

# Exam Questions N10-009

CompTIA Network+ Exam

<https://www.2passeasy.com/dumps/N10-009/>



### NEW QUESTION 1

- (Topic 3)

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

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

**Answer:** A

#### Explanation:

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

? Network Hardening - N10-008 CompTIA Network+ : 4.3 - YouTube<sup>1</sup>

? CompTIA Network+ Certification Exam Objectives, page 151

### NEW QUESTION 2

- (Topic 3)

Which of the following would most likely affect design considerations when building out an IDF?

- A. The source panel amperage
- B. The fire suppression system
- C. The humidity levels
- D. The cable transmission speeds

**Answer:** B

#### Explanation:

The fire suppression system is a design consideration when building out an IDF because it can affect the safety and reliability of the network equipment and cabling. A fire suppression system is a system that detects and extinguishes fires in a building, using water, gas, or chemicals. Depending on the type of fire suppression system, it can have different impacts on the IDF design, such as:

? Water-based systems, such as sprinklers, can damage the network equipment and cabling if they are activated by a fire or a false alarm. Therefore, the IDF should be designed to protect the equipment and cabling from water exposure, such as using waterproof cabinets, drip pans, and conduits.

? Gas-based systems, such as clean agent systems, can displace the oxygen in the IDF and cause suffocation for anyone inside. Therefore, the IDF should be designed to allow for ventilation and air circulation, as well as warning signs and alarms to alert anyone in the IDF before the gas is released.

? Chemical-based systems, such as dry chemical systems, can leave a residue on the network equipment and cabling that can affect their performance and lifespan. Therefore, the IDF should be designed to minimize the contact between the chemical and the equipment and cabling, as well as provide a means for cleaning and restoring them after a fire.

The other options are not correct because:

? The source panel amperage is not a design consideration when building out an IDF, as it is determined by the electrical circuit and the power needs of the network equipment and cabling. The source panel amperage does not affect the layout, location, or protection of the IDF.

? The humidity levels are not a design consideration when building out an IDF, as they are controlled by the HVAC system and the ventilation of the IDF. The humidity levels do not affect the layout, location, or protection of the IDF.

? The cable transmission speeds are not a design consideration when building out an IDF, as they are determined by the type and quality of the network cabling and the network equipment. The cable transmission speeds do not affect the layout, location, or protection of the IDF.

### NEW QUESTION 3

- (Topic 3)

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

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

**Answer:** B

#### Explanation:

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

### NEW QUESTION 4

- (Topic 3)

An organization has a security requirement that all network connections can be traced back to a user. A network administrator needs to identify a solution to implement on the wireless network. Which of the following is the best solution?

- A. Implementing enterprise authentication
- B. Requiring the use of PSKs
- C. Configuring a captive portal for users
- D. Enforcing wired equivalent protection

**Answer:** A

#### Explanation:

Enterprise authentication is a method of securing wireless networks that uses an external authentication server, such as RADIUS, to verify the identity of users and devices. Enterprise authentication can provide user traceability by logging the network connections and activities of each authenticated user. This can help the organization meet its security requirement and comply with any regulations or policies that mandate user accountability<sup>12</sup>.

References:

? CompTIA Network+ N10-008 Certification Exam Objectives, page 83

? CompTIA Network+ Cert Guide: Wireless Networking, page 13

#### NEW QUESTION 5

- (Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 6

- (Topic 3)

A network administrator needs to create an SVI on a Layer 3-capable device to separate voice and data traffic. Which of the following best explains this use case?

- A. A physical interface used for trunking logical ports
- B. A physical interface used for management access
- C. A logical interface used for the routing of VLANs
- D. A logical interface used when the number of physical ports is insufficient

**Answer:** C

#### Explanation:

An SVI, or switched virtual interface, is a logical interface that is created on a Layer 3- capable device, such as a multilayer switch or a router. An SVI is associated with a VLAN and can be used to route traffic between different VLANs on the same device or across multiple devices. An SVI can also provide management access, security features, and quality of service (QoS) for the VLAN. An SVI is different from a physical interface, which is a port that connects to a physical device or network. A physical interface can be used for trunking, which is a method of carrying multiple VLANs over a single link, or for connecting to a single VLAN. An SVI is also different from a subinterface, which is a logical division of a physical interface that can be assigned to different VLANs.

References:

? VLANs and Trunking – N10-008 CompTIA Network+ : 2.11

? Switched Virtual Interfaces – N10-008 CompTIA Network+ : 2.22

#### NEW QUESTION 7

- (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 8

- (Topic 3)

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

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

**Answer:** D

#### Explanation:

A DHCP relay is a network device that forwards DHCP requests from clients on one subnet to a DHCP server on another subnet. This allows the DHCP server to assign IP addresses and other network configuration parameters to clients across different subnets. A DHCP scope is a range of IP addresses that a DHCP server can assign to clients. A DHCP snooping is a security feature that filters and validates DHCP messages on a switch. A DHCP reservation is a way to assign a specific IP address to a specific client

based on its MAC address. References: Part 2 of the current page talks about DHCP relay and its functions. You can also find more information about DHCP relay

on [this page].

#### NEW QUESTION 9

- (Topic 3)

Which of the following protocols can be routed?

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

**Answer: C**

#### Explanation:

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

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

Fibre Channel is a protocol that provides high-speed and low-latency communication between servers and storage devices<sup>1</sup>. Fibre Channel cannot be routed because it does not use IP networks, but rather its own dedicated network infrastructure. Fibre Channel operates at the physical layer and the data link layer and requires special cables, switches, and adapters to support it. Fibre Channel can also be used to access block-level storage devices over a network, such as SAN.

NetBEUI (NetBIOS Extended User Interface) is an old protocol that provides session-level communication between devices on a local network<sup>1</sup>. NetBEUI cannot be routed because it does not contain a network address, only a device address. NetBEUI operates at the transport layer and relies on NetBIOS for name resolution. NetBEUI is obsolete and has been replaced by other protocols, such as TCP/IP.

#### NEW QUESTION 10

- (Topic 3)

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

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

**Answer: C**

#### NEW QUESTION 10

- (Topic 3)

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

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

**Answer: A**

#### NEW QUESTION 15

- (Topic 3)

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

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

**Answer: A**

#### NEW QUESTION 16

- (Topic 3)

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

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

**Answer: B**

#### Explanation:

One of the best practices to secure the network would be to disable unneeded switchports in the guest waiting area. This will prevent unauthorized users from connecting to the network through these ports. It's important to identify which switchports are not in use and disable them, as this will prevent unauthorized access

to the network. Other practices such as ensuring all guests sign an NDA, lowering the radio strength to reduce Wi-Fi coverage in the waiting area and enabling MAC filtering to block unknown hardware addresses are not as effective in securing the network as disabling unneeded switchports. Enforcing an NDA with guests may not stop a malicious user from attempting to access the network, reducing the radio strength only limits the Wi-Fi coverage, and MAC filtering can be easily bypassed by hackers.

