EDUSUM

#1 Online Certification Guide

N10-007

Network+

A Success Guide to Prepare-
CompTIA Network+

edusum.com

Table of Contents

Introduction to N10-007 Exam on CompTIA Network+

Use this quick start guide to collect all the information about CompTIA Network+ (N10-007) Certification exam. This study guide provides a list of objectives and resources that will help you prepare for items on the N10-007 CompTIA Network+ exam. The Sample Questions will help you identify the type and difficulty level of the questions and the Practice Exams will make you familiar with the format and environment of an exam. You should refer this guide carefully before attempting your actual CompTIA N+ certification exam.

The CompTIA Network+ certification is mainly targeted to those candidates who want to build their career in Networking domain. The CompTIA Certified Network+ Professional exam verifies that the candidate possesses the fundamental knowledge and proven skills in the area of CompTIA N+.

CompTIA N10-007 Certification Details:

Exam Name	CompTIA Certified Network+ Professional
Exam Code	N10-007
Exam Price	$302 (USD)
Duration	90 min
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**

CompTIA N10-007 Exam Syllabus:

Topic	Details
Networking Concepts 23%	
Explain the purposes and uses of ports and protocols.	1. Protocols and ports 1. SSH 22 2. DNS 53 3. SMTP 25 4. SFTP 22 5. FTP 20, 21 6. TFTP 69 7. TELNET 23 8. DHCP 67, 68 9. HTTP 80 10. HTTPS 443 11. SNMP 161 12. RDP 3389 13. NTP 123 14. SIP 5060, 5061 15. SMB445 16. POP 110 17. IMAP 143 18. LDAP 389 19. LDAPS 636 20. H.323 1720 2. Protocol types 1. ICMP 2. UDP 3. TCP 4. 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 6. Layer 6 – Presentation 7. Layer 7 – Application
Explain the concepts and characteristics of routing and switching.	1. Properties of network traffic 1. Broadcast domains 2. CSMA/CD 3. CSMA/CA 4. Collision domains 5. Protocol data units

Topic	Details
	6. MTU 7. Broadcast 8. Multicast 9. Unicast 2. Segmentation and interface properties 1. VLANs 2. Trunking (802.1q) 3. Tagging and untagging ports 4. Port mirroring 5. Switching loops/spanning tree 6. PoE and PoE+ (802.3af, 802.3at) 7. DMZ 8. MAC address table 9. ARP table 3. Routing 1. Routing protocols (IPv4 and IPv6) Distance-vector routing protocols RIP EIGRP Link-state routing protocols OSPF Hybrid BGP 2. Routing types Static Dynamic Default 4. IPv6 concepts 1. Addressing 2. Tunneling 3. Dual stack 4. Router advertisement 5. Neighbor discovery 5. Performance concepts

Topic	Details
	1. Traffic shaping 2. QoS 3. Diffserv 4. 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 1. Classful Classes A, B, C, D, and E 2. Classless VLSM CIDR notation (IPv4 vs. IPv6) 7. Address assignments 1. DHCP 2. DHCPv6 3. Static 4. APIPA 5. EUI64 6. IP reservations
Compare and contrast the characteristics of network topologies, types and technologies.	1. Wired topologies 1. Logical vs. physical 2. Star 3. Ring 4. Mesh 5. Bus 2. Wireless topologies 1. Mesh

Topic	Details
	2. Ad hoc 3. Infrastructure 3. Types 1. LAN 2. WLAN 3. MAN 4. WAN 5. CAN 6. SAN 7. PAN 4. Technologies that facilitate the Internet of Things (IoT) 1. Z-Wave 2. Ant+ 3. Bluetooth 4. NFC 5. IR 6. RFID 7. 802.11
Given a scenario, implement the appropriate wireless technologies and configurations.	1. 802.11 standards 1. a 2. b 3. g 4. n 5. ac 2. Cellular 1. GSM 2. TDMA 3. CDMA 3. Frequencies 1. 2.4GHz 2. 5.0GHz 4. Speed and distance requirements 5. Channel bandwidth 6. Channel bonding 7. MIMO/MU-MIMO

