

# CompTIA

## Exam Questions N10-008

CompTIA Network+Exam



#### NEW QUESTION 1

- (Topic 1)

A network technician needs to ensure outside users are unable to telnet into any of the servers at the datacenter. Which of the following ports should be blocked when checking firewall configuration?

- A. 22
- B. 23
- C. 80
- D. 3389
- E. 8080

**Answer:** B

#### Explanation:

Port 23 should be blocked when checking firewall configuration to prevent outside users from telnetting into any of the servers at the datacenter. Port 23 is the default port for Telnet, which is an insecure protocol that allows remote access to servers and network devices. Telnet sends data in clear text, which can be easily intercepted and compromised by attackers. A more secure alternative is SSH, which uses port 22 and encrypts data. References: <https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html>

#### NEW QUESTION 2

- (Topic 1)

A network engineer is investigating reports of poor network performance. Upon reviewing a report, the engineer finds that jitter at the office is greater than 10ms on the only WAN connection available. Which of the following would be MOST affected by this statistic?

- A. A VoIP sales call with a customer
- B. An in-office video call with a coworker
- C. Routing table from the ISP
- D. Firewall CPU processing time

**Answer:** A

#### Explanation:

A VoIP sales call with a customer would be most affected by jitter greater than 10ms on the WAN connection. Jitter is the variation in delay of packets arriving at the destination. It can cause choppy or distorted audio quality for VoIP applications, especially over WAN links that have limited bandwidth and high latency. The recommended jitter for VoIP is less than 10ms. References: <https://www.voip-info.org/voip-jitter/>

#### NEW QUESTION 3

- (Topic 1)

A network administrator is implementing OSPF on all of a company's network devices. Which of the following will MOST likely replace all the company's hubs?

- A. A Layer 3 switch
- B. A proxy server
- C. A NGFW
- D. A WLAN controller

**Answer:** A

#### Explanation:

A Layer 3 switch will likely replace all the company's hubs when implementing OSPF on all of its network devices. A Layer 3 switch combines the functionality of a traditional Layer 2 switch with the routing capabilities of a router. By implementing OSPF on a Layer 3 switch, an organization can improve network performance and reduce the risk of network congestion. References: Network+ Certification Study Guide, Chapter 5: Network Security

#### NEW QUESTION 4

- (Topic 1)

Which of the following DNS records works as an alias to another record?

- A. AAAA
- B. CNAME
- C. MX
- D. SOA

**Answer:** B

#### Explanation:

The DNS record that works as an alias to another record is called CNAME (Canonical Name). CNAME records are used to create an alias for a domain name that points to another domain name.

References:

? CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 2: The OSI Model and Networking Protocols, Objective 2.3: Given a scenario, implement and configure the appropriate addressing schema.

#### NEW QUESTION 5

- (Topic 1)

A store owner would like to have secure wireless access available for both business equipment and patron use. Which of the following features should be configured to allow different wireless access through the same equipment?

- A. MIMO
- B. TKIP

- C. LTE
- D. SSID

**Answer:** D

**Explanation:**

SSID (Service Set Identifier) is a feature that should be configured to allow different wireless access through the same equipment. SSID is the name of a wireless network that identifies it from other networks in the same area. A wireless access point (AP) can support multiple SSIDs with different security settings and network policies. For example, a store owner can create one SSID for business equipment and another SSID for patron use, and assign different passwords, VLANs, and QoS levels for each SSID. References: <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/70931-multiple-ssid.html>

**NEW QUESTION 6**

- (Topic 1)

A network engineer is investigating reports of poor network performance. Upon reviewing a device configuration, the engineer finds that duplex settings are mismatched on both ends. Which of the following would be the MOST likely result of this finding?

- A. Increased CRC errors
- B. Increased giants and runts
- C. Increased switching loops
- D. Increased device temperature

**Answer:** A

**Explanation:**

Mismatched duplex settings can cause an increase in CRC errors, which are errors in data transmission that can result in corrupted data. References: CompTIA Network+ Certification Study Guide, Chapter 4: Infrastructure.

**NEW QUESTION 7**

- (Topic 1)

A technician is assisting a user who cannot connect to a network resource. The technician first checks for a link light. According to troubleshooting methodology, this is an example of:

- A. using a bottom-to-top approach.
- B. establishing a plan of action.
- C. documenting a finding.
- D. questioning the obvious.

**Answer:** A

**Explanation:**

Using a bottom-to-top approach means starting from the physical layer and moving up the OSI model to troubleshoot a network problem. Checking for a link light is a physical layer check that verifies the connectivity of the network cable and device. References: <https://www.professormesser.com/network-plus/n10-007/troubleshooting-methodologies-2/>

**NEW QUESTION 8**

- (Topic 1)

A systems administrator needs to improve WiFi performance in a densely populated office tower and use the latest standard. There is a mix of devices that use 2.4 GHz and 5 GHz. Which of the following should the systems administrator select to meet this requirement?

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

**Answer:** B

**Explanation:**

802.11ax is the latest WiFi standard that improves WiFi performance in densely populated environments and supports both 2.4 GHz and 5 GHz bands. 802.11ac is the previous standard that only supports 5 GHz band. 802.11g and 802.11n are older standards that support 2.4 GHz band only or both bands respectively. References: [https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)), <https://www.techtarget.com/searchnetworking/tip/Whats-the-difference-between-80211ax-vs-80211ac>

**NEW QUESTION 9**

- (Topic 1)

Which of the following types of devices can provide content filtering and threat protection, and manage multiple IPSec site-to-site connections?

- A. Layer 3 switch
- B. VPN headend
- C. Next-generation firewall
- D. Proxy server
- E. Intrusion prevention

**Answer:** C

**Explanation:**

Next-generation firewalls can provide content filtering and threat protection, and can manage multiple IPSec site-to-site connections. References: CompTIA Network+ Certification Study Guide, Chapter 5: Network Security.

**NEW QUESTION 10**

- (Topic 1)

Which of the following systems would MOST likely be found in a screened subnet?

- A. RADIUS
- B. FTP
- C. SQL
- D. LDAP

**Answer: B**

**Explanation:**

FTP (File Transfer Protocol) is a system that would most likely be found in a screened subnet. A screened subnet, or triple-homed firewall, is a network architecture where a single firewall is used with three network interfaces. It provides additional protection from outside cyber attacks by adding a perimeter network to isolate or separate the internal network from the public-facing internet. A screened subnet typically hosts systems that need to be accessed by both internal and external users, such as web servers, email servers, or FTP servers. References: <https://www.techtarget.com/searchsecurity/definition/screened-subnet#:~:text=A%20screened%20subnet%2C%20or%20triple-homed%20firewall%2C%20refers%20to,a%20perimeter%20network%20to%20isolate%20or%20separate%20the> 1

**NEW QUESTION 10**

- (Topic 1)

Which of the following factors should be considered when evaluating a firewall to protect a datacenter's east-west traffic?

- A. Replication traffic between an on-premises server and a remote backup facility
- B. Traffic between VMs running on different hosts
- C. Concurrent connections generated by Internet DDoS attacks
- D. VPN traffic from remote offices to the datacenter's VMs

**Answer: B**

**Explanation:**

When evaluating a firewall to protect a datacenter's east-west traffic, it is important to consider traffic between VMs running on different hosts. This type of traffic is referred to as east-west traffic and is often protected by internal firewalls. By implementing firewalls, an organization can protect their internal network against threats such as lateral movement, which can be caused by attackers who have breached a perimeter firewall. References: Network+ Certification Study Guide, Chapter 5: Network Security

**NEW QUESTION 11**

- (Topic 1)

A workstation is configured with the following network details:

IP address	Subnet mask	Default gateway
10.1.2.23	10.1.2.0/27	10.1.2.1

Software on the workstation needs to send a query to the local subnet broadcast address. To which of the following addresses should the software be configured to send the query?

- A. 10.1.2.0
- B. 10.1.2.1
- C. 10.1.2.23
- D. 10.1.2.255
- E. 10.1.2.31

**Answer: D**

**Explanation:**

The software on the workstation should be configured to send the query to 10.1.2.255, which is the local subnet broadcast address. A broadcast address is a special address that allows a device to send a message to all devices on the same subnet. It is usually derived by setting all the host bits to 1 in the network address. In this case, the network address is 10.1.2.0/27, which has 27 network bits and 5 host bits. By setting all the host bits to 1, we get 10.1.2.31 as the broadcast address in decimal notation, or 10.1.2.255 in dotted decimal notation. References: <https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html>

**NEW QUESTION 15**

- (Topic 1)

An IT organization needs to optimize speeds for global content distribution and wants to reduce latency in high-density user locations. Which of the following technologies BEST meets the organization's requirements?

- A. Load balancing
- B. Geofencing
- C. Public cloud
- D. Content delivery network
- E. Infrastructure as a service

**Answer: D**

**Explanation:**

A content delivery network (CDN) is a distributed network of servers that delivers web content to users based on their geographic location. By replicating content across multiple servers in various locations, a CDN can optimize speed and reduce latency in high-density user locations.

### NEW QUESTION 20

- (Topic 1)

A network engineer configured new firewalls with the correct configuration to be deployed to each remote branch. Unneeded services were disabled, and all firewall rules were applied successfully. Which of the following should the network engineer perform NEXT to ensure all the firewalls are hardened successfully?

- A. Ensure an implicit permit rule is enabled
- B. Configure the log settings on the firewalls to the central syslog server
- C. Update the firewalls with current firmware and software
- D. Use the same complex passwords on all firewalls

**Answer: C**

#### Explanation:

Updating the firewalls with current firmware and software is an important step to ensure all the firewalls are hardened successfully, as it can fix any known vulnerabilities or bugs and provide new features or enhancements. Enabling an implicit permit rule is not a good practice for firewall hardening, as it can allow unwanted traffic to pass through the firewall. Configuring the log settings on the firewalls to the central syslog server is a good practice for monitoring and auditing purposes, but it does not harden the firewalls themselves. Using the same complex passwords on all firewalls is not a good practice for password security, as it can increase the risk of compromise if one firewall is breached. References: CompTIA Network+ Certification Exam Objectives Version 2.0 (Exam Number: N10-006), Domain 3.0 Network Security, Objective 3.3 Given a scenario, implement network hardening techniques.

### NEW QUESTION 23

- (Topic 1)

Which of the following ports is commonly used by VoIP phones?

- A. 20
- B. 143
- C. 445
- D. 5060

**Answer: D**

#### Explanation:

TCP/UDP port 5060 is commonly used by VoIP phones. It is the default port for SIP (Session Initiation Protocol), which is a signaling protocol that establishes, modifies, and terminates multimedia sessions over IP networks. SIP is widely used for VoIP applications such as voice and video calls. References: <https://www.voip-info.org/session-initiation-protocol/>

### NEW QUESTION 25

- (Topic 1)

A network device is configured to send critical events to a syslog server; however, the following alerts are not being received:  
Severity 5 LINK-UPDOWN: Interface 1/1, changed state to down  
Severity 5 LINK-UPDOWN: Interface 1/3, changed state to down  
Which of the following describes the reason why the events are not being received?

- A. The network device is not configured to log that level to the syslog server
- B. The network device was down and could not send the event
- C. The syslog server is not compatible with the network device
- D. The syslog server did not have the correct MIB loaded to receive the message

**Answer: A**

#### Explanation:

The reason why the alerts are not being received is that the network device is not configured to log that level to the syslog server. The severity level for the events may need to be adjusted in order for them to be sent to the syslog server. References: Network+ Certification Study Guide, Chapter 8: Network Troubleshooting

### NEW QUESTION 27

- (Topic 1)

An engineer is configuring redundant network links between switches. Which of the following should the engineer enable to prevent network stability issues?

- A. 802.1Q
- B. STP
- C. Flow control
- D. CSMA/CD

**Answer: B**

#### Explanation:

Spanning Tree Protocol (STP) should be enabled when configuring redundant network links between switches. STP ensures that only one active path is used at a time, preventing network loops and stability issues.

References:

? CompTIA Network+ Certification Study Guide

### NEW QUESTION 30

- (Topic 1)

Which of the following would be BEST to use to detect a MAC spoofing attack?

- A. Internet Control Message Protocol
- B. Reverse Address Resolution Protocol
- C. Dynamic Host Configuration Protocol
- D. Internet Message Access Protocol

**Answer:** B

**Explanation:**

Reverse Address Resolution Protocol (RARP) is a protocol that allows a device to obtain its MAC address from its IP address. A MAC spoofing attack is an attack where a device pretends to have a different MAC address than its actual one. RARP can be used to detect a MAC spoofing attack by comparing the MAC address obtained from RARP with the MAC address obtained from other sources, such as ARP or DHCP. References: [https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)), <https://www.techopedia.com/definition/25597/reverse-address-resolution-protocol-rarp>

**NEW QUESTION 35**

- (Topic 1)

Which of the following can be used to centrally manage credentials for various types of administrative privileges on configured network devices?

- A. SSO
- B. TACACS+
- C. Zero Trust
- D. Separation of duties
- E. Multifactor authentication

**Answer:** B

**Explanation:**

TACACS+ (Terminal Access Controller Access Control System Plus) can be used to centrally manage credentials for various types of administrative privileges on configured network devices. This protocol separates authentication, authorization, and accounting (AAA) functions, providing more granular control over access to network resources.

References:

? Network+ N10-007 Certification Exam Objectives, Objective 4.2: Given a scenario, implement secure network administration principles.

**NEW QUESTION 37**

- (Topic 1)

An engineer notices some late collisions on a half-duplex link. The engineer verifies that the devices on both ends of the connection are configured for half duplex. Which of the following is the MOST likely cause of this issue?

- A. The link is improperly terminated
- B. One of the devices is misconfigured
- C. The cable length is excessive
- D. One of the devices has a hardware issue

**Answer:** C

**Explanation:**

In a half-duplex link, devices can only send or receive data at one time, not simultaneously. Late collisions occur when devices transmit data at the same time after waiting for a clear channel. One of the causes of late collisions is excessive cable length, which increases the propagation delay and makes it harder for devices to detect collisions. The link termination, device configuration, and device hardware are not likely to cause late collisions on a half-duplex link.

**NEW QUESTION 38**

- (Topic 1)

A company hired a technician to find all the devices connected within a network. Which of the following software tools would BEST assist the technician in completing this task?

- A. IP scanner
- B. Terminal emulator
- C. NetFlow analyzer
- D. Port scanner

**Answer:** A

**Explanation:**

To find all devices connected within a network, a technician can use an IP scanner. An IP scanner sends a ping request to all IP addresses within a specified range and then identifies the active devices that respond to the request.

**NEW QUESTION 42**

- (Topic 1)

The network administrator is informed that a user's email password is frequently hacked by brute-force programs. Which of the following policies should the network administrator implement to BEST mitigate this issue? (Choose two.)

