EDUSUM

#1 Online Certification Guide

CompTIA N10-009 Certification Questions and Answers PDF

CompTIA Network+ CERTIFICATION QUESTIONS & ANSWERS

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

Table of Contents

Getting Ready for the N10-009 Exam:

Use proven study tips and techniques to prepare for the N10-009 exam confidently. Boost your readiness, improve your understanding regarding the Core, and increase your chances of success in the CompTIA Network+ with our comprehensive guide. Start your journey towards exam excellence today.

CompTIA Network+ Certification Details:

Exam Name	CompTIA Network+
Exam Code	N10-009
Exam Price	$369 (USD)
Duration	90 mins
Number of Questions	90
Passing Score	720 / 900
Books / Training	CertMaster Perform Network+ CertMaster Learn Network+ CertMaster Practice for Network+ Training CompTIA Instructor-Led Training
Schedule Exam	Pearson VUE
Sample Questions	CompTIA Network+ Sample Questions
Practice Exam	CompTIA N10-009 Certification Practice Exam

Explore N10-009 Syllabus:

Topic	Details
	Networking Concepts - 23%
Explain concepts related to the Open Systems Interconnection (OSI) reference model.	- Layer 1 - Physical - Layer 2 - Data link - Layer 3 - Network - Layer 4 - Transport - Layer 5 - Session - Layer 6 - Presentation - Layer 7 - Application
Compare and contrast networking appliances, applications, and functions.	- Physical and virtual appliances • Router • Switch • Firewall • Intrusion detection system (IDS)/intrusion prevention system (IPS) • Load balancer • Proxy • Network-attached storage (NAS) • Storage area network (SAN) • Wireless - Access point (AP) - Controller

Topic	Details
	- Applications • Content delivery network (CDN) - Functions • Virtual private network (VPN) • Quality of service (QoS) • Time to live (TTL)
Summarize cloud concepts and connectivity options.	- Network functions virtualization (NFV) - Virtual private cloud (VPC) - Network security groups - Network security lists - Cloud gateways • Internet gateway • Network address translation (NAT) gateway - Cloud connectivity options • VPN • Direct Connect - Deployment models • Public • Private • Hybrid - Service models • Software as a service (SaaS) • Infrastructure as a service (IaaS) • Platform as a service (PaaS) - Scalability - Elasticity - Multitenancy
Explain common networking ports, protocols, services, and traffic types.	- Protocols • File Transfer Protocol (FTP) • Secure File Transfer Protocol (SFTP) • Secure Shell (SSH) • Telnet • Simple Mail Transfer Protocol (SMTP) • Domain Name System (DNS) • Dynamic Host Configuration Protocol (DHCP) • Trivial File Transfer Protocol (TFTP) • Hypertext Transfer Protocol (HTTP) • Network Time Protocol (NTP) • Simple Network Management Protocol (SNMP) • Lightweight Directory Access Protocol (LDAP) • Hypertext Transfer Protocol Secure (HTTPS) • Server Message Block (SMB) • Syslog • Simple Mail Transfer Protocol Secure (SMTPS) • Lightweight Directory Access Protocol over SSL (LDAPS) • Structured Query Language (SQL) Server • Remote Desktop Protocol (RDP) • Session Initiation Protocol (SIP) - Ports • 20/21 • 22

Topic	Details
	• 22 • 23 • 25 • 53 • 67/68 • 69 • 80 • 123 • 161/162 • 389 • 443 • 445 • 514 • 587 • 636 • 1433 • 3389 • 5060/5061 - Internet Protocol (IP) types • Internet Control Message Protocol (ICMP) • Transmission Control Protocol (TCP) • User Datagram Protocol (UDP) • Generic Routing Encapsulation (GRE) • Internet Protocol Security (IPSec) - Authentication Header (AH) - Encapsulating Security Payload (ESP) - Internet Key Exchange (IKE) • Traffic types - Unicast - Multicast - Anycast - Broadcast
Compare and contrast transmission media and transceivers.	- Wireless • 802.11 standards • Cellular • Satellite - Wired • 802.3 standards • Single-mode vs. multimode fiber • Direct attach copper (DAC) cable - Twinaxial cable • Coaxial cable • Cable speeds • Plenum vs. non-plenum cable - Transceivers • Protocol - Ethernet - Fibre Channel (FC) • Form factors - Small form-factor pluggable (SFP) - Quad small form-factor pluggable (QSFP)

