COMPTIA N10-008

CompTIA Network+ Certification Questions & Answers

Get Instant Access to Vital Exam Acing Materials | Study Guide | Sample Questions | Practice Test

N10-008

CompTIA Certified Network+

90 Questions Exam – 720 / 900 Cut Score – Duration of 90 minutes




EDUSUM

#1 Online Certification Guide

Table of Contents:

Discover More about the N10-008 Certification

Are you interested in passing the CompTIA N10-008 exam? First discover, who benefits from the N10-008 certification. The N10-008 is suitable for a candidate if he wants to learn about Core. Passing the N10-008 exam earns you the CompTIA Certified Network+ title.

While preparing for the N10-008 exam, many candidates struggle to get the necessary materials. But do not worry; your struggling days are over. The N10-008 PDF contains some of the most valuable preparation tips and the details and instant access to useful **N10-008 study materials just at one click.**

CompTIA N10-008 Network+ Certification Details:

Exam Name	CompTIA Certified Network+
Exam Code	N10-008
Exam Price	$358 (USD)
Duration	90 mins
Number of Questions	90
Passing Score	720 / 900
Books / Training	**eLearning** **Virtual Lab** **Study Guides** **Instructor-Led Training**
Schedule Exam	**CompTIA Marketplace** **Pearson VUE**
Sample Questions	**CompTIA Network+ Sample Questions**
Practice Exam	**CompTIA N10-008 Certification Practice Exam**

N10-008 Syllabus:

Topic	Details
Networking Fundamentals - 24%	
Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.	- OSI model • Layer 1 – Physical • Layer 2 – Data link • Layer 3 – Network • Layer 4 – Transport • Layer 5 – Session • Layer 6 – Presentation • Layer 7 – Application - Data encapsulation and decapsulation within the OSI model context • Ethernet header • Internet Protocol (IP) header • Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) headers • TCP flags • Payload • Maximum transmission unit (MTU)
Explain the characteristics of network topologies and network types.	- Mesh - Star/hub-and-spoke - Bus - Ring - Hybrid - Network types and characteristics • Peer-to-peer • Client-server • Local area network (LAN) • Metropolitan area network (MAN)

Topic	Details
	• Wide area network (WAN) • Wireless local area network (WLAN) • Personal area network (PAN) • Campus area network (CAN) • Storage area network (SAN) • Software-defined wide area network (SDWAN) • Multiprotocol label switching (MPLS) • Multipoint generic routing encapsulation (mGRE) - Service-related entry point • Demarcation point • Smartjack - Virtual network concepts • vSwitch • Virtual network interface card (vNIC) • Network function virtualization (NFV) • Hypervisor - Provider links • Satellite • Digital subscriber line (DSL) • Cable • Leased line • Metro-optical
Summarize the types of cables and connectors and explain which is the appropriate type for a solution.	- Copper • Twisted pair 1. Cat 5 2. Cat 5e 3. Cat 6 4. Cat 6a 5. Cat 7 6. Cat 8 • Coaxial/RG-6

Topic	Details
	• Twinaxial • Termination standards 1. TIA/EIA-568A 2. TIA/EIA-568B - Fiber • Single-mode • Multimode - Connector types • Local connector (LC), straight tip (ST), subscriber connector (SC), mechanical transfer (MT), registered jack (RJ) 1. Angled physical contact (APC) 2. Ultra-physical contact (UPC) • RJ11 • RJ45 • F-type connector • Transceivers/media converters • Transceiver type 1. Small form-factor pluggable (SFP) 2. Enhanced form-factor pluggable (SFP+) 3. Quad small form-factor pluggable (QSFP) 4. Enhanced quad small form-factor pluggable (QSFP+) - Cable management • Patch panel/patch bay • Fiber distribution panel • Punchdown block 1. 66 2. 110 3. Krone 4. Bix - Ethernet standards

