

# Exam Questions N10-008

CompTIA Network+Exam

<https://www.2passeasy.com/dumps/N10-008/>



### NEW QUESTION 1

- (Topic 1)

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

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

**Answer:** B

#### Explanation:

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

### NEW QUESTION 2

- (Topic 1)

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

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

**Answer:** D

#### Explanation:

IDS stands for intrusion detection system, which is a network appliance that monitors network traffic and alerts administrators of any suspicious or malicious activity. An IDS can warn of unapproved devices that are accessing the network by detecting anomalies, signatures, or behaviors that indicate unauthorized access attempts or attacks. References: [https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)), <https://www.cisco.com/c/en/us/products/security/what-is-an-intrusion-detection-system-ids.html>

### NEW QUESTION 3

- (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 4

- (Topic 1)

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

IP address:	10.0.0.1
Subnet mask:	255.255.255.0
Gateway:	10.0.0.254

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

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

**Answer:** A

#### Explanation:

Decreasing the lease duration on the DHCP server will cause clients to renew their IP address leases more frequently, freeing up IP addresses for other clients to

use. References: CompTIA Network+ Certification Study Guide, Chapter 3: IP Addressing.

#### NEW QUESTION 5

- (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\\_c78-660083.html](https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/data_sheet_c78-660083.html)

#### NEW QUESTION 6

- (Topic 1)

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 7

- (Topic 1)

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

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

**Answer: D**

#### Explanation:

In a star topology, all devices on a network connect to a central hub or switch, which acts as a common connection point. Ethernet LANs typically use a star topology, with each device connected to a central switch. References: ? Network+ N10-008 Objectives: 2.2 Explain common logical network topologies and their characteristics.

#### NEW QUESTION 8

- (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 internet1. 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 9

- (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 10**

- (Topic 1)

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

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

**Answer:** D

**Explanation:**

MDIX (medium-dependent interface crossover) is a feature that allows network devices to automatically detect and configure the appropriate cabling type, eliminating the need for crossover cables. By enabling MDIX on the switches, a technician can use the original Cat 6 cable to create a crossover connection.

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

**NEW QUESTION 10**

- (Topic 1)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 13**

- (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**

- (Topic 1)

Which of the following is used to track and document various types of known vulnerabilities?

- A. CVE
- B. Penetration testing
- C. Zero-day
- D. SIEM
- E. Least privilege

**Answer:** A

**Explanation:**

CVE stands for Common Vulnerabilities and Exposures, which is a list of publicly disclosed cybersecurity vulnerabilities that is free to search, use, and incorporate into products and services. CVE provides a standardized identifier and description for each vulnerability, as well as references to related sources of information. CVE helps to track and document various types of known vulnerabilities and facilitates communication and coordination among security professionals. 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://cve.mitre.org/cve/>

**NEW QUESTION 20**

- (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 23**

- (Topic 1)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 26**

- (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 27

- (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 31

- (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 32

- (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 33

- (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 38

- (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 42**

- (Topic 2)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 44**

- (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 46**

- (Topic 2)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 48**

- (Topic 2)

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

- A. The lab environment's IDS is blocking the network traffic. The technician can whitelist the new application in the IDS.
- B. The lab environment is located in the DMZ, and traffic to the LAN zone is denied by default.
- C. The technician can move the computer to another zone or request an exception from the administrator.

- D. The lab environment has lost connectivity to the company router, and the switch needs to be rebooted
- 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 52**

- (Topic 2)

A Chief Information Officer (CIO) wants to improve the availability of a company's SQL database Which of the following technologies should be utilized to achieve maximum availability?

- A. Clustering
- B. Port aggregation
- C. NIC teaming
- D. Snapshots

**Answer:** A

**Explanation:**

Clustering is a technique that involves grouping multiple servers or instances together to provide high availability and fault tolerance for a database. Clustering can help improve the availability of a SQL database by allowing automatic failover and load balancing between the cluster nodes. If one node fails or becomes overloaded, another node can take over the database operations without disrupting the service. References: <https://www.educba.com/sql-cluster/>

**NEW QUESTION 53**

- (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 57**

- (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 58**

- (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-works.html>

**NEW QUESTION 61**

- (Topic 2)

A systems administrator is running a VoIP network and is experiencing jitter and high latency. Which of the following would BEST help the administrator determine the cause of these issues?

- A. Enabling RADIUS on the network
- B. Configuring SNMP traps on the network
- C. Implementing LDAP on the network
- D. Establishing NTP on the network

**Answer:** B

**Explanation:**

SNMP (Simple Network Management Protocol) is a protocol that allows network devices to communicate with a network management system (NMS) for monitoring and configuration purposes. SNMP traps are unsolicited messages sent by network devices to the NMS when certain events or conditions occur, such as errors, failures, or thresholds. Configuring SNMP traps on the network would best help the administrator determine the cause of jitter and high latency on a VoIP network, as they would provide real-time alerts and information about the network performance and status. Enabling RADIUS on the network is not relevant to troubleshooting VoIP issues, as RADIUS is a protocol that provides authentication, authorization, and accounting services for network access. Implementing LDAP on the network is also not relevant to troubleshooting VoIP issues, as LDAP is a protocol that provides directory services for storing and querying information about users, groups, devices, etc. Establishing NTP on the network is not directly related to troubleshooting VoIP issues, as NTP is a protocol that synchronizes the clocks of network devices.

**NEW QUESTION 65**

- (Topic 2)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 66**

- (Topic 3)

A network resource was accessed by an outsider as a result of a successful phishing campaign. Which of the following strategies should be employed to mitigate the effects of phishing?

- A. Multifactor authentication
- B. Single sign-on
- C. RADIUS
- D. VPN

**Answer:** A

**Explanation:**

Multifactor authentication is a security measure that requires users to provide multiple pieces of evidence before they can access a network resource. This could include requiring users to enter a username, password, and a code sent to the user's mobile phone before they are allowed access. This ensures that the user is who they say they are, reducing the risk of malicious actors gaining access to network resources as a result of a successful phishing campaign.

**NEW QUESTION 69**

- (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 73**

- (Topic 3)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 74**

- (Topic 3)

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

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

**Answer:** C

**NEW QUESTION 75**

- (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 80**

- (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 84**

- (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 89**

- (Topic 3)

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

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

**Answer:** D

**Explanation:**

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

a PoE injector to boot up. References:

? Part 3 of the current page talks about PoE and PoE injectors as a way to power WAPs.

? [This article] explains how PoE injectors work and how to use them.

**NEW QUESTION 92**

- (Topic 3)

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

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

**Answer:** B

**Explanation:**

A software-defined network (SDN) is a network architecture that decouples the control plane from the data plane and centralizes the network intelligence in a software controller. The control plane is the part of the network that makes decisions about how to route traffic, while the data plane is the part of the network that forwards traffic based on the control plane's instructions. The control layer is the layer in an SDN that contains the controller and the routing protocols that communicate with the network devices. The control layer is responsible for managing and configuring the network devices and providing them with the necessary information to forward traffic. References: <https://www.comptia.org/training/books/network-n10-008-study-guide> (page 378)

**NEW QUESTION 95**

- (Topic 3)

A company is opening a new building on the other side of its campus. The distance from the closest building to the new building is 1,804ft (550m). The company needs to connect the networking equipment in the new building to the Other buildings on the campus without using a repeater. Which Of the following transceivers should the company use?

