

# CompTIA

## Exam Questions N10-008

CompTIA Network+Exam



#### NEW QUESTION 1

- (Topic 1)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 2

- (Topic 1)

Which of the following would need to be configured to ensure a device with a specific MAC address is always assigned the same IP address from DHCP?

- A. Scope options
- B. Reservation
- C. Dynamic assignment
- D. Exclusion
- E. Static assignment

**Answer:** B

#### Explanation:

A reservation should be configured to ensure a device with a specific MAC address is always assigned the same IP address from DHCP. A reservation is a feature of DHCP that allows an administrator to assign a fixed IP address to a device based on its MAC address. This way, the device will always receive the same IP address from the DHCP server, even if it is powered off or disconnected from the network for a long time. References: <https://docs.microsoft.com/en-us/windows-server/troubleshoot/configure-dhcp-reservations>

#### NEW QUESTION 3

- (Topic 1)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 4

- (Topic 1)

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

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

**Answer:** B

#### Explanation:

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

References:

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

#### NEW QUESTION 5

- (Topic 1)

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

- A. MIMO
- B. TKIP
- C. LTE

D. SSID

**Answer:** D

**Explanation:**

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

**NEW QUESTION 6**

- (Topic 1)

A website administrator is concerned the company's static website could be defaced by hackers or used as a pivot point to attack internal systems. Which of the following should a network security administrator recommend to assist with detecting these activities?

- A. Implement file integrity monitoring.
- B. Change the default credentials.
- C. Use SSL encryption.
- D. Update the web-server software.

**Answer:** A

**Explanation:**

Implementing file integrity monitoring (FIM) would assist with detecting activities such as website defacement or internal system attacks. FIM is a process that monitors and alerts on changes to files or directories that are critical for security or functionality. FIM can help detect unauthorized modifications, malware infections, data breaches, or configuration errors. FIM can also help with compliance and auditing requirements. References: <https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/what-is-file-integrity-monitoring/>

**NEW QUESTION 7**

- (Topic 1)

Which of the following BEST describes a network appliance that warns of unapproved devices that are accessing the network?

- A. Firewall
- B. AP
- C. Proxy server
- D. IDS

**Answer:** D

**Explanation:**

IDS stands for intrusion detection system, which is a network appliance that monitors network traffic and alerts administrators of any suspicious or malicious activity. An IDS can warn of unapproved devices that are accessing the network by detecting anomalies, signatures, or behaviors that indicate unauthorized access attempts or attacks. 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.cisco.com/c/en/us/products/security/what-is-an-intrusion-detection-system-ids.html>

**NEW QUESTION 8**

- (Topic 1)

A technician receives feedback that some users are experiencing high amounts of jitter while using the wireless network. While troubleshooting the network, the technician uses the ping command with the IP address of the default gateway and verifies large variations in latency. The technician thinks the issue may be interference from other networks and non-802.11 devices. Which of the following tools should the technician use to troubleshoot the issue?

- A. NetFlow analyzer
- B. Bandwidth analyzer
- C. Protocol analyzer
- D. Spectrum analyzer

**Answer:** D

**Explanation:**

A spectrum analyzer is a tool that measures the frequency and amplitude of signals in a wireless network. It can be used to troubleshoot issues related to interference from other networks and non-802.11 devices, such as microwave ovens or cordless phones, by identifying the sources and levels of interference in the wireless spectrum. A spectrum analyzer can also help to optimize the channel selection and placement of wireless access points. 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.flukenetworks.com/blog/cabling-chronicles/what-spectrum-analyzer-and-how-do-you-use-it>

**NEW QUESTION 9**

- (Topic 1)

A technician is troubleshooting a network switch that seems to stop responding to requests intermittently whenever the logging level is set for debugging. Which of the following metrics should the technician check to begin troubleshooting the issue?

- A. Audit logs
- B. CPU utilization
- C. CRC errors
- D. Jitter

**Answer:** B

**Explanation:**

CPU utilization is a metric that measures the percentage of time a CPU spends executing instructions. When the logging level is set for debugging, the router may generate a large amount of logging data, which can increase CPU utilization and cause the router to stop responding to requests intermittently. References: ? Network+ N10-008 Objectives: 2.1 Given a scenario, troubleshoot common physical connectivity issues.

#### NEW QUESTION 10

- (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 10

- (Topic 1)

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

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

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 11

- (Topic 1)

A technician is connecting multiple switches to create a large network for a new office. The switches are unmanaged Layer 2 switches with multiple connections between each pair. The network is experiencing an extreme amount of latency. Which of the following is MOST likely occurring?

- A. Ethernet collisions
- B. A DDoS attack
- C. A broadcast storm
- D. Routing loops

**Answer: C**

#### Explanation:

A broadcast storm is most likely occurring when connecting multiple unmanaged Layer 2 switches with multiple connections between each pair. A broadcast storm is a situation where broadcast packets flood a network segment and consume all the available bandwidth. It can be caused by loops in the network topology, where broadcast packets are endlessly forwarded by switches without any loop prevention mechanism. Unmanaged switches do not support features such as Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP) that can detect and block loops. References: <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10556-16.html>

#### NEW QUESTION 12

- (Topic 1)

An administrator is writing a script to periodically log the IPv6 and MAC addresses of all the devices on a network segment. Which of the following switch features will MOST likely be used to assist with this task?

- A. Spanning Tree Protocol
- B. Neighbor Discovery Protocol
- C. Link Aggregation Control Protocol
- D. Address Resolution Protocol

**Answer: B**

#### Explanation:

The switch feature that is most likely to be used to assist with logging IPv6 and MAC addresses of devices on a network segment is Neighbor Discovery Protocol (NDP). NDP is used by IPv6 to discover and maintain information about other nodes on the network, including their IPv6 and MAC addresses. By periodically querying NDP, the administrator can log this information for auditing purposes. References: ? CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 2: The OSI Model and Networking Protocols, Objective 2.1: Compare and contrast TCP and UDP ports, protocols, and their purposes.

#### NEW QUESTION 16

- (Topic 1)

A network administrator discovers that users in an adjacent building are connecting to the company's guest wireless network to download inappropriate material. Which of the following can the administrator do to MOST easily mitigate this issue?

- A. Reduce the wireless power levels
- B. Adjust the wireless channels
- C. Enable wireless client isolation
- D. Enable wireless port security

**Answer:** A

**Explanation:**

Reducing the wireless power levels can limit the range of the guest wireless network and prevent users in an adjacent building from connecting to it. Adjusting the wireless channels or enabling wireless client isolation will not affect the signal strength or coverage of the guest network. Enabling wireless port security will not work on a guest network that does not use authentication or MAC address filtering. References: CompTIA Network+ Certification Exam Objectives Version 2.0 (Exam Number: N10-006), Domain 2.0 Network Operations, Objective 2.5 Given a scenario, implement appropriate wireless configuration settings; Guest WiFi Security - Cisco Umbrella

**NEW QUESTION 21**

- (Topic 1)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 24**

- (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 26**

- (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 31**

- (Topic 1)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 35**

- (Topic 1)

Which of the following TCP ports is used by the Windows OS for file sharing?

- A. 53
- B. 389
- C. 445
- D. 1433

**Answer:** C

**Explanation:**

TCP port 445 is used by the Windows OS for file sharing. It is also known as SMB (Server Message Block) or CIFS (Common Internet File System) and allows users to access files, printers, and other shared resources on a network. References: <https://docs.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3>

**NEW QUESTION 40**

- (Topic 1)

A network device is configured to send critical events to a syslog server; however, the following alerts are not being received:

Severity 5 LINK-UPDOWN: Interface 1/1, changed state to down Severity 5 LINK-UPDOWN: Interface 1/3, changed state to down

Which of the following describes the reason why the events are not being received?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 43**

- (Topic 1)

A network engineer performs the following tasks to increase server bandwidth: Connects two network cables from the server to a switch stack

Configure LACP on the switchports

Verifies the correct configurations on the switch interfaces Which of the following needs to be configured on the server?

- A. Load balancing
- B. Multipathing
- C. NIC teaming
- D. Clustering

**Answer:** C

**Explanation:**

NIC teaming is a technique that combines two or more network interface cards (NICs) on a server into a single logical interface that can increase bandwidth, provide redundancy, and balance traffic. NIC teaming can be configured with different modes and algorithms depending on the desired outcome. Link Aggregation Control Protocol (LACP) is a protocol that enables NIC teaming by dynamically bundling multiple links between two devices into one logical link. 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://docs.microsoft.com/en-us/windows-server/networking/technologies/nic-teaming/nic-teaming>

**NEW QUESTION 44**

- (Topic 1)

An engineer notices some late collisions on a half-duplex link. The engineer verifies that the devices on both ends of the connection are configured for half duplex.

Which of the following is the MOST likely cause of this issue?

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

**Answer:** C

**Explanation:**

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

devices to detect collisions. The link termination, device configuration, and device hardware are not likely to cause late collisions on a half-duplex link.

**NEW QUESTION 48**

- (Topic 1)

A user tries to ping 192.168.1.100 from the command prompt on the 192.168.2.101 network but gets the following response: U.U.U.U. Which of the following needs to be configured for these networks to reach each other?

- A. Network address translation
- B. Default gateway
- C. Loopback
- D. Routing protocol

**Answer: B**

**Explanation:**

A default gateway is a device that routes traffic from one network to another network, such as the Internet. A default gateway is usually configured on each host device to specify the IP address of the router that connects the host's network to other networks. In this case, the user's device and the destination device are on different networks (192.168.1.0/24 and 192.168.2.0/24), so the user needs to configure a default gateway on their device to reach the destination device.

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/25761/default-gateway>

**NEW QUESTION 51**

SIMULATION - (Topic 1)

You are tasked with verifying the following requirements are met in order to ensure network security.

