

# CompTIA

## Exam Questions N10-009

CompTIA Network+ Exam



### NEW QUESTION 1

- (Exam Topic 1)

A network technician is installing new software on a Windows-based server in a different geographical location. Which of the following would be BEST for the technician to use to perform this task?

- A. RDP
- B. SSH
- C. FTP
- D. DNS

**Answer:** A

#### Explanation:

RDP (Remote Desktop Protocol) is the best option for a network technician to use when installing new software on a Windows-based server in a different geographical location. This protocol allows the technician to connect to the server remotely and control it as if they were physically present.

References:

➤ Network+ N10-007 Certification Exam Objectives, Objective 2.2: Given a scenario, implement the appropriate network-based security and troubleshoot common connectivity issues.

### NEW QUESTION 2

- (Exam 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:

Short 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 3

- (Exam Topic 1)

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

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

**Answer:** C

#### Explanation:

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

### NEW QUESTION 4

- (Exam Topic 1)

Wireless users are reporting intermittent internet connectivity. Connectivity is restored when the users disconnect and reconnect, utilizing the web authentication process each time. The network administrator can see the devices connected to the APs at all times. Which of the following steps will MOST likely determine the cause of the issue?

- A. Verify the session time-out configuration on the captive portal settings
- B. Check for encryption protocol mismatch on the client's wireless settings
- C. Confirm that a valid passphrase is being used during the web authentication
- D. Investigate for a client's disassociation caused by an evil twin AP

**Answer:** A

#### Explanation:

A captive portal is a web page that requires users to authenticate before they can access the internet. If the session time-out configuration is too short, users may experience intermittent internet connectivity and have to reconnect using the web authentication process each time. The network administrator can verify the session time-out configuration on the captive portal settings and adjust it if needed. References: CompTIA Network+ Certification Exam Objectives Version 2.0 (Exam Number: N10-006), Domain 1.0 Network Architecture, Objective 1.8 Explain the purposes and use cases for advanced networking devices.

**NEW QUESTION 5**

- (Exam Topic 1)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 6**

- (Exam Topic 1)

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

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

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

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

**Answer:** A

**Explanation:**

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

References:

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

**NEW QUESTION 7**

- (Exam Topic 1)

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

Configure LACP on the switchports

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

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

**Answer:** C

**Explanation:**

NIC teaming is a technique that combines two or more network interface cards (NICs) on a server into a single logical interface that can increase bandwidth, provide redundancy, and balance traffic. NIC teaming can be configured with different modes and algorithms depending on the desired outcome. Link Aggregation Control Protocol (LACP) is a protocol that enables NIC teaming by dynamically bundling multiple links between two devices into one logical link. References: [https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)), <https://docs.microsoft.com/en-us/windows-server/networking/technologies/nic-teaming/nic-teaming>

**NEW QUESTION 8**

- (Exam Topic 1)

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

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

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

- A. Reconfigure the channels to reduce overlap

- B. Replace the omni antennas with directional antennas
- C. Update the SSIDs on all the APs
- D. Decrease power in AP 3 and AP 4

**Answer:** A

**Explanation:**

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

References:

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

**NEW QUESTION 9**

- (Exam Topic 1)

Which of the following transceiver types can support up to 40Gbps?

- A. SFP+
- B. QSFP+
- C. QSFP
- D. SFP

**Answer:** B

**Explanation:**

QSFP+ is a transceiver type that can support up to 40Gbps. It stands for Quad Small Form-factor Pluggable Plus and uses four lanes of data to achieve high-speed transmission. It is commonly used for data center and high-performance computing applications. References:

[https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/data\\_sheet\\_c78-6600](https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/data_sheet_c78-6600)

**NEW QUESTION 10**

- (Exam 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 10**

- (Exam Topic 1)

Within the realm of network security, Zero Trust:

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

**Answer:** A

**Explanation:**

Zero Trust is a security framework that requires all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. Zero Trust prevents attackers from moving laterally through a system by applying granular policies and controls based on the principle of least privilege and by segmenting and encrypting data flows across the network. References: [https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)),

<https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/>

**NEW QUESTION 14**

- (Exam Topic 1)

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

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

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

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

**Answer:** A

**Explanation:**

The reason why the alerts are not being received is that the network device is not configured to log that level to the syslog server. The severity level for the events

may need to be adjusted in order for them to be sent to the syslog server. References: Network+ Certification Study Guide, Chapter 8: Network Troubleshooting

#### NEW QUESTION 16

- (Exam 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 21

- (Exam Topic 1)

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 23

- (Exam Topic 1)

Client devices cannot enter a network, and the network administrator determines the DHCP scope is exhausted. The administrator wants to avoid creating a new DHCP pool. Which of the following can the administrator perform to resolve the issue?