- A. 10GBASE-SW
- B. 10GBASE-LR
- C. 10GBASE-LX4 over multimode fiber
- D. 10GBASE-SR

**Answer:** B

**Explanation:**

10GBASE-LR is a standard for 10 Gbps Ethernet over single-mode fiber optic cable. It can support a maximum distance of 6.2 miles (10 km), which is much longer than the distance between the buildings. 10GBASE-SW, 10GBASE-LX4, and 10GBASE-SR are all standards for 10 Gbps Ethernet over multimode fiber optic cable, which have shorter maximum distances ranging from 984ft (300m) to 1,312ft (400m).

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 96**

- (Topic 3)

A network technician wants to deploy a new wireless access point to reduce user latency. Currently, the organization has the following deployed:

Which of the following channels should the new device broadcast on?

- A. Channel 3
- B. Channel 9

- C. Channel 10
- D. Channel 11

**Answer:** D

**Explanation:**

The best channel for a new wireless access point is one that does not overlap with the existing channels used by other devices. Overlapping channels can cause interference and degrade the performance of the wireless network. According to the web search results, the 2.4 GHz band has 11 channels in the U.S., but only channels 1, 6, and 11 are non-overlapping. Since the existing devices are using channels 1 and 6, the new device should use channel 11 to avoid adjacent-channel interference<sup>12</sup>

References<sup>1</sup>: Why Channels 1, 6 and 11? | MetaGeek <sup>2</sup>: How to Choose the Best Wi-Fi Channels for Your Network - Lifewire

**NEW QUESTION 99**

- (Topic 3)

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

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

**Answer:** B

**NEW QUESTION 102**

- (Topic 3)

Which of the following architectures would allow the network-forwarding elements to adapt to new business requirements with the least amount of operating effort?

- A. Software-defined network
- B. Spine and leaf
- C. Three-tier
- D. Backbone

**Answer:** A

**Explanation:**

Software-defined network (SDN) is a network architecture that allows the network-forwarding elements to be controlled by a centralized software application. This enables the network to adapt to new business requirements with the least amount of operating effort, as the network administrator can configure and manage the network from a single console, without having to manually configure each device individually. SDN also provides more flexibility, agility, and scalability for the network, as it can dynamically adjust the network resources and policies based on the application needs and traffic conditions.

References:

? CompTIA Network+ Certification Exam Objectives, page 5, section 1.3: "Explain the concepts and characteristics of routing and switching."

? Software-Defined Networking – CompTIA Network+ N10-007 – 1.3, video lecture by Professor Messer.

**NEW QUESTION 103**

- (Topic 3)

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

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

**Answer:** A

**Explanation:**

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

References

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

? 2: CompTIA Network+ Certification Exam Objectives, page 13

? 3: CompTIA Network+ N10-008 Certification Study Guide, page 250

? 4: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 14

**NEW QUESTION 104**

- (Topic 3)

A network technician wants to find the shortest path from one node to every other node in the network. Which of the following algorithms will provide the FASTEST convergence time?

- A. A static algorithm
- B. A link-state algorithm
- C. A distance-vector algorithm
- D. A path-vector algorithm

**Answer:** B

**Explanation:**

A link-state algorithm is a routing algorithm that uses information about the state of each link in the network to calculate the shortest path from one node to every

other node. A link-state algorithm requires each router to maintain a complete map of the network topology and exchange link-state advertisements with its neighbors periodically or when a change occurs. A link-state algorithm uses a mathematical formula called Dijkstra's algorithm to find the shortest path based on the link costs. A link-state algorithm provides the fastest convergence time because it can quickly detect and adapt to network changes. References: [CompTIA Network+ Certification Exam Objectives], [Link-state routing protocol - Wikipedia]

#### NEW QUESTION 105

- (Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 110

- (Topic 3)

Which of the following fiber connector types is the most likely to be used on a network interface card?

- A. LC
- B. SC
- C. ST
- D. MPO

**Answer:** A

#### Explanation:

LC (local connector) is the most likely fiber connector type to be used on a network interface card, because it is a small form factor connector that can fit more interfaces on a single card. LC connectors use square connectors that have a locking mechanism on the top, similar to an RJ45 copper connector. LC connectors are also compatible with SFP (small form-factor pluggable) modules that are often used to link a gigabit Ethernet port with a fiber network<sup>12</sup>.

References:

? Optical Fiber Connectors – CompTIA Network+ N10-007 – 2.11

? CompTIA Network+ Certification Exam Objectives<sup>2</sup>

#### NEW QUESTION 114

- (Topic 3)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 118

- (Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 120

- (Topic 3)

A technician monitors a switch interface and notices it is not forwarding frames on a trunked port. However, the cable and interfaces are in working order. Which of the following is MOST likely the cause of the issue?

- A. STP policy
- B. Flow control
- C. 802.1Q configuration



D. Frame size

**Answer: C**

**Explanation:**

802.1Q configuration is the most likely cause of the issue where a switch interface is not forwarding frames on a trunked port. 802.1Q is a standard that defines how to create and manage virtual LANs (VLANs) on a switched network. VLANs are logical segments of a network that group devices based on criteria such as function, department, or security level. VLANs can improve network performance, security, and manageability by reducing broadcast domains, isolating traffic, and enforcing policies. A trunked port is a switch port that can carry traffic from multiple VLANs over a single physical link by adding a VLAN tag to each frame. A VLAN tag is a 4-byte header that identifies the VLAN ID and priority of each frame. A trunked port requires 802.1Q configuration to specify which VLANs are allowed or disallowed on the port, and which VLAN is the native or untagged VLAN. If the 802.1Q configuration is incorrect or mismatched between switches, frames may be dropped or misrouted on the trunked port. References: [CompTIA Network+ Certification Exam Objectives], VLAN Trunking Protocol (VTP) Explained | NetworkLessons.com

**NEW QUESTION 124**

- (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 125**

- (Topic 3)

Which of the following is the best action to take before sending a network router to be recycled as electronic waste?

- A. Turn on port security.
- B. Shred the switch hard drive.
- C. Back up and erase the configuration.
- D. Remove the company asset ID tag.

**Answer: C**

**Explanation:**

Before disposing of a network router, it is important to back up and erase the configuration to prevent unauthorized access to sensitive data and network settings. A network router may contain information such as passwords, IP addresses, firewall rules, VPN settings, and other network parameters that could be exploited by hackers or malicious users. By backing up the configuration, you can preserve the network settings for future reference or reuse. By erasing the configuration, you can wipe out the data and restore the router to its factory default state.

**NEW QUESTION 130**

- (Topic 3)

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 133**

- (Topic 3)

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

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

**Answer:** A

**Explanation:**

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

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

**NEW QUESTION 137**

- (Topic 3)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 142**

- (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 143**

- (Topic 3)

During the troubleshooting of an E1 line, the point-to-point link on the core router was accidentally unplugged and left unconnected for several hours. However, the network management team was not notified. Which of the following could have been configured to allow early detection and possible resolution of the issue?

