SC), mechanical transfer (MT), registered jack (RJ) - Angled physical contact (APC) ○ 1.3.3.1.2 - Local connector (LC), straight tip (ST), subscriber connector (SC), mechanical transfer (MT), registered jack (RJ) - Ultra-physical contact (UPC) ○ 1.3.3.2 - RJ11 ○ 1.3.3.3 - RJ45 ○ 1.3.3.4 - F-type connector ○ 1.3.3.5 - Transceivers/media converters ○ 1.3.3.6 - Transceiver type ○ 1.3.3.6.1 - Transceiver type - Small form-factor pluggable (SFP) ○ 1.3.3.6.2 - Transceiver type - Enhanced form-factor pluggable (SFP+) ○ 1.3.3.6.3 - Transceiver type - Quad small form-factor pluggable (QSFP) ○ 1.3.3.6.4 - Transceiver type - Enhanced quad small form-factor pluggable (QSFP+) 1.3.4 - Cable management ○ 1.3.4.1 - Patch panel/patch bay ○ 1.3.4.2 - Fiber distribution panel ○ 1.3.4.2 - Punchdown block ○ 1.3.4.2.1 - Punchdown block - 66 ○ 1.3.4.2.2 - Punchdown block - 110 ○ 1.3.4.2.3 - Punchdown block - Krone ○ 1.3.4.2.4 - Punchdown block - Bix 1.3.5 - Ethernet standards ○ 1.3.5.1 - Copper ○ 1.3.5.1.1 - Copper - 10BASE-T ○ 1.3.5.1.2 - Copper - 100BASE-TX ○ 1.3.5.1.3 - Copper - 1000BASE-T ○ 1.3.5.1.4 - Copper - 10GBASE-T ○ 1.3.5.1.5 - Copper - 40GBASE-T ○ 1.3.5.2 - Fiber ○ 1.3.5.2.1 - 100BASE-FX ○ 1.3.5.2.2 - 100BASE-SX	

	○ 1.3.5.2.3 - 1000BASE-SX ○ 1.3.5.2.4 - 1000BASE-LX ○ 1.3.5.2.5 - 10GBASE-SR ○ 1.3.5.2.6 - 10GBASE-LR ○ 1.3.5.2.7 - Coarse wavelength division multiplexing (CWDM) ○ 1.3.5.2.8 - Dense wavelength division multiplexing (DWDM) ○ 1.3.5.2.8 - Bidirectional wavelength division multiplexing (WDM)	
1.4	Given a scenario, configure a subnet and use appropriate IP addressing schemes. 1.4.1 - Public vs. private ○ 1.4.1.1 - RFC1918 ○ 1.4.1.2 - Network address translation (NAT) ○ 1.4.1.3 - Port address translation (PAT) 1.4.2 - IPv4 vs. IPv6 ○ 1.4.2.1 - Automatic Private IP Addressing (APIPA) ○ 1.4.2.2 - Extended unique identifier (EUI-64) ○ 1.4.2.3 - Multicast ○ 1.4.2.4 - Unicast ○ 1.4.2.5 - Anycast ○ 1.4.2.6 - Broadcast ○ 1.4.2.7 - Link local ○ 1.4.2.8 - Loopback ○ 1.4.2.9 - Default gateway 1.4.3 - IPv4 subnetting ○ 1.4.3.1 - Classless (variable-length subnet mask) ○ 1.4.3.2 - Classful ○ 1.4.3.2.1 - Classful - A ○ 1.4.3.2.2 - Classful - B ○ 1.4.3.2.3 - Classful - C ○ 1.4.3.2.4 - Classful - D ○ 1.4.3.2.5 - Classful - E ○ 1.4.3.3 - Classless Inter-Domain Routing (CIDR) notation 1.4.4 - IPv6 concepts ○ 1.4.4.1 - Tunneling ○ 1.4.4.2 - Dual stack ○ 1.4.4.3 - Shorthand notation ○ 1.4.4.4 - Router advertisement	2.1 4.1, 4.2, 4.7, 4.8 7.5, 7.6

