EDUSUM

#1 Online Certification Guide

COMPTIA N10-009

CompTIA Network+ Certification Questions & Answers

Exam Summary – Syllabus –Questions

N10-009

CompTIA Network+

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

Table of Contents:

Know Your N10-009 Certification Well:

The N10-009 is best suitable for candidates who want to gain knowledge in the CompTIA Core. Before you start your N10-009 preparation you may struggle to get all the crucial Network+ materials like N10-009 syllabus, sample questions, study guide.

But don't worry the N10-009 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 N10-009 syllabus?
- How many questions are there in the N10-009 exam?
- Which Practice test would help me to pass the N10-009 exam at the first attempt?

Passing the N10-009 exam makes you CompTIA 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 N10-009 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**

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 - 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

Topic	Details
	- 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)

Topic	Details
	• 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 • 22 • 23 • 25 • 53 • 67/68 • 69 • 80 • 123 • 161/162 • 389 • 443 • 445 • 514 • 587 • 636 • 1433 • 3389

Topic	Details
	• 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

Topic	Details
	- Fibre Channel (FC) • Form factors - Small form-factor pluggable (SFP) - Quad small form-factor pluggable (QSFP) - 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

Topic	Details
	• 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 - Configuration drift/compliance - Upgrades - Dynamic inventories

Topic	Details
	• 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	- Virtual Local Area Network (VLAN)

Topic	Details
technologies and features.	• 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 • 6GHz • Band steering - Service set identifier (SSID) • Basic service set identifier (BSSID) • Extended service set identifier (ESSID) - Network types • Mesh networks

Topic	Details
	• 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

Topic	Details
	• 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) • 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

Topic	Details
	- 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

Topic	Details
	• Warm site • Hot site - High-availability approaches • Active-active • Active-passive - Testing • Tabletop exercises • 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

Topic	Details
	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 • Certificates - Public key infrastructure (PKI) - Self-signed • Identity and access management (IAM)

Topic	Details
	- 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)

Topic	Details
	- 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 - 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)

Topic	Details
	• 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

Topic	Details
	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 - 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)

Topic	Details
	- 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

Topic	Details
	- Channel overlap • 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

Topic	Details
	• show config • show arp • show vlan • show power

CompTIA N10-009 Sample Questions:

Question: 1

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: 2

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: 3

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: 4

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: 5

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: 6

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

Question: 7

Which of the following ports is a secure protocol?

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

Answer: c

Question: 8

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: 9

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: 10

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

Study Guide to Crack CompTIA Network+ N10-009 Exam:

- Getting details of the N10-009 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 N10-009 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 N10-009 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 N10-009 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 N10-009 practice tests is must. Continuous practice will make you an expert in all syllabus areas.