CompTIA

CertMaster Learn Network+

N10-009

OBJECTIVE MAPPING

CompTIA Network+ (N10-009) Certification Exam

Mappings

Objective Mapping

	Exam Objective	Lesson Index
1.0	Networking Concepts	
1.1	Explain concepts related to the Open Systems Interconnection (OSI) reference model.	1.2, 1.3 4.1 13.1 14.3
1.2	Compare and contrast networking appliances, applications, and functions.	1.1, 1.3 3.2 5.1, 5.4 6.5 7.2, 7.4 8.6 10.5 11.1 12.2, 12.3, 12.4 13.2 14.1, 14.2, 14.3
1.3	Summarize cloud concepts and connectivity options.	14.2, 14.3
1.4	Explain common networking ports, protocols, services, and traffic types.	4.1, 4.5 6.1, 6.2, 6.3, 6.5, 6.6 7.2, 7.3 8.3 10.2 13.2, 13.3
1.5	Compare and contrast transmission media and transceivers.	2.1, 2.2, 2.3, 2.4, 2.6 3.1 12.1 13.1 14.1
1.6	Compare and contrast network topologies, architectures, and types.	1.1 5.5 14.1

	Exam Objective	Lesson Index
1.7	Given a scenario, use appropriate IPv4 network addressing.	4.2, 4.3, 4.5 5.1 6.3
1.8	Summarize evolving use cases for modern network environments.	1.2 4.5 13.2 14.4
2.0	**Network Implementation**	
2.1	Explain characteristics of routing technologies.	5.1, 5.2, 5.3, 5.6 7.4
2.2	Given a scenario, configure switching technologies and features.	2.1 3.2, 3.3 5.1, 5.6
2.3	Given a scenario, select and configure wireless devices and technologies.	12.1, 12.2, 12.3
2.4	Explain important factors of physical installations.	2.3, 2.4, 2.5
3.0	**Network Operations**	
3.1	Explain the purpose of organizational processes and procedures.	2.5 8.1 12.2
3.2	Given a scenario, use network monitoring technologies.	8.2, 8.3, 8.4, 8.5, 8.6 10.4
3.3	Explain disaster recovery (DR) concepts.	7.4
3.4	Given a scenario, implement IPv4 and IPv6 network services.	6.2, 6.3, 6.4, 6.5, 6.6 7.1
3.5	Compare and contrast network access and management methods.	13.2, 13.3
4.0	**Network Security**	
4.1	Explain the importance of basic network security concepts.	9.1, 9.2, 9.3 10.1, 10.2, 10.3 11.1, 11.2, 11.3 12.3 13.2

	Exam Objective	Lesson Index
4.2	Summarize various types of attacks and their impact to the network.	9.2, 9.3, 9.4, 9.5 12.3, 12.4
4.3	Given a scenario, apply network security features, defense techniques, and solutions.	3.1, 3.4 10.1, 10.3, 10.4, 10.5 11.1
5.0	Network Troubleshooting	
5.1	Explain the troubleshooting methodology.	1.2, 1.4
5.2	Given a scenario, troubleshoot common cabling and physical interface issues.	2.2, 2.4, 2.6 3.1, 3.3, 3.4 7.3 12.4
5.3	Given a scenario, troubleshoot common issues with network services.	3.3, 3.4 4.4, 4.6 5.7 6.4 10.5
5.4	Given a scenario, troubleshoot common performance issues.	2.1 8.6 12.2, 12.4
5.5	Given a scenario, use the appropriate tool or protocol to solve networking issues.	2.6 3.4 4.4 5.1, 5.6 6.1, 6.4, 6.5, 6.6 7.2 8.2, 8.5, 8.6 9.3 10.3 12.4 13.3

Detailed Objective Mapping

1.0 Networking Concepts

1.1 Explain concepts related to the Open Systems Interconnection (OSI) reference model.	
Exam Objective	Course Resource
Layer 1 - Physical	1.2.1 Open Systems Interconnection Model 1.2.3 Layer 1 - Physical 1.2.8 OSI Model Summary 1.3.2 Physical Layer Functions 1.3.8 Lab: Explore a Single Location in a Lab 13.1.1 Wide Area Networks and the OSI Model
Layer 2 - Data link	1.2.1 Open Systems Interconnection Model 1.2.4 Layer 2 - Data Link 1.2.8 OSI Model Summary 1.3.3 Data Link Layer Functions 1.3.8 Lab: Explore a Single Location in a Lab 4.1.2 Layer 2 vs. Layer 3 Addressing and Forwarding 13.1.1 Wide Area Networks and the OSI Model
Layer 3 - Network	1.2.1 Open Systems Interconnection Model 1.2.5 Layer 3 - Network 1.2.8 OSI Model Summary 1.3.4 Network Layer Functions 1.3.6 The Internet 1.3.7 Binary and Hexadecimal 1.3.8 Lab: Explore a Single Location in a Lab 4.1.2 Layer 2 vs. Layer 3 Addressing and Forwarding 13.1.1 Wide Area Networks and the OSI Model 14.3.5 Cloud Firewall Security

1.1 Explain concepts related to the Open Systems Interconnection (OSI) reference model.	
Exam Objective	Course Resource
Layer 4 - Transport	1.2.1 Open Systems Interconnection Model 1.2.6 Layer 4 - Transport 1.2.8 OSI Model Summary 1.3.5 Transport and Application Layer and Security Functions 1.3.7 Binary and Hexadecimal 1.3.8 Lab: Explore a Single Location in a Lab 14.3.5 Cloud Firewall Security
Layer 5 - Session	1.2.1 Open Systems Interconnection Model 1.2.7 Upper Layers 1.2.8 OSI Model Summary 1.3.8 Lab: Explore a Single Location in a Lab
Layer 6 - Presentation	1.2.1 Open Systems Interconnection Model 1.2.7 Upper Layers 1.2.8 OSI Model Summary 1.3.8 Lab: Explore a Single Location in a Lab
Layer 7 - Application	1.2.1 Open Systems Interconnection Model 1.2.7 Upper Layers 1.2.8 OSI Model Summary 1.3.5 Transport and Application Layer and Security Functions 1.3.8 Lab: Explore a Single Location in a Lab 14.3.5 Cloud Firewall Security

1.2 Compare and contrast networking appliances, applications, and functions.	
Exam Objective	Course Resource
Physical and virtual appliances	1.1.1 Networking Concepts 1.1.2 Network Types 1.3.1 SOHO Routers 1.3.3 Data Link Layer Functions 1.3.9 Lab: Create a Home Wireless Network 3.2.2 Bridges 3.2.6 Cisco IoS Basics 3.2.9 Lab: Cisco IoS Basics 5.1.1 Routing Tables and Path Selection 5.1.4 Packet Forwarding 5.1.9 Lab: Install an Enterprise Router 5.4.1 Firewall Uses and Types 5.4.2 Firewall Selection and Placement 7.2.6 Network Attached Storage 7.4.5 Load Balancers 7.4.8 Lab: Configure NIC Teaming 10.5.1 Security Rules and ACL Configuration 11.1.7 Intrusion Detection and Prevention Systems 14.1.3 Storage Area Networks

1.2 Compare and contrast networking appliances, applications, and functions.	
Exam Objective	Course Resource
Physical and virtual appliances Router	1.3.1 SOHO Routers 1.3.2 Physical Layer Functions 1.3.3 Data Link Layer Functions 1.3.4 Network Layer Functions 1.3.5 Transport and Application Layer and Security Functions 1.3.6 The Internet 1.3.9 Lab: Create a Home Wireless Network 1.3.10 Lab: Create a SOHO Network 5.1.1 Routing Tables and Path Selection 5.1.4 Packet Forwarding 5.1.5 Fragmentation 5.1.6 Router Configuration 5.1.9 Lab: Install an Enterprise Router 10.5.9 Lab: Restrict Telnet and SSH Access 10.5.10 Lab: Permit Traffic 10.5.11 Lab: Block Source Hosts
Physical and virtual appliances Switch	1.3.3 Data Link Layer Functions 3.2.1 Hubs 3.2.3 Switches 3.2.4 Ethernet Switch Types 3.2.5 Switch Interface Configuration 3.2.7 Lab: Install a Switch in the Rack 3.2.8 Lab: Secure a Switch
Physical and virtual appliances Firewall	1.3.5 Transport and Application Layer and Security Functions 5.4.1 Firewall Uses and Types 5.4.2 Firewall Selection and Placement 10.5.1 Security Rules and ACL Configuration 10.5.4 Misconfigured Firewall and ACL Issues 10.5.5 Creating Firewall ACLs 10.5.7 Lab: Configure a Security Appliance 10.5.8 Lab: Configure a Perimeter Firewall 14.3.5 Cloud Firewall Security

1.2 Compare and contrast networking appliances, applications, and functions.	
Exam Objective	Course Resource
Physical and virtual appliances Intrusion detection system (IDS) / intrusion prevention system (IPS)	11.1.7 Intrusion Detection and Prevention Systems 11.1.8 Implementing Intrusion Detection and Prevention 11.1.9 Lab: Implement Intrusion Prevention
Physical and virtual appliances Load balancer	7.4.5 Load Balancers 7.4.8 Lab: Configure NIC Teaming
Physical and virtual appliances Proxy	10.5.2 Proxy Servers
Physical and virtual appliances Network-attached storage (NAS)	7.2.5 Server Message Block 7.2.6 Network Attached Storage
Physical and virtual appliances Storage area network (SAN)	14.1.3 Storage Area Networks 14.1.4 Fibre Channel 14.1.5 Lab: Configure an iSCSI Target 14.1.6 Lab: Configure an iSCSI Initiator
Physical and virtual appliances Wireless	1.3.9 Lab: Create a Home Wireless Network 1.3.10 Lab: Create a SOHO Network 12.2.8 Lab: Design an Indoor Wireless Network 12.2.9 Lab: Design an Outdoor Wireless Network 12.2.10 Lab: Implement an Enterprise Wireless Network 12.3.3 Enterprise Authentication 12.3.9 Lab: Secure an Enterprise Wireless Network 12.3.10 Lab: Secure a Home Wireless Network 12.4.9 Lab: Optimize a Wireless Network
Physical and virtual appliances *Wireless* Access point (AP)	12.2.8 Lab: Design an Indoor Wireless Network 12.2.9 Lab: Design an Outdoor Wireless Network 12.2.10 Lab: Implement an Enterprise Wireless Network 12.3.10 Lab: Secure a Home Wireless Network
Physical and virtual appliances *Wireless* Controller	12.2.5 Wireless Controllers 12.2.10 Lab: Implement an Enterprise Wireless Network 12.3.3 Enterprise Authentication 12.3.9 Lab: Secure an Enterprise Wireless Network 12.4.9 Lab: Optimize a Wireless Network
Applications	1.1.1 Networking Concepts 14.2.4 Content Delivery Networks

1.2 Compare and contrast networking appliances, applications, and functions.	
Exam Objective	Course Resource
Applications Content delivery network (CDN)	14.2.4 Content Delivery Networks
Functions	1.1.1 Networking Concepts 5.1.4 Packet Forwarding
Functions Virtual private network (VPN)	13.2.2 Tunneling Protocols 13.2.8 Lab: Configure a Remote Access VPN 13.2.9 Lab: Configure an iPad VPN Connection 13.2.10 Lab: Configure a RADIUS Solution
Functions Quality of service (QoS)	8.6.1 Common Performance Issues 8.6.6 Traffic Shaping
Functions Time to live (TTL)	5.1.4 Packet Forwarding 6.5.8 DNS Server Configuration

1.3 Summarize cloud concepts and connectivity options.	
Exam Objective	Course Resource
Network functions virtualization (NFV)	14.3.1 Cloud Instances
Virtual private cloud (VPC)	14.3.2 Virtual Private Clouds 14.3.3 Cloud Gateways 14.3.4 Cloud Connectivity Options
Network security groups	14.3.6 Security Groups and Security Lists
Network security lists	14.3.6 Security Groups and Security Lists
Cloud gateways	14.3.3 Cloud Gateways 14.3.4 Cloud Connectivity Options
Cloud gateways Internet gateway	14.3.3 Cloud Gateways 14.3.4 Cloud Connectivity Options
Cloud gateways Network address translation (NAT) gateway	14.3.3 Cloud Gateways 14.3.4 Cloud Connectivity Options
Cloud connectivity options	14.3.4 Cloud Connectivity Options

