CompTIA

Exam Questions N10-009

CompTIA Network+ Exam

NEW QUESTION 1
- (Topic 3)
A network technician is attempting to harden a commercial switch that was recently purchased. Which of the following hardening techniques best mitigates the use of publicly available information?

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

Answer: A

Explanation:
Changing the default password is a hardening technique that best mitigates the use of publicly available information, such as vendor documentation, online forums, or hacking tools, that may reveal the default credentials of a commercial switch. By changing the default password to a strong and unique one, the network technician can prevent unauthorized access to the switch configuration and management. References:
? Network Hardening - N10-008 CompTIA Network+ : 4.3 - YouTube1
? CompTIA Network+ Certification Exam Objectives, page 151

NEW QUESTION 2
- (Topic 3)
Which of the following can have multiple VLAN interfaces?

A. Hub
B. Layer 3 switch
C. Bridge
D. Load balancer

Answer: B

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

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

Answer: C

Explanation:
An SVI, or switched virtual interface, is a logical interface that is created on a Layer 3- capable device, such as a multilayer switch or a router. An SVI is associated with a VLAN and can be used to route traffic between different VLANs on the same device or across multiple devices. An SVI can also provide management access, security features, and quality of service (QoS) for the VLAN. An SVI is different from a physical interface, which is a port that connects to a physical device or network. A physical interface can be used for trunking, which is a method of carrying multiple VLANs over a single link, or for connecting to a single VLAN. An SVI is also different from a subinterface, which is a logical division of a physical interface that can be assigned to different VLANs.
References:
? VLANs and Trunking – N10-008 CompTIA Network+ : 2.11
? Switched Virtual Interfaces – N10-008 CompTIA Network+ : 2.22

NEW QUESTION 4
- (Topic 3)
A user is required to log in to a main web application, which then grants the user access to all other programs needed to complete job-related tasks. Which of the following authentication methods does this setup describe?

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

Answer: A

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

NEW QUESTION 5
- (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 6
- (Topic 3)
A customer is adding fiber connectivity between adjacent buildings. A technician terminates the multimode cable to the fiber patch panel. After the technician connects the fiber patch cable, the indicator light
does not come on. Which of the following should a technician try first to troubleshoot this issue?

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

Answer: A

Explanation:
One of the most common causes of fiber connectivity issues is the reversal of the fibers. This means that the transmit (TX) and receive (RX) ports on one end of the fiber link are not matched with the corresponding ports on the other end. For example, if the TX port on one device is connected to the TX port on another device, and the same for the RX ports, then the devices will not be able to communicate with each other. This can result in no indicator light, no link, or no data transmission12.
To troubleshoot this issue, the technician should first try to reverse the fibers. This can be done by swapping the connectors at one end of the fiber patch cable, or by using a crossover adapter or cable that reverses the polarity of the fibers. The technician should then check if the indicator light comes on and if the devices can communicate properly12. The other options are not the first steps to troubleshoot this issue. Reterminating the fibers is a time-consuming and costly process that should be done only if there is evidence of physical damage or poor quality of the termination. Verifying the fiber size is not relevant in this scenario, as multimode fiber is compatible with multimode fiber, and any mismatch in core diameter or bandwidth would result in high attenuation, not complete loss of signal. Examining the cable runs for visual faults is a useful technique, but it requires a special tool called a visual fault locator (VFL) that emits a visible red light through the fiber and shows any breaks or bends along the cable. However, a VFL cannot detect polarity issues or connector problems, so it is not sufficient to troubleshoot this issue

NEW QUESTION 7
- (Topic 3)
A technician discovered that some information on the local database server was changed during a tile transfer to a remote server. Which of the following should concern the technician the MOST?

A. Confidentiality
B. Integrity
C. DDoS
D. On-path attack

Answer: B

Explanation:
The technician should be most concerned about data integrity and security. If information on the local database server was changed during a file transfer to a remote server, it could indicate that unauthorized access or modifications were made to the data. It could also indicate a failure in the file transfer process, which could result in data loss or corruption. The technician should investigate the cause of the changes and take steps to prevent it from happening again in the future. Additionally, they should verify the integrity of the data and restore it from a backup if necessary to ensure that the correct and complete data is available. The technician should also take appropriate actions such as notifying the system administrator and management of the incident, and following the incident management process to minimize the damage caused by the incident.

NEW QUESTION 8
- (Topic 3)
Which of the following is the best action to take before sending a network router to be recycled as electronic waste?

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

Answer: C

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

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

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

Answer: B

Explanation:
The most likely reason why only eight cameras turn on is that the PoE switch does not
have enough power budget to supply all 12 cameras. The engineer should check the voltage and wattage ratings of the PoE switch and the cameras, and make sure they are compatible and sufficient. The Ethernet cable type, transceiver compatibility, and DHCP addressing are less likely to cause this problem, as they would affect the data transmission rather than the power delivery.
References:
? CompTIA Network+ N10-008 Certification Study Guide, page 181
? CompTIA Network+ N10-008 Cert Guide, Deluxe Edition, page 352
? PoE Troubleshooting: The Common PoE Errors and Solutions3

NEW QUESTION 10
- (Topic 3)
While troubleshooting a network, a VoIP systems engineer discovers a significant inconsistency in the amount of time required for data to reach its destination and return. Which of the following terms best describes this issue?

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

Answer: C

Explanation:
Jitter is the variation in the delay of data packets over a network. It is caused by factors such as network congestion, routing changes, packet loss, or improper queuing. Jitter affects the quality of VoIP calls because it can cause gaps, distortion, or out-of-order delivery of voice data. Jitter can be measured by the difference between the expected and actual arrival times of packets2. To reduce jitter, VoIP systems use buffers to store and reorder packets before playing them back. However, too much buffering can also increase latency, which is the total time it takes for data to travel from one point to another3.
References2 - VoIP Troubleshooting: 5 Fixes for Common Connection Issues - Nextiva3 - Troubleshooting VoIP — Is it You or the Network? - PingPlotter

NEW QUESTION 12
- (Topic 3)
Which of the following is used to elect an STP root?

A. A bridge ID
B. A bridge protocol data unit
C. Interface port priority
D. A switch's root port

Answer: B

Explanation:
"Using special STP frames known as bridge protocol data units (BPDUs), switches communicate with other switches to prevent loops from happening in the first place. Configuration BPDUs establish the topology, where one switch is elected root bridge and acts as the center of the STP universe. Each switch then uses the root bridge as a reference point to maintain a loop-free topology."

NEW QUESTION 15
- (Topic 3)
A bank installed a new smart TV to stream online video services, but the smart TV was not able to connect to the branch Wi-Fi. The next day. a technician was able to connect the TV to the Wi-Fi, but a bank laptop lost network access at the same time. Which of the following is the MOST likely cause?

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

Answer: A

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

NEW QUESTION 20
- (Topic 3)
Users in a branch can access an ln-house database server, but II is taking too long to fetch records. The analyst does not know whether the Issue is being caused by network latency. Which of the following will the analyst MOST likely use to retrieve the metrics that are needed to resolve this issue?

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

Answer: A

NEW QUESTION 24
- (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 27
- (Topic 3)
Which of the following fiber connector types is the most likely to be used on a network interface card?

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

Answer: A

Explanation:
LC (local connector) is the most likely fiber connector type to be used on a network interface card, because it is a small form factor connector that can fit more interfaces on a single card. LC connectors use square connectors that have a locking mechanism on the top, similar to an RJ45 copper connector. LC connectors are also compatible with SFP (small form-factor pluggable) modules that are often used to link a gigabit Ethernet port with a fiber network12.
References:
? Optical Fiber Connectors – CompTIA Network+ N10-007 – 2.11
? CompTIA Network+ Certification Exam Objectives2

NEW QUESTION 28
- (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 32

- (Topic 3)
Users are reporting performance issues when attempting to access the main fileshare server. Which of the following steps should a network administrator perform next based on the network troubleshooting methodology?

A. Implement a fix to resolve the connectivity issues.
B. Determine if anything has changed.
C. Establish a theory of probable cause.
D. Document all findings, actions, and lessons learned.

Answer: B

Explanation:
According to the network troubleshooting methodology, the first step is to identify the problem and gather information about the current state of the network using the network troubleshooting tools that are available1. The next step is to determine if anything has changed in the network configuration, environment, or usage that could have caused or contributed to the performance issues1. This step helps to narrow down the possible causes and eliminate irrelevant factors. For example, the network administrator could check if there were any recent updates, patches, or modifications to the fileshare server or the network devices that connect to it. They could also check if there was an increase in network traffic or demand for the fileshare server resources2.
The other options are not correct because they are not the next steps in the network troubleshooting methodology. Implementing a fix to resolve the connectivity issues (A) is premature without determining the root cause of the problem. Establishing a theory of probable cause © is a later step that requires testing and verification. Documenting all findings, actions, and lessons learned (D) is the final step that should be done after resolving the problem and restoring normal network operations1.

NEW QUESTION 37
- (Topic 3)
Users are reporting poor wireless performance in some areas of an industrial plant The wireless controller is measuring a tow EIRP value compared to me recommendations noted on me most recent site survey. Which of the following should be verified or replaced for the EIRP value to meet the site survey's specifications? (Select TWO).

A. AP transmit power
B. Channel utilization
C. Signal loss
D. Update ARP tables
E. Antenna gain
F. AP association time

Answer: AE

Explanation:
? AP transmit power: You should check if your APs have sufficient power output and adjust them if needed. You should also make sure they are not exceeding regulatory limits for your region.
? Antenna gain: You should check if your antennas have adequate gain for your coverage area and replace them if needed. You should also make sure they are aligned properly and not obstructed by any objects.
In the scenario described, the wireless controller is measuring a low EIRP value compared to the recommendations noted in the most recent site survey. EIRP is the combination of the power transmitted by the access point and the antenna gain. Therefore, to increase the EIRP value to meet the site survey's specifications, the administrator should verify or replace the AP transmit power (option A) and the antenna gain (option E). This can be achieved by adjusting the transmit power settings on the AP or by replacing the AP's antenna with one that has a higher gain

NEW QUESTION 41
- (Topic 3)
A network administrator is adding a new switch to the network. Which of the following network hardening techniques would be BEST to use once the switch is in production?

A. Disable unneeded ports
B. Disable SSH service
C. Disable MAC filtering
D. Disable port security

Answer: A

NEW QUESTION 43
- (Topic 3)
A company has multiple offices around the world. The computer rooms in some office locations are too warm Dedicated sensors are in each room, but the process of checking each sensor takes a long time. Which of the following options can the company put In place to automate temperature readings with internal resources?

A. Implement NetFlow.
B. Hire a programmer to write a script to perform the checks
C. Utilize ping to measure the response.
D. Use SNMP with an existing collector server

Answer: D

Explanation:
SNMP (Simple Network Management Protocol) is a protocol that allows network devices to communicate with a management server. By using SNMP, the company can set up an SNMP agent on each sensor, which will report its temperature readings to an existing collector server. This will enable the company to monitor the temperatures of all their sensors in real-time without the need for manual checks. Additionally, SNMP's scalability means that even if the company adds more rooms or sensors, the existing system can be easily expanded to accommodate them.

NEW QUESTION 44
- (Topic 3)

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

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

Answer: A

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

NEW QUESTION 48
- (Topic 3)
The Chief Executive Officer of a company wants to ensure business operations are not disrupted in the event of a disaster. The solution must have fully redundant equipment, real-time synchronization, and zero data loss. Which Of the following should be prepared?

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

Answer: C

Explanation:
A hot site is a backup site that is fully equipped and ready to take over the operations of the primary site in the event of a disaster. A hot site has real-time synchronization with the primary site and can provide zero data loss. A hot site is the most expensive and reliable option for disaster recovery.
References: Network+ Study Guide Objective 5.3: Explain common scanning, monitoring and patching processes and summarize their expected outputs.

NEW QUESTION 53
- (Topic 3)
A technician installed an 8-port switch in a user's office. The user needs to add a second computer in the office, so the technician connects both PCs to the switch and connects the switch to the wall jack. However, the new PC cannot connect to network resources. The technician then observes the following:
• The new computer does not get an IP address on the client's VLAN.
• Both computers have a link light on their NICs.
• The new PC appears to be operating normally except for the network issue.
• The existing computer operates normally.
Which of the following should the technician do NEXT to address the situation?

A. Contact the network team to resolve the port security issue.
B. Contact the server team to have a record created in DNS for the new PC.
C. Contact the security team to review the logs on the company's SIEM.
D. Contact the application team to check NetFlow data from the connected switch.

Answer: A

NEW QUESTION 58
- (Topic 3)
Due to space constraints in an IDF, a network administrator can only a do a single switch to
accommodate three data networks. The administrator needs a configuration that will allow each device to access its expected network without additional connections. The configuration must also allow each device to access the rest of the network. Which of the following should the administrator do to meet these requirements? (Select TWO).

A. Untag the three VLANs across the uplink
B. Tag an individual VLAN across the uplink
C. Untag an individual VLAN per device port
D. Tag an individual VLAN per device port
E. Tag the three VLANs across the uplink.
F. Tag the three VLANs per device port.

Answer: AC

Explanation:
To achieve this, you should do two things:
? Tag the three VLANs across the uplink port that connects to another switch or router. This will allow data packets from different VLANs to cross over into other networks.
? Untag an individual VLAN per device port that connects to an end device. This will assign each device to its expected network without additional connections.

NEW QUESTION 61
- (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 65
- (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 69
- (Topic 3)
An IT intern moved the location of a WAP from one conference room to another. The WAP was unable to boot following the move. Which of the following should be used to fix the issue?

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

Answer: D

Explanation:
A PoE injector is a device that provides power over Ethernet (PoE) to a WAP or other network device that does not have a built-in power supply. A PoE injector connects to a power outlet and an Ethernet cable, and sends both power and data to the WAP. If the WAP was moved to a location where there is no power outlet or PoE switch, it would need
a PoE injector to boot up. References:
? Part 3 of the current page talks about PoE and PoE injectors as a way to power WAPs.
? [This article] explains how PoE injectors work and how to use them.

NEW QUESTION 73
- (Topic 3)
A network administrator is preparing new switches that will be deployed to support a network extension project. The lead network engineer has already provided documentation to ensure the switches are set up properly Which of the following did the engineer most likely provide?

A. Physical network diagram
B. Site survey reports
C. Baseline configurations
D. Logical network diagram

Answer: C

Explanation:
Baseline configurations are the standard settings and parameters that are applied to network devices, such as switches, routers, firewalls, etc., to ensure consistent performance, security, and functionality across the network. Baseline configurations can include aspects such as IP addresses, VLANs, passwords, protocols, access lists, firmware versions, etc. Baseline configurations are usually documented and updated regularly to reflect any changes or modifications made to the network devices.
The lead network engineer most likely provided baseline configurations to the network administrator to ensure that the new switches are set up properly and in accordance with the network design and policies. Baseline configurations can help to simplify the deployment process, reduce errors and inconsistencies, and facilitate troubleshooting and maintenance.
The other options are not correct because they are not the most likely documentation that the lead network engineer provided to the network administrator. They are:
? Physical network diagram. A physical network diagram is a graphical representation of the physical layout and connections of the network devices and components, such as cables, ports, switches, routers, servers, etc. A physical network diagram can help to visualize the network topology, identify the locations and distances of the devices, and plan for cabling and power requirements. However, a physical network diagram does not provide the specific settings and parameters that need to be configured on the network devices, such as the switches.
? Site survey reports. A site survey report is a document that summarizes the findings and recommendations of a site survey, which is a process of assessing the suitability and readiness of a location for installing and operating network devices and components. A site survey report can include aspects such as environmental conditions, power and cooling availability, security and safety measures, interference and noise sources, signal coverage and quality, etc. A site survey report can help to identify and resolve any potential issues or challenges that may affect the network performance and reliability. However, a site survey report does not provide the specific settings and parameters that need to be configured on the network devices, such as the switches.
? Logical network diagram. A logical network diagram is a graphical representation of the logical structure and functionality of the network devices and

components, such as subnets, IP addresses, VLANs, protocols, routing, firewall rules, etc. A logical network diagram can help to understand the network design, architecture, and policies, as well as the data flow and communication paths between the devices. However, a logical network diagram does not provide the specific settings and parameters that need to be configured on the network devices, such as the switches.
References1: Network+ (Plus) Certification | CompTIA IT Certifications2: What is a Baseline Configuration? - Definition from Techopedia3: What is a Physical Network Diagram? - Definition from Techopedia4: What is a Site Survey? - Definition from Techopedia5: [What is a Logical Network Diagram? - Definition from Techopedia]

NEW QUESTION 77
- (Topic 3)
A technician received a report that some users in a large, 30-floor building are having intermittent connectivity issues. Users on each floor have stable connectivity, but do not have connectivity to other floors. Which of the following devices is MOST likely causing the issue?