Topic	Details
	- Connector types • Subscriber connector (SC) • Local connector (LC) • Straight tip (ST) • Multi-fiber push on (MPO) • Registered jack (RJ)11 • RJ45 • F-type
Compare and contrast network topologies, architectures, and types.	- Mesh - Hybrid - Star/hub and spoke - Spine and leaf - Point to point - Three-tier hierarchical model • Core • Distribution • - Access - Collapsed core - Traffic flows • North-south • East-west
Given a scenario, use appropriate IPv4 network addressing.	- Public vs. private • Automatic Private IP Addressing (APIPA) • RFC1918 • Loopback/localhost - Subnetting • Variable Length Subnet Mask (VLSM) • Classless Inter-domain Routing (CIDR) - IPv4 address classes • Class A • Class B • Class C • Class D • Class E
Summarize evolving use cases for modern network environments.	- Software-defined network (SDN) and software-defined wide area network (SD-WAN) • Application aware • Zero-touch provisioning • Transport agnostic • Central policy management - Virtual Extensible Local Area Network (VXLAN) • Data center interconnect (DCI) • Layer 2 encapsulation - Zero trust architecture (ZTA) • Policy-based authentication • Authorization • Least privilege access - Secure Access Secure Edge (SASE)/Security Service Edge (SSE) - Infrastructure as code (IaC) • Automation - Playbooks/templates/reusable tasks

Topic	Details
	- Configuration drift/compliance - Upgrades - Dynamic inventories • Source control - Version control - Central repository - Conflict identification - Branching - IPv6 addressing • Mitigating address exhaustion • Compatibility requirements - Tunneling - Dual stack - NAT64
Network Implementation - 20%	
Explain characteristics of routing technologies.	- Static routing - Dynamic routing • Border Gateway Protocol (BGP) • Enhanced Interior Gateway Routing Protocol (EIGRP) • Open Shortest Path First (OSPF) - Route selection • Administrative distance • Prefix length • Metric - Address translation • NAT • Port address translation (PAT) - First Hop Redundancy Protocol (FHRP) - Virtual IP (VIP) - Subinterfaces
Given a scenario, configure switching technologies and features.	- Virtual Local Area Network (VLAN) • VLAN database • Switch Virtual Interface (SVI) - Interface configuration • Native VLAN • Voice VLAN • 802.1Q tagging • Link aggregation • Speed • Duplex - Spanning tree - Maximum transmission unit (MTU) • Jumbo frames
Given a scenario, select and configure wireless devices and technologies.	- Channels • Channel width • Non-overlapping channels • Regulatory impacts - 802.11h - Frequency options • 2.4GHz • 5GHz

Topic	Details
	• 6GHz • Band steering - Service set identifier (SSID) • Basic service set identifier (BSSID) • Extended service set identifier (ESSID) - Network types • Mesh networks • Ad hoc • Point to point • Infrastructure - Encryption • Wi-Fi Protected Access 2 (WPA2) • WPA3 - Guest networks • Captive portals - Authentication • Pre-shared key (PSK) vs. Enterprise - Antennas • Omnidirectional vs. directional - Autonomous vs. lightweight access point
Explain important factors of physical installations.	- Important installation implications • Locations - Intermediate distribution frame (IDF) - Main distribution frame (MDF) • Rack size • Port-side exhaust/intake • Cabling - Patch panel - Fiber distribution panel • Lockable
Network Operations - 19%	
Explain the purpose of organizational processes and procedures.	- Documentation • Physical vs. logical diagrams • Rack diagrams • Cable maps and diagrams • Network diagrams - Layer 1 - Layer 2 - Layer 3 • Asset inventory - Hardware - Software - Licensing - Warranty support • IP address management (IPAM) • Service-level agreement (SLA) • Wireless survey/heat map - Life-cycle management • End-of-life (EOL) • End-of-support (EOS)

