



CompTIA Network+ N10-009 Practice Questions

Shared by Daugherty on 13-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page



Question 1

Question Type: MultipleChoice

A network administrator is migrating a domain to a different provider. As part of the onboarding process, the new provider requests domain ownership proof. Which of the following records would the administrator most likely need to create?

Options:

- A- A
- B- CNAME
- C- PTR
- D- TXT

Answer:

D

Explanation:

The best answer is D. TXT. When a provider asks an administrator to prove ownership of a domain, the most common method is to have the administrator place a specific verification value inside a DNS TXT record. The provider then checks public DNS for that value. If the expected text is present, it confirms that the person managing the migration has control over the domain's DNS settings.

This matches how TXT records are commonly used in real network environments. They are flexible and can store readable text strings for verification, policy, and security-related purposes. In Network+ study material, TXT records are frequently associated with things like domain validation and email-related configurations such as SPF and other verification mechanisms.

The other record types do not fit this task. An A record maps a hostname to an IPv4 address. A CNAME points one name to another name. A PTR record is used for reverse DNS, mapping an IP address back to a hostname. None of those are typically created just to prove domain ownership during provider onboarding.

The key clue is the phrase "domain ownership proof", which strongly points to a TXT record.

Question 2

Question Type: MultipleChoice

A network administrator is configuring a network for a new site that will have 150 users. Within the next year, the site is expected to grow by ten users. Each user will have two IP addresses, one for a computer and one for a phone connected to the network. Which of the following classful IPv4 address ranges will be best-suited for the network?

Options:

- A- Class D
- B- Class B
- C- Class A
- D- Class C

Answer:

D

Explanation:

IPv4 addresses are divided into classes:

Class A: Supports 16,777,214 hosts (large enterprises).

Class B: Supports 65,534 hosts (medium to large networks).

Class C: Supports 254 hosts (small to medium networks).

Class D: Used for multicast, not for assigning IPs to hosts.

Step-by-step Calculation:

The network will have 150 users initially, with a projected growth of 10 users, totaling 160 users.

Each user has two devices, so $160 \times 2 = 320$ IP addresses needed.

A Class C subnet has 254 usable IPs by default, which is not sufficient.

A Class B subnet can support thousands of hosts, making it the most appropriate option.

Incorrect Options:

A . Class D: Reserved for multicast, not for host assignments.

C . Class A: Overkill for a network of this size.

D . Class C: Cannot support 320 hosts without subnetting, making Class B the best choice.

CompTIA Network+ N10-009 Official Study Guide -- Chapter on IP Addressing and Subnetting

Question 3

Question Type: MultipleChoice

A user cannot access an external server for a client after connecting to a VPN. Which of the following commands would a support agent most likely use to examine the issue? (Select two).

Options:

- A- nslookup
- B- tcpdump
- C- arp
- D- dig
- E- tracert
- F- route print

Answer:

E, F

Explanation:

When a user connects to a VPN and experiences connectivity issues to an external server, the problem is often related to routing or network path issues.

E . tracert:

Traces the path packets take from the user's device to the destination server.

Helps determine if the traffic is being blocked or misrouted.

F . route print:

Displays the device's routing table.

Helps diagnose whether traffic is being sent to the VPN tunnel instead of the correct external server.

Incorrect Options:

A . nslookup: Used for resolving domain names to IPs (DNS troubleshooting), but this issue is likely routing-related.

- B . tcpdump: Captures packets for deep packet analysis, not typically the first step in diagnosing a VPN-related access issue.
- C . arp: Used for resolving local network MAC addresses, not relevant for external VPN issues.
- D . dig: Like nslookup, used for DNS queries, but not useful for routing problems.

CompTIA Network+ N10-009 Official Study Guide -- Chapter on Troubleshooting Network Connectivity

Question 4

Question Type: MultipleChoice

A customer calls the help desk to report issues connection to the internet. The customer can reach a local database server. A technician goes to the site and examines the configuration:

Which of the following is causing the user's issue?

Options:

- A- Incorrect DNS
- B- Unreachable gateway
- C- Failed root bridge
- D- Poor upstream routing

Answer:

B

Explanation:

The customer can access local resources (a database server), which means local networking is working. However, the inability to reach the internet suggests an issue with the default gateway. If the default gateway is unreachable, packets will not be routed outside the local network.

Breakdown of Options:

A . Incorrect DNS -- DNS issues would cause problems resolving domain names, but the user should still be able to access external resources via IP addresses.