#### NEW QUESTION 19

- (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 21

- (Topic 3)

A network technician is investigating a trouble ticket for a user who does not have network connectivity. All patch cables between the wall jacks and computers in the building were upgraded over the weekend from Cat 5 to Cat 6. The newly installed cable is crimped with a TIA/EIA 568A on one end and a TIA/EIA 568B on the other end.

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

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 23

- (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 28

- (Topic 3)

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

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 29

- (Topic 3)

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

- A. VLAN hopping
- B. Evil twin



- C. DNS poisoning
- D. Social engineering

**Answer:** B

### NEW QUESTION 30

- (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 33

- (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 34

- (Topic 3)

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

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

**Answer:** D

#### Explanation:

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

References

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

### NEW QUESTION 37

- (Topic 3)

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

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 40

- (Topic 3)

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 45

- (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 48

- (Topic 3)

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

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

**Answer: A**

#### NEW QUESTION 50

- (Topic 3)

Which of the following technologies would MOST likely be used to prevent the loss of connection between a virtual server and network storage devices?

- A. Multipathing
- B. VRRP
- C. Port aggregation
- D. NIC teaming

**Answer: D**

#### Explanation:

NIC teaming is a technology that allows multiple network interface cards (NICs) to work together as a single logical interface, providing redundancy and load balancing. This can prevent the loss of connection between a virtual server and network storage devices if one of the NICs fails or becomes disconnected. References: [CompTIA Network+ Certification Exam Objectives], Domain 2.0 Networking Concepts, Objective 2.5: Explain the purposes and use cases for advanced networking devices, Subobjective: NIC bonding/teaming

#### NEW QUESTION 53

- (Topic 3)

A security engineer is trying to connect cameras to a 12-port PoE switch, but only eight cameras turn on. Which of the following should the engineer check first?

- A. Ethernet cable type
- B. Voltage
- C. Transceiver compatibility
- D. DHCP addressing

**Answer: B**

#### Explanation:

The most likely reason why only eight cameras turn on is that the PoE switch does not have enough power budget to supply all 12 cameras. The engineer should check the voltage and wattage ratings of the PoE switch and the cameras, and make

sure they are compatible and sufficient. The Ethernet cable type, transceiver compatibility, and DHCP addressing are less likely to cause this problem, as they would affect the data transmission rather than the power delivery.

References:

? CompTIA Network+ N10-008 Certification Study Guide, page 181

? CompTIA Network+ N10-008 Cert Guide, Deluxe Edition, page 352

? PoE Troubleshooting: The Common PoE Errors and Solutions3

### NEW QUESTION 55

- (Topic 3)

While troubleshooting a network, a VoIP systems engineer discovers a significant inconsistency in the amount of time required for data to reach its destination and return. Which of the following terms best describes this issue?

- A. Bandwidth
- B. Latency
- C. Jitter
- D. Throughput

**Answer:** C

#### Explanation:

Jitter is the variation in the delay of data packets over a network. It is caused by factors such as network congestion, routing changes, packet loss, or improper queuing. Jitter affects the quality of VoIP calls because it can cause gaps, distortion, or out-of-order delivery of voice data. Jitter can be measured by the difference between the expected and actual arrival times of packets2. To reduce jitter, VoIP systems use buffers to store and reorder packets before playing them back. However, too much buffering can also increase latency, which is the total time it takes for data to travel from one point to another3.

References2 - VoIP Troubleshooting: 5 Fixes for Common Connection Issues - Nextiva3 - Troubleshooting VoIP — Is it You or the Network? - PingPlotter

### NEW QUESTION 60

- (Topic 3)

Which of the following combinations of single cables and transceivers will allow a server to have 40GB of network throughput? (Select two).

- A. SFP+
- B. SFP
- C. QSFP+
- D. Multimode
- E. Cat 6a
- F. Cat5e

**Answer:** CD

#### Explanation:

QSFP+ is a type of transceiver that supports 40 gigabit Ethernet (40GbE) over four lanes of 10 gigabit Ethernet (10GbE) each. QSFP+ stands for quad small form-factor pluggable plus, and it is a compact and hot-swappable module that plugs into a QSFP+ port on a network device. QSFP+ transceivers can support various types of cables and connectors, such as direct attach copper (DAC), active optical cable (AOC), or fiber optic cable. Multimode is a type of fiber optic cable that supports multiple modes of light propagation within the core. Multimode fiber optic cable can carry higher bandwidth and data rates than single-mode fiber optic cable, but over shorter distances. Multimode fiber optic cable is commonly used for short-reach applications, such as within a data center or a campus network. Multimode fiber optic cable can be paired with QSFP+ transceivers to achieve 40GbE connectivity.

The other options are not correct because they do not support 40GbE. They are:

? SFP+. SFP+ is a type of transceiver that supports 10 gigabit Ethernet (10GbE) over a single lane. SFP+ stands for small form-factor pluggable plus, and it is a compact and hot-swappable module that plugs into an SFP+ port on a network device. SFP+ transceivers can support various types of cables and connectors, such as direct attach copper (DAC), active optical cable (AOC), or fiber optic cable. However, SFP+ transceivers cannot support 40GbE by themselves, unless they are used in a breakout configuration with a QSFP+ transceiver.

? SFP. SFP is a type of transceiver that supports 1 gigabit Ethernet (1GbE) over a single lane. SFP stands for small form-factor pluggable, and it is a compact and hot-swappable module that plugs into an SFP port on a network device. SFP transceivers can support various types of cables and connectors, such as twisted-pair copper, coaxial cable, or fiber optic cable. However, SFP transceivers cannot support 40GbE by themselves, unless they are used in a breakout configuration with a QSFP+ transceiver.

? Cat 6a. Cat 6a is a type of twisted-pair copper cable that supports 10 gigabit

Ethernet (10GbE) over distances up to 100 meters. Cat 6a stands for category 6 augmented, and it is an enhanced version of Cat 6 cable that offers better performance and reduced crosstalk. Cat 6a cable can be paired with 10Gbase-T transceivers to achieve 10GbE connectivity. However, Cat 6a cable cannot support 40GbE by itself, unless it is used in a breakout configuration with a QSFP+ transceiver.

? Cat 5e. Cat 5e is a type of twisted-pair copper cable that supports 1 gigabit

Ethernet (1GbE) over distances up to 100 meters. Cat 5e stands for category 5 enhanced, and it is an improved version of Cat 5 cable that offers better performance and reduced crosstalk. Cat 5e cable can be paired with 1000base-T transceivers to achieve 1GbE connectivity. However, Cat 5e cable cannot support 40GbE by itself, unless it is used in a breakout configuration with a QSFP+ transceiver.

References1: QSFP+ - an overview | ScienceDirect Topics2: Multimode Fiber - an overview | ScienceDirect Topics3: Network+ (Plus) Certification | CompTIA IT Certifications4: SFP+ - an overview | ScienceDirect Topics5: SFP - an overview | ScienceDirect Topics6: Cat 6a - an overview | ScienceDirect Topics7: [Cat 5e - an overview | ScienceDirect Topics]

### NEW QUESTION 63

- (Topic 3)

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

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

**Answer:** A

#### Explanation:

Access points (APs) can be configured and centrally managed using a wireless LAN controller (WLC). A WLC is a device that connects to multiple APs and



provides centralized management and control of those APs. The WLC can be used to configure settings such as wireless network parameters, security settings, and quality of service (QoS) policies. Additionally, the WLC can be used to monitor the status of connected APs, track client connections, and gather statistics on network usage. Some vendors such as Cisco, Aruba, Ruckus, etc. provide wireless LAN controllers as part of their wireless networking solutions.

