CompTIA®

CertMaster Perform Network+

N10-009

COURSE OUTLINE

List of Modules

1.0 Explaining Network Topologies

1.1 Networking Overview

1.1.1 Networking Concepts
1.1.2 Network Types
1.1.3 Network Topology
1.1.4 Star Topology
1.1.5 Mesh Topology
1.1.6 Network Topologies
1.1.7 Lab: Create Network Topologies
1.1.8 Lesson Review

1.2 OSI Model Concepts

1.2.1 Open Systems Interconnection Model
1.2.2 Data Encapsulation and Decapsulation
1.2.3 Layer 1 - Physical
1.2.4 Layer 2 - Data Link
1.2.5 Layer 3 - Network
1.2.6 Layer 4 - Transport
1.2.7 Upper Layers
1.2.8 OSI Model Summary
1.2.9 Lesson Review

1.3 SOHO Networks

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
1.3.7 Binary and Hexadecimal
1.3.8 Lab: Explore a Single Location in a Lab
1.3.9 Lab: Create a Home Wireless Network
1.3.10 Lab: Create a SOHO Network
1.3.11 Lesson Review

1.4 Troubleshooting Methodology

- 1.4.1 Network Troubleshooting Methodology
- 1.4.2 Identify the Problem
- 1.4.3 Identify Problem Symptoms
- 1.4.4 Establish a Theory of Probable Cause
- 1.4.5 Test the Theory to Determine the Cause
- 1.4.6 Establish a Plan of Action
- 1.4.7 Implement the Solution
- 1.4.8 Verify the Solution
- 1.4.9 Document Findings, Actions, and Outcomes
- 1.4.10 Lab: Troubleshooting Methodology
- 1.4.11 Lesson Review

1.5 Module Quiz

2.0 Supporting Cabling and Physical Installations

2.1 Ethernet

- 2.1.1 Network Data Transmission
- 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
- 2.1.7 Ethernet Specifications
- 2.1.8 Lab: Reconnect to an Ethernet Network
- 2.1.9 Lesson Review

2.2 Copper Cables and Connectors

- 2.2.1 Unshielded Twisted Pair Cable
- 2.2.2 Shielded and Screened Twisted Pair Cable
- 2.2.3 Cat Cable Standards
- 2.2.4 Twisted Pair Connector Types
- 2.2.5 Plenum and Riser-rated Cable
- 2.2.6 Coaxial and Twinaxial Cable and Connectors
- 2.2.7 Lab: Connect to an Ethernet Network
- 2.2.8 Lab: Connect a Cable Modem
- 2.2.9 Identify Cabling
- 2.2.10 Identify Connectors
- 2.2.11 Lesson Review

2.3 Wiring Implementation

2.3.1 Structured Cabling System
2.3.2 T568A and T568B Termination Standards
2.3.3 Patch Panels
2.3.4 Structured Cable Installation
2.3.5 Termination Tools and Techniques
2.3.6 Lab: Explore Multiple Locations in a Lab
2.3.7 Lab: Connect Network Devices
2.3.8 Lab: Connect Patch Panel Cables 1
2.3.9 Lab: Connect Patch Panel Cables 2
2.3.10 Lesson Review

2.4 Fiber Optic Cables and Connectors

2.4.1 Fiber Optic Cable Considerations
2.4.2 Single Mode Fiber and Multimode Fiber
2.4.3 Fiber Optic Connector Types
2.4.4 Fiber Optic Cable Installation
2.4.5 Fiber Distribution Panels
2.4.6 Multi-Fiber Push On Connectors
2.4.7 Wavelength Division Multiplexing
2.4.8 Lab: Connect Fiber Optic Cables
2.4.9 Identify Fiber Optic Connectors
2.4.10 Lesson Review

2.5 Physical Installation Factors

2.5.1 Rack Systems
2.5.2 Humidity and Temperature
2.5.3 Power Management
2.5.4 Fire Suppression
2.5.5 Lesson Review

2.6 Cable Troubleshooting

- 2.6.1 Specification and Limitations
- 2.6.2 Cable Issues
- 2.6.3 Cable Category Issues
- 2.6.4 Cable Testers
- 2.6.5 Wire Map Testers and Tone Generators
- 2.6.6 Attenuation and Interference Issues
- 2.6.7 Crosstalk Issues
- 2.6.8 Fiber Optic Cable Testing Tools
- 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
- 2.6.16 Lesson Review