- A. Install load balancers
- B. Install more switches
- C. Decrease the number of VLANs
- D. Reduce the lease time

**Answer: D**

#### Explanation:

To resolve the issue of DHCP scope exhaustion without creating a new DHCP pool, the administrator can reduce the lease time. By decreasing the lease time, the IP addresses assigned by DHCP will be released back to the DHCP scope more quickly, allowing them to be assigned to new devices.

References:

- CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 2: The OSI Model and Networking Protocols, Objective 2.3: Given a scenario, implement and configure the appropriate addressing schema.
- <https://www.networkcomputing.com/data-centers/10-tips-optimizing-dhcp-performance>

#### NEW QUESTION 26

- (Exam Topic 1)

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

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

**Answer: A**

#### Explanation:

Using a bottom-to-top approach means starting from the physical layer and moving up the OSI model to troubleshoot a network problem. Checking for a link light is a physical layer check that verifies the connectivity of the network cable and device. References:

<https://www.professormesser.com/network-plus/n10-007/troubleshooting-methodologies-2/>

#### NEW QUESTION 31

- (Exam Topic 1)

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

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

**Answer:** B

**Explanation:**

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

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

**NEW QUESTION 32**

- (Exam Topic 1)

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

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

**Answer:** C

**Explanation:**

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

[https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)), <https://www.techopedia.com/definition/950/subnet-mask>

**NEW QUESTION 37**

- (Exam 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 42**

- (Exam 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 46**

- (Exam Topic 2)

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

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

**Answer:** B

**Explanation:**

Giants are packets that exceed the configured MTU (Maximum Transmission Unit) of a switchport or interface, which causes them to be dropped or fragmented by the switch or router. The MTU is the maximum size of a packet that can be transmitted without fragmentation on a given medium or protocol. Giants can indicate misconfiguration or mismatch of MTU values between devices or interfaces on a network, which can cause performance issues or errors. CRC errors are errors that occur when the cyclic redundancy check (CRC) value of a packet does not match the calculated CRC value at the destination, which indicates corruption or alteration of data during transmission due to noise, interference, faulty cabling, etc., but not necessarily exceeding MTU values. Runt packets 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 48**

- (Exam Topic 2)

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

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

**Answer:** E

**Explanation:**

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

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

**NEW QUESTION 52**

- (Exam 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-c>

**NEW QUESTION 56**

- (Exam Topic 2)

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

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

**Answer:** B

**Explanation:**

RJ11 is a type of connector that is commonly used for analog phone lines. RJ11 has four wires and six positions, but only two or four of them are used. A technician can crimp an RJ11 connector to a new phone line to install an analog desk phone for a new receptionist. References:

<https://www.comptia.org/blog/what-is-rj11>

**NEW QUESTION 57**

- (Exam Topic 2)

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

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

D. Encryption type

**Answer:** A

**Explanation:**

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

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

**NEW QUESTION 62**

- (Exam Topic 2)

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

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

**Answer:** B

**Explanation:**

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

<https://www.vmware.com/topics/glossary/content/hypervisor>

**NEW QUESTION 63**

- (Exam Topic 2)

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

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

**Answer:** B

**Explanation:**

VPN (Virtual Private Network) is the most appropriate way to enable secure remote printing. VPN is a technology that creates a secure and encrypted tunnel over a public network such as the Internet. It allows remote users or sites to access a private network as if they were directly connected to it. VPN can be used for various purposes such as accessing corporate resources, bypassing geo-restrictions, or enhancing privacy and security. VPN can also be used for remote printing by allowing users to connect to a printer on the private network and send print jobs securely over the VPN tunnel. References:

<https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-work>

**NEW QUESTION 66**

- (Exam 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 71**

- (Exam Topic 2)

A network technician is investigating an issue with a desktop that is not connecting to the network. The desktop was connecting successfully the previous day, and no changes were made to the environment. The technician locates the switchport where the device is connected and observes the LED status light on the switchport is not lit even though the desktop is turned on Other devices that are plugged into the switch are connecting to the network successfully Which of the following is MOST likely the cause of the desktop not connecting?