- A. Captive portal
- B. Two-factor authentication
- C. Complex passwords
- D. Geofencing
- E. Role-based access
- F. Explicit deny

**Answer:** BC

**Explanation:**

Two-factor authentication (2FA) is a method of verifying a user's identity by requiring two pieces of evidence, such as something the user knows (e.g., a password) and something the user has (e.g., a token or a smartphone). 2FA adds an extra layer of security that makes it harder for hackers to access a user's account by brute-force programs. Complex passwords are passwords that are long, random, and use a combination of uppercase and lowercase letters, numbers,

and symbols. Complex passwords are more resistant to brute-force attacks than simple or common passwords. References: [https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)), <https://www.csoonline.com/article/3225913/what-is-two-factor-authentication-2fa-how-to-enable-it-and-why-you-should.html>, <https://www.howtogeek.com/195430/how-to-create-a-strong-password-and-remember-it/>

#### NEW QUESTION 44

- (Topic 1)

A technician is troubleshooting a wireless connectivity issue in a small office located in a high-rise building. Several APs are mounted in this office. The users report that the network connections frequently disconnect and reconnect throughout the day. Which of the following is the MOST likely cause of this issue?

- A. The AP association time is set too low
- B. EIRP needs to be boosted
- C. Channel overlap is occurring
- D. The RSSI is misreported

**Answer: C**

#### Explanation:

Channel overlap is a common cause of wireless connectivity issues, especially in high-density environments where multiple APs are operating on the same or adjacent frequencies. Channel overlap can cause interference, signal degradation, and performance loss for wireless devices. The AP association time, EIRP, and RSSI are not likely to cause frequent disconnects and reconnects for wireless users.

#### NEW QUESTION 49

- (Topic 1)

Which of the following is used to prioritize Internet usage per application and per user on the network?

- A. Bandwidth management
- B. Load balance routing
- C. Border Gateway Protocol
- D. Administrative distance

**Answer: A**

#### Explanation:

Bandwidth management is used to prioritize Internet usage per application and per user on the network. This allows an organization to allocate network resources to mission-critical applications and users, while limiting the bandwidth available to non-business-critical applications. References: Network+ Certification Study Guide, Chapter 2: Network Operations

#### NEW QUESTION 51

- (Topic 1)

According to troubleshooting methodology, which of the following should the technician do NEXT after determining the most likely probable cause of an issue?

- A. Establish a plan of action to resolve the issue and identify potential effects
- B. Verify full system functionality and, if applicable, implement preventive measures
- C. Implement the solution or escalate as necessary
- D. Test the theory to determine the cause

**Answer: A**

#### Explanation:

According to troubleshooting methodology, after determining the most likely probable cause of an issue, the next step is to establish a plan of action to resolve the issue and identify potential effects. This step involves defining the steps needed to implement a solution, considering the possible consequences of each step, and obtaining approval from relevant stakeholders if necessary. References: [https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)), <https://www.comptia.org/blog/the-comptia-guide-to-it-troubleshooting>

#### NEW QUESTION 56

SIMULATION - (Topic 1)

SIMULATION

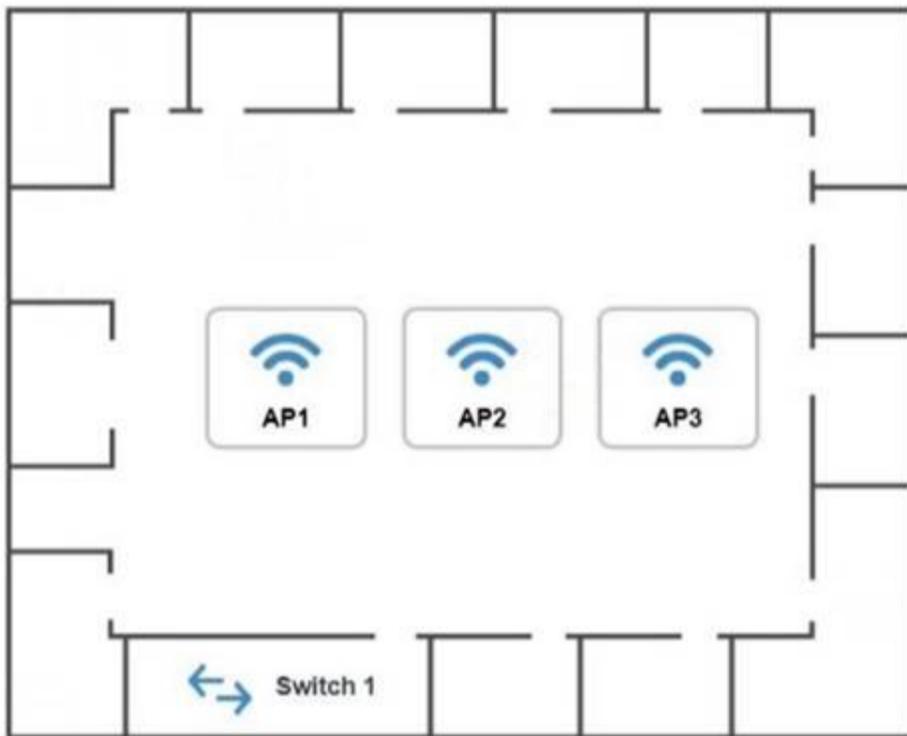
You have been tasked with setting up a wireless network in an office. The network will consist of 3 Access Points and a single switch. The network must meet the following parameters:

The SSIDs need to be configured as CorpNet with a key of S3cr3t! The wireless signals should not interfere with each other

The subnet the Access Points and switch are on should only support 30 devices maximum The Access Points should be configured to only support TKIP clients at a maximum speed INSTRUCTIONS

Click on the wireless devices and review their information and adjust the settings of the access points to meet the given requirements.

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



192.168.1.2  
Speed: Auto  
Duplex: Auto

### AP1 Configuration

https://ap1.setup.do

#### Basic Configuration

Access Point Name: AP1

IP Address: /

Gateway: 192.168.1.1

SSID:

SSID Broadcast:  Yes  No

#### Wireless

Mode:

Channel:

#### Wired

Speed:  Auto  100  1000

Duplex:  Auto  Half  Full

#### Security Configuration

Security Settings:  None  WEP  WPA  WPA2  WPA2 - Enterprise

Key or Passphrase:

### AP2 Configuration

https://ap2.setup.do

#### Basic Configuration

Access Point Name: AP2

IP Address: /

Gateway: 192.168.1.1

SSID:

SSID Broadcast:  Yes  No

#### Wireless

Mode:   
 B  
 G

Channel:   
 1  
 2  
 3  
 4  
 5  
 6  
 7  
 8  
 9  
 10  
 11

#### Wired

Speed:  Auto  100  1000

Duplex:  Auto  Half  Full

#### Security Configuration

Security Settings:  None  WEP  WPA  WPA2  WPA2 - Enterprise

Key or Passphrase:

Reset to Default Save Close

### AP3 Configuration

https://ap3.setup.do

#### Basic Configuration

Access Point Name: AP3

IP Address: /

Gateway: 192.168.1.1

SSID:

SSID Broadcast:  Yes  No

#### Wireless

Mode:   
 B  
 G

Channel:   
 1  
 2  
 3  
 4  
 5  
 6  
 7  
 8  
 9  
 10  
 11

#### Wired

Speed:  Auto  100  1000

Duplex:  Auto  Half  Full

#### Security Configuration

Security Settings:  None  WEP  WPA  WPA2  WPA2 - Enterprise

Key or Passphrase:

Reset to Default Save Close

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

On the first exhibit, the layout should be as follows

The screenshot shows the 'AP1 Configuration' web interface. At the top, there is a blue header with the title 'AP1 Configuration' and a close button. Below the header is a navigation bar with back, forward, and refresh icons, and a URL field containing 'https://ap1.setup.do'. The main content area is divided into three sections: 'Basic Configuration', 'Wireless', and 'Security Configuration'. In the 'Basic Configuration' section, the 'Access Point Name' is 'AP1', 'IP Address' is '192.168.1.32', 'Gateway' is '192.168.1.1', 'SSID' is 'CorpNet', and 'SSID Broadcast' is set to 'Yes'. The 'Wireless' section shows 'Mode' as 'B' and 'Channel' as '3'. The 'Wired' section shows 'Speed' as '100' and 'Duplex' as 'Full'. The 'Security Configuration' section shows 'Security Settings' as 'WPA2 - Enterprise' and 'Key or Passphrase' as 'S3cr3t!'. The interface uses a clean, modern design with a blue and white color scheme and yellow highlights for selected or active elements.

Graphical user interface, text, application, chat or text message Description automatically generated

This screenshot is similar to the first one, but it highlights the 'IP Address' field. The IP address '192.168.1.32' is displayed, and a dropdown menu is open to its right, showing the number '27'. The rest of the configuration is identical to the first screenshot.

Graphical user interface Description automatically generated

This is a close-up view of the 'Security Configuration' section. It shows the 'Security Settings' with radio buttons for 'None', 'WEP', 'WPA', 'WPA2', and 'WPA2 - Enterprise'. The 'WPA2 - Enterprise' option is selected. Below it is a text input field for the 'Key or Passphrase' containing the text 'S3cr3t!'.

Graphical user interface, text, application, chat or text message Description automatically generated

**AP1 Configuration**
✕

← → ↻

IP Address  /

Gateway

SSID

SSID Broadcast  Yes  No

**Wireless**

Mode

Channel

**Wired**

Speed  Auto  100  1000

Duplex  Auto  Half  Full

**Security Configuration**

Security Settings  None  WEP  WPA  WPA2  WPA2 - Enterprise

Key or Passphrase

Reset to Default
Save
Close

Graphical user interface  
 Description automatically generated  
 Exhibit 2 as follows  
 Access Point Name AP2

**AP2 Configuration**
✕

← → ↻

**Basic Configuration**

Access Point Name

IP Address  /

Gateway

SSID

SSID Broadcast  Yes  No

**Wireless**

Mode

Channel

**Wired**

Speed  Auto  100  1000

Duplex  Auto  Half  Full

**Security Configuration**

Reset to Default
Save
Close

Graphical user interface  
 Description automatically generated

**Security Configuration**

Security Settings  None  WEP  WPA  WPA2  WPA2 - Enterprise

Key or Passphrase

Graphical user interface, text, application, chat or text message  
Description automatically generated

**AP2 Configuration** ✕

← → ↻

IP Address  /

Gateway

SSID

SSID Broadcast  Yes  No

**Wireless**

Mode

Channel

**Wired**

Speed  Auto  100  1000

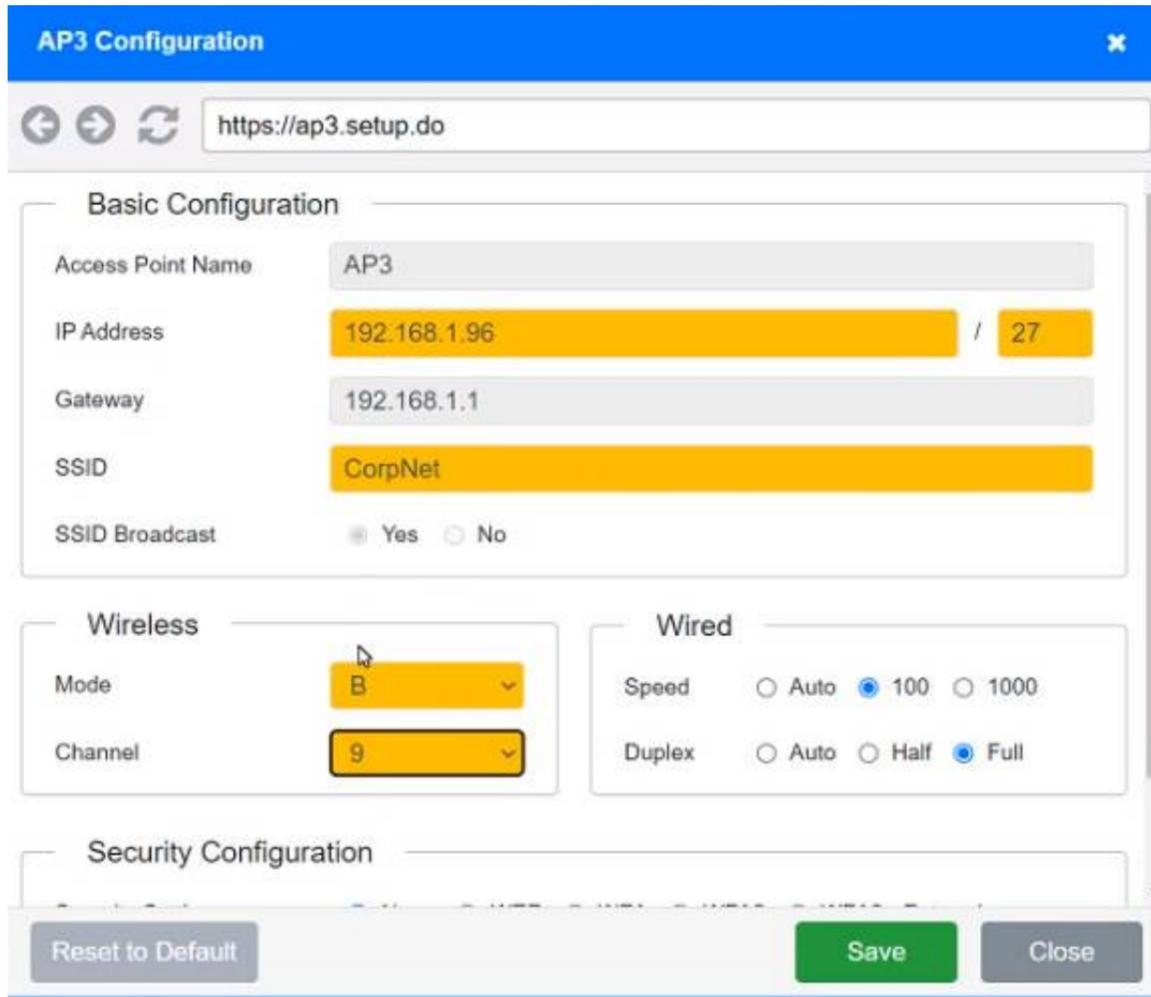
Duplex  Auto  Half  Full

**Security Configuration**

Security Settings  None  WEP  WPA  WPA2  WPA2 - Enterprise

Key or Passphrase

Graphical user interface  
Description automatically generated  
Exhibit 3 as follows  
Access Point Name AP3



