

## N10-009 Dumps

### CompTIA Network+ Exam

<https://www.certleader.com/N10-009-dumps.html>



**NEW QUESTION 1**

- (Exam Topic 1)

A company built a new building at its headquarters location. The new building is connected to the company's LAN via fiber-optic cable. Multiple users in the new building are unable to access the company's intranet site via their web browser, but they are able to access internet sites. Which of the following describes how the network administrator can resolve this issue?

- A. Correct the DNS server entries in the DHCP scope
- B. Correct the external firewall gateway address
- C. Correct the NTP server settings on the clients
- D. Correct a TFTP Issue on the company's server

**Answer:** A

**Explanation:**

If multiple users in a new building are unable to access the company's intranet site via their web browser but are able to access internet sites, the network administrator can resolve this issue by correcting the DNS server entries in the DHCP scope. The DHCP scope is responsible for assigning IP addresses and DNS server addresses to clients. If the DNS server entries are incorrect, clients will not be able to access intranet sites.

References:

> CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 4: Network Implementations, Objective 4.4: Explain the purpose and properties of DHCP.

**NEW QUESTION 2**

- (Exam Topic 1)

A technician wants to deploy a new wireless network that comprises 30 WAPs installed throughout a three-story office building. All the APs will broadcast the same SSID for client access. Which of the following BEST describes this deployment?

- A. Extended service set
- B. Basic service set
- C. Unified service set
- D. Independent basic service set

**Answer:** A

**Explanation:**

An extended service set (ESS) is a wireless network that consists of multiple access points (APs) that share the same SSID and are connected by a wired network. An ESS allows wireless clients to roam seamlessly between different APs without losing connectivity. A basic service set (BSS) is a wireless network that consists of a single AP and its associated clients. An independent basic service set (IBSS) is a wireless network that consists of a group of clients that communicate directly without an AP. A unified service set is not a standard term for a wireless network. 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://en.wikipedia.org/wiki/Service\\_set\\_\(802.11\\_network\)](https://en.wikipedia.org/wiki/Service_set_(802.11_network))

**NEW QUESTION 3**

- (Exam Topic 1)

Which of the following devices would be used to manage a corporate WLAN?

- A. A wireless NAS
- B. A wireless bridge
- C. A wireless router
- D. A wireless controller

**Answer:** D

**Explanation:**

A wireless controller is used to manage a corporate WLAN, providing centralized management and configuration of access points. References: CompTIA Network+ Certification Study Guide, Chapter 8: Wireless Networks.

**NEW QUESTION 4**

- (Exam Topic 1)

A technician is installing a high-density wireless network and wants to use an available frequency that supports the maximum number of channels to reduce interference. Which of the following standard 802.11 frequency ranges should the technician look for while reviewing WAP specifications?

- A. 2.4GHz
- B. 5GHz
- C. 6GHz
- D. 900MHz

**Answer:** B

**Explanation:**

\* 802.11 a/b/g/n/ac wireless networks operate in two frequency ranges: 2.4 GHz and 5 GHz. The 5 GHz frequency range supports more channels than the 2.4 GHz frequency range, making it a better choice for high-density wireless networks.

References: CompTIA Network+ Certification Study Guide, Sixth Edition by Glen E. Clarke

**NEW QUESTION 5**

- (Exam 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 6**

- (Exam Topic 1)

The management team needs to ensure unnecessary modifications to the corporate network are not permitted and version control is maintained. Which of the following documents would BEST support this?

- A. An incident response plan
- B. A business continuity plan
- C. A change management policy
- D. An acceptable use policy

**Answer:** C

**Explanation:**

A change management policy is a document that outlines the procedures and guidelines for making changes to a network or system, including how changes are approved, tested, and implemented. By following a change management policy, organizations can ensure that unnecessary modifications to the network are not permitted and version control is maintained. References:

➤ Network+ N10-008 Objectives: 1.6 Given a scenario, implement network configuration and change management best practices.

**NEW QUESTION 7**

- (Exam Topic 1)

Access to a datacenter should be individually recorded by a card reader even when multiple employees enter the facility at the same time. Which of the following allows the enforcement of this policy?

- A. Motion detection
- B. Access control vestibules
- C. Smart lockers
- D. Cameras

**Answer:** B

**Explanation:**

The most effective security mechanism against physical intrusions due to stolen credentials would likely be a combination of several of these options. However, of the options provided, the most effective security mechanism would probably be an access control vestibule. An access control vestibule is a secure area that is located between the outer perimeter of a facility and the inner secure area. It is designed to provide an additional layer of security by requiring that individuals pass through a series of security checks before being allowed access to the secure area. This could include biometric authentication, access card readers, and motion detection cameras.

Access control vestibules allow the enforcement of the policy that access to a datacenter should be individually recorded by a card reader even when multiple employees enter the facility at the same time. An access control vestibule is a physical security device that consists of two doors with an interlocking mechanism. Only one door can be opened at a time, and only one person can pass through each door. This prevents tailgating or piggybacking, where unauthorized persons follow authorized persons into a secure area. An access control vestibule can also be integrated with a card reader or other authentication system to record each individual's access. References: <https://www.boonedam.us/blog/what-are-access-control-vestibules>

**NEW QUESTION 8**

- (Exam Topic 1)

A technician is installing a new fiber connection to a network device in a datacenter. The connection from the device to the switch also traverses a patch panel connection. The chain of connections is in the following order:

Device  
LC/LC patch cable Patch panel  
Cross-connect fiber cable Patch panel  
LC/LC patch cable Switch

The connection is not working. The technician has changed both patch cables with known working patch cables. The device had been tested and was working properly before being installed. Which of the following is the MOST likely cause of the issue?

- A. TX/RX is reversed
- B. An incorrect cable was used
- C. The device failed during installation
- D. Attenuation is occurring

**Answer:** A

**Explanation:**

The most likely cause of the issue where the fiber connection from a device to a switch is not working is that the TX/RX (transmit/receive) is reversed. When connecting fiber optic cables, it is important to ensure that the TX of one device is connected to the RX of the other device and vice versa. If the TX/RX is reversed, data cannot be transmitted successfully.

References:

➤ CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 5: Network Operations, Objective 5.1: Given a scenario, use appropriate documentation and diagrams to manage the network.

**NEW QUESTION 9**

- (Exam Topic 1)

Several WIFI users are reporting the inability to connect to the network. WLAN users on the guest network are able to access all network resources without any performance issues. The following table summarizes the findings after a site survey of the area in question:

Location	AP 1	AP 2	AP 3	AP 4
SSID	Corp1	Corp1	Corp1/Guest	Corp1/Guest
Channel	2	1	5	11
RSSI	-81dBm	-82dBm	-44dBm	-41dBm
Antenna type	Omni	Omni	Directional	Directional

Which of the following should a wireless technician do NEXT to troubleshoot this issue?

- A. Reconfigure the channels to reduce overlap
- B. Replace the omni antennas with directional antennas
- C. Update the SSIDs on all the APs
- D. Decrease power in AP 3 and AP 4

**Answer: A**

**Explanation:**

Based on the site survey table, we can see that AP 2, AP 3, and AP 4 are all broadcasting on the same channel, which can cause interference and affect performance. Therefore, the next step a wireless technician should take to troubleshoot this issue is to reconfigure the channels to reduce overlap. This will help to improve network performance and eliminate any interference.

References:

➤ Network+ N10-007 Certification Exam Objectives, Objective 2.8: Given a scenario, troubleshoot common wireless problems and perform site surveys.

**NEW QUESTION 10**

- (Exam 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 10**

- (Exam Topic 1)

A new cabling certification is being requested every time a network technician rebuilds one end of a Cat 6 (vendor-certified) cable to create a crossover connection that is used to connect switches. Which of the following would address this issue by allowing the use of the original cable?

- A. CSMA/CD
- B. LACP
- C. PoE+
- D. MDIX

**Answer: D**

**Explanation:**

MDIX (medium-dependent interface crossover) is a feature that allows network devices to automatically detect and configure the appropriate cabling type, eliminating the need for crossover cables. By enabling MDIX on the switches, a technician can use the original Cat 6 cable to create a crossover connection. References: CompTIA Network+ Certification Study Guide, Sixth Edition by Glen E. Clarke

**NEW QUESTION 15**

- (Exam Topic 1)

Within the realm of network security, Zero Trust:

- A. prevents attackers from moving laterally through a system.
- B. allows a server to communicate with outside networks without a firewall.
- C. block malicious software that is too new to be found in virus definitions.
- D. stops infected files from being downloaded via websites.

**Answer: A**

**Explanation:**

Zero Trust is a security framework that requires all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. Zero Trust prevents attackers from moving laterally through a system by applying granular policies and controls based on the principle of least privilege and by segmenting and encrypting data flows across the network. 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.crowdstrike.com/cybersecurity-101/zero-trust-security/>

**NEW QUESTION 16**

- (Exam Topic 1)

A technician is deploying a new switch model and would like to add it to the existing network monitoring software. The technician wants to know what metrics can be gathered from a given switch. Which of the following should the technician utilize for the switch?

- A. MIB
- B. Trap
- C. Syslog
- D. Audit log

**Answer:** A

**Explanation:**

To determine what metrics can be gathered from a given switch, a technician should utilize the Management Information Base (MIB). The MIB is a database of network management information that is used to manage and monitor network devices. It contains information about device configuration, status, and performance. References: Network+ Certification Study Guide, Chapter 5: Network Security

**NEW QUESTION 21**

- (Exam Topic 1)

A client recently added 100 users who are using VMs. All users have since reported slow or unresponsive desktops. Reports show minimal network congestion, zero packet loss, and acceptable packet delay. Which of the following metrics will MOST accurately show the underlying performance issues? (Choose two.)

- A. CPU usage
- B. Memory
- C. Temperature
- D. Bandwidth
- E. Latency
- F. Jitter

**Answer:** AB

**NEW QUESTION 26**

- (Exam Topic 1)

A network administrator is designing a new datacenter in a different region that will need to communicate to the old datacenter with a secure connection. Which of the following access methods would provide the BEST security for this new datacenter?

- A. Virtual network computing
- B. Secure Socket Shell
- C. In-band connection
- D. Site-to-site VPN

**Answer:** D

**Explanation:**

Site-to-site VPN provides the best security for connecting a new datacenter to an old one because it creates a secure tunnel between the two locations, protecting data in transit. References: CompTIA Network+ Certification Study Guide, Chapter 5: Network Security.

**NEW QUESTION 30**

- (Exam Topic 1)

A network technician is reviewing the interface counters on a router interface. The technician is attempting to confirm a cabling issue. Given the following information:

Metric	Value
Last cleared	7 minutes, 34 seconds
# of packets output	6915
# of packets input	270
CRCs	183
Giants	0
Runts	0
Multicasts	14

Which of the following metrics confirms there is a cabling issue?

- A. Last cleared
- B. Number of packets output
- C. CRCs
- D. Giants
- E. Multicasts

**Answer:** C

**Explanation:**

CRC stands for Cyclic Redundancy Check, and it is a type of error-detecting code used to detect accidental changes to raw data. If the CRC count is increasing on a particular interface, it indicates that there might be an issue with the cabling, which is causing data corruption. References:

➤ Network+ N10-008 Objectives: 2.1 Given a scenario, troubleshoot common physical connectivity issues.

**NEW QUESTION 31**

- (Exam Topic 1)

A network is experiencing a number of CRC errors during normal network communication. At which of the following layers of the OSI model will the administrator MOST likely start to troubleshoot?

- A. Layer 1
- B. Layer 2
- C. Layer 3
- D. Layer 4
- E. Layer 5
- F. Layer 6
- G. Layer 7

**Answer:** A

**Explanation:**

CRC errors are cyclic redundancy check errors that occur when data is corrupted during transmission. CRC errors are usually caused by physical layer issues such as faulty cables, connectors, ports, or interference. The network administrator will most likely start to troubleshoot at layer 1 of the OSI model, which is the physical layer that deals with the transmission of bits over a medium. References: CompTIA Network+ Certification Exam Objectives Version 2.0 (Exam Number: N10-006), Domain 4.0 Network Troubleshooting and Tools, Objective 4.1 Given a scenario, implement network troubleshooting methodology.

**NEW QUESTION 34**

- (Exam 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 37**

- (Exam Topic 1)

Which of the following is the physical topology for an Ethernet LAN?

- A. Bus
- B. Ring
- C. Mesh
- D. Star

**Answer:** D

**Explanation:**

In a star topology, all devices on a network connect to a central hub or switch, which acts as a common connection point. Ethernet LANs typically use a star topology, with each device connected to a central switch. References:

➤ Network+ N10-008 Objectives: 2.2 Explain common logical network topologies and their characteristics.

**NEW QUESTION 41**

- (Exam Topic 1)

**SIMULATION**

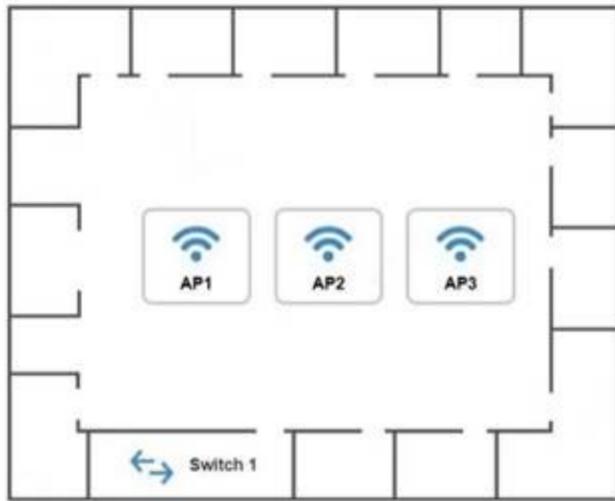
You have been tasked with setting up a wireless network in an office. The network will consist of 3 Access Points and a single switch. The network must meet the following parameters:

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.



