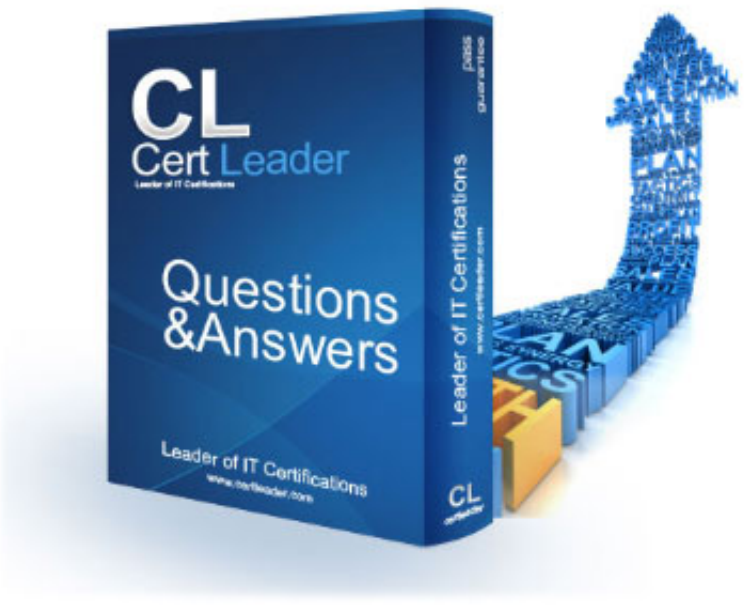
N10-009 Dumps

CompTIA Network+ Exam

https://www.certleader.com/N10-009-dumps.html



NEW QUESTION 1
- (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 2
- (Topic 3)
A user notifies a network administrator about losing access to a remote file server. The network administrator is able to ping the server and verifies the current firewall rules do not block access to the network fileshare. Which of the following tools would help identify which ports are open on the remote file server?

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

Answer: B

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

NEW QUESTION 3
- (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 4
- (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 5

- (Topic 3)
The following DHCP scope was configured for a new VLAN dedicated to a large deployment of 325 loT sensors:

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

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

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

Answer: B

NEW QUESTION 6
- (Topic 3)
A network technician 13 troubleshooting a specific port on a switch. Which of the following commands should the technician use to see the port configuration?

A. show route
B. show Interface
C. show arp
D. show port

Answer: B

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

NEW QUESTION 7
- (Topic 3)
A Wi-Fi network was recently deployed in a new, multilevel budding. 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 8
- (Topic 3)
Which of the following technologies would MOST likely De 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 9
- (Topic 3)
A technician monitors a switch interface and notices it is not forwarding frames on a trunked port. However, the cable and interfaces are in working order. Which of the following is MOST likely the cause of the issue?

A. STP policy
B. Flow control
C. 802.1Q configuration
D. Frame size

Answer: C

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

NEW QUESTION 10
- (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 10
- (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 13
- (Topic 3)
Which of the following DNS records maps an alias to a true name?

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

Answer: D

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

NEW QUESTION 18
- (Topic 3)
A network administrator would like to purchase a device that provides access ports to endpoints and has the ability to route between networks. Which of the following would be BEST for the administrator to purchase?

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

Answer: B

NEW QUESTION 21
- (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 22
- (Topic 3)
Network traffic is being compromised by DNS poisoning every time a company's router is connected to the internet. The network team detects a non-authorized DNS server being assigned to the network clients and remediates the incident by setting a trusted DNS server, but the issue occurs again after internet exposure. Which of the following best practices should be implemented on the router?

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

Answer: A

NEW QUESTION 26
- (Topic 3)
Which of the following would be used to adjust resources dynamically for a virtual web server under variable loads?

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

Answer: B

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

NEW QUESTION 27
- (Topic 3)
A network architect is developing documentation for an upcoming IPv4/IPv6 dual-stack implementation The architect wants to shorten the following IPv6 address: ef82:0000:00O0:000O:0O00:1ab1:1234:1bc2. Which of the following is the MOST appropriate shortened version?

A. ef82:0:lab1:1234:1bc2
B. ef82:0:;1ab1:1234:1bc2
C. ef82:0:0:0:0:1ab1:1234:1bc2
D. ef82::1ab1:1234:1bc2

Answer: D

Explanation:
The most appropriate shortened version of the IPv6 address ef82:0000:00O0:000O:0O00:1ab1:1234:1bc2 is ef82::1ab1:1234:1bc2. IPv6 addresses are 128-bit hexadecimal values that are divided into eight groups of 16 bits each, separated by colons. IPv6 addresses can be shortened by using two rules: omitting leading zeros within each group, and replacing one or more consecutive groups of zeros with a double colon (::). Only one double colon can be used in an address. Applying these rules to the given address results in ef82::1ab1:1234:1bc2. References: CompTIA Network+ N10-008 Certification Study Guide, page 114; The Official CompTIA Network+ Student Guide (Exam N10-008), page 5-7.

NEW QUESTION 31
- (Topic 3)
A company is opening a new building on the other side of its campus. The distance from the closest building to the new building is 1,804ft (550m). The company needs to connect the networking equipment in the new building to the Other buildings on the campus without using a repeater. Which Of the following transceivers should the company use?

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

Answer: B

Explanation:
10GBASE-LR is a standard for 10 Gbps Ethernet over single-mode fiber optic cable. It can support a maximum distance of 6.2 miles (10 km), which is much longer than the distance between the buildings. 10GBASE-SW, 10GBASE-LX4, and 10GBASE- SR are all standards for 10 Gbps Ethernet over multimode fiber optic cable, which have shorter maximum distances ranging from 984ft (300m) to 1,312ft (400m).
References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 1.5: Compare and contrast network cabling types, standards and speeds.

NEW QUESTION 33
- (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 38
- (Topic 3)
A VOIP phone is plugged in to a port but cannot receive calls. Which Of the following needs to be done on the port to address the issue?

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

Answer: C

Explanation:
To enable a VOIP phone to receive calls on a port, the traffic needs to be tagged to the voice VLAN that is configured on the switch. This allows the phone to communicate with the voice network and the PBX server. Tagging the traffic also separates the voice traffic from the data traffic that may be coming from a computer connected to the phone. The port should be configured to tag the traffic for the voice VLAN and untag the traffic for the data VLAN1. Trunking all VLANs on the port is unnecessary and may cause security issues. Configuring the native VLAN is not relevant for this issue. Disabling VLANs would prevent the phone from working at all.
References:
Optical Fiber Connectors – CompTIA Network+ N10-007 – 2.13
? VoIP and computer on separate VLANs through one cable1

NEW QUESTION 42
- (Topic 3)
A network administrator installed an additional IDF during a building expansion project. Which of the following documents need to be updated to reflect the change? (Select TWO).

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

Answer: AF

NEW QUESTION 46
- (Topic 3)
A network administrator is configuring a new switch and wants to connect two ports to the core switch to ensure redundancy. Which of the following configurations would meet this
requirement?

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

Answer: D

Explanation:
Link aggregation is a technique that allows multiple physical ports to be combined into a single logical channel, which provides increased bandwidth, load balancing, and redundancy. Link aggregation can be configured using protocols such as Link Aggregation Control Protocol (LACP) or static methods.
References
? Link aggregation is one of the common Ethernet switching features covered in Objective 2.3 of the CompTIA Network+ N10-008 certification exam1.
? Link aggregation can be used to connect two ports to the core switch to ensure redundancy23.
? Link aggregation can be configured using LACP or static methods23.
1: CompTIA Network+ Certification Exam Objectives, page 5 2: Interface Configurations – N10-008 CompTIA Network+ : 2.3 3: CompTIA Network+ N10-008 Cert Guide, Chapter 11, page 323

NEW QUESTION 47
- (Topic 3)
Which of the following best describe the functions of Layer 2 of the OSI model? (Select two).

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

Answer: AD

Explanation:
Layer 2 of the OSI model, also known as the data link layer, is responsible for physical addressing and error detecting. Physical addressing refers to the use of MAC addresses to identify and locate devices on a network segment. Error detecting refers to the use of techniques such as checksums and CRCs to identify and correct errors in the data frames.
References:
? OSI Model | Computer Networking | CompTIA1

NEW QUESTION 50
- (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 54
- (Topic 3)
Which of the following describes traffic going in and out of a data center from the internet?

A. Demarcation point
B. North-South
C. Fibre Channel
D. Spine and leaf

Answer: B

NEW QUESTION 55
- (Topic 3)
A technician is working on a ticket for a user in the human resources department who received a new PC that does not connect to the internet. All users in human resources can access the
internet. The technician can ping the PC from the human resources router but not from the IT network. Which of the following is the most likely cause of the issue?

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

Answer: D

Explanation:
An incorrect default gateway can cause a PC to not connect to the internet, because the default gateway is the device that routes traffic from the local network to other networks. If the PC has a wrong default gateway configured, it may not be able to reach the internet router or the IT network router. The technician can ping the PC from the human resources router because they are on the same local network, but not from the IT network router because they are on different networks.
A duplicate IP address can cause a PC to not communicate with other devices on the same network, because the IP address is the unique identifier of a device on a network. If two devices have the same IP address, they may cause IP conflicts and packet loss. However, a duplicate IP address would not prevent the technician from pinging the PC from the human resources router, because they are on the same network.
A misconfigured RIP can cause a router to not learn or advertise routes to other networks, because RIP is a routing protocol that dynamically exchanges routing information between routers. If a router has a wrong RIP configuration, it may not be able to reach or share routes with other routers. However, a misconfigured RIP would not affect the PC's connectivity to the internet, because the PC does not use RIP.
An improper VLAN assignment can cause a PC to not communicate with other devices on the same or different networks, because a VLAN is a logical segmentation of a network that isolates traffic based on criteria such as function, security, or performance. If a PC is assigned to a wrong VLAN, it may not be able to access the resources or services that it needs. However, an improper VLAN assignment would not prevent the technician from pinging the PC from the human resources router, because they are on the same physical network.
References
What is a Default Gateway?
What's an IP Conflict and How Do You Resolve It? What is RIP (Routing Information Protocol)?
What is a VLAN? How to Set Up a VLAN Network
CompTIA Network+ Certification All-in-One Exam Guide, Eighth Edition (Exam N10-008)

NEW QUESTION 60
- (Topic 3)
A technician is deploying a new SSID for an industrial control system. The control devices require the network to use encryption that employs TKIP and a symmetrical password to connect. Which of the following should the technician configure to ensure compatibility with the control devices?

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

Answer: C

Explanation:
"WPA uses Temporal Key Integrity Protocol (TKIP) for enhanced encryption. TKIP uses RC4 for the encryption algorithm, and the CompTIA Network+ exam may reference TKIP-RC4 in a discussion of wireless."
" WPA2 uses Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) for integrity checking and Advanced Encryption Standard (AES) for encryption. On the Network+ exam, you might find this referenced as simply CCMP-AES"

NEW QUESTION 65
- (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 node12. SLAAC uses link-local addresses and the interface's MAC address or a random number to generate the host portion of the IPv6 address2. SLAAC also relies on Router Solicitation (RS) and Router Advertisement (RA) messages to obtain the network prefix and other information from a router12. 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 accordingly3.
References1 - IPv6 Stateless Address Auto-configuration (SLAAC) | NetworkAcademy.io2 - IPv6 SLAAC – Stateless Address Autoconfiguration - Study-CCNA3 - Mastering IPv6
SLAAC Concepts and Configuration - Cisco Press

NEW QUESTION 66
- (Topic 3)
Which of the following ports is a secure protocol?