**AP3 Configuration**

https://ap3.setup.do

**Basic Configuration**

Access Point Name: AP3

IP Address: 192.168.1.96 / 27

Gateway: 192.168.1.1

SSID: CorpNet

SSID Broadcast:  Yes  No

**Wireless**

Mode: B

Channel: 9

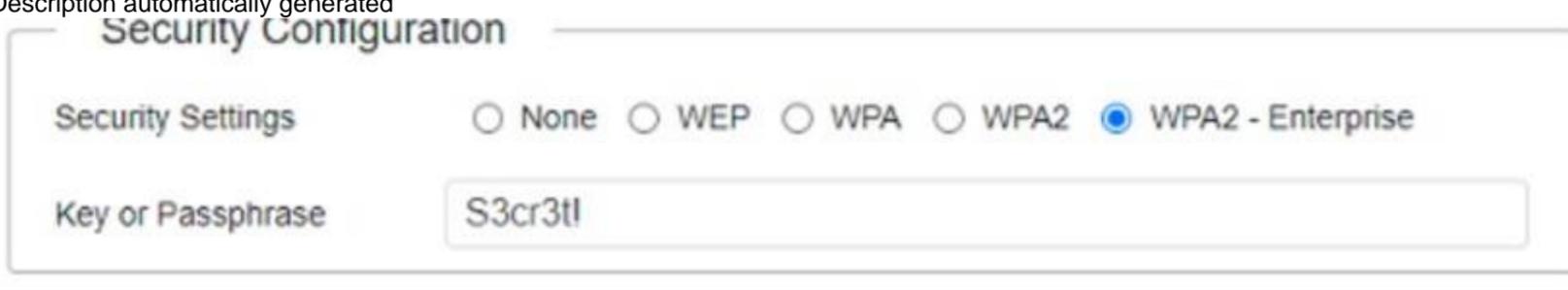
**Wired**

Speed:  Auto  100  1000

Duplex:  Auto  Half  Full

Reset to Default Save Close

Graphical user interface  
 Description automatically generated

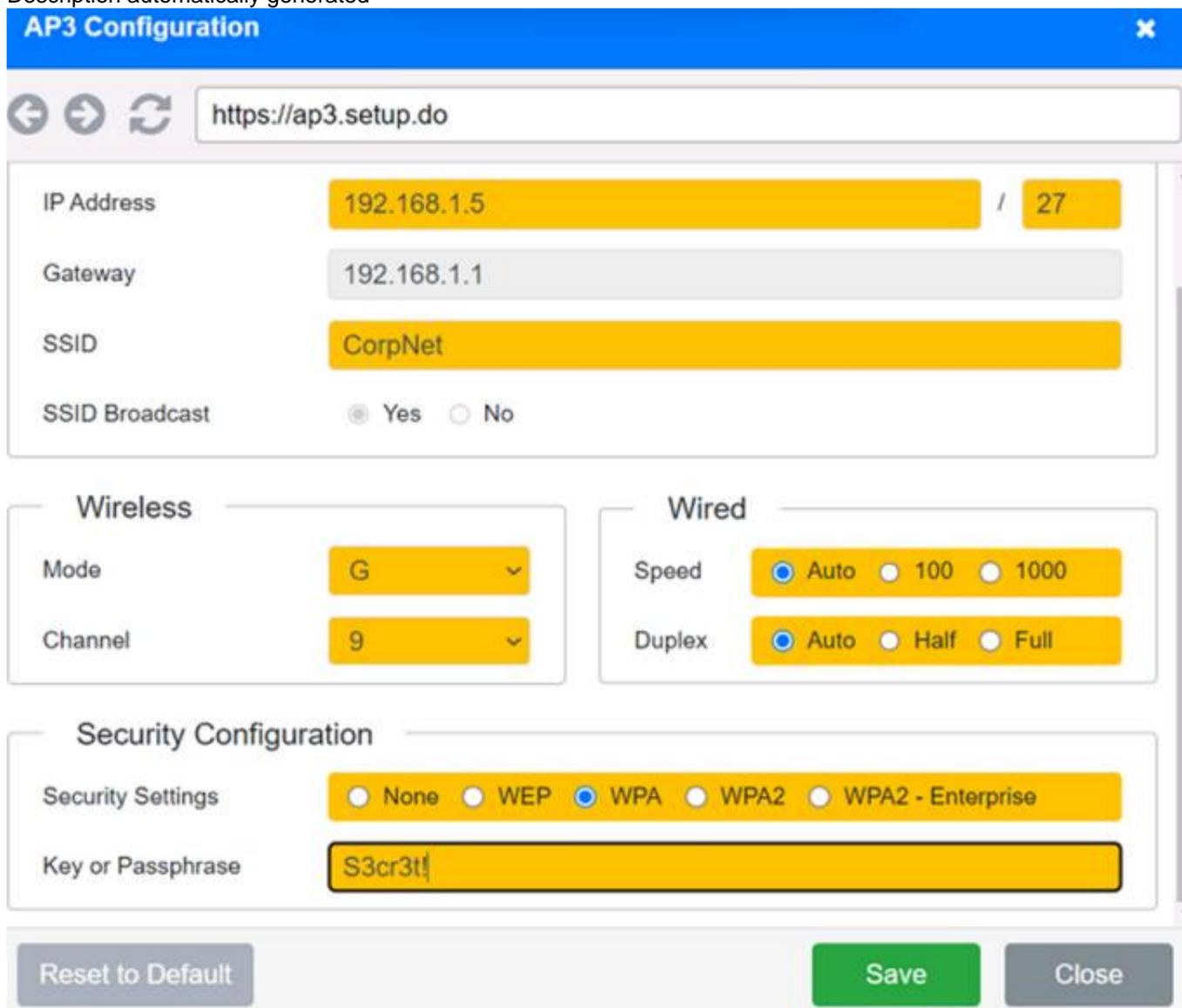


**Security Configuration**

Security Settings:  None  WEP  WPA  WPA2  WPA2 - Enterprise

Key or Passphrase: S3cr3t!

Graphical user interface, text, application, chat or text message  
 Description automatically generated



**AP3 Configuration**

https://ap3.setup.do

IP Address: 192.168.1.5 / 27

Gateway: 192.168.1.1

SSID: CorpNet

SSID Broadcast:  Yes  No

**Wireless**

Mode: G

Channel: 9

**Wired**

Speed:  Auto  100  1000

Duplex:  Auto  Half  Full

**Security Configuration**

Security Settings:  None  WEP  WPA  WPA2  WPA2 - Enterprise

Key or Passphrase: S3cr3t!

Reset to Default Save Close

Graphical user interface  
 Description automatically generated

#### NEW QUESTION 60

- (Topic 1)

A technician is installing multiple UPS units in a major retail store. The technician is required to keep track of all changes to new and old equipment. Which of the following will allow the technician to record these changes?

- A. Asset tags
- B. A smart locker
- C. An access control vestibule
- D. A camera

**Answer:** A

#### Explanation:

Asset tags will allow the technician to record changes to new and old equipment when installing multiple UPS units in a major retail store. Asset tags are labels or stickers that are attached to physical assets such as computers, printers, servers, or UPS units. They usually contain information such as asset name, serial number, barcode, QR code, or RFID chip that can be scanned or read by an asset management system or software. Asset tags help track inventory, location, status, maintenance, and ownership of assets. References: <https://www.camcode.com/asset-tags/asset-tagging-guide/>

#### NEW QUESTION 64

- (Topic 1)

Which of the following connector types would have the MOST flexibility?

- A. SFP
- B. BNC
- C. LC
- D. RJ45

**Answer:** A

#### Explanation:

SFP (Small Form-factor Pluggable) is a connector type that has the most flexibility. It is a hot-swappable transceiver that can support different speeds, distances, and media types depending on the module inserted. It can be used for both copper and fiber connections and supports various protocols such as Ethernet, Fibre Channel, and SONET. References: <https://www.fs.com/what-is-sfp-transceiver-aid-11.html>

#### NEW QUESTION 69

- (Topic 2)

A network technician is reviewing an upcoming project's requirements to implement IaaS. Which of the following should the technician consider?

- A. Software installation processes
- B. Type of database to be installed
- C. Operating system maintenance
- D. Server hardware requirements

**Answer:** D

#### Explanation:

IaaS stands for Infrastructure as a Service, which is a cloud computing model that provides virtualized computing resources such as servers, storage, and networking over the Internet. When implementing IaaS, the network technician should consider the server hardware requirements, such as CPU, RAM, disk space, and network bandwidth, that are needed to run the applications and services on the cloud. The other options are not relevant to IaaS, as they are either handled by the cloud provider or by the end-user. References: <https://www.comptia.org/blog/what-is-iaas>

#### NEW QUESTION 71

- (Topic 2)

A technician is deploying a low-density wireless network and is contending with multiple types of building materials. Which of the following wireless frequencies would allow for the LEAST signal attenuation?

- A. 2.4GHz
- B. 5GHz
- C. 850MHz
- D. 900MHz

**Answer:** A

#### Explanation:

2.4GHz is the wireless frequency that would allow for the least signal attenuation when deploying a low-density wireless network with multiple types of building materials. Signal attenuation is the loss of signal strength or quality as it travels through a medium or over a distance. Signal attenuation can be affected by various factors such as distance, interference, reflection, refraction, diffraction, scattering, or absorption. Generally, lower frequencies have less signal attenuation than higher frequencies because they can penetrate obstacles better and travel farther. Therefore, 2.4GHz would have less signal attenuation than 5GHz, 850MHz, or 900MHz. References: <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-omni-vs-direct.html>

#### NEW QUESTION 72

- (Topic 2)

A network technician has multimode fiber optic cable available in an existing IDF. Which of the following Ethernet standards should the technician use to connect the network switch to the existing fiber?

- A. 10GBaseT
- B. 1000BaseT
- C. 1000BaseSX
- D. 1000BaseLX

**Answer:** C

**Explanation:**

1000BaseSX is an Ethernet standard that should be used to connect the network switch to the existing multimode fiber optic cable. 1000BaseSX is a Gigabit Ethernet standard that uses short-wavelength laser (850 nm) over multimode fiber optic cable. It can support distances up to 550 meters depending on the cable type and quality. It is suitable for short-range network segments such as campus or building backbone networks. References: [https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/gigabit-ethernet-gbic-sfp-modules/product\\_data\\_sheet09186a008014cb5e.html](https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/gigabit-ethernet-gbic-sfp-modules/product_data_sheet09186a008014cb5e.html)

**NEW QUESTION 73**

- (Topic 2)

An IT technician suspects a break in one of the uplinks that provides connectivity to the core switch. Which of the following command-line tools should the technician use to determine where the incident is occurring?

- A. nslookup
- B. show config
- C. netstat
- D. show interface
- E. show counters

**Answer:** D

**Explanation:**

show interface is a command-line tool that displays information about the status, configuration, and statistics of an interface on a network device. A technician can use show interface to determine where the incident is occurring in a network by checking the uplink status, speed, duplex mode, errors, collisions, and other parameters of each interface. References: <https://www.comptia.org/blog/what-is-show-interface>

**NEW QUESTION 77**

- (Topic 2)

A network engineer is designing a new secure wireless network. The engineer has been given the following requirements:

- \* 1 Must not use plaintext passwords
- \* 2 Must be certificate based
- \* 3. Must be vendor neutral

Which of the following methods should the engineer select?

- A. TWP-RC4
- B. CCMP-AES
- C. EAP-TLS
- D. WPA2

**Answer:** C

**Explanation:**

EAP-TLS is the method that should be selected to meet the requirements for designing a new secure wireless network. EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) is an authentication protocol that uses X.509 digital certificates for both clients and servers. It provides strong security and mutual authentication by using TLS encryption and public key cryptography. It does not use plaintext passwords or shared secrets that can be compromised or guessed. It is also an open standard that is vendor neutral and supported by most wireless devices<sup>1</sup>. References: <https://www.securew2.com/blog/what-is-eap-tls>  
1

**NEW QUESTION 81**

- (Topic 2)

A network technician was troubleshooting an issue for a user who was being directed to cloned websites that were stealing credentials. The URLs were correct for the websites but an incorrect IP address was revealed when the technician used ping on the user's PC. After checking the settings, the technician found the DNS server address was incorrect. Which of the following describes the issue?

- A. Rogue DHCP server
- B. Misconfigured HSRP
- C. DNS poisoning
- D. Exhausted IP scope

**Answer:** C

**Explanation:**

DNS poisoning is a type of attack that modifies the DNS records of a domain name to point to a malicious IP address instead of the legitimate one. This can result in users being directed to cloned websites that are stealing credentials, even if they enter the correct URL for the website. The incorrect DNS server address on the user's PC could be a sign of DNS poisoning, as the attacker could have compromised the DNS server or spoofed its response to redirect the user's queries. References: <https://www.comptia.org/blog/what-is-dns-poisoning>

**NEW QUESTION 85**

- (Topic 2)

A user is having difficulty with video conferencing and is looking for assistance. Which of the following would BEST improve performance?

- A. Packet shaping
- B. Quality of service
- C. Port mirroring
- D. Load balancing

**Answer:** B

**Explanation:**

Quality of service (QoS) is a mechanism that prioritizes network traffic based on different criteria, such as application type, source and destination address, port number, etc., and allocates bandwidth and resources accordingly. QoS would best improve performance for video conferencing, as it would ensure that video traffic gets higher priority and lower latency than other types of traffic on the network. Packet shaping is a technique that controls the rate or volume of network traffic by delaying or dropping packets that exceed certain thresholds or violate certain policies, which may not improve performance for video conferencing if it causes packet loss or jitter. Port mirroring is a technique that copies traffic from one port to another port on a switch for monitoring or analysis purposes, which does not improve performance for video conferencing at all. Load balancing is a technique that distributes network traffic across multiple servers or devices for improved availability and scalability, which does not

#### NEW QUESTION 88

- (Topic 2)

A network administrator needs to implement an HDMI over IP solution. Which of the following will the network administrator MOST likely use to ensure smooth video delivery?

- A. Link aggregation control
- B. Port tagging
- C. Jumbo frames
- D. Media access control

**Answer: C**

#### Explanation:

Giants are packets that exceed the configured MTU (Maximum Transmission Unit) of a switchport or interface, which causes them to be dropped or fragmented by the switch or router. The MTU is the maximum size of a packet that can be transmitted without fragmentation on a given medium or protocol. Giants can indicate misconfiguration or mismatch of MTU values between devices or interfaces on a network, which can cause performance issues or errors. CRC errors are errors that occur when the cyclic redundancy check (CRC) value of a packet does not match the calculated CRC value at the destination, which indicates corruption or alteration of data during transmission due to noise, interference, faulty cabling, etc., but not necessarily exceeding MTU values. Runts are packets that are smaller than the minimum size allowed by the medium or protocol, which causes them to be dropped or ignored by the switch or router. Flooding is a technique where a switch sends packets to all ports except the source port when it does not have an entry for the destination MAC address in its MAC address table, which can cause congestion or broadcast storms on a network.

#### NEW QUESTION 90

- (Topic 2)

Which of the following OSI model layers is where conversations between applications are established, coordinated, and terminated?

- A. Session
- B. Physical
- C. Presentation
- D. Data link

**Answer: A**

#### Explanation:

Reference: <https://www.techtarget.com/searchnetworking/definition/OSI#:~:text=The%20session%20layer,and%20terminates%20conversations%20between%20applications.>

The session layer is where conversations between applications are established, coordinated, and terminated. It is responsible for creating, maintaining, and ending sessions between different devices or processes. The physical layer deals with the transmission of bits over a medium. The presentation layer formats and translates data for different applications. The data link layer provides reliable and error-free delivery of frames within a network.

#### NEW QUESTION 93

- (Topic 2)

A small, family-run business uses a single SOHO router to provide Internet and WiFi to its employees. At the start of a new week, employees come in and find their usual WiFi network is no longer available, and there is a new wireless network to which they cannot connect. Given that information, which of the following should have been done to avoid this situation?

- A. The device firmware should have been kept current.
- B. Unsecure protocols should have been disabled.
- C. Parental controls should have been enabled.
- D. The default credentials should have been changed.