- A. Transceiver mismatch
- B. VLAN mismatch
- C. Port security
- D. Damaged cable
- E. Duplex mismatch

**Answer:** D

**Explanation:**

A damaged cable is most likely the cause of the desktop not connecting to the network. A damaged cable can cause physical layer issues such as loss of signal, attenuation, interference, or crosstalk. These issues can prevent the desktop from establishing a link with the switch and result in the LED status light on the switchport being off. Other possible causes of physical layer issues are faulty connectors, ports, or transceivers. References: <https://www.cisco.com/c/en/us/support/docs/lan-switching/ethernet/14119-37.html>

**NEW QUESTION 74**

- (Exam Topic 2)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 76**

- (Exam Topic 2)

The following instructions were published about the proper network configuration for a videoconferencing device:

"Configure a valid static RFC1918 address for your network. Check the option to use a connection over NAT." Which of the following is a valid IP address configuration for the device?

- A. FE80::1
- B. 100.64.0.1
- C. 169.254.1.2
- D. 172.19.0.2
- E. 224.0.0.12

**Answer:** D

**Explanation:**

\* 172.19.0.2 is a valid IP address configuration for the device that uses a static RFC1918 address for the network and allows for a connection over NAT (Network Address Translation). RFC1918 addresses are private IP addresses that are not routable on the public Internet and are used for internal networks. The RFC1918 address ranges are 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. NAT is a technique that translates private IP addresses to public IP addresses when communicating with external networks, such as the Internet. FE80::1 is an IPv6 link-local address that is not a static RFC1918 address and does not allow for a connection over NAT. 100.64.1.1 is an IPv4 address that belongs to the shared address space range (100.64.0.0/10) that is used for carrier-grade NAT (CGN) between service providers and subscribers, which is not a static RFC1918 address and does not allow for a connection over NAT. 169.254.1.2 is an IPv4 link-local address that is automatically assigned by a device when it cannot obtain an IP address from a DHCP server or manual configuration, which is not a static RFC1918 address and does not allow for a connection over NAT. 224.0.0.12 is an IPv4 multicast address that is used for VRRP (Virtual Router Redundancy Protocol), which is not a static RFC1918 address and does not allow for a connection over NAT.

**NEW QUESTION 81**

- (Exam Topic 2)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 82**

- (Exam Topic 2)

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

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

**Answer:** A

**Explanation:**

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

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

#### NEW QUESTION 85

- (Exam Topic 2)

A company that uses VoIP telephones is experiencing intermittent issues with one-way audio and dropped conversations. The manufacturer says the system will work if ping times are less than 50ms. The company has recorded the following ping times:

10ms	10ms	10ms	100ms	70ms	5ms	5ms	80ms	100ms	5ms	5ms
------	------	------	-------	------	-----	-----	------	-------	-----	-----

Which of the following is MOST likely causing the issue?

- A. Attenuation
- B. Latency
- C. VLAN mismatch
- D. Jitter

**Answer: D**

#### Explanation:

Jitter is most likely causing the issue of intermittent one-way audio and dropped conversations for the company that uses VoIP telephones. Jitter is a variation in delay of packets arriving at the destination. It can cause choppy or distorted audio quality for VoIP applications, especially over WAN links that have limited bandwidth and high latency. The recommended jitter for VoIP is less than 10ms. The company has recorded ping times that exceed 50ms, which indicates high jitter and latency on their network. References: <https://www.voip-info.org/voip-jitter/> 1

#### NEW QUESTION 87

- (Exam Topic 2)

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

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

**Answer: D**

#### Explanation:

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

#### NEW QUESTION 91

- (Exam 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 95

- (Exam 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 100**

- (Exam Topic 3)

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

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

**Answer:** D

**Explanation:**

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

Therefore, the correct answer is option D, NetFlow.

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

**NEW QUESTION 103**

- (Exam 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 107**

- (Exam 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 109**

- (Exam Topic 3)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 113**

- (Exam Topic 3)

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

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

**Answer:** A

**Explanation:**

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

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

**NEW QUESTION 114**

- (Exam Topic 3)

A technician thinks one of the router ports is flapping. Which of the following available resources should the technician use in order to determine if the router is flapping?

- A. Audit logs
- B. NetFlow
- C. Syslog
- D. Traffic logs

**Answer:** C

**Explanation:**

Syslog is a protocol that allows network devices to send event messages to a centralized server or console for logging and analysis<sup>1</sup>. Syslog can help a technician to determine if a router port is flapping by providing timestamps, severity levels, and descriptions of the events that occur on the router, such as interface up or down, link state change, or error messages. Syslog can also help to identify the cause and frequency of the port flapping and troubleshoot the issue.

Audit logs are records of actions or events that occur on a system or network, such as user login, file access, configuration change, or policy violation. Audit logs can help to monitor and verify the activities and behaviors of users, devices, or applications on a system or network. Audit logs can also help to detect and investigate security incidents, compliance issues, or performance problems. However, audit logs do not provide detailed information about router port flapping.

