

## N10-009<sup>Q&As</sup>

CompTIA Network+

### Pass CompTIA N10-009 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.leads4pass.com/n10-009.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA  
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



## QUESTION 1

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?

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

Correct Answer: A

Reference: CompTIA Network+ Certification Exam Objectives - Remote Access Methods section.

---

## QUESTION 2

A network administrator is configuring a wireless network with an ESSID. Which of the following is a user benefit of ESSID compared to SSID?

- A. Stronger wireless connection
- B. Roaming between access points
- C. Advanced security
- D. Increased throughput

Correct Answer: B

An Extended Service Set Identifier (ESSID) allows multiple access points to share the same SSID, enabling seamless roaming for users. This means that users can move between different access points within the same ESSID without losing connection or having to reauthenticate. This provides a better user experience, especially in large environments such as office buildings or campuses. References: CompTIA Network+ study materials.

---

## QUESTION 3

Which of the following can support a jumbo frame?

- A. Access point
- B. Bridge
- C. Hub D. Switch

Correct Answer: D

Definition of Jumbo Frames:

uk.co.certification.simulator.questionpool.PList@47d929cb Why Switches Support Jumbo Frames:

Incompatibility of Other Devices:

Practical Application:

References:

CompTIA Network+ course materials and networking hardware documentation.

---

## QUESTION 4

Which of the following is most likely to be implemented to actively mitigate intrusions on a host device?

- A. HIDS
- B. NIDS
- C. HIPS
- D. NIPS

Correct Answer: C

HIPS is designed to operate on individual host devices (like workstations, servers, etc.) and can actively prevent and mitigate intrusions. It not only detects malicious activities but also has the capability to automatically take action against these threats, such as blocking network traffic or quarantining malware.

---

## QUESTION 5

A network administrator is notified that a user cannot access resources on the network. The network administrator checks the physical connections to the workstation labeled User and sees the Ethernet is properly connected. However, the network interface's indicator lights are not blinking on either the computer or the switch. Which of the following is the most likely cause?

- A. The switch failed.
- B. The default gateway is wrong.
- C. The port is shut down.
- D. The VLAN assignment is incorrect.

Correct Answer: C

If the port is shut down, it means that the switch has disabled the port and is not sending or receiving any traffic on it. This would explain why the network interface's indicator lights are not blinking on either the computer or the switch, and why the user cannot access resources on the network. The port could be shut down manually by the network administrator, or automatically by the switch due to security or error conditions.