#### NEW QUESTION 65

- (Topic 3)

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

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

**Answer:** D

#### Explanation:

A CNAME (Canonical Name) record is a type of DNS (Domain Name System) record that maps an alias name to a canonical or true domain name. For example, a CNAME record can map blog.example.com to example.com, which means that blog.example.com is an alias of example.com. A CNAME record is useful when you want to point multiple subdomains to the same IP address, or when you want to change the IP address of a domain without affecting the subdomains<sup>1</sup>.

#### NEW QUESTION 67

- (Topic 3)

Which of the following focuses on application delivery?

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

**Answer:** C

#### Explanation:

SaaS is the cloud computing model that focuses on application delivery. SaaS stands for Software as a Service, which is a cloud computing model that provides software applications over the internet. SaaS allows customers to access and use software applications without installing or maintaining them on their own devices or servers. SaaS offers advantages such as scalability, accessibility, compatibility, and cost-effectiveness.

Customers can use SaaS applications on demand and pay only for what they use. References: [CompTIA Network+ Certification Exam Objectives], What Is Software as a Service (SaaS)? | IBM

#### NEW QUESTION 70

- (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 74

- (Topic 3)

Which of the following is the most accurate NTP time source that is capable of being accessed across a network connection?

- A. Stratum 0 device
- B. Stratum 1 device
- C. Stratum 7 device
- D. Stratum 16 device

**Answer:** B

#### Explanation:

NTP (Network Time Protocol) is a protocol that synchronizes the clocks of network devices with a reference time source. NTP uses a hierarchical system of time sources, called strata, to distribute the time information. A stratum 0 device is the most accurate time source, such as an atomic clock or a GPS receiver, but it is not directly accessible across a network connection. A stratum 1 device is a network device that is directly connected to a stratum 0 device, such as a dedicated NTP server or a router with a GPS antenna, and it acts as a primary time server for other network devices. A stratum 2 device is a network device that synchronizes its time with a stratum 1 device, and so on. The higher the stratum number, the lower the accuracy and reliability of the time source. A stratum 16 device is a network device that has no valid time source and is considered unsynchronized.

References:

? Part 1 of current page talks about how Bing is your AI-powered copilot for the web and provides various examples of how it can help you with different tasks, such as writing a joke, creating a table, or summarizing research. However, it does not mention anything about NTP or time sources.

? Part 2 of current page shows the search results for “ai powered search bing chat”, which include web, image, and news results. However, none of these results

seem to be relevant to the question, as they are mostly about Bing's features, products, or announcements, not about NTP or time sources.

? Therefore, I cannot find the answer or the explanation from the current page. I have to use my own knowledge and information from other sources to verify the answer and provide a short but comprehensive explanation. I will cite these sources using numerical references.

? : CompTIA Network+ Certification Exam Objectives, Version 8.0, Domain 2.0: Infrastructure, Objective 2.5: Given a scenario, implement network time synchronization, Subobjective 2.5.1: NTP, <https://www.comptia.jp/pdf/comptia-network-n10-008-exam-objectives.pdf>

? : Network Time Protocol (NTP), <https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-58/154-ntp.html>

? : How NTP Works, <https://www.meinbergglobal.com/english/info/ntp.htm>

#### NEW QUESTION 77

- (Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 81

- (Topic 3)

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

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 82

- (Topic 3)

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

- A. SNMPv3
- B. SSh
- C. Telnet
- D. IPSec
- E. ESP
- F. Syslog

**Answer:** BD

#### NEW QUESTION 86

- (Topic 3)

A customer connects a firewall to an ISP router that translates traffic destined for the internet. The customer can connect to the internet but not to the remote site. Which of the following will verify the status of NAT?

- A. tcpdump
- B. nmap
- C. ipconfig
- D. tracer

**Answer:** A

#### Explanation:

tcpdump is a command-line tool that can capture and analyze network traffic on a given interface. tcpdump can verify the status of NAT by showing the source and destination IP addresses of the packets before and after they pass through the ISP router that translates traffic destined for the internet. tcpdump can also show the NAT protocol and port numbers used by the router. nmap, ipconfig, and tracer are not suitable tools for verifying the status of NAT, as they do not show the IP address translation process.

References

? 1: Network Address Translation – N10-008 CompTIA Network+ : 1.4

? 2: CompTIA Network+ N10-008 Certification Study Guide, page 95-96

? 3: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 16

? 4: CompTIA Network+ N10-008 Certification Practice Test, question 7

#### NEW QUESTION 89

- (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 90**

- (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 93**

- (Topic 3)

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

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

**Answer:** D

**NEW QUESTION 97**

- (Topic 3)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 99**

- (Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 100

- (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 103

- (Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 105

- (Topic 3)

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

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

**Answer:** C

#### Explanation:

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

References:

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

? VoIP and computer on separate VLANs through one cable

#### NEW QUESTION 106

- (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 110

- (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 114**

- (Topic 3)

A technician received a report that some users in a large, 30-floor building are having intermittent connectivity issues. Users on each floor have stable connectivity, but do not have connectivity to other floors. Which of the following devices is MOST likely causing the issue?

- A. User devices
- B. Edge devices
- C. Access switch
- D. Core switch

**Answer:** D

**Explanation:**

A core switch is the most likely device causing the issue where users on each floor have stable connectivity, but do not have connectivity to other floors. A core switch is a high-performance switch that connects multiple access switches in a network. An access switch is a switch that connects end devices, such as computers and printers, to the network. A core switch acts as the backbone of the network, providing interconnection and routing between different subnets or VLANs. If the core switch is malfunctioning or misconfigured, it can prevent communication between different segments of the network, resulting in intermittent connectivity issues. References: [CompTIA Network+ Certification Exam Objectives], Core Switch vs Access Switch: What Are the Differences?

**NEW QUESTION 115**

- (Topic 3)

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

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

**Answer:** C

**Explanation:**

Port mirroring is a technique that allows a network administrator to monitor the traffic on a specific port on a switch by sending a copy of the packets seen on that port to another port where a monitoring device is connected<sup>1</sup>. Port mirroring can be used to analyze and debug data, diagnose errors, or perform security audits on the network without affecting the normal operation of the switch

**NEW QUESTION 116**

- (Topic 3)

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

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

Which of the following configurations on the PC is incorrect?

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

**Answer:** C

**Explanation:**

The default gateway is the IP address of the router that connects the PC to other networks. The default gateway should be on the same subnet as the PC's IPv4 address. However, in this case, the default gateway is 192.168.9.1, which is on a different subnet than the PC's IPv4 address of 192.168.8.15. Therefore, the default gateway configuration on the PC is incorrect and prevents the PC from reaching the file server on another subnet.