NetFlow is a protocol that collects and analyzes network traffic data for monitoring and troubleshooting purposes<sup>2</sup>. NetFlow can help to identify the sources, destinations, volumes, and types of traffic on a network. NetFlow can also help to optimize network performance, security, and capacity planning. However, NetFlow does not provide detailed information about router port flapping.

Traffic logs are records of network traffic that pass through a device or application, such as a firewall, proxy, or web server. Traffic logs can help to monitor and filter the network traffic based on rules or policies. Traffic logs can also help to detect and prevent malicious traffic, such as malware, attacks, or unauthorized access. However, traffic logs do not provide detailed information about router port flapping.

**NEW QUESTION 119**

- (Exam 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 124**

- (Exam Topic 3)

During a risk assessment which of the following should be considered when planning to mitigate high CPU utilization of a firewall?

- A. Recovery time objective
- B. Uninterruptible power supply
- C. NIC teaming
- D. Load balancing

**Answer:** D

**Explanation:**

The recovery time objective (RTO) is the maximum tolerable length of time that a computer, system, network or application can be down after a failure or disaster occurs. This does nothing to help with CPU utilization. Load balancing does this.

**NEW QUESTION 128**

- (Exam Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 131

- (Exam Topic 3)

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

- A. F-type connector
- B. TIA/EIA-568-B
- C. LC
- D. SC

**Answer:** B

#### Explanation:

The termination that the technician should use when running a cable from the ISP's port to the front desk is B. TIA/EIA-568-B. This is a standard pin-out for Cat 6 cables that is used for Ethernet and other network physical layers1. It specifies how to arrange the eight wires in an RJ45 connector, which is a common type of connector for network cables.

#### NEW QUESTION 134

- (Exam Topic 3)

A network technician is implementing a solution that will allow end users to gain access to multiple applications after logging on. Which of the following authentication methods would allow this type of access?

- A. SSO
- B. LDAP
- C. EAP
- D. TACACS+

**Answer:** A

#### NEW QUESTION 138

- (Exam Topic 3)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 139

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 144

- (Exam Topic 3)

A technician knows the MAC address of a device and is attempting to find the device's IP address. Which of the following should the technician look at to find the IP address? (Select TWO).

- A. ARP table
- B. DHCP leases
- C. IP route table
- D. DNS cache
- E. MAC address table

F. STP topology

**Answer:** BE

#### NEW QUESTION 148

- (Exam Topic 3)

A network administrator needs to provide evidence to confirm that recent network outages were caused by increased traffic generated by a recently released application. Which of the following actions will BEST support the administrator's response?

- A. Generate a network baseline report for comparison.
- B. Export the firewall traffic logs.
- C. Collect the router's NetFlow data.
- D. Plot interface statistics for dropped packets.

**Answer:** C

#### NEW QUESTION 153

- (Exam 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 158

- (Exam Topic 3)

Which of the following bandwidth management techniques uses buffers at the client side to prevent TCP retransmissions from occurring when the ISP starts to drop packets of specific types that exceed the agreed traffic rate?

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

**Answer:** D

#### NEW QUESTION 160

- (Exam Topic 3)

ARP spoofing would normally be a part of:

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

**Answer:** A

#### NEW QUESTION 161

- (Exam Topic 3)

A large metropolitan city is looking to standardize the ability for police department laptops to connect to the city government's VPN. The city would like a wireless solution that provides the largest coverage across the city with a minimal number of transmission towers. Latency and overall bandwidth needs are not high priorities. Which of the following would BEST meet the city's needs?

- A. 5G
- B. LTE
- C. Wi-Fi 4
- D. Wi-Fi 5
- E. Wi-Fi 6

**Answer:** B

#### NEW QUESTION 165

- (Exam Topic 3)

An IT technician successfully connects to the corporate wireless network at a bank. While performing some tests, the technician observes that the physical

address of the DHCP server has changed even though the network connection has not been lost. Which of the following would BEST explain this change?

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 168**

- (Exam Topic 3)

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

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

**Answer: C**

**Explanation:**

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

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

**NEW QUESTION 170**

- (Exam Topic 3)

A network administrator is trying to add network redundancy for the server farm. Which of the following can the network administrator configure to BEST provide this capability?

- A. VRRP
- B. DNS
- C. UPS
- D. RPO

**Answer: A**

**Explanation:**

VRRP is an open standard protocol, which is used to provide redundancy in a network. It is a network layer protocol (protocol number-112). The number of routers (group members) in a group acts as a virtual logical router which will be the default gateway of all the local hosts. If one router goes down, one of the other group members can take place for the responsibilities for forwarding the traffic.