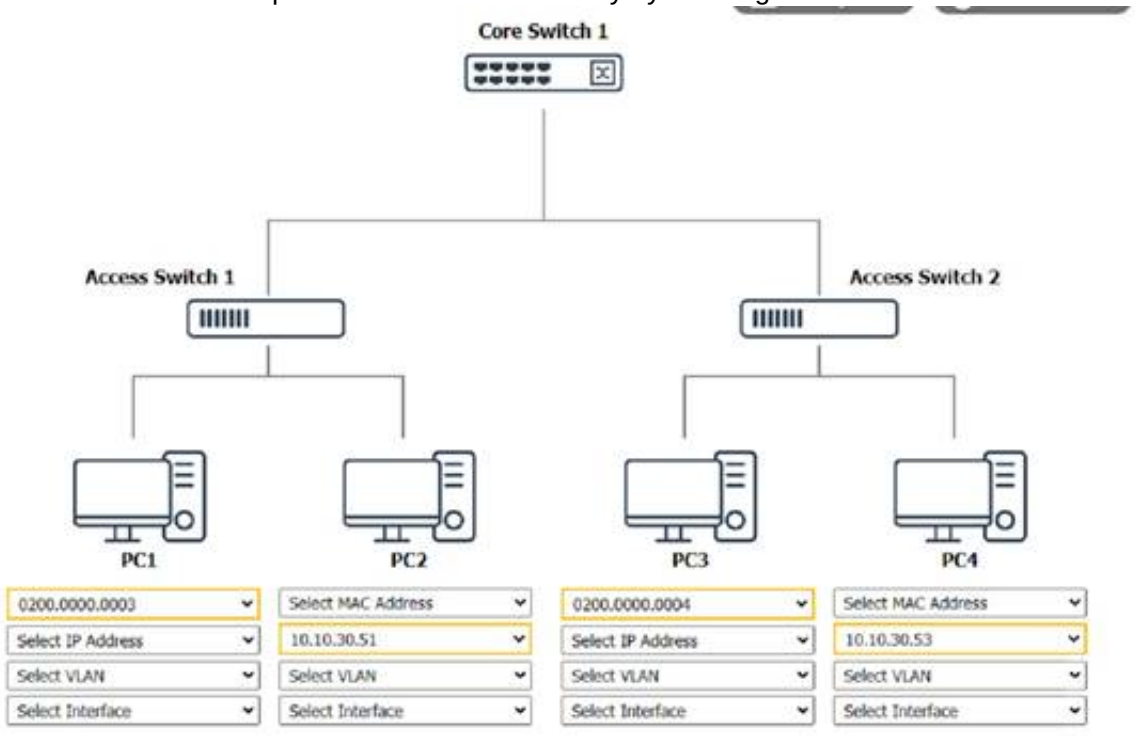
A. 20
B. 23
C. 443
D. 445

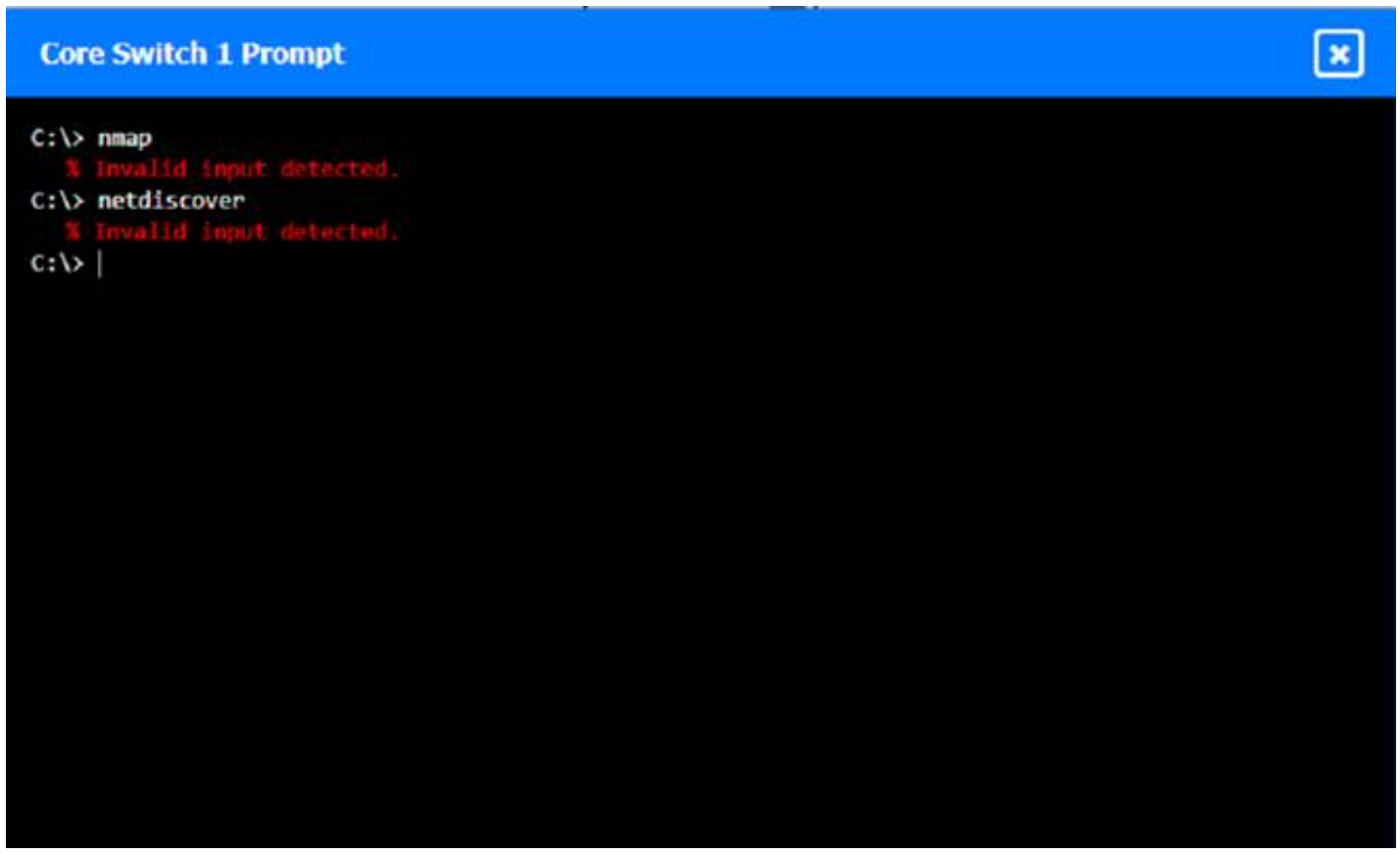
Answer: C

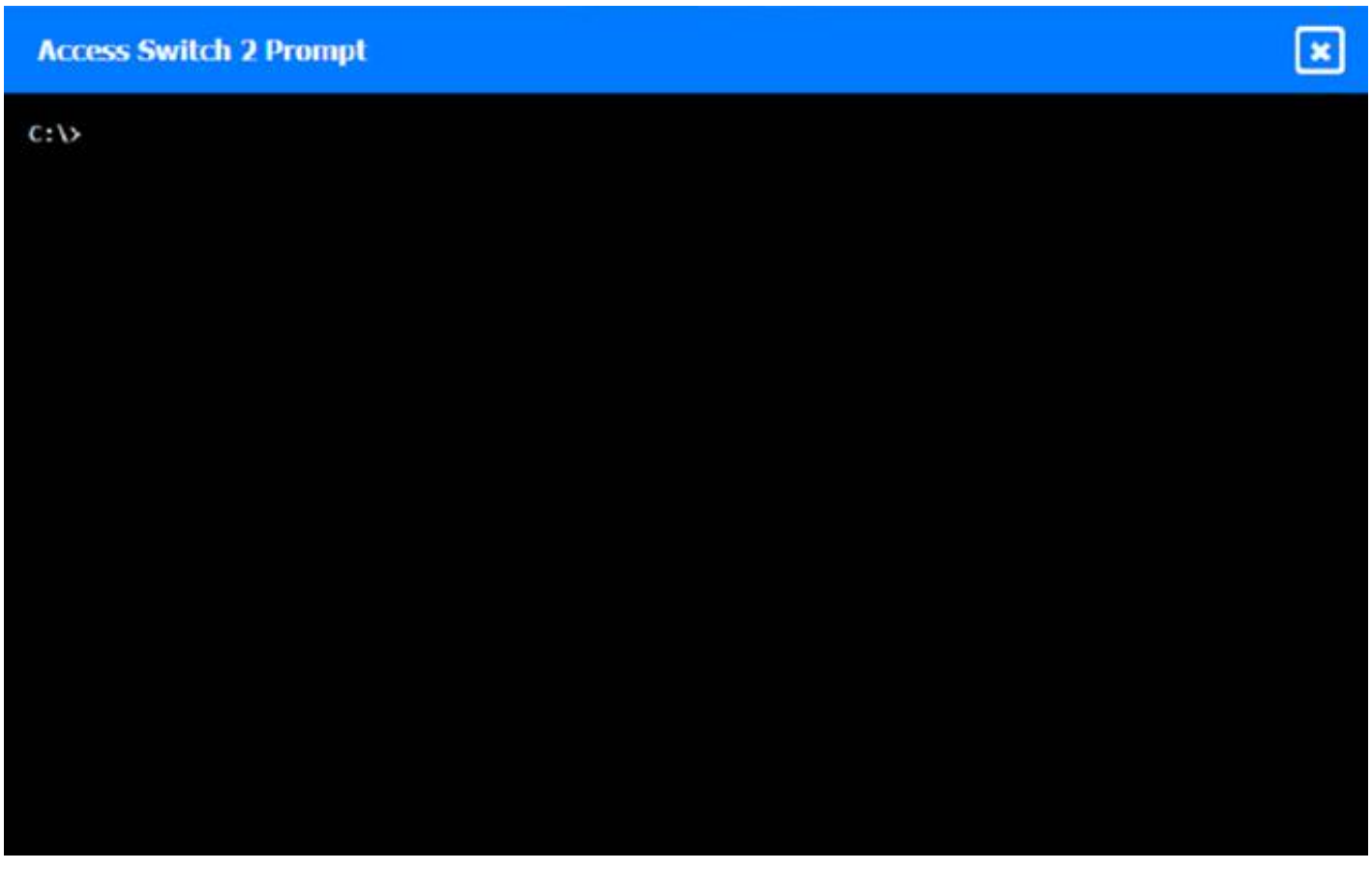
Explanation:
This is the port number for HTTPS, which stands for Hypertext Transfer Protocol Secure. HTTPS is a secure version of HTTP, which is the protocol used to communicate between web browsers and web servers. HTTPS encrypts the data sent and received using SSL/TLS, which are cryptographic protocols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

NEW QUESTION 71

SIMULATION - (Topic 3)
A network technician was recently onboarded to a company. A manager has
tasked the technician with documenting the network and has provided the technician With partial information from previous documentation.
Instructions:
Click on each switch to perform a network discovery by entering commands into the terminal. Fill in the missing information using drop-down menus provided.







A. Mastered
B. Not Mastered

Answer: A

Explanation:
(Note: Ips will be change on each simulation task, so we have given example answer for the understanding)
To perform a network discovery by entering commands into the terminal, you can use the following steps:
? Click on each switch to open its terminal window.
? Enter the command show ip interface brief to display the IP addresses and statuses of the switch interfaces.
? Enter the command show vlan brief to display the VLAN configurations and assignments of the switch interfaces.
? Enter the command show cdp neighbors to display the information about the neighboring devices that are connected to the switch.
? Fill in the missing information in the diagram using the drop-down menus provided. Here is an example of how to fill in the missing information for Core Switch 1:
? The IP address of Core Switch 1 is 192.168.1.1.
? The VLAN configuration of Core Switch 1 is VLAN 1: 192.168.1.0/24, VLAN 2: 192.168.2.0/24, VLAN 3: 192.168.3.0/24.
? The neighboring devices of Core Switch 1 are Access Switch 1 and Access Switch 2.
? The interfaces that connect Core Switch 1 to Access Switch 1 are GigabitEthernet0/1 and GigabitEthernet0/2.
? The interfaces that connect Core Switch 1 to Access Switch 2 are GigabitEthernet0/3 and GigabitEthernet0/4.
You can use the same steps to fill in the missing information for Access Switch 1 and Access Switch 2.

NEW QUESTION 76
- (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 79
- (Topic 3)
After installing a new wireless access point, an engineer tests the device and sees that it is not performing at the rated speeds. Which of the following should the engineer do to troubleshoot the issue? (Select two).

A. Ensure a bottleneck is not coming from other devices on the network.
B. Install the latest firmware for the device.
C. Create a new VLAN for the access point.
D. Make sure the SSID is not longer than 16 characters.
E. Configure the AP in autonomous mode.
F. Install a wireless LAN controller.

Answer: AB

Explanation:
One possible cause of poor wireless performance is a bottleneck in the network, which means that other devices or applications are consuming too much bandwidth or resources and limiting the speed of the wireless access point. To troubleshoot this issue, the engineer should ensure that there is no congestion or

interference from other devices on the network, such as wired clients, servers, routers, switches, or other wireless access points. The engineer can use tools such as network analyzers, bandwidth monitors, or ping tests to check the network traffic and latency12.
Another possible cause of poor wireless performance is outdated firmware on the device, which may contain bugs or vulnerabilities that affect the functionality or security of the wireless access point. To troubleshoot this issue, the engineer should install the latest firmware for the device from the manufacturer's website or support portal. The engineer should follow the instructions carefully and backup the configuration before updating the firmware. The engineer can also check the release notes or changelog of the firmware to see if there are any improvements or fixes related to the wireless performance3 .
The other options are not relevant to troubleshooting poor wireless performance. Creating a new VLAN for the access point may help with network segmentation or security, but it will not improve the speed of the wireless connection. Making sure the SSID is not longer than 16 characters may help with compatibility or readability, but it will not affect the wireless performance. Configuring the AP in autonomous mode may give more control or flexibility to the engineer, but it will not enhance the wireless speed. Installing a wireless LAN controller may help with managing multiple access points or deploying advanced features, but it will not increase the wireless performance.

NEW QUESTION 84
- (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 87
- (Topic 3)
Which of the following would be BEST suited for a long cable run with a 40Gbps bandwidth?

A. Cat 5e
B. Cat 6a
C. Cat 7
D. Cat 8

Answer: C

Explanation:
Cat 7 is a type of twisted-pair copper cable that supports up to 40 Gbps bandwidth and up to 100 meters cable length. Cat 7 is suitable for long cable runs that require high-speed data transmission. Cat 7 has better shielding and crosstalk prevention than lower categories of cables.
References: Network+ Study Guide Objective 1.5: Compare and contrast network cabling types, features and their purposes.

NEW QUESTION 88
- (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 90
- (Topic 3)
A network engineer is troubleshooting application connectivity issues between a server and a client. The network engineer needs to view the certificate exchange between the two hosts. Which of the following tools should the network engineer use?

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

Answer: B

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

NEW QUESTION 94
- (Topic 3)
A network technician needs to use an RFC1918 IP space for a new office that only has a single public IP address. Which of the following subnets should the

technician use for the LAN?

A. 10.10.10.0/24
B. 127.16.10.0/24
C. 174.16.10.0/24
D. 198.18.10.0/24

Answer: A

Explanation:
The RFC1918 IP space is a set of private IP addresses that are not routable on the public Internet and can be used for internal networks. The RFC1918 IP space consists of three ranges: 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/161 Out of the four options, only A. 10.10.10.0/24 belongs to one of these ranges, specifically the 10.0.0.0/8 range. Therefore, the technician should use this subnet for the LAN.
References1: https://en.wikipedia.org/wiki/Private_network

NEW QUESTION 96
- (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 100
- (Topic 3)
Which of the following would be the BEST choice to connect branch sites to a main office securely?

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

Answer: A

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

NEW QUESTION 103
- (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 108

- (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 112
- (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 116
- (Topic 3)
To comply with an industry regulation, all communication destined to a secure server should be logged and archived on a storage device. Which of the Mowing can be configured to fulfill this requirement?

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

Answer: B

NEW QUESTION 118
- (Topic 3)
Which of the following connectors and terminations are required to make a Cat 6 cable that connects from a PC to a non-capable MDIX switch? (Select TWO).

A. T1A-568-A - TIA-568-B
B. TIA-568-B - TIA-568-B
C. RJ11
D. RJ45
E. F-type

Answer: AD

NEW QUESTION 122
- (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 127
- (Topic 3)
A network administrator is setting up a web-based application for a company. The application needs to be continually accessible to all end users.
Which of the following would best ensure this need is fulfilled?

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

Answer: D

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

NEW QUESTION 129
- (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 131
- (Topic 3)
Which of the following can be used to limit the ability of devices to perform only HTTPS connections to an internet update server without exposing the devices to the public internet?

A. Allow connections only to an internal proxy server.
B. Deploy an IDS system and place it in line with the traffic.
C. Create a screened network and move the devices to it.
D. Use a host-based network firewall on each device.

Answer: A

Explanation:
An internal proxy server is a server that acts as an intermediary between internal devices and external servers on the internet. An internal proxy server can be used to limit the ability of devices to perform only HTTPS connections to an internet update server by filtering and forwarding the requests and responses based on predefined rules or policies. An internal proxy server can also prevent the devices from being exposed to the public internet by hiding their IP addresses and providing a layer of security and privacy.

NEW QUESTION 134
- (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 137
- (Topic 3)
An infrastructure company is implementing a cabling solution to connect sites on multiple continents. Which of the following cable types should the company use for this project?

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

Answer: B

Explanation:
Single-mode fiber is a type of optical fiber that has a small core diameter and allows only one mode of light to propagate. This reduces signal attenuation and increases transmission distance, making it suitable for long-distance communication networks.
Single-mode fiber can carry data over thousands of kilometers without requiring repeaters or amplifiers. Single-mode fiber is also immune to electromagnetic interference and has a higher bandwidth than multimode fiber. Therefore, single-mode fiber is the best cable type for connecting sites on multiple continents.
References: [CompTIA Network+ Certification Exam Objectives], [Single-mode optical fiber - Wikipedia]
Single-mode fiber optic cable uses a single ray of light to transmit data. This allows it to achieve very low attenuation and high bandwidth.
Multimode fiber optic cable uses multiple rays of light to transmit data. This results in higher attenuation and lower bandwidth than single-mode cable.
Twisted pair copper cable uses two insulated copper wires to transmit data. It is less expensive than fiber optic cable, but it has higher attenuation and lower bandwidth. When choosing a cable type for a long-distance application, it is important to consider the following factors:
? Attenuation: The amount of signal loss that occurs over the length of the cable.
? Bandwidth: The amount of data that can be transmitted over the cable per second.
? Cost: The cost of the cable and installation.
Single-mode fiber optic cable is the best choice for long-distance applications because it
has the lowest attenuation and highest bandwidth of any cable type. However, it is also the most expensive cable type.

