TestOut®

TestOut Network Pro – English 5.0.x

Objective Mappings:

TestOut Network Pro
CompTIA N10-007

Revised: 2018-03-06

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 Objective

Section	Title	Objectives
0.0	**Introduction**	
0.1	Network Pro Introduction	
0.2	Use the Simulator	
1.0	**Networking Basics**	
1.1	Networking Overview	
1.2	Network Topologies	
1.3	The OSI Model	
1.4	Network Protocols	
1.5	Numbering Systems	
2.0	**Cables and Connectors**	
2.1	Twisted Pair	1.1 Given a scenario, implement a cabling solution to establish network communication.
2.2	Coaxial	1.1 Given a scenario, implement a cabling solution to establish network communication.
2.3	Fiber Optic	1.1 Given a scenario, implement a cabling solution to establish network communication.
2.4	Wiring Implementation	1.1 Given a scenario, implement a cabling solution to establish network communication.
2.5	Troubleshoot Network Media	5.1 Given a scenario, troubleshoot issues with networking media or devices to establish network communication.
3.0	**Networking Devices**	

3.1	Network Adapters	1.2 Given a scenario, deploy appropriate wired networking or internetworking device(s). 5.1 Given a scenario, troubleshoot issues with networking media or devices to establish network communication.
3.2	Network Devices	1.2 Given a scenario, deploy appropriate wired networking or internetworking device(s). 5.1 Given a scenario, troubleshoot issues with networking media or devices to establish network communication.
3.3	Internetwork Devices	1.2 Given a scenario, deploy appropriate wired networking or internetworking device(s). 5.1 Given a scenario, troubleshoot issues with networking media or devices to establish network communication.
4.0	**Ethernet**	
4.1	Ethernet	
4.2	Ethernet Specifications	1.1 Given a scenario, implement a cabling solution to establish network communication.
4.3	Connect Network Devices	1.1 Given a scenario, implement a cabling solution to establish network communication. 1.2 Given a scenario, deploy appropriate wired networking or internetworking device(s).
4.4	Troubleshoot Physical Connectivity	1.2 Given a scenario, deploy appropriate wired networking or internetworking device(s). 5.1 Given a scenario, troubleshoot issues with networking media or devices to establish network communication.
5.0	**IP Configuration**	
5.1	IP Addressing	2.1 Given a scenario, configure IP addressing, DNS, and DHCP for a network host.
5.2	APIPA and Alternate Addressing	2.1 Given a scenario, configure IP addressing, DNS, and DHCP for a network host.
5.3	DHCP Server Configuration	3.1 Given a scenario, configure DHCP services for a network subnet.
5.4	DHCP Relay	3.1 Given a scenario, configure DHCP services for a network subnet.

5.5	DNS Name Resolution	3.2 Given a scenario, configure DNS for the network.
5.6	IP Version 6	2.1 Given a scenario, configure IP addressing, DNS, and DHCP for a network host.
5.7	Multicast	
5.8	Troubleshoot IP Configuration Issues	3.4 Given a scenario, use network tools to discover network devices and resources. 5.2 Given a scenario, troubleshoot IP configuration issues to establish network communication.
5.9	Troubleshoot IP Communications	3.4 Given a scenario, use network tools to discover network devices and resources. 5.2 Given a scenario, troubleshoot IP configuration issues to establish network communication.
5.10	Troubleshoot Name Resolution	3.4 Given a scenario, use network tools to discover network devices and resources. 5.3 Given a scenario, troubleshoot wired or wireless network connectivity to establish network communication.
6.0	**Switch Management**	
6.1	Switch Access	2.3 Given a scenario, perform basic router configuration tasks.
6.2	Switch IP Configuration	4.3 Given a scenario, configure security for a switch.
6.3	Switch Interface Configuration	2.2 Given a scenario, perform basic switch configuration tasks.
6.4	Virtual LANs	3.6 Given a scenario, configure virtual networking.
6.5	Trunking	
6.6	Spanning Tree Protocol	
6.7	Switch Troubleshooting	

7.0	Routing	
7.1	Routing Basics	2.3 Given a scenario, perform basic router configuration tasks.
7.2	Routing Protocols	2.3 Given a scenario, perform basic router configuration tasks.
7.3	Network Address Translation	
7.4	Routing Troubleshooting	5.1 Given a scenario, troubleshoot issues with networking media or devices to establish network communication.
8.0	**Firewalls**	
8.1	Firewalls	4.1 Given a scenario, configure a host firewall to provide local security.
8.2	Security Appliances	4.5 Given a scenario, perform administrative tasks on a network security appliance.
8.3	Firewall Design and Implementation	4.1 Given a scenario, configure a host firewall to provide local security.
9.0	**Network Customization**	
9.1	Network-Based Storage	
9.2	Voice over IP (VoIP)	2.5 Given a scenario, configure a VoIP endpoint.
9.3	Virtualization	3.6 Given a scenario, configure virtual networking.
9.4	Virtual Networking	3.6 Given a scenario, configure virtual networking.
9.5	Cloud Computing	
10.0	**Wireless Networking**	
10.1	Wireless Concepts	1.3 Given a scenario, implement appropriate wireless networking device(s).

		2.4 Given a scenario, establish a wireless network connection for a device on the network.
10.2	Wireless Standards	1.3 Given a scenario, implement appropriate wireless networking device(s). 2.4 Given a scenario, establish a wireless network connection for a device on the network.
10.3	Wireless Configuration	1.3 Given a scenario, implement appropriate wireless networking device(s). 2.4 Given a scenario, establish a wireless network connection for a device on the network.
10.4	Wireless Network Design	1.3 Given a scenario, implement appropriate wireless networking device(s). 2.4 Given a scenario, establish a wireless network connection for a device on the network.
10.5	Wireless Network Implementation	1.3 Given a scenario, implement appropriate wireless networking device(s). 2.4 Given a scenario, establish a wireless network connection for a device on the network.
10.6	Wireless Security	1.3 Given a scenario, implement appropriate wireless networking device(s). 2.4 Given a scenario, establish a wireless network connection for a device on the network. 4.2 Given a scenario, secure an enterprise wireless network.
10.7	Wireless Troubleshooting	5.3 Given a scenario, troubleshoot wired or wireless network connectivity to establish network communication.
11.0	**Wide Area Networks (WANs)**	
11.1	WAN Concepts	1.2 Given a scenario, deploy appropriate wired networking or internetworking device(s). 1.3 Given a scenario, implement appropriate wireless networking device(s).
11.2	WAN Connections	1.2 Given a scenario, deploy appropriate wired networking or internetworking device(s). 1.3 Given a scenario, implement appropriate wireless networking device(s).

