CompTIA Network+ N10-009 Free Sample (30 Questions)

Unofficial practice material. Not affiliated with or endorsed by CompTIA.

This free sample contains 30 of the 700 questions from the full CompTIA Network+ (N10-009) question bank.

Q1. The mail administrator configures the firewall to allow the company's mail server to exchange email directly with mail servers on the internet. Which port should be permitted outbound from the mail server?

A) TCP 143

B) TCP 25

C) TCP 587

D) TCP 110

Correct answer: B

Explanation: SMTP on TCP port 25 is used for server-to-server (MTA-to-MTA) mail relay across the internet. C is the near-miss: TCP 587 is the message submission port used by email clients sending to their own mail server, not for server-to-server relay. D is wrong because TCP 110 is POP3 for clients retrieving mail. A is wrong because TCP 143 is IMAP for clients accessing mailboxes.

Q2. Match each protocol to its default port: 1) DNS | 2) HTTPS | 3) SSH — with: X) 53 (TCP/UDP) | Y) 443 (TCP) | Z) 22 (TCP). Which pairing is correct?

A) 1-Y, 2-Z, 3-X

B) 1-X, 2-Y, 3-Z

C) 1-Z, 2-X, 3-Y

D) 1-X, 2-Z, 3-Y

Correct answer: B

Explanation: DNS resolves names on port 53 (1-X); HTTPS secures web traffic with TLS on TCP 443 (2-Y); SSH provides encrypted remote CLI administration on TCP 22 (3-Z). D is the near-miss — it correctly identifies the DNS port but swaps the HTTPS and SSH ports, an easy mistake since both are encrypted TCP services. A pairs DNS with 443, and C scrambles all three pairings.

Q3. A technician runs "ping 127.0.0.1" on a workstation that cannot reach the network. The ping succeeds. What does this result prove?

A) The workstation's DNS resolution is working correctly

B) The local TCP/IP stack is installed and functioning

C) The DHCP server is responding to client requests

D) The workstation can reach hosts on the internet

Correct answer: B

Explanation: Pinging the loopback address tests only the local machine's TCP/IP stack, NIC driver path, and OS networking — success means the local stack works and the fault lies elsewhere (cable, switch, configuration). D is wrong because loopback never leaves the host. A is wrong because no name resolution is involved. C is wrong because DHCP plays no role in a loopback ping.

Q4. A router interface is configured with 10.10.5.200/20. Which subnet does this address belong to?

A) 10.10.16.0/20

B) 10.10.5.0/20

C) 10.10.4.0/20

D) 10.10.0.0/20

Correct answer: D

Explanation: A /20 has a block size of 16 in the third octet (256 – 240), so subnets increment 0, 16, 32…; third-octet value 5 falls in the 0–15 block, giving 10.10.0.0/20. B is the near-miss — it treats the mask as /24. C is not on a 16-boundary. A is the next subnet up, outside this address's range.

Q5. An auditor reviews firewall rules and finds four addresses labeled "internal private." Which one is NOT actually a private address?

A) 172.31.255.254

B) 172.32.1.1

C) 172.20.0.1

D) 172.16.5.5

Correct answer: B

Explanation: The 172.16.0.0/12 private range spans 172.16.0.0 through 172.31.255.255, so 172.32.1.1 falls just outside it and is a public address. A, C, and D all fall within 172.16.0.0–172.31.255.255 and are genuinely private — A sits at the very top edge of the range, making it a tempting but incorrect choice.

Q6. A user types "intranet.company.com" into a browser and reaches the internal portal. Which service translated that name into an IP address?

A) NTP

B) SNMP

C) DHCP

D) DNS

Correct answer: D

Explanation: DNS (Domain Name System) resolves hostnames to IP addresses. C is the near-miss: DHCP assigns IP addresses but does not resolve names. B is wrong because SNMP monitors devices. A is wrong because NTP synchronizes clocks.