NEW QUESTION 140
- (Topic 3)
A network technician is troubleshooting a connection to a web server. The Technician Is unable to ping the server but is able to verify connectivity to the web service using Tenet. Which of the following protocols is being blocked by me firewall?

A. UDP
B. ARP
C. ICMP
D. TCP

Answer: C

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

NEW QUESTION 142
- (Topic 3)
A network administrator wants to know which systems on the network are at risk of a known vulnerability. Which of the following should the administrator reference?

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

Answer: E

Explanation:
A Common Vulnerabilities and Exposures (CVE) is a publicly available database of known security vulnerabilities and exposures that affect various software and hardware products. A CVE entry provides a standardized identifier, a brief description, and references to related sources of information for each vulnerability or exposure. A network administrator can reference the CVE database to check if any of the systems on the network are affected by a known vulnerability, and if so, what are the potential impacts and mitigations.
A Service Level Agreement (SLA) is a contract between a service provider and a customer that defines the expected level and quality of service, such as availability, performance, and security. An SLA does not provide information on specific vulnerabilities or exposures affecting the systems or services.
A Patch Management Policy is a set of rules and procedures that govern how patches are applied to systems and software to fix bugs, improve functionality, or address security issues. A patch management policy can help prevent or reduce the risk of vulnerabilities or exposures, but it does not provide information on specific vulnerabilities or exposures affecting the systems or software.
A Non-Disclosure Agreement (NDA) is a legal contract between two or more parties that prohibits the disclosure of confidential or proprietary information to unauthorized parties. An NDA does not provide information on specific vulnerabilities or exposures affecting the systems or information.
A Site Survey Report is a document that summarizes the results of a physical inspection and assessment of a network site, such as the layout, infrastructure, equipment, and environmental conditions. A site survey report can help identify and resolve potential network issues, such as interference, signal strength, or coverage, but it does not provide information on specific vulnerabilities or exposures affecting the network devices or software.
References
What is CVE?
What is a Service Level Agreement (SLA)? Guide to Enterprise Patch Management Planning
NDA, MSA, SOW and SLA. Confidentiality agreements when you outsource QA Site Survey Report

NEW QUESTION 146
- (Topic 3)
A network administrator is setting up a new phone system and needs to define the location where VoIP phones can download configuration files. Which of the following DHCP services can be used to accomplish this task?

A. Scope options
B. Exclusion ranges

C. Lease time
D. Relay

Answer: A

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

NEW QUESTION 147
- (Topic 3)
A technician is concerned about unauthorized personnel moving assets that are installed in a data center server rack. The technician installs a networked sensor that sends an alert when the server rack door is opened. Which of the following did the technician install?

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

Answer: D

Explanation:
Tamper detection is a physical security feature that can alert the technician when someone opens the server rack door without authorization. Tamper detection sensors can be installed inside the equipment or on the rack itself, and they can send an alert via email, SMS, or other methods. Tamper detection can help prevent unauthorized access, theft, or damage to the network assets.
References:
? Physical Security – N10-008 CompTIA Network+ : 4.51

NEW QUESTION 150
- (Topic 3)
A technician is consolidating a topology with multiple SSIDs into one unique SSiD deployment. Which of the following features will be possible after this new configuration?

A. Seamless roaming
B. Basic service set
C. WPA
D. MU-MIMO

Answer: A

NEW QUESTION 152
- (Topic 3)
A technician is configuring a static IP address on a new device in a newly created subnet. The work order specifies the following requirements:
• The IP address should use the highest address available in the subnet.
• The default gateway needs to be set to 172.28.85.94.
• The subnet mask needs to be 255.255.255.224.
Which of the following addresses should the engineer apply to the device?

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

Answer: A

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

NEW QUESTION 155
- (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 158
- (Topic 3)

A network technician is investigating why a core switch is logging excessive amounts of data to the syslog server. The running configuration of the switch showed the following logging information:
ip ssh logging events logging level debugging logging host 192.168.1.100 logging synchronous
Which of the following changes should the technician make to best fix the issue?

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

Answer: D

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

NEW QUESTION 159
- (Topic 3)
A company has been added to an unapproved list because of spam. The network administrator confirmed that a workstation was infected by malware. Which of the following processes did the administrator use to identify the root cause?

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

Answer: A

Explanation:
One possible process that the administrator used to identify the root cause of the spam issue is traffic analysis. Traffic analysis is a technique that monitors and analyzes the network traffic that flows between devices or applications. Traffic analysis can help troubleshoot network problems by identifying the source, destination, volume, frequency, and content of the network packets12.
To use traffic analysis to identify the root cause of the spam issue, the administrator could follow these steps:
? Install a traffic analysis tool on the server or a device that is connected to the same
network as the server, such as Wireshark3, tcpdump4, or Microsoft Network Monitor5.
? Start capturing the network traffic and filter it by using the IP address or hostname
of the server, or by using a specific port or protocol that is used by the email service, such as SMTP (port 25), POP3 (port 110), or IMAP (port 143).
? Analyze the filtered traffic and look for any signs of abnormal or malicious activity, such as high volume of outgoing emails, unknown recipients, suspicious attachments, or spam keywords.
? Trace back the source of the spam emails to the infected workstation by using its IP address or MAC address.
? Isolate and clean up the infected workstation by using an antivirus or malware removal tool.
The other options are not processes that the administrator used to identify the root cause of the spam issue. Availability monitoring is a technique that measures and reports the uptime and downtime of a network device or service. Availability monitoring can help troubleshoot network problems by detecting any failures or outages that affect the network performance. Baseline metrics are a set of standard measurements that establish the normal behavior or performance of a network device or service. Baseline metrics can help troubleshoot network problems by comparing the current state of the network with the expected state and identifying any deviations or anomalies. Network discovery is a technique that scans and maps the network devices and services that are connected to a network. Network discovery can help troubleshoot network problems by providing a comprehensive and updated view of the network topology and configuration.

NEW QUESTION 164
- (Topic 3)
Which of the following protocols should be used when Layer 3 availability is of the highest concern?

A. LACP
B. LDAP
C. FHRP
D. DHCP

Answer: C

Explanation:
FHRP stands for First Hop Redundancy Protocol, which is a group of protocols that allow routers or switches to provide backup or failover for the default gateway in a network. FHRP ensures that the network traffic can reach its destination even if the primary gateway fails or becomes unavailable. Some examples of FHRP protocols are HSRP, VRRP, and GLBP.
References
? 1: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 18
? 2: CompTIA Network+ N10-008 Certification Practice Test, question 9
? 3: CompTIA Network+ Study Guide: Exam N10-008, 5th Edition, page 263
? 4: CompTIA Network+ (N10-008) Practice Exam w/PBQ & Solution, question 5
? 5: What’s on the CompTIA Network+ 008 certification? | CompTIA, section 3.1

NEW QUESTION 169
- (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 174
- (Topic 3)
Which of the following is MOST appropriate for enforcing bandwidth limits when the performance of an application is not affected by the use of buffering but is heavily impacted by packet drops?

A. Traffic shaping
B. Traffic policing
C. Traffic marking
D. Traffic classification

Answer: B

Explanation:
Traffic policing is a mechanism that monitors the traffic in any network and enforces a bandwidth limit by discarding packets that exceed a certain rate1. This can reduce congestion and ensure fair allocation of bandwidth among different applications or users. However, discarding packets can also affect the performance and quality of some applications, especially those that are sensitive to packet loss, such as voice or video. Traffic shaping is a congestion control mechanism that delays packets that exceed a certain rate instead of discarding them1. This can smooth out traffic bursts and avoid packet loss, but it also introduces latency and jitter. Traffic shaping can be beneficial for applications that can tolerate some delay but not packet loss, such as file transfers or streaming.
Traffic marking is a mechanism that assigns different priority levels to packets based on their type, source, destination, or other criteria2. This can help to differentiate between different classes of service and apply different policies or treatments to them. However, traffic marking does not enforce bandwidth limits by itself; it only provides information for other mechanisms to act upon.
Traffic classification is a process that identifies and categorizes packets based on their characteristics, such as protocol, port number, payload, or behavior. This can help to distinguish between different types of traffic and apply appropriate policies or actions to them. However, traffic classification does not enforce bandwidth limits by itself; it only provides input for other mechanisms to use.

NEW QUESTION 178
- (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 two1. 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 source2.
•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 tag3.
•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 182
- (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 186
- (Topic 3)
A user reports that a crucial fileshare is unreachable following a network upgrade that was completed the night before. A network technician confirms the problem exists. Which of the following
troubleshooting Steps should the network technician perform NEXT?

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

Answer: A

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

NEW QUESTION 188
- (Topic 3)
A technician is contracted to install a redundant cluster of devices from the ISP In case of a hardware failure within the network. Which of the following would provide the BEST redundant solution in Layer 2 devices?

A. Multiple routers
B. Multiple switches
C. Multiple firewalls
D. Multiple budges

Answer: B

NEW QUESTION 191
- (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 194
- (Topic 3)
Which of the following is used when a workstation sends a DHCP broadcast to a server on another LAN?

A. Reservation
B. Dynamic assignment
C. Helper address
D. DHCP offer

Answer: C

Explanation:
A helper address is an IP address that is configured on a router interface to forward DHCP broadcast messages to a DHCP server on another LAN. A DHCP broadcast message is a message that a workstation sends when it needs to obtain an IP address from a DHCP server. Since broadcast messages are not routed across different networks, a helper address is needed to relay the DHCP broadcast message to the DHCP server on another network. References: https://www.comptia.org/training/books/network-n10-008- study-guide (page 199)

NEW QUESTION 197
- (Topic 3)
Which of the following would be used to indicate when unauthorized access to physical internal hardware has occurred?

A. Motion detectors
B. Radio frequency identification tags
C. Tamper evident seal
D. Locking racks

Answer: C

Explanation:
A tamper evident seal is a device or material that provides a visible indication of unauthorized access to physical internal hardware. Tamper evident seals can be stickers, labels, tapes, locks, or seals that are designed to break, tear, or change color when someone tries to open, remove, or tamper with them. Tamper evident seals can help deter and detect physical security breaches, such as theft, vandalism, or sabotage of hardware devices12. Tamper evident seals can also provide evidence for forensic analysis and legal action3.
References
1 - What Is Hardware Security? Definition, Threats, and Best Practices 2 - Device Physical Security Guideline | Information Security Office
3 - What is unauthorized physical access? – Heimduo

NEW QUESTION 202
- (Topic 3)
An organization has experienced an increase in malicious spear-phishing campaigns and wants to mitigate the risk of hyperlinks from inbound emails.
Which of the following appliances would best enable this capability?

A. Email protection gateway
B. DNS server
C. Proxy server
D. Endpoint email client
E. Sandbox

Answer: A

Explanation:
An email protection gateway is an appliance that can filter and block malicious emails and attachments before they reach the recipients. An email protection gateway can mitigate the risk of hyperlinks from inbound emails by scanning the links for malicious content, rewriting the links to point to a safe domain, or blocking the links altogether. An email protection gateway can also perform other functions such as spam filtering, antivirus scanning, encryption, and data loss prevention.
A DNS server, a proxy server, an endpoint email client, and a sandbox are not appliances that can enable this capability, as they have different purposes and functions.
References
? 1: CompTIA Network+ N10-008 Certification Study Guide, page 304
? 2: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 15
? 3: CompTIA Network+ N10-008 Certification Practice Test, question 5
? 4: Email Protection Gateway – N10-008 CompTIA Network+ : 3.2

NEW QUESTION 204
- (Topic 3)
A network engineer is investigating reports of poor network performance. Upon reviewing a report, the engineer finds hundreds of CRC errors on an interface.
Which of the following is the MOST likely cause of these errors?

A. A bad wire on the Cat 5e cable
B. The wrong VLAN assignment to the switchport
C. A misconfigured QoS setting on the router
D. Both sides of the switch trunk set to full duplex

Answer: A

NEW QUESTION 208
- (Topic 3)
A technician is troubleshooting a user's connectivity issues and finds that the computer's IP address was changed to 169.254.0.1.
Which of the following is the most likely reason?

A. Two or more computers have the same IP address in the ARP table.
B. The computer automatically set this address because the DHCP was not available.
C. The computer was set up to perform as an NTP server.
D. The computer is on a VPN and is the first to obtain a different IP address in that network.

Answer: B

Explanation:
IP addresses beginning with 169.254. are called link-local addresses or APIPA (Automatic Private IP Addressing)1. They are assigned by the computer itself when it cannot reach a DHCP server to obtain a valid IP address from the network2. This can happen for several reasons, such as a faulty router, a misconfigured network, or a disconnected cable3.
To troubleshoot this issue, the technician should check the network settings, the router configuration, and the physical connection of the computer. The technician should also try to renew the IP address by using the command ipconfig /renew in Windows or dhclient in Linux. If the problem persists, the technician may need to contact the network administrator or the ISP for further assistance.

NEW QUESTION 210
- (Topic 3)

A network administrator is reviewing north-south traffic to determine whether a security threat exists. Which of the following explains the type of traffic the administrator is reviewing?

A. Data flowing between application servers
B. Data flowing between the perimeter network and application servers
C. Data flowing in and out of the data center
D. Data flowing between local on-site support and backup servers

Answer: C

Explanation:
North-south traffic is any communication between components of a data center and another system, which is physically out of the boundary of the data center. It is also referred to as client-server traffic, as it usually involves requests from end users or external applications to the data center resources. For example, when a user accesses a web application hosted in a data center, the traffic between the user's browser and the web server is considered north-south traffic.

NEW QUESTION 213
- (Topic 3)
A newly installed VoIP phone is not getting the DHCP IP address it needs to connect to the phone system. Which of the following tasks needs to be completed to allow the phone to operate correctly?

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

Answer: A

NEW QUESTION 217
- (Topic 3)
A network technician is selecting new network hardware, and availability is the main concern. Which of the following availability concepts should the technician consider?

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

Answer: A

Explanation:
The availability concept that the network technician should consider when selecting new network hardware is RTO (Recovery Time Objective). RTO is a metric that defines the maximum acceptable time for restoring a system or service after a disruption or failure. RTO is based on the impact and cost of downtime for the business and its customers. RTO helps determine the level of redundancy and backup needed for network hardware to ensure high availability and minimize downtime. References: CompTIA Network+ N10-008 Certification Study Guide, page 346; The Official CompTIA Network+ Student Guide (Exam N10-008), page 13-9.

NEW QUESTION 221
- (Topic 3)
A network administrator is testing performance improvements by configuring channel bonding on an 802.Hac AP. Although a site survey detected the majority of the 5GHz frequency spectrum was idle, being used only by the company's WLAN and a nearby government radio system, the AP is not allowing the administrator to manually configure a large portion of the 5GHz frequency range. Which of the following would be BEST to configure for the WLAN being tested?