**NEW QUESTION 174**

- (Exam Topic 3)

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 175**

- (Exam Topic 3)

Which of the following BEST describes a spirit-tunnel client-to-server VPN connection?

- A. The client sends an network traffic down the VPN tunnel
- B. The client has two different IP addresses that can be connected to a remote site from two different ISPs to ensure availability
- C. The client sends some network traffic down the VPN tunnel and other traffic to the local gateway.
- D. The client connects to multiple remote sites at the same time

**Answer: C**

**Explanation:**

In a split-tunnel VPN, the client can access both the local network and the remote network simultaneously, with some network traffic sent through the VPN tunnel and other traffic sent to the local gateway. This approach allows for more efficient use of bandwidth and reduces the load on the VPN server. It also allows the client to continue accessing local resources while connected to the remote network.

**NEW QUESTION 178**

- (Exam Topic 3)

To comply with an industry regulation, all communication destined to a secure server should be logged and archived on a storage device. Which of the following can be configured to fulfill this requirement?

- A. QoS traffic classification
- B. Port mirroring
- C. Flow control
- D. Link Aggregation Control Protocol

**Answer:** B

**NEW QUESTION 179**

- (Exam Topic 3)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 183**

- (Exam Topic 3)

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

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

**Answer:** A

**Explanation:**

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

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

**NEW QUESTION 188**

- (Exam Topic 3)

A newly installed VoIP phone is not getting the DHCP IP address it needs to connect to the phone system. Which of the following tasks needs to be completed to allow the phone to operate correctly?

- A. Assign the phone's switchport to the correct VLAN
- B. Statically assign the phone's gateway address.
- C. Configure a route on the VoIP network router.
- D. Implement a VoIP gateway

**Answer:** A

**NEW QUESTION 190**

- (Exam Topic 3)

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

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

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 194**

- (Exam 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 197**

- (Exam Topic 3)

Given the following Information:

Connection	Cable length	Cable type	Configuration
PC A to switch 1	394ft (120m)	Cat 5	Straight through
Switch 1 to switch 2	3.3ft (1m)	Cat 6	Crossover
Switch 2 to PC B	16ft (5m)	Cat 5	Straight through

Which of the following would cause performance degradation between PC A and PC B'?

- A. Attenuation
- B. Interference
- C. Decibel loss
- D. Incorrect pinout

**Answer:** D

**NEW QUESTION 200**

- (Exam 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 204**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 207**

- (Exam Topic 3)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 210**

- (Exam Topic 3)

Which of the following is a valid and cost-effective solution to connect a fiber cable into a network switch without available SFP ports?

- A. Use a media converter and a UTP cable
- B. Install an additional transceiver module and use GBICs
- C. Change the type of connector from SC to F-type
- D. Use a loopback adapter to make the connection

**Answer:** A

#### NEW QUESTION 213

- (Exam Topic 3)

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

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 214

- (Exam Topic 3)

A technician is configuring a wireless network and needs to ensure users agree to an AUP before connecting. Which of the following should be implemented to achieve this goal?

- A. Captive portal
- B. Geofencing
- C. Wireless client isolation
- D. Role-based access

**Answer:** A

#### NEW QUESTION 219

- (Exam Topic 3)

A network engineer developed a plan of action to resolve an ongoing issue. Which of the following steps should the engineer take NEXT?

- A. Verify full system functionality and implement preventative measures.
- B. Implement the solution to resolve the problem.
- C. Document findings, actions, outcomes, and lessons learned.
- D. Establish a theory of probable cause.

**Answer:** B

#### Explanation:

Network troubleshooting is a repeatable process, which means that you can break it down into clear steps that anyone can follow. Identify the Problem. ... Develop a Theory. ... Test the Theory. ... Plan of Action. ... Implement the Solution. ... Verify System Functionality. ... Document the Issue. Theory of probable cause is before Plan of action. <https://www.comptia.org/content/guides/a-guide-to-network-troubleshooting>

#### NEW QUESTION 222

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 227

- (Exam Topic 3)

A company is designing a SAN and would like to use STP as its medium for communication. Which of the following protocols would BEST suit the company's needs?

- A. SFTP
- B. Fibre Channel
- C. iSCSI
- D. FTP

**Answer:** B

**Explanation:**

A SAN also employs a series of protocols enabling software to communicate or prepare data for storage. The most common protocol is the Fibre Channel Protocol (FCP), which maps SCSI commands over FC technology. The iSCSI SANs will employ an iSCSI protocol that maps SCSI commands over TCP/IP.