---

**QUESTION 6****HOTSPOT**

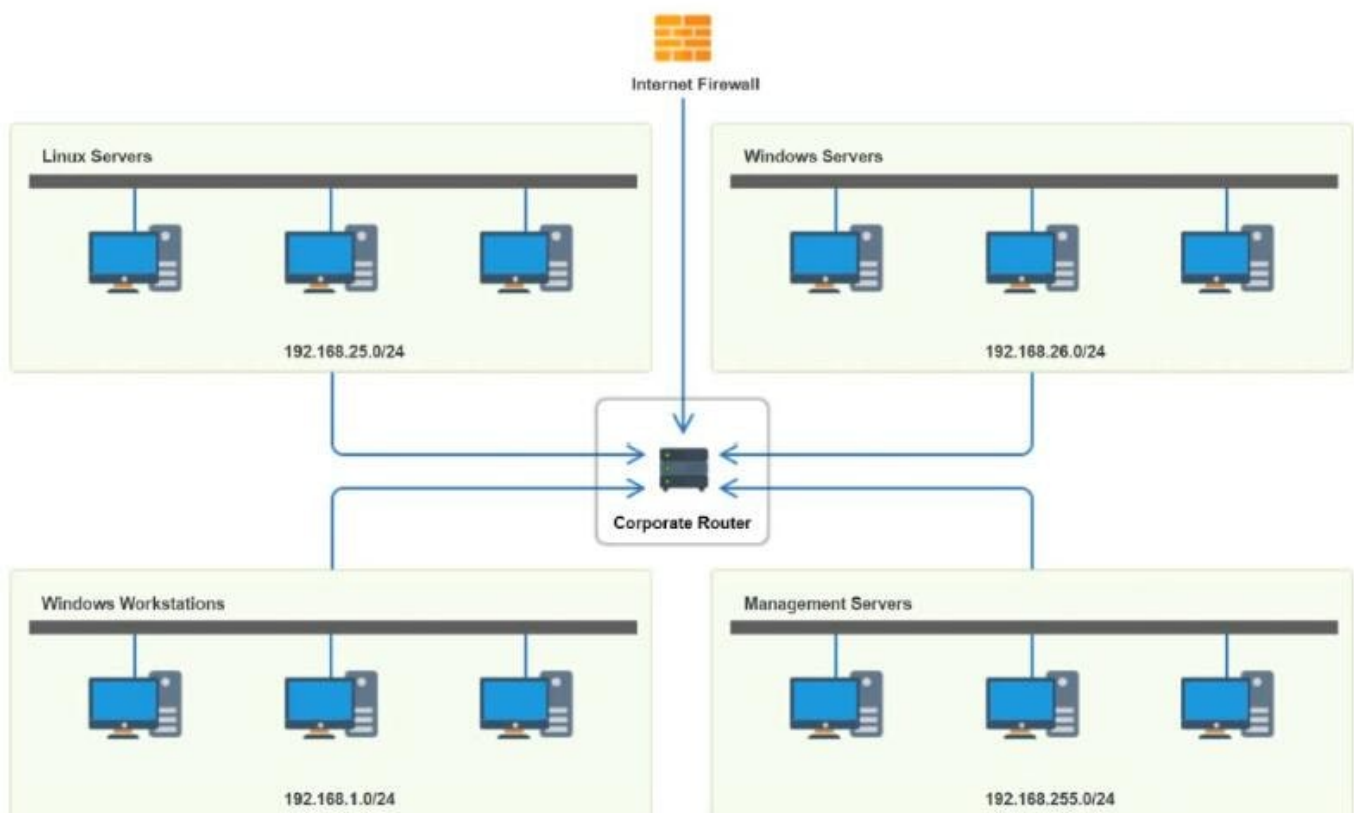
You have been tasked with implementing an ACL on the router that will:

1. Permit the most commonly used secure remote access technologies from the management network to all other local network segments.
2. Ensure the user subnet cannot use the most commonly used remote access technologies in the Linux and Windows Server segments.
3. Prohibit any traffic that has not been specifically allowed.

**INSRCTIONS**

Use the drop-downs to complete the ACL.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Hot Area:

Router Access Control List <span style="float: right;">✕</span>					
Rule	Source	Destination	Protocol	Service	Action
1	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
2	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
3	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
4	192.168.255.0	192.168.26.0	TCP	SMB	Allow
5	192.168.255.0	Any	Any	Any	Deny
6	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
7	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
8	192.168.1.0	Any	Any	Any	Allow
9	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	Any	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny

Correct Answer:

Router Access Control List <span style="float: right;">✕</span>					
Rule	Source	Destination	Protocol	Service	Action
1	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
2	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
3	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
4	192.168.255.0	192.168.26.0	TCP	SMB	Allow
5	192.168.255.0	Any	Any	Any	Deny
6	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
7	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
8	192.168.1.0	Any	Any	Any	Allow
9	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	Any	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny

## QUESTION 7

A customer connects a firewall to an ISP router that translates traffic destined for the internet. The customer can connect to the internet but not to the remote site. Which of the following will verify the status of NAT?

- A. tcpdump
- B. nmap
- C. ipconfig
- D. tracert

Correct Answer: A

tcpdump is a command-line tool that can capture and analyze network traffic on a given interface. tcpdump can verify the status of NAT by showing the source and destination IP addresses of the packets before and after they pass through the ISP router that translates traffic destined for the internet. tcpdump can also show the NAT protocol and port numbers used by the router. nmap, ipconfig, and tracert are not suitable tools for verifying the status of NAT, as they do not show the IP address translation process.

---

## QUESTION 8

Which of the following steps of the troubleshooting methodology would most likely include checking through each level of the OSI model after the problem has been identified?