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

Answer: D

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

NEW QUESTION 78
- (Topic 3)
A wireless technician is working to upgrade the wireless infrastructure for a company. The company currently uses the 802.11g wireless standard on all access points. The company requires backward compatibility and is requesting the least expensive solution. Which of the following should the technician recommend to the company?

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

Answer: D

Explanation:
* 802.11n is a wireless standard that supports data rates up to 600 Mbps and operates in both 2.4 GHz and 5 GHz frequency bands. 802.11n is backward compatible with 802.11g, which operates only in 2.4 GHz band. 802.11n is the least expensive solution that can upgrade the wireless infrastructure for the company, as it does not require replacing all the access points or wireless devices

NEW QUESTION 81
- (Topic 3)
While setting up a new workstation, a technician discovers that the network connection is only 100 full duplex (FD), although it is connected to a gigabit switch. While reviewing the interface information in the switch CLI, the technician notes the port is operating at IOOFD but Shows many RX and TX errors. The technician moves the computer to another switchport and experiences the same issues.
Which of the following is MOST likely the cause of the low data rate and port errors?

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

Answer: B

NEW QUESTION 85
- (Topic 3)
A network technician has determined the cause of a network disruption. Which of the following is the NEXT step for the technician to perform?

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

Answer: C

NEW QUESTION 88
- (Topic 3)
Which of the following is the most secure connection used to inspect and provide controlled internet access when remote employees are connected to the corporate network?

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

Answer: B

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

NEW QUESTION 93
- (Topic 3)
A customer needs to distribute Ethernet to multiple computers in an office. The customer would like to use non-proprietary standards. Which of the following blocks does the technician need to install?

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

Answer: A

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

NEW QUESTION 96
- (Topic 3)
A WAN technician reviews activity and identifies newly installed hardware that is causing outages over an eight-hour period. Which of the following should be considered FIRST?

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

Answer: D

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

NEW QUESTION 100
- (Topic 3)
A company's web server is hosted at a local ISP. This is an example of:

A. allocation.
B. an on-premises data center.
C. a branch office.
D. a cloud provider.

Answer: D

NEW QUESTION 101
- (Topic 3)
Users are reporting intermittent Wi-Fi connectivity in specific parts of a building. Which of the following should the network administrator check FIRST when troubleshooting this issue? (Select TWO).

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

Answer: AC

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

NEW QUESTION 105

- (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 109
- (Topic 3)
During a risk assessment which of the following should be considered when planning to mitigate high CPU utilization of a firewall?

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

Answer: D

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

NEW QUESTION 114
- (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 119
- (Topic 3)
Which of the following network cables involves bouncing light off of protective cladding?

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

Answer: D

Explanation:
Multimode fiber optic cables use multiple paths of light that bounce off the cladding, which is a layer of glass or plastic that surrounds the core of the cable.
https://www.explainthatstuff.com/fiberoptics.html

NEW QUESTION 120
- (Topic 3)
A network technician is attempting to increase throughput by configuring link port aggregation between a Gigabit Ethernet distribution switch and a Fast Ethernet access switch. Which of the following is the BEST choice concerning speed and duplex for all interfaces that are participating in the link aggregation?

A. Half duplex and 1GB speed
B. Full duplex and 1GB speed
C. Half duplex and 10OMB speed
D. Full duplex and 100MB speed

Answer: B

Explanation:
The best choice for configuring link port aggregation between a Gigabit Ethernet distribution switch and a Fast Ethernet access switch is to use full duplex and 1GB speed for all interfaces that are participating in the link aggregation. This will allow for maximum throughput, as the full duplex connection will enable simultaneous sending and receiving of data, and the 1GB speed will ensure that the data is transferred quickly. According to the CompTIA Network+ Study Guide,

“Full-duplex Ethernet allows the network adapter to transmit and receive data simultaneously, which can result in double the bandwidth of half-duplex Ethernet.” Additionally, the official text states, “Ethernet and Fast Ethernet use different speeds for data transmission, with Ethernet being 1,000 megabits (1 gigabit) per second and Fast Ethernet being 100 megabits per second.”

NEW QUESTION 121
- (Topic 3)
To reduce costs and increase mobility, a Chief Technology Officer (CTO) wants to adopt cloud services for the organization and its affiliates. To reduce the impact for users, the CTO wants key services to run from the on-site data center and enterprise services to run in the cloud. Which of the following deployment models is the best choice for the organization?

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

Answer: B

Explanation:
A hybrid cloud deployment model is a combination of on-premise and cloud solutions, where some resources are hosted in-house and some are hosted by a cloud provider. A hybrid cloud model can offer the benefits of both public and private clouds, such as scalability, cost-efficiency, security, and control12. A hybrid cloud model can also reduce the impact for users, as they can access the key services from the on-site data center and the enterprise services from the cloud

NEW QUESTION 122
- (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 125
- (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 127
- (Topic 3)
During an annual review of policy documents, a company decided to adjust its recovery time frames. The company agreed that critical applications can be down for no more than six hours, and the acceptable amount of data loss is no more than two hours. Which of the following should be documented as the RPO?

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

Answer: A

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

NEW QUESTION 132
- (Topic 3)
A company has a geographically remote office. In order to connect to the internet, the company has decided to use a satellite WAN link. Which of the following is the GREATEST concern for this type of connection?

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

Answer: C

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

NEW QUESTION 137
- (Topic 3)
A network administrator is in the process of installing 35 PoE security cameras. After the administrator installed and tested the new cables, the administrator installed the cameras. However, a small number of the cameras do not work. Which of the following is the most likely reason?

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

Answer: B

Explanation:
The power budget is the total amount of power that a PoE switch or injector can provide to the connected PoE devices. If the power budget is exceeded, some of the PoE devices may not receive enough power to function properly. To troubleshoot this issue, the network administrator should check the power consumption of each PoE device and the power capacity of the PoE switch or injector.
References:
? PoE Troubleshooting: The Common PoE Errors and Solutions1
? Security Camera Won’t Work - Top 10 Solutions to Fix2
? CompTIA Network+ N10-008 Exam Objectives https://www.comptia.org/certifications/network#examdetails

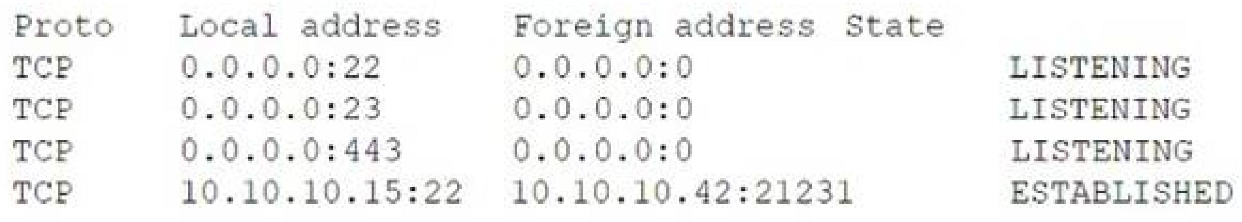
NEW QUESTION 142
- (Topic 3)
A security team would like to use a system in an isolated network to record the actions of potential attackers. Which of the following solutions is the security team implementing?

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

Answer: B

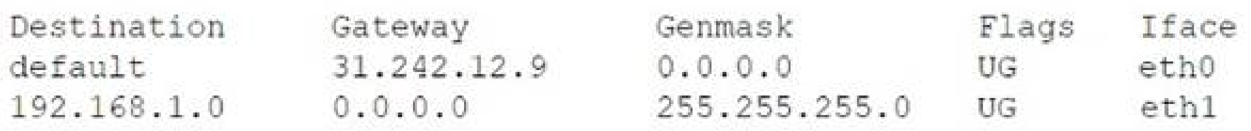
Explanation:
The solution that the security team is implementing to record the actions of potential attackers in an isolated network is a honeypot. A honeypot is a decoy system that simulates a real network or service, but has no actual value or function. A honeypot is designed to attract and trap attackers 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 144
- (Topic 3)
A network technician is troubleshooting an issue that involves connecting to a server via SSH. The server has one network interface that does not support subinterfaces. The technician
runs a command on the server and receives the following output:



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

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



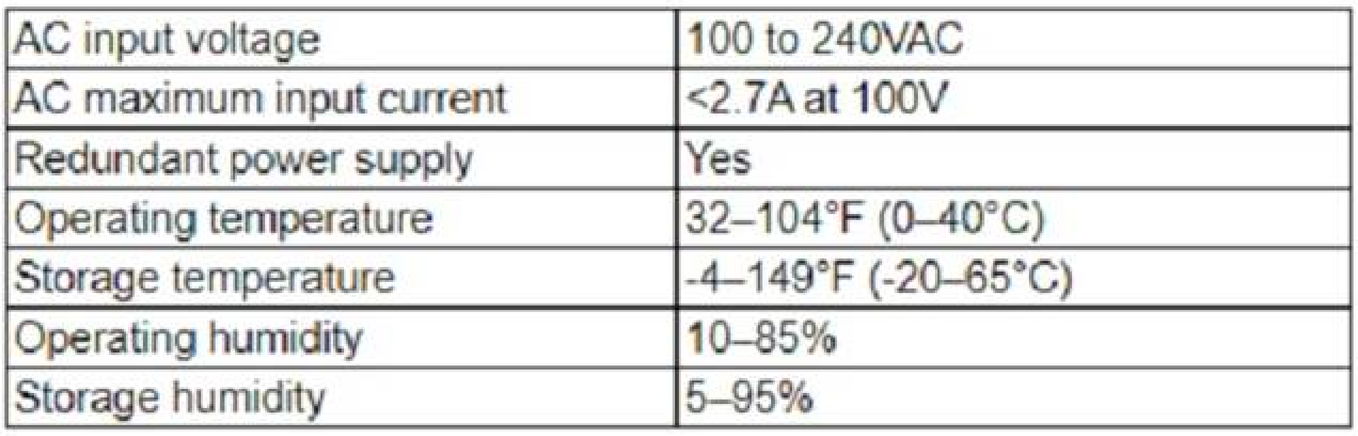
```
Destination     Gateway         Genmask         Flags   Iface
default         31.242.12.9     0.0.0.0         UG      eth0
192.168.1.0     0.0.0.0         255.255.255.0   UG      eth1
```

Which of the following best explains the issue?

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

Answer: C

NEW QUESTION 145
- (Topic 3)
A network engineer is installing hardware in a newly renovated data center. Major concerns that were addressed during the renovation induded air circulation, building power redundancy, and the need for continuous monitoring. The network engineer IS creating alerts based on the following operation specifications:



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

Which of the following should the network engineer configure?

A. Environmental monitoring alerts for humidity greater than 95%
B. SIEM to parse syslog events for a failed power supply
C. SNMP traps to report when the chassis temperature exceeds 950F (3500)
D. UPS monitoring to report when input voltage drops below 220VAC

Answer: C

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

NEW QUESTION 146
- (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 149

- (Topic 3)
An engineer needs to verity the external record tor SMTP traffic. The engineer logged in to the server and entered the nslookup command. Which of the following commands should the engineer send before entering the DNS name?

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

Answer: D

NEW QUESTION 153
- (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 157
- (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 160
- (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 163
- (Topic 3)
Which of the following can be used to aggregate logs from different devices and would make analysis less difficult?

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

Answer: B

Explanation:
SIEM stands for Security Information and Event Management, and it is a system that collects, normalizes, and analyzes log data from different sources in a centralized platform. SIEM can help identify security incidents, monitor network performance, and generate reports and alerts. SIEM can make log analysis less difficult by providing a unified view of the log data, correlating events across different devices, and applying rules and filters to detect anomalies and patterns12.
References: 1: CompTIA Network+ N10-008 Cert Guide - Chapter 14: Network Monitoring32: Log Aggregation: What It Is & How It Works | Datadog4

NEW QUESTION 167
- (Topic 3)
While using a secure conference call connection over a corporate VPN, a user moves from a cellular connection to a hotel wireless network. Although the wireless connection and the VPN show a connected status, no network connectivity is present. Which of the following is the most likely cause of this issue?

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

Answer: C

Explanation:
A captive portal is a web page that is displayed to newly connected users of a Wi-Fi network before they are granted broader access to network resources. Captive portals are commonly used to present a landing or log-in page which may require authentication, payment, acceptance of an end-user license agreement, acceptable use policy, survey completion, or other valid credentials that both the host and user agree to adhere by123
A possible cause of the issue is that the user has not completed the captive portal authentication process, which prevents the VPN from establishing a secure connection over the Wi-Fi network. The user may need to open a web browser and follow the instructions on the captive portal page to gain full access to the internet.

NEW QUESTION 169
- (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 170
- (Topic 3)
A technician uses a badge to enter a security checkpoint on a corporate campus. An unknown individual quickly walks in behind the technician without speaking. Which of the following types of attacks did the technician experience?

A. Tailgating
B. Evil twin
C. On-path
D. Piggybacking

Answer: A

Explanation:
Tailgating is a type of physical security attack where an unauthorized person follows an authorized person into a restricted area without their consent or knowledge. Tailgating can allow an attacker to bypass security measures and gain access to sensitive information or resources. In this scenario, the technician experienced tailgating when the unknown individual walked in behind the technician without speaking. Piggybacking is similar to tailgating, but it involves the consent or cooperation of the authorized person. Evil twin is a type of wireless network attack where an attacker sets up a rogue access point that mimics a legitimate one. On-path is a type of network attack where an attacker intercepts and modifies traffic between two parties.
References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 3.2: Given a scenario, use appropriate network hardening techniques.

NEW QUESTION 174
- (Topic 3)
Which of the following describes when an active exploit is used to gain access to a network?

