ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

A client wants to increase overall security after a recent breach. Which of the following would be best to implement? (Select two.)

A. Least privilege network access
B. Dynamic inventeries
C. Central policy management
D. Zero-touch provisioning
E. Configuration drift prevention
F. Subnet range limits

Answer: A,C

Explanation:

To increase overall security after a recent breach, implementing least privilege network access and central policy management are effective strategies.

Least Privilege Network Access: This principle ensures that users and devices are granted only the access necessary to perform their functions, minimizing the potential for unauthorized access or breaches. By limiting permissions, the risk of an attacker gaining access to critical parts of the network is reduced.

Central Policy Management: Centralized management of security policies allows for consistent and streamlined implementation of security measures across the entire network. This helps in quickly responding to security incidents, ensuring compliance with security protocols, and reducing the chances of misconfigurations.

Network Reference:

CompTIA Network+ N10-007 Official Certification Guide: Discusses network security principles, including least privilege and policy management.

Cisco Networking Academy: Provides training on implementing security policies and access controls. Network+ Certification All-in-One Exam Guide: Covers strategies for enhancing network security and managing policies effectively.

Question: 2

A network administrator needs to connect two routers in a point-to-point configuration and conserve IP space. Which of the following subnets should the administrator use?

A. 724
B. /26
C. /28
D. /30

Answer: D

Explanation:

Using a /30 subnet mask is the most efficient way to conserve IP space for a point-to-point connection between two routers. A /30 subnet provides four IP addresses, two of which can be assigned to the router interfaces, one for the network address, and one for the broadcast address. This makes it ideal for point-to-point links where only two usable IP addresses are needed.Reference: CompTIA Network+ study materials and subnetting principles.

Question: 3

A network administrator determines that some switch ports have more errors present than expected. The administrator traces the cabling associated with these ports. Which of the following would most likely be causing the errors?

A. arp
B. tracert
C. nmap
D. ipconfig

Answer: D

Explanation:

Question: 4

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

A. Dig
B. Nmap
C. Tracert
D. nslookup

Answer: B

Explanation:

Nmap (Network Mapper) is a powerful network scanning tool used to discover hosts and services on a computer network. It can be used to identify which ports are open on a remote server, which can help diagnose access issues to services like a remote file server.

Port Scanning: Nmap can perform comprehensive port scans to determine which ports are open and what services are running on those ports.

Network Discovery: It provides detailed information about the host's operating system, service versions, and network configuration.

Security Audits: Besides troubleshooting, Nmap is also used for security auditing and identifying potential vulnerabilities.

Network Reference:

CompTIA Network+ N10-007 Official Certification Guide: Covers network scanning tools and their uses.

Nmap Documentation: Official documentation provides extensive details on how to use Nmap for port scanning and network diagnostics.

Network+ Certification All-in-One Exam Guide: Discusses various network utilities, including Nmap, and their applications in network troubleshooting.

Question: 5

Which of the following allows for the interception of traffic between the source and destination?

A. Self-signed certificate
B. VLAN hopping
C. On-path attack
D. Phishing

Answer: C

Explanation:

An on-path attack (formerly known as a man-in-the-middle (MITM) attack) involves intercepting and potentially altering communications between two parties without their knowledge. This can be done via techniques like ARP poisoning, rogue access points, or SSL stripping.

Breakdown of Options:

A . Self-signed certificate – These are untrusted SSL certificates but do not intercept traffic.

B . VLAN hopping – VLAN hopping exploits VLAN misconfigurations but does not necessarily intercept communications.

C . On-path attack – Correct answer. This intercepts and modifies traffic between two endpoints.

D . Phishing – Phishing tricks users into revealing credentials rather than intercepting network traffic.

Reference:

CompTIA Network+ (N10-009) Official Study Guide – Domain 3.2: Explain common security concepts. NIST SP 800-115: Guide to Security Testing and Assessments

Question: 6

A network technician is terminating a cable to a fiber patch panel in the MDF. Which of the following connector types is most likely in use?

A. F-type
B. RJ11

C. BNC
D. SC

Answer: D

Explanation:

In a fiber patch panel, the SC (Subscriber Connector or Standard Connector) is commonly used because of its push-pull design and reliability in enterprise environments.

Breakdown of Options:

A . F-type – Used for coaxial cables (e.g., cable TV), not fiber.

B . RJ11 – Used for telephone lines, not fiber.

C . BNC – Used for coaxial connections, not fiber.

D . SC – Q Correct answer. A standard fiber optic connector used in patch panels.

Reference:

CompTIA Network+ (N10-009) Official Study Guide – Domain 1.1: Compare and contrast physical network connectors.

Question: 7

A network administrator is planning to implement device monitoring to enhance network visibility. The security that the solution provides authentication and encryption. Which of the following meets these requirements?

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

Answer: D

Explanation:

SNMPv3 (Simple Network Management Protocol version 3) provides device monitoring with authentication and encryption. This enhances network visibility and security by ensuring that monitoring data is securely transmitted and access to network devices is authenticated. Authentication: SNMPv3 includes robust mechanisms for authenticating users accessing network devices.

Encryption: It provides encryption to protect the integrity and confidentiality of the data being transmitted.

Network Management: SNMPv3 allows for detailed monitoring and management of network devices, ensuring better control and security.

Network Reference:

CompTIA Network+ N10-007 Official Certification Guide: Covers SNMP versions, their features, and security enhancements in SNMPv3.

Cisco Networking Academy: Provides training on implementing and securing SNMP for network

management.

Network+ Certification All-in-One Exam Guide: Explains the benefits and security features of SNMPv3 for network monitoring.

Question: 8

A network engineer is designing a secure communication link between two sites. The entire data stream needs to remain confidential. Which of the following will achieve this goal?

A. GRE
B. IKE
C. ESP
D. AH

Answer: C

Explanation:

Definition of ESP (Encapsulating Security Payload):

ESP is a part of the IPsec protocol suite designed to provide confidentiality, integrity, and authenticity of data by encrypting the payload and optional ESP trailer.

Ensuring Confidentiality:

Encryption: ESP encrypts the payload, ensuring that the data remains confidential during transmission. Only authorized parties with the correct decryption keys can access the data.

Modes of Operation: ESP can operate in transport mode (encrypts only the payload) or tunnel mode (encrypts the entire IP packet), both providing strong encryption to secure data between sites.

Comparison with Other Protocols:

GRE (Generic Routing Encapsulation): A tunneling protocol that does not provide encryption or security features.

IKE (Internet Key Exchange): A protocol used to set up a secure, authenticated communications channel, but it does not encrypt the data itself.

AH (Authentication Header): Provides integrity and authentication for IP packets but does not encrypt the payload.

Implementation:

Use ESP as part of an IPsec VPN configuration to encrypt and secure communication between two sites. This involves setting up IPsec policies and ensuring both endpoints are configured to use ESP for data encryption.

Reference:

CompTIA Network+ study materials on IPsec and secure communication protocols.

Question: 9

Which of the following allows a remote user to connect to the network?

A. Command-line interface

B. API gateway
C. Client-to-site VPN
D. Jump box

Answer: C

Explanation:

A Client-to-Site VPN allows a remote user to securely connect to a company's internal network, providing access as if they were physically on-site.

Question: 10

Following a fire in a data center, the cabling was replaced. Soon after, an administrator notices network issues. Which of the following are the most likely causes of the network issues? (Select two).

A. The switches are not the correct voltage.
B. The HVAC system was not verified as fully functional after the fire.
C. The VLAN database was not deleted before the equipment was brought back online.
D. The RJ45 cables were replaced with unshielded cables.
E. The wrong transceiver type was used for the new termination.
F. The new RJ45 cables are a higher category than the old ones.

Answer: D,E

Explanation:

Unshielded cables (D) are more prone to interference and may not be suitable for certain environments, especially after a fire where interference could be heightened.
Using the wrong transceiver (E) for new terminations can lead to compatibility issues, causing network failures.

Question: 11

Which of the following could provide a lightweight and private connection to a remote box?

A. Site-to-site VPN
B. Telnet
C. Console
D. Secure Shell

Answer: D

Explanation:

Secure Shell (SSH) is a protocol used to securely access remote devices over an unsecured network. It provides encrypted command-line access and is a lightweight and secure method of remote administration.

A . Site-to-site VPN connects entire networks, not just a single host.

B . Telnet is not secure; it transmits data (including credentials) in plaintext.

C . Console access is direct via serial cable, not remote.

Reference:

CompTIA Network+ N10-009 Official Objectives: 2.6 – Configure and troubleshoot remote access.

Question: 12

A network technician is troubleshooting network latency and has determined the issue to be occuring two network switches(Switch10 and Switch11). Symptoms reported included poor video performance and slow file copying. Given the following informtion:

Mfcfr 1 -■ 'r-2* .-----....';].up .|.

Kit itca ^Hf __:rrl 1 ;c !_._ '.UTJJ. '

?'\] 'v "■■ irrst* ?^'^+" ry--- ■ r;-^, 5 IT""

_sj_. LiZkELi J-LL-'., = 7^iS=4 ^.'1EE, . ___'_j. . ^^.'13

Swrt.17111 'n>: ■ J - nt.r- fa - --' UUTJl

ETO 1L.. crws, rpu-1 A^K \e J ; t _htL? ■'LniJl.

1912$ ftnlnu? inpol$_r$ ^VU^M byla>$_r$ ft rjAba, J"^ $_{rl}$ jn^1 i

I2s1A tartet: o-mt, 2J?tf4 1 *•/"!, . nnrs$_r$ _ slants

Which of the following should the technician most likely do to resolve the issue?

A. Disable automatic negotiation on Switch11.
B. Modify Switch10 MTU value to 1500.
C. Configure STP on both switches.
D. Change the native VLAN on the ports.

Answer: B

Explanation:

Question: 13

Which of the following network devices converts wireless signals to electronic signals?

A. Router
B. Firewall
C. Access point
D. Load balancer

Answer: C

Explanation:

Role of an Access Point (AP):

Wireless to Wired Conversion: An access point (AP) is a device that allows wireless devices to connect to a wired network using Wi-Fi. It converts wireless signals (radio waves) into electronic signals that can be understood by wired network devices.

Functionality:

Signal Conversion: The AP receives wireless signals from devices such as laptops, smartphones, and tablets, converts them into electronic signals, and transmits them over the wired network.

Connectivity: APs provide a bridge between wireless and wired segments of the network, enabling seamless communication.

Comparison with Other Devices:

Router: Directs traffic between different networks and may include built-in AP functionality but is not primarily responsible for converting wireless to electronic signals.

Firewall: Protects the network by controlling incoming and outgoing traffic based on security rules, not involved in signal conversion.

Load Balancer: Distributes network or application traffic across multiple servers to ensure reliability and performance, not involved in signal conversion.

Deployment:

APs are commonly used in environments where wireless connectivity is needed, such as offices, homes, and public spaces. They enhance mobility and provide flexible network access.

Reference:

CompTIA Network+ study materials on wireless networking and access points.

Question: 14

Which of the following disaster recovery metrics is used to describe the amount of data that is lost since the last backup?

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

Answer: C

Explanation:

Definition of RPO:

Recovery Point Objective (RPO) is a disaster recovery metric that describes the maximum acceptable amount of data loss measured in time. It indicates the point in time to which data must be recovered to resume normal operations after a disaster.

For example, if the RPO is set to 24 hours, then the business could tolerate losing up to 24 hours' worth of data in the event of a disruption.

Why RPO is Important:

RPO is critical for determining backup frequency and helps businesses decide how often they need to back up their data. A lower RPO means more frequent backups and less potential data loss.

Comparison with Other Metrics:

MTTR (Mean Time to Repair): Refers to the average time required to repair a system or component and return it to normal operation.

RTO (Recovery Time Objective): The maximum acceptable length of time that a computer, system, network, or application can be down after a failure or disaster occurs.

MTBF (Mean Time Between Failures): The predicted elapsed time between inherent failures of a system during operation.

How RPO is Used in Disaster Recovery:

Organizations establish RPOs to ensure that they can recover data within a timeframe that is acceptable to business operations. This involves creating a backup plan that meets the RPO requirements.

Reference:

CompTIA Network+ study materials and certification guides.

Question: 15

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:

Definition of Fiber Connector Types:

LC (Lucent Connector): A small form-factor fiber optic connector with a push-pull latching mechanism, commonly used for high-density applications.

SC (Subscriber Connector or Standard Connector): A larger form-factor connector with a push-pull latching mechanism, often used in datacom and telecom applications.

ST (Straight Tip): A bayonet-style connector, typically used in multimode fiber optic networks.

MPO (Multi-fiber Push On): A connector designed to support multiple fibers (typically 12 or 24 fibers), used in high-density cabling environments.

Common Usage:

LC Connectors: Due to their small size, LC connectors are widely used in network interface cards (NICs) and high-density environments such as data centers. They allow for more connections in a smaller space compared to SC and ST connectors.

SC and ST Connectors: These are larger and more commonly used in patch panels and older fiber installations but are less suitable for high-density applications.

MPO Connectors: Primarily used for trunk cables in data centers and high-density applications but not typically on individual network interface cards.

Selection Criteria:

The small form-factor and high-density capabilities of LC connectors make them the preferred choice for network interface cards, where space and connection density are critical considerations.

Reference:
CompTIA Network+ study materials on fiber optics and connector types.

Question: 16

A network administrator wants to implement security zones in the corporate network to control access to only individuals inside of the corporation. Which of the following security zones is the best solution?

A. Extranet
B. Trusted
C. VPN
D. Public

Answer: B

Explanation:

Introduction to Security Zones:
Security zones are logical segments within a network designed to enforce security policies and control access. They help in segregating and securing different parts of the network.
Types of Security Zones:
Trusted Zone: This is the most secure zone, typically used for internal corporate networks where only trusted users have access.
Extranet: This zone allows controlled access to external partners, vendors, or customers.
VPN (Virtual Private Network): While VPNs are used to create secure connections over the internet, they are not a security zone themselves.
Public Zone: This zone is the least secure and is typically used for public-facing services accessible by anyone.
Trusted Zone Implementation:
The trusted zone is configured to include internal corporate users and resources. Access controls, firewalls, and other security measures ensure that only authorized personnel can access this zone. Internal network segments, such as the finance department, HR, and other critical functions, are usually placed in the trusted zone.
Example Configuration:
Firewall Rules: Set up rules to allow traffic only from internal IP addresses.
Access Control Lists (ACLs): Implement ACLs on routers and switches to restrict access based on IP addresses and other criteria.
Segmentation: Use VLANs and subnetting to segment and isolate the trusted zone from other zones.
Explanation of the Options:
A . Extranet: Suitable for external partners, not for internal-only access.
B . Trusted: The correct answer, as it provides controlled access to internal corporate users.
C . VPN: A method for secure remote access, not a security zone itself.
D . Public: Suitable for public access, not for internal corporate users.
Conclusion:
Implementing a trusted zone is the best solution for controlling access within a corporate network. It ensures that only trusted internal users can access sensitive resources, enhancing network security. Reference:
CompTIA Network+ guide detailing security zones and their implementation in a corporate network (see

page Ref 9†Basic Configuration Commands).

Question: 17

Which of the following attacks can cause users who are attempting to access a company website to be directed to an entirely different website?

A. DNS poisoning
B. Denial-of-service
C. Social engineering
D. ARP spoofing

Answer: A

Explanation:

Network segmentation involves dividing a network into smaller segments or subnets. This is particularly important when integrating OT (Operational Technology) devices to ensure that these devices are isolated from other parts of the network. Segmentation helps protect the OT devices from potential threats and minimizes the impact of any security incidents. It also helps manage traffic and improves overall network performance.Reference: CompTIA Network+ study materials.

Question: 18

A network administrator is troubleshooting issues with a DHCP server at a university. More students have recently arrived on campus, and the users are unable to obtain an IP address. Which of the

following should the administrator do to address the issue?

A. Enable IP helper.
B. Change the subnet mask.
C. Increase the scope size.
D. Add address exclusions.

Answer: C

Explanation:

The issue is that more students have arrived on campus, meaning the available IP addresses are exhausted. To fix this, the administrator should increase the DHCP scope size to allow more devices to obtain IP addresses.

Breakdown of Options:

A . Enable IP helper – IP helper is used to forward DHCP requests across different subnets. However, the problem here is that the DHCP scope is full, not that requests are not reaching the server.

B . Change the subnet mask – The subnet mask determines the number of available hosts, but changing it without increasing the IP pool does not help.

C . Increase the scope size – Correct answer. Expanding the DHCP scope provides more IP addresses for assignment.

D . Add address exclusions – Exclusions reserve IP addresses, which would further reduce available addresses instead of solving the issue.

Reference:

CompTIA Network+ (N10-009) Official Study Guide – Domain 2.4: Compare and contrast IP addressing schemes.

RFC 2131: Dynamic Host Configuration Protocol (DHCP)

Question: 19

SIMULATION

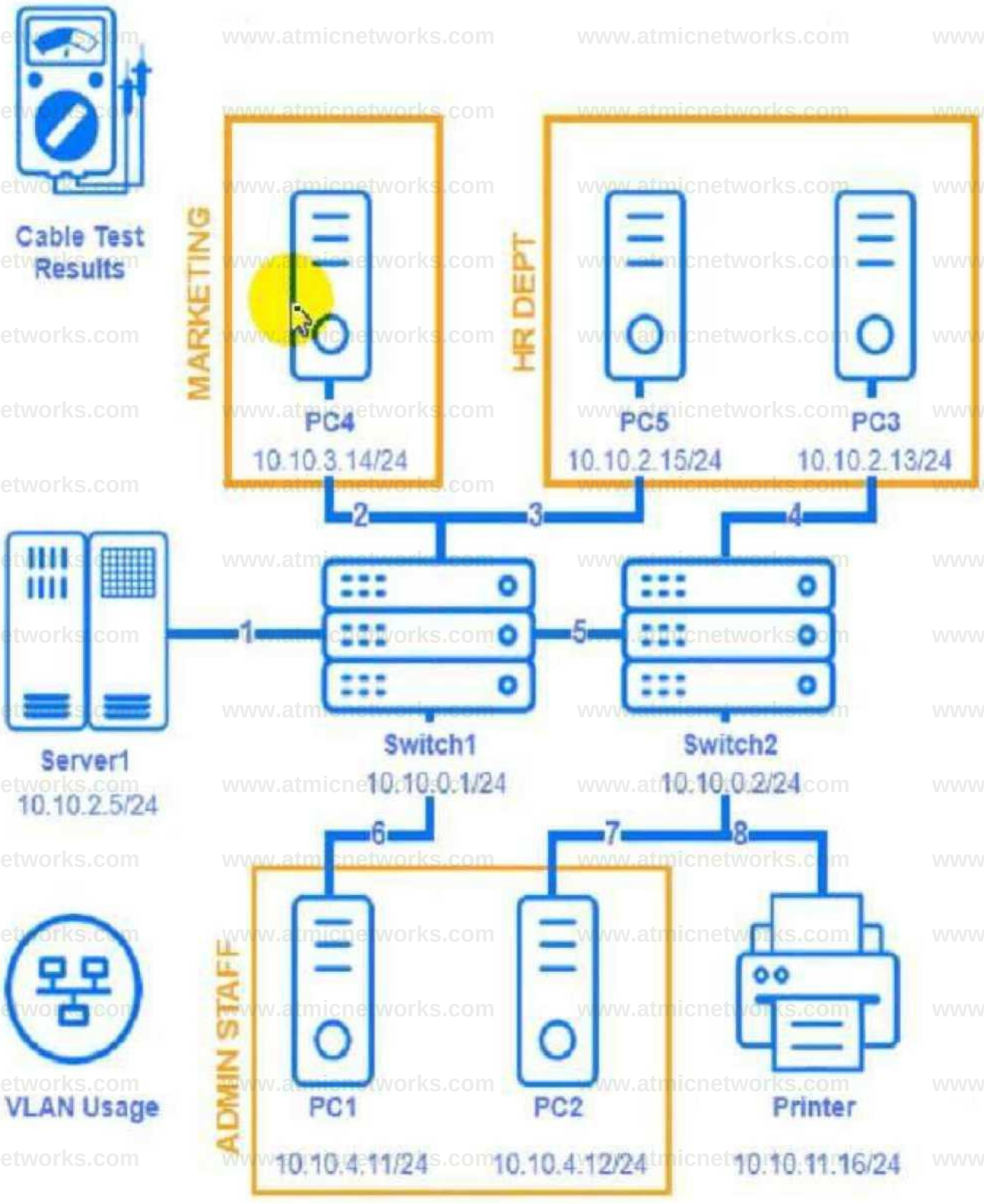
A network technician needs to resolve some issues with a customer's SOHO network.

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.



Cable Test Results:

Cable 1:

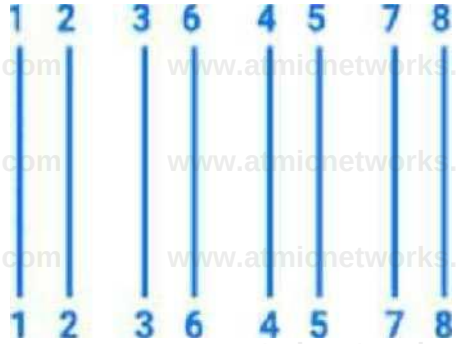
Cable 1 Cable 2 Cable 3 Cable 4 Cable 5 Cable 6 Cable 7 Cable 8

