EDUSUM
#1 Online Certification Guide

COMPTIA N10-008

CompTIA Network+ Certification Questions & Answers

Exam Summary – Syllabus –Questions

N10-008
CompTIA Certified Network+
90 Questions Exam – 720/900 Cut Score – Duration of 90 minutes

Table of Contents:

Know Your N10-008 Certification Well:

The N10-008 is best suitable for candidates who want to gain knowledge in the CompTIA Core. Before you start your N10-008 preparation you may struggle to get all the crucial Network+ materials like N10-008 syllabus, sample questions, study guide.

But don't worry the N10-008 PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-

- What is in the N10-008 syllabus?
- How many questions are there in the N10-008 exam?
- Which Practice test would help me to pass the N10-008 exam at the first attempt?

Passing the N10-008 exam makes you CompTIA Certified Network+. Having the Network+ certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

CompTIA N10-008 Network+ Certification Details:

Exam Name	CompTIA Certified Network+
Exam Code	N10-008
Exam Price	$338 (USD)
Duration	90 mins
Number of Questions	90
Passing Score	720 / 900
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) • Wide area network (WAN) • Wireless local area network (WLAN) • Personal area network (PAN) • Campus area network (CAN)

Topic	Details
	• 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 • Twinaxial • Termination standards 1. TIA/EIA-568A 2. TIA/EIA-568B - Fiber • Single-mode • Multimode

Topic	Details
	- 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 • 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)

Topic	Details
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 • 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	- Protocol sand Ports • File Transfer Protocol (FTP) 20/21 • Secure Shell (SSH) 22

Topic	Details
encrypted alternatives.	- 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 - 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

Topic	**Details**
	• Scope • Exclusion ranges • Reservation • Dynamic assignment • Static assignment • Lease time • Scope options • 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

Topic	Details
	• Access/edge - Software-defined networking • 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 • Automation/orchestration - Connectivity options

Topic	Details
	• 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 • Printer • Physical access control devices • Cameras • Heating, ventilation, and air conditioning (HVAC) sensors • Internet of Things (IoT) 1. Refrigerator 2. Smart speakers

Topic	Details
	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) • 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)

Topic	Details
	- 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 • 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)

Topic	Details
	• 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 • 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

Topic	Details
	- Environmental factors and sensors • Temperature • Humidity • Electrical • Flooding - Baselines - NetFlow data - Uptime/downtime
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 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

Topic	Details
	- Common agreements • Non-disclosure agreement (NDA) • Service-level agreement (SLA) • Memorandum of understanding (MOU)
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 • Extensible Authentication Protocol (EAP) - Risk Management • Security risk assessments 1. Threat assessment 2. Vulnerability assessment

Topic	**Details**
	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 • 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

Topic	Details
	• 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 • 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

Topic	**Details**
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 • 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

Topic	Details
	• 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 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

Topic	Details
	• 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
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

Topic	Details
	• nmap - Basic network platform commands • show interface • show config • 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 • Interface status

Topic	Details
	- 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

CompTIA N10-008 Sample Questions:

Question: 1

A network technician is tasked with troubleshooting intermittent network connectivity issues within an organization. Which of the following are possible network service issues?

(Select TWO)

a) Duplicate IP address
b) Phishing
c) MAC filtering
d) Exhausted DHCP scope
e) NIC teaming
f) Content filter

Answer: a, d

Question: 2

A technician is called to troubleshoot a client PC that is not connecting to the network. The technician first examines the LEDs on the NIC and connection to the wall jack. Then the technician runs a loopback test on the NIC.

Which of the following troubleshooting skills is the technician demonstrating?

a) Inductive reasoning
b) OSI model bottom-to-top
c) Trial-and-error
d) Divide and conquer

Answer: b

Question: 3

Which of the following components should be used to manage multiple virtual machines existing on one host?

a) Hypervisor
b) Virtual router
c) Virtual switch
d) Virtual NIC

Answer: a

Question: 4

A network technician is connecting to a switch to modify the configuration. DHCP is not enabled on the management port.

Which of the following does the technician need to configure to connect to the device?

a) IP address
b) Default gateway
c) DNS address
d) Loopback address

Answer: a

Question: 5

A network technician has been notified that an available wireless SSID is using insecure WEP encryption and has been asked to investigate what other options are available on the existing wireless hardware. The technician has found that the WAPs support AES-CCMP.

Which of the following should the technician configure?

a) WPA2
b) MAC filtering
c) MD5
d) WPS

Answer: a

Question: 6

Users within an office building report wireless connectivity is sporadic. A wireless technician troubleshooting the issue notices there are multiple WAPs visible in the same hallway within 20ft (6m) of one another.

Which of the following is causing the issue?

a) Incorrect antenna type
b) Interference
c) Frequency mismatch
d) Signal reflection

Answer: b

Question: 7

One purpose of network segmentation is to:

a) protect sensitive data from the rest of the network.
b) make file transfers easier for end-users.
c) allow certain services to talk to each other without a choke point
d) hold all hardened baseline images for deployment.

Answer: a

Question: 8

In troubleshooting network performance issues on a computer, a technician finds that the CAT5e cable was run through a conduit with power lines. There is plenty of spare room in the conduit, and a cable continuity test is successful.

Which of the following is the MOST likely issue?

a) Attenuation
b) Crosstalk
c) Incorrect cable type
d) EMI
e) VLAN misconfiguration

Answer: d

Question: 9

Which of the following is aimed at irreversibly damaging and disabling IoT devices?

a) PDoS
b) Spoofing
c) Ransomware
d) Logic bomb
e) MITM

Answer: a

Question: 10

An architect designs the building blueprint for a new office. The IT team has to purchase equipment and cabling.

Upon inspection of the building layout, it is discovered that no designation was made for network infrastructure wiring, cabling, and services for the building.

Which of the following needs to be documented in the blueprint for building connectivity?

a) HVAC
b) Server room
c) MDF
d) Mechanical room

Answer: c

Study Guide to Crack CompTIA Network+ N10-008 Exam:

- Getting details of the N10-008 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the N10-008 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the CompTIA provided training for N10-008 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the N10-008 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on N10-008 practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for N10-008 Certification

Make EduSum.com your best friend during your CompTIA Network+ exam preparation. We provide authentic practice tests for the N10-008 exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual N10-008 exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don’t bother if you don’t get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the N10-008 exam.

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