Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html#header)

**Appendix**

**A**

**CompTIA Network+ N10-008 Certification Exam Objectives**

* Appendix Introduction
* Domain 1.0 Networking Fundamentals—24% of Examination
* Domain 2.0 Network Implementations—19% of Examination
* Domain 3.0 Network Operations—16% of Examination
* Domain 4.0 Network Security—19% of Examination
* Domain 5.0 Network Troubleshooting—22% of Examination

Go to pg.

**help**

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html#header)

Appendix Introduction

This text covers material related to all the examination objectives for the CompTIA Network+ exam N10-008, which was released by CompTIA (the Computing Technology Industry Association) in 2021. The official list of objectives is available at CompTIA’s website, [comptia.org](http://comptia.org/%22%20%5Ct%20%22_blank). For your reference, the following tables list each exam objective and the module of this course that explains the objective, plus the amount of the exam that will cover each certification domain. Each objective belongs to one of five domains (or main categories) of networking expertise. For example, the task of comparing and contrasting different 802.11 standards belongs to Objective 2.4 in the “Network Implementations” domain, which altogether accounts for 19 percent of the exam’s content.

| **Domain** | **Percentage of examination** |
| --- | --- |
| 1.0 Networking Fundamentals | 24% |
| 2.0 Network Implementations | 19% |
| 3.0 Network Operations | 16% |
| 4.0 Network Security | 19% |
| 5.0 Network Troubleshooting | 22% |
| **Total** | **100%** |

As you read through the exam objectives, pay close attention to the verbs used in each objective, as these words indicate how deeply you should know the content listed. For example, an objective that says, “Explain the purposes …” or “Compare and contrast …” expects you to understand the concepts listed, be able to identify those concepts in a scenario, and answer questions about the concepts. However, an objective that says, “Given a scenario, use …” or “Given a scenario, implement …” expects you to be able to put those concepts to work. Any objective that begins with the words “Given a scenario” is likely to show up on the exam as a performance-based question rather than simply as a multiple-choice question.

Go to pg.

**help**

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html#header)

Domain 1.0 Networking Fundamentals—24% of Examination





Go to pg.

**help**

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html#header)

Domain 2.0 Network Implementations—19% of Examination

| **Objective** | **Section** | **Bloom’s Taxonomy** |
| --- | --- | --- |
| * 2.1

**Compare and contrast various devices, their features, and their appropriate placement on the network.*** + Networking devices
		- Layer 2 switch
		- Layer 3 capable switch
		- Router
		- Hub
		- Access point
		- Bridge
		- Wireless LAN controller
		- Load balancer
		- Proxy server
		- Cable modem
		- DSL modem
		- Repeater
		- Voice gateway
		- Media converter
		- Intrusion prevention system (IPS)/intrusion detection system (IDS) device
		- Firewall
		- VPN headend
	+ Networked devices
		- Voice over Internet Protocol (VoIP) phone
		- Printer
		- Physical access control devices
		- Cameras
		- Heating, ventilation, and air conditioning (HVAC) sensors
		- Internet of Things (IoT)
			* Refrigerator
			* Smart speakers
			* Smart thermostats
			* Smart doorbells
		- Industrial control systems/supervisory control and data acquisition (SCADA)
 | 1: Network Hardware1: The Seven-Layer OSI Model2: Components of Structured Cabling3: Ports and Sockets4: Remote Access Protocols5: Transmission Basics5: Fiber-Optic Cable6: Characteristics of Wireless Transmissions7: Physical Architecture7: Network Availability9: WAN Connectivity10: Physical Security11: Network Security Tools | Understand |
| * 2.2

**Compare and contrast routing technologies and bandwidth management concepts.*** + Routing
		- Dynamic routing
			* Protocols [Routing Internet Protocol (RIP), Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Border Gateway Protocol (BGP)]
			* Link state vs. distance vector vs. hybrid
		- Static routing
		- Default route
		- Administrative distance
		- Exterior vs. interior
		- Time to live
	+ Bandwidth management
		- Traffic shaping
		- Quality of service (QoS)
 | 9: Routing Protocols9: WAN Connectivity12: Manage Network Traffic | Understand |
| * 2.3