**Answer: D**

#### Explanation:

The default credentials are the username and password that come with a device or service when it is first installed or configured. They are often easy to guess or find online, which makes them vulnerable to unauthorized access or attacks. The default credentials should be changed to something unique and strong as soon as possible to avoid this situation. If the default credentials were not changed, someone could have accessed the SOHO router and changed the WiFi settings without the employees' knowledge. References: <https://www.comptia.org/blog/network-security-basics-6-easy-ways-to-protect-your-network>

#### NEW QUESTION 96

- (Topic 2)

A user recently made changes to a PC that caused it to be unable to access websites by both FQDN and IP. Local resources, such as the file server, remain accessible. Which of the following settings did the user MOST likely misconfigure?

- A. Static IP
- B. Default gateway
- C. DNS entries
- D. Local host file

**Answer: B**

**Explanation:**

The default gateway is the setting that the user most likely misconfigured on the PC that caused it to be unable to access websites by both FQDN and IP. The default gateway is a device, usually a router or a firewall, that connects a local network to other networks such as the Internet. It acts as an intermediary between devices on different networks and forwards packets based on their destination IP addresses. If the default gateway is not configured correctly on a PC, it will not be able to communicate with devices outside its local network, such as web servers or DNS servers. References: <https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/16448-default-gateway.html>

**NEW QUESTION 100**

- (Topic 2)

A network administrator wants to analyze attacks directed toward the company's network. Which of the following must the network administrator implement to assist in this goal?

- A. A honeypot
- B. Network segmentation
- C. Antivirus
- D. A screened subnet

**Answer: A**

**Explanation:**

A honeypot is a decoy system that is intentionally left vulnerable or exposed to attract attackers and divert them from the real targets. A honeypot can also be used to collect information about the attackers' techniques and motives. A network administrator can implement a honeypot to analyze attacks directed toward the company's network, as a honeypot can help identify the source, target, method, and impact of an attack, as well as provide recommendations for remediation. References: <https://www.comptia.org/blog/what-is-a-honeypot>

**NEW QUESTION 104**

- (Topic 2)

A technician is troubleshooting a previously encountered issue. Which of the following should the technician reference to find what solution was implemented to resolve the issue?

- A. Standard operating procedures
- B. Configuration baseline documents
- C. Work instructions
- D. Change management documentation

**Answer: D**

**Explanation:**

Change management documentation is a record of the changes that have been made to a system or process, including the reason, date, time, and impact of each change. A technician can reference this documentation to find what solution was implemented to resolve a previously encountered issue, as well as any potential side effects or dependencies of the change. References: <https://www.comptia.org/blog/what-is-change-management>

**NEW QUESTION 108**

- (Topic 2)

A technician wants to install a WAP in the center of a room that provides service in a radius surrounding a radio. Which of the following antenna types should the AP utilize?

- A. Omni
- B. Directional
- C. Yagi
- D. Parabolic

**Answer: A**

**Explanation:**

An omni antenna should be used by the AP to provide service in a radius surrounding a radio. An omni antenna is a type of antenna that has a 360-degree horizontal radiation pattern. It can provide wireless coverage in all directions from the antenna with varying degrees of vertical coverage. It is suitable for indoor environments where users are located around the AP. References: <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-omni-vs-direct.html>

**NEW QUESTION 109**

- (Topic 2)

Which of the following technologies allows traffic to be sent through two different ISPs to increase performance?

- A. Fault tolerance
- B. Quality of service
- C. Load balancing
- D. Port aggregation

**Answer: C**

**Explanation:**

Load balancing is a technology that allows traffic to be sent through two different ISPs to increase performance. Load balancing is a process of distributing network traffic across multiple servers or links to optimize resource utilization, throughput, latency, and reliability. Load balancing can be implemented at different layers of the OSI model, such as layer 4 (transport) or layer 7 (application). Load balancing can also be used for outbound traffic by using multiple ISPs and routing protocols such as BGP (Border Gateway Protocol) to select the best path for each packet. References: [https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/border-gateway-protocol-bgp/prod\\_white\\_paper0900aecd806c4eeb.html](https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/border-gateway-protocol-bgp/prod_white_paper0900aecd806c4eeb.html)

#### NEW QUESTION 112

- (Topic 3)

A security administrator is trying to prevent incorrect IP addresses from being assigned to clients on the network. Which of the following would MOST likely prevent this and allow the network to continue to operate?

- A. Configuring DHCP snooping on the switch
- B. Preventing broadcast messages leaving the client network
- C. Blocking ports 67/68 on the client network
- D. Enabling port security on access ports

**Answer:** A

#### Explanation:

To prevent incorrect IP addresses from being assigned to clients on the network and allow the network to continue to operate, the security administrator should consider configuring DHCP (Dynamic Host Configuration Protocol) snooping on the switch. DHCP snooping is a security feature that is used to prevent unauthorized DHCP servers from operating on a network. It works by allowing the switch to monitor and validate DHCP traffic on the network, ensuring that only legitimate DHCP messages are forwarded to clients. This can help to prevent incorrect IP addresses from being assigned to clients, as it ensures that only authorized DHCP servers are able to provide IP addresses to clients on the network.

#### NEW QUESTION 113

- (Topic 3)

A network administrator is working to configure a new device to provide Layer 2 connectivity to various endpoints including several WAPs. Which of the following devices will the administrator MOST likely configure?

- A. WLAN controller
- B. Cable modem
- C. Load balancer
- D. Switch
- E. Hub

**Answer:** D

#### Explanation:

A switch is a device that provides Layer 2 connectivity to various endpoints by forwarding frames based on MAC addresses. A switch can also connect to several WAPs (wireless access points) to provide wireless connectivity to wireless devices.

#### NEW QUESTION 115

- (Topic 3)

While setting up a new workstation, a technician discovers that the network connection is only 100 full duplex (FD), although it is connected to a gigabit switch. While reviewing the interface information in the switch CLI, the technician notes the port is operating at IOOFD but Shows many RX and TX errors. The technician moves the computer to another switchport and experiences the same issues. Which of the following is MOST likely the cause of the low data rate and port errors?

- A. Bad switch ports
- B. Duplex issues
- C. Cable length
- D. Incorrect pinout

**Answer:** B

#### NEW QUESTION 119

- (Topic 3)

A network administrator installed an additional IDF during a building expansion project. Which of the following documents need to be updated to reflect the change? (Select TWO).

- A. Data loss prevention policy
- B. BYOD policy
- C. Acceptable use policy
- D. Non-disclosure agreement
- E. Disaster recovery plan
- F. Physical network diagram

**Answer:** AF

#### NEW QUESTION 123

- (Topic 3)

An IT intern moved the location of a WAP from one conference room to another. The WAP was unable to boot following the move. Which of the following should be used to fix the issue?

- A. Antenna
- B. WLAN controller
- C. Media converter
- D. PoE injector

**Answer:** D

#### Explanation:

A PoE injector is a device that provides power over Ethernet (PoE) to a WAP or other network device that does not have a built-in power supply. A PoE injector connects to a power outlet and an Ethernet cable, and sends both power and data to the WAP. If the WAP was moved to a location where there is no power outlet

or PoE switch, it would need  
a PoE injector to boot up. References:  
? Part 3 of the current page talks about PoE and PoE injectors as a way to power WAPs.  
? [This article] explains how PoE injectors work and how to use them.

#### NEW QUESTION 127

- (Topic 3)

A network administrator is investigating a performance issue on a dual-link connection—VPN and MPLS—to a partner network. The MPLS is the primary path, and the VPN is used as a backup. While communicating, the delay is measured at 18ms, which is higher than the 6ms expected when the MPLS link is operational but lower than the 30ms expected for the VPN connection. Which of the following will MOST likely point to the root cause of the Issue?

- A. Checking the routing tables on both sides to ensure there is no asymmetric routing
- B. Checking on the partner network for a missing route pointing to the VPN connection
- C. Running iPerf on both sides to confirm the delay that is measured is accurate
- D. Checking for an incorrect VLAN assignment affecting the MPLS traffic

**Answer:** A

#### Explanation:

Asymmetric routing can occur when two routers have different paths for the same two hosts, resulting in increased latency and possible packet loss. According to the CompTIA Network+ Study Manual, "If the path from the source to the destination is not the same in both directions, the packets will take different routes and the latency can increase significantly." To confirm this, the network administrator should check the routing tables on both sides of the connection and ensure that the same path is used in both directions.

#### NEW QUESTION 129

- (Topic 3)

A user calls the IT department to report being unable to log in after locking the computer. The user resets the password, but later in the day the user is again unable to log in after locking the computer. Which of the following attacks against the user IS MOST likely taking place?

- A. Brute-force
- B. On-path
- C. Deauthentication
- D. Phishing

**Answer:** A

#### NEW QUESTION 133

- (Topic 3)

A company is reviewing ways to cut the overall cost of its IT budget. A network technician suggests removing various computer programs from the IT budget and only providing these programs on an as-needed basis. Which of the following models would meet this requirement?

- A. Multitenancy
- B. IaaS
- C. SaaS
- D. VPN

**Answer:** C

#### Explanation:

SaaS stands for Software as a Service and is a cloud computing model where software applications are hosted and delivered over the internet by a service provider. SaaS can help the company cut the overall cost of its IT budget by eliminating the need to purchase, install, update, and maintain various computer programs on its own devices. The company can access the programs on an as-needed basis and pay only for what it uses. Multitenancy is a feature of cloud computing where multiple customers share the same physical or virtual resources. IaaS stands for Infrastructure as a Service and is a cloud computing model where computing resources such as servers, storage, and networking are provided over the internet by a service provider. VPN stands for Virtual Private Network and is a technology that creates a secure and encrypted connection over a public network.

References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 1.9: Compare and contrast common network service types.

#### NEW QUESTION 135

- (Topic 3)

A company has multiple offices around the world. The computer rooms in some office locations are too warm. Dedicated sensors are in each room, but the process of checking each sensor takes a long time. Which of the following options can the company put in place to automate temperature readings with internal resources?

- A. Implement NetFlow.
- B. Hire a programmer to write a script to perform the checks.
- C. Utilize ping to measure the response.
- D. Use SNMP with an existing collector server.

**Answer:** D

#### Explanation:

SNMP (Simple Network Management Protocol) is a protocol that allows network devices to communicate with a management server. By using SNMP, the company can set up an SNMP agent on each sensor, which will report its temperature readings to an existing collector server. This will enable the company to monitor the temperatures of all their sensors in real-time without the need for manual checks. Additionally, SNMP's scalability means that even if the company adds more rooms or sensors, the existing system can be easily expanded to accommodate them.

#### NEW QUESTION 139

- (Topic 3)

A customer is hosting an internal database server. None of the users are able to connect to the server, even though it appears to be working properly. Which of the following is the best way to verify traffic to and from the server?

- A. Protocol analyzer
- B. nmap
- C. ipconfig
- D. Speed test

**Answer:** A

**Explanation:**

A protocol analyzer is the best way to verify traffic to and from the server. A protocol analyzer, also known as a packet sniffer or network analyzer, is a tool that captures and analyzes the network packets that are sent and received by a device. A protocol analyzer can show the source and destination IP addresses, ports, protocols, and payload of each packet, as well as any errors or anomalies in the network communication. A protocol analyzer can help troubleshoot network connectivity issues by identifying the root cause of the problem, such as misconfigured firewall rules, incorrect routing, or faulty network devices<sup>12</sup>.

To use a protocol analyzer to verify traffic to and from the server, the customer can follow these steps:

? Install a protocol analyzer tool on a device that is connected to the same network as the server, such as Wireshark<sup>3</sup> or Microsoft Network Monitor<sup>4</sup>.

? Select the network interface that is used to communicate with the server, and start capturing the network traffic.

? Filter the captured traffic by using the IP address or hostname of the server, or by using a specific port or protocol that is used by the database service.

? Analyze the filtered traffic and look for any signs of successful or failed connection attempts, such as TCP SYN, ACK, or RST packets, or ICMP messages.

? If there are no connection attempts to or from the server, then there may be a problem with the network configuration or device settings that prevent the traffic from reaching the server.

? If there are connection attempts but they are rejected or dropped by the server, then there may be a problem with the server configuration or service settings that prevent the traffic from being accepted by the server.

The other options are not the best ways to verify traffic to and from the server. nmap is a tool that can scan a network and discover hosts and services, but it cannot capture and analyze the network packets in detail. ipconfig is a command that can display and configure the IP settings of a device, but it cannot monitor or test the network communication with another device. Speed test is a tool that can measure the bandwidth and latency of a network connection, but it cannot diagnose or troubleshoot specific network problems.

**NEW QUESTION 143**

- (Topic 3)

Which of the following would be used to adjust resources dynamically for a virtual web server under variable loads?

- A. Elastic computing
- B. Scalable networking
- C. Hybrid deployment
- D. Multitenant hosting

**Answer:** B

**Explanation:**

A technique used to adjust resources dynamically for a virtual web server under variable loads is called auto-scaling. Auto-scaling automatically increases or decreases the number of instances of a virtual web server in response to changes in demand, ensuring that the right amount of resources are available to handle incoming traffic. This can help to improve the availability and performance of a web application, as well as reduce costs by avoiding the need to provision and maintain excess capacity.

**NEW QUESTION 145**

- (Topic 3)

Which of the following attacks utilizes a network packet that contains multiple network tags?

- A. MAC flooding
- B. VLAN hopping
- C. DNS spoofing
- D. ARP poisoning

**Answer:** B

**NEW QUESTION 149**

- (Topic 3)

Which of the following protocols can be used to change device configurations via encrypted and authenticated sessions? (Select TWO).

- A. SNMPv3
- B. SSh
- C. Telnet
- D. IPSec
- E. ESP
- F. Syslog

**Answer:** BD

**NEW QUESTION 153**

- (Topic 3)

A network administrator would like to purchase a device that provides access ports to endpoints and has the ability to route between networks. Which of the following would be BEST for the administrator to purchase?

- A. An IPS
- B. A Layer 3 switch
- C. A router

D. A wireless LAN controller

**Answer:** B

#### NEW QUESTION 155

- (Topic 3)

Which of the following combinations of single cables and transceivers will allow a server to have 40GB of network throughput? (Select two).

- A. SFP+
- B. SFP
- C. QSFP+
- D. Multimode
- E. Cat 6a
- F. Cat5e

**Answer:** CD

#### Explanation:

QSFP+ is a type of transceiver that supports 40 gigabit Ethernet (40GbE) over four lanes of 10 gigabit Ethernet (10GbE) each. QSFP+ stands for quad small form-factor pluggable plus, and it is a compact and hot-swappable module that plugs into a QSFP+ port on a network device. QSFP+ transceivers can support various types of cables and connectors, such as direct attach copper (DAC), active optical cable (AOC), or fiber optic cable. Multimode is a type of fiber optic cable that supports multiple modes of light propagation within the core. Multimode fiber optic cable can carry higher bandwidth and data rates than single-mode fiber optic cable, but over shorter distances. Multimode fiber optic cable is commonly used for short-reach applications, such as within a data center or a campus network. Multimode fiber optic cable can be paired with QSFP+ transceivers to achieve 40GbE connectivity.

The other options are not correct because they do not support 40GbE. They are:

? SFP+. SFP+ is a type of transceiver that supports 10 gigabit Ethernet (10GbE) over a single lane. SFP+ stands for small form-factor pluggable plus, and it is a compact and hot-swappable module that plugs into an SFP+ port on a network device. SFP+ transceivers can support various types of cables and connectors, such as direct attach copper (DAC), active optical cable (AOC), or fiber optic cable. However, SFP+ transceivers cannot support 40GbE by themselves, unless they are used in a breakout configuration with a QSFP+ transceiver.