**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:   
B  
G

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

**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:

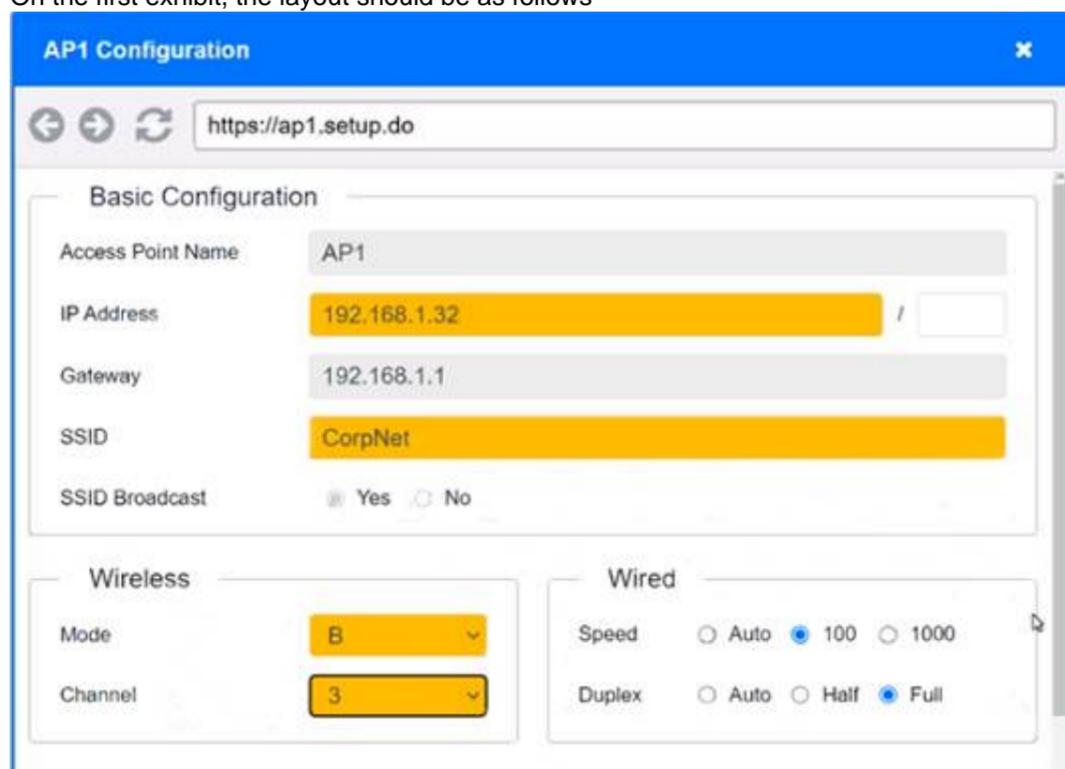
Reset to Default Save Close

- A. Mastered
- B. Not Mastered

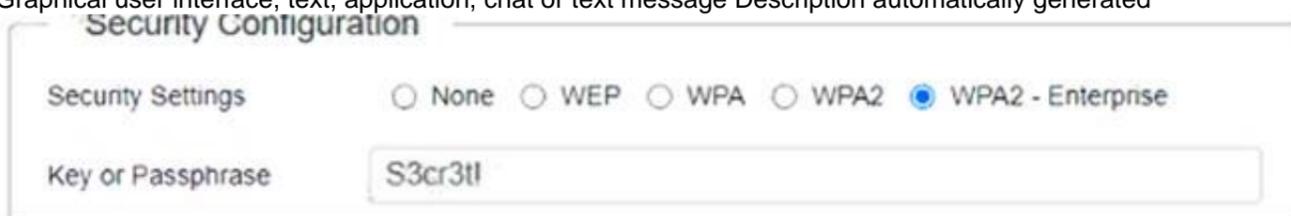
Answer: A

**Explanation:**

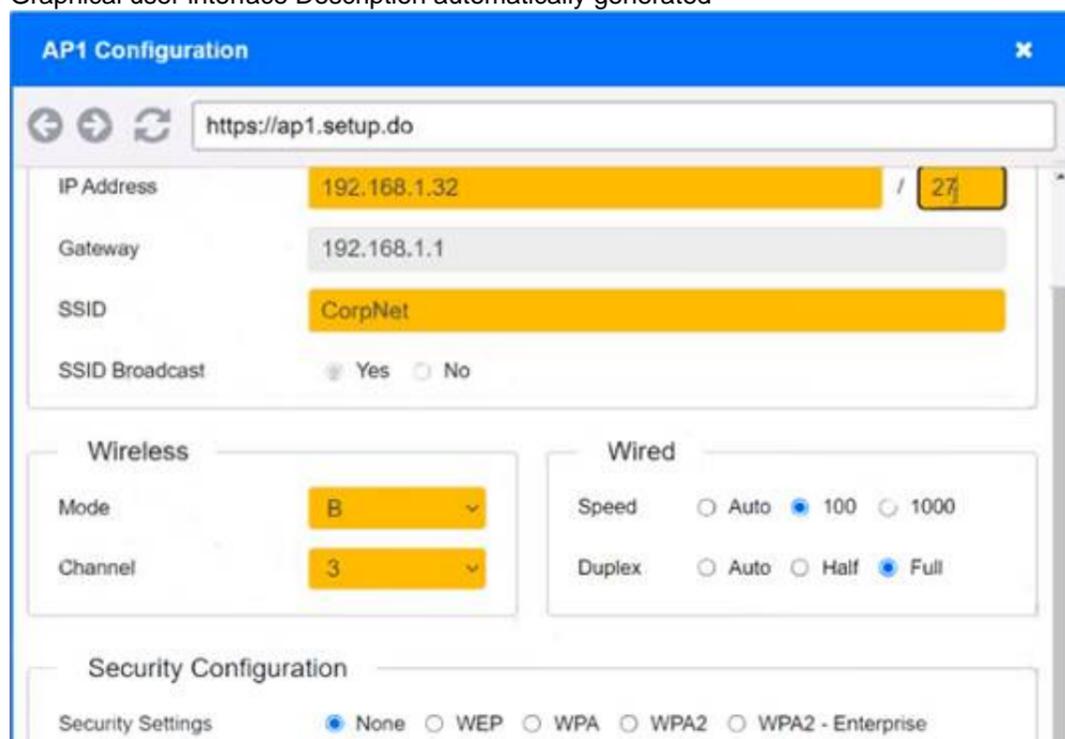
On the first exhibit, the layout should be as follows



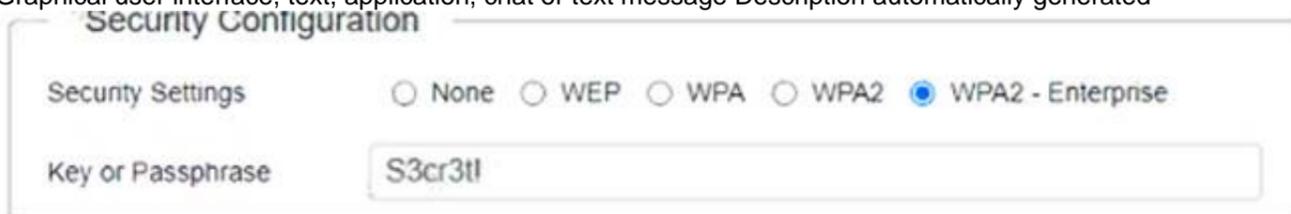
Graphical user interface, text, application, chat or text message Description automatically generated



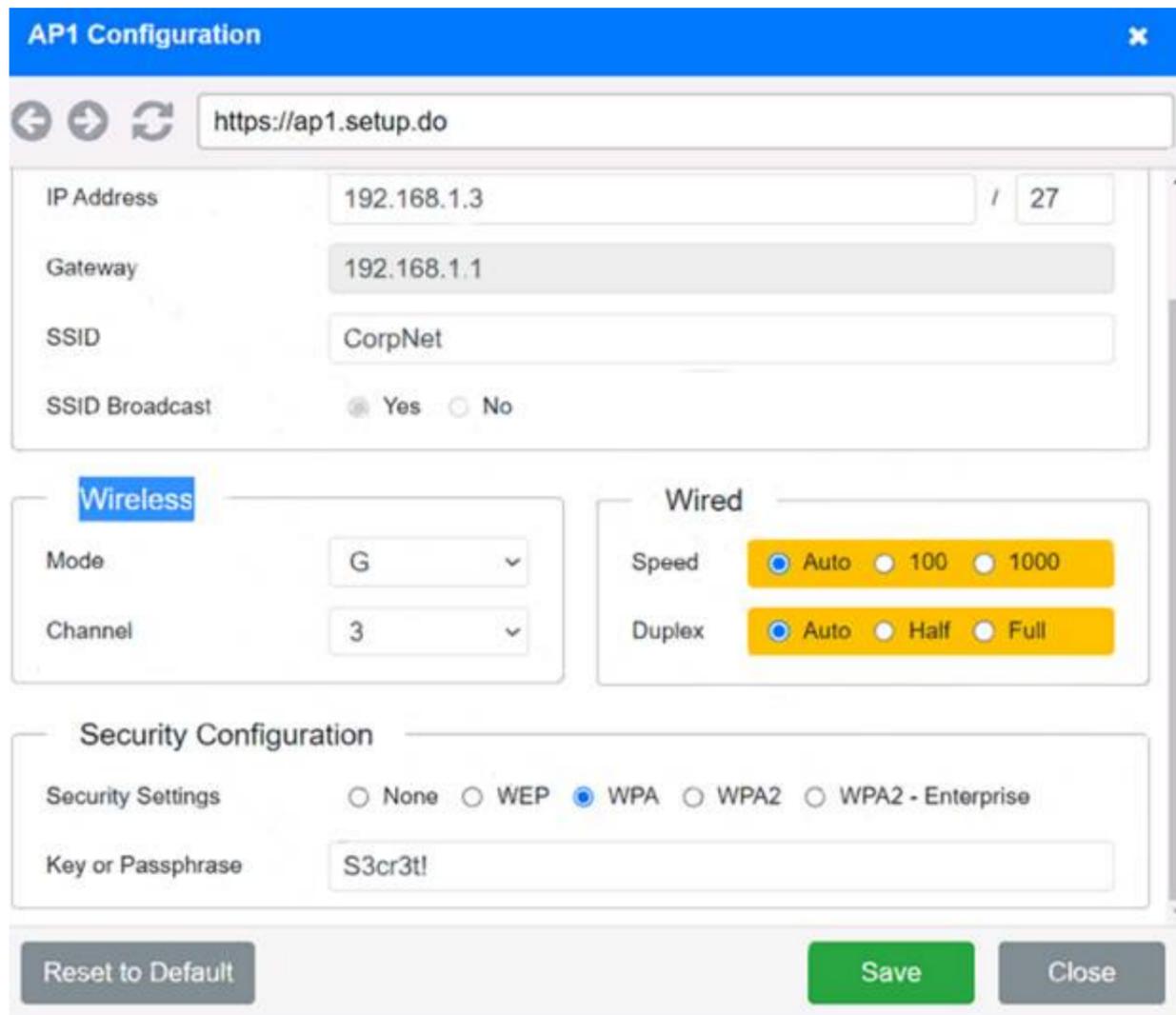
Graphical user interface Description automatically generated