2.7 Module Quiz

3.0 Configuring Interfaces and Switches

3.1 Network Interfaces

- 3.1.1 Network Interface Cards
- 3.1.2 Modular Transceivers
- 3.1.3 Transceiver Mismatch Issues
- 3.1.4 Transceiver Signal Strength Issues
- 3.1.5 Ethernet Frame Format
- 3.1.6 Media Access Control Address Format
- 3.1.7 Compare Network Adapters
- 3.1.8 Lab: Select and Install a Network Adapter
- 3.1.9 Lab: Connect a Media Converter
- 3.1.10 Lesson Review

3.2 Ethernet Switches

- 3.2.1 Hubs
- 3.2.2 Bridges
- 3.2.3 Switches
- 3.2.4 Ethernet Switch Types
- 3.2.5 Switch Interface Configuration
- 3.2.6 Cisco IoS Basics (8:37)
- 3.2.7 Lab: Install a Switch in the Rack
- 3.2.8 Lab: Secure a Switch
- 3.2.9 Lab: Cisco IoS Basics
- 3.2.10 Lesson Review

3.3 Switch Port Configuration

- 3.3.1 Link Aggregation and NIC Teaming
- 3.3.2 Maximum Transmission Unit
- 3.3.3 Spanning Tree Protocol
- 3.3.4 Spanning Tree Protocol Configuration
- 3.3.5 Power Over Ethernet
- 3.3.6 Lab: Configure Port Aggregation
- 3.3.7 Lab: Enable Jumbo Frame Support
- 3.3.8 Lab: Configure PoE
- 3.3.9 Lesson Review

3.4 Switch Troubleshooting

- 3.4.1 Hardware Failure Issues
- 3.4.2 Port Status Indicators
- 3.4.3 Switch Show Commands
- 3.4.4 Interface Error Counters
- 3.4.5 MAC Address Table
- 3.4.6 Network Loop and Broadcast Storm Issues
- 3.4.7 Power Over Ethernet Issues
- 3.4.8 Lab: Troubleshoot Disabled Ports
- 3.4.9 Lab: Switching Loop
- 3.4.10 Lesson Review

3.5 Module Quiz

3.6 Checkpoint Review

4.0 Configuring Network Addressing

4.1 Internet Protocol Basics

4.1.1 IPv4 Datagram Header
4.1.2 Layer 2 vs. Layer 3 Addressing and Forwarding
4.1.3 Address Resolution Protocol
4.1.4 Unicast and Broadcast Addressing
4.1.5 Multicast and Anycast Addressing
4.1.6 Lab: Explore Packets and Frames
4.1.7 Lab: Explore ARP in Wireshark
4.1.8 Lesson Review

4.2 IP Version 4 Addressing

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
4.2.12 Lesson Review

4.3 IP Version 4 Subnetting

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
4.3.5 Classless Inter-Domain Routing
4.3.6 Variable Length Subnet Masks
4.3.7 Lab: Configure IP Networks and Subnets
4.3.8 Lesson Review

4.4 IP Troubleshooting Tools

4.4.1 ipconfig
4.4.2 ifconfig and ip
4.4.3 arp
4.4.4 ping
4.4.5 Lab: IPv4 Troubleshooting Tools
4.4.6 Lab: IPv4 Troubleshooting tools for Linux
4.4.7 Lab: Use IPv4 Test Tools
4.4.8 Lesson Review

4.5 IP Version 6

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
4.5.10 Lesson Review

4.6 IP Troubleshooting

4.6.1 IP Configuration Issues
4.6.2 Duplicate IP and MAC Address Issues
4.6.3 IP Forwarding Issues
4.6.4 Lab: Use ping and tracert on Windows
4.6.5 Lab: Use ping and traceroute on Linux
4.6.6 Lab: Assisted Troubleshooting 1
4.6.7 Lab: Assisted Troubleshooting 2
4.6.8 Lab: Assisted Troubleshooting 3
4.6.9 Live Lab: Explore the VM Lab Environment
4.6.10 Applied Live Lab: Troubleshoot IP Configuration
4.6.11 Lesson Review

4.7 Module Quiz

5.0 Configuring Routing and Advanced Switching

5.1 Routing Technologies

- 5.1.1 Routing Tables and Path Selection
- 5.1.2 Static and Default Routes
- 5.1.3 Routing Table Example
- 5.1.4 Packet Forwarding
- 5.1.5 Fragmentation
- 5.1.6 Router Configuration
- 5.1.7 Routing Table Tools
- 5.1.8 tracert and traceroute
- 5.1.9 Lab: Install an Enterprise Router
- 5.1.10 Lab: Cisco Troubleshooting Tools
- 5.1.11 Lesson Review