Topic	Details
	• Software management - Patches and bug fixes - Operating system (OS) - Firmware • Decommissioning - Change management • Request process tracking/service request - Configuration management • Production configuration • Backup configuration • Baseline/golden configuration
Given a scenario, use network monitoring technologies.	- Methods • SNMP - Traps - Management information base (MIB) - Versions 1. v2c 2. v3 - Community strings - Authentication • Flow data • Packet capture • Baseline metrics - Anomaly alerting/notification • Log aggregation - Syslog collector - Security information and event management (SIEM) • Application programming interface (API) integration • Port mirroring - Solutions • Network discovery - Ad hoc - Scheduled • Traffic analysis • Performance monitoring • Availability monitoring • Configuration monitoring
Explain disaster recovery (DR) concepts.	- DR metrics • Recovery point objective (RPO) • Recovery time objective (RTO) • Mean time to repair (MTTR) • Mean time between failures (MTBF) - DR sites • Cold site • Warm site • Hot site - High-availability approaches • Active-active • Active-passive - Testing • Tabletop exercises

Topic	Details
	• Validation tests
Given a scenario, implement IPv4 and IPv6 network services.	- Dynamic addressing • DHCP - Reservations - Scope - Lease time - Options - Relay/IP helper - Exclusions • Stateless address autoconfiguration (SLAAC) - Name resolution • DNS - Domain Name Security Extensions (DNSSEC) - DNS over HTTPS (DoH) and DNS over TLS (DoT) - Record types 1. Address (A) 2. AAAA 3. Canonical name (CNAME) 4. Mail exchange (MX) 5. Text (TXT) 6. Nameserver (NS) 7. Pointer (PTR) - Zone types 1. Forward 2. Reverse - Authoritative vs. non-authoritative - Primary vs. secondary - Recursive • Hosts file - Time protocols • NTP • Precision Time Protocol (PTP) • Network Time Security (NTS)
Compare and contrast network access and management methods.	- Site-to-site VPN - Client-to-site VPN • Clientless • Split tunnel vs. full tunnel - Connection methods • SSH • Graphical user interface (GUI) • API • Console - Jump box/host - In-band vs. out-of-band management
Network Security - 14%	
Explain the importance of basic network security concepts.	- Logical security • Encryption - Data in transit - Data at rest

Topic	Details
	• Certificates - Public key infrastructure (PKI) - Self-signed • Identity and access management (IAM) - Authentication - Multifactor authentication (MFA) - Single sign-on (SSO) - Remote Authentication Dial-in User Service (RADIUS) - LDAP - Security Assertion Markup Language (SAML) - Terminal Access Controller Access Control System Plus (TACACS+) - Time-based authentication - Authorization 1. Least privilege 2. Role-based access control • Geofencing - Physical security • Camera • Locks - Deception technologies • Honeypot • Honeynet - Common security terminology • Risk • Vulnerability • Exploit • Threat • Confidentiality, Integrity, and Availability (CIA) triad - Audits and regulatory compliance • Data locality • Payment Card Industry Data Security Standards (PCI DSS) • General Data Protection Regulation (GDPR) - Network segmentation enforcement • Internet of Things (IoT) and Industrial Internet of Things (IIoT) • Supervisory control and data acquisition (SCADA), industrial control System (ICS), operational technology (OT) • Guest • Bring your own device (BYOD)
Summarize various types of attacks and their impact to the network.	- Denial-of-service (DoS)/distributed denial-of-service (DDoS) - VLAN hopping - Media Access Control (MAC) flooding - Address Resolution Protocol (ARP) poisoning - ARP spoofing - DNS poisoning - DNS spoofing - Rogue devices and services • DHCP • AP

Topic	Details
	- Evil twin - On-path attack - Social engineering • Phishing • Dumpster diving • Shoulder surfing • Tailgating - Malware
Given a scenario, apply network security features, defense techniques, and solutions.	- Device hardening • Disable unused ports and services • Change default passwords - Network access control (NAC) • Port security • 802.1X • MAC filtering - Key management - Security rules • Access control list (ACL) • Uniform Resource Locator (URL) filtering • Content filtering - Zones • Trusted vs. untrusted • Screened subnet
Network Troubleshooting - 24%	
Explain the 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 theory is confirmed, determine next steps to resolve problem • If theory is not confirmed, establish 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 implement preventive measures if applicable - Document findings, actions, outcomes, and lessons learned throughout the process
Given a scenario, troubleshoot common cabling and physical interface issues.	- Cable issues • Incorrect cable - Single mode vs. multimode