Requirements: Datacenter

Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage

Provide a dedicated server to resolve IP addresses and hostnames correctly and handle port 53 traffic

Building A

Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage

Provide devices to support 5 additional different office users Add an additional mobile user

Replace the Telnet server with a more secure solution Screened subnet

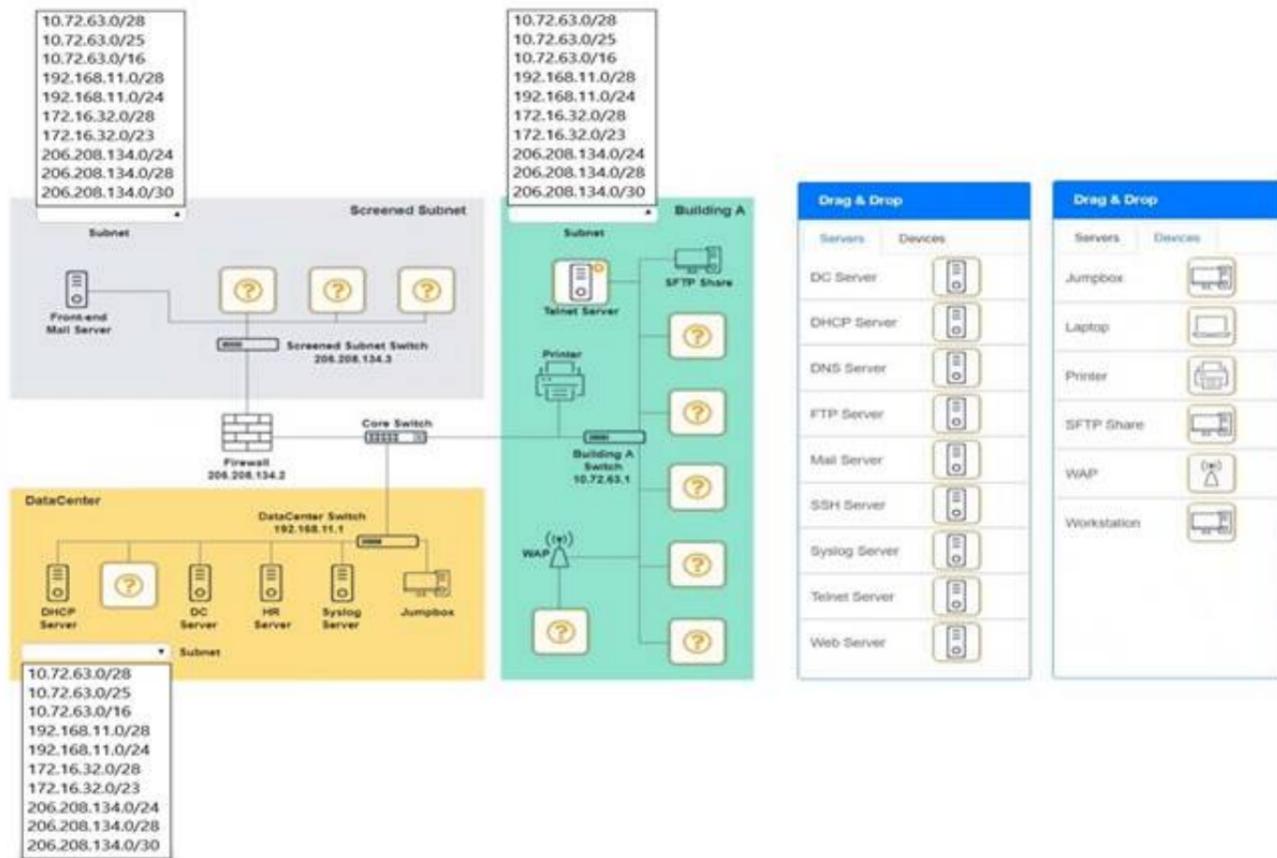
Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage

Provide a server to handle external 80/443 traffic Provide a server to handle port 20/21 traffic INSTRUCTIONS

Drag and drop objects onto the appropriate locations. Objects can be used multiple times and not all placeholders need to be filled.

Available objects are located in both the Servers and Devices tabs of the Drag & Drop menu.

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



- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Screened Subnet devices – Web server, FTP server

Building A devices – SSH server top left, workstations on all 5 on the right, laptop on bottom left

DataCenter devices – DNS server.

**Drag & Drop**

Servers	Devices
DC Server	
DHCP Server	
DNS Server	
FTP Server	
Mail Server	
SSH Server	
Syslog Server	
Telnet Server	
Web Server	

Servers	Devices
DC Server	S1
DHCP Server	S2
DNS Server	S3
FTP Server	S4
Mail Server	S5
SSH Server	S6
Syslog Server	S7
Telnet Server	S8
Web Server	S9

Servers	Devices
Jumpbox	D1
Laptop	D2
Printer	D3
SFTP Share	D4
WAP	D5
Workstation	D6

A screenshot of a computer  
 Description automatically generated

**NEW QUESTION 56**

- (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 57**

- (Topic 1)

Which of the following is the LARGEST MTU for a standard Ethernet frame?

- A. 1452
- B. 1492
- C. 1500
- D. 2304

**Answer:** C

**Explanation:**

The maximum transmission unit (MTU) is the largest size of a data packet that can be transmitted over a network. A standard Ethernet frame supports an MTU of 1500 bytes, which is the default value for most Ethernet networks. Larger MTUs are possible with jumbo frames, but they are not widely supported and may cause fragmentation or compatibility issues. 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/Maximum\\_transmission\\_unit](https://en.wikipedia.org/wiki/Maximum_transmission_unit)

**NEW QUESTION 58**

- (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:** B

**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 63**

- (Topic 1)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 64**

- (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:**

802.11a/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 66**

SIMULATION - (Topic 1)

SIMULATION

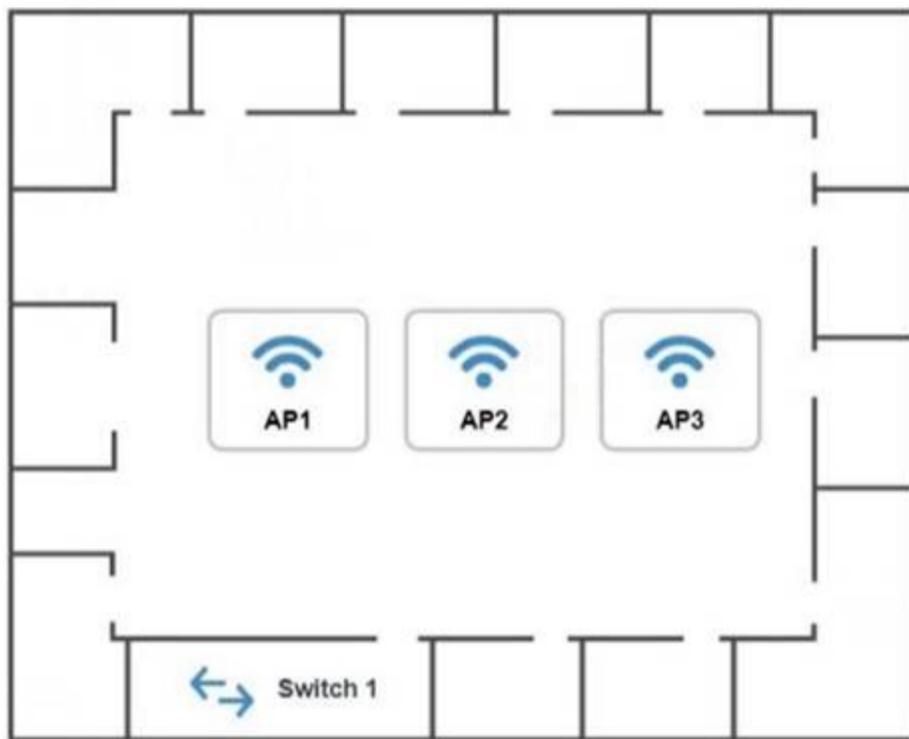
You have been tasked with setting up a wireless network in an office. The network will consist of 3 Access Points and a single switch. The network must meet the following parameters:

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

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

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

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



192.168.1.2  
 Speed: Auto  
 Duplex: Auto

### AP1 Configuration

https://ap1.setup.do

#### Basic Configuration

Access Point Name: AP1

IP Address: /

Gateway: 192.168.1.1

SSID:

SSID Broadcast:  Yes  No

#### Wireless

Mode:

Channel:

#### Wired

Speed:  Auto  100  1000

Duplex:  Auto  Half  Full

#### Security Configuration

Security Settings:  None  WEP  WPA  WPA2  WPA2 - Enterprise

Key or Passphrase:

### AP2 Configuration

https://ap2.setup.do

#### Basic Configuration

Access Point Name: AP2

IP Address: /

Gateway: 192.168.1.1

SSID:

SSID Broadcast:  Yes  No

#### Wireless

Mode:   
 B  
 G

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

#### Wired

Speed:  Auto  100  1000

Duplex:  Auto  Half  Full

#### Security Configuration

Security Settings:  None  WEP  WPA  WPA2  WPA2 - Enterprise

Key or Passphrase:

### AP3 Configuration

https://ap3.setup.do

#### Basic Configuration

Access Point Name: AP3

IP Address: /

Gateway: 192.168.1.1

SSID:

SSID Broadcast:  Yes  No

#### Wireless

Mode:   
 B  
 G

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

#### Wired

Speed:  Auto  100  1000

Duplex:  Auto  Half  Full

#### Security Configuration

Security Settings:  None  WEP  WPA  WPA2  WPA2 - Enterprise

Key or Passphrase:

Reset to Default Save Close

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

On the first exhibit, the layout should be as follows

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

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

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

Graphical user interface Description automatically generated

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

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

**AP1 Configuration** ✕

←
→
↻

IP Address  /

Gateway

SSID

SSID Broadcast  Yes  No

Wireless

Mode

Channel

Wired

Speed  Auto  100  1000

Duplex  Auto  Half  Full

Security Configuration

Security Settings  None  WEP  WPA  WPA2  WPA2 - Enterprise

Key or Passphrase

Reset to Default

Save

Close

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

**AP2 Configuration** ✕

←
→
↻

Basic Configuration

Access Point Name

IP Address  /

Gateway

SSID

SSID Broadcast  Yes  No

Wireless

Mode

Channel

Wired

Speed  Auto  100  1000

Duplex  Auto  Half  Full

Security Configuration

Reset to Default

Save

Close

Graphical user interface  
 Description automatically generated

**Security Configuration**

Security Settings  None  WEP  WPA  WPA2  WPA2 - Enterprise

Key or Passphrase

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

**AP2 Configuration** ✕

← → ↻

IP Address  /

Gateway

SSID

SSID Broadcast  Yes  No

**Wireless**

Mode

Channel

**Wired**

Speed  Auto  100  1000

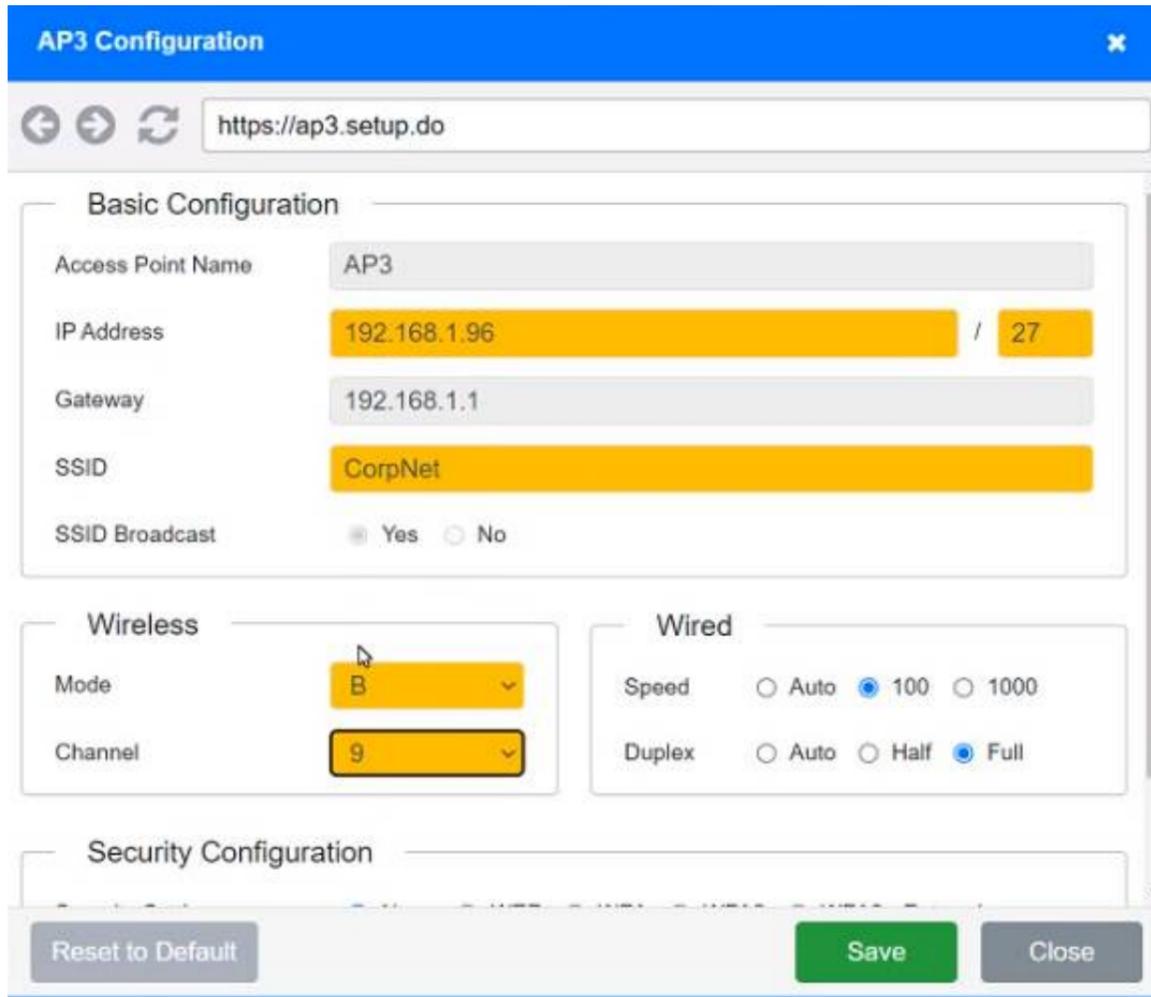
Duplex  Auto  Half  Full

**Security Configuration**

Security Settings  None  WEP  WPA  WPA2  WPA2 - Enterprise

Key or Passphrase

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



**AP3 Configuration**

https://ap3.setup.do

**Basic Configuration**

Access Point Name: AP3

IP Address: 192.168.1.96 / 27

Gateway: 192.168.1.1

SSID: CorpNet

SSID Broadcast:  Yes  No

**Wireless**

Mode: B

Channel: 9

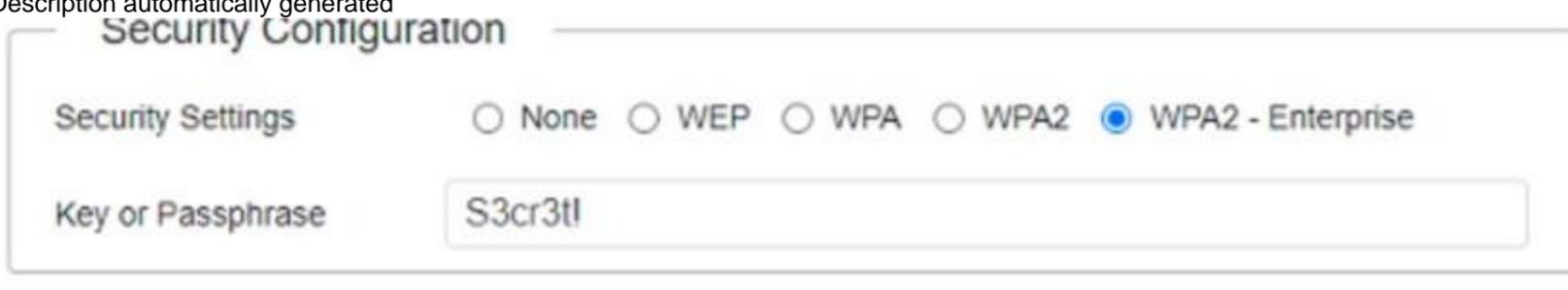
**Wired**

Speed:  Auto  100  1000

Duplex:  Auto  Half  Full

Reset to Default Save Close

Graphical user interface  
 Description automatically generated

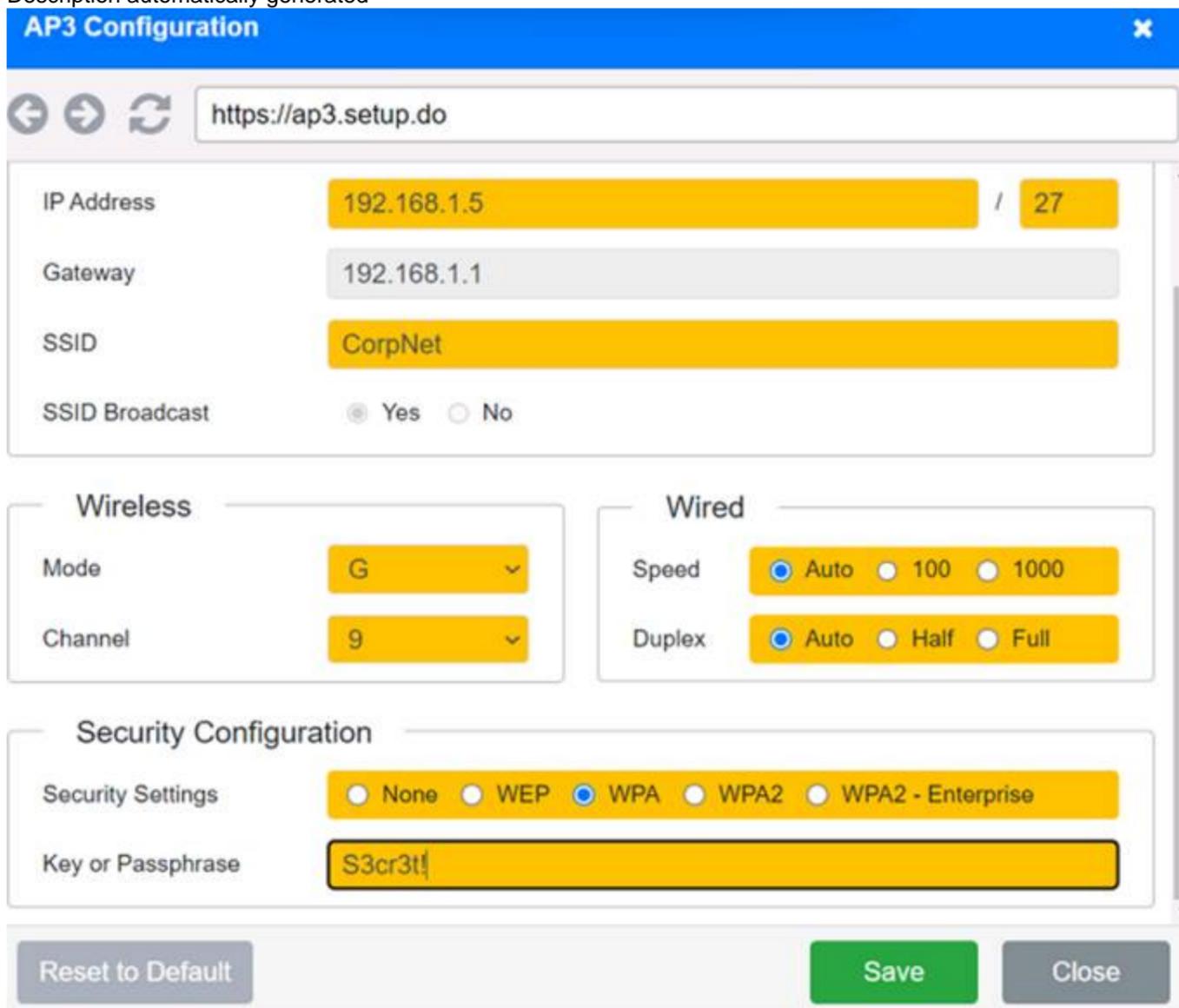


**Security Configuration**

Security Settings:  None  WEP  WPA  WPA2  WPA2 - Enterprise

Key or Passphrase: S3cr3t!

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



**AP3 Configuration**

https://ap3.setup.do

IP Address: 192.168.1.5 / 27

Gateway: 192.168.1.1

SSID: CorpNet

SSID Broadcast:  Yes  No

**Wireless**

Mode: G

Channel: 9

**Wired**

Speed:  Auto  100  1000

Duplex:  Auto  Half  Full

**Security Configuration**

Security Settings:  None  WEP  WPA  WPA2  WPA2 - Enterprise

Key or Passphrase: S3cr3t!

Reset to Default Save Close

Graphical user interface  
 Description automatically generated

### NEW QUESTION 68

- (Topic 1)

An IT director is setting up new disaster and HA policies for a company. Limited downtime is critical to operations. To meet corporate requirements, the director set up two different datacenters across the country that will stay current on data and applications. In the event of an outage, the company can immediately switch from one datacenter to another. Which of the following does this BEST describe?

- A. A warm site
- B. Data mirroring
- C. Multipathing
- D. Load balancing
- E. A hot site

**Answer:** E

#### **Explanation:**

A hot site is a fully redundant site that can take over operations immediately if the primary site goes down. In this scenario, the company has set up two different datacenters across the country that are current on data and applications, and they can immediately switch from one datacenter to another in case of an outage.

References:

? Network+ N10-008 Objectives: 1.5 Compare and contrast disaster recovery concepts and methodologies.

### NEW QUESTION 73

- (Topic 1)

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

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

**Answer:** A

#### **Explanation:**

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

### NEW QUESTION 74

- (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 77

- (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 80

- (Topic 2)

A technician is implementing a new wireless network to serve guests at a local office. The network needs to provide Internet access but disallow associated stations from communicating with each other. Which of the following would BEST accomplish this requirement?