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

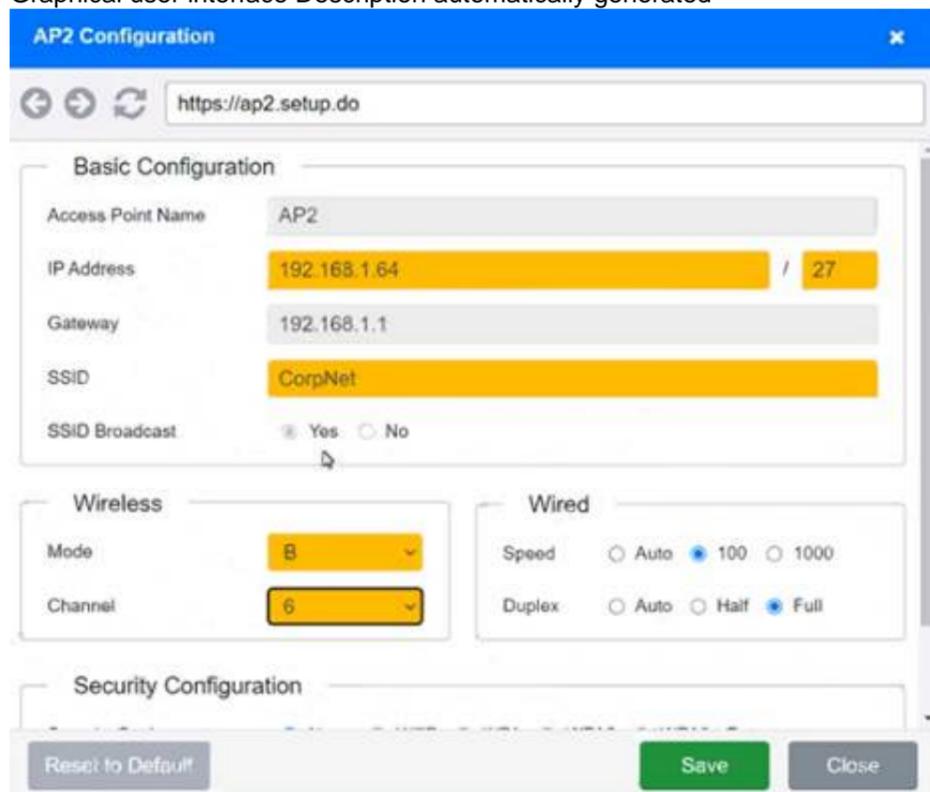


Graphical user interface Description automatically generated



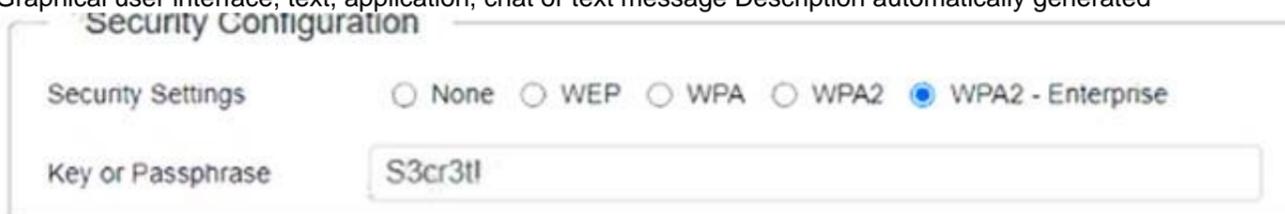
The screenshot shows the 'AP1 Configuration' web interface. At the top, there is a blue header with the title and a close button. Below the header is a navigation bar with back, forward, and refresh icons, and a URL field containing 'https://ap1.setup.do'. The main configuration area is divided into several sections: 'Basic Configuration' with fields for IP Address (192.168.1.3), Gateway (192.168.1.1), SSID (CorpNet), and SSID Broadcast (Yes/No); 'Wireless' settings with Mode (G) and Channel (3); 'Wired' settings with Speed (Auto, 100, 1000) and Duplex (Auto, Half, Full); and 'Security Configuration' with Security Settings (None, WEP, WPA, WPA2, WPA2 - Enterprise) and a Key or Passphrase field (S3cr3t!). At the bottom, there are three buttons: 'Reset to Default', 'Save', and 'Close'.

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



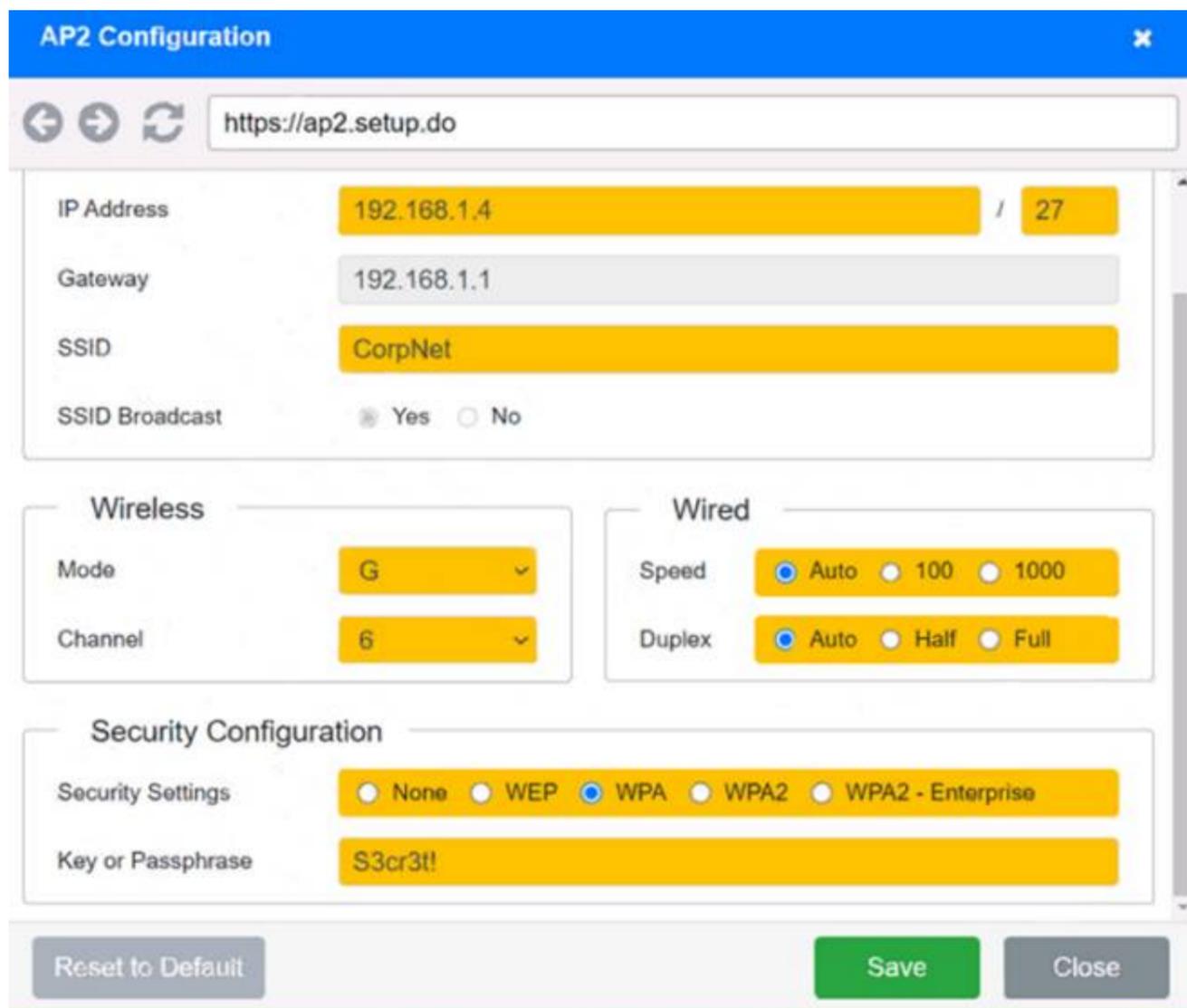
The screenshot shows the 'AP2 Configuration' web interface. It has a similar layout to AP1, with a blue header and a navigation bar. The 'Basic Configuration' section includes fields for Access Point Name (AP2), IP Address (192.168.1.64), Gateway (192.168.1.1), SSID (CorpNet), and SSID Broadcast (Yes/No). The 'Wireless' section shows Mode (B) and Channel (6). The 'Wired' section shows Speed (Auto, 100, 1000) and Duplex (Auto, Half, Full). The 'Security Configuration' section is partially visible at the bottom. Buttons for 'Reset to Default', 'Save', and 'Close' are at the bottom.

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



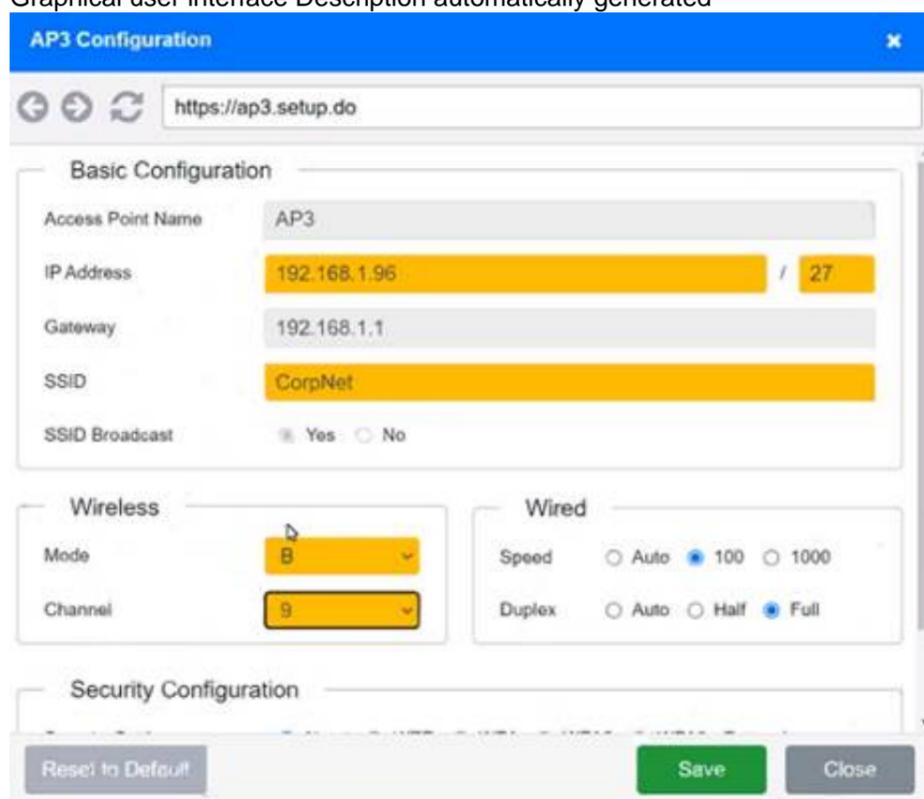
This is a close-up of the 'Security Configuration' section from the AP2 configuration page. It shows 'Security Settings' with radio buttons for None, WEP, WPA, WPA2, and WPA2 - Enterprise (which is selected). Below it is a 'Key or Passphrase' field containing the text 'S3cr3t!'.

Graphical user interface Description automatically generated



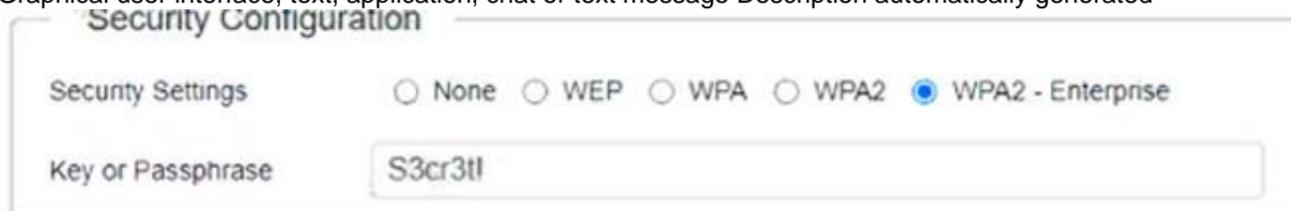
The screenshot shows the 'AP2 Configuration' web interface. At the top, there is a navigation bar with a blue header and a close button. Below it is a browser address bar showing 'https://ap2.setup.do'. The main configuration area is divided into several sections: 'Basic Configuration' with fields for IP Address (192.168.1.4), Gateway (192.168.1.1), SSID (CorpNet), and SSID Broadcast (Yes); 'Wireless' section with Mode (G) and Channel (6); 'Wired' section with Speed (Auto) and Duplex (Auto); and 'Security Configuration' with Security Settings (WPA) and Key or Passphrase (S3cr3t!). At the bottom, there are three buttons: 'Reset to Default', 'Save', and 'Close'.

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



The screenshot shows the 'AP3 Configuration' web interface. It has a similar layout to AP2. The 'Basic Configuration' section shows Access Point Name (AP3), IP Address (192.168.1.96), Gateway (192.168.1.1), SSID (CorpNet), and SSID Broadcast (Yes). The 'Wireless' section shows Mode (B) and Channel (9). The 'Wired' section shows Speed (100) and Duplex (Full). The 'Security Configuration' section is partially visible at the bottom. Buttons for 'Reset to Default', 'Save', and 'Close' are at the bottom.

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



This is a close-up of the 'Security Configuration' section from the AP3 interface. It shows 'Security Settings' with radio buttons for None, WEP, WPA, WPA2, and WPA2 - Enterprise (which is selected). Below it is a text field for 'Key or Passphrase' containing the text 'S3cr3t!'.

Graphical user interface Description automatically generated

The screenshot shows the AP3 Configuration web interface. The browser address bar displays `https://ap3.setup.do`. The configuration fields are as follows:

- IP Address:** 192.168.1.5 / 27
- Gateway:** 192.168.1.1
- SSID:** CorpNet
- SSID Broadcast:**  Yes  No
- Wireless Mode:** G
- Wireless Channel:** 9
- Wired Speed:**  Auto  100  1000
- Wired Duplex:**  Auto  Half  Full
- Security Settings:**  None  WEP  WPA  WPA2  WPA2 - Enterprise
- Key or Passphrase:** S3cr3t!

At the bottom, there are three buttons: "Reset to Default", "Save", and "Close".

**NEW QUESTION 43**

- (Exam Topic 1)

A network administrator walks into a datacenter and notices an unknown person is following closely. The administrator stops and directs the person to the security desk. Which of the following attacks did the network administrator prevent?

- A. Evil twin
- B. Tailgating
- C. Piggybacking
- D. Shoulder surfing

**Answer: B**

**Explanation:**

: Tailgating is a physical security attack where an unauthorized person follows an authorized person into a restricted area without proper identification or authorization. The network administrator prevented this attack by stopping and directing the person to the security desk. References: CompTIA Network+ Certification Exam Objectives Version 2.0 (Exam Number: N10-006), Domain 3.0 Network Security, Objective 3.1 Compare and contrast risk-related concepts.