Topic	Details
	- Category 5/6/7/8 - Shielded twisted pair (STP) vs. unshielded twisted pair (UTP) • Signal degradation - Crosstalk - Interference - Attenuation • Improper termination • Transmitter (TX)/Receiver (RX) transposed - Interface issues • Increasing interface counters - Cyclic redundancy check (CRC) - Runts - Giants - Drops • Port status - Error disabled - Administratively down - Suspended - Hardware issues • Power over Ethernet (PoE) - Power budget exceeded - Incorrect standard • Transceivers - Mismatch - Signal strength
Given a scenario, troubleshoot common issues with network services.	- Switching issues • STP - Network loops - Root bridge selection - Port roles - Port states • Incorrect VLAN assignment • ACLs - Route selection • Routing table • Default routes - Address pool exhaustion - Incorrect default gateway - Incorrect IP address • Duplicate IP address - Incorrect subnet mask
Given a scenario, troubleshoot common performance issues.	- Congestion/contention - Bottlenecking - Bandwidth • Throughput capacity - Latency - Packet loss - Jitter - Wireless • Interference - Channel overlap

Topic	Details
	• Signal degradation or loss • Insufficient wireless coverage • Client disassociation issues • Roaming misconfiguration
Given a scenario, use the appropriate tool or protocol to solve networking issues.	- Software tools • Protocol analyzer • Command line - ping - traceroute/tracert - nslookup - tcpdump - dig - netstat - ip/ifconfig/ipconfig - arp • Nmap • Link Layer Discovery Protocol (LLDP)/Cisco Discovery Protocol (CDP) • Speed tester - Hardware tools • Toner • Cable tester • Taps • Wi-Fi analyzer • Visual fault locator - Basic networking device commands • show mac-address-table • show route • show interface • show config • show arp • show vlan • show power

Prepare with N10-009 Sample Questions:

Question: 1

Which of the following kinds of targeted attacks uses multiple computers or bots to request the same resource repeatedly?

a) On-path
b) MAC flooding
c) ARP spoofing
d) DDoS

Answer: d

Question: 2

Which of the following ports is a secure protocol?

a) 20
b) 23
c) 443
d) 445

Answer: c

Question: 3

While working in a coffee shop, an attacker watches a user log in to a corporate system and writes down the user's log-in credentials. Which of the following social engineering attacks is this an example of?

a) Phishing
b) Dumpster diving
c) Shoulder surfing
d) Tailgating

Answer: c

Question: 4

Which of the following antenna types would most likely be used in a network repeater that is housed in a central point in a home office?

a) Omnidirectional
b) Parabolic
c) High-gain
d) Patch

Answer: a

Question: 5

A network engineer wants to improve network availability. Which of the following should the engineer install in the main closet?

a) A voltage monitor
b) A gaseous fire suppression system
c) Lockable cabinets
d) An uninterruptible power supply

Answer: d

Question: 6

Which of the following should a junior security administrator recommend implementing to mitigate malicious network activity?

a) IPS
b) Honeypot
c) SIEM
d) VPN

Answer: a

Question: 7

Which of the following refers to a weakness in a mechanism or technical process?

a) Vulnerability
b) Risk
c) Exploit
d) Threat

Answer: a

Question: 8

Which of the following cloud deployment models involves servers that are hosted at a company's property and are only used by that company?

a) Public
b) Private
c) Hybrid
d) Community

Answer: b

Question: 9

A technician is troubleshooting a user's connectivity issues and finds that the computer's IP address was changed to 169.254.0.1. Which of the following is the most likely reason?

a) Two or more computers have the same IP address in the ARP table.
b) The computer automatically set this address because the DHCP was not available.
c) The computer was set up to perform as an NTP server.
d) The computer is on a VPN and is the first to obtain a different IP address in that network.

Answer: b

Question: 10

Which of the following is the first step a network administrator should take in the troubleshooting methodology?

a) Establish a plan of action.
b) Document findings and outcomes.
c) Test the theory to determine cause.
d) Identify the problem.