? SFP. SFP is a type of transceiver that supports 1 gigabit Ethernet (1GbE) over a single lane. SFP stands for small form-factor pluggable, and it is a compact and hot-swappable module that plugs into an SFP port on a network device. SFP transceivers can support various types of cables and connectors, such as twisted-pair copper, coaxial cable, or fiber optic cable. However, SFP transceivers cannot support 40GbE by themselves, unless they are used in a breakout configuration with a QSFP+ transceiver.

? Cat 6a. Cat 6a is a type of twisted-pair copper cable that supports 10 gigabit

Ethernet (10GbE) over distances up to 100 meters. Cat 6a stands for category 6 augmented, and it is an enhanced version of Cat 6 cable that offers better performance and reduced crosstalk. Cat 6a cable can be paired with 10Gbase-T transceivers to achieve 10GbE connectivity. However, Cat 6a cable cannot support 40GbE by itself, unless it is used in a breakout configuration with a QSFP+ transceiver.

? Cat 5e. Cat 5e is a type of twisted-pair copper cable that supports 1 gigabit

Ethernet (1GbE) over distances up to 100 meters. Cat 5e stands for category 5 enhanced, and it is an improved version of Cat 5 cable that offers better performance and reduced crosstalk. Cat 5e cable can be paired with 1000base-T transceivers to achieve 1GbE connectivity. However, Cat 5e cable cannot support 40GbE by itself, unless it is used in a breakout configuration with a QSFP+ transceiver.

References1: QSFP+ - an overview | ScienceDirect Topics2: Multimode Fiber - an overview | ScienceDirect Topics3: Network+ (Plus) Certification | CompTIA IT Certifications4: SFP+ - an overview | ScienceDirect Topics5: SFP - an overview | ScienceDirect Topics6: Cat 6a - an overview | ScienceDirect Topics7: [Cat 5e - an overview | ScienceDirect Topics]

#### NEW QUESTION 160

- (Topic 3)

Which of the following records can be used to track the number of changes on a DNS zone?

- A. SOA
- B. SRV
- C. PTR
- D. NS

**Answer:** A

#### Explanation:

The DNS 'start of authority' (SOA) record stores important information about a domain or zone such as the email address of the administrator, when the domain was last updated, and how long the server should wait between refreshes. All DNS zones need an SOA record in order to conform to IETF standards. SOA records are also important for zone transfers.

#### NEW QUESTION 165

- (Topic 3)

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 come on. Which of the following should a technician try first to troubleshoot this issue?

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

**Answer:** A

#### Explanation:

One of the most common causes of fiber connectivity issues is the reversal of the fibers. This means that the transmit (TX) and receive (RX) ports on one end of the fiber link are not matched with the corresponding ports on the other end. For example, if the TX port on one device is connected to the TX port on another device, and the same for the RX ports, then the devices will not be able to communicate with each other. This can result in no indicator light, no link, or no data transmission.

To troubleshoot this issue, the technician should first try to reverse the fibers. This can be done by swapping the connectors at one end of the fiber patch cable, or

by using a crossover adapter or cable that reverses the polarity of the fibers. The technician should then check if the indicator light comes on and if the devices can communicate properly. The other options are not the first steps to troubleshoot this issue. Reterminating the fibers is a time-consuming and costly process that should be done only if there is evidence of physical damage or poor quality of the termination. Verifying the fiber size is not relevant in this scenario, as multimode fiber is compatible with multimode fiber, and any mismatch in core diameter or bandwidth would result in high attenuation, not complete loss of signal. Examining the cable runs for visual faults is a useful technique, but it requires a special tool called a visual fault locator (VFL) that emits a visible red light through the fiber and shows any breaks or bends along the cable. However, a VFL cannot detect polarity issues or connector problems, so it is not sufficient to troubleshoot this issue

#### NEW QUESTION 166

- (Topic 3)

A user calls the help desk to report being unable to reach a file server. The technician logs in to the user's computer and verifies that pings fail to respond back when trying to reach the file server. Which of the following would BEST help the technician verify whether the file server is reachable?

- A. netstat
- B. ipconfig
- C. nslookup
- D. traceroute

**Answer: D**

#### Explanation:

Traceroute is a network diagnostic tool that allows you to trace the path that network packets take from one device to another. By running traceroute to the file server, the technician can see the sequence of devices and networks that the packets pass through on their way to the file server. This can help the technician to determine if there is a problem with the network connection between the user's computer and the file server, or if the issue is with the file server itself.

#### NEW QUESTION 168

- (Topic 3)

A technician is expanding a wireless network and adding new access points. The company requires that each access point broadcast the same SSID. Which of the following should the technician implement for this requirement?

- A. MIMO
- B. Roaming
- C. Channel bonding
- D. Extended service set

**Answer: D**

#### Explanation:

An extended service set (ESS) is a wireless network that consists of two or more access points (APs) that share the same SSID and are connected by a distribution system, such as a switch or a router. An ESS allows wireless clients to roam seamlessly between different APs without losing connectivity or changing network settings. An ESS can also increase the coverage area and capacity of a wireless network

#### NEW QUESTION 172

- (Topic 3)

A technician removes an old PC from the network and replaces it with a new PC that is unable to connect to the LAN. Which of the following is MOST likely the cause of the issue?

- A. Port security
- B. Port tagging
- C. Port aggregation
- D. Port mirroring

**Answer: A**

#### Explanation:

It is most likely that the issue is caused by port security, as this is a feature that can prevent new devices from connecting to the LAN. Port tagging, port aggregation, and port mirroring are all features that are used to manage traffic on the network, but they are not related to the connectivity of new devices. If the technician has configured port security on the network and the new PC does not meet the security requirements, it will not be able to connect to the LAN.

#### NEW QUESTION 175

- (Topic 3)

A network is experiencing extreme latency when accessing a particular website. Which of the following commands will BEST help identify the issue?

- A. ipconfig
- B. netstat
- C. tracert
- D. ping

**Answer: C**

#### NEW QUESTION 177

- (Topic 3)

Which of the following is the MOST appropriate use case for the deployment of a clientless VPN?

- A. Secure web access to internal corporate resources.
- B. Upgrade security via the use of an NFV technology
- C. Connect two data centers across the internet.
- D. Increase VPN availability by using a SDWAN technology.

**Answer:** A

**NEW QUESTION 178**

- (Topic 3)

A company's publicly accessible servers are connected to a switch between the company's ISP-connected router and the firewall in front of the company network. The firewall is stateful, and the router is running an ACL. Which of the following best describes the area between the router and the firewall?

- A. Untrusted zone
- B. Screened subnet
- C. Trusted zone
- D. Private VLAN

**Answer:** B

**Explanation:**

A screened subnet is a network segment that is isolated from both the internal and external networks by firewalls or routers. It is used to host publicly accessible servers that need some protection from external attacks, but also need to be separated from the internal network for security reasons.

References

- ? 1: Seven-Second Subnetting – N10-008 CompTIA Network+ : 1.4
- ? 2: CompTIA Network+ Study Guide: Exam N10-008, 5th Edition, page 56
- ? 3: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 22

**NEW QUESTION 182**

- (Topic 3)

An organization has a security requirement that all network connections can be traced back to a user. A network administrator needs to identify a solution to implement on the wireless network. Which of the following is the best solution?

- A. Implementing enterprise authentication
- B. Requiring the use of PSKs
- C. Configuring a captive portal for users
- D. Enforcing wired equivalent protection

**Answer:** A

**Explanation:**

Enterprise authentication is a method of securing wireless networks that uses an external authentication server, such as RADIUS, to verify the identity of users and devices. Enterprise authentication can provide user traceability by logging the network connections and activities of each authenticated user. This can help the organization meet its security requirement and comply with any regulations or policies that mandate user accountability.

References:

- ? CompTIA Network+ N10-008 Certification Exam Objectives, page 83
- ? CompTIA Network+ Cert Guide: Wireless Networking, page 13

**NEW QUESTION 184**

- (Topic 3)

Which of the following compromises internet-connected devices and makes them vulnerable to becoming part of a botnet? (Select TWO).

- A. Deauthentication attack
- B. Malware infection
- C. IP spoofing
- D. Firmware corruption
- E. Use of default credentials
- F. Dictionary attack

**Answer:** BE

**NEW QUESTION 185**

- (Topic 3)

A technician is contracted to install a redundant cluster of devices from the ISP. In case of a hardware failure within the network. Which of the following would provide the BEST redundant solution in Layer 2 devices?

- A. Multiple routers
- B. Multiple switches
- C. Multiple firewalls
- D. Multiple budgets

**Answer:** B

**NEW QUESTION 188**

- (Topic 3)

A company realizes that only half of its employees work in the office, and the employees who work from home no longer need a computer at the office. Which of the following security measures should the network administrator implement when removing a computer from a cubicle?

- A. Disable DHCP on the computer being removed.
- B. Place the switch port in a private VLAN.
- C. Apply a firewall rule to block the computer's IP address.
- D. Remove the employee's network access.

**Answer:** D

**Explanation:**

The best security measure to implement when removing a computer from a cubicle is to remove the employee's network access. This will prevent the employee from accessing any network resources or data from the computer, as well as prevent any unauthorized users from using the computer to access the network. Removing the employee's network access can be done by deleting or disabling the user account, revoking the credentials, or changing the permissions. The other options are not as effective or necessary as removing the employee's network access. They are:

- Disabling DHCP on the computer being removed will prevent the computer from obtaining an IP address from the network, but it will not prevent the computer from using a static IP address or accessing the network through another device.
- Placing the switch port in a private VLAN will isolate the computer from other devices on the network, but it will not prevent the computer from accessing the network through another port or device.
- Applying a firewall rule to block the computer's IP address will prevent the computer from communicating with the network, but it will not prevent the computer from changing its IP address or accessing the network through another device.

References

- 1: CompTIA Network+ N10-008 Cert Guide - O'Reilly Media 2: Network+ (Plus) Certification | CompTIA IT Certifications
- 3: 10 Ways to Secure Office Workstations - Computer Security

**NEW QUESTION 192**

- (Topic 3)

Which of the following most likely occurs when an attacker is between the target and a legitimate server?

- A. IP spoofing
- B. VLAN hopping
- C. Rogue DHCP
- D. On-path attack

**Answer: D**

**Explanation:**

An on-path attack (also known as a man-in-the-middle attack) is a type of security attack where the attacker places themselves between two devices (often a web browser and a web server) and intercepts or modifies communications between the two<sup>1</sup>. The attacker can then collect information as well as impersonate either of the two agents. For example, an on-path attacker could capture login credentials, redirect traffic to malicious sites, or inject malware into legitimate web pages. The other options are not correct because they describe different types of attacks:

- IP spoofing is the practice of forging the source IP address of a packet to make it appear as if it came from a trusted or authorized source<sup>2</sup>.
- VLAN hopping is a technique that allows an attacker to access a VLAN that they are not authorized to access by sending packets with a modified VLAN tag<sup>3</sup>.
- Rogue DHCP is a scenario where an unauthorized DHCP server offers IP configuration parameters to clients on a network, potentially causing network disruption or redirection to malicious sites<sup>4</sup>.

References

- 2: Understanding Targeted Attacks: What is a Targeted Attack? 3: Types of attacks - Security on the web | MDN
- 1: What is an on-path attacker? | Cloudflare
- 4: [What is a Rogue DHCP Server? - Definition from Techopedia]

**NEW QUESTION 195**

- (Topic 3)

Which of the following types of connections would need to be set up to provide access from the internal network to an external network so multiple satellite offices can communicate securely using various ports and protocols?

- A. Client-to-site VPN
- B. Clientless VPN
- C. RDP
- D. Site-to-site VPN
- E. SSH

**Answer: D**

**NEW QUESTION 198**

- (Topic 3)

A company with multiple routers would like to implement an HA network gateway with the least amount of downtime possible. This solution should not require changes on the gateway setting of the network clients. Which of the following should a technician configure?

- A. Automate a continuous backup and restore process of the system's state of the active gateway.
- B. Use a static assignment of the gateway IP address on the network clients.
- C. Configure DHCP relay and allow clients to receive a new IP setting.
- D. Configure a shared VIP and deploy VRRP on the routers.

**Answer: D**

**Explanation:**

The open standard protocol Virtual Router Redundancy Protocol (VRRP) is similar to HSRP, the differences mainly being in terminology and packet formats. In VRRP, the active router is known as the master, and all other routers in the group are known as backup routers. There is no specific standby router; instead, all backup routers monitor the status of the master, and in the event of a failure, a new master router is selected from the available backup routers based on priority

**NEW QUESTION 200**

- (Topic 3)

A network security engineer is responding to a security incident. The engineer suspects that an attacker used an authorized administrator account to make configuration changes to the boundary firewall. Which of the following should the network security engineer review?

- A. Network traffic logs
- B. Audit logs
- C. Syslogs
- D. Event logs

**Answer:** B

**Explanation:**

Audit logs are records of the actions performed by users or processes on a system or network device. They can provide information about who made what changes, when, and why. Audit logs are essential for detecting and investigating security incidents, as well as for ensuring compliance with policies and regulations. Audit logs can help the network security engineer to identify the source of the unauthorized configuration changes to the boundary firewall, as well as the scope and impact of the changes.

References1 - Changes to Cyber Essentials requirements – April 2021 update2 - 8 Firewall Best Practices for Securing the Network3 - How to secure your network boundaries with a firewall

**NEW QUESTION 202**

SIMULATION - (Topic 3)

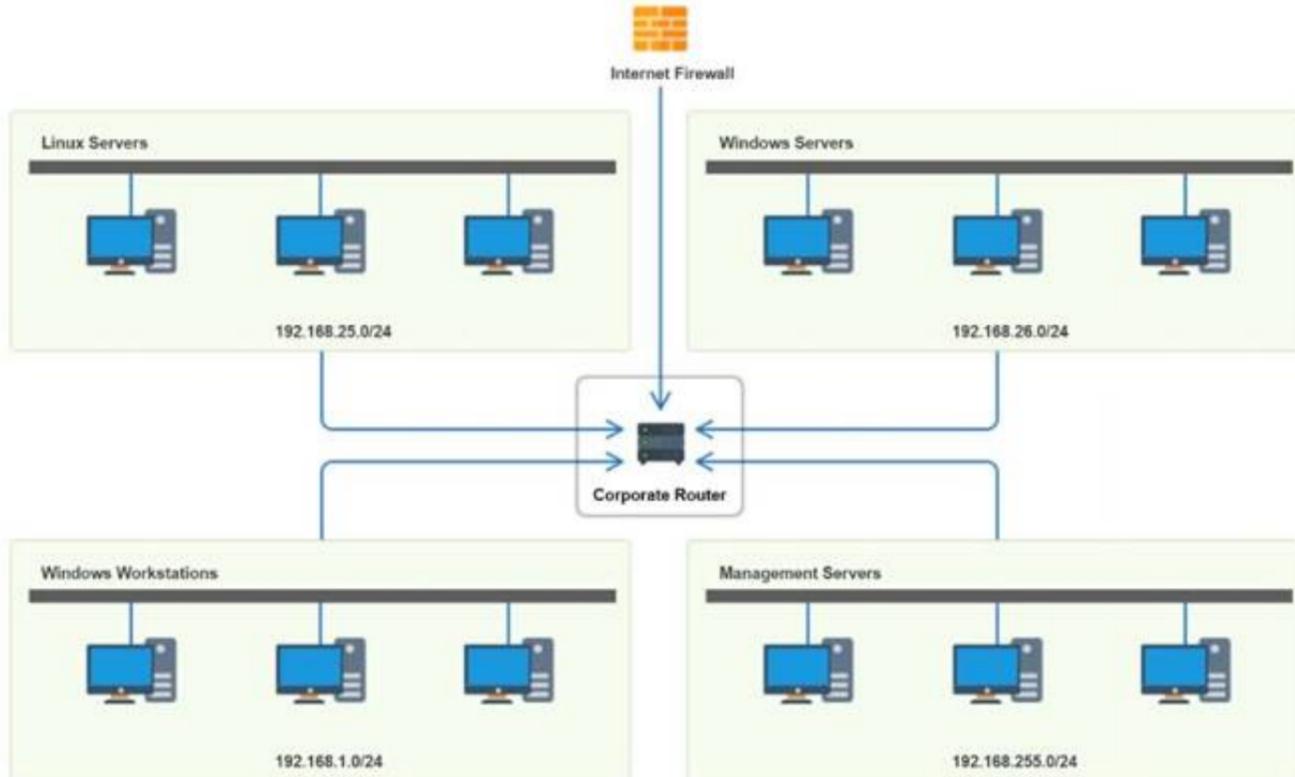
You have been tasked with implementing an ACL on the router that will:

- \* 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.