- A. Traps
- B. MIB
- C. OID
- D. Baselines

**Answer:** A

**Explanation:**

Traps are unsolicited messages sent by network devices to a network management system (NMS) when an event or a change in status occurs. Traps can help notify the network management team of any issues or problems on the network, such as a link failure or a device reboot. Traps can also trigger actions or alerts on the NMS, such as sending an email or logging the event. MIB stands for Management Information Base and is a database of information that can be accessed and managed by an NMS using SNMP (Simple Network Management Protocol). OID stands for Object Identifier and is a unique name that identifies a specific variable in the MIB. Baselines are measurements of normal network performance and behavior that can be used for comparison and analysis. References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 2.5: Given a scenario, use remote access methods.

**NEW QUESTION 145**

- (Topic 3)

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

- A. 80.87.78 0 - 80.87.78.14
- B. 80.87.78 0 - 80.87.78.110
- C. 80.87.78 1 - 80.87.78.62
- D. 80.87.78.1 - 80.87.78.158

**Answer:** C

**Explanation:**

The network 80.87.78.0/26 is a Class A network with a subnet mask of /26, which means that it contains 26 bits of network information and 6 bits of host information.  
The range of valid host addresses for this network is 80.87.78.1 to 80.87.78.62. Any addresses outside of this range are reserved for special purposes or are not used.

**NEW QUESTION 150**

- (Topic 3)

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

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

**Answer:** C

**Explanation:**

The time-to-live (TTL) field is the mechanism for ending loops at Layer 3, which is the network layer of the OSI model. The TTL field is an 8-bit field that indicates the maximum time or number of hops that an IP packet can travel before it is discarded. Every time an IP packet passes through a router, the router decrements the TTL value by one. If the TTL value reaches zero, the router drops the packet and sends an ICMP message back to the source, informing that the packet has expired. This way, the TTL field prevents an IP packet from looping endlessly in a network with routing errors or cycles<sup>123</sup>.

The other options are not mechanisms for ending loops at Layer 3. The checksum field is a 16-bit field that is used to verify the integrity of the IP header. The checksum field is calculated by adding all the 16-bit words in the header and taking the one's complement of the result. If the checksum field does not match the calculated value, the IP packet is considered corrupted and discarded<sup>12</sup>. The type field, also known as the type of service (TOS) or differentiated services code point (DSCP) field, is an 8-bit field that is used to specify the quality of service (QoS) or priority of the IP packet. The type field can indicate how the packet should be handled in terms of delay, throughput, reliability, or cost<sup>12</sup>. The protocol field is an 8-bit field that is used to identify the transport layer protocol that is encapsulated in the IP packet. The protocol field can indicate whether the payload is a TCP segment, a UDP datagram, an ICMP message, or another protocol<sup>12</sup>.

**NEW QUESTION 152**

- (Topic 3)

A customer needs six usable IP addresses. Which of the following best meets this requirement?

- A. 255.255.255.128
- B. 255.255.255.192
- C. 255.255.255.224
- D. 255.255.255.240

**Answer:** C

**NEW QUESTION 154**

- (Topic 3)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 155**

- (Topic 3)

A network technician is troubleshooting a port channel issue. When logging in to one of the switches, the technician sees the following information displayed:

Native VLAN mismatch detected on interface g0/1

Which of the following layers of the OSI model is most likely to be where the issue resides?

- A. Layer 2
- B. Layer 3
- C. Layer 5
- D. Layer 6

**Answer:** A

**Explanation:**

Layer 2 of the OSI model is the data link layer, which is responsible for transferring data between adjacent nodes on a network. It uses protocols such as Ethernet, PPP, and HDLC to encapsulate data into frames and add MAC addresses for source and destination identification. It also uses protocols such as STP, LACP, and CDP to manage the physical links and prevent loops, aggregate bandwidth, and discover neighboring devices<sup>12</sup>

A native VLAN mismatch is a common Layer 2 issue that occurs when two switches are connected by a trunk port, but have different native VLANs configured on their interfaces. A native VLAN is the VLAN that is assigned to untagged frames on a trunk port. If the native VLANs do not match, the switches will drop the untagged frames and generate an error message. This can cause connectivity problems and security risks on the network<sup>345</sup>

To resolve a native VLAN mismatch, the network technician should ensure that both switches have the same native VLAN configured on their trunk ports, or use a different port mode such as access or general.

#### NEW QUESTION 157

- (Topic 3)

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

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

**Answer:** C

#### Explanation:

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

#### References

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

#### NEW QUESTION 161

- (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 163

- (Topic 3)

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

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

**Answer:** A

#### Explanation:

Establishing a theory of probable cause is the third step in the general troubleshooting process, after identifying the problem and gathering information. Establishing a theory of probable cause involves using the information gathered to formulate one or more possible explanations for the problem and testing them to verify or eliminate them. In this scenario, the network technician has confirmed the problem exists and should proceed to establish a theory of probable cause based on the information available, such as the network upgrade that was completed the night before. Implementing a solution to fix the problem is the fifth step in the general troubleshooting process, after establishing a plan of action. Implementing a solution involves applying the chosen method or technique to resolve the problem and verifying its effectiveness. In this scenario, the network technician has not established a plan of action yet and should not implement a solution without knowing the cause of the problem. Creating a plan of action to resolve the problem is the fourth step in the general troubleshooting process, after establishing a theory of probable cause. Creating a plan of action involves selecting the best method or technique to address the problem based on the available resources, constraints, and risks. In this scenario, the network technician has not established a theory of probable cause yet and should not create a plan of action without knowing the cause of the problem. Documenting the problem and the solution is the seventh and final step in the general troubleshooting process, after implementing preventive measures. Documenting the problem and the solution involves recording the details of the problem, its symptoms, its cause, its solution, and its preventive measures for future reference and improvement. In this scenario, the network technician has not implemented preventive measures yet and should not document the problem and the solution without resolving and preventing it.

#### NEW QUESTION 164

- (Topic 3)

A network architect needs to create a wireless field network to provide reliable service to public safety vehicles. Which of the following types of networks is the best solution?

- A. Mesh
- B. Ad hoc



- C. Point-to-point
- D. Infrastructure

**Answer:** A

**Explanation:**

A mesh network is the best solution for creating a wireless field network to provide reliable service to public safety vehicles. A mesh network is a type of wireless network that consists of multiple nodes that communicate with each other directly or through intermediate nodes, forming a web-like topology. A mesh network does not rely on a central access point or router, but rather on the cooperation and coordination of the nodes themselves. A mesh network has several advantages for public safety applications, such as:

? High availability and resilience: A mesh network can automatically route around failures or congestion, ensuring that the network remains operational even if some nodes are damaged or disconnected. A mesh network can also self-heal and self-configure, adapting to changes in the network topology or environment.

? Extended coverage and scalability: A mesh network can extend the wireless signal beyond the range of a single node, by using other nodes as relays or repeaters. A mesh network can also accommodate more nodes and devices, by adding more links and paths between them.

? Low cost and easy deployment: A mesh network can reduce the cost and complexity of installing and maintaining a wireless infrastructure, by eliminating the need for expensive cabling, towers, or antennas. A mesh network can also be deployed quickly and flexibly, by simply adding or removing nodes as needed.