Answer: d

Study Tips to Pass the CompTIA Network+ Exam:

Understand the N10-009 Exam Format:

Before diving into your study routine, it's essential to familiarize yourself with the N10-009 exam format. Take the time to review the exam syllabus understand the test structure, and identify the key areas of focus. Prior knowledge of what to expect on exam day will help you tailor your study plan.

Make A Study Schedule for the N10-009 Exam:

To effectively prepare for the N10-009 exam, make a study schedule that fits your lifestyle and learning style. Set specific time slots for studying each day and focus on the topics based on their importance and your proficiency level. Consistency is a must, so stick to your schedule and avoid procrastination.

Study from Different Resources:

Make sure to expand beyond one source of study material. Utilize multiple resources such as textbooks, online courses, practice exams, and study guides to understand the N10-009 exam topics comprehensively. Each resource offers unique insights and explanations that can enhance your learning experience.

Practice Regularly for the N10-009 Exam:

Practice makes you perfect for the N10-009 exam preparation as well. Regular practice allows you to reinforce your knowledge of key concepts, enhance your problem-solving skills, and familiarize yourself with the exam format. Dedicate time to solving practice questions and sample tests to gauge your progress.

Take Breaks and Rest:

While it's essential to study, taking breaks and allowing yourself to rest is equally important. Overloading your brain with information without adequate rest can lead to burnout and decreased productivity. Set short breaks during your study sessions to recharge and maintain focus.

Stay Organized During the N10-009 Exam Preparation:

Stay organized throughout your N10-009 study journey by keeping track of your progress and materials. Maintain a tidy study space, use folders or digital tools to organize your notes and resources, and create a checklist of topics to cover. An organized approach helps you stay on track and minimize stress.

Seek Clarification from Mentors:

Feel free to seek clarification if you encounter any confusing or challenging concepts during your study sessions. Reach out to peers, instructors, or online forums for assistance. Clarifying doubts early on will prevent misunderstandings and ensure you have a solid grasp of the material.

Regular Revision Plays A vital Role for the N10-009 Exam:

Consistent revision is essential for the long-term retention of information. Review previously covered topics to reinforce your understanding and identify any areas requiring additional attention. Reviewing regularly will help solidify your knowledge and boost your confidence.

Practice Time Management for the N10-009 Exam:

Effective time management is crucial on exam day to ensure you complete all sections within the allocated time frame. During your practice sessions, simulate N10-009 exam conditions and practice pacing yourself accordingly. Develop strategies for tackling each section efficiently to maximize your score.

Stay Positive and Confident:

Lastly, always have a positive mindset and believe in your abilities. Stay confident in your preparation efforts and trust that you have adequately equipped yourself to tackle the N10-009 exam. Visualize success, stay focused, and approach the exam calmly and confidently.

Benefits of Earning the N10-009 Exam:

- Achieving the N10-009 certification opens doors to new career opportunities and advancement within your field.
- The rigorous preparation required for the N10-009 exam equips you with in-depth knowledge and practical skills relevant to your profession.
- Holding the N10-009 certification demonstrates your expertise and commitment to excellence, earning recognition from peers and employers.
- Certified professionals often grab higher salaries and enjoy greater earning potential than their non-certified counterparts.
- Obtaining the N10-009 certification validates your proficiency and credibility, instilling confidence in clients, employers, and colleagues.

Discover the Reliable Practice Test for the N10-009 Certification:

Edusum brings you comprehensive information about the N10-009 exam. We offer genuine practice tests tailored for the N10-009 certification. What benefits do these practice tests offer? You'll encounter authentic exam-like questions crafted by industry experts, providing an opportunity to enhance your performance in the actual exam. Count on Edusum for rigorous, unlimited access to N10-009 practice tests over two months, enabling you to bolster your confidence steadily. Through dedicated practice, many candidates have succeeded in streamlining their journey towards obtaining the CompTIA Network+.

Concluding Thoughts:

Preparing for the N10-009 exam requires dedication, strategy, and effective study techniques. These study tips can enhance your preparation, boost your confidence, and improve your chances of passing the exam with flying colors. Remember to stay focused, stay organized, and believe in yourself. Good luck!