**Given a scenario, configure and deploy common Ethernet switching features.*** + Data virtual local area network (VLAN)
	+ Voice VLAN
	+ Port configurations
		- Port tagging/802.1Q
		- Port aggregation
			* Link Aggregation Control Protocol (LACP)
		- Duplex
		- Speed
		- Flow control
		- Port mirroring
		- Port security
		- Jumbo frames
		- Auto-medium-dependent interface crossover (MDI-X)
	+ Media access control (MAC) address tables
	+ Power over Ethernet (PoE)/Power over Ethernet plus (PoE+)
	+ Spanning Tree Protocol
	+ Carrier-sense multiple access with collision detection (CSMA/CD)
	+ Address Resolution Protocol (ARP)
	+ Neighbor Discovery Protocol
 | 3: Addressing Overview4: TCP/IP Core Protocols5: Transmission Basics5: Copper Cable7: Physical Architecture7: Network Availability8: Virtual LANs (VLANs)11: Network Security Tools12: Collect Network Data12: Manage Network Traffic | Apply |
| * 2.4

**Given a scenario, install and configure the appropriate wireless standards and technologies.*** + 802.11 standards
		- a
		- b
		- g
		- n (WiFi 4)
		- ac (WiFi 5)
		- ax (WiFi 6)
	+ Frequencies and range
		- 2.4GHz
		- 5GHz
	+ Channels
		- Regulatory impacts
	+ Channel bonding
	+ Service set identifier (SSID)
		- Basic service set
		- Extended service set
		- Independent basic service set (Ad-hoc)
		- Roaming
	+ Antenna types
		- Omni
		- Directional
	+ Encryption standards
		- WiFi Protected Access (WPA)/WPA2 Personal [Advanced Encryption Standard (AES)/Temporal Key Integrity Protocol (TKIP)]
		- WPA/WPA2 Enterprise (AES/TKIP)
	+ Cellular technologies
		- Code-division multiple access (CDMA)
		- Global System for Mobile Communications (GSM)
		- Long-Term Evolution (LTE)
		- 3G, 4G, 5G
	+ Multiple input, multiple output (MIMO) and multi-user MIMO (MU-MIMO)
 | 6: Characteristics of Wireless Transmissions9: Wireless WANs | Apply |



Go to pg.

**help**

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html#header)

Domain 3.0 Network Operations—16% of Examination

| **Objective** | **Section** | **Bloom’s Taxonomy** |
| --- | --- | --- |
| * 3.1

**Given a scenario, use the appropriate statistics and sensors to ensure network availability.*** + Performance metrics/sensors
		- Device/chassis
			* Temperature
			* Central processing unit (CPU) usage
			* Memory
		- Network metrics
			* Bandwidth
			* Latency
			* Jitter
	+ SNMP
		- Traps
		- Object identifiers (OIDs)
		- Management information bases (MIBs)
	+ Network device logs
		- Log reviews
			* Traffic logs
			* Audit logs
			* Syslog
		- Logging levels/severity levels
	+ Interface statistics/status
		- Link state (up/down)
		- Speed/duplex
		- Send/receive traffic
		- Cyclic redundancy checks (CRCs)
		- Protocol packet and byte counts
	+ Interface errors or alerts
		- CRC errors
		- Giants
		- Runts
		- Encapsulation errors
	+ Environmental factors and sensors
		- Temperature
		- Humidity
		- Electrical
		- Flooding
	+ Baselines
	+ NetFlow data
	+ Uptime/downtime
 | 2: Components of Structured Cabling5: Transmission Basics7: Cloud Architecture9: Troubleshooting Connections12: Collect Network Data12: Manage Network Traffic | Apply |
| * 3.2