B . Unreachable gateway -- Correct answer. If the default gateway is incorrect or unreachable,

the device cannot route traffic to the internet.

C . Failed root bridge -- STP (Spanning Tree Protocol) failures cause switching issues, but the user can still access local devices, meaning STP is not the problem.

D . Poor upstream routing -- Would affect the entire network, not just one user.

CompTIA Network+ (N10-009) Official Study Guide -- Domain 2.3: Explain network routing concepts.

Question 5

Question Type: MultipleChoice

A systems administrator needs to connect two laptops to a printer via Wi-Fi. The office does not have access points and cannot purchase any. Which option best wireless network types best fulfills this requirement?

Options:

- A- Mesh
- B- Infrastructure
- C- Ad hoc
- D- Point-to-point

Answer:

C

Explanation:

Comprehensive and Detailed Explanation (aligned to N10-009):

An ad hoc wireless network allows devices to connect directly to each other without an access point. This is suitable for small, temporary setups like two laptops and a printer.

A . Mesh requires multiple nodes forming a larger distributed network.

B . Infrastructure requires an AP, which is not available here.

D . Point-to-point is typically for long-distance wireless links between two fixed endpoints.

Reference (CompTIA Network+ N10-009):

Question 6

Question Type: MultipleChoice

A network administrator is configuring a new switch and wants to ensure that only assigned devices can connect to the switch. Which of the following should the administrator do?

Options:

- A- Configure ACLs.
- B- Implement a captive portal.
- C- Enable port security.
- D- Disable unnecessary services.

Answer:

C

Question 7

Question Type: MultipleChoice

A network administrator needs to assign IP addresses to a newly installed network. They choose 192.168.1.0/24 as their network address and need to create three subnets with 30 hosts on each subnet. Which option best is a valid subnet mask that will meet the requirements?

Options:

- A- 255.255.255.128
- B- 255.255.255.192
- C- 255.255.255.224
- D- 255.255.255.240

Answer:

C

Explanation:

Understanding the Requirements

Network Address: 192.168.1.0/24

The /24 notation means a subnet mask of 255.255.255.0, providing 256 total addresses (192.168.1.0--192.168.1.255).

Usable hosts: $256 - 2$ (network and broadcast) = 254.

Goal: Create 3 subnets, each with 30 hosts.

Each subnet needs enough addresses to accommodate 30 hosts, plus 2 reserved addresses (network and broadcast) per subnet.

Total addresses per subnet = 30 (hosts) + 2 (network/broadcast) = 32 addresses.

Subnetting Basics (Networking Fundamentals)

Subnet Mask: Determines how many bits are borrowed from the host portion to create subnets.

Original Mask: /24 (255.255.255.0) = 24 network bits, 8 host bits.

Formulae:

Number of subnets = $2^{(\text{number of borrowed bits})}$.

Number of addresses per subnet = $2^{(\text{remaining host bits})}$.

Usable hosts per subnet = $2^{(\text{remaining host bits})} - 2$.

We need:

At least 3 subnets.

At least 32 addresses per subnet (to fit 30 hosts + 2 reserved).

Step-by-Step Analysis

Determine Addresses Needed per Subnet:

32 addresses is a power of 2 ($2^5 = 32$).

This means each subnet requires 5 host bits (since $2^5 = 32$ total addresses, and $32 - 2 = 30$ usable hosts).

Calculate Remaining Bits:

Original network has 8 host bits (/24).

If 5 bits are left for hosts, we borrow: $8 - 5 = 3$ bits for subnetting.

New Subnet Mask:

Original mask: /24 (24 network bits).

Borrow 3 bits: $24 + 3 = /27$.

$/27 = 255.255.255.224$ (binary: 11111111.11111111.11111111.11100000).

Verify Requirements:

Number of Subnets: $2^3 = 8$ subnets (meets the requirement of at least 3).

Addresses per Subnet: $2^5 = 32$ addresses.

Usable Hosts per Subnet: $32 - 2 = 30$ hosts (exactly meets the requirement).

Subnet Breakdown:

Increment: $256 - 224 = 32$ (each subnet increments by 32 in the fourth octet).

Subnets:

192.168.1.0--192.168.1.31 (Network: .0, Broadcast: .31, Hosts: .1--.30)

192.168.1.32--192.168.1.63 (Network: .32, Broadcast: .63, Hosts: .33--.62)

192.168.1.64--192.168.1.95 (Network: .64, Broadcast: .95, Hosts: .65--.94)

(And 5 more subnets up to 192.168.1.255.)