- A. Wireless client isolation
- B. Port security
- C. Device geofencing
- D. DHCP snooping

**Answer:** A

**Explanation:**

Wireless client isolation is a feature on wireless routers that limits the connectivity between wireless devices connected to the same network. It prevents them from accessing resources on other wireless or wired devices, as a security measure to reduce attacks and threats. This feature can be useful for guest and BYOD SSIDs, but it can also be disabled on the router's settings. References: <https://www.howtogeek.com/179089/lock-down-your-wi-fi-network-with-your-routers-wireless-isolation-option/>

**NEW QUESTION 81**

- (Topic 2)

A network administrator is required to ensure that auditors have read-only access to the system logs, while systems administrators have read and write access to the system logs, and operators have no access to the system logs. The network administrator has configured security groups for each of these functional categories. Which of the following security capabilities will allow the network administrator to maintain these permissions with the LEAST administrative effort?

- A. Mandatory access control
- B. User-based permissions
- C. Role-based access
- D. Least privilege

**Answer:** C

**Explanation:**

Role-based access is a security capability that assigns permissions to users based on their roles or functions within an organization. It allows the network administrator to maintain these permissions with the least administrative effort, as they only need to configure the security groups for each role once and then assign users to those groups. Mandatory access control is a security capability that assigns permissions based on security labels or classifications, which requires more administrative effort to maintain. User-based permissions are a security capability that assigns permissions to individual users, which is not scalable or efficient for large organizations. Least privilege is a security principle that states that users should only have the minimum level of access required to perform their tasks, which is not a security capability by itself.

**NEW QUESTION 86**

- (Topic 2)

A network administrator is setting up several IoT devices on a new VLAN and wants to accomplish the following

- \* 1. Reduce manual configuration on each system
- \* 2. Assign a specific IP address to each system
- \* 3. Allow devices to move to different switchports on the same VLAN

Which of the following should the network administrator do to accomplish these requirements?

- A. Set up a reservation for each device
- B. Configure a static IP on each device
- C. Implement private VLANs for each device
- D. Use DHCP exclusions to address each device

**Answer:** A

**Explanation:**

A reservation is a feature of DHCP that assigns a specific IP address to a device based on its MAC address. This way, the device will always receive the same IP address from the DHCP server, regardless of its location or connection time. A network administrator can set up a reservation for each IoT device to accomplish the requirements of reducing manual configuration, assigning a specific IP address, and allowing devices to move to different switchports on the same VLAN. References: <https://www.comptia.org/blog/what-is-dhcp>

**NEW QUESTION 89**

- (Topic 2)

Which of the following is a system that is installed directly on a server's hardware and abstracts the hardware from any guest machines?

- A. Storage array
- B. Type 1 hypervisor
- C. Virtual machine
- D. Guest OS

**Answer:** B

**Explanation:**

A type 1 hypervisor is a system that is installed directly on a server's hardware and abstracts the hardware from any guest machines. A hypervisor is a software layer that enables virtualization by creating and managing virtual machines (VMs) on a physical host. A type 1 hypervisor, also known as a bare-metal hypervisor or a native hypervisor, runs directly on the host's hardware without requiring an underlying operating system (OS). It provides better performance and security than a type 2 hypervisor, which runs on top of an existing OS and relies on it for hardware access. References: <https://www.vmware.com/topics/glossary/content/hypervisor>

**NEW QUESTION 90**

- (Topic 2)

A wireless network was installed in a warehouse for employees to scan crates with a wireless handheld scanner. The wireless network was placed in the corner of the building near the ceiling for maximum coverage. However, users in the offices adjacent to the warehouse have noticed a large amount of signal overlap from the new network. Additionally, warehouse employees report difficulty connecting to the wireless network from the other side of the building; however, they have no issues when they are near the antenna. Which of the following is MOST likely the cause?

- A. The wireless signal is being refracted by the warehouse's windows
- B. The antenna's power level was set too high and is overlapping
- C. An omnidirectional antenna was used instead of a unidirectional antenna
- D. The wireless access points are using channels from the 5GHz spectrum

**Answer:** C

**Explanation:**

An omnidirectional antenna was used instead of a unidirectional antenna, which is most likely the cause of the wireless network issues. An omnidirectional antenna provides wireless coverage in all directions from the antenna, which can cause signal overlap with adjacent offices and interference with other wireless networks. A unidirectional antenna, on the other hand, provides wireless coverage in a specific direction from the antenna, which can reduce signal overlap and interference and increase signal range and quality. A unidirectional antenna would be more suitable for a warehouse environment where users are located on one side of the building. References: <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-omni-vs-direct.html> 1

**NEW QUESTION 93**

- (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 95**

- (Topic 2)

A firewall administrator is implementing a rule that directs HTTP traffic to an internal server listening on a non-standard socket Which of the following types of rules is the administrator implementing?

- A. NAT
- B. PAT
- C. STP
- D. SNAT
- E. ARP

**Answer:** B

**Explanation:**

The firewall administrator is implementing a PAT (Port Address Translation) rule that directs HTTP traffic to an internal server listening on a non-standard socket. PAT is a type of NAT (Network Address Translation) that allows multiple devices to share a single public IP address by using different port numbers. PAT can also be used to redirect traffic from one port to another port on the same or different IP address. This can be useful for security or load balancing purposes. For example, a firewall administrator can configure a PAT rule that redirects HTTP traffic (port 80) from the public IP address of the firewall to an internal server that listens on a non-standard port (such as 8080) on its private IP address. References: <https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13772-12.html>

**NEW QUESTION 98**

- (Topic 2)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 100**

- (Topic 2)

A user reports a weak signal when walking 20ft (61 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 101

- (Topic 2)

An organization with one core and five distribution switches is transitioning from a star to a full-mesh topology. Which of the following is the number of additional network connections needed?

- A. 5
- B. 7
- C. 10
- D. 15

**Answer: C**

#### Explanation:

10 additional network connections are needed to transition from a star to a full-mesh topology. A star topology is a network topology where each device is connected to a central device, such as a switch or a hub. A full-mesh topology is a network topology where each device is directly connected to every other device. The number of connections needed for a full-mesh topology can be calculated by the formula  $n(n-1)/2$ , where  $n$  is the number of devices. In this case, there are six devices (one core and five distribution switches), so the number of connections needed for a full-mesh topology is  $6(6-1)/2 = 15$ . Since there are already five connections in the star topology (one from each distribution switch to the core switch), the number of additional connections needed is  $15 - 5 = 10$ . References: <https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html>

#### NEW QUESTION 105

- (Topic 2)

A network technician is investigating an issue with handheld devices in a warehouse. Devices have not been connecting to the nearest APs, but they have been connecting to an AP on the far side of the warehouse. Which of the following is the MOST likely cause of this issue?

- A. The nearest APs are configured for 802.11g.
- B. An incorrect channel assignment is on the nearest APs.
- C. The power level is too high for the AP on the far side.
- D. Interference exists around the AP on the far side.

**Answer: C**

#### Explanation:

The power level is a setting that determines how strong the wireless signal is from an access point (AP). If the power level is too high for an AP on the far side of a warehouse, it can cause interference and overlap with other APs on the same channel or frequency. This can result in handheld devices not connecting to the nearest APs, but connecting to the AP on the far side instead. A technician should adjust the power level of the AP on the far side to reduce interference and improve connectivity. References: <https://www.comptia.org/blog/what-is-power-level>

#### NEW QUESTION 109

- (Topic 2)

A network administrator has been directed to present the network alerts from the past week to the company's executive staff. Which of the following will provide the BEST collection and presentation of this data?

- A. A port scan printout
- B. A consolidated report of various network devices
- C. A report from the SIEM tool
- D. A report from a vulnerability scan done yesterday

**Answer: C**

#### Explanation:

SIEM stands for Security Information and Event Management, which is a tool that collects, analyzes, and correlates data from various network devices and sources to provide alerts and reports on security incidents and events. A report from the SIEM tool can provide a comprehensive overview of the network alerts from the past week to the executive staff, highlighting any potential threats, vulnerabilities, or anomalies. References: <https://www.comptia.org/blog/what-is-siem>

#### NEW QUESTION 112

- (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 113

- (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 116

- (Topic 2)

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

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

**Answer:** B

#### Explanation:

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

### NEW QUESTION 117

- (Topic 2)

A client moving into a new office wants the IP network set up to accommodate 412 network-connected devices that are all on the same subnet. The subnet needs to be as small as possible. Which of the following subnet masks should be used to achieve the required result?

- A. 255.255.0.0
- B. 255.255.252.0
- C. 255.255.254.0
- D. 255.255.255.0

**Answer:** B

#### Explanation:

255.255.252.0 is a subnet mask that allows for 1022 network-connected devices on the same subnet, which is the smallest subnet that can accommodate 412 devices. The subnet mask determines how many bits are used for the network portion and how many bits are used for the host portion of an IP address. A smaller subnet mask means more bits are used for the network portion and less bits are used for the host portion, which reduces the number of available hosts on the subnet. 255.255.0.0 allows for 65534 hosts on the same subnet, which is too large. 255.255.254.0 allows for 510 hosts on the same subnet, which is also too large. 255.255.255.0 allows for 254 hosts on the same subnet, which is too small.

### NEW QUESTION 122

- (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 124

- (Topic 2)

A network technician is investigating an IP phone that does not register in the VoIP system. Although it received an IP address, it did not receive the necessary DHCP options. The information that is needed for the registration is distributed by the DHCP scope. All other IP phones are working properly. Which of the following does the technician need to verify?

- A. VLAN mismatch
- B. Transceiver mismatch
- C. Latency
- D. DHCP exhaustion

**Answer:** A

#### Explanation:

A VLAN mismatch is the most likely reason why an IP phone does not receive the necessary DHCP options for registration. A VLAN mismatch occurs when a device is connected to a switch port that belongs to a different VLAN than the device's intended VLAN. This can cause communication problems or prevent access to network resources. For example, if an IP phone is connected to a switch port that belongs to the data VLAN instead of the voice VLAN, it may not receive the DHCP options that contain information such as the TFTP server address, the NTP server address, or the default gateway address for the voice VLAN. These DHCP options are essential for the IP phone to register with the VoIP system and function properly. References: <https://www.cisco.com/c/en/us/support/docs/voice-unified-communications/unified-communications-manager-callmanager/13979-dhcp-option-150-00.html>

#### NEW QUESTION 125

- (Topic 2)

Which of the following protocols will a security appliance that is correlating network events from multiple devices MOST likely rely on to receive event messages?