Q7. Users report choppy, robotic-sounding voice calls. Monitoring shows the delay of voice packets swinging between 20 ms and 300 ms throughout the calls. Which condition best explains the symptoms?

A) Insufficient bandwidth

B) Consistently high latency

C) A duplex mismatch

D) Jitter

Correct answer: D

Explanation: Jitter — variation in delay — causes packets to arrive unevenly, and the voice buffer cannot smooth 20→300 ms swings, producing choppy audio. B is the near-miss: constant high latency causes talk-over delay, not choppiness. A would cause drops and quality loss, but the key clue is the varying delay, not a shortage of capacity. C causes collisions/errors on a link, not delay variation.

Q8. All computers, printers, and the file server inside a single office building are connected to the same switched network. Which network type does this describe?

A) MAN

B) LAN

C) PAN

D) WAN

Correct answer: B

Explanation: A LAN (local area network) covers a small geographic area such as a building or campus under one administration. D is wrong because a WAN spans large distances like cities or countries. A is wrong because a MAN covers an entire metropolitan area, larger than one building. C is wrong because a PAN covers only a few meters around a person (e.g., Bluetooth devices).

Q9. Match each technology to its description:

A) 1-X, 2-Y, 3-Z

B) 1-Y, 2-X, 3-Z

C) 1-Z, 2-Y, 3-X

D) 1-X, 2-Z, 3-Y

Correct answer: A

Explanation: DWDM packs dozens of tightly spaced wavelengths onto one fiber pair (1-X), matching the 32-wavelength scenario; CWDM uses wider channel spacing with far fewer channels, around 18 maximum (2-Y); 10GBASE-LR is a single-wavelength 10 Gbps optic (3-Z). B) swaps DWDM and CWDM, which would cap the design at roughly 18 channels. C) is wrong on all three. D) mislabels CWDM as single-wavelength and LR as coarse multiplexing.

Q10. A junior admin pasted this switchport config for review. The port connects to a single IP phone with a PC plugged into the phone's built-in mini-switch:

A) Add a second cable run so the phone and PC each get a dedicated switch port

B) Replace the phone with a model that has no built-in mini-switch to simplify the topology

C) Convert the port to a trunk that allows every VLAN on the switch

D) Keep data untagged and configure the voice (auxiliary) VLAN for tagged phone traffic

Correct answer: D

Explanation: The config puts voice and PC data in one access VLAN, so PC bursts contend with voice frames and destroy call quality. D) is the standard fix: the port stays an access port carrying untagged PC data while the auxiliary voice VLAN lets the phone tag its voice frames, separating the broadcast domains and enabling QoS on voice. A) and B) abandon the phone's built-in switch instead of using the voice-VLAN feature designed for it. C) is the near-miss -- a trunk would carry both VLANs, but trunking every VLAN to a phone port is unnecessary and widens the VLAN-hopping attack surface.

Q11. A branch router's only path to the Internet is through the headquarters router. What is the best routing configuration on the branch router?

A) No route is needed; the router will learn the path automatically via ARP

B) Configure a static route for every Internet prefix the branch might visit

C) Accept the full Internet BGP routing table from the headquarters router

D) Configure a default static route (0.0.0.0/0) pointing toward headquarters

Correct answer: D

Explanation: A default route sends all unknown destinations toward HQ, which is correct when there is exactly one exit path — simple and always accurate. C) is massive overkill for a single-homed branch. B) is impossible to maintain for the whole Internet. A) is wrong because routers do not learn routes without a protocol or static configuration.

Q12. Which statement accurately describes TCP?

A) It is faster than UDP because its larger packets move more data per segment

B) It is connectionless and sends data immediately with no setup or handshaking

C) It skips error checking and sequencing to keep overhead as low as possible

D) It uses a three-way handshake to establish a connection before data transfer

Correct answer: D

Explanation: TCP is connection-oriented and performs a SYN, SYN-ACK, ACK three-way handshake to establish a reliable session before sending data. A is a common misconception: TCP's acknowledgments, sequencing, and retransmissions add overhead, so it is generally slower than UDP for the same payload despite larger segments. B describes UDP, the classic near-miss distractor. C is wrong because TCP does provide error checking, sequencing, and retransmission — that reliability is its defining trait.