11.3	Internet Connectivity	1.2 Given a scenario, deploy appropriate wired networking or internetworking device(s). 1.3 Given a scenario, implement appropriate wireless networking device(s).
11.4	Remote Access	4.4 Given a scenario, configure systems and remote devices to create and use a VPN connection.
11.5	WAN Troubleshooting	5.1 Given a scenario, troubleshoot issues with networking media or devices to establish network communication. 5.3 Given a scenario, troubleshoot wired or wireless network connectivity to establish network communication.
12.0	**Network Policies and Procedures**	
12.1	Network Design, Documentation, and Policies	
12.2	Risk Management	
12.3	Security Policies	
13.0	**Network Security**	
13.1	Physical Security	
13.2	Social Engineering	4.6 Given a scenario, respond to social engineering exploits.
13.3	Network Vulnerabilities and Threats 1	4.6 Given a scenario, respond to social engineering exploits.
13.4	Network Vulnerabilities and Threats 2	4.6 Given a scenario, respond to social engineering exploits.
13.5	Authentication	4.6 Given a scenario, respond to social engineering exploits.
13.6	Secure Protocols	
13.7	Remote Access Security	4.4 Given a scenario, configure systems and remote devices to create and use a VPN connection.

13.8	Troubleshoot Network Security Issues	
14.0	**Network Hardening**	
14.1	Detection and Prevention	4.5 Given a scenario, perform administrative tasks on a network security appliance.
14.2	Penetration Testing	
14.3	Network Hardening	4.3 Given a scenario, configure security for a switch.
15.0	**Network Management**	
15.1	Update Management	
15.2	Data Protection	3.5 Given a scenario, perform data and server backup and recovery tasks.
15.3	Remote Management	3.3 Given a scenario, configure Remote Desktop to allow remote access to systems.
15.4	Mobile Device Management	
15.5	Data Center Management	
15.6	Monitoring	3.4 Given a scenario, use network tools to discover network devices and resources.
15.7	Log File Management	3.4 Given a scenario, use network tools to discover network devices and resources.
15.8	Network Management with SNMP	3.4 Given a scenario, use network tools to discover network devices and resources.
16.0	**Network Optimization**	
16.1	Optimization	
16.2	Troubleshooting Methodology	

A.0	**Network Pro Practice Exams**	
A.1	Preparing for Network Pro Certification	
A.2	Network Pro Question Review	
B.0	**Network+ Practice Exams**	
B.1	Preparing for Network+ Certification	
B.2	Network+ Question Review (20 Random Questions)	
B.3	Network+ Question Review (All Questions)	

Objective Mapping: TestOut Network Pro Objective to LabSim Section

#	Domain	Section
1.0	**Networking Hardware**	
1.1	Given a scenario, implement a cabling solution to establish network communication.	2.1, 2.2, 2.3, 2.4 4.2, 4.3
1.2	Given a scenario, deploy appropriate wired networking or internetworking device(s).	3.1, 3.2, 3.3 4.3, 4.4 11.1, 11.2, 11.3
1.3	Given a scenario, implement appropriate wireless networking device(s).	10.1, 10.2, 10.3, 10.4, 10.5, 10.6 11.1, 11.2, 11.3
2.0	**Network Device Configuration**	
2.1	Given a scenario, configure IP addressing, DNS, and DHCP for a network host.	5.1, 5.2, 5.6
2.2	Given a scenario, perform basic switch configuration tasks.	6.3
2.3	Given a scenario, perform basic router configuration tasks.	6.1 7.1, 7.2
2.4	Given a scenario, establish a wireless network connection for a device on the network.	10.1, 10.2, 10.3, 10.4, 10.5, 10.6
2.5	Given a scenario, configure a VoIP endpoint.	9.2
3.0	**Network Management**	
3.1	Given a scenario, configure DHCP services for a network subnet.	5.3, 5.4

3.2	Given a scenario, configure DNS for the network.	5.5
3.3	Given a scenario, configure Remote Desktop to allow remote access to systems.	15.3
3.4	Given a scenario, use network tools to discover network devices and resources.	5.8, 5.9, 5.10 15.6, 15.7, 15.8
3.5	Given a scenario, perform data and server backup and recovery tasks.	15.2
3.6	Given a scenario, configure virtual networking.	6.4 9.3, 9.4
4.0	**Network Security**	
4.1	Given a scenario, configure a host firewall to provide local security.	8.1, 8.3
4.2	Given a scenario, secure an enterprise wireless network.	10.6
4.3	Given a scenario, configure security for a switch.	6.2 14.3
4.4	Given a scenario, configure systems and remote devices to create and use a VPN connection.	11.4 13.7
4.5	Given a scenario, perform administrative tasks on a network security appliance.	8.2 14.1
4.6	Given a scenario, respond to social engineering exploits.	13.2, 13.3, 13.4, 13.5
5.0	**Network Troubleshooting**	
5.1	Given a scenario, troubleshoot issues with networking media or devices to establish network communication.	2.5 3.1, 3.2, 3.3 4.4

		7.4 11.5
5.2	Given a scenario, troubleshoot IP configuration issues to establish network communication.	5.8, 5.9
5.3	Given a scenario, troubleshoot wired or wireless network connectivity to establish network communication.	5.10 10.7 11.5

Objective Mapping: LabSim Section to CompTIA N10-007 Objective

Section	Title	Objectives
0.0	**Introduction**	
0.1	Network Pro Introduction	
0.2	Use the Simulator	
1.0	**Networking Basics**	
1.1	Networking Overview	1.5 Compare and contrast the characteristics of network topologies, types and technologies. Types o LAN o MAN o WAN o CAN
1.2	Network Topologies	1.5 Compare and contrast the characteristics of network topologies, types and technologies. Wired topologies o Logical vs. physical o Star o Ring o Mesh o Bus
1.3	The OSI Model	1.2 Explain devices, applications, protocols and services at their appropriate OSI layers. Layer 1 – Physical Layer 2 – Data link Layer 3 – Network Layer 4 – Transport Layer 5 – Session Layer 6 – Presentation Layer 7 – Application