	○ 1.4.4.5 - Stateless address autoconfiguration (SLAAC) 1.4.5 - Virtual IP (VIP) 1.4.6 - Subinterfaces	
1.5	Explain common ports and protocols, their application, and encrypted alternatives. 1.5.1 - File Transfer Protocol (FTP) Ports 20/21 1.5.2 - Secure Shell (SSH) Port 22 1.5.3 - Secure File Transfer Protocol (SFTP) Port 22 1.5.4 - Telnet Port 23 1.5.5 - Simple Mail Transfer Protocol (SMTP) Port 25 1.5.6 - Domain Name System (DNS) Port 53 1.5.7 - Dynamic Host Configuration Protocol (DHCP) Ports 67/68 1.5.8 - Trivial File Transfer Protocol (TFTP) Port 69 1.5.9 - Hypertext Transfer Protocol (HTTP) Port 80 1.5.10 - Post Office Protocol v3 (POP3) Port 110 1.5.11 - Network Time Protocol (NTP) Port 123 1.5.12 - Internet Message Access Protocol (IMAP) Port 143 1.5.13 - Simple Network Management Protocol (SNMP) Ports 161/162 1.5.14 - Lightweight Directory Access Protocol (LDAP) Port 389 1.5.15 - Hypertext Transfer Protocol Secure (HTTPS) [Secure Sockets Layer (SSL)] Port 443 1.5.16 - HTTPS [Transport Layer Security (TLS)] Port 443 1.5.17 - Server Message Block (SMB) Port 445 1.5.18 - Syslog Port 514 1.5.19 - SMTP TLS Port 587 1.5.20 - Lightweight Directory Access Protocol (over SSL) (LDAPS) Port 636 1.5.21 - IMAP over SSL Port993 1.5.22 - POP3 over SSL Port 995 1.5.23 - Structured Query Language (SQL) Server Port 1433 1.5.24 - SQLnet Port 1521 1.5.25 - MySQL Port 3306 1.5.26 - Remote Desktop Protocol (RDP) Port 3389 1.5.27 - Session Initiation Protocol (SIP) Ports 5060/5061 1.5.28 - IP protocol types ○ 1.5.28.1 - Internet Control Message Protocol (ICMP) ○ 1.5.28.2 - TCP ○ 1.5.28.3 - UDP ○ 1.5.28.4 - Generic Routing Encapsulation (GRE)	2.4

	○ 1.5.28.5 - Internet Protocol Security (IPSec) ○ 1.5.28.5.1 - Internet Protocol Security (IPSec) - Authentication Header (AH)/Encapsulating Security Payload (ESP) 1.5.29 - Connectionless vs. connection-oriented	
1.6	Explain the use and purpose of network services. 1.6.1 - DHCP ○ 1.6.1.1 - Scope ○ 1.6.1.2 - Exclusion ranges ○ 1.6.1.3 - Reservation ○ 1.6.1.4 - Dynamic assignment ○ 1.6.1.5 - Static assignment ○ 1.6.1.6 - Lease time ○ 1.6.1.7 - Scope options ○ 1.6.1.8 - Available leases ○ 1.6.1.9 - DHCP relay ○ 1.6.1.10 - IP helper/UDP forwarding 1.6.2 - DNS ○ 1.6.2.1 - Record types ○ 1.6.2.1.1 - Record types - Address (A) ○ 1.6.2.1.2 - Record types - Canonical name (CNAME) ○ 1.6.2.1.3 - Record types - Mail exchange (MX) ○ 1.6.2.1.4 - Record types - Authentication, authorization, accounting, auditing (AAAA ○ 1.6.2.1.5 - Record types - Start of authority (SOA) ○ 1.6.2.1.6 - Record types - Pointer (PTR) ○ 1.6.2.1.7 - Record types - Text (TXT) ○ 1.6.2.1.8 - Record types - Service (SRV) ○ 1.6.2.1.9 - Record types - Name server (NS) ○ 1.6.2.2 - Global hierarchy ○ 1.6.2.2.1 - Global hierarchy - Root DNS servers ○ 1.6.2.2.2 - Global hierarchy - Internal vs. external ○ 1.6.2.2.3 - Global hierarchy - Zone transfers ○ 1.6.2.2.4 - Global hierarchy - Authoritative name servers ○ 1.6.2.2.5 - Global hierarchy - Time to live (TTL) ○ 1.6.2.2.6 - Global hierarchy - DNS caching ○ 1.6.2.2.7 - Global hierarchy - Reverse DNS/reverse lookup/forward lookup	4.3, 4.4, 4.5, 4.6