**NEW QUESTION 120**

- (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 121**

- (Topic 3)



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

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 126**

- (Topic 3)

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

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

**Answer: C**

**Explanation:**

Documenting the lessons learned is the best method for passing along the exact steps other technicians should follow in case the issue arises again. Lessons learned are the knowledge and experience gained from completing a project or solving a problem. Documenting the lessons learned helps to capture the best practices, challenges, solutions, and recommendations for future reference and improvement. Documenting the lessons learned can also help to update the knowledge base, standard operating procedures, or policies related to the issue. References: [CompTIA Network+ Certification Exam Objectives], Lessons Learned: Definition & Examples for Project Managers

**NEW QUESTION 128**

- (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 133**

- (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 137**

- (Topic 3)

A network engineer needs to change an entire subnet of SLAAC-configured workstation addresses. Which of the following methods would be the best for the engineer to use?

- A. Change the address prefix in ARP in order for the workstations to retrieve their new addresses.
- B. Change the address prefix in a router in order for the router to advertise the new prefix with an ND.
- C. Change the address prefix scope in a DHCP server in order for the workstations to retrieve their new addresses.
- D. Change the workstations' address prefix manually because an automated method does not exist.

**Answer:** B

**Explanation:**

SLAAC (Stateless Address Autoconfiguration) is a mechanism that enables each host on the network to auto-configure a unique IPv6 address without any device keeping track of which address is assigned to which node<sup>12</sup>. SLAAC uses link-local addresses and the interface's MAC address or a random number to generate the host portion of the IPv6 address<sup>2</sup>. SLAAC also relies on Router Solicitation (RS) and Router Advertisement (RA) messages to obtain the network prefix and other information from a router<sup>12</sup>. Therefore, to change an entire subnet of SLAAC-configured workstation addresses, the network engineer needs to change the address prefix in a router and let the router advertise the new prefix with an ND (Neighbor Discovery) message. This way, the workstations will receive the new prefix and update their IPv6 addresses accordingly<sup>3</sup>.

References<sup>1</sup> - IPv6 Stateless Address Auto-configuration (SLAAC) | NetworkAcademy.io<sup>2</sup> - IPv6 SLAAC – Stateless Address Autoconfiguration - Study-CCNA3 - Mastering IPv6

SLAAC Concepts and Configuration - Cisco Press

**NEW QUESTION 141**

- (Topic 3)

To access production applications and data, developers must first connect remotely to a different server From there, the developers are able to access production data Which of the following does this BEST represent?

- A. A management plane
- B. A proxy server
- C. An out-of-band management device
- D. A site-to-site VPN
- E. A jump box

**Answer:** E

**NEW QUESTION 142**

- (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 146**

- (Topic 3)

Users are reporting intermittent Wi-Fi connectivity in specific parts of a building. Which of the following should the network administrator check FIRST when troubleshooting this issue? (Select TWO).

- A. Site survey
- B. EIRP
- C. AP placement
- D. Captive portal
- E. SSID assignment
- F. AP association time

**Answer:** AC

**Explanation:**

This is a coverage issue. WAP placement and power need to be checked. Site survey should be done NEXT because it takes a while.

**NEW QUESTION 148**

- (Topic 3)

Which of the following should a network administrator configure when adding OT devices to an organization's architecture?

- A. Honeynet
- B. Data-at-rest encryption
- C. Time-based authentication
- D. Network segmentation

**Answer:** D

**Explanation:**

Network segmentation is the process of dividing a network into smaller subnets or segments, each with its own security policies and access controls. This can help isolate OT devices from IT devices, guest networks, and other potential threats, as well as improve network performance and efficiency. Network segmentation is a recommended security practice for OT environments, as it can limit the attack surface, contain the damage of a breach, and comply with regulatory standards.

<https://sectrio.com/complete-guide-to-ot-network-segmentation/>

**NEW QUESTION 152**

- (Topic 3)

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

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

**Answer:** B

**Explanation:**

A SAN also employs a series of protocols enabling software to communicate or prepare data for storage. The most common protocol is the Fibre Channel Protocol (FCP), which maps SCSI commands over FC technology. The iSCSI SANs will employ an iSCSI protocol that maps SCSI commands over TCP/IP. STP (Spanning Tree Protocol) is a protocol used to prevent loops in Ethernet networks, and it is not a medium for communication in a storage area network (SAN). However, Fibre Channel is a protocol that is specifically designed for high-speed data transfer in SAN environments. It is a dedicated channel technology that provides high throughput and low latency, making it ideal for SANs. Therefore, Fibre Channel would be the best protocol for the company to use for its SAN. SFTP (Secure File Transfer Protocol), iSCSI (Internet Small Computer System Interface), and FTP (File Transfer Protocol) are protocols used for transferring files over a network and are not suitable for use in a SAN environment.

**NEW QUESTION 157**

- (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 160**

- (Topic 3)

A network administrator is reviewing the following metrics from a network management system regarding a switchport. The administrator suspects an issue because users are calling in regards to the switchport's performance:

Metric	Value
Uptime	201 days, 3 hours, 18 minutes
MDIX	On
CRCs	0
Giants	2508
Output queue maximum	40
Packets input	136208849
Packets output	64458087024

Based on the information in the chart above, which of the following is the cause of these performance issues?

- A. The connected device is exceeding the configured MTU.
- B. The connected device is sending too many packets
- C. The switchport has been up for too long
- D. The connected device is receiving too many packets.
- E. The switchport does not have enough CRCs

**Answer:** A

**NEW QUESTION 164**

- (Topic 3)

Which of the following network cables involves bouncing light off of protective cladding?

- A. Twinaxial
- B. Coaxial
- C. Single-mode
- D. Multimode

**Answer:** D

**Explanation:**

Multimode fiber optic cables use multiple paths of light that bounce off the cladding, which is a layer of glass or plastic that surrounds the core of the cable.

<https://www.explainthatstuff.com/fiberoptics.html>

#### NEW QUESTION 168

- (Topic 3)

A Chief Executive Officer and a network administrator came to an agreement With a vendor to purchase new equipment for the data center A document was drafted so all parties would be Informed about the scope of the project before It started. Which of the following terms BEST describes the document used?

- A. Contract
- B. Project charter
- C. Memorandum of understanding
- D. Non-disclosure agreement

**Answer: B**

#### Explanation:

The document used to inform all parties about the scope of the project before it starts is likely a project charter.

A project charter is a document that outlines the key aspects of a project, including the project's objectives, scope, stakeholders, and resources. It serves as a formal agreement between the project team and the stakeholders, and helps to define the project's goals and constraints.

A project charter typically includes information about the project's scope, including the specific deliverables that are expected and any constraints or limitations that may impact the project. It may also include details about the project team and stakeholders, the project schedule and budget, and the roles and responsibilities of each party.

By creating a project charter, the Chief Executive Officer and the network administrator can ensure that all parties involved in the project have a clear understanding of the project's goals and objectives, and can help to prevent misunderstandings or miscommunications during the project.

What is in a project charter?

A project charter is a formal short document that states a project exists and provides project managers with written authority to begin work. A project charter document describes a project to create a shared understanding of its goals, objectives and resource requirements before the project is scoped out in detail.