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

Answer: A

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

NEW QUESTION 176

SIMULATION - (Topic 3)

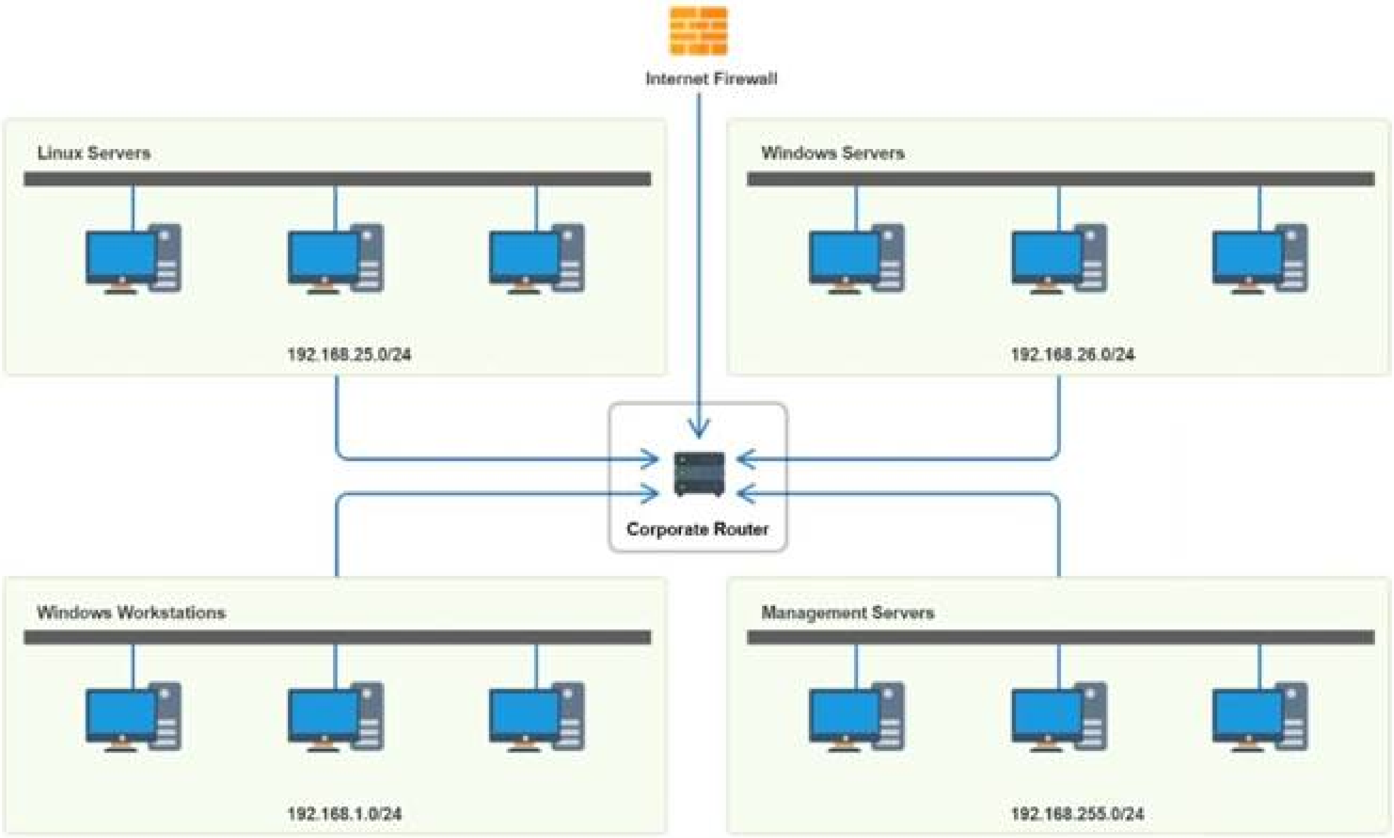
You have been tasked with implementing an ACL on the router that will:

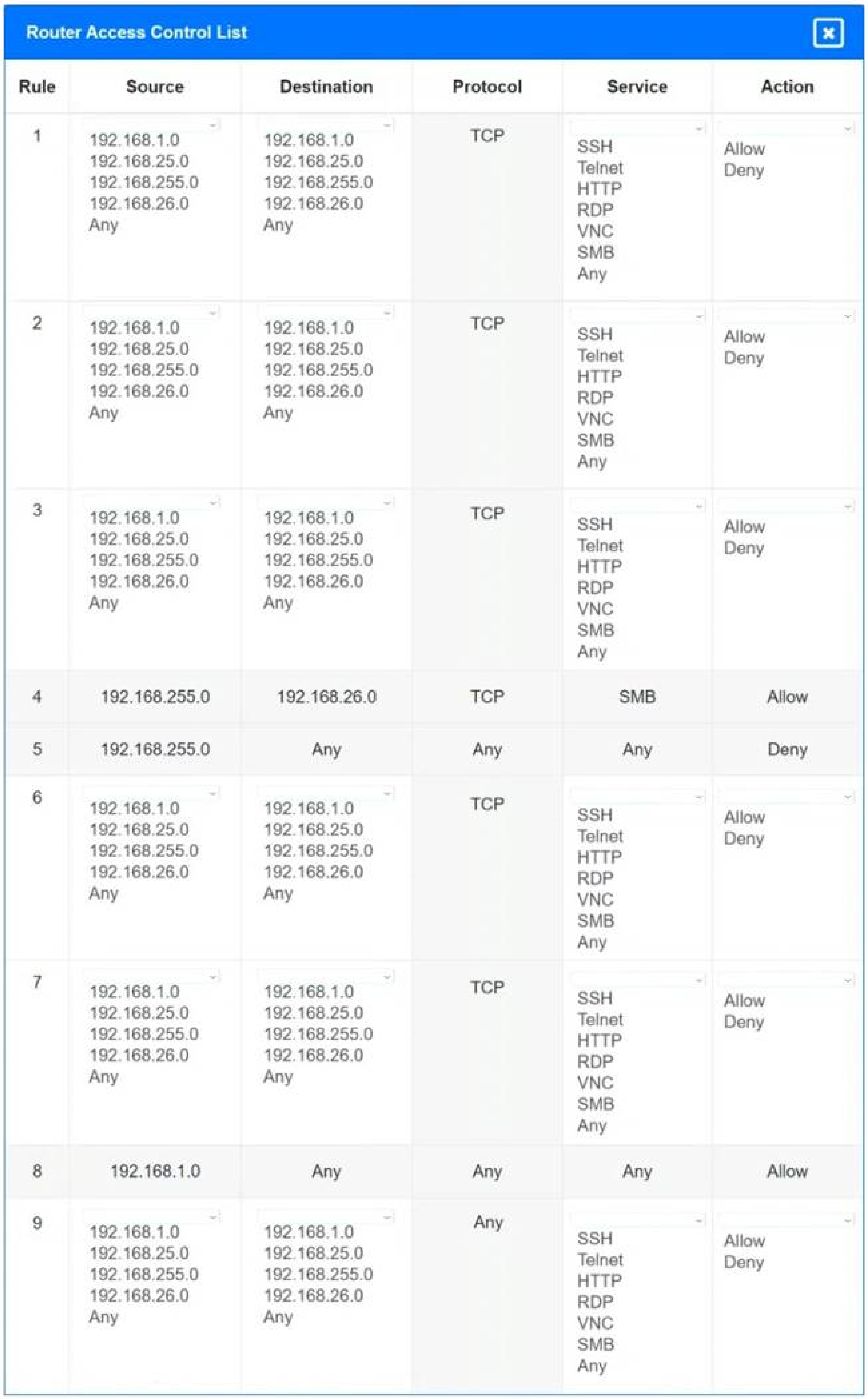
* 1. Permit the most commonly used secure remote access technologies from the management network to all other local network segments
* 2. Ensure the user subnet cannot use the most commonly used remote access technologies in the Linux and Windows Server segments.
* 3. Prohibit any traffic that has not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

INSTRUCTIONS

Use the drop-downs to complete the ACL

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





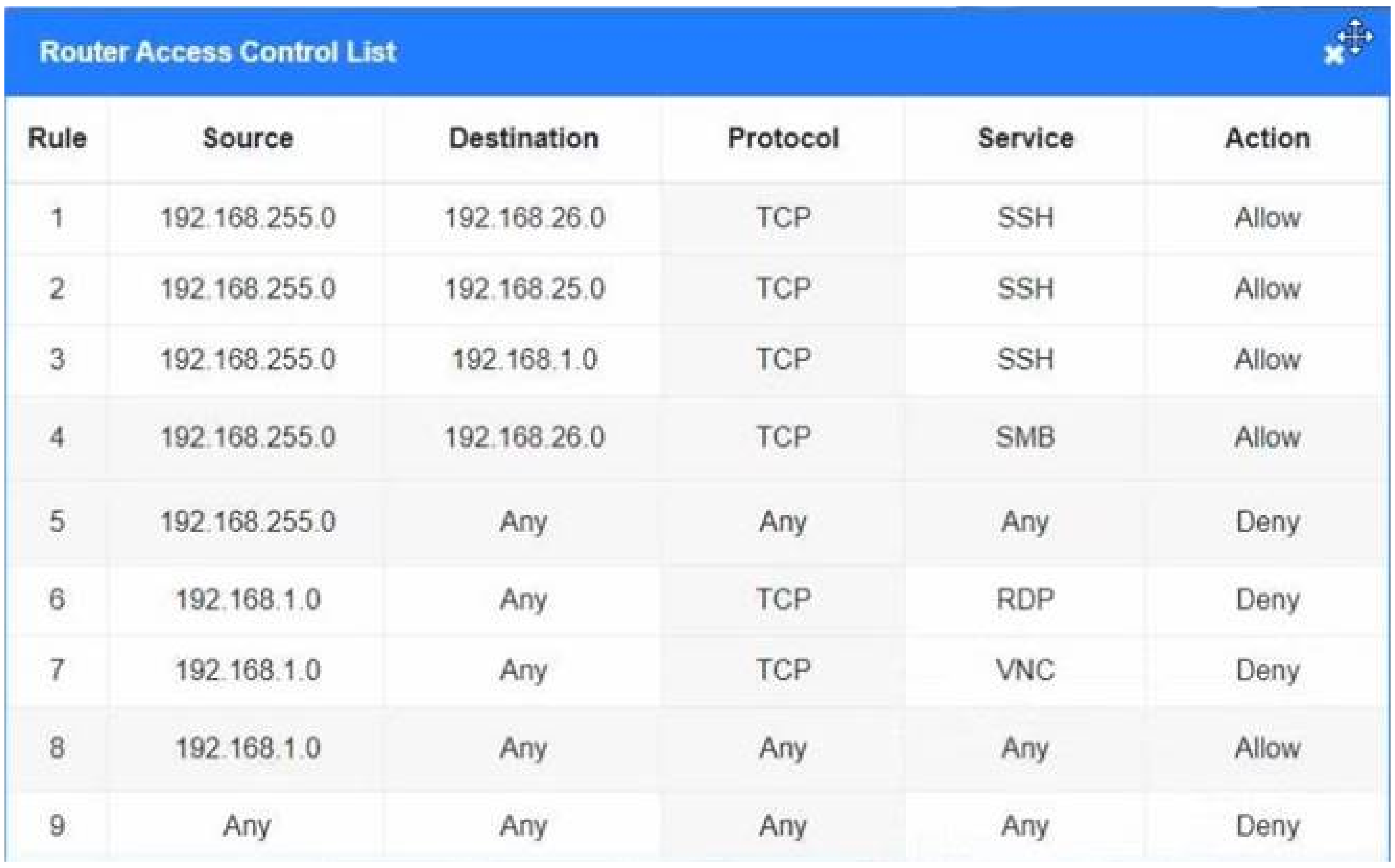
Router Access Control List

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Router Access Control List

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

NEW QUESTION 180

- (Topic 3)
A company with multiple routers would like to implement an HA network gateway with the least amount of downtime possible. This solution should not require changes on the gateway setting of the network clients. Which of the following should a technician configure?

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

Answer: D

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

NEW QUESTION 182

- (Topic 3)
A coffee shop owner hired a network consultant to provide recommendations for installing a new wireless network. The coffee shop customers expect high speeds even when the network is congested. Which of the following standards should the consultant recommend?

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

Answer: B

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

NEW QUESTION 187

- (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 188

- (Topic 3)
A user wants to avoid using a password to access a third-party website. Which of the following does the user need in order to allow this type of access to the third-party website?

A. Multifactor

B. RADIUS
C. SSO
D. Local authentication

Answer: C

NEW QUESTION 191
- (Topic 3)
After a firewall replacement, some alarms and metrics related to network availability stopped updating on a monitoring system relying on SNMP. Which of the following should the network
administrator do first?

A. Modify the device's MIB on the monitoring system.
B. Configure syslog to send events to the monitoring system.
C. Use port mirroring to redirect traffic to the monitoring system.
D. Deploy SMB to transfer data to the monitoring syste

Answer: A

Explanation:

SNMP (Simple Network Management Protocol) is a protocol that allows network devices to communicate with a monitoring system and provide information about their status, performance, and configuration. SNMP relies on MIBs (Management Information Bases), which are collections of objects that define the types of information that can be accessed or modified on a device1.
When a firewall replacement occurs, the new firewall may have a different MIB than the old one, which means that the monitoring system may not be able to recognize or interpret the data sent by the new firewall. This can cause some alarms and metrics related to network availability to stop updating on the monitoring system. To fix this, the network administrator should modify the device’s MIB on the monitoring system, so that it matches the MIB of the new firewall and can correctly process the SNMP data2.
The other options are not relevant to the issue. Configuring syslog to send events to the monitoring system would not affect the SNMP data, as syslog is a different protocol that sends log messages from network devices to a central server. Using port mirroring to redirect traffic to the monitoring system would not help, as port mirroring is a technique that copies traffic from one port to another for analysis or troubleshooting purposes, but does not change the format or content of the traffic. Deploying SMB to transfer data to the monitoring system would not work, as SMB is a protocol that allows file sharing and access between network devices, but does not support SNMP data.
ReferencesGrafana & Prometheus SNMP: advanced network monitoring guideConfiguring Windows Systems for Monitoring with SNMP - ScienceLogic

NEW QUESTION 195
- (Topic 3)
Clients have reported slowness between a branch and a hub location. The senior engineer suspects asymmetrical routing is causing the issue. Which of the following should the engineer run on both the source and the destination network devices to validate this theory?

A. traceroute
B. ping
C. route
D. nslookup

Answer: A

Explanation:

Asymmetric routing occurs when traffic does not traverse the same path in both directions of a conversation. This can cause problems when there are stateful devices, such as firewalls or NAT devices, in the path that expect the traffic to be symmetrical. Asymmetric routing can also result in suboptimal TCP performance, as TCP assumes that the SYN and ACK packets take the same path1.
To validate the theory of asymmetric routing, the engineer should run the traceroute command on both the source and the destination network devices. The traceroute command shows the route that packets take to reach a destination, by displaying the IP addresses and hostnames of the routers along the path, as well as the time taken for each hop. By comparing the output of the traceroute command from both ends, the engineer can determine if the traffic is taking different paths in each direction, and identify where the asymmetry occurs2.
The ping command is not sufficient to validate the theory of asymmetric routing, as it only tests the connectivity and latency between two devices, but does not show the intermediate hops or the path taken by the packets. The route command shows the routing table of a device, but does not show the actual path taken by the packets. The nslookup command resolves a hostname to an IP address, or vice versa, but does not show the route or the connectivity between two devices.
ReferencesHow to Find & Fix Asymmetric Routing Issues | AuvikIdentifying and Troubleshooting Asymmetric Routing in WAAS - Cisco Community

NEW QUESTION 199
- (Topic 3)
A network engineer has added a new route on a border router and is trying to determine if traffic is using the new route. Which of the following commands should the engineer use?

A. ping
B. arp
C. tracert
D. route

Answer: C

Explanation:

The tracert command is a network diagnostic tool that traces the route of packets from the source host to the destination host. It displays the IP addresses and hostnames of the routers along the path, as well as the time taken for each hop. The tracert command can be used to determine if traffic is using the new route by comparing the output before and after adding the route. If the new route is effective, the tracert command should show a different or shorter path to the destination host.
ReferencesNetworking Commands For Troubleshooting Windows - GeeksforGeeksNine Switch Commands Every Cisco Network Engineer Needs to Know

NEW QUESTION 204
- (Topic 3)
A medical building offers patients Wi-Fi in the waiting room. Which of the following security features would be the BEST solution to provide secure connections and keep the medical data protected?

A. Isolating the guest network
B. Securing SNMP
C. MAC filtering
D. Disabling unneeded switchports

Answer: A

NEW QUESTION 209
- (Topic 3)
A technician is installing the Wi-Fi infrastructure for legacy industrial machinery at a warehouse. The equipment only supports 802.11a and 802.11b standards. Speed of transmission is the top business requirement. Which of the following is the correct maximum speed for this scenario?

A. 11Mbps
B. 54Mbps
C. 128Mbps
D. 144Mbps

Answer: B

Explanation:
802.11b (Wi-Fi 1) 11 Mbps
100 meter maximum effective range 802.11a (Wi-Fi 2)
54 Mbps
50 meter maximum effective range

NEW QUESTION 212
- (Topic 3)
A network technician is implementing a solution that will allow end users to gain access to multiple applications after logging on. Which of the following authentication methods would allow this type of access?