1.3 Summarize cloud concepts and connectivity options.	
Exam Objective	Course Resource
Cloud connectivity options VPN	14.3.4 Cloud Connectivity Options
Cloud connectivity options Direct Connect	14.3.4 Cloud Connectivity Options
Deployment models	14.2.2 Cloud Deployment Models
Deployment models Public	14.2.2 Cloud Deployment Models
Deployment models Private	14.2.2 Cloud Deployment Models
Deployment models Hybrid	14.2.2 Cloud Deployment Models
Service models	14.2.3 Cloud Service Models
Service models Software as a service (SaaS)	14.2.3 Cloud Service Models
Service models Infrastructure as a service (IaaS)	14.2.3 Cloud Service Models
Service models Platform as a service (PaaS)	14.2.3 Cloud Service Models
Scalability	14.2.1 Cloud Scalability and Elasticity
Elasticity	14.2.1 Cloud Scalability and Elasticity
Multitenancy	14.2.2 Cloud Deployment Models

1.4 Explain common networking ports, protocols, services, and traffic types.	
Exam Objective	Course Resource
Protocols and Ports	6.1.1 Transport Layer Ports and Connections 6.1.6 Common TCP and UDP Ports 7.2.1 Hyper Text Transfer Protocol 7.2.2 HTTP Secure 7.2.3 File Transfer Protocol 7.2.4 Secure File Transfer Protocol 7.2.7 Database Services 7.2.8 Lab: Verify Secure Web Services 7.3.1 Simple Mail Transfer Protocol 7.3.2 Internet Message Access Protocol 7.3.3 Voice and Video Services 7.3.4 VoIP Protocols 7.3.5 VoIP Phones 7.3.6 Lab: Connect VoIP 1 7.3.7 Lab: Connect VoIP 2
Protocols and Ports File Transfer Protocol (FTP) - 20/21	6.1.6 Common TCP and UDP Ports 7.2.3 File Transfer Protocol 7.2.4 Secure File Transfer Protocol
Protocols and Ports Secure File Transfer Protocol (SFTP) - 22	6.1.6 Common TCP and UDP Ports 7.2.4 Secure File Transfer Protocol
Protocols and Ports Secure Shell (SSH) - 22	6.1.6 Common TCP and UDP Ports 13.3.1 Remote Host Access 13.3.2 Secure Shell
Protocols and Ports Telnet - 23	6.1.6 Common TCP and UDP Ports 13.3.3 Telnet
Protocols and Ports Simple Mail Transfer Protocol (SMTP) - 25	6.1.6 Common TCP and UDP Ports 7.3.1 Simple Mail Transfer Protocol 7.3.2 Internet Message Access Protocol
Protocols and Ports Domain Name System (DNS) - 53	6.1.6 Common TCP and UDP Ports 6.5.1 Host Names and Domain Names 6.5.8 DNS Server Configuration

1.4 Explain common networking ports, protocols, services, and traffic types.	
Exam Objective	Course Resource
Protocols and Ports Dynamic Host Configuration Protocol (DHCP) - 67/68	6.1.6 Common TCP and UDP Ports 6.2.1 DHCP Process 6.2.2 DHCP Server Configuration
Protocols and Ports Trivial File Transfer Protocol (TFTP) - 69	6.1.6 Common TCP and UDP Ports 7.2.3 File Transfer Protocol
Protocols and Ports Hypertext Transfer Protocol (HTTP) - 80	6.1.6 Common TCP and UDP Ports 7.2.1 Hyper Text Transfer Protocol
Protocols and Ports Network Time Protocol (NTP) - 123	6.1.6 Common TCP and UDP Ports
Protocols and Ports Simple Network Management Protocol (SNMP) -161/162	6.1.6 Common TCP and UDP Ports 8.3.1 SNMP Agents and Monitors 8.3.2 SNMP Security 8.3.3 Configuring an SNMP System on a Router
Protocols and Ports Lightweight Directory Access Protocol (LDAP) - 389	6.1.6 Common TCP and UDP Ports 10.2.3 Lightweight Directory Access Protocol 10.2.5 Lab: Manage Account Policies
Protocols and Ports Hypertext Transfer Protocol Secure (HTTPS) - 443	6.1.6 Common TCP and UDP Ports 7.2.2 HTTP Secure 7.2.9 Lab: Scan for Web Services with Nmap 7.3.2 Internet Message Access Protocol
Protocols and Ports Server Message Block (SMB) - 445	6.1.6 Common TCP and UDP Ports 7.2.5 Server Message Block
Protocols and Ports Syslog - 514	6.1.6 Common TCP and UDP Ports
Protocols and Ports Simple Mail Transfer Protocol Secure (SMTPS) - 587	6.1.6 Common TCP and UDP Ports 7.3.1 Simple Mail Transfer Protocol
Protocols and Ports Lightweight Directory Access Protocol over SSL (LDAPS) - 636	6.1.6 Common TCP and UDP Ports 10.2.4 LDAP Secure 10.2.5 Lab: Manage Account Policies

1.4 Explain common networking ports, protocols, services, and traffic types.	
Exam Objective	Course Resource
Protocols and Ports Structured Query Language (SQL) Server - 1433	6.1.6 Common TCP and UDP Ports 7.2.7 Database Services
Protocols and Ports Remote Desktop Protocol (RDP) - 3389	6.1.6 Common TCP and UDP Ports 13.3.1 Remote Host Access 13.3.4 Remote Desktop Protocol 13.3.8 Lab: Allow Remote Desktop Connections
Protocols and Ports Session Initiation Protocol (SIP) - 5060/5061	6.1.6 Common TCP and UDP Ports 7.3.4 VoIP Protocols 7.3.5 VoIP Phones
Internet Protocol (IP) types	4.1.1 IPv4 Datagram Header 4.1.2 Layer 2 vs. Layer 3 Addressing and Forwarding 4.1.3 Address Resolution Protocol 4.1.6 Lab: Explore Packets and Frames 4.1.7 Lab: Explore ARP in Wireshark 6.1.2 Transmission Control Protocol 6.1.3 TCP Handshake and Teardown 6.1.4 User Datagram Protocol 6.1.7 Lab: Explore Three-way Handshake in Wireshark 13.2.4 Internet Key Exchange
Internet Protocol (IP) types Internet Control Message Protocol (ICMP)	4.1.1 IPv4 Datagram Header 6.3.2 IPv6 Interface Autoconfiguration and Testing 6.6.1 Client DNS Issues
Internet Protocol (IP) types Transmission Control Protocol (TCP)	6.1.2 Transmission Control Protocol 6.1.3 TCP Handshake and Teardown 6.1.7 Lab: Explore Three-way Handshake in Wireshark
Internet Protocol (IP) types User Datagram Protocol (UDP)	6.1.4 User Datagram Protocol 6.1.6 Common TCP and UDP Ports
Internet Protocol (IP) types Generic Routing Encapsulation (GRE)	13.2.2 Tunneling Protocols
Internet Protocol (IP) types Internet Protocol Security (IPSec)	13.2.2 Tunneling Protocols 13.2.3 Internet Protocol Security

1.4 Explain common networking ports, protocols, services, and traffic types.	
Exam Objective	Course Resource
Internet Protocol (IP) types *Internet Protocol Security (IPSec)* Authentication Header (AH)	13.2.3 Internet Protocol Security
Internet Protocol (IP) types *Internet Protocol Security (IPSec)* Encapsulating Security Payload (ESP)	13.2.2 Tunneling Protocols 13.2.3 Internet Protocol Security
Internet Protocol (IP) types *Internet Protocol Security (IPSec)* Internet Key Exchange (IKE)	13.2.2 Tunneling Protocols 13.2.4 Internet Key Exchange
Traffic types	4.1.4 Unicast and Broadcast Addressing 4.1.5 Multicast and Anycast Addressing
Traffic types Unicast	4.1.4 Unicast and Broadcast Addressing 4.5.4 IPv6 Unicast Addressing
Traffic types Multicast	4.1.5 Multicast and Anycast Addressing 4.5.6 IPv6 Multicast and Anycast Addressing
Traffic types Anycast	4.1.5 Multicast and Anycast Addressing 4.5.6 IPv6 Multicast and Anycast Addressing
Traffic types Broadcast	4.1.4 Unicast and Broadcast Addressing

1.5 Compare and contrast transmission media and transceivers.	
Exam Objective	Course Resource
Wireless	12.1.1 IEEE 802.11 Wireless Standards 12.1.2 IEEE 802.11a and 5GHz Channel Bandwidth 12.1.4 IEEE 802.11n, MIMO, and Channel Bonding 12.1.6 Multiuser MIMO and Band Steering 12.1.7 Cellular Technologies 12.1.8 Satellite Technologies 12.1.9 Lab: Configure Wireless Profiles

1.5 Compare and contrast transmission media and transceivers.	
Exam Objective	Course Resource
Wireless 802.11 standards	12.1.1 IEEE 802.11 Wireless Standards 12.1.2 IEEE 802.11a and 5GHz Channel Bandwidth 12.1.4 IEEE 802.11n, MIMO, and Channel Bonding 12.1.6 Multiuser MIMO and Band Steering
Wireless Cellular	12.1.7 Cellular Technologies
Wireless Satellite	12.1.8 Satellite Technologies
Wired	2.1.1 Network Data Transmission 2.1.2 Ethernet Standards 2.1.6 Fiber Ethernet Standards 2.1.8 Lab: Reconnect to an Ethernet Network 2.2.1 Unshielded Twisted Pair Cable 2.2.3 Cat Cable Standards 2.2.8 Lab: Connect a Cable Modem 2.4.1 Fiber Optic Cable Considerations 2.4.8 Lab: Connect Fiber Optic Cables 2.6.10 Lab: Explore Physical Connectivity 1 2.6.11 Lab: Explore Physical Connectivity 2 13.1.2 Internet Access Types 13.1.3 Fiber to the Curb and Fiber to the Premises
Wired 802.3 standards	2.1.2 Ethernet Standards
Wired Single-mode vs. multimode fiber	2.1.6 Fiber Ethernet Standards 2.4.2 Single Mode Fiber and Multimode Fiber
Wired Direct attach copper (DAC) cable	2.2.6 Coaxial and Twinaxial Cable and Connectors 3.1.2 Modular Transceivers
Wired *Direct attach copper (DC) cable* Twinaxial cable	2.2.6 Coaxial and Twinaxial Cable and Connectors
Wired Coaxial cable	2.1.2 Ethernet Standards 2.2.6 Coaxial and Twinaxial Cable and Connectors

1.5 Compare and contrast transmission media and transceivers.	
Exam Objective	Course Resource
Wired Cable speeds	2.1.2 Ethernet Standards 2.1.4 100BASE-TX Fast Ethernet Standards 2.1.5 Gigabit Ethernet Standards 2.6.1 Specification and Limitations
Wired Plenum vs. non-plenum cable	2.2.5 Plenum and Riser-rated Cable
Transceivers	3.1.1 Network Interface Cards 3.1.2 Modular Transceivers 3.1.4 Transceiver Signal Strength Issues 3.1.8 Lab: Select and Install a Network Adapter 3.1.9 Lab: Connect a Media Converter 14.1.4 Fibre Channel
Transceivers Protocol	3.1.2 Modular Transceivers
Transceivers *Protocol* Ethernet	2.1.2 Ethernet Standards 2.1.3 Media Access Control and Collision Domains 2.1.4 100BASE-TX Fast Ethernet Standards 2.1.5 Gigabit Ethernet Standards 2.1.6 Fiber Ethernet Standards 2.1.8 Lab: Reconnect to an Ethernet Network 2.2.7 Lab: Connect to an Ethernet Network 3.1.2 Modular Transceivers 3.1.5 Ethernet Frame Format
Transceivers *Protocol* Fibre Channel (FC)	3.1.2 Modular Transceivers 14.1.4 Fibre Channel
Transceivers Form factors	3.1.2 Modular Transceivers
Transceivers *Form factors* Small form-factor pluggable (SFP)	3.1.2 Modular Transceivers