What are the 5 elements of the project charter?

What Are the Contents of a Project Charter? A project charter should always include an overview, an outline of scope, an approximate schedule, a budget estimate, anticipated risks, and key stakeholders

#### NEW QUESTION 172

- (Topic 3)

Network connectivity in an extensive forest reserve was achieved using fiber optics. A network fault was detected, and now the repair team needs to check the integrity of the fiber cable. Which of me following actions can reduce repair time?

- A. Using a tone generator and wire map to determine the fault location
- B. Using a multimeter to locate the fault point
- C. Using an OTDR In one end of the optic cable to get the liber length information
- D. Using a spectrum analyzer and comparing the current wavelength with a working baseline

**Answer: C**

#### NEW QUESTION 176

- (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 10OMB 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 178

- (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 179

- (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 181

- (Topic 3)

A firewall administrator observes log entries of traffic being allowed to a web server on port 80 and port 443. The policy for this server is to only allow traffic on port 443. The firewall administrator needs to investigate how this change occurred to prevent a reoccurrence. Which of the following should the firewall administrator do next?

- A. Consult the firewall audit logs.
- B. Change the policy to allow port 80.
- C. Remove the server object from the firewall policy.
- D. Check the network baseline.

**Answer:** A

#### Explanation:

Firewall audit logs are records of the changes made to the firewall configuration, policies, and rules. They can help the firewall administrator to track who, when, and what changes were made to the firewall, and identify any unauthorized or erroneous modifications that could cause security issues or network outages. By consulting the firewall audit logs, the firewall administrator can investigate how the change that allowed traffic on port 80 to the web server occurred, and prevent it from happening again

#### NEW QUESTION 182

- (Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 183

- (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 187

- (Topic 3)

A company wants to invest in new hardware for the core network infrastructure. The management team requires that the infrastructure be capable of being repaired in less than 60 minutes if any major part fails. Which of the following metrics is MOST likely associated with this requirement?

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

**Answer:** B

#### Explanation:

MTTR is directly related to how quickly a system can be repaired if any major part fails. The management team requires that the infrastructure be capable of being repaired in less than 60 minutes, which means they have a low MTTR requirement.

MTTR stands for Mean Time To Repair and is a metric used to measure the average amount of time it takes to repair a failed component or system. In this case, the requirement is for the infrastructure to be capable of being repaired in less than 60 minutes if any major part fails, which means the MTTR should be less than 60 minutes.

#### NEW QUESTION 189

- (Topic 3)

Which of the following layers of the OSI model has new protocols activated when a user moves from a wireless to a wired connection?

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



**Answer:** A

**Explanation:**

"The Data Link layer also determines how data is placed on the wire by using an access method. The wired access method, carrier-sense multiple access with collision detection (CSMA/CD), was once used by all wired Ethernet networks, but is automatically disabled on switched full-duplex links, which have been the norm for decades. Carrier-sense multiple access with collision avoidance (CSMA/CA) is used by wireless networks, in a similar fashion."

**NEW QUESTION 190**

- (Topic 3)

An administrator is setting up a multicast server on a network, but the firewall seems to be dropping the traffic. After logging in to the device, the administrator sees the following entries:

Rule	Action	Source	Destination	Port
1	Deny	Any	172.30.10.50	Any
2	Deny	Any	232.1.4.9	Any
3	Deny	Any	242.9.15.4	Any
4	Deny	Any	175.50.10.10	Any

Which of the following firewall rules is MOST likely causing the issue?

- A. Rule 1
- B. Rule 2
- C. Rule 3
- D. Rule 4

**Answer:** A

**NEW QUESTION 191**

- (Topic 3)

A technician is setting up DNS records on local servers for the company's cloud DNS to enable access by hostname. Which of the following records should be used?

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

**Answer:** A

**Explanation:**

An A record, also known as an address record, is a type of DNS record that maps a hostname to an IPv4 address. An A record is used to resolve a domain name to an IP address, so that clients can connect to the server or service by using the domain name instead of the IP address. For example, an A record can map [www.example.com](http://www.example.com) to 192.0.2.1.

An A record is the most common type of DNS record for cloud DNS, as it allows the company to use a custom domain name for their cloud services, such as web hosting, email, or storage. An A record can also be used to create subdomains, such as [blog.example.com](http://blog.example.com) or [mail.example.com](http://mail.example.com), that point to different IP addresses or servers. The other options are not correct because they are not the best type of DNS record for cloud DNS. They are:

? MX. MX stands for mail exchange, and it is a type of DNS record that specifies the mail servers that are responsible for receiving and delivering email messages for a domain name. MX records are used for email services, but they are not sufficient for cloud DNS, as they do not map a hostname to an IP address.

? CNAME. CNAME stands for canonical name, and it is a type of DNS record that specifies an alias name for another domain name. CNAME records are used to create multiple names for the same IP address or server, such as [www.example.com](http://www.example.com) and [example.com](http://example.com). CNAME records are useful for cloud DNS, but they are not the best type, as they depend on another A record to resolve the IP address.

? NS. NS stands for name server, and it is a type of DNS record that delegates a DNS zone to an authoritative server. NS records are used to specify which DNS servers are responsible for answering queries for a domain name or a subdomain. NS records are essential for cloud DNS, but they are not the best type, as they do not map a hostname to an IP address.

References1: DNS records overview | Google Cloud2: Network+ (Plus) Certification | CompTIA IT Certifications3: CloudDNS: What is a DNS record?

**NEW QUESTION 193**

- (Topic 3)

Which of the following types of data center architectures will MOST likely be used in a large SDN and can be extended beyond the data center?

- A. iSCSI
- B. FCoE
- C. Three-tiered network
- D. Spine and leaf
- E. Top-of-rack switching

**Answer:** D

**Explanation:**

The type of data center architecture that will most likely be used in a large SDN and can be extended beyond the data center is spine and leaf. Spine and leaf is a network topology that consists of two layers of switches: spine switches and leaf switches. Spine switches are interconnected to each other and form the core of the network, while leaf switches are connected to each spine switch and form the access layer of the network. Spine and leaf topology provides high scalability, performance, and flexibility for data center networks, especially for SDN (Software Defined Networking) environments that require dynamic traffic flows and virtualization. References: CompTIA Network+ N10-008 Certification Study Guide, page 16; The Official CompTIA Network+ Student Guide (Exam N10-008), page 1-9.

#### NEW QUESTION 195

- (Topic 3)

An online gaming company needs a cloud solution that will allow for more virtual resources to be deployed when tournaments are held. The number of users who access the service increases during tournaments. The company also needs the resources to return to baseline levels once the resources are not needed in order to reduce cost. Which of the following cloud concepts would provide the best solution?

- A. Scalability
- B. Hybrid
- C. Multitenancy
- D. Elasticity

**Answer: D**

#### Explanation:

Elasticity is the ability of a cloud service to automatically adjust the amount of resources allocated to meet the changing demand of the users. Elasticity enables a cloud service to scale up or down resources quickly and efficiently, without requiring manual intervention or planning. Elasticity is ideal for scenarios where the demand is unpredictable, dynamic, or seasonal, such as online gaming tournaments. By using elasticity, the online gaming company can ensure optimal performance and user experience during peak times, while also saving costs and avoiding overprovisioning during off-peak times.