5.2 Dynamic Routing Technologies

- 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
- 5.2.6 Route Selection
- 5.2.7 Lesson Review

5.3 Network 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
- 5.3.5 Lesson Review

5.4 Firewalls

5.4.1 Firewall Uses and Types
5.4.2 Firewall Selection and Placement
5.4.3 Lesson Review

5.5 Enterprise Network Topologies

5.5.1 Hybrid Topology
5.5.2 Three-Tiered Network Hierarchy
5.5.3 Compare Three-tier Hierarchical Model
5.5.4 Lab: Create a Three-tier Network
5.5.5 Lesson Review

5.6 Virtual LANs

5.6.1 Virtual LANs and Subnets
5.6.2 Virtual LAN IDs and Membership
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
5.6.8 Lab: Configure Switch IP and VLAN - GUI
5.6.9 Lab: Create VLANs - GUI
5.6.10 Lab: Configure Trunking
5.6.11 Lab: Configure Switch IP Settings - CLI
5.6.12 Lab: Configure Management VLAN Settings - CLI
5.6.13 Lesson Review

5.7 Routing and VLAN Troubleshooting

5.7.1 Routing Table Issues
5.7.2 Default Route and Routing Loop Issues
5.7.3 VLAN Assignment Issues
5.7.4 Lesson Review

5.8 Module Quiz

6.0 Implementing Network Services

6.1 Transport and Application Layer Protocols

6.1.1 Transport Layer Ports and Connections
6.1.2 Transmission Control Protocol
6.1.3 TCP Handshake and Teardown
6.1.4 User Datagram Protocol
6.1.5 netstat
6.1.6 Common TCP and UDP Ports
6.1.7 Lab: Explore Three-way Handshake in Wireshark
6.1.8 Lab: View Open Ports with netstat
6.1.9 Lesson Review

6.2 Dynamic Host Configuration Protocol

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 (2:22)
6.2.10 Lab: Configure Client Addressing for DHCP
6.2.11 Lesson Review

6.3 APIPA and SLAAC

6.3.1 Automatic Private IP Addressing
6.3.2 IPv6 Interface Autoconfiguration and Testing
6.3.3 DHCPv6 Server Configuration
6.3.4 Lab: Explore APIPA Addressing
6.3.5 Lab: Explore APIPA Addressing in Network Modeler
6.3.6 Set Up Alternate Addressing (3:33)
6.3.7 Lesson Review

6.4 DHCP Relay and Troubleshooting

6.4.1 DHCP Relay and IP Helper
6.4.2 DHCP Issues
6.4.3 Troubleshooting DHCP Exhaustion (4:09)
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 Applied Live Lab: Troubleshoot Address Pool Exhaustion
6.4.8 Lab: Explore DHCP Troubleshooting
6.4.9 Lab: Troubleshoot IP Configuration 1
6.4.10 Lab: Troubleshoot IP Configuration 2
6.4.11 Lab: Troubleshoot IP Configuration 3
6.4.12 Lesson Review

6.5 Domain Name System

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 (4:24)
6.5.17 Applied Live Lab: Configure DNS Records
6.5.18 Lesson Review

6.6 DNS Troubleshooting

- 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
- 6.6.7 Applied Live Lab: Report DNS Configuration
- 6.6.8 Lesson Review

6.7 Module Quiz

6.8 Checkpoint Review

7.0 Explaining Application Services

7.1 Application Security and Time Synchronization

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
7.1.5 Applied Live Lab: Troubleshoot Time Synchronization Issues
7.1.6 Lesson Review

7.2 Web, File, Print, and Database Services

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
7.2.5 Server Message Block
7.2.6 Network Attached Storage
7.2.7 Database Services
7.2.8 Live Lab: Verify Secure Web Services
7.2.9 Lab: Scan for Web Services with Nmap
7.2.10 Lesson Review