1.4	Network Protocols	1.1 Explain the purposes and uses of ports and protocols. Protocols and ports o SSH 22 o DNS 53 o SMTP 25 o SFTP 22 o FTP 20, 21 o TFTP 69 o TELNET 23 o DHCP 67, 68 o HTTP 80 o HTTPS 443 o SNMP 161 o RDP 3389 o NTP 123 o SIP 5060, 5061 o SMB 445 o POP 110 o IMAP 143 o LDAP 389 o LDAPS 636 o H.323 1720 Protocol types o ICMP o UDP o TCP o IP Connection-oriented vs. connectionless 1.8 Explain the functions of network services. NTP 3.4 Given a scenario, use remote access methods. RDP Telnet 4.2 Explain authentication and access controls. Authorization, authentication and accounting

		o LDAP
1.5	Numbering Systems	
2.0	**Cables and Connectors**	
2.1	Twisted Pair	2.1 Given a scenario, deploy the appropriate cabling solution. Media types o Copper - UTP o Copper - STP Plenum vs. PVC Connector types o Copper - RJ-45 o Copper - RJ-11 Copper cable standards o Cat 3 o Cat 5 o Cat 5e o Cat 6 o Cat 6a o Cat 7
2.2	Coaxial	2.1 Given a scenario, deploy the appropriate cabling solution. Media types o Copper - Coaxial Connector types o Copper - BNC o Copper - DB-9 o Copper - DB-25 o Copper - F-type Copper cable standards o RG-6 o RG-59 3.4 Given a scenario, use remote access methods. Out-of-band management

		o Modem
2.3	Fiber Optic	2.1 Given a scenario, deploy the appropriate cabling solution. Media types o Copper - Coaxial o Fiber - Single-mode o Fiber - Multimode Connector types o Fiber - LC o Fiber - ST o Fiber - SC - APC o Fiber - SC - UPC o Fiber - SC - MTRJ 2.2 Given a scenario, determine the appropriate placement of networking devices on a network and install/configure them. Media converter
2.4	Wiring Implementation	2.1 Given a scenario, deploy the appropriate cabling solution. Termination points o 66 block o 110 block o Patch panel o Fiber distribution panel Copper termination standards o TIA/EIA 568a o TIA/EIA 568b 2.5 Compare and contrast WAN technologies. Termination o Demarcation point o Smart jack 3.1 Given a scenario, use appropriate documentation and diagrams to manage the network. Wiring and port locations

		IDF/MDF documentation
2.5	Troubleshoot Network Media	2.5 Compare and contrast WAN technologies. Termination o Smart jack 5.2 Given a scenario, use the appropriate tool. Hardware tools o Crimper o Punchdown tool o OTDR o Multimeter o Light meter o Tone generator o Cable tester o Loopback adapter o Spectrum analyzer Software tools o Bandwidth speed tester 5.3 Given a scenario, troubleshoot common wired connectivity and performance issues. Attenuation Crosstalk EMI Open/short Incorrect pin-out Incorrect cable type Transceiver mismatch TX/RX reverse Damaged cables Bent pins 5.4 Given a scenario, troubleshoot common wireless connectivity and performance issues. Reflection Refraction Absorption

		Attenuation
3.0	**Networking Devices**	
3.1	Network Adapters	2.1 Given a scenario, deploy the appropriate cabling solution. Transceivers o SFP o GBIC o SFP+ o QSFP o Characteristics of fiber transceivers - Bidirectional 2.2 Given a scenario, determine the appropriate placement of networking devices on a network and install/configure them. Modems
3.2	Network Devices	2.2 Given a scenario, determine the appropriate placement of networking devices on a network and install/configure them. Switch Hub
3.3	Internetwork Devices	2.2 Given a scenario, determine the appropriate placement of networking devices on a network and install/configure them. Firewall Router 2.3 Explain the purposes and use cases for advanced networking devices. Multilayer switch
4.0	**Ethernet**	

4.1	Ethernet	1.3 Explain the concepts and characteristics of routing and switching. Properties of network traffic o CSMA/CD 2.1 Given a scenario, deploy the appropriate cabling solution. Transceivers o Characteristics of fiber transceivers - Duplex
4.2	Ethernet Specifications	2.1 Given a scenario, deploy the appropriate cabling solution. Ethernet deployment standards o 100BaseT o 1000BaseT o 1000BaseLX o 1000BaseSX o 10GBaseT
4.3	Connect Network Devices	2.1 Given a scenario, deploy the appropriate cabling solution. Connector types o Copper - DB-9 o Copper - DB-25 Copper termination standards o Crossover o Straight-through
4.4	Troubleshoot Physical Connectivity	1.5 Compare and contrast the characteristics of network topologies, types and technologies. Wired topologies o Logical vs. physical o Star o Ring o Mesh o Bus 5.3 Given a scenario, troubleshoot common wired connectivity and performance issues.

		Duplex/speed mismatch Network connection LED status indicators 5.5 Given a scenario, troubleshoot common network service issues. Hardware failure
5.0	**IP Configuration**	
5.1	IP Addressing	1.3 Explain the concepts and characteristics of routing and switching. Properties of network traffic o Broadcast 1.4 Given a scenario, configure the appropriate IP addressing components. Default gateway Subnet mask Subnetting o Classful (Classes A, B, C, D, and E) o Classless (VLSM, CIDR notation (IPv4 vs. IPv6)) Address assignments o DHCP o Static
5.2	APIPA and Alternate Addressing	1.4 Given a scenario, configure the appropriate IP addressing components. Address assignments o APIPA
5.3	DHCP Server Configuration	1.4 Given a scenario, configure the appropriate IP addressing components. Address assignments o DHCP o IP reservations 1.8 Explain the functions of network services.

		DHCP service o MAC reservations o Pools o IP exclusions o Scope options o Lease time
5.4	DHCP Relay	1.8 Explain the functions of network services. DHCP service o DHCP relay/IP helper
5.5	DNS Name Resolution	1.8 Explain the functions of network services. DNS service o Record types - A, AAA o Record types - TXT (SPF, DKIM) o Record types - SRV o Record types - MX o Record types - CNAME o Record types - NS o Record types - PTR o Internal vs. external DNS o Third-party/cloud-hosted DNS o Hierarchy o Forward vs. reverse zone
5.6	IP Version 6	1.3 Explain the concepts and characteristics of routing and switching. IPv6 concepts o Addressing o Tunneling o Dual stack o Router advertisement o Neighbor discovery 1.4 Given a scenario, configure the appropriate IP addressing components. Loopback and reserved

		Default gateway Address assignments o DHCPv6 o EUI64 1.8 Explain the functions of network services. IPAM
5.7	Multicast	1.3 Explain the concepts and characteristics of routing and switching. Properties of network traffic o Multicast o Unicast
5.8	Troubleshoot IP Configuration Issues	5.2 Given a scenario, use the appropriate tool. Software tools o Command line - ifconfig o Command line - ipconfig 5.5 Given a scenario, troubleshoot common network service issues. Incorrect gateway Incorrect netmask Duplicate IP addresses Duplicate MAC addresses Expired IP address Rogue DHCP server Exhausted DHCP scope
5.9	Troubleshoot IP Communications	1.3 Explain the concepts and characteristics of routing and switching. Segmentation and interface properties o ARP table 5.2 Given a scenario, use the appropriate tool. Software tools

		o Command line - ping o Command line - tracert, traceroute o Command line - netstat o Command line - arp o Command line - tcpdump o Command line - route 5.5 Given a scenario, troubleshoot common network service issues. Unresponsive service
5.10	Troubleshoot Name Resolution	5.2 Given a scenario, use the appropriate tool. Software tools o Command line - nslookup o Command line - dig 5.5 Given a scenario, troubleshoot common network service issues. Names not resolving
6.0	**Switch Management**	
6.1	Switch Access	3.4 Given a scenario, use remote access methods. Out-of-band management o Console router
6.2	Switch IP Configuration	
6.3	Switch Interface Configuration	1.3 Explain the concepts and characteristics of routing and switching. Segmentation and interface properties o Port mirroring
6.4	Virtual LANs	1.3 Explain the concepts and characteristics of routing and switching.