**NEW QUESTION 46**

- (Exam Topic 1)

A user reports being unable to access network resources after making some changes in the office. Which of the following should a network technician do FIRST?

- A. Check the system's IP address
- B. Do a ping test against the servers
- C. Reseat the cables into the back of the PC
- D. Ask what changes were made

**Answer: D**

**Explanation:**

When a user reports being unable to access network resources after making some changes, the network technician should first ask the user what changes were made. This information can help the technician identify the cause of the issue and determine the appropriate course of action. References: CompTIA Network+ Certification Study Guide, Sixth Edition by Glen E. Clarke

**NEW QUESTION 50**

- (Exam 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:**

\* 802.11 ax 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 55**

- (Exam Topic 1)

Which of the following is MOST likely to generate significant East-West traffic in a datacenter?

- A. A backup of a large video presentation to cloud storage for archival purposes
- B. A duplication of a hosted virtual server to another physical server for redundancy
- C. A download of navigation data to a portable device for offline access
- D. A query from an IoT device to a cloud-hosted server for a firmware update

**Answer: B**

**Explanation:**

East-West traffic refers to data flows between servers or devices within the same datacenter. When a hosted virtual server is duplicated to another physical server for redundancy, it generates significant East-West traffic as the data is replicated between the two servers. References:

> Network+ N10-008 Objectives: 3.3 Given a scenario, implement secure network architecture concepts.

**NEW QUESTION 57**

- (Exam 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 62**

- (Exam Topic 1)

The following configuration is applied to a DHCP server connected to a VPN concentrator:

```
IP address:      10.0.0.1
Subnet mask:    255.255.255.0
Gateway:       10.0.0.254
```

There are 300 non-concurrent sales representatives who log in for one hour a day to upload reports, and 252 of these representatives are able to connect to the VPN without any issues. The remaining sales representatives cannot connect to the VPN over the course of the day. Which of the following can be done to resolve the issue without utilizing additional resources?

- A. Decrease the lease duration
- B. Reboot the DHCP server
- C. Install a new VPN concentrator
- D. Configure a new router

**Answer: A**

**Explanation:**

Decreasing the lease duration on the DHCP server will cause clients to renew their IP address leases more frequently, freeing up IP addresses for other clients to use. References: CompTIA Network+ Certification Study Guide, Chapter 3: IP Addressing.

**NEW QUESTION 65**

- (Exam Topic 1)

A network technician is manually configuring the network settings for a new device and is told the network block is 192.168.0.0/20. Which of the following subnets should the technician use?

- A. 255.255.128.0
- B. 255.255.192.0
- C. 255.255.240.0
- D. 255.255.248.0

**Answer: C**

**Explanation:**

A subnet mask is a binary number that indicates which bits of an IP address belong to the network portion and which bits belong to the host portion. A slash notation (/n) indicates how many bits are used for the network portion. A /20 notation means that 20 bits are used for the network portion and 12 bits are used for the host portion. To convert /20 to a dotted decimal notation, we need to write 20 ones followed by 12 zeros in binary and then divide them into four octets separated by dots. This gives us 11111111.11111111.11110000.00000000 or 255.255.240.0 in decimal. 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/950/subnet->

mask

**NEW QUESTION 70**

- (Exam Topic 2)

A SaaS provider has decided to leave an unpatched VM available via a public DMZ port. With which of the following concepts is this technique MOST closely associated?

- A. Insider threat
- B. War driving
- C. Evil twin
- D. Honeypot

**Answer: D**

**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. In the scenario, the SaaS provider has left an unpatched VM available via a public DMZ port, which could be a honeypot technique to lure attackers and monitor their activities. References: <https://www.comptia.org/blog/what-is-a-honey-pot>

**NEW QUESTION 75**

- (Exam Topic 2)

A network technician is observing the behavior of an unmanaged switch when a new device is added to the network and transmits data. Which of the following BEST describes how the switch processes this information?

- A. The data is flooded out of every port
- B. including the one on which it came in.
- C. The data is flooded out of every port but only in the VLAN where it is located.
- D. The data is flooded out of every port, except the one on which it came in
- E. The data is flooded out of every port, excluding the VLAN where it is located

**Answer: C**

**Explanation:**

The switch processes the data by flooding it out of every port, except the one on which it came in. Flooding is a process where a switch sends a data frame to all ports except the source port when it does not have an entry for the destination MAC address in its MAC address table. Flooding allows the switch to learn the MAC addresses of the devices connected to its ports and update its MAC address table accordingly. Flooding also ensures that the data frame reaches its intended destination, even if the switch does not know its location. References: <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10556-16.html>

**NEW QUESTION 76**

- (Exam 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 DNS 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 81**

- (Exam Topic 2)

A corporation has a critical system that would cause unrecoverable damage to the brand if it was taken offline. Which of the following disaster recovery solutions should the corporation implement?

- A. Full backups
- B. Load balancing
- C. Hot site
- D. Snapshots

**Answer: C**

**Explanation:**

A hot site is the disaster recovery solution that the corporation should implement for its critical system that would cause unrecoverable damage to the brand if it was taken offline. A hot site is a fully operational backup site that can take over the primary site's functions in case of a disaster or disruption. A hot site has all the necessary hardware, software, data, network connections, and personnel to resume normal operations with minimal downtime. A hot site is suitable for systems that require high availability and cannot afford any data loss or interruption. References: <https://www.enterprisestorageforum.com/management/disaster-recovery-site/> 1

**NEW QUESTION 84**

- (Exam Topic 2)

Which of the following is used to provide networking capability for VMs at Layer 2 of the OSI model?

- A. VPN
- B. VRRP
- C. vSwitch
- D. VIP

**Answer: C**

**Explanation:**

A vSwitch (virtual switch) is a software-based switch that provides networking capability for VMs (virtual machines) at Layer 2 of the OSI model. It connects the VMs to each other or to external networks using virtual NICs (network interface cards). A VPN (virtual private network) is a technology that creates a secure tunnel over a public network for remote access or site-to-site connectivity. VRRP (Virtual Router Redundancy Protocol) is a protocol that provides high availability for routers by creating a virtual router with multiple physical routers. A VIP (virtual IP) is an IP address that can be shared by multiple servers or devices for load balancing or failover purposes.

**NEW QUESTION 89**

- (Exam Topic 2)

A network administrator is reviewing interface errors on a switch. Which of the following indicates that a switchport is receiving packets in excess of the configured MTU?

- A. CRC errors
- B. Giants
- C. Runts
- D. Flooding

**Answer: B**

**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 94**

- (Exam Topic 2)

A network administrator is downloading a large patch that will be uploaded to several enterprise switches simultaneously during the day's upgrade cycle. Which of the following should the administrator do to help ensure the upgrade process will be less likely to cause problems with the switches?

- A. Confirm the patch's MD5 hash prior to the upgrade
- B. Schedule the switches to reboot after an appropriate amount of time.
- C. Download each switch's current configuration before the upgrade
- D. Utilize FTP rather than TFTP to upload the patch

**Answer: A**

**Explanation:**

The network administrator should confirm the patch's MD5 hash prior to the upgrade to help ensure the upgrade process will be less likely to cause problems with the switches. MD5 (Message Digest 5) is a cryptographic hash function that produces a 128-bit hash value for any given input. It can be used to verify the integrity and authenticity of a file by comparing its hash value with a known or expected value. If the hash values match, it means that the file has not been corrupted or tampered with during transmission or storage. If the hash values do not match, it means that the file may be damaged or malicious and should not be used for the upgrade. References:

<https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/15292-scp.html>

**NEW QUESTION 97**

- (Exam Topic 2)

There are two managed legacy switches running that cannot be replaced or upgraded. These switches do not support cryptographic functions, but they are password protected. Which of the following should a network administrator configure to BEST prevent unauthorized access?

- A. Enable a management access list
- B. Disable access to unnecessary services.
- C. Configure a stronger password for access
- D. Disable access to remote management
- E. Use an out-of-band access method.

**Answer: E**

**Explanation:**

Using an out-of-band access method is the best way to prevent unauthorized access to the legacy switches that do not support cryptographic functions. Out-of-band access is a method of accessing a network device through a dedicated channel that is separate from the main network traffic. Out-of-band access can use physical connections such as serial console ports or dial-up modems, or logical connections such as VPNs or firewalls. Out-of-band access provides more security and reliability than in-band access, which uses the same network as the data traffic and may be vulnerable to attacks or failures. References:

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/configuration/15mt/fundamentals-15-mt-book/>

**NEW QUESTION 99**

- (Exam Topic 2)

A lab environment hosts Internet-facing web servers and other experimental machines, which technicians use for various tasks. A technician installs software on one of the web servers to allow communication to the company's file server, but it is unable to connect to it. Other machines in the building are able to retrieve files from the file server. Which of the following is the MOST likely reason the web server cannot retrieve the files, and what should be done to resolve the problem?

- A. The lab environment's IDS is blocking the network traffic. The technician can whitelist the new application in the IDS.
- B. The lab environment is located in the DMZ, and traffic to the LAN zone is denied by default.
- C. The technician can move the computer to another zone or request an exception from the administrator.
- D. The lab environment has lost connectivity to the company router, and the switch needs to be rebooted. The technician can get the key to the wiring closet and manually restart the switch.
- E. The lab environment is currently set up with hubs instead of switches, and the requests are getting bounced back. The technician can submit a request for upgraded equipment to management.

**Answer: B**

**Explanation:**

The lab environment is located in the DMZ, and traffic to the LAN zone is denied by default. This is the most likely reason why the web server cannot retrieve files from the file server, and the technician can either move the computer to another zone or request an exception from the administrator to resolve the problem. A DMZ (Demilitarized Zone) is a network segment that separates the internal network (LAN) from the external network (Internet). It usually hosts public-facing servers such as web servers, email servers, or FTP servers that need to be accessed by both internal and external users. A firewall is used to control the traffic between the DMZ and the LAN zones, and usually denies traffic from the DMZ to the LAN by default for security reasons. Therefore, if a web server in the DMZ needs to communicate with a file server in the LAN, it would need a special rule or permission from the firewall administrator. References: <https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html>

**NEW QUESTION 100**

- (Exam Topic 2)

Which of the following protocol types describes secure communication on port 443?

- A. ICMP
- B. UDP
- C. TCP
- D. IP

**Answer: C**

**Explanation:**

TCP is the protocol type that describes secure communication on port 443. TCP (Transmission Control Protocol) is a connection-oriented protocol that provides reliable and ordered delivery of data packets over an IP network. TCP uses port numbers to identify different applications or services on a device. Port 443 is the default port for HTTPS (Hypertext Transfer Protocol Secure), which is an extension of HTTP that uses SSL (Secure Sockets Layer) or TLS (Transport Layer Security) encryption to protect data in transit between a web server and a web browser. References: <https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html>

**NEW QUESTION 102**

- (Exam Topic 2)

An ARP request is broadcasted and sends the following request. "Who is 192.168.1.200? Tell 192.168.1.55"

At which of the following layers of the OSI model does this request operate?

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

**Answer: B**

**Explanation:**

An ARP request operates at the data link layer of the OSI model. ARP (Address Resolution Protocol) is a protocol that maps IP addresses to MAC addresses on a local area network. It allows devices to communicate with each other without knowing their MAC addresses beforehand. ARP operates at the data link layer (layer 2) of the OSI model, which is responsible for framing and addressing data packets on a physical medium. References: <https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html>

**NEW QUESTION 104**

- (Exam Topic 2)

A user reports a weak signal when walking 20ft (6.1 m) away from the WAP in one direction, but a strong signal when walking 20ft in the opposite direction. The technician has reviewed the configuration and confirmed the channel type is correct. There is no jitter or latency on the connection. Which of the following would be the MOST likely cause of the issue?

- A. Antenna type
- B. Power levels
- C. Frequency
- D. Encryption type

**Answer: A**

**Explanation:**

The antenna type affects the signal strength and coverage of a WAP. Different types of antennas have different radiation patterns and gain, which determine how far and wide the signal can reach. If the user experiences a weak signal in one direction but a strong signal in the opposite direction, it could mean that the antenna type is not suitable for the desired coverage area. The technician should consider changing the antenna type to one that has a more balanced or directional

radiation pattern. References:

<https://community.cisco.com/t5/wireless-small-business/wap200-poor-signal-strength/td-p/1565796>

**NEW QUESTION 106**

- (Exam Topic 2)

Which of the following attacks encrypts user data and requires a proper backup implementation to recover?

- A. DDoS
- B. Phishing
- C. Ransomware
- D. MAC spoofing

**Answer: C**

**Explanation:**

Ransomware is a type of malware that encrypts user data and demands a ransom for its decryption. Ransomware can prevent users from accessing their files and applications, and cause data loss or corruption. A proper backup implementation is essential to recover from a ransomware attack, as it can help restore the encrypted data without paying the ransom or relying on the attackers' decryption key. References: <https://www.comptia.org/blog/what-is-ransomware>

**NEW QUESTION 110**

- (Exam Topic 2)

A local firm has hired a consulting company to clean up its IT infrastructure. The consulting company notices remote printing is accomplished by port forwarding via publicly accessible IPs through the firm's firewall. Which of the following would be the MOST appropriate way to enable secure remote printing?

