



**Free Questions for N10-008 by certsdeals**

**Shared by Horn on 29-01-2024**

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

# Question 1

---

**Question Type: MultipleChoice**

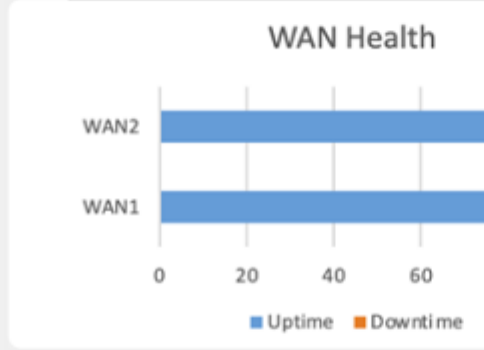
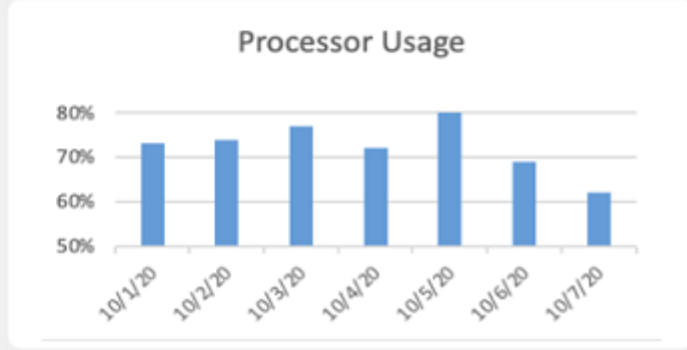
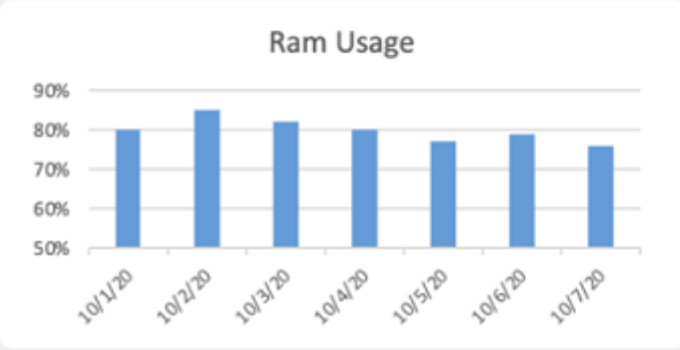
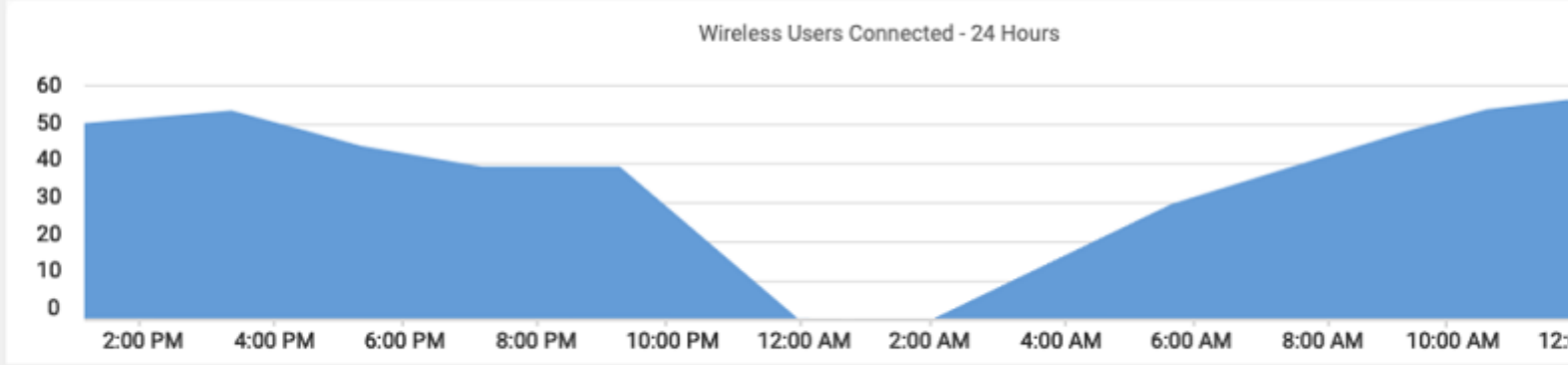
---

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.



