EDUSUM

#1 Online Certification Guide

COMPTIA N10-007

CompTIA Network+ Certification Questions & Answers

Exam Summary – Syllabus –Questions

N10-007

CompTIA Certified Network+

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

Table of Contents:

Know Your N10-007 Certification Well:

The N10-007 is best suitable for candidates who want to gain knowledge in the CompTIA Core. Before you start your N10-007 preparation you may struggle to get all the crucial Network+ materials like N10-007 syllabus, sample questions, study guide.

But don't worry the N10-007 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 N10-007 syllabus?
- How many questions are there in the N10-007 exam?
- Which Practice test would help me to pass the N10-007 exam at the first attempt?

Passing the N10-007 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 N10-007 Network+ Certification Details:

Exam Name	CompTIA Certified Network+ Professional
Exam Code	N10-007
Exam Price	$338 (USD)
Duration	90 mins
Number of Questions	90
Passing Score	720 / 900
Schedule Exam	**Pearson VUE**
Sample Questions	**CompTIA Network+ Sample Questions**
Practice Exam	**CompTIA N10-007 Certification Practice Exam**

N10-007 Syllabus:

Topic	Details
Networking Concepts - 23%	
Explain the purposes and uses of ports and protocols.	1. Protocols and ports - SSH 22 - DNS 53 - SMTP 25 - SFTP 22 - FTP 20, 21 - TFTP 69 - TELNET 23 - DHCP 67, 68 - HTTP 80 - HTTPS 443 - SNMP 161 - RDP 3389 - NTP 123 - SIP 5060, 5061 - SMB445 - POP 110 - IMAP 143 - LDAP 389 - LDAPS 636 - H.323 1720 2. Protocol types - ICMP - UDP - TCP - IP 3. Connection-oriented vs. connectionless
Explain devices, applications, protocols and services at their appropriate OSI layers.	1. Layer 1 – Physical 2. Layer 2 – Data link 3. Layer 3 – Network 4. Layer 4 – Transport 5. Layer 5 – Session

Topic	Details
	6. Layer 6 – Presentation 7. Layer 7 – Application
Explain the concepts and characteristics of routing and switching.	1. Properties of network traffic • Broadcast domains • CSMA/CD • CSMA/CA • Collision domains • Protocol data units • MTU • Broadcast • Multicast • Unicast 2. Segmentation and interface properties • VLANs • Trunking (802.1q) • Tagging and untagging ports • Port mirroring • Switching loops/spanning tree • PoE and PoE+ (802.3af, 802.3at) • DMZ • MAC address table • ARP table 3. Routing • Routing protocols (IPv4 and IPv6) - Distance-vector routing protocols ○ RIP ○ EIGRP - Link-state routing protocols ○ OSPF - Hybrid ○ BGP • Routing types Static

Topic	Details
	Dynamic Default 4. IPv6 concepts • Addressing • Tunneling • Dual stack • Router advertisement • Neighbor discovery 5. Performance concepts • Traffic shaping • QoS • Diffserv • CoS 6. NAT/PAT 7. Port forwarding 8. Access control list 9. Distributed switching 10. Packet-switched vs. circuit switched network 11. Software-defined networking
Given a scenario, configure the appropriate IP addressing components.	1. Private vs. public 2. Loopback and reserved 3. Default gateway 4. Virtual IP 5. Subnet mask 6. Subnetting • Classful Classes A, B, C, D, and E • Classless VLSM CIDR notation (IPv4 vs. IPv6) 7. Address assignments • DHCP

Topic	Details
	- DHCPv6 - Static - APIPA - EUI64 - IP reservations
Compare and contrast the characteristics of network topologies, types and technologies.	1. Wired topologies - Logical vs. physical - Star - Ring - Mesh - Bus 2. Wireless topologies - Mesh - Ad hoc - Infrastructure 3. Types - LAN - WLAN - MAN - WAN - CAN - SAN - PAN 4. Technologies that facilitate the Internet of Things (IoT) - Z-Wave - Ant+ - Bluetooth - NFC - IR - RFID - 802.11