Three subnets fit perfectly with 30 hosts each.

Evaluating the Options

A . 255.255.255.128 (/25):

Borrow 1 bit: $24 + 1 = /25$.

Subnets: $2^1 = 2$ (not enough, need 3).

Host bits: 7 ($2^7 = 128$ addresses, 126 hosts).

Why Not: Only 2 subnets, fails the requirement.

B . 255.255.255.192 (/26):

Borrow 2 bits: $24 + 2 = /26$.

Subnets: $2^2 = 4$ (meets 3).

Host bits: 6 ($2^6 = 64$ addresses, 62 hosts).

Why Not: 62 hosts exceeds 30, but it's overkill; /27 is more efficient and still valid.

C . 255.255.255.224 (/27):

Borrow 3 bits: $24 + 3 = /27$.

Subnets: $2^3 = 8$ (meets 3).

Host bits: 5 ($2^5 = 32$ addresses, 30 hosts).

Why Yes: Perfectly fits 3 subnets with exactly 30 hosts each.

D . 255.255.255.240 (/28):

Borrow 4 bits: $24 + 4 = /28$.

Subnets: $2^4 = 16$ (meets 3).

Host bits: 4 ($2^4 = 16$ addresses, 14 hosts).

Why Not: Only 14 hosts per subnet, fails the 30-host requirement.

Why /27 (255.255.255.224) is Best

It provides exactly 30 usable hosts per subnet, avoiding waste while meeting the minimum requirement.

It allows 8 subnets, exceeding the need for 3, ensuring flexibility.

The study guide emphasizes efficient subnet design, and /27 balances host count and subnet availability.

CompTIA Network+ Context

Networking Fundamentals: Subnetting is a core skill, requiring understanding of CIDR, binary conversion, and address allocation.

Example from Study Guide: Similar problems calculate subnet masks for specific host counts, reinforcing /27 as a common solution for ~30 hosts.

Question 8

Question Type: MultipleChoice

A network administrator needs to monitor data from recently installed firewalls in multiple locations. Which option best solutions would best meet the administrator's needs?

Options:

A- IDS

B- IPS

C- SIEM

D- SNMPv2

Answer:

C

Explanation:

SIEM (Security Information and Event Management) systems are used to aggregate and analyze log data from various sources, including firewalls, to detect potential security incidents and assist in regulatory compliance. The document explains:

"SIEM solutions aggregate and analyze log and event data from multiple devices, including firewalls, across different locations. They help in real-time monitoring, incident response, and ensuring compliance with security policies."

Question 9

Question Type: MultipleChoice

A technician is deploying new networking hardware for company branch offices. The bridge priority must be properly set. Which option best should the technician configure?

Options:

- A- Spanning tree protocol
- B- Jumbo frames
- C- Perimeter network
- D- Port security

Answer:

A

Explanation:

Spanning Tree Protocol (STP) uses bridge priority values to determine the root bridge in a switched network topology. Correctly configuring bridge priority helps in maintaining a loop-free and efficient network. The document explains:

"Spanning Tree Protocol (STP) uses bridge priority values to determine which switch will be the root bridge, ensuring loop prevention and efficient path selection within the network."

Question 10

Question Type: MultipleChoice

A user connects to a corporate VPN via a web browser and is able to use TLS to access the internal financial system to input a time card. Which of the following best describes how the VPN is being used?

Options:

- A- Clientless
- B- Client-to-site
- C- Full tunnel
- D- Site-to-site

Answer:

A

Question 11

Question Type: MultipleChoice

A customer is adding fiber connectivity between adjacent buildings. A technician terminates the multimode cable to the fiber patch panel. After the technician connects the fiber patch cable, the indicator light does not turn on. Which of the following should a technician try first to troubleshoot this issue?

Options:

- A- Reverse the fibers.
- B- Rereminate the fibers.
- C- Verify the fiber size.
- D- Examine the cable runs for visual faults.

Answer:

A

Explanation:

When working with fiber optic cables, one common issue is that the transmit (TX) and receive (RX) fibers might be reversed. The first step in troubleshooting should be to reverse the fibers at one end to ensure they are correctly aligned (TX to RX and RX to TX). This is a simple and quick step to rule out a common issue before moving on to more complex troubleshooting. Reference: CompTIA Network+ study materials.



To Get Premium Files for N10-009 Visit

<https://www.p2pexams.com/products/n10-009>

For More Free Questions Visit

<https://www.p2pexams.com/comptia/pdf/n10-009>

20%
DISCOUNT

P2P
exams