A. Upgrade the equipment to an AP that supports manual configuration of the ElRP power settings.
B. Switch to 802.11
C. disable channel auto-selection, and enforce channel bonding on the configuration.
D. Set up the AP to perform a dynamic selection of the frequency according to regulatory requirements.
E. Deactivate the band 5GHz to avoid Interference with the government radio

Answer: C

NEW QUESTION 224
- (Topic 3)
A network technician needs to install patch cords from the UTP patch panel to the access switch for a newly occupied set of offices. The patch panel is not labeled for easy jack identification. Which of the following tools provides the easiest way to identify the appropriate patch panel port?

A. Toner
B. Laptop
C. Cable tester
D. Visual fault locator

Answer: A

Explanation:
A toner is a tool that generates an audible signal that can be traced by a probe. A network technician can use a toner to identify the appropriate patch panel port by connecting the toner to one end of the patch cord and using the probe to scan the patch panel until the signal is detected. A toner is the easiest way to identify the patch panel port when the patch panel is not labeled, as it does not require a laptop, a cable tester, or a visual fault locator.
A toner can also be used to locate breaks or shorts in a cable, or to verify continuity. References:
? Using a Toner and Probe - CompTIA Network+ Certification (N10-008): The Total
Course Video

? CompTIA Network+ Certification Exam Objectives, page 141

NEW QUESTION 225
- (Topic 3)
Which of the following is a document that states what the minimum performance expectations are within a network?

A. Memorandum of understanding
B. Service-level agreement
C. Non-disclosure agreement
D. Baseline metrics

Answer: B

Explanation:
A service-level agreement (SLA) is a document that states what the minimum performance expectations are within a network, such as uptime, throughput, latency, and security. An SLA is usually signed between a service provider and a customer, and it specifies the penalties or remedies if the service level is not met

NEW QUESTION 229
- (Topic 3)
Which of the following ports should be used to securely receive mail that is synchronized across multiple devices?

A. 25
B. 110
C. 443
D. 993

Answer: D

NEW QUESTION 230
- (Topic 3)
Which of the following attacks, if successful, would provide a malicious user who is connected to an isolated guest network access to the corporate network?

A. VLAN hopping
B. On-path attack
C. IP spoofing
D. Evil twin

Answer: A

Explanation:
The attack which, if successful, would provide a malicious user who is connected to an isolated guest network access to the corporate network is VLAN hopping. VLAN hopping is an attack technique which involves tricking a switch into sending traffic from one VLAN to another. This is done by sending specially crafted packets, which force the switch to send traffic from one VLAN to another, thus allowing the malicious user to gain access to the corporate network.
VLAN hopping is an attack technique which involves tricking a switch into sending traffic from one VLAN to another. This is done by sending specially crafted packets, which force the switch to send traffic from one VLAN to another, thus allowing the malicious user to gain access to the corporate network. According to the CompTIA Network+ N10-008 Exam Guide VLAN hopping is a type of attack that is used to gain access to network resources that are not meant to be accessible by a user on a guest network.

NEW QUESTION 234
- (Topic 3)
A network manager wants to view network traffic for devices connected to a switch. A network engineer connects an appliance to a free port on the switch and needs to configure the switch port connected to the appliance. Which of the following is the best option for the engineer to enable?

A. Trunking
B. Port mirroring
C. Full duplex
D. SNMP

Answer: B

Explanation:
Port mirroring is a feature that allows a switch to copy the traffic from one or more ports to another port, where a network analyzer or a monitoring device can capture and analyze the traffic. Port mirroring is useful for troubleshooting and security purposes, as it allows the network engineer to see the traffic that is passing through the switch without affecting the normal operation of the network.
References
? 1: Port Mirroring - CompTIA Network+ Certification (N10-008): The Total Course [Video]
? 2: CompTIA Network+ Certification Exam Objectives, page 5
? 3: CompTIA Network+ N10-005: 2.1 – Port Mirroring - Professor Messer IT Certification Training Courses
? 4: CompTIA Network+ N10-005: 1.4 – Port Mirroring

NEW QUESTION 239
- (Topic 3)
A newly installed multifunction copier needs to be set up so scanned documents can be emailed to recipients. Which of the following ports from the copier's IP address should be allowed?

A. 22
B. 25
C. 53

D. 80

Answer: B

Explanation:
Port 25 is the port number that is commonly used for Simple Mail Transfer Protocol (SMTP), which is a protocol that allows sending and receiving email messages over a network1. Port 25 from the copier's IP address should be allowed so that scanned documents can be emailed to recipients.
Port 22 is the port number that is commonly used for Secure Shell (SSH), which is a protocol that allows secure and encrypted remote access and control of a device over a network1. Port 22 from the copier's IP address is not necessary for emailing scanned documents.
Port 53 is the port number that is commonly used for Domain Name System (DNS), which is a protocol that allows resolving domain names to IP addresses and vice versa on a network1. Port 53 from the copier's IP address is not necessary for emailing scanned documents.
Port 80 is the port number that is commonly used for Hypertext Transfer Protocol (HTTP), which is a protocol that allows transferring web pages and other resources over a network1. Port 80 from the copier's IP address is not necessary for emailing scanned documents.

NEW QUESTION 244
- (Topic 3)
A systems administrator wants to use the least amount of equipment to segment two departments that nave cables terminating in the same room. Which of the following would allow this to occur?

A. A load balancer
B. A proxy server
C. A Layer 3 switch
D. A hub
E. A Layer 7 firewall
F. The RSSI was not strong enough on the link

Answer: D

NEW QUESTION 247
- (Topic 3)
A new office space is being designed. The network switches are up. but no services are running yet A network engineer plugs in a laptop configured as a DHCP client to a switch Which ol the following IP addresses should be assigned to the laptop?

A. 10.1.1.1
B. 169.254.1.128
C. 172 16 128 128
D. 192 168.0.1

Answer: B

Explanation:
When a DHCP client is connected to a network and no DHCP server is available, the client can automatically configure a link-local address in the 169.254.0.0/16 range using the Automatic Private IP Addressing (APIPA) feature. So, the correct answer is option B, 169.254.1.128. This is also known as an APIPA address.
Reference: CompTIA Network+ Study Guide, Exam N10-007, Fourth Edition, by Todd
Lammle (Chapter 4: IP Addressing)

NEW QUESTION 250
- (Topic 3)
A company is deploying a SAN at headquarters and a branch office 1, 000ml (1,609km) away that w« access small amounts of data. Which of the following types of connections would be MOST cost effective to implement?

A. ISCSI
B. FCoE
C. Ethernet
D. FC

Answer: A

Explanation:
Mike Meyers
"Internet Small Computer Systems Interface (iSCSI) is built on top of TCP/IP, enabling devices that use the SCSI protocol to communicate across existing networks using cheap, readily available hardware."
Jason Dion
"iSCSI (IP Small Computer System Interface)
- Lower cost, built using Ethernet switches (<10 Gbps)
- Relies on configuration allowing jumbo frames over the network"

NEW QUESTION 254
- (Topic 3)
An engineer needs to restrict the database servers that are in the same subnet from communicating with each other. The database servers will still need to communicate with the application servers in a different subnet. In some cases, the database servers will be clustered, and the servers will need to communicate with other cluster members. Which of the following technologies will be BEST to use to implement this filtering without creating rules?

A. Private VLANs
B. Access control lists
C. Firewalls
D. Control plane policing

Answer: A

Explanation:
"Use private VLANs: Also known as port isolation, creating a private VLAN is a method of restricting switch ports (now called private ports) so that they can communicate only with a particular uplink. The private VLAN usually has numerous private ports and only one uplink, which is usually connected to a router, or firewall."

NEW QUESTION 257
- (Topic 3)
A user reports that a new VoIP phone works properly but the computer that is connected to the phone cannot access any network resources. Which of the following MOST Likely needs to be configured correctly to provide network connectivity to the computer?

A. Port duplex settings
B. Port aggregation
C. ARP settings
D. VLAN tags
E. MDIX settings

Answer: D

Explanation:
VLAN (virtual LAN) tags are used to identify packets as belonging to a particular VLAN. VLANs are used to segment a network into logical sub-networks, and each VLAN is assigned a unique VLAN tag. If the VLAN tag is not configured correctly, the computer may not be able to access network resources.

NEW QUESTION 262
- (Topic 3)
Which of the following will reduce routing table lookups by performing packet forwarding decisions independently of the network layer header?

A. MPLS
B. mGRE
C. EIGRP
D. VRRP

Answer: A

Explanation:
Multiprotocol Label Switching, or MPLS, is a networking technology that routes traffic using the shortest path based on “labels,” rather than network addresses, to handle forwarding over private wide area networks. As a scalable and protocol- independent solution, MPLS assigns labels to each data packet, controlling the path the packet follows. MPLS greatly improves the speed of traffic, so users don’t experience downtime when connected to the network.

NEW QUESTION 263
- (Topic 3)
A technician needs to set up a wireless connection that utilizes MIMO on non-overlapping channels. Which of the following would be the best choice?

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

Answer: D

Explanation:
802.11n is the best choice for setting up a wireless connection that utilizes MIMO on non-overlapping channels. 802.11n is a wireless standard that offers faster speeds and longer range than previous standards. 802.11n uses multiple-input multiple- output (MIMO) technology, which allows multiple antennas to transmit and receive multiple spatial streams of data simultaneously. MIMO can improve wireless performance, reliability, and capacity by exploiting multipath propagation and spatial diversity. 802.11n also uses non-overlapping channels in both the 2.4 GHz and 5 GHz frequency bands to
avoid interference and increase bandwidth. Non-overlapping channels are channels that do not share any part of their frequency spectrum with other channels.
References: [CompTIA Network+ Certification Exam Objectives], 802.11n - Wikipedia

NEW QUESTION 265
- (Topic 3)
A technician wants to monitor and provide traffic segmentation across the network. The technician would like to assign each department a specific identifier. Which of the following will the technician MOST likely use?

A. Flow control
B. Traffic shaping
C. VLAN tagging
D. Network performance baselines

Answer: C

Explanation:
To monitor and provide traffic segmentation across the network, a technician may use the concept of VLANs (Virtual Local Area Networks). VLANs are a way of dividing a single physical network into multiple logical networks, each with its own unique identifier or "tag."
By assigning each department a specific VLAN identifier, the technician can segment the network traffic and ensure that the different departments' traffic is kept separate from one another. This can help to improve network security, performance, and scalability, as well as allowing for better monitoring and control of the network traffic.
To implement VLANs, the technician will need to configure VLAN tagging on the network devices, such as switches and routers, and assign each department's devices to the appropriate VLAN. The technician may also need to configure VLAN trunking to allow the different VLANs to communicate with each other.
By using VLANs, the technician can effectively monitor and segment the network traffic, providing better control and visibility into the network.

NEW QUESTION 266
- (Topic 3)
Several end users viewing a training video report seeing pixelated images while watching. A network administrator reviews the core switch and is unable to find an immediate cause. Which of the following BEST explains what is occurring?

A. Jitter
B. Bandwidth
C. Latency
D. Giants

Answer: A

Explanation:
"Jitter is the loss of packets due to an overworked WAP. Jitter shows up as choppy conversations over a video call, strange jumps in the middle of an online game—pretty much anything that feels like the network has missed some data. Latency is when data stops moving for a moment due to a WAP being unable to do the work. This manifests as a Word document that stops loading, for example, or an online file that stops downloading."

NEW QUESTION 269
- (Topic 3)
A false camera is installed outside a building to assist with physical security. Which of the following is the device assisting?

A. Detection
B. Recovery
C. Identification
D. Prevention

Answer: A

NEW QUESTION 270
- (Topic 3)
An IT administrator received an assignment with the following objectives
• Conduct a total scan within the company's network tor all connected hosts
• Detect all the types of operating systems running on all devices
• Discover all services offered by hosts on the network
• Find open ports and detect security risks.
Which of the following command-line tools can be used to achieve these objectives?

A. nmap
B. arp
C. netatat
D. tcpdump

Answer: A

Explanation:
Nmap (Network Mapper) is a free and open source command line tool that can be used to scan a network for all connected hosts, detect the types of operating systems running on all devices, discover all services offered by hosts on the network, find open ports, and detect security risks. Nmap is commonly used by system administrators and security professionals to audit a network's security and identify possible vulnerabilities. Nmap can be used to discover active hosts, scan ports, fingerprint operating systems, detect running services, and more. Reference: CompTIA Network+ Study Manual, 8th Edition, page 592.

NEW QUESTION 275
- (Topic 3)
Which of the following OSI model layers are responsible for handling packets from the sources to the destination and checking for errors? (Select two).

A. Physical
B. Session
C. Data link
D. Network
E. Presentation
F. Application

Answer: CD

Explanation:
The data link and network layers are responsible for handling packets from the source to the destination and checking for errors. The data link layer is the second layer of the OSI model, which is a conceptual framework that describes how different network functions are organized and interact. The data link layer is responsible for providing reliable and efficient data transmission between two adjacent nodes on a network. The data link layer uses frames as its unit of data, and adds a header and a trailer to each frame that contain information such as source and destination MAC addresses, frame type, and error detection code. The data link layer can check for errors by using techniques such as parity check, checksum, or cyclic redundancy check (CRC). The network layer is the third layer of the OSI model, which is responsible for providing logical addressing and routing of packets across different networks. The network layer uses packets as its unit of data, and adds a header to each packet that contains information such as source and destination IP addresses, protocol type, and hop count. The network layer can check for errors by using techniques such as Internet Control Message Protocol (ICMP), which can send and receive error messages or diagnostic information. References: [CompTIA Network+ Certification Exam Objectives], Data Link Layer - an overview | ScienceDirect Topics, Network Layer - an overview | ScienceDirect Topics

NEW QUESTION 279
- (Topic 3)
Which of the following routing protocols is BEST suited for use on a perimeter router?

A. OSPF
B. RIPv2
C. EIGRP
D. BGP

Answer: D

Explanation:
BGP stands for Border Gateway Protocol and it is used to exchange routing information between autonomous systems (AS) on the Internet. A perimeter router is a router that connects an AS to another AS or to the Internet. Therefore, BGP is the best suited routing protocol for a perimeter router.
References: Network+ Study Guide Objective 2.4: Compare and contrast the characteristics of network topologies, types and technologies.

NEW QUESTION 283
- (Topic 3)
A global company has acquired a local company. The companies are geographically separate. The IP address ranges for the two companies are as follows:
· Global company: 10.0.0.0/16
· Local company: 10.0.0.0/24
Which of the following can the network engineer do to quickly connect the two companies?

A. Assign static routing to advertise the local company's network.
B. Assign an overlapping IP address range to both companies.
C. Assign a new IP address range to the local company.
D. Assign a NAT range to the local company.

Answer: C

Explanation:
Assigning a new IP address range to the local company is the best option to quickly connect the two companies without causing any IP address conflicts or overlaps. This option requires reconfiguring the local company’s network devices and updating the routing tables on both sides, but it avoids the need for any NAT or static routing solutions that may introduce additional complexity, cost, or performance issues12 References1: Connecting Networks with Overlapping IP Ranges 2: What Is Network Address Translation (NAT)?

NEW QUESTION 287
- (Topic 3)
Which of the following most likely determines the size of a rack for installation? {Select two).