Topic	Details
	8. Unidirectional/omnidirectiona 9. Site surveys
Summarize cloud concepts and their purposes.	1. Types of services 1. SaaS 2. PaaS 3. IaaS 2. Cloud delivery models 1. Private 2. Public 3. Hybrid 3. Connectivity methods 4. Security implications/considerations 5. Relationship between local and cloud resources
Explain the functions of network services.	1. DNS service 1. Record types A, AAAA TXT (SPF, DKIM) SRV MX CNAME NS PTR 2. Internal vs. external DNS 3. Third-party/cloud-hosted DNS 4. Hierarchy 5. Forward vs. reverse zone 2. DHCP service 1. MAC reservations 2. Pools 3. IP exclusions 4. Scope options 5. Lease time 6. TTL 7. DHCP relay/IP helper 3. NTP 4. IPAM

Topic	Details
Infrastructure 18%	
Given a scenario, deploy the appropriate cabling solution.	1. Media types 1. Copper UTP STP Coaxial 2. Fiber Single-mode Multimode 2. Plenum vs. PVC 3. Connector types 1. Copper RJ-45 RJ-11 BNC DB-9 DB-25 F-type 2. Fiber LC ST 3. SC APC UPC 4. MTR 4. Transceivers 1. SFP 2. GBIC 3. SFP+ 4. QSFP 5. Characteristics of fiber transceivers

Topic	Details
	Bidirectional Duplex 5. Termination points 1. 66 block 2. 110 block 3. Patch panel 4. Fiber distribution panel 6. Copper cable standards 1. Cat 3 2. Cat 5 3. Cat 5e 4. Cat 6 5. Cat 6e 6. Cat 7 7. RG-6 8. RG-59 7. Copper termination standards 1. TIA/EIA 568a 2. TIA/EIA 568b 3. Crossover 4. Straight-through 8. Ethernet deployment standards 1. 100BaseT 2. 1000BaseT 3. 1000BaseLX 4. 1000BaseSX 5. 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

Topic	Details
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 11. VoIP gateway 12. Content filter
Explain the purposes of virtualization and network storage technologies.	1. Virtual networking components 1. Virtual switch 2. Virtual firewall 3. Virtual NIC 4. Virtual router 5. Hypervisor 2. Network storage types 1. NAS 2. SAN 3. Connection type 1. FCoE 2. Fibre Channel 3. iSCSI 4. InfiniBand 4. Jumbo frame
Compare and contrast WAN technologies.	1. Service type 1. ISDN 2. T1/T3 3. E1/E3 4. OC-3 – OC-192 5. DSL 6. Metropolitan Ethernet 7. Cable broadband 8. Dial-up 9. PRI 2. Transmission mediums

Topic	Details
	1. Satellite 2. Copper 3. Fiber 4. Wireless 3. Characteristics of service 1. MPLS 2. ATM 3. Frame relay 4. PPPoE 5. PPP 6. DMVPN 7. SIP trunk 4. Termination 1. Demarcation point 2. CSU/DSU 3. 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 1. Fault tolerance 2. High availability 3. Load balancing 4. NIC teaming 5. Port aggregation 6. Clustering 7. Power management Battery backups/UPS Power generators Dual power supplies Redundant circuits 2. Recovery

Topic	Details
	1. Cold sites 2. Warm sites 3. Hot sites 4. Backups Full Differential Incrementa 5. Snapshots 3. MTTR 4. MTBF 5. SLA requirements
Explain common scanning, monitoring and patching processes and summarize their expected outputs.	1. Processes 1. Log reviewing 2. Port scanning 3. Vulnerability scanning 4. Patch management Rollback 5. Reviewing baselines 6. Packet/traffic analysis 2. Event management 1. Notifications 2. Alerts 3. SIEM 3. SNMP monitors 1. MIB 4. Metrics 1. Error rate 2. Utilization 3. Packet drops 4. Bandwidth/throughput
Given a scenario, use remote access methods.	1. VPN 1. IPSec 2. SSL/TLS/DTLS 3. Site-to-site 4. Client-to-site