1.5 Compare and contrast transmission media and transceivers.	
Exam Objective	Course Resource
Transceivers *Form factors* Quad small form-factor pluggable (QSFP)	3.1.2 Modular Transceivers
Connector types	2.3.2 T568A and T568B Termination Standards 2.3.5 Termination Tools and Techniques 2.3.6 Lab: Explore Multiple Locations in a Lab 2.3.7 Lab: Connect Network Devices 2.4.3 Fiber Optic Connector Types 2.4.4 Fiber Optic Cable Installation
Connector types Subscriber connector (SC)	2.4.3 Fiber Optic Connector Types
Connector types Local connector (LC)	2.4.3 Fiber Optic Connector Types
Connector types Straight tip (ST)	2.4.3 Fiber Optic Connector Types
Connector types Multi-fiber push on (MPO)	2.4.6 Multi-Fiber Push On Connectors
Connector types Registered jack (RJ)11	2.2.4 Twisted Pair Connector Types
Connector types RJ45	2.2.4 Twisted Pair Connector Types
Connector types F-type	2.2.6 Coaxial and Twinaxial Cable and Connectors
Connector types Bayonet Neill–Concelman (BNC)	2.2.6 Coaxial and Twinaxial Cable and Connectors

1.6 Compare and contrast network topologies, architectures, and types.	
Exam Objective	Course Resource
Mesh	1.1.5 Mesh Topology
Hybrid	5.5.1 Hybrid Topology

1.6 Compare and contrast network topologies, architectures, and types.	
Exam Objective	Course Resource
Star/hub and spoke	1.1.2 Network Types 1.1.3 Network Topology 1.1.4 Star Topology 1.1.7 Lab: Create Network Topologies
Spine and leaf	14.1.2 Spine and Leaf Topology
Point to point	1.1.3 Network Topology 1.1.7 Lab: Create Network Topologies
Three-tier hierarchical model	1.1.2 Network Types 5.5.2 Three-Tiered Network Hierarchy 5.5.4 Lab: Create a Three-tier Network
Three-tier hierarchical model Core	5.5.2 Three-Tiered Network Hierarchy 5.5.4 Lab: Create a Three-tier Network
Three-tier hierarchical model Distribution	5.5.2 Three-Tiered Network Hierarchy 5.5.4 Lab: Create a Three-tier Network
Three-tier hierarchical model Access	5.5.2 Three-Tiered Network Hierarchy 5.5.4 Lab: Create a Three-tier Network
Collapsed core	5.5.2 Three-Tiered Network Hierarchy
Traffic flows	14.1.1 Data Center Network Design
Traffic flows North-south	14.1.1 Data Center Network Design
Traffic flows East-west	14.1.1 Data Center Network Design

1.7 Given a scenario, use appropriate IPv4 network addressing.	
Exam Objective	Course Resource
Public vs. private	4.3.1 Classful Addressing 4.3.2 Public vs Private Addressing 4.3.3 Other Reserved Address Ranges 4.3.4 IPv4 Address Scheme Design

1.7 Given a scenario, use appropriate IPv4 network addressing.	
Exam Objective	Course Resource
Public vs. private Automatic private IP Addressing (APIPA)	4.5.5 IPv6 Link Local Addressing 6.3.1 Automatic Private IP Addressing 6.3.4 Lab: Explore APIPA Addressing 6.3.5 Lab: Explore APIPA Addressing in Network Modeler 6.3.6 Set Up Alternate Addressing
Public vs. private RFC1918	4.3.1 Classful Addressing 4.3.2 Public vs Private Addressing
Public vs. private Loopback/localhost	4.3.1 Classful Addressing 4.3.3 Other Reserved Address Ranges 5.1.6 Router Configuration
Subnetting	4.2.1 IPv4 Address Format 4.2.2 Network Masks 4.2.3 Subnet Masks 4.2.4 Host Address Ranges 4.2.5 Default Gateway 4.2.6 Broadcast Addresses 4.2.7 IP Interface Configuration in Windows 4.2.8 IP Interface Configuration in Linux 4.2.9 Lab: Configure IP Addresses 4.2.10 Lab: Configure IP Addresses on Mobile Devices 4.2.11 Lab: Configure IP Addresses on Linux 4.3.1 Classful Addressing 4.3.4 IPv4 Address Scheme Design 4.3.5 Classless Inter-Domain Routing 4.3.6 Variable Length Subnet Masks 4.3.7 Lab: Configure IP Networks and Subnets
Subnetting Variable Length Subnet Mask (VLSM)	4.3.1 Classful Addressing 4.3.6 Variable Length Subnet Masks
Subnettting Classless Inter-domain Routing (CIDR)	4.3.1 Classful Addressing 4.3.5 Classless Inter-Domain Routing
IPv4 address classes	4.2.1 IPv4 Address Format 4.3.1 Classful Addressing 4.3.2 Public vs Private Addressing 4.3.7 Lab: Configure IP Networks and Subnets

1.7 Given a scenario, use appropriate IPv4 network addressing.	
Exam Objective	Course Resource
IPv4 address classes Class A	4.3.1 Classful Addressing 4.3.2 Public vs Private Addressing 4.3.3 Other Reserved Address Ranges
IPv4 address classes Class B	4.3.1 Classful Addressing 4.3.2 Public vs Private Addressing
IPv4 address classes Class C	4.3.1 Classful Addressing 4.3.2 Public vs Private Addressing 4.3.3 Other Reserved Address Ranges
IPv4 address classes Class D	4.3.1 Classful Addressing 4.3.3 Other Reserved Address Ranges
IPv4 address classes Class E	4.3.1 Classful Addressing

1.8 Summarize evolving use cases for modern network environments.	
Exam Objective	Course Resource
Software-defined network (SDN) and software-defined wide area network (SD-WAN)	14.4.4 Software-Defined Networking 14.4.5 Software-Defined WAN
Software-defined network (SDN) and software-defined wide area network (SD-WAN) Application aware	14.4.4 Software-Defined Networking
Software-defined network (SDN) and software-defined wide area network (SD-WAN) Zero-touch provisioning	14.4.4 Software-Defined Networking
Software-defined network (SDN) and software-defined wide area network (SD-WAN) Transport agnostic	14.4.4 Software-Defined Networking
Software-defined network (SDN) and software-defined wide area network (SD-WAN) Central policy management	14.4.4 Software-Defined Networking

1.8 Summarize evolving use cases for modern network environments.	
Exam Objective	Course Resource
Virtual Extensible Local Area Network (VXLAN)	14.4.6 Overlay Networks
Virtual Extensible Local Area Network (VXLAN) Data center interconnect (DCI)	14.4.6 Overlay Networks
Virtual Extensible Local Area Network (VXLAN) Layer 2 encapsulation	1.2.2 Data Encapsulation and Decapsulation 14.4.6 Overlay Networks
Zero trust architecture (ZTA)	14.4.7 Zero Trust Architecture
Zero trust architecture (ZTA) Policy-based authentication	14.4.7 Zero Trust Architecture
Zero trust architecture (ZTA) Authorization	14.4.7 Zero Trust Architecture
Zero trust architecture (ZTA) Least privilege access	14.4.7 Zero Trust Architecture
Secure Access Secure Edge (SASE)/Security Service Edge (SSE)	14.4.8 Secure Access Service Edge
Infrastructure as code (IaC)	14.4.1 Infrastructure as Code
Infrastructure as code (IaC) Automation	14.4.1 Infrastructure as Code
Infrastructure as code (IaC) *Automation* Playbooks/templates/ reusable tasks	14.4.1 Infrastructure as Code
Infrastructure as code (IaC) *Automation* Configuration drift/compliance	14.4.3 Source Control
Infrastructure as code (IaC) *Automation* Upgrades	14.4.2 Uses for Infrastructure as Code
Infrastructure as code (IaC) *Automation* Dynamic inventories	14.4.2 Uses for Infrastructure as Code

1.8 Summarize evolving use cases for modern network environments.	
Exam Objective	Course Resource
Infrastructure as code (IaC) Source control	14.4.3 Source Control
Infrastructure as code (IaC) *Source control* Version control	14.4.3 Source Control
Infrastructure as code (IaC) *Source control* Central repository	14.4.3 Source Control
Infrastructure as code (IaC) *Source control* Conflict identification	14.4.3 Source Control
Infrastructure as code (IaC) *Source control* Branching	14.4.3 Source Control
IPv6 addressing	4.5.1 IPv4 vs IPv6 4.5.2 IPv6 Address Format 4.5.3 IPv6 Network Prefixes 4.5.4 IPv6 Unicast Addressing 4.5.5 IPv6 Link Local Addressing 4.5.6 IPv6 Multicast and Anycast Addressing 4.5.7 IPv4 and IPv6 Transition Mechanisms 4.5.8 Common IPv6 Address Prefixes 4.5.9 Lab: Configure an IPv6 Address
IPv6 addressing Mitigating address exhaustion	4.5.1 IPv4 vs IPv6 4.5.9 Lab: Configure an IPv6 Address
IPv6 addressing Compatibility requirements	4.5.7 IPv4 and IPv6 Transition Mechanisms 4.5.9 Lab: Configure an IPv6 Address
IPv6 addressing *Compatibility requirements* Tunneling	4.5.7 IPv4 and IPv6 Transition Mechanisms 4.5.9 Lab: Configure an IPv6 Address 13.2.2 Tunneling Protocols
IPv6 addressing *Compatibility requirements* Dual stack	4.5.7 IPv4 and IPv6 Transition Mechanisms 4.5.9 Lab: Configure an IPv6 Address

1.8 Summarize evolving use cases for modern network environments.	
Exam Objective	Course Resource
IPv6 addressing *Compatibility requirements* NAT64	4.5.7 IPv4 and IPv6 Transition Mechanisms 4.5.9 Lab: Configure an IPv6 Address

2.0 Network Implementation

2.1 Explain characteristics of routing technologies.	
Exam Objective	Course Resource
Static routing	5.1.2 Static and Default Routes 5.1.3 Routing Table Example 5.1.4 Packet Forwarding
Dynamic routing	5.1.3 Routing Table Example 5.1.4 Packet Forwarding 5.2.1 Dynamic Routing Protocols 5.2.2 Routing Information Protocol 5.2.3 Enhanced Interior Gateway Routing Protocol 5.2.4 Open Shortest Path First 5.2.5 Border Gateway Protocol
Dynamic routing Border Gateway Protocol (BGP)	5.2.1 Dynamic Routing Protocols 5.2.5 Border Gateway Protocol
Dynamic routing Enhanced Interior Gateway Routing Protocol (EIGRP)	5.2.3 Enhanced Interior Gateway Routing Protocol
Dynamic routing Open Shortest Path First (OSPF)	5.2.4 Open Shortest Path First
Route selection	5.2.1 Dynamic Routing Protocols 5.2.6 Route Selection
Route selection Administrative distance	5.2.6 Route Selection
Route selection Prefix length	5.2.6 Route Selection
Route selection Metric	5.2.1 Dynamic Routing Protocols 5.2.6 Route Selection
Address translation	5.3.1 Edge Routers 5.3.2 Network Address Translation Types 5.3.3 Port Address Translation 5.3.4 Lab: Configure NAT

2.1 Explain characteristics of routing technologies.	
Exam Objective	Course Resource
Address translation NAT	5.3.2 Network Address Translation Types 5.3.4 Lab: Configure NAT
Address translation Port address translation (PAT)	5.3.3 Port Address Translation
First Hop Redundancy Protocol (FHRP)	7.4.7 First Hop Redundancy
Virtual IP (VIP)	7.4.8 Lab: Configure NIC Teaming
Subinterfaces	5.6.1 Virtual LANs and Subnets