A. KVM size
B. Switch depth
C. Hard drive size
D. Cooling fan speed
E. Outlet amperage
F. Server height

Answer: BF

Explanation:
The size of a rack for installation depends on several factors, such as the available space, the power and cooling requirements, and the dimensions of the equipment to be installed. Two of the most important dimensions to consider are the switch depth and the server height. Switch depth refers to the length of the switch from front to back, which determines how much space is needed inside the rack. Server height refers to the vertical space occupied by the server, which is measured in rack units (RU) or U. One rack unit is equal to 1.75 inches. The height of the rack should be able to accommodate the total number of rack units needed for the servers and other devices, as well as some extra space for cable management and airflow. References: CompTIA Network+ N10-008 Cert Guide, Chapter 2, Section 2.5

NEW QUESTION 292
- (Topic 3)
A security engineer is installing a new IOS on the network. The engineer has asked a network administrator to ensure all traffic entering and leaving the router interface is available for the IDS. Which of the following should the network administrator do?

A. Install a network tap for the IDS
B. Configure ACLs to route traffic to the IDS.
C. Install an additional NIC into the IDS
D. Install a loopback adapter for the IDS.
E. Add an additional route on the router for the IDS.

Answer: A

Explanation:
a network tap is a way of connecting an IDS out of band, which means it does not interfere with the normal network traffic. A network tap allows you to view a copy of the network traffic transmitted over the media being tapped.

NEW QUESTION 294
- (Topic 3)
Given the following Information:

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

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

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

Answer: D

NEW QUESTION 299
- (Topic 3)
A network administrator is planning to implement device monitoring to enhance network visibility. The security team requires that the solution provides authentication and encryption.
Which of the following meets these requirements?

A. SIEM
B. Syslog
C. NetFlow
D. SNMPv3

Answer: D

Explanation:
SNMPv3 is a protocol that allows network administrators to monitor and manage network devices such as routers, switches, servers, printers, and more. SNMPv3 provides authentication and encryption features that ensure the security and integrity of the data exchanged between the management station and the network devices. SNMPv3 uses a user-based security model (USM) that supports three levels of security: noAuthNoPriv, authNoPriv, and authPriv. The noAuthNoPriv level provides no authentication or encryption, the authNoPriv level provides authentication but no encryption, and the authPriv level provides both authentication and encryption12.
References
? SNMP is one of the common network monitoring protocols covered in Objective 3.1 of the CompTIA Network+ N10-008 certification exam3.
? SNMPv3 provides authentication and encryption features for network monitoring12.
? SNMPv3 uses a user-based security model with three levels of security12.
1: SNMP - N10-008 CompTIA Network+ : 3.1 - Professor Messer IT Certification Training Courses 2: CompTIA Network+ N10-008 Cert Guide, Chapter 13, page 413 3: CompTIA Network+ Certification Exam Objectives, page 7

NEW QUESTION 303
- (Topic 3)
A switch is connected to another switch. Incompatible hardware causes a surge in traffic on both switches. Which of the following configurations will cause traffic to pause, allowing the switches to drain buffers?

A. Speed
B. Flow control
C. 802.1Q
D. Duplex

Answer: B

Explanation:
Flow control is a mechanism that allows a network device to regulate the amount of traffic it can receive or send. Flow control can help prevent congestion and buffer overflow by sending pause frames or signals to the sender when the receiver's buffer is full or nearly full. Flow control can cause traffic to pause, allowing the switches to drain buffers and resume normal operation. Speed is a parameter that determines the data transfer rate of a network link. 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 308
- (Topic 3)
A client utilizes mobile tablets to view high-resolution images and videos via Wi-Fi within a corporate office building. The previous administrator installed multiple high-density APs with Wi-Fi 5, providing maximum coverage, but the measured performance is still below expected levels. Which of the following would provide the best solution?

A. Channel bonding
B. EIRP power settings
C. Antenna polarization
D. A directional antenna

Answer: A

Explanation:
Channel bonding is a technique that allows two or more adjacent channels to be combined into a wider channel, increasing the data rate and throughput of the wireless network. Channel bonding can improve the performance of the Wi-Fi network by utilizing more of the available spectrum and reducing interference from

other devices. Channel bonding is supported by Wi-Fi 5 (802.11ac) and Wi-Fi 6 (802.11ax) standards.
References: CompTIA Network+ N10-008 Cert Guide, Chapter 4, Section 4.2

NEW QUESTION 312
- (Topic 3)
Which of the following uses the link-state routing algorithm and operates within a single autonomous system?

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

Answer: B

Explanation:
OSPF uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS). OSPF is perhaps the most widely used interior gateway protocol (IGP) in large enterprise networks

NEW QUESTION 314
- (Topic 3)
Which of the following has the capability to centrally manage configuration, logging, and firmware versioning for distributed devices?

A. WLAN controller
B. Load balancer
C. SIEM solution
D. Syslog server

Answer: A

Explanation:
A WLAN controller is a device that manages and controls multiple wireless access points (WAPs) in a wireless LAN (WLAN). A WLAN controller has the capability to centrally manage configuration, logging, and firmware versioning for distributed WAPs. A WLAN controller can also provide load balancing, security, and quality of service (QoS) for the WLAN.
References: Network+ Study Guide Objective 3.1: Explain the purposes and use cases for advanced networking devices.

NEW QUESTION 316
- (Topic 3)
A technician manages a DHCP scope but needs to allocate a portion of the scope’s subnet for statically assigned devices. Which of the following DHCP concepts would be BEST to use to prevent IP address conflicts?

A. Dynamic assignment
B. Exclusion range
C. Address reservation
D. IP helper

Answer: B

Explanation:
To prevent IP address conflicts when allocating a portion of a DHCP scope's subnet for statically assigned devices, it is recommended to use the concept of DHCP exclusion ranges. DHCP exclusion ranges allow a DHCP administrator to specify a range of IP addresses within the scope that should not be assigned to DHCP clients. This can be useful in situations where some devices on the network need to be assigned static IP addresses, as it ensures that the statically assigned addresses do not overlap with addresses assigned by the DHCP server. To set up a DHCP exclusion range, the administrator needs to specify the start and end IP addresses of the range, as well as the subnet mask. The DHCP server will then exclude the specified range of addresses from its pool of available addresses, and will not assign them to DHCP clients. By using DHCP exclusion ranges, the technician can ensure that the statically assigned addresses do not conflict with addresses assigned by the DHCP server, and can prevent IP address conflicts on the network.
Anthony Sequeira
"Another frequent configuration you might make in a DHCP implementation is to configure an exclusion range. This is a portion of the address pool that you never want leased out to clients in the network. Perhaps you have numbered your servers 192.168.1.1–192.168.1.10. Because the servers are statically configured with these addresses, you exclude these addresses from the 192.168.1.0/24 pool of addresses."
Mike Meyers
"Exclusion ranges represent an IP address or range of IP addresses from the pool of addresses that are not to be given out by the DHCP server. Exclusions should be made for the static addresses manually configured on servers and router interfaces, so these IP addresses won’t be offered to DHCP clients."

NEW QUESTION 319
- (Topic 3)
An administrator wants to increase the availability of a server that is connected to the office network. Which of the following allows for multiple NICs to share a single IP address and offers maximum performance while providing fault tolerance in the event of a NIC failure?

A. Multipathing
B. Spanning Tree Protocol
C. First Hop Redundancy Protocol
D. Elasticity

Answer: A

Explanation:
Reference: https://docs.oracle.com/cd/E19455-01/806-6547/6jffv7oma/index.html

NEW QUESTION 323
- (Topic 3)
A network contains 25 access points. Which of the following devices would be best to change configurations on all the devices remotely?

A. WLAN controller
B. Load balancer
C. Bridge
D. Layer 3 switch

Answer: A

Explanation:
A WLAN controller is a device that can centrally manage and configure multiple access points in a wireless network. A WLAN controller can change settings on all the devices remotely, such as SSIDs, security policies, firmware updates, and channel assignments. A WLAN controller can also monitor the performance and status of the access points and provide load balancing and fault tolerance

NEW QUESTION 327
- (Topic 3)
A software developer changed positions within a company and is now a sales engineer. The security team discovered that the former software developer had been modifying code to implement small features requested by customers. Which of the following would be the best thing for the security administrator to implement to prevent this from happening?

A. A software patching policy
B. A role-based access control policy
C. Firewalls on the software development servers
D. Longer and more complex password requirements

Answer: B

Explanation:
A role-based access control (RBAC) policy is a security measure that assigns permissions and privileges to users based on their roles and responsibilities within an organization. RBAC helps to enforce the principle of least privilege, which states that users should only have the minimum level of access required to perform their tasks. RBAC also helps to prevent unauthorized access, modification, or misuse of sensitive data or resources by limiting the scope and impact of user actions.
A software patching policy, firewalls on the software development servers, and longer and more complex password requirements are all good security practices, but they do not directly address the issue of preventing the former software developer from modifying code. A software patching policy ensures that software is updated regularly to fix bugs and vulnerabilities, but it does not prevent a user from introducing new code changes. Firewalls on the software development servers protect the servers from external attacks, but they do not prevent a user from accessing the servers internally. Longer and more complex password requirements make it harder for attackers to guess or crack passwords, but they do not prevent a user from using their own valid credentials.
References
1: Role-Based Access Control (RBAC) - Definition and Examples 2: Network+ (Plus) Certification | CompTIA IT Certifications
3: [What is the Principle of Least Privilege? - Definition from Techopedia]

NEW QUESTION 329
- (Topic 3)
An administrator is attempting to add a new system to monitoring but is unsuccessful. The administrator notices the system is similar to another one on the network; however, the new one has an updated OS version. Which of the following should the administrator consider updating?

A. Management information bases
B. System baseline
C. Network device logs
D. SNMP traps

Answer: A

NEW QUESTION 331
- (Topic 3)
Two network technicians are installing a fiber-optic link between routers. The technicians used a light meter to verify the correct fibers However, when they connect the fibers to the router interface the link does not connect. Which of the following would explain the issue? (Select TWO).

A. They used the wrong type of fiber transceiver.
B. Incorrect TX/RX polarity exists on the link
C. The connection has duplexing configuration issues.
D. Halogen light fixtures are causing interference.
E. One of the technicians installed a loopback adapter.
F. The RSSI was not strong enough on the link

Answer: AB

NEW QUESTION 333
- (Topic 3)
An administrator would like to have two servers at different geographical locations provide fault tolerance and high performance while appearing as one URL to users. Which of the following should the administrator implement?

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

Answer: B

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

NEW QUESTION 336
- (Topic 3)
A network engineer needs to enable device monitoring using authentication and encryption. Which of the following protocols offers this option?

A. ESP
B. SNMPv3
C. NetFIow
D. SSLv3

Answer: B

Explanation:
SNMPv3 is a protocol that offers device monitoring using authentication and encryption. SNMP stands for Simple Network Management Protocol, and it is a standard way of collecting and organizing information about network devices, such as routers, switches, servers, printers, and so on. SNMPv3 is the latest version of SNMP, and it provides enhanced security features, such as data integrity, data origin authentication, data confidentiality, and access control. SNMPv3 can use different algorithms to encrypt and authenticate the communication between the network management system and the
network devices12. References:
? Network Monitoring Tools – CompTIA Network+ N10-006 – 2.12
? CompTIA Network+ N10-008 Certification Exam Objectives, page 93

NEW QUESTION 337
- (Topic 3)
A technician is checking network devices to look for opportunities to improve security Which of the following toots would BEST accomplish this task?

A. Wi-Fi analyzer
B. Protocol analyzer
C. Nmap
D. IP scanner

Answer: B

Explanation:
A protocol analyzer is a tool that can capture and analyze network traffic and identify security issues such as unauthorized devices, malicious packets, or misconfigured settings.
A Wi-Fi analyzer is a tool that can measure the signal strength, interference, and channel usage of wireless networks, but it cannot provide detailed information about network security.
Nmap and IP scanner are tools that can scan network hosts and ports for open services, vulnerabilities, or operating systems, but they cannot monitor network traffic in real time.

NEW QUESTION 342
- (Topic 3)
A network is secured and is only accessible via TLS and IPSec VPNs. Which of the following would need to be present to allow a user to access network resources on a laptop without logging in to the VPN application?

A. Site-to-site
B. Secure Shell
C. In-band management
D. Remote desktop connection

Answer: A

Explanation:
A site-to-site VPN is a type of VPN that connects two or more networks over the Internet using a secure tunnel. A site-to-site VPN allows users to access network resources on a laptop without logging in to the VPN application, as long as the laptop is connected to one of the networks in the VPN. A site-to-site VPN is transparent to the users and does not require any additional software or configuration on the client devices. References: Network+ Study Guide Objective 3.4: Explain the purposes and use cases for VPNs.

NEW QUESTION 346
- (Topic 3)
Which of the following would MOST likely utilize PoE?

A. A camera
B. A printer
C. A hub
D. A modem

Answer: A

Explanation:
A camera is most likely to utilize PoE (Power over Ethernet). PoE is a technology that allows electrical power to be delivered over Ethernet cables. It is used to

power a variety of devices, such as cameras, phones, access points, and other networking equipment.Cameras are particularly well-suited for PoE because they are often installed in locations where it is difficult or impossible to run electrical power. By using PoE, cameras can be powered directly over the Ethernet cable, eliminating the need for separate power cables and outlets.Other devices, such as printers, hubs, and modems, are less likely to utilize PoE because they typically do not need to be powered over Ethernet. These devices are usually powered by AC (alternating current) power and are typically connected to a power outlet rather than an Ethernet cable.