Uplink Name	Uplink Speed	Total Usage	Average Throughput	Loss	Average Latency	J
WAN1	10G	26,690GB Up/1,708.4GB Down	353MBs Up/23.42MBs Down	2.51%	24ms	9
WAN2	1G	930GB Up/138GB Down	12.21MBs Up/1.82MBs Down	0.01%	11ms	3

Which WAN station should be preferred for VoIP traffic?

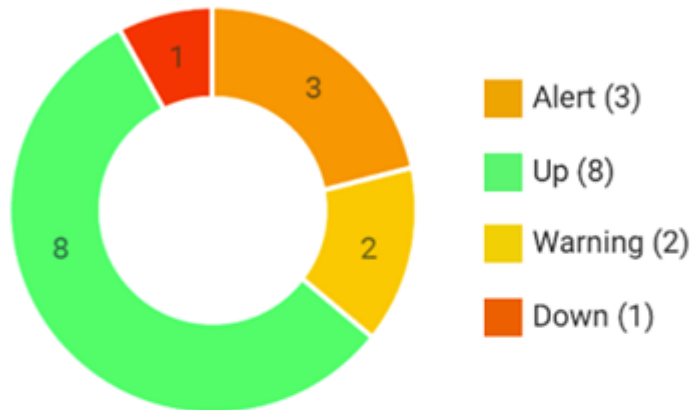
WAN 1

Select WAN

WAN 1



## Device Status



## Top Hosts

	SRC Host	Pkts	Flows	Bits
1	206.208.133.9	8.73 Mp	77	104.69 Gb
2	10.1.90.53	13.45 Mp	10	80.93 Gb
3	10.1.90.55	12.41 Mp	7	74.68 Gb
4	10.1.59.81	259.42 kp	23	3.01 Gb
5	10.1.99.22	182.53 kp	2	2.08 Gb
6	10.1.99.14	433.96 kp	11	2.08 Gb
7	10.1.99.28	164.84 kp	1	1.79 Gb
8	10.1.99.10	840.56 kp	180	1.70 Gb
9	10.1.99.24	135.64 kp	2	1.54 Gb
10	10.1.99.60	133.33 kp	1	1.51 Gb

Which device is experiencing connectivity issues?

Select Answer

Router A

Router B

WAP1

WAP2

WirelessController

Switch A

Switch B

DHCP Server

Web Server

APP Server

## Options:

---

A- See the answer and solution below

## 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

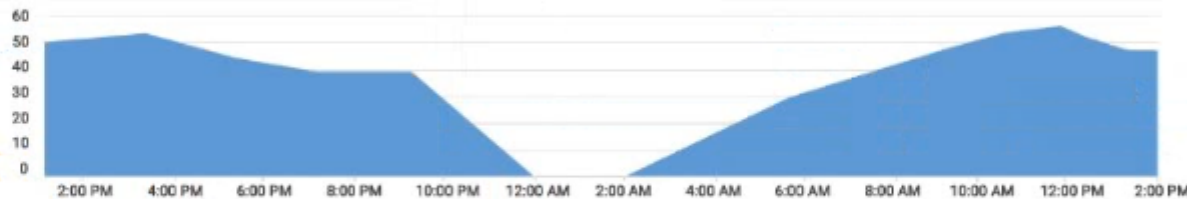
For VoIP traffic, low latency and jitter are particularly important to ensure voice quality. While WAN 1 has higher bandwidth and throughput, it also has higher latency and jitter compared to WAN 2. However, WAN 2 has much lower loss, lower latency, and lower jitter, which are more favorable for VoIP 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.