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

Answer: A

NEW QUESTION 215
- (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 218
- (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 223
- (Topic 3)
Many IP security cameras use RTSP to control media playback. Which of the following default transport layer port numbers does RTSP use?

A. 445
B. 554
C. 587
D. 5060

Answer: B

Explanation:
RTSP stands for Real Time Streaming Protocol and is an application-level network protocol designed for controlling media playback on streaming media servers. RTSP uses the default transport layer port number 554 for both TCP and UDP1. Port 445 is used for SMB (Server Message Block), a protocol for file and printer sharing. Port 587 is used for SMTP (Simple Mail Transfer Protocol), a protocol for sending email messages. Port 5060 is used for SIP (Session Initiation Protocol), a protocol for initiating and managing multimedia sessions.
References: 1 Real Time Streaming Protocol - Wikipedia (https://en.wikipedia.org/wiki/Real_Time_Streaming_Protocol)

NEW QUESTION 228
- (Topic 3)
Which of the following would be the MOST cost-effective recovery solution for a company's lower-priority applications?

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

Answer: C

NEW QUESTION 229
- (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 234
- (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 236
- (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 241
- (Topic 3)
A Fortune 500 firm is deciding On the kind or data center equipment to install given its five- year budget Outlook. The Chief Information comparing equipment based on the life expectancy Of different models. Which Of the following concepts BEST represents this metric?

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

Answer: A

NEW QUESTION 244
- (Topic 3)
Which of the following can be used to validate domain ownership by verifying the presence of pre-agreed content contained in a DNS record?

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

Answer: D

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

NEW QUESTION 247
- (Topic 3)
A network administrator needs to change where the outside DNS records are hosted.
Which of the following records should the administrator change at the registrar to accomplish this task?

A. NS
B. SOA
C. PTR
D. CNAME

Answer: A

Explanation:
NS stands for Name Server, and it is a DNS record that specifies which servers are authoritative for a domain. The registrar is the entity that manages the domain registration and delegation, and it maintains the NS records for each domain. To change where the outside DNS records are hosted, the network administrator needs to change the NS records at the registrar to point to the new DNS servers that will host the outside DNS records.
References:
? DNS Record Types – N10-008 CompTIA Network+ : 1.61
? CompTIA Network+ N10-008 Cert Guide, page 1472

NEW QUESTION 251
- (Topic 3)
A technician is investigating an issue with connectivity at customer's location. The technician confirms that users can access resources locally but not over the internet The technician theorizes that the local router has failed and investigates further. The technician's testing results show that the route is functional: however, users still are unable to reach resources on the internal. Which of the following describes what the technician should do NEXT?

A. Document the lessons learned
B. Escalate the issue
C. identify the symptoms.

D. Question users for additional information

Answer: C

Explanation:
According to the CompTIA Network+ troubleshooting model123, this is the first step in troubleshooting a network problem. The technician should gather information about the current state of the network, such as error messages, device status, network topology, and user feedback. This can help narrow down the scope of the problem and eliminate possible causes.

NEW QUESTION 253
- (Topic 3)
A network administrator is getting reports of some internal users who cannot connect to network resources. The users slate they were able to connect last week, but not today. No changes have been configured on the network devices or server during the last few weeks. Which of the following is the MOST likely cause of the issue?

A. The client DHCP scope is fully utilized
B. The wired network is experiencing electrical interference
C. The captive portal is down and needs to be restarted
D. SNMP traps are being received
E. The packet counter on the router interface is high.

Answer: A

NEW QUESTION 256
- (Topic 3)
An attacker targeting a large company was able to inject malicious A records into internal name resolution servers. Which of the following attack types was MOST likely used?

A. DNS poisoning
B. On-path
C. IP spoofing
D. Rogue DHCP

Answer: A

NEW QUESTION 258
- (Topic 3)
A technician is configuring a bandwidth-monitoring tool that supports payloads of 1,600 bytes. Which of the following should the technician configure for this tool?

A. LACP
B. Flow control
C. Port mirroring
D. Jumbo frames

Answer: D

Explanation:
Jumbo frames are Ethernet frames that can carry more than the standard 1,500 bytes of payload data. Jumbo frames can support payloads of up to 9,000 bytes, depending on the network device and configuration. Jumbo frames can improve network performance by reducing the overhead of packet headers and increasing the efficiency of data transmission. Jumbo frames can also reduce the CPU utilization of the sender and receiver devices, as they require fewer interrupts and processing cycles. However, jumbo frames also have some drawbacks, such as increased latency, fragmentation, and compatibility issues. Therefore, jumbo frames should be used with caution and only in networks that support them end-to-end.
A technician who is configuring a bandwidth-monitoring tool that supports payloads of 1,600 bytes should enable jumbo frames for this tool, as this would allow the tool to capture and analyze more data per frame and provide more accurate and detailed results. However, the technician should also ensure that the network devices and interfaces that the tool is connected to also support jumbo frames, and that the MTU (maximum transmission unit) is set to the same value across the network path.
ReferencesWhat are Jumbo Frames?How to Enable Jumbo FramesCompTIA Network+ Certification All-in-One Exam Guide, Eighth Edition (Exam N10-008)

NEW QUESTION 261
- (Topic 3)
Which of the following best describes what an organization would use port address translation for?

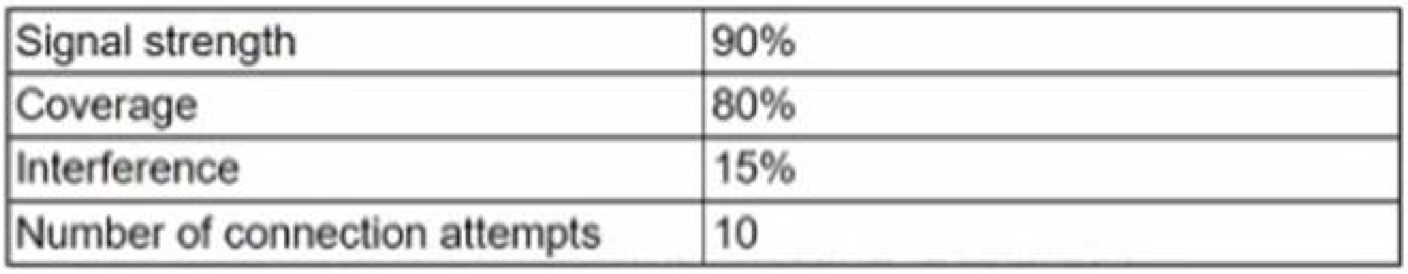
A. VLANs on the perimeter
B. Public address on the perimeter router
C. Non-routable address on the perimeter router
D. Servers on the perimeter

Answer: B

Explanation:
The best answer is B. Public address on the perimeter router.
Port address translation (PAT) is a function that allows multiple users within a private network to make use of a minimal number of IP addresses. Its basic function is to share a single IP public address between multiple clients who need to use the Internet publicly. It is an extension of network address translation (NAT)1.
PAT works by creating dynamic NAT mapping, in which a global (public) IP address and a unique port number are selected. The router keeps a NAT table entry for every unique combination of the private IP address and port, with translation to the global address and a unique port number2.
Therefore, an organization would use PAT for having a public address on the perimeter router, which can be shared by many hosts on the private network using different port numbers. This can reduce the bandwidth consumption and cost of the organization's internet connection, as well as provide some security benefits by hiding the internal network structure3.
The other options are not correct because:

? VLANs on the perimeter are not related to PAT, as they are used to segment the network into logical groups based on different criteria, such as function, security, or performance4.
? Non-routable address on the perimeter router would not allow the organization to access the Internet or the cloud, as non-routable addresses are not valid on the public network and cannot be translated by PAT5.
? Servers on the perimeter are not a reason to use PAT, as servers usually have static IP addresses and do not need to share a public address with other hosts. Servers on the perimeter may use NAT, but not PAT, to map their private IP addresses to a public IP address2.

NEW QUESTION 262
- (Topic 3)
A new student is given credentials to log on to the campus Wi-Fi. The student stores the password in a laptop and is able to connect; however, the student is not able to connect with a phone when only a short distance from the laptop. Given the following information:



Signal strength	90%
Coverage	80%
Interference	15%
Number of connection attempts	10

Which of the following is MOST likely causing this connection failure?

A. Transmission speed
B. Incorrect passphrase
C. Channel overlap
D. Antenna cable attenuation/signal loss

Answer: B

NEW QUESTION 265
- (Topic 3)
A network administrator is preparing answers for an annual risk assessment that is required for compliance purposes. Which of the following would be an example of an internal threat?

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

Answer: A

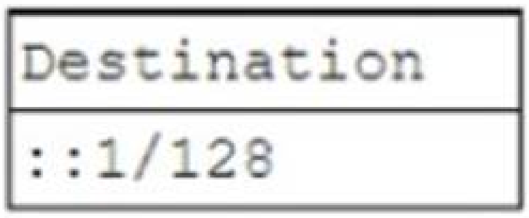
Explanation:
Insider threat= insider threat is defined as the threat that an employee or a contractor will use his or her authorized access, wittingly or unwittingly, to do harm

NEW QUESTION 267
- (Topic 3)
A systems operator is granted access to a monitoring application, configuration application,
and timekeeping application. The operator is denied access to the financial and project management applications by the system's security configuration. Which of the following BEST describes the security principle in use?

A. Network access control
B. Least privilege
C. Multifactor authentication
D. Separation of duties

Answer: D

NEW QUESTION 272
- (Topic 3)
An application is not working. When the log files are reviewed, the application continuously tries to reach the following destination:



Destination
::1/128

Which of the following is most likely associated with this IP address?

A. APIPA
B. Default gateway
C. Link local
D. Loopback

Answer: D

Explanation:
The IP address ::1/128 is the loopback address of the local host in IPv6, which is the equivalent of the 127.0.0.1 in IPv4. The loopback address is a virtual interface

that loops all traffic back to itself, the local host. The loopback address is used for testing and troubleshooting purposes, such as checking the connectivity and configuration of the network stack. If an application tries to reach the loopback address, it means that it is not communicating with any external network or server, but only with itself.
The other options are not correct because they are not associated with the IP address ::1/128. They are:
? APIPA. APIPA stands for Automatic Private IP Addressing, which is a feature that allows a device to assign itself a private IPv4 address in the range of 169.254.0.0/16 when no DHCP server is available. APIPA does not apply to IPv6 addresses, and it is not related to the loopback address.
? Default gateway. The default gateway is the IP address of the router or device that connects a local network to other networks. The default gateway is usually the first or last usable IP address in a subnet, and it is not the same as the loopback address.
? Link local. Link local addresses are IPv6 addresses that are used for communication within a single network segment or link. Link local addresses have the prefix fe80::/10, and they are not routable or reachable from other networks. Link local addresses are not the same as the loopback address.
References1: Loopback Address - ::1/128 - ipUpTime.net2: Network+ (Plus) Certification | CompTIA IT Certifications3: Reserved IP addresses - Wikipedia

NEW QUESTION 273
- (Topic 3)
A public, wireless ISP mounts its access points on top of traffic signal poles. Fiber-optic cables are installed from a fiber switch through the ground and up the pole to a fiber-copper media converter, and then connected to the AP. In one location, the switchport is showing sporadic link loss to the attached AP. A similar link loss is not seen at the AP interface. The fiber-optic cable is moved to another unused switchport with a similar result. Which of the following steps should the assigned technician complete NEXT?

A. Disable and enable the switchport.
B. Clean the fiber-optic cable ends.
C. Replace the media converter.
D. Replace the copper patch cord.

Answer: B

Explanation:
Fiber-optic cables are cables that use light signals to transmit data over long distances at high speeds. Fiber-optic cables are sensitive to dirt, dust, moisture, or other contaminants that can interfere with the light signals and cause link loss or signal degradation. To troubleshoot link loss issues with fiber-optic cables, one of the steps that should be completed next is to clean the fiber-optic cable ends with a lint-free cloth or a specialized cleaning tool. Cleaning the fiber-optic cable ends can remove any dirt or debris that may be blocking or reflecting the light signals and restore the link quality.

NEW QUESTION 274
- (Topic 3)
Which or the following devices and encapsulations are found at me data link layer? (Select TWO)

A. Session
B. Frame
C. Firewall
D. Switch
E. Packet
F. Router

Answer: BD

Explanation:
The data link layer is responsible for defining the format of data on the network and providing physical transmission of data. Devices that operate at this layer include switches and network interface cards (NICs). Encapsulations that are used at this layer include frames, which are units of data that contain a header, payload, and trailer. Frames are used to identify the source and destination of data on the network and to perform error detection. References: CompTIA Network+ N10-008 Certification Study Guide, page 9; The Official CompTIA Network+ Student Guide (Exam N10-008), page 1-6.

NEW QUESTION 275
- (Topic 3)
A network administrator needs to provide remote clients with access to an internal web application. Which of the following methods provides the highest flexibility and compatibility while encrypting only the connection to the web application?

A. Clientless VPN
B. Virtual desktop
C. Virtual network computing
D. mGRE tunnel

Answer: A

Explanation:
A clientless VPN is a method of providing remote clients with access to an internal web application without installing any additional software or dedicated VPN client on their devices. Instead, users access the VPN through a web browser, utilizing a web portal or gateway provided by the VPN service. This method provides the highest flexibility and compatibility, as it supports various operating systems and devices, and encrypts only the connection to the web application, not the entire traffic of the device.

NEW QUESTION 280
- (Topic 3)
A cafeteria is lacing lawsuits related to criminal internet access that was made over its guest network. The marketing team, however, insists on keeping the cafeteria phone number as the wireless passphrase. Which of the following actions would Improve wireless security while accommodating the marketing team and accepting the terms of use?

A. Setting WLAN security to use EAP-TLS
B. Deploying a captive portal tor user authentication
C. Using geofencing to limit the area covered by the WLAN
D. Configuring guest network isolation

Answer: B

Explanation:
A captive portal is a web page that is presented to a user before they are allowed to access a network. It is used to authenticate users and to ensure that all users have accepted the terms of use for the network. By deploying a captive portal, the cafeteria can require users to enter their phone number as the passphrase, while still providing an additional layer of security. Reference: CompTIA Network+ Study Guide, 8th Edition, page 182.

NEW QUESTION 283
- (Topic 3)
Which of the following is an example of on-demand scalable hardware that is typically housed in the vendor's data center?

A. DaaS
B. laaS
C. PaaS
D. SaaS

Answer: B

Explanation:
IaaS is an example of on-demand scalable hardware that is typically housed in the vendor’s data center. IaaS stands for Infrastructure as a Service, which is a cloud computing model that provides virtualized computing resources over the internet. IaaS allows customers to rent servers, storage, network devices, and other hardware components from a cloud service provider, rather than purchasing and maintaining them on-premise. IaaS offers advantages such as scalability, flexibility, cost-effectiveness, and reliability. Customers can adjust their hardware resources according to their needs and pay
only for what they use. Customers can also access their hardware resources from anywhere via a web browser or an API. References: [CompTIA Network+ Certification Exam Objectives], What Is Infrastructure as a Service (IaaS)? | IBM

NEW QUESTION 286
- (Topic 3)
Which of the following requires network devices to be managed ustng a different set of IP addresses?

A. Console
B. Split tunnel
C. Jump box
D. Out of band

Answer: D

Explanation:
Out of band management is a process for accessing and managing network devices and infrastructure at remote locations through a separate management plane from the production network. Out of band management requires network devices to be managed using a different set of IP addresses than the ones used for in-band management or data traffic. This provides a secure and dedicated alternate access method to administer connected devices and IT assets without using the corporate LAN.

NEW QUESTION 288
- (Topic 3)
A technician is tasked with setting up a mail server and a DNS server. The mail port should be secured and have the ability to transfer large files. Which of the following ports should be opened? (Select TWO).