Length 22M

VLAN VLAN 2

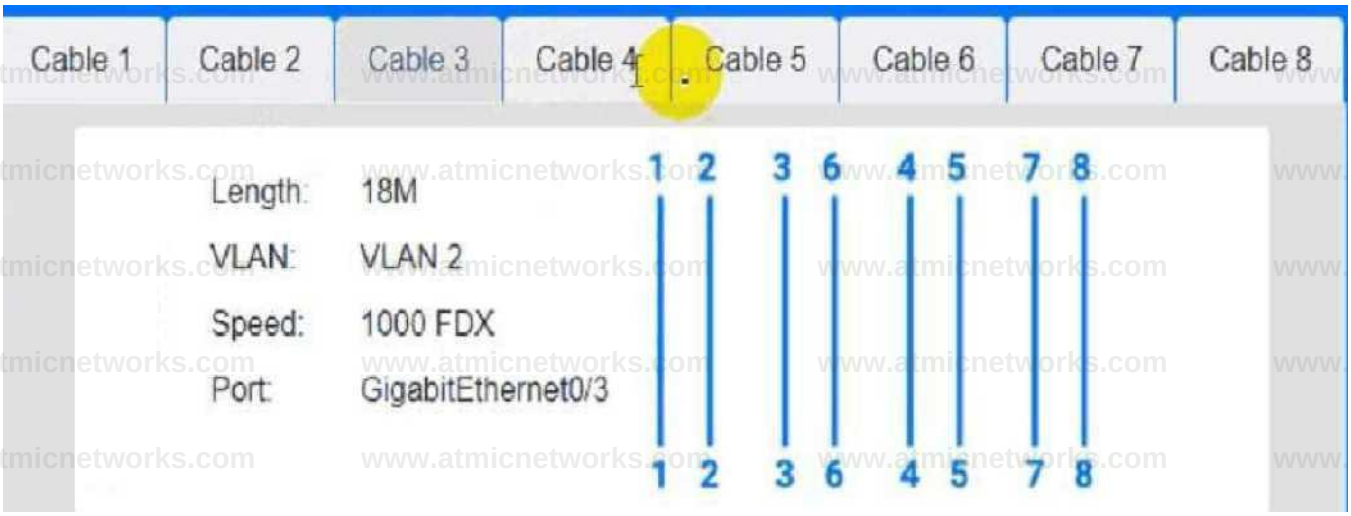
Speed: 1000 FDX

Port: GigabitEthernetO/1

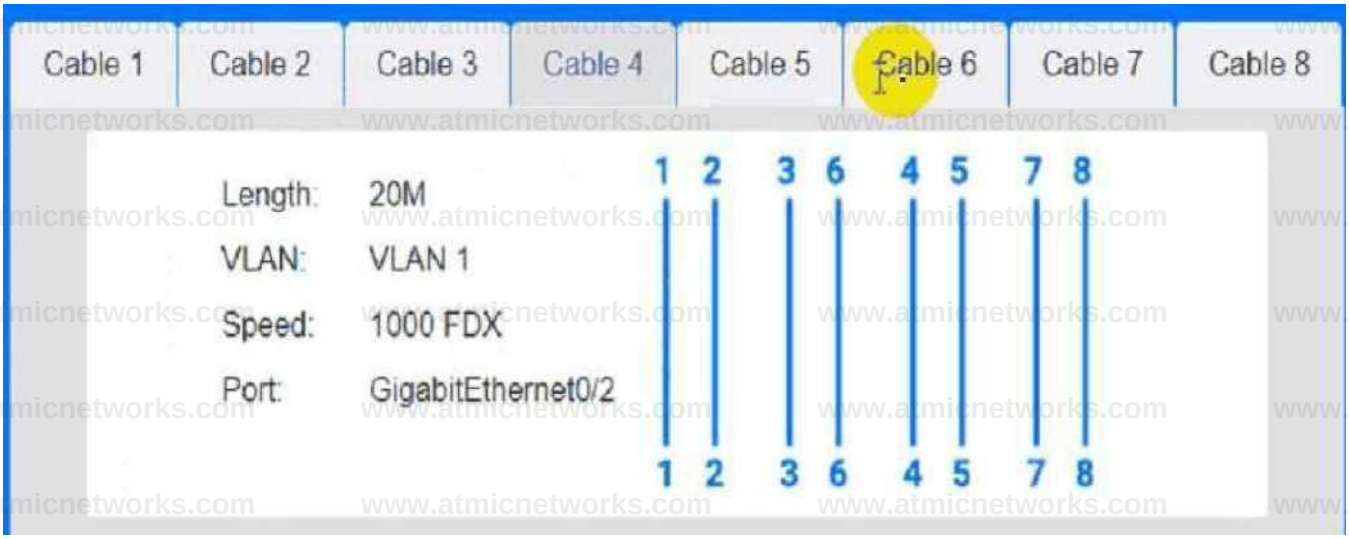


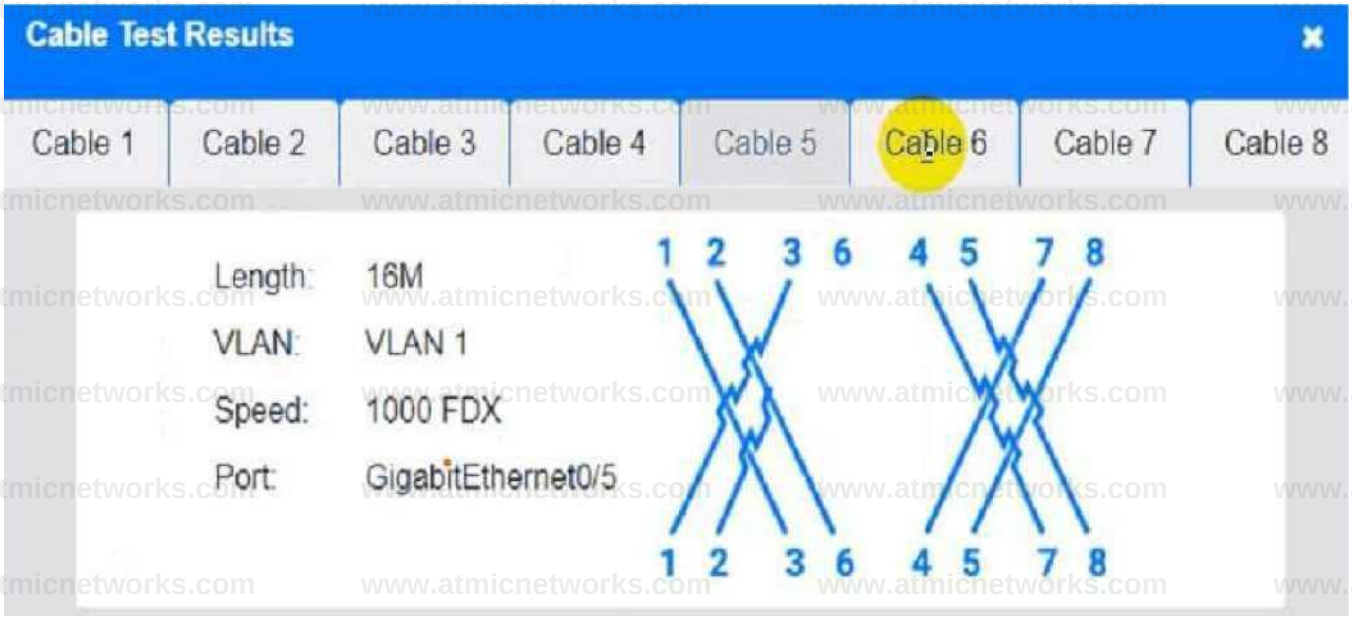
Cable 2:

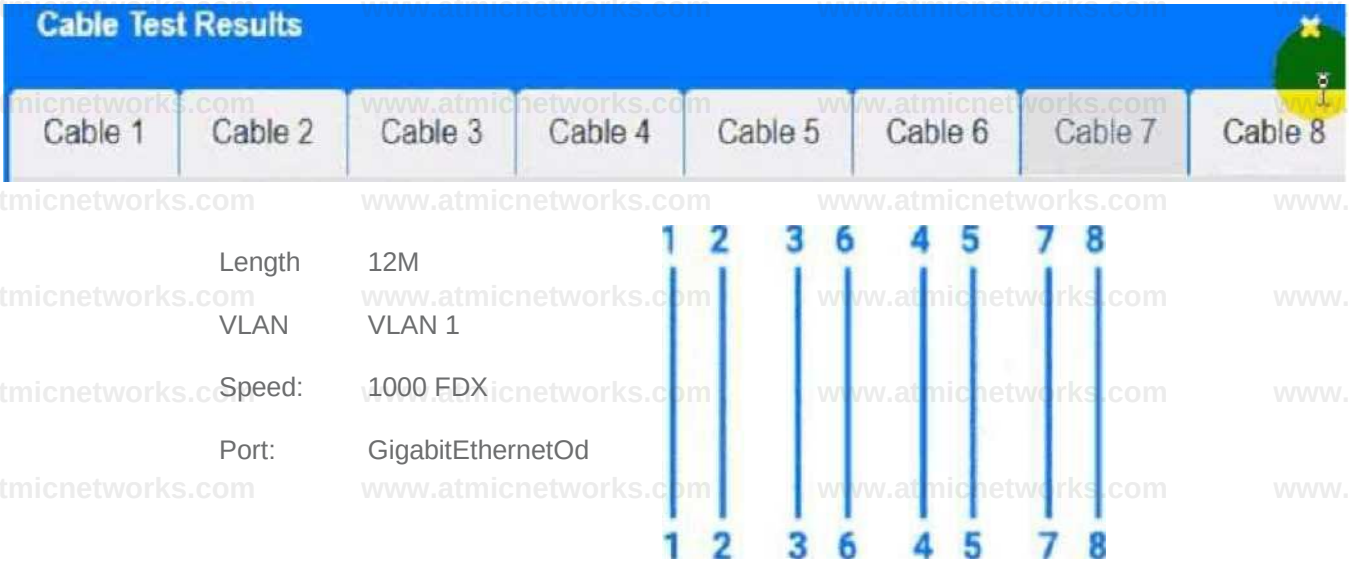
Cable 3:



Cable 4:







Printer

HP Network Configuration Page

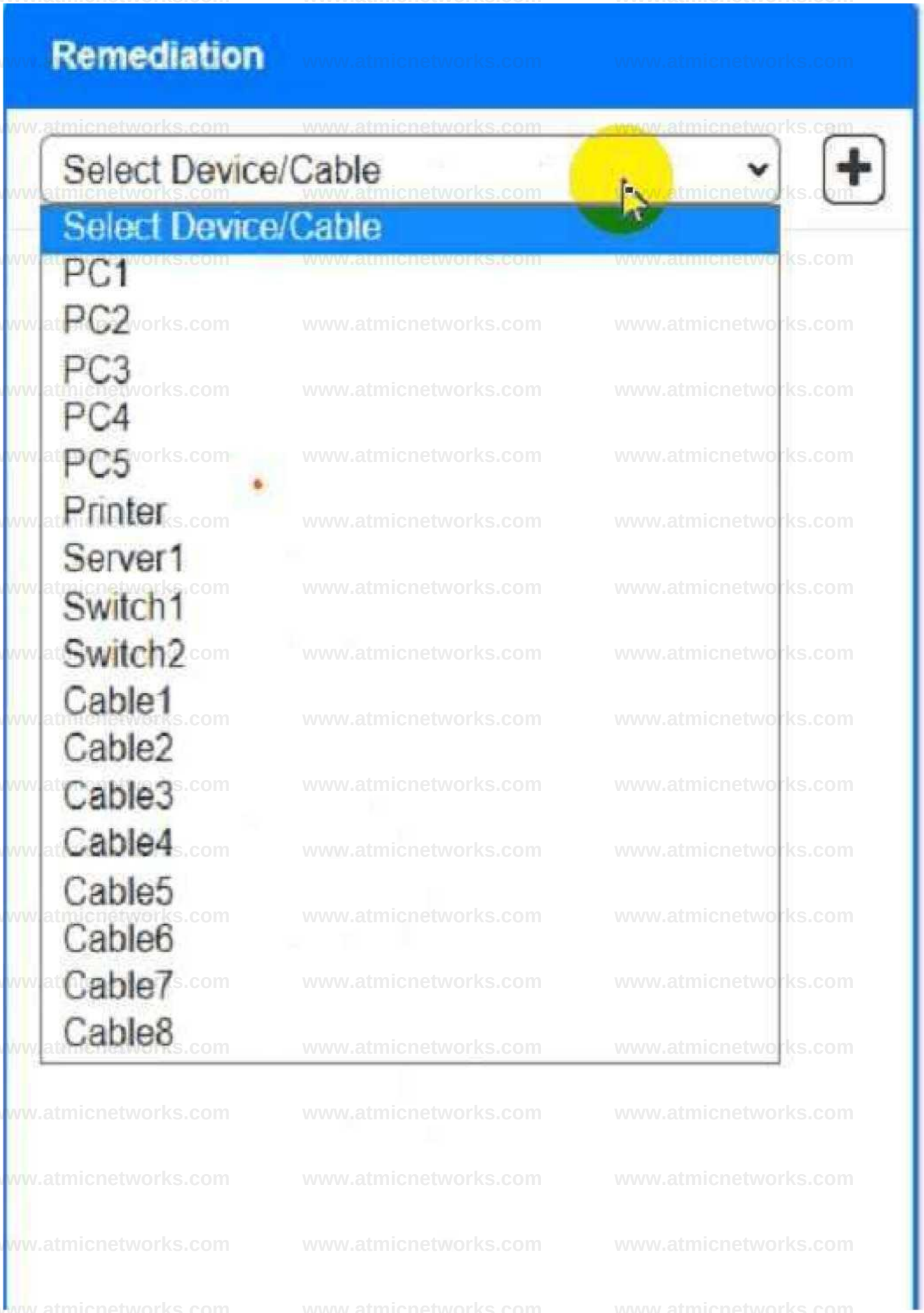
Model HP Officejet Pro 8610

General Information

Network Status	Ready
Active Connection Type	Wired
URL(s) for Embedded Web Server http //HP4D30EC http //192.168 2 9	
Firmware Revision	FDP1CN1347AI\
Hostname	HP4D30EC
Serial Number	CN3AO1KG42
Internet	Not Connected

802.3 Wired

Hardware Address (MAC)	9cb6 54 4d 30 ec



Answer: See the Explanation for detailed information on this simulation.

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.

Question: 20

A network administrator is connecting two Layer 2 switches in a network. These switches must transfer data in multiple networks. Which of the following would fulfill this requirement?

A. Jumbo frames
B. 802.1Q tagging

C. Native VLAN
D. Link aggregation

Answer: B

Explanation:

802.1 Q tagging, also known as VLAN tagging, is used to identify VLANs on a trunk link between switches. This allows the switches to transfer data for multiple VLANs (or networks) over a single physical connection. This method ensures that traffic from different VLANs is properly separated and managed across the network.Reference: CompTIA Network+ study materials.

Question: 21

Network administrators are using the Telnet protocol to administer network devices that are on the 192.168.1.0/24 subnet. Which of the following tools should the administrator use to best identify the devices?

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

Answer: B

Explanation:

nmap (Network Mapper) is the best tool in this scenario. It can scan the 192.168.1.0/24 subnet to discover live hosts, open ports (like Telnet on port 23), and device types. It's ideal for mapping and auditing the network.
A . dig is a DNS lookup tool; not useful for identifying hosts on a subnet.
C . tracert shows the path packets take to a destination, not for host discovery.
D . telnet is the protocol being used, not a tool for scanning or identifying devices.
Reference:
CompTIA Network+ N10-009 Official Objectives: 5.1 – Given a scenario, use the appropriate network troubleshooting tools.

Question: 22

Two companies successfully merged. Following the merger, a network administrator identified a

connection bottleneck. The newly formed company plans to acquire a high-end 40GB switch and redesign the network from a three-tier model to a collapsed core. Which of the following should the administrator do until the new devices are acquired?

A. Implement the FHRP.
B. Configure a route selection metric change.

C. Install a load balancer.
D. Enable link aggregation.

Answer: D

Explanation:

- The issue described is a network bottleneck due to increased traffic after a merger.
- A collapsed core architecture consolidates the core and distribution layers into a single layer to improve efficiency and reduce latency.
- Until the 40GB switch is acquired, Link Aggregation (LAG) (IEEE 802.3ad / LACP) can be used to combine multiple physical links into a single logical link, increasing bandwidth and reducing bottlenecks.
- FHRP (First Hop Redundancy Protocol) (A) is used for gateway redundancy, not link aggregation.
- Route selection metric changes (B) help with routing decisions but don't address physical link congestion.
- Load balancers (C) distribute traffic for applications, not network links.

Reference: CompTIA Network+ N10-009 Official Documentation – Network Architecture and Performance Optimization.

Question: 23

Which of the following most likely requires the use of subinterfaces?

A. A router with only one available LAN port
B. A firewall performing deep packet inspection
C. A hub utilizing jumbo frames
D. A switch using Spanning Tree Protocol

Answer: A

Explanation:

Introduction to Subinterfaces:

Subinterfaces are logical interfaces created on a single physical interface. They are used to enable a router to support multiple networks on a single physical interface.

Use Case for Subinterfaces:

Subinterfaces are commonly used in scenarios where VLANs are implemented. A router with a single physical LAN port can be configured with multiple subinterfaces, each associated with a different VLAN.

This setup allows the router to route traffic between different VLANs.

Example Configuration:

Consider a router with a single physical interface GigabitEthernet0/0 and two VLANs, 10 and 20.

```
interface GigabitEthernet0/0.10
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.0 !
interface GigabitEthernet0/0.20
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.0
```

The encapsulation dot1Q command specifies the VLAN ID.

Explanation of the Options:

A . A router with only one available LAN port: This is correct. Subinterfaces allow a single physical interface to manage multiple networks, making it essential for routers with limited physical interfaces.

B . A firewall performing deep packet inspection: Firewalls can use subinterfaces, but it is not a requirement for deep packet inspection.

C . A hub utilizing jumbo frames: Hubs do not use subinterfaces as they operate at Layer 1 and do not manage IP addressing.

D . A switch using Spanning Tree Protocol: STP is a protocol for preventing loops in a network and does not require subinterfaces.

Conclusion:

Subinterfaces provide a practical solution for routing between multiple VLANs on a router with limited physical interfaces. They allow network administrators to optimize the use of available hardware resources efficiently.

Reference:

CompTIA Network+ guide detailing VLAN configurations and the use of subinterfaces (see page Ref 9†Basic Configuration Commands).

Question: 24

A network engineer is completing a new VoIP installation, but the phones cannot find the TFTP server to download the configuration files. Which of the following DHCP features would help the phone reach the TFTP server?

A. Exclusions
B. Lease time
C. Options
D. Scope

Answer: C

Explanation:

DHCP Options: DHCP options allow additional configuration parameters, such as the address of a TFTP server, to be provided to clients during the DHCP lease process. This is essential for VoIP phones
to locate the server for configuration files.

Exclusions (A): Prevents certain IP addresses from being assigned by DHCP but does not direct devices to servers.

Lease time (B): Determines how long an IP address is assigned but does not impact TFTP settings. Scope (D): Defines a range of IP addresses but does not include additional server information.

Reference: CompTIA Network+ Official Study Guide, Domain 1.3 (DHCP Configuration).

Question: 25

A network administrator performed upgrades on a server and installed a new NIC to improve performance. Following the upgrades, usera are unable to reach the server. Which of the following is the most likely reason.

A. The PoE power budget was exceeded.
B. TX/RX was transposed.

C. A port security violation occured.
D. An incorrect cable type was installed.

Answer: D

Explanation:

When a network administrator installs a new Network Interface Card (NIC) and users are unable to reach the server, one of the common issues is the use of an incorrect cable type. Network cables must match the specifications required by the NIC and the network infrastructure (e.g., Cat5e, Cat6 for Ethernet).

NIC Compatibility: The new NIC might require a specific type of cable to function properly. Using a cable not rated for the NIC's required speeds or capabilities can result in connectivity issues. Cable Standards: Different NICs and network devices might need different cabling standards (straight-through vs. crossover cables, or specific fiber optic types).

Connection Types: Ensuring that the cable connectors are appropriate for the NIC ports (e.g., RJ45 for Ethernet, LC connectors for fiber optics).

Network Reference:

CompTIA Network+ N10-007 Official Certification Guide: Discusses network cabling standards and NIC specifications.

Cisco Networking Academy: Provides insights into cabling and NIC configurations for optimal network performance.

Network+ Certification All-in-One Exam Guide: Offers comprehensive details on troubleshooting network connectivity issues, including cabling problems.

Question: 26

A support agent receives a report that a remote user's wired devices are constantly disconnecting and have slow speeds. Upon inspection, the support agent sees that the user's coaxial modern has a signal power of -97dB.

A. Removing any spliters connecte to the line
B. Switching the devices to wireless
C. Moving the devices closer to the modern
D. Lowering the network speed

Answer: A

Explanation:

A signal power of -97dB indicates a very weak signal, which can cause connectivity issues and slow speeds. Splitters on a coaxial line can degrade the signal quality further, so removing them can help improve the signal strength and overall connection quality.

Signal Quality: Splitters can reduce the signal strength by dividing the signal among multiple lines, which can be detrimental when the signal is already weak.

Direct Connection: Ensuring a direct connection from the modem to the incoming line can maximize signal quality and reduce potential points of failure.

Network Reference:

CompTIA Network+ N10-007 Official Certification Guide: Discusses troubleshooting connectivity issues and the impact of signal strength on network performance.

Cisco Networking Academy: Provides insights on maintaining optimal signal quality in network setups.

Network+ Certification All-in-One Exam Guide: Covers common network issues, including those related to signal degradation and ways to mitigate them.

Question: 27

A company experiences an incident involving a user who connects an unmanaged switch to the network. Which of the following technologies should the company implement to help avoid similar incidents without conducting an asset inventory?

A. Screened subnet
B. 802.1X
C. MAC filtering
D. Port security

Answer: D

Explanation:

Port security is a Layer 2 security feature that restricts the number of devices connecting to a network switch port. It helps prevent unauthorized devices, such as an unmanaged switch, from being connected to the network.

How Port Security Works:

Limits the number of MAC addresses that can connect to a port.

Can shut down or restrict the port if an unauthorized device is detected.

Prevents users from plugging in unauthorized networking equipment (e.g., unmanaged switches, hubs).

Incorrect Options:

A . Screened Subnet: A screened subnet (DMZ) is used for isolating external-facing servers, not for controlling unauthorized network connections.

B . 802.1X: Provides authentication for devices but requires a RADIUS server, which is a more complex solution than port security.

C . MAC Filtering: Controls which MAC addresses can connect but is difficult to manage and can be spoofed.

Reference:

CompTIA Network+ N10-009 Official Study Guide – Chapter on Network Security Controls

Question: 28

Which of the following technologies are X.509 certificates most commonly associated with?

A. PKI
B. VLAN tagging
C. LDAP
D. MFA

Answer: A

Explanation:

X.509 certificates are most commonly associated with Public Key Infrastructure (PKI). These certificates are used for a variety of security functions, including digital signatures, encryption, and authentication.

PKI: X.509 certificates are a fundamental component of PKI, used to manage encryption keys and authenticate users and devices.

Digital Certificates: They are used to establish secure communications over networks, such as SSL/TLS for websites and secure email communication.

Authentication and Encryption: X.509 certificates provide the means to securely exchange keys and verify identities in various applications, ensuring data integrity and confidentiality.

Network Reference:

CompTIA Network+ N10-007 Official Certification Guide: Covers PKI and the role of X.509 certificates in network security.

Cisco Networking Academy: Provides training on PKI, certificates, and secure communications. Network+ Certification All-in-One Exam Guide: Explains PKI, X.509 certificates, and their applications in securing network communications.

Question: 29

A help desk technician receives a report that users cannot access internet URLs. The technician performs ping tests and finds that sites fail when a URL is used but succeed when an IP is used. Which of the following tools should the technician utilize next?

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

Answer: D

Explanation:

The issue is clearly related to DNS resolution, as IP-based connections succeed but domain namebased ones fail.

E. dig (Domain Information Groper) is a DNS lookup tool used to troubleshoot DNS problems by querying name servers directly.

Other tools are less relevant here:

A . tcpdump is a packet analyzer and is more advanced for deeper traffic analysis.

B . tracert is used to trace the route to a destination, not ideal for DNS issues.

C . nmap is a port scanner and network mapper, not for resolving DNS problems.

Reference:

CompTIA Network+ N10-009 Official Objectives: 5.1 – Given a scenario, use the appropriate network troubleshooting tools.

Question: 30

A network manager wants to implement a SIEM system to correlate system events. Which of the following protocols should the network manager verify?

A. NTP
B. DNS
C. LDAP
D. DHCP

Answer: A

Explanation:

Role of NTP (Network Time Protocol):
NTP is used to synchronize the clocks of network devices to a reference time source. Accurate time synchronization is critical for correlating events and logs from different systems.
Importance for SIEM Systems:
Event Correlation: SIEM (Security Information and Event Management) systems collect and analyze log data from various sources. Accurate timestamps are essential for correlating events across multiple systems.
Time Consistency: Without synchronized time, it is challenging to piece together the sequence of events during an incident, making forensic analysis difficult.
Comparison with Other Protocols:
DNS (Domain Name System): Translates domain names to IP addresses but is not related to time synchronization.
LDAP (Lightweight Directory Access Protocol): Used for directory services, such as user authentication and authorization.
DHCP (Dynamic Host Configuration Protocol): Assigns IP addresses to devices on a network but does not handle time synchronization.
Implementation:
Ensure that all network devices, servers, and endpoints are synchronized using NTP. This can be achieved by configuring devices to use an NTP server, which could be a local server or an external time source.
Reference:
CompTIA Network+ study materials on network protocols and SIEM systems.

Question: 31

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

A. Mesh
B. Ad hoc
C. Point-to-point
D. Infrastructure

Answer: A

Explanation:

A mesh network is the best solution for providing reliable wireless service to public safety vehicles. In a mesh network, each node (vehicle) can connect to multiple other nodes, providing multiple paths for data to travel. This enhances reliability and redundancy, ensuring continuous connectivity even if one or more nodes fail. Mesh networks are highly resilient and are well-suited for dynamic and mobile environments such as public safety operations.Reference: CompTIA Network+ study materials.

Question: 32

Which of the following is most likely responsible for the security and handling of personal data in Europe?

A. GDPR
B. SCADA
C. SAML
D. PCI DSS

Answer: A

Explanation:

Definition of GDPR:
General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas.
Scope and Objectives:
GDPR aims to give individuals control over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.
It enforces rules about data protection, requiring companies to protect the personal data and privacy of EU citizens for transactions that occur within EU member states.
Comparison with Other Options:
SCADA (Supervisory Control and Data Acquisition): Refers to control systems used in industrial and infrastructure processes, not related to personal data protection.
SAML (Security Assertion Markup Language): A standard for exchanging authentication and authorization data between parties, not specifically for personal data protection.
PCI DSS (Payment Card Industry Data Security Standard): A set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment, not specific to personal data protection in Europe.
Key Provisions:
GDPR includes provisions for data processing, data subject rights, obligations of data controllers and processors, and penalties for non-compliance.
Reference:
CompTIA Network+ study materials on regulatory and compliance standards.

Question: 33

A network administrator is configuring a network for a new site that will have 150 users. Within the next year, the site is expected to grow by ten users. Each user will have two IP addresses, one for a computer and one for a phone connected to the network. Which of the following classful IPv4 address ranges will be best-suited for the network?