A mesh network is especially suitable for public safety vehicles, because it can provide reliable wireless communication in challenging scenarios, such as:

? Disaster response: A mesh network can be deployed rapidly in areas where the existing wireless infrastructure is damaged or unavailable, such as after an earthquake, flood, or fire. A mesh network can also support emergency services, such as fire fighting, search and rescue, or medical assistance, by enabling data, voice, and video transmission among the responders and command centers.

? Mobile surveillance: A mesh network can enable real-time monitoring and control of public safety vehicles, such as police cars, ambulances, or drones, by providing high-bandwidth and low-latency wireless connectivity. A mesh network can also support video streaming, location tracking, remote sensing, or analytics applications for public safety purposes.

? Event management: A mesh network can enhance the security and efficiency of large-scale events, such as concerts, festivals, or parades, by providing wireless coverage and capacity for the event organizers and participants. A mesh network can also support crowd management, traffic control, or public announcement applications for event management.

The other options are not the best solutions for creating a wireless field network to provide reliable service to public safety vehicles. An ad hoc network is a type of wireless network that consists of devices that communicate with each other directly without any central coordination or infrastructure. An ad hoc network is simple and flexible, but it has limited scalability and performance. A point-to-point network is a type of wireless network that consists of two devices that communicate with each other over a single link. A point-to-point network is fast and secure, but it has limited coverage and functionality. An infrastructure network is a type of wireless network that consists of devices that communicate with each other through an access point or router. An infrastructure network is stable and robust, but it has high cost and complexity.

**NEW QUESTION 169**

- (Topic 3)

A network administrator is looking for a solution to extend Layer 2 capabilities and replicate backups between sites. Which of the following is the best solution?

- A. Security Service Edge
- B. Data center interconnect
- C. Infrastructure as code
- D. Zero trust architecture

**Answer:** B

**Explanation:**

Data center interconnect (DCI) is a solution that allows Layer 2 connectivity and data replication between geographically dispersed data centers. DCI can be implemented using various technologies, such as optical networks, MPLS, VPNs, or Ethernet. DCI can provide benefits such as improved disaster recovery, load balancing, resource pooling, and cloud services.

References:

? Data Center Interconnect - CompTIA Network+ N10-008 Domain 1.4 - YouTube

? CompTIA Network+ Certification Exam Objectives, page 92

**NEW QUESTION 170**

- (Topic 3)

A business purchased redundant internet connectivity from two separate ISPs. Which of the following is the business MOST likely implementing?

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

**Answer:** C

**Explanation:**

Multipathing is a technique that allows a device to use more than one path to communicate with another device. This provides redundancy, load balancing, and fault tolerance for network connections. A business that purchased redundant internet connectivity from two separate ISPs is most likely implementing multipathing to ensure continuous access to the internet in case one ISP fails or becomes

congested. References: CompTIA Network+ N10-008 Certification Study Guide, page 437; The Official CompTIA Network+ Student Guide (Exam N10-008), page 16-8.

**NEW QUESTION 175**

- (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 180

- (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 185

- (Topic 3)

A network technician is troubleshooting a network issue for employees who have reported issues with speed when accessing a server in another subnet. The server is in another building that is 410ft (125m) away from the employees' building. The 10GBASE-T connection between the two buildings uses Cat 5e. Which of the following BEST explains the speed issue?

- A. The connection type is not rated for that distance
- B. A broadcast storm is occurring on the subnet.
- C. The cable run has interference on it
- D. The connection should be made using a Cat 6 cable

**Answer:** D

#### Explanation:

The 10GBASE-T connection between the two buildings uses Cat 5e, which is not rated for a distance of 410ft (125m). According to the CompTIA Network+ Study Manual, for 10GBASE-T connections, "Cat 5e is rated for up to 55m, Cat 6a is rated for 100m, and Cat 7 is rated for 150m." Therefore, the speed issue is likely due to the fact that the connection type is not rated for the distance between the two buildings. To resolve the issue, the technician should consider using a Cat 6a or Cat 7 cable to increase the distance the connection is rated for.

#### NEW QUESTION 188

- (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 189

- (Topic 3)

Which of the following describes when an active exploit is used to gain access to a network?

- A. Penetration testing
- B. Vulnerability testing
- C. Risk assessment
- D. Posture assessment
- E. Baseline testing

**Answer:** A

**Explanation:**

Penetration testing is a type of security testing that is used to assess the security of a system or network by actively exploiting known vulnerabilities. It is used to simulate an attack on the system and identify any weaknesses that may be exploited by malicious actors. As stated in the CompTIA Security+ Study Guide, "penetration testing is a type of security assessment that attempts to gain unauthorized access to networks and systems by exploiting security vulnerabilities."

**NEW QUESTION 191**

- (Topic 3)

Which of the following describes a network in which users and devices need to mutually authenticate before any network resource can be accessed?

- A. Least privilege
- B. Local authentication
- C. Zero trust
- D. Need to know

**Answer:** C

**Explanation:**

A zero trust network is a network in which users and devices need to mutually authenticate before any network resource can be accessed. A zero trust network assumes that no one and nothing can be trusted by default, even if they were previously verified or are within the network perimeter. A zero trust network uses various technologies and practices, such as data and log aggregation, cybersecurity analytics, continuous diagnostics and mitigation, user behavior analytics, microsegmentation, and identity and access management, to enforce granular and dynamic policies based on the context and behavior of the users and devices<sup>123</sup>.

References:

? What is Zero Trust? | Internet of Things | CompTIA<sup>3</sup>

? The Death of the Perimeter: Zero Trust is (Almost) Here to Stay | Cybersecurity | CompTIA<sup>2</sup>

? CompTIA Network+ Certification Exam N10-008 Practice Test 17 - ExamCompass<sup>1</sup>

**NEW QUESTION 195**

- (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 196**

- (Topic 3)

An on-call network technician receives an automated email alert stating that a power supply on a firewall has just powered down. Which of the following protocols would best allow for this level of detailed device monitoring?

- A. TFTP
- B. TLS
- C. SSL
- D. SNMP

**Answer:** D

**Explanation:**

SNMP stands for Simple Network Management Protocol, and it is a protocol that allows network devices to communicate their status, performance, and configuration information to a central management system. SNMP can be used to monitor and manage various aspects of network devices, such as CPU usage, memory utilization, interface statistics, temperature, voltage, power supply, etc. SNMP can also generate alerts or notifications when certain events or thresholds are reached, such as a power supply failure, a link down, or a high traffic volume. SNMP is widely used for network monitoring and troubleshooting purposes, as it provides a comprehensive and detailed view of the network health and performance.

The other options are not correct because they are not protocols that allow for detailed device monitoring. They are:

? TFTP. TFTP stands for Trivial File Transfer Protocol, and it is a protocol that allows for simple and fast file transfer between network devices. TFTP is often used to transfer configuration files, firmware updates, or boot images to network devices, such as routers, switches, or firewalls. TFTP does not provide any monitoring or management capabilities for network devices, nor does it generate any alerts or notifications.

? TLS. TLS stands for Transport Layer Security, and it is a protocol that provides encryption and authentication for data transmission over a network. TLS is often used to secure web traffic, email, or other applications that use TCP as the transport protocol. TLS does not provide any monitoring or management capabilities for network devices, nor does it generate any alerts or notifications.