	○ 1.6.2.2.8 - Global hierarchy - Recursive lookup/iterative lookup 1.6.3 - NTP ○ 1.6.3.1 - Stratum ○ 1.6.3.2 - Clients ○ 1.6.3.4 - Servers	
1.7	Explain basic corporate and datacenter network architecture. 1.7.1 - Three-tiered ○ 1.7.1.1 - Core ○ 1.7.1.2 - Distribution/aggregation layer ○ 1.7.1.3 - Access/edge 1.7.2 - Software-defined networking ○ 1.7.2.1 - Application layer ○ 1.7.2.2 - Control layer ○ 1.7.2.3 - Infrastructure layer ○ 1.7.2.4 - Management plane 1.7.3 - Spine and leaf ○ 1.7.3.1 - Software-defined network ○ 1.7.3.2 - Top-of-rack switching ○ 1.7.3.3 - Backbone 1.7.4 - Branch office vs. on-premises datacenter vs. colocation 1.7.5 - Storage area networks ○ 1.7.5.1 - Connection types ○ 1.7.5.1.1 - Connection types - Fibre Channel over Ethernet (FCoE) ○ 1.7.5.1.2 - Connection types - Fibre Channel ○ 1.7.5.1.3 - Connection types - Internet Small Computer Systems Interface (iSCSI)	8.1
1.8	Summarize cloud concepts and connectivity options. 1.8.1 - Deployment models ○ 1.8.1.1 - Public ○ 18.1.2 - Private ○ 1.8.1.3 - Hybrid ○ 1.8.1.4 - Community 1.8.2 - Service models ○ 1.8.2.1 - Software as a service (SaaS)	8.5

	○ 1.8.2.2 - Infrastructure as a service (IaaS) ○ 1.8.2.3 - Platform as a service (PaaS) ○ 1.8.2.4 - Desktop as a service (DaaS) 1.8.3 - Infrastructure as code ○ 1.8.3.1 - Automation/orchestration 1.8.4 - Connectivity options ○ 1.8.4.1 - Virtual private network (VPN) ○ 1.8.4.2 - Private-direct connection to cloud provider 1.8.5 - Multitenancy 1.8.6 - Elasticity 1.8.7 - Scalability 1.8.8 - Security implications	
2.0	**Network Implementations**	
2.1	Compare and contrast various devices, their features, and their appropriate placement on the network. 2.1.1 - Networking devices ○ 2.1.1.1 - Layer 2 switch ○ 2.1.1.2 - Layer 3 capable switch ○ 2.1.1.3 - Router ○ 2.1.1.4 - Hub ○ 2.1.1.5 - Access point ○ 2.1.1.6 - Bridge ○ 2.1.1.7 - Wireless LAN controller ○ 2.1.1.8 - Load balancer ○ 2.1.1.9 - Proxy server ○ 2.1.1.10 - Cable modem ○ 2.1.1.11 - DSL modem ○ 2.1.1.12 - Repeater ○ 2.1.1.13 - Voice gateway ○ 2.1.1.14 - Media Converter ○ 2.1.1.15 - Intrusion prevention system (IPS)/intrusion detection system (IDS) device ○ 2.1.1.16 - Firewall ○ 2.1.1.17 - VPN headend 2.1.2 - Networked devices ○ 2.1.2.1 - Voice over Internet Protocol (VoIP) phone	2.1 3.5, 3.6 6.2, 6.4 7.1, 7.2, 7.3, 7.4 8.2, 8.6 12.6 14.1

	○ 2.1.2.2 - Printer ○ 2.1.2.3 - Physical access control devices ○ 2.1.2.4 - Cameras ○ 2.1.2.5 - Heating, ventilation, and air conditioning (HVAC) sensors ○ 2.1.2.6 - Internet of Things (IoT) ○ 2.1.2.6.1 - Internet of Things (IoT) - Refrigerator ○ 2.1.2.6.2 - Internet of Things (IoT) - Smart speakers ○ 2.1.2.6.3 - Internet of Things (IoT) - Smart thermostats ○ 2.1.2.6.4 - Internet of Things (IoT) - Smart doorbells ○ 2.1.2.7 - Industrial control systems/supervisory control and data acquisition (SCADA)	
2.2	Compare and contrast routing technologies and bandwidth management concepts. 2.2.1 - Routing ○ 2.2.1.1 - Dynamic routing ○ 2.2.1.1.1 - Dynamic routing - Protocols [Routing Internet Protocol (RIP), Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol ○ 2.2.1.1.2 - Dynamic routing - Link state vs. distance vector vs. hybrid ○ 2.2.1.2 - Static routing ○ 2.2.1.3 - Default route ○ 2.2.1.4 - Administrative distance ○ 2.2.1.5 - Exterior vs. interior ○ 2.2.1.6 - Time to live 2.2.2 - Bandwidth management ○ 2.2.2.1 - Traffic shaping ○ 2.2.2.2 - Quality of service (QoS)	7.5 8.2
2.3	Given a scenario, configure and deploy common Ethernet switching features. 2.3.1 - Data virtual local area network (VLAN) 2.3.2 - Voice VLAN 2.3.3 - Port configurations ○ 2.3.3.1 - Port tagging/802.1Q ○ 2.3.3.2 - Port aggregation ○ 2.3.3.2.1 -Port aggregation - Link Aggregation Control Protocl (LACP) ○ 2.3.3.3 - Duplex	2.3 3.5 5.1 7.2, 7.3, 7.4, 7.5 14.1