Wireless Client Distribution



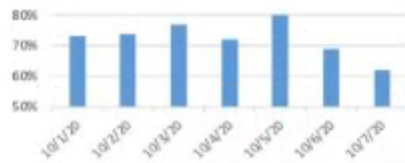
Wireless Users Connected - 24 Hours



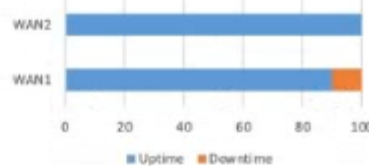
Ram Usage



Processor Usage



WAN Health



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 traffic?

WAN 2

Device Monitoring:




the device that is experiencing connectivity issues is the APP Server or Router 1, which has a status of Down. This means that the server is not responding to network requests or sending any data.

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

Network Health    Device Monitoring    Show Question    Reset All Answers

### Device Status



- Alert (3)
- Up (8)
- Warning (2)
- Down (1)

### Top Hosts

	SRC Host	Pkts	Flows	Bits
1	206.208.133.9	8.73 Mp	77	104.69 Gb
2	10.1.90.53	13.45 Mp	10	80.93 Gb
3	10.1.90.55	12.41 Mp	7	74.68 Gb
4	10.1.59.81	259.42 kp	23	3.01 Gb
5	10.1.99.22	182.53 kp	2	2.08 Gb
6	10.1.99.14	433.96 kp	11	2.08 Gb
7	10.1.99.28	164.84 kp	1	1.79 Gb
8	10.1.99.10	840.56 kp	180	1.70 Gb
9	10.1.99.24	135.64 kp	2	1.54 Gb
10	10.1.99.60	133.33 kp	1	1.51 Gb

Which device is experiencing connectivity issues?    Router A

Which workstation IP is generating the MOST traffic?    206.208.133.9

## Question 2

---

**Question Type:** MultipleChoice

---

A network technician needs to resolve some issues with a customer's SOHO network. The customer reports that some of the PCs are not connecting to the network, while others appear to be working as intended.

### INSTRUCTIONS

Troubleshoot all the network components.

Review the cable test results first, then diagnose by clicking on the appropriate PC, server, and Layer 2 switch.

Identify any components with a problem and recommend a solution to correct each problem.

If at any time you would like to bring back the initial state of the simulation, please

click the Reset All button.

## Cable Test Results ✕

- Switch 1 Length : 16M Port : GigabitEthernet0/5
- Switch 2 VLAN : VLAN 10 Speed : 1000 FDX
- Server
- PC1
- PC2
- PC3
- PC4
- PC5
- PC6