- A. SSH
- B. VPN
- C. Telnet
- D. SSL

**Answer: B**

**Explanation:**

VPN (Virtual Private Network) is the most appropriate way to enable secure remote printing. VPN is a technology that creates a secure and encrypted tunnel over a public network such as the Internet. It allows remote users or sites to access a private network as if they were directly connected to it. VPN can be used for various purposes such as accessing corporate resources, bypassing geo-restrictions, or enhancing privacy and security. VPN can also be used for remote printing by allowing users to connect to a printer on the private network and send print jobs securely over the VPN tunnel. References: <https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-work>

**NEW QUESTION 112**

- (Exam Topic 2)

A company is being acquired by a large corporation. As part of the acquisition process, the company's address should now redirect clients to the corporate organization page. Which of the following DNS records needs to be created?

- A. SOA
- B. NS
- C. CNAME
- D. TXT

**Answer: C**

**Explanation:**

Reference:

<https://www.namecheap.com/support/knowledgebase/article.aspx/9604/2237/types-of-domain-redirects-301-302>

CNAME (Canonical Name) is a type of DNS record that maps an alias name to another name, which can be either another alias or the canonical name of a host or domain. A CNAME record can be used to redirect clients from one domain name to another domain name, such as from the company's address to the corporate organization page. SOA (Start of Authority) is a type of DNS record that specifies authoritative information about a DNS zone, such as the primary name server, contact email address, serial number, refresh interval, etc., which does not redirect clients to another domain name. NS (Name Server) is a type of DNS record that specifies which name server is authoritative for a domain or subdomain, which does not redirect clients to another domain name. TXT (Text) is a type of DNS record that provides arbitrary text information about a domain or subdomain, such as SPF (Sender Policy Framework) records or DKIM (DomainKeys Identified Mail) records, which does not redirect clients to another domain name.

**NEW QUESTION 114**

- (Exam Topic 2)

Given the following output:

```
192.168.22.1    00-13-5d-00-e6-23
192.168.22.15  00-15-88-00-58-00
192.168.22.10  00-13-5d-00-e6-23
192.168.22.100 00-13-5d-00-e6-23
```

Which of the following attacks is this MOST likely an example of?

- A. ARP poisoning
- B. VLAN hopping
- C. Rogue access point
- D. Amplified DoS

**Answer: A**

**Explanation:**

The output is most likely an example of an ARP poisoning attack. ARP poisoning, also known as ARP spoofing, is a type of attack that exploits the ARP protocol to associate a malicious device's MAC address with a legitimate IP address on a local area network. This allows the attacker to intercept, modify, or redirect network traffic between two devices without their knowledge. The output shows that there are multiple entries for the same IP address (192.168.1.1) with different MAC addresses in the ARP cache of the device. This indicates that an attacker has sent fake ARP replies to trick the device into believing that its MAC address is associated with the IP address of another device (such as the default gateway). References: <https://www.cisco.com/c/en/us/about/security-center/arp-spoofing.html>

**NEW QUESTION 117**

- (Exam Topic 2)

A network administrator decided to use SLAAC in an extensive IPv6 deployment to alleviate IP address management. The devices were properly connected into the LAN but autoconfiguration of the IP address did not occur as expected. Which of the following should the network administrator verify?

- A. The network gateway is configured to send router advertisements.
- B. A DHCP server is present on the same broadcast domain as the clients.
- C. The devices support dual stack on the network layer.
- D. The local gateway supports anycast routing.

**Answer:** A

**Explanation:**

SLAAC (Stateless Address Autoconfiguration) is a method for IPv6 devices to automatically configure their IP addresses based on the network prefix advertised by a router. The router sends periodic router advertisements (RAs) that contain the network prefix and other parameters for the devices to use. If the network gateway is not configured to send RAs, then SLAAC will not work. A DHCP server is not needed for SLAAC, as the devices generate their own addresses without relying on a server. Dual stack and anycast routing are not related to SLAAC.

**NEW QUESTION 119**

- (Exam Topic 2)

A network technician is configuring a new firewall for a company with the necessary access requirements to be allowed through the firewall. Which of the following would normally be applied as the LAST rule in the firewall?

- A. Secure SNMP
- B. Port security
- C. Implicit deny
- D. DHCP snooping

**Answer:** C

**Explanation:**

Implicit deny is a firewall rule that blocks all traffic that is not explicitly allowed by other rules. Implicit deny is usually applied as the last rule in the firewall to ensure that only the necessary access requirements are allowed through the firewall and that any unwanted or malicious traffic is rejected. Implicit deny can also provide a default security policy and a baseline for auditing and logging purposes.

Secure SNMP is a protocol that allows network devices to send event messages to a centralized server or console for logging and analysis. Secure SNMP can be used to monitor and manage the status, performance, and configuration of network devices. Secure SNMP can also help to detect and respond to potential problems or faults on the network. However, secure SNMP is not a firewall rule; it is a network management protocol.

Port security is a feature that allows a switch to restrict the devices that can connect to a specific port based on their MAC addresses. Port security can help to prevent unauthorized access, spoofing, or MAC flooding attacks on the switch. However, port security is not a firewall rule; it is a switch feature.

DHCP snooping is a feature that allows a switch to filter DHCP messages and prevent rogue DHCP servers from assigning IP addresses to devices on the network. DHCP snooping can help to prevent IP address conflicts, spoofing, or denial-of-service attacks on the network. However, DHCP snooping is not a firewall rule; it is a switch feature.

**NEW QUESTION 120**

- (Exam Topic 2)

A network requirement calls for segmenting departments into different networks. The campus network is set up with users of each department in multiple buildings. Which of the following should be configured to keep the design simple and efficient?

- A. MDIX
- B. Jumbo frames
- C. Port tagging
- D. Flow control

**Answer:** C

**Explanation:**

Port tagging is a technique that involves adding a tag or identifier to the frames or packets that belong to a certain VLAN. A VLAN is a logical segment of a network that isolates traffic between different groups of devices. Port tagging allows devices on different physical ports or switches to communicate with each other as if they were on the same port or switch. Port tagging can help keep the design simple and efficient by reducing the number of physical ports and switches needed to segment departments into different networks. References: <https://www.comptia.org/blog/what-is-port-tagging>

**NEW QUESTION 122**

- (Exam 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 123**

- (Exam 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\\_](https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/border-gateway-protocol-bgp/prod_white_)

**NEW QUESTION 128**

- (Exam Topic 2)

During the security audit of a financial firm the Chief Executive Officer (CEO) questions why there are three employees who perform very distinct functions on the server. There is an administrator for creating users another for assigning the users to groups and a third who is the only administrator to perform file rights assignment Which of the following mitigation techniques is being applied?

- A. Privileged user accounts
- B. Role separation
- C. Container administration
- D. Job rotation

**Answer:** B

**Explanation:**

Role separation is a security principle that involves dividing the tasks and privileges for a specific business process among multiple users. This reduces the risk of fraud and errors, as no one user has complete control over the process. In the scenario, there are three employees who perform very distinct functions on the server, which is an example of role separation. References: <https://hyperproof.io/resource/segregation-of-duties/>

**NEW QUESTION 131**

- (Exam Topic 2)

A technician is connecting DSL for a new customer. After installing and connecting the on-premises equipment, the technician verifies DSL synchronization. When connecting to a workstation, however, the link LEDs on the workstation and modem do not light up. Which of the following should the technician perform during troubleshooting?

- A. Identify the switching loops between the modem and the workstation.
- B. Check for asymmetrical routing on the modem.
- C. Look for a rogue DHCP server on the network.
- D. Replace the cable connecting the modem and the workstation.

**Answer:** D

**Explanation:**

If the link LEDs on the workstation and modem do not light up when connecting to a workstation, it could indicate a problem with the cable connecting them. The cable could be damaged, defective, or incompatible with the devices. A technician should replace the cable with a known good one and check if the link LEDs light up. If not, the problem could be with the network interface cards (NICs) on the workstation or modem. References: <https://www.comptia.org/blog/what-is-link-light>

**NEW QUESTION 135**

- (Exam Topic 2)

Which of the following is MOST commonly used to address CVEs on network equipment and/or operating systems?

- A. Vulnerability assessment
- B. Factory reset
- C. Firmware update
- D. Screened subnet

**Answer:** C

**Explanation:**

Firmware is a type of software that controls the low-level functions of a hardware device, such as a router, switch, printer, or camera. Firmware updates are patches or upgrades that fix bugs, improve performance, add features, or address security vulnerabilities in firmware. Firmware updates are commonly used to address CVEs (Common Vulnerabilities and Exposures) on network equipment and operating systems, as CVEs are publicly known flaws that can be exploited by attackers. References:

<https://www.comptia.org/blog/what-is-firmware>

**NEW QUESTION 139**

- (Exam Topic 2)

A customer wants to segregate the traffic between guests on a hypervisor. Which of the following does a technician need to configure to meet the requirement?

- A. Virtual switches
- B. OSPF routing
- C. Load balancers
- D. NIC teaming
- E. Fibre Channel

**Answer:** A

**Explanation:**

A virtual switch is a software-based switch that connects virtual machines on a hypervisor. A virtual switch can create and manage VLANs, which are logical segments of a network that isolate traffic between different groups of devices. A customer can use virtual switches to segregate the traffic between guests on a hypervisor by creating a separate VLAN for each guest and assigning it to a virtual switch port. References: <https://www.comptia.org/blog/what-is-a-virtual-switch>

**NEW QUESTION 144**

- (Exam Topic 2)

A city has hired a new employee who needs to be able to work when traveling at home and at the municipal sourcing of a neighboring city that snares services. The employee is issued a laptop, and a technician needs to train the employee on the appropriate solutions for secure access to the network from all the possible locations. On which of the following solutions would the technician MOST likely train the employee?

- A. Site-to-site VPNs between the two city locations and client-to-site software on the employee's laptop for all other remote access
- B. Client-to-site VPNs between the travel locations and site-to-site software on the employee's laptop for all other remote access
- C. Client-to-site VPNs between the two city locations and site-to-site software on the employee's laptop for all other remote access
- D. Site-to-site VPNs between the home and city locations and site-to-site software on the employee's laptop for all other remote access

**Answer:** A

**Explanation:**

The technician would most likely train the employee on using site-to-site VPNs between the two city locations and client-to-site software on the employee's laptop for all other remote access. A VPN (Virtual Private Network) is a technology that creates a secure and encrypted tunnel over a public network such as the Internet. It allows remote users or sites to access a private network as if they were directly connected to it. A site-to-site VPN connects two or more networks, such as branch offices or data centers, using a VPN gateway device at each site. A client-to-site VPN connects individual users, such as mobile workers or telecommuters, using a VPN client software on their devices. In this scenario, the employee needs to access the network from different locations, such as home, travel, or another city. Therefore, the technician would train the employee on how to use site-to-site VPNs to connect to the network from another city location that shares services, and how to use client-to-site software to connect to the network from home or travel locations. References: <https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-work>

**NEW QUESTION 146**

- (Exam Topic 3)

Which of the following network devices can perform routing between VLANs?

- A. Layer 2 switch
- B. Layer 3 switch
- C. Load balancer
- D. Bridge

**Answer:** B

**Explanation:**

<https://www.practicalnetworking.net/stand-alone/routing-between-vlans/#:~:text=A%20router%20will%20perfo>

**NEW QUESTION 149**

- (Exam Topic 3)

A network technician needs to ensure the company's external mail server can pass reverse lookup checks. Which of the following records would the technician MOST likely configure? (Choose Correct option and give explanation directly from CompTIA Network+ Study guide or documents)

- A. PTR
- B. AAAA
- C. SPF
- D. CNAME

**Answer:** A

**Explanation:**

A PTR (Pointer) record is used to map an IP address to a domain name, which is necessary for reverse lookup checks. Reverse lookup checks are performed by external mail servers to verify the identity of the sender of the email. By configuring a PTR record, the network technician can ensure that the company's external mail server can pass these checks. According to the CompTIA Network+ Study Guide, "A PTR record is used to map an IP address to a domain name, and it is often used for email authentication."

**NEW QUESTION 150**

- (Exam Topic 3)

An administrator is investigating reports of network slowness in a building. While looking at the uplink interface statistics in the switch's CLI, the administrator discovers the uplink is at 100% utilization. However, the administrator is unsure how to identify what traffic is causing the saturation. Which of the following tools should the administrator utilize to identify the source and destination addresses of the traffic?

- A. SNMP
- B. Traps
- C. Syslog
- D. NetFlow

**Answer: D**

**Explanation:**

To identify the source and destination addresses of the traffic causing network saturation, the network administrator should use a network protocol analyzer that supports the NetFlow protocol. NetFlow is a network protocol that collects IP traffic information as it enters or exits an interface and sends it to a NetFlow collector for analysis. This data includes the source and destination addresses of the traffic, the ports used, and the number of bytes and packets transferred.

Therefore, the correct answer is option D, NetFlow.

Reference: CompTIA Network+ Study Guide, Exam N10-007, Fourth Edition, by Todd Lammler (Chapter 6: Network Devices)

**NEW QUESTION 154**

- (Exam Topic 3)

A technician is checking network devices to look for opportunities to improve security. Which of the following tools would BEST accomplish this task?

