Download CompTIA N10-009 Exam Dumps Free

Shared by Bowman on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A wireless technician wants to implement a technology that will allow user devices to automatically navigate to the best available frequency standard. Which option best technologies should the technician use?

Options:

A- Band steering
B- Wireless LAN controller
C- Directional antenna
D- Autonomous access point

Answer:

A

Explanation:

Band Steering: This technology enables wireless devices to connect to the most optimal frequency band (2.4 GHz or 5 GHz) by encouraging capable devices to switch to the less congested 5 GHz band. This improves overall network performance and prevents overcrowding on the 2.4 GHz band.

Wireless LAN controller (B): This manages multiple access points in a network but does not handle frequency optimization.

Directional antenna (C): This focuses the signal in a specific direction but does not affect frequency selection.

Autonomous access point (D): This operates independently but lacks advanced features like band steering.

==========

Question 2

Question Type: MultipleChoice

A company's network is experiencing high latency and packet loss during peak hours. Network

monitoring tools show increased traffic on a switch. Which of the following should a network technician implement to reduce the network congestion and improve performance?

Options:

A- Load balancing
B- Port mirroring
C- Quality of Service
D- Spanning Tree Protocol

Answer:

C

Explanation:

Quality of Service (QoS): This is a feature used in networking to prioritize certain types of traffic. By configuring QoS, network administrators can allocate higher bandwidth to time-sensitive applications like VoIP, video conferencing, or critical business applications during peak usage times. This helps to reduce latency and packet loss, which are often caused by congestion.

Load Balancing (A): While load balancing is useful in distributing traffic across multiple servers or paths, it does not address congestion on a single switch.

Port Mirroring (B): This is used for monitoring network traffic for troubleshooting and diagnostics but does not alleviate congestion.

Spanning Tree Protocol (D): STP prevents switching loops in redundant network topologies, but it is not designed to handle traffic prioritization or congestion issues.

Question 3

Question Type: MultipleChoice

A company is implementing a wireless solution in a high-density environment. Which of the following 802.11 standards is used when a company is concerned about device saturation and converage?

Options:

A- 802.11ac
B- 802.11ax
C- 802.11g
D- 802.11n

Answer:

B

Explanation:

802.11ax, also known as Wi-Fi 6, is designed for high-density environments and improves device saturation and coverage compared to previous standards.

802.11ac: While it offers high throughput, it is not optimized for high-density environments as effectively as 802.11ax.

802.11ax (Wi-Fi 6): Introduces features like OFDMA, MU-MIMO, and BSS Coloring, which enhance performance in crowded environments, reduce latency, and increase the number of devices that can be connected simultaneously.

802.11g and 802.11n: Older standards that do not offer the same level of efficiency or support for high device density as 802.11ax.

Network Reference:

CompTIA Network+ N10-007 Official Certification Guide: Covers the 802.11 standards and their capabilities.

Cisco Networking Academy: Provides training on Wi-Fi technologies and best practices for high-density deployments.

Network+ Certification All-in-One Exam Guide: Discusses the various 802.11 standards and their applications in different environments.

Question 4

Question Type: MultipleChoice

Which option best steps in the troubleshooting methodology would be next after putting preventive measures in place?

Options:

A- Implement the solution.
B- Verify system functionality.
C- Establish a plan of action.
D- Test the theory to determine cause.

Answer:

B

Explanation:

After implementing a solution and putting preventive measures in place, the next step is to verify that the system is functioning correctly. This ensures that the issue has been fully resolved.