2.2 Given a scenario, configure switching technologies and features.	
Exam Objective	Course Resource
Virtual Local Area Network (VLAN)	5.6.1 Virtual LANs and Subnets 5.6.2 Virtual LAN IDs and Membership 5.6.7 VLAN Routing 5.6.8 Lab: Configure Switch IP and VLAN - GUI 5.6.9 Lab: Create VLANs - GUI 5.6.12 Lab: Configure Management VLAN Settings - CLI
Virtual Local Area Network (VLAN) VLAN database	5.6.2 Virtual LAN IDs and Membership
Virtual Local Area Network (VLAN) Switch Virtual Interface (SVI)	5.6.1 Virtual LANs and Subnets 5.6.7 VLAN Routing 5.6.8 Lab: Configure Switch IP and VLAN - GUI
Interface configuration	3.2.5 Switch Interface Configuration 5.6.3 Trunking and IEEE 802.1Q 5.6.4 Tagged and Untagged Ports 5.6.5 Voice VLANs 5.6.6 Default VLAN and Native VLAN 5.6.7 VLAN Routing 5.6.9 Lab: Create VLANs - GUI 5.6.10 Lab: Configure Trunking 5.6.11 Lab: Configure Switch IP Settings - CLI
Interface configuration Native VLAN	5.6.6 Default VLAN and Native VLAN

2.2 Given a scenario, configure switching technologies and features.	
Exam Objective	Course Resource
Interface configuration Voice VLAN	5.6.5 Voice VLANs
Interface configuration 802.1Q tagging	5.6.3 Trunking and IEEE 802.1Q
Interface configuration Link aggregation	3.3.1 Link Aggregation and NIC Teaming 3.3.6 Lab: Configure Port Aggregation
Interface configuration Speed	3.2.5 Switch Interface Configuration
Interface configuration Duplex	2.1.3 Media Access Control and Collision Domains 2.1.4 100BASE-TX Fast Ethernet Standards 3.2.5 Switch Interface Configuration
Spanning tree	3.3.3 Spanning Tree Protocol 3.3.4 Spanning Tree Protocol Configuration
Maximum transmission unit (MTU)	3.3.2 Maximum Transmission Unit 3.3.7 Lab: Enable Jumbo Frame Support 5.1.5 Fragmentation
Maximum transmission unit (MTU) Jumbo frames	3.3.2 Maximum Transmission Unit 3.3.7 Lab: Enable Jumbo Frame Support 5.1.5 Fragmentation

2.3 Given a scenario, select and configure wireless devices and technologies.	
Exam Objective	Course Resource
Channels	12.1.2 IEEE 802.11a and 5GHz Channel Bandwidth 12.1.3 IEEE 8021b/g and 2.4GHz Channel Bandwidth 12.1.4 IEEE 802.11n, MIMO, and Channel Bonding
Channels Channel width	12.1.3 IEEE 8021b/g and 2.4GHz Channel Bandwidth
Channels Non-overlapping channels	12.1.3 IEEE 8021b/g and 2.4GHz Channel Bandwidth

2.3 Given a scenario, select and configure wireless devices and technologies.	
Exam Objective	Course Resource
Channels Regulatory impacts	12.1.2 IEEE 802.11a and 5GHz Channel Bandwidth 12.1.3 IEEE 8021b/g and 2.4GHz Channel Bandwidth 12.1.4 IEEE 802.11n, MIMO, and Channel Bonding
Channels *Regulatory impacts* 802.11h	12.1.2 IEEE 802.11a and 5GHz Channel Bandwidth
Frequency options	12.1.2 IEEE 802.11a and 5GHz Channel Bandwidth 12.1.4 IEEE 802.11n, MIMO, and Channel Bonding 12.1.5 Wi-Fi 5 and Wi-Fi 6 12.1.6 Multiuser MIMO and Band Steering 12.1.7 Cellular Technologies 12.2.1 Infrastructure Network Type
Frequency options 2.4GHz	12.1.2 IEEE 802.11a and 5GHz Channel Bandwidth 12.1.3 IEEE 8021b/g and 2.4GHz Channel Bandwidth 12.1.4 IEEE 802.11n, MIMO, and Channel Bonding 12.1.5 Wi-Fi 5 and Wi-Fi 6 12.2.2 Range and Signal Strength
Frequency options 5GHz	12.1.2 IEEE 802.11a and 5GHz Channel Bandwidth 12.1.4 IEEE 802.11n, MIMO, and Channel Bonding 12.1.5 Wi-Fi 5 and Wi-Fi 6 12.1.7 Cellular Technologies
Frequency options 6GHz	12.1.5 Wi-Fi 5 and Wi-Fi 6 12.1.7 Cellular Technologies
Frequency options Band steering	12.1.6 Multiuser MIMO and Band Steering
Service set identifier (SSID)	12.2.1 Infrastructure Network Type 12.2.4 Wireless Roaming
Service set identifier (SSID) Basic service set identifier (BSSID)	12.2.1 Infrastructure Network Type
Service set identifier (SSID) Extended service set identifier (ESSID)	12.2.4 Wireless Roaming
Network types	12.2.1 Infrastructure Network Type 12.2.7 Other Wireless Network Types

2.3 Given a scenario, select and configure wireless devices and technologies.	
Exam Objective	Course Resource
Network types Mesh networks	12.2.7 Other Wireless Network Types
Network types Ad hoc	12.2.7 Other Wireless Network Types
Network types Point to point	12.2.7 Other Wireless Network Types
Network types Infrastructure	12.2.1 Infrastructure Network Type
Encryption	12.3.1 Wi-Fi Encryption Standards 12.3.2 Personal Authentication 12.3.3 Enterprise Authentication
Encryption Wi-Fi Protected Access 2 (WPA2)	12.3.1 Wi-Fi Encryption Standards 12.3.2 Personal Authentication 12.3.3 Enterprise Authentication
Encryption WPA3	12.3.1 Wi-Fi Encryption Standards 12.3.2 Personal Authentication 12.3.3 Enterprise Authentication
Guest networks	12.3.4 Guest Networks and Captive Portals 12.3.7 Lab: Configure a Captive Portal
Guest networks Captive portals	12.3.4 Guest Networks and Captive Portals 12.3.7 Lab: Configure a Captive Portal
Authentication	12.3.2 Personal Authentication
Authentication Pre-shared key (PSK) vs. Enterprise	12.3.2 Personal Authentication
Antennas	12.2.6 Antenna Types 12.2.8 Lab: Design an Indoor Wireless Network 12.2.9 Lab: Design an Outdoor Wireless Network
Antennas Omnidirectional vs. directional	12.2.6 Antenna Types 12.2.8 Lab: Design an Indoor Wireless Network 12.2.9 Lab: Design an Outdoor Wireless Network
Autonomous vs. lightweight access point	12.2.5 Wireless Controllers

2.4 Explain important factors of physical installations.	
Exam Objective	Course Resource
Important installation implications	2.5.1 Rack Systems
Important installation implications Locations	2.3.1 Structured Cabling System
Important installation implications *Locations* Intermediate distribution frame (IDF)	2.3.1 Structured Cabling System
Important installation implications *Locations* Main distribution frame (MDF)	2.3.1 Structured Cabling System
Important installation implications Rack size	2.5.1 Rack Systems
Important installation implications Port-side exhaust/intake	2.5.1 Rack Systems
Important installation implications Cabling	2.3.1 Structured Cabling System 2.3.4 Structured Cable Installation 2.3.6 Lab: Explore Multiple Locations in a Lab 2.3.8 Lab: Connect Patch Panel Cables 1 2.3.9 Lab: Connect Patch Panel Cables 2 2.4.4 Fiber Optic Cable Installation 2.4.7 Wavelength Division Multiplexing
Important installation implications *Cabling* Patch panel	2.3.3 Patch Panels 2.3.8 Lab: Connect Patch Panel Cables 1 2.3.9 Lab: Connect Patch Panel Cables 2
Important installation implications *Cabling* Fiber distribution panel	2.4.5 Fiber Distribution Panels
Important installation implications Lockable	2.5.1 Rack Systems
Power	2.5.2 Humidity and Temperature 2.5.3 Power Management

2.4 Explain important factors of physical installations.	
Exam Objective	Course Resource
Power Uninterruptible power supply (UPS)	2.5.3 Power Management
Power Power distribution unit (PDU)	2.5.3 Power Management
Power Power load	2.5.3 Power Management
Power Voltage	2.5.3 Power Management
Environmental factors	2.5.1 Rack Systems 2.5.2 Humidity and Temperature 2.5.4 Fire Suppression
Environmental factors Humidity	2.5.2 Humidity and Temperature
Environmental factors Fire suppression	2.5.4 Fire Suppression
Environmental factors Temperature	2.5.1 Rack Systems 2.5.2 Humidity and Temperature

3.0 Network Operations

3.1 Explain the purpose of organizational processes and procedures.	
Exam Objective	Course Resource
Documentation	8.1.7 Physical Network Diagrams 8.1.8 Logical Network Diagrams 8.1.10 Common Agreements 12.2.3 Wireless Surveys and Heat Maps
Documentation Physical vs. logical diagrams	8.1.7 Physical Network Diagrams
Documentation Rack diagrams	2.5.1 Rack Systems 8.1.7 Physical Network Diagrams
Documentation Cable maps and diagrams	8.1.7 Physical Network Diagrams
Documentation Network diagrams	8.1.8 Logical Network Diagrams
Documentation *Network diagrams* Layer 1	8.1.8 Logical Network Diagrams
Documentation *Network diagrams* Layer 2	8.1.8 Logical Network Diagrams
Documentation *Network diagrams* Layer 3	8.1.8 Logical Network Diagrams
Documentation Asset inventory	8.1.4 Asset Inventory Documentation
Documentation *Asset inventory* Hardware	8.1.4 Asset Inventory Documentation
Documentation *Asset inventory* Software	8.1.4 Asset Inventory Documentation

3.1 Explain the purpose of organizational processes and procedures.	
Exam Objective	Course Resource
Documentation *Asset inventory* Licensing	8.1.4 Asset Inventory Documentation
Documentation *Asset inventory* Warranty support	8.1.4 Asset Inventory Documentation
Documentation IP address management (IPAM)	8.1.9 IP Address Management
Documentation Service-level agreement (SLA)	8.1.10 Common Agreements
Documentation Wireless survey/heat map	12.2.3 Wireless Surveys and Heat Maps
Life-cycle management	8.1.5 Lifecycle Management 8.1.6 Decommissioning 8.1.11 Lab: Update Firmware
Life-cycle management End-of-life (EOL)	8.1.5 Lifecycle Management
Life-cycle management End-of-support (EOS)	8.1.5 Lifecycle Management
Life-cycle management Software management	8.1.5 Lifecycle Management
Life-cycle management *Software management* Patches and bug fixes	8.1.5 Lifecycle Management
Life-cycle management *Software management* Operating system (OS)	8.1.5 Lifecycle Management
Life-cycle management *Software management* Firmware	8.1.5 Lifecycle Management 8.1.11 Lab: Update Firmware
Life-cycle management Decommissioning	8.1.6 Decommissioning

3.1 Explain the purpose of organizational processes and procedures.	
Exam Objective	Course Resource
Change management	8.1.1 Configuration Management 8.1.3 Change Management
Change management Request process tracking/service request	8.1.3 Change Management
Configuration management	8.1.1 Configuration Management 8.1.2 Network Device Backup Management
Configuration management Production configuration	8.1.1 Configuration Management
Configuration management Backup configuration	8.1.1 Configuration Management 8.1.2 Network Device Backup Management
Configuration management Baseline/golden configuration	8.1.1 Configuration Management

3.2 Given a scenario, use networking monitoring technologies.	
Exam Objective	Course Resource
Methods	8.2.1 Network Discovery 8.3.1 SNMP Agents and Monitors 8.3.2 SNMP Security 8.3.3 Configuring an SNMP System on a Router 8.3.4 Monitoring a Switch with SNMP 8.4.4 Security Information and Event Management
Methods SNMP	8.2.1 Network Discovery 8.3.1 SNMP Agents and Monitors 8.3.2 SNMP Security 8.3.3 Configuring an SNMP System on a Router 8.3.4 Monitoring a Switch with SNMP 8.3.5 Configuring SNMP Trap
Methods *SNMP* Traps	8.3.1 SNMP Agents and Monitors 8.3.4 Monitoring a Switch with SNMP 8.3.5 Configuring SNMP Trap