	○ 2.3.3.4 - Speed ○ 2.3.3.5 - Flow control ○ 2.3.3.6 - Port mirroring ○ 2.3.3.7 - Port security ○ 2.3.3.8 - Jumbo frames ○ 2.3.3.9 - Auto-medium-dependent interface crossover (MDI-X) 2.3.4 - Media access control (MAC) address tables 2.3.5 - Power over Ethernet (PoE)/Power over Ethernet plus (PoE+) 2.3.6 - Spanning Tree Protocol 2.3.7 - Carrier-sense multiple access with collision detection (CSMA/CD) 2.3.8 - Address Resolution Protocol (ARP) 2.3.9 - Neighbor Discovery Protocol	
2.4	Given a scenario, install and configure the appropriate wireless standards and technologies. 2.4.1 - 802.11 standards ○ 2.4.1.1 - a ○ 2.4.1.2 - b ○ 2.4.1.3 - g ○ 2.4.1.4 - n (WiFi 4) ○ 2.4.1.5 - ac (WiFi 5) ○ 2.4.1.6 - ax (WiFi 6) 2.4.2 - Frequencies and range ○ 2.4.2.1 - 2.4GHz ○ 2.4.2.2 - 5GHz 2.4.3 - Channels ○ 2.4.3.1 - Regulatory impacts 2.4.4 - Channel bonding 2.4.5 - Service set identifier (SSID) ○ 2.4.5.1 - Basic service set ○ 2.4.5.2 - Extended service set ○ 2.4.5.3 - Independent basic service set (Ad-hoc) ○ 2.4.5.4 - Roaming 2.4.6 - Antenna types ○ 2.4.6.1 - Omni ○ 2.4.6.2 - Directional 2.4.7 - Encryption standards	9.1, 9.2, 9.3, 9.4 10.2

	○ 2.4.7.1 - WiFi Protected Access (WPA)/WPA2 Personal [Advanced Encryption Standard (AES)/Temporal Key Integrity Protocol (TKIP)] ○ 2.4.7.2 - WPA/WPA2 Enterprise (AES/TKIP) 2.4.8 - Cellular technologies ○ 2.4.8.1 - Code-division multiple access (CDMA) ○ 2.4.8.2 - Global System for Mobile Communications (GSM) ○ 2.4.8.3 - Long-Term Evolution (LTE) ○ 2.4.8.4 - 3G, 4G, 5G 2.4.9 - Multiple input, multiple output (MIMO) and multi-user MIMO (MU-MIMO)	
3.0	**Network Operations**	
3.1	Given a scenario, use the appropriate statistics and sensors to ensure network availability. 3.1.1 - Performance metrics/sensors ○ 3.1.1.1 - Device/chassis ○ 3.1.1.1.1 - Device/chassis - Temperature ○ 3.1.1.1.2 - Device/chassis - Central processing unit (CPU) usage ○ 3.1.1.1.3 - Device/chassis - Memory ○ 3.1.1.2 - Network metrics ○ 3.1.1.2.1 - Network metrics - Bandwidth ○ 3.1.1.2.2 - Network metrics - Latency ○ 3.1.1.2.3 - Network metrics - Jitter 3.1.2 - SNMP ○ 3.1.2.1 - Traps ○ 3.1.2.2 - Object identifiers (OIDs) ○ 3.1.2.3 - Management information bases (MIBs) 3.1.3 - Network device logs ○ 3.1.3.1 - Log reviews ○ 3.1.3.1.1 - Log reviews - Traffic logs ○ 3.1.3.1.2 - Log reviews - Audit logs ○ 3.1.3.1.3 - Log reviews - Syslog ○ 3.1.3.2 - Logging levels/severity levels 3.1.4 - Interface statistics/status ○ 3.1.4.1 - Link state (up/down) ○ 3.1.4.2 - Speed/duplex ○ 3.1.4.3 - Send/receive traffic ○ 3.1.4.4 - Cyclic redundancy checks (CRCs)	11.1, 11.2, 11.3, 11.4 13.2