Q13. Users report choppy voice calls whenever large file transfers run, though bandwidth utilization stays below 60%. What is the best fix?

A) Enlarge the DHCP scope to give voice traffic more addresses

B) Change the native VLAN on the trunks to isolate voice frames

C) Implement QoS: mark voice DSCP EF and prioritize it in switch queuing

D) Purchase more Internet bandwidth to absorb the file transfers

Correct answer: C

Explanation: The symptom is queuing delay and jitter, not a bandwidth shortage — voice packets wait behind data bursts; marking voice DSCP EF (46) and giving it priority queuing protects calls regardless of data load. D) is the near-miss: more bandwidth rarely fixes jitter when utilization is already low. A) and B) are unrelated to voice quality.

Q14. Compliance requires that syslog messages sent to the central collector be encrypted in transit. Which destination should the engineer configure?

A) UDP 162

B) UDP 514

C) TCP 6514 with TLS

D) TCP 443 to the NMS web UI

Correct answer: C

Explanation: Syslog over TLS uses TCP 6514, encrypting log transport end to end; B is the near-miss because UDP 514 is the traditional syslog port but sends messages in plaintext; A is SNMP traps; D reaches a web interface, not the syslog collector.

Q15. Remote users complain that web browsing is very slow whenever the VPN is connected because all traffic is tunneled through headquarters. Which VPN option resolves this?

A) Split tunneling

B) Full tunneling

C) Site-to-site VPN

D) Disabling encryption

Correct answer: A

Explanation: Split tunneling sends only corporate-bound traffic through the VPN while internet traffic goes directly out the local connection, relieving the HQ bottleneck; B is the near-miss because full tunneling is the current (problematic) configuration; C connects sites, not individual remote users; D would weaken security without fixing routing.

Q16. A UPS can sustain the data center for 20 minutes, but a utility outage lasts 6 hours. Which component bridges this gap?

A) Larger UPS batteries alone

B) Surge protector

C) Diesel generator

D) Second UPS in parallel

Correct answer: C

Explanation: Generators provide long-duration power by burning fuel, covering outages far beyond battery runtime; A is the near-miss because bigger batteries add minutes, not hours, and are impractical at data center scale; C only clamps spikes; D adds redundancy, not extended runtime.

Q17. A recovery site has servers, storage, and network connectivity installed but holds no current data. What type of site is this?

A) Hot site

B) Production site

C) Warm site

D) Cold site

Correct answer: C

Explanation: A warm site has hardware ready but requires data restoration before operation; A is the near-miss because a hot site is fully operational with current data; D provides only space and utilities; B is the live environment.

Q18. Backup tapes are rotated to an offsite vault weekly. Which risk does this primarily address?

A) Site-level disaster destroying on-site copies

B) Accidental deletion of files by end users

C) Slow backup performance during the backup window

D) Expired licenses on the backup software

Correct answer: A

Explanation: Geographic separation ensures a surviving copy when fire, flood, or theft destroys the primary site; B is the near-miss because versioning/retention addresses deletions, while offsite addresses location loss; C and D are unrelated.

Q19. A new help-desk intern is granted read-only access to the ticketing system and no access to servers, network gear, or financial records. Which principle is being applied?

A) Least privilege

B) Due diligence

C) Need to know

D) Separation of duties

Correct answer: A

Explanation: Granting only the minimum rights needed to do the job is least privilege. C is the near-miss: need-to-know is closely related but refers to limiting access to specific information, while least privilege covers the overall scope of rights; D requires splitting a sensitive task across people; B means taking reasonable care, not an access rule.

Q20. A visitor plugs a laptop into an empty but active wall jack in a conference room and gains LAN access. Which hardening step would have prevented this?