==========

Question 5

Question Type: MultipleChoice

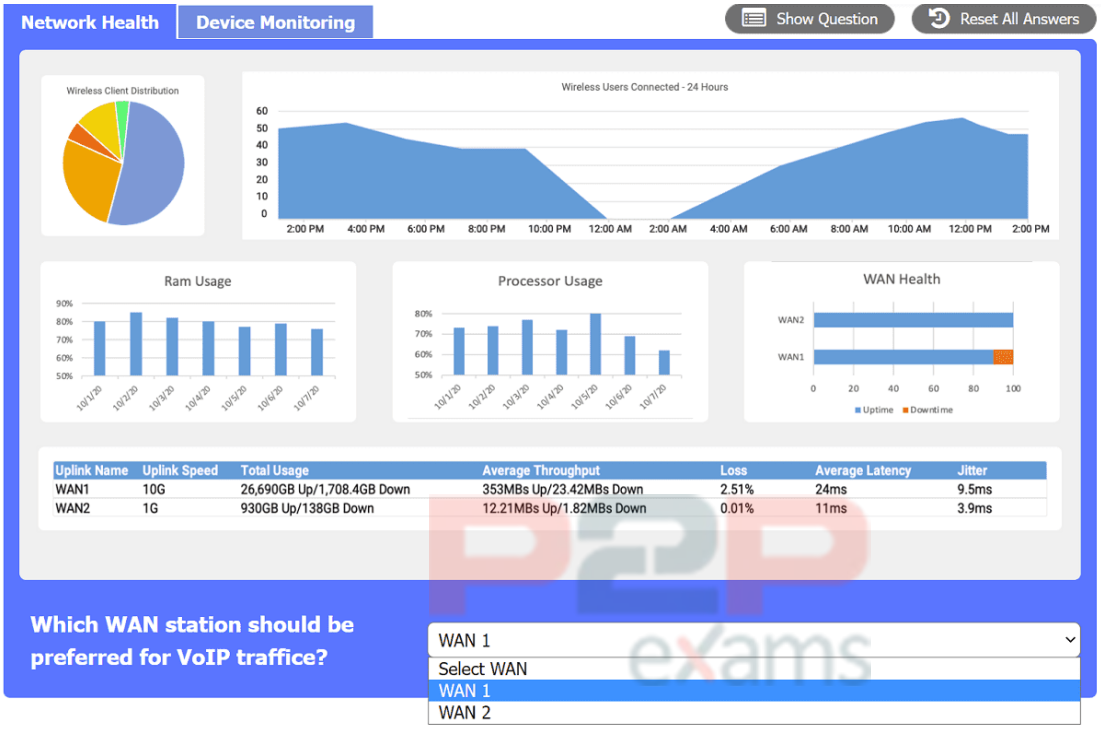
SIMULATION

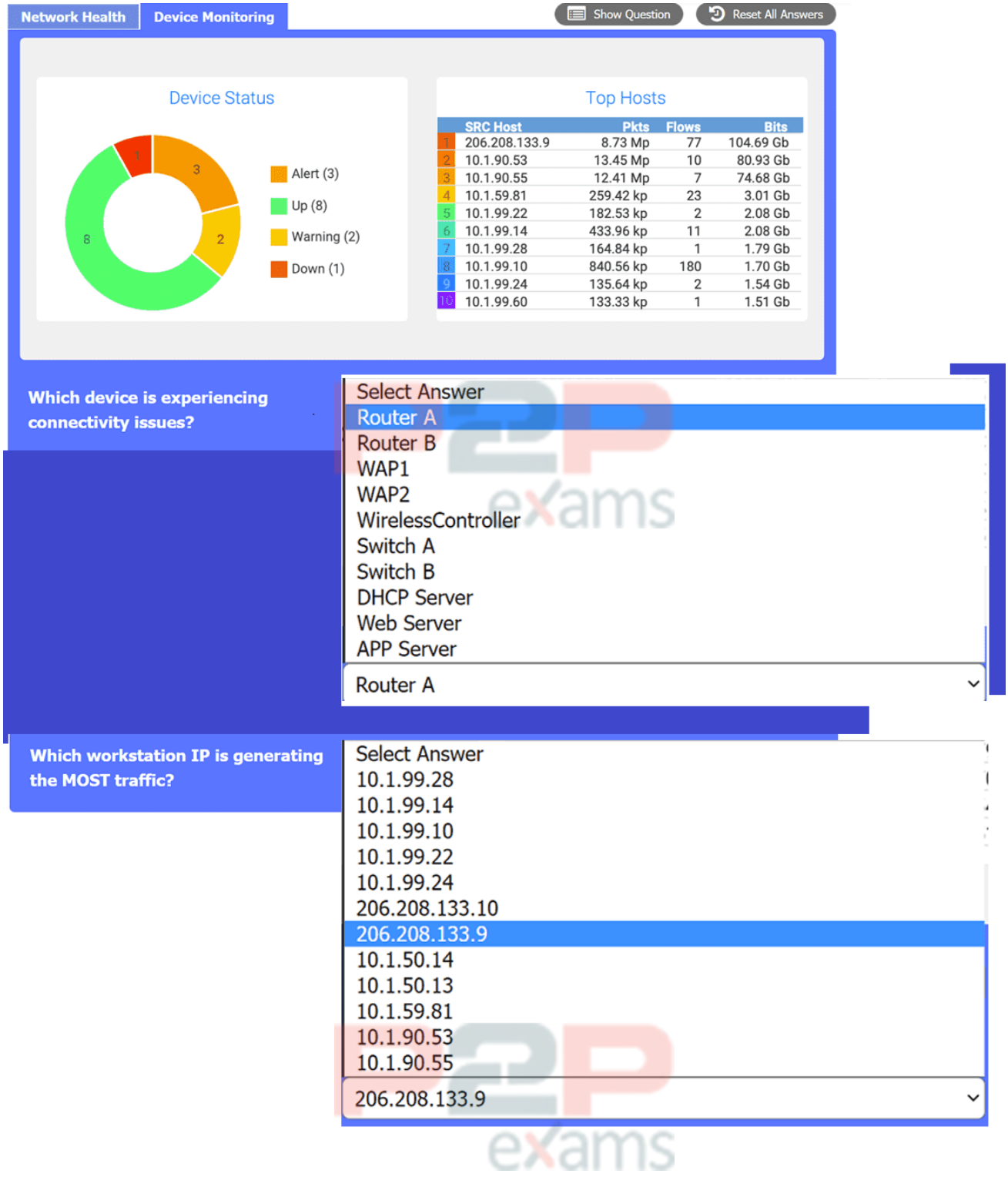
After a recent power outage, users are reporting performance issues accessing the application servers. Wireless users are also reporting intermittent Internet issues.

