

# CompTIA

## Exam Questions N10-008

CompTIA Network+Exam



### NEW QUESTION 1

- (Topic 1)

Branch users are experiencing issues with videoconferencing. Which of the following will the company MOST likely configure to improve performance for these applications?

- A. Link Aggregation Control Protocol
- B. Dynamic routing
- C. Quality of service
- D. Network load balancer
- E. Static IP addresses

**Answer:** C

#### Explanation:

To improve performance for videoconferencing, the company should configure Quality of Service (QoS). This technology allows for the prioritization of network traffic, ensuring that videoconferencing traffic is given higher priority and therefore better performance. Link Aggregation Control Protocol (LACP), Dynamic routing, Network load balancer, and Static IP addresses are not directly related to improving performance for videoconferencing.

References:

? Network+ N10-007 Certification Exam Objectives, Objective 2.6: Given a scenario, implement and configure the appropriate wireless security and implement the appropriate QoS concepts.

### NEW QUESTION 2

- (Topic 1)

Which of the following service models would MOST likely be used to replace on-premises servers with a cloud solution?

- A. PaaS
- B. IaaS
- C. SaaS
- D. Disaster recovery as a Service (DRaaS)

**Answer:** B

#### Explanation:

IaaS stands for Infrastructure as a Service, which is a cloud service model that provides virtualized computing resources over the Internet, such as servers, storage, networking, and operating systems. IaaS allows customers to replace their on-premises servers with cloud servers that can be scaled up or down on demand and pay only for what they use. PaaS stands for Platform as a Service, which provides customers with a cloud-based platform for developing, testing, and deploying applications without managing the underlying infrastructure. SaaS stands for Software as a Service, which provides customers with access to cloud-based software applications over the Internet without installing or maintaining them on their devices. Disaster recovery as a Service (DRaaS) is a type of cloud service that provides customers with backup and recovery solutions for their data and applications in case of a disaster.

### NEW QUESTION 3

- (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 4

- (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 5

- (Topic 1)

A network administrator is installing a wireless network at a client's office. Which of the following IEEE 802.11 standards would be BEST to use for multiple simultaneous client access?

- A. CDMA
- B. CSMA/CD
- C. CSMA/CA
- D. GSM

**Answer: C**

**Explanation:**

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) is an IEEE 802.11 standard that would be best to use for multiple simultaneous client access on a wireless network. CSMA/CA is a media access control method that allows multiple devices to share the same wireless channel without causing collisions or interference. It works by having each device sense the channel before transmitting data and waiting for an acknowledgment from the receiver after each transmission. If the channel is busy or no acknowledgment is received, the device will back off and retry later with a random delay. References: <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-csma-ca.html>

**NEW QUESTION 6**

- (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 7**

- (Topic 1)

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

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 8**

- (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 9**

- (Topic 1)

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

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

**Answer:** B

**Explanation:**

East-West traffic refers to data flows between servers or devices within the same datacenter. When a hosted virtual server is duplicated to another physical server for redundancy, it generates significant East-West traffic as the data is replicated between the two servers. References:  
? Network+ N10-008 Objectives: 3.3 Given a scenario, implement secure network architecture concepts.

**NEW QUESTION 10**

- (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 10**

- (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 11**

- (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 13**

- (Topic 1)

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

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

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

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

**Answer: C**

**Explanation:**

CRC stands for Cyclic Redundancy Check, and it is a type of error-detecting code used to detect accidental changes to raw data. If the CRC count is increasing on a particular interface, it indicates that there might be an issue with the cabling, which is causing data corruption. References: ? Network+ N10-008 Objectives: 2.1 Given a scenario, troubleshoot common physical connectivity issues.

**NEW QUESTION 14**

- (Topic 1)

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

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 16**

- (Topic 1)

A network administrator needs to query the NSs for a remote application. Which of the following commands would BEST help the administrator accomplish this task?

- A. dig
- B. arp
- C. show interface
- D. hostname

**Answer: A**

**Explanation:**

The dig command is used to query the NSs for a remote application. It is a command-line tool that is commonly used to troubleshoot DNS issues. When used with specific options, dig can be used to obtain information about domain names, IP addresses, and DNS records. References: Network+ Certification Study Guide, Chapter 3: Network Infrastructure

**NEW QUESTION 18**

- (Topic 1)

Given the following information:

Protocol	Local address	Foreign address	State
TCP	127.0.0.1:57779	Desktop-Open:57780	Established
TCP	127.0.0.1:57780	Desktop-Open:57779	Established

Which of the following command-line tools would generate this output?

- A. netstat
- B. arp
- C. dig
- D. tracet

**Answer:** D

**Explanation:**

Tracert is a command-line tool that traces the route of a packet from a source to a destination and displays the number of hops and the round-trip time for each hop. The output shown in the question is an example of a tracert output, which shows five hops with their IP addresses and hostnames (if available) and three latency measurements for each hop in milliseconds. 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.lumen.com/help/en-us/network/traceroute/understanding-the-traceroute-output.html>

**NEW QUESTION 20**

- (Topic 1)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 23**

- (Topic 1)

Which of the following routing protocols is used to exchange route information between public autonomous systems?

- A. OSPF
- B. BGP
- C. EGRIP
- D. RIP

**Answer:** B

**Explanation:**

BGP (Border Gateway Protocol) is a routing protocol used to exchange route information between public autonomous systems (AS). OSPF (Open Shortest Path First), EGRIP (Enhanced Interior Gateway Routing Protocol), and RIP (Routing Information Protocol) are all used for internal routing within a single AS. Therefore, BGP is the correct option to choose for this question.

References:

? Network+ N10-007 Certification Exam Objectives, Objective 3.3: Given a scenario, configure and apply the appropriate routing protocol.

? Cisco: Border Gateway Protocol (BGP) Overview

**NEW QUESTION 27**

- (Topic 1)

Which of the following provides redundancy on a file server to ensure the server is still connected to a LAN even in the event of a port failure on a switch?

- A. NIC teaming
- B. Load balancer
- C. RAID array
- D. PDUs

**Answer:** A

**Explanation:**

NIC teaming, also known as network interface card teaming or link aggregation, allows multiple network interface cards to be grouped together to provide redundancy and increased throughput. In the event of a port failure on a switch, NIC teaming ensures that the file server remains connected to the LAN by automatically switching to another network interface card.