Topic	Details
Given a scenario, implement the appropriate wireless technologies and configurations.	1. 802.11 standards • a • b • g • n • ac 2. Cellular • GSM • TDMA • CDMA 3. Frequencies • 2.4GHz • 5.0GHz 4. Speed and distance requirements 5. Channel bandwidth 6. Channel bonding 7. MIMO/MU-MIMO 8. Unidirectional/omnidirectiona 9. Site surveys
Summarize cloud concepts and their purposes.	1. Types of services • SaaS • PaaS • IaaS 2. Cloud delivery models • Private • Public • Hybrid 3. Connectivity methods 4. Security implications/considerations 5. Relationship between local and cloud resources
Explain the functions of network services.	1. DNS service • Record types A, AAAA

Topic	Details
	TXT (SPF, DKIM) SRV MX CNAME NS PTR • Internal vs. external DNS • Third-party/cloud-hosted DNS • Hierarchy • Forward vs. reverse zone 2. DHCP service • MAC reservations • Pools • IP exclusions • Scope options • Lease time • TTL • DHCP relay/IP helper 3. NTP 4. IPAM
Infrastructure - 18%	
Given a scenario, deploy the appropriate cabling solution.	1. Media types • Copper UTP STP Coaxial • Fiber Single-mode Multimode 2. Plenum vs. PVC 3. Connector types

Topic	Details
	• Copper RJ-45 RJ-11 BNC DB-9 DB-25 F-type • Fiber LC ST • SC APC UPC • MTR 4. Transceivers • SFP • GBIC • SFP+ • QSFP • Characteristics of fiber transceivers Bidirectional Duplex 5. Termination points • 66 block • 110 block • Patch panel • Fiber distribution panel 6. Copper cable standards • Cat 3 • Cat 5

Topic	Details
	• Cat 5e • Cat 6 • Cat 6a • Cat 7 • RG-6 • RG-59 7. Copper termination standards • TIA/EIA 568a • TIA/EIA 568b • Crossover • Straight-through 8. Ethernet deployment standards • 100BaseT • 1000BaseT • 1000BaseLX • 1000BaseSX • 10GBaseT
Given a scenario, determine the appropriate placement of networking devices on a network and install/configure them.	1. Firewall 2. Router 3. Switch 4. Hub 5. Bridge 6. Modems 7. Wireless access point 8. Media converter 9. Wireless range extender 10. VoIP endpoint
Explain the purposes and use cases for advanced networking devices.	1. Multilayer switch 2. Wireless controller 3. Load balancer 4. IDS/IPS 5. Proxy server 6. VPN concentrator 7. AAA/RADIUS server 8. UTM appliance 9. NGFW/Layer 7 firewall 10. VoIP PBX

Topic	Details
	11. VoIP gateway 12. Content filter
Explain the purposes of virtualization and network storage technologies.	1. Virtual networking components • Virtual switch • Virtual firewall • Virtual NIC • Virtual router • Hypervisor 2. Network storage types • NAS • SAN 3. Connection type • FCoE • Fibre Channel • iSCSI • InfiniBand 4. Jumbo frame
Compare and contrast WAN technologies.	1. Service type • ISDN • T1/T3 • E1/E3 • OC-3 – OC-192 • DSL • Metropolitan Ethernet • Cable broadband • Dial-up • PRI 2. Transmission mediums • Satellite • Copper • Fiber • Wireless 3. Characteristics of service

Topic	Details
	• MPLS • ATM • Frame relay • PPPoE • PPP • DMVPN • SIP trunk 4. Termination • Demarcation point • CSU/DSU • Smart jack
Network Operations - 17%	
Given a scenario, use appropriate documentation and diagrams to manage the network.	1. Diagram symbols 2. Standard operating procedures/ work instructions 3. Logical vs. physical diagrams 4. Rack diagrams 5. Change management documentation 6. Wiring and port locations 7. IDF/MDF documentation 8. Labeling 9. Network configuration and performance baselines 10. Inventory management
Compare and contrast business continuity and disaster recovery concepts.	1. Availability concepts • Fault tolerance • High availability • Load balancing • NIC teaming • Port aggregation • Clustering • Power management Battery backups/UPS Power generators Dual power supplies Redundant circuits

Topic	Details
	2. Recovery - Cold sites - Warm sites - Hot sites - Backups Full Differential Incrementa - Snapshots 3. MTTR 4. MTBF 5. SLA requirements
Explain common scanning, monitoring and patching processes and summarize their expected outputs.	1. Processes - Log reviewing - Port scanning - Vulnerability scanning - Patch management Rollback - Reviewing baselines - Packet/traffic analysis 2. Event management - Notifications - Alerts - SIEM 3. SNMP monitors - MIB 4. Metrics - Error rate - Utilization - Packet drops - Bandwidth/throughput
Given a scenario, use remote access methods.	1. VPN - IPSec