A. Class D
B. Class B
C. Class A
D. Class C

Answer: D

Explanation:

IPv4 addresses are divided into classes:
Class A: Supports 16,777,214 hosts (large enterprises).
Class B: Supports 65,534 hosts (medium to large networks).
Class C: Supports 254 hosts (small to medium networks).
Class D: Used for multicast, not for assigning IPs to hosts.
Step-by-step Calculation:
The network will have 150 users initially, with a projected growth of 10 users, totaling 160 users.
Each user has two devices, so 160 × 2 = 320 IP addresses needed.
A Class C subnet has 254 usable IPs by default, which is not sufficient.
A Class B subnet can support thousands of hosts, making it the most appropriate option.
Incorrect Options:
A . Class D: Reserved for multicast, not for host assignments.
C . Class A: Overkill for a network of this size.
D . Class C: Cannot support 320 hosts without subnetting, making Class B the best choice.
Reference:
CompTIA Network+ N10-009 Official Study Guide – Chapter on IP Addressing and Subnetting

Question: 34

A network administrator is developing a method of device monitoring with the following requirements:

- Allows for explicit, by user, privilege management
- Includes centralized logging of changes
- Offers widely accessible remote management
- Provides support of service accounts

Which of the following will most closely meet these requirements?

A. SNMP
B. API
C. SIEM
D. SSO

Answer: B

Explanation:

- API (Application Programming Interface) enables secure and granular access control, remote management, and logging, making it ideal for network monitoring.
- SNMP (A) is mainly used for device monitoring but lacks centralized logging and user-based privilege control.
- SIEM (C) is a security monitoring tool focused on log collection, not device management.
- SSO (D) is related to authentication, not monitoring.

Reference: CompTIA Network+ N10-009 Official Documentation – Network Monitoring & Management Technologies.

Question: 35

A network administrator is unable to ping a remote server from a newly connected workstation that has been added to the network. Ping to 127.0.0.1 on the workstation is failing. Which of the following should the administrator perform to diagnose the problem?

A. Verify the NIC interface status.
B. Verify the network is not congested.
C. Verify the router is not dropping packets.
D. Verify that DNS is resolving correctly.

Answer: A

Explanation:

The failure of a ping to 127.0.0.1 (the loopback address) indicates a problem with the workstation's TCP/IP stack or network interface card (NIC). Since 127.0.0.1 is a local address, the issue is not related to the network, router, or DNS. The first step in diagnosing this issue is to verify the NIC interface status to ensure the network adapter is functioning and properly configured.

Why not Verify the network is not congested? Network congestion affects external connectivity, not the loopback address.

Why not Verify the router is not dropping packets? Router issues are irrelevant since the loopback ping fails locally.

Why not Verify that DNS is resolving correctly? DNS resolution is not involved in pinging 127.0.0.1, which uses a direct IP address.

Reference:CompTIA Network+ N10-009 Objective 5.2: Explain the troubleshooting methodology. The CompTIA Network+ Study Guide (e.g., Chapter 13: Network Troubleshooting) emphasizes that a failed loopback ping indicates a local TCP/IP stack or NIC issue, and checking the NIC status is the first diagnostic step.

Question: 36

A network engineer needs to virtualize network services, including a router at a remote branch location. Which of the following solutions meets the requirements?

A. NFV
B. VRF

C. VLAN

D. VPC

Answer: A

Explanation:

Network Functions Virtualization (NFV): NFV is a technology that virtualizes network services like routing, firewalls, and load balancers. It allows these services to run on virtual machines rather than requiring dedicated hardware. This is ideal for remote branch locations where deploying physical devices is costly and complex.

VRF (B): Virtual Routing and Forwarding is used for segmenting routing tables but does not virtualize services.

VLAN (C): Virtual Local Area Networks help segregate broadcast domains but are unrelated to virtualizing network functions.

VPC (D): Virtual Private Cloud is used for cloud computing but does not pertain to virtualizing network services.

Reference: CompTIA Network+ Official Study Guide, Domain 2.1 (Virtualization and Cloud Concepts).

Question: 37

A technician needs to set up a wireless connection that utilizes MIMO on non-overlapping channels. Which of the following would be the best choice?

A. 802.11a

B. 802.11b

C. 802.11g

D. 802.11n

Answer: D

Explanation:

The 802.11n standard supports MIMO (Multiple Input Multiple Output), which allows multiple antennas to increase data throughput and improve reliability. Additionally, it uses non-overlapping channels in the 5 GHz band (and optionally the 2.4 GHz band), making it a good choice for high-speed, interference-resistant wireless connections. (Reference: CompTIA Network+ Study Guide, Chapter on Wireless Technologies)

Question: 38

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 involves dividing a network into smaller segments or subnets. This is particularly important when integrating OT (Operational Technology) devices to ensure that these

devices are isolated from other parts of the network. Segmentation helps protect the OT devices from potential threats and minimizes the impact of any security incidents. It also helps manage traffic and improves overall network performance.Reference: CompTIA Network+ study materials.

Question: 39

A company is purchasing a 40Gbps broadband connection service from an ISP. Which of the following should most likely be configured on the 10G switch to take advantage of the new service?

A. 802.1Q tagging

B. Jumbo frames

C. Half duplex

D. Link aggregation

Answer: D

Explanation:

Since the switch supports only 10Gbps per port, achieving 40Gbps throughput requires link aggregation (LACP), which combines multiple 10Gbps links into one logical interface for higher bandwidth.

Breakdown of Options:

A . 802.1Q tagging – VLAN tagging helps segment traffic but does not increase throughput.

B . Jumbo frames – Jumbo frames reduce overhead but do not increase bandwidth.

C . Half duplex – Half duplex restricts communication, reducing performance instead of improving it. D . Link aggregation – Correct answer. LACP combines multiple 10Gbps links to provide a 40Gbps connection.

Reference:

CompTIA Network+ (N10-009) Official Study Guide – Domain 1.2: Compare and contrast network topologies and technologies.

IEEE 802.3ad: Link Aggregation Control Protocol (LACP)

Question: 40

A user connects to a corporate VPN via a web browser and is able to use TLS to access the internal financial system to input a time card. Which of the following best describes how the VPN is being used?

A. Clientless

B. Client-to-site
C. Full tunnel
D. Site-to-site

Answer: A

Explanation:

Reference: CompTIA Network+ Certification Exam Objectives - Remote Access Methods section.

Question: 41

A network administrator's device is experiencing severe Wi-Fi interference within the corporate headquarters causing the device to constantly drop off the network. Which of the following is most likely the cause of the issue?

A. Too much wireless reflection
B. Too much wireless absorption
C. Too many wireless repeaters
D. Too many client connections

Answer: A

Explanation:
Reference: CompTIA Network+ Certification Exam Objectives - Wireless Networks section.

Question: 42

A company's marketing team created a new application and would like to create a DNS record for newapplication.comptia.org that always resolves to the same address as www.comptia.org. Which of the following records should the administrator use?

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

Answer: C

Explanation:

A CNAME (Canonical Name) record is used in DNS to alias one domain name to another. This means that newapplication.comptia.org can be made to resolve to the same IP address as www.comptia.org by creating a CNAME record pointing newapplication.comptia.org to www.comptia.org. SOA (Start of Authority) is used for DNS zone information, MX (Mail Exchange) is for mail server records, and NS (Name Server) is for specifying authoritative

DNS servers.

Reference:

The DNS section of the CompTIA Network+ materials describes the use of CNAME records for creating domain aliases.

Question: 43

Which of the following would be violated if an employee accidentally deleted a customer's data?

A. Integrity
B. Confidentiality
C. Vulnerability
D. Availability

Answer: D

Explanation:

Availability refers to ensuring that data is accessible when needed. If a customer's data is accidentally deleted, it impacts availability, as the data can no longer be accessed.

Question: 44

Which of the following are the best device-hardening techniques for network security? (Select two).

A. Disabling unused ports
B. Performing regular scanning of unauthorized devices
C. Monitoring system logs for irregularities
D. Enabling logical security such as SSO
E. Changing default passwords
F. Ensuring least privilege concepts are in place

Answer: A,E

Explanation:

Disabling unused ports prevents unauthorized access and reduces the attack surface by ensuring that no inactive or unmonitored entry points are available for exploitation. Changing default passwords is critical for security because default credentials are widely known and can easily be exploited by attackers. These techniques are fundamental steps in hardening devices against unauthorized access and ensuring network security. Reference: CompTIA Network+ Exam Objectives and official study guides.

Question: 45

An administrator is setting up an SNMP server for use in the enterprise network and needs to create device IDs within a

MIB. Which of the following describes the function of a MIB?

A. DHCP relay device
B. Policy enforcement point
C. Definition file for event translation
D. Network access controller

Answer: C

Explanation:

MIB (Management Information Base): A MIB is a database used for managing the entities in a communication network. The MIB is used by Simple Network Management Protocol (SNMP) to translate events into a readable format, enabling network administrators to manage and monitor network devices effectively.
Function of MIB: MIBs contain definitions and information about all objects that can be managed on a network using SNMP. These objects are defined using a hierarchical namespace containing object identifiers (OIDs).
CompTIA Network+ materials discussing SNMP and MIB functionality.

Question: 46

Newly crimped 26ft (8m) STP Cat 6 patch cables were recently installed in one room to replace cables that were damaged by a vacuum cleaner. Now, users in that room are unable to connect to the network. A network technician tests the existing cables first. The 177ft (54m) cable that runs from the core switch to the access switch on the floor is working, as is the 115ft (35m) cable run from the access switch to the wall jack in the office. Which of the following is the most likely reason the users cannot connect to the network?

A. Mixed UTP and STP cables are being used.
B. The patch cables are not plenum rated.
C. The cable distance is exceeded.
D. An incorrect pinout on the patch cable is being used.

Answer: D

Explanation:

An incorrect pinout on the patch cable could prevent network connectivity due to mismatched wiring. Even if the cables are the correct length and type, a pinout issue can cause continuity problems and prevent data transmission. Proper crimping with the correct pinout is essential for network cables to function. (Reference: CompTIA Network+ Study Guide, Chapter on Network Media and Topologies)

Question: 47

A company's network is experiencing high latency and packet loss during peak hours. Network monitoring tools show increased traffic on a switch. Which of the following should a network technician implement to reduce the network congestion and improve performance?

A. Load balancing
B. Port mirroring
C. Quality of Service
D. Spanning Tree Protocol

Answer: C

Explanation:

Quality of Service (QoS): This is a feature used in networking to prioritize certain types of traffic. By configuring QoS, network administrators can allocate higher bandwidth to time-sensitive applications like VoIP, video conferencing, or critical business applications during peak usage times. This helps to reduce latency and packet loss, which are often caused by congestion.

Load Balancing (A): While load balancing is useful in distributing traffic across multiple servers or paths, it does not address congestion on a single switch.

Port Mirroring (B): This is used for monitoring network traffic for troubleshooting and diagnostics but does not alleviate congestion.

Spanning Tree Protocol (D): STP prevents switching loops in redundant network topologies, but it is not designed to handle traffic prioritization or congestion issues.

Reference: CompTIA Network+ Official Study Guide, Domain 1.5 (Network Optimization), Domain 2.1 (Network Management).

Question: 48

Which of the following connectors provides console access to a switch?

A. ST
B. RJ45
C. BNC
D. SFP

Answer: B

Explanation:

Console Access:

Purpose: Console access to a switch allows administrators to configure and manage the device directly. This is typically done using a terminal emulator program on a computer.

RJ45 Connector:

Common Use: The RJ45 connector is widely used for Ethernet cables and also for console connections to network devices like switches and routers.

Console Cables: Console cables often have an RJ45 connector on one end (for the switch) and a DB9 serial connector on the other end (for the computer).

Comparison with Other Connectors:

ST (Straight Tip): A fiber optic connector used for networking, not for console access.

BNC (Bayonet Neill-Concelman): A connector used for coaxial cable, typically in older network setups and not for console access.

SFP (Small Form-factor Pluggable): A modular transceiver used for network interfaces, not for console access.

Practical Application:

Connection Process: Connect the RJ45 end of the console cable to the console port of the switch.

Connect the DB9 end (or USB via adapter) to the computer. Use a terminal emulator (e.g., PuTTY, Tera Term) to access the switch's command-line interface (CLI).

Reference:

CompTIA Network+ study materials on network devices and connectors.

Question: 49

Which of the following is the correct order of components in a bottom-up approach for the three-tier hierarchical model?

A. Access, distribution, and core
B. Core, root, and distribution
C. Core, spine, and leaf
D. Access, core, and roof

Answer: A

Explanation:

The three-tier hierarchical model in network design consists of three layers: access, distribution, and core. The access layer is where devices like PCs and printers connect to the network. The distribution layer aggregates the data received from the access layer switches before it is transmitted to the core layer, which is responsible for high-speed data transfer and routing. This approach improves scalability and performance in larger networks. Reference: CompTIA Network+ Exam Objectives and official study guides.

Question: 50

While troubleshooting connectivity issues, a junior network administrator is given explicit instructions to test the host's TCP/IP stack first. Which of the following commands should the network administrator run?

A. ping 127.0.0.1
B. ping 169.254.1.1
C. ping 172.16.1.1
D. ping 192.168.1.1

Answer: A

Explanation:

The loopback address 127.0.0.1 is used to test the TCP/IP stack of the local machine. Pinging this address confirms whether the local system's networking stack is functioning correctly.

Question: 51

A network administrator is reviewing a production web server and observes the following output from the netstat command:

Which of the following actions should the network administrator take to harden the security of the web server?

A. Disable the unused ports.
B. Enforce access control lists.
C. Perform content filtering.
D. Set up a screened subnet.

Answer: A

Explanation:

The netstat output shows that multiple ports are open, including Telnet (23), FTP (20), and TFTP (69), which are potential security risks. Disabling unused ports minimizes the attack surface, reducing security vulnerabilities.

Breakdown of Options:

A . Disable the unused ports – Correct answer. Unused ports should be closed to prevent unauthorized access.

B . Enforce access control lists – ACLs help control access but do not disable unnecessary services.

C . Perform content filtering – Content filtering controls web traffic, not port security.

D . Set up a screened subnet – A DMZ (screened subnet) improves security but does not address open ports.

Reference:

CompTIA Network+ (N10-009) Official Study Guide – Domain 3.4: Given a scenario, implement network security measures.

CIS Benchmark for Linux & Windows Server Hardening

Question: 52

Which of the following cloud service models most likely requires the greatest up-front expense by the customer when migrating a data center to the cloud?

A. Infrastructure as a service
B. Software as a service
C. Platform as a service
D. Network as a service

Answer: A

Explanation:

Reference: CompTIA Network+ Certification Exam Objectives - Cloud Models section.

Question: 53

Which of the following steps in the troubleshooting methodology includes checking logs for recent changes?

A. Identify the problem.
B. Document the findings and outcomes.
C. Test the theory to determine cause.
D. Establish a plan of action.

Answer: A

Explanation:

Reference: CompTIA Network+ Certification Exam Objectives - Troubleshooting section.

Question: 54

An organization requires the ability to send encrypted email messages to a partner from an email server that is hosted on premises. The organization prefers to use the standard default ports when creating firewall rules. Which of the following ports should be open to satisfy the requirements?

A. 110
B. 143
C. 587
D. 636

Answer: C

Explanation:

Port 587 is the standard default port for sending email (SMTP) with TLS encryption, which is used to secure email transmissions between mail servers or between clients and mail servers. Allowing

traffic over port 587 enables secure email sending while maintaining standard protocol usage. (Reference: CompTIA Network+ Study Guide, Chapter on Ports and Protocols)

Question: 55

A data center interconnect using a VXLAN was recently implemented. A network engineer observes slow performance and fragmentation on the interconnect. Which of the following technologies will resolve the issue?

A. 802.1Q tagging
B. Spanning tree
C. Link aggregation

D. Jumbo frames

Answer: D

Explanation:

VXLAN (Virtual Extensible LAN) encapsulates Ethernet frames inside UDP packets, increasing packet size. This can lead to fragmentation and performance degradation unless Jumbo Frames are enabled. Breakdown of Options:

A . 802.1Q tagging – VLAN tagging enables segmentation but does not address fragmentation issues.

B . Spanning tree – STP prevents loops but does not improve performance for VXLAN traffic.

C . Link aggregation – LACP combines links for higher bandwidth but does not prevent fragmentation. D . Jumbo frames – Correct answer. Enabling Jumbo Frames allows larger packet sizes, reducing fragmentation and improving VXLAN performance.

Reference:

CompTIA Network+ (N10-009) Official Study Guide – Domain 2.3: Explain network performance concepts.

RFC 7348: VXLAN: A Framework for Overlaying Virtualized Layer 2 Networks

Question: 56

Which of the following is the MOST appropriate solution to extend the network to a building located across the street from the main facility?

A. Multimode fiber
B. 802.11ac wireless bridge
C. Cat 6 copper
D. Loopback adapter

Answer: B

Explanation:

An 802.11ac wireless bridge is the most practical solution to connect two nearby buildings without trenching or laying physical cable. It provides high-speed, point-to-point connectivity using directional antennas.

A . Multimode fiber is effective but expensive and typically limited to 500 meters or less.

C . Cat 6 copper is only rated for up to 100 meters — not viable for a street-wide distance.

D . Loopback adapter is a troubleshooting tool, not for network extension.

Reference:

CompTIA Network+ N10-009 Official Objectives: 1.3 – Compare and contrast various network topologies, types, and technologies.

Question: 57

Which of the following panels would be best to facilitate a central termination point for all network cables on the floor of a company building?

A. Patch
B. UPS
C. MDF
D. Rack

Answer: A

Explanation:
Reference: CompTIA Network+ Certification Exam Objectives - Network Installation section.

Question: 58

Early in the morning, an administrator installs a new DHCP server. In the afternoon, some users report they are experiencing network outages. Which of the following is the most likely issue?

A. Theadministrator didnot provisionenough IP addresses.
B. Theadministrator configured an incorrect default gateway.
C. Theadministrator didnot provisionenough routes.
D. Theadministrator didnot provisionenough MAC addresses.

Answer: A

Explanation:

When a DHCP server is installed and not enough IP addresses are provisioned, users may start experiencing network outages once the available IP addresses are exhausted. DHCP servers assign IP addresses to devices on the network, and if the pool of addresses is too small, new devices or those renewing their lease may fail to obtain an IP address, resulting in network connectivity issues.Reference: CompTIA Network+ study materials.

Question: 59

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 the best choice for the CTO's requirements. It allows the organization to run key services from the on-site data center while leveraging the cloud for enterprise services. This approach provides flexibility, scalability, and cost savings, while also minimizing disruptions to users by keeping critical services local. The hybrid model integrates both private and public cloud environments, offering the benefits of both.Reference: CompTIA Network+ study materials and cloud computing principles.

Question: 60

A network administrator needs to deploy a subnet using an IP address range that can support at least 260 devices with the fewest wasted addresses. Which of the following subnets should the administrator use?

A. 172.16.0.0/24
B. 172.25.2.0/23
C. 172.30.1.0/22
D. 172.33.0.0/21

Answer: B

Explanation:

To support at least 260 hosts, you need at least 512 total IP addresses (accounting for network/broadcast overhead).
/23 (255.255.254.0) gives 510 usable IPs, ideal for 260 devices with minimal waste.
/24 (255.255.255.0) gives only 254 usable — not enough.
/22 (1022 usable) and /21 (2046 usable) would work but result in significant address waste.
Reference:
CompTIA Network+ N10-009 Official Objectives: 2.1 – Given a scenario, configure and apply IP addressing schemes.

Question: 61

Which of the following steps of the troubleshooting methodology comes after testing the theory to determine cause?

A. Verify full system functionality.
B. Document the findings and outcomes.
C. Establish a plan of action.
D. Identify the problem.

Answer: C

Explanation:

The CompTIA Troubleshooting Methodology states that after testing the theory, the next step is to establish a plan of action to resolve the issue.

Troubleshooting Steps:

Identify the problem.

Establish a theory of probable cause.

Test the theory to determine the cause.

Establish a plan of action and implement the solution. Q (Correct step)

Verify full system functionality.

Document findings, actions, and outcomes.

Breakdown of Options:

A . Verify full system functionality – Happens after implementing the solution.

B . Document the findings and outcomes – Final step, happens after resolving the issue.

C . Establish a plan of action – Q Correct answer. Comes immediately after confirming the cause.

D . Identify the problem – First step, already completed.

Reference:

CompTIA Network+ (N10-009) Official Study Guide – Domain 5.1: Explain network troubleshooting methodology.

Question: 62

Which of the following is an XML-based security concept that works by passing sensitve information about users, such as log-in information and attributes, to providers.

A. IAM

B. MFA

C. RADIUS

D. SAML

Answer: D

Explanation:

Security Assertion Markup Language (SAML) is an XML-based standard used for exchanging authentication and authorization data between parties, particularly between an identity provider (IdP) and a service provider (SP). SAML is commonly used in Single Sign-On (SSO) solutions to pass sensitive user information, such as login credentials and attributes, securely between the identity provider and the service provider.

SAML (Security Assertion Markup Language): Facilitates web-based authentication and authorization, allowing users to access multiple services with a single set of credentials.

XML-based: Uses XML to encode the authentication and authorization data, ensuring secure transmission of user information.

Identity Federation: Enables secure sharing of identity information across different security domains, making it ideal for enterprise SSO solutions.

Network Reference:

CompTIA Network+ N10-007 Official Certification Guide: Covers authentication protocols, including SAML.

Cisco Networking Academy: Provides training on identity management and federation technologies. Network+ Certification All-in-One Exam Guide: Explains SAML and its role in secure identity management and SSO.

Question: 63

Which of the following is the next step to take after successfully testing a root cause theory?

A. Determine resolution steps.
B. Duplicate the problem in a lab.
C. Present the theory for approval.
D. Implement the solution to the problem.

Answer: A

Explanation:

Troubleshooting Methodology:

Confirming the Root Cause: After testing and confirming the theory, the next logical step is to address the issue by implementing a solution.

Implementation of the Solution:

Resolve the Issue: Implement the identified solution to rectify the problem. This step involves making necessary changes to the network configuration, replacing faulty hardware, or applying software patches.

Documentation: Document the solution and the steps taken to resolve the issue to provide a reference for future troubleshooting.

Comparison with Other Steps:

Determine Resolution Steps: This is part of the implementation process where specific actions are outlined, but the actual next step after testing is to implement those steps.

Duplicate the Problem in a Lab: This step is typically done earlier in the troubleshooting process to understand the problem, not after confirming the root cause.

Present the Theory for Approval: In some scenarios, presenting the theory might be necessary for major changes, but generally, once the root cause is confirmed, the solution should be implemented. Final Verification:

After implementing the solution, it is important to verify that the issue is resolved and that normal operations are restored.

This may involve monitoring the network and testing to ensure no further issues arise.

Reference:

CompTIA Network+ study materials on troubleshooting methodologies and best practices.

Question: 64

A technician is planning an equipment installation into a rack in a data center that practices hot aisle/cold aisle ventilation.

Which of the following directions should the equipment exhaust face when installed in the rack?

A. Sides B. Top C. Front D. Rear

Answer: D

Explanation:

In a data center that uses hot aisle/cold aisle ventilation, equipment is typically installed so that cool air enters from the cold aisle (front) and hot air is exhausted to the hot aisle (rear). This configuration maximizes cooling efficiency.

Question: 65

After running a Cat 8 cable using passthrough plugs, an electrician notices that connected cables are experiencing a lot of cross talk. Which of the following troubleshooting steps should the electrician take first?

A. Inspect the connectors for any wires that are touching or exposed.
B. Restore default settings on the connected devices.
C. Terminate the connections again.
D. Check for radio frequency interference in the area.

Answer: A

Explanation:

Cross talk can often be caused by improper termination of cables. The first step in troubleshooting should be to inspect the connectors for any wires that might be touching or exposed. Ensuring that all wires are correctly seated and that no conductors are exposed can help reduce or eliminate cross talk. This step should be taken before attempting to re-terminate the connections or check for other sources of interference.Reference: CompTIA Network+ study materials.

Question: 66

A network administrator is configuring a new switch and wants to ensure that only assigned devices can connect to the switch. Which of the following should the administrator do?

A. Configure ACLs.
B. Implement a captive portal.
C. Enable port security.
D. Disable unnecessaryservices.

Answer: C

Explanation:

Reference: CompTIA Network+ Certification Exam Objectives - Network Security section.

Question: 67

Which of the following protocols provides remote access utilizing port 22?

A. SSH
B. Telnet
C. TLS

D. RDP

Answer: A

Explanation:

SSH (Secure Shell) is a protocol used to securely connect to a remote server/system over a network. It operates on port 22 and provides encrypted communication, unlike Telnet which operates on port 23 and is not secure. TLS is used for securing HTTP connections (HTTPS) and operates on ports like 443, while RDP (Remote Desktop Protocol) is used for remote desktop connections and operates on port 3389.