The other options are not correct because they do not address the specific needs of the online gaming company. They are:

- Scalability is the ability of a cloud service to handle an increase or decrease in the demand of the users by adding or removing resources. Scalability is similar to elasticity, but it is more manual, planned, and predictive, while elasticity is automatic, prompt, and reactive. Scalability is suitable for scenarios where the demand is steady, predictable, or gradual, such as a growing business or a long-term project.
- Hybrid is a type of cloud model that combines two or more clouds, such as on-premises private, hosted private, or public, that can be centrally managed to enable interoperability for various use cases. Hybrid cloud can offer benefits such as flexibility, security, and cost- efficiency, but it does not directly address the need for dynamic resource allocation for the online gaming company.
- Multitenancy is a feature of cloud services that allows multiple users or customers to share the same physical or virtual resources, such as servers, databases, or applications, while maintaining isolation and privacy. Multitenancy can offer benefits such as efficiency, scalability, and cost-effectiveness, but it does not directly address the need for dynamic resource allocation for the online gaming company.

#### References

1: Understand cloud concepts | Microsoft Press Store 2: What Is Hybrid Cloud? - Cisco

3: Difference between Elasticity and Scalability in Cloud Computing 4: Scalability and Elasticity in Cloud Computing - GeeksforGeeks

#### NEW QUESTION 199

- (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 200

- (Topic 3)

During an annual review of policy documents, a company decided to adjust its recovery time frames. The company agreed that critical applications can be down for no more than six hours, and the acceptable amount of data loss is no more than two hours. Which of the following should be documented as the RPO?

- A. Two hours
- B. Four hours
- C. Six hours
- D. Eight hours

**Answer: A**

#### Explanation:

" RPO designates the variable amount of data that will be lost or will have to be re-entered during network downtime. RTO designates the amount of "real time" that can pass before the disruption begins to seriously and unacceptably impede the flow of normal business operations."

#### NEW QUESTION 203

- (Topic 3)

Which of the following disaster recovery metrics describes the average length of time a piece of equipment can be expected to operate normally?

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

**Answer: D**

**Explanation:**

MTBF is the disaster recovery metric that describes the average length of time a piece of equipment can be expected to operate normally. MTBF stands for mean time between failures, which is a measure of the reliability and availability of a device or system. MTBF is calculated by dividing the total operating time by the number of failures that occurred during that time. MTBF indicates how often a device or system fails and how long it can run without interruption. A higher MTBF means a lower failure rate and a longer operational life span. References: [CompTIA Network+ Certification Exam Objectives], What Is Mean Time Between Failures (MTBF)? | Definition & Examples | Forcepoint

**NEW QUESTION 205**

- (Topic 3)

A company has a geographically remote office. In order to connect to the internet, the company has decided to use a satellite WAN link. Which of the following is the GREATEST concern for this type of connection?

- A. Duplex
- B. Collisions
- C. Jitter
- D. Encapsulation

**Answer: C**

**Explanation:**

Jitter is the variation in latency or delay of packets in a network. Satellite WAN links have high latency and are prone to jitter, which can affect the quality of voice and video applications. Jitter is the greatest concern for this type of connection

**NEW QUESTION 208**

- (Topic 3)

Which of the following would be used to enforce and schedule critical updates with supervisory approval and include backup plans in case of failure?

- A. Business continuity plan
- B. Onboarding and offboarding policies
- C. Acceptable use policy
- D. System life cycle
- E. Change management

**Answer: A**

**NEW QUESTION 209**

- (Topic 3)

A customer calls the help desk to report that users are unable to access any network resources. The issue started earlier in the day when an employee rearranged the wiring closet. A technician goes to the site but does not observe any obvious damage. The statistics output on the switch indicates high CPU-J usage, and all the lights on the switch are blinking rapidly in unison. Which of the following is the most likely explanation for these symptoms?

- A. The switch was rebooted and set to run in safe mode.
- B. The line between the switch and the upstream router was removed.
- C. A cable was looped and created a broadcast storm.
- D. A Cat 6 cable from the modem to the router was replaced with Cat 5e.

**Answer: C**

**Explanation:**

A cable was looped and created a broadcast storm is the most likely explanation for the symptoms of high CPU usage and blinking lights on the switch. A cable loop is a situation where a switch port is connected to another switch port on the same switch or another switch, creating a circular path for network traffic. A cable loop can cause a broadcast storm, which is a network phenomenon where a large number of broadcast or multicast packets are flooded on the network, consuming bandwidth and CPU resources. A broadcast storm can cause network congestion, performance degradation, or failure. A cable loop can occur when an employee rearranges the wiring closet without proper documentation or verification. A cable loop can be prevented or detected by using Spanning Tree Protocol (STP) or loop detection features on the switch. References: [CompTIA Network+ Certification Exam Objectives], What Is a Broadcast Storm? | Definition & Examples | Forcepoint

**NEW QUESTION 214**

- (Topic 3)

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

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

**Answer: A**

**NEW QUESTION 215**

- (Topic 3)

A security team updated a web server to require https:// in the URL. Although the IP address did not change, users report being unable to reach the site. Which of the following should the security team do to allow users to reach the server again?

- A. Configure the switch port with the correct VLAN.
- B. Configure inbound firewall rules to allow traffic to port 443.
- C. Configure the router to include the subnet of the server.
- D. Configure the server with a default route.

**Answer:** B

**Explanation:**

One possible reason why users are unable to reach the site after the security team updated the web server to require https:// in the URL is that the firewall rules are blocking the traffic to port 443. Port 443 is the default port for HTTPS, which is the protocol that encrypts and secures the web communication. If the firewall rules do not allow inbound traffic to port 443, then users will not be able to access the web server using HTTPS.

To troubleshoot this issue, the security team should configure inbound firewall rules to allow traffic to port 443. This can be done by using the firewall-cmd command on RHEL 8.2, which is a tool that manages firewalld, the default firewall service on RHEL. The command to add a rule to allow traffic to port 443 is: firewall-cmd --permanent --add-port=443/tcp

The --permanent option makes the rule persistent across reboots, and the --add-port option specifies the port number and protocol (TCP) to allow. After adding the rule, the security

team should reload the firewalld service to apply the changes: firewall-cmd --reload

The security team can verify that the rule is active by using this command:

firewall-cmd --list-ports

The output should show 443/tcp among the ports that are allowed.

The other options are not relevant to troubleshooting this issue. Configuring the switch port with the correct VLAN may help with network segmentation or isolation, but it will not affect the HTTPS protocol or port. Configuring the router to include the subnet of the server may help with network routing or connectivity, but it will not enable HTTPS communication. Configuring the server with a default route may help with network access or reachability, but it will not allow HTTPS traffic.

**NEW QUESTION 220**

- (Topic 3)

An engineer is using a tool to run an ICMP sweep of a network to find devices that are online. When reviewing the results, the engineer notices a number of workstations that are currently verified as being online are not listed in the report.