		Segmentation and interface properties o VLANs
6.5	Trunking	1.3 Explain the concepts and characteristics of routing and switching. Properties of network traffic o Broadcast domains Segmentation and interface properties o VLANs o Trunking (802.1q) o Tagging and untagging ports 4.6 Explain common mitigation techniques and their purposes. Change native VLAN
6.6	Spanning Tree Protocol	1.3 Explain the concepts and characteristics of routing and switching. Properties of network traffic o Protocol data units Segmentation and interface properties o Switching loops/spanning tree
6.7	Switch Troubleshooting	1.3 Explain the concepts and characteristics of routing and switching. Segmentation and interface properties o MAC address table 5.3 Given a scenario, troubleshoot common wired connectivity and performance issues. Bad port Duplex/speed mismatch VLAN mismatch Network connection LED status indicators
7.0	**Routing**	

7.1	Routing Basics	1.3 Explain the concepts and characteristics of routing and switching. Routing o Routing types - Default - Static - Dynamic
7.2	Routing Protocols	1.3 Explain the concepts and characteristics of routing and switching. Properties of network traffic o MTU Routing o Routing protocols (IPv4 and IPv6) - Distance-vector routing protocols (RIP, EIGRP) o Routing protocols (IPv4 and IPv6) - Link-state routing protocols (OSPF) o Routing protocols (IPv4 and IPv6) - Hybrid (BGP) o Routing types - Default - Static - Dynamic 1.4 Given a scenario, configure the appropriate IP addressing components. Virtual IP 5.3 Given a scenario, troubleshoot common wired connectivity and performance issues. Latency
7.3	Network Address Translation	1.3 Explain the concepts and characteristics of routing and switching. NAT/PAT Port forwarding 1.4 Given a scenario, configure the appropriate IP addressing components. Private vs. public
7.4	Routing Troubleshooting	5.3 Given a scenario, troubleshoot common wired connectivity and performance issues. Latency

8.0	Firewalls	
8.1	Firewalls	1.1 Explain the purposes and uses of ports and protocols. Protocols and ports o SSH 22 o DNS 53 o SMTP 25 o SFTP 22 o FTP 20, 21 o TFTP 69 o TELNET 23 o DHCP 67, 68 o HTTP 80 o HTTPS 443 o SNMP 161 o RDP 3389 o NTP 123 o SIP 5060, 5061 o SMB 445 o POP 110 o IMAP 143 o LDAP 389 o LDAPS 636 o H.323 1720 1.3 Explain the concepts and characteristics of routing and switching. Access control list 2.2 Given a scenario, determine the appropriate placement of networking devices on a network and install/configure them. Firewall 2.3 Explain the purposes and use cases for advanced networking devices. Proxy server UTM appliance NGFW/Layer 7 firewall

		Content filter 4.6 Explain common mitigation techniques and their purposes. Restricting access via ACLs 5.2 Given a scenario, use the appropriate tool. Software tools o Command line - iptables
8.2	Security Appliances	2.2 Given a scenario, determine the appropriate placement of networking devices on a network and install/configure them. Firewall 2.3 Explain the purposes and use cases for advanced networking devices. IDS/IPS UTM appliance Content filter
8.3	Firewall Design and Implementation	1.3 Explain the concepts and characteristics of routing and switching. Segmentation and interface properties o DMZ 2.2 Given a scenario, determine the appropriate placement of networking devices on a network and install/configure them. Firewall 2.3 Explain the purposes and use cases for advanced networking devices. Proxy server 4.2 Explain authentication and access controls.

		Access control o MAC filtering o Access control list 5.5 Given a scenario, troubleshoot common network service issues. Incorrect firewall settings Incorrect ACL settings
9.0	**Network Customization**	
9.1	Network-Based Storage	1.5 Compare and contrast the characteristics of network topologies, types and technologies. Types o SAN 2.4 Explain the purposes of virtualization and network storage technologies. Network storage types o NAS o SAN Connection type o FCoE o Fibre Channel o iSCSI o InfiniBand 3.2 Compare and contrast business continuity and disaster recovery concepts. Availability concepts o Load balancing o Clustering
9.2	Voice over IP (VoIP)	1.3 Explain the concepts and characteristics of routing and switching. Segmentation and interface properties o PoE and PoE+ (802.3af, 802.3at)

		2.2 Given a scenario, determine the appropriate placement of networking devices on a network and install/configure them. VoIP endpoint 2.3 Explain the purposes and use cases for advanced networking devices. VoIP PBX VoIP gateway 2.4 Explain the purposes of virtualization and network storage technologies. Jumbo frame 5.3 Given a scenario, troubleshoot common wired connectivity and performance issues. Latency Jitter 5.4 Given a scenario, troubleshoot common wireless connectivity and performance issues. Latency Jitter
9.3	Virtualization	
9.4	Virtual Networking	1.3 Explain the concepts and characteristics of routing and switching. Software-defined networking 2.4 Explain the purposes of virtualization and network storage technologies. Virtual networking components o Virtual switch o Virtual firewall o Virtual NIC o Virtual router o Hypervisor