3.2 Given a scenario, use networking monitoring technologies.	
Exam Objective	Course Resource
Methods *SNMP* Management information base (MIB)	8.3.1 SNMP Agents and Monitors 8.3.2 SNMP Security 8.3.4 Monitoring a Switch with SNMP 8.3.5 Configuring SNMP Trap
Methods *SNMP* Versions	8.3.1 SNMP Agents and Monitors
Methods *SNMP* v2c	8.3.1 SNMP Agents and Monitors
Methods *SNMP* v3	8.3.1 SNMP Agents and Monitors
Methods *SNMP* Community strings	8.3.1 SNMP Agents and Monitors 8.3.2 SNMP Security
Methods *SNMP* Authentication	8.3.2 SNMP Security
Methods Flow data	8.6.1 Common Performance Issues 8.6.2 Interface Statistics 8.6.3 Flow Data 8.6.8 Monitoring Interface Statistics
Methods Packet capture	8.5.1 Packet Capture 8.5.4 Using Wireshark to Troubleshoot Network Issues 8.5.5 Lab: Troubleshoot with Wireshark
Methods Baseline metrics	8.4.3 Event Prioritization and Alerting 8.6.8 Monitoring Interface Statistics
Methods *Baseline metrics* Anomaly alerting/notification	8.4.3 Event Prioritization and Alerting

3.2 Given a scenario, use networking monitoring technologies.	
Exam Objective	Course Resource
Methods Log aggregation	8.4.1 Network Device Logs 8.4.2 Log Collectors and Syslog 8.4.3 Event Prioritization and Alerting 8.4.4 Security Information and Event Management 8.4.5 Log Reviews 8.4.6 Lab: Configure Logging in pfSense 8.4.7 Lab: Evaluate Event Logs in pfSense 8.4.8 Lab: Auditing Device Logs on a Cisco Switch 8.4.9 Lab: Configure Logging on Linux 8.4.10 Lab: View Event Logs
Methods *Log aggregation* Syslog collector	8.4.2 Log Collectors and Syslog 8.4.3 Event Prioritization and Alerting 8.4.8 Lab: Auditing Device Logs on a Cisco Switch 8.4.9 Lab: Configure Logging on Linux 8.4.10 Lab: View Event Logs
Methods *Log aggregation* Security information and event management (SIEM)	8.4.4 Security Information and Event Management 8.4.10 Lab: View Event Logs
Methods Application programming Interface (API) integration	8.4.4 Security Information and Event Management
Methods Port mirroring	8.5.1 Packet Capture 8.5.6 Lab: Configure Port Mirroring 10.4.8 Port Mirroring
Solutions	8.2.1 Network Discovery 8.2.5 Performance Monitoring 8.2.6 Availability Monitoring 8.2.7 Configuration Monitoring
Solutions Network discovery	8.2.1 Network Discovery
Solutions *Network discovery* Ad hoc	8.2.1 Network Discovery

3.2 Given a scenario, use networking monitoring technologies.	
Exam Objective	Course Resource
Solutions *Network discovery* Scheduled	8.2.1 Network Discovery
Solutions Traffic analysis	8.6.1 Common Performance Issues 8.6.3 Flow Data 8.6.4 Traffic Testing Tools 8.6.5 Bandwidth Management
Solutions Performance monitoring	8.2.5 Performance Monitoring 8.6.4 Traffic Testing Tools
Solutions Availability monitoring	8.2.5 Performance Monitoring 8.2.6 Availability Monitoring
Solutions Configuration monitoring	8.2.7 Configuration Monitoring

3.3 Explain disaster recovery (DR) concepts.	
Exam Objective	Course Resource
DR metrics	7.4.1 Disaster Recovery Concepts 7.4.2 Disaster Recovery Metrics 7.4.4 Fault Tolerance and Redundancy
DR metrics Recovery point objective (RPO)	7.4.1 Disaster Recovery Concepts 7.4.2 Disaster Recovery Metrics
DR metrics Recovery time objective (RTO)	7.4.2 Disaster Recovery Metrics
DR metrics Mean time to repair (MTTR)	7.4.2 Disaster Recovery Metrics 7.4.4 Fault Tolerance and Redundancy
DR metrics Mean time between failures (MTBF)	7.4.2 Disaster Recovery Metrics 7.4.4 Fault Tolerance and Redundancy
DR sites	7.4.3 Disaster Recovery Sites
DR sites Cold site	7.4.3 Disaster Recovery Sites

3.3 Explain disaster recovery (DR) concepts.	
Exam Objective	Course Resource
DR sites Warm site	7.4.3 Disaster Recovery Sites
DR sites Hot site	7.4.3 Disaster Recovery Sites
High-availability approaches	7.4.4 Fault Tolerance and Redundancy 7.4.6 High Availability Clusters
High-availability approaches Active-active	7.4.6 High Availability Clusters
High-availability approaches Active-passive	7.4.6 High Availability Clusters
Testing	7.4.1 Disaster Recovery Concepts
Testing Tabletop exercises	7.4.1 Disaster Recovery Concepts
Testing Validation tests	7.4.1 Disaster Recovery Concepts

3.4 Given a scenario, implement IPv4 and IPv6 network services.	
Exam Objective	Course Resource
Dynamic addressing	6.2.3 DHCP Options 6.2.4 DHCP Reservations and Exclusions 6.2.6 Lab: Configure DHCP Server Options 6.2.7 Lab: Create DHCP Exclusions 6.2.8 Lab: Create DHCP Client Reservations 6.2.9 Configure Client Addressing 6.2.10 Lab: Configure Client Addressing for DHCP 6.3.2 IPv6 Interface Autoconfiguration and Testing 6.3.3 DHCPv6 Server Configuration 6.4.1 DHCP Relay and IP Helper 6.4.2 DHCP Issues 6.4.3 Troubleshooting DHCP Exhaustion 6.4.4 Lab: Configure a DHCP Relay Agent 6.4.5 Lab: Add a DHCP Server on Another Subnet 6.4.7 Lab: Explore DHCP Troubleshooting 6.4.10 Lab: Troubleshoot IP Configuration 3

3.4 Given a scenario, implement IPv4 and IPv6 network services.	
Exam Objective	Course Resource
Dynamic addressing DHCP	6.2.1 DHCP Process 6.2.2 DHCP Server Configuration 6.2.3 DHCP Options 6.2.4 DHCP Reservations and Exclusions 6.2.5 Lab: Configure a DHCP Server 6.2.6 Lab: Configure DHCP Server Options 6.2.7 Lab: Create DHCP Exclusions 6.2.8 Lab: Create DHCP Client Reservations 6.2.9 Configure Client Addressing 6.2.10 Lab: Configure Client Addressing for DHCP 6.3.2 IPv6 Interface Autoconfiguration and Testing 6.3.3 DHCPv6 Server Configuration 6.3.6 Set Up Alternate Addressing 6.4.1 DHCP Relay and IP Helper 6.4.2 DHCP Issues 6.4.3 Troubleshooting DHCP Exhaustion 6.4.4 Lab: Configure a DHCP Relay Agent 6.4.5 Lab: Add a DHCP Server on Another Subnet 6.4.6 Lab: Troubleshoot Address Pool Exhaustion 6.4.7 Lab: Explore DHCP Troubleshooting 6.4.8 Lab: Troubleshoot IP Configuration 1 6.4.9 Lab: Troubleshoot IP Configuration 2 6.4.10 Lab: Troubleshoot IP Configuration 3 6.6.1 Client DNS Issues
Dynamic addressing *DHCP* Reservations	6.2.1 DHCP Process 6.2.4 DHCP Reservations and Exclusions 6.2.5 Lab: Configure a DHCP Server 6.2.8 Lab: Create DHCP Client Reservations 6.2.10 Lab: Configure Client Addressing for DHCP 6.3.2 IPv6 Interface Autoconfiguration and Testing

3.4 Given a scenario, implement IPv4 and IPv6 network services.	
Exam Objective	Course Resource
Dynamic addressing *DHCP* Scope	6.2.1 DHCP Process 6.2.2 DHCP Server Configuration 6.2.5 Lab: Configure a DHCP Server 6.2.10 Lab: Configure Client Addressing for DHCP 6.3.2 IPv6 Interface Autoconfiguration and Testing 6.3.6 Set Up Alternate Addressing 6.4.2 DHCP Issues 6.4.4 Lab: Configure a DHCP Relay Agent 6.4.5 Lab: Add a DHCP Server on Another Subnet
Dynamic addressing *DHCP* Lease time	6.2.1 DHCP Process 6.2.2 DHCP Server Configuration 6.2.3 DHCP Options 6.2.5 Lab: Configure a DHCP Server 6.2.10 Lab: Configure Client Addressing for DHCP 6.3.2 IPv6 Interface Autoconfiguration and Testing
Dynamic addressing *DHCP* Options	6.2.1 DHCP Process 6.2.3 DHCP Options 6.2.5 Lab: Configure a DHCP Server 6.2.6 Lab: Configure DHCP Server Options 6.2.10 Lab: Configure Client Addressing for DHCP 6.3.2 IPv6 Interface Autoconfiguration and Testing
Dynamic addressing *DHCP* Relay/IP helper	6.2.1 DHCP Process 6.2.10 Lab: Configure Client Addressing for DHCP 6.3.2 IPv6 Interface Autoconfiguration and Testing 6.4.1 DHCP Relay and IP Helper 6.4.4 Lab: Configure a DHCP Relay Agent
Dynamic addressing *DHCP* Exclusions	6.2.1 DHCP Process 6.2.4 DHCP Reservations and Exclusions 6.2.5 Lab: Configure a DHCP Server 6.2.7 Lab: Create DHCP Exclusions 6.2.10 Lab: Configure Client Addressing for DHCP 6.3.2 IPv6 Interface Autoconfiguration and Testing
Dynamic addressing Stateless address autoconfiguration (SLAAC)	6.3.2 IPv6 Interface Autoconfiguration and Testing

3.4 Given a scenario, implement IPv4 and IPv6 network services.	
Exam Objective	Course Resource
Name resolution	6.5.1 Host Names and Domain Names 6.5.2 DNS Hierarchy 6.5.3 Name Resolution Using DNS 6.5.5 Host Address and Canonical Name Records 6.5.8 DNS Server Configuration 6.5.9 Internal vs External DNS 6.5.10 DNS Security 6.5.11 Lab: Configure DNS Addresses 6.5.12 Lab: Create Standard DNS Zones 6.5.13 Lab: Create Host Records 6.5.14 Lab: Create CNAME Records 6.5.15 Lab: Troubleshoot DNS Records 6.5.16 Configuring DNS Caching on Linux 6.6.1 Client DNS Issues 6.6.2 Name Resolution Issues 6.6.3 nslookup 6.6.4 dig

3.4 Given a scenario, implement IPv4 and IPv6 network services.	
Exam Objective	Course Resource
Name resolution DNS	6.5.1 Host Names and Domain Names 6.5.2 DNS Hierarchy 6.5.3 Name Resolution Using DNS 6.5.4 Resource Record Types 6.5.5 Host Address and Canonical Name Records 6.5.6 Mail Exchange, Service, and Text Records 6.5.7 Pointer Records 6.5.8 DNS Server Configuration 6.5.9 Internal vs External DNS 6.5.10 DNS Security 6.5.11 Lab: Configure DNS Addresses 6.5.12 Lab: Create Standard DNS Zones 6.5.13 Lab: Create Host Records 6.5.14 Lab: Create CNAME Records 6.5.15 Lab: Troubleshoot DNS Records 6.5.16 Configuring DNS Caching on Linux 6.6.1 Client DNS Issues 6.6.2 Name Resolution Issues 6.6.3 nslookup 6.6.4 dig 6.6.5 Lab: Explore nslookup 6.6.6 Lab: Use nslookup
Name resolution *DNS* Domain Name Security Extensions (DNSSEC)	6.5.10 DNS Security
Name resolution *DNS* DNS over HTTPS (DoH) and DNS over TLS (DoT)	6.5.10 DNS Security
Name resolution *DNS* Record types	6.5.3 Name Resolution Using DNS 6.5.4 Resource Record Types 6.5.6 Mail Exchange, Service, and Text Records 6.5.8 DNS Server Configuration 6.5.9 Internal vs External DNS