A. 22
B. 53
C. 110
D. 389
E. 995
F. 3389

Answer: BE

Explanation:
Port 53 is used for DNS, which is a service that translates domain names into IP addresses. Port 995 is used for POP3S, which is a protocol for receiving email messages securely. POP3S supports large file transfers and encryption. Therefore, these two ports should be opened for the mail server and the DNS server project

NEW QUESTION 292
- (Topic 3)
A technician is assisting a user who cannot connect to a website. The technician attempts to ping the default gateway and DNS server of the workstation. According to troubleshooting methodology, this is an example of:

A. a divide-and-conquer approach.
B. a bottom-up approach.
C. a top-to-bottom approach.
D. implementing a solution.

Answer: A

NEW QUESTION 295
- (Topic 3)
A company’s VoIP phone connection is cutting in and out. Which of the following should be configured to resolve this issue?

A. 802.1 Q tagging
B. Jumbo frames
C. Native VLAN
D. Link aggregation

Answer: A

Explanation:
* 802.1 Q tagging is a method of adding a VLAN identifier to an Ethernet frame to indicate which VLAN the frame belongs to. This allows different VLANs to share the same physical link and device without interfering with each other. 802.1 Q tagging also supports a quality of service (QoS) scheme that can prioritize different classes of traffic based on the priority code point (PCP) field in the tag12
VoIP phone connection issues can be caused by network congestion, packet loss, jitter, or latency, which affect the quality and reliability of voice transmission over the Internet. By using 802.1 Q tagging, VoIP traffic can be separated from other data traffic and assigned a higher priority level, which reduces the chances of dropping or delaying voice packets. 802.1 Q tagging can also improve the security and scalability of VoIP networks by isolating different voice domains and preventing unauthorized access34

NEW QUESTION 296
- (Topic 3)
A network manager wants to set up a remote access system for the engineering staff. Access to this system will be over a public IP and secured with an ACL. Which of the following best describes this system?

A. VPN
B. Secure Shell
C. Jump server
D. API

Answer: C

Explanation:
A jump server is a system that allows remote access to internal devices through a single, secure device on the public network. A jump server can be configured with an access control list (ACL) to limit who can access the system and what devices they can connect to. A jump server can also use secure protocols such as SSH or VPN to encrypt the communication between the remote user and the internal device. A jump server is different from a VPN, which creates a virtual private network between the remote user and the internal network. A jump server is also different from a secure shell, which is a protocol that allows remote command execution and file transfer. An API is an application programming interface that allows software components to interact with each other.
References:
? Other Network Appliances – SY0-601 CompTIA Security+ : 3.31

NEW QUESTION 300
- (Topic 3)
A security engineer wants to provide a secure, dedicated, alternate access method into an IT network infrastructure to administer connected devices and IT assets. Which of the following is the engineer most likely to implement?

A. Remote desktop gateway
B. Authentication and authorization controls
C. Out-of-band management
D. Secure Shell

Answer: C

Explanation:
Out-of-band management is a method of accessing network devices and IT assets through a dedicated channel that is separate from the normal data traffic. This provides a secure and alternate way to administer the network infrastructure, especially in case of failures or emergencies. Remote desktop gateway is a service that allows remote access to desktops and applications on a network. Authentication and authorization controls are mechanisms that verify the identity and permissions of users and devices on a network. Secure Shell is a protocol that encrypts the communication between a client and a server on a network.

NEW QUESTION 304
- (Topic 3)
A customer called the help desk to report a network issue. The customer recently added a hub between the switch and the router in order to duplicate the traffic flow to a logging device. After adding the hub, all the Other network components that were connected to the switch slowed more than expected. Which Of the following is the MOST likely cause Of the issue?

A. Duplex mismatch
B. Flow control failure
C. STP malfunction
D. 802.1Q disabled

Answer: A

Explanation:
A duplex mismatch is a situation where two devices on a network have different duplex settings, such as full-duplex or half-duplex. Full-duplex means that a device can send and receive data simultaneously, while half-duplex means that a device can only send or receive data at a time. A duplex mismatch can cause performance issues, such as collisions, errors, or slow throughput. In this scenario, the customer added a hub between the switch and the router. A hub is a device that operates at half-duplex and broadcasts all traffic to all ports. A switch and a router are devices that operate at full-duplex and forward traffic to specific ports. Therefore, adding a hub between the switch and the router can cause a duplex mismatch and slow down all the other network components that were connected to the switch.
References: https://www.comparitech.com/net-admin/hub-vs-switch-vs-router/ https://www.cisco.com/c/en/us/support/docs/lan-switching/ethernet/10561-3.html

NEW QUESTION 306
- (Topic 3)

A network engineer turned on logging to assist with troubleshooting a suspected configuration issue informative log information?

A. FATAL
B. ERROR
C. DEBUG
D. WARN

Answer: C

Explanation:
DEBUG is the log level that provides the most informative log information for troubleshooting a suspected configuration issue. Logging is a feature that allows network devices to record events and messages related to their operation and status. Logging can help network engineers to monitor, diagnose, and resolve network problems. Log levels are categories that indicate the severity or importance of a log message. Different log levels provide different amounts of detail and verbosity. DEBUG is the lowest log level, which means it provides the most detailed and verbose information about every action and event that occurs on a network device. DEBUG can help network engineers to identify configuration errors, misbehaving processes, or unexpected outcomes. However, DEBUG can also generate a lot of noise and overhead, which can affect the performance and availability of the network device. Therefore, DEBUG should be used sparingly and only when necessary. References: [CompTIA Network+ Certification Exam
Objectives], Understanding Logging Levels - Cisco

NEW QUESTION 311
- (Topic 3)
Which of the following does OSPF use to communicate routing updates?

A. Unicast
B. Anycast
C. Multicast
D. Broadcast

Answer: C

Explanation:
OSPF uses multicast to communicate routing updates among routers within the same area. OSPF routers send and receive link-state advertisements (LSAs) using IP multicast addresses 224.0.0.5 (all OSPF routers) and 224.0.0.6 (all OSPF designated routers) 1. Multicast allows OSPF to send routing updates efficiently and selectively, without flooding the entire network or requiring acknowledgments from every router

NEW QUESTION 314
- (Topic 3)
ARP spoofing would normally be a part of:

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

Answer: A

NEW QUESTION 317
- (Topic 3)
Which of the following is the MOST effective security control to keep a company's physical perimeter protected against intrusions leveraged by social-engineering techniques?

A. Employee training
B. Biometric lockers
C. Access control vestibule
D. Motion detection

Answer: A

Explanation:
The most effective security control to keep a company’s physical perimeter protected against intrusions leveraged by social-engineering techniques is employee training. Employee training is a process of educating and raising awareness among staff members about security policies, procedures, and best practices. Employee training can help prevent social-engineering attacks, which are attempts to manipulate or deceive people into revealing sensitive information or granting unauthorized access to resources. Social-engineering techniques can include phishing, impersonation, tailgating, dumpster diving, or baiting. References: CompTIA Network+ N10-008 Certification Study Guide, page 343; The Official CompTIA Network+ Student Guide (Exam N10-008), page 13-8.

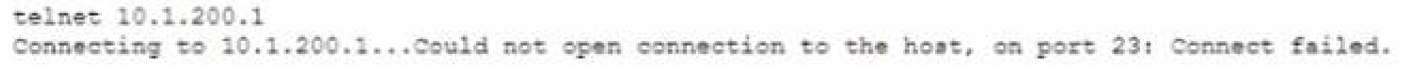
NEW QUESTION 322
- (Topic 3)
Which of the following needs to be tested to achieve a Cat 6a certification for a company's data cawing?

A. RJ11
B. LC ports
C. Patch panel
D. F-type connector

Answer: D

NEW QUESTION 323
- (Topic 3)

A network engineer receives the following when connecting to a switch to configure a port:



```
telnet 10.1.200.1
Connecting to 10.1.200.1...Could not open connection to the host, on port 23: Connect failed.
```

Which of the following is the MOST likely cause for the failure?

A. The network engineer is using the wrong protocol
B. The network engineer does not have permission to configure the device
C. SNMP has been secured with an ACL
D. The switchport the engineer is trying to configure is down

Answer: D

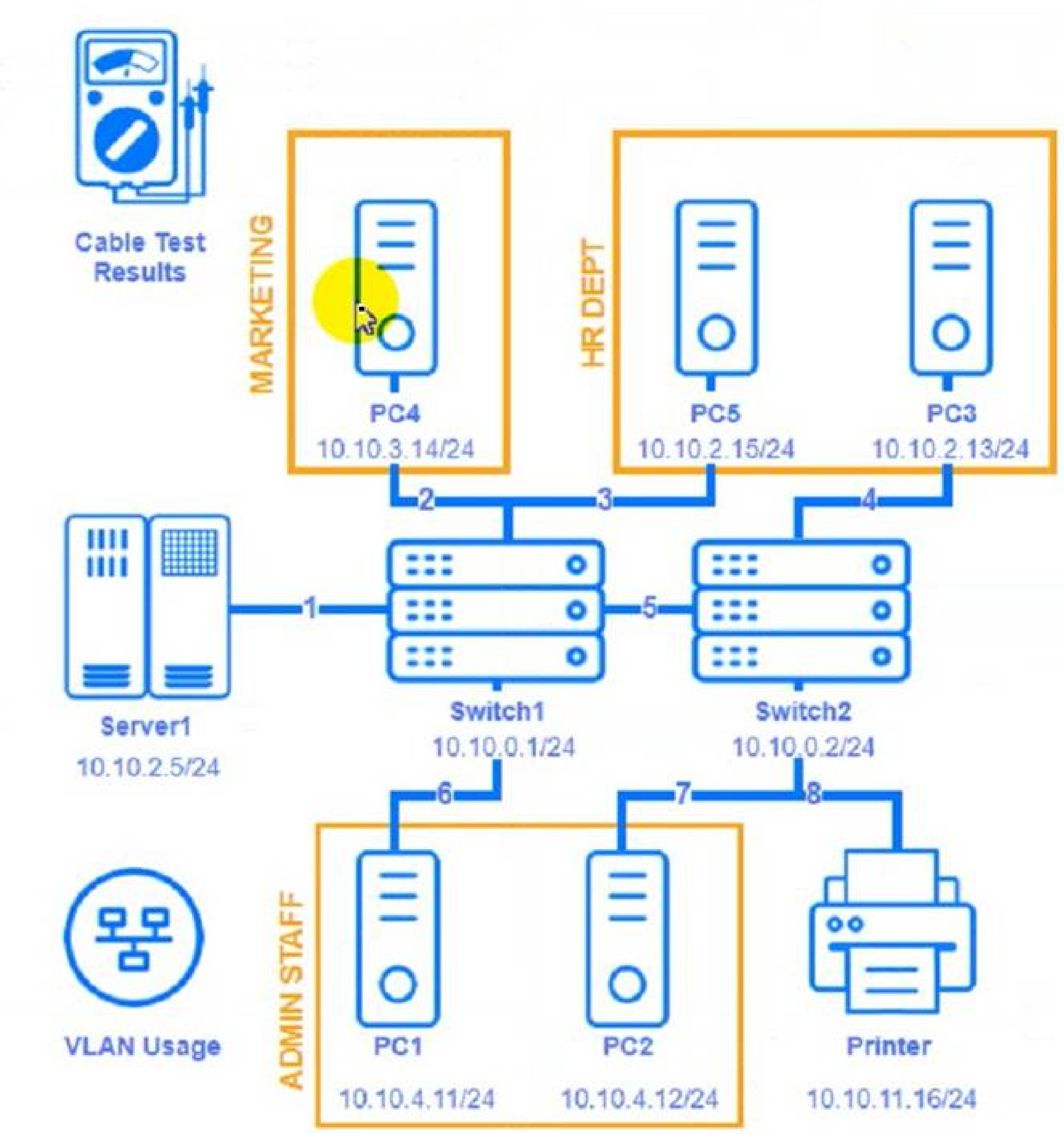
NEW QUESTION 328
- (Topic 3)
An administrator wants to increase the availability of a server that is connected to the office network. Which of the following allows for multiple NICs to share a single IP address and offers maximum performance while providing fault tolerance in the event of a NIC failure?

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 330
SIMULATION - (Topic 3)
A network technician needs to resolve some issues with a customer's SOHO network.
The customer reports that some of the devices are not connecting to the network, while others appear to work as intended.
INSTRUCTIONS
Troubleshoot all the network components and review the cable test results by Clicking on each device and cable.
Diagnose the appropriate component(s) by identifying any components with a problem and recommend a solution to correct each problem.



```
C:\>
```

```
C:\>
```

```
C:\>
```