Topic	Details
	• SSL/TLS/DTLS • Site-to-site • Client-to-site 2. RDP 3. SSH 4. VNC 5. Telnet 6. HTTPS/management URL 7. Remote file access • FTP/FTPS • SFTP • TFTP 8. Out-of-band management • Modem • Console router
Identify policies and best practices.	1. Privileged user agreement 2. Password policy 3. On-boarding/off-boarding procedures 4. Licensing restrictions 5. International export controls 6. Data loss prevention 7. Remote access policies 8. Incident response policies 9. BYOD 10. AUP 11. NDA 12. System life cycle • Asset disposal 13. Safety procedures and policies
Network Security - 20%	
Summarize the purposes of physical security devices.	1. Detection • Motion detection • Video surveillance • Asset tracking tags

Topic	Details
	• Tamper detection 2. Prevention • Badges • Biometrics • Smart cards • Key fob • Locks
Explain authentication and access controls.	1. Authorization, authentication and accounting • RADIUS • TACACS+ • Kerberos • Single sign-on • Local authentication • LDAP • Certificates • Auditing and logging 2. Multifactor authentication • Something you know • Something you have • Something you are • Somewhere you are • Something you do 3. Access control • 802.1x • NAC • Port security • MAC filtering • Captive portal • Access control lists
Given a scenario, secure a basic wireless network.	1. WPA 2. WPA2 3. TKIP-RC4

Topic	Details
	4. CCMP-AES 5. Authentication and authorization - EAP PEAP EAP-FAST EAP-TLS - Shared or open - Preshared key - MAC filtering 6. Geofencing
Summarize common networking attacks.	1. DoS - Reflective - Amplified - Distributed 2. Social engineering 3. Insider threat 4. Logic bomb 5. Rogue access point 6. Evil twin 7. War-driving 8. Phishing 9. Ransomware 10. DNS poisoning 11. ARP poisoning 12. Spoofing 13. Deauthentication 14. Brute force 15. VLAN hopping 16. Man-in-the-middle 17. Exploits vs. vulnerabilities
Given a scenario, implement network device hardening.	1. Changing default credentials 2. Avoiding common passwords 3. Upgrading firmware 4. Patching and updates 5. File hashing

Topic	Details
	6. Disabling unnecessary services 7. Using secure protocols 8. Generating new keys 9. Disabling unused ports - IP ports - Device ports (physical and virtual)
Explain common mitigation techniques and their purposes.	1. Signature management 2. Device hardening 3. Change native VLAN 4. Switch port protection - Spanning tree - Flood guard - BPDU guard - Root guard - DHCP snooping 5. Network segmentation - DMZ - VLAN 6. Privileged user account 7. File integrity monitoring 8. Role separation 9. Restricting access via ACLs 10. Honeypot/honeynet 11. Penetration testing
Network Troubleshooting and Tools - 22%	
Explain the network troubleshooting methodology.	1. Identify the problem - Gather information - Duplicate the problem, if possible - Question users - Identify symptoms - Determine if anything has changed - Approach multiple problems individually 2. Establish a theory of probable cause

Topic	Details
	- Question the obvious - Consider multiple approaches Top-to-bottom/bottom-to-top OSI model Divide and conquer 3. Test the theory to determine the cause - Once the theory is confirmed, determine the next steps to resolve the problem - If the theory is not confirmed, reestablish a new theory or escalate 4. Establish a plan of action to resolve the problem and identify potential effects 5. Implement the solution or escalate as necessary 6. Verify full system functionality and, if applicable, implement preventive measures 7. Document findings, actions, and outcomes
Given a scenario, use the appropriate tool.	1. Hardware tools - Crimper - Cable tester - Punchdown tool - OTDR - Light meter - Tone generator - Loopback adapter - Multimeter - Spectrum analyzer 2. Software tools - Packet sniffer - Port scanner - Protocol analyzer - WiFi analyzer - Bandwidth speed tester - Command line ping