Reference:

The CompTIA Network+ materials and tutorials cover SSH as the standard protocol for secure remote access, highlighting its operation on port 22.

Question: 68

Which of the following are environmental factors that should be considered when installing equipment in a building? (Select two).

A. Fire suppression system
B. UPS location
C. Humidity control
D. Power load
E. Floor construction type
F. Proximity to nearest MDF

Answer: A

Explanation:

When installing equipment in a building, environmental factors are critical to ensure the safety and longevity of the equipment. A fire suppression system is essential to protect the equipment from fire hazards. Humidity control is crucial to prevent moisture-related damage, such ascorrosion and short circuits, which can adversely affect electronic components. Both factors are vital for maintaining an optimal environment for networking equipment.Reference: CompTIA Network+ study materials.

Question: 69

A network administrator deployed wireless networking in the office are
a. When users visit the outdoor patio and try to download emails with large attachments or stream training videos, they notice buffering issues. Which of the following is the most likely cause?

A. Network congestion
B. Wireless interference
C. Signal degradation
D. Client disassociation

Answer: C

Explanation:

The most likely cause of buffering issues when moving outdoors is signal degradation. Wireless signals weaken as they travel through obstacles such as walls, glass, and air, leading to weaker connections and reduced data rates.

Breakdown of Options:

A . Network congestion – While congestion can slow down network speeds, it affects all users, not just those moving outdoors.

B . Wireless interference – Interference is possible but is more likely caused by other wireless signals rather than outdoor movement.

C . Signal degradation – Correct answer. Wireless signals weaken with distance and obstacles such as walls, reducing performance.

D . Client disassociation – Disassociation occurs when clients lose connection to the AP, but the question states that users experience buffering, indicating they are still connected but with a weak signal.

Reference:

CompTIA Network+ (N10-009) Official Study Guide – Domain 1.6: Analyze wireless networking technologies.

IEEE 802.11 standards: Wi-Fi propagation characteristics

Question: 70

A company discovers on video surveillance recordings that an unauthorized person installed a rogue access point in its secure facility. Which of the following allowed the unauthorized person to do this?

A. Evil twin
B. Honeytrap
C. Wardriving
D. Tailgating

Answer: D

Explanation:

Tailgating is a physical security breach where someone follows an authorized person into a restricted area without proper credentials. Once inside, the attacker can install rogue devices like unauthorized APs.

A . Evil twin is a wireless attack where an attacker sets up a fake AP.

B . Honeytrap is used to attract attackers for analysis.

C . Wardriving involves scanning for unsecured Wi-Fi networks while driving, not physical intrusion.

Reference:

CompTIA Network+ N10-009 Official Objectives: 4.2 – Identify common security threats and vulnerabilities.

Question: 71

A systems administrator is configuring a new device to be added to the network. The administrator is planning to perform device hardening prior to connecting the device. Which of the following should the administrator do first?

A. Update the network ACLs.
B. Place the device in a screened subnet.
C. Enable content filtering.
D. Change the default admin passwords.

Answer: D

Explanation:

Changing default admin passwords is a fundamental first step in device hardening to prevent unauthorized access.

Question: 72

Which of the following allows a user to connect to an isolated device on a stand-alone network?

A. Jump box
B. API gateway
C. Secure Shell (SSH)
D. Clientless VPN

Answer: A

Explanation:

A jump box is a hardened system that provides secure access to isolated or sensitive devices on a separate network.
Breakdown of Options:
A . Jump box – Q Correct answer. Acts as a middle point for secure remote access.
B . API gateway – Used for managing API calls, not remote access to isolated devices.
C . Secure Shell (SSH) – Requires direct connectivity, which may not be available for an isolated device.
D . Clientless VPN – Allows web-based VPN access, but does not guarantee access to isolated devices.
Reference:
CompTIA Network+ (N10-009) Official Study Guide – Domain 3.4: Implement secure remote access methods.

Question: 73

Which of the following explains what happens if a packet is lost in transit when using UDP?

A. The data link layer will recognize the error and resend the packet.
B. IP uses the TTL field to track packet hops and will resend the packet if necessary.
C. If the sender does not receive a UDP acknowledgement, the packet will be resent.
D. Some applications will recognize the loss and initiate a resend of the packet if necessary.

Answer: D

Explanation:

UDP (User Datagram Protocol) is a connectionless protocol that does not provide built-in

mechanisms for error detection, retransmission, or acknowledgments. If a UDP packet is lost in transit, the protocol itself does not handle retransmission. However, some applications using UDP (e.g., TFTP or custom streaming protocols) may implement their own mechanisms to detect packet loss and request retransmission if needed.

Why not A? The data link layer (Layer 2) handles frame-level errors within a single network segment, not end-to-end packet loss across networks.

Why not B? The IP TTL (Time to Live) field prevents routing loops by decrementing with each hop, but IP does not handle retransmission.

Why not C? UDP does not use acknowledgments, so the sender does not expect or receive them. Reference:CompTIA Network+ N10-009 Objective 1.4: Explain the characteristics of network topologies and protocols. The CompTIA Network+ Study Guide (e.g., Chapter 4: Network Protocols) explains that UDP is a “fire-and-forget” protocol, and any retransmission logic must be handled by the application layer.

Question: 74

A client with a 2.4GHz wireless network has stated that the entire office is experiencing intermittent issues with laptops after the WAP was moved. Which of the following is the most likely reason for these issues?

A. The network uses a non-overlapping channel.
B. The signal is reflecting too much.
C. The network has excessive noise.
D. A microwave is in the office.

Answer: D

Explanation:

Microwaves are known to interfere with the 2.4GHz frequency, which is the same frequency used by many wireless networks. This can cause signal degradation and intermittent connectivity issues, especially if the WAP is placed near such devices.

Question: 75

An investment bank is seeking a DR backup solution. Which of the following provides the most cost effective backup site?

A. Hot
B. Cold
C. Cluster
D. Warm

Answer: B

Explanation:

- Cold sites are the most cost-effective disaster recovery (DR) option since they require the least infrastructure investment. They provide space and power but no pre-configured systems.
- Hot sites (A) are fully operational and very expensive.
- Warm sites (D) offer some pre-configured hardware but still require setup, making them more costly than cold sites.
- Clusters (C) are active failover systems, not DR sites.

Reference: CompTIA Network+ N10-009 Official Documentation – Disaster Recovery & Business Continuity Planning.

Question: 76

A company reports that their facsimile machine no longer has a dial tone when trying to send a fax. The phone cable is damaged on one end. Which of the following types of connectors should a technician replace?

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

Answer: D

Explanation:

Fax machines use analog phone lines, which are connected using RJ11 connectors. These are standard telephone connectors with 4 or 6 positions and are used for POTS (Plain Old Telephone Service) lines.

F-type is used for coaxial cables (e.g., TV and cable modems).

RJ45 is used for Ethernet network connections.

SC (Subscriber Connector) is used for fiber optic connections, not analog telephone lines. Reference: CompTIA Network+ N10-009 Official Objectives: 2.4 – Compare and contrast common network connectors.

Question: 77

A junior network technician at a large company needs to create networks from a Class C address with 14 hosts per subnet. Which of the following numbers of host bits is required?

A. One

B. Two
C. Three
D. Four

Answer: D

Explanation:

Question: 78

A company has observed increased user traffic to gambling websites and wants to limit this behavior on work computers. Which of the following should the company most likely implement?

A. ACLs
B. Content filter
C. Port security
D. Screened subnet

Answer: B

Explanation:

A content filter blocks access to specific websites based on category, URL, or keywords. This is the best solution to restrict gambling websites.

Breakdown of Options:

A . ACLs – Control network access, not specific web content.

B . Content filter – Q Correct answer. Used to block access to unwanted websites.

C . Port security – Prevents unauthorized device connections, not web traffic filtering.

D . Screened subnet – A DMZ isolates public-facing servers, not user restrictions.

Reference:

CompTIA Network+ (N10-009) Official Study Guide – Domain 3.3: Given a scenario, implement network security measures.

Question: 79

A company is hosting a secure that requires all connections to the server to be encrypted. A junior administrator needs to harded the web server. The following ports on the web server. The following ports on the web server are open:

443
80
22
587

Which of the following ports should be disabled?

A. 22
B. 80
C. 443
D. 587

Answer: B

Explanation:

For a web server that requires all connections to be encrypted, port 80 (HTTP) should be disabled. Port 80 is used for unencrypted web traffic, whereas port 443 is used for HTTPS, which provides encrypted communication.

Port 80 (HTTP): This port is used for unsecured web traffic. Disabling this port ensures that all web traffic must use HTTPS, which encrypts the data in transit.

Port 443 (HTTPS): This port is used for secure web traffic via SSL/TLS encryption. Keeping this port open ensures that secure connections can be made to the web server.

Other Ports:

Port 22: Used for SSH, providing secure remote access and file transfers.

Port 587: Used for secure email submission (SMTP) with encryption.

Network Reference:

CompTIA Network+ N10-007 Official Certification Guide: Discusses the roles and security implications of various ports and protocols.

Cisco Networking Academy: Provides training on secure web server configuration and port management.

Network+ Certification All-in-One Exam Guide: Covers port security and best practices for securing web servers.

Question: 80

Which of the following describes the best reason for using BGP?

A. Preventing a loop within a LAN
B. Improving reconvergence times
C. Exchanging router updates with a different ISP
D. Sharing routes with a Layer 3 switch

Answer: C

Explanation:

BGP (Border Gateway Protocol) is used for routing data between different ISPs, making it essential for the functioning of the internet. Its primary use is for exchanging routing information between autonomous systems, especially different ISPs.

Preventing loops within a LAN ishandled by protocols

like Spanning Tree Protocol (STP), while improving reconvergence times and sharing routes with a Layer 3 switch are functions of other protocols or internal mechanisms.

Reference:

The CompTIA Network+ training emphasizes BGP's role in the exchange of routing information across different ISPs and autonomous systems.

Question: 81

Which of the following ports creates a secure connection to a directory service?

A. 22
B. 389
C. 445
D. 636

Answer: D

Explanation:

LDAP (Lightweight Directory Access Protocol) uses port 389 for standard connections and port 636 for LDAP over SSL (LDAPS), which secures directory service communication.
Breakdown of Options:
A . 22 – SSH port, not used for directory services.
B . 389 – Used for LDAP, but not encrypted.
C . 445 – Used for SMB file sharing, not LDAP.
D. 636 – Correct answer. LDAPS (LDAP over SSL/TLS) secures directory authentication.
Reference:
CompTIA Network+ (N10-009) Official Study Guide – Domain 3.1: Compare and contrast network protocols.
RFC 4511: Lightweight Directory Access Protocol (LDAP)

Question: 82

Which of the following dynamic routing protocols is used on the internet?

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

Answer: B

Explanation:

BGP (Border Gateway Protocol) is the only dynamic routing protocol used across the internet. It's

classified as an Exterior Gateway Protocol (EGP), responsible for routing between different autonomous systems (ASes).
A . EIGRP and D. OSPF are Interior Gateway Protocols (IGPs), used within organizations.
C . RIP is an outdated IGP with limited use, unsuitable for internet-scale routing.
Reference:
CompTIA Network+ N10-009 Official Objectives: 3.1 – Compare and contrast various routing technologies.

Question: 83

A technician is planning an equipement installation into a rack in a data center that practices hot aisle/cold aise ventilation.
Which of the following directions should the equipement exhaust face when installed in the rack?

A. Sides
B. Top
C. Front
D. Rear

Answer: C

Explanation:

In a data center that practices hot aisle/cold aisle ventilation, equipment should be installed so that the exhaust faces the rear of the rack. This setup ensures that hot air is expelled into the hot aisle, maintaining proper airflow and cooling efficiency.

Hot Aisle/Cold Aisle Configuration: Equipment intake should face the cold aisle where cool air is supplied, and exhaust should face the hot aisle where hot air is expelled.

Cooling Efficiency: Proper orientation of equipment helps maintain an efficient cooling environment by segregating hot and cold air, preventing overheating and improving energy efficiency.

Network Reference:

CompTIA Network+ N10-007 Official Certification Guide: Discusses data center design principles, including hot aisle/cold aisle configurations.

Cisco Data Center Design Guide: Provides best practices for data center layout and equipment installation.

Network+ Certification All-in-One Exam Guide: Covers data center environmental controls and ventilation strategies.

Question: 84

SIMULATION

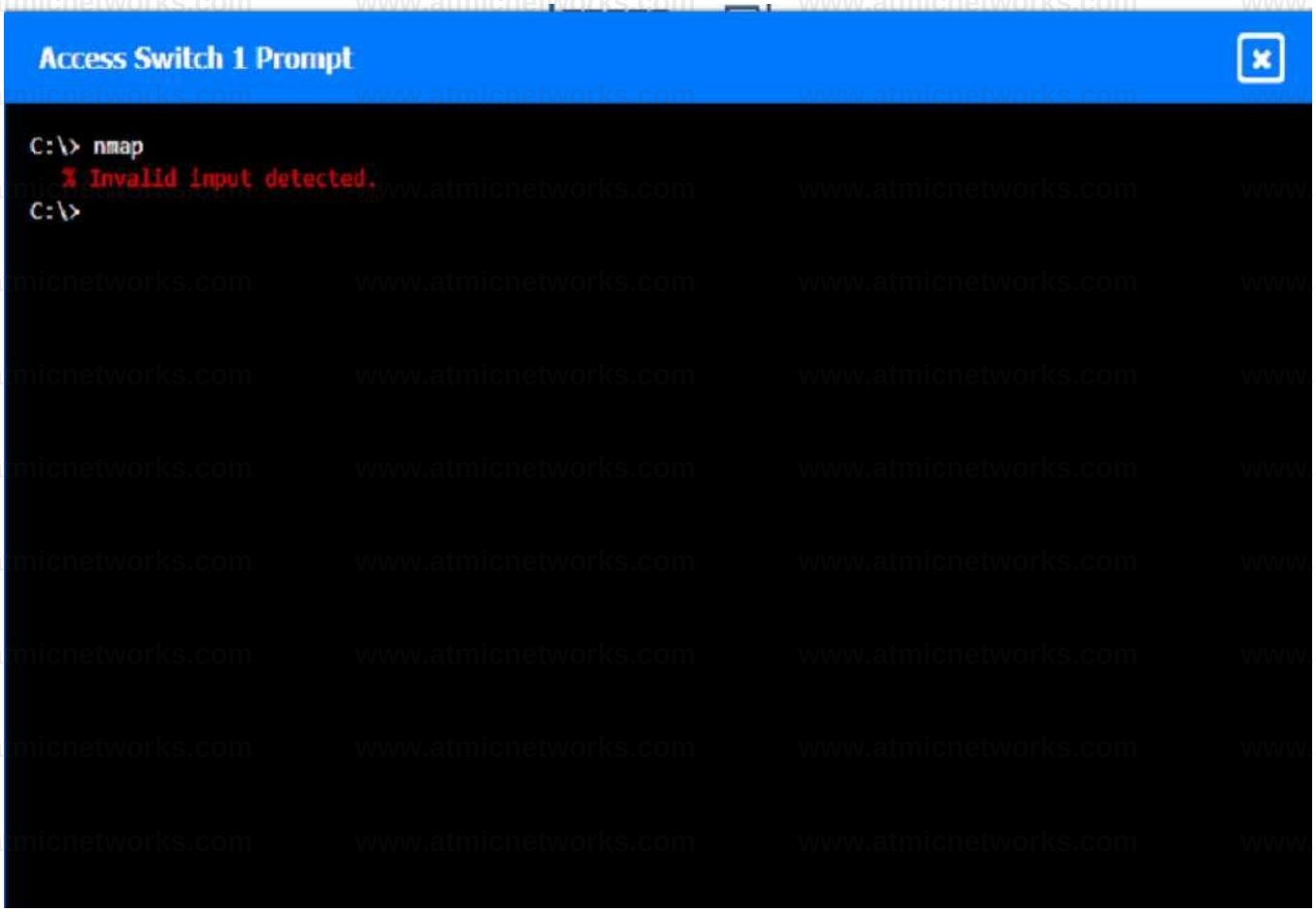
A network technician was recently onboarded to a company. A manager has tasked the technician with documenting the network and has provided the technician With partial information from previous documentation.

Instructions:

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

Core Switch 1 Prompt

```
C:\> nmap

C:\> netdiscover

C:\> |
```



Answer: See the Explanation for detailed information on this simulation.

Explanation:

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

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

Click on each switch to open its terminal window.

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

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

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

Fill in the missing information in the diagram using the drop-down menus provided.

Here is an example of how to fill in the missing information for Core Switch 1:

The IP address of Core Switch 1 is 192.168.1.1.

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

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

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

GigabitEthernet0/2.

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

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

Question: 85

Users at a satellite office are experiencing issues when using videoconferencing. Which of the following should a technician focus on first to rectify these issues?

A. Quality of service
B. Network signal
C. Time to live
D. Load balancing

Answer: A

Explanation:

Quality of Service (QoS) is crucial for real-time services like video conferencing. It prioritizes voice and video packets over less critical traffic (like file downloads), reducing latency, jitter, and packet loss.

B . Network signal may apply to wireless, but it's not specific to video issues.

C . Time to live (TTL) affects packet lifespan, not performance or quality.

D . Load balancing manages traffic across multiple paths but doesn't prioritize real-time traffic like QoS does.

Reference:

CompTIA Network+ N10-009 Official Objectives: 3.6 – Explain the characteristics of network topologies and types.

Question: 86

SIMULATION

A network technician needs to resolve some issues with a customer's SOHO network. The customer reports that some of the PCs are not connecting to the network, while others appear to be working as intended.

INSTRUCTIONS

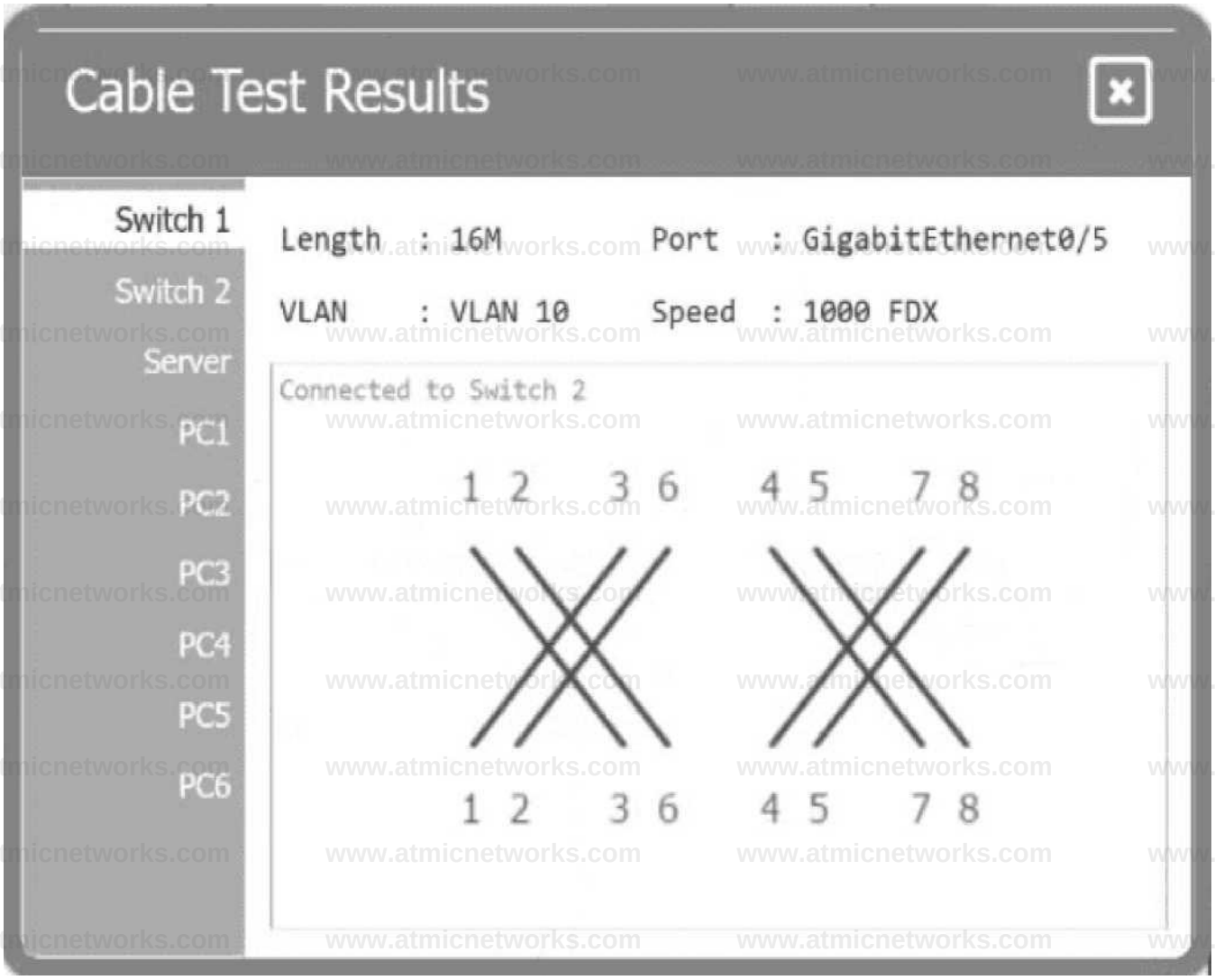
Troubleshoot all the network components.

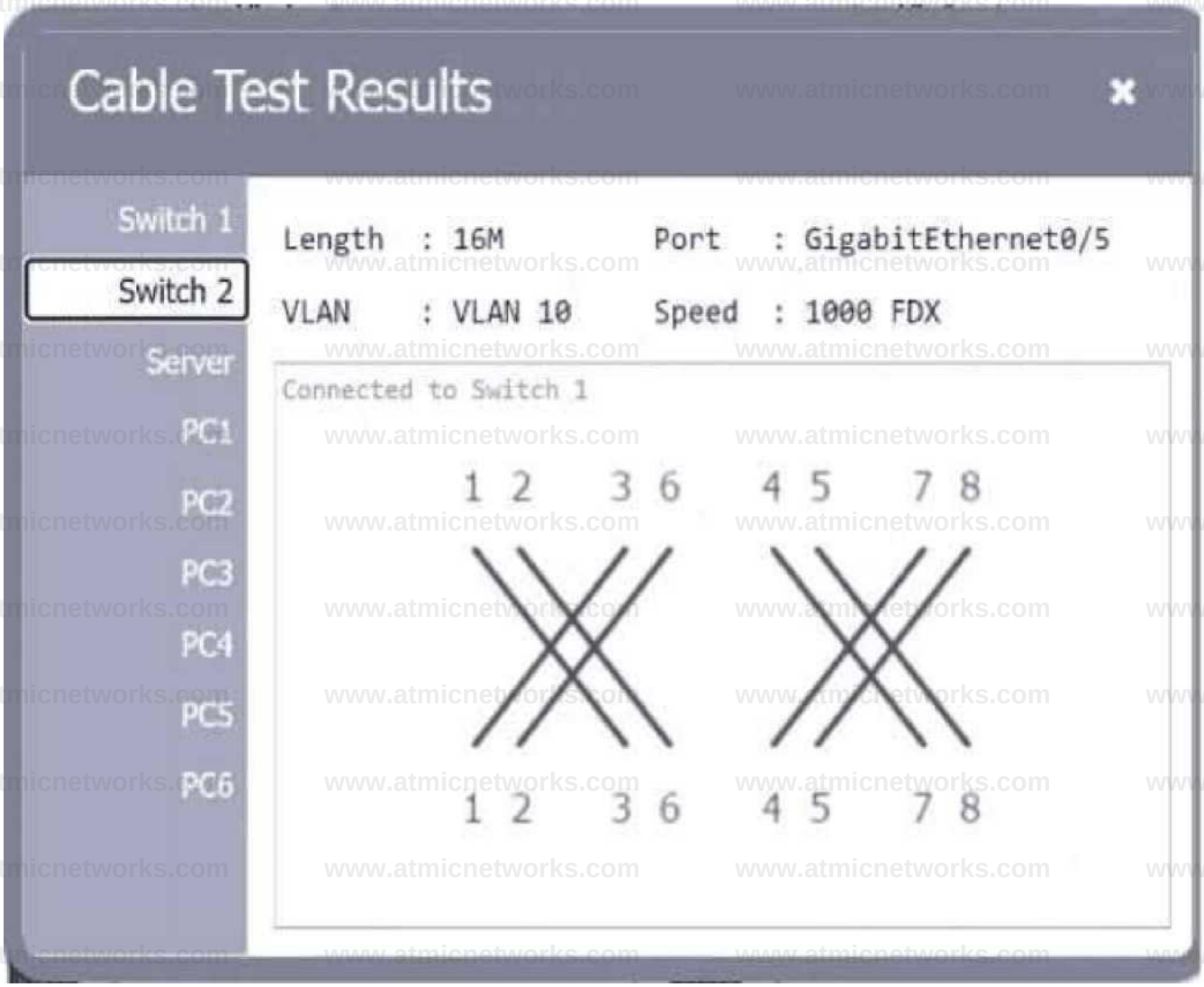
Review the cable test results first, then diagnose by clicking on the appropriate PC, server, and Layer 2 switch.