- A. Syslog
- B. Session Initiation Protocol
- C. Secure File Transfer Protocol
- D. Server Message Block

**Answer:** A

#### Explanation:

Syslog is a protocol that provides a standard way for network devices and applications to send event messages to a logging server or a security appliance. Syslog messages can contain information about security incidents, errors, warnings, system status, configuration changes, and other events. A security appliance that is correlating network events from multiple devices can rely on Syslog to receive event messages from different sources and formats. References: <https://www.comptia.org/blog/what-is-syslog>

#### NEW QUESTION 130

- (Topic 2)

An IDS was installed behind the edge firewall after a network was breached. The network was then breached again even though the IDS logged the attack. Which of the following should be used in place of these devices to prevent future attacks?

- A. A network tap
- B. A proxy server
- C. A UTM appliance
- D. A content filter

**Answer:** C

#### Explanation:

A UTM appliance stands for Unified Threat Management appliance, which is a device that combines multiple security functions into one solution. A UTM appliance can provide firewall, IDS/IPS, antivirus, VPN, web filtering, and other security features. A network technician can use a UTM appliance in place of an edge firewall and an IDS to prevent future attacks, as a UTM appliance can block malicious traffic and detect and respond to intrusions more effectively. References: <https://www.comptia.org/blog/what-is-utm>

#### NEW QUESTION 134

- (Topic 2)

Which of the following policies is MOST commonly used for guest captive portals?

- A. AUP
- B. DLP
- C. BYOD
- D. NDA

**Answer:** A

#### Explanation:

AUP stands for Acceptable Use Policy, which is a policy that defines the rules and guidelines for using a network or service. A guest captive portal is a web page that requires users to agree to the AUP before accessing the Internet or other network resources. This is a common way to enforce security and legal compliance for guest users. References: [https://www.arubanetworks.com/techdocs/Instant\\_87\\_WebHelp/Content/instant-ug/captive-portal/captive-portal.htm](https://www.arubanetworks.com/techdocs/Instant_87_WebHelp/Content/instant-ug/captive-portal/captive-portal.htm)

#### NEW QUESTION 137

- (Topic 2)

Two remote offices need to be connected securely over an untrustworthy MAN. Each office needs to access network shares at the other site. Which of the

following will BEST provide this functionality?

- A. Client-to-site VPN
- B. Third-party VPN service
- C. Site-to-site VPN
- D. Split-tunnel VPN

**Answer: C**

**Explanation:**

A site-to-site VPN is a type of VPN that connects two or more remote offices securely over an untrustworthy network, such as the Internet. A site-to-site VPN allows each office to access network shares and resources at the other site, as if they were on the same local network. A site-to-site VPN encrypts and tunnels the traffic between the offices, ensuring privacy and integrity of the data. References: <https://www.comptia.org/blog/what-is-a-site-to-site-vpn>

**NEW QUESTION 139**

- (Topic 2)

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

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 140**

- (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 141**

- (Topic 2)

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

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

**Answer: A**

**Explanation:**

An omni antenna should be used by the AP to provide service in a radius surrounding a radio. An omni antenna is a type of antenna that has a 360-degree horizontal radiation pattern. It can provide wireless coverage in all directions from the antenna with varying degrees of vertical coverage. It is suitable for indoor environments where users are located around the AP. References: <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-omni-vs-direct.html> 1

**NEW QUESTION 142**

- (Topic 2)

A network technician is installing an analog desk phone for a new receptionist. After running a new phone line, the technician now needs to connect on a new connector. Which of the following connectors would MOST likely be used in this case?

- A. DB9
- B. RJ11
- C. RJ45
- D. DB25

**Answer:** B

**Explanation:**

RJ11 is a type of connector that is commonly used for analog phone lines. RJ11 has four wires and six positions, but only two or four of them are used. A technician can crimp an RJ11 connector to a new phone line to install an analog desk phone for a new receptionist. References: <https://www.comptia.org/blog/what-is-rj11>

**NEW QUESTION 145**

- (Topic 2)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 146**

- (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 148**

- (Topic 3)

A technician is troubleshooting a workstation about network connectivity issues on a workstation. Upon investigation, the technician notes the workstation is showing an APIPA address on the network interface. The technician verifies that the VLAN assignment is correct and that the network interface has connectivity. Which of the following is most likely the issue the workstation is experiencing?

- A. DHCP exhaustion
- B. A rogue DHCP server
- C. A DNS server outage
- D. An incorrect subnet mask

**Answer:** A

**Explanation:**

DHCP exhaustion is a situation where the DHCP server runs out of available IP addresses to assign to clients. This can happen due to misconfiguration, malicious attacks, or high demand. When a client requests an IP address from the DHCP server and does not receive a response, it may resort to using an APIPA address, which is a self-assigned address in the range of 169.254.0.1 to 169.254.255.254. APIPA addresses are only valid for local communication and cannot access the internet or other networks. Therefore, a workstation showing an APIPA address indicates that it failed to obtain a valid IP address from the DHCP server, most likely due to DHCP exhaustion

**NEW QUESTION 150**

- (Topic 3)

A technician completed troubleshooting and was able to fix an issue. Which of the following is the BEST method the technician can use to pass along the exact steps other technicians should follow in case the issue arises again?

- A. Use change management to build a database
- B. Send an email stating that the issue is resolved.
- C. Document the lessons learned
- D. Close the ticket and inform the users.

**Answer:** C

**Explanation:**

Documenting the lessons learned is the best method for passing along the exact steps other technicians should follow in case the issue arises again. Lessons learned are the knowledge and experience gained from completing a project or solving a problem. Documenting the lessons learned helps to capture the best

practices, challenges, solutions, and recommendations for future reference and improvement. Documenting the lessons learned can also help to update the knowledge base, standard operating procedures, or policies related to the issue. References: [CompTIA Network+ Certification Exam Objectives], Lessons Learned: Definition & Examples for Project Managers

#### NEW QUESTION 154

- (Topic 3)

A technician is working on a ticket for a user in the human resources department who received a new PC that does not connect to the internet. All users in human resources can access the internet. The technician can ping the PC from the human resources router but not from the IT network. Which of the following is the most likely cause of the issue?

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

**Answer:** D

#### Explanation:

An incorrect default gateway can cause a PC to not connect to the internet, because the default gateway is the device that routes traffic from the local network to other networks. If the PC has a wrong default gateway configured, it may not be able to reach the internet router or the IT network router. The technician can ping the PC from the human resources router because they are on the same local network, but not from the IT network router because they are on different networks. A duplicate IP address can cause a PC to not communicate with other devices on the same network, because the IP address is the unique identifier of a device on a network. If two devices have the same IP address, they may cause IP conflicts and packet loss. However, a duplicate IP address would not prevent the technician from pinging the PC from the human resources router, because they are on the same network.

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

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

References

What is a Default Gateway?

What's an IP Conflict and How Do You Resolve It? What is RIP (Routing Information Protocol)?

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

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

#### NEW QUESTION 158

- (Topic 3)

A network administrator is concerned about a rainbow table being used to help access network resources. Which of the following must be addressed to reduce the likelihood of a rainbow table being effective?

- A. Password policy
- B. Remote access policy
- C. Acceptable use policy
- D. Data loss prevention policy

**Answer:** A

#### Explanation:

A password policy must be addressed to reduce the likelihood of a rainbow table being effective. A rainbow table is a precomputed table of hashed passwords and their corresponding plaintext values. A rainbow table can be used to crack hashed passwords by performing a reverse lookup of the hash value in the table. A password policy is a set of rules and guidelines that define how passwords should be created, used, and managed in an organization. A password policy can help prevent rainbow table attacks by enforcing strong password requirements, such as length, complexity, expiration, and history. A strong password is one that is hard to guess or crack by using common methods such as brute force or dictionary attacks. References: [CompTIA Network+ Certification Exam Objectives], What Is Rainbow Table Attack? | Kaspersky, Password Policy Best Practices | Thycotic

#### NEW QUESTION 159

- (Topic 3)

A network technician has determined the cause of a network disruption. Which of the following is the NEXT step for the technician to perform?

- A. Validate the findings in a top-to-bottom approach
- B. Duplicate the issue, if possible
- C. Establish a plan of action to resolve the issue
- D. Document the findings and actions

**Answer:** C

#### NEW QUESTION 164

- (Topic 3)

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

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

Answer: B

#### NEW QUESTION 168

- (Topic 3)

Which of the following devices would be used to extend the range of a wireless network?

- A. A repeater
- B. A media converter
- C. A router
- D. A switch

Answer: A

#### Explanation:

A repeater is a device used to extend the range of a wireless network by receiving, amplifying, and retransmitting wireless signals. It is typically used to extend the range of a wireless network in a large area, such as an office building or a campus. Repeaters can also be used to connect multiple wireless networks together, allowing users to move seamlessly between networks. As stated in the CompTIA Network+ Study Manual, "a wireless repeater is used to extend the range of a wireless network by repeating the signal from one access point to another."

#### NEW QUESTION 170

- (Topic 3)

A network administrator is configuring a new switch and wants to connect two ports to the core switch to ensure redundancy. Which of the following configurations would meet this requirement?

- A. Full duplex
- B. 802.1Q tagging
- C. Native VLAN
- D. Link aggregation

Answer: D

#### Explanation:

Link aggregation is a technique that allows multiple physical ports to be combined into a single logical channel, which provides increased bandwidth, load balancing, and redundancy. Link aggregation can be configured using protocols such as Link Aggregation Control Protocol (LACP) or static methods.

References

? Link aggregation is one of the common Ethernet switching features covered in Objective 2.3 of the CompTIA Network+ N10-008 certification exam1.

? Link aggregation can be used to connect two ports to the core switch to ensure redundancy23.

? Link aggregation can be configured using LACP or static methods23.

1: CompTIA Network+ Certification Exam Objectives, page 5 2: Interface Configurations – N10-008 CompTIA Network+ : 2.3 3: CompTIA Network+ N10-008 Cert Guide, Chapter 11, page 323

#### NEW QUESTION 171

- (Topic 3)

A VOIP phone is plugged in to a port but cannot receive calls. Which Of the following needs to be done on the port to address the issue?

- A. Trunk all VLANs on the port.
- B. Configure the native VLAN.
- C. Tag the traffic to voice VLAN.
- D. Disable VLANs.

Answer: C

#### Explanation:

To enable a VOIP phone to receive calls on a port, the traffic needs to be tagged to the voice VLAN that is configured on the switch. This allows the phone to communicate with the voice network and the PBX server. Tagging the traffic also separates the voice traffic from the data traffic that may be coming from a computer connected to the phone. The port should be configured to tag the traffic for the voice VLAN and untag the traffic for the data VLAN1. Trunking all VLANs on the port is unnecessary and may cause security issues. Configuring the native VLAN is not relevant for this issue. Disabling VLANs would prevent the phone from working at all.