Topic	Details
	2. RDP 3. SSH 4. VNC 5. Telnet 6. HTTPS/management URL 7. Remote file access 1. FTP/FTPS 2. SFTP 3. TFTP 8. Out-of-band management 1. Modem 2. 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 1. Asset disposal 13. Safety procedures and policies
Network Security 20%	
Summarize the purposes of physical security devices.	1. Detection 1. Motion detection 2. Video surveillance 3. Asset tracking tags 4. Tamper detection 2. Prevention 1. Badges 2. Biometrics 3. Smart cards 4. Key fob

Topic	Details
	5. Locks
Explain authentication and access controls.	1. Authorization, authentication and accounting 1. RADIUS 2. TACACS+ 3. Kerberos 4. Single sign-on 5. Local authentication 6. LDAP 7. Certificates 8. Auditing and logging 2. Multifactor authentication 1. Something you know 2. Something you have 3. Something you are 4. Somewhere you are 5. Something you do 3. Access control 1. 802.1x 2. NAC 3. Port security 4. MAC filtering 5. Captive portal 6. Access control lists
Given a scenario, secure a basic wireless network.	1. WPA 2. WPA2 3. TKIP-RC4 4. CCMP-AES 5. Authentication and authorization 1. EAP PEAP EAP-FAST EAP-TLS 2. Shared or open 3. Preshared key 4. MAC filtering

Topic	Details
	6. Geofencing

Summarize common networking attacks.	1. DoS
	    1. Reflective
	    2. Amplified
	    3. 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
	6. Disabling unnecessary services
	7. Using secure protocols
	8. Generating new keys
	9. Disabling unused ports
	    1. IP ports
	    2. 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
	    1. Spanning tree
	    2. Flood guard
	    3. BPDU guard
	    4. Root guard
	    5. DHCP snooping

Topic	Details
	5. Network segmentation 1. DMZ 2. 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 1. Gather information 2. Duplicate the problem, if possible 3. Question users 4. Identify symptoms 5. Determine if anything has changed 6. Approach multiple problems individually 2. Establish a theory of probable cause 1. Question the obvious 2. Consider multiple approaches Top-to-bottom/bottom-to-top OSI model Divide and conquer 3. Test the theory to determine the cause 1. Once the theory is confirmed, determine the next steps to resolve the problem 2. 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 1. Cable tester 2. Punchdown tool

Topic	Details
	3. OTDR 4. Light meter 5. Tone generator 6. Loopback adapter 7. Multimeter 8. Spectrum analyzer 2. Software tools 1. Packet sniffer 2. Port scanner 3. Protocol analyzer 4. WiFi analyzer 5. Bandwidth speed tester 6. Command line ping 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

Topic	Details
	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 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

N10-007 Sample Questions:

01. 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.

02. An incident response policy often ends with which phase?
a) Prepare
b) Contain
c) Review
d) Eradicate

03. 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

04. If a network has the five nines of availability, how much downtime does it experience per year?
a) 30 seconds
b) 5 minutes
c) 12 minutes
d) 26 minutes

05. A broken copper strand in a circuit is known as which of the following?
a) Short
b) Impedance
c) Open
d) Split pair

06. Which network infrastructure device primarily makes forwarding decisions based on Layer 2 MAC addresses?
a) Router
b) Switch
c) Hub
d) Multilayer switch

07. From the following list, identify the detection methods commonly used by IPS sensors.
(Choose three.)
a) Signature based
b) Distribution based
c) Policy based
d) Behavior based

08. By default, the automatic update feature on most modern operating systems is
a) Turned on
b) Disabled
c) Set to manual
d) Ineffective

09. Windowing is provided at what layer of the OSI reference model?
a) Data link layer
b) Network layer
c) Physical layer
d) Transport layer

10. How many channels on an E1 circuit are available for voice, video, or data?
a) 30
b) 23
c) 24
d) 32

Answers to N10-007 Exam Questions:

Question: 01 Answer: c	Question: 02 Answer: c	Question: 03 Answer: d	Question: 04 Answer: b	Question: 05 Answer: c
Question: 06 Answer: b	Question: 07 Answer: a, c, d	Question: 08 Answer: a	Question: 09 Answer: d	Question: 10 Answer: a

Note: If you find any typo or data entry error in these sample questions, we request you to update us by commenting on this page or write an email on feedback@edusum.com