Topic	Details
	• Copper 1. 10BASE-T 2. 100BASE-TX 3. 1000BASE-T 4. 10GBASE-T 5. 40GBASE-T • Fiber 1. 100BASE-FX 2. 100BASE-SX 3. 1000BASE-SX 4. 1000BASE-LX 5. 10GBASE-SR 6. 10GBASE-LR 7. Coarse wavelength division multiplexing (CWDM) 8. Dense wavelength division multiplexing (DWDM) 9. Bidirectional wavelength division multiplexing (WDM)
Given a scenario, configure a subnet and use appropriate IP addressing schemes.	- Public vs. private • RFC1918 • Network address translation (NAT) • Port address translation (PAT) - IPv4 vs. IPv6 • Automatic Private IP Addressing (APIPA) • Extended unique identifier (EUI-64) • Multicast • Unicast • Anycast • Broadcast • Link local • Loopback • Default gateway - IPv4 subnetting

Topic	Details
	• Classless (variable-length subnet mask) • Classful 1. A 2. B 3. C 4. D 5. E • Classless Inter-Domain Routing (CIDR) notation - IPv6 concepts • Tunneling • Dual stack • Shorthand notation • Router advertisement • Stateless address autoconfiguration (SLAAC) - Virtual IP (VIP) - Subinterfaces
Explain common ports and protocols, their application, and encrypted alternatives.	- Protocol sand Ports • File Transfer Protocol (FTP) 20/21 • Secure Shell (SSH) 22 • Secure File Transfer Protocol (SFTP) 22 • Telnet 23 • Simple Mail Transfer Protocol (SMTP) 25 • Domain Name System (DNS) 53 • Dynamic Host Configuration Protocol (DHCP) 67/68 • Trivial File Transfer Protocol (TFTP) 69 • Hypertext Transfer Protocol (HTTP) 80 • Post Office Protocol v3 (POP3) 110 • Network Time Protocol (NTP) 123 • Internet Message Access Protocol (IMAP) 143 • Simple Network Management Protocol (SNMP) 161/162

Topic	Details
	• Lightweight Directory Access Protocol (LDAP) 389 • Hypertext Transfer Protocol Secure (HTTPS) [Secure Sockets Layer (SSL)] 443 • HTTPS [Transport Layer Security (TLS)] 443 • Server Message Block (SMB) 445 • Syslog 514 • SMTP TLS 587 • Lightweight Directory Access Protocol (over SSL) (LDAPS) 636 • IMAP over SSL 993 • POP3 over SSL 995 • Structured Query Language (SQL) Server 1433 • SQLnet 1521 • MySQL 3306 • Remote Desktop Protocol (RDP) 3389 • Session Initiation Protocol (SIP) 5060/5061 • IP protocol types 1. Internet Control Message Protocol (ICMP) 2. TCP 3. UDP 4. Generic Routing Encapsulation (GRE) 5. Internet Protocol Security (IPSec) - Authentication Header (AH)/Encapsulating Security Payload (ESP) - Connectionless vs. connection-oriented
Explain the use and purpose of network services.	- DHCP • Scope • Exclusion ranges • Reservation • Dynamic assignment • Static assignment • Lease time • Scope options

Topic	Details
	• Available leases • DHCP relay • IP helper/UDP forwarding - DNS • Record types 1. Address (A vs. AAAA) 2. Canonical name (CNAME) 3. Mail exchange (MX) 4. Start of authority (SOA) 5. Pointer (PTR) 6. Text (TXT) 7. Service (SRV) 8. Name server (NS) • Global hierarchy 1. Root DNS servers • Internal vs. external • Zone transfers • Authoritative name servers • Time to live (TTL) • DNS caching • Reverse DNS/reverse lookup/forward lookup • Recursive lookup/iterative lookup - NTP • Stratum • Clients • Servers
Explain basic corporate and datacenter network architecture.	- Three-tiered • Core • Distribution/aggregation layer • Access/edge - Software-defined networking

Topic	Details
	• Application layer • Control layer • Infrastructure layer • Management plane - Spine and leaf • Software-defined network • Top-of-rack switching • Backbone - Traffic flows • North-South • East-West - Branch office vs. on-premises datacenter vs. colocation - Storage area networks • Connection types 1. Fibre Channel over Ethernet (FCoE) 2. Fibre Channel 3. Internet Small Computer Systems Interface (iSCSI)
Summarize cloud concepts and connectivity options.	- Deployment models • Public • Private • Hybrid • Community - Service models • Software as a service (SaaS) • Infrastructure as a service (IaaS) • Platform as a service (PaaS) • Desktop as a service (DaaS) - Infrastructure as code