References:

Optical Fiber Connectors – CompTIA Network+ N10-007 – 2.13

? VoIP and computer on separate VLANs through one cable1

#### NEW QUESTION 173

- (Topic 3)

An IT administrator is creating an alias to the primary customer's domain. Which of the following DNS record types does this represent?

- A. CNAME
- B. MX
- C. A
- D. PTR

Answer: A

#### Explanation:

A CNAME record is a type of DNS record that maps an alias name to a canonical name, or the primary domain name. A CNAME record is used to create subdomains or alternative names for the same website, without having to specify the IP address for each alias. For example, a CNAME record can map [www.example.com](http://www.example.com) to [example.com](http://example.com), or [mail.example.com](http://mail.example.com) to [example.com](http://example.com). References: CompTIA Network+ N10-008 Cert Guide, Chapter 2, Section 2.4

#### NEW QUESTION 174

- (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 177

- (Topic 3)

The power company notifies a network administrator that it will be turning off the power to the building over the weekend. Which of the following is the BEST solution to prevent the servers from going down?

- A. Redundant power supplies
- B. Uninterruptible power supply
- C. Generator
- D. Power distribution unit

**Answer:** A

#### NEW QUESTION 180

- (Topic 3)

Which of the following routing technologies is used to prevent network failure at the gateway by protecting data traffic from a failed router?

- A. BGP
- B. OSPF
- C. EIGRP
- D. FHRP

**Answer:** D

#### Explanation:

FHRP stands for First Hop Redundancy Protocol, and it is a group of protocols that allow routers to work together to provide backup or failover for the default gateway in a network. FHRP can prevent network failure at the gateway by protecting data traffic from a failed router and ensuring that there is always an active router to forward packets. Some examples of FHRP protocols are HSRP, VRRP, and GLBP12.

References: 1: CompTIA Network+ N10-008 Cert Guide - Chapter 13: Routing Protocols32: First Hop Redundancy Protocols (FHRP) Explained4

#### NEW QUESTION 183

- (Topic 3)

Which of the following redundant devices creates broadcast storms when connected together on a high-availability network?

- A. Switches
- B. Routers
- C. Access points
- D. Servers

**Answer:** A

#### Explanation:

Switches are devices that forward data based on MAC addresses. They create separate collision domains for each port, which reduces the chance of collisions on the network. However, if multiple switches are connected together without proper configuration, they can create broadcast storms, which are situations where broadcast frames are endlessly forwarded between switches, consuming network bandwidth and resources. Broadcast storms can be prevented by using protocols such as Spanning Tree Protocol (STP), which eliminates loops in the network topology. References: CompTIA Network+ N10-008 Certification Study Guide, page 67; The Official CompTIA Network+ Student Guide (Exam N10-008), page 2-14.

#### NEW QUESTION 188

- (Topic 3)

The Chief Executive Officer of a company wants to ensure business operations are not disrupted in the event of a disaster. The solution must have fully redundant equipment, real-time synchronization, and zero data loss. Which Of the following should be prepared?

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

**Answer:** C

**Explanation:**

A hot site is a backup site that is fully equipped and ready to take over the operations of the primary site in the event of a disaster. A hot site has real-time synchronization with the primary site and can provide zero data loss. A hot site is the most expensive and reliable option for disaster recovery.

References: Network+ Study Guide Objective 5.3: Explain common scanning, monitoring and patching processes and summarize their expected outputs.

**NEW QUESTION 191**

- (Topic 3)

A network technician needs to ensure that all files on a company's network can be moved in a safe and protected manner without interception from someone who is not the intended recipient. Which of the following would allow the network technician to meet these requirements?

- A. FTP
- B. TFTP
- C. SMTP
- D. SFTP

**Answer:** D

**NEW QUESTION 195**

- (Topic 3)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 200**

- (Topic 3)

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

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

**Answer:** A

**Explanation:**

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

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

? Install a protocol analyzer tool on a device that is connected to the same network as the server, such as Wireshark3 or Microsoft Network Monitor4.

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

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

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

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

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

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

**NEW QUESTION 204**

- (Topic 3)

Network traffic is being compromised by DNS poisoning every time a company's router is connected to the internet. The network team detects a non-authorized DNS server being assigned to the network clients and remediates the incident by setting a trusted DNS server, but the issue occurs again after internet exposure. Which of the following best practices should be implemented on the router?

- A. Change the device's default password.
- B. Disable router advertisement guard.
- C. Activate control plane policing.
- D. Disable unneeded network services.

Answer: A

#### NEW QUESTION 205

- (Topic 3)

An ISP is providing Internet to a retail store and has terminated its point of connection using a standard Cat 6 pin-out. Which of the following terminations should the technician use when running a cable from the ISP's port to the front desk?

- A. F-type connector
- B. TIA/EIA-56S-B
- C. LC
- D. SC

Answer: B

#### Explanation:

The termination that the technician should use when running a cable from the ISP's port to the front desk is B. TIA/EIA-568-B. This is a standard pin-out for Cat 6 cables that is used for Ethernet and other network physical layers. It specifies how to arrange the eight wires in an RJ45 connector, which is a common type of connector for network cables.

#### NEW QUESTION 207

- (Topic 3)

Users are reporting poor wireless performance in some areas of an industrial plant. The wireless controller is measuring a low EIRP value compared to the recommendations noted on the most recent site survey. Which of the following should be verified or replaced for the EIRP value to meet the site survey's specifications? (Select TWO).

- A. AP transmit power
- B. Channel utilization
- C. Signal loss
- D. Update ARP tables
- E. Antenna gain
- F. AP association time

Answer: AE

#### Explanation:

? AP transmit power: You should check if your APs have sufficient power output and adjust them if needed. You should also make sure they are not exceeding regulatory limits for your region.

? Antenna gain: You should check if your antennas have adequate gain for your coverage area and replace them if needed. You should also make sure they are aligned properly and not obstructed by any objects.

In the scenario described, the wireless controller is measuring a low EIRP value compared to the recommendations noted in the most recent site survey. EIRP is the combination of the power transmitted by the access point and the antenna gain. Therefore, to increase the EIRP value to meet the site survey's specifications, the administrator should verify or replace the AP transmit power (option A) and the antenna gain (option E). This can be achieved by adjusting the transmit power settings on the AP or by replacing the AP's antenna with one that has a higher gain.

#### NEW QUESTION 209

- (Topic 3)

A company is considering shifting its business to the cloud. The management team is concerned at the availability of the third-party cloud service. Which of the following should the management team consult to determine the promised availability of the cloud provider?

- A. Memorandum of understanding
- B. Business continuity plan
- C. Disaster recovery plan
- D. Service-level agreement

Answer: D

#### Explanation:

A Service-level agreement (SLA) is a document that outlines the responsibilities of a cloud service provider and the customer. It typically includes the agreed-upon availability of the cloud service provider, the expected uptime for the service, and the cost of any downtime or other service interruptions. Consulting the SLA is the best way for the management team to determine the promised availability of the cloud provider. Reference: CompTIA Cloud+ Study Guide, 6th Edition, page 28.

#### NEW QUESTION 210

- (Topic 3)

Which of the following, in addition to a password, can be asked of a user for MFA?

- A. PIN
- B. Favorite color
- C. Hard token
- D. Mother's maiden name

Answer: A

#### Explanation:

MFA stands for Multi-Factor Authentication, which is a method of verifying the identity of a user by requiring two or more pieces of evidence that belong to different categories: something the user knows, something the user has, or something the user is. A password is something the user knows, and it is usually combined with another factor such as a PIN (Personal Identification Number) or a hard token (a physical device that generates a one-time code) that the user has. A favorite color or a mother's maiden name are not suitable for MFA, as they are also something the user knows and can be easily guessed or compromised.

References

? 1: Multi-Factor Authentication – N10-008 CompTIA Network+ : 3.1

- ? 2: CompTIA Network+ Certification Exam Objectives, page 13
- ? 3: CompTIA Network+ N10-008 Certification Study Guide, page 250
- ? 4: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 14

#### NEW QUESTION 211

- (Topic 3)

Which of the following BEST describes a north-south traffic flow?

- A. A public internet user accessing a published web server
- B. A database server communicating with another clustered database server
- C. A Layer 3 switch advertising routes to a router
- D. A management application connecting to managed devices

**Answer: A**

#### Explanation:

A north-south traffic flow is a term used to describe the communication between a user or device outside the network and a server or service inside the network. For example, a public internet user accessing a published web server is a north-south traffic flow. This type of traffic flow typically crosses the network perimeter and requires security measures such as firewalls and VPNs. References: CompTIA Network+ N10-008 Certification Study Guide, page 16; The Official CompTIA Network+ Student Guide (Exam N10-008), page 1- 9.

North-south traffic flow refers to the flow of traffic between the internal network of an organization and the external world. This type of traffic typically flows from the internet to the organization's internal network, and back again.

Examples of north-south traffic flow include:

- ? A public internet user accessing a published web server
- ? A remote employee connecting to a VPN
- ? An email client sending email to an external server
- ? A customer connecting to an e-commerce website

References:

- ? CompTIA Network+ N10-008 Exam Objectives, Version 5.0, August 2022, page 12
- ? CompTIA Network+ Certification Study Guide, Seventh Edition, Todd Lammle, Sybex, 2022, page 17

#### NEW QUESTION 214

- (Topic 3)

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

- A. An IPS
- B. A Layer 3 switch
- C. A router
- D. A wireless LAN controller

**Answer: B**

#### NEW QUESTION 216

- (Topic 3)

A network administrator is reviewing the network device logs on a syslog server. The messages are normal but the stamps on the messages are incorrect. Which of the following actions should the administrator take to ensure the log message time stamps are correct?

- A. Change the NTP settings on the network device
- B. Change the time on the syslog server
- C. Update the network device firmware
- D. Adjust the timeout settings on the syslog server
- E. Adjust the SSH settings on the network device.

**Answer: A**

#### NEW QUESTION 219

- (Topic 3)

A customer reports there is no access to resources following the replacement of switches. A technician goes to the site to examine the configuration and discovers redundant links between two switches. Which of the following is the reason the network is not functional?

- A. The ARP cache has become corrupt.
- B. CSMA/CD protocols have failed.
- C. STP is not configured.
- D. The switches are incompatible models

**Answer: C**

#### Explanation:

The reason the network is not functional is that STP (Spanning Tree Protocol) is not configured on the switches. STP is a protocol that prevents loops in a network topology by blocking redundant links between switches. If STP is not enabled, the switches will forward broadcast frames endlessly, creating a broadcast storm that consumes network resources and disrupts communication. References: CompTIA Network+ N10-008 Certification Study Guide, page 67; The Official CompTIA Network+ Student Guide (Exam N10-008), page 2-14.