Identify any components with a problem and recommend a solution to correct each problem.

If at any time you would like to bring back

the initial state of the simulation, please
click the Reset All button.



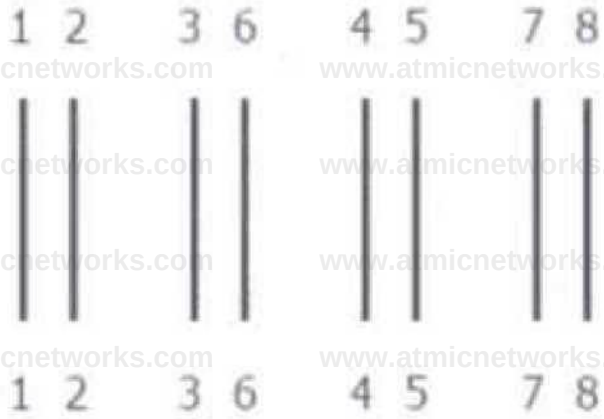


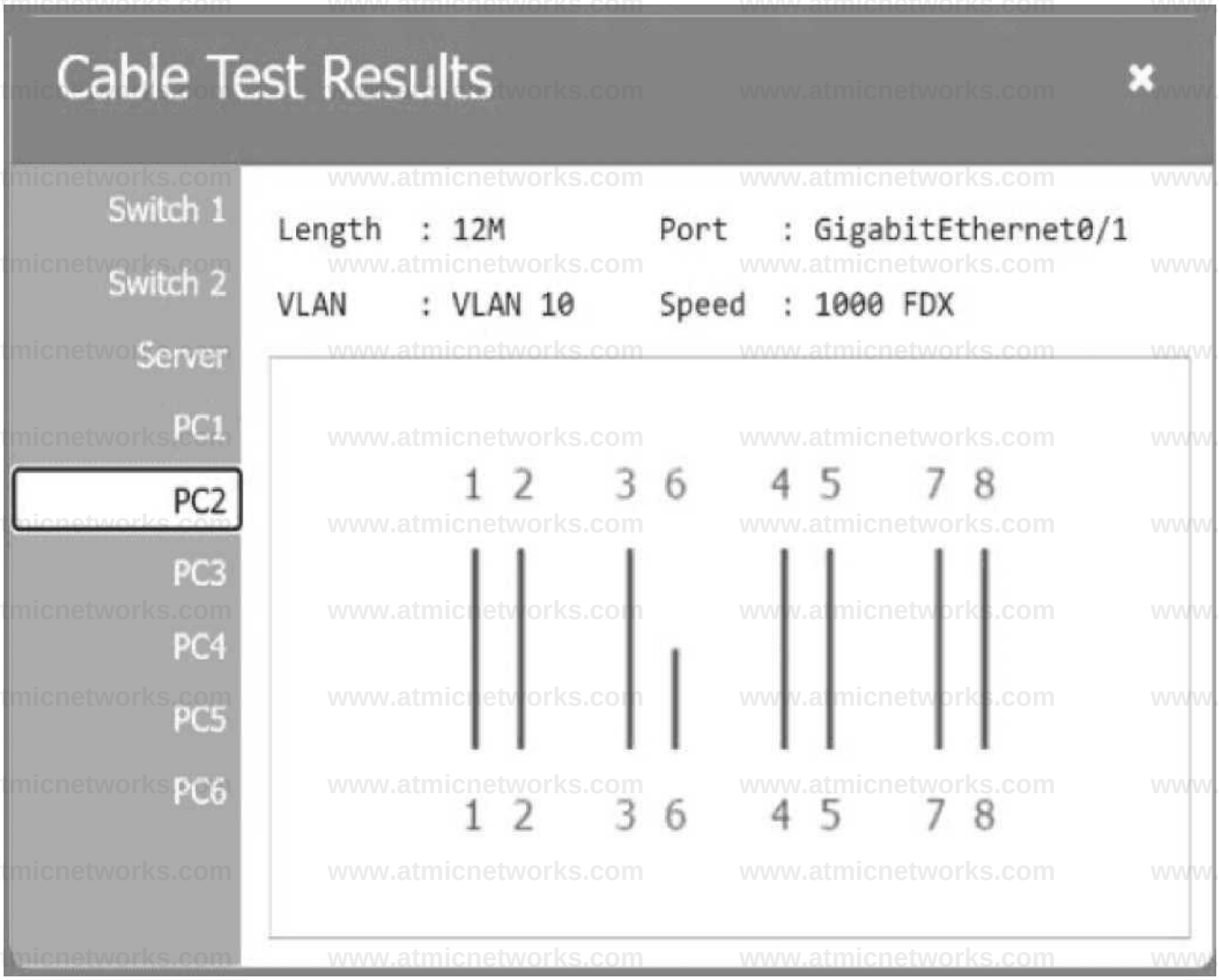
Cable Test Results

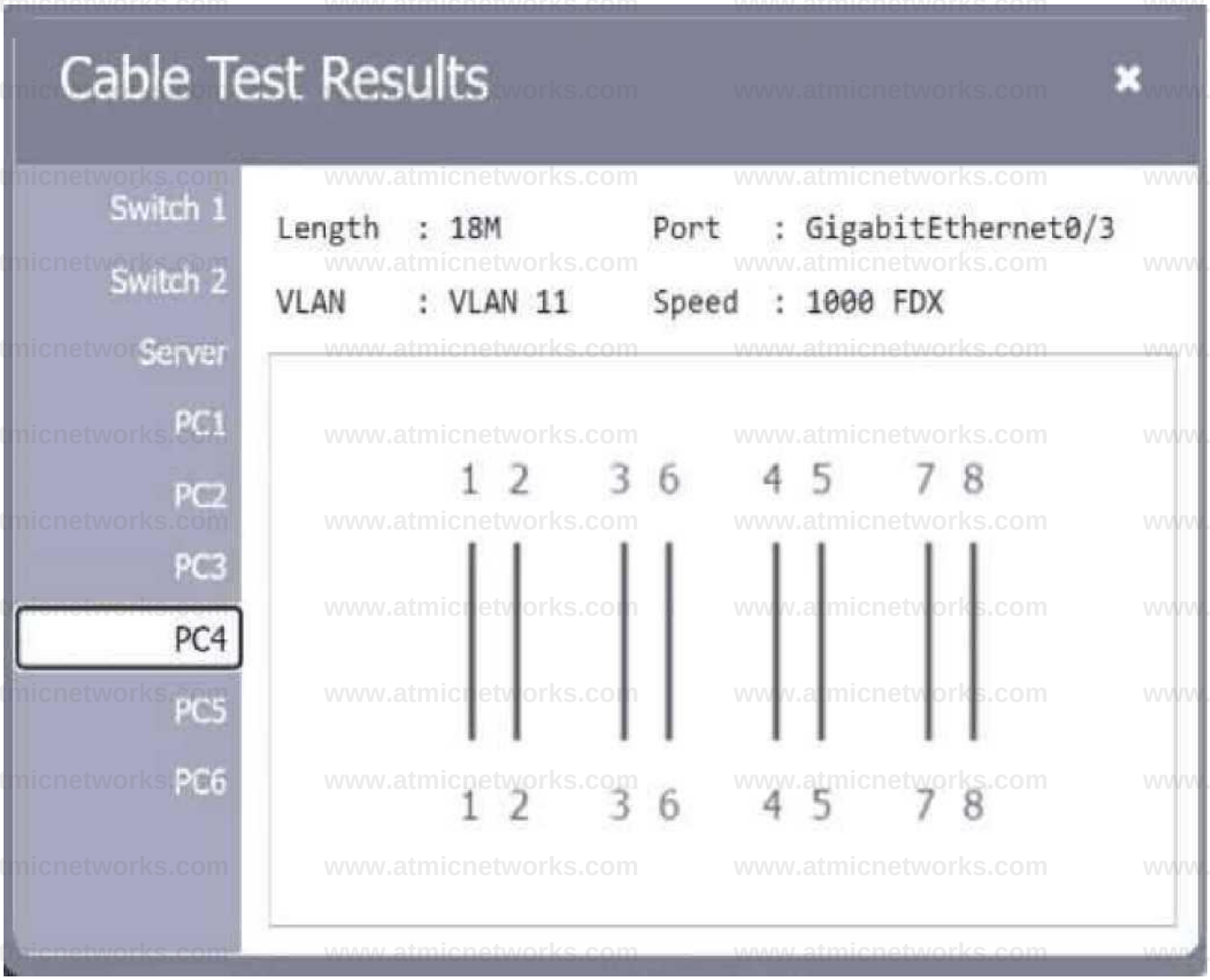
Switch 1
Switch 2
Server
PC1
PC2
PC3
PC4
PC5
PC6

Length : 22M Port : GigabitEthernet0/1

VLAN : VLAN 10 Speed : 1000 FDX



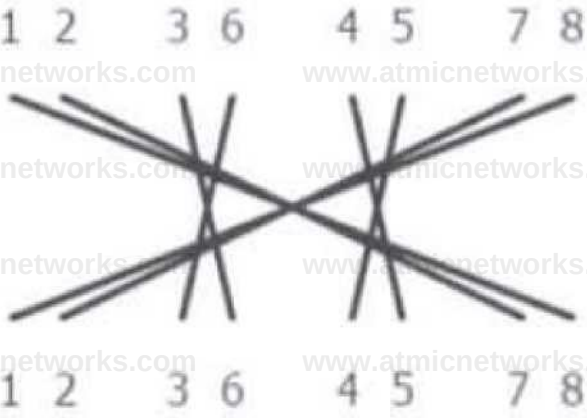


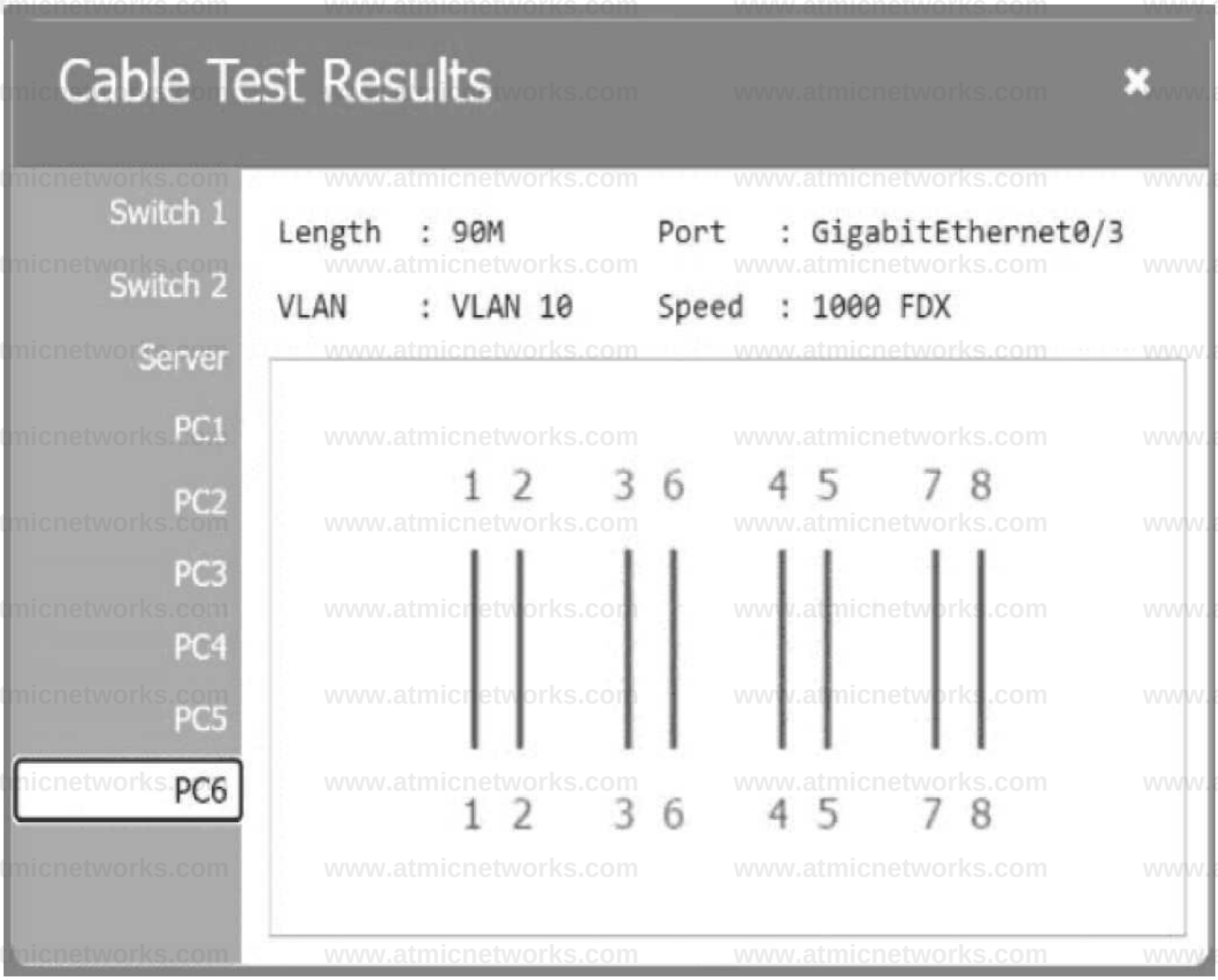


Cable Test Results

Switch 1
Switch 2
Server
PC1
PC2
PC3
PC4
PC5
PC6

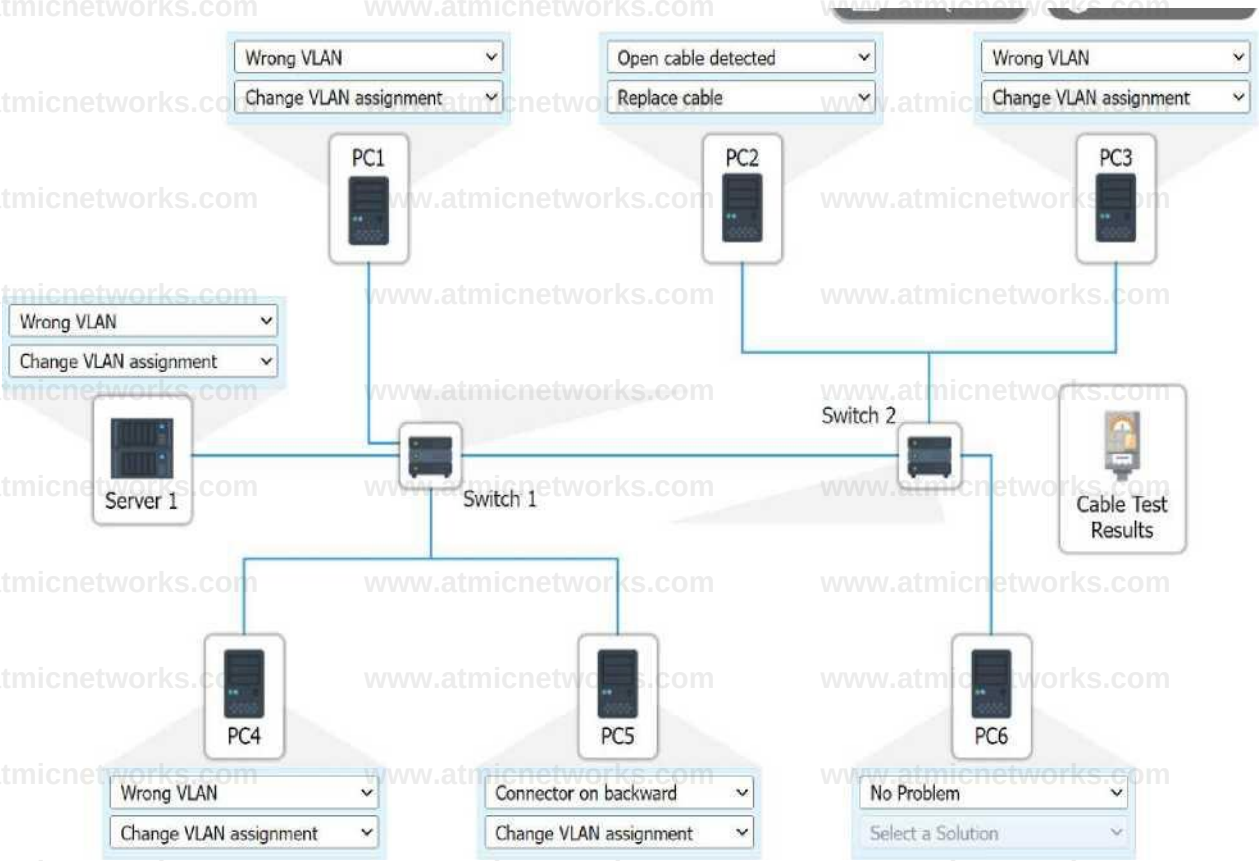
Length : 33M Port : GigabitEthernet0/4
VLAN : VLAN 10 Speed : 1000 FDX





Answer: See the answer and solution below:

Explanation:



A computer network diagram with many boxes and text AI-generated content may be incorrect.

Question: 87

A storage network requires reduced overhead and increased efficiency for the amout of data being sent. Which of the following should an engineer likely configure to meet these requirements>?

A. Link speed
B. Jumbo frames
C. QoS
D. 802.1q tagging

Answer: B

Explanation:

Jumbo frames are Ethernet frames with a payload greater than the standard maximum transmission unit (MTU) of 1500 bytes. Configuring jumbo frames can reduce overhead and increase efficiency in storage networks by allowing more data to be sent in each frame, thus reducing the number of frames needed to transmit the same amount of data.

Reduced Overhead: By sending larger frames, the relative overhead for headers and acknowledgments is reduced.

Increased Efficiency: Larger frames mean fewer packets to process, leading to better utilization of network bandwidth and improved performance in high-throughput environments like storage networks.

Configuration: Requires support from all devices in the network path, including switches and network

interface cards (NICs).

Network Reference:

CompTIA Network+ N10-007 Official Certification Guide: Explains jumbo frames and their benefits in reducing network overhead.

Cisco Networking Academy: Provides training on network optimization techniques, including the use of jumbo frames.

Network+ Certification All-in-One Exam Guide: Covers advanced Ethernet features, including jumbo frames and their configuration for improved network performance.

Question: 88

A network technician is troubleshooting a faulty NIC and tests the theory. Which of the following should the technician do next?

A. Develop a theory.
B. Establish a plan of action.
C. Implement the solution.
D. Document the findings.

Answer: C

Explanation:

Once the theory has been tested and confirmed, the next step is to implement the solution based on the CompTIA troubleshooting model.

CompTIA Troubleshooting Model:

Identify the problem.

Establish a theory of probable cause.

Test the theory.

Establish a plan of action and implement the solution. Q (Correct step)

Verify full system functionality.

Document findings, actions, and outcomes.

Breakdown of Options:

A . Develop a theory – The theory has already been developed and tested.

B . Establish a plan of action – This happens before implementation, but since the issue is confirmed, it's time to act.

C . Implement the solution – Correct answer. The problem is confirmed, so the fix should be applied.

D . Document the findings – Documentation is the final step, not the next one.

Reference:

CompTIA Network+ (N10-009) Official Study Guide – Domain 5.1: Explain network troubleshooting methodology.

Question: 89

A company wants to implement a disaster recovery site or non-critical applicance, which can

tolerance a short period of downltime. Which of the followig type of sites should the company impelement to achive this goal?

A. Hot
B. Cold
C. Warm
D. Passive

Answer: C

Explanation:

A warm site is a compromise between a hot site and a cold site, providing a balance between cost and recovery time. It is partially equipped with the necessary hardware, software, and infrastructure, allowing for a quicker recovery compared to a cold site but at a lower cost than a hot site. Recovery Time: Warm sites can be operational within hours to a day, making them suitable for non- critical applications that can tolerate short downtimes.
Cost-Effectiveness: Warm sites are more economical than hot sites as they do not require all systems to be fully operational at all times.
Network Reference:
CompTIA Network+ N10-007 Official Certification Guide: Discusses disaster recovery strategies and the different types of recovery sites.
Cisco Networking Academy: Provides training on disaster recovery planning and site selection. Network+ Certification All-in-One Exam Guide: Explains the characteristics of hot, warm, and cold sites and their use cases in disaster recovery planning.
Warm sites offer a practical solution for maintaining business continuity for non-critical applications, balancing the need for availability with cost considerations.

Question: 90

A network consultant needs to decide between running an ethernet uplink or using the built-in 5GHz-to-point functionality on a WAP. Which of the following documents provides the best information to assist the consultant with this decision?

A. Site survey results
B. Physical diagram
C. Service-level agreement
D. Logical diagram

Answer: A

Explanation:

Question: 91

SIMULATION

A network technician replaced an access layer switch and needs to reconfigure it to allow the connected devices to connect to the correct networks.

INSTRUCTIONS

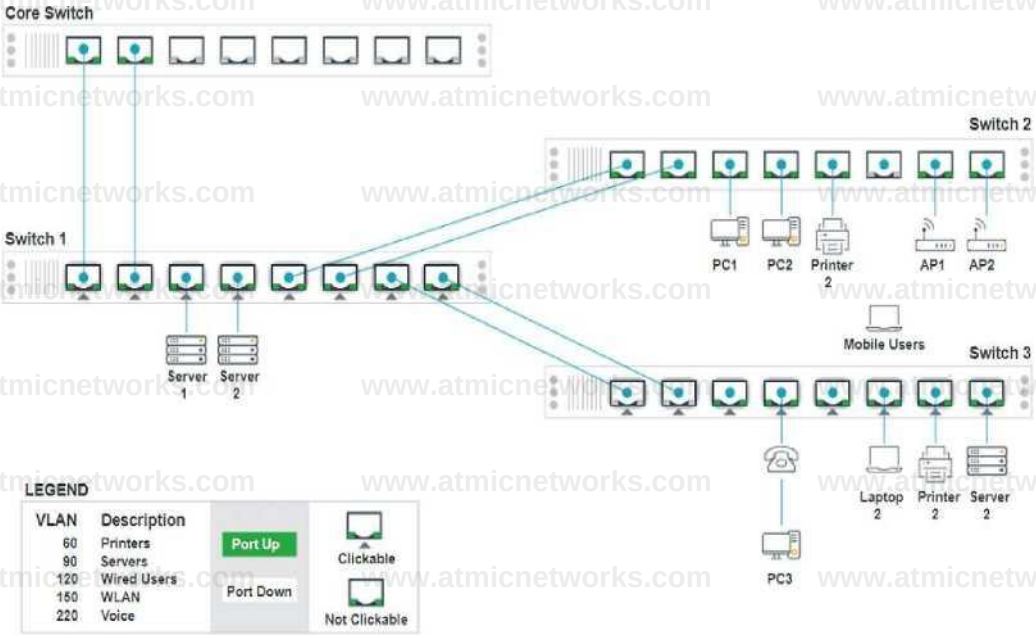
Click on the appropriate port(s) on Switch 1 and Switch 3 to verify or reconfigure the correct settings:

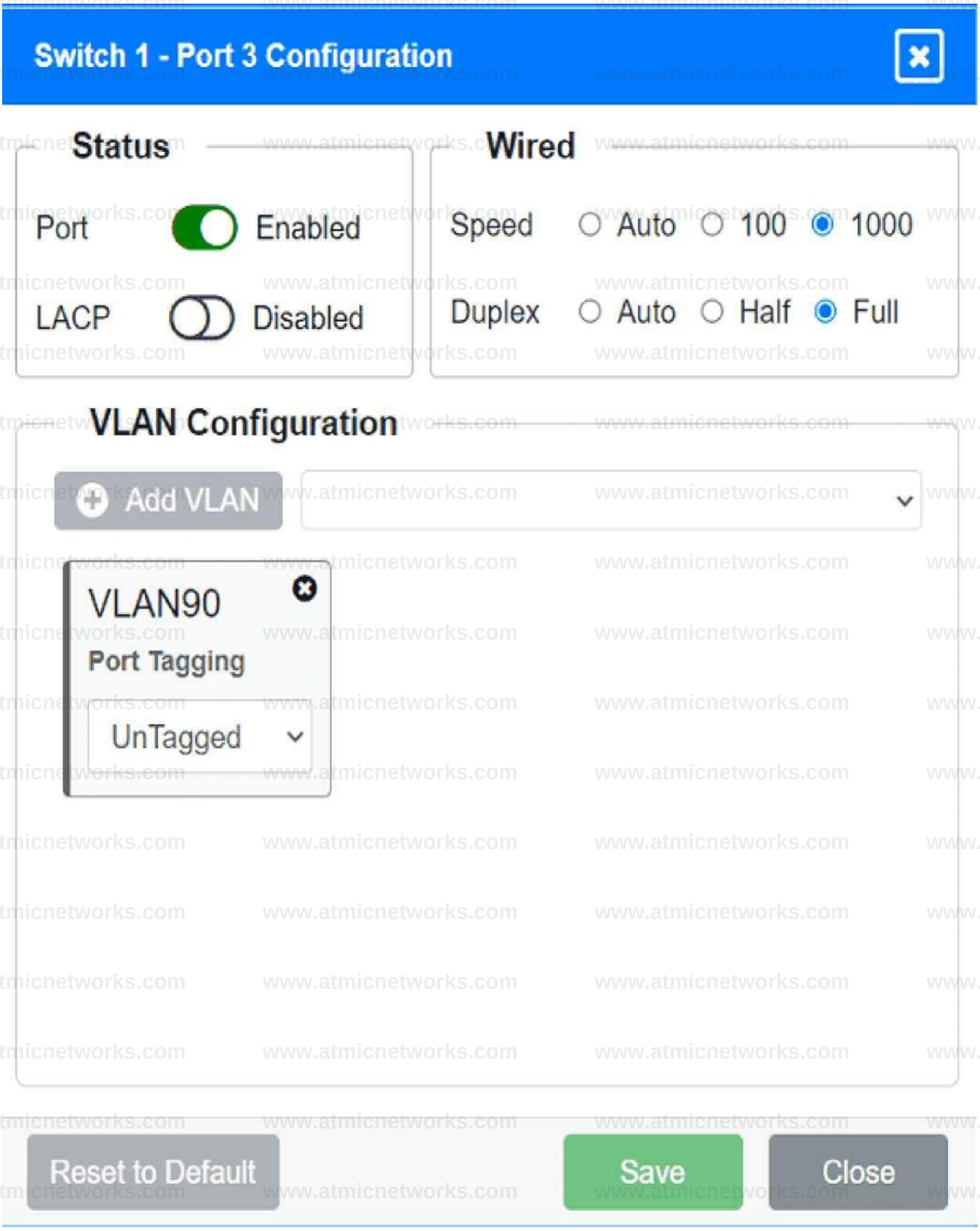
· Ensure each device accesses only its correctly associated network.