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

**NEW QUESTION 29**

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

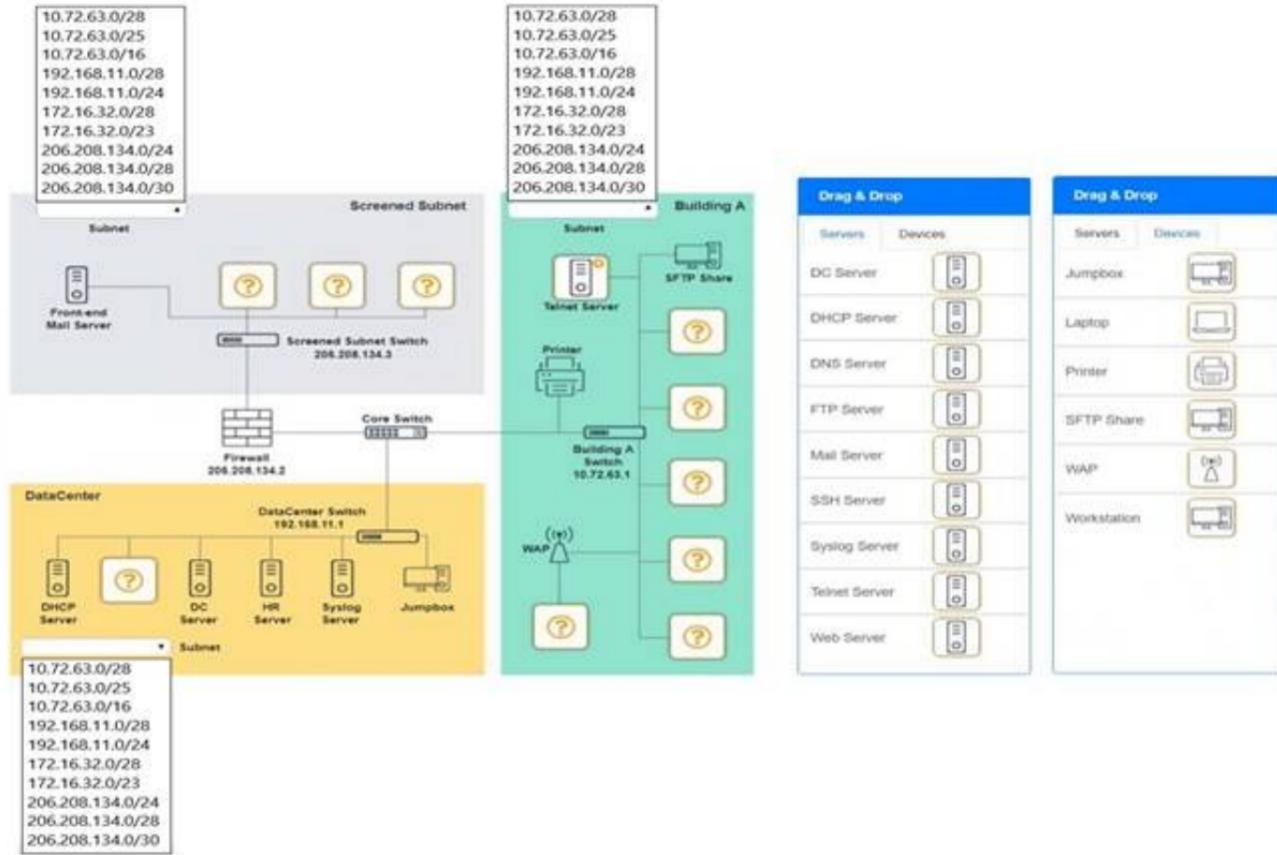
Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage

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.

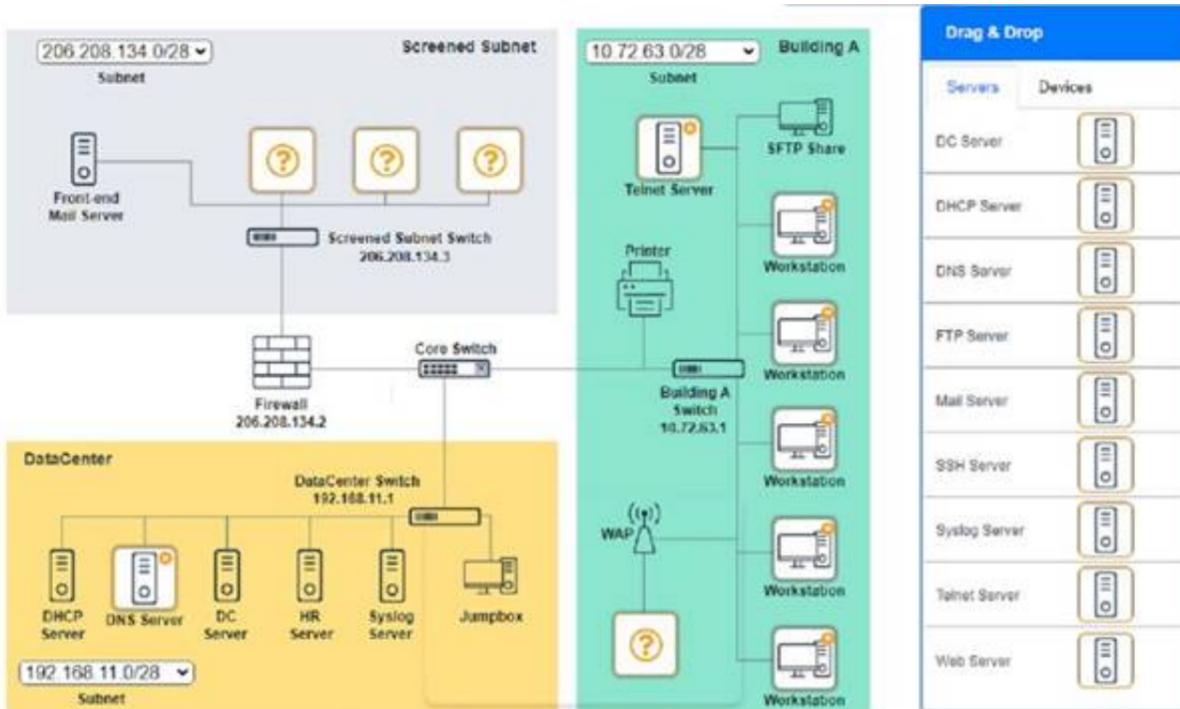


- A. Mastered
- B. Not Mastered

**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.





A screenshot of a computer  
 Description automatically generated

**NEW QUESTION 34**

- (Topic 1)

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 36**

- (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 37**

- (Topic 1)

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

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

**Answer: D**

**Explanation:**

When a user reports being unable to access network resources after making some changes, the network technician should first ask the user what changes were made. This information can help the technician identify the cause of the issue and determine the appropriate course of action.

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

**NEW QUESTION 41**

- (Topic 1)

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

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

**Answer: B**

**Explanation:**

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

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

**NEW QUESTION 43**

- (Topic 1)

A network administrator redesigned the positioning of the APs to create adjacent areas of wireless coverage. After project validation, some users still report poor connectivity when their devices maintain an association to a distanced AP. Which of the following should the network administrator check FIRST?

- A. Validate the roaming settings on the APs and WLAN clients
- B. Verify that the AP antenna type is correct for the new layout
- C. Check to see if MU-MIMO was properly activated on the APs
- D. Deactivate the 2.4GHz band on the APS

**Answer: A**

**Explanation:**

The network administrator should check the roaming settings on the APs and WLAN clients first. Roaming is the process of switching from one AP to another without losing connectivity. If the roaming settings are not configured properly, some users may experience poor connectivity when their devices stay connected to a distant AP instead of switching to a closer one. References: <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068- roam->

faq.html

#### NEW QUESTION 45

- (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 49

- (Topic 1)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 54

- (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 56

- (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 61

- (Topic 2)

A network administrator is configuring a database server and would like to ensure the database engine is listening on a certain port. Which of the following commands should the administrator use to accomplish this goal?

- A. nslookup
- B. netstat -a

- C. ipconfig /a
- D. arp -a

**Answer:** B

**Explanation:**

netstat -a is a command that displays information about active TCP connections and listening ports on a system. A network administrator can use netstat -a to check if the database engine is listening on a certain port, as well as verify if there are any connections established to or from that port. References: <https://www.comptia.org/blog/what-is-netstat>

**NEW QUESTION 63**

- (Topic 2)

A business is using the local cable company to provide Internet access. Which of the following types of cabling will the cable company MOST likely use from the demarcation point back to the central office?

- A. Multimode
- B. Cat 5e
- C. RG-6
- D. Cat 6
- E. 100BASE-T

**Answer:** C

**Explanation:**

RG-6 is a type of coaxial cable that is commonly used by cable companies to provide Internet access from the demarcation point back to the central office. It has a thicker conductor and better shielding than RG-59, which is another type of coaxial cable. Multimode and Cat 5e are types of fiber optic and twisted pair cables respectively, which are not typically used by cable companies. Cat 6 and 100BASE-T are standards for twisted pair cables, not types of cabling.