**Explain the purpose of organizational documents and policies.*** + Plans and procedures
		- Change management
		- Incident response plan
		- Disaster recovery plan
		- Business continuity plan
		- System life cycle
		- Standard operating procedures
	+ Hardening and security policies
		- Password policy
		- Acceptable use policy
		- Bring your own device (BYOD) policy
		- Remote access policy
		- Onboarding and offboarding policy
		- Security policy
		- Data loss prevention
	+ Common documentation
		- Physical network diagram
			* Floor plan
			* Rack diagram
			* Intermediate distribution frame (IDF)/main distribution frame (MDF) documentation
		- Logical network diagram
		- Wiring diagram
		- Site survey report
		- Audit and assessment report
		- Baseline configurations
	+ Common agreements
		- Non-disclosure agreement (NDA)
		- Service-level agreement (SLA)
		- Memorandum of understanding (MOU)
 | 2: Network Documentation2: Change Management4: Remote Access Protocols10: Security Risks10: Security Assessment10: Device Hardening10: Security Policies for Users12: Plan Response and Recovery Strategies | Understand |
| * 3.3

**Explain high availability and disaster recovery concepts and summarize which is the best solution.*** + Load balancing
	+ Multipathing
	+ Network interface card (NIC) teaming
	+ Redundant hardware/clusters
		- Switches
		- Routers
		- Firewalls
	+ Facilities and infrastructure support
		- Uninterruptible power supply (UPS)
		- Power distribution units (PDUs)
		- Generator
		- HVAC
		- Fire suppression
	+ Redundancy and high availability (HA) concepts
		- Cold site
		- Warm site
		- Hot site
		- Cloud site
		- Active-active vs. active-passive
			* Multiple Internet service providers (ISPs)/diverse paths
			* Virtual Router Redundancy Protocol (VRRP)/First Hop Redundancy Protocol (FHRP)
		- Mean time to repair (MTTR)
		- Mean time between failure (MTBF)
		- Recovery time objective (RTO)
		- Recovery point objective (RPO)
	+ Network device backup/restore
		- State
		- Configuration
 | 1: Safety Procedures and Policies2: Components of Structured Cabling7: Physical Architecture7: Network Availability9: Routing Protocols11: Network Security Tools12: Plan Response and Recovery Strategies | Understand |



Go to pg.

**help**

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html#header)

Domain 4.0 Network Security—19% of Examination

| **Objective** | **Section** | **Bloom’s Taxonomy** |
| --- | --- | --- |
| * 4.1

**Explain common security concepts.*** + Confidentiality, integrity, availability (CIA)
	+ Threats
		- Internal
		- External
	+ Vulnerabilities
		- Common vulnerabilities and exposures (CVE)
		- Zero-day
	+ Exploits
	+ Least privilege
	+ Role-based access
	+ Zero Trust
	+ Defense in depth
		- Network segmentation enforcement
		- Screened subnet [previously known as demilitarized zone (DMZ)]
		- Separation of duties
		- Network access control
		- Honeypot
	+ Authentication methods
		- Multifactor
		- Terminal Access Controller Access-Control System Plus (TACACS+)
		- Single sign-on (SSO)
		- Remote Authentication Dial-in User Service (RADIUS)
		- LDAP
		- Kerberos
		- Local authentication
		- 802.1X
		- Extensible Authentication Protocol (EAP)
	+ Risk Management
		- Security risk assessments
			* Threat assessment
			* Vulnerability assessment
			* Penetration testing
			* Posture assessment
		- Business risk assessments
			* Process assessment
			* Vendor assessment
	+ Security information and event management (SIEM)
 | 4: Encryption Protocols4: Troubleshooting Network Issues6: Wi-Fi Network Security7: Physical Architecture8: Network Segmentation8: Virtual LANs (VLANs)10: Security Risks10: Security Assessment10: Device Hardening11: Network Hardening by Design11: Network Security Tools11: Authentication, Authorization, and Accounting (AAA)11: Authentication Technologies | Understand |
| * 4.2

**Compare and contrast common types of attacks.*** + Technology-based
		- Denial-of-service (DoS)/distributed denial-of-service (DDoS)
			* Botnet/command and control
		- On-path attack (previously known as man-in-the-middle attack)
		- DNS poisoning
		- VLAN hopping
		- ARP spoofing
		- Rogue DHCP
		- Rogue access point (AP)
		- Evil twin
		- Ransomware
		- Password attacks
			* Brute-force
			* Dictionary
		- MAC spoofing
		- IP spoofing
		- Deauthentication
		- Malware
	+ Human and environmental
		- Social engineering
			* Phishing
			* Tailgating
			* Piggybacking
			* Shoulder surfing
 | 4: Remote Access Protocols4: Troubleshooting Network Issues6: Wi-Fi Network Security8: Virtual LANs (VLANs)10: Security Risks10: Security Policies for Users11: Network Hardening by Design | Understand |
| * 4.3