#### NEW QUESTION 220

- (Topic 3)

Which of the following DNS records maps an alias to a true name?

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

**Answer:** D

**Explanation:**

A CNAME (Canonical Name) record is a type of DNS (Domain Name System) record that maps an alias name to a canonical or true domain name. For example, a CNAME record can map `blog.example.com` to `example.com`, which means that `blog.example.com` is an alias of `example.com`. A CNAME record is useful when you want to point multiple subdomains to the same IP address, or when you want to change the IP address of a domain without affecting the subdomains1.

**NEW QUESTION 223**

- (Topic 3)

A bank installed a new smart TV to stream online video services, but the smart TV was not able to connect to the branch Wi-Fi. The next day, a technician was able to connect the TV to the Wi-Fi, but a bank laptop lost network access at the same time. Which of the following is the MOST likely cause?

- A. DHCP scope exhaustion
- B. AP configuration reset
- C. Hidden SSID
- D. Channel overlap

**Answer:** A

**Explanation:**

DHCP scope exhaustion is the situation when a DHCP server runs out of available IP addresses to assign to clients. DHCP stands for Dynamic Host Configuration Protocol, which is a network protocol that automatically assigns IP addresses and other configuration parameters to clients on a network. A DHCP scope is a range of IP addresses that a DHCP server can distribute to clients. If the DHCP scope is exhausted, new clients will not be able to obtain an IP address and connect to the network. This can explain why the smart TV was not able to connect to the branch Wi-Fi on the first day, and why the bank laptop lost network access on the next day when the TV was connected. The technician should either increase the size of the DHCP scope or reduce the lease time of the IP addresses to avoid DHCP scope exhaustion. References: [CompTIA Network+ Certification Exam Objectives], DHCP Scope Exhaustion - What Is It? How Do You Fix It?

**NEW QUESTION 224**

- (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 227**

- (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 229**

- (Topic 3)

Which of the following documents is MOST likely to be associated with identifying and documenting critical applications?

- A. Software development life-cycle policy
- B. User acceptance testing plan
- C. Change management policy
- D. Business continuity plan

**Answer:** D

**Explanation:**

A business continuity plan (BCP) is a document that outlines the procedures and strategies to ensure the continuity of critical business functions in the event of a disaster or disruption. A BCP is most likely to be associated with identifying and documenting critical applications that are essential for the organization's operations and recovery. A BCP also defines the roles and responsibilities of the staff, the backup and restore processes, the communication channels, and the testing and maintenance schedules.

References: Network+ Study Guide Objective 5.2: Explain disaster recovery and business continuity concepts.

**NEW QUESTION 233**

- (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 238**

- (Topic 3)

A technician is troubleshooting network connectivity from a wall jack. Readings from a multimeter indicate extremely low ohmic values instead of the rated impedance from the switchport. Which of the following is the MOST likely cause of this issue?

- A. Incorrect transceivers
- B. Faulty LED
- C. Short circuit
- D. Upgraded OS version on switch

**Answer:** C

**Explanation:**

A short circuit is a condition where two conductors in a circuit are connected unintentionally, creating a low resistance path for the current. This causes the voltage to drop and the current to increase, which can damage the circuit or cause a fire. A multimeter can measure the resistance or impedance of a circuit, and if it shows extremely low values, it indicates a short circuit.

**NEW QUESTION 241**

- (Topic 3)

A company receives a cease-and-desist order from its ISP regarding prohibited torrent activity. Which of the following should be implemented to comply with the cease-and-desist order?

- A. MAC security
- B. Content filtering
- C. Screened subnet
- D. Perimeter network

**Answer:** B

**Explanation:**

Content filtering is a technique that blocks or allows access to certain types of web content, based on predefined criteria or policies. Content filtering can be used to comply with the cease-and-desist order by preventing users from accessing torrent sites or downloading torrent files, which are often used for illegal file sharing or piracy. Content filtering can also protect the network from malware, phishing, or inappropriate content. References: CompTIA Network+ N10-008 Cert Guide - O'Reilly Media, Chapter 14: Securing a Basic Network, page 520

**NEW QUESTION 244**

- (Topic 3)

A network technician is troubleshooting a specific port on a switch. Which of the following commands should the technician use to see the port configuration?

- A. show route
- B. show interface
- C. show arp
- D. show port

**Answer:** B

**Explanation:**

To see the configuration of a specific port on a switch, the network technician should use the "show interface" command. This command provides detailed information about the interface, including the current configuration, status, and statistics for the interface.

**NEW QUESTION 249**

- (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 253**

- (Topic 3)

A customer is adding fiber connectivity between adjacent buildings. A technician terminates the multimode cable to the fiber patch panel. After the technician connects the fiber patch cable, the indicator light does not come on. Which of the following should a technician try first to troubleshoot this issue?

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

**Answer:** A

**Explanation:**

One of the most common causes of fiber connectivity issues is the reversal of the fibers. This means that the transmit (TX) and receive (RX) ports on one end of the fiber link are not matched with the corresponding ports on the other end. For example, if the TX port on one device is connected to the TX port on another device, and the same for the RX ports, then the devices will not be able to communicate with each other. This can result in no indicator light, no link, or no data transmission<sup>12</sup>.

To troubleshoot this issue, the technician should first try to reverse the fibers. This can be done by swapping the connectors at one end of the fiber patch cable, or by using a crossover adapter or cable that reverses the polarity of the fibers. The technician should then check if the indicator light comes on and if the devices can communicate properly<sup>12</sup>. The other options are not the first steps to troubleshoot this issue. Rereminating the fibers is a time-consuming and costly process that should be done only if there is evidence of physical damage or poor quality of the termination. Verifying the fiber size is not relevant in this scenario, as multimode fiber is compatible with multimode fiber, and any mismatch in core diameter or bandwidth would result in high attenuation, not complete loss of signal. Examining the cable runs for visual faults is a useful technique, but it requires a special tool called a visual fault locator (VFL) that emits a visible red light through the fiber and shows any breaks or bends along the cable. However, a VFL cannot detect polarity issues or connector problems, so it is not sufficient to troubleshoot this issue

**NEW QUESTION 255**

- (Topic 3)

The following DHCP scope was configured for a new VLAN dedicated to a large deployment of 325 IoT sensors:

```
DHCP network scope: 10.10.0.0/24
Exclusion range: 10.10.10.1-10.10.10.10
Gateway: 10.10.0.1
DNS: 10.10.0.2
DHCP option 66 (TFTP): 10.10.10.4
DHCP option 4 (NTP): 10.10.10.5
```

The first 244 IoT sensors were able to connect to the TFTP server, download the configuration file, and register to an IoT management system. The other sensors are being shown as offline. Which of the following should be performed to determine the MOST likely cause of the partial deployment of the sensors?

- A. Check the gateway connectivity to the TFTP server.
- B. Check the DHCP network scope.
- C. Check whether the NTP server is online.
- D. Check the IoT devices for a hardware failure.

**Answer:** B

**NEW QUESTION 256**

- (Topic 3)

A network administrator is trying to create a subnet, which is the most efficient size possible, for 31 laptops. Which of the following network subnets would be best in this situation?

- A. 10.10.10.0/24
- B. 10.10.10.0/25
- C. 10.10.10.0/26
- D. 10.10.10.0/27

**Answer:** D

**Explanation:**

A /27 subnet mask has 32 IP addresses, of which 30 are usable for hosts. This is the smallest subnet that can accommodate 31 laptops, as the other options have either too few or too many IP addresses. A /27 subnet mask is equivalent to 255.255.255.224 in decimal notation, and has a wildcard mask of 0.0.0.31. The network address is 10.10.10.0, and the broadcast address is 10.10.10.31. The usable host range is 10.10.10.1 to 10.10.10.30.

References

- 1: Subnet Cheat Sheet – 24 Subnet Mask, 30, 26, 27, 29, and other IP Address CIDR Network References
- 2: IP Subnet Calculator

#### NEW QUESTION 261

- (Topic 3)

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

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

**Answer: D**

#### Explanation:

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

#### NEW QUESTION 262

- (Topic 3)

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

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

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 263

- (Topic 3)

A user notifies a network administrator about losing access to a remote file server. The network administrator is able to ping the server and verifies the current firewall rules do not block access to the network fileshare. Which of the following tools would help identify which ports are open on the remote file server?

- A. dig
- B. nmap
- C. tracert
- D. nslookup

**Answer: B**

#### Explanation:

nmap is the tool that would help identify which ports are open on the remote file server. nmap stands for Network Mapper, which is a free and open-source tool that can perform various network scanning and discovery tasks. nmap can help identify which ports are open on a remote device by sending probes or packets to different ports and analyzing the responses. nmap can also provide information about the operating system, services, versions, firewalls, or vulnerabilities of the remote device. nmap can be useful for network administrators, security professionals, or hackers to monitor, audit, or attack network devices. References: [CompTIA Network+ Certification Exam Objectives], Nmap - Free Security Scanner For Network Exploration & Security Audits

#### NEW QUESTION 268

- (Topic 3)

Which of the following IP packet header fields is the mechanism for ending loops at Layer 3?

- A. Checksum
- B. Type
- C. Time-to-live
- D. Protocol

**Answer: C**

#### Explanation:

The time-to-live (TTL) field is the mechanism for ending loops at Layer 3, which is the network layer of the OSI model. The TTL field is an 8-bit field that indicates the maximum time or number of hops that an IP packet can travel before it is discarded. Every time an IP packet passes through a router, the router decrements the TTL value by one. If the TTL value reaches zero, the router drops the packet and sends an ICMP message back to the source, informing that the packet has expired. This way, the TTL field prevents an IP packet from looping endlessly in a network with routing errors or cycles.

The other options are not mechanisms for ending loops at Layer 3. The checksum field is a 16-bit field that is used to verify the integrity of the IP header. The checksum field is calculated by adding all the 16-bit words in the header and taking the one's complement of the result. If the checksum field does not match the calculated value, the IP packet is considered corrupted and discarded. The type field, also known as the type of service (TOS) or differentiated services code point (DSCP) field, is an 8-bit field that is used to specify the quality of service (QoS) or priority of the IP packet. The type field can indicate how the packet should be handled in terms of delay, throughput, reliability, or cost. The protocol field is an 8-bit field that is used to identify the transport layer protocol that is encapsulated in the IP packet. The protocol field can indicate whether the payload is a TCP segment, a UDP datagram, an ICMP message, or another protocol.