STP (Spanning Tree Protocol) is a protocol used to prevent loops in Ethernet networks, and it is not a medium for communication in a storage area network (SAN). However, Fibre Channel is a protocol that is specifically designed for high-speed data transfer in SAN environments. It is a dedicated channel technology that provides high throughput and low latency, making it ideal for SANs. Therefore, Fibre Channel would be the best protocol for the company to use for its SAN. SFTP (Secure File Transfer Protocol), iSCSI (Internet Small Computer System Interface), and FTP (File Transfer Protocol) are protocols used for transferring files over a network and are not suitable for use in a SAN environment.

**NEW QUESTION 230**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 231**

- (Exam 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 233**

- (Exam Topic 3)

After a critical power issue, the network team was not receiving UPS status notifications. The network team would like to be alerted on these status changes. Which of the following would be BEST to use for these notifications?

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

**Answer:** A

**NEW QUESTION 236**

- (Exam 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 237**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 241**

- (Exam Topic 3)

Which of the following documents would be used to define uptime commitments from a provider, along with details on measurement and enforcement?

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

**Answer:** B

**Explanation:**

A service level agreement (SLA) is a document that is used to define uptime commitments from a provider, along with details on measurement and enforcement. An SLA is a contract between a service provider and a customer that outlines the level of service that the provider is committed to providing and the terms under which that service will be delivered.

**NEW QUESTION 245**

- (Exam Topic 3)

Which of the following connector types would be used to connect to the demarcation point and provide network access to a cable modem?

- A. F-type
- B. RJ45
- C. LC
- D. RJ11

**Answer:** A

**Explanation:**

An F-type connector is a type of coaxial connector that is commonly used to connect a cable modem to the demarcation point, which is the point at which the cable provider's network ends and the customer's network begins. The F-type connector is a threaded connector that is typically used for television, cable modem, and satellite antenna connections.

**NEW QUESTION 246**

- (Exam Topic 3)

A network administrator needs to monitor traffic on a specific port on a switch. Which of the following should the administrator configure to accomplish the task?

- A. Port security
- B. Port tagging
- C. Port mirroring
- D. Media access control

**Answer:** C

**Explanation:**

Port mirroring is a feature that allows a network technician to monitor traffic on a specific port on a switch by copying all the traffic from that port to another port where a monitoring device is connected. Port mirroring can be used for troubleshooting, analysis, or security purposes, such as detecting network anomalies, performance issues, or malicious activities. References:  
<https://www.comptia.org/training/books/network-n10-008-study-guide> (page 156)

**NEW QUESTION 248**

- (Exam Topic 3)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 252**

- (Exam Topic 3)

A company's data center is hosted at its corporate office to ensure greater control over the security of sensitive data. During times when there are increased workloads, some of the company's non-sensitive data is shifted to an external cloud provider. Which of the following cloud deployment models does this describe?

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

**Answer:** A

**NEW QUESTION 256**

- (Exam Topic 3)

A network engineer is designing a wireless network that has the following requirements:

- Network speed must be higher than 100Mbps
- Must use the 2.4GHz and 5GHz bands

Which of the following 802.11 standards should the engineer select?

- A. 802.11a
- B. 802.11b
- C. 802.11g
- D. 802.11n

**Answer: D**

**Explanation:**

\* 802.11n is a wireless standard that supports up to 600 Mbps data rate and operates in both the 2.4 GHz and 5 GHz frequency bands. 802.11n uses multiple-input multiple-output (MIMO) technology to increase the number of spatial streams and improve the wireless performance and range. 802.11n meets the requirements of the wireless network design.

References: Network+ Study Guide Objective 1.6: Explain the functions of network services.

**NEW QUESTION 257**

- (Exam Topic 3)

A corporate client is experiencing global system outages. The IT team has identified multiple potential underlying causes throughout the enterprise. Each team member has been assigned an area to trouble shoot. Which of the following approaches is being used?

- A. Divide-and-conquer
- B. Top-to-bottom
- C. Bottom-to-top
- D. Determine if anything changed

**Answer: A**

**NEW QUESTION 260**

- (Exam Topic 3)

Network users reported that a recent firmware upgrade to a firewall did not resolve the issue that prompted the upgrade. Which of the following should be performed NEXT?

- A. Reopen the service ticket, request a new maintenance window, and roll back to the anterior firmware version.
- B. Gather additional information to ensure users' concerns are not been caused by a different issue with similar symptoms.
- C. Employ a divide-and-conquer troubleshooting methodology by engaging the firewall vendor's support.
- D. Escalate the issue to the IT management team in order to negotiate a new SLA with the user's manager.