The tool was configured to scan using the following information: Network address: 172.28.16.0

CIDR: /22

The engineer collected the following information from the client workstation: IP address: 172.28.17.206

Subnet mask: 255.255.252.0

Which of the following MOST likely explains why the tool is failing to detect some workstations?

- A. The scanned network range is incorrect.
- B. The subnet mask on the client is misconfigured.
- C. The workstation has a firewall enabled.
- D. The tool is unable to scan remote networks.

**Answer:** C

**Explanation:**

A firewall is a device or software that filters and controls the incoming and outgoing network traffic based on predefined rules. A firewall can block ICMP packets, which are used for ping and other diagnostic tools. If the workstation has a firewall enabled, it may not respond to the ICMP sweep and appear as offline. The engineer should check the firewall settings on the workstation and allow ICMP traffic if needed.

References: Network+ Study Guide Objective 4.1: Given a scenario, use the appropriate tool.

**NEW QUESTION 225**

- (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 230**

- (Topic 3)

A security team would like to use a system in an isolated network to record the actions of potential attackers. Which of the following solutions is the security team implementing?

- A. Perimeter network
- B. Honeypot
- C. Zero trust infrastructure
- D. Network segmentation

**Answer:** B

**Explanation:**

The solution that the security team is implementing to record the actions of potential attackers in an isolated network is a honeypot. A honeypot is a decoy system that simulates a real network or service, but has no actual value or function. A honeypot is designed to attract and trap attackers who try to infiltrate or compromise the network, and then monitor and analyze their behavior and techniques. A honeypot can help the security team learn about the attackers' motives, methods, and tools, and improve their defense

strategies accordingly. References: CompTIA Network+ N10-008 Certification Study Guide, page 358; The Official CompTIA Network+ Student Guide (Exam N10-008), page 14-1.



**NEW QUESTION 233**

- (Topic 3)

Which of the following allows for an 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 234**

- (Topic 3)

A Network engineer is investigating issues on a Layer 2 Switch. The department typically snares a Switchport during meetings for presentations, but after the first user Shares, no Other users can connect. Which Of the following is MOST likely related to this issue?

- A. Spanning Tree Protocol is enabled on the switch.
- B. VLAN trunking is enabled on the switch.
- C. Port security is configured on the switch.
- D. Dynamic ARP inspection is configured on the switch.

**Answer:** C**NEW QUESTION 236**

- (Topic 3)

A network administrator is installing a new server in the data center. The administrator is concerned the amount of traffic generated will exceed 1GB. and higher-throughput NiCs are not available for installation. Which of the following is the BEST solution for this issue?

- A. Install an additional NIC and configure LACP.
- B. Remove some of the applications from the server.
- C. Configure the NIC to use full duplex
- D. Configure port mirroring to send traffic to another server.
- E. Install a SSD to decrease data processing time.

**Answer:** A**NEW QUESTION 238**

- (Topic 3)

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

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

**Answer:** A**Explanation:**

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

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

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

**NEW QUESTION 241**

- (Topic 3)

A network technician is troubleshooting an issue that involves connecting to a server via SSH. The server has one network interface that does not support subinterfaces. The technician

runs a command on the server and receives the following output:

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

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



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

Which of the following best explains the issue?

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

**Answer:** C

#### NEW QUESTION 242

- (Topic 3)

During a recent security audit, a contracted penetration tester discovered the organization uses a number of insecure protocols. Which of the following ports should be disallowed so only encrypted protocols are allowed? (Select TWO).

- A. 22
- B. 23
- C. 69
- D. 443
- E. 587
- F. 8080

**Answer:** BC

#### NEW QUESTION 247

- (Topic 3)

A network deployment engineer is deploying a new single-channel 10G optical connection. Which of the following optics should the engineer MOST likely use to satisfy this requirement?

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

**Answer:** D

#### Explanation:

SFP+ is a type of optical transceiver that supports 10G single-channel transmission over fiber optic cables. SFP+ stands for small form-factor pluggable plus, and it is compatible with SFP slots on switches and routers.

#### NEW QUESTION 252

- (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 257

- (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 258

- (Topic 3)

Which of the following is a benefit of the spine-and-leaf network topology?

- A. Increased network security
- B. Stable network latency
- C. Simplified network management
- D. Eliminated need for inter-VLAN routing

**Answer:** A

#### NEW QUESTION 263

- (Topic 3)

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

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

**Answer:** B

#### Explanation:

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

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

#### NEW QUESTION 268

- (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 272

- (Topic 3)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 276

- (Topic 3)

Which of the following is most likely to have the HIGHEST latency while being the most accessible?

- A. Satellite
- B. DSL
- C. Cable
- D. 4G

**Answer:** A

#### NEW QUESTION 277

- (Topic 3)

A network administrator received complaints of intermittent network connectivity issues. The administrator investigates and finds that the network design contains potential loop scenarios. Which of the following should the administrator do?

- A. Enable spanning tree.
- B. Configure port security.
- C. Change switch port speed limits.
- D. Enforce 802.1Q tagging.

**Answer:** A

#### Explanation:

Spanning tree is a protocol that prevents network loops by dynamically disabling or enabling switch ports based on the network topology. Network loops can cause intermittent connectivity issues, such as broadcast storms, MAC address table instability, and multiple frame transmission. By enabling spanning tree, the network administrator can ensure that there is only one active path between any two network devices at any given time. References:

? CompTIA Network+ N10-008 Certification Exam Objectives, page 91

? CompTIA Network+ Cert Guide: Switching and Virtual LANs, page 172

#### NEW QUESTION 280

- (Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 285

- (Topic 3)

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

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

**Answer:** A

#### Explanation:

A router-on-a-stick is a configuration that allows a single router interface to route traffic between multiple VLANs on a network<sup>1</sup>. A router-on-a-stick requires sub-interfaces to be configured on the router interface, one for each VLAN. Each sub-interface is assigned a VLAN ID and an IP address that belongs to the corresponding VLAN subnet. The router interface is connected to a switch port that is configured as a trunk port, which allows traffic from multiple VLANs to pass through. The router then performs inter-VLAN routing by forwarding packets between the sub-interfaces based on their destination IP addresses. Inter-VLAN routing is a process that allows devices on different VLANs to communicate with each other. Inter-VLAN routing can be performed by a router-on-a-stick configuration, as explained above, or by a multilayer switch that has routing capabilities. A multilayer switch does not require sub-interfaces to be configured for inter-VLAN routing; instead, it uses switch virtual interfaces (SVIs) that are associated with each VLAN. An SVI is a logical interface that represents a VLAN on a switch and has an IP address that belongs to the VLAN subnet. The switch then performs inter-VLAN routing by forwarding packets between the SVIs based on their destination IP addresses.

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

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

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

#### NEW QUESTION 290

- (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.