? SSL. SSL stands for Secure Sockets Layer, and it is a protocol that provides encryption and authentication for data transmission over a network. SSL is the predecessor of TLS, and it is still used to secure some web traffic, email, or other applications that use TCP as the transport protocol. SSL does not provide any monitoring or management capabilities for network devices, nor does it generate any alerts or notifications.

References<sup>1</sup>: What is SNMP? - Definition from WhatIs.com<sup>2</sup>: Network+ (Plus) Certification

| CompTIA IT Certifications<sup>3</sup>: What is TFTP? - Definition from WhatIs.com<sup>4</sup>: What is TLS? - Definition from WhatIs.com<sup>5</sup>: What is SSL? - Definition from WhatIs.com

### NEW QUESTION 201

- (Topic 3)

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

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

**Answer:** A

#### Explanation:

One possible process that the administrator used to identify the root cause of the spam issue is traffic analysis. Traffic analysis is a technique that monitors and analyzes the network traffic that flows between devices or applications. Traffic analysis can help troubleshoot network problems by identifying the source, destination, volume, frequency, and content of the network packets<sup>12</sup>.

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

? Install a traffic analysis tool on the server or a device that is connected to the same network as the server, such as Wireshark<sup>3</sup>, tcpdump<sup>4</sup>, or Microsoft Network Monitor<sup>5</sup>.

? Start capturing the network traffic and filter it by using the IP address or hostname of the server, or by using a specific port or protocol that is used by the email service, such as SMTP (port 25), POP3 (port 110), or IMAP (port 143).

? Analyze the filtered traffic and look for any signs of abnormal or malicious activity, such as high volume of outgoing emails, unknown recipients, suspicious attachments, or spam keywords.

? Trace back the source of the spam emails to the infected workstation by using its IP address or MAC address.

? Isolate and clean up the infected workstation by using an antivirus or malware removal tool.

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

### NEW QUESTION 206

- (Topic 3)

A network technician is investigating why a core switch is logging excessive amounts of data to the syslog server. The running configuration of the switch showed the following logging information:

```
ip ssh logging events logging level debugging logging host 192.168.1.100 logging synchronous
```

Which of the following changes should the technician make to best fix the issue?

- A. Update the logging host IP.
- B. Change to asynchronous logging.
- C. Stop logging SSH events.
- D. Adjust the logging level.

**Answer:** D

#### Explanation:

The logging level debugging is the highest level of logging, which means that the switch will log every possible event, including low-priority and verbose messages. This can result in excessive amounts of data being sent to the syslog server, which can affect the performance and storage of the server. To fix the issue, the technician should adjust the logging level to a lower value, such as informational, warning, or error, depending on the desired level of detail and severity. This will reduce the amount of log data generated by the switch and only send the relevant and necessary messages to the syslog server.

<https://betterstack.com/community/guides/logging/log-levels-explained/>

### NEW QUESTION 207

- (Topic 3)

A user stores large graphic files. The time required to transfer the files to the server is excessive due to network congestion. The user's budget does not allow for the current switches to be replaced. Which of the following can be used to provide FASTER transfer times?

- A. Half duplex
- B. Jumbo frames
- C. LACP
- D. 802.1Q

**Answer:** B

#### Explanation:

Jumbo frames are Ethernet frames that can carry more than 1500 bytes of payload data. Jumbo frames can reduce the overhead and improve the throughput of large file transfers, as fewer frames are needed to send the same amount of data. Jumbo frames can be used to provide faster transfer times, as long as the network devices support them.

### NEW QUESTION 212

- (Topic 3)

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

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

**Answer:** A

**Explanation:**

One of the features that can be configured to ensure that GRE overhead does not affect payload is A. jumbo frames. Jumbo frames are Ethernet frames that have a payload size larger than 1500 bytes, which is the standard maximum transmission unit (MTU) for Ethernet. By using jumbo frames, more data can be sent in each packet, reducing the overhead ratio and improving efficiency.

Auto medium-dependent interface (MDI), interface crossover, and collision detection are features related to Ethernet physical layer connectivity, but they do not affect GRE overhead or payload.

**NEW QUESTION 214**

- (Topic 3)

Following the implementation of a BYOO policy, some users in a high-density environment report slowness over the wireless connection. Some wireless controller reports indicate high latency and airtime contention. Which of the following is the most probable root cause?

- A. The AP is configured with 2.4GHz frequency, which the new personal devices do not support.
- B. The AP is configured with 2.4GHz frequency without band-steering capabilities.
- C. The AP is configured with 5Ghz frequency with band-steering capabilities.
- D. The AP is configured with 5Ghz frequency.
- E. which the new personal devices do not support

**Answer:** B

**Explanation:**

Band-steering is a feature that allows an AP to steer dual-band capable clients to the less congested 5GHz frequency, leaving the 2.4GHz frequency for legacy clients. Without band-steering, the AP may have more clients competing for the same channel on the 2.4GHz frequency, resulting in high latency and airtime contention.

References:

? According to the CompTIA Network+ Certification Exam Objectives, one of the topics covered in the exam is "Given a scenario, use appropriate wireless technologies and configurations". One of the subtopics is "Band steering" 1.

? According to the Polifi: Airtime Policy Enforcement for WiFi paper, "Band steering allows the access point to disable the 2.4 GHz band from probing the client device, so it responds only to the 5 GHz band, reducing the congestion on the 2.4 GHz band while taking advantage of the faster 5GHz band to improve user's network experience." 2.

? According to the Aruba Air Slice Tech Brief, "Air Slice minimizes airtime contention and efficiently groups Wi-Fi 6 and non-Wi-Fi 6 client devices to guarantee bit rate, and provide bounded latency and jitter simultaneously." 3.

**NEW QUESTION 219**

- (Topic 3)

A technician is concerned about unauthorized personnel moving assets that are installed in a data center server rack. The technician installs a networked sensor that sends an alert when the server rack door is opened. Which of the following did the technician install?

- A. Cipher lock
- B. Asset tags
- C. Access control vestibule
- D. Tamper detection

**Answer:** D

**Explanation:**

Tamper detection is a physical security feature that can alert the technician when someone opens the server rack door without authorization. Tamper detection sensors can be installed inside the equipment or on the rack itself, and they can send an alert via email, SMS, or other methods. Tamper detection can help prevent unauthorized access, theft, or damage to the network assets.

References:

? Physical Security – N10-008 CompTIA Network+ : 4.51

**NEW QUESTION 224**

- (Topic 3)

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

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

**Answer:** A

**Explanation:**

Cat 8 keystone are shielded to prevent interference from external sources, but they also require proper grounding to avoid interference from within the cable.

Wrapping the end connections with copper tape before terminating them is one way to ensure a good ground connection and reduce interference. Using passthrough modular crimping plugs, connecting the RX/TX wires to different pins, or running a speed test on a slow device are not relevant or effective steps to troubleshoot the issue.

References:

? CompTIA Network+ N10-008 Certification Study Guide, page 191

? CompTIA Network+ N10-008 Cert Guide, Deluxe Edition, page 362

? CAT8 RJ45 Keystone Problem : r/HomeNetworking2

? How to Terminate Cat8 Shielded Keystone Jacks3

**NEW QUESTION 229**



- (Topic 3)

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 231**

- (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 me 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 232**

- (Topic 3)

An engineer needs to verity the external record tor 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 234**

- (Topic 3)

An infrastructure company is implementing a cabling solution to connect sites on multiple continents. Which of the following cable types should the company use for this project?