**NEW QUESTION 64**

- (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 66**

- (Topic 2)

Which of the following services can provide data storage, hardware options, and scalability to a third-party company that cannot afford new devices?

- A. SaaS
- B. IaaS
- C. PaaS
- D. DaaS

**Answer:** B

**Explanation:**

IaaS stands for Infrastructure as a Service, which is a cloud computing model that provides virtualized computing resources such as servers, storage, and networking over the Internet. IaaS can provide data storage, hardware options, and scalability to a third-party company that cannot afford new devices by allowing them to rent or lease the infrastructure they need from a cloud provider. The company can pay only for what they use and scale up or down as needed. References: <https://www.comptia.org/blog/what-is-iaas>

**NEW QUESTION 70**

- (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 71**

- (Topic 2)

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

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

**Answer: E**

**Explanation:**

Using an out-of-band access method is the best way to prevent unauthorized access to the legacy switches that do not support cryptographic functions. Out-of-band access is a method of accessing a network device through a dedicated channel that is separate from the main network traffic. Out-of-band access can use physical connections such as serial console ports or dial-up modems, or logical connections such as VPNs or firewalls. Out-of-band access provides more security and reliability than in-band access, which uses the same network as the data traffic and may be vulnerable to attacks or failures. References: <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/configuration/15mt/fundamentals-15-mt-book/cf-out-band-mgmt.html>

**NEW QUESTION 76**

- (Topic 2)

A network technician needs to correlate security events to analyze a suspected intrusion. Which of the following should the technician use?

- A. SNMP
- B. Log review
- C. Vulnerability scanning
- D. SIEM

**Answer: D**

**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 network technician can use SIEM to correlate security events to analyze a suspected intrusion, as SIEM 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-siem>

**NEW QUESTION 77**

- (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 80**

- (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 83

- (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 84

- (Topic 2)

A company wants to implement a large number of WAPs throughout its building and allow users to be able to move around the building without dropping their connections Which of the following pieces of equipment would be able to handle this requirement?

- A. A VPN concentrator
- B. A load balancer
- C. A wireless controller
- D. A RADIUS server

**Answer: C**

#### Explanation:

A wireless controller would be able to handle the requirement of implementing a large number of WAPs throughout the building and allowing users to move around without dropping their connections. A wireless controller is a device that centrally manages and configures multiple wireless access points (WAPs) on a network. It can provide features such as load balancing, roaming, security, QoS, and monitoring for the wireless network. A wireless controller can also support wireless mesh networks, where some WAPs act as relays for other WAPs to extend the wireless coverage. References: <https://www.cisco.com/c/en/us/products/wireless/wireless-lan-controller/index.html>

### NEW QUESTION 89

- (Topic 2)

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

- A. The lab environment's IDS is blocking the network traffic 1 he technician can whitelist the new application in the IDS
- B. The lab environment is located in the DM2, and traffic to the LAN zone is denied by default
- C. The technician can move the computer to another zone or request an exception from the administrator.
- D. The lab environment has lost connectivity to the company router, and the switch needs to be rebooted
- E. The technician can get the key to the wiring closet and manually restart the switch
- F. The lab environment is currently set up with hubs instead of switches, and the requests are getting bounced back The technician can submit a request for upgraded equipment to management.

**Answer: B**

#### Explanation:

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

### NEW QUESTION 90

- (Topic 2)

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 95

- (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 97

- (Topic 2)

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 102

- (Topic 2)

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

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

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 103

- (Topic 2)

A network field technician is installing and configuring a secure wireless network. The technician performs a site survey. Which of the following documents would MOST likely be created as a result of the site survey?

- A. Physical diagram
- B. Heat map
- C. Asset list
- D. Device map

**Answer: B**

#### Explanation:

A heat map would most likely be created as a result of the site survey. A heat map is a graphical representation of the wireless signal strength and coverage in a given area. It can show the location of APs, antennas, walls, obstacles, interference sources, and dead zones. It can help with planning, optimizing, and

troubleshooting wireless networks. References: <https://www.netspotapp.com/what-is-a-wifi-heatmap.html>

#### NEW QUESTION 105

- (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 107

- (Topic 2)

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

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

**Answer:** B

#### Explanation:

The default gateway is the setting that the user most likely misconfigured on the PC that caused it to be unable to access websites by both FQDN and IP. The default gateway is a device, usually a router or a firewall, that connects a local network to other networks such as the Internet. It acts as an intermediary between devices on different networks and forwards packets based on their destination IP addresses. If the default gateway is not configured correctly on a PC, it will not be able to communicate with devices outside its local network, such as web servers or DNS servers. References:

<https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/16448-default-gateway.html>

#### NEW QUESTION 109

- (Topic 2)

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

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

**Answer:** A

#### Explanation:

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

<https://www.comptia.org/blog/what-is-a-virtual-switch>

#### NEW QUESTION 113

- (Topic 2)

A network administrator is talking to different vendors about acquiring technology to support a new project for a large company. Which of the following documents will MOST likely need to be signed before information about the project is shared?

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

**Answer:** B

#### Explanation:

NDA stands for Non-Disclosure Agreement, which is a legal contract between two or more parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes, but wish to restrict access to by others. A network administrator may need to sign an NDA before sharing information about a new project with different vendors, as the project may involve sensitive or proprietary data that the company wants to protect from competitors or unauthorized use. References: <https://www.adobe.com/sign/esignature-resources/sign-nda.html>

#### NEW QUESTION 116

- (Topic 2)

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

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

**Answer: D**

#### Explanation:

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

#### NEW QUESTION 119

- (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 123

- (Topic 2)

Which of the following uses the destination IP address to forward packets?

- A. A bridge
- B. A Layer 2 switch
- C. A router
- D. A repeater

**Answer: C**

#### Explanation:

A router is a device that uses the destination IP address to forward packets between different networks. A bridge and a Layer 2 switch operate at the data link layer and use MAC addresses to forward frames within the same network. A repeater is a device that amplifies or regenerates signals at the physical layer.

#### NEW QUESTION 126

- (Topic 3)

A network administrator notices excessive wireless traffic occurring on an access point after normal business hours. The access point is located on an exterior wall. Which of the following should the administrator do to limit wireless access outside the building?

- A. Set up a private VLAN.
- B. Disable roaming on the WAP.
- C. Change to a directional antenna.
- D. Stop broadcasting of the SSID.

**Answer: C**

#### Explanation:

A directional antenna is a type of antenna that radiates or receives radio waves in a specific direction. This can help limit wireless access outside the building by focusing the signal towards the intended area and reducing the signal strength in other directions. A private VLAN is a feature that isolates network devices within a VLAN. Disabling roaming on the WAP prevents wireless clients from switching to another WAP when the signal is weak. Stopping broadcasting of the SSID hides the network name from wireless clients, but does not prevent them from connecting if they know the SSID.

References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 3.1: Given a scenario, install and configure wireless LAN infrastructure and implement the appropriate technologies in support of wireless capable devices.

#### NEW QUESTION 131

- (Topic 3)

A WAN technician reviews activity and identifies newly installed hardware that is causing outages over an eight-hour period. Which of the following should be considered FIRST?

- A. Network performance baselines
- B. VLAN assignments
- C. Routing table
- D. Device configuration review

**Answer:** D

**Explanation:**

The most likely cause of outages due to newly installed hardware is a misconfiguration of the device settings. Therefore, the first step should be to review the device configuration and check for any errors or inconsistencies that might affect the WAN connectivity. References: Network+ Study Guide Objective 2.1: Explain the importance of network documentation.