- A. Wi-Fi analyzer
- B. Protocol analyzer
- C. Nmap
- D. IP scanner

**Answer: B**

**Explanation:**

A protocol analyzer is a tool that can capture and analyze network traffic and identify security issues such as unauthorized devices, malicious packets, or misconfigured settings.

A Wi-Fi analyzer is a tool that can measure the signal strength, interference, and channel usage of wireless networks, but it cannot provide detailed information about network security.

Nmap and IP scanner are tools that can scan network hosts and ports for open services, vulnerabilities, or operating systems, but they cannot monitor network traffic in real time.

**NEW QUESTION 155**

- (Exam 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 159**

- (Exam Topic 3)

Which of the following provides guidance to an employee about restricting non-business access to the company's videoconferencing solution?

- A. Acceptable use policy
- B. Data loss prevention
- C. Remote access policy
- D. Standard operating procedure

**Answer: A**

**Explanation:**

An acceptable use policy (AUP) is a set of rules that outline the proper and improper use of an organization's resources, such as its videoconferencing solution. An AUP can provide guidance to employees about what is expected of them when using the organization's videoconferencing solution, including restricting non-business access to it.

**NEW QUESTION 162**

- (Exam Topic 3)

Which of the following OSI model layers would allow a user to access and download files from a remote computer?

- A. Session
- B. Presentation
- C. Network
- D. Application

**Answer: D**

**Explanation:**

The application layer of the OSI model (Open Systems Interconnection) is responsible for providing services to applications that allow users to access and download files from a remote computer. These services include file transfer, email, and web access, as well as other related services. In order for a user to access and download files from a remote computer, the application layer must provide the necessary services that allow the user to interact with the remote computer.

**NEW QUESTION 163**

- (Exam Topic 3)

A security vendor needs to add a note to the DNS to validate the ownership of a company domain before services begin. Which of the following records did the security company MOST likely ask the company to configure?

- A. TXT
- B. AAAA
- C. CNAME
- D. SRV

**Answer:** A

**Explanation:**

TXT stands for Text and is a type of DNS record that can store arbitrary text data associated with a domain name. TXT records can be used for various purposes, such as verifying the ownership of a domain, providing information about a domain, or implementing security mechanisms such as SPF (Sender Policy Framework) or DKIM (DomainKeys Identified Mail). In this scenario, the security company most likely asked the company to configure a TXT record with a specific value that can prove the ownership of the domain. AAAA stands for IPv6 Address and is a type of DNS record that maps a domain name to an IPv6 address. CNAME stands for Canonical Name and is a type of DNS record that maps an alias name to another name. SRV stands for Service and is a type of DNS record that specifies the location of a service on a network.

References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 1.8: Explain the purposes and use cases for advanced networking devices.

**NEW QUESTION 168**

- (Exam Topic 3)

Which of the following would be BEST to install to find and block any malicious users within a network?

- A. IDS
- B. IPS
- C. SCADA
- D. ICS

**Answer:** B

**Explanation:**

IPS takes action itself to block the attempted intrusion or otherwise remediate the incident. IDS is designed to only provide an alert about a potential incident, which enables a security operations center (SOC) analyst to investigate the event and determine whether it requires further action.

**NEW QUESTION 172**

- (Exam Topic 3)

Due to a surge in business, a company is onboarding an unusually high number of salespeople. The salespeople are assigned desktops that are wired to the network. The last few salespeople to be onboarded are able to access corporate materials on the network but not sales-specific resources. Which of the following is MOST likely the cause?

- A. The switch was configured with port security.
- B. Newly added machines are running into DHCP conflicts.
- C. The IPS was not configured to recognize the new users.
- D. Recently added users were assigned to the wrong VLAN

**Answer:** D

**NEW QUESTION 173**

- (Exam 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 174**

- (Exam Topic 3)

Which of the following would be the MOST cost-effective recovery solution for a company's lower-priority applications?

- A. Warm site

- B. Cloud site
- C. Hot site
- D. Cold site

**Answer:** C

**NEW QUESTION 177**

- (Exam Topic 3)

A user reports that a new VoIP phone works properly but the computer that is connected to the phone cannot access any network resources. Which of the following MOST Likely needs to be configured correctly to provide network connectivity to the computer?

- A. Port duplex settings
- B. Port aggregation
- C. ARP settings
- D. VLAN tags
- E. MDIX settings

**Answer:** D

**Explanation:**

VLAN (virtual LAN) tags are used to identify packets as belonging to a particular VLAN. VLANs are used to segment a network into logical sub-networks, and each VLAN is assigned a unique VLAN tag. If the VLAN tag is not configured correctly, the computer may not be able to access network resources.

**NEW QUESTION 179**

- (Exam Topic 3)

A new global ISP needs to connect from central offices in North America to the United Kingdom. Which of the following would be the BEST cabling solution for this project?

- A. Single-mode
- B. Coaxial
- C. Cat 6a
- D. Twinaxial

**Answer:** A

**Explanation:**

For a new global ISP to connect from central offices in North America to the United Kingdom, the best cabling solution would be single-mode fiber optic cable. Single-mode fiber optic cable is a type of cable that is used to transmit data over long distances using light signals. It is typically used in long-haul communication networks, such as those that connect different countries or continents.

**NEW QUESTION 184**

- (Exam Topic 3)

A public, wireless ISP mounts its access points on top of traffic signal poles. Fiber-optic cables are installed from a fiber switch through the ground and up the pole to a fiber-copper media converter, and then connected to the AP. In one location, the switchport is showing sporadic link loss to the attached AP. A similar link loss is not seen at the AP interface. The fiber-optic cable is moved to another unused switchport with a similar result. Which of the following steps should the assigned technician complete NEXT?

- A. Disable and enable the switchport.
- B. Clean the fiber-optic cable ends.
- C. Replace the media converter.
- D. Replace the copper patch cord.

**Answer:** B

**Explanation:**

Fiber-optic cables are cables that use light signals to transmit data over long distances at high speeds.

Fiber-optic cables are sensitive to dirt, dust, moisture, or other contaminants that can interfere with the light signals and cause link loss or signal degradation. To troubleshoot link loss issues with fiber-optic cables, one of the steps that should be completed next is to clean the fiber-optic cable ends with a lint-free cloth or a specialized cleaning tool. Cleaning the fiber-optic cable ends can remove any dirt or debris that may be blocking or reflecting the light signals and restore the link quality.

**NEW QUESTION 186**

- (Exam Topic 3)

Users within a corporate network need to connect to the Internet, but corporate network policy does not allow direct connections. Which of the following is MOST likely to be used?

- A. Proxy server
- B. VPN client
- C. Bridge
- D. VLAN

**Answer:** A

**NEW QUESTION 191**

- (Exam Topic 3)

Which of the following describes the ability of a corporate IT department to expand its cloud-hosted VM environment with minimal effort?

- A. Scalability

- B. Load balancing
- C. Multitenancy
- D. Geo-redundancy

**Answer:** A

**Explanation:**

Scalability is the ability of a corporate IT department to expand its cloud-hosted virtual machine (VM) environment with minimal effort. This allows IT departments to quickly and easily scale up their cloud environment to meet increased demand. Scalability also allows for the efficient use of resources, as IT departments can quickly and easily scale up or down as needed.

**NEW QUESTION 194**

- (Exam Topic 3)

A network administrator is getting reports of some internal users who cannot connect to network resources. The users state they were able to connect last week, but not today. No changes have been configured on the network devices or server during the last few weeks. Which of the following is the MOST likely cause of the issue?

- A. The client DHCP scope is fully utilized
- B. The wired network is experiencing electrical interference
- C. The captive portal is down and needs to be restarted
- D. SNMP traps are being received
- E. The packet counter on the router interface is high.

**Answer:** A

**NEW QUESTION 195**

- (Exam 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 197**

- (Exam Topic 3)

A technician discovered that some information on the local database server was changed during a file transfer to a remote server. Which of the following should concern the technician the MOST?

- A. Confidentiality
- B. Integrity
- C. DDoS
- D. On-path attack

**Answer:** B

**Explanation:**

The technician should be most concerned about data integrity and security. If information on the local database server was changed during a file transfer to a remote server, it could indicate that unauthorized access or modifications were made to the data. It could also indicate a failure in the file transfer process, which could result in data loss or corruption. The technician should investigate the cause of the changes and take steps to prevent it from happening again in the future. Additionally, they should verify the integrity of the data and restore it from a backup if necessary to ensure that the correct and complete data is available. The technician should also take appropriate actions such as notifying the system administrator and management of the incident, and following the incident management process to minimize the damage caused by the incident.

**NEW QUESTION 198**

- (Exam Topic 3)

A new company recently moved into an empty office space. Within days, users in the next office began noticing increased latency and packet drops with their Wi-Fi-connected devices. Which of the following is the MOST likely reason for this issue?

- A. Channel overlap
- B. Distance from the AP
- C. Bandwidth latency
- D. RF attenuation
- E. Network congestion

**Answer:** A

**NEW QUESTION 203**

- (Exam Topic 3)

Which of the following protocols is widely used in large-scale enterprise networks to support complex networks with multiple routers and balance traffic load on multiple links?

- A. OSPF
- B. RIPv2
- C. QoS
- D. STP

**Answer:** A

#### NEW QUESTION 206

- (Exam Topic 3)

A Wi-Fi network was originally configured to be able to handle interference from a microwave oven. The microwave oven was recently removed from the office. Now the network administrator wants to optimize the system to maximize the range of the signal. The main sources of signal degradation are the numerous cubicles and wooden walls between the WAP and the intended destination. Which of the following actions should the administrator take?

- A. Implement CDMA.
- B. Change from omni to directional.
- C. Change the SSID.
- D. Change the frequency.

**Answer:** D

#### Explanation:

- the microwave was already removed from the office
- the signal is OK now
- Notice that the question mentions "numerous cubicles and wooden walls" - meaning the signal now won't have the interference as before
- KEY POINT: the admin wants to "maximize the range of the signal:"

Manually change the frequency to 2.4 GHz for more reliable speeds and range. While 5 GHz gives you a stronger signal, it doesn't travel through walls or ceilings as well, so it doesn't give you the best range.

"Microwave ovens: Older microwave ovens, which might not have sufficient shielding, can emit relatively high-powered signals in the 2.4GHz band, resulting in significant interference with WLAN devices operating in the 2.4GHz band."

#### NEW QUESTION 210

- (Exam Topic 3)

ARP spoofing would normally be a part of:

- A. an on-path attack.
- B. DNS poisoning.
- C. a DoS attack.
- D. a rogue access point.

**Answer:** A

#### NEW QUESTION 211

- (Exam Topic 3)

An IT technician successfully connects to the corporate wireless network at a bank. While performing some tests, the technician observes that the physical address of the DHCP server has changed even though the network connection has not been lost. Which of the following would BEST explain this change?

- A. Server upgrade
- B. Duplicate IP address
- C. Scope exhaustion
- D. Rogue server

**Answer:** D

#### Explanation:

A rogue server is a DHCP server on a network that is not under the administrative control of the network staff 1. It may provide incorrect IP addresses or other network configuration information to devices on the network, causing them to lose connectivity or be vulnerable to attacks2. The physical address of the DHCP server may change if a rogue server takes over the role of assigning IP addresses to devices on the network. This can be detected by monitoring DHCP traffic or using tools such as RogueChecker2.

#### NEW QUESTION 216

- (Exam 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:** A

#### 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 217**

- (Exam Topic 3)

An administrator would like to allow Windows clients from outside the office to access workstations without using third-party software. Which of the following access methods would meet this requirement?

- A. Remote desktop gateway
- B. Split tunnel
- C. Site-to-site VPN
- D. VNC

**Answer:** A

**Explanation:**

To allow Windows clients from outside the office to access workstations without using third-party software, the administrator can use the Remote Desktop Protocol (RDP). RDP is a built-in feature of the Windows operating system that allows users to remotely connect to and control other Windows computers over a network connection.

To use RDP, the administrator will need to enable the Remote Desktop feature on the workstations that need to be accessed, and ensure that the appropriate firewall rules are in place to allow RDP traffic to pass through. The administrator will also need to provide the remote users with the necessary credentials to access the workstations.

Once RDP is set up and configured, the remote users can use the Remote Desktop client on their own computers to connect to the workstations and access them as if they were physically present in the office. This allows the administrator to provide remote access to the workstations without the need for any additional software or third-party tools.

**NEW QUESTION 220**

- (Exam Topic 3)

An international company is transferring its IT assets including a number of WAPs from the United States to an office in Europe for deployment. Which of the following considerations should the company research before implementing the wireless hardware?

- A. WPA2 cipher
- B. Regulatory Impacts
- C. CDMA configuration
- D. 802.11 standards

**Answer:** B

**Explanation:**

When transferring IT assets, including wireless access points (WAPs), from one country to another, it's important to research the regulatory impacts of the move. Different countries have different regulations and compliance requirements for wireless devices, such as frequency bands, power levels, and encryption standards. Failing to comply with these regulations can result in fines or other penalties.

**NEW QUESTION 221**

- (Exam Topic 3)

A network engineer needs to create a subnet that has the capacity for five VLANs, with the following number of clients to be allowed on each:

VLAN 10	50 users
VLAN 20	35 users
VLAN 30	20 users
VLAN 40	75 users
VLAN 50	130 users

Which of the following is the SMALLEST subnet capable of this setup that also has the capacity to double the number of clients in the future?