Connected to Switch 2

1 2 3 6 4 5 7 8

1 2 3 6 4 5 7 8

# Cable Test Results



Switch 1

Switch 2

Server

PC1

PC2

PC3

PC4

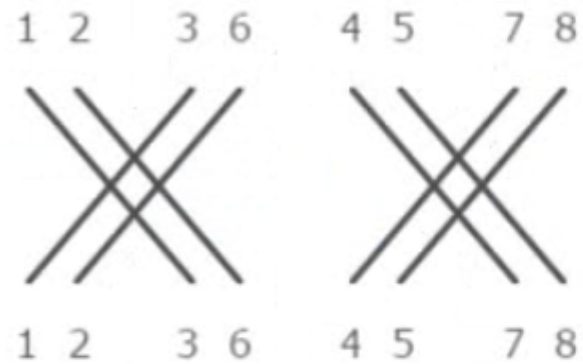
PC5

PC6

Length : 16M      Port : GigabitEthernet0/5

VLAN : VLAN 10      Speed : 1000 FDX

Connected to Switch 1





# Cable Test Results



Switch 1

Length : 42M

Port : GigabitEthernet0/2

Switch 2

VLAN : VLAN 10

Speed : 1000 FDX

Server

**PC1**

PC2

PC3

PC4

PC5

PC6



# Cable Test Results



Switch 1

Length : 12M

Port : GigabitEthernet0/1

Switch 2

VLAN : VLAN 10

Speed : 1000 FDX

Server

PC1

**PC2**

PC3

PC4

PC5

PC6



# Cable Test Results



Switch 1

Length : 20M

Port : GigabitEthernet0/2

Switch 2

VLAN : VLAN 10

Speed : 1000 FDX

Server

PC1

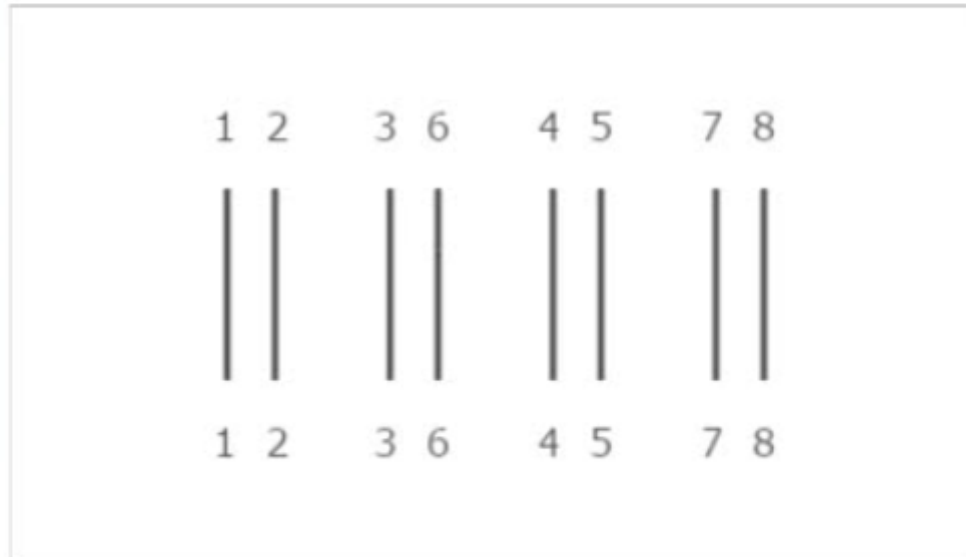
PC2

**PC3**

PC4

PC5

PC6





# Cable Test Results



Switch 1

Length : 18M

Port : GigabitEthernet0/3

Switch 2

VLAN : VLAN 11

Speed : 1000 FDX

Server

PC1

PC2

PC3

PC4

PC5

PC6



# Cable Test Results



Switch 1

Length : 33M      Port : GigabitEthernet0/4

Switch 2

VLAN : VLAN 10      Speed : 1000 FDX

Server

PC1

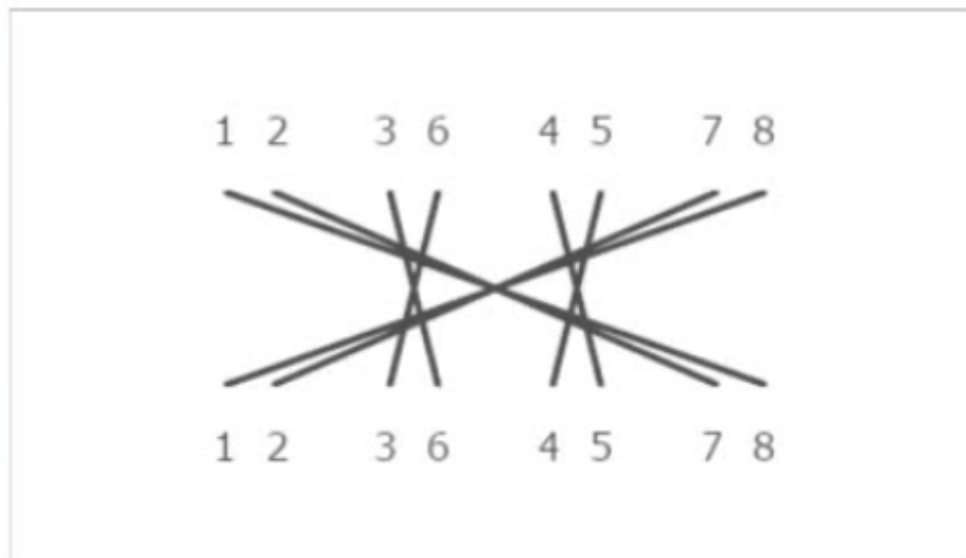
PC2

PC3

PC4

**PC5**

PC6





No Problem  
Cable short detected  
Open cable detected  
Connector on backward  
Bad subnet  
Wrong VLAN  
Cable too long  
Port shut down  
Crossover cable used

No Problem

Select a Solution

Select a Solution  
Replace cable  
Change subnet mask  
Change VLAN assignment  
Change IP address  
Enable Spanning Tree Protocol  
Enable port security

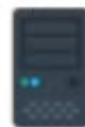
No Problem  
Cable short detected  
Open cable detected  
Connector on backward  
Bad subnet  
Wrong VLAN  
Cable too long  
Port shut down  
Crossover cable used

No Problem

Select a Solution

Select a Solution  
Replace cable  
Change subnet mask  
Change VLAN assignment  
Change IP address  
Enable Spanning Tree Protocol  
Enable port security  
Flush ARP cache  
Change gateway address  
Change DNS Address  
Release and renew IP address

PC1



No Problem  
Cable short detected  
Open cable detected  
Connector on backward  
Bad subnet  
Wrong VLAN  
Cable too long  
Port shut down  
Crossover cable used

No Problem

Select a Solution

Select a Solution  
Replace cable  
Change subnet mask  
Change VLAN assignment  