- A. Cat 7
- B. Single-mode
- C. Multimode
- D. Cat 6

**Answer: B**

**Explanation:**

Single-mode fiber is a type of optical fiber that has a small core diameter and allows only one mode of light to propagate. This reduces signal attenuation and increases transmission distance, making it suitable for long-distance communication networks.

Single-mode fiber can carry data over thousands of kilometers without requiring repeaters or amplifiers. Single-mode fiber is also immune to electromagnetic interference and has a higher bandwidth than multimode fiber. Therefore, single-mode fiber is the best cable type for connecting sites on multiple continents. References: [CompTIA Network+ Certification Exam Objectives], [Single-mode optical fiber - Wikipedia]

Single-mode fiber optic cable uses a single ray of light to transmit data. This allows it to achieve very low attenuation and high bandwidth.

Multimode fiber optic cable uses multiple rays of light to transmit data. This results in higher attenuation and lower bandwidth than single-mode cable.

Twisted pair copper cable uses two insulated copper wires to transmit data. It is less expensive than fiber optic cable, but it has higher attenuation and lower bandwidth. When choosing a cable type for a long-distance application, it is important to consider the following factors:

? Attenuation: The amount of signal loss that occurs over the length of the cable.

? Bandwidth: The amount of data that can be transmitted over the cable per second.

? Cost: The cost of the cable and installation.

Single-mode fiber optic cable is the best choice for long-distance applications because it

has the lowest attenuation and highest bandwidth of any cable type. However, it is also the most expensive cable type.



#### NEW QUESTION 236

- (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 238

- (Topic 3)

A network administrator is setting up a web-based application for a company. The application needs to be continually accessible to all end users.

Which of the following would best ensure this need is fulfilled?

- A. NIC teaming
- B. Cold site
- C. Snapshots
- D. High availability

**Answer: D**

#### Explanation:

High availability is a quality of a system or component that assures a high level of operational performance for a given period of time. High availability means that an IT system, component, or application can operate at a high level, continuously, without intervention, for a given time period. High-availability infrastructure is configured to deliver quality performance and handle different loads and failures with minimal or zero downtime. High availability is important for web-based applications, as it ensures that the application is always accessible to the end users, even in the event of a server or component failure. High availability can be achieved by eliminating single points of failure, implementing redundancy, load balancing, and failover mechanisms.

#### NEW QUESTION 239

- (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 244

- (Topic 3)

Which of the following allows for devices within a network to share a highly reliable time source?

- A. NTP
- B. SNMP

- C. SIP
- D. DNS

**Answer:** A

**Explanation:**

Network Time Protocol (NTP) is a protocol used to maintain a highly accurate and reliable clock time on all devices within a network. NTP works by synchronizing the time of all the devices within a network to a single, highly accurate time source. This allows for the time of all the devices to be kept in sync with each other, ensuring a consistent and reliable time source for all devices within the network.

**NEW QUESTION 245**

- (Topic 3)

A network administrator is in the process of installing 35 PoE security cameras. After the administrator installed and tested the new cables, the administrator installed the cameras. However, a small number of the cameras do not work. Which of the following is the most likely reason?

- A. Incorrect wiring standard
- B. Power budget exceeded
- C. Signal attenuation
- D. Wrong voltage

**Answer:** B

**Explanation:**

The power budget is the total amount of power that a PoE switch or injector can provide to the connected PoE devices. If the power budget is exceeded, some of the PoE devices may not receive enough power to function properly. To troubleshoot this issue, the network administrator should check the power consumption of each PoE device and the power capacity of the PoE switch or injector.

References:

? PoE Troubleshooting: The Common PoE Errors and Solutions<sup>1</sup>

? Security Camera Won't Work - Top 10 Solutions to Fix<sup>2</sup>

? CompTIA Network+ N10-008 Exam Objectives <https://www.comptia.org/certifications/network#examdetails>

**NEW QUESTION 249**

- (Topic 3)

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

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

**Answer:** B

**Explanation:**

Wireless AC is a wireless standard that supports up to 1.3Gbps data rate and operates in the 5GHz frequency band only. Wireless AC is also backward compatible with wireless A and N devices that use the 5GHz band. Wireless AC is suitable for high-performance applications such as HD video streaming and online gaming.

References: Network+ Study Guide Objective 2.2: Explain the purposes and properties of routing and switching. Subobjective: Wireless standards and their characteristics.

**NEW QUESTION 254**

- (Topic 3)

An organization would like to implement a disaster recovery strategy that does not require a facility agreement or idle hardware. Which of the following strategies MOST likely meets the organization's requirements?

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

**Answer:** A

**Explanation:**

A cloud site is a type of disaster recovery site that uses cloud computing services to provide backup and recovery of data and applications in the event of a disaster<sup>1</sup>. A cloud site does not require a facility agreement or idle hardware, as the cloud provider manages the infrastructure and resources on demand. A cloud site can also offer scalability, flexibility, and cost-effectiveness compared to other types of disaster recovery sites.

**NEW QUESTION 259**

- (Topic 3)

A network team is getting reports that air conditioning is out in an IDF. The team would like to determine whether additional network issues are occurring. Which of the following should the network team do?

- A. Confirm that memory usage on the network devices in the IDF is normal.
- B. Access network baseline data for references to an air conditioning issue.
- C. Verify severity levels on the corporate syslog server.
- D. Check for SNMP traps from a network device in the IDF.
- E. Review interface statistics looking for cyclic redundancy errors.

**Answer:** D

**Explanation:**

"Baselines play an integral part in network documentation because they let you monitor the network's overall performance. In simple terms, a baseline is a measure of performance that indicates how hard the network is working and where network resources are spent. The purpose of a baseline is to provide a basis of comparison. For example, you can compare the network's performance results taken in March to results taken in June, or from one year to the next. More commonly, you would compare the baseline information at a time when the network is having a problem to information recorded when the network was operating with greater efficiency. Such comparisons help you determine whether there has been a problem with the network, how significant that problem is, and even where the problem lies."

**NEW QUESTION 262**

- (Topic 3)

Which of the following would be the BEST choice to connect branch sites to a main office securely?

- A. VPN headend
- B. Proxy server
- C. Bridge
- D. Load balancer

**Answer:** A

**Explanation:**

Host-to-Site, or Client-to-Site, VPN allows for remote servers, clients, and other hosts to establish tunnels through a VPN gateway (or VPN headend) via a private network. The tunnel between the headend and the client host encapsulates and encrypts data.

**NEW QUESTION 264**

- (Topic 3)

A user from a remote office is reporting slow file transfers. Which of the following tools will an engineer MOST likely use to get detailed measurement data?

- A. Packet capture
- B. IPerf
- C. SIEM log review
- D. Internet speed test

**Answer:** B

**Explanation:**

An engineer will most likely use IPerf to get detailed measurement data about the user's slow file transfers. IPerf is a tool used for measuring network performance and bandwidth, and it can be used to measure the speed and throughput of file transfers from the remote office. It can also provide detailed information about the latency and jitter of the connection, which can be used to troubleshoot the slow file transfers. Reference: CompTIA Network+ Study Manual (Chapter 10, Page 214).