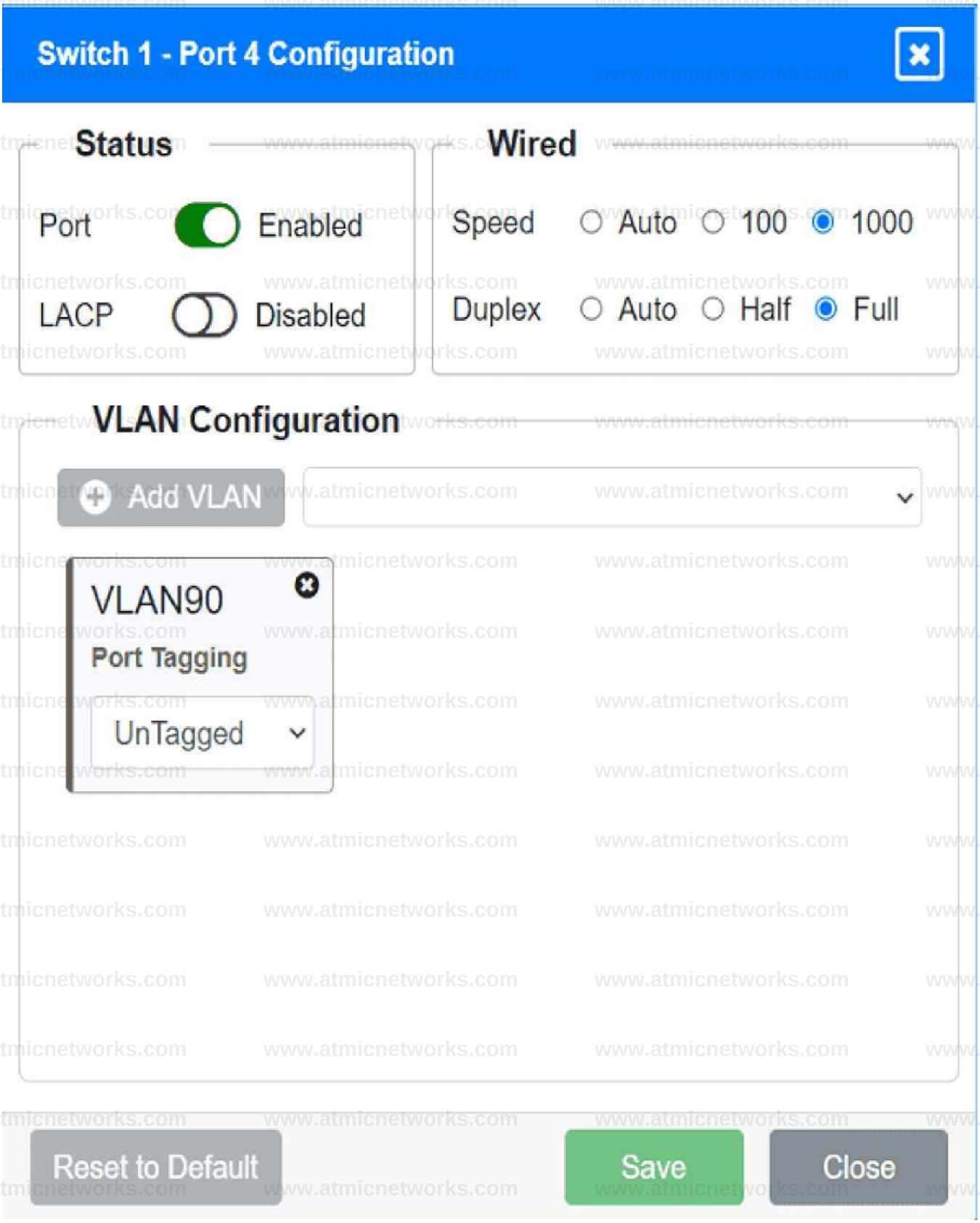
· Disable all unused switchports.

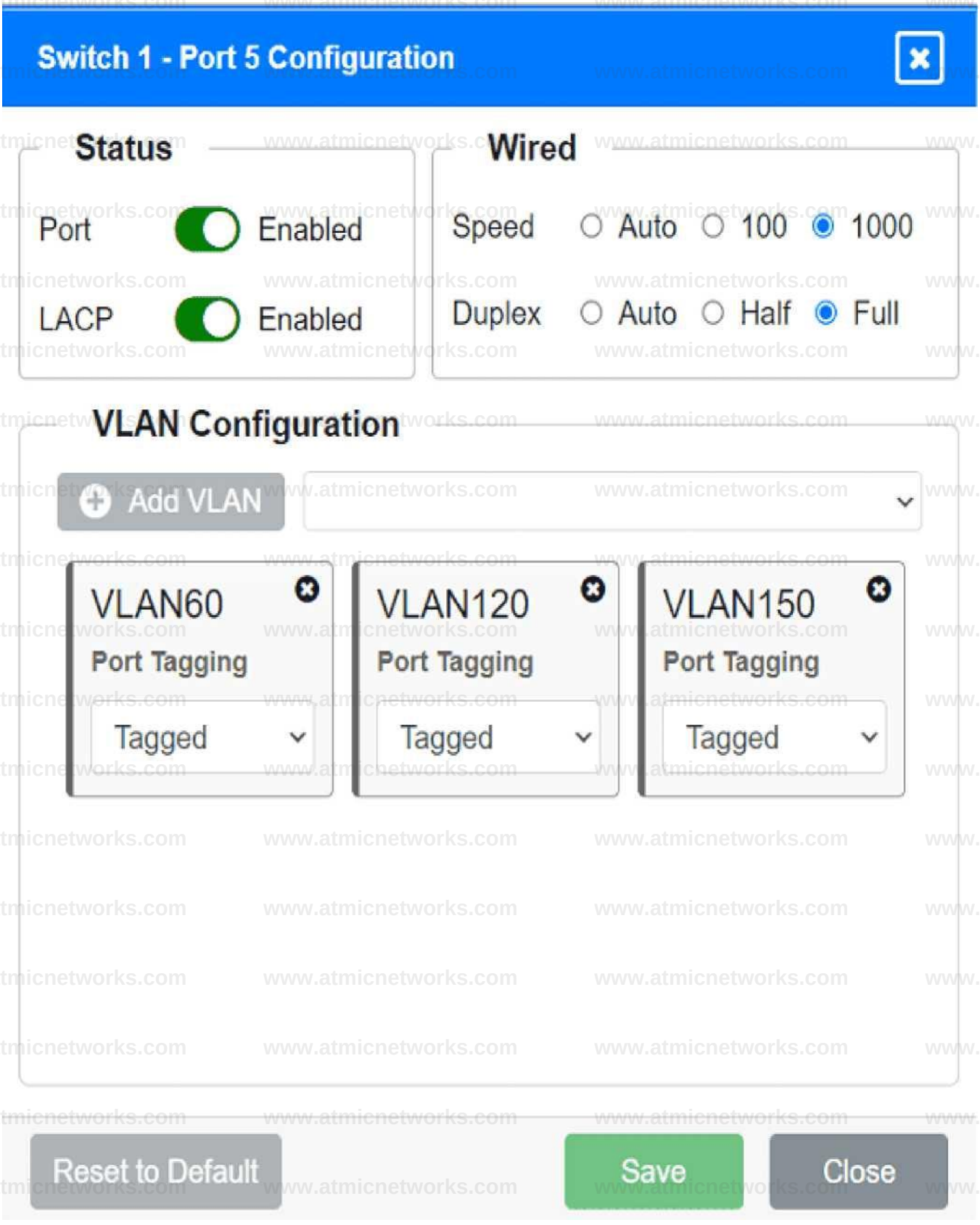
. Require fault-tolerant connections between the switches.

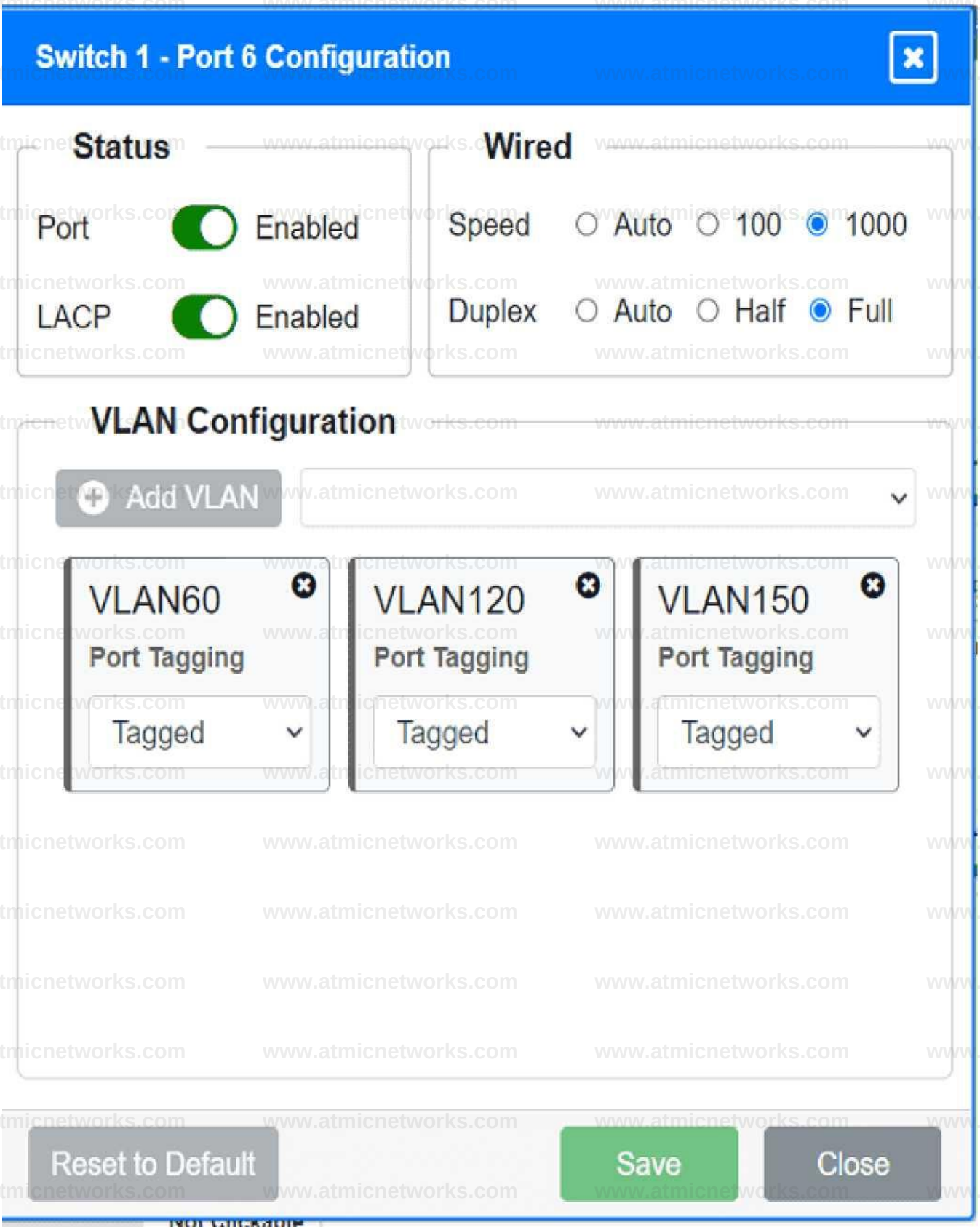
. Only make necessary changes to complete the above requirements.

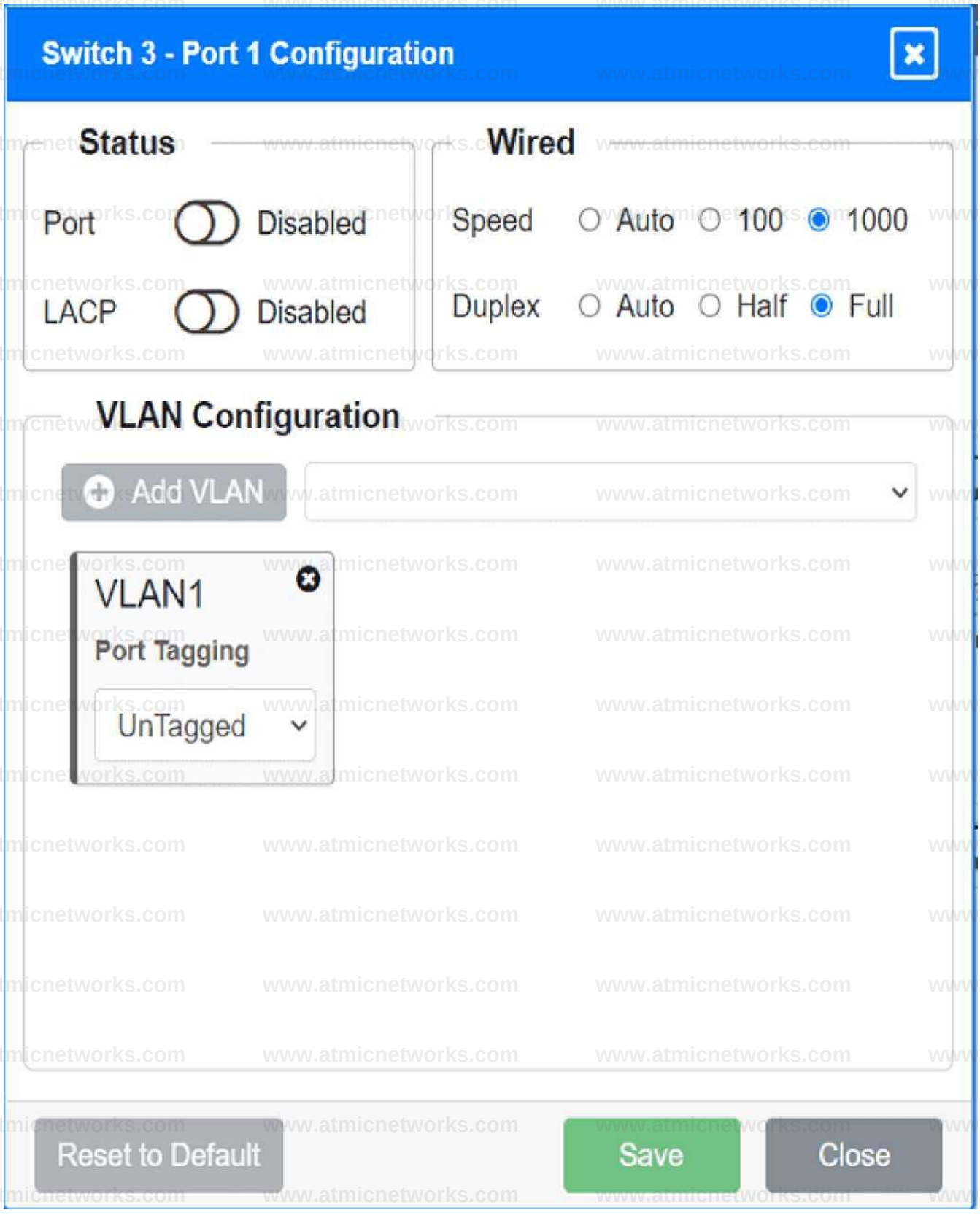


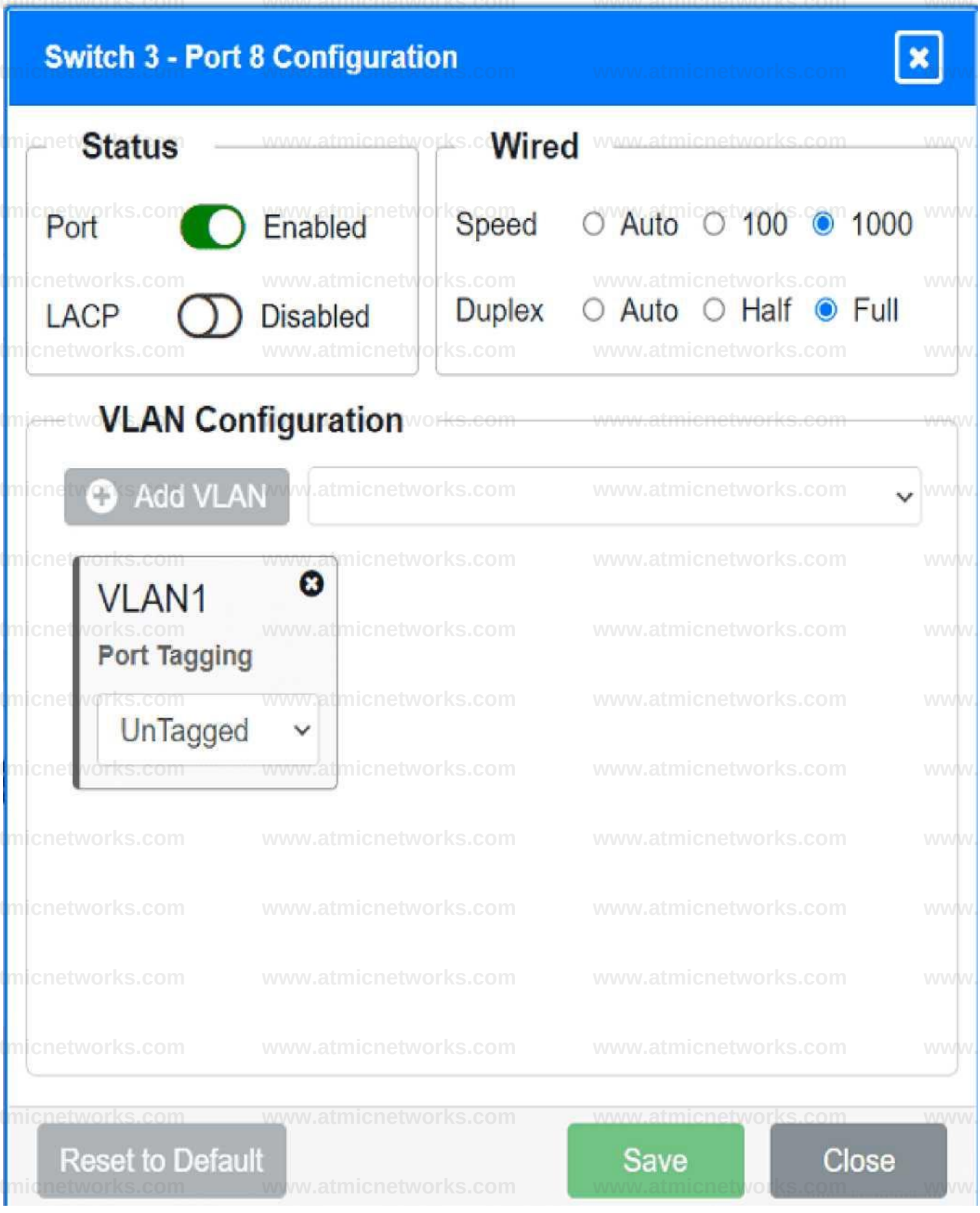









Switch 3 - Port 1 Configuration
Status
Port
Disabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN1
Port Tagging
UnTagged
Reset to Default
Save
Close



Answer: See the solution below in Explanation.

Explanation:

To provide a complete solution for configuring the access layer switches, let's proceed with the following steps:

Identify the correct VLANs for each device and port.

Enable necessary ports and disable unused ports.

Configure fault-tolerant connections between the switches.

Port 1 Configuration (Uplink to Core Switch)

Status: Enabled

LACP: Enabled

Speed: 1000

Duplex: Full

VLAN Configuration: Tagged for VLAN60, VLAN90, VLAN120, VLAN150, VLAN220

Port 2 Configuration (Uplink to Core Switch)

Status: Enabled

LACP: Enabled

Speed: 1000

Duplex: Full

VLAN Configuration: Tagged for VLAN60, VLAN90, VLAN120, VLAN150, VLAN220

Port 3 Configuration (Server Connection)

Status: Enabled

LACP: Disabled

Speed: 1000

Duplex: Full

VLAN Configuration: Untagged for VLAN90 (Servers)

Port 4 Configuration (Server Connection)

Status: Enabled

LACP: Disabled

Speed: 1000

Duplex: Full

VLAN Configuration: Untagged for VLAN90 (Servers)

Port 5 Configuration (Wired Users and WLAN)

Status: Enabled

LACP: Enabled

Speed: 1000

Duplex: Full

VLAN Configuration: Tagged for VLAN60, VLAN120, VLAN150

Port 6 Configuration (Wired Users and WLAN)

Status: Enabled

LACP: Enabled

Speed: 1000

Duplex: Full

VLAN Configuration: Tagged for VLAN60, VLAN120, VLAN150

Port 7 Configuration (Voice and Wired Users)

Status: Enabled

LACP: Enabled

Speed: 1000

Duplex: Full

VLAN Configuration: Tagged for VLAN60, VLAN90, VLAN120, VLAN220

Port 8 Configuration (Voice, Printers, and Wired Users)

Status: Enabled

LACP: Enabled

Speed: 1000

Duplex: Full

VLAN Configuration: Tagged for VLAN60, VLAN90, VLAN120, VLAN220

Port 1 Configuration (Unused)

Status: Disabled

LACP: Disabled

Port 2 Configuration (Unused)

Status: Disabled

LACP: Disabled

Port 3 Configuration (Connection to Device)

Status: Enabled

LACP: Disabled

Speed: 1000

Duplex: Full

VLAN Configuration: Untagged for VLAN1 (Default)

Port 4 Configuration (Connection to Device)

Status: Enabled

LACP: Disabled

Speed: 1000

Duplex: Full

VLAN Configuration: Untagged for VLAN1 (Default)

Port 5 Configuration (Connection to Device)

Status: Enabled

LACP: Disabled

Speed: 1000

Duplex: Full

VLAN Configuration: Untagged for VLAN1 (Default)

Port 6 Configuration (Connection to Device)

Status: Enabled

LACP: Disabled

Speed: 1000

Duplex: Full

VLAN Configuration: Untagged for VLAN1 (Default)

Port 7 Configuration (Connection to Device)

Status: Enabled

LACP: Disabled

Speed: 1000

Duplex: Full

VLAN Configuration: Untagged for VLAN1 (Default)

Ports 1 and 2 on Switch 1 are configured as trunk ports with VLAN tagging enabled for all necessary VLANs.