Topic	Details
	tracert, traceroute nslookup ipconfig ifconfig iptables netstat tcpdump pathping nmap route arp dig
Given a scenario, troubleshoot common wired connectivity and performance issues.	1. Attenuation 2. Latency 3. Jitter 4. Crosstalk 5. EMI 6. Open/short 7. Incorrect pin-out 8. Incorrect cable type 9. Bad port 10. Transceiver mismatch 11. TX/RX reverse 12. Duplex/speed mismatch 13. Damaged cables 14. Bent pins 15. Bottlenecks 16. VLAN mismatch 17. Network connection LED status indicators
Given a scenario, troubleshoot common wireless connectivity and performance issues.	1. Reflection 2. Refraction 3. Absorption 4. Latency 5. Jitter 6. Attenuation 7. Incorrect antenna type

Topic	Details
	8. Interference 9. Incorrect antenna placement 10. Channel overlap 11. Overcapacity 12. Distance limitations 13. Frequency mismatch 14. Wrong SSID 15. Wrong passphrase 16. Security type mismatch 17. Power levels 18. Signal-to-noise ratio
Given a scenario, troubleshoot common network service issues.	1. Names not resolving 2. Incorrect gateway 3. Incorrect netmask 4. Duplicate IP addresses 5. Duplicate MAC addresses 6. Expired IP address 7. Rogue DHCP server 8. Untrusted SSL certificate 9. Incorrect time 10. Exhausted DHCP scope 11. Blocked TCP/UDP ports 12. Incorrect host-based firewall settings 13. Incorrect ACL settings 14. Unresponsive service 15. Hardware failure

CompTIA N10-007 Sample Questions:

Question: 1

Which of the following tools would a technician use to secure a CAT5e cable to a 110 block?

a) Wire strippers
b) Snips
c) Crimpers
d) Punch down

Answer: d

Question: 2

A home user reports that a speed test website shows the following information:
Download speed: 33.3Mbps
Upload speed: 10.2Mbps
Which of the following is the correct interpretation of these results?

a) The home PC downloaded 33.3 MB of data to the website and uploaded 10.2 MB of data from the website.
b) The website upload bandwidth is saturated, and it does not match the download speed.
c) The home PC is receiving data at 33.3 Mbps and sending data at 10.2 Mbps.
d) The website is downloading data to its server at 33.3 Mbps and uploading data from its server at 10.2 Mbps.

Answer: c

Question: 3

A system administrator is connecting workstations to a switch. During testing and verification, the system administrator notices latency with processing data on the workstations. The system administrator then notices that the workstations are connected to 100Mb ports on the switch and the workstations have 1Gb NICs.

Which of the following issues is the system administrator having with the switch and the workstations?

a) Speed and duplex mismatch
b) Bad switch ports
c) Bad NICs
d) Misconfigured IP

Answer: a

Question: 4

Which of the following WAN technologies would have the HIGHEST latency?

a) Satellite
b) Cable
c) DSL
d) Frame-relay

Answer: a

Question: 5

An SVI involves assigning an IP address to what?

a) VLAN
b) Switch
c) Firewall
d) PBX

Answer: a

Question: 6

A technician is configuring mobile devices for new employees. Which of the following documents should be updated to show that the new employees are receiving these mobile devices?

a) Network diagram
b) Asset management
c) Organizational chart
d) Standard operating procedure
e) Change management

Answer: b

Question: 7

If the network is congested and the destination device requests that the source device slow its transmission, what will occur?

a) The source will stop responding for 30 seconds and then continue transmitting.
b) The source will find a different route to send the data.
c) The destination will drop all packets for 30 seconds.
d) Nothing will happen.

Answer: d

Question: 8

Which of the following describes a process that can translate internal network IP addresses to external ones?

a) Change control
b) NAT
c) PAT
d) Remote terminal emulation

Answer: b

Question: 9

You experience connectivity problems with your SOHO network. What can you change in an attempt to solve this problem?

a) Shorten the SSID.
b) Remove all encryption.
c) Lower the transfer rate.
d) Raise the transfer rate.

Answer: c

Question: 10

What is the term used for the number of hops necessary to reach a node?

a) Jump list
b) Link stops
c) Connections
d) Hop count

Answer: d

Study Guide to Crack CompTIA Network+ N10-007 Exam:

- Getting details of the N10-007 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 N10-007 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 N10-007 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 N10-007 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 N10-007 practice tests is must. Continuous practice will make you an expert in all syllabus areas.