A) Increasing the DHCP lease time to reduce renewals

B) Enabling SNMP traps

C) Enabling jumbo frames on the switch ports

D) Disabling unused switch ports

Correct answer: D

Explanation: Administratively shutting down ports that aren't in use removes the physical attack surface. B is tempting as a detective control, but traps only alert after access has occurred; A and C are unrelated performance settings.

Q21. Match each AAA function to its port and transport: 1) RADIUS authentication | 2) RADIUS accounting | 3) TACACS+ — with: X) UDP 1812 | Y) UDP 1813 | Z) TCP 49. Which pairing is correct?

A) 1-X, 2-Z, 3-Y

B) 1-Z, 2-Y, 3-X

C) 1-X, 2-Y, 3-Z

D) 1-Y, 2-X, 3-Z

Correct answer: C

Explanation: RADIUS authentication uses UDP 1812 (1-X); RADIUS accounting uses UDP 1813 (2-Y); TACACS+ uses TCP 49 (3-Z). B is the near-miss — it swaps the RADIUS authentication port with TACACS+, confusing the two AAA protocols' transports and numbers.

Q22. A small business has no RADIUS server but wants the strongest practical Wi-Fi security for employee laptops. Which should it deploy?

A) An open network with a captive portal

B) WPA2-Enterprise

C) WPA3-Personal

D) WPA2-Personal with WPS enabled

Correct answer: C

Explanation: WPA3-Personal (SAE) is the strongest option that doesn't need RADIUS infrastructure. B is tempting as "Enterprise," but it requires a RADIUS server the business lacks; C retains the crackable WPS PIN; A provides no encryption at all.

Q23. Place the steps of the CompTIA troubleshooting methodology in the correct order: 1. Implement the solution or escalate 2. Document findings, actions, and outcomes 3. Establish a theory of probable cause 4. Identify the problem 5. Verify full system functionality and implement preventive measures 6. Test the theory to determine the cause 7. Establish a plan of action and identify potential effects

A) $4 \rightarrow 6 \rightarrow 3 \rightarrow 7 \rightarrow 1 \rightarrow 2 \rightarrow 5$

B) $4 \rightarrow 3 \rightarrow 6 \rightarrow 7 \rightarrow 1 \rightarrow 5 \rightarrow 2$

C) $3 \rightarrow 4 \rightarrow 6 \rightarrow 1 \rightarrow 7 \rightarrow 5 \rightarrow 2$

D) $4 \rightarrow 3 \rightarrow 6 \rightarrow 1 \rightarrow 7 \rightarrow 5 \rightarrow 2$

Correct answer: B

Explanation: The correct sequence is identify the problem, establish a theory, test the theory, establish a plan of action, implement the solution, verify functionality, then document. C is tempting because theorizing feels like it comes first, but identification precedes theory; C also skips establishing a plan before implementing, which is a classic exam trap; D implements the solution before establishing a plan of action, which is illogical.

Q24. A technician pings a printer at 192.168.10.45 on the local subnet and immediately receives "Destination host unreachable" with no "Reply from" line. What does this indicate?

A) The local PC could not resolve the printer's MAC address, likely because the printer is offline

B) The default gateway has no route to the 192.168.10.0 network, so it cannot forward the echo requests

C) The DNS server has no record for the printer, preventing name resolution before the ping is sent

D) A firewall on the printer is blocking ICMP echo requests, silently discarding the probes

Correct answer: A

Explanation: Without a "Reply from" line, the unreachable message comes from the local TCP/IP stack, which sends it when ARP fails to resolve the destination MAC — typical when the target is powered off or disconnected. B would show "Reply from <gateway IP>," D would produce "Request timed out" instead, and C is irrelevant since an IP address was pinged directly.

Q25. A server port shows errors. You check the exhibit from "show interfaces" and answer the question.