**NEW QUESTION 265**

- (Topic 3)

A network engineer is troubleshooting application connectivity issues between a server and a client. The network engineer needs to view the certificate exchange between the two hosts. Which of the following tools should the network engineer use?

- A. dig
- B. tcpdump
- C. nmap
- D. traceroute

**Answer:** B

**Explanation:**

tcpdump is a tool that can capture and analyze network traffic, including the certificate exchange between two hosts. It can display the contents of packets, such as the SSL/TLS handshake, which involves the exchange of certificates. dig is a tool that can query DNS servers for domain name information. nmap is a tool that can scan ports and services on a network. traceroute is a tool that can show the path and hops between a source and a destination.

**NEW QUESTION 266**

- (Topic 3)

A network administrator wants to test the throughput of a new metro Ethernet circuit to verify that its performance matches the requirements specified in the SLA. Which of the following would BEST help measure the throughput?

- A. iPerf
- B. Ping
- C. NetFlow
- D. Netstat

**Answer:** A

**NEW QUESTION 269**

- (Topic 3)

A network technician is troubleshooting a connectivity issue. All users within the network report that they are unable to navigate to websites on the internet; however, they can still access local network resources. The technician issues a command and receives the following results:

```
Pinging comptia.com [172.67.217.56] with 32 bytes of data:  
Reply from 172.67.217.56: TTL expired in transit.  
Reply from 172.67.217.56: TTL expired in transit.  
Reply from 172.67.217.56: TTL expired in transit.  
Reply from 172.67.217.56: TTL expired in transit.
```

Which of the following best explains the result of this command?

- A. Incorrect VLAN settings
- B. Upstream routing loop
- C. Network collisions
- D. DNS misconfiguration

**Answer:** D

**Explanation:**

The users are unable to navigate to websites on the internet but can access local network resources, indicating a possible DNS issue. The ping command result showing “TTL expired in transit” suggests that packets are not reaching their destination due to a DNS misconfiguration that is not resolving website names into IP addresses correctly<sup>3</sup>. A possible solution is to check and correct the DNS server settings on the network devices<sup>4</sup>.

References: 3: What does “TTL expired in transit” mean?<sup>5</sup>4: CompTIA Network+ N10-008 Cert Guide - Chapter 14: Network Monitoring<sup>2</sup>

**NEW QUESTION 274**

- (Topic 3)

Which of the following DHCP settings would be used to ensure a device gets the same IP address each time it is connected to the network?

- A. Scope options
- B. Reservation
- C. Exclusion
- D. Relay
- E. Pool

**Answer:** A

**NEW QUESTION 275**

- (Topic 3)

A network technician recently installed 35 additional workstations. After installation, some users are unable to access network resources. Many of the original workstations that are experiencing the network access issue were offline when the new workstations were turned on. Which of the following is the MOST likely cause of this issue?

- A. Incorrect VLAN setting
- B. Insufficient DHCP scope
- C. Improper NIC setting
- D. Duplicate IP address

**Answer:** B

**NEW QUESTION 280**

- (Topic 3)

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

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

**Answer:** B

**Explanation:**

A hybrid cloud deployment model is a combination of on-premise and cloud solutions, where some resources are hosted in-house and some are hosted by a cloud provider. A hybrid cloud model can offer the benefits of both public and private clouds, such as scalability, cost-efficiency, security, and control<sup>12</sup>. A hybrid cloud model can also reduce the impact for users, as they can access the key services from the on-site data center and the enterprise services from the cloud

**NEW QUESTION 283**

- (Topic 3)

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

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

**Answer:** C



**Explanation:**

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

References:

? An Overview of DNS - N10-008 CompTIA Network+ : 1.61

? DNS Configuration – CompTIA A+ 220-11012

? CompTIA Network+ Certification Exam Objectives, page 53

**NEW QUESTION 287**

- (Topic 3)

Which of the following options represents the participating computers in a network?

- A. Nodes
- B. CPUs
- C. Servers
- D. Clients

**Answer:** A

**NEW QUESTION 290**

- (Topic 3)

A network technician is attempting to increase throughput by configuring link port aggregation between a Gigabit Ethernet distribution switch and a Fast Ethernet access switch. Which of the following is the BEST choice concerning speed and duplex for all interfaces that are participating in the link aggregation?

- A. Half duplex and 1GB speed
- B. Full duplex and 1GB speed
- C. Half duplex and 100MB speed
- D. Full duplex and 100MB speed

**Answer:** B

**Explanation:**

The best choice for configuring link port aggregation between a Gigabit Ethernet distribution switch and a Fast Ethernet access switch is to use full duplex and 1GB speed for all interfaces that are participating in the link aggregation. This will allow for maximum throughput, as the full duplex connection will enable simultaneous sending and receiving of data, and the 1GB speed will ensure that the data is transferred quickly. According to the CompTIA Network+ Study Guide, "Full-duplex Ethernet allows the network adapter to transmit and receive data simultaneously, which can result in double the bandwidth of half-duplex Ethernet." Additionally, the official text states, "Ethernet and Fast Ethernet use different speeds for data transmission, with Ethernet being 1,000 megabits (1 gigabit) per second and Fast Ethernet being 100 megabits per second."

**NEW QUESTION 295**

- (Topic 3)

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

- A. Fiber distribution panel
- B. 110 punchdown block
- C. PDU
- D. TIA/EIA-568A patch bay
- E. Cat 6 patch panel

**Answer:** A

**Explanation:**

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

**NEW QUESTION 297**

- (Topic 3)

Which of the following ports is a secure protocol?

- A. 20
- B. 23
- C. 443
- D. 445

**Answer:** C

**Explanation:**

This is the port number for HTTPS, which stands for Hypertext Transfer Protocol Secure. HTTPS is a secure version of HTTP, which is the protocol used to communicate between web browsers and web servers. HTTPS encrypts the data sent and received using SSL/TLS, which are cryptographic protocols that provide authentication, confidentiality, and integrity. HTTPS is commonly used for online transactions, such as banking and shopping, where security and privacy are important

**NEW QUESTION 300**

SIMULATION - (Topic 3)

A network technician was recently onboarded to a company. A manager has



tasked the technician with documenting the network and has provided the technician With partial information from previous documentation.

Instructions:

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

<div style="border: 1px solid #ccc; padding: 2px;">0200.0000.0003</div> <div style="border: 1px solid #ccc; padding: 2px;">Select IP Address</div> <div style="border: 1px solid #ccc; padding: 2px;">Select VLAN</div> <div style="border: 1px solid #ccc; padding: 2px;">Select Interface</div>	<div style="border: 1px solid #ccc; padding: 2px;">Select MAC Address</div> <div style="border: 1px solid #ccc; padding: 2px;">10.10.30.51</div> <div style="border: 1px solid #ccc; padding: 2px;">Select VLAN</div> <div style="border: 1px solid #ccc; padding: 2px;">Select Interface</div>	<div style="border: 1px solid #ccc; padding: 2px;">0200.0000.0004</div> <div style="border: 1px solid #ccc; padding: 2px;">Select IP Address</div> <div style="border: 1px solid #ccc; padding: 2px;">Select VLAN</div> <div style="border: 1px solid #ccc; padding: 2px;">Select Interface</div>	<div style="border: 1px solid #ccc; padding: 2px;">Select MAC Address</div> <div style="border: 1px solid #ccc; padding: 2px;">10.10.30.53</div> <div style="border: 1px solid #ccc; padding: 2px;">Select VLAN</div> <div style="border: 1px solid #ccc; padding: 2px;">Select Interface</div>
---	---	---	---