	○ 3.1.4.5 - Protocol packet and byte counts 3.1.5 - Interface errors or alerts ○ 3.1.5.1 - CRC errors ○ 3.1.5.2 - Giants ○ 3.1.5.3 - Runts ○ 3.1.5.4 - Encapsulation errors 3.1.6 - Environmental factors and sensors ○ 3.1.6.1 - Temperature ○ 3.1.6.2 - Humidity ○ 3.1.6.3 - Electrical ○ 3.1.6.4 - Flooding 3.1.7 - Baselines 3.1.8 - NetFlow data 3.1.9 - Uptime/downtime	
3.2	Explain the purpose of organizational documents and policies. 3.2.1 - Plans and procedures ○ 3.2.1.1 - Change management ○ 3.2.1.2 - Incident response plan ○ 3.2.1.3 - Disaster recovery plan ○ 3.2.1.4 - Business continuity plan ○ 3.2.1.5 - System life cycle ○ 3.2.1.6 - Standard operating procedures 3.2.2 - Hardening and security policies ○ 3.2.2.1 - Password policy ○ 3.2.2.2 - Acceptable use policy ○ 3.2.2.3 - Bring your own device (BYOD) policy ○ 3.2.2.4 - Remote access policy ○ 3.2.2.5 - Onboarding and offboarding policy ○ 3.2.2.6 - Security policy ○ 3.2.2.4 - Data loss prevention 3.2.3 - Common documentation ○ 3.2.3.1 - Physical network diagram ○ 3.2.3.1.1 - Physical network diagram - Floor plan ○ 3.2.3.1.2 - Physical network diagram - Rack diagram ○ 3.2.3.1.3 - Physical network diagram - Intermediate distribution frame (IDF)/main distribution frame (MDF) documentation	3.6 10.3 11.5 13.3

	○ 3.2.3.2 - Logical network diagram ○ 3.2.3.3 - Wiring diagram ○ 3.2.3.4 - Site survey report ○ 3.2.3.5 - Audit and assessment report ○ 3.2.3.6 - Baseline configurations 3.2.4 - Common agreements ○ 3.2.4.1 - Non-disclosure agreement (NDA) ○ 3.2.4.2 - Service-level agreement (SLA) ○ 3.2.4.3 - Memorandum of understanding (MOU)	
3.3	Explain high availability and disaster recovery concepts and summarize which is the best solution. 3.3.1 - Load balancing 3.3.2 - Multipathing 3.3.3 - Network interface card (NIC) teaming 3.3.4 - Redundant hardware/clusters ○ 3.3.4.1 - Switches ○ 3.3.4.2 - Routers ○ 3.3.4.3 - Firewalls 3.3.5 - Facilities and infrastructure support ○ 3.3.5.1 - Uninterruptible power supply (UPS) ○ 3.3.5.2 - Power distribution units (PDUs) ○ 3.3.5.3 - Generatos ○ 3.3.5.4 - HVAC ○ 3.3.5.5 - Fire suppression 3.3.6 - Redundancy and high availability (HA) concepts ○ 3.3.6.1 - Cold site ○ 3.3.6.2 - Warm site ○ 3.3.6.3 - Hot site ○ 3.3.6.4 - Cloud site ○ 3.3.6.5 - Active-active vs. active-passive ○ 3.3.6.5.1 - Active-active vs. active-passive - Multiple Internet service providers (ISPs)/diverse paths ○ 3.3.6.5.2 - Active-active vs. active-passive - Virtual Router Redundancy Protocol (VRRP)/First Hop Redundancy Protocol (FHRP) ○ 3.3.6.6 - Mean time to repair (MTTR) ○ 3.3.6.7 - Mean time between failure (MTBF) ○ 3.3.6.8 - Recovery time objective (RTO)	2.1 7.5 11.6, 11.7 13.4

	○ 3.3.6.9 - Recovery point objective (RPO) 3.3.7 - Network device backup/restore ○ 3.3.7.1 - State ○ 3.3.7.2 - Configuration	
4.0	**Network Security**	
4.1	Explain common security concepts. 4.1.1 - Confidentiality, integrity, availability (CIA) 4.1.2 - Threats ○ 4.1.2.1 - Internal ○ 4.1.2.2 - External 4.1.3 - Vulnerabilities ○ 4.1.3.1 - Common vulnerabilities and exposures (CVE) ○ 4.1.3.2 - Zero-day 4.1.4 - Exploits 4.1.5 - Least privilege 4.1.6 - Role-based access 4.1.7 - Zero Trust 4.1.8 - Defense in depth ○ 4.1.8.1 - Network segmentation enforcement ○ 4.1.8.2 - Screened subnet [previously known as demilitarized zone (DMZ)] ○ 4.1.8.3 - Separation of duties ○ 4.1.8.4 - Network access control ○ 4.1.8.5 - Honeypot 4.1.9 - Authentication methods ○ 4.1.9.1 - Multifactor ○ 4.1.9.2 - Terminal Access Controller Access-Control System Plus (TACACS+) ○ 4.1.9.3 - Single sign-on (SSO) ○ 4.1.9.4 - Remote Authentication Dial-in User Service (RADIUS ○ 4.1.9.5 - LDAP ○ 4.1.9.6 - Kerberos ○ 4.1.9.7 - Local authentication ○ 4.1.9.8 - 802.1X ○ 4.1.9.9 - Extensible Authentication Protocol (EAP) 4.1.10 - Risk Management ○ 4.1.10.1 - Security risk assessments	6.2, 6.3 7.4 10.3 12.1, 12.2 13.2, 13.3