A) A Layer 1 problem such as a damaged cable, EMI, or a faulty NIC

B) A broadcast storm on the VLAN, flooding the port with excessive broadcast traffic

C) An incorrect VLAN assignment on the port, placing the server in the wrong broadcast domain

D) A duplex mismatch between the switch and the server, causing collisions and retransmissions

Correct answer: A

Explanation: CRC/input errors with zero collisions on a full-duplex link point below Layer 2 — damaged cable, interference, or bad hardware — so A is correct. D is the near-miss, but a duplex mismatch on a full-duplex link produces collisions and late collisions, not clean CRC errors; B would show high broadcast counters rather than CRC errors; C causes loss of connectivity, not frame corruption.

Q26. A technician suspects a duplex mismatch on a switch-to-server link. Which command provides the BEST evidence?

A) show version — it displays the IOS version, uptime, and hardware details

B) show interfaces — it shows duplex status plus collision and error counters

C) show arp — it displays the ARP table mapping IP addresses to MAC addresses

D) show ip route — it displays the routing table with codes and metrics

Correct answer: B

Explanation: show interfaces directly reports negotiated duplex and the collision/FCS counters that betray a mismatch. D shows routes; C shows ARP mappings; A shows IOS version — none reveal duplex state or Layer 2 errors.

Q27. Workstations receive valid IP addresses and can ping by IP, but no names resolve. You review the exhibit from "ipconfig /all" and answer the question.

A) A routing loop exists, circulating packets until TTL expiration

B) The workstations' cables are faulty, breaking physical connectivity

C) DHCP scope option 6 (DNS servers) is missing or misconfigured

D) The default gateway is wrong, blocking all off-subnet traffic

Correct answer: C

Explanation: IP works but DNS servers were never delivered to the clients — option 6 defines them in DHCP — so C is correct. D would break ping-by-IP beyond the subnet; A produces TTL symptoms; B would break all connectivity.

Q28. A fiber link shows light on the receive meter but the link will not come up. The technician discovers the transmit and receive strands are crossed at one end. What is the fix?

A) Swap the TX/RX strands so transmit connects to receive at each end

B) Change the IP addresses on both ends to resolve the conflict

C) Replace the fiber with copper to eliminate the optical issue

D) Increase the laser transmit power to overcome the signal loss

Correct answer: A

Explanation: Fiber links require TX→RX crossover — with strands crossed, each side transmits into the other's transmit. Swapping one end's pair corrects it. C is drastic overkill; D doesn't fix misdirected light; B is a Layer 3 red herring for a Layer 1 problem.

Q29. Users on VoIP-over-Wi-Fi calls experience dropped audio when walking between buildings, though data applications recover seamlessly. What is the MOST likely cause?

A) A failing internet connection, disrupting all traffic to external networks

B) An incorrect MTU on the APs, fragmenting the voice packets in transit

C) Poor roaming — a coverage gap or slow AP transition breaks the real-time session

D) A DHCP scope exhaustion, preventing new clients from obtaining addresses

Correct answer: C

Explanation: Voice can't tolerate the gap during a slow roam, while TCP-based data apps retransmit and recover — the symptom split points at roaming. D would block new connections entirely; B affects packet size, not mobility; A would break all traffic, not just roaming voice.

Q30. A technician reports: ping to the gateway is <1 ms, pings beyond it time out, traceroute dies at the third ISP hop, but a looking glass in another country successfully reaches the company's public servers. What is the MOST likely conclusion?

A) The ISP's outbound path or filtering beyond hop 3 is faulty — inbound connectivity works

B) A routing loop exists inside the company network, circulating packets until TTL expires

C) The local gateway is misconfigured, blocking all outbound traffic from the LAN

D) The company's firewall is blocking all outbound traffic at the network edge

Correct answer: A

Explanation: The looking glass proves the company's network is reachable from the outside, while the local traceroute dying at the ISP's third hop localizes the fault to the ISP's forward path — likely filtering or an outage. D is the near-miss, but a local firewall block wouldn't stop the trace at the ISP's hop 3; C is ruled out by the <1 ms gateway ping; B would show repeating hops, not a clean die-off at the ISP.