Ports 3 and 4 on Switch 1 are configured for server connections with VLAN 90 untagged.

Ports 5, 6, 7, and 8 on Switch 1 are configured for devices needing access to multiple VLANs.

Unused ports on Switch 3 are disabled.

Ports 3, 4, 5, 6, and 7 on Switch 3 are enabled for default VLAN1.

Core Switch Ports should be configured as needed for uplinks to Switch 1.
Ensure LACP is enabled for redundancy on trunk ports between switches.
By following these configurations, each device will access only its correctly associated network, unused switch ports will be disabled, and fault-tolerant connections will be established between the switches.

Question: 92

Users cannot connect to an internal website with an IP address 10.249.3.76. A network administrator runs a command and receives the following output:

1 3ms 2ms 3ms 192.168.25.234
2 2ms 3ms 1ms 192.168.3.100
3 4ms 5ms 2ms 10.249.3.1
4 *
5 ’
6 *
7 •

Which of the following command-line tools is the network administrator using?

A. tracert
B. netstat
C. tcpdump
D. nmap

Answer: A

Explanation:

Understanding Tracert:
tracert (Traceroute in Windows) is a command-line tool used to trace the path that packets take from the source to the destination. It records the route (the specific gateways at each hop) and measures transit delays of packets across an IP network.
Output Analysis:
The output shows a series of IP addresses with corresponding round-trip times (RTTs) in milliseconds.
The asterisks (*) indicate that no response was received from those hops, which is typical for routers or firewalls that block ICMP packets used by tracert.
Comparison with Other Tools:
netstat: Displays network connections, routing tables, interface statistics, and more, but does not trace packet routes.
tcpdump: Captures network packets for analysis, used for detailed network traffic inspection.
nmap: A network scanning tool used to discover hosts and services on a network, not for tracing packet routes.
Usage:
tracert helps identify the path to a destination and locate points of failure or congestion in the network.
Reference:
CompTIA Network+ study materials on network troubleshooting and diagnostic tools.

Question: 93

A network engineer configures a new switch and connects it to an existing switch for expansion and redundancy. Users immediately lose connectivity to the network. The network engineer notes the following spanning tree information from both switches:

Switch 1

Port State Cost

1 Forward 2

2 Forward 2

Switch 2

Port State Cost

1 Forward 2

2 Forward 2

Which of the following best describes the issue?

A. The port cost should not be equal.
B. The ports should use link aggregation.
C. A root bridge needs to be identified.
D. The switch should be configured for RSTP.

Answer: C

Explanation:

The issue is that no root bridge has been identified. In STP, a root bridge is necessary to manage redundant paths and avoid loops in the network. Without a root bridge, all switches will assume they can forward traffic, causing a network loop and connectivity problems.

Question: 94

Which of the following attacks would most likely cause duplicate IP addresses in a network?

A. Rogue DHCP server
B. DNS poisoning
C. Social engineering
D. Denial-of-service

Answer: A

Explanation:

Definition of a Rogue DHCP Server:

A rogue DHCP server is an unauthorized DHCP server on a network, which can assign IP addresses to devices

without proper control, leading to IP address conflicts.

Impact of a Rogue DHCP Server:

IP Address Conflicts: Multiple devices may receive the same IP address from different DHCP servers, causing network connectivity issues.

Network Disruption: Devices may be assigned incorrect network configuration settings, disrupting network services and connectivity.

Comparison with Other Attacks:

DNS poisoning: Alters DNS records to redirect traffic to malicious sites, but does not cause IP address conflicts.

Social engineering: Involves manipulating individuals to gain unauthorized access or information, not directly related to IP address conflicts.

Denial-of-service (DoS): Floods a network or service with excessive traffic to disrupt operations, but does not cause duplicate IP addresses.

Prevention and Detection:

Implement network access control measures to prevent unauthorized devices from acting as DHCP servers.

Use DHCP snooping on switches to allow DHCP responses only from authorized DHCP servers.

Reference:

CompTIA Network+ study materials on network security threats and mitigation techniques.

Question: 95

Which of the following best describes the transmission format that occurs at the transport layer over connectionless communication?

A. Datagram
B. Segment
C. Frames
D. Packets

Answer: A

Explanation:

At the transport layer, connectionless communication is typically handled using the User Datagram Protocol (UDP), which transmits data in units called datagrams. Unlike TCP, UDP does not establish a connection before sending data and does not guarantee delivery, making datagrams the correct term for the transmission format in this context. Reference: CompTIA Network+ Exam Objectives and official study guides.

Question: 96

A network technician sets up a computer on the accounting department floor for a user from the marketing department. The user reports that they cannot access the marketing department's shared drives but can access the internet. Which of the following is the most likely cause of this issue?

A. Mismatched switchport duplex

B. Misconfigured gateway settings
C. Incorrect VLAN assignment
D. SVI is assigned to the wrong IP address

Answer: C

Explanation:

The user's inability to access the marketing department's shared drives, despite having internet access, suggests a network segmentation issue. The most likely cause is an incorrect VLAN assignment. The computer is physically located on the accounting department floor, and the switchport is likely configured for the accounting VLAN, not the marketing VLAN. VLANs segment network traffic, and if the computer is in the wrong VLAN, it cannot communicate with the marketing department's resources.

Why not Mismatched switchport duplex? Duplex mismatches cause performance issues (e.g., packet loss) but not specific access denials to shared drives.

Why not Misconfigured gateway settings? Incorrect gateway settings would prevent internet access, which the user has.

Why not SVI is assigned to the wrong IP address? A Switch Virtual Interface (SVI) with an incorrect IP address affects inter-VLAN routing, but this would likely impact multiple users, not just one. Reference:CompTIA Network+ N10-009 Objective 2.2: Explain the purpose of network segmentation and VLAN configuration. The CompTIA Network+ Study Guide (e.g., Chapter 6: Switching) explains that VLANs isolate traffic, and incorrect VLAN assignments prevent access to resources on other VLANs.

Question: 97

Which of the following protocols is used to route traffic on the public internet?

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

Answer: A

Explanation:

Border Gateway Protocol (BGP) is the primary protocol used to route traffic on the public internet. It allows ISPs and large networks to exchange routing information, making it an Exterior Gateway Protocol (EGP).

Breakdown of Options:

A . BGP – Correct answer. Used for internet routing and exchanges routing information between ISPs. B . OSPF – An Interior Gateway Protocol (IGP) used for routing within an autonomous system (not the public internet).

C . EIGRP – Cisco's proprietary IGP, used within private networks, not the public internet.
D . RIP – An older distance-vector protocol, not scalable for the internet.

Reference:

CompTIA Network+ (N10-009) Official Study Guide – Domain 1.4: Explain routing technologies.
RFC 4271: Border Gateway Protocol 4 (BGP-4)

Question: 98

A customer recently moved into a new office and notices that some wall plates are not working and are not properly labeled Which of the following tools would be best to identify the proper wiring in the IDF?

A. Toner and probe
B. Cable tester
C. Visual fault locator
D. Network tap

Answer: A

Explanation:

A toner and probe tool, also known as a tone generator and probe, is used to trace and identify individual cables within a bundle or to locate the termination points of cables in wiring closets and patch panels. It generates a tone that can be picked up by the probe, helping technicians quickly and accurately identify and label wall plates and wiring. This is the best tool for identifying proper wiring in the Intermediate Distribution Frame (IDF). Reference: CompTIA Network+ Exam Objectives and official study guides.

Question: 99

A technician is implementing a new SD-WAN device with a default configuration. The technician receives a URL via email and connects the new device to the internet to complete the installation.
Which of the following is this an example of?

A. SASE device installation
B. Zero-touch provisioning
C. Infrastructure as code
D. Configuration management

Answer: B

Explanation:

This process describes Zero-touch provisioning (ZTP), where a device automatically pulls its configuration from a cloud controller or URL once connected to the internet. It's common in SD-WAN

and modern network appliances.
A . SASE (Secure Access Service Edge) refers to cloud-delivered network security, not a provisioning method.
C . Infrastructure as code automates infrastructure deployment using code, but this scenario specifically fits

ZTP.

D . Configuration management tracks and maintains system configurations but doesn't describe the installation process.

Reference:

CompTIA Network+ N10-009 Official Objectives: 4.3 – Explain remote access methods and automation.

Question: 100

Which of the following typically uses compromised systems that become part of a bot network?

A. Evil twin attack
B. DDoS attack
C. XML injection
D. Brute-force password attack

Answer: B

Explanation:

A DDoS (Distributed Denial of Service) attack is often launched from botnets — networks of compromised systems (bots or zombies) under the control of an attacker. These devices flood the target with traffic to disrupt services.

A . Evil twin attack is a wireless spoofing method.

C . XML injection targets web applications.

D . Brute-force attacks repeatedly guess passwords but don't involve a botnet by default. Reference:

CompTIA Network+ N10-009 Official Objectives: 4.2 – Identify common security threats and vulnerabilities.

Question: 101

A network administrator recently updated configurations on a Layer 3 switch. Following the updates, users report being unable to reach a specific file server. Which of the following is the most likely cause?

A. Incorrect ACLs
B. Switching loop
C. Duplicate IP addresses
D. Wrong default route

Answer: A

Explanation:

- Since this issue occurred after a configuration change on a Layer 3 switch, the most likely cause is misconfigured ACLs (Access Control Lists).
- ACLs control which traffic is allowed or denied, so an incorrect ACL may be blocking access to the file server.
- Why not the other options?
- Switching loop (B): A switching loop occurs at Layer 2 (not Layer 3) and causes network-wide broadcast

storms, not just loss of access to a file server.

- Duplicate IP addresses (C): This would cause connectivity issues for the devices with the conflict, but not necessarily prevent all users from accessing the file server.
- Wrong default route (D): The default route is used for traffic leaving the local network. If users are unable to access an internal file server, this is unlikely to be the issue.

Reference:

CompTIA Network+ (N10-009) Official Guide – Chapter 8: Network Access Control and ACLs

Question: 102

Which of the following connectors allows a singular QSFP transceiver to have several physical connections?

A. RJ45
B. ST
C. LC
D. MPO

Answer: D

Explanation:

The MPO (Multi-fiber Push On) connector is designed to handle multiple fiber strands in a single connector, and it is commonly used with high-density transceivers like QSFP (Quad Small Form-factor Pluggable).

QSFP can support up to four channels (hence "quad"), and MPO connectors can interface multiple fibers (e.g., 8, 12, 24), making them ideal for 40Gbps or 100Gbps deployments.

RJ45 (A) is used for Ethernet over copper.

ST (B) and LC (C) are single-fiber connectors — they don't support the multi-fiber needs of QSFP setups.

Q Therefore, MPO is the correct connector type for this use case.

Reference:CompTIA Network+ N10-009 Official Study Guide — Objective 3.1: "Compare and contrast different types of connectors and transceivers."

Question: 103

A network engineer discovers network traffic that is sending confidential information to an unauthorized and unknown destination. Which of the following best describes the cause of this network traffic?

A. Adware
B. Ransomware
C. Darkware
D. Malware

Answer: D

Explanation:

Malware refers to any malicious software that can exfiltrate confidential data, including spyware, trojans, and rootkits. This fits the scenario where unauthorized data transfer is occurring.

Breakdown of Options:

A . Adware – Displays ads, does not typically steal data.

B . Ransomware – Encrypts files but does not exfiltrate data.

C . Darkware – Not a real cybersecurity term.

D . Malware – Correct answer. Malicious software is responsible for unauthorized data exfiltration.

Reference:

CompTIA Network+ (N10-009) Official Study Guide – Domain 3.5: Given a scenario, implement cybersecurity measures.

NIST 800-83: Malware Incident Prevention & Handling

Question: 104

Users at an organization report that the wireless network is not working in some areas of the building. Users report that other wireless network SSIDs are visible when searching for the network, but the organization's network is not displayed. Which of the following is the most likely cause?

A. Interference or channel overlap
B. Insufficient wireless coverage
C. Roaming misconfiguration
D. Client disassociation issues

Answer: B

Explanation:

If the company's SSID is not visible in some areas while other networks are still visible, the most likely cause is insufficient wireless coverage. The wireless signal does not reach those areas, meaning additional access points or signal boosters may be required.

Breakdown of Options:

A . Interference or channel overlap – Would cause slow or unstable connections, but the SSID should still be visible.

B . Insufficient wireless coverage – Q Correct answer. If the SSID is not appearing, the signal is too weak in that area.

C . Roaming misconfiguration – Would cause devices to stay on weaker APs instead of switching, but the SSID should still be visible.

D . Client disassociation issues – This would disconnect users, but they should still see the network.

Reference:

CompTIA Network+ (N10-009) Official Study Guide – Domain 1.6: Explain wireless concepts and technologies.

Question: 105

An administrator is configuring a switch that will be placed in an area of the office that is accessible to

customers. Which of the following is the best way for the administrator to mitigate unknown devices from connecting to the network?

A. SSE
B. ACL
C. Perimeter network
D. 802.1x

Answer: D

Explanation:

802.1x is a network access control protocol that provides an authentication mechanism to devices trying to connect to a LAN or WLAN. This ensures that only authorized devices can access the network, making it ideal for mitigating the risk of unknown devices connecting to the network, especially in accessible areas.
802.1x Authentication: Requires devices to authenticate using credentials (e.g., username and password, certificates) before gaining network access.
Access Control: Prevents unauthorized devices from connecting to the network, enhancing security in public or semi-public areas.
Implementation: Typically used in conjunction with a RADIUS server to manage authentication requests.
Network Reference:
CompTIA Network+ N10-007 Official Certification Guide: Covers 802.1x and its role in network security.
Cisco Networking Academy: Provides training on implementing 802.1x for secure network access control.
Network+ Certification All-in-One Exam Guide: Explains the benefits and configuration of 802.1x authentication in securing network access.

Question: 106

Which of the following is most closely associated with a dedicated link to a cloud environment and may not include encryption?

A. Direct Connect
B. Internet gateway
C. Captive portal
D. VPN

Answer: A

Explanation:

Direct Connect refers to a dedicated network connection between an on-premises network and a cloud service provider (such as AWS Direct Connect). This link bypasses the public internet, providing a more reliable and higher-bandwidth connection. It may not inherently include encryption because it relies on the security measures of the dedicated physical connection itself. In contrast, other options like VPN typically involve encryption as they traverse the public internet.

Reference:

CompTIA Network+ full course material indicates that Direct Connect type services offer dedicated, private connections which might not include encryption due to the dedicated and secure nature of the link itself.

Question: 107

Which of the following ports is used for secure email?

A. 25
B. 110
C. 143
D. 587

Answer: D

Explanation:

Port 587 is used for secure email submission. This port is designated for message submission by mail clients to mail servers using the SMTP protocol, typically with STARTTLS for encryption.

Port 25: Traditionally used for SMTP relay, but not secure and often blocked by ISPs for outgoing mail due to spam concerns.

Port 110: Used for POP3 (Post Office Protocol version 3), not typically secured.

Port 143: Used for IMAP (Internet Message Access Protocol), which can be secured with STARTTLS or SSL/TLS.

Port 587: Specifically used for authenticated email submission (SMTP) with encryption, ensuring secure transmission of email from clients to servers.

Network Reference:

CompTIA Network+ N10-007 Official Certification Guide: Discusses email protocols and ports, including secure email transmission.

Cisco Networking Academy: Provides training on securing email communications and the use of appropriate ports.

Network+ Certification All-in-One Exam Guide: Explains email protocols, ports, and security considerations for email transmission.

Question: 108

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

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

Answer: B

Explanation:

VLAN hopping is an attack where an attacker crafts packets with multiple VLAN tags, allowing them to traverse VLAN boundaries improperly. This can result in gaining unauthorized access to network segments that are supposed to be isolated. The other options do not involve the use of multiple network tags. MAC flooding aims to overwhelm a switch's MAC address table, DNS spoofing involves forging DNS responses, and ARP poisoning involves sending fake ARP messages.

Reference:

According to the CompTIA Network+ course materials, VLAN hopping exploits the tagging mechanism in network packets to gain unauthorized access.

Question: 109

SIMULATION

You are tasked with verifying the following requirements are met in order to ensure network security.

Requirements:

Datacenter

Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage

Provide a dedicated server to resolve IP addresses and hostnames correctly and handle port 53 traffic

Building A

Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage

Provide devices to support 5 additional different office users

Add an additional mobile user

Replace the Telnet server with a more secure solution

Screened subnet

Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage

Provide a server to handle external 80/443 traffic

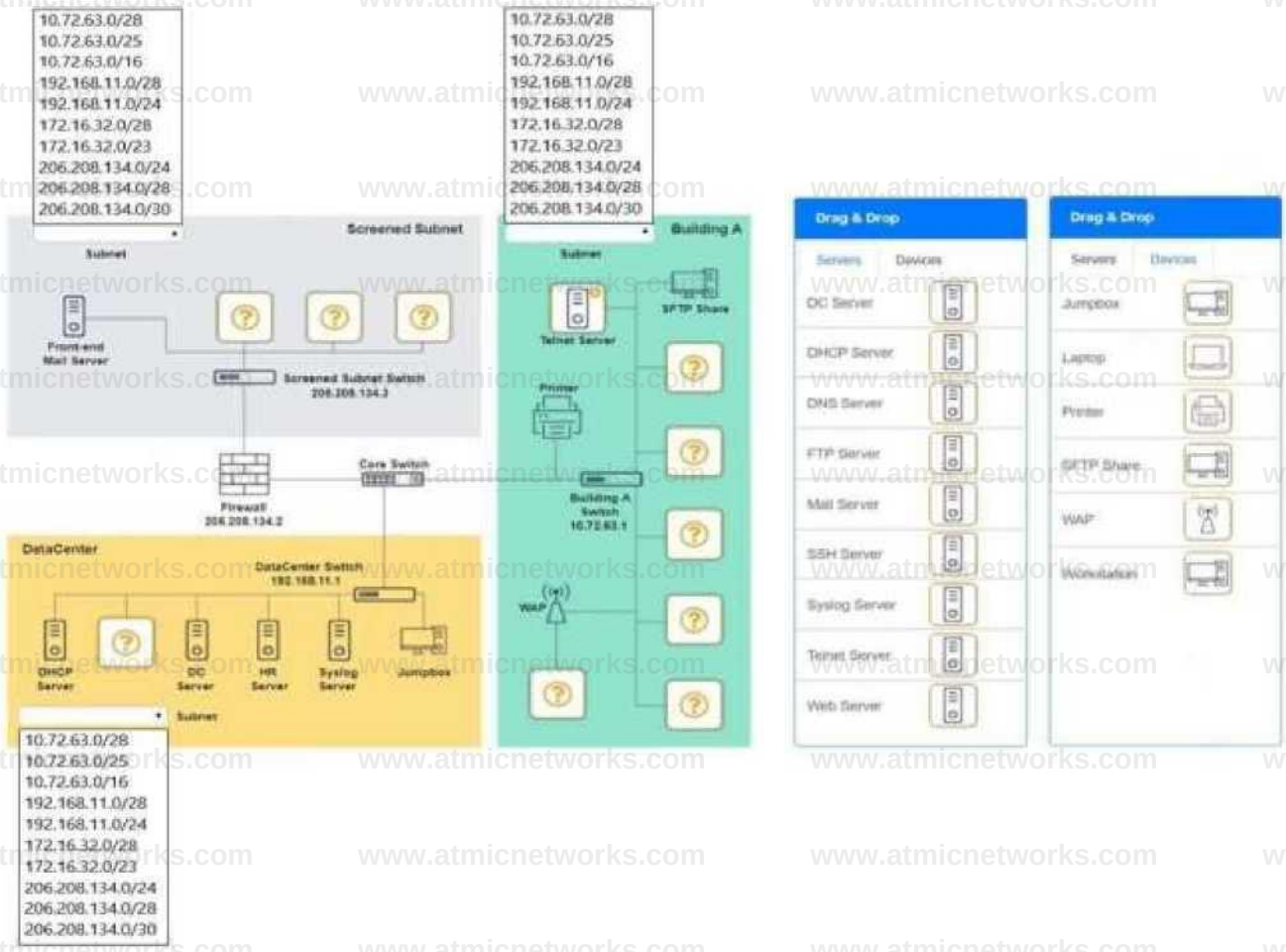
Provide a server to handle port 20/21 traffic

INSTRUCTIONS

Drag and drop objects onto the appropriate locations. Objects can be used multiple times and not all placeholders need to be filled.

Available objects are located in both the Servers and Devices tabs of the Drag & Drop menu.

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

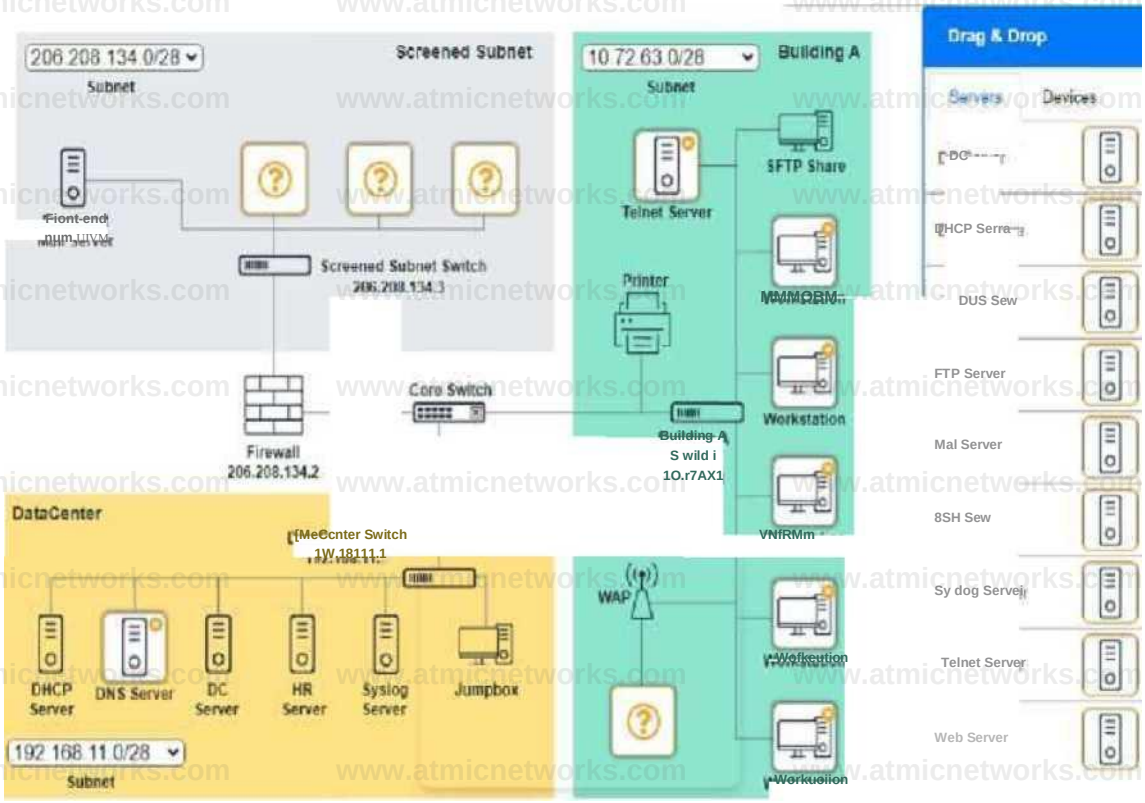


Answer: See explanation below.