	○ 4.1.10.1.1 - Security risk assessments - Threat assessment ○ 4.1.10.1.2 - Security risk assessments - Vulnerability assessment ○ 4.1.10.1.3 - Security risk assessments - Penetration testing ○ 4.1.10.1.4 - Security risk assessments - Posture assessment ○ 4.1.10.2 - Business risk assessments ○ 4.1.10.2.1 - Business risk assessments - Process assessment ○ 4.1.10.2.2 - Business risk assessments - Vendor assessment 4.1.11 - Security information and event management (SIEM)	
4.2	Compare and contrast common types of attacks. 4.2.1 - Technology-based ○ 4.2.1.1 - Denial-of-service (DoS)/distributed denial-of-service (DDoS) ○ 4.2.1.1.1 - Denial-of-service (DoS)/distributed denial-of-service (DDoS) - Botnet/command and control ○ 4.2.1.2 - On-path attack (previously known as man-in-the-middle attack) ○ 4.2.1.3 - DNS poisoning ○ 4.2.1.4 - VLAN hopping ○ 4.2.1.5 - ARP spoofing ○ 4.2.1.6 - Rogue DHCP ○ 4.2.1.7 - Rogue access point (AP) ○ 4.2.1.8 - Evil twin ○ 4.2.1.9 - Ransomware ○ 4.2.1.10 - Password attacks ○ 4.2.1.10.1 - Password attacks - Brute-force ○ 4.2.1.10.2 - Password attacks - Dictionary ○ 4.2.1.11 - MAC spoofing ○ 4.2.1.12 - IP spoofing ○ 4.2.1.13 - Deauthentication ○ 4.2.1.14 - Malware 4.2.2 - Human and environmental ○ 4.2.2.1 - Social engineering ○ 4.2.2.1.1 - Social engineering - Phishing ○ 4.2.2.1.2 - Social engineering - Tailgating ○ 4.2.2.1.3 - Social engineering - Piggybacking ○ 4.2.2.1.4 - Social engineering - Shoulder surfing	7.4 9.5 12.4, 12.5, 12.6 14.1

4.3	Given a scenario, apply network hardening techniques. 4.3.1 - Best practices ○ 4.3.1.1 - Secure SNMP ○ 4.3.1.2 - Router Advertisement (RA) Guard ○ 4.3.1.3 - Port security ○ 4.3.1.4 - Dynamic ARP inspection ○ 4.3.1.5 - Control plane policing ○ 4.3.1.6 - Private VLANs ○ 4.3.1.7 - Disable unneeded switchports ○ 4.3.1.8 - Disable unneeded network services ○ 4.3.1.9 - Change default passwords ○ 4.3.1.10 - Password complexity/length ○ 4.3.1.11 - Enable DHCP snooping ○ 4.3.1.12 - Change default VLAN ○ 4.3.1.13 - Patch and firmware management ○ 4.3.1.14 - Access control list ○ 4.3.1.15 - Role-based access ○ 4.3.1.16 - Firewall rules ○ 4.3.1.16.1 - Firewall rules - Explicit deny ○ 4.3.1.16.2 - Firewall rules - Implicit deny 4.3.2 - Wireless security ○ 4.3.2.1 - MAC filtering ○ 4.3.2.2 - Antenna placement ○ 4.3.2.3 - Power levels ○ 4.3.2.4 - Wireless client isolation ○ 4.3.2.5 - Guest network isolation ○ 4.3.2.6 - Preshared keys (PSKs) ○ 4.3.2.7 - EAP ○ 4.3.2.8 - Geofencing ○ 4.3.2.9 - Captive portal 4.3.3 - IoT access considerations	6.1, 6.2 7.4 9.5 12.6 13.1, 13.3, 13.4
4.4	Compare and contrast remote access methods and security implications. 4.4.1 - Site-to-site VPN 4.4.2 - Client-to-site VPN ○ 4.4.2.1 - Clientless VPN	7.1, 7.2 8.3 10.4 11.8 13.2