**INSTRUCTIONS**

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.



Router Access Control List					
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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Router Access Control List					
Rule	Source	Destination	Protocol	Service	Action
1	192.168.255.0	192.168.26.0	TCP	SSH	Allow
2	192.168.255.0	192.168.25.0	TCP	SSH	Allow
3	192.168.255.0	192.168.1.0	TCP	SSH	Allow
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	Any	TCP	RDP	Deny
7	192.168.1.0	Any	TCP	VNC	Deny
8	192.168.1.0	Any	Any	Any	Allow
9	Any	Any	Any	Any	Deny

### NEW QUESTION 203

- (Topic 3)

A network administrator is configuring a firewall to allow for a new cloud-based email server. The company standard is to use SMTP to route email traffic. Which of the following ports, by default, should be reserved for this purpose?

- A. 23
- B. 25
- C. 53
- D. 110

**Answer:** B

#### Explanation:

Port 25, by default, should be reserved for SMTP traffic to allow for a new cloud-based email server. SMTP stands for Simple Mail Transfer Protocol, which is a network protocol that enables email communication between mail servers and clients. SMTP uses port 25 as its default port for sending and receiving email messages over TCP/IP networks. A cloud-based email server is an email server that is hosted on a cloud service provider's infrastructure, rather than on-premise or in-house. A cloud-based email server can offer advantages such as scalability, reliability, security, and cost-effectiveness. To allow for a new cloud-based email server, a firewall should be configured to open port 25 for SMTP traffic. References: [CompTIA Network+ Certification Exam Objectives], What Is SMTP? | Mailtrap Blog, Cloud Email Server: What Is It & How Does It Work? | Zoho Mail

### NEW QUESTION 205

- (Topic 3)

A company has been added to an unapproved list because of spam. The network administrator confirmed that a workstation was infected by malware. Which of the following processes did the administrator use to identify the root cause?

- A. Traffic analysis
- B. Availability monitoring
- C. Baseline metrics
- D. Network discovery

**Answer:** A

#### Explanation:

One possible process that the administrator used to identify the root cause of the spam issue is traffic analysis. Traffic analysis is a technique that monitors and analyzes the network traffic that flows between devices or applications. Traffic analysis can help troubleshoot network problems by identifying the source, destination, volume, frequency, and content of the network packets.

To use traffic analysis to identify the root cause of the spam issue, the administrator could follow these steps:

- ? Install a traffic analysis tool on the server or a device that is connected to the same network as the server, such as Wireshark<sup>3</sup>, tcpdump<sup>4</sup>, or Microsoft Network Monitor<sup>5</sup>.
- ? Start capturing the network traffic and filter it by using the IP address or hostname of the server, or by using a specific port or protocol that is used by the email service, such as SMTP (port 25), POP3 (port 110), or IMAP (port 143).
- ? Analyze the filtered traffic and look for any signs of abnormal or malicious activity, such as high volume of outgoing emails, unknown recipients, suspicious attachments, or spam keywords.
- ? Trace back the source of the spam emails to the infected workstation by using its IP address or MAC address.
- ? Isolate and clean up the infected workstation by using an antivirus or malware removal tool.

The other options are not processes that the administrator used to identify the root cause of the spam issue. Availability monitoring is a technique that measures and reports the uptime and downtime of a network device or service. Availability monitoring can help troubleshoot network problems by detecting any failures or outages that affect the network performance. Baseline metrics are a set of standard measurements that establish the normal behavior or performance of a network device or service. Baseline metrics can help troubleshoot network problems by comparing the current state of the network with the expected state and identifying any deviations or anomalies. Network discovery is a technique that scans and maps the network devices and services that are connected to a network. Network discovery can help troubleshoot network problems by providing a comprehensive and updated view of the network topology and configuration.

### NEW QUESTION 207

- (Topic 3)

Which of the following would be used to forward requests and replies between a DHCP server and client?

- A. Relay
- B. Lease
- C. Scope
- D. Range

**Answer: B**

#### NEW QUESTION 209

- (Topic 3)

While using a secure conference call connection over a corporate VPN, a user moves from a cellular connection to a hotel wireless network. Although the wireless connection and the VPN show a connected status, no network connectivity is present. Which of the following is the most likely cause of this issue?

- A. MAC filtering is configured on the wireless connection.
- B. The VPN and the WLAN connection have an encryption protocol mismatch.
- C. The WLAN is using a captive portal that requires further authentication.
- D. Wireless client isolation is enforced on the WLAN settings.

**Answer: C**

#### Explanation:

A captive portal is a web page that is displayed to newly connected users of a Wi-Fi network before they are granted broader access to network resources. Captive portals are commonly used to present a landing or log-in page which may require authentication, payment, acceptance of an end-user license agreement, acceptable use policy, survey completion, or other valid credentials that both the host and user agree to adhere by123

A possible cause of the issue is that the user has not completed the captive portal authentication process, which prevents the VPN from establishing a secure connection over the Wi-Fi network. The user may need to open a web browser and follow the instructions on the captive portal page to gain full access to the internet.

#### NEW QUESTION 213

- (Topic 3)

Which of the following network types is composed of computers that can all communicate with one another with equal permissions and allows users to directly share what is on or attached to their computers?

- A. Local area network
- B. Peer-to-peer network
- C. Client-server network
- D. Personal area network

**Answer: B**

#### Explanation:

A peer-to-peer network is a type of network in which each computer (or node) can communicate directly with any other node, without requiring a central server or authority. Each node can act as both a client and a server, and can share its own resources, such as files, printers, or internet connection, with other nodes. A peer-to-peer network allows users to directly access and exchange what is on or attached to their computers, with equal permissions and responsibilities

#### NEW QUESTION 214

- (Topic 3)

Which of the following can be used to identify users after an action has occurred?

- A. Access control vestibule
- B. Cameras
- C. Asset tag
- D. Motion detectors

**Answer: B**

#### Explanation:

Cameras can be used to identify users after an action has occurred by recording their faces, clothing, or other distinctive features. Cameras are often used as a deterrent and a forensic tool for security purposes. Access control vestibules, asset tags, and motion detectors are not effective in identifying users, but rather in controlling access, tracking assets, and detecting movement.

References:

CompTIA Network+ N10-008 Certification Exam Objectives, Domain 5.0: Network Security, Subobjective 5.1: Summarize the importance of physical security controls, page 231 CompTIA Network+ Certification All-in-One Exam Guide, Eighth Edition (Exam N10-008), Chapter 18: Network Security, Section: Physical Security, page 7372

#### NEW QUESTION 218

- (Topic 3)

AGRE tunnel has been configured between two remote sites. Which of the following features, when configured, ensures GRE overhead does not affect payload?

- A. jumbo frames
- B. Auto medium-dependent Interface
- C. Interface crossover
- D. Collision detection

**Answer: A**

**Explanation:**

One of the features that can be configured to ensure that GRE overhead does not affect payload is A. jumbo frames. Jumbo frames are Ethernet frames that have a payload size larger than 1500 bytes, which is the standard maximum transmission unit (MTU) for Ethernet. By using jumbo frames, more data can be sent in each packet, reducing the overhead ratio and improving efficiency. Auto medium-dependent interface (MDI), interface crossover, and collision detection are features related to Ethernet physical layer connectivity, but they do not affect GRE overhead or payload.

**NEW QUESTION 223**

- (Topic 3)

A network administrator installed a new data and VoIP network. Users are now experiencing poor call quality when making calls. Which of the following should the administrator do to increase VoIP performance?

- A. Configure a voice VLAN.
- B. Configure LACP on all VoIP phones.
- C. Configure PoE on the network.
- D. Configure jumbo frames on the network.

**Answer: A**

**Explanation:**

"Benefits of Voice VLAN

It ensures that your VoIP (Voice over Internet Phone) devices do not have to contend directly with all the broadcasts and other traffic from the data VLAN. A voice VLAN can simplify network configuration in some circumstances."

<https://community.fs.com/blog/auto-voip-vs-voice-vlan-what-s-the-difference.html> Jumbo Frames

"When jumbo frames on a VoIP/UC network are enabled, it can cause the same kind of delay to your network transmissions."

"VoIP uses will always not benefit from jumbo frame, as VoIP like gaming, is latency and time sensitive. Jumbo Frame for Internet Purpose: You will not see any performance boost as the files that came across the internet does not support jumbo frame."

<https://www.ankmax.com/newsinfo/1358641.html#:~:text=VoIP%20uses%20will%20always%20not,does%20not%20support%20jumbo%20frame.>

"To summarize this general best practice guide, you should NOT enable jumbo frame feature as a general home user."

**NEW QUESTION 225**

- (Topic 3)

Which of the following is a benefit of the spine-and-leaf network topology?

- A. Increased network security
- B. Stable network latency
- C. Simplified network management
- D. Eliminated need for inter-VLAN routing

**Answer: A**

**NEW QUESTION 230**

- (Topic 3)

A network engineer is concerned about VLAN hopping happening on the network. Which of the following should the engineer do to address this concern?

- A. Configure private VLANs.
- B. Change the default VLAN.
- C. Implement ACLs on the VLAN.
- D. Enable dynamic ARP inspection.

**Answer: B**

**Explanation:**

VLAN hopping is a type of attack that allows an attacker to access or manipulate traffic on a different VLAN than the one they are connected to. One way to prevent VLAN hopping is to change the default VLAN on a switch. The default VLAN is the VLAN that is assigned to all ports on a switch by default, usually VLAN 1. If an attacker connects to an unused port on a switch that has not been configured with a specific VLAN, they can access or spoof traffic on the default VLAN. By changing the default VLAN to an unused or isolated VLAN, the network administrator can prevent unauthorized access or interference with legitimate traffic on other VLANs. References: <https://www.comptia.org/training/books/network-n10-008-study-guide> (page 308)

**NEW QUESTION 233**

- (Topic 3)

After installing a series of Cat 8 keystones, a data center architect notices higher than normal interference during tests. Which of the following steps should the architect take to troubleshoot the issue?

- A. Check to see if the end connections were wrapped in copper tape before terminating.
- B. Use passthrough modular crimping plugs instead of traditional crimping plugs.
- C. Connect the RX/TX wires to different pins.
- D. Run a speed test on a device that can only achieve 100Mbps speeds.

**Answer: A**

**Explanation:**

Cat 8 keystones are shielded to prevent interference from external sources, but they also require proper grounding to avoid interference from within the cable. Wrapping the end connections with copper tape before terminating them is one way to ensure a good ground connection and reduce interference. Using passthrough modular crimping plugs, connecting the RX/TX wires to different pins, or running a speed test on a slow device are not relevant or effective steps to troubleshoot the issue.

References:

- ? CompTIA Network+ N10-008 Certification Study Guide, page 191
- ? CompTIA Network+ N10-008 Cert Guide, Deluxe Edition, page 362
- ? CAT8 RJ45 Keystone Problem : r/HomeNetworking2
- ? How to Terminate Cat8 Shielded Keystone Jacks3

**NEW QUESTION 238**

- (Topic 3)

During a recent security audit, a contracted penetration tester discovered the organization uses a number of insecure protocols. Which of the following ports should be disallowed so only encrypted protocols are allowed? (Select TWO).

- A. 22
- B. 23
- C. 69
- D. 443
- E. 587
- F. 8080

**Answer:** BC

**NEW QUESTION 242**

- (Topic 3)

Which of the following cloud deployment models involves servers that are hosted at a company's property and are only used by that company?

- A. Public
- B. Private
- C. Hybrid
- D. Community

**Answer:** B

**Explanation:**

A private cloud deployment model involves servers that are hosted at a company's property and are only used by that company. A private cloud provides exclusive access and control over the cloud resources to the company, as well as higher security and privacy. However, a private cloud also requires more investment and maintenance from the company, compared to other cloud deployment models<sup>1</sup>

**NEW QUESTION 243**

- (Topic 3)

Which of the following can be used to limit the ability of devices to perform only HTTPS connections to an internet update server without exposing the devices to the public internet?

- A. Allow connections only to an internal proxy server.
- B. Deploy an IDS system and place it in line with the traffic.
- C. Create a screened network and move the devices to it.
- D. Use a host-based network firewall on each device.

**Answer:** A

**Explanation:**

An internal proxy server is a server that acts as an intermediary between internal devices and external servers on the internet. An internal proxy server can be used to limit the ability of devices to perform only HTTPS connections to an internet update server by filtering and forwarding the requests and responses based on predefined rules or policies. An internal proxy server can also prevent the devices from being exposed to the public internet by hiding their IP addresses and providing a layer of security and privacy.

**NEW QUESTION 246**

- (Topic 3)

A network administrator is looking at switch features and is unsure whether to purchase a model with PoE. Which of the following devices that commonly utilize PoE should the administrator consider? (Select TWO)

- A. VoIP phones
- B. Cameras
- C. Printers
- D. Cable modems
- E. Laptops
- F. UPSs

**Answer:** AB

**Explanation:**

Power over Ethernet (PoE) is a technology that allows network-connected devices to receive power over the same Ethernet cables that are used for data transfer. PoE is commonly used to power devices such as VoIP phones and cameras, making it an ideal choice for network administrators looking for a cost-effective solution. PoE is not typically used for other devices such as printers, cable modems, laptops, and UPSs.

**NEW QUESTION 248**

- (Topic 3)

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?

- 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**

#### NEW QUESTION 253

- (Topic 3)

A network administrator is installing a new server in the data center. The administrator is concerned the amount of traffic generated will exceed 1GB, and higher-throughput NiCs are not available for installation. Which of the following is the BEST solution for this issue?