Change IP address  
Enable Spanning Tree Protocol  
Enable port security  
Flush ARP cache  
Change gateway address  
Change DNS Address  
Release and renew IP address

PC2



**Options:**

---

**A-** See the answer and solution below

**Answer:**

---

A

## Question 3

---

**Question Type:** MultipleChoice

---

A company's management team wants to implement NAC on the wired and wireless networks. Which of the following is an authentication component that must be used in this solution?

**Options:**

---

**A-** IPSec

**B-** 802.1X

**C-** EAP

**D-** TACACS+

**Answer:**

---

B

**Explanation:**

---

802.1X is an authentication component that must be used in a network access control (NAC) solution. NAC is a method of enforcing security policies on devices that want to access a network, by verifying their identity, compliance, and authorization. 802.1X is a standard that defines how to provide authentication for devices trying to connect to a LAN or WLAN. It uses the Extensible Authentication Protocol (EAP) to exchange authentication information between the device (supplicant), the network access device (authenticator), and the authentication server (typically RADIUS or TACACS+). 802.1X can prevent unauthorized devices from accessing the network, and can also assign them to different VLANs or apply different policies based on their role or group.

IPSec is a protocol suite that provides encryption, authentication, and integrity for IP packets. It can be used to create secure VPN tunnels between networks or hosts. IPSec is not an authentication component for NAC, but rather a security component for protecting data in transit.

EAP is a framework that supports multiple authentication methods, such as passwords, certificates, tokens, or biometrics. EAP is used by 802.1X to provide authentication for network access, but it is not a component by itself. EAP requires a carrier protocol, such as 802.1X, to transport the authentication messages.

TACACS+ is a protocol that provides authentication, authorization, and accounting (AAA) services for network devices or users. It can be used as an authentication server for 802.1X, but it is not an authentication component for NAC by itself. TACACS+ requires a client-server protocol, such as 802.1X, to communicate with the network access device.