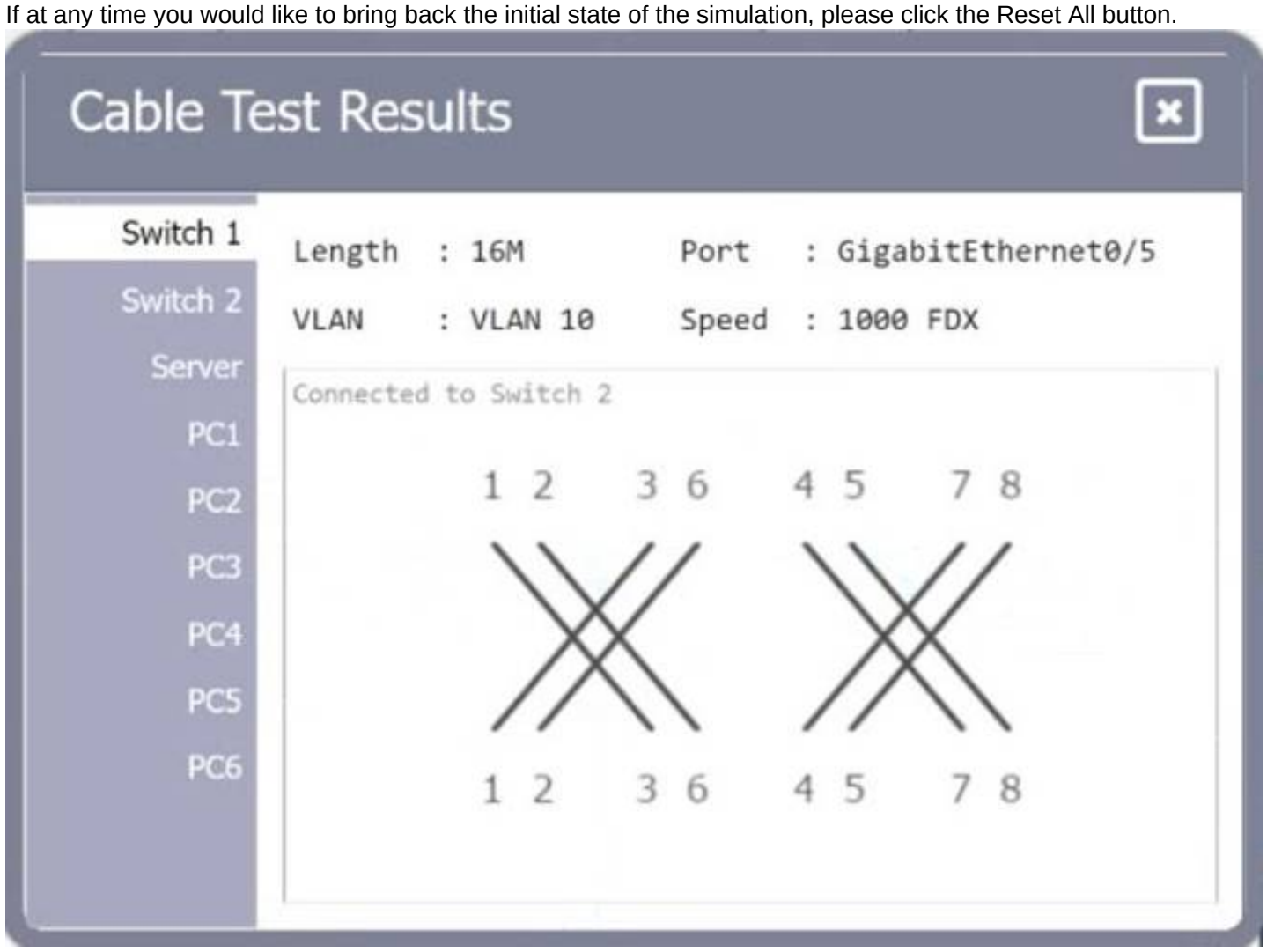
NEW QUESTION 348
- (Topic 3)
A network engineer is interested in using wireless technologies in densely forested areas. Which of the following frequencies would be best for this use?

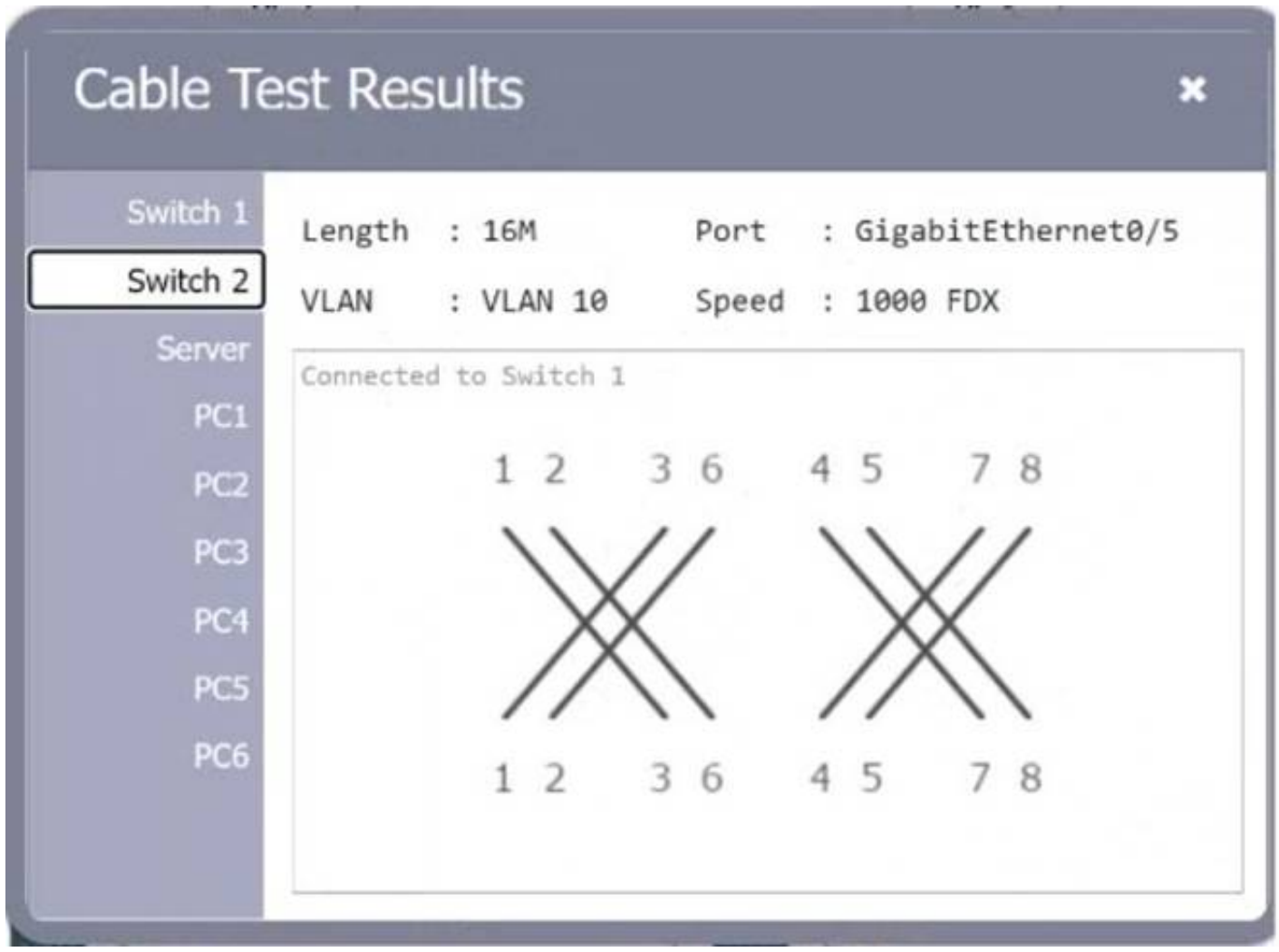
A. 2.4GHz
B. 5GHz
C. 5.9GHz
D. 6GHz

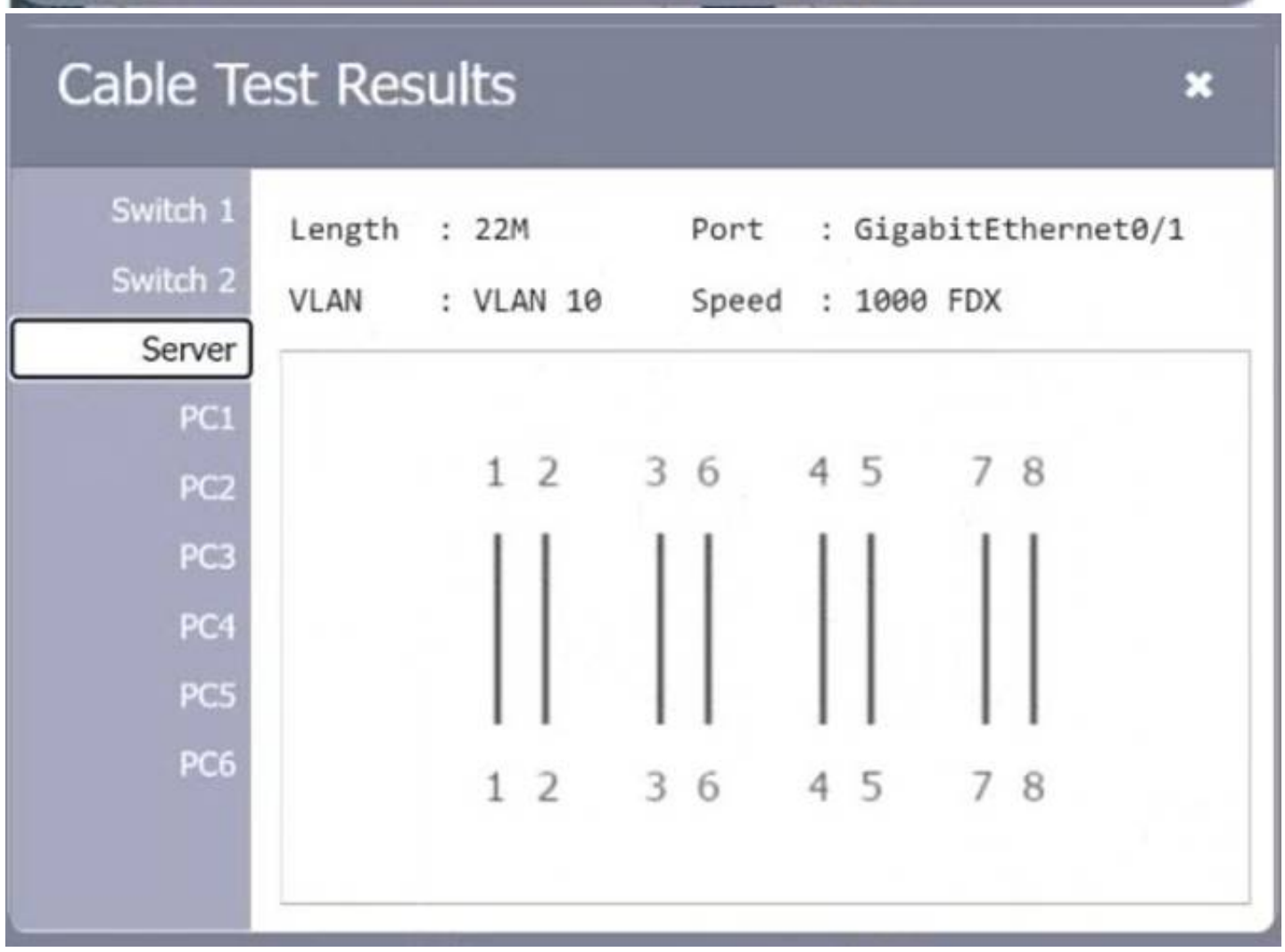
Answer: A

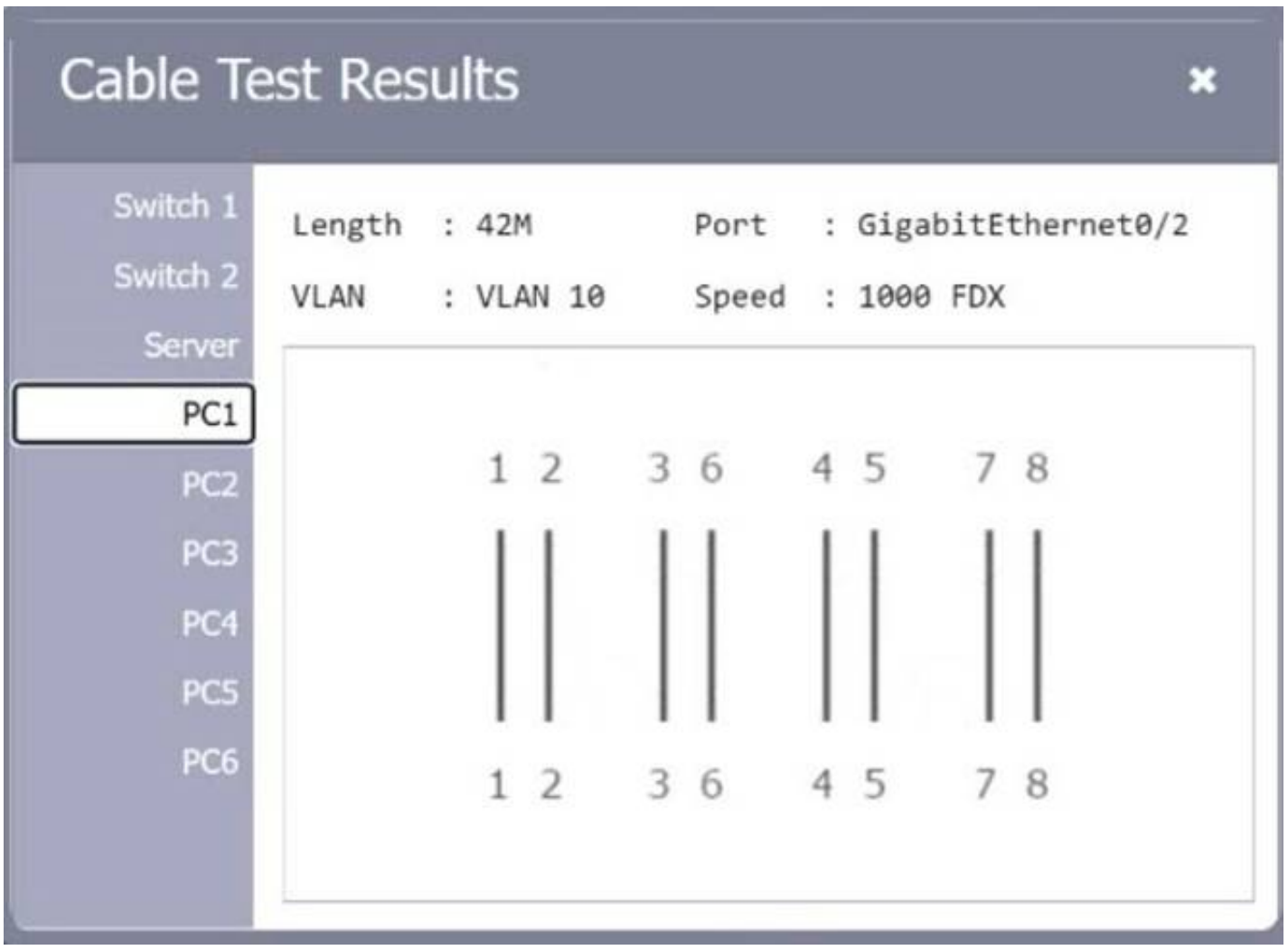
Explanation:
2.4GHz frequency has better penetration and range than higher frequencies in forested environments, where there are many obstacles and interference sources.
References:
? Wireless in The Woods: Experimental Evaluation of IEEE 802.11a/b/g in Forested Environments1
? High-Speed Wireless Access in Forested Rural Areas Using Analog Radio Over Fiber2