		Jumbo frame
9.5	Cloud Computing	1.7 Summarize cloud concepts and their purposes. Types of services o SaaS o PaaS o IaaS Cloud delivery models o Private o Public o Hybrid Connectivity methods Security implications/ considerations Relationship between local and cloud resources
10.0	**Wireless Networking**	
10.1	Wireless Concepts	1.3 Explain the concepts and characteristics of routing and switching. Properties of network traffic o CSMA/CA 1.5 Compare and contrast the characteristics of network topologies, types and technologies. Wireless topologies o Mesh o Ad hoc o Infrastructure 2.5 Compare and contrast WAN technologies. Transmission mediums o Wireless
10.2	Wireless Standards	1.5 Compare and contrast the characteristics of network topologies, types and technologies. Types

		o PAN Technologies that facilitate the Internet of Things (IoT) o Bluetooth o IR o RFID 1.6 Given a scenario, implement the appropriate wireless technologies and configurations. 802.11 standards o a o b o g o n o ac Frequencies o 2.4GHz o 5.0GHz Speed and distance requirements Channel bandwidth Channel bonding MIMO/MU-MIMO 5.4 Given a scenario, troubleshoot common wireless connectivity and performance issues. Channel overlap
10.3	Wireless Configuration	2.2 Given a scenario, determine the appropriate placement of networking devices on a network and install/configure them. Bridge Wireless access point Wireless range extender 2.3 Explain the purposes and use cases for advanced networking devices. Wireless controller
10.4	Wireless Network Design	1.5 Compare and contrast the characteristics of network topologies, types and technologies. Types

		o WLAN Technologies that facilitate the Internet of Things (IoT) o Z-Wave o Ant+ o NFC o 802.11 1.6 Given a scenario, implement the appropriate wireless technologies and configurations. Speed and distance requirements MIMO/MU-MIMO Unidirectional/ omnidirectional Site survey 2.2 Given a scenario, determine the appropriate placement of networking devices on a network and install/configure them. Bridge Wireless access point 2.3 Explain the purposes and use cases for advanced networking devices. Wireless controller 5.2 Given a scenario, use the appropriate tool. Hardware tools o Spectrum analyzer 5.4 Given a scenario, troubleshoot common wireless connectivity and performance issues. Overcapacity
10.5	Wireless Network Implementation	2.2 Given a scenario, determine the appropriate placement of networking devices on a network and install/configure them. Bridge Wireless access point

		2.3 Explain the purposes and use cases for advanced networking devices. Wireless controller 5.3 Given a scenario, troubleshoot common wired connectivity and performance issues. Bottlenecks
10.6	Wireless Security	2.3 Explain the purposes and use cases for advanced networking devices. Wireless controller 4.2 Explain authentication and access controls. Access control o MAC filtering 4.3 Given a scenario, secure a basic wireless network. WPA WPA2 TKIP-RC4 CCMP-AES Authentication and authorization o Shared or open o Preshared key o MAC filtering Geofencing 4.4 Summarize common networking attacks. Rogue access point Evil twin War-driving Deauthentication
10.7	Wireless Troubleshooting	5.2 Given a scenario, use the appropriate tool. Software tools

		o WiFi analyzer 5.4 Given a scenario, troubleshoot common wireless connectivity and performance issues. Reflection Refraction Absorption Latency Incorrect antenna type Interference Incorrect antenna placement Distance limitations Frequency mismatch Wrong SSID Wrong passphrase Security type mismatch Power levels Signal-to-noise ratio
11.0	**Wide Area Networks (WANs)**	
11.1	WAN Concepts	1.3 Explain the concepts and characteristics of routing and switching. Distributed switching Packet-switched vs. circuit-switched network 2.5 Compare and contrast WAN technologies. Service type o ISDN o T1/T3 o E1/E3 o OC-3 o OC-192 o Metropolitan Ethernet o PRI Transmission mediums o Copper o Fiber Characteristics of service o MPLS

		o ATM o Frame relay o SIP trunk Termination o Demarcation point o CSU/DSU
11.2	WAN Connections	2.5 Compare and contrast WAN technologies. Characteristics of service o PPP
11.3	Internet Connectivity	1.6 Given a scenario, implement the appropriate wireless technologies and configurations. Cellular o GSM o TDMA o CDMA 2.5 Compare and contrast WAN technologies. Service type o ISDN o DSL o Cable broadband o PRI o Dial-up Transmission mediums o Satellite
11.4	Remote Access	2.3 Explain the purposes and use cases for advanced networking devices. AAA/RADIUS server 2.5 Compare and contrast WAN technologies. Characteristics of service o PPPoE

		o PPP 3.5 Identify policies and best practices. Remote access policies 4.2 Explain authentication and access controls. Authorization, authentication and accounting o RADIUS o TACACS+
11.5	WAN Troubleshooting	5.5 Given a scenario, troubleshoot common network service issues. Incorrect time
12.0	**Network Policies and Procedures**	
12.1	Network Design, Documentation, and Policies	1.7 Summarize cloud concepts and their purposes. Security implications/considerations 3.1 Given a scenario, use appropriate documentation and diagrams to manage the network. Diagram symbols Standard operating procedures/work instructions Logical vs. physical diagrams Rack diagrams Wiring and port locations Network configuration and performance baselines Inventory management 3.2 Compare and contrast business continuity and disaster recovery concepts. MTTR MTBF

		3.3 Explain common scanning, monitoring and patching processes and summarize their expected outputs. Processes o Reviewing baselines 3.5 Identify policies and best practices. System life cycle o Asset disposal
12.2	Risk Management	3.1 Given a scenario, use appropriate documentation and diagrams to manage the network. Change management documentation 3.5 Identify policies and best practices. Incident response policies 4.6 Explain common mitigation techniques and their purposes. Role separation
12.3	Security Policies	3.2 Compare and contrast business continuity and disaster recovery concepts. SLA requirements 3.5 Identify policies and best practices. Privileged user agreement Password policy On-boarding/off-boarding procedures Licensing restrictions International export controls Data loss prevention Remote access policies AUP NDA

		Safety procedures and policies 4.6 Explain common mitigation techniques and their purposes. Privileged user account Role separation
13.0	**Network Security**	
13.1	Physical Security	4.1 Summarize the purposes of physical security devices. Detection o Motion detection o Video surveillance o Asset tracking tags o Tamper detection Prevention o Badges o Biometrics o Smart cards o Key fob o Locks
13.2	Social Engineering	4.4 Summarize common networking attacks. Social engineering Insider threat Phishing
13.3	Network Vulnerabilities and Threats 1	4.4 Summarize common networking attacks. DoS o Reflective o Amplified o Distributed Logic bomb Ransomware DNS poisoning ARP poisoning

		Spoofing Man-in-the-middle
13.4	Network Vulnerabilities and Threats 2	4.4 Summarize common networking attacks. Phishing Brute force VLAN hopping 4.5 Given a scenario, implement network device hardening. Changing default credentials Avoiding common passwords
13.5	Authentication	4.2 Explain authentication and access controls. Authorization, authentication and accounting o Kerberos o Single sign-on o Auditing and logging o Certificates Multifactor authentication o Something you know o Something you have o Something you are o Somewhere you are o Something you do Access control o 802.1x o Captive portal 4.3 Given a scenario, secure a basic wireless network. Authentication and authorization o EAP - PEAP o EAP - EAP-FAST o EAP - EAP-TLS 4.6 Explain common mitigation techniques and their purposes.