3.4 Given a scenario, implement IPv4 and IPv6 network services.	
Exam Objective	Course Resource
Name resolution *DNS* Address (A)	6.5.5 Host Address and Canonical Name Records 6.5.13 Lab: Create Host Records
Name resolution *DNS* AAAA	6.5.5 Host Address and Canonical Name Records
Name resolution *DNS* Canonical name (CNAME)	6.5.5 Host Address and Canonical Name Records 6.5.14 Lab: Create CNAME Records
Name resolution *DNS* Mail exchange (MX)	6.5.6 Mail Exchange, Service, and Text Records 6.6.3 nslookup 6.6.4 dig
Name resolution *DNS* Text	6.5.6 Mail Exchange, Service, and Text Records
Name resolution *DNS* Nameserver (NS)	6.5.4 Resource Record Types 6.5.9 Internal vs External DNS
Name resolution *DNS* Pointer	6.5.7 Pointer Records
Name resolution *DNS* Zone types	6.5.3 Name Resolution Using DNS 6.5.9 Internal vs External DNS 6.5.12 Lab: Create Standard DNS Zones 6.5.13 Lab: Create Host Records 6.5.14 Lab: Create CNAME Records
Name resolution *DNS* Forward	6.5.3 Name Resolution Using DNS 6.5.14 Lab: Create CNAME Records
Name resolution *DNS* Reverse	6.5.7 Pointer Records 6.5.8 DNS Server Configuration 6.5.9 Internal vs External DNS 6.5.13 Lab: Create Host Records

3.4 Given a scenario, implement IPv4 and IPv6 network services.	
Exam Objective	Course Resource
Name resolution *DNS* Authoritative vs. non-authoritative	6.5.8 DNS Server Configuration 6.5.9 Internal vs External DNS
Name resolution *DNS* Primary vs. secondary	6.5.8 DNS Server Configuration
Name resolution *DNS* Recursive	6.5.3 Name Resolution Using DNS 6.5.9 Internal vs External DNS
Name resolution Hosts file	6.6.1 Client DNS Issues 6.6.2 Name Resolution Issues 6.6.3 nslookup
Time protocols	7.1.1 Transport Layer Security 7.1.2 Network Time Protocol 7.1.3 Precision Time Protocol 7.1.4 Lab: Configure NTP on Linux
Time protocols NTP	7.1.1 Transport Layer Security 7.1.2 Network Time Protocol 7.1.3 Precision Time Protocol 7.1.4 Lab: Configure NTP on Linux
Time protocols Precision Time Protocol (PTP)	7.1.1 Transport Layer Security 7.1.3 Precision Time Protocol
Time protocols Network Time Security (NTS)	7.1.1 Transport Layer Security

3.5 Compare and contrast network access and management methods.	
Exam Objective	Course Resource
Site-to-site VPN	13.2.7 Site-to-Site VPNs 13.2.8 Lab: Configure a Remote Access VPN
Client-to-site VPN	13.2.5 Client-to-Site VPNs 13.2.6 Clientless VPNs 13.2.8 Lab: Configure a Remote Access VPN 13.3.4 Remote Desktop Protocol
Client-to-site VPN Clientless	13.2.6 Clientless VPNs
Client-to-site VPN Split tunnel vs. full tunnel	13.2.5 Client-to-Site VPNs
Connection methods	13.3.1 Remote Host Access 13.3.2 Secure Shell 13.3.5 Console Connections and Out-of-Bound Management 13.3.7 API Connection Methods
Connection methods SSH	13.3.1 Remote Host Access 13.3.2 Secure Shell
Connection methods Graphical user interface (GUI)	13.3.4 Remote Desktop Protocol
Connection methods API	13.3.7 API Connection Methods
Connection methods Console	13.3.5 Console Connections and Out-of-Bound Management
Jump box/host	13.3.6 Jump Boxes
In-band vs. out-of-band management	13.3.5 Console Connections and Out-of-Bound Management

4.0 Network Security

4.1 Explain the importance of basic network security concepts.	
Exam Objective	Course Resource
Logical security	9.1.2 Security Audits and Assessments 9.1.4 Encryption 11.3.3 Geofencing
Logical security Encryption	9.1.4 Encryption
Logical security *Encryption* Data in transit	9.1.4 Encryption
Logical security *Encryption* Data at rest	9.1.4 Encryption
Logical security Certificates	10.1.5 Digital Certificates and PKI
Logical security *Certificates* Public key infrastructure (PKI)	10.1.5 Digital Certificates and PKI
Logical security *Certificates* Self-signed	10.1.5 Digital Certificates and PKI
Logical security Identity and access management (IAM)	10.1.1 Access Control
Logical security *Identity and access management (IAM)* Authentication	10.1.1 Access Control 10.1.2 Authentication Methods 10.1.3 Local Authentication 10.1.4 Single Sign-On and Kerberos 10.1.8 Remote Authentication 10.3.4 Scanning for Unsecure Protocols 13.2.1 Remote Access Considerations

4.1 Explain the importance of basic network security concepts.	
Exam Objective	Course Resource
Logical security *Identity and access management (IAM)* *Authentication* Multifactor authentication (MFA)	10.1.2 Authentication Methods 10.1.3 Local Authentication 10.3.4 Scanning for Unsecure Protocols
Logical security *Identity and access management (IAM)* *Authentication* Single sign-on (SSO)	10.1.3 Local Authentication 10.1.4 Single Sign-On and Kerberos 10.3.4 Scanning for Unsecure Protocols
Logical security *Identity and access management (IAM)* *Authentication* Remote Authentication Dial-in User Service (RADIUS)	10.1.8 Remote Authentication 10.3.4 Scanning for Unsecure Protocols 12.3.3 Enterprise Authentication 13.2.1 Remote Access Considerations 13.2.10 Lab: Configure a RADIUS Solution
Logical security *Identity and access management (IAM)* *Authentication* LDAP	10.2.3 Lightweight Directory Access Protocol 10.2.4 LDAP Secure 10.2.5 Lab: Manage Account Policies 10.3.4 Scanning for Unsecure Protocols
Logical security *Identity and access management (IAM)* *Authentication* Security Assertion Markup Language (SAML)	10.1.7 Federated Identity and SAML
Logical security *Identity and access management (IAM)* *Authentication* Terminal Access Controller Access Control System Plus (TACACS+)	10.1.8 Remote Authentication 12.3.3 Enterprise Authentication 13.2.1 Remote Access Considerations

4.1 Explain the importance of basic network security concepts.	
Exam Objective	Course Resource
Logical security *Identity and access management (IAM)* *Authentication* Time-based authentication	10.1.3 Local Authentication
Logical security *Identity and access management (IAM)* Authorization	10.1.1 Access Control 10.1.2 Authentication Methods 10.2.2 Privileged Access Management 10.2.5 Lab: Manage Account Policies
Logical security *Identity and access management (IAM)* *Authorization* Least privilege	10.2.2 Privileged Access Management 10.2.5 Lab: Manage Account Policies
Logical security *Identity and access management (IAM)* *Authorization* Role-based access control	10.2.1 Authorization and Role-Based Access Control 10.2.5 Lab: Manage Account Policies
Logical security Geofencing	11.3.3 Geofencing
Physical security	11.3.1 Locks 11.3.2 Cameras 11.3.4 Lab: Implement Physical Security
Physical security Camera	11.3.2 Cameras 11.3.4 Lab: Implement Physical Security
Physical security Locks	11.3.1 Locks 11.3.4 Lab: Implement Physical Security
Deception technologies	9.1.6 Deception Technologies 9.1.7 Lab: Create a Honeypot
Deception technologies Honeypot	9.1.6 Deception Technologies 9.1.7 Lab: Create a Honeypot

4.1 Explain the importance of basic network security concepts.	
Exam Objective	Course Resource
Deception technologies Honeynet	9.1.6 Deception Technologies
Common security terminology	9.1.1 Common Security Terminology 9.1.5 Vulnerability and Exploit Types
Common security terminology Risk	9.1.1 Common Security Terminology 9.1.2 Security Audits and Assessments
Common security terminology Vulnerability	9.1.1 Common Security Terminology 9.1.5 Vulnerability and Exploit Types
Common security terminology Exploit	9.1.1 Common Security Terminology 9.1.5 Vulnerability and Exploit Types
Common security terminology Threat	9.1.1 Common Security Terminology 9.1.5 Vulnerability and Exploit Types 9.2.1 Threat Types and Assessment 9.3.5 Using SMAC to Spoof MAC Addresses 9.3.8 Lab: Spoof MAC Addresses with SMAC
Common security terminology Confidentiality, Integrity, and Availability (CIA) triad	9.1.1 Common Security Terminology
Audits and regulatory compliance	9.1.2 Security Audits and Assessments 9.1.3 Regulatory Compliance
Audits and regulatory compliance Data locality	9.1.3 Regulatory Compliance
Audits and regulatory compliance Payment Card Industry Data Security Standards (PCI DSS)	9.1.3 Regulatory Compliance
Audits and regulatory compliance General Data Protection Regulation (GDPR)	9.1.3 Regulatory Compliance
Network segmentation enforcement	11.1.5 Lab: Configure a Screened Subnet (DMZ) 11.2.1 IoT Devices 11.2.4 IoT Network Security

4.1 Explain the importance of basic network security concepts.	
Exam Objective	Course Resource
Network segmentation enforcement Internet of Things (IoT) and Industrial Internet of Things (IIoT)	11.2.1 IoT Devices 11.2.3 IoT Networks 11.2.4 IoT Network Security 11.2.5 Lab: Scan for IoT Devices
Network segmentation enforcement Supervisory control and data acquisition (SCADA), industrial control System (ICS), operational technology (OT)	11.2.2 Industrial Embedded Systems
Network segmentation enforcement Guest	12.3.5 Bring Your Own Device Issues 12.3.8 Lab: Create a Guest Network for BYOD
Network segmentation enforcement Bring your own device (BYOD)	12.3.5 Bring Your Own Device Issues 12.3.8 Lab: Create a Guest Network for BYOD

4.2 Summarize various types of attacks and their impact to the network.	
Exam Objective	Course Resource
Denial-of-service (DoS)/distributed denial-of-service (DDoS)	9.2.2 Attack Types 9.2.3 Distributed DoS Attacks and Botnets 9.2.5 Lab: Analyze a DoS Attack 9.2.6 Lab: Analyze a DDoS Attack 12.3.11 Lab: Enable Wireless Intrusion Prevention
VLAN hopping	9.3.6 VLAN Hopping Attacks
Media Access Control (MAC) flooding	9.3.4 MAC Flooding Attack
Address Resolution Protocol (ARP) poisoning	9.3.3 Poison ARP 9.3.7 Lab: Poison ARP and Analyze with Wireshark
ARP spoofing	9.3.1 On-Path Attacks
DNS poisoning	9.2.4 Malware Attacks 9.4.4 DNS Attacks 9.4.5 Poisoning DNS 9.4.8 Lab: Poison DNS
DNS spoofing	9.4.4 DNS Attacks 9.4.9 Lab: Analyze DNS Spoofing

4.2 Summarize various types of attacks and their impact to the network.	
Exam Objective	Course Resource
Rogue devices and services	9.4.1 Rogue Devices and Services 9.4.2 Rogue DHCP 9.4.3 Setting Up DHCP Snooping 9.4.6 Lab: Discover a Rogue DHCP Server 9.4.7 Lab: Configure DHCP Snooping 12.3.6 Wireless Network Attacks 12.3.11 Lab: Enable Wireless Intrusion Prevention 12.4.9 Lab: Optimize a Wireless Network
Rogue devices and services DHCP	9.4.2 Rogue DHCP 9.4.3 Setting Up DHCP Snooping 9.4.6 Lab: Discover a Rogue DHCP Server 9.4.7 Lab: Configure DHCP Snooping 12.3.11 Lab: Enable Wireless Intrusion Prevention
Rogue devices and services AP	12.3.6 Wireless Network Attacks
Evil twin	12.3.6 Wireless Network Attacks
On-path attack	9.3.1 On-Path Attacks 9.3.2 Performing an On-Path DHCP Attack 9.3.9 Lab: Perform a DHCP Spoofing On-Path Attack 9.4.8 Lab: Poison DNS
Social engineering	9.5.1 Social Engineering Attacks 9.5.2 Password Attacks 9.5.3 Lab: Respond to Social Engineering Exploits 9.5.4 Lab: Crack a Password with John the Ripper
Social engineering Phishing	9.5.1 Social Engineering Attacks 9.5.3 Lab: Respond to Social Engineering Exploits
Social engineering Dumpster diving	9.5.1 Social Engineering Attacks
Social engineering Shoulder surfing	9.5.1 Social Engineering Attacks
Social engineering Tailgating	9.5.1 Social Engineering Attacks