- A. Install an additional NIC and configure LACP.
- B. Remove some of the applications from the server.
- C. Configure the NIC to use full duplex
- D. Configure port mirroring to send traffic to another server.
- E. Install a SSD to decrease data processing time.

**Answer: A**

#### NEW QUESTION 254

- (Topic 3)

A network technician needs to select an AP that will support at least 1.3Gbps and 5GHz only. Which of the following wireless standards must the AP support to meet the requirements?

- A. B
- B. AC
- C. AX
- D. N
- E. G

**Answer: B**

#### Explanation:

Wireless AC is a wireless standard that supports up to 1.3Gbps data rate and operates in the 5GHz frequency band only. Wireless AC is also backward compatible with wireless A and N devices that use the 5GHz band. Wireless AC is suitable for high-performance applications such as HD video streaming and online gaming. References: Network+ Study Guide Objective 2.2: Explain the purposes and properties of routing and switching. Subobjective: Wireless standards and their characteristics.

#### NEW QUESTION 259

- (Topic 3)

A company has a geographically remote office. In order to connect to the internet, the company has decided to use a satellite WAN link. Which of the following is the GREATEST concern for this type of connection?

- A. Duplex
- B. Collisions
- C. Jitter
- D. Encapsulation

**Answer: C**

#### Explanation:

Jitter is the variation in latency or delay of packets in a network. Satellite WAN links have high latency and are prone to jitter, which can affect the quality of voice and video applications. Jitter is the greatest concern for this type of connection

#### NEW QUESTION 263

- (Topic 3)

Which of the following types of data center architectures will MOST likely be used in a large SDN and can be extended beyond the data center?

- A. iSCSI
- B. FCoE
- C. Three-tiered network

- D. Spine and leaf
- E. Top-of-rack switching

**Answer:** D

**Explanation:**

The type of data center architecture that will most likely be used in a large SDN and can be extended beyond the data center is spine and leaf. Spine and leaf is a network topology that consists of two layers of switches: spine switches and leaf switches. Spine switches are interconnected to each other and form the core of the network, while leaf switches are connected to each spine switch and form the access layer of the network. Spine and leaf topology provides high scalability, performance, and flexibility for data center networks, especially for SDN (Software Defined Networking) environments that require dynamic traffic flows and virtualization. References: CompTIA Network+ N10-008 Certification Study Guide, page 16; The Official CompTIA Network+ Student Guide (Exam N10-008), page 1-9.

**NEW QUESTION 266**

- (Topic 3)

Which of the following cloud components can filter inbound and outbound traffic between cloud resources?

- A. NAT gateways
- B. Service endpoints
- C. Network security groups
- D. Virtual private cloud

**Answer:** C

**Explanation:**

Network security groups are cloud components that can filter inbound and outbound traffic between cloud resources based on rules and priorities. Network security groups can be applied to virtual machines, subnets, or network interfaces to control the network access and security. Network security groups can allow or deny traffic based on the source, destination, port, and protocol of the packets. Network security groups are different from NAT gateways, service endpoints, and virtual private clouds, which are other cloud components that have different functions and purposes.

References

- ? 1: Network Security Groups – N10-008 CompTIA Network+ : 3.2
- ? 2: CompTIA Network+ N10-008 Certification Study Guide, page 329-330
- ? 3: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 17
- ? 4: CompTIA Network+ N10-008 Certification Practice Test, question 10

**NEW QUESTION 270**

- (Topic 3)

Which of the following layers of the OSI model has new protocols activated when a user moves from a wireless to a wired connection?

- A. Data link
- B. Network
- C. Transport
- D. Session

**Answer:** A

**Explanation:**

"The Data Link layer also determines how data is placed on the wire by using an access method. The wired access method, carrier-sense multiple access with collision detection (CSMA/CD), was once used by all wired Ethernet networks, but is automatically disabled on switched full-duplex links, which have been the norm for decades. Carrier-sense multiple access with collision avoidance (CSMA/CA) is used by wireless networks, in a similar fashion."

**NEW QUESTION 273**

- (Topic 3)

A network technician needs to use an RFC1918 IP space for a new office that only has a single public IP address. Which of the following subnets should the technician use for the LAN?

- A. 10.10.10.0/24
- B. 127.16.10.0/24
- C. 174.16.10.0/24
- D. 198.18.10.0/24

**Answer:** A

**Explanation:**

The RFC1918 IP space is a set of private IP addresses that are not routable on the public Internet and can be used for internal networks. The RFC1918 IP space consists of three ranges: 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. Out of the four options, only A. 10.10.10.0/24 belongs to one of these ranges, specifically the 10.0.0.0/8 range. Therefore, the technician should use this subnet for the LAN.

References1: [https://en.wikipedia.org/wiki/Private\\_network](https://en.wikipedia.org/wiki/Private_network)

**NEW QUESTION 278**

- (Topic 3)

To reduce costs and increase mobility, a Chief Technology Officer (CTO) wants to adopt cloud services for the organization and its affiliates. To reduce the impact for users, the CTO wants key services to run from the on-site data center and enterprise services to run in the cloud. Which of the following deployment models is the best choice for the organization?

- A. Public
- B. Hybrid
- C. SaaS
- D. Private

**Answer:** B

**Explanation:**

A hybrid cloud deployment model is a combination of on-premise and cloud solutions, where some resources are hosted in-house and some are hosted by a cloud provider. A hybrid cloud model can offer the benefits of both public and private clouds, such as scalability, cost-efficiency, security, and control. A hybrid cloud model can also reduce the impact for users, as they can access the key services from the on-site data center and the enterprise services from the cloud

**NEW QUESTION 279**

- (Topic 3)

A user took a laptop on a trip and made changes to the network parameters while at the airport. The user can access all internet websites but not corporate intranet websites. Which of the following is the most likely cause of the issue?

- A. Duplicate IP address
- B. Duplicate SSID
- C. Incorrect DNS
- D. Incorrect subnet mask

**Answer:** C

**Explanation:**

DNS (Domain Name System) is a service that translates domain names into IP addresses. Corporate intranet websites are usually hosted on private IP addresses that are not accessible from the public internet. Therefore, the user's laptop needs to use the correct DNS server that can resolve the intranet domain names to the private IP addresses. If the user changed the network parameters at the airport and did not revert them back, the laptop might be using a public DNS server that does not have the records for the intranet websites. This would cause the user to access all internet websites but not corporate intranet websites.

References:

- ? An Overview of DNS - N10-008 CompTIA Network+ : 1.61
- ? DNS Configuration – CompTIA A+ 220-11012
- ? CompTIA Network+ Certification Exam Objectives, page 53

**NEW QUESTION 280**

- (Topic 3)

Which of the following documents dictates the uptimes that were agreed upon by the involved parties?

- A. MOU
- B. BYOD
- C. SLA
- D. NDA

**Answer:** C

**Explanation:**

An SLA (Service Level Agreement) is a document that defines the expected level of service and performance guaranteed by a service provider to a customer. It usually specifies metrics such as uptime, availability, reliability, response time, and compensation or penalties for not meeting the agreed standards. An SLA is a way of ensuring that both parties are clear about their roles and responsibilities, and that the customer receives the quality of service they paid for.

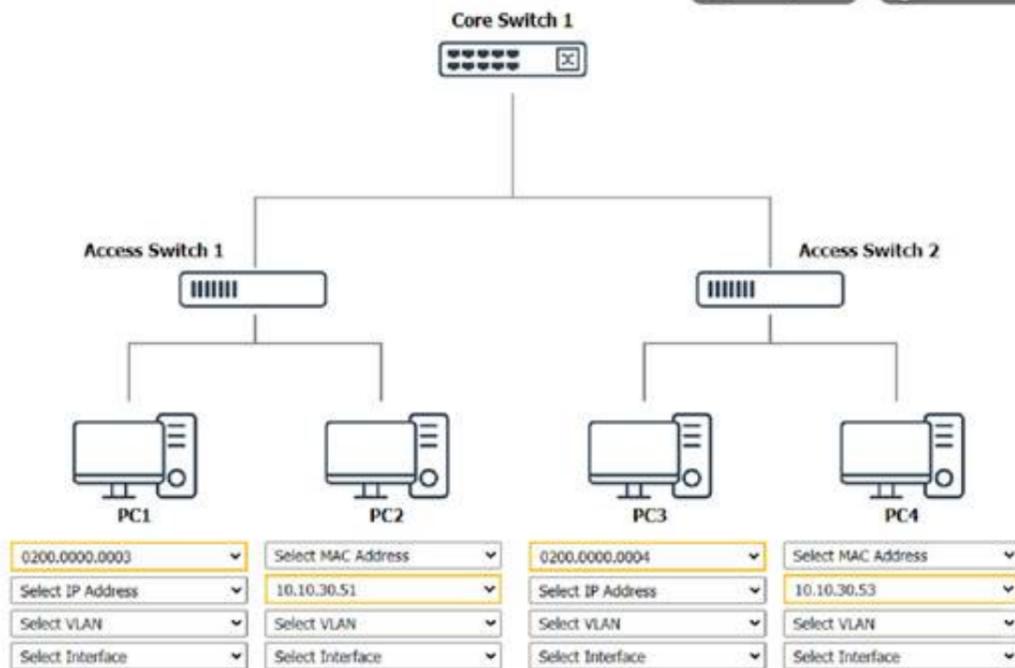
**NEW QUESTION 281**

SIMULATION - (Topic 3)

A network technician was recently onboarded to a company. A manager has tasked the technician with documenting the network and has provided the technician With partial information from previous documentation.

Instructions:

Click on each switch to perform a network discovery by entering commands into the terminal. Fill in the missing information using drop-down menus provided.



### Core Switch 1 Prompt



```
C:\> nmap
% Invalid input detected.
C:\> netdiscover
% Invalid input detected.
C:\> |
```

### Access Switch 1 Prompt



```
C:\> nmap
% Invalid input detected.
C:\>
```

### Access Switch 2 Prompt



```
C:\>
```

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

(Note: Ips will be change on each simulation task, so we have given example answer for the understanding)

To perform a network discovery by entering commands into the terminal, you can use the following steps:

? Click on each switch to open its terminal window.

? Enter the command show ip interface brief to display the IP addresses and statuses of the switch interfaces.

? Enter the command show vlan brief to display the VLAN configurations and assignments of the switch interfaces.

? Enter the command show cdp neighbors to display the information about the neighboring devices that are connected to the switch.

? Fill in the missing information in the diagram using the drop-down menus provided. Here is an example of how to fill in the missing information for Core Switch 1:

? The IP address of Core Switch 1 is 192.168.1.1.

? The VLAN configuration of Core Switch 1 is VLAN 1: 192.168.1.0/24, VLAN 2: 192.168.2.0/24, VLAN 3: 192.168.3.0/24.

? The neighboring devices of Core Switch 1 are Access Switch 1 and Access Switch 2.

? The interfaces that connect Core Switch 1 to Access Switch 1 are GigabitEthernet0/1 and GigabitEthernet0/2.

? The interfaces that connect Core Switch 1 to Access Switch 2 are GigabitEthernet0/3 and GigabitEthernet0/4.

You can use the same steps to fill in the missing information for Access Switch 1 and Access Switch 2.

**NEW QUESTION 284**

- (Topic 3)

A security engineer is trying to determine whether an internal server was accessed by hosts on the internet. The internal server was shut down during the investigation Which of the following will the engineer review to determine whether the internal server had an unauthorized access attempt?

- A. The server's syslog
- B. The NetFlow statistics
- C. The firewall logs
- D. The audit logs on the core switch

**Answer: A**

**NEW QUESTION 289**

- (Topic 3)

A company's web server is hosted at a local ISP. This is an example of:

- A. allocation.
- B. an on-premises data center.
- C. a branch office.
- D. a cloud provider.

**Answer: D**

**NEW QUESTION 290**

- (Topic 3)

A company is sending a switch to a remote site to be reused. An administrator needs to move the switch and ensure no network settings persist. Which of the following databases does the administrator need to delete?

- A. VLAN
- B. STP
- C. ARP
- D. Trunking

**Answer: A**

**Explanation:**

The VLAN database is the database that stores the VLAN configuration information on a switch, such as the VLAN IDs, names, and ports. The VLAN database is stored in a separate file from the switch configuration file, and it is not affected by the erase startup- config or reload commands. Therefore, to delete the VLAN database, the administrator needs to use a specific command, such as delete flash:vlan.dat or delete vlan.dat, depending on the switch model. Deleting the VLAN database will ensure that no network settings related to VLANs persist on the switch when it is moved to a remote site. References

? 1: CompTIA Network+ N10-008 Certification Study Guide, page 163

? 2: N10-008 CompTIA Network+ : 5.5 - Professor Messer IT Certification Training Courses

? 3: CompTIA Network+ (N10-008) Practice Exam w/PBQ & Solution, question 6

**NEW QUESTION 292**

- (Topic 3)

A company has a geographically remote office concern for this type of connection?

- A. Duplex
- B. Collisions
- C. Jitter
- D. Encapsulation

**Answer: C**

**Explanation:**

Jitter is the variation in the delay of packets arriving at a destination. Jitter can cause problems for real-time applications, such as voice and video, that require consistent and smooth delivery of packets. A geographically remote office that connects to the main office via a WAN link may experience high jitter due to factors such as network congestion, routing changes, or link quality. Jitter can be reduced by using quality of service (QoS) mechanisms that prioritize and shape traffic according to its importance and

sensitivity. References: [CompTIA Network+ Certification Exam Objectives], What is Jitter?

| Network Jitter Explained | SolarWinds

### NEW QUESTION 297

- (Topic 3)

Which of the following would MOST likely be used to review disaster recovery information for a system?

- A. Business continuity plan
- B. System life cycle
- C. Change management
- D. Standard operating procedures

**Answer:** A

#### **Explanation:**

The document that would most likely be used to review disaster recovery information for a system is a business continuity plan (BCP). A BCP is a document that outlines the procedures and resources needed to maintain or resume critical business functions in the event of a disaster or disruption. A BCP typically includes a disaster recovery plan (DRP), which is a subset of the BCP that focuses on restoring IT systems and data after a disaster. A BCP also covers other aspects of business continuity, such as risk assessment, business impact analysis, emergency response, crisis management, and testing. References: CompTIA Network+ N10-008 Certification Study Guide, page 346; The Official CompTIA Network+ Student Guide (Exam N10-008), page 13-9.

### NEW QUESTION 301

- (Topic 3)

A network administrator is designing a wireless network. The administrator must ensure a rented office space has a sufficient signal. Reducing exposure to the wireless network is important, but it is secondary to the primary objective. Which of the following would MOST likely facilitate the correct accessibility to the Wi-Fi network?

- A. Polarization
- B. Channel utilization
- C. Channel bonding
- D. Antenna type
- E. MU-MIMO

**Answer:** B

### NEW QUESTION 303

- (Topic 3)

A network engineer is designing a secure communication link between two sites. The entire data stream needs to remain confidential. Which of the following will achieve this goal?