References1: What is SNMP? - Definition from WhatIs.com2: Network+ (Plus) Certification

| CompTIA IT Certifications3: What is TFTP? - Definition from WhatIs.com4: What is TLS? - Definition from WhatIs.com5: What is SSL? - Definition from WhatIs.com

**NEW QUESTION 291**

- (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 295**

- (Topic 3)

A desktop support department has observed slow wireless speeds for a new line of laptops using the organization's standard image. No other devices have experienced the same issue. Which of the following should the network administrator recommend troubleshooting FIRST to resolve this issue?

- A. Increasing wireless signal power
- B. Installing a new WAP
- C. Changing the protocol associated to the SSID
- D. Updating the device wireless drivers

**Answer:** D

**Explanation:**

Wireless drivers can affect the performance and compatibility of your wireless connection5. If only a new line of laptops using the organization's standard image has experienced slow wireless speeds, it could be that their wireless drivers are outdated or incompatible with the network. Updating the device wireless drivers could resolve this issue.

Wireless drivers play an important role in the performance of a wireless connection, as they control how the device interacts with the wireless network. If the laptops in question are using an outdated version of the wireless driver, it could be causing the slow speeds. The network administrator should recommend updating the device wireless drivers first to see if this resolves the issue.

**NEW QUESTION 296**

- (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 299**

- (Topic 3)



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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 301**

- (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 306**

- (Topic 3)

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

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

**Answer:** D

**NEW QUESTION 308**

- (Topic 3)

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

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

**Answer:** B

**NEW QUESTION 310**

- (Topic 3)

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

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

**Answer:** D

**Explanation:**

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

• IP spoofing is the practice of forging the source IP address of a packet to make it appear as if it came from a trusted or authorized source.

• VLAN hopping is a technique that allows an attacker to access a VLAN that they are not authorized to access by sending packets with a modified VLAN tag.



•Rogue DHCP is a scenario where an unauthorized DHCP server offers IP configuration parameters to clients on a network, potentially causing network disruption or redirection to malicious sites4.

References

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

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

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

### NEW QUESTION 313

- (Topic 3)

A PC user who is on a local network reports very slow speeds when accessing files on the network server The user's PC Is connecting, but file downloads are very slow when compared to other users' download speeds The PC's NIC should be capable of Gigabit Ethernet. Which of the following will MOST likely fix the issue?

- A. Releasing and renewing the PC's IP address
- B. Replacing the patch cable
- C. Reseating the NIC inside the PC
- D. Flushing the DNS cache

**Answer: B**

#### Explanation:

A slow download speed can be caused by a faulty patch cable, which is the cable used to connect the user's PC to the network server. If the patch cable is damaged, the connection will be slower than expected, resulting in slow download speeds. Replacing the patch cable is the most likely solution to this issue, as it will provide a new, reliable connection that should allow for faster download speeds.

### NEW QUESTION 317

- (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 320

- (Topic 3)

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

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

**Answer: B**

### NEW QUESTION 322

- (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 as12:

? 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 as12:

? 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<sup>3</sup>. 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 327

- (Topic 3)

Which of the following is a characteristic of the application layer?

- A. It relies upon other layers for packet delivery.
- B. It checks independently for packet loss.
- C. It encrypts data in transit.
- D. It performs address translation.

**Answer:** A

#### Explanation:

The application layer is the highest layer of the OSI model, and it provides the interface between the user and the network. It does not handle the details of packet delivery, such as addressing, routing, error checking, or encryption. Those functions are performed by the lower layers of the OSI model. The application layer only focuses on the format, content, and presentation of the data.

References:

? Understanding the OSI Model – N10-008 CompTIA Network+ : 1.11

? CompTIA Network+ Certification Exam Objectives, page 92

#### NEW QUESTION 331

- (Topic 3)

A junior network engineer is trying to change the native network ID to a non-default value that can then be applied consistently throughout the network environment. Which of the following issues is the engineer attempting to prevent?

- A. DDoS
- B. ARP spoofing
- C. VLAN hopping
- D. Rogue DHCP

**Answer:** C

#### Explanation:

VLAN hopping is a type of network attack where an attacker can send or receive traffic from a VLAN that they are not supposed to access. VLAN hopping can allow an attacker to bypass security policies, access sensitive data, or launch other attacks on the network. VLAN hopping can be performed using two methods: double tagging and switch spoofing<sup>1</sup>.

Double tagging is where the attacker sends a frame with two VLAN tags, one for the native VLAN and one for the target VLAN. The native VLAN is the VLAN that is used for untagged traffic on a trunk port. If the attacker's access port is in the same VLAN as the native VLAN, the switch will accept the frame and forward it on the trunk port. The switch will remove the first tag, which is the native VLAN, and send the frame with the second tag, which is the target VLAN. The frame will then reach the target VLAN and be processed by the devices in that VLAN.

Switch spoofing is where the attacker sends Dynamic Trunking Protocol (DTP) packets and tries to negotiate a trunk with the switch. DTP is a Cisco protocol that allows switches to automatically form trunks between them. If the switch's port is configured with the default dynamic auto or dynamic desirable mode, it will accept the DTP packets and form a trunk with the attacker. The attacker will then have access to all VLANs on the trunk.

To prevent VLAN hopping, the junior network engineer is trying to change the native network ID to a non-default value that can then be applied consistently throughout the network environment. This means that the engineer is changing the VLAN that is used for untagged traffic on the trunk ports to a different VLAN than the default VLAN 1. This will prevent double tagging attacks, as the attacker's access port will not be in the same VLAN as the native VLAN, and the switch will not accept the frames with two tags. The engineer should also disable DTP on the trunk ports and use the switchport nonegotiate command to prevent switch spoofing attacks<sup>2</sup>.

ReferencesVLAN Hopping - NetworkLessons.comVLAN Hopping on Native VLAN - Cisco Community

#### NEW QUESTION 333

- (Topic 3)

A network consultant is installing a new wireless network with the following specifications:

5GHz

1,300Mbps 20/40/80MHz

Which of the following standards should the network consultant use?

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

**Answer:** B

#### NEW QUESTION 335

- (Topic 3)

A user cannot connect to the network, although others in the office are unaffected. The network technician sees that the link lights on the NIC are not on. The technician needs to check which switchport the user is connected to, but the cabling is not labeled. Which of the following is the best way for the technician to find where the computer is connected?

- A. Look up the computer's IP address in the switch ARP table.
- B. Use a cable tester to trace the cable.
- C. Look up the computer's MAC address in the switch CAM table.
- D. Use a tone generator to trace the cable.

**Answer:** D

#### Explanation:

A tone generator is a device that emits an audible signal on a wire. A tone probe is a device that detects the signal on the wire. By attaching the tone generator to one end of the cable and using the tone probe to scan the other end, the technician can identify which switchport the cable is connected to. This method does not require any knowledge of the computer's IP or MAC address, or access to the switch configuration. It is also faster and more reliable than physically tracing the cable or disconnecting the cable and looking for the link light to go out on the switch.

ReferencesHow to find what port im connected to on a switch from my PC?Switch Port Monitoring Guide - ComparitechFinding Out Which Network Switch Port My Computer is Connected

#### NEW QUESTION 338

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual N10-009 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the N10-009 Product From:

<https://www.2passeasy.com/dumps/N10-009/>

## Money Back Guarantee

### N10-009 Practice Exam Features:

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