- A. 10.0.0.0/21
- B. 10.0.0.0/22
- C. 10.0.0.0/23
- D. 10.0.0.0/24

**Answer:** B

**NEW QUESTION 225**

- (Exam Topic 3)

An employee working in a warehouse facility is experiencing interruptions in mobile applications while walking around the facility. According to a recent site survey, the WLAN comprises autonomous APs that are directly connected to the internet, providing adequate signal coverage. Which of the following is the BEST solution to improve network stability?

- A. Implement client roaming using an extended service deployment employing a wireless controller.
- B. Remove omnidirectional antennas and adopt a directional bridge.
- C. Ensure all APs of the warehouse support MIMO and Wi-Fi 4.
- D. Verify that the level of EIRP power settings is set to the maximum permitted by regulations.

**Answer:** A

**Explanation:**

Client roaming refers to the ability of a wireless device to seamlessly connect to a different access point (AP) as the user moves around the facility. This can help to improve network stability and reduce interruptions in mobile applications. An extended service deployment is a type of wireless network configuration that uses

multiple APs to cover a large area, such as a warehouse facility. By using a wireless controller to manage the APs, the network can be better optimized for client roaming, which can improve network stability.

"Roaming With multiple WAPs in an ESS, clients will connect to whichever WAP has the strongest signal. As clients move through the space covered by the broadcast area, they will change WAP connections seamlessly, a process called roaming."

**NEW QUESTION 229**

- (Exam Topic 3)

An ISP is unable to provide services to a user in a remote area through cable and DSL. Which of the following is the NEXT best solution to provide services without adding external infrastructure?

- A. Fiber
- B. Leased line
- C. Satellite
- D. Metro optical

**Answer: C**

**Explanation:**

If an ISP is unable to provide services to a user in a remote area through cable and DSL, the next best solution to provide services without adding external infrastructure would likely be satellite. Satellite is a wireless communication technology that uses a network of satellites orbiting the Earth to transmit and receive data. It is well-suited for providing connectivity to remote or rural areas where other types of infrastructure may not be available or may be cost-prohibitive to install.

**NEW QUESTION 234**

- (Exam Topic 3)

Which of the following can have multiple VLAN interfaces?

- A. Hub
- B. Layer 3 switch
- C. Bridge
- D. Load balancer

**Answer: B**

**NEW QUESTION 236**

- (Exam Topic 3)

A network administrator is implementing process changes based on recommendations following a recent penetration test. The testers used a method to gain access to the network that involved exploiting a publicly available and fixed remote code execution vulnerability in the VPN appliance. Which of the following should the administrator do to BEST prevent this from happening again?

- A. Change default passwords on internet-facing hardware.
- B. Implement robust ACLs with explicit deny-all entries.
- C. Create private VLANs for management plane traffic.
- D. Routinely upgrade all network equipment firmware.

**Answer: D**

**Explanation:**

Firmware is the software that runs on network equipment such as routers, switches, and VPN appliances. Firmware updates often contain bug fixes, security patches, and performance improvements that can prevent or mitigate vulnerabilities and attacks. By routinely upgrading all network equipment firmware, a network administrator can ensure that the network devices are running the latest and most secure versions of firmware and avoid exploiting known and fixed remote code execution vulnerabilities in the VPN appliance. References: <https://www.comptia.org/training/books/network-n10-008-study-guide> (page 462)

**NEW QUESTION 241**

- (Exam Topic 3)

Due to space constraints in an IDF, a network administrator can only do a single switch to accommodate three data networks. The administrator needs a configuration that will allow each device to access its expected network without additional connections. The configuration must also allow each device to access the rest of the network. Which of the following should the administrator do to meet these requirements? (Select TWO).

- A. Untag the three VLANs across the uplink
- B. Tag an individual VLAN across the uplink
- C. Untag an individual VLAN per device port
- D. Tag an individual VLAN per device port
- E. Tag the three VLANs across the uplink.
- F. Tag the three VLANs per device port.

**Answer: AC**

**Explanation:**

To achieve this, you should do two things:

- Tag the three VLANs across the uplink port that connects to another switch or router. This will allow data packets from different VLANs to cross over into other networks.
- Untag an individual VLAN per device port that connects to an end device. This will assign each device to its expected network without additional connections.

**NEW QUESTION 246**

- (Exam Topic 3)

A Wi-Fi network was recently deployed in a new, multilevel building. Several issues are now being reported related to latency and drops in coverage. Which of the following is the FIRST step to troubleshoot the issues?

- A. Perform a site survey.
- B. Review the AP placement
- C. Monitor channel utilization.
- D. Test cable attenuation.

**Answer:** A

**NEW QUESTION 249**

- (Exam Topic 3)

A network administrator is setting up a new phone system and needs to define the location where VoIP phones can download configuration files. Which of the following DHCP services can be used to accomplish this task?

- A. Scope options
- B. Exclusion ranges
- C. Lease time
- D. Relay

**Answer:** A

**Explanation:**

To define the location where VoIP phones can download configuration files, the network administrator can use scope options within the Dynamic Host Configuration Protocol (DHCP) service. Scope options are a set of values that can be configured within a DHCP scope, which defines a range of IP addresses that can be leased to clients on a network. One of the scope options that can be configured is the option for the location of the configuration file server, which specifies the URL or IP address of the server where the configuration files can be downloaded.

<https://pbxbook.com/voip/dhcpcfg.html>

**NEW QUESTION 252**

- (Exam Topic 3)

A new office space is being designed. The network switches are up, but no services are running yet. A network engineer plugs in a laptop configured as a DHCP client to a switch. Which of the following IP addresses should be assigned to the laptop?

- A. 10.1.1.1
- B. 169.254.1.128
- C. 172.16.128.128
- D. 192.168.0.1

**Answer:** B

**Explanation:**

When a DHCP client is connected to a network and no DHCP server is available, the client can automatically configure a link-local address in the 169.254.0.0/16 range using the Automatic Private IP Addressing (APIPA) feature. So, the correct answer is option B, 169.254.1.128. This is also known as an APIPA address.

Reference: CompTIA Network+ Study Guide, Exam N10-007, Fourth Edition, by Todd Lammle (Chapter 4: IP Addressing)

**NEW QUESTION 254**

- (Exam Topic 3)

An engineer needs to verify the external record for SMTP traffic. The engineer logged in to the server and entered the nslookup command. Which of the following commands should the engineer send before entering the DNS name?

- A. set type=A
- B. is -d company-mail.com
- C. set domain=company.mail.com
- D. set querytype=Mx

**Answer:** D

**NEW QUESTION 255**

- (Exam 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 fall 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 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 256**

- (Exam Topic 3)

Which of the following should be used to manage outside cables that need to be routed to various multimode uplinks?

- A. Fiber distribution panel
- B. 110 punchdown block

- C. PDU
- D. TIA/EIA-568A patch bay
- E. Cat 6 patch panel

**Answer:** A

**Explanation:**

A fiber distribution panel is a device that provides a central location for connecting and managing fiber optic cables and optical modules. It can support various types and speeds of fiber optic links, including multimode uplinks. Therefore, a fiber distribution panel should be used to manage outside cables that need to be routed to various multimode uplinks.

**NEW QUESTION 261**

- (Exam Topic 3)

A new student is given credentials to log on to the campus Wi-Fi. The student stores the password in a laptop and is able to connect; however, the student is not able to connect with a phone when only a short distance from the laptop. Given the following information:

Signal strength	90%
Coverage	80%
Interference	15%
Number of connection attempts	10

Which of the following is MOST likely causing this connection failure?

- A. Transmission speed
- B. Incorrect passphrase
- C. Channel overlap
- D. Antenna cable attenuation/signal loss

**Answer:** B

**NEW QUESTION 264**

- (Exam Topic 3)

A technician is configuring a static IP address on a new device in a newly created subnet. The work order specifies the following requirements:

- The IP address should use the highest address available in the subnet.
- The default gateway needs to be set to 172.28.85.94.
- The subnet mask needs to be 255.255.255.224.

Which of the following addresses should the engineer apply to the device?

- A. 172.28.85.93
- B. 172.28.85.95
- C. 172.28.85.254
- D. 172.28.85.255

**Answer:** A

**Explanation:**

<https://www.tunnelsup.com/subnet-calculator/> IP Address: 172.28.85.95/27  
Netmask: 255.255.255.224  
Network Address: 172.28.85.64  
Usable Host Range: 172.28.85.65 - 172.28.85.94  
Broadcast Address: 172.28.85.95

**NEW QUESTION 266**

- (Exam Topic 3)

A network administrator is testing performance improvements by configuring channel bonding on an 802.Hac AP. Although a site survey detected the majority of the 5GHz frequency spectrum was idle, being used only by the company's WLAN and a nearby government radio system, the AP is not allowing the administrator to manually configure a large portion of the 5GHz frequency range. Which of the following would be BEST to configure for the WLAN being tested?

- A. Upgrade the equipment to an AP that supports manual configuration of the EIRP power settings.
- B. Switch to 802.11
- C. disable channel auto-selection, and enforce channel bonding on the configuration.
- D. Set up the AP to perform a dynamic selection of the frequency according to regulatory requirements.
- E. Deactivate the band 5GHz to avoid Interference with the government radio

**Answer:** C

**NEW QUESTION 269**

- (Exam 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 274**

- (Exam 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 277**

- (Exam Topic 3)

In which of the following components do routing protocols belong in a software-defined network?

- A. Infrastructure layer
- B. Control layer
- C. Application layer
- D. Management plane

**Answer: B**

**Explanation:**

A software-defined network (SDN) is a network architecture that decouples the control plane from the data plane and centralizes the network intelligence in a software controller. The control plane is the part of the network that makes decisions about how to route traffic, while the data plane is the part of the network that forwards traffic based on the control plane's instructions. The control layer is the layer in an SDN that contains the controller and the routing protocols that communicate with the network devices. The control layer is responsible for managing and configuring the network devices and providing them with the necessary information to forward traffic. References:

<https://www.comptia.org/training/books/network-n10-008-study-guide> (page 378)

**NEW QUESTION 281**

- (Exam Topic 3)

A device is connected to a managed Layer 3 network switch. The MAC address of the device is known, but the static IP address assigned to the device is not. Which of the following features of a Layer 3 network switch should be used to determine the IPv4 address of the device?

- A. MAC table
- B. Neighbor Discovery Protocol
- C. ARP table
- D. IPConfig
- E. ACL table

**Answer: C**

**Explanation:**

The ARP table is a database that is used by a device to map MAC addresses to their corresponding IP addresses. When a device sends a packet to another device on the same network, it uses the MAC address of the destination device to deliver the packet. The ARP table allows the device to determine the IP address of the destination device based on its MAC address.

**NEW QUESTION 285**

- (Exam Topic 3)

A coffee shop owner hired a network consultant to provide recommendations for installing a new wireless network. The coffee shop customers expect high speeds even when the network is congested. Which of the following standards should the consultant recommend?

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

**Answer: B**

**Explanation:**

\* 802.11 ax is the latest and most advanced wireless standard, providing higher speeds, lower latency, and more capacity than previous standards. It also supports OFDMA, which allows multiple devices to share a channel and reduce congestion. The other options are older standards that have lower bandwidth, range, and efficiency than 802.11ax. Therefore, 802.11 ax is the best option for the coffee shop owner who wants to provide high speeds even when the network is congested.

**NEW QUESTION 288**

- (Exam Topic 3)

A network administrator received a report stating a critical vulnerability was detected on an application that is exposed to the internet. Which of the following is the appropriate NEXT step?

- A. Check for the existence of a known exploit in order to assess the risk
- B. Immediately shut down the vulnerable application server.
- C. Install a network access control agent on the server.
- D. Deploy a new server to host the application.

**Answer: A**

**Explanation:**

The appropriate next step in this situation would be to check for the existence of a known exploit in order to assess the risk. This is important because it will help the network administrator determine the severity of the vulnerability and the potential impact it could have on the organization. Once the network administrator has assessed the risk, they can then take appropriate action to address the vulnerability. This might include patching the application, deploying a new server to host the application, or implementing other security measures to mitigate the risk. It is generally not advisable to immediately shut down the vulnerable application server, as this could disrupt business operations and cause significant downtime. Similarly, installing a network access control agent on the server may not be the most effective solution, as it would not address the underlying vulnerability.

**NEW QUESTION 293**

- (Exam Topic 3)

A technician is troubleshooting reports that a networked printer is unavailable. The printer's IP address is configured with a DHCP reservation, but the address cannot be pinged from the print server in the same subnet. Which of the following is MOST likely the cause of the connectivity failure?

- A. Incorrect VLAN
- B. DNS failure
- C. DHCP scope exhaustion
- D. Incorrect gateway

**Answer: D**

**NEW QUESTION 296**

- (Exam Topic 3)

A network engineer is investigating reports of poor network performance. Upon reviewing a report, the engineer finds hundreds of CRC errors on an interface. Which of the following is the MOST likely cause of these errors?

- A. A bad wire on the Cat 5e cable
- B. The wrong VLAN assignment to the switchport
- C. A misconfigured QoS setting on the router
- D. Both sides of the switch trunk set to full duplex

**Answer: A**

**NEW QUESTION 298**

- (Exam Topic 3)

Which of the following would be the MOST likely attack used to bypass an access control vestibule?