Topic	Details
	• Automation/orchestration - Connectivity options • Virtual private network (VPN) • Private-direct connection to cloud provider - Multitenancy - Elasticity - Scalability - Security implications
Network Implementations - 19%	
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

Topic	Details
	• Printer • Physical access control devices • Cameras • Heating, ventilation, and air conditioning (HVAC) sensors • Internet of Things (IoT) 1. Refrigerator 2. Smart speakers 3. Smart thermostats 4. Smart doorbells • Industrial control systems/supervisory control and data acquisition (SCADA)
Compare and contrast routing technologies and bandwidth management concepts.	- Routing • Dynamic routing 1. Protocols [Routing Internet Protocol (RIP), Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Border Gateway Protocol (BGP)] 2. 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)
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 1. Link Aggregation Control Protocol (LACP)

Topic	Details
	• 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
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

Topic	Details
	• 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)
Network Operations - 16%	
Given a scenario, use the appropriate statistics and sensors to ensure network availability.	- Performance metrics/sensors • Device/chassis 1. Temperature 2. Central processing unit (CPU) usage 3. Memory • Network metrics 1. Bandwidth 2. Latency 3. Jitter - SNMP

Topic	Details
	• Traps • Object identifiers (OIDs) • Management information bases (MIBs) - Network device logs • Log reviews 1. Traffic logs 2. Audit logs 3. 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
Explain the purpose of organizational	- Plans and procedures

Topic	Details
documents and policies.	• 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 1. Floor plan 2. Rack diagram 3. 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)

Topic	Details
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 1. Multiple Internet service providers (ISPs)/diverse paths 2. 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

Topic	Details
Network Security - 19%	
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

Topic	Details
	• Extensible Authentication Protocol (EAP) - Risk Management • Security risk assessments 1. Threat assessment 2. Vulnerability assessment 3. Penetration testing 4. Posture assessment • Business risk assessments 1. Process assessment 2. Vendor assessment - Security information and event management (SIEM)
Compare and contrast common types of attacks.	- Technology-based • Denial-of-service (DoS)/distributed denial-of-service (DDoS) 1. 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 1. Brute-force 2. Dictionary • MAC spoofing • IP spoofing • Deauthentication • Malware - Human and environmental

Topic	Details
	• Social engineering 1. Phishing 2. Tailgating 3. Piggybacking 4. Shoulder surfing
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 1. Explicit deny 2. Implicit deny - Wireless security • MAC filtering • Antenna placement • Power levels • Wireless client isolation • Guest network isolation • Preshared keys (PSKs) • EAP

Topic	Details
	• Geofencing • Captive portal - IoT access considerations
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
Explain the importance of physical security.	- Detection methods • Camera • Motion detection • Asset tags • Tamper detection - Prevention methods • Employee training • Access control hardware 1. Badge readers 2. Biometrics • Locking racks • Locking cabinets • Access control vestibule (previously known as a mantrap) • Smart lockers - Asset disposal

Topic	Details
	• Factory reset/wipe configuration • Sanitize devices for disposal
Network Troubleshooting - 22%	
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 1. Top-to-bottom/bottom-to-top OSI model 2. 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
Given a scenario, troubleshoot common cable connectivity	- Specifications and limitations • Throughput • Speed

Topic	Details
issues and select the appropriate tools.	• 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

Topic	Details
	• Fusion splicers • Spectrum analyzers • Snips/cutters • Cable stripper • Fiber light meter
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 tool • ping • ipconfig/ifconfig/ip • nslookup/dig • traceroute/tracert • arp • netstat • hostname • route • telnet • tcpdump • nmap - Basic network platform commands • show interface • show config

Topic	Details
	• show route
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 1. Placement 2. Type 3. Polarization • Channel utilization • AP association time • Site survey - Common issues • Interference 1. 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
Given a scenario, troubleshoot general networking issues.	- Considerations • Device configuration review • Routing tables

Topic	Details
	• 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

Broaden Your Knowledge with CompTIA N10-008 Sample Questions:

Question: 1

You suspect that an intruder has gained access to your network. You want to see how many failed logon attempts were made in one day to help determine how the person got in. Which of the following might you do?

a) Review the history logs.
b) Review the security logs.
c) Review the logon logs.
d) Review the performance logs.