#### NEW QUESTION 271

- (Topic 3)

A network technician is investigating a trouble ticket for a user who does not have network connectivity. All patch cables between the wall jacks and computers in

the building were upgraded over the weekend from Cat 5 to Cat 6. The newly installed cable is crimped with a TIA/EIA 568A on one end and a TIA/EIA 568B on the other end.

Which of the following should the technician do to MOST likely fix the issue?

- A. Ensure the switchport has PoE enabled.
- B. Crimp the cable as a straight-through cable.
- C. Ensure the switchport has STP enabled.
- D. Crimp the cable as a rollover cable.

**Answer: B**

**Explanation:**

A straight-through cable is a type of twisted pair cable that has the same wiring standard (TIA/EIA 568A or 568B) on both ends. This is the most common type of cable used for connecting devices of different types, such as a computer and a switch. A cable that has different wiring standards on each end (TIA/EIA 568A on one end and 568B on the other) is called a crossover cable, which is used for connecting devices of the same type, such as two computers or two switches. Therefore, the technician should crimp the cable as a straight-through cable to fix the issue.

**NEW QUESTION 272**

- (Topic 3)

A user is required to log in to a main web application, which then grants the user access to all other programs needed to complete job-related tasks. Which of the following authentication methods does this setup describe?

- A. SSO
- B. RADIUS
- C. TACACS+
- D. Multifactor authentication
- E. 802.1X

**Answer: A**

**Explanation:**

The authentication method that this setup describes is SSO (Single Sign-On). SSO is a technique that allows a user to log in once to a main web application and then access multiple other applications or services without having to re-enter credentials. SSO simplifies the user experience and reduces the number of passwords to remember and manage. References: CompTIA Network+ N10-008 Certification Study Guide, page 371; The Official CompTIA Network+ Student Guide (Exam N10-008), page 14-5.

**NEW QUESTION 273**

- (Topic 3)

A user in a branch office reports that access to all files has been lost after receiving a new PC. All other users in the branch can access fileshares. The IT engineer who is troubleshooting this incident is able to ping the workstation from the branch router, but the machine cannot ping the router. Which of the following is MOST likely the cause of the incident?

- A. Incorrect subnet mask
- B. Incorrect DNS server
- C. Incorrect IP class
- D. Incorrect TCP port

**Answer: A**

**NEW QUESTION 275**

- (Topic 3)

Which of the following is required for hosts to receive DHCP addresses from a server that is located on a different subnet?

- A. DHCP scope
- B. DHCP snooping
- C. DHCP reservations
- D. DHCP relay

**Answer: D**

**Explanation:**

A DHCP relay is a network device that forwards DHCP requests from clients on one subnet to a DHCP server on another subnet. This allows the DHCP server to assign IP addresses and other network configuration parameters to clients across different subnets. A DHCP scope is a range of IP addresses that a DHCP server can assign to clients. A DHCP snooping is a security feature that filters and validates DHCP messages on a switch. A DHCP reservation is a way to assign a specific IP address to a specific client based on its MAC address. References: Part 2 of the current page talks about DHCP relay and its functions. You can also find more information about DHCP relay on [this page].

**NEW QUESTION 278**

- (Topic 3)

Which of the following protocols can be routed?

- A. FCoE
- B. Fibre Channel
- C. iSCSI
- D. NetBEUI

**Answer: C**

**Explanation:**

iSCSI (Internet Small Computer System Interface) is a protocol that allows SCSI commands to be transported over IP networks<sup>1</sup>. iSCSI can be routed because it contains a network address and a device address, as required by a routable protocol<sup>2</sup>. iSCSI can be used to access block-level storage devices over a network, such as SAN (Storage Area Network).

FCoE (Fibre Channel over Ethernet) is a protocol that allows Fibre Channel frames to be encapsulated and transported over Ethernet networks<sup>1</sup>. FCoE cannot be routed because it does not contain a network address, only a device address. FCoE operates at the data link layer and requires special switches and adapters to support it. FCoE can also be used to access block-level storage devices over a network, such as SAN.

Fibre Channel is a protocol that provides high-speed and low-latency communication between servers and storage devices<sup>1</sup>. Fibre Channel cannot be routed because it does not use IP networks, but rather its own dedicated network infrastructure. Fibre Channel operates at the physical layer and the data link layer and requires special cables, switches, and adapters to support it. Fibre Channel can also be used to access block-level storage devices over a network, such as SAN. NetBEUI (NetBIOS Extended User Interface) is an old protocol that provides session-level communication between devices on a local network<sup>1</sup>. NetBEUI cannot be routed because it does not contain a network address, only a device address. NetBEUI operates at the transport layer and relies on NetBIOS for name resolution. NetBEUI is obsolete and has been replaced by other protocols, such as TCP/IP.

**NEW QUESTION 282**

- (Topic 3)

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

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

**Answer: B**

**Explanation:**

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

References

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

**NEW QUESTION 287**

- (Topic 3)

During an incident, an analyst sends reports regularly to the investigation and leadership teams. Which of the following best describes how PII should be safeguarded during an incident?

- A. Implement data encryption and store the data so only the company has access.
- B. Ensure permissions are limited to the investigation team and encrypt the data.
- C. Implement data encryption and create a standardized procedure for deleting data that is no longer needed.
- D. Ensure the permissions are open only to the company.

**Answer: C**

**Explanation:**

PII stands for Personally Identifiable Information, which is any data that can be used to identify, contact, or locate a specific individual, such as name, address, phone number, email, social security number, and so on. PII should be safeguarded during an incident to protect the privacy and security of the individuals involved, and to comply with the legal and ethical obligations of the organization. One way to safeguard PII during an incident is to implement data encryption, which is a process of transforming data into an unreadable format that can only be accessed by authorized parties who have the decryption key. Data encryption can prevent unauthorized access, modification, or disclosure of PII by malicious actors or third parties. Another way to safeguard PII during an incident is to create a standardized procedure for deleting data that is no longer needed, such as after the incident is resolved or the investigation is completed. Deleting data that is no longer needed can reduce the risk of data breaches, data leaks, or data theft, and can also save storage space and resources. A standardized procedure for deleting data can ensure that the data is erased securely and completely, and that the deletion process is documented and audited.

References

- ? 1: CompTIA Network+ N10-008 Certification Study Guide, page 304-305
- ? 2: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 13
- ? 3: CompTIA Network+ N10-008 Certification Practice Test, question 5
- ? 4: Data Encryption – N10-008 CompTIA Network+ : 3.1

**NEW QUESTION 290**

- (Topic 3)

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

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

**Answer: BE**

**NEW QUESTION 294**

- (Topic 3)

A network administrator is configuring logging on an edge switch. The requirements are to log each time a switch port goes up or down. Which of the following logging levels will provide this information?

- A. Warnings
- B. Notifications
- C. Alert
- D. Errors

**Answer: B**

**Explanation:**

Notifications are the lowest logging level and will provide the desired information regarding switch port up/down activity. According to the CompTIA Network+ Study Manual, notifications "are used for logging normal activities, such as port up/down events, link changes, and link flaps."

**NEW QUESTION 295**

- (Topic 3)

A network technician is attempting to harden a commercial switch that was recently purchased. Which of the following hardening techniques best mitigates the use of publicly available information?

- A. Changing the default password
- B. Blocking inbound SSH connections
- C. Removing the gateway from the network configuration
- D. Restricting physical access to the switch

**Answer: A**

**Explanation:**

Changing the default password is a hardening technique that best mitigates the use of publicly available information, such as vendor documentation, online forums, or hacking tools, that may reveal the default credentials of a commercial switch. By changing the default password to a strong and unique one, the network technician can prevent unauthorized access to the switch configuration and management. References:

? Network Hardening - N10-008 CompTIA Network+ : 4.3 - YouTube1

? CompTIA Network+ Certification Exam Objectives, page 151

**NEW QUESTION 299**

- (Topic 3)

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

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

**Answer: B**

**NEW QUESTION 301**

- (Topic 3)

A user reports that a crucial fileshare is unreachable following a network upgrade that was completed the night before. A network technician confirms the problem exists. Which of the following troubleshooting Steps should the network technician perform NEXT?

- A. Establish a theory of probable cause.
- B. Implement a solution to fix the problem.
- C. Create a plan of action to resolve the problem.
- D. Document the problem and the solution.

**Answer: A**

**Explanation:**

Establishing a theory of probable cause is the third step in the general troubleshooting process, after identifying the problem and gathering information. Establishing a theory of probable cause involves using the information gathered to formulate one or more possible explanations for the problem and testing them to verify or eliminate them. In this scenario, the network technician has confirmed the problem exists

and should proceed to establish a theory of probable cause based on the information available, such as the network upgrade that was completed the night before.

Implementing a solution to fix the problem is the fifth step in the general troubleshooting process, after establishing a plan of action. Implementing a solution involves applying the chosen method or technique to resolve the problem and verifying its effectiveness. In this scenario, the network technician has not established a plan of action yet and should not implement a solution without knowing the cause of the problem.

Creating a plan of action to resolve the problem is the fourth step in the general troubleshooting process, after establishing a theory of probable cause. Creating a plan of action involves selecting the best method or technique to address the problem based on the available resources, constraints, and risks. In this scenario, the network technician has not established a theory of probable cause yet and should not create a plan of action without knowing the cause of the problem.

Documenting the problem and the solution is the seventh and final step in the general troubleshooting process, after implementing preventive measures.

Documenting the problem and the solution involves recording the details of the problem, its symptoms, its cause, its solution, and its preventive measures for future reference and improvement. In this scenario, the network technician has not implemented preventive measures yet and should not document the problem and the solution without resolving and preventing it.

**NEW QUESTION 306**

- (Topic 3)

An AP uses a 98ft (30m) Cat 6 cable to connect to an access switch. The cable is wired through a duct close to a three-phase motor installation. Anytime the three-phase is turned on, all users connected to the switch experience high latency on the network. Which Of the following is MOST likely the cause Of the issue?

- A. Interference
- B. Attenuation
- C. Open circuit

D. Short circuit

**Answer:** A

**Explanation:**

Interference is a phenomenon that occurs when unwanted signals or noise affect the transmission or reception of data signals on a network. Interference can cause network issues such as high latency, low throughput, packet loss, or errors. Interference can be caused by various sources, such as electromagnetic fields, radio waves, power lines, or electrical devices. In this scenario, the three-phase motor installation is a source of interference that affects the Cat 6 cable that connects the AP to the access switch. The cable is wired through a duct close to the motor installation, which exposes it to the electromagnetic fields generated by the motor. Anytime the motor is turned on, the interference causes high latency for all users connected to the switch.

**NEW QUESTION 310**

.....

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

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

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

2nd - Questions and Answers in PDF Format

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

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

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