INSTRUCTIONS

Click on each tab at the top of the screen. Select a widget to view information, then

use the drop-down menus to answer the associated questions. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.


Network Health
Device Monitoring
Show Question
Reset All Answers
Wireless Client Distribution
Wireless Users Connected - 24 Hours
60
50
40
30
20
10
0
2:00 PM
4:00 PM
6:00 PM
8:00 PM
10:00 PM
12:00 AM
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
2:00 PM
Ram Usage
90%
80%
70%
60%
50%
10/1/20
10/2/20
10/3/20
10/4/20
10/5/20
10/6/20
10/7/20
Processor Usage
80%
70%
60%
50%
10/1/20
10/2/20
10/3/20
10/4/20
10/5/20
10/6/20
10/7/20
WAN Health
WAN2
WAN1
0
20
40
60
80
100
Uptime
Downtime
Uplink Name
Uplink Speed
Total Usage
Average Throughput
Loss
Average Latency
Jitter
WAN1
10G
26,690GB Up/1,708.4GB Down
353MBs Up/23.42MBs Down
2.51%
24ms
9.5ms
WAN2
1G
930GB Up/138GB Down
12.21MBs Up/1.82MBs Down
0.01%
11ms
3.9ms
Which WAN station should be preferred for VoIP traffice?
WAN 1
Select WAN
WAN 1
WAN 2



Options:

A- See the solution below in Explanation

Answer:

A

Explanation:

Network Health:

WAN 2 appears to have a lower average latency and loss percentage, which would make it the preferred WAN station for VoIP traffic. VoIP traffic requires low latency and packet loss to ensure good voice quality and reliability. WAN 1 seems to have higher RAM and processor usage, which could also affect the performance of VoIP traffic.

Here's the summary of the key metrics for WAN 1 and WAN 2 from the image provided:

WAN 1:

Uplink Speed: 10G

Total Usage: 26.969GB Up / 1.748GB Down

Average Throughput: 353MBps Up / 23.42MBps Down

Loss: 2.51%

Average Latency: 24ms

Jitter: 9.5ms

WAN 2:

Uplink Speed: 1G

Total Usage: 930GB Up / 138GB Down

Average Throughput: 12.21MBps Up / 1.82MBps Down

Loss: 0.01%

Average Latency: 11ms

Jitter: 3.9ms

For VoIP traffic, low latency and jitter are particularly important to ensure voice quality. While WAN 1 has higher bandwidth and throughput, it also has higher latency and jitter compared to WAN 2. However, WAN 2 has much lower loss, lower latency, and lower jitter, which are more favorable for VoIP traffic that is sensitive to delays and variation in packet arrival times.