**Given a scenario, apply network hardening techniques.*** + Best practices
		- Secure SNMP
		- Router Advertisement (RA) Guard
		- Port security
		- Dynamic ARP inspection
		- Control plane policing
		- Private VLANs
		- Disable unneeded switchports
		- Disable unneeded network services
		- Change default passwords
		- Password complexity/length
		- Enable DHCP snooping
		- Change default VLAN
		- Patch and firmware management
		- Access control list
		- Role-based access
		- Firewall rules
			* Explicit deny
			* Implicit deny
	+ Wireless security
		- MAC filtering
		- Antenna placement
		- Power levels
		- Wireless client isolation
		- Guest network isolation
		- Preshared keys (PSKs)
		- EAP
		- Geofencing
		- Captive portal
	+ IoT access considerations
 | 2: Change Management6: Wi-Fi Network Security7: Physical Architecture8: Virtual LANs (VLANs)10: Device Hardening10: Security Policies for Users11: Network Hardening by Design11: Network Security Tools11: Authentication, Authorization, and Accounting (AAA)12: Collect Network Data | Apply |
| * 4.4

**Compare and contrast remote access methods and security implications.*** + Site-to-site VPN
	+ Client-to-site VPN
		- Clientless VPN
		- Split tunnel vs. full tunnel
	+ Remote desktop connection
	+ Remote desktop gateway
	+ SSH
	+ Virtual network computing (VNC)
	+ Virtual desktop
	+ Authentication and authorization considerations
	+ In-band vs. out-of-band management
 | 4: Remote Access Protocols11: Authentication, Authorization, and Accounting (AAA) | Understand |
| * 4.5

**Explain the importance of physical security.*** + Detection methods
		- Camera
		- Motion detection
		- Asset tags
		- Tamper detection
	+ Prevention methods
		- Employee training
		- Access control hardware
			* Badge readers
			* Biometrics
		- Locking racks
		- Locking cabinets
		- Access control vestibule (previously known as a mantrap)
		- Smart lockers
	+ Asset disposal
		- Factory reset/wipe configuration
		- Sanitize devices for disposal
 | 10: Security Risks10: Physical Security10: Device Hardening | Understand |



Go to pg.

**help**

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html#header)

Domain 5.0 Network Troubleshooting—22% of Examination

| **Objective** | **Section** | **Bloom’s Taxonomy** |
| --- | --- | --- |
| * 5.1

**Explain the network troubleshooting methodology.*** + Identify the problem
		- Gather information
		- Question users
		- Identify symptoms
		- Determine if anything has changed
		- Duplicate the problem, if possible
		- Approach multiple problems individually
	+ Establish a theory of probable cause
		- Question the obvious
		- Consider multiple approaches
			* Top-to-bottom/bottom-to-top OSI model
			* Divide and conquer
	+ Test the theory to determine the cause
		- If the theory is confirmed, determine the next steps to resolve the problem
		- If the theory is not confirmed, reestablish a new theory or escalate
	+ Establish a plan of action to resolve the problem and identify potential effects
	+ Implement the solution or escalate as necessary
	+ Verify full system functionality and, if applicable, implement preventive measures
	+ Document findings, actions, outcomes, and lessons learned
 | 1: Troubleshooting Network Problems | Understand |
| * 5.2

**Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.*** + Specifications and limitations
		- Throughput
		- Speed
		- Distance
	+ Cable considerations
		- Shielded and unshielded
		- Plenum and riser-rated
	+ Cable application
		- Rollover cable/console cable
		- Crossover cable
		- Power over Ethernet
	+ Common issues
		- Attenuation
		- Interference
		- Decibel (dB) loss
		- Incorrect pinout
		- Bad ports
		- Open/short
		- Light-emitting diode (LED) status indicators
		- Incorrect transceivers
		- Duplexing issues
		- Transmit and receive (TX/RX) reversed
		- Dirty optical cables
	+ Common tools
		- Cable crimper
		- Punchdown tool
		- Tone generator
		- Loopback adapter
		- Optical time-domain reflectometer (OTDR)
		- Multimeter
		- Cable tester
		- Wire map
		- Tap
		- Fusion splicers
		- Spectrum analyzers
		- Snips/cutters
		- Cable stripper
		- Fiber light meter
 | 2: Components of Structured Cabling5: Transmission Basics5: Copper Cable5: Fiber-Optic Cable5: Cable Troubleshooting Tools6: Troubleshooting Wi-Fi Networks11: Network Security Tools | Analyze |
| * 5.3

**Given a scenario, use the appropriate network software tools and commands.*** + Software tools
		- WiFi analyzer
		- Protocol analyzer/packet capture
		- Bandwidth speed tester
		- Port scanner
		- iperf
		- NetFlow analyzers
		- Trivial File Transfer Protocol (TFTP) server
		- Terminal emulator
		- IP scanner
	+ Command line tools
		- ping
		- ipconfig/ifconfig/ip
		- nslookup/dig
		- traceroute/tracert
		- arp
		- netstat
		- hostname
		- route
		- telnet
		- tcpdump
		- nmap
	+ Basic network platform commands
		- show interface
		- show config
		- show route
 | 2: Network Documentation3: Troubleshooting Address Problems4: TCP/IP Core Protocols4: Remote Access Protocols4: Troubleshooting Network Issues6: Troubleshooting Wi-Fi Networks9: Routing Protocols9: WAN Connectivity9: Troubleshooting Connections10: Security Assessment12: Collect Network Data12: Manage Network Traffic | Apply |
| * 5.4

**Given a scenario, troubleshoot common wireless connectivity issues.*** + Specifications and limitations
		- Throughput
		- Speed
		- Distance
		- Received signal strength indication (RSSI) signal strength
		- Effective isotropic radiated power (EIRP)/power settings
	+ Considerations
		- Antennas
			* Placement
			* Type
			* Polarization
		- Channel utilization
		- AP association time
		- Site survey
	+ Common issues
		- Interference
			* Channel overlap
		- Antenna cable attenuation/signal loss
		- RF attenuation/signal loss
		- Wrong SSID
		- Incorrect passphrase
		- Encryption protocol mismatch
		- Insufficient wireless coverage
		- Captive portal issues
		- Client disassociation issues
 | 6: Characteristics of Wireless Transmissions6: Wi-Fi Network Security6: Troubleshooting Wi-Fi Networks | Analyze |
| * 5.5

**Given a scenario, troubleshoot general networking issues.*** + Considerations
		- Device configuration review
		- Routing tables
		- Interface status
		- VLAN assignment
		- Network performance baselines
	+ Common issues
		- Collisions
		- Broadcast storm
		- Duplicate MAC address
		- Duplicate IP address
		- Multicast flooding
		- Asymmetrical routing
		- Switching loops
		- Routing loops
		- Rogue DHCP server
		- DHCP scope exhaustion
		- IP setting issues
			* Incorrect gateway
			* Incorrect subnet mask
			* Incorrect IP address
			* Incorrect DNS
		- Missing route
		- Low optical link budget
		- Certificate issues
		- Hardware failure
		- Host-based/network-based firewall settings
		- Blocked services, ports, or addresses
		- Incorrect VLAN
		- DNS issues
		- NTP issues
		- BYOD challenges
		- Licensed feature issues
		- Network performance issues
 | 1: Troubleshooting Network Problems3: IP Addresses3: Troubleshooting Address Problems4: TCP/IP Core Protocols4: Troubleshooting Network Issues5: Fiber-Optic Cable7: Physical Architecture8: Virtual LANs (VLANs)9: Troubleshooting Connections10: Device Hardening10: Security Policies for Users11: Network Hardening by Design11: Network Security Tools12: Manage Network Traffic | Analyze |



Go to pg.

**help**