Core Switch 1 Prompt
✕

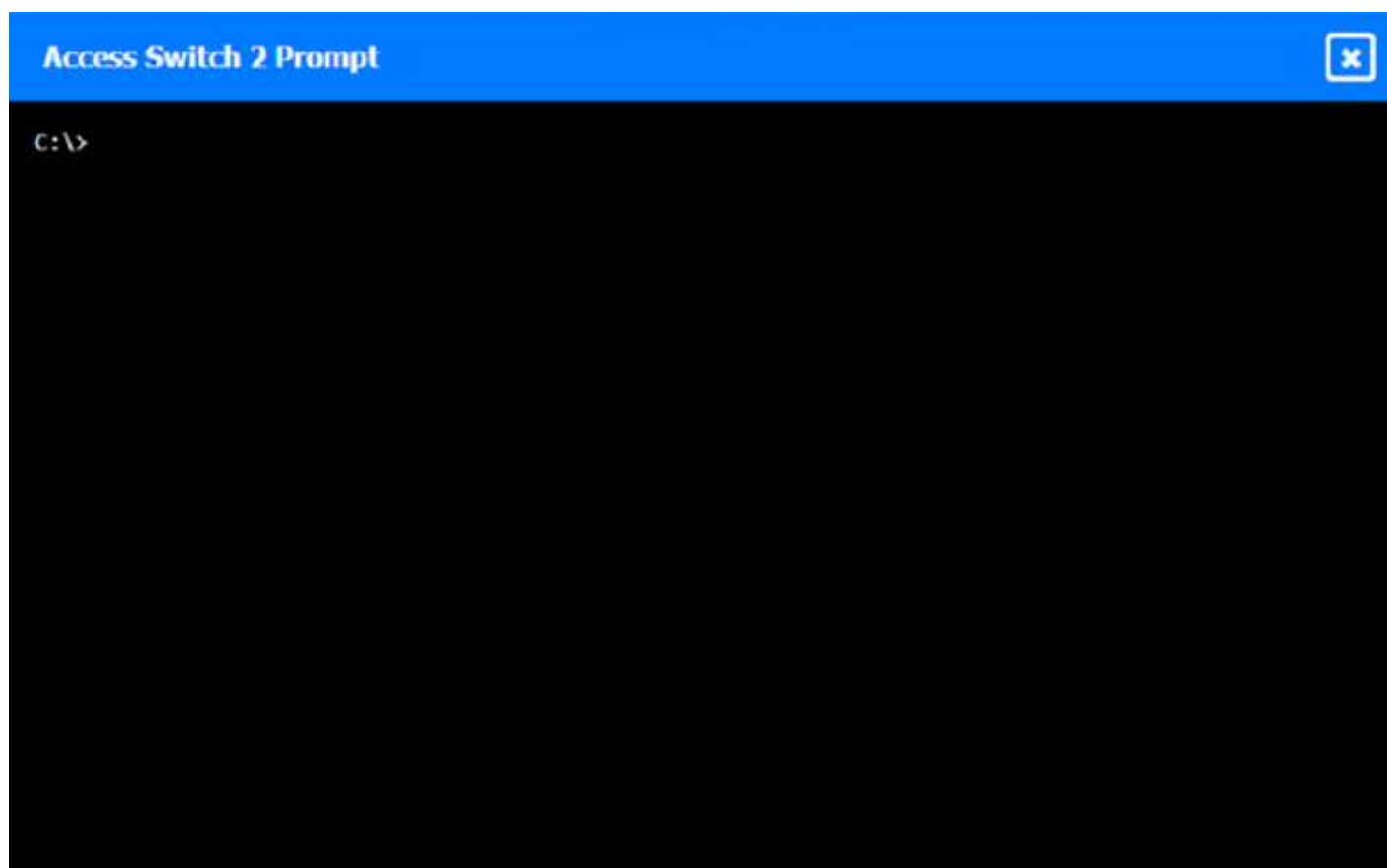
```

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

Access Switch 1 Prompt
✕

```

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



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

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

? Click on each switch to open its terminal window.

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

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

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

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

? The IP address of Core Switch 1 is 192.168.1.1.

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

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

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

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

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

**NEW QUESTION 302**

- (Topic 3)

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

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

**Answer:** A

**NEW QUESTION 306**

- (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 308**

- (Topic 3)

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

following databases does the administrator need to delete?

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

**Answer:** A

**Explanation:**

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

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

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

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

**NEW QUESTION 313**

- (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 318**

- (Topic 3)

A company wants to set up a backup data center that can become active during a disaster. The site needs to contain network equipment and connectivity. Which of the following strategies should the company employ?

- A. Active-active
- B. Warm
- C. Cold
- D. Cloud

**Answer:** B

**Explanation:**

Active-active refers to more than one NIC being active at the same time. In my opinion, this question is referring to a recovery site (hot, warm, cold, cloud)

**NEW QUESTION 322**

- (Topic 3)

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

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

**Answer:** A

**NEW QUESTION 324**

- (Topic 3)

A wireless network technician is receiving reports from some users who are unable to see both of the corporate SSIDs on their mobile devices. A site survey was recently commissioned, and the results verified acceptable RSSI from both APs in all user areas. The APs support modern wireless standards and are all broadcasting their SSIDs. The following table shows some of the current AP settings:

Name	Power	Directionality	Wireless standard	Authentication standard	SSID
AP1	Medium	Omnidirectional	802.11b	WPA2 - PSK	CORP01
AP2	High	Directional	802.11a	WPA2 - PSK	CORP02

Which of the following changes would result in all of the user devices being capable of seeing both corporate SSIDs?

- A. Implementing the WPA2 Enterprise authentication standard
- B. Implementing omnidirectional antennas for both APs
- C. Configuring the highest power settings for both APs
- D. Configuring both APs to use the 802.11ac wireless standard

**Answer:** D

**Explanation:**

The change that would result in all of the user devices being capable of seeing both corporate SSIDs is configuring both APs to use the 802.11ac wireless standard. 802.11ac is a wireless standard that operates in the 5 GHz frequency band and offers high data rates and performance. However, not all wireless devices support 802.11ac, especially older ones that only operate in the 2.4 GHz frequency band. In the table, AP1 uses 802.11b, which is an outdated wireless standard that operates in the 2.4 GHz frequency band and offers low data rates and performance. AP2 uses 802.11a, which is an older wireless standard that operates in the 5 GHz frequency band and offers moderate data rates and performance. Therefore, some user devices may not be able to see both SSIDs because they are incompatible with either 802.11b or 802.11a. By configuring both APs to use 802.11ac, which is backward compatible with previous wireless standards, all user devices should be able to see both SSIDs. References: CompTIA Network+ N10-008 Certification Study Guide, page 75; The Official CompTIA Network+ Student Guide (Exam N10-008), page 2-18.

#### NEW QUESTION 329

.....



## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual N10-008 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the N10-008 Product From:

<https://www.2passeasy.com/dumps/N10-008/>

## Money Back Guarantee

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

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