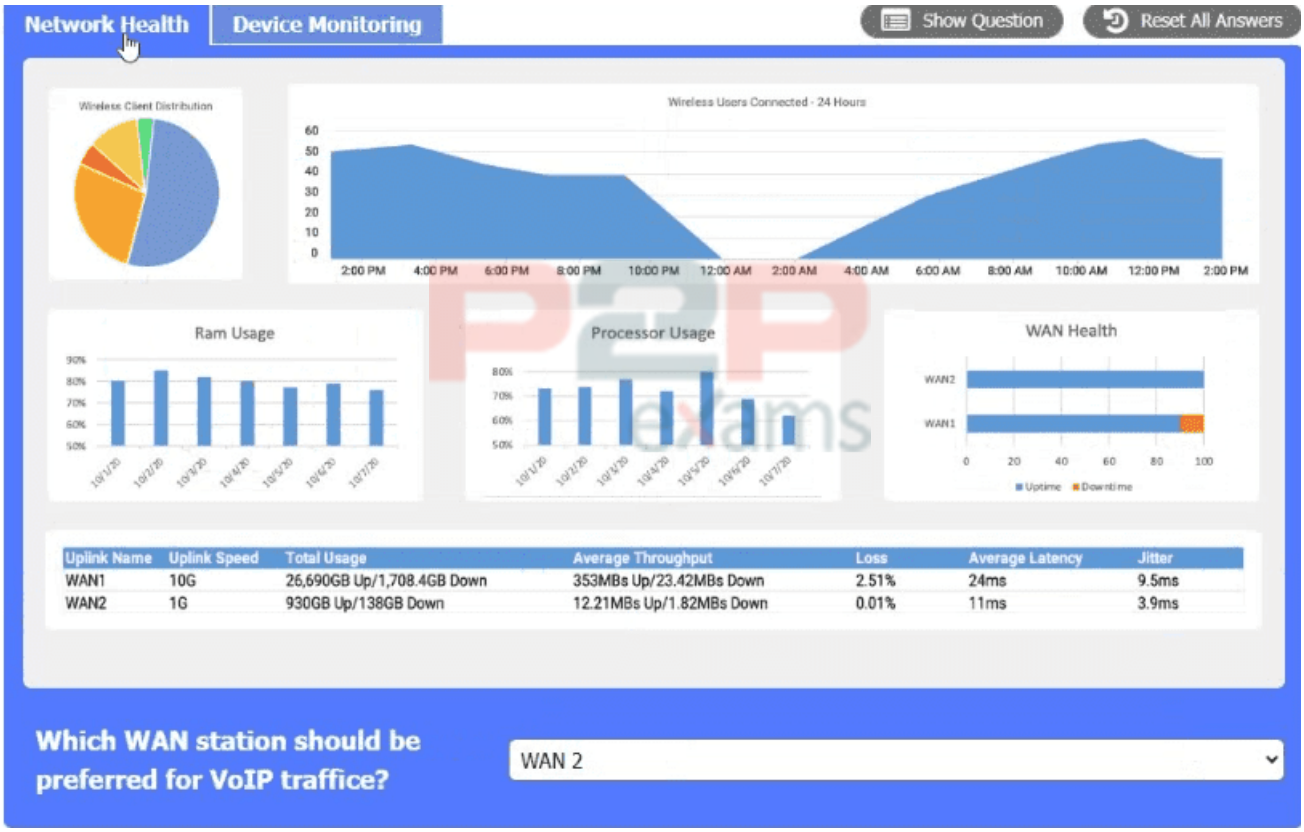
Given this information, WAN 2 would generally be preferred for VoIP traffic due to its lower latency, lower jitter, and significantly lower loss percentage, despite its lower bandwidth compared to WAN 1. The high bandwidth of WAN 1 may be more suitable for other types of traffic that are less sensitive to latency and jitter, such as bulk data transfers.

Device Monitoring:

the device that is experiencing connectivity issues is theAPP Server or Router 1, which has a

status ofDown. This means that the server is not responding to network requests or sending any dat

a. You may want to check the physical connection, power supply, and configuration of the APP Server to troubleshoot the problem.



Question 6

Question Type: MultipleChoice

An IT manager needs to connect ten sites in a mesh network. Each needs to be secured with reduced provisioning time. Which option best technologies will best meet this requirement?

Options:

A- SD-WAN
B- VXLAN
C- VPN
D- NFV

Answer:

A

Explanation:

Definition of SD-WAN:

Software-Defined Wide Area Network (SD-WAN) is a technology that simplifies the management and operation of a WAN by decoupling the networking hardware from its control mechanism. It allows for centralized management and enhanced security.