- A. Establish a theory.
- B. Implement the solution.
- C. Create a plan of action.
- D. Verify functionality.

Correct Answer: D

Introduction to Troubleshooting Methodology:

[uk.co.certification.simulator.questionpool.PList@7e548c79](https://www.pearsoncmg.com/api/v1/print/networking/9780132851442_chapter09.pdf) Troubleshooting Steps:

Verifying Functionality:

of the Options:

Conclusion:

References:

CompTIA Network+ guide explaining the troubleshooting methodology and the importance of verifying functionality (see page Ref 9Basic Configuration Commands).

---



**QUESTION 9**

A customer needs six usable IP addresses. Which of the following best meets this requirement?

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

Correct Answer: D

Reference: CompTIA Network+ Certification Exam Objectives - IP Addressing section.

---

**QUESTION 10**

A customer recently moved into a new office and notices that some wall plates are not working and are not properly labeled

Which of the following tools would be best to identify the proper wiring in the IDF?

- A. Toner and probe
- B. Cable tester
- C. Visual fault locator
- D. Network tap

Correct Answer: A

A toner and probe tool, also known as a tone generator and probe, is used to trace and identify individual cables within a bundle or to locate the termination points of cables in wiring closets and patch panels. It generates a tone that can be picked up by the probe, helping technicians quickly and accurately identify and label wall plates and wiring. This is the best tool for identifying proper wiring in the Intermediate Distribution Frame (IDF). References: CompTIA Network+ Exam Objectives and official study guides.

---

**QUESTION 11**

Which of the following is the most likely reason an insurance brokerage would enforce VPN usage?

- A. To encrypt sensitive data in transit
- B. To secure the endpoint
- C. To maintain contractual agreements
- D. To comply with data retention requirements

Correct Answer: A

The most likely reason an insurance brokerage would enforce VPN usage is to encrypt sensitive data in transit. VPNs (Virtual Private Networks) create a secure tunnel between the user's device and the corporate network, ensuring that data

is encrypted and protected from interception.

Encryption: VPNs encrypt data, preventing unauthorized access and ensuring data privacy during transmission over public or unsecured networks. Data Protection: Essential for industries handling sensitive information, such as insurance

brokerages, to protect customer data and comply with regulatory requirements.

Security: Enhances overall network security by providing secure remote access for employees.

Network References:

CompTIA Network+ N10-007 Official Certification Guide: Discusses the role of VPNs in securing data in transit.

Cisco Networking Academy: Provides training on VPN technologies and their importance in data security.

Network+ Certification All-in-One guide: Explains VPN usage and its benefits in protecting sensitive information.

---

## QUESTION 12

A network administrator is reviewing north-south traffic to determine whether a security threat exists. Which of the following explains the type of traffic the administrator is reviewing?

- A. Data flowing between application servers
- B. Data flowing between the perimeter network and application servers
- C. Data flowing in and out of the data center
- D. Data flowing between local on-site support and backup servers

Correct Answer: C

---

## QUESTION 13

A technician is trying to install a VoIP phone, but the phone is not turning on. The technician checks the cable going from the phone to the switch, and the cable is good. Which of the following actions IS needed for this phone to work?

- A. Add a POE injector
- B. Enable MDIX.
- C. Use a crossover cable.
- D. Reconfigure the port.

Correct Answer: A

## QUESTION 14

A technician is working on a solution to isolate traffic between specific types of devices, servers, and users on the internal firewall. Which of the following traffic flows should be isolated?

- A. East-west
- B. Access/edge
- C. Core/distribution
- D. North-south

Correct Answer: A

---

## QUESTION 15

A network administrator is troubleshooting an issue on a newly configured college campus network. A Linux workstation can connect to the internet, but it fails to connect to the campus intranet, which is located on another campus. Which of the following commands should the administrator run next to troubleshoot the connection?

- A. ifconfig
- B. traceroute
- C. nmap
- D. dig

Correct Answer: B

[N10-009 VCE Dumps](#)

[N10-009 Exam Questions](#)

[N10-009 Braindumps](#)