- A. Tailgating
- B. Phishing
- C. Evil twin
- D. Brute-force

**Answer: A**

**Explanation:**

Tailgating is when someone follows an authorized person into a restricted area without having the proper credentials. This is usually done by pretending to be with the authorized person, or by offering assistance. Tailgating is a social engineering attack and does not require any technical skill.

**NEW QUESTION 302**

- (Exam Topic 3)

Which of the following can be used to validate domain ownership by verifying the presence of pre-agreed content contained in a DNS record?

- A. SOA
- B. SRV
- C. AAA
- D. TXT

**Answer:** D

**Explanation:**

"One final usage of the TXT resource record is how some cloud service providers, such as Azure, validate ownership of custom domains. You are provided with data to include in your TXT record, and once that is created, the domain is verified and able to be used. The thought is that if you control the DNS, then you own the domain name."

**NEW QUESTION 303**

- (Exam Topic 3)

A network technician is configuring a wireless access point and wants to only allow company-owned devices to associate with the network. The access point uses PSKs, and a network authentication system does not exist on the network. Which of the following should the technician implement?

- A. Captive portal
- B. Guest network isolation
- C. MAC filtering
- D. Geofencing

**Answer:** C

**Explanation:**

MAC filtering is a method of allowing only company-owned devices to associate with the network by using their MAC addresses as identifiers. A MAC address is a unique identifier assigned to each network interface card (NIC) by the manufacturer. MAC filtering can be configured on the wireless access point to allow or deny access based on the MAC address of the device. This way, only devices with known MAC addresses can connect to the network. References: <https://www.comptia.org/training/books/network-n10-008-study-guide> (page 323)

**NEW QUESTION 304**

- (Exam Topic 3)

Which of the following is MOST appropriate for enforcing bandwidth limits when the performance of an application is not affected by the use of buffering but is heavily impacted by packet drops?

- A. Traffic shaping
- B. Traffic policing
- C. Traffic marking
- D. Traffic classification

**Answer:** B

**Explanation:**

Traffic policing is a mechanism that monitors the traffic in any network and enforces a bandwidth limit by discarding packets that exceed a certain rate<sup>1</sup>. This can reduce congestion and ensure fair allocation of bandwidth among different applications or users. However, discarding packets can also affect the performance and quality of some applications, especially those that are sensitive to packet loss, such as voice or video.

Traffic shaping is a congestion control mechanism that delays packets that exceed a certain rate instead of discarding them<sup>1</sup>. This can smooth out traffic bursts and avoid packet loss, but it also introduces latency and jitter. Traffic shaping can be beneficial for applications that can tolerate some delay but not packet loss, such as file transfers or streaming.

Traffic marking is a mechanism that assigns different priority levels to packets based on their type, source, destination, or other criteria<sup>2</sup>. This can help to differentiate between different classes of service and apply different policies or treatments to them. However, traffic marking does not enforce bandwidth limits by itself; it only provides information for other mechanisms to act upon.

Traffic classification is a process that identifies and categorizes packets based on their characteristics, such as protocol, port number, payload, or behavior. This can help to distinguish between different types of traffic and apply appropriate policies or actions to them. However, traffic classification does not enforce bandwidth limits by itself; it only provides input for other mechanisms to use.

**NEW QUESTION 308**

- (Exam 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 312**

- (Exam Topic 3)

Two network technicians are installing a fiber-optic link between routers. The technicians used a light meter to verify the correct fibers. However, when they connect the fibers to the router interface the link does not connect. Which of the following would explain the issue? (Select TWO).

- A. They used the wrong type of fiber transceiver.
- B. Incorrect TX/RX polarity exists on the link.
- C. The connection has duplexing configuration issues.
- D. Halogen light fixtures are causing interference.
- E. One of the technicians installed a loopback adapter.

F. The RSSI was not strong enough on the link

**Answer:** AB

**NEW QUESTION 315**

- (Exam Topic 3)

A technician is equipped with a tablet, a smartphone, and a laptop to troubleshoot a switch with the help of support over the phone. However, the technician is having issues interconnecting all these tools in troubleshooting the switch. Which Of the following should the technician use to gain connectivity?

- A. PAN
- B. WAN
- C. LAN
- D. MAN

**Answer:** A

**Explanation:**

A PAN stands for Personal Area Network and it is a type of network that connects devices within a small range, such as a few meters. A PAN can use wireless technologies such as Bluetooth or Wi-Fi to interconnect devices such as tablets, smartphones, and laptops. A technician can use a PAN to gain connectivity among these tools and troubleshoot the switch.

References: Network+ Study Guide Objective 1.2: Explain devices, applications, protocols and services at their appropriate OSI layers.

**NEW QUESTION 319**

- (Exam Topic 3)

A network administrator is troubleshooting a connectivity performance issue. As part of the troubleshooting process, the administrator performs a traceout from the client to the server, and also from the server to the client. While comparing the outputs, the administrator notes they show different hops between the hosts. Which of the following BEST explains these findings?

- A. Asymmetric routing
- B. A routing loop
- C. A switch loop
- D. An incorrect gateway

**Answer:** C

**NEW QUESTION 322**

- (Exam Topic 3)

A technician is troubleshooting a connectivity issue with an end user. The end user can access local network shares and intranet pages but is unable to access the internet or remote resources. Which of the following needs to be reconfigured?

- A. The IP address
- B. The subnet mask
- C. The gateway address
- D. The DNS servers

**Answer:** C

**NEW QUESTION 325**

- (Exam Topic 3)

A network administrator wants to check all network connections and see the output in integer form. Which of the following commands should the administrator run on the command line?

- A. netstat
- B. netstat -a
- C. netstat —e
- D. netstat —n

**Answer:** A

**NEW QUESTION 327**

- (Exam Topic 3)

An organization is interested in purchasing a backup solution that supports the organization's goals. Which of the following concepts would specify the maximum duration that a given service can be down before impacting operations?

- A. MTTR
- B. RTO
- C. MTBF
- D. RPO

**Answer:** B

**Explanation:**

The maximum duration that a given service can be down before it impacts operations is often referred to as the Recovery Time Objective (RTO). RTO is a key consideration in any backup and disaster recovery plan, as it determines how quickly the organization needs to be able to recover from a disruption or failure. It is typically expressed in terms of time, and it helps to inform the design and implementation of the backup solution. For example, if an organization has a critical service that must be available 24/7, it may have a very low RTO, requiring that the service be restored within a matter of minutes or even seconds. On the other hand, if the service can be down for a longer period of time without significantly impacting operations, the organization may have a higher RTO. When selecting a backup solution, it is important to consider the organization's RTO requirements and ensure that the solution is capable of meeting those needs. A solution that

does not meet the organization's RTO requirements may not be sufficient to ensure the availability of critical services in the event of a disruption or failure.

**NEW QUESTION 330**

- (Exam 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 332**

- (Exam Topic 3)

A cafeteria is facing lawsuits related to criminal internet access that was made over its guest network. The marketing team, however, insists on keeping the cafeteria phone number as the wireless passphrase. Which of the following actions would improve wireless security while accommodating the marketing team and accepting the terms of use?

- A. Setting WLAN security to use EAP-TLS
- B. Deploying a captive portal for user authentication
- C. Using geofencing to limit the area covered by the WLAN
- D. Configuring guest network isolation

**Answer: B**

**Explanation:**

A captive portal is a web page that is presented to a user before they are allowed to access a network. It is used to authenticate users and to ensure that all users have accepted the terms of use for the network. By deploying a captive portal, the cafeteria can require users to enter their phone number as the passphrase, while still providing an additional layer of security. Reference: CompTIA Network+ Study Guide, 8th Edition, page 182.

**NEW QUESTION 336**

- (Exam Topic 3)

Which of the following describes traffic going in and out of a data center from the internet?

- A. Demarcation point
- B. North-South
- C. Fibre Channel
- D. Spine and leaf

**Answer: B**

**NEW QUESTION 338**

- (Exam Topic 3)

A PC and a network server have no network connectivity, and a help desk technician is attempting to resolve the issue. The technician plans to run a constant ping command from a Windows workstation while testing various possible reasons for the connectivity issue. Which of the following should the technician use?

- A. ping -w
- B. ping -i
- C. ping -s
- D. ping -t

**Answer: D**

**Explanation:**

ping -t is an option for the ping command in Windows that allows the user to send continuous ping requests to a target until stopped by pressing Ctrl-C. This can help the technician run a constant ping command while testing various possible reasons for the connectivity issue. ping -w is an option for the ping command in Windows that allows the user to specify a timeout value in milliseconds for each ping request. ping -i is an option for the ping command in Linux that allows the user to specify the time interval in seconds between each ping request. ping -s is an option for the ping command in Linux that allows the user to specify the size of the data payload in bytes for each ping request.

References: How to Use the Ping Command in Windows - Lifewire (<https://www.lifewire.com/ping-command-2618099>)

**NEW QUESTION 341**

- (Exam Topic 3)

A network administrator is given the network 80.87.78.0/26 for specific device assignments. Which of the following describes this network?

- A. 80.87.78.0 - 80.87.78.14
- B. 80.87.78.0 - 80.87.78.110
- C. 80.87.78.1 - 80.87.78.62
- D. 80.87.78.1 - 80.87.78.158

**Answer: C**

**Explanation:**

The network 80.87.78.0/26 is a Class A network with a subnet mask of /26, which means that it contains 26 bits of network information and 6 bits of host

information. The range of valid host addresses for this network is 80.87.78.1 to 80.87.78.62. Any addresses outside of this range are reserved for special purposes or are not used.

**NEW QUESTION 344**

- (Exam Topic 3)

Which of the following can be used to store various types of devices and provide contactless delivery to users?

- A. Asset tags
- B. Biometrics
- C. Access control vestibules
- D. Smart lockers

**Answer:** C

**NEW QUESTION 348**

- (Exam Topic 3)

An engineer recently decided to upgrade the firmware on a router. During the upgrade, the help desk received calls about a network outage, and a critical ticket was opened. The network manager would like to create a policy to prevent this from happening in the future. Which of the following documents should the manager create?

- A. Change management
- B. incident response
- C. Standard operating procedure
- D. System life cycle

**Answer:** A

**NEW QUESTION 350**

- (Exam 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 355**

- (Exam 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%20n> "To summarize this general best practice guide, you should NOT enable jumbo frame feature as a general home user."

**NEW QUESTION 358**

- (Exam Topic 3)

A technician uses a badge to enter a security checkpoint on a corporate campus. An unknown individual quickly walks in behind the technician without speaking. Which of the following types of attacks did the technician experience?

- A. Tailgating
- B. Evil twin
- C. On-path
- D. Piggybacking

**Answer:** A

**Explanation:**

Tailgating is a type of physical security attack where an unauthorized person follows an authorized person into a restricted area without their consent or knowledge. Tailgating can allow an attacker to bypass security measures and gain access to sensitive information or resources. In this scenario, the technician experienced tailgating when the unknown individual walked in behind the technician without speaking. Piggybacking is similar to tailgating, but it involves the consent or cooperation of the authorized person. Evil twin is a type of wireless network attack where an attacker sets up a rogue access point that mimics a legitimate one. On-path is a type of network attack where an attacker intercepts and modifies traffic between two parties.

References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 3.2: Given a scenario, use appropriate network hardening techniques.

**NEW QUESTION 360**

- (Exam Topic 3)

Classification using labels according to information sensitivity and impact in case of unauthorized access or leakage is a mandatory component of:

- A. an acceptable use policy.
- B. a memorandum of understanding.
- C. data loss prevention,
- D. a non-disclosure agreement.

**Answer: C**

**Explanation:**

Data loss prevention (DLP) is a set of tools and processes that aim to prevent unauthorized access or leakage of sensitive information. One of the components of DLP is data classification, which involves labeling data according to its information sensitivity and impact in case of unauthorized disclosure. Data classification helps to identify and protect the most critical and confidential data and apply appropriate security controls and policies. References: Network+ Study Guide Objective 5.1: Explain the importance of policies, processes and procedures for IT governance. Subobjective: Data loss prevention.

**NEW QUESTION 365**

- (Exam Topic 3)

A network administrator determines that even when optimal wireless coverage is configured, the network users still report constant disconnections. After troubleshooting, the administrator determines that moving from one location to another causes the disconnection. Which of the following settings should provide better network stability?

- A. Client association timeout
- B. RSSI roaming threshold
- C. RF attenuation ratio
- D. EIRP power setting

**Answer: B**

**Explanation:**

In this case, the most likely cause of the constant disconnections when moving from one location to another is likely due to a problem with the roaming functionality of the wireless network. The setting that would likely provide better network stability in this situation is the RSSI roaming threshold, which determines the signal strength required for a client device to remain connected to the wireless network. If the roaming threshold is set too low, the client device may disconnect and reconnect to the network too frequently as it moves between different access points. On the other hand, if the threshold is set too high, the client device may not roam to a new access point when necessary, leading to a loss of connectivity. Adjusting the RSSI roaming threshold to an appropriate value may help to improve the stability of the wireless network in this situation.

**NEW QUESTION 369**

- (Exam Topic 3)

A network client is trying to connect to the wrong TCP port. Which of the following responses would the client MOST likely receive?

- A. RST
- B. FIN
- C. ICMP Time Exceeded
- D. Redirect

**Answer: A**

**NEW QUESTION 370**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your N10-009 Exam with Our Prep Materials Via below:**

<https://www.certleader.com/N10-009-dumps.html>