**NEW QUESTION 133**

- (Topic 3)

A customer needs to distribute Ethernet to multiple computers in an office. The customer would like to use non-proprietary standards. Which of the following blocks does the technician need to install?

- A. 110
- B. 66
- C. Bix
- D. Krone

**Answer:** A

**Explanation:**

A 110 block is a type of punch-down block that is used to distribute Ethernet to multiple computers in an office. A punch-down block is a device that connects one group of wires to another group of wires by using a special tool that pushes the wires into slots on the block. A 110 block is a non-proprietary standard that supports up to Category 6 cabling and can be used for voice or data applications. References: <https://www.comptia.org/training/books/network-n10-008-study-guide> (page 64)

**NEW QUESTION 137**

- (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 140**

- (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 144**

- (Topic 3)

Which of the following is the most secure connection used to inspect and provide controlled internet access when remote employees are connected to the corporate network?

- A. Site-to-site VPN
- B. Full-tunnel VPN
- C. Split-tunnel VPN
- D. SSH

**Answer: B**

**Explanation:**

A full-tunnel VPN is a type of virtual private network (VPN) that encrypts and routes all the traffic from the remote device to the corporate network, regardless of the destination or protocol. This provides a secure connection for the remote employees to access the corporate resources, as well as inspect and control the internet access through the corporate firewall and proxy servers. A full-tunnel VPN also prevents any leakage of sensitive data or exposure to malicious attacks from the public internet. A full-tunnel VPN is more secure than a split-tunnel VPN, which only encrypts and routes the traffic destined for the corporate network, while allowing the traffic for other destinations to bypass the VPN and use the local internet connection. A site-to-site VPN is a type of VPN that connects two or more networks, such as branch offices or data centers, over the internet. It is not suitable for connecting individual remote employees to the corporate network. SSH stands for Secure Shell, and it is a protocol that allows secure remote login and command execution over an encrypted channel. It is not a type of VPN, and it does not provide controlled internet access. References: CompTIA Network+ N10-008 Cert Guide, Chapter 5, Section 5.3

**NEW QUESTION 146**

- (Topic 3)

A technician is investigating why a PC cannot reach a file server with the IP address 192.168.8.129. Given the following TCP/IP network configuration:

Link-local IPv6 address	fe80::28e4:a7cc:a55e:4bea
IPv4 address	192.168.8.105
Subnet mask	255.255.255.128
Default gateway	192.168.8.1

Which of the following configurations on the PC is incorrect?

- A. Subnet mask
- B. IPv4 address
- C. Default gateway
- D. IPv6 address

**Answer: C**

**Explanation:**

The default gateway is the IP address of the router that connects the PC to other networks. The default gateway should be on the same subnet as the PC's IPv4 address. However, in this case, the default gateway is 192.168.9.1, which is on a different subnet than the PC's IPv4 address of 192.168.8.105. Therefore, the default gateway configuration on the PC is incorrect and prevents the PC from reaching the file server on another subnet.

**NEW QUESTION 151**

- (Topic 3)

Which of the following best describe the functions of Layer 2 of the OSI model? (Select two).

- A. Local addressing
- B. Error preventing
- C. Logical addressing
- D. Error detecting
- E. Port addressing
- F. Error correcting

**Answer: AD**

**Explanation:**

Layer 2 of the OSI model, also known as the data link layer, is responsible for physical addressing and error detecting. Physical addressing refers to the use of MAC addresses to identify and locate devices on a network segment. Error detecting refers to the use of techniques such as checksums and CRCs to identify and correct errors in the data frames.

References:

? OSI Model | Computer Networking | CompTIA1

**NEW QUESTION 156**

- (Topic 3)

A wireless technician is working to upgrade the wireless infrastructure for a company. The company currently uses the 802.11g wireless standard on all access points. The company requires backward compatibility and is requesting the least expensive solution. Which of the following should the technician recommend to the company?

- A. 802.11a
- B. 802.11ac
- C. 802Hax
- D. 802.11n

**Answer: D**

**Explanation:**

\* 802.11n is a wireless standard that supports data rates up to 600 Mbps and operates in both 2.4 GHz and 5 GHz frequency bands. 802.11n is backward

compatible with 802.11g, which operates only in 2.4 GHz band. 802.11n is the least expensive solution that can upgrade the wireless infrastructure for the company, as it does not require replacing all the access points or wireless devices

**NEW QUESTION 160**

- (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 165**

- (Topic 3)

Which of the following is the IEEE link cost for a Fast Ethernet interface in STP calculations?

- A. 2
- B. 4
- C. 19
- D. 100

**Answer:** D

**Explanation:**

The IEEE standard for link cost for a Fast Ethernet interface is 100, and for a Gigabit Ethernet interface is 19. These values are based on the bandwidth of the interface, with lower values indicating a higher-bandwidth interface.

**NEW QUESTION 167**

- (Topic 3)

Which of the following topologies is designed to fully support applications hosted in on- premises data centers, public or private clouds, and SaaS services?

- A. SDWAN
- B. MAN
- C. PAN
- D. MPLS

**Answer:** A

**NEW QUESTION 170**

- (Topic 3)

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

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

**Answer:** AF

**NEW QUESTION 171**

- (Topic 3)

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

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

**Answer:** D

**NEW QUESTION 173**

- (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 174

- (Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 176

- (Topic 3)

A network architect is developing documentation for an upcoming IPv4/IPv6 dual-stack implementation. The architect wants to shorten the following IPv6 address: ef82:0000:0000:0000:0000:1ab1:1234:1bc2. Which of the following is the MOST appropriate shortened version?

- A. ef82:0:1ab1:1234:1bc2
- B. ef82:0::1ab1:1234:1bc2
- C. ef82:0:0:0:0:1ab1:1234:1bc2
- D. ef82::1ab1:1234:1bc2

**Answer:** D

#### Explanation:

The most appropriate shortened version of the IPv6 address ef82:0000:0000:0000:0000:1ab1:1234:1bc2 is ef82::1ab1:1234:1bc2. IPv6 addresses are 128-bit hexadecimal values that are divided into eight groups of 16 bits each, separated by colons. IPv6 addresses can be shortened by using two rules: omitting leading zeros within each group, and replacing one or more consecutive groups of zeros with a double colon (::). Only one double colon can be used in an address. Applying these rules to the given address results in ef82::1ab1:1234:1bc2. References: CompTIA Network+ N10-008 Certification Study Guide, page 114; The Official CompTIA Network+ Student Guide (Exam N10-008), page 5-7.

#### NEW QUESTION 177

- (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 182

- (Topic 3)

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

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 184

- (Topic 3)

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

- A. SNMPv3

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

**Answer:** BD

#### NEW QUESTION 189

- (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 192

- (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 193

- (Topic 3)

Users in a branch can access an In-house database server, but it is taking too long to fetch records. The analyst does not know whether the issue is being caused by network latency. Which of the following will the analyst MOST likely use to retrieve the metrics that are needed to resolve this issue?

- A. SNMP
- B. Link state
- C. Syslog
- D. QoS
- E. Traffic shaping

**Answer:** A

#### NEW QUESTION 196

- (Topic 3)

Which of the following devices is used to configure and centrally manage access points installed at different locations?

- A. Wireless controller
- B. Load balancer
- C. Proxy server
- D. VPN concentrator

**Answer:** A

#### Explanation:

Access points (APs) can be configured and centrally managed using a wireless LAN controller (WLC). A WLC is a device that connects to multiple APs and provides centralized management and control of those APs. The WLC can be used to configure settings such as wireless network parameters, security settings, and quality of service (QoS) policies. Additionally, the WLC can be used to monitor the status of connected APs, track client connections, and gather statistics on network usage. Some vendors such as Cisco, Aruba, Ruckus, etc. provide wireless LAN controllers as part of their wireless networking solutions.