PC5 - HR DEPT

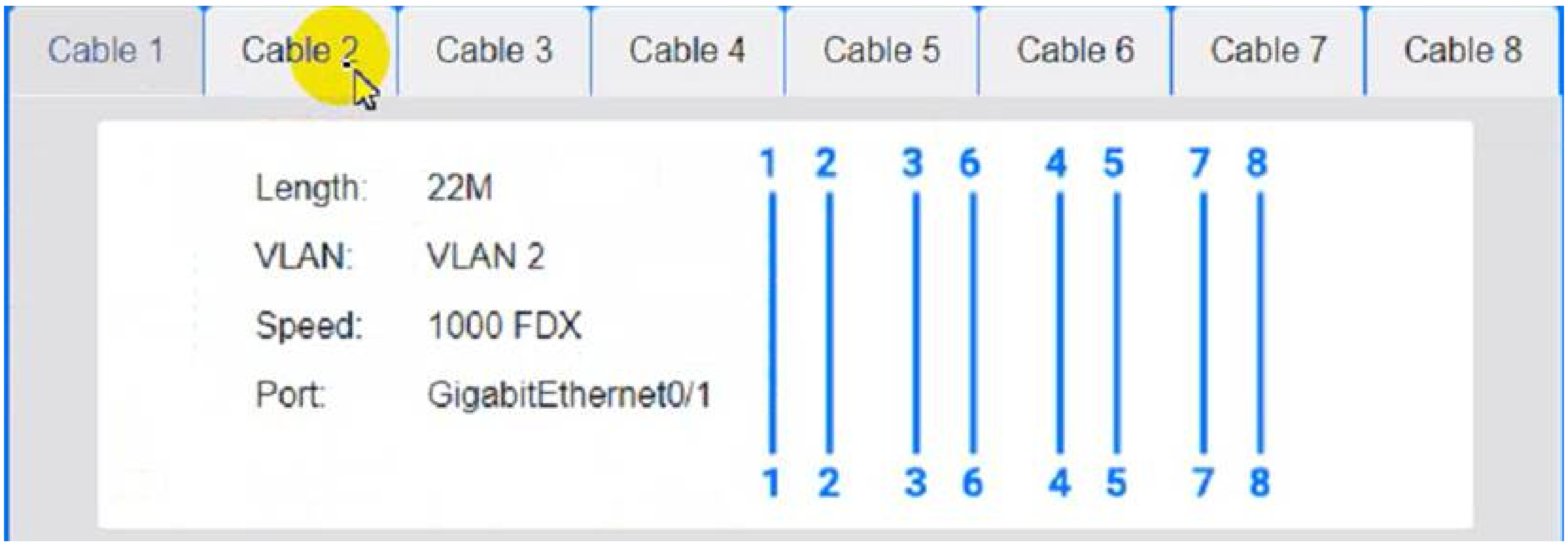
```
C:\>
```

Server1

```
C:\>
```

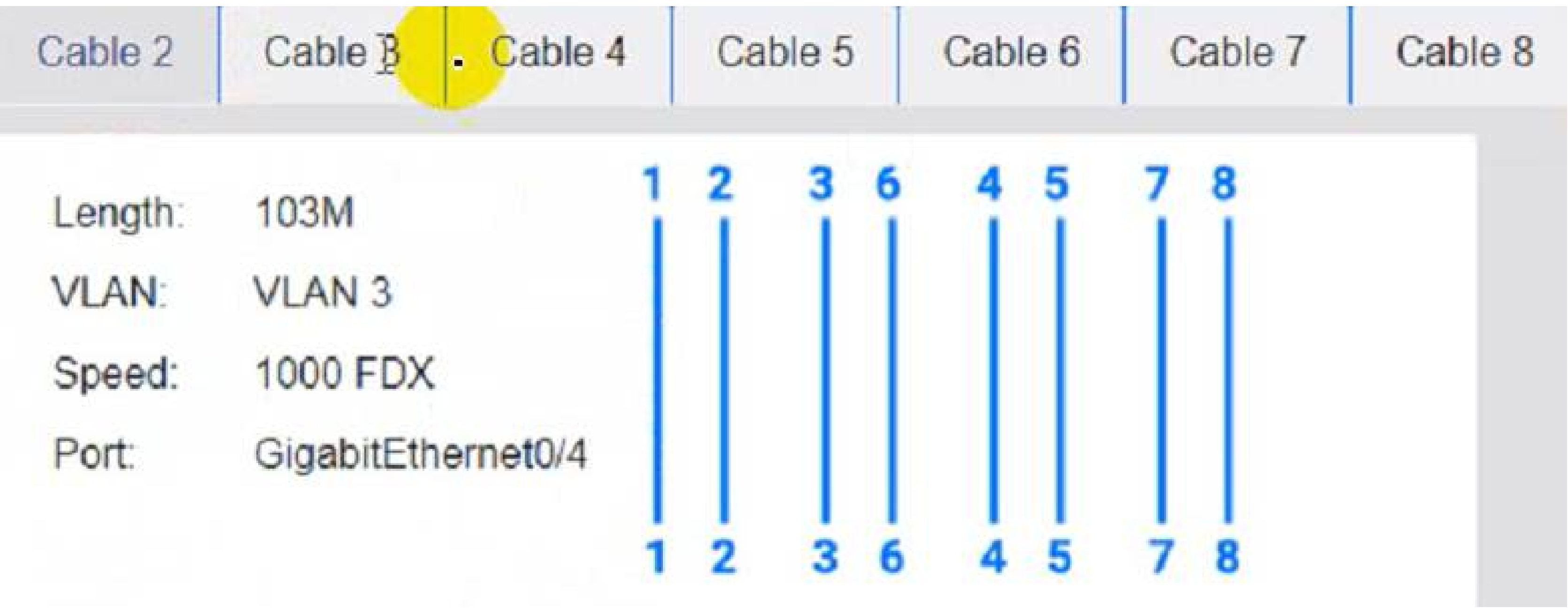
Cable Test Results:

Cable 1:



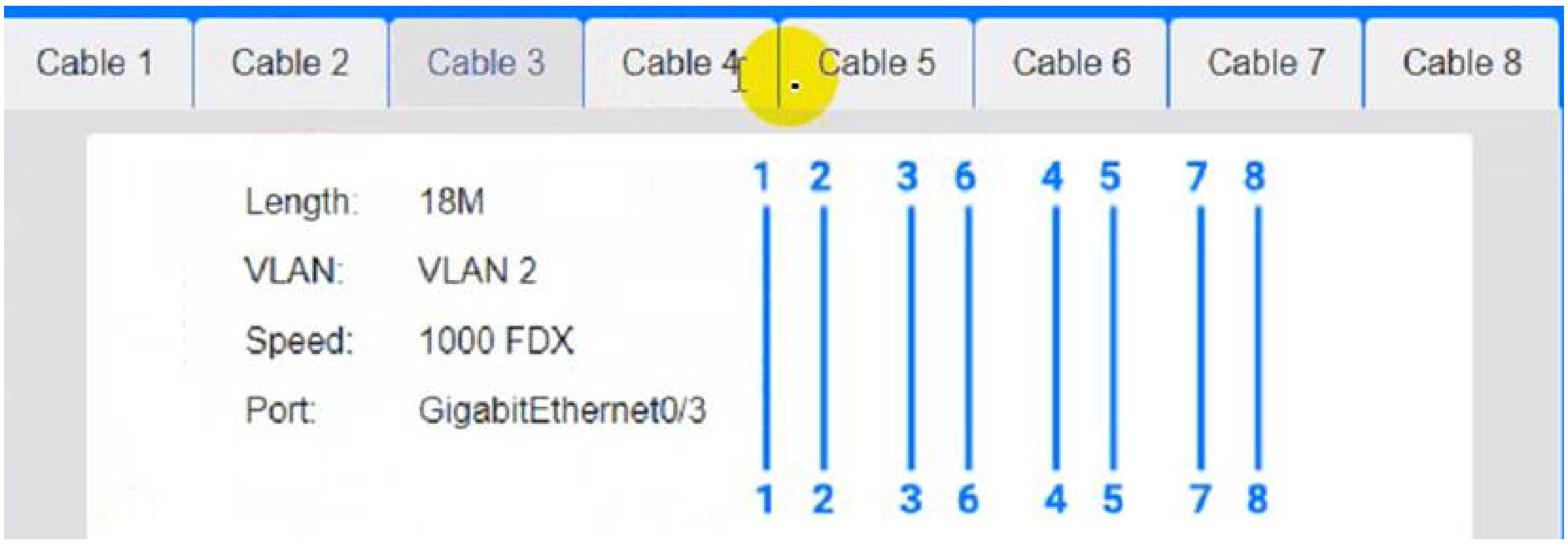
Length: 22M
VLAN: VLAN 2
Speed: 1000 FDX
Port: GigabitEthernet0/1

Cable 2:



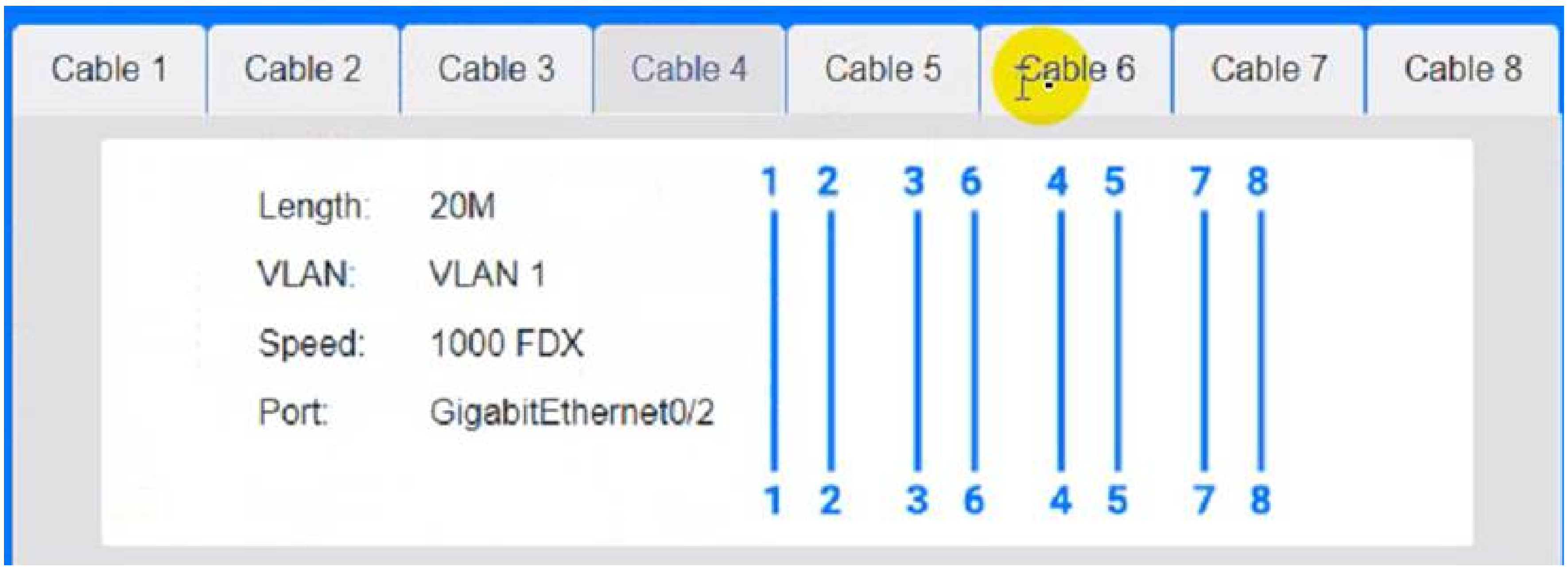
Length: 103M
VLAN: VLAN 3
Speed: 1000 FDX
Port: GigabitEthernet0/4

Cable 3:

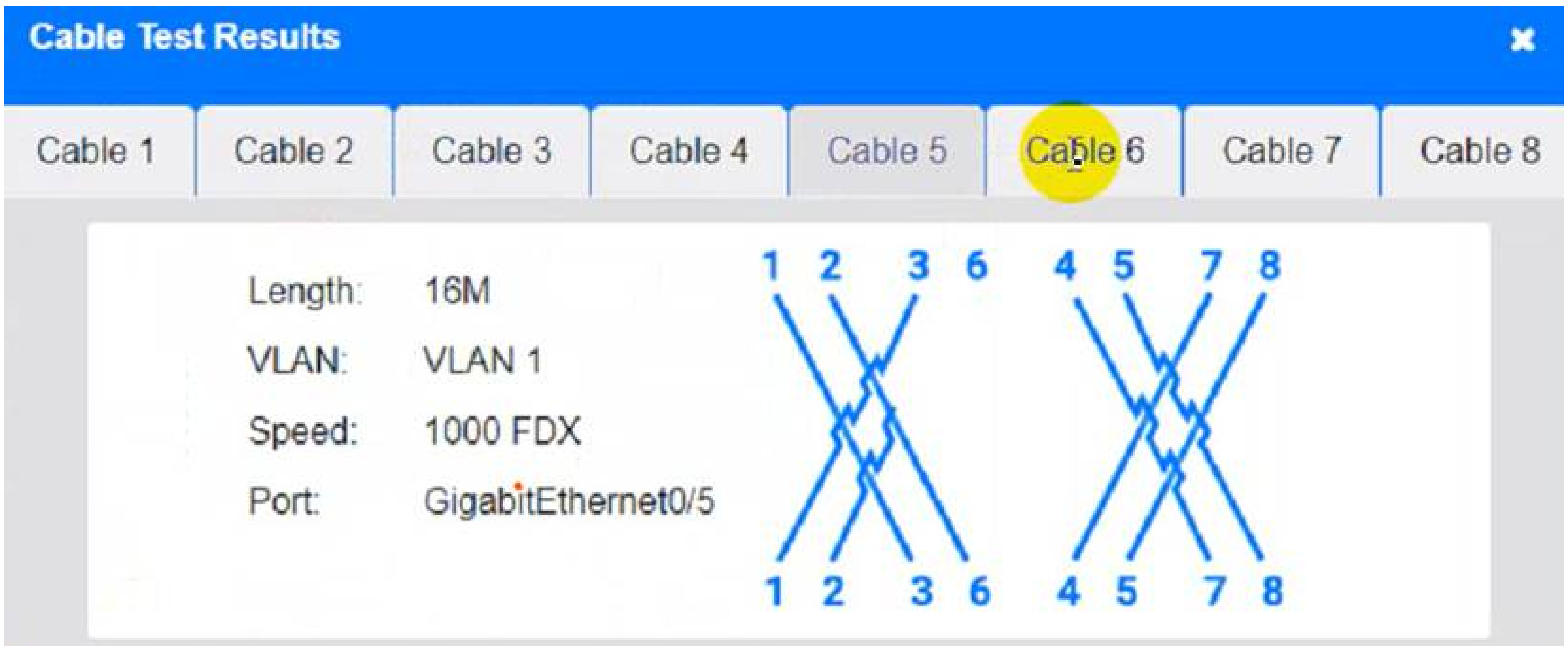


Length: 18M
VLAN: VLAN 2
Speed: 1000 FDX
Port: GigabitEthernet0/3

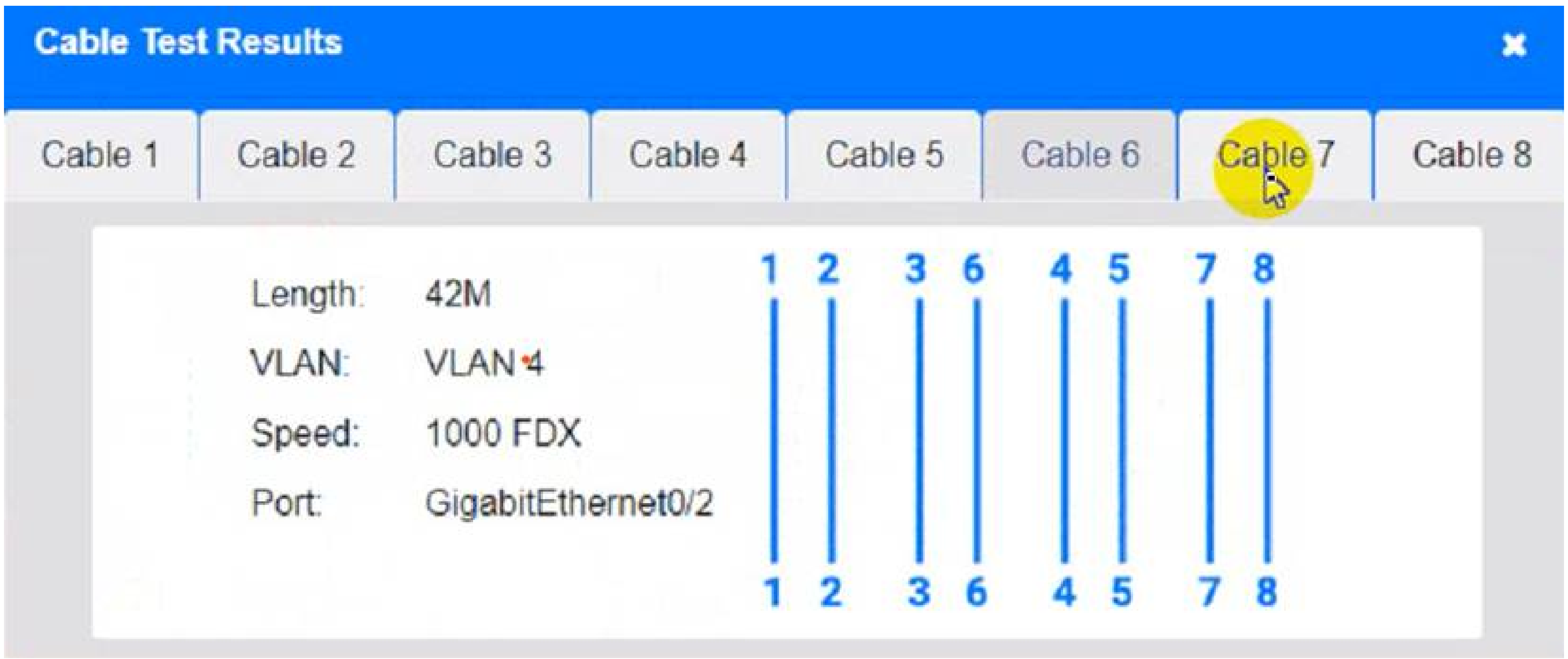
Cable 4:



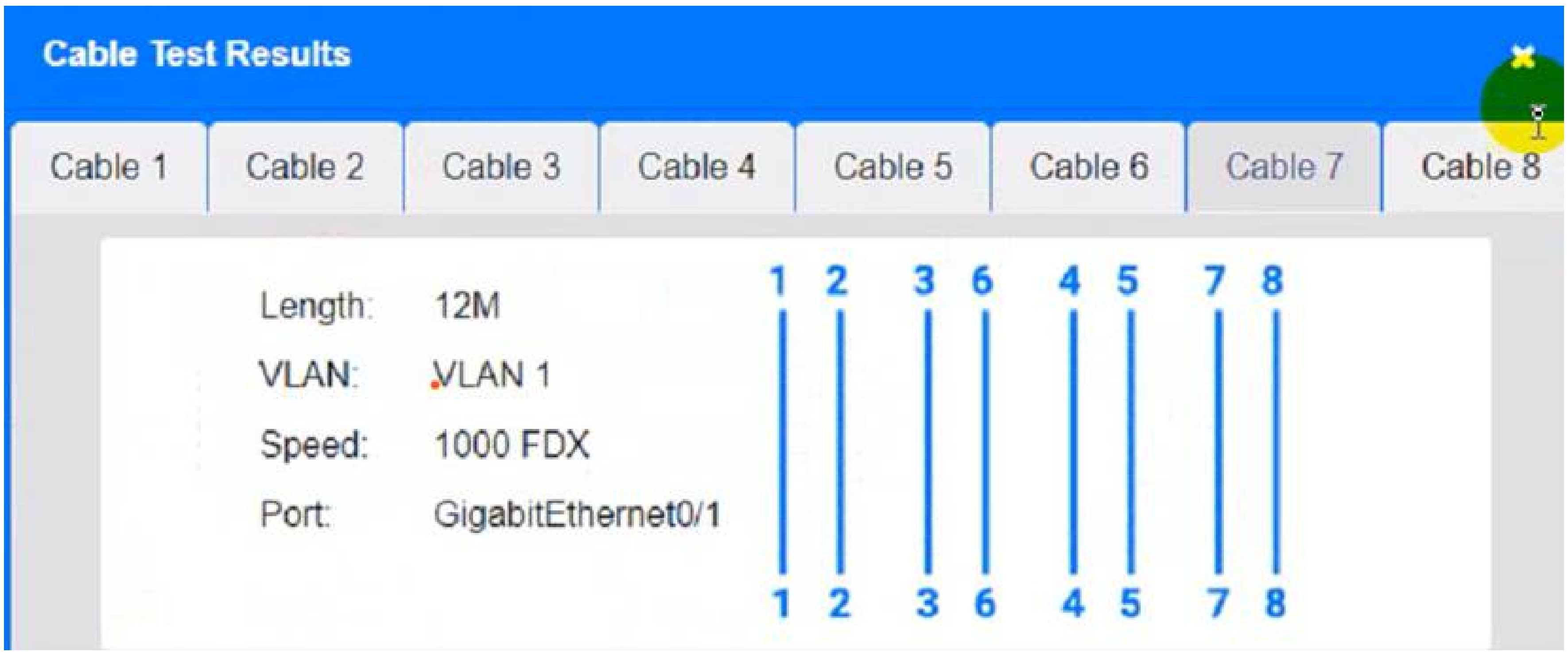
Length: 20M
VLAN: VLAN 1
Speed: 1000 FDX
Port: GigabitEthernet0/2