**Answer: B**

**Explanation:**

Before taking any further action, it is important to verify that the problem reported by the users is the same as the one that prompted the firmware upgrade. It is possible that the firmware upgrade did resolve the original issue, but a new or different issue has arisen with similar symptoms. By gathering additional information from the users, such as error messages, screenshots, logs, or network traces, the technician can confirm or rule out this possibility and avoid wasting time and resources on unnecessary steps.

Reopening the service ticket, requesting a new maintenance window, and rolling back to the anterior firmware version (A) is a possible option if the firmware upgrade did not resolve the original issue and caused more problems. However, this should not be done without first verifying that the users' concerns are related to the firmware upgrade and not a different issue.

Employing a divide-and-conquer troubleshooting methodology by engaging the firewall vendor's support © is another possible option if the technician needs assistance from the vendor to diagnose or resolve the issue. However, this should also not be done without first gathering additional information from the users to narrow down the scope of the problem and provide relevant details to the vendor.

Escalating the issue to the IT management team in order to negotiate a new SLA with the user's manager (D) is not a relevant option at this stage. An SLA (Service Level Agreement) is a contract that defines the expectations and responsibilities of both parties in terms of service quality, availability, performance, and response time. Negotiating a new SLA does not address the root cause of the issue or help to resolve it. Moreover, escalating an issue to management should only be done when all other options have been exhausted or when there is a significant impact or risk to the business.

**NEW QUESTION 262**

- (Exam Topic 3)

At which of the following OSI model layers does a MAC filter list for a wireless infrastructure operate?

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

**Answer: D**

**Explanation:**

A MAC filter list is a security feature that allows or denies access to a wireless network based on the MAC address of the device. A MAC address is a unique identifier assigned to a network interface card (NIC) at the physical layer of the OSI model. However, MAC filtering operates at the data link layer of the OSI model, where MAC addresses are used to encapsulate and deliver data frames between devices on the same network segment.

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 266**

- (Exam Topic 3)

A technician is deploying a new SSID for an industrial control system. The control devices require the network to use encryption that employs TKIP and a symmetrical password to connect. Which of the following should the technician configure to ensure compatibility with the control devices?

- A. WPA2-Enterprise
- B. WPA-Enterprise
- C. WPA-PSK
- D. WPA2-PSK

**Answer:** C

**Explanation:**

"WPA uses Temporal Key Integrity Protocol (TKIP) for enhanced encryption. TKIP uses RC4 for the encryption algorithm, and the CompTIA Network+ exam may reference TKIP-RC4 in a discussion of wireless."

" WPA2 uses Counter Mode with Cipher Block Chaining Message Authentication Code

Protocol (CCMP) for integrity checking and Advanced Encryption Standard (AES) for encryption. On the Network+ exam, you might find this referenced as simply CCMP-AES"

**NEW QUESTION 271**

- (Exam Topic 3)

A technician is monitoring a network interface and notices the device is dropping packets. The cable and interfaces, however, are in working order. Which of the following is MOST likely the cause?

- A. OID duplication
- B. MIB mismatch
- C. CPU usage
- D. Encapsulation errors

**Answer:** C

**NEW QUESTION 272**

- (Exam Topic 3)

A network administrator is decommissioning a server. Which of the following will the network administrator MOST likely consult?

- A. Onboarding and off boarding policies
- B. Business continuity plan
- C. Password requirements
- D. Change management documentation

**Answer:** D

**NEW QUESTION 275**

- (Exam Topic 3)

Which of the following would enable a network technician to implement dynamic routing?

- A. An IPS
- B. A bridge
- C. A Layer 3 switch
- D. A hub

**Answer:** C

**NEW QUESTION 278**

- (Exam Topic 3)

While setting up a new workstation, a technician discovers that the network connection is only 100 full duplex (FD), although it is connected to a gigabit switch.

While reviewing the interface information in the switch CLI, the technician notes the port is operating at IOOFD but Shows many RX and TX errors. The technician moves the computer to another switchport and experiences the same issues.

Which of the following is MOST likely the cause of the low data rate and port errors?

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

**Answer:** B

**NEW QUESTION 279**

- (Exam Topic 3)

A company needs to virtualize a replica of its internal physical network without changing the logical topology and the way that devices behave and are managed.

Which of the following technologies meets this requirement?