#### NEW QUESTION 201

- (Topic 3)

Which of the following is most likely to be implemented to actively mitigate intrusions on a host device?

- A. HIDS
- B. MDS
- C. HIPS
- D. NIPS

**Answer:** A

**Explanation:**

HIDS (host-based intrusion detection system) is a type of security software that monitors and analyzes the activity on a host device, such as a computer or a server. HIDS can detect and alert on intrusions, such as malware infections, unauthorized access, configuration changes, or policy violations. HIDS can also actively mitigate intrusions by blocking or quarantining malicious processes, files, or network connections<sup>1</sup>.

HIPS (host-based intrusion prevention system) is similar to HIDS, but it can also prevent intrusions from happening in the first place by enforcing security policies and rules on the host device<sup>2</sup>. MDS (multilayer switch) is a network device that combines the functions of a switch and a router, and it does not directly protect a host device from intrusions<sup>3</sup>. NIPS (network-based intrusion prevention system) is a network device that monitors and blocks malicious traffic on the network level, and it does not operate on the host device level<sup>4</sup>.

**NEW QUESTION 205**

- (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 206**

- (Topic 3)

A large number of PCs are obtaining an APIPA IP address, and a number of new computers were added to the network. Which of the following is MOST likely causing the PCs to obtain an APIPA address?

- A. Rogue DHCP server
- B. Network collision
- C. Incorrect DNS settings
- D. DHCP scope exhaustion

**Answer:** D

**Explanation:**

DHCP scope exhaustion means that there are no more available IP addresses in the DHCP server's pool of addresses to assign to new devices on the network. When this happens, the devices will use APIPA (Automatic Private IP Addressing) to self-configure an IP address in the range of 169.254.0.1 to 169.254.255.254. These addresses are not routable and can only communicate with other devices on the same local network.

A rogue DHCP server (A) is an unauthorized DHCP server that can cause IP address conflicts or security issues by assigning IP addresses to devices on the network. A network collision (B) is a situation where two or more devices try to send data on the same network segment at the same time, causing interference and data loss. Incorrect DNS settings © can prevent devices from resolving domain names to IP addresses, but they do not affect the DHCP process.

**NEW QUESTION 207**

- (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 212**

- (Topic 3)

A technician is expanding a wireless network and adding new access points. The company requires that each access point broadcast the same SSID. Which of the

following should the technician implement for this requirement?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 217**

- (Topic 3)

Which of the following types of attacks can be used to gain credentials by setting up rogue APs with identical corporate SSIDs?

- A. VLAN hopping
- B. Evil twin
- C. DNS poisoning
- D. Social engineering

**Answer:** B

**NEW QUESTION 222**

- (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 223**

- (Topic 3)

A company streams video to multiple devices across a campus. When this happens, several users report a degradation of network performance. Which of the following would MOST likely address this issue?

- A. Enable IGMP snooping on the switches.
- B. Implement another DHCP server.
- C. Reconfigure port tagging for the video traffic.
- D. Change the SSID of the APs

**Answer:** A

**NEW QUESTION 225**

- (Topic 3)

A technician is trying to install a VoIP phone, but the phone is not turning on. The technician checks the cable going from the phone to the switch, and the cable is good. Which of the following actions IS needed for this phone to work?

- A. Add a POE injector
- B. Enable MDIX.
- C. Use a crossover cable.
- D. Reconfigure the port.

**Answer:** A

**NEW QUESTION 228**

- (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 233

- (Topic 3)

A company is moving to a new building designed with a guest waiting area that has existing network ports. Which of the following practices would BEST secure the network?

- A. Ensure all guests sign an NDA.
- B. Disable unneeded switchports in the area.
- C. Lower the radio strength to reduce Wi-Fi coverage in the waiting area.
- D. Enable MAC filtering to block unknown hardware addresses.

**Answer:** B

#### Explanation:

One of the best practices to secure the network would be to disable unneeded switchports in the guest waiting area. This will prevent unauthorized users from connecting to the network through these ports. It's important to identify which switchports are not in use and disable them, as this will prevent unauthorized access to the network. Other practices such as ensuring all guests sign an NDA, lowering the radio strength to reduce Wi-Fi coverage in the waiting area and enabling MAC filtering to block unknown hardware addresses are not as effective in securing the network as disabling unneeded switchports. Enforcing an NDA with guests may not stop a malicious user from attempting to access the network, reducing the radio strength only limits the Wi-Fi coverage, and MAC filtering can be easily bypassed by hackers.

#### NEW QUESTION 238

- (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 242

- (Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 246

- (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 248

- (Topic 3)

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

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

**Answer: D**

**Explanation:**

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

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

**NEW QUESTION 250**

- (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 254**

- (Topic 3)

When accessing corporate network resources, users are required to authenticate to each application they try to access. Which of the following concepts does this BEST represent?

- A. SSO
- B. Zero Trust
- C. VPN
- D. Role-based access control

**Answer: B**

**NEW QUESTION 258**

- (Topic 3)

A network administrator is troubleshooting a connection to a remote site. The administrator runs a command and sees the following output:

```
Tracing route to 10.10.0.22 over a maximum of 30 hops:
 0  14ms  20ms  15ms  192.168.1.253
 1  10ms  15ms  12ms  172.16.0.21
 2   5ms   10ms  10ms  10.10.5.3
 3  10ms  15ms  12ms  10.12.2.1
 4   5ms   10ms  10ms  10.10.5.3
 5  10ms  15ms  12ms  10.12.2.1
 6   5ms   10ms  10ms  10.10.5.3
 7  10ms  15ms  12ms  10.12.2.1
```

Which of the following is the cause of the connection issue?

- A. Routing loop
- B. Asymmetrical routing
- C. Broadcast storm
- D. Switching loop

**Answer: A**

**Explanation:**

The cause of the connection issue is a routing loop. A routing loop is a situation where a packet is forwarded in circles between routers, never reaching its destination. A routing loop can be caused by misconfigured or inconsistent routing tables, or by routing protocols that do not update their information properly. A routing loop can be detected by using the traceroute command, which shows the path taken by a packet from the source to the destination. The traceroute output in the image shows that the packet is bouncing back and forth between two routers, 10.12.2.1 and 10.12.2.2, indicating a routing loop. References: CompTIA Network+ N10-008 Certification Study Guide, page 181; The Official CompTIA Network+ Student Guide (Exam N10-008), page 7-9.

**NEW QUESTION 259**

- (Topic 3)

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

- A. IP spoofing

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

**Answer: D**

**Explanation:**

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

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

References

2: Understanding Targeted Attacks: What is a Targeted Attack? 3: Types of attacks - Security on the web | MDN

1: What is an on-path attacker? | Cloudflare

4: [What is a Rogue DHCP Server? - Definition from Techopedia]

**NEW QUESTION 260**

- (Topic 3)

Which of the following fouling protocols is generally used by major ISPs for handing large- scale internet traffic?

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

**Answer: D**

**NEW QUESTION 261**

- (Topic 3)

A network technician receives a report about a performance issue on a client PC that is connected to port 1/3 on a network switch. The technician observes the following configuration output from the switch:

1/1	Client PC	Connected	Full	1000
1/2	Client PC	Connected	Full	1000
1/3	Client PC	Connected	Full	10

Which of the following is a cause of the issue on port 1/3?