	○ 4.4.2.2 - Split tunnel vs. full tunnel 4.4.3 - Remote desktop connection 4.4.4 - Remote desktop gateway 4.4.5 - SSH 4.4.6 - Virtual network computing (VNC) 4.4.7 - Virtual desktop 4.4.8 - Authentication and authorization considerations 4.4.9 - In-band vs. out-of-band management	
4.5	Explain the importance of physical security. 4.5.1 - Detection methods ○ 4.5.1.1 - Camera ○ 4.5.1.2 - Motion detection ○ 4.5.1.3 - Asset tags ○ 4.5.1.4 - Tamper detection 4.5.2 - Prevention methods ○ 4.5.2.1 - Employee training ○ 4.5.2.2 - Access control hardware ○ 4.5.2.2.1 - Access control hardware - Badge readers ○ 4.5.2.2.2 - Access control hardware - Biometrics ○ 4.5.2.3 - Locking racks ○ 4.5.2.4 - Locking cabinets ○ 4.5.2.5 - Access control vestibule (previously known as a mantrap) ○ 4.5.2.6 - Smart lockers 4.5.3 - Asset disposal ○ 4.5.3.1 - Factory reset/wipe configuration ○ 4.5.3.2 - Sanitize devices for disposal	12.2, 12.3 13.2
5.0	**Network Troubleshooting**	
5.1	Explain the network troubleshooting methodology. 5.1.1 - Identify the problem ○ 5.1.1.1 - Gather information ○ 5.1.1.2 - Question users ○ 5.1.1.3 - Identify symptoms	14.2

	○ 5.1.1.4 - Determine if anything has changed ○ 5.1.1.5 - Duplicate the problem, if possible ○ 5.1.1.6 - Approach multiple problems individually 5.1.2 - Establish a theory of probable cause ○ 5.1.2.1 - Question the obvious ○ 5.1.2.2 - Consider multiple approaches ○ 5.1.2.2.1 - Consider multiple approaches - Top-to-bottom/bottom-to-top OSI model ○ 5.1.2.2.2 - Consider multiple approaches -Divide and conquer 5.1.3 - Test the theory to determine the cause ○ 5.1.3.1 - If the theory is confirmed, determine the next steps to resolve the problem ○ 5.1.3.2 - If the theory is not confirmed, reestablish a new theory or escalate 5.1.4 - Establish a plan of action to resolve the problem and identify potential effects 5.1.5 - Implement the solution or escalate as necessary 5.1.6 - Verify full system functionality and, if applicable, implement preventive measure 5.1.7 - Document findings, actions, outcomes, and lessons learned	
5.2	Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools. 5.2.1 - Specifications and limitations ○ 5.2.1.1 - Throughput ○ 5.2.1.2 - Speed ○ 5.2.1.3 - Distance 5.2.2 - Cable considerations ○ 5.2.2.1 - Shielded and unshielded ○ 5.2.2.2 - Plenum and riser-rated 5.2.3 - Cable application ○ 5.2.3.1 - Rollover cable/console cable ○ 5.2.3.2 - Crossover cable ○ 5.2.3.3 - Power over Ethernet 5.2.4 - Common issues ○ 5.2.4.1 - Attenuation ○ 5.2.4.2 - Interference ○ 5.2.4.3 - Decibel (dB) loss ○ 5.2.4.4 - Incorrect pinout ○ 5.2.4.5 - Bad ports ○ 5.2.4.6 - Open/short ○ 5.2.4.7 - Light-emitting diode (LED) status indicators ○ 5.2.4.8 - Incorrect transceivers	3.1, 3.3, 3.4 5.2, 5.3

	○ 5.2.4.9 - Duplexing issues ○ 5.2.4.10 - Transmit and receive (TX/RX) reversed ○ 5.2.4.11 - Dirty optical cables 5.2.5 - Common tools ○ 5.2.5.1 - Cable crimper ○ 5.2.5.2 - Punchdown tool ○ 5.2.5.3 - Tone generator ○ 5.2.5.4 - Loopback adapter ○ 5.2.5.5 - Optical time-domain reflectometer (OTDR) ○ 5.2.5.6 - Multimeter ○ 5.2.5.7 - Cable tester ○ 5.2.5.8 - Wire map ○ 5.2.5.9 - Tap ○ 5.2.5.10 - Fusion splicers ○ 5.2.5.11 - Spectrum analyzers ○ 5.2.5.12 - Snips/cutters ○ 5.2.5.13 - Cable stripper ○ 5.2.5.14 - Fiber light meter	
5.3	Given a scenario, use the appropriate network software tools and commands. 5.3.1 - Software tools ○ 5.3.1.1 - WiFi analyzer ○ 5.3.1.2 - Protocol analyzer/packet capture ○ 5.3.1.3 - Bandwidth speed tester ○ 5.3.1.4 - Port scanner ○ 5.3.1.5 - iperf ○ 5.3.1.6 - NetFlow analyzers ○ 5.3.1.7 - Trivial File Transfer Protocol (TFTP) server ○ 5.3.1.8 - Terminal emulator ○ 5.3.1.9 - IP scanner 5.3.2 - Command line tool ○ 5.3.2.1 - ping ○ 5.3.2.2 - ipconfig/ifconfig/ip ○ 5.3.2.3 - nslookup/dig ○ 5.3.2.4 - traceroute/tracert ○ 5.3.2.5 - arp ○ 5.3.2.6 - netstat	4.9, 4.10, 4.11 11.4 14.3