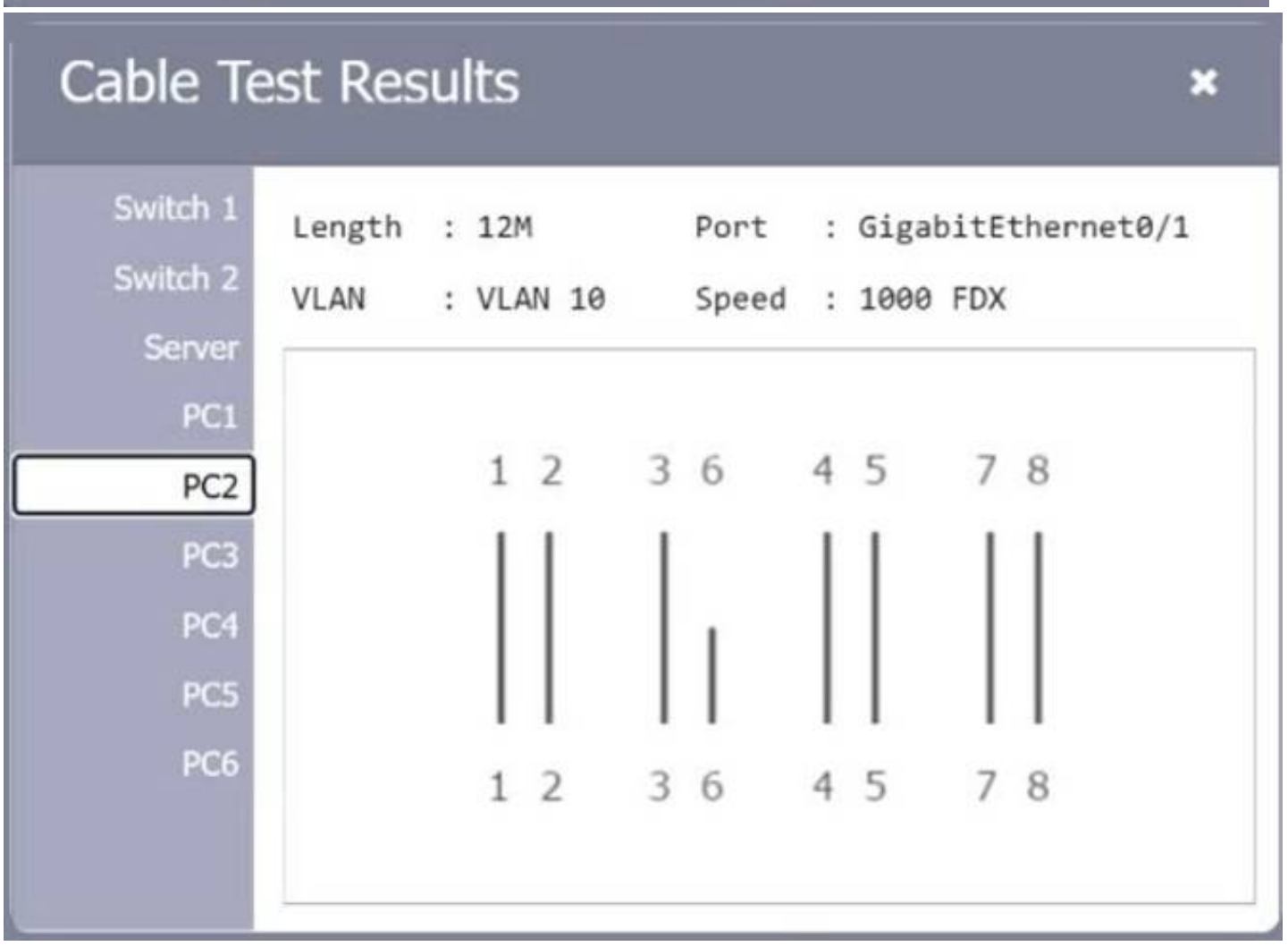
NEW QUESTION 353
SIMULATION - (Topic 3)
A network technician needs to resolve some issues with a customer's SOHO network. The customer reports that some of the PCs are not connecting to the network, while others appear to be working as intended.
INSTRUCTIONS
Troubleshoot all the network components.
Review the cable test results first, then diagnose by clicking on the appropriate PC, server, and Layer 2 switch.
Identify any components with a problem and recommend a solution to correct each problem.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

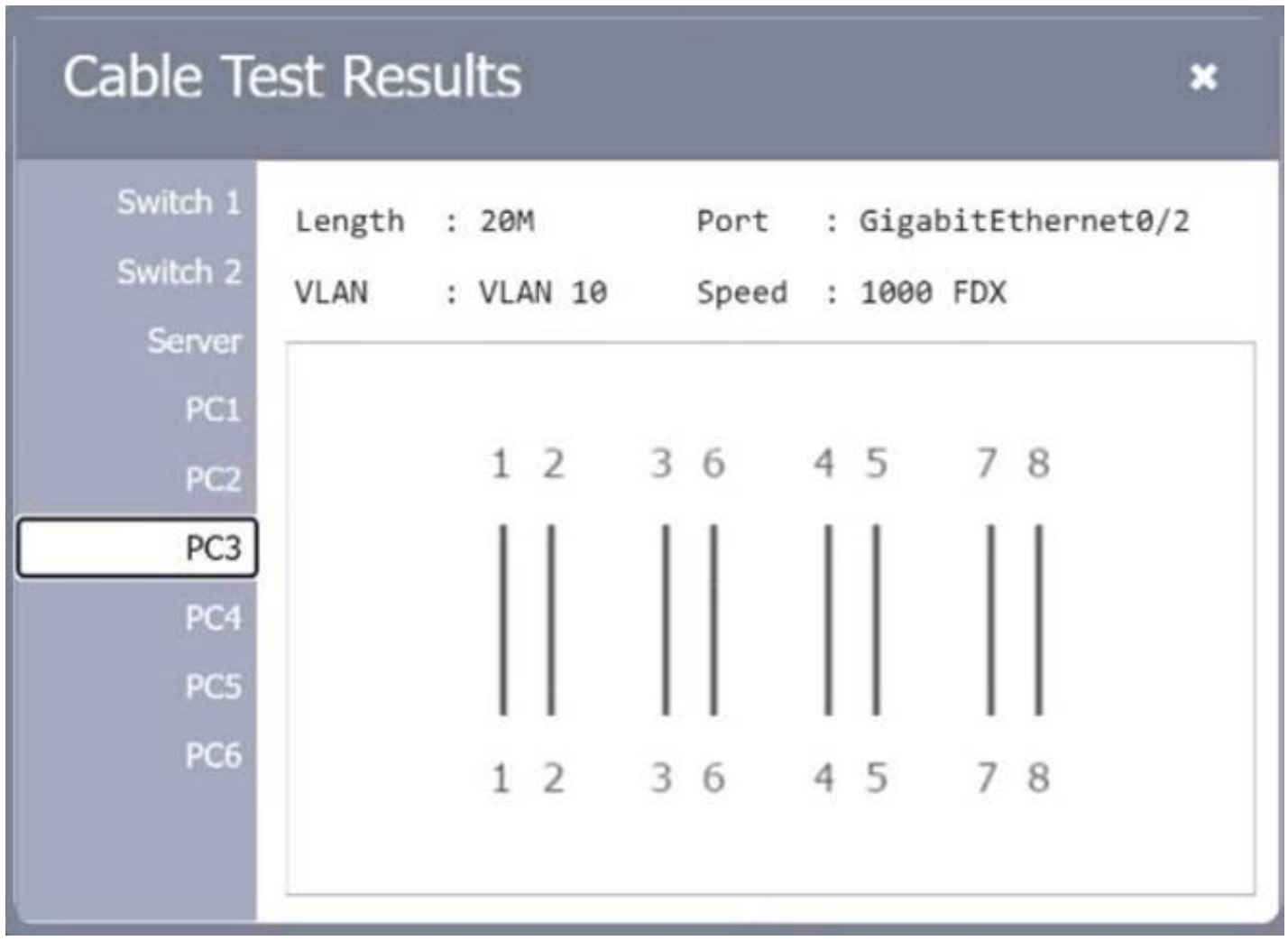


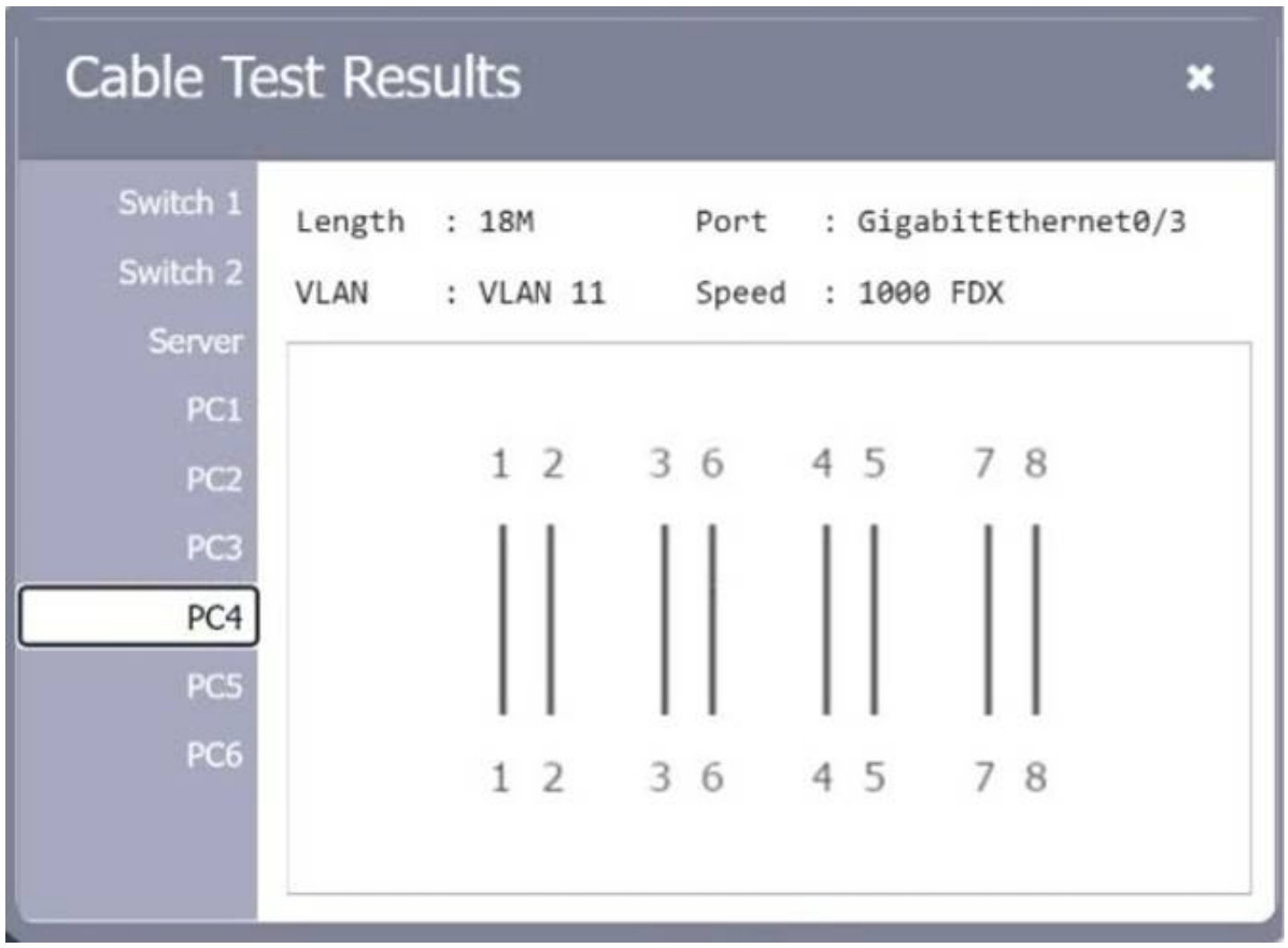

Cable Test Results
Switch 1
Switch 2
Server
PC1
PC2
PC3
PC4
PC5
PC6
Length : 16M
Port : GigabitEthernet0/5
VLAN : VLAN 10
Speed : 1000 FDX
Connected to Switch 1
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8

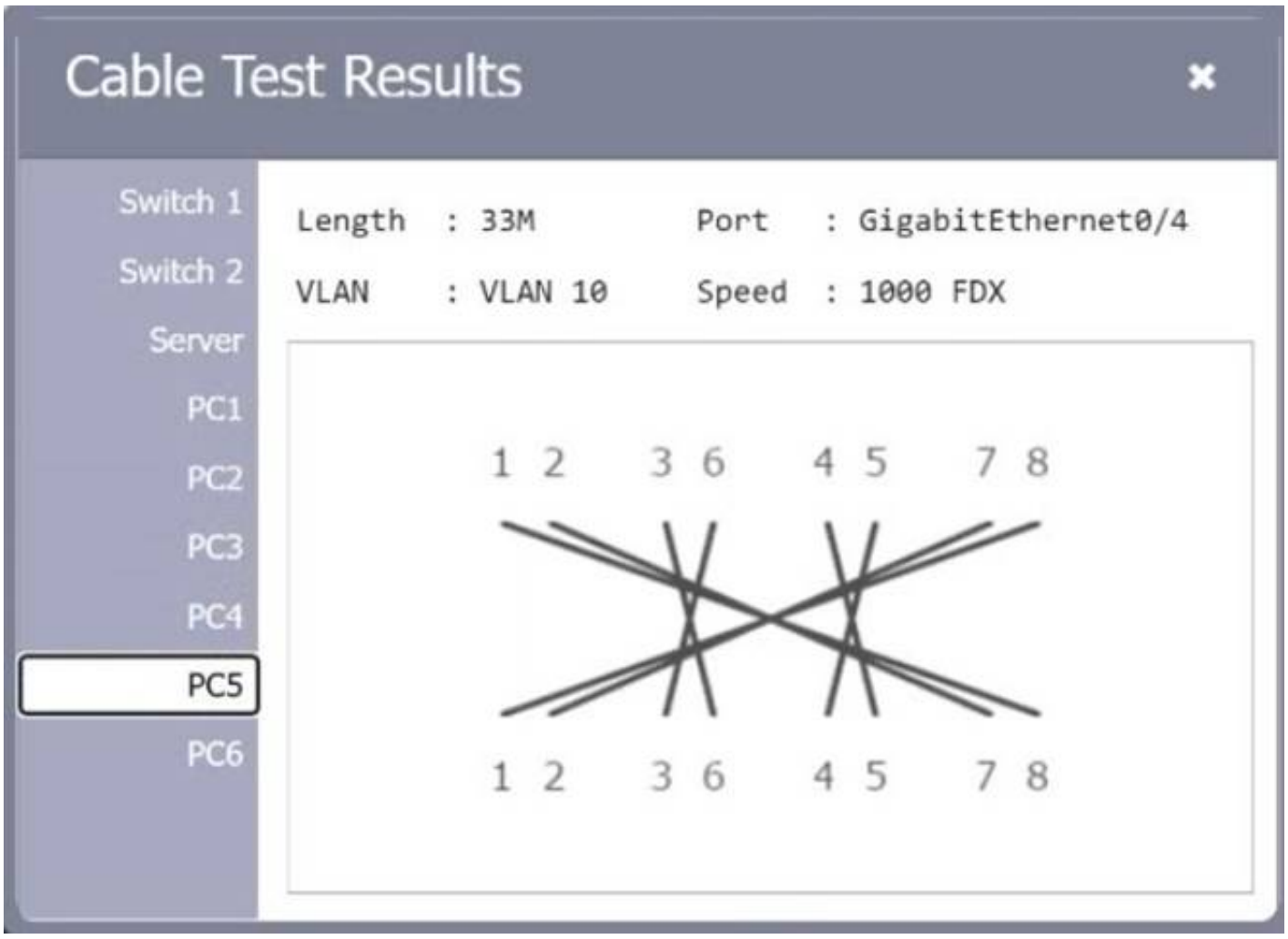

Cable Test Results
Switch 1
Switch 2
Server
PC1
PC2
PC3
PC4
PC5
PC6
Length : 22M
Port : GigabitEthernet0/1
VLAN : VLAN 10
Speed : 1000 FDX
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8