		Signature management
13.6	Secure Protocols	3.4 Given a scenario, use remote access methods. VPN o SSL/TLS/DTLS 4.4 Summarize common networking attacks. Exploits vs. vulnerabilities 4.5 Given a scenario, implement network device hardening. File hashing Using secure protocols Generating new keys 4.6 Explain common mitigation techniques and their purposes. File integrity monitoring
13.7	Remote Access Security	2.3 Explain the purposes and use cases for advanced networking devices. VPN concentrator 2.5 Compare and contrast WAN technologies. Characteristics of service o DMVPN 3.4 Given a scenario, use remote access methods. VPN o IPSec o SSL/TLS/DTLS o Site-to-site o Client-to-site

13.8	Troubleshoot Network Security Issues	4.2 Explain authentication and access controls. Authorization, authentication and accounting o Local authentication 4.4 Summarize common networking attacks. Exploits vs. vulnerabilities 4.5 Given a scenario, implement network device hardening. Disabling unused ports o IP ports o Device ports (physical and virtual) 5.5 Given a scenario, troubleshoot common network service issues. Untrusted SSL certificate Blocked TCP/UDP ports
14.0	**Network Hardening**	
14.1	Detection and Prevention	2.3 Explain the purposes and use cases for advanced networking devices. IDS/IPS 3.3 Explain common scanning, monitoring and patching processes and summarize their expected outputs. Processes o Port scanning o Vulnerability scanning Event management o SIEM 4.5 Given a scenario, implement network device hardening. Disabling unused ports o IP ports

		o Device ports (physical and virtual) 4.6 Explain common mitigation techniques and their purposes. Honeypot/honeynet 5.2 Given a scenario, use the appropriate tool. Software tools o Port scanner
14.2	Penetration Testing	4.6 Explain common mitigation techniques and their purposes. Penetration testing 5.2 Given a scenario, use the appropriate tool. Software tools o Command line - nmap
14.3	Network Hardening	3.4 Given a scenario, use remote access methods. SSH HTTPS/management URL Remote file access o FTP/FTPS o SFTP o TFTP 4.2 Explain authentication and access controls. Access control o NAC o Port security 4.5 Given a scenario, implement network device hardening. Disabling unnecessary services Disabling unused ports

		o IP ports o Device ports (physical and virtual) 4.6 Explain common mitigation techniques and their purposes. Device hardening Switch port protection o Spanning tree o DHCP snooping o Flood guard o BPDU guard o Root guard
15.0	**Network Management**	
15.1	Update Management	3.3 Explain common scanning, monitoring and patching processes and summarize their expected outputs. Processes o Patch management - Rollback 4.5 Given a scenario, implement network device hardening. Upgrading firmware Patching and updates
15.2	Data Protection	3.2 Compare and contrast business continuity and disaster recovery concepts. Recovery o Cold sites o Warm sites o Hot sites o Backups - Full o Backups - Differential o Backups - Incremental Snapshots

15.3	Remote Management	3.4 Given a scenario, use remote access methods. VNC 3.5 Identify policies and best practices. Remote access policies
15.4	Mobile Device Management	3.5 Identify policies and best practices. On-boarding/off-boarding procedures Remote access policies BYOD
15.5	Data Center Management	3.1 Given a scenario, use appropriate documentation and diagrams to manage the network. Labeling 3.2 Compare and contrast business continuity and disaster recovery concepts. Availability concepts o Power management - Battery backups/UPS o Power management - Power generators o Power management - Dual power supplies o Power management - Redundant circuits
15.6	Monitoring	3.3 Explain common scanning, monitoring and patching processes and summarize their expected outputs. Processes o Log reviewing o Packet/traffic analysis Event management o Notifications o Alerts Metrics o Error rate o Utilization o Packet drops

		o Bandwidth/throughput 5.2 Given a scenario, use the appropriate tool. Software tools o Packet sniffer o Protocol analyzer
15.7	Log File Management	3.3 Explain common scanning, monitoring and patching processes and summarize their expected outputs. Processes o Log reviewing
15.8	Network Management with SNMP	3.3 Explain common scanning, monitoring and patching processes and summarize their expected outputs. Event management o Notifications o Alerts SNMP monitors o MIB
16.0	**Network Optimization**	
16.1	Optimization	1.3 Explain the concepts and characteristics of routing and switching. Properties of network traffic o Broadcast domains o Collision domains Performance concepts o Traffic shaping o QoS o Diffserv o CoS 2.3 Explain the purposes and use cases for advanced networking devices.

		Load balancer 3.2 Compare and contrast business continuity and disaster recovery concepts. Availability concepts o Fault tolerance o High availability o NIC teaming o Port aggregation 4.6 Explain common mitigation techniques and their purposes. Network segmentation o VLAN o DMZ
16.2	Troubleshooting Methodology	1.8 Explain the functions of network services. DHCP service o TTL 5.1 Explain the network troubleshooting methodology. Identify the problem o Gather information o Duplicate the problem, if possible o Question users o Identify symptoms o Determine if anything has changed o Approach multiple problems individually Establish a theory of probable cause o Question the obvious o Consider multiple approaches - Top-to-bottom/bottom-to-top OSI model o Consider multiple approaches - Divide and conquer Test the theory to determine the cause o Once the theory is confirmed, determine the next steps to resolve the problem o If the theory is not confirmed, reestablish a new theory or escalate Establish a plan of action to resolve the problem and identify potential effects Implement the solution or escalate as necessary

		Verify full system functionality and, if applicable, implement preventive measures Document findings, actions, and outcomes 5.2 Given a scenario, use the appropriate tool. Software tools o Command line - ping o Command line - tracert, traceroute o Command line - nslookup o Command line - pathping
A.0	**Network Pro Practice Exams**	
A.1	Preparing for Network Pro Certification	
A.2	Network Pro Question Review	
B.0	**Network+ Practice Exams**	
B.1	Preparing for Network+ Certification	
B.2	Network+ Question Review (20 Random Questions)	
B.3	Network+ Question Review (All Questions)	

Objective Mapping: CompTIA N10-007 Objective to TestOut Section

#	Domain	Section
1.0	**Networking Concepts**	
1.1	Explain the purposes and uses of ports and protocols. Protocols and ports o SSH 22 o DNS 53 o SMTP 25 o SFTP 22 o FTP 20, 21 o TFTP 69 o TELNET 23 o DHCP 67, 68 o HTTP 80 o HTTPS 443 o SNMP 161 o RDP 3389 o NTP 123 o SIP 5060, 5061 o SMB 445 o POP 110 o IMAP 143 o LDAP 389 o LDAPS 636 o H.323 1720 Protocol types o ICMP o UDP o TCP o IP Connection-oriented vs. connectionless	1.4 8.1
1.2	Explain devices, applications, protocols and services at their appropriate OSI layers. Layer 1 – Physical Layer 2 – Data link Layer 3 – Network	1.3