- A. NFV
- B. SDWAN
- C. VIP
- D. MPLS

**Answer:** A

**Explanation:**

Network Function Virtualization (NFV) is a technology that allows for the virtualization of a replica of a network's physical topology and the way it behaves without changing the logical topology and the way that devices are managed. NFV allows for the virtualization of network functions such as routers, firewalls, and switches, resulting in increased flexibility and scalability. This makes NFV an ideal technology for companies looking to virtualize a replica of their internal physical network.

**NEW QUESTION 283**

- (Exam 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 288**

- (Exam Topic 3)

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

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

**Answer:** BE

**NEW QUESTION 291**

- (Exam Topic 3)

An administrator would like to have two servers at different geographical locations provide fault tolerance and high performance while appearing as one URL to users. Which of the following should the administrator implement?

- A. Load balancing
- B. Multipathing
- C. NIC teaming
- D. Warm site

**Answer:** A

**Explanation:**

Load balancing is a technique that can be used to provide fault tolerance and high performance while appearing as one URL to users. It is achieved by distributing the workload across multiple servers, which are usually located in different geographical locations. This allows for high performance and fault tolerance, as if one server fails, the other will take its place. Additionally, the multiple servers appear as one URL to the users, eliminating the need for the users to switch between servers.

**NEW QUESTION 294**

- (Exam Topic 3)

Logs show an unauthorized IP address entering a secure part of the network every night at 8:00 pm. The network administrator is concerned that this IP address will cause an issue to a critical server and would like to deny the IP address at the edge of the network. Which of the following solutions would address these concerns?

- A. Changing the VLAN of the web server
- B. Changing the server's IP address
- C. Implementing an ACL
- D. Instating a rule on the firewall connected to the web server

**Answer:** D

**NEW QUESTION 299**

- (Exam 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 303**

- (Exam Topic 3)

A network administrator is preparing answers for an annual risk assessment that is required for compliance purposes. Which of the following would be an example

of an internal threat?

- A. An approved vendor with on-site offices
- B. An infected client that pulls reports from the firm
- C. A malicious attacker from within the same country
- D. A malicious attacker attempting to socially engineer access into corporate offices

**Answer:** A

**Explanation:**

Insider threat= insider threat is defined as the threat that an employee or a contractor will use his or her authorized access, wittingly or unwittingly, to do harm

**NEW QUESTION 305**

- (Exam Topic 3)

A network administrator has received calls every day for the past few weeks from three users who cannot access the network. The administrator asks all the users to reboot their PCs, but the same users still cannot access the system. The following day, three different users report the same issue, and the administrator asks them all to reboot their PCs; however, this does not fix the issue. Which of the following is MOST likely occurring?

- A. Incorrect firewall settings
- B. Inappropriate VLAN assignment
- C. Hardware failure
- D. Overloaded CAM table in switch
- E. DHCP scope exhaustion

**Answer:** E

**NEW QUESTION 306**

- (Exam Topic 3)

An IT technician is working on a support ticket regarding an unreachable web-site. The technician has utilized the ping command to the website, but the site is still unreachable. Which of the following tools should the technician use NEXT?

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

**Answer:** B

**Explanation:**

tracert is a command-line tool that can trace the route of a packet from the source to the destination. It can show the number of hops, the IP address and hostname of each router, and the round-trip time for each hop. tracert can help the technician troubleshoot the unreachable website by identifying where the packet is dropped or delayed along the path. ipconfig is a command-line tool that can display and configure the IP settings of a network interface. arp is a command-line tool that can display and manipulate the Address Resolution Protocol (ARP) cache, which maps IP addresses to MAC addresses. netstat is a command-line tool that can display network connections, routing tables, and statistics.

References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 2.4: Given a scenario, use appropriate software tools to troubleshoot connectivity issues.

**NEW QUESTION 309**

- (Exam Topic 3)

A technician notices that equipment is being moved around and misplaced in the server room, even though the room has locked doors and cabinets. Which of the following would be the BEST solution to identify who is responsible?

- A. Install motion detection
- B. Install cameras.
- C. Install tamper detection.
- D. Hire a security guard.

**Answer:** B

**Explanation:**

Installing cameras in the server room is the best solution to identify who is responsible for the equipment being moved and misplaced. Cameras provide a way to monitor the server room in real time and can be used to identify suspicious activity. Additionally, they provide a way to review past activity and allow you to review footage to determine who may be responsible for the misplacement of equipment.

**NEW QUESTION 314**

.....

## 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

### N10-009 Practice Exam Features:

- \* N10-009 Questions and Answers Updated Frequently
- \* N10-009 Practice Questions Verified by Expert Senior Certified Staff
- \* N10-009 Most Realistic Questions that Guarantee you a Pass on Your First Try
- \* N10-009 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The N10-009 Practice Test Here](#)**