7.3 Email and Voice 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
7.3.8 Lesson Review

7.4 Disaster Recovery and High Availability

- 7.4.1 Disaster Recovery Concepts
- 7.4.2 Disaster Recovery Metrics
- 7.4.3 Disaster Recovery Sites
- 7.4.4 Fault Tolerance and Redundancy
- 7.4.5 Load Balancers
- 7.4.6 High Availability Clusters
- 7.4.7 First Hop Redundancy
- 7.4.8 Lab: Configure NIC Teaming
- 7.4.9 Live Lab: Configure First Hop Redundancy
- 7.4.10 Lesson Review

7.5 Module Quiz

8.0 Supporting Network Management

8.1 Organizational Policies and Documentation

8.1.1 Configuration Management
8.1.2 Network Device Backup Management
8.1.3 Live Lab: Backup and Restore Network Appliances
8.1.4 Change Management
8.1.5 Asset Inventory Documentation
8.1.6 Lifecycle Management
8.1.7 Decommissioning
8.1.8 Physical Network Diagrams
8.1.9 Logical Network Diagrams
8.1.10 IP Address Management
8.1.11 Common Agreements
8.1.12 Lab: Update Firmware
8.1.13 Live Lab: Update Network Documentation
8.1.14 Lesson Review

8.2 Host Discovery and Monitoring

8.2.1 Network Discovery
8.2.2 Nmap
8.2.3 Nmap Port Scanning
8.2.4 Discovery Protocols
8.2.5 Performance Monitoring
8.2.6 Availability Monitoring
8.2.7 Configuration Monitoring
8.2.8 Lab: Scan Using Zenmap
8.2.9 Applied Live Lab: Perform Network Discovery
8.2.10 Lesson Review

8.3 Simple Network Management Protocol

8.3.1 SNMP Agents and Monitors
8.3.2 SNMP Security
8.3.3 Configuring an SNMP System on a Router (2:39)
8.3.4 Monitoring a Switch with SNMP (1:56)
8.3.5 Configuring SNMP Trap (5:42)
8.3.6 Applied Live Lab: Configure SNMP
8.3.7 Lesson Review

8.4 Event Management

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
8.4.11 Live Lab: Configure Log Collection
8.4.12 Lesson Review

8.5 Packet Capture and Analysis

8.5.1 Packet Capture
8.5.2 tcpdump
8.5.3 Protocol Analyzers
8.5.4 Using Wireshark to Troubleshoot Network Issues (4:23)
8.5.5 Lab: Troubleshoot with Wireshark
8.5.6 Lab: Configure Port Mirroring
8.5.7 Lesson Review

8.6 Traffic Monitoring

8.6.1 Common Performance Issues
8.6.2 Interface Statistics
8.6.3 Flow Data
8.6.4 Traffic Testing Tools
8.6.5 Bandwidth Management
8.6.6 Traffic Shaping
8.6.7 Lab: Configure QoS
8.6.8 Monitoring Interface Statistics (5:09)
8.6.9 Live Lab: Configure Flow Collection and Analysis
8.6.10 Applied Live Lab: Troubleshoot Network Service Issues
8.6.11 Lesson Review

8.7 Module Quiz

9.0 Explaining Network Security Concepts

9.1 Security Concepts

- 9.1.1 Common Security Terminology
- 9.1.2 Security Audits and Assessments
- 9.1.3 Regulatory Compliance
- 9.1.4 Encryption
- 9.1.5 Vulnerability and Exploit Types
- 9.1.6 Deception Technologies
- 9.1.7 Lab: Create a Honeypot
- 9.1.8 Lesson Review

9.2 Network Threats and Attacks

- 9.2.1 Threat Types and Assessment
- 9.2.2 Attack Types
- 9.2.3 Distributed DoS Attacks and Botnets
- 9.2.4 Malware Attacks
- 9.2.5 Lab: Analyze a DoS Attack
- 9.2.6 Lab: Analyze a DDoS Attack
- 9.2.7 Lesson Review

9.3 Spoofing Attacks

- 9.3.1 On-Path Attacks
- 9.3.2 Performing an On-Path DHCP Attack (6:59)
- 9.3.3 Poison ARP (5:45)
- 9.3.4 MAC Flooding Attack
- 9.3.5 Using SMAC to Spoof MAC Addresses (3:46)
- 9.3.6 VLAN Hopping Attacks
- 9.3.7 Lab: Poison ARP and Analyze with Wireshark
- 9.3.8 Lab: Spoof MAC Addresses with SMAC
- 9.3.9 Lab: Perform a DHCP Spoofing On-Path Attack
- 9.3.10 Lesson Review