[Reference What is 802.1X Network Access Control \(NAC\)? Compare TACACS + and RADIUS 802.1X: What EXACTLY is it regarding WPA and EAP? CompTIA Network+ Certification All-in-One Exam Guide, Eighth Edition \(Exam N10-008\)](#)

## Question 4

---

**Question Type:** MultipleChoice

---

A technician is troubleshooting a client's report about poor wireless performance. Using a client monitor, the technician notes the following information:

SSID	Signal (RSSI)	Channel
Corporate	-50	9
Corporate	-69	10
Corporate	-67	11
Corporate	-63	6

Which of the following is most likely the cause of the issue?

## Options:

---

- A- Channel overlap
- B- Poor signal
- C- Incorrect power settings
- D- Wrong antenna type

## Answer:

---

A

## Explanation:

---

Channel overlap is a situation where multiple wireless networks use the same or adjacent frequency channels, causing interference and degradation of performance. According to the image, the corporate SSID is using channels 9, 10, 11, and 6, which are overlapping with each other and with other networks in the area. This can reduce the signal quality and strength, increase the noise and latency, and cause dropouts and connectivity issues. To avoid channel overlap, it is recommended to use non-overlapping channels, such as 1, 6, and 11, in the 2.4 GHz band, or to switch to the 5 GHz band if possible<sup>12</sup>.

Reference

1 - What happens when wifi channels overlap? - Server Fault

2 - Is it better to use a crowded 2.4GHz Wi-Fi channel 1, 6, 11 or "unused" 3, 4, 8, or 9? - Super User



## Question 5

---

**Question Type:** MultipleChoice

---

A technician is working on a ticket for a user in the human resources department who received a new PC that does not connect to the internet. All users in human resources can access the

internet. The technician can ping the PC from the human resources router but not from the IT network. Which of the following is the most likely cause of the issue?

### Options:

---

- A- Duplicate IP address
- B- Misconfigured RIP
- C- Improper VLAN assignment
- D- Incorrect default gateway

### Answer:

---

D

## **Explanation:**

---

An incorrect default gateway can cause a PC to not connect to the internet, because the default gateway is the device that routes traffic from the local network to other networks. If the PC has a wrong default gateway configured, it may not be able to reach the internet router or the IT network router. The technician can ping the PC from the human resources router because they are on the same local network, but not from the IT network router because they are on different networks.

A duplicate IP address can cause a PC to not communicate with other devices on the same network, because the IP address is the unique identifier of a device on a network. If two devices have the same IP address, they may cause IP conflicts and packet loss. However, a duplicate IP address would not prevent the technician from pinging the PC from the human resources router, because they are on the same network.

A misconfigured RIP can cause a router to not learn or advertise routes to other networks, because RIP is a routing protocol that dynamically exchanges routing information between routers. If a router has a wrong RIP configuration, it may not be able to reach or share routes with other routers. However, a misconfigured RIP would not affect the PC's connectivity to the internet, because the PC does not use RIP.

An improper VLAN assignment can cause a PC to not communicate with other devices on the same or different networks, because a VLAN is a logical segmentation of a network that isolates traffic based on criteria such as function, security, or performance. If a PC is assigned to a wrong VLAN, it may not be able to access the resources or services that it needs. However, an improper VLAN assignment would not prevent the technician from pinging the PC from the human resources router, because they are on the same physical network.

## Reference

What is a Default Gateway?

What's an IP Conflict and How Do You Resolve It?

What is RIP (Routing Information Protocol)?

What is a VLAN? How to Set Up a VLAN Network

CompTIA Network+ Certification All-in-One Exam Guide, Eighth Edition (Exam N10-008)

## Question 6

---

**Question Type:** MultipleChoice

---

Which of the following best describes the purpose of an access control vestibule?

### Options:

---

- A- To mitigate an on-path attack
- B- To mitigate tailgating
- C- To mitigate phishing
- D- To mitigate snooping

**Answer:**

---

B

**Explanation:**

---

An access control vestibule, also known as a mantrap, is a physical security access control system that consists of a small space with two sets of interlocking doors. The first set of doors must close before the second set opens, preventing unauthorized individuals from following authorized individuals into facilities with controlled access. This activity, also known as tailgating, results in unauthorized access to the facility. An access control vestibule can help deter and detect tailgating attempts, as well as provide a containment area while authorization for physical access is verified.