	Layer 4 – Transport Layer 5 – Session Layer 6 – Presentation Layer 7 – Application	
1.3	Explain the concepts and characteristics of routing and switching. Properties of network traffic o Broadcast domains o CSMA/CD o CSMA/CA o Collision domains o Protocol data units o MTU o Broadcast o Multicast o Unicast Segmentation and interface properties o VLANs o Trunking (802.1q) o Tagging and untagging ports o Port mirroring o Switching loops/spanning tree o PoE and PoE+ (802.3af, 802.3at) o DMZ o MAC address table o ARP table Routing o Routing protocols (IPv4 and IPv6) - Distance-vector routing protocols (RIP, EIGRP) o Routing protocols (IPv4 and IPv6) - Link-state routing protocols (OSPF) o Routing protocols (IPv4 and IPv6) - Hybrid (BGP) o Routing types - Default - Static - Dynamic IPv6 concepts o Addressing o Tunneling o Dual stack o Router advertisement o Neighbor discovery Performance concepts o Traffic shaping o QoS o Diffserv	4.1 5.1, 5.6, 5.7, 5.9 6.3, 6.4, 6.5, 6.6, 6.7 7.1, 7.2, 7.3 8.1, 8.3 9.2, 9.4 10.1 11.1 16.1

	o CoS NAT/PAT Port forwarding Access control list Distributed switching Packet-switched vs. circuit-switched network Software-defined networking	
1.4	Given a scenario, configure the appropriate IP addressing components. Private vs. public Loopback and reserved Default gateway Virtual IP Subnet mask Subnetting o Classful (Classes A, B, C, D, and E) o Classless (VLSM, CIDR notation (IPv4 vs. IPv6)) Address assignments o DHCP o DHCPv6 o Static o IP reservations o EUI64 o APIPA	5.1, 5.2, 5.3, 5.6 7.2, 7.3
1.5	Compare and contrast the characteristics of network topologies, types and technologies. Wired topologies o Logical vs. physical o Star o Ring o Mesh o Bus Wireless topologies o Mesh o Ad hoc o Infrastructure Types o LAN o MAN	1.1, 1.2 4.4 9.1 10.1, 10.2, 10.4

	o WAN o CAN o PAN o WLAN o SAN Technologies that facilitate the Internet of Things (IoT) o Z-Wave o Ant+ o Bluetooth o NFC o IR o RFID o 802.11	
1.6	Given a scenario, implement the appropriate wireless technologies and configurations. 802.11 standards o a o b o g o n o ac Cellular o GSM o TDMA o CDMA Frequencies o 2.4GHz o 5.0GHz Speed and distance requirements Channel bandwidth Channel bonding MIMO/MU-MIMO Unidirectional/ omnidirectional Site survey	10.2, 10.4 11.3
1.7	Summarize cloud concepts and their purposes. Types of services o SaaS o PaaS	9.5 12.1

	o IaaS Cloud delivery models o Private o Public o Hybrid Connectivity methods Security implications/ considerations Relationship between local and cloud resources	
1.8	Explain the functions of network services. DNS service o Record types - A, AAA o Record types - TXT (SPF, DKIM) o Record types - SRV o Record types - MX o Record types - CNAME o Record types - NS o Record types - PTR o Internal vs. external DNS o Third-party/cloud-hosted DNS o Hierarchy o Forward vs. reverse zone DHCP service o MAC reservations o Pools o IP exclusions o Scope options o Lease time o TTL o DHCP relay/IP helper NTP IPAM	1.4 5.3, 5.4, 5.5, 5.6 16.2
2.0	**Infrastructure**	
2.1	Given a scenario, deploy the appropriate cabling solution. Media types o Copper - UTP	2.1, 2.2, 2.3, 2.4 3.1 4.1, 4.2, 4.3

- Copper - STP
- Copper - Coaxial
- Fiber - Single-mode
- Fiber - Multimode

Plenum vs. PVC

Connector types

- Copper - RJ-45
- Copper - RJ-11
- Copper - BNC
- Copper - DB-9
- Copper - DB-25
- Copper - F-type
- Fiber - LC
- Fiber - ST
- Fiber - SC - APC
- Fiber - SC - UPC
- Fiber - SC - MTRJ

Transceivers

- SFP
- GBIC
- SFP+
- QSFP
- Characteristics of fiber transceivers - Bidirectional
- Characteristics of fiber transceivers - Duplex

Termination points

- 66 block
- 110 block
- Patch panel
- Fiber distribution panel

Copper cable standards

- Cat 3
- Cat 5
- Cat 5e
- Cat 6
- Cat 6a
- Cat 7
- RG-6
- RG-59

Copper termination standards

- Crossover
- Straight-through
- TIA/EIA 568a
- TIA/EIA 568b

	Ethernet deployment standards o 100BaseT o 1000BaseT o 1000BaseLX o 1000BaseSX o 10GBaseT	
2.2	Given a scenario, determine the appropriate placement of networking devices on a network and install/configure them. Firewall Router Switch Hub Bridge Modems Wireless access point Media converter Wireless range extender VoIP endpoint	2.3 3.1, 3.2, 3.3 8.1, 8.2, 8.3 9.2 10.3, 10.4, 10.5
2.3	Explain the purposes and use cases for advanced networking devices. Multilayer switch Wireless controller Load balancer IDS/IPS Proxy server VPN concentrator AAA/RADIUS server UTM appliance NGFW/Layer 7 firewall VoIP PBX VoIP gateway Content filter	3.3 8.1, 8.2, 8.3 9.2 10.3, 10.4, 10.5, 10.6 11.4 13.7 14.1 16.1
2.4	Explain the purposes of virtualization and network storage technologies. Virtual networking components o Virtual switch	9.1, 9.2, 9.4

	o Virtual firewall o Virtual NIC o Virtual router o Hypervisor Network storage types o NAS o SAN Connection type o FCoE o Fibre Channel o iSCSI o InfiniBand Jumbo frame	
2.5	Compare and contrast WAN technologies. Service type o ISDN o T1/T3 o E1/E3 o OC-3 o OC-192 o DSL o Metropolitan Ethernet o Cable broadband o PRI o Dial-up Transmission mediums o Satellite o Copper o Fiber o Wireless Characteristics of service o MPLS o ATM o Frame relay o PPPoE o PPP o DMVPN o SIP trunk Termination o Demarcation point	2.4, 2.5 10.1 11.1, 11.2, 11.3, 11.4 13.7

	o CSU/DSU o Smart jack	
3.0	**Network Operations**	
3.1	Given a scenario, use appropriate documentation and diagrams to manage the network. Diagram symbols Standard operating procedures/work instructions Logical vs. physical diagrams Rack diagrams Change management documentation Wiring and port locations IDF/MDF documentation Labeling Network configuration and performance baselines Inventory management	2.4 12.1, 12.2 15.5
3.2	Compare and contrast business continuity and disaster recovery concepts. Availability concepts o Fault tolerance o High availability o NIC teaming o Load balancing o Port aggregation o Clustering o Power management - Battery backups/UPS o Power management - Power generators o Power management - Dual power supplies o Power management - Redundant circuits Recovery o Cold sites o Warm sites o Hot sites o Backups - Full o Backups - Differential o Backups - Incremental o Snapshots MTTR	9.1 12.1, 12.3 15.2, 15.5 16.1