- A. Speed
- B. Duplex
- C. Errors
- D. VLAN

**Answer: A**

**NEW QUESTION 262**

- (Topic 3)

An IT technician needs to increase bandwidth to a server. The server has multiple gigabit ports. Which of the following can be used to accomplish this without replacing hardware?

- A. STP
- B. 802.1Q
- C. Duplex
- D. LACP

**Answer: D**

**Explanation:**

LACP stands for Link Aggregation Control Protocol and is a protocol that allows multiple physical ports to be combined into a single logical port. This can increase bandwidth, redundancy, and load balancing for a server. LACP is part of the IEEE 802.3ad standard for link aggregation. STP stands for Spanning Tree Protocol and is a protocol that prevents loops in a network by blocking redundant links. 802.1Q is a standard for VLAN (Virtual Local Area Network) tagging, which allows multiple logical networks to share the same physical infrastructure. Duplex is a mode of communication that determines how data is transmitted and received on a link. Full duplex allows simultaneous transmission and reception, while half duplex allows only one direction at a time.

References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 1.5: Compare and contrast network cabling types, standards and speeds.

**NEW QUESTION 266**

- (Topic 3)

A network security administrator needs to monitor the contents of data sent between a secure network and the rest of the company. Which of the following monitoring methods will accomplish this task?

- A. Port mirroring
- B. Flow data
- C. Syslog entries

D. SNMP traps

**Answer:** A

**Explanation:**

Port mirroring is a method of monitoring network traffic by copying the data packets from one port to another port on the same switch or router. This allows the network security administrator to analyze the contents of the data sent between different networks without affecting the performance or security of the original traffic. Port mirroring can be configured to capture all traffic or only specific types of traffic, such as VLANs, protocols, or IP addresses.

References:

- ? Port Mirroring - CompTIA Network+ N10-008 Domain 3.1 - YouTube1
- ? CompTIA Network+ Certification Exam Objectives, page 142

**NEW QUESTION 267**

- (Topic 3)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 271**

- (Topic 3)

Which of the following is most likely responsible for the security and handling of personal data in Europe?

- A. GDPR
- B. SCADA
- C. SAML
- D. PCI DSS

**Answer:** A

**Explanation:**

GDPR stands for General Data Protection Regulation, which is a European Union regulation on information privacy and security. It applies to any organization that collects or processes personal data of individuals in the EU, and it sets out rules and requirements for data protection, consent, breach notification, and enforcement1

References1: [https://en.wikipedia.org/wiki/General\\_Data\\_Protection\\_Regulation](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation)

**NEW QUESTION 272**

SIMULATION - (Topic 3)

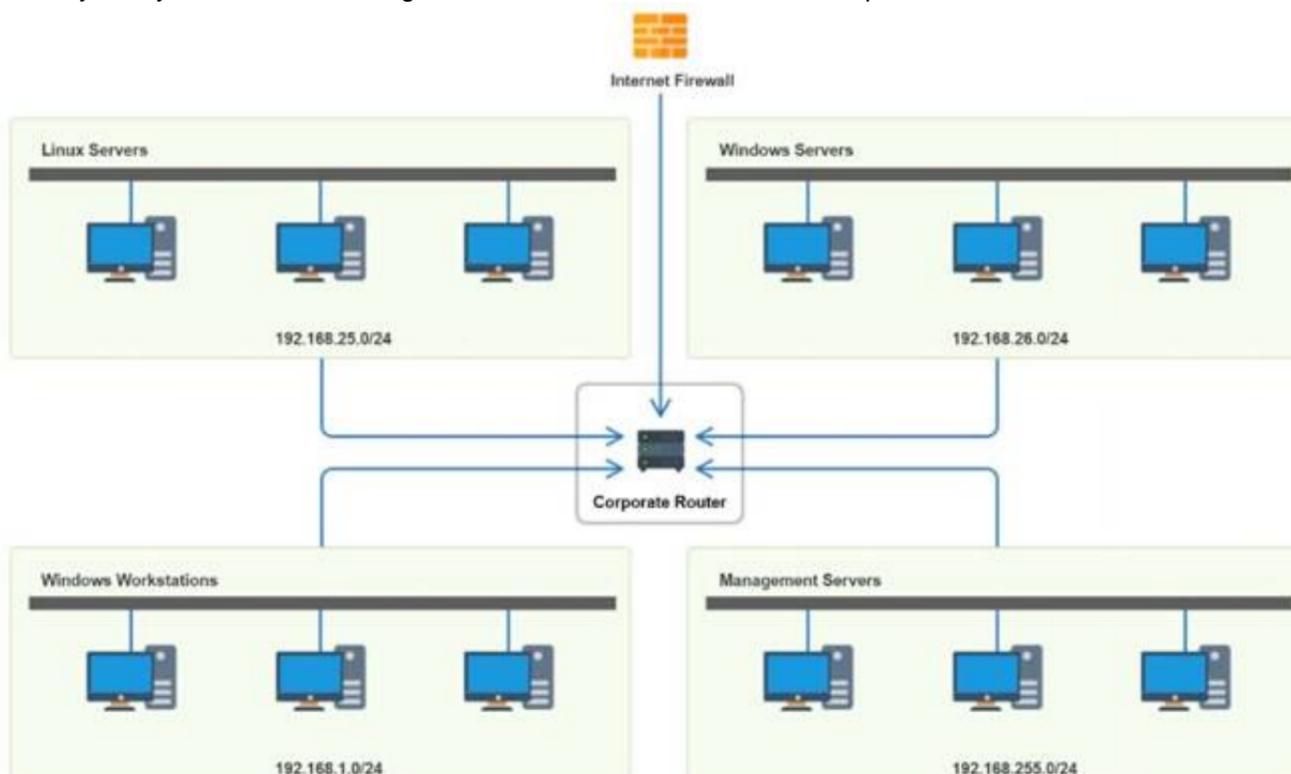
You have been tasked with implementing an ACL on the router that will:

- \* 1. Permit the most commonly used secure remote access technologies from the management network to all other local network segments
- \* 2. Ensure the user subnet cannot use the most commonly used remote access technologies in the Linux and Windows Server segments.
- \* 3. Prohibit any traffic that has not been specifically allowed.

**INSTRUCTIONS**

Use the drop-downs to complete the ACL

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



Router Access Control List					
Rule	Source	Destination	Protocol	Service	Action
1	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
2	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
3	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
4	192.168.255.0	192.168.26.0	TCP	SMB	Allow
5	192.168.255.0	Any	Any	Any	Deny
6	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
7	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
8	192.168.1.0	Any	Any	Any	Allow
9	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	Any	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Router Access Control List					
Rule	Source	Destination	Protocol	Service	Action
1	192.168.255.0	192.168.26.0	TCP	SSH	Allow
2	192.168.255.0	192.168.25.0	TCP	SSH	Allow
3	192.168.255.0	192.168.1.0	TCP	SSH	Allow
4	192.168.255.0	192.168.26.0	TCP	SMB	Allow
5	192.168.255.0	Any	Any	Any	Deny
6	192.168.1.0	Any	TCP	RDP	Deny
7	192.168.1.0	Any	TCP	VNC	Deny
8	192.168.1.0	Any	Any	Any	Allow
9	Any	Any	Any	Any	Deny

**NEW QUESTION 276**

- (Topic 3)

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

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 279**

SIMULATION - (Topic 3)

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

**INSTRUCTIONS**

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

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

The simulation interface displays several monitoring widgets:

- Wireless Client Distribution:** A pie chart showing the distribution of wireless clients.
- Wireless Users Connected - 24 Hours:** A line graph showing the number of wireless users connected over a 24-hour period.
- Ram Usage:** A bar chart showing memory usage across different servers.
- Processor Usage:** A bar chart showing CPU usage across different servers.
- WAN Health:** A bar chart comparing the health of WAN1 and WAN2.
- Uplink Performance Table:**

Uplink Name	Uplink Speed	Total Usage	Average Throughput	Loss	Average Latency	Jitter
WAN1	10G	26,690GB Up/1,708.4GB Down	353MBs Up/23.42MBs Down	2.51%	24ms	9.5ms
WAN2	1G	930GB Up/138GB Down	12.21MBs Up/1.82MBs Down	0.01%	11ms	3.9ms

**Question:** Which WAN station should be preferred for VoIP traffic?

**Answer:** WAN 1

Network Health
Device Monitoring
Show Question
Reset All Answers

Device Status

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

Top Hosts

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

**Which device is experiencing connectivity issues?**

Select Answer

- Router A
- Router B
- WAP1
- WAP2
- WirelessController
- Switch A
- Switch B
- DHCP Server
- Web Server
- APP Server

Router A

**Which workstation IP is generating the MOST traffic?**

Select Answer

- 10.1.99.28
- 10.1.99.14
- 10.1.99.10
- 10.1.99.22
- 10.1.99.24
- 206.208.133.10
- 206.208.133.9
- 10.1.50.14
- 10.1.50.13
- 10.1.59.81
- 10.1.90.53
- 10.1.90.55

206.208.133.9

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Network Health:

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

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

? WAN 1:

? WAN 2:

For VoIP traffic, low latency and jitter are particularly important to ensure voice quality. While WAN 1 has higher bandwidth and throughput, it also has higher latency and jitter

compared to WAN 2. However, WAN 2 has much lower loss, lower latency, and lower jitter, which are more favorable for VoIP traffic that is sensitive to delays and variation in packet arrival times.

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

Network Health | Device Monitoring

Show Question | Reset All Answers

Uplink Name	Uplink Speed	Total Usage	Average Throughput	Loss	Average Latency	Jitter
WAN1	10G	26,690GB Up/1,708.4GB Down	353MBs Up/23.42MBs Down	2.51%	24ms	9.5ms
WAN2	1G	930GB Up/138GB Down	12.21MBs Up/1.82MBs Down	0.01%	11ms	3.9ms

Which WAN station should be preferred for VoIP traffic?

**Device Monitoring:**

the device that is experiencing connectivity issues is the APP Server or Router 1, which has a status of Down. This means that the server is not responding to network requests or sending any data. You may want to check the physical connection, power supply, and configuration of the APP Server to troubleshoot the problem.

Network Health | Device Monitoring

Show Question | Reset All Answers

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

Which device is experiencing connectivity issues?

Which workstation IP is generating the MOST traffic?

A screenshot of a computer  
 Description automatically generated

**NEW QUESTION 281**

- (Topic 3)

A network technician is responding to an issue with a local company. To which of the following documents should the network technician refer to determine the scope of the issue?

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

**Answer: D**

**Explanation:**

SLA stands for Service Level Agreement, and it is a contract that defines the expectations and responsibilities between a service provider and a customer. SLA can specify the quality, availability, and performance metrics of the service, as well as the penalties for non-compliance and the procedures for resolving issues. SLA can help the network technician determine the scope of the issue by providing the baseline and target values for the service, the escalation process and contacts, and the service credits or remedies for the customer.

CompTIA Network+ N10-008 Cert Guide - Chapter 15: Network Troubleshooting Methodology 35: What is a Service Level Agreement (SLA)? | ITIL | AXELOS

**NEW QUESTION 284**

- (Topic 3)

A technician is equipped with a tablet, a smartphone, and a laptop to troubleshoot a switch with the help of support over the phone. However, the technician is

having issues interconnecting all these tools in troubleshooting the switch. Which Of the following should the technician use to gain connectivity?

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

**Answer:** A

**Explanation:**

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

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

**NEW QUESTION 287**

- (Topic 3)

Which of the following situations would require an engineer to configure subinterfaces?

- A. In a router-on-a-stick deployment with multiple VLANs
- B. In order to enable inter-VLAN routing on a multilayer switch
- C. When configuring VLAN trunk links between switches
- D. After connecting a router that does not support 802.1Q VLAN tags

**Answer:** A

**Explanation:**

A router-on-a-stick is a configuration that allows a single router interface to route traffic between multiple VLANs on a network. A router-on-a-stick requires sub-interfaces to be configured on the router interface, one for each VLAN. Each sub-interface is assigned a VLAN ID and an IP address that belongs to the corresponding VLAN subnet. The router interface is connected to a switch port that is configured as a trunk port, which allows traffic from multiple VLANs to pass through. The router then performs inter-VLAN routing by forwarding packets between the sub-interfaces based on their destination IP addresses. Inter-VLAN routing is a process that allows devices on different VLANs to communicate with each other. Inter-VLAN routing can be performed by a router-on-a-stick configuration, as explained above, or by a multilayer switch that has routing capabilities. A multilayer switch does not require sub-interfaces to be configured for inter-VLAN routing; instead, it uses switch virtual interfaces (SVIs) that are associated with each VLAN. An SVI is a logical interface that represents a VLAN on a switch and has an IP address that belongs to the VLAN subnet. The switch then performs inter-VLAN routing by forwarding packets between the SVIs based on their destination IP addresses.

VLAN trunking is a method that allows traffic from multiple VLANs to be carried over a single link between switches or routers. VLAN trunking requires the use of a tagging protocol, such as 802.1Q, that adds a header to each frame that identifies its VLAN ID. VLAN trunking does not require sub-interfaces to be configured on the switches or routers; instead, it uses trunk ports that are configured to allow or deny traffic from specific VLANs. The switches or routers then forward packets between the trunk ports based on their VLAN IDs.

\* 802.1Q is a standard that defines how VLAN tagging and trunking are performed on Ethernet networks.

\* 802.1Q adds a 4-byte header to each frame that contains a 12-bit field for the VLAN ID and a 3-bit field for the priority level. 802.1Q does not require sub-interfaces to be configured on the switches or routers; instead, it uses trunk ports that are configured to support 802.1Q tagging and untagging. The switches or routers then forward packets between the trunk ports based on their VLAN IDs and priority levels.

**NEW QUESTION 292**

- (Topic 3)

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

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

**Answer:** B

**NEW QUESTION 296**

- (Topic 3)

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

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

**Answer:** C

**Explanation:**

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

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

**NEW QUESTION 300**

- (Topic 3)

Which of the following network types is composed of computers that can all communicate with one another with equal permissions and allows users to directly

share what is on or attached to their computers?

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 305**

- (Topic 3)

A company needs a redundant link to provide a channel to the management network in an incident response scenario. Which of the following remote access methods provides the BEST solution?

- A. Out-of-band access
- B. Split-tunnel connections
- C. Virtual network computing
- D. Remote desktop gateways

**Answer: A**

**Explanation:**

Out-of-band access is a remote access method that provides a separate, independent channel for accessing network devices and systems. Out-of-band access uses a dedicated network connection or a separate communication channel, such as a dial-up or cellular connection, to provide access to network devices and systems. This allows an administrator to access the management network even if the primary network connection is unavailable or impaired. Out-of-band access is a good solution for providing a redundant link to the management network in an incident response scenario because it can be used to access the network even if the primary connection is unavailable or impaired.

**NEW QUESTION 306**

- (Topic 3)

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

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

**Answer: B**

**Explanation:**

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

References:

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

**NEW QUESTION 311**

- (Topic 3)

Which of the following can be used to aggregate logs from different devices and would make analysis less difficult?