Reference

Access Control Vestibules: Types and Peculiarities

Mantrap (access control)

PE-3 (8): Access Control Vestibules

## Question 7

---

**Question Type:** MultipleChoice

---

A network administrator wants to know which systems on the network are at risk of a known vulnerability. Which of the following should the administrator reference?

**Options:**

---

- A- SLA
- B- Patch management policy
- C- NDA
- D- Site survey report
- E- CVE

**Answer:**

---

E

**Explanation:**

---

A Common Vulnerabilities and Exposures (CVE) is a publicly available database of known security vulnerabilities and exposures that affect various software and hardware products. A CVE entry provides a standardized identifier, a brief description, and references to related sources of information for each vulnerability or exposure. A network administrator can reference the CVE database to check if any of the systems on the network are affected by a known vulnerability, and if so, what are the potential impacts and mitigations.

A Service Level Agreement (SLA) is a contract between a service provider and a customer that defines the expected level and quality of service, such as availability, performance, and security. An SLA does not provide information on specific vulnerabilities or exposures affecting the systems or services.

A Patch Management Policy is a set of rules and procedures that govern how patches are applied to systems and software to fix bugs, improve functionality, or address security issues. A patch management policy can help prevent or reduce the risk of vulnerabilities or exposures, but it does not provide information on specific vulnerabilities or exposures affecting the systems or software.

A Non-Disclosure Agreement (NDA) is a legal contract between two or more parties that prohibits the disclosure of confidential or proprietary information to unauthorized parties. An NDA does not provide information on specific vulnerabilities or exposures affecting the systems or information.

A Site Survey Report is a document that summarizes the results of a physical inspection and assessment of a network site, such as the layout, infrastructure, equipment, and environmental conditions. A site survey report can help identify and resolve potential network issues, such as interference, signal strength, or coverage, but it does not provide information on specific vulnerabilities or exposures affecting the network devices or software.

Reference

What is CVE?

What is a Service Level Agreement (SLA)?

Guide to Enterprise Patch Management Planning

NDA, MSA, SOW and SLA. Confidentiality agreements when you outsource QA

Site Survey Report

## Question 8

---

**Question Type:** MultipleChoice

---

A network engineer installed a new fiber uplink for an office and wants to make sure that the link meets throughput requirements. Which of the following tools should the engineer use to

verify that the new link is sufficient?

**Options:**

---

**A-** tcpdump

**B-** ping

**C-** iperf

**D-** netstat

**Answer:**

---

C

## Explanation:

---

iperf is a tool that can measure the bandwidth and quality of a network link by generating and transferring TCP or UDP data streams. iperf can report the maximum achievable throughput, packet loss, jitter, and other statistics for a given link. iperf can be used to test both the uplink and downlink performance of a network link by running it on two endpoints and specifying the direction and duration of the test. iperf can help the engineer verify that the new fiber uplink meets the throughput requirements for the office network.

tcpdump is a tool that can capture and analyze network traffic by filtering and displaying packets based on various criteria. tcpdump can help the engineer troubleshoot network problems, monitor network activity, and inspect packet contents, but it cannot measure the throughput or quality of a network link.

ping is a tool that can test the reachability and latency of a network host by sending and receiving ICMP echo packets. ping can help the engineer check if the new fiber uplink is connected and responsive, and how long it takes for packets to travel between the endpoints, but it cannot measure the throughput or quality of a network link.

netstat is a tool that can display information about the network connections, routing tables, interfaces, and protocols on a network host. netstat can help the engineer view the status and details of the network connections using the new fiber uplink, but it cannot measure the throughput or quality of a network link.

## Reference

[iperf - The ultimate speed test tool for TCP, UDP and SCTP](#)

[How to use iperf to test local network LAN speed in Windows 10](#)

[How to Test Network Performance Between Two Linux Servers](#)



What is tcpdump?