4.2 Summarize various types of attacks and their impact to the network.	
Exam Objective	Course Resource
Malware	9.2.2 Attack Types 9.2.4 Malware Attacks

4.3 Given a scenario, apply network security features, defense techniques, and solutions.	
Exam Objective	Course Resource
Device hardening	10.3.1 Defense in Depth 10.3.2 Device and Service Hardening 10.3.3 View Linux Services 10.3.4 Scanning for Unsecure Protocols 10.3.5 Lab: Scan for Unsecure Protocols 10.3.6 Lab: Enable and Disable Linux Services 10.3.7 Lab: Disable Network Service
Device hardening Disable unused ports and services	10.3.1 Defense in Depth 10.3.2 Device and Service Hardening 10.3.3 View Linux Services 10.3.5 Lab: Scan for Unsecure Protocols 10.3.6 Lab: Enable and Disable Linux Services 10.3.7 Lab: Disable Network Service
Device hardening Change default passwords	10.3.1 Defense in Depth 10.3.2 Device and Service Hardening 10.3.5 Lab: Scan for Unsecure Protocols
Network access control (NAC)	10.4.1 Network Access Control and Port Security 10.4.2 Lab: Secure Access to a Switch 10.4.3 Lab: Secure Access to a Switch 2 10.4.4 Lab: Disable Switch Ports - GUI 10.4.5 Extensible Authentication Protocol and IEEE 802.1X 10.4.6 Port Guards 10.4.7 Lab: Harden a Switch 10.4.8 Port Mirroring

4.3 Given a scenario, apply network security features, defense techniques, and solutions.	
Exam Objective	Course Resource
Network access control (NAC) Port security	10.4.1 Network Access Control and Port Security 10.4.2 Lab: Secure Access to a Switch 10.4.3 Lab: Secure Access to a Switch 2 10.4.4 Lab: Disable Switch Ports - GUI 10.4.6 Port Guards 10.4.7 Lab: Harden a Switch 10.4.8 Port Mirroring
Network access control (NAC) 802.1X	10.4.5 Extensible Authentication Protocol and IEEE 802.1X 10.4.6 Port Guards 10.4.7 Lab: Harden a Switch
Network access control (NAC) MAC filtering	3.1.6 Media Access Control Address Format 3.4.5 MAC Address Table 10.4.1 Network Access Control and Port Security 10.4.2 Lab: Secure Access to a Switch 10.4.3 Lab: Secure Access to a Switch 2 10.4.4 Lab: Disable Switch Ports - GUI 10.4.6 Port Guards 10.4.7 Lab: Harden a Switch
Key management	10.1.6 Key Management
Security rules	10.5.1 Security Rules and ACL Configuration 10.5.3 Content Filtering 10.5.5 Creating Firewall ACLs 10.5.6 Lab: Configure Network Security Appliance Access 10.5.7 Lab: Configure a Security Appliance 10.5.8 Lab: Configure a Perimeter Firewall 10.5.9 Lab: Restrict Telnet and SSH Access 10.5.10 Lab: Permit Traffic 10.5.11 Lab: Block Source Hosts

4.3 Given a scenario, apply network security features, defense techniques, and solutions.	
Exam Objective	Course Resource
Security rules Access control list (ACL)	10.5.1 Security Rules and ACL Configuration 10.5.5 Creating Firewall ACLs 10.5.6 Lab: Configure Network Security Appliance Access 10.5.7 Lab: Configure a Security Appliance 10.5.8 Lab: Configure a Perimeter Firewall 10.5.10 Lab: Permit Traffic 10.5.11 Lab: Block Source Hosts
Security rules Uniform Resource Locator (URL) filtering	10.5.1 Security Rules and ACL Configuration 10.5.7 Lab: Configure a Security Appliance 10.5.8 Lab: Configure a Perimeter Firewall 10.5.9 Lab: Restrict Telnet and SSH Access 10.5.10 Lab: Permit Traffic
Security rules Content filtering	10.5.1 Security Rules and ACL Configuration 10.5.3 Content Filtering 10.5.7 Lab: Configure a Security Appliance 10.5.8 Lab: Configure a Perimeter Firewall 10.5.10 Lab: Permit Traffic
Zones	11.1.1 Network Security Zones 11.1.2 Configuring a Screened Subnet 11.1.3 Perimeter Networks 11.1.4 Screened Subnets 11.1.5 Lab: Configure a Screened Subnet (DMZ) 11.1.6 Lab: Configure Screened Subnets
Zones Trusted vs. untrusted	11.1.1 Network Security Zones 11.1.3 Perimeter Networks
Zones Screened subnet	11.1.1 Network Security Zones 11.1.2 Configuring a Screened Subnet 11.1.4 Screened Subnets 11.1.5 Lab: Configure a Screened Subnet (DMZ) 11.1.6 Lab: Configure Screened Subnets

5.0 Network Troubleshooting

5.1 Explain the troubleshooting methodology.	
Exam Objective	Course Resource
Identify the problem	1.4.1 Network Troubleshooting Methodology 1.4.2 Identify the Problem 1.4.3 Identify Problem Symptoms 1.4.10 Lab: Troubleshooting Methodology
Identify the problem Gather information	1.4.2 Identify the Problem 1.4.3 Identify Problem Symptoms
Identify the problem Question users	1.4.2 Identify the Problem 1.4.3 Identify Problem Symptoms
Identify the problem Identify symptoms	1.4.2 Identify the Problem 1.4.3 Identify Problem Symptoms
Identify the problem Determine if anything has changed	1.4.2 Identify the Problem 1.4.3 Identify Problem Symptoms
Identify the problem Duplicate the problem, if possible	1.4.2 Identify the Problem 1.4.3 Identify Problem Symptoms
Identify the problem Approach multiple problems individually	1.4.2 Identify the Problem 1.4.3 Identify Problem Symptoms
Establish a theory of probable cause	1.4.1 Network Troubleshooting Methodology 1.4.4 Establish a Theory of Probable Cause 1.4.10 Lab: Troubleshooting Methodology
Establish a theory of probable cause Question the obvious	1.4.4 Establish a Theory of Probable Cause
Establish a theory of probable cause Consider multiple approaches	1.4.4 Establish a Theory of Probable Cause
Establish a theory of probable cause *Consider multiple approaches* Top-to-bottom/bottom-to-top OSI model	1.2.8 OSI Model Summary 1.4.4 Establish a Theory of Probable Cause

5.1 Explain the troubleshooting methodology.	
Exam Objective	Course Resource
Establish a theory of probable cause *Consider multiple approaches* Divide and conquer	1.4.4 Establish a Theory of Probable Cause
Test the theory to determine the cause	1.4.1 Network Troubleshooting Methodology 1.4.5 Test the Theory to Determine the Cause 1.4.10 Lab: Troubleshooting Methodology
Test the theory to determine the cause If theory is confirmed, determine next steps to resolve problem	1.4.5 Test the Theory to Determine the Cause
Test the theory to determine the cause If theory is not confirmed, establish a new theory or escalate	1.4.5 Test the Theory to Determine the Cause
Establish a plan of action to resolve the problem and identify potential effects	1.4.1 Network Troubleshooting Methodology 1.4.6 Establish a Plan of Action 1.4.10 Lab: Troubleshooting Methodology
Implement the solution or escalate as necessary	1.4.1 Network Troubleshooting Methodology 1.4.7 Implement the Solution 1.4.10 Lab: Troubleshooting Methodology
Verify full system functionality and implement preventive measures if applicable	1.4.1 Network Troubleshooting Methodology 1.4.8 Verify the Solution 1.4.10 Lab: Troubleshooting Methodology
Document findings, actions, outcomes, and lessons learned throughout the process	1.4.1 Network Troubleshooting Methodology 1.4.9 Document Findings, Actions, and Outcomes 1.4.10 Lab: Troubleshooting Methodology

5.2 Given a scenario, troubleshoot common cabling and physical interface issues.	
Exam Objective	Course Resource
Cable issues	2.6.1 Specification and Limitations 2.6.2 Cable Issues 2.6.6 Attenuation and Interference Issues 2.6.7 Crosstalk Issues 2.6.9 Cable Troubleshooting Strategies 2.6.10 Lab: Explore Physical Connectivity 1 2.6.11 Lab: Explore Physical Connectivity 2 2.6.12 Lab: Troubleshoot Physical Connectivity 1 2.6.13 Lab: Troubleshoot Physical Connectivity 2 2.6.14 Lab: Troubleshoot Physical Connectivity 3 2.6.15 Lab: Troubleshoot Physical Connectivity 4 12.4.2 Insufficient Wireless Coverage Issues
Cable issues Incorrect cable	2.6.8 Fiber Optic Cable Testing Tools
Cable issues *Incorrect cable* Single mode vs. multimode	2.4.2 Single Mode Fiber and Multimode Fiber
Cable issues *Incorrect cable* Category 5/6/7/8	2.6.3 Cable Category Issues
Cable issues *Incorrect cable* Shielded twisted pair (STP) vs. unshielded twisted pair (UTP)	2.2.1 Unshielded Twisted Pair Cable 2.2.2 Shielded and Screened Twisted Pair Cable
Cable issues Signal degradation	2.6.1 Specification and Limitations
Cable issues *Signal degradation* Crosstalk	2.6.7 Crosstalk Issues
Cable issues *Signal degradation* Interference	2.6.1 Specification and Limitations 2.6.6 Attenuation and Interference Issues

5.2 Given a scenario, troubleshoot common cabling and physical interface issues.	
Exam Objective	Course Resource
Cable issues *Signal degradation* Attenuation	2.6.1 Specification and Limitations 2.6.6 Attenuation and Interference Issues 12.4.2 Insufficient Wireless Coverage Issues
Cable issues Improper termination	2.6.5 Wire Map Testers and Tone Generators 2.6.7 Crosstalk Issues
Cable issues Transmitter (TX)/Receiver (RX) transposed	2.4.7 Wavelength Division Multiplexing
Interface issues	3.4.4 Interface Error Counters
Interface issues Increasing interface counters	3.4.4 Interface Error Counters
Interface issues *Increasing interface counters* Cyclic redundancy check (CRC)	3.1.5 Ethernet Frame Format 3.4.4 Interface Error Counters
Interface issues *Increasing interface counters* Runts	3.4.4 Interface Error Counters
Interface issues *Increasing interface counters* Giants	3.4.4 Interface Error Counters
Interface issues *Increasing interface counters* Drops	3.4.4 Interface Error Counters
Interface issues Port status	3.4.4 Interface Error Counters
Interface issues *Port status* Error disabled	3.4.4 Interface Error Counters
Interface issues *Port status* Administratively down	3.4.4 Interface Error Counters

5.2 Given a scenario, troubleshoot common cabling and physical interface issues.	
Exam Objective	Course Resource
Interface issues *Port status* Suspended	3.4.4 Interface Error Counters
Hardware issues	3.1.4 Transceiver Signal Strength Issues 3.4.1 Hardware Failure Issues 3.4.7 Power Over Ethernet Issues
Hardware issues Power over Ethernet (PoE)	3.3.5 Power Over Ethernet 3.3.8 Lab: Configure PoE 3.4.1 Hardware Failure Issues 3.4.7 Power Over Ethernet Issues 7.3.7 Lab: Connect VoIP 2
Hardware issues *Power over Ethernet (PoE)* Power budget exceeded	3.4.1 Hardware Failure Issues
Hardware issues *Power over Ethernet (PoE)* Incorrect standard	3.4.1 Hardware Failure Issues
Hardware issues Transceivers	3.1.3 Transceiver Mismatch Issues
Hardware issues *Transceivers* Mismatch	3.1.3 Transceiver Mismatch Issues
Hardware issues *Transceivers* Signal strength	3.1.4 Transceiver Signal Strength Issues