	○ 5.3.2.7 - hostname ○ 5.3.2.8 - route ○ 5.3.2.9 - telnet ○ 5.3.2.10 - tcpdump ○ 5.3.2.11 - nmap 5.3.3 - Basic network platform commands ○ 5.3.3.1 - show interface ○ 5.3.3.2 - show config ○ 5.3.3.3 - show route	
5.4	Given a scenario, troubleshoot common wireless connectivity issues. 5.4.1 - Specifications and limitations ○ 5.4.1.1 - Throughput ○ 5.4.1.2 - Speed ○ 5.4.1.3 - Distance ○ 5.4.1.4 - Received signal strength indication (RSSI) signal strength ○ 5.4.1.5 - Effective isotropic radiated power (EIRP)/power settings 5.4.2 - Considerations ○ 5.4.2.1 - Antennas ○ 5.4.2.1.1 - Antennas - Placement ○ 5.4.2.1.2 - Antennas - Type ○ 5.4.2.1.3 - Antennas - Polarization ○ 5.4.2.2 - Channel utilization ○ 5.4.2.3 - AP association time ○ 5.4.2.4 - Site survey 5.4.3 - Common issues ○ 5.4.3.1 - Interference ○ 5.4.3.1.1 - Interference - Channel overlap ○ 5.4.3.2 - Antenna cable attenuation/signal loss ○ 5.4.3.3 - RF attenuation/signal loss ○ 5.4.3.4 - Wrong SSID ○ 5.4.3.5 - Incorrect passphrase ○ 5.4.3.6 - Encryption protocol mismatch ○ 5.4.3.7 - Insufficient wireless coverage ○ 5.4.3.8 - Captive portal issues ○ 5.4.3.9 - Client disassociation issues	9.3, 9.6

5.5	Given a scenario, troubleshoot general networking issues. 5.5.1 - Considerations ○ 5.5.1.1 - Device configuration review ○ 5.5.1.2 - Routing tables ○ 5.5.1.3 - Interface status ○ 5.5.1.4 - VLAN assignment ○ 5.5.1.5 - Network performance baselines 5.5.2 - Common issues ○ 5.5.2.1 - Collisions ○ 5.5.2.2 - Broadcast storm ○ 5.5.2.3 - Duplicate MAC address ○ 5.5.2.4 - Duplicate IP address ○ 5.5.2.5 - Multicast flooding ○ 5.5.2.6 - Asymmetrical routing ○ 5.5.2.7 - Switching loops ○ 5.5.2.8 - Routing loops ○ 5.5.2.9 - Rogue DHCP server ○ 5.5.2.10 - DHCP scope exhaustion ○ 5.5.2.11 - IP setting issues ○ 5.5.2.11.1 - IP setting issues - Incorrect gateway ○ 5.5.2.11.2 - IP setting issues - Incorect subnet mask ○ 5.5.2.11.3 - IP setting issues - Incorrect IP address ○ 5.5.2.11.4 - IP setting issues - Incorrect DNS ○ 5.5.2.12 - Missing route ○ 5.5.2.13 - Low optical link budget ○ 5.5.2.14 - Certificate issues ○ 5.5.2.15 - Hardware failure ○ 5.5.2.16 - Host-based/network-based firewall settings ○ 5.5.2.17 - Blocked services, ports, or addresses ○ 5.5.2.18 - Incorrect VLAN ○ 5.5.2.19 - DNS issues ○ 5.5.2.20 - NTP issues ○ 5.5.2.21 - BYOD challenges ○ 5.5.2.22 - Licensed feature issues ○ 5.5.2.23 - Network performance issues	4.9, 4.11 6.2 7.7 9.5 13.2 14.1, 14.2