9.4 Rogue System Attacks

9.4.1 Rogue Devices and Services
9.4.2 Rogue DHCP
9.4.3 Setting Up DHCP Snooping (1:45)
9.4.4 DNS Attacks
9.4.5 Poisoning DNS (6:19)
9.4.6 Lab: Discover a Rogue DHCP Server
9.4.7 Lab: Configure DHCP Snooping
9.4.8 Lab: Poison DNS
9.4.9 Lab: Analyze DNS Spoofing
9.4.10 Applied Live Lab: Analyze Network Attacks
9.4.11 Lesson Review

9.5 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
9.5.5 Lesson Review

9.6 Module Quiz

9.7 Checkpoint Review

10.0 Applying Network Security Features

10.1 Authentication

- 10.1.1 Access Control
- 10.1.2 Authentication Methods
- 10.1.3 Local Authentication
- 10.1.4 Single Sign-On and Kerberos
- 10.1.5 Digital Certificates and PKI
- 10.1.6 Key Management
- 10.1.7 Federated Identity and SAML
- 10.1.8 Remote Authentication
- 10.1.9 Live Lab: Deploy a Digital Certificate
- 10.1.10 Lesson Review

10.2 Authorization and Account Management

- 10.2.1 Authorization and Role-Based Access Control
- 10.2.2 Privileged Access Management
- 10.2.3 Lightweight Directory Access Protocol
- 10.2.4 LDAP Secure
- 10.2.5 Lab: Manage Account Policies
- 10.2.6 Live Lab: Configure Management Privileges
- 10.2.7 Lesson Review

10.3 Network 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 (4:51)
- 10.3.5 Lab: Scan for Unsecure Protocols
- 10.3.6 Lab: Enable and Disable Linux Services
- 10.3.7 Lab: Disable Network Service
- 10.3.8 Lesson Review

10.4 Switch 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
10.4.5 Extensible Authentication Protocol and IEEE 802.1X
10.4.6 Port Guards
10.4.7 Lab: Harden a Switch
10.4.8 Port Mirroring
10.4.9 Lesson Review

10.5 Network Security Rules

10.5.1 Security Rules and ACL Configuration
10.5.2 Proxy Servers
10.5.3 Content Filtering
10.5.4 Misconfigured Firewall and ACL Issues
10.5.5 Creating Firewall ACLs (5:51)
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
10.5.12 Applied Live Lab: Troubleshoot Service and Security Issues
10.5.13 Lesson Review

10.6 Module Quiz

11.0 Supporting Network Security Design

11.1 Zone-based Security

- 11.1.1 Network Security Zones
- 11.1.2 Configuring a Screened Subnet (3:40)
- 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
- 11.1.7 Intrusion Detection and Prevention Systems
- 11.1.8 Implementing Intrusion Detection and Prevention (6:18)
- 11.1.9 Lab: Implement Intrusion Prevention
- 11.1.10 Lesson Review

11.2 Internet of Things

- 11.2.1 IoT Devices
- 11.2.2 Industrial Embedded Systems
- 11.2.3 IoT Networks
- 11.2.4 IoT Network Security
- 11.2.5 Lab: Scan for IoT Devices
- 11.2.6 Lesson Review

11.3 Physical Security

- 11.3.1 Locks
- 11.3.2 Cameras
- 11.3.3 Geofencing
- 11.3.4 Lab: Implement Physical Security
- 11.3.5 Lesson Review

11.4 Module Quiz

12.0 Configuring Wireless Networks

12.1 Wireless Concepts and Standards

12.1.1 IEEE 802.11 Wireless Standards
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
12.1.6 Multiuser MIMO and Band Steering
12.1.7 Cellular Technologies
12.1.8 Satellite Technologies
12.1.9 Lab: Configure Wireless Profiles
12.1.10 Lesson Review

12.2 Enterprise Wireless Network Design

12.2.1 Infrastructure Network Type
12.2.2 Range and Signal Strength
12.2.3 Wireless Surveys and Heat Maps
12.2.4 Wireless Roaming
12.2.5 Wireless Controllers
12.2.6 Antenna Types
12.2.7 Other Wireless Network Types
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
12.2.11 Lesson Review