Answer: b

Question: 2

A client on your network has had no problems accessing the wireless network in the past, but recently she moved to a new office. Since the move, she cannot access the network. Which of the following is most likely the cause of the problem?

a) The SSIDs on the client and the AP are different.
b) The SSID has been erased.
c) The client has incorrect broadcast settings.
d) The client system has moved too far from the AP.

Answer: d

Question: 3

Because of a recent security breach, you have been asked to design a security strategy that will allow data to travel encrypted through both the Internet and intranet. Which of the following protocols would you use?

a) IPSec
b) SST
c) CHAP
d) FTP

Answer: a

Question: 4

In an Ethernet network, what technology is being implemented when a system wants to send data to another system and first checks to see whether the network medium is free?

a) QoS
b) MDI-X
c) Jumbo frames
d) CSMA/CD

Answer: d

Question: 5

TCP is an example of what kind of transport protocol?

a) Connection oriented
b) Connection reliant
c) Connection dependent
d) Connectionless

Answer: a

Question: 6

One of the programmers has asked that DHCP always issue his workstation the same IP address. What feature of DHCP enables you to accomplish this?

a) Stipulation
b) Rider
c) Reservation
d) Provision

Answer: c

Question: 7

What are two features supported in SNMPv3 and not previous versions?

a) Authentication
b) Dynamic mapping
c) Platform independence
d) Encryption

Answer: a, d

Question: 8

During a discussion with your ISP's technical support representative, she mentions that you might have been using the wrong FQDN. Which TCP/IP-based network service is she referring to?

a) DHCP
b) WINS
c) SNMP
d) DNS

Answer: d

Question: 9

When a WAN is confined to a certain geographic area, such as a city, it is known as a.

a) LAN
b) MAN
c) VAN
d) VPN

Answer: b

Question: 10

Logical unit numbers (LUNs) came from the SCSI world and use "targets" that hold up to how many devices?

a) 4
b) 6
c) 8
d) 128

Answer: c

Avail the Study Guide to Pass CompTIA N10-008 Network+ Exam:

- Find out about the N10-008 syllabus topics. Visiting the official site offers an idea about the exam structure and other important study resources. Going through the syllabus topics help to plan the exam in an organized manner.
- Once you are done exploring the **N10-008 syllabus**, it is time to plan for studying and covering the syllabus topics from the core. Chalk out the best plan for yourself to cover each part of the syllabus in a hassle-free manner.
- A study schedule helps you to stay calm throughout your exam preparation. It should contain your materials and thoughts like study hours, number of topics for daily studying mentioned on it. The best bet to clear the exam is to follow your schedule rigorously.
- The candidate should not miss out on the scope to learn from the N10-008 training. Joining the CompTIA provided training for N10-008 exam helps a candidate to strengthen his practical knowledge base from the certification.
- Learning about the probable questions and gaining knowledge regarding the exam structure helps a lot. Go through the **N10-008 sample questions** and boost your knowledge
- Make yourself a pro through online practicing the syllabus topics. N10-008 practice tests would guide you on your strengths and weaknesses regarding the syllabus topics. Through rigorous practicing, you can improve the weaker sections too. Learn well about time management during exam and become confident gradually with practice tests.

Career Benefits:

- Passing the N10-008 exam, helps a candidate to prosper highly in his career. Having the certification on the resume adds to the candidate's benefit and helps to get the best opportunities.

Here Is the Trusted Practice Test for the N10-008 Certification

EduSum.Com is here with all the necessary details regarding the N10-008 exam. We provide authentic practice tests for the N10-008 exam. What do you gain from these practice tests? You get to experience the real exam-like questions made by industry experts and get a scope to improve your performance in the actual exam. Rely on EduSum.Com for rigorous, unlimited two-month attempts on the **N10-008 practice tests**, and gradually build your confidence. Rigorous practice made many aspirants successful and made their journey easy towards grabbing the CompTIA Certified Network+.

Start Online Practice of N10-008 Exam by visiting URL
https://www.edusum.com/comptia/n10-008-comptia-network