- A. Syslog
- B. SIEM
- C. Event logs
- D. NetFlow

**Answer: B**

**Explanation:**

SIEM stands for Security Information and Event Management, and it is a system that collects, normalizes, and analyzes log data from different sources in a centralized platform. SIEM can help identify security incidents, monitor network performance, and generate reports and alerts. SIEM can make log analysis less difficult by providing a unified view of the log data, correlating events across different devices, and applying rules and filters to detect anomalies and patterns<sup>12</sup>.

References: 1: CompTIA Network+ N10-008 Cert Guide - Chapter 14: Network Monitoring<sup>32</sup>: Log Aggregation: What It Is & How It Works | Datadog<sup>4</sup>

**NEW QUESTION 314**

- (Topic 3)

A technician is consolidating a topology with multiple SSIDs into one unique SSID deployment. Which of the following features will be possible after this new configuration?

- A. Seamless roaming
- B. Basic service set
- C. WPA

D. MU-MIMO

**Answer:** A

#### NEW QUESTION 318

- (Topic 3)

Which of the following is a requirement when certifying a network cabling as Cat 7?

- A. Ensure the patch panel is certified for the same category.
- B. Limit 10Gb transmissions to 180ft (55m).
- C. Use F-type connectors on the network terminations.
- D. Ensure the termination standard is TIA/EIA-568-A.

**Answer:** D

#### Explanation:

Category 7 (Cat 7) is a cabling standard that supports 10GBASE-T Ethernet connections up to 100 meters (328 feet). In order for a cabling system to be certified as Cat 7, all components, including the patch panel, must meet the TIA/EIA-568-A standard. This standard requires the use of shielded cables with F-type connectors for the network terminations. Reference: CompTIA Network+ Study Manual, 8th Edition, page 158.

#### NEW QUESTION 319

- (Topic 3)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 322

- (Topic 3)

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

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

**Answer:** E

#### Explanation:

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

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

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

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

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

References

What is CVE?

What is a Service Level Agreement (SLA)? Guide to Enterprise Patch Management Planning

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

#### NEW QUESTION 324

- (Topic 3)

A network technician is troubleshooting a connection to a web server. The Technician is unable to ping the server but is able to verify connectivity to the web service using Tenet. Which of the following protocols is being blocked by the firewall?

A. UDP

- B. ARP
- C. ICMP
- D. TCP

**Answer: C**

**Explanation:**

ICMP (Internet Control Message Protocol) is a protocol that is used to send error and control messages between network devices, such as ping requests and replies. ICMP is being blocked by the firewall, which prevents the network technician from pinging the web server. TCP (Transmission Control Protocol) is a protocol that provides reliable and ordered delivery of data between network devices, such as web service requests and responses using HTTP (Hypertext Transfer Protocol). TCP is not being blocked by the firewall, which allows the network technician to verify connectivity to the web service using Telnet. UDP (User Datagram Protocol) is a protocol that provides fast and efficient delivery of data between network devices, but does not guarantee reliability or order. UDP is used for applications such as streaming media or online gaming. ARP (Address Resolution Protocol) is a protocol that resolves IP addresses to MAC addresses on a local network. References: [CompTIA Network+ Certification Exam Objectives], Domain 2.0 Networking Concepts, Objective 2.1: Compare and contrast OSI and TCP/IP models, Subobjective: TCP/IP model layers (Application/Transport/Internet/Network Interface)

**NEW QUESTION 328**

- (Topic 3)

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

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

**Answer: D**

**NEW QUESTION 331**

- (Topic 3)

A network engineer is installing hardware in a newly renovated data center. Major concerns that were addressed during the renovation included air circulation, building power redundancy, and the need for continuous monitoring. The network engineer is creating alerts based on the following operation specifications:

AC input voltage	100 to 240VAC
AC maximum input current	<2.7A at 100V
Redundant power supply	Yes
Operating temperature	32–104°F (0–40°C)
Storage temperature	-4–149°F (-20–65°C)
Operating humidity	10–85%
Storage humidity	5–95%

Which of the following should the network engineer configure?

- A. Environmental monitoring alerts for humidity greater than 95%
- B. SIEM to parse syslog events for a failed power supply
- C. SNMP traps to report when the chassis temperature exceeds 95°F (35°C)
- D. UPS monitoring to report when input voltage drops below 220VAC

**Answer: C**

**Explanation:**

The alert that the network engineer should configure based on the operation specifications is SNMP traps to report when the chassis temperature exceeds 95°F (35°C). SNMP (Simple Network Management Protocol) is a protocol that allows network devices to communicate their status and performance information to a central management system, called an SNMP manager. SNMP traps are messages that are sent by network devices to notify the SNMP manager of an event or condition that requires attention, such as an error, a failure, or a threshold violation. In this case, the network engineer should configure SNMP traps on the network devices to send an alert when their chassis temperature exceeds 95°F (35°C), which is the maximum operating temperature specified in the table. This alert would help the network engineer monitor and troubleshoot any overheating issues that could affect the network performance or availability. References: CompTIA Network+ N10-008 Certification Study Guide, page 228; The Official CompTIA Network+ Student Guide (Exam N10-008), page 8-11.

**NEW QUESTION 332**

- (Topic 3)

A network technician is troubleshooting an issue that involves connecting to a server via SSH. The server has one network interface that does not support subinterfaces. The technician runs a command on the server and receives the following output:

```

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

```

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

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

Which of the following best explains the issue?

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

**Answer:** C

#### NEW QUESTION 335

- (Topic 3)

A technician is investigating packet loss to a device that has varying data bursts throughout the day. Which of the following will the technician MOST likely configure to resolve the issue?

- A. Flow control
- B. Jumbo frames
- C. Duplex
- D. Port mirroring

**Answer:** A

#### Explanation:

Ethernet flow control is a mechanism for temporarily stopping the transmission of data on Ethernet family computer networks. The goal of this mechanism is to avoid packet loss in the presence of network congestion.

Flow control is a mechanism that allows a device to regulate the amount of data it receives from another device, ensuring that the receiving device is not overwhelmed with data. If the device experiencing packet loss is receiving large bursts of data at times when it is not able to process it quickly enough, configuring flow control could help prevent packets from being lost.

"In theory, flow control can help with situations like a host that can't keep up with the flow of traffic. It enables the host to send an Ethernet PAUSE frame, which asks the switch to hold up for some amount of time so the host can catch its breath. If the switch can, it'll buffer transmissions until the pause expires, and then start sending again. If the host catches up early, it can send another PAUSE frame with a delay of zero to ask the switch to resume. In practice, flow control can cause latency trouble for modern real-time applications such as VoIP, and the same needs are usually met by QoS"

#### NEW QUESTION 336

- (Topic 3)

A network administrator requires redundant routers on the network, but only one default gateway is configurable on a workstation. Which of the following will allow for redundant routers with a single IP address?

- A. EIGRP
- B. VRRP
- C. MPLS
- D. STP

**Answer:** B

#### Explanation:

Virtual Router Redundancy Protocol (VRRP) is a protocol that allows for redundant routers on the network with a single IP address. VRRP works by creating a virtual router that consists of one master router and one or more backup routers. The virtual router has its own IP address and MAC address that are shared among the routers in the group. The master router responds to traffic sent to the virtual router's IP address, while the backup routers monitor the master router's status. If the master router fails, one of the backup routers takes over as the new master router and continues to respond to traffic. This way, VRRP provides high availability and fault tolerance for the network. References: <https://www.comptia.org/training/books/network-n10-008-study-guide> (page 230)

#### NEW QUESTION 337

.....

## **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 First Try
- \* N10-008 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

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