12.3 Wireless Security

12.3.1 Wi-Fi Encryption Standards
12.3.2 Personal Authentication
12.3.3 Enterprise Authentication
12.3.4 Guest Networks and Captive Portals
12.3.5 Bring Your Own Device Issues
12.3.6 Wireless Network Attacks
12.3.7 Lab: Configure a Captive Portal
12.3.8 Lab: Create a Guest Network for BYOD
12.3.9 Lab: Secure an Enterprise Wireless Network
12.3.10 Lab: Secure a Home Wireless Network
12.3.11 Lab: Enable Wireless Intrusion Prevention
12.3.12 Lesson Review

12.4 Wireless Troubleshooting

12.4.1 Wireless Performance Assessment
12.4.2 Insufficient Wireless Coverage Issues
12.4.3 Channel Overlap Issues
12.4.4 Interference Issues
12.4.5 Roaming and Client Disassociation Issues
12.4.6 Overcapacity 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
12.4.10 Lesson Review

12.5 Module Quiz

12.6 Checkpoint Review

13.0 Comparing Remote Access Methods

13.1 WAN and Internet Connectivity

- 13.1.1 Wide Area Networks and the OSI Model
- 13.1.2 Internet Access Types
- 13.1.3 Fiber to the Curb and Fiber to the Premises
- 13.1.4 Lesson Review

13.2 Virtual Private Networks

- 13.2.1 Remote Access Considerations
- 13.2.2 Tunneling Protocols
- 13.2.3 Internet Protocol Security
- 13.2.4 Internet Key Exchange
- 13.2.5 Client-to-Site VPNs
- 13.2.6 Clientless VPNs
- 13.2.7 Site-to-Site VPNs
- 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
- 13.2.11 Lesson Review

13.3 Remote Management

- 13.3.1 Remote Host Access
- 13.3.2 Secure Shell
- 13.3.3 Telnet
- 13.3.4 Remote Desktop Protocol
- 13.3.5 Console Connections and Out-of-Bound Management
- 13.3.6 Jump Boxes
- 13.3.7 API Connection Methods
- 13.3.8 Lab: Allow Remote Desktop Connections
- 13.3.9 Lab: Use PowerShell Remote
- 13.3.10 Live Lab: Configure a Jump Box
- 13.3.11 Lesson Review

13.4 Module Quiz

14.0 Summarizing Cloud Concepts

14.1 Datacenter and Storage Networks

- 14.1.1 Data Center Network Design
- 14.1.2 Spine and Leaf Topology
- 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
- 14.1.7 Lesson Review

14.2 Cloud Concepts

- 14.2.1 Cloud Scalability and Elasticity
- 14.2.2 Cloud Deployment Models
- 14.2.3 Cloud Service Models
- 14.2.4 Content Delivery Networks
- 14.2.5 Lab: Live Deploy a Cloud VM
- 14.2.6 Lesson Review

14.3 Cloud Networking

- 14.3.1 Cloud Instances
- 14.3.2 Virtual Private Clouds
- 14.3.3 Cloud Gateways
- 14.3.4 Cloud Connectivity Options
- 14.3.5 Cloud Firewall Security
- 14.3.6 Security Groups and Security Lists
- 14.3.7 Live Lab: Configure Cloud Networking
- 14.3.8 Lesson Review

14.4 Modern Network Environments

14.4.1 Infrastructure as Code
14.4.2 Uses for Infrastructure as Code
14.4.3 Source Control
14.4.4 Software-Defined Networking
14.4.5 Software-Defined WAN
14.4.6 Overlay Networks
14.4.7 Zero Trust Architecture
14.4.8 Secure Access Service Edge
14.4.9 Lesson Review

14.5 Module Quiz

A.0 Network Sandbox

A.1 Network Sandbox Lab

B.0 CompTIA Network+ N10-009 Practice Exams

B.1 Prepare for CompTIA Network+ Certification

B.1.1 Why Should I Take a Certification Exam?

B.1.2 Exam Details for CompTIA Network+ N10-009

B.1.3 Exam Objectives for CompTIA Network+ N10-009

B.1.4 Course Mapping with CompTIA Network+ N10-009 Exam Objectives

B.1.5 How to Take the Certification Exam

B.1.6 Tips for Taking the Certification Exam

B.2 CompTIA Network+ N10-009 Practice Materials

B.2.1 Exam Practice 1: Networking Concepts

B.2.2 Exam Practice 2: Network Implementations

B.2.3 Exam Practice 3: Network Operations

B.2.4 Exam Practice 4: Network Security

B.2.5 Exam Practice 5: Network Troubleshooting

B.2.6 Skills Practice: Competency in Networking

B.2.7 Practice Test: CompTIA Network+ N10-009