	MTBF SLA requirements	
3.3	Explain common scanning, monitoring and patching processes and summarize their expected outputs. Processes o Log reviewing o Port scanning o Vulnerability scanning o Patch management - Rollback o Reviewing baselines o Packet/traffic analysis Event management o Notifications o Alerts o SIEM SNMP monitors o MIB Metrics o Error rate o Utilization o Packet drops o Bandwidth/throughput	12.1 14.1 15.1, 15.6, 15.7, 15.8
3.4	Given a scenario, use remote access methods. VPN o IPSec o SSL/TLS/DTLS o Site-to-site o Client-to-site RDP SSH VNC Telnet HTTPS/management URL Remote file access o FTP/FTPS o SFTP o TFTP Out-of-band management	1.4 2.2 6.1 13.6, 13.7 14.3 15.3

	o Modem o Console router	
3.5	Identify policies and best practices. Privileged user agreement Password policy On-boarding/off-boarding procedures Licensing restrictions International export controls Data loss prevention Remote access policies Incident response policies BYOD AUP NDA System life cycle o Asset disposal Safety procedures and policies	11.4 12.1, 12.2, 12.3 15.3, 15.4
4.0	**Network Security**	
4.1	Summarize the purposes of physical security devices. Detection o Motion detection o Video surveillance o Asset tracking tags o Tamper detection Prevention o Badges o Biometrics o Smart cards o Key fob o Locks	13.1
4.2	Explain authentication and access controls. Authorization, authentication and accounting	1.4 8.3

	o RADIUS o TACACS+ o Kerberos o Single sign-on o Auditing and logging o Certificates o Local authentication o LDAP Multifactor authentication o Something you know o Something you have o Something you are o Somewhere you are o Something you do Access control o 802.1x o NAC o Port security o MAC filtering o Captive portal o Access control list	10.6 11.4 13.5, 13.8 14.3
4.3	Given a scenario, secure a basic wireless network. WPA WPA2 TKIP-RC4 CCMP-AES Authentication and authorization o EAP - PEAP o EAP - EAP-FAST o EAP - EAP-TLS o Shared or open o Preshared key o MAC filtering Geofencing	10.6 13.5
4.4	Summarize common networking attacks. DoS o Reflective	10.6 13.2, 13.3, 13.4, 13.6, 13.8

	o Amplified o Distributed Social engineering Insider threat Logic bomb Rogue access point Evil twin War-driving Phishing Ransomware DNS poisoning ARP poisoning Spoofing Deauthentication Brute force VLAN hopping Man-in-the-middle Exploits vs. vulnerabilities	
4.5	Given a scenario, implement network device hardening. Changing default credentials Avoiding common passwords Upgrading firmware Patching and updates File hashing Disabling unnecessary services Using secure protocols Generating new keys Disabling unused ports o IP ports o Device ports (physical and virtual)	13.4, 13.6, 13.8 14.1, 14.3 15.1
4.6	Explain common mitigation techniques and their purposes. Signature management Device hardening Change native VLAN Switch port protection o Spanning tree o DHCP snooping	6.5 8.1 12.2, 12.3 13.5, 13.6 14.1, 14.2, 14.3

	o Flood guard o BPDU guard o Root guard Network segmentation o VLAN o DMZ Privileged user account File integrity monitoring Role separation Restricting access via ACLs Honeypot/honeynet Penetration testing	16.1
5.0	**Network Troubleshooting and Tools**	
5.1	Explain the network troubleshooting methodology. Identify the problem o Gather information o Duplicate the problem, if possible o Question users o Identify symptoms o Determine if anything has changed o Approach multiple problems individually Establish a theory of probable cause o Question the obvious o Consider multiple approaches - Top-to-bottom/bottom-to-top OSI model o Consider multiple approaches - Divide and conquer Test the theory to determine the cause o Once the theory is confirmed, determine the next steps to resolve the problem o If the theory is not confirmed, reestablish a new theory or escalate Establish a plan of action to resolve the problem and identify potential effects Implement the solution or escalate as necessary Verify full system functionality and, if applicable, implement preventive measures Document findings, actions, and outcomes	16.2
5.2	Given a scenario, use the appropriate tool. Hardware tools o Crimper	2.5 5.8, 5.9, 5.10 8.1

	o Punchdown tool o OTDR o Multimeter o Light meter o Tone generator o Cable tester o Loopback adapter o Spectrum analyzer Software tools o Port scanner o WiFi analyzer o Packet sniffer o Protocol analyzer o Bandwidth speed tester o Command line - ping o Command line - tracert, traceroute o Command line - nslookup o Command line - pathping o Command line - netstat o Command line - arp o Command line - ifconfig o Command line - ipconfig o Command line - iptables o Command line - tcpdump o Command line - nmap o Command line - route o Command line - dig	10.4, 10.7 14.1, 14.2 15.6 16.2
5.3	Given a scenario, troubleshoot common wired connectivity and performance issues. Attenuation Latency Jitter Crosstalk EMI Open/short Incorrect pin-out Incorrect cable type Bad port Transceiver mismatch TX/RX reverse Duplex/speed mismatch	2.5 4.4 6.7 7.2, 7.4 9.2 10.5

	Damaged cables Bent pins Bottlenecks VLAN mismatch Network connection LED status indicators	
5.4	Given a scenario, troubleshoot common wireless connectivity and performance issues. Reflection Refraction Absorption Latency Jitter Attenuation Incorrect antenna type Interference Incorrect antenna placement Channel overlap Overcapacity Distance limitations Frequency mismatch Wrong SSID Wrong passphrase Security type mismatch Power levels Signal-to-noise ratio	2.5 9.2 10.2, 10.4, 10.7
5.5	Given a scenario, troubleshoot common network service issues. Names not resolving Incorrect gateway Incorrect netmask Duplicate IP addresses Duplicate MAC addresses Expired IP address Rogue DHCP server Untrusted SSL certificate Incorrect time Exhausted DHCP scope Blocked TCP/UDP ports Incorrect firewall settings	4.4 5.8, 5.9, 5.10 8.3 11.5 13.8

	Incorrect ACL settings Unresponsive service Hardware failure	