5.3 Given a scenario, troubleshoot common issues with network services.	
Exam Objective	Course Resource
Switching issues	3.3.3 Spanning Tree Protocol 3.3.4 Spanning Tree Protocol Configuration 3.4.2 Port Status Indicators 3.4.5 MAC Address Table 3.4.9 Lab: Switching Loop 5.7.3 VLAN Assignment Issues 10.5.4 Misconfigured Firewall and ACL Issues
Switching issues STP	3.3.3 Spanning Tree Protocol 3.3.4 Spanning Tree Protocol Configuration 3.4.2 Port Status Indicators 3.4.5 MAC Address Table
Switching issues *STP* Network loops	3.4.5 MAC Address Table 3.4.6 Network Loop and Broadcast Storm Issues 3.4.9 Lab: Switching Loop
Switching issues *STP* Root bridge selection	3.3.4 Spanning Tree Protocol Configuration
Switching issues *STP* Port roles	3.3.3 Spanning Tree Protocol 3.3.4 Spanning Tree Protocol Configuration
Switching issues *STP* Port states	3.3.3 Spanning Tree Protocol 3.3.4 Spanning Tree Protocol Configuration 3.4.2 Port Status Indicators
Switching issues Incorrect VLAN assignment	5.7.3 VLAN Assignment Issues
Switching issues ACLs	10.5.1 Security Rules and ACL Configuration 10.5.4 Misconfigured Firewall and ACL Issues
Route selection	5.7.1 Routing Table Issues 5.7.2 Default Route and Routing Loop Issues
Route selection Routing table	5.7.1 Routing Table Issues 5.7.2 Default Route and Routing Loop Issues

5.3 Given a scenario, troubleshoot common issues with network services.	
Exam Objective	Course Resource
Route selection Default routes	5.7.1 Routing Table Issues 5.7.2 Default Route and Routing Loop Issues
Address pool exhaustion	6.4.2 DHCP Issues 6.4.3 Troubleshooting DHCP Exhaustion 6.4.6 Lab: Troubleshoot Address Pool Exhaustion
Incorrect default gateway	4.4.4 ping
Incorrect IP address	4.6.1 IP Configuration Issues
Incorrect IP address Duplicate IP address	4.6.2 Duplicate IP and MAC Address Issues
Incorrect subnet mask	4.6.1 IP Configuration Issues

5.4 Given a scenario, troubleshoot common performance issues.	
Exam Objective	Course Resource
Congestion/contention	8.6.1 Common Performance Issues 8.6.2 Interface Statistics 8.6.5 Bandwidth Management 8.6.6 Traffic Shaping
Bottlenecking	8.6.1 Common Performance Issues 8.6.2 Interface Statistics 8.6.5 Bandwidth Management 8.6.6 Traffic Shaping
Bandwidth	2.1.1 Network Data Transmission 8.6.1 Common Performance Issues 8.6.2 Interface Statistics 8.6.5 Bandwidth Management 8.6.6 Traffic Shaping 8.6.7 Lab: Configure QoS 12.4.1 Wireless Performance Assessment 12.4.6 Overcapacity Issues

5.4 Given a scenario, troubleshoot common performance issues.	
Exam Objective	Course Resource
Bandwidth Throughput capacity	8.6.1 Common Performance Issues 8.6.2 Interface Statistics 8.6.5 Bandwidth Management 8.6.6 Traffic Shaping 8.6.7 Lab: Configure QoS 12.4.1 Wireless Performance Assessment 12.4.6 Overcapacity Issues
Latency	8.6.1 Common Performance Issues 8.6.2 Interface Statistics 8.6.6 Traffic Shaping
Packet loss	8.6.1 Common Performance Issues 8.6.2 Interface Statistics
Jitter	8.6.1 Common Performance Issues
Wireless	12.4.1 Wireless Performance Assessment 12.4.3 Channel Overlap Issues 12.4.4 Interference Issues 12.4.5 Roaming and Client Disassociation Issues 12.4.7 Lab: Explore Wireless Network Problems 12.4.8 Lab: Troubleshoot Wireless Network Problems 12.4.9 Lab: Optimize a Wireless Network
Wireless Interference	12.4.3 Channel Overlap Issues 12.4.4 Interference Issues 12.4.7 Lab: Explore Wireless Network Problems 12.4.9 Lab: Optimize a Wireless Network
Wireless *Interference* Channel overlap	12.4.3 Channel Overlap Issues
Wireless Signal degradation or loss	12.2.2 Range and Signal Strength 12.4.1 Wireless Performance Assessment 12.4.2 Insufficient Wireless Coverage Issues 12.4.7 Lab: Explore Wireless Network Problems
Wireless Insufficient wireless coverage	12.4.2 Insufficient Wireless Coverage Issues 12.4.7 Lab: Explore Wireless Network Problems 12.4.8 Lab: Troubleshoot Wireless Network Problems

5.4 Given a scenario, troubleshoot common performance issues.	
Exam Objective	Course Resource
Wireless Client disassociation issues	12.4.5 Roaming and Client Disassociation Issues
Wireless Roaming misconfiguration	12.4.5 Roaming and Client Disassociation Issues

5.5 Given a scenario, use the appropriate tool or protocol to solve networking issues.	
Exam Objective	Course Resource
Software tools	2.6.8 Fiber Optic Cable Testing Tools 4.4.1 ipconfig 4.4.2 ifconfig and ip 4.4.3 arp 4.4.5 Lab: IPv4 Troubleshooting Tools 4.4.6 Lab: IPv4 Troubleshooting tools for Linux 5.1.8 tracert and traceroute 5.1.10 Lab: Cisco Troubleshooting Tools 6.1.5 netstat 6.1.8 Lab: View Open Ports with netstat 6.4.7 Lab: Explore DHCP Troubleshooting 6.4.8 Lab: Troubleshoot IP Configuration 1 6.4.9 Lab: Troubleshoot IP Configuration 2 6.4.10 Lab: Troubleshoot IP Configuration 3 6.5.15 Lab: Troubleshoot DNS Records 6.5.16 Configuring DNS Caching on Linux 7.2.8 Lab: Scan for Web Services with Nmap 8.2.2 Nmap 8.2.3 Nmap Port Scanning 8.2.4 Discovery Protocols 8.2.8 Lab: Scan Using Zenmap 8.5.2 tcpdump 8.5.3 Protocol Analyzers 8.5.4 Using Wireshark to Troubleshoot Network Issues 8.5.5 Lab: Troubleshoot with Wireshark 8.6.4 Traffic Testing Tools

5.5 Given a scenario, use the appropriate tool or protocol to solve networking issues.	
Exam Objective	Course Resource
Software tools Protocol analyzer	8.5.3 Protocol Analyzers 8.5.4 Using Wireshark to Troubleshoot Network Issues 8.5.5 Lab: Troubleshoot with Wireshark 9.3.7 Lab: Poison ARP and Analyze with Wireshark
Software tools Command line	4.4.1 ipconfig 4.4.2 ifconfig and ip 4.4.3 arp 4.4.5 Lab: IPv4 Troubleshooting Tools 4.4.6 Lab: IPv4 Troubleshooting tools for Linux 4.4.7 Lab: Use IPv4 Test Tools 6.4.8 Lab: Explore DHCP Troubleshooting 6.4.9 Lab: Troubleshoot IP Configuration 1
Software tools *Command line* ping	4.4.3 arp 4.4.4 ping 4.4.5 Lab: IPv4 Troubleshooting Tools 4.4.7 Lab: Use IPv4 Test Tools 6.4.7 Lab: Explore DHCP Troubleshooting 6.4.9 Lab: Troubleshoot IP Configuration 2 6.4.10 Lab: Troubleshoot IP Configuration 3 6.5.15 Lab: Troubleshoot DNS Records 6.6.1 Client DNS Issues 6.6.2 Name Resolution Issues
Software tools *Command line* traceroute/tracert	5.1.8 tracert and traceroute 5.1.10 Lab: Cisco Troubleshooting Tools 6.4.7 Lab: Explore DHCP Troubleshooting 6.4.9 Lab: Troubleshoot IP Configuration 2 6.4.10 Lab: Troubleshoot IP Configuration 3 13.3.9 Lab: Use PowerShell Remote
Software tools *Command line* nslookup	6.5.16 Configuring DNS Caching on Linux 6.6.2 Name Resolution Issues 6.6.3 nslookup 6.6.5 Lab: Explore nslookup 6.6.6 Lab: Use nslookup 10.3.5 Lab: Scan for Unsecure Protocols

5.5 Given a scenario, use the appropriate tool or protocol to solve networking issues.	
Exam Objective	Course Resource
Software tools *Command line* tcpdump	8.5.2 tcpdump
Software tools *Command line* dig	6.6.4 dig
Software tools *Command line* netstat	6.1.5 netstat 6.1.8 Lab: View Open Ports with netstat
Software tools *Command line* ip/ifconfig/ipconfig	4.4.1 ipconfig 4.4.2 ifconfig and ip 4.4.5 Lab: IPv4 Troubleshooting Tools 4.4.6 Lab: IPv4 Troubleshooting tools for Linux 4.4.7 Lab: Use IPv4 Test Tools 6.4.6 Lab: Troubleshoot Address Pool Exhaustion 6.4.8 Lab: Troubleshoot IP Configuration 1 6.4.9 Lab: Troubleshoot IP Configuration 2 6.4.10 Lab: Troubleshoot IP Configuration 3 6.6.1 Client DNS Issues 6.6.2 Name Resolution Issues
Software tools *Command line* arp	4.4.5 Lab: IPv4 Troubleshooting Tools 4.4.7 Lab: Use IPv4 Test Tools 6.4.7 Lab: Explore DHCP Troubleshooting
Software tools Nmap	7.2.8 Lab: Scan for Web Services with Nmap 8.2.2 Nmap 8.2.3 Nmap Port Scanning
Software tools Link Layer Discovery Protocol (LLDP)/Cisco Discovery Protocol (CDP)	8.2.4 Discovery Protocols
Software tools Speed tester	8.6.4 Traffic Testing Tools

5.5 Given a scenario, use the appropriate tool or protocol to solve networking issues.	
Exam Objective	Course Resource
Hardware tools	2.6.5 Wire Map Testers and Tone Generators 2.6.8 Fiber Optic Cable Testing Tools 8.5.1 Packet Capture 12.4.1 Wireless Performance Assessment
Hardware tools Toner	2.6.5 Wire Map Testers and Tone Generators
Hardware tools Cable tester	2.6.4 Cable Testers 2.6.5 Wire Map Testers and Tone Generators
Hardware tools Taps	8.5.1 Packet Capture
Hardware tools Wi-Fi analyzer	12.4.1 Wireless Performance Assessment
Hardware tools Visual fault locator	2.6.8 Fiber Optic Cable Testing Tools
Basic networking device commands	3.4.3 Switch Show Commands 3.4.8 Lab: Troubleshoot Disabled Ports 5.1.7 Routing Table Tools 5.1.10 Lab: Cisco Troubleshooting Tools
Basic networking device commands show mac-address-table	3.4.3 Switch Show Commands 3.4.5 MAC Address Table 3.4.8 Lab: Troubleshoot Disabled Ports
Basic networking device commands show route	5.1.7 Routing Table Tools 5.1.10 Lab: Cisco Troubleshooting Tools
Basic networking device commands show interface	3.4.3 Switch Show Commands 3.4.8 Lab: Troubleshoot Disabled Ports
Basic networking device commands show config	3.4.3 Switch Show Commands 3.4.8 Lab: Troubleshoot Disabled Ports
Basic networking device commands show arp	5.1.7 Routing Table Tools 5.1.10 Lab: Cisco Troubleshooting Tools
Basic networking device commands show vlan	5.6.2 Virtual LAN IDs and Membership

5.5 Given a scenario, use the appropriate tool or protocol to solve networking issues.	
Exam Objective	Course Resource
Basic networking device commands show power	3.4.3 Switch Show Commands 3.4.8 Lab: Troubleshoot Disabled Ports