8 Common Network Utilities Explained

Monitoring Your Network: ping, netstat, tcpdump, and Ethereal

Netstat vs. Nmap vs. Netcat: Understanding the Differences

## Question 9

---

**Question Type:** MultipleChoice

---

Which of the following would be used to indicate when unauthorized access to physical internal hardware has occurred?

### Options:

---

- A- Motion detectors
- B- Radio frequency identification tags
- C- Tamper evident seal
- D- Locking racks

**Answer:**

---

C

**Explanation:**

---

A tamper evident seal is a device or material that provides a visible indication of unauthorized access to physical internal hardware. Tamper evident seals can be stickers, labels, tapes, locks, or seals that are designed to break, tear, or change color when someone tries to open, remove, or tamper with them. Tamper evident seals can help deter and detect physical security breaches, such as theft, vandalism, or sabotage of hardware devices<sup>12</sup>. Tamper evident seals can also provide evidence for forensic analysis and legal action<sup>3</sup>.

## Reference

1 - What Is Hardware Security? Definition, Threats, and Best Practices

2 - Device Physical Security Guideline | Information Security Office

3 - What is unauthorized physical access? -- Heimduo

## Question 10

---

**Question Type:** MultipleChoice

---

A network engineer is upgrading an existing edge gateway. The company currently uses a router and needs to be able to filter on all OSI layers. Which of the following should the engineer use to upgrade the gateway?

**Options:**

---

A- NGFW

B- Proxy

C- Layer 3 switch

D- Load balancer

**Answer:**

---

A

**Explanation:**

---

A Next-Generation Firewall (NGFW) is a type of firewall that can filter traffic on all OSI layers, as well as provide advanced security features such as application awareness, intrusion prevention, and threat intelligence. A NGFW can replace a traditional router at the edge of a network and provide better protection against network attacks.

A proxy is a server that acts as an intermediary between clients and servers, forwarding requests and responses. A proxy can filter traffic on the application layer (layer 7), but not on the lower layers of the OSI model.

A layer 3 switch is a device that can perform both switching and routing functions. A layer 3 switch can filter traffic on the network layer (layer 3), but not on the higher or lower layers of the OSI model.

A load balancer is a device that distributes incoming traffic among a group of servers, improving performance and reliability. A load balancer can filter traffic on the transport layer (layer 4), but not on the higher or lower layers of the OSI model.

Reference

What is a Next-Generation Firewall?

What is a Reverse Proxy vs. Load Balancer?

Load Balancers Vs Api Gateway Vs Reverse Proxy

Reverse Proxy and Load Balancer: Understanding the Difference

CompTIA Network+ Certification All-in-One Exam Guide, Eighth Edition (Exam N10-008)

## Question 11

---

**Question Type:** MultipleChoice

---

A network technician is troubleshooting an issue that involves connecting to a server via SSH. The server has one network interface that does not support subinterfaces. The technician

runs a command on the server and receives the following output:

```
Proto Local address Foreign address State
TCP 0.0.0.0:22 0.0.0.0:0 LISTENING
TCP 0.0.0.0:23 0.0.0.0:0 LISTENING
TCP 0.0.0.0:443 0.0.0.0:0 LISTENING
TCP 10.10.10.15:22 10.10.10.42:21231 ESTABLISHED
```

On the host, the technician runs another command and receives the following:

```
Destination Gateway Genmask Flags Iface
default 31.242.12.9 0.0.0.0 UG eth0
192.168.1.0 0.0.0.0 255.255.255.0 UG eth1
```

Which of the following best explains the issue?

### Options:

---

**A-** A firewall is blocking access to the server.

- B-** The server is plugged into a trunk port.
- C-** The host does not have a route to the server.
- D-** The server is not running the SSH daemon.

**Answer:**

---

C

**To Get Premium Files for N10-008 Visit**

**<https://www.p2pexams.com/products/n10-008>**

**For More Free Questions Visit**

**<https://www.p2pexams.com/comptia/pdf/n10-008>**