Length: 16M
VLAN: VLAN 1
Speed: 1000 FDX
Port: GigabitEthernet0/5



Length: 42M
VLAN: VLAN 4
Speed: 1000 FDX
Port: GigabitEthernet0/2



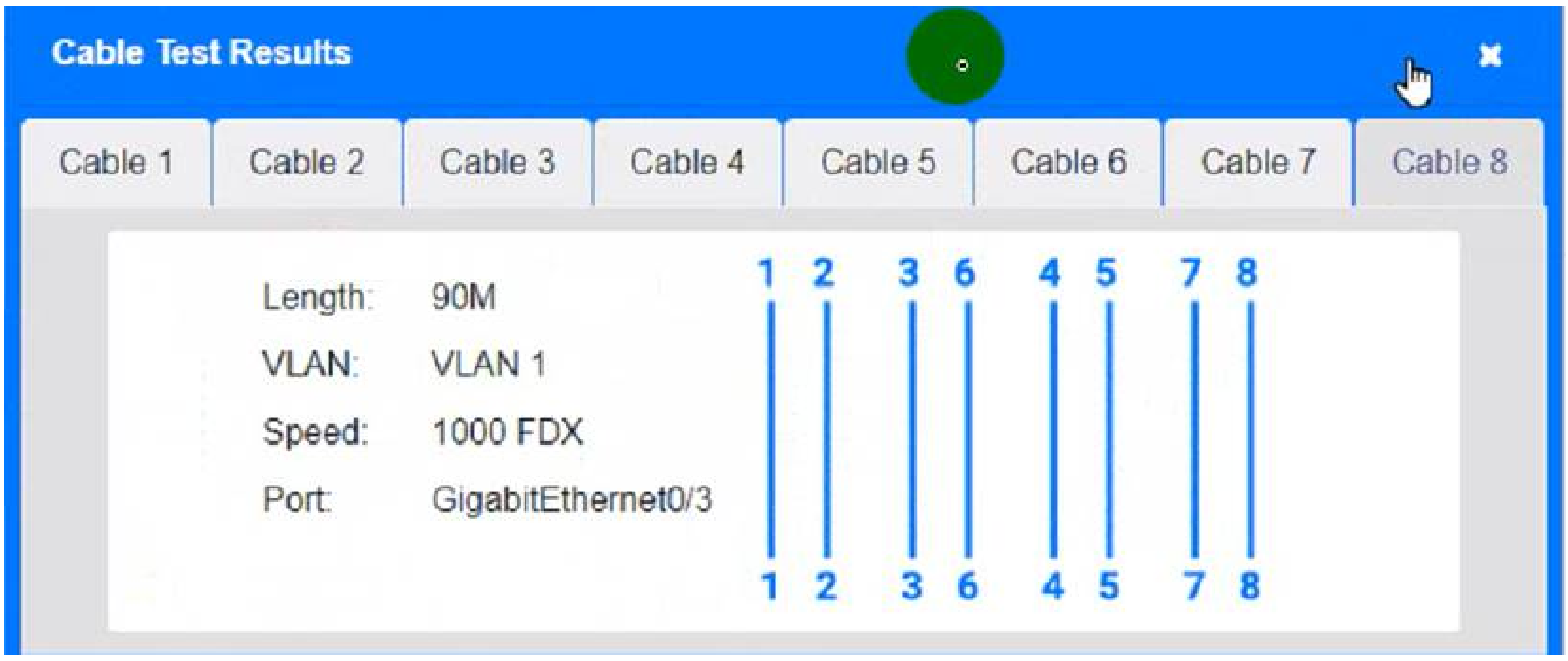
Cable Test Results

Length: 12M

VLAN: VLAN 1

Speed: 1000 FDX

Port: GigabitEthernet0/1



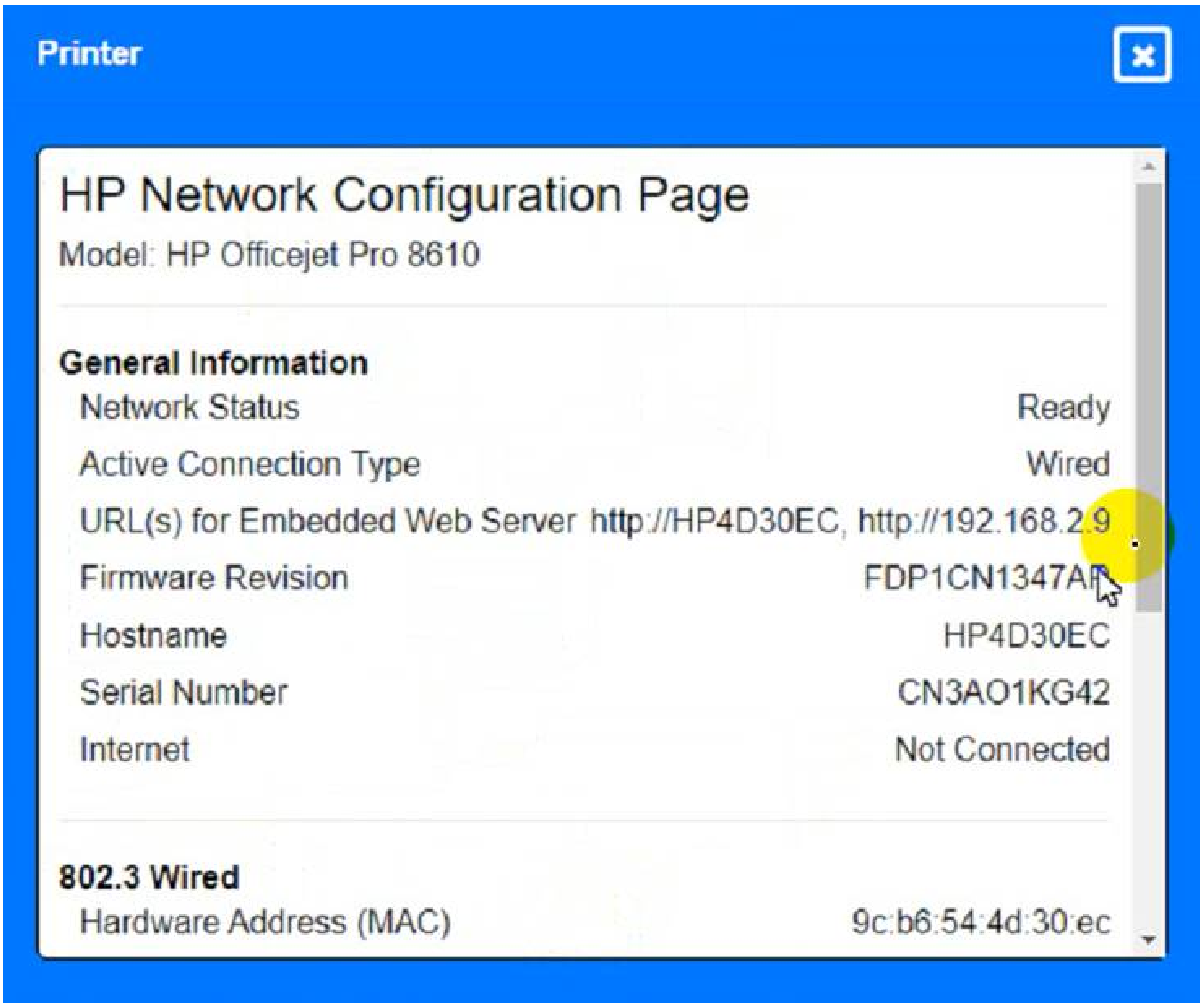
Cable Test Results

Length: 90M

VLAN: VLAN 1

Speed: 1000 FDX

Port: GigabitEthernet0/3



Printer

HP Network Configuration Page

Model: HP Officejet Pro 8610

General Information

Network Status Ready

Active Connection Type Wired

URL(s) for Embedded Web Server http://HP4D30EC, http://192.168.2.9

Firmware Revision FDP1CN1347AR

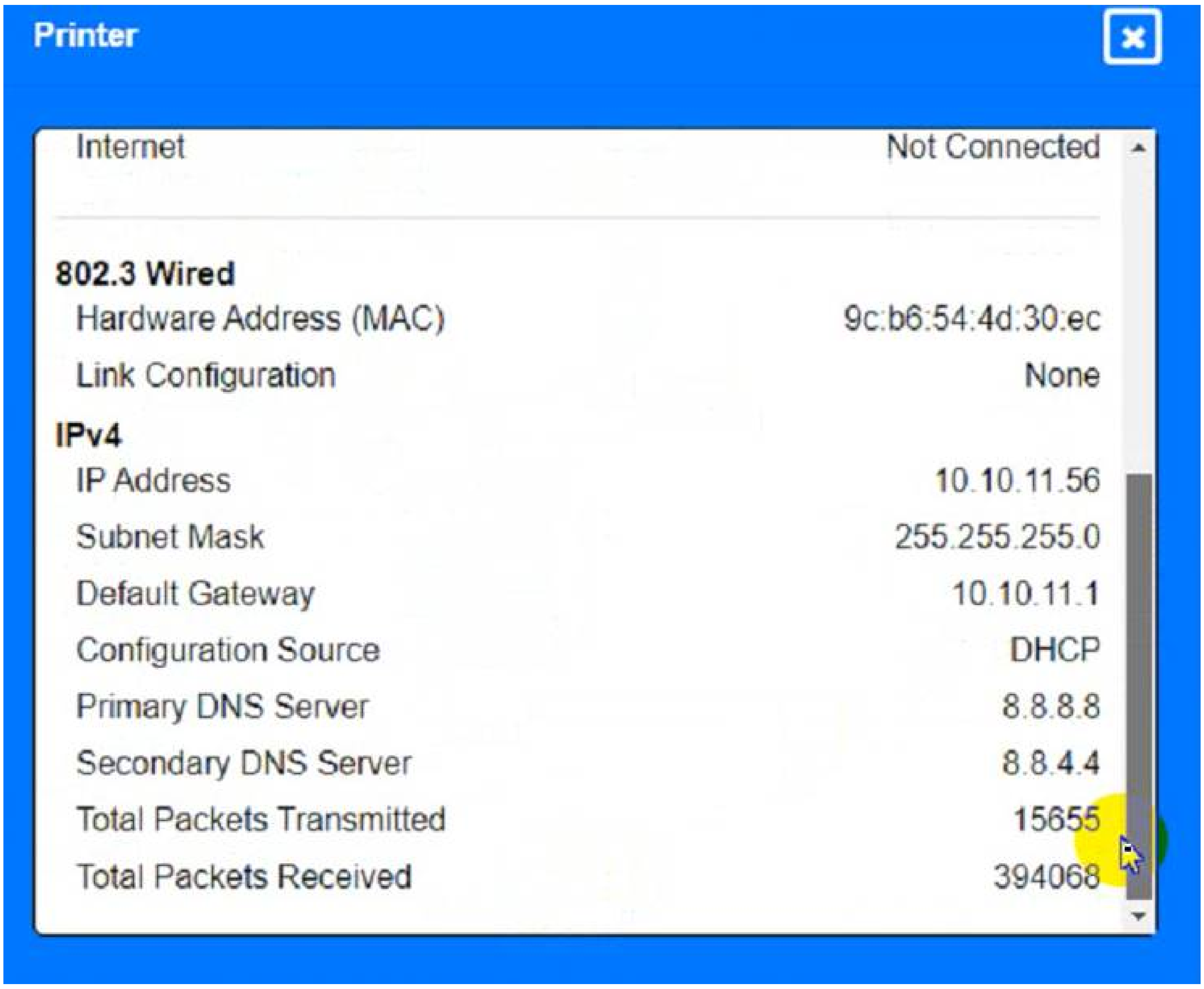
Hostname HP4D30EC

Serial Number CN3AO1KG42

Internet Not Connected

802.3 Wired

Hardware Address (MAC) 9c:b6:54:4d:30:ec



Printer

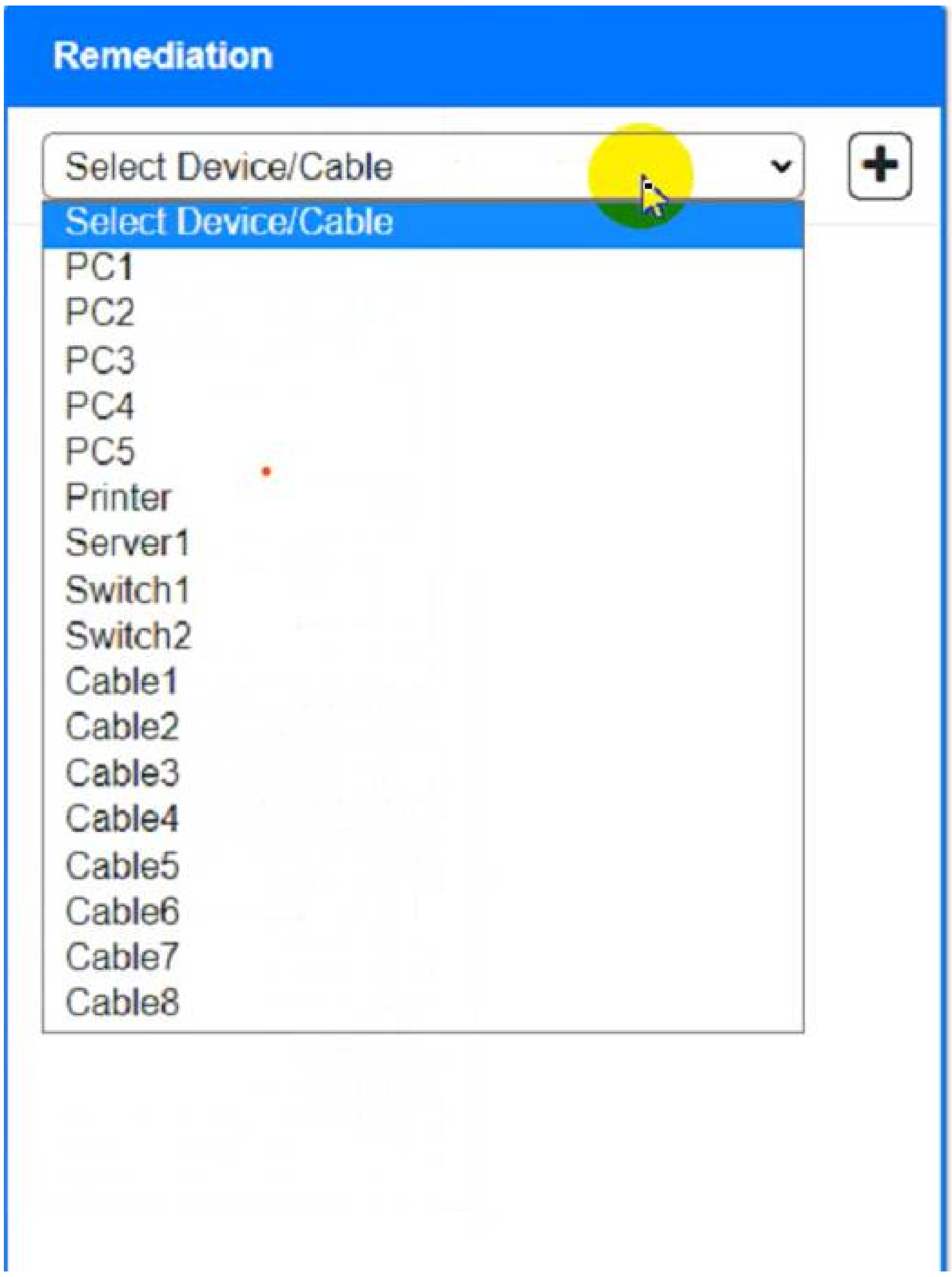
Internet	Not Connected

802.3 Wired

Hardware Address (MAC)	9c:b6:54:4d:30:ec
Link Configuration	None

IPv4

IP Address	10.10.11.56
Subnet Mask	255.255.255.0
Default Gateway	10.10.11.1
Configuration Source	DHCP
Primary DNS Server	8.8.8.8
Secondary DNS Server	8.8.4.4
Total Packets Transmitted	15655
Total Packets Received	394068



Remediation

Select Device/Cable

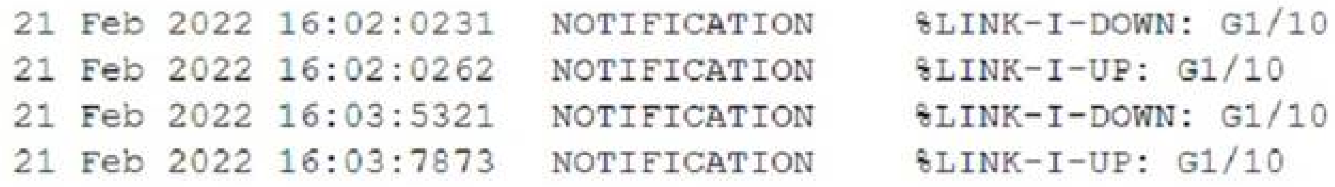
A. Mastered

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 troubleshoot all the network components and review the cable test results, you can use the following steps:
? Click on each device and cable to open its information window.
? Review the information and identify any problems or errors that may affect the network connectivity or performance.
? Diagnose the appropriate component(s) by identifying any components with a problem and recommend a solution to correct each problem.
? Fill in the remediation form using the drop-down menus provided. Here is an example of how to fill in the remediation form for PC1:
? The component with a problem is PC1.
? The problem is Incorrect IP address.
? The solution is Change the IP address to 192.168.1.10.
You can use the same steps to fill in the remediation form for other components.
To enter commands in each device, you can use the following steps:
? Click on the device to open its terminal window.
? Enter the command ipconfig /all to display the IP configuration of the device, including its IP address, subnet mask, default gateway, and DNS servers.
? Enter the command ping <IP address> to test the connectivity and reachability to another device on the network by sending and receiving echo packets. Replace <IP address> with the IP address of the destination device, such as 192.168.1.1 for Core Switch 1.
? Enter the command tracert <IP address> to trace the route and measure the latency of packets from the device to another device on the network by sending and receiving packets with increasing TTL values. Replace <IP address> with the IP address of the destination device, such as 192.168.1.1 for Core Switch 1.
Here is an example of how to enter commands in PC1:
? Click on PC1 to open its terminal window.
? Enter the command ipconfig /all to display the IP configuration of PC1. You should see that PC1 has an incorrect IP address of 192.168.2.10, which belongs to VLAN
2 instead of VLAN 1.
? Enter the command ping 192.168.1.1 to test the connectivity to Core Switch 1. You should see that PC1 is unable to ping Core Switch 1 because they are on different subnets.
? Enter the command tracert 192.168.1.1 to trace the route to Core Switch 1. You should see that PC1 is unable to reach Core Switch 1 because there is no route between them.
You can use the same steps to enter commands in other devices, such as PC3, PC4, PC5, and Server 1.

NEW QUESTION 331
- (Topic 3)
A technician is troubleshooting intermittent connectivity between devices and viewing the following syslog entries from a switch:



```
21 Feb 2022 16:02:0231  NOTIFICATION   %LINK-I-DOWN: G1/10
21 Feb 2022 16:02:0262  NOTIFICATION   %LINK-I-UP: G1/10
21 Feb 2022 16:03:5321  NOTIFICATION   %LINK-I-DOWN: G1/10
21 Feb 2022 16:03:7873  NOTIFICATION   %LINK-I-UP: G1/10
```

Which of the following are these entries indicative of?

A. DDoS attack
B. Jitter
C. Latency
D. Link flapping

Answer: D

Explanation:
The syslog entries are indicative of link flapping, which is when a switch port rapidly transitions between the up and down states. This can cause intermittent connectivity issues, network instability, and increased CPU utilization on the switch. Link flapping can be caused by various factors, such as faulty cables, misconfigured interfaces, duplex mismatches, or network attacks. To troubleshoot link flapping, the technician should check the physical layer, verify the interface settings, and monitor the network traffic for anomalies. References:
? What is Link Flapping? - CompTIA1
? Troubleshooting Switch Port and Interface Problems - Cisco2
? Network Troubleshooting - N10-008 CompTIA Network+ : 4.1 - YouTube3

NEW QUESTION 334
- (Topic 3)
A corporate client is experiencing global system outages. The IT team has identified multiple potential underlying causes throughout the enterprise Each team member has been assigned an area to trouble shoot. Which of the following approaches is being used?

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

Answer: A

NEW QUESTION 337
- (Topic 3)
To find the best subnet mask that meets the requirement of six usable IP addresses, we need to calculate the number of host bits and the number of host addresses for each option. The number of host bits is the number of 0s in the binary representation of the subnet mask, and the number of host addresses is

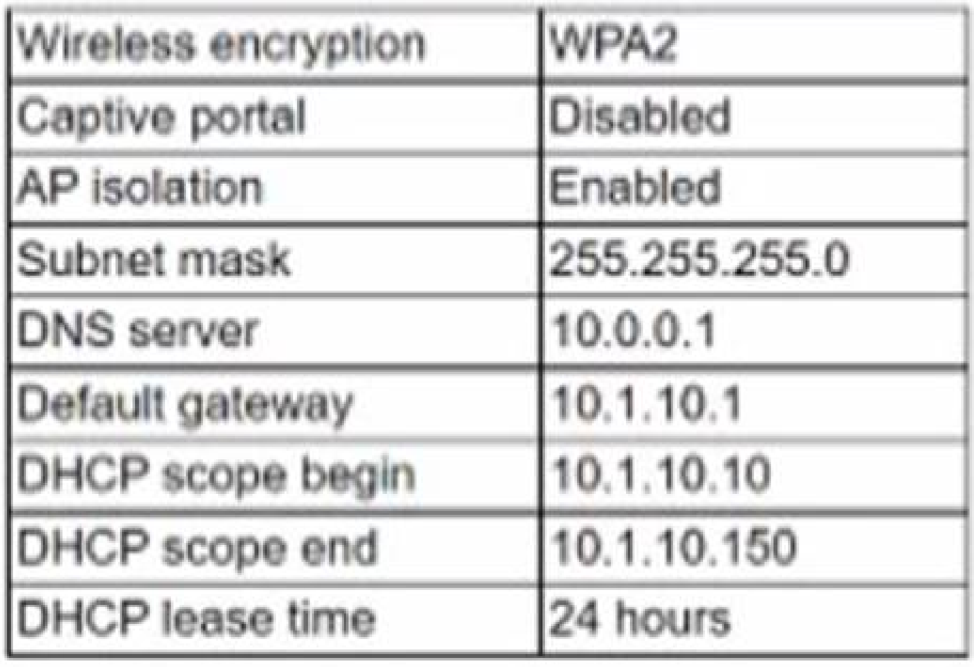
2^host bits - 2 (the -2 is to exclude the network address and the broadcast address). The option that has the smallest number of host addresses that is greater than or equal to six is the best choice. Here are the calculations for each option:

A. 255.255.255.128Binary: 11111111.11111111.11111111.10000000Host bits: 7Host addresses: 2^7 - 2 = 126 - 2 = 124This option has too many host addresses for the requirement.
B. 255.255.255.192Binary: 11111111.11111111.11111111.11000000Host bits: 6Host addresses: 2^6 - 2 = 64 - 2 = 62This option also has too many host addresses for the requirement.
C. 255.255.255.224Binary: 11111111.11111111.11111111.11100000Host bits: 5Host addresses: 2^5 - 2 = 32 - 2 = 30This option has the smallest number of host addresses that is greater than or equal to six, so this is the best choice.
D. 255.255.255.240Binary: 11111111.11111111.11111111.11110000Host bits: 4Host addresses: 2^4 - 2 = 16 - 2 = 14This option has fewer host addresses than the requirement, so this is not a valid choice.

Answer: C

Explanation:
This subnet mask will allow you to have six usable IP addresses in each subnet, with a minimum of wasted addresses. You can use the following formula to calculate the number of subnets and the subnet ID for each subnet:
Number of subnets = 2^network bits Subnet ID = (subnet number - 1) x number of host addresses + network address
The network bits are the number of 1s in the binary representation of the subnet mask, and the network address is the first address in the range. For example, if your range is 192.168.1.0/27, then the network bits are 27, the network address is 192.168.1.0, and the number of host addresses is 30. Therefore, the number of subnets is 2^27, and the subnet ID for the first subnet is (1 - 1) x 30 + 192.168.1.0 = 192.168.1.0. The subnet ID for the second subnet is (2 - 1) x 30 + 192.168.1.0 = 192.168.1.32, and so on.
References
? Subnet masks are covered in Objective 1.4 of the CompTIA Network+ N10-008 certification exam1.
? Subnet masks can be calculated based on binary and CIDR-block notations2.
? Subnet masks can be used to determine the number of host bits and host addresses3.
1: CompTIA Network+ Certification Exam Objectives, page 4 2: IPv4 Subnet Masks – N10- 008 CompTIA Network+ : 1.41 3: Calculating IPv4 Subnets and Hosts – N10-008 CompTIA Network+ : 1.44

NEW QUESTION 339
- (Topic 3)
A company ranis out a largo event space and includes wireless internet access for each tenant. Tenants reserve a two-hour window from the company each week, which includes a tenant-specific SSID However, all users share the company's network hardware.



Wireless encryption	WPA2
Captive portal	Disabled
AP isolation	Enabled
Subnet mask	255.255.255.0
DNS server	10.0.0.1
Default gateway	10.1.10.1
DHCP scope begin	10.1.10.10
DHCP scope end	10.1.10.150
DHCP lease time	24 hours

The network support team is receiving complaints from tenants that some users are unable to connect to the wireless network Upon investigation, the support teams discovers a pattern indicating that after a tenant with a particularly large attendance ends its sessions, tenants throughout the day are unable to connect. The following settings are common lo all network configurations:
Which of the following actions would MOST likely reduce this Issue? (Select TWO).

A. Change to WPA encryption
B. Change the DNS server to 10.1.10.1.
C. Change the default gateway to 10.0.0.1.
D. Change the DHCP scope end to 10.1.10.250
E. Disable AP isolation
F. Change the subnet mask lo 255.255.255.192.
G. Reduce the DHCP lease time to four hours.

Answer: DG

NEW QUESTION 344
- (Topic 3)
Which of the following BEST describes a spirt-tunnel client-to-server VPN connection?

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

Answer: C

Explanation:

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

NEW QUESTION 347
- (Topic 3)
A network technician is installing a wireless network in an office building. After performing a site survey, the technician determines the area is very saturated on the 2.4GHz and the 5GHz bands. Which of the following wireless standards should the network technician implement?

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

Answer: B

Explanation:
* 802.11 ax is the latest wireless standard that operates in both the 2.4GHz and the 5GHz bands. It offers higher throughput, lower latency, and improved efficiency compared to previous standards. It also uses technologies such as OFDMA and MU-MIMO to reduce interference and increase capacity in dense environments. Therefore, 802.11 ax is the best choice for a wireless network in an office building with high saturation on both bands. References
? Part 3 of current page talks about the benefits of 802.11 ax and how it improves network performance in congested areas1.
? CompTIA Network+ N10-008 Exam Cram covers the wireless standards and their characteristics in Chapter 5. It also provides practice questions and explanations for the exam.

NEW QUESTION 348
- (Topic 3)
A network administrator needs to configure a server to use the most accurate NTP reference available. Which of the following NTP devices should the administrator select?

A. Stratum 1
B. Stratum 2
C. Stratum 3
D. Stratum 4

Answer: A

Explanation:
Stratum 1 devices are the most accurate ntp time sources accessible via a network connection. A Stratum 1 device would normally be synchronised via a Stratum 0 reference clock.
Reference: https://endruntechnologies.com/products/ntp-time-servers/stratum1

NEW QUESTION 353
- (Topic 3)
A user is tricked into providing log-in credentials to an attacker over the telephone. Which of the following attacks is this an example of?

A. Shoulder surfing
B. Tailgating
C. Phishing
D. Dumpster diving

Answer: C

Explanation:
Phishing is a type of social engineering attack that uses email, phone, SMS, or other forms of personal communication to trick users into revealing sensitive information, such as log-in credentials, to an attacker. In this case, the user was deceived by a phone call that pretended to be from a legitimate source and asked for their log-in details.

NEW QUESTION 354
- (Topic 3)
Which of the following demarcation connections would be MOST appropriate to use with a cable modem being installed in a SOHO situation?

A. RG6
B. Cat 6
C. RJ11
D. Multimode fiber

Answer: A

Explanation:
RG6 is a type of coaxial cable that is commonly used for cable TV and internet services. A cable modem is a device that modulates and demodulates signals over a coaxial cable network to provide broadband internet access. A SOHO situation refers to a small office/home office environment that typically has a single cable modem connected to a single coaxial cable outlet. Therefore, RG6 is the most appropriate demarcation connection for a cable modem in a SOHO situation. References: [CompTIA Network+ Certification Exam Objectives], What Is RG6 Cable? | Techwalla

NEW QUESTION 356
......