Benefits of SD-WAN:

Reduced Provisioning Time: SD-WAN enables quick and easy deployment of new sites with centralized control and automation.

Security: Incorporates advanced security features such as encryption, secure tunneling, and integrated firewalls.

Scalability: Easily scales to accommodate additional sites and bandwidth requirements.

Comparison with Other Technologies:

VXLAN (Virtual Extensible LAN): Primarily used for network virtualization within data centers.

VPN (Virtual Private Network): Provides secure connections but does not offer the centralized management and provisioning efficiency of SD-WAN.

NFV (Network Functions Virtualization): Virtualizes network services but does not specifically address WAN management and provisioning.

Implementation:

SD-WAN solutions are implemented by deploying edge devices at each site and connecting them to a central controller. This allows for dynamic routing, traffic management, and security policy enforcement.

CompTIA Network+ course materials and networking solution guides.

Question 7

Question Type: MultipleChoice

Users at a satellite office are experiencing issues when using videoconferencing. Which of the following should a technician focus on first to rectify these issues?

Options:

A- Quality of service
B- Network signal
C- Time to live
D- Load balancing

Answer:

A

Explanation:

Quality of Service (QoS) is crucial for real-time services like video conferencing. It prioritizes voice and video packets over less critical traffic (like file downloads), reducing latency, jitter, and packet loss.

B . Network signal may apply to wireless, but it's not specific to video issues.

C . Time to live (TTL) affects packet lifespan, not performance or quality.

D . Load balancing manages traffic across multiple paths but doesn't prioritize real-time traffic like QoS does.

Reference:

CompTIA Network+ N10-009 Official Objectives: 3.6 -- Explain the characteristics of network topologies and types.

Question 8

Question Type: MultipleChoice

A network technician needs to connect a new user to the company's Wi-Fi network called SSID: business. When attempting to connect, two networks are listed as possible choices: SSID: business and SSID: myaccess. Which of the following attacks is occurring?

Options:

A- On-path
B- Rogue AP
C- Evil twin

D- Tailgating

Answer:

C

Explanation:

An evil twin attack occurs when an attacker creates a fraudulent AP with an SSID very similar (or identical) to the legitimate one. Users may accidentally connect, allowing the attacker to capture traffic and credentials.

A . On-path is the consequence of connecting to the evil twin, not the initial attack itself.

B . Rogue AP is any unauthorized access point, but the key here is the malicious mimicry of a legitimate SSID --- specifically an evil twin.

D . Tailgating is a physical social engineering attack, unrelated to Wi-Fi.

Reference (CompTIA Network+ N10-009):

Domain: Network Security --- Wireless threats (rogue APs, evil twins).

Question 9

Question Type: MultipleChoice

A network administrator notices uncommon communication between VMs on ephemeral ports on the same subnet. The administrator is concerned about that traffic moving laterally within the network. Which option best describes the type of traffic flow the administrator is analyzing?

Options:

A- East-west
B- Point-to-point
C- Horizontal-scaling
D- Hub-and-spoke

Answer:

A

Explanation:

When traffic moves laterally between VMs within the same network or subnet, it is known as east-west traffic. This contrasts with north-south traffic, which refers to communication between internal and external networks.

Breakdown of Options:

A . East-west -- Correct answer. This refers to traffic between internal servers or VMs, which is a common security concern.

B . Point-to-point -- Point-to-point describes a direct connection between two devices, but does not specifically define lateral movement.

C . Horizontal-scaling -- This refers to adding more instances or nodes in cloud computing, unrelated to traffic flow.

D . Hub-and-spoke -- This network topology describes a centralized design, not lateral traffic.

CompTIA Network+ (N10-009) Official Study Guide -- Domain 1.4: Analyze traffic patterns and behavior.

NIST SP 800-207: Zero Trust Architecture (ZTA) -- East-West traffic monitoring

Question 10

Question Type: MultipleChoice

A network architect needs to create a wireless field network to provide reliable service to public safety vehicles. Which of the following types of networks is the best solution?

Options:

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

Answer:

A

Explanation:

A mesh network is the best solution for providing reliable wireless service to public safety vehicles. In a mesh network, each node (vehicle) can connect to multiple other nodes, providing multiple paths for data to travel. This enhances reliability and redundancy, ensuring continuous connectivity even if one or more nodes fail. Mesh networks are highly resilient and are well-suited for dynamic and mobile environments such as public safety operations.Reference: CompTIA Network+ study materials.

P2P exams