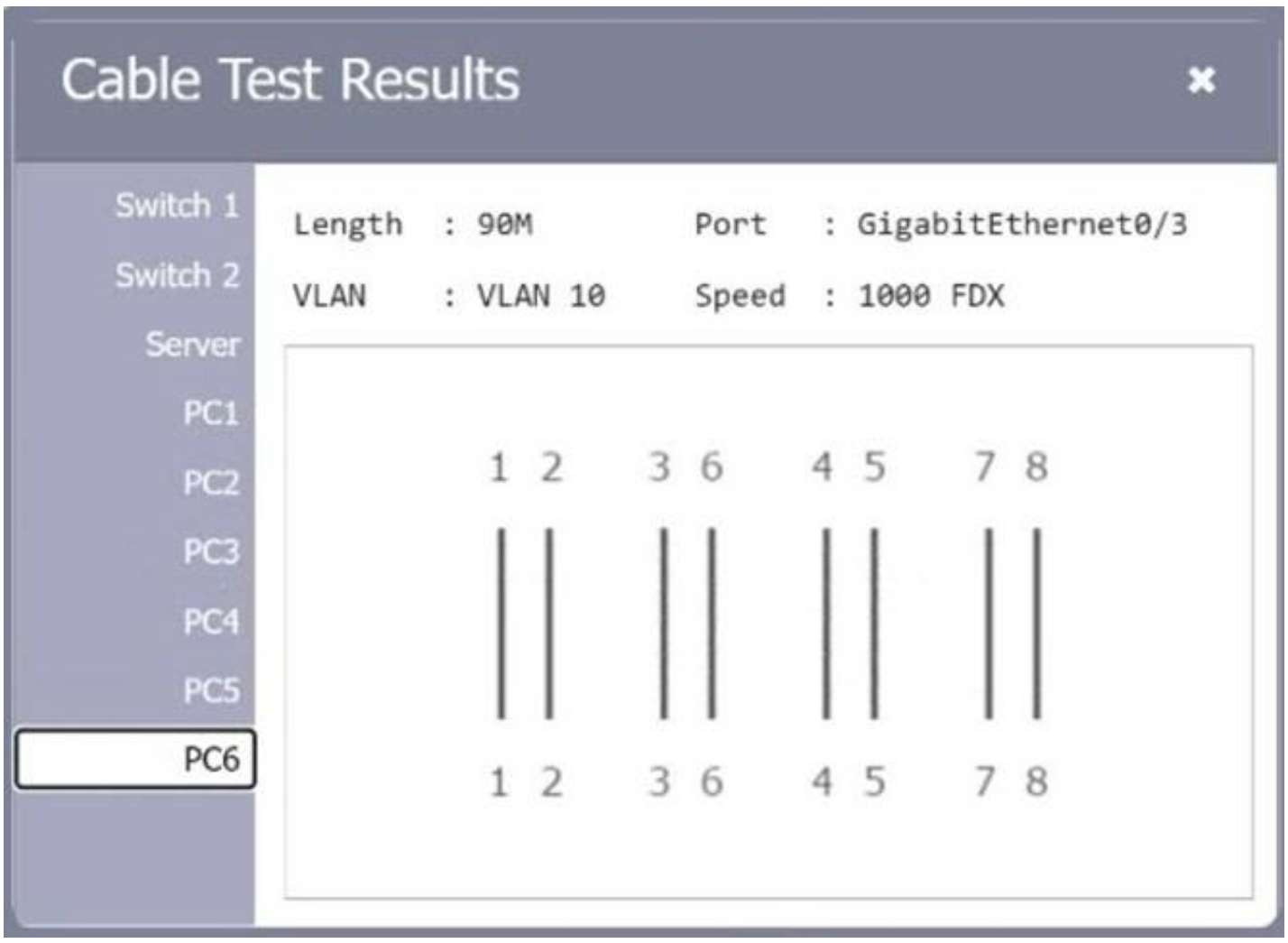

Cable Test Results
Switch 1
Switch 2
Server
PC1
PC2
PC3
PC4
PC5
PC6
Length : 42M
Port : GigabitEthernet0/2
VLAN : VLAN 10
Speed : 1000 FDX
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8

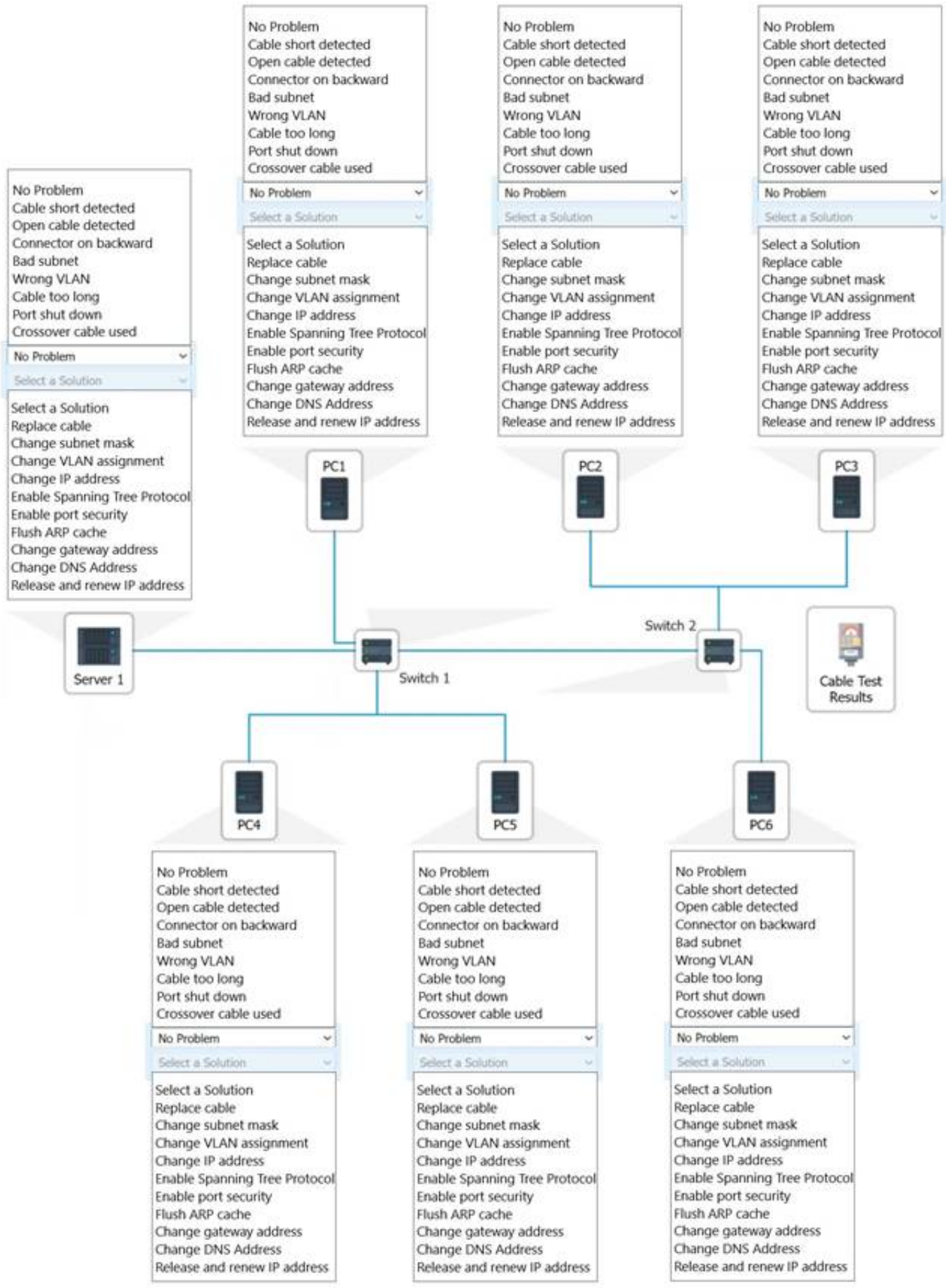

Cable Test Results
Switch 1
Switch 2
Server
PC1
PC2
PC3
PC4
PC5
PC6
Length : 12M
Port : GigabitEthernet0/1
VLAN : VLAN 10
Speed : 1000 FDX
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8


Cable Test Results
Switch 1
Switch 2
Server
PC1
PC2
PC3
PC4
PC5
PC6
Length : 20M
Port : GigabitEthernet0/2
VLAN : VLAN 10
Speed : 1000 FDX
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8


Cable Test Results
Switch 1
Switch 2
Server
PC1
PC2
PC3
PC4
PC5
PC6
Length : 18M
Port : GigabitEthernet0/3
VLAN : VLAN 11
Speed : 1000 FDX
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8


Cable Test Results
Switch 1
Switch 2
Server
PC1
PC2
PC3
PC4
PC5
PC6
Length : 33M
Port : GigabitEthernet0/4
VLAN : VLAN 10
Speed : 1000 FDX
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8


Cable Test Results
Switch 1
Switch 2
Server
PC1
PC2
PC3
PC4
PC5
PC6
Length : 90M
Port : GigabitEthernet0/3
VLAN : VLAN 10
Speed : 1000 FDX
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8

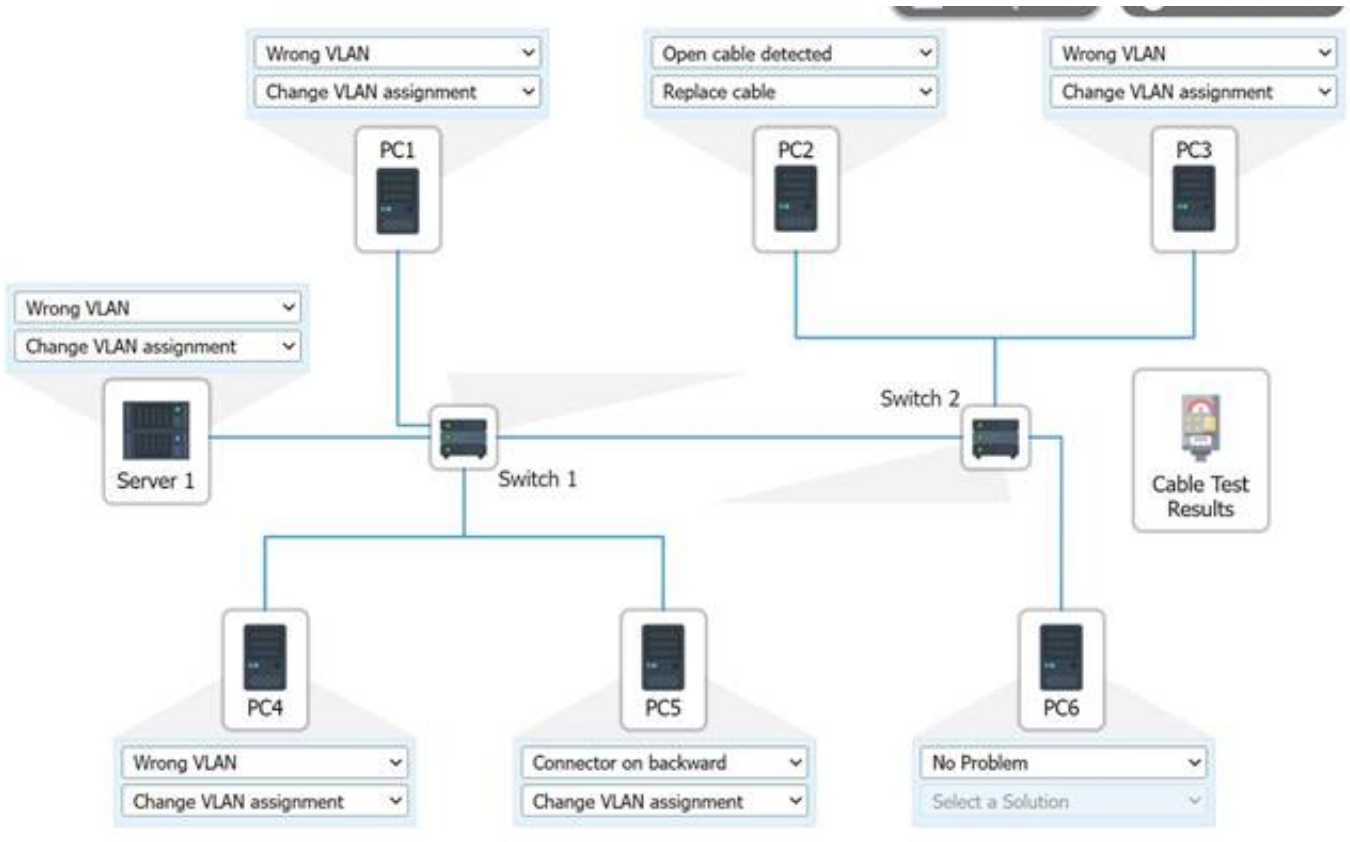


A. Mastered

B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 358
- (Topic 3)
Users ate moving back into an office that had been vacant for awhile. Ten workstations are hooked up in the office, but one workstation cannot obtain a link with (he switch. A network engineer checks the documentation and cable labeling, and everything is hooked up as expected. The engineer moves the connection lo a different switchport. but a link still cannot be obtained. When the engineer puts a tone generator on (he infrastructure cable, no tone is heard at the far end. Which of the following issues is the engineer MOST likely trying to find?

A. A bad switchport
B. A break in the cable
C. A cable short
D. Cable interference

Answer: B

Explanation:
A break in the cable means that there is no electrical continuity between the two ends of the cable, which prevents the signal from reaching the switch. A tone generator is a device that sends an audible signal through the cable, and if no tone is heard at the far end, it indicates a break in the cable.

NEW QUESTION 359
- (Topic 3)
After HVAC failures caused network outages, the support team decides to monitor the temperatures of all the devices. The network administrator cannot find a command that will display this information. Which of the following will retrieve the necessary information?

A. SNMP OID values
B. NetFlow data export
C. Network baseline configurations
D. Security information and event management

Answer: A

Explanation:
The network administrator can use the Simple Network Management Protocol (SNMP) to monitor the temperatures of all the devices. SNMP is a widely-used protocol for managing and monitoring network devices, such as routers, switches, servers, and other networking equipment. SNMP allows network administrators to gather information about the performance and status of devices on the network, including temperature readings.
To retrieve the temperature information, the administrator will have to configure SNMP on the devices and configure SNMP manager software on their computer. Once the SNMP manager software is configured, it will be able to send SNMP requests to the devices and retrieve information such as temperature, voltage, fan speeds, etc. Many network devices have built-in SNMP support, and the administrator may also need to install SNMP agent software on the devices to enable SNMP monitoring.
The administrator can also use some specific command or tool like IPMI (Intelligent Platform Management Interface) or DCIM (Data Center Infrastructure Management) tools for monitoring the temperatures of all the devices.

NEW QUESTION 362
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your N10-009 Exam with Our Prep Materials Via below:

https://www.certleader.com/N10-009-dumps.html