- A. GRE
- B. IKE
- C. ESP
- D. AH

**Answer:** C

#### **Explanation:**

ESP stands for Encapsulating Security Payload, and it is a protocol that provides confidentiality, integrity, and authentication for IP packets. ESP encrypts the payload of the IP packet, which contains the data stream, and adds a header and a trailer that contain security information. ESP can be used to create a secure communication link between two sites by using a VPN tunnel that protects the data stream from unauthorized access or modification. GRE stands for Generic Routing Encapsulation, and it is a protocol that encapsulates one network protocol inside another. GRE does not provide encryption or security by itself, but it can be combined with ESP or other protocols to create a secure VPN tunnel. IKE stands for Internet Key Exchange, and it is a protocol that negotiates and establishes security associations for IPsec, which is a suite of protocols that includes ESP and AH. IKE does not encrypt or protect the data stream, but it enables the secure exchange of keys and parameters for IPsec. AH stands for Authentication Header, and it is a protocol that provides integrity and authentication for IP packets. AH does not encrypt the payload of the IP packet, which means the data stream is not confidential. AH adds a header that contains security information and a checksum that verifies the integrity of the packet.

### NEW QUESTION 305

- (Topic 3)

Which of the following is the primary function of the core layer of the three-tiered model?

- A. Routing
- B. Repeating
- C. Bridging
- D. Switching

**Answer:** A

#### **Explanation:**

<https://www.omniseu.com/cisco-certified-network-associate-ccna/three-tier-hierarchical-network-model.php>

Core Layer consists of biggest, fastest, and most expensive routers with the highest model numbers and Core Layer is considered as the back bone of networks. Core Layer routers are used to merge geographically separated networks. The Core Layer routers move information on the network as fast as possible. The switches operating at core layer switches packets as fast as possible.

### NEW QUESTION 306

- (Topic 3)

A company, which is located in a coastal town, retrofitted an office building for a new data center. The underground fiber optics were brought in and connected to the switches in the basement network MDF. A server data center was built on the fifth floor with the two rooms vertically connected by fiber optics. Which of the following types of environmental sensors is MOST needed?

- A. Temperature sensor in the network MDF
- B. Water sensor in the network MDF
- C. Temperature sensor in the data center
- D. Water sensor in the data center

**Answer: B**

**Explanation:**

A water sensor is a type of environmental sensor that detects the presence of water or moisture in an area. A water sensor is most needed in a network main distribution frame (MDF) that is located in a basement near underground fiber-optic cables. A network MDF is a central point where all the network connections converge and where network equipment such as switches and routers are located. If water leaks into the basement and damages the fiber-optic cables or the network equipment, it can cause network outages, performance degradation, or data loss. A water sensor can alert the network administrator of any water intrusion and help prevent or minimize the damage. References: <https://www.comptia.org/training/books/network-n10-008-study-guide> (page 446)

**NEW QUESTION 311**

- (Topic 3)

Which of the following network management methods is able to perform various automated tasks?

- A. SSH
- B. CLI
- C. GUI
- D. API

**Answer: D**

**Explanation:**

API stands for Application Programming Interface, which is a set of rules and protocols that allow different software applications to communicate and exchange data. Network automation can use APIs to perform various automated tasks, such as configuring devices, provisioning resources, monitoring performance, and optimizing networks. APIs can enable network automation to interact with different network elements, platforms, and services, regardless of their vendor, technology, or architecture.

The other options are not correct because:

? SSH stands for Secure Shell, which is a protocol that allows secure remote access to a network device. SSH can be used to manually configure and manage a network device, but it does not automate network tasks by itself.

? CLI stands for Command-Line Interface, which is a text-based interface that allows users to interact with a network device by typing commands. CLI can be used to manually configure and manage a network device, but it does not automate network tasks by itself.

? GUI stands for Graphical User Interface, which is a visual interface that allows users to interact with a network device by using icons, menus, and windows. GUI can be used to manually configure and manage a network device, but it does not automate network tasks by itself.

**NEW QUESTION 313**

- (Topic 3)

A network technician is troubleshooting internet connectivity issues with users in a subnet. From a host, the technician runs and then attempts to navigate to a website using a web browser.

The technician receives the following output:

```
16:35:58.756583 IP (tos 0x0, ttl 64, id 56522, offset 0, flags [DF], proto UDP (17), length 57)
  192.168.1.15.44232 > 192.168.1.252.53: 50327 + A? comptia.com. (29)
16:35:58.835371 IP (tos 0x0, ttl 64, id 56523, offset 0, flags [DF], proto UDP (17), length 57)
  192.168.1.15.44232 > 192.168.1.252.53: 50327 + A? comptia.com. (29)
16:35:59.652312 IP (tos 0x0, ttl 64, id 56524, offset 0, flags [DF], proto UDP (17), length 57)
  192.168.1.15.44232 > 192.168.1.252.53: 50327 + A? comptia.com. (29)
16:36:00.765212 IP (tos 0x0, ttl 64, id 56525, offset 0, flags [DF], proto UDP (17), length 57)
  192.168.1.15.44232 > 192.168.1.252.53: 50327 + A? comptia.com. (29)
```

Afterward, the browser displays an error. Which of the following explains this issue?

- A. A routing loop is within the network.
- B. The host is configured with incorrect DNS settings
- C. A broadcast storm is occurring on the subnet
- D. The host is missing a route to the website.

**Answer: B**

**Explanation:**

The issue is that the host is configured with incorrect DNS settings. DNS (Domain Name System) is a service that resolves domain names to IP addresses. For example, the domain name [www.comptia.org](http://www.comptia.org) is resolved to the IP address 104.18.25.140 by a DNS server. If the host has incorrect DNS settings, such as an invalid or unreachable DNS server address, it will not be able to resolve domain names to IP addresses, and therefore it will not be able to access websites by their names. The output in the image shows that the host can ping the IP address of [www.comptia.org](http://www.comptia.org), but it cannot ping the domain name itself, indicating a DNS problem. References: CompTIA Network+ N10-008 Certification Study Guide, page 154; The Official CompTIA Network+ Student Guide (Exam N10-008), page 6-8.

**NEW QUESTION 318**

- (Topic 3)

A corporation is looking for a method to secure all traffic between a branch office and its data center in order to provide a zero-touch experience for all staff members who work there. Which of the following would BEST meet this requirement?

- A. Site-to-site VPN
- B. VNC
- C. Remote desktop gateway
- D. Virtual LANs

**Answer: A**

**Explanation:**

A site-to-site VPN is a method that creates a secure and encrypted connection between two internet gateways, such as routers or firewalls, that belong to different networks<sup>1</sup>. A site-to-site VPN can secure all traffic between a branch office and its data center by creating a virtual tunnel that protects the data from interception or tampering. A site-to-site VPN can also provide a zero-touch experience for all staff members who work there, as they do not need to install any software or configure any settings on their devices to access the data center resources. They can simply use their local network as if they were physically connected to the data center network.

VNC (Virtual Network Computing) is a method that allows remote access and control of a computer's desktop from another device over a network<sup>2</sup>. VNC can enable staff members to work remotely by accessing their office computers from their home computers or mobile devices. However, VNC does not secure all traffic between a branch office and its data center, as it only works at the application layer and does not encrypt the network layer. VNC also does not provide a zero-touch experience for staff members, as they need to install software and configure settings on both the host and the client devices.

Remote desktop gateway is a method that allows remote access and control of a computer's desktop from another device over a network using the Remote Desktop Protocol (RDP). Remote desktop gateway can also enable staff members to work remotely by accessing their office computers from their home computers or mobile devices. However, remote desktop gateway does not secure all traffic between a branch office and its data center, as it only works at the application layer and does not encrypt the network layer. Remote desktop gateway also does not provide a zero-touch experience for staff members, as they need to install software and configure settings on both the host and the client devices.

Virtual LANs (VLANs) are methods that create logical subdivisions of a physical network based on criteria such as function, department, or security level. VLANs can improve network performance, security, and management by reducing broadcast domains, isolating traffic, and enforcing policies. However, VLANs do not secure all traffic between a branch office and its data center, as they only work at the data link layer and do not encrypt the network layer. VLANs also do not provide a zero-touch experience for staff members, as they need to configure settings on their network devices to join or leave a VLAN.

**NEW QUESTION 323**

- (Topic 3)

Which of the following is a cost-effective advantage of a split-tunnel VPN?

- A. Web traffic is filtered through a web filter.
- B. More bandwidth is required on the company's internet connection.
- C. Monitoring detects insecure machines on the company's network.
- D. Cloud-based traffic flows outside of the company's network.

**Answer: D**

**Explanation:**

A split-tunnel VPN is a configuration where only specific traffic is routed through a VPN, while the remaining data is sent directly over the internet. This can reduce the bandwidth consumption and cost of the company's internet connection, as cloud-based traffic does not need to pass through the VPN tunnel. A web filter, monitoring, and security are not advantages of a split-tunnel VPN, as they may require all traffic to go through the VPN.

<https://www.auvik.com/franklyit/blog/vpn-split-tunneling/>

**NEW QUESTION 324**

- (Topic 3)

A network technician is working at a new office location and needs to connect one laptop to another to transfer files. The laptops are newer models and do not have Ethernet ports. Access points are not available either. Which Of the following types Of wireless network SSIDs does the network technician need to configure to be able to connect the laptops together?

- A. Independent Basic Service Set
- B. Extended Service Set
- C. Distribution System Service
- D. Basic Service Set

**Answer: C**

**Explanation:**

An Independent Basic Service Set (IBSS) is a type of wireless network that does not require an access point or a wired network. An IBSS allows wireless devices to communicate directly with each other using ad hoc mode. An IBSS is also known as an ad hoc network or a peer-to-peer network. A network technician can configure an IBSS to connect two laptops together and transfer files.

References: Network+ Study Guide Objective 1.4: Explain the properties and characteristics of TCP/IP

**NEW QUESTION 325**

- (Topic 3)

A small office has a wireless network with several access points that are used by mobile devices. Users occasionally report that the wireless connection drops or becomes very slow. Reports confirm that this only happens when the devices are connected to the office wireless network. Which of the following is MOST likely the cause?

- A. The configuration of the encryption protocol
- B. Interference from other devices
- C. Insufficient bandwidth capacity
- D. Duplicate SSIDs

**Answer: B**

**Explanation:**

Interference from other devices can cause wireless connection drops or slow performance. This can happen when devices use the same or overlapping frequency channels as the wireless network, such as cordless phones, microwaves, Bluetooth devices, etc. To avoid interference, it is recommended to use non-overlapping channels and avoid placing wireless access points near potential sources of interference. References: Network+ Study Guide Objective 2.1: Explain the purposes and use cases for advanced network devices. Subobjective: Wireless controllers.

**NEW QUESTION 330**

- (Topic 3)

A company joins a bank's financial network and establishes a connection to the clearinghouse servers in the range 192.168.124.0/27. An IT technician then realizes the range exists within the VM pool at the data center. Which of the following is the BEST way for the technician to connect to the bank's servers?

- A. NAT
- B. PAT
- C. CIDR
- D. SLAAC

**Answer:** A

#### NEW QUESTION 335

- (Topic 3)

A network technician is deploying multiple switches for a new office. The switches are separately managed and need to be cabled in to support dual firewalls in a HA setup. Which of the following should the technician enable to support proper stability of the network switches?

- A. NTP
- B. CDMA
- C. STP
- D. LACP
- E. 802.1Q

**Answer:** C

#### Explanation:

STP stands for Spanning Tree Protocol, which is a network protocol that prevents loops in a switched network by blocking redundant links. STP allows only one active path between any two network devices, and dynamically reconfigures the network topology in case of link failures or changes. STP is essential for proper stability of the network switches, especially when they are cabled in a redundant or complex topology that involves multiple switches and firewalls. Without STP, loops can cause broadcast storms, MAC address table instability, and duplicate frames, which can degrade the network performance and availability. References: [CompTIA Network+ Certification Exam Objectives], Spanning Tree Protocol (STP) Explained | NetworkLessons.com

#### NEW QUESTION 336

- (Topic 3)

Several users with older devices are reporting intermittent connectivity while in an outdoor patio area. After some research, the network administrator determines that an outdoor WAP might help with the issue. However, the company does not want the signal to bleed into the building and cause interference. Which of the following should the network administrator perform to BEST resolve the issue?

- A. Disable the SSID broadcast on the WAP in the patio area.
- B. Install a WAP and enable 5GHz only within the patio area.
- C. Install a directional WAP in the direction of the patio.
- D. Install a repeater on the back wall of the patio area.

**Answer:** C

#### NEW QUESTION 338

- (Topic 3)

After rebooting an AP a user is no longer able to connect to the enterprise LAN. A technician plugs a laptop in to the same network jack and receives the IP 169.254.0.0. Which of the following is MOST likely causing the issue?

- A. DHCP scope exhaustion
- B. Signal attenuation
- C. Channel overlap
- D. Improper DNS configuration

**Answer:** A

#### Explanation:

DHCP scope exhaustion occurs when the number of available IP addresses to be leased from a DHCP server have been used up. This could be caused by a large number of clients on the network, or a misconfigured DHCP scope. When this happens, clients will be assigned an IP address from the APIPA range (169.254.0.0 to 169.254.255.255). To resolve this issue, the DHCP scope needs to be expanded or adjusted to accommodate the number of clients on the network.

#### NEW QUESTION 340

- (Topic 3)

While walking from the parking lot to an access-controlled door an employee sees an authorized user open the door. Then the employee notices that another person catches the door before it closes and goes inside. Which of the following attacks is taking place?

- A. Tailgating
- B. Piggybacking
- C. Shoulder surfing
- D. Phishing

**Answer:** A

#### Explanation:

The difference between piggybacking and tailgating is that with piggybacking, the person is willfully and intentionally letting you in. In this particular case, the person caught the door before it closed, so it is tailgating.

Tailgating is a physical security attack that occurs when an unauthorized person follows an authorized person through a secured door or gate without their knowledge or consent. Tailgating can allow an attacker to bypass access control mechanisms and gain entry to restricted areas or resources. Tailgating can also pose a safety risk for the authorized person and other occupants of the facility.

Piggybacking is a physical security attack that occurs when an unauthorized person follows an authorized person through a secured door or gate with their knowledge or consent. Piggybacking can also allow an attacker to bypass access control mechanisms and gain entry to restricted areas or resources.

Piggybacking can also violate security policies and compromise the accountability of the authorized person.

Shoulder surfing is a physical security attack that occurs when an unauthorized person observes or records an authorized person's confidential information, such

as passwords, PINs, or credit card numbers. Shoulder surfing can allow an attacker to steal credentials and access sensitive data or systems. Shoulder surfing can also violate privacy and confidentiality rights of the authorized person.

Phishing is a cyber security attack that occurs when an unauthorized person sends fraudulent emails or messages that appear to come from legitimate sources, such as banks, companies, or government agencies. Phishing can trick recipients into clicking on malicious links, opening malicious attachments, or providing personal or financial information. Phishing can allow an attacker to install malware, steal credentials, or perform identity theft. Phishing does not involve physical access to secured doors or gates.

**NEW QUESTION 341**

.....

## **Thank You for Trying Our Product**

### **We offer two products:**

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### **N10-008 Practice Exam Features:**

- \* N10-008 Questions and Answers Updated Frequently
- \* N10-008 Practice Questions Verified by Expert Senior Certified Staff
- \* N10-008 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* N10-008 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The N10-008 Practice Test Here](#)**