Explanation:

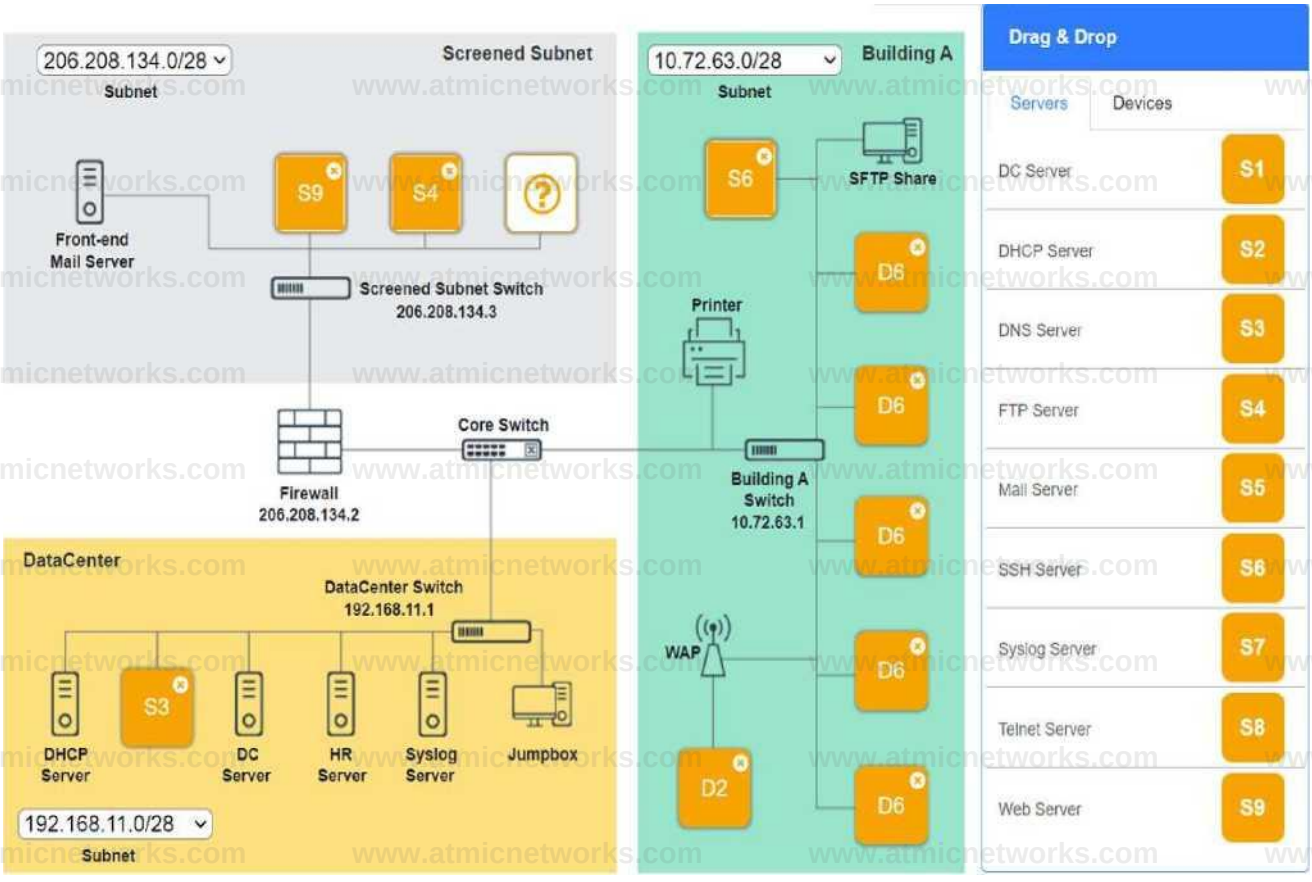
Screened Subnet devices – Web server, FTP server

Building A devices – SSH server top left, workstations on all 5 on the right, laptop on bottom left DataCenter devices – DNS server.



b

A screenshot of a computer AI-generated content may be incorrect.



A screenshot of a computer AI-generated content may be incorrect.

A screenshot of a computer AI-generated content may be incorrect.

Question: 110

A network technician receives a new ticket while working on another issue. The new ticket is critical to business operations. Which of the following documents should the technician reference to determine which ticket to complete first?

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

Answer: C

Explanation:

An SLA (Service Level Agreement) defines performance expectations, including response time, prioritization, and resolution time for services and support issues. It helps the technician determine which task has higher priority based on business impact.

A . NDA (Non-Disclosure Agreement) relates to confidentiality, not task prioritization.

B . AUP (Acceptable Use Policy) defines user behavior, not issue handling.

D . MOU (Memorandum of Understanding) outlines informal agreements and doesn't define ticket priorities.

Reference:

CompTIA Network+ N10-009 Official Objectives: 4.1 – Compare and contrast common documentation types.

Question: 111

A network administrator installs new cabling to connect new computers and access points. After deploying the equipment, the administrator notices a few of the devices are not connecting properly. The administrator moves the devices to a different port, but it does not resolve the issue. Which of the following should the administrator verify next?

A. Power budget
B. Device requirements
C. Port status
D. Cable termination

Answer: D

Explanation:

- Cable termination issues (e.g., improper crimping, loose connectors) can cause connectivity failures.
- Power budget (A) applies to PoE devices, not general cabling issues.
- Device requirements (B) relate to software/hardware compatibility, not wiring faults.
- Port status (C) would help if the issue was switch-related, but since moving devices didn't help, it's likely a cabling issue.

Reference: CompTIA Network+ N10-009 Official Documentation – Cabling & Physical Layer Troubleshooting.

Question: 112

A user's home mesh wireless network is experiencing latency issues. A technician has:

- Performed a speed test.
- Rebooted the devices.
- Performed a site survey.
- Performed a wireless packet capture.

The technician reviews the following information:

The technician notices in the packet capture that frames were retransmitted. Which of the following is the most likely cause of the user's network issue?

A. The SSIDs should not be the same.
B. The network has too much overlap.
C. The devices are incompatible with the mesh network.
D. The nodes are underpowered.

Answer: B

Explanation:

- Too much overlap on the same channel (all devices on channel 11) causes interference, leading to retransmissions and high latency.
- Same SSIDs (A) are expected in mesh networks.
- Device compatibility (C) would show different symptoms.
- Node power (D) affects coverage, not congestion.

Reference: CompTIA Network+ N10-009 Official Documentation – Wireless Troubleshooting & Signal Interference.

Question: 113

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 reason?

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

Answer: B

Explanation:

When installing multiple Power over Ethernet (PoE) devices like security cameras, it is crucial to ensure that the total power requirement does not exceed the power budget of the PoE switch. Each PoE switch has a maximum power capacity, and exceeding this capacity can cause some devices to fail to receive power.

PoE Standards: PoE switches conform to standards such as IEEE 802.3af (PoE) and 802.3at (PoE+), each with specific power limits per port and total power capacity.
Power Calculation: Adding up the power requirements of all connected PoE devices can help determine if the total power budget of the switch is exceeded.
Symptoms: When the power budget is exceeded, some devices, typically those farthest from the switch or connected last, may not power up or function correctly.
Network Reference:
CompTIA Network+ N10-007 Official Certification Guide: Covers PoE standards and troubleshooting power issues.
Cisco Networking Academy: Discusses PoE technologies, power budgeting, and managing PoE devices.
Network+ Certification All-in-One Exam Guide: Provides information on PoE setup, including power budget considerations.

Question: 114

A network engineer is setting up a new VoIP network for a customer. The current network is segmented only for computers and servers. No additional switch ports can be used in the new network. Which of the following does the engineer need to do to configure the network correctly? (Select TWO).

A. Change network translation definitions
B. Enable 802.1Q
C. Implement a routing protocol
D. Set up voice VLANs
E. Reconfigure the DNS
F. Place devices in the perimeter network

Answer: B,D

Explanation:

To support VoIP on the same physical ports used by computers:
B . Enable 802.1Q: This standard supports VLAN tagging, allowing voice and data traffic to share the same port using separate VLANs.
D . Set up voice VLANs: Separating voice traffic into its own VLAN improves QoS and manageability.
Other options are not directly related to configuring VoIP over existing ports:
A . Network translation definitions (NAT) are unrelated to switch-level VLAN configuration.
C . Routing protocols are not necessary at the switch level for VLAN setup.
E . DNS is not required for the switch or VLAN setup.
F . Perimeter network (DMZ) is used for public-facing servers, not VoIP VLANs.
Reference:
CompTIA Network+ N10-009 Official Objectives: 2.3 – Given a scenario, configure and verify VLANs.
CompTIA Network+ N10-009 Official Objectives: 3.6 – Explain the characteristics of network topologies and types.

Question: 115

A network administrator wants to configure a backup route in case the primary route fails. A dynamic routing protocol is not installed on the router. Which of the following routing features should the administrator choose to accomplish

this task?

A. Neighbor adjacency
B. Link state flooding
C. Administrative distance
D. Hop count

Answer: C

Explanation:

Introduction to Administrative Distance

Administrative distance (AD) is a value used by routers to rank routes from different routing protocols. AD represents the trustworthiness of the source of the route. Lower AD values are more preferred. If a router has multiple routes to a destination from different sources, it will choose the route with the lowest AD.

Static Routes and Backup Routes

When a dynamic routing protocol is not used, static routes can be employed. Static routes are manually configured routes. To ensure a backup route, multiple static routes to the same destination can be configured with different AD values.

Configuring Static Routes with Administrative Distance

The primary route is configured with a lower AD value, making it the preferred route. The backup route is configured with a higher AD value. In the event of the primary route failure, the router will then use the backup route.

Example Configuration:

plaintext

Copy code

ip route 192.168.1.0 255.255.255.0 10.0.0.1 1

ip route 192.168.1.0 255.255.255.0 10.0.0.2 10

In the above example, 192.168.1.0/24 is the destination network.

10 .0.0.1 is the next-hop IP address for the primary route with an AD of 1.

11 .0.0.2 is the next-hop IP address for the backup route with an AD of 10.

Verification:

After configuration, use the show ip route command to verify that the primary route is in use and the backup route is listed as a candidate for use if the primary route fails.

Reference:

CompTIA Network+ guide explains the concept of administrative distance and its use in static routing configuration (see page Ref 9†Basic Configuration Commands).

Question: 116

A user's desk has a workstation and an IP phone. The user is unable to browse the internet on the workstation, but the phone works. Which of the following configurations is required?

A. Voice VLAN
B. Native VLAN
C. Data VLAN
D. Trunk port

Answer: C

Explanation:

If the IP phone works but the workstation doesn't, it indicates that the Voice VLAN is functioning correctly, but the Data VLAN (C) is either misconfigured or missing. The workstation typically connects through the phone, which tags voice and data traffic separately using VLANs.

A . Voice VLAN is for the IP phone, which is already working.

B . Native VLAN is for untagged traffic on trunk ports, but doesn't control access directly.

D . Trunk port is more relevant to switch interconnections than individual workstation ports.

Reference:

CompTIA Network+ N10-009 Official Objectives: 2.3 – Given a scenario, configure and verify VLANs.

Question: 117

A network administrator needs to divide 192.168.1.0/24 into two equal halves. Which of the following subnet masks should the administrator use?

A. 255.255.0.0
B. 255.255.254.0
C. 255.255.255.0
D. 255.255.255.128

Answer: D

Explanation:

Understanding Subnetting:

Original Network: 192.168.1.0/24 has a subnet mask of 255.255.255.0, which allows for 256 IP addresses (including network and broadcast addresses).

Objective: Divide this network into two equal subnets.

Calculating Subnet Mask:

New Subnet Mask: To divide 192.168.1.0/24 into two equal halves, we need to borrow one bit from the host portion of the address, changing the subnet mask to 255.255.255.128 (/25).

Subnet Breakdown:

First Subnet: 192.168.1.0/25 (192.168.1.0 - 192.168.1.127)

Second Subnet: 192.168.1.128/25 (192.168.1.128 - 192.168.1.255)

Verification:

Each subnet now has 128 IP addresses (126 usable IP addresses, excluding the network and broadcast addresses).

Comparison with Other Options:

255.255. 0.0 (/16): Provides a much larger network, not dividing the original /24 network.

255.255.254. 0 (/23): Also creates a larger subnet, encompassing more than the original /24 network.

255.255.255. 0 (/24): Maintains the original subnet size, not dividing it.

Reference:

CompTIA Network+ study materials on subnetting and IP addressing.

Question: 118

Due to concerns around single points of failure, a company decided to add an additional WAN to the network. The company added a second MPLS vendor to the current MPLS WAN and deployed an additional WAN router at each site. Both MPLS providers use OSPF on the WAN network, and EIGRP is run internally. The first site to go live with the new WAN is successful, but when the second site is activated, significant network issues occur. Which of the following is the most likely cause for the WAN instability?

A. A changed CDP neighbor
B. Asymmetrical routing
C. A switching loop
D. An incorrect IP address

Answer: B

Explanation:

Asymmetrical routing occurs when packets take different paths to and from the destination, leading to instability in network communication. The use of two different MPLS providers with OSPF can lead to this type of routing issue, especially if the paths aren't carefully configured and managed. This can cause unexpected routing behaviors and instability in a dual-WAN setup. (Reference: CompTIA Network+ Study Guide, Chapter on Network Routing)

Question: 119

Which of the following services runs on port 636?

A. SMTP
B. Syslog
C. TFTP
D. LDAPS

Answer: D

Explanation:

LDAP over SSL (LDAPS) uses port 636 to provide secure, encrypted authentication for directory services.
Breakdown of Options:
A . SMTP (Simple Mail Transfer Protocol) – Uses port 25, not 636.
B . Syslog – Uses port 514 (UDP), not 636.
C . TFTP (Trivial File Transfer Protocol) – Uses port 69 (UDP), not 636.
D . LDAPS (Lightweight Directory Access Protocol Secure) – Q Correct answer. Uses port 636 for secure directory authentication.
Reference:
CompTIA Network+ (N10-009) Official Study Guide – Domain 3.1: Compare and contrast network protocols.
RFC 4511: Lightweight Directory Access Protocol (LDAP)

Question: 120

A Chief Executive Officer (CEO) of a company purchases a new phone that will be used while traveling to different countries. The CEO needs to be able to place outgoing calls and receive incoming calls on the phone using a SIM card. Which of the following cellular technologies does the CEO's phone need?

A. WDMA
B. CDMA
C. GSM
D. SLA

Answer: C

Explanation:

GSM (Global System for Mobile communications) is the international standard that uses SIM cards to authenticate and connect phones to the cellular network. GSM allows users to place and receive calls while traveling globally, provided they have a SIM card. CDMA, on the other hand, does not use SIM cards in the same way and is primarily used in the United States. (Reference: CompTIA Network+ Study Guide, Chapter on Network Fundamentals)

Question: 121

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 turn 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:

When working with fiber optic cables, one common issue is that the transmit (TX) and receive (RX) fibers might be reversed. The first step in troubleshooting should be to reverse the fibers at one end to ensure they are correctly aligned (TX to RX and RX to TX). This is a simple and quick step to rule out a common issue before moving on to more complex troubleshooting.Reference: CompTIA Network+ study materials.

Question: 122

In an environment with one router, which of the following will allow a network engineer to communicate between VLANs without purchasing additional hardware?

A. Subinterfaces
B. VXLAN
C. Layer 3 switch
D. VIR

Answer: A

Explanation:

A subinterface is a logical interface created on a single physical router interface that allows routing between VLANs (known as Router-on-a-Stick (ROAS)). This method is commonly used when only one physical router is available, allowing inter-VLAN communication without additional hardware.

- Why not the other options?
- VXLAN (B) – This is used for extending Layer 2 networks over a Layer 3 infrastructure, primarily in data centers. It does not directly enable inter-VLAN communication.
- Layer 3 switch (C) – A Layer 3 switch can route between VLANs, but the scenario states that purchasing additional hardware is not an option.
- VIR (D) – This is not a standard networking term in the context of VLAN communication. Reference:

CompTIA Network+ (N10-009) Official Guide – Chapter 8: VLANs and Inter-VLAN Routing

Question: 123

Which of the following protocol ports should be used to securely transfer a file?

A. 22
B. 69
C. 80
D. 3389

Answer: A

Explanation:

Port 22 is used for SFTP (Secure File Transfer Protocol) and SCP (Secure Copy Protocol), which encrypt file transfers using SSH (Secure Shell). This ensures data is transmitted securely over the network.

- Why not the other options?
- Port 69 (B) – TFTP (Trivial File Transfer Protocol): Transfers files but is not secure (no encryption).
- Port 80 (C) – HTTP: Used for web traffic, not for file transfer.
- Port 3389 (D) – RDP (Remote Desktop Protocol): Used for remote desktop access, not file transfer. Reference:

CompTIA Network+ (N10-009) Official Guide – Chapter 5: Network Protocols and Ports

Question: 124

A university is implementing a new campus wireless network. A network administrator needs to configure the network to support a large number of devices and high-bandwidth demands from students.

Which of the following wireless technologies should the administrator consider for this scenario?

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

Answer: B

Explanation:

Wi-Fi 6E is the best choice for high-density environments, such as a university campus. It:
Supports more devices with OFDMA (Orthogonal Frequency-Division Multiple Access)
Uses the 6GHz band, reducing congestion
Provides faster speeds and lower latency
This makes Wi-Fi 6E ideal for large networks with high-bandwidth demands, like those in a university setting.

Breakdown of Options:
A . Bluetooth – Used for short-range, low-power connections, not large-scale wireless networks.
B . Wi-Fi 6E – Q Correct answer. Designed for high-density environments, improving speed and efficiency.
C . 5G – Used for mobile networks, but not ideal for campus-wide local wireless infrastructure.
D . LTE – Used for cellular data, not for campus-wide Wi-Fi.
Reference:
CompTIA Network+ (N10-009) Official Study Guide – Domain 1.6: Compare and contrast wireless networking technologies.
IEEE 802.11ax (Wi-Fi 6E): Enhancements for high-efficiency wireless networking

Question: 125

A company recently converted most of the office laptops to connect wirelessly to the corporate network. After a high-traffic malware attack, narrowing the event to a specific user was difficult because of the wireless configuration. Which of the following actions should the company take?

A. Restrict users to the 5GHz frequency.
B. Upgrade to a mesh network.
C. Migrate from PSK to Enterprise.
D. Implement WPA2 encryption.

Answer: C

Explanation:

Using Pre-Shared Key (PSK) authentication means that all users share the same Wi-Fi password, making it difficult to identify individual users when security incidents occur.
Migrating to WPA2-Enterprise (or WPA3-Enterprise) replaces PSK authentication with individual user credentials using 802.1X authentication and a RADIUS server. This allows the organization to: Track and log specific user activity
Enforce per-user authentication policies
Improve network security

Breakdown of Options:

A . Restrict users to the 5GHz frequency – Improves performance but does not enhance user tracking or security.

B . Upgrade to a mesh network – A mesh network improves coverage, not security tracking.

C . Migrate from PSK to Enterprise – Q Correct answer. WPA2-Enterprise or WPA3-Enterprise uses individual user authentication, allowing per-user tracking.

D . Implement WPA2 encryption – WPA2 is already widely used; it does not resolve the tracking issue.

Reference:

CompTIA Network+ (N10-009) Official Study Guide – Domain 3.4: Given a scenario, implement wireless security measures.

IEEE 802.1X: Authentication framework for network access control

Question: 126

Which of the following would most likely be utilized to implement encryption in transit when using HTTPS?

A. SSH

B. TLS

C. SCADA

D. RADIUS

Answer: B

Explanation:

TLS (Transport Layer Security) is the protocol that provides encryption in transit for HTTPS. It ensures data is encrypted between the client (browser) and the web server, protecting it from interception or tampering.

A . SSH is used for secure terminal access, not HTTPS.

C . SCADA refers to control systems, not encryption protocols.

D . RADIUS is an authentication protocol, not for encrypting HTTPS traffic.

Reference:

CompTIA Network+ N10-009 Official Objectives: 4.2 – Identify common security threats and vulnerabilities.

CompTIA Network+ N10-009 Official Objectives: 4.6 – Explain authentication and access controls.

Question: 127

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

A. 255.255.255.128

B. 255.255.255.192

C. 255.255.255.224

D. 255.255.255.240

Answer: D

Explanation:

Reference: CompTIA Network+ Certification Exam Objectives - IP Addressing section.

Question: 128

A network administrator notices uncommon communication between VMs on ephemeral ports on the same subnet. The administrator is concerned about that traffic moving laterally within the network. Which of the following describes the type of traffic flow the administrator is analyzing?

A. East-west
B. Point-to-point
C. Horizontal-scaling
D. Hub-and-spoke

Answer: A

Explanation:

When traffic moves laterally between VMs within the same network or subnet, it is known as eastwest traffic. This contrasts with north-south traffic, which refers to communication between internal and external networks.
Breakdown of Options:
A . East-west – Correct answer. This refers to traffic between internal servers or VMs, which is a common security concern.
B . Point-to-point – Point-to-point describes a direct connection between two devices, but does not specifically define lateral movement.
C . Horizontal-scaling – This refers to adding more instances or nodes in cloud computing, unrelated to traffic flow.
D . Hub-and-spoke – This network topology describes a centralized design, not lateral traffic. Reference:
CompTIA Network+ (N10-009) Official Study Guide – Domain 1.4: Analyze traffic patterns and behavior.
NIST SP 800-207: Zero Trust Architecture (ZTA) – East-West traffic monitoring

Question: 129

A customer calls the help desk to report issues connection to the internet. The customer can reach a local database server. A technician goes to the site and examines the configuration:

Which of the following is causing the user's issue?

A. Incorrect DNS
B. Unreachable gateway
C. Failed root bridge
D. Poor upstream routing

Answer: B

Explanation:

The customer can access local resources (a database server), which means local networking is working. However, the inability to reach the internet suggests an issue with the default gateway. If the default gateway is unreachable, packets will not be routed outside the local network.

Breakdown of Options:

A . Incorrect DNS – DNS issues would cause problems resolving domain names, but the user should still be able to access external resources via IP addresses.

B . Unreachable gateway – Q Correct answer. If the default gateway is incorrect or unreachable, the device cannot route traffic to the internet.

C . Failed root bridge – STP (Spanning Tree Protocol) failures cause switching issues, but the user can still access local devices, meaning STP is not the problem.

D . Poor upstream routing – Would affect the entire network, not just one user.

Reference:

CompTIA Network+ (N10-009) Official Study Guide – Domain 2.3: Explain network routing concepts.

Question: 130

Which of the following is a cost-effective advantage of a split-tunnel VPN?

A. Web traffic is filtered through a web filter.
B. More bandwidth is required on the company's internet connection.
C. Monitoring detects insecure machines on the company's network.
D. Cloud-based traffic flows outside of the company's network.

Answer: D

Explanation:

A split-tunnel VPN allows certain traffic (e.g., cloud-based services) to bypass the VPN and go directly to the Internet. This reduces the amount of traffic that needs to traverse the company's VPN and Internet connection, conserving bandwidth and reducing costs. It also means that not all traffic is subject to the same level of inspection or filtering, which can improve performance for cloud-based services.Reference: CompTIA Network+ study materials.

Question: 131

A user cannot access an external server for a client after connecting to a VPN. Which of the following commands would a support agent most likely use to examine the issue? (Select two).

A. nslookup
B. tcpdump
C. arp
D. dig
E. tracert
F. route print

Answer: E,F

Explanation:

When a user connects to a VPN and experiences connectivity issues to an external server, the problem is often related

to routing or network path issues.

E . tracert:

Traces the path packets take from the user's device to the destination server.

Helps determine if the traffic is being blocked or misrouted.

F . route print:

Displays the device's routing table.

Helps diagnose whether traffic is being sent to the VPN tunnel instead of the correct external server.

Incorrect Options:

A . nslookup: Used for resolving domain names to IPs (DNS troubleshooting), but this issue is likely routing-related.

B . tcpdump: Captures packets for deep packet analysis, not typically the first step in diagnosing a VPN-related access issue.

C . arp: Used for resolving local network MAC addresses, not relevant for external VPN issues.

D . dig: Like nslookup, used for DNS queries, but not useful for routing problems.

Reference:

CompTIA Network+ N10-009 Official Study Guide – Chapter on Troubleshooting Network Connectivity

Question: 132

Which of the following facilities is the best example of a warm site in the event of information system disruption?

A. A combination of public and private cloud services to restore data
B. A partial infrastructure, software, and data on site
C. A full electrical infrastructure in place, but no customer devices on site
D. A full infrastructure in place, but no current data on site

Answer: D

Explanation:

A warm site typically has a full infrastructure ready, but it lacks the most up-to-date data or is not immediately operational. It requires some configuration or data restoration to become fully functional.

Question: 133

Which of the following is most commonly associated with many systems sharing one IP address in the public IP-addressing space?

A. PAT
B. NAT
C. VIP
D. NAT64

Answer: A

Explanation:

Port Address Translation (PAT) allows multiple internal devices to share a single public IP address by assigning each device a unique port number. This is the most common method used in environments where many systems need internet access but there are limited public IP addresses.

Question: 134

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

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

Answer: B

Explanation:

Content filtering can be used to block or restrict access to websites and services that facilitate torrenting and other prohibited activities. By implementing content filtering, the company can comply with the ISP's cease-and-desist order and prevent users from accessing torrent sites and engaging in prohibited activities.Reference: CompTIA Network+ study materials.

Question: 135

SIMULATION

Users are unable to access files on their department share located on file server 2.
The network administrator has been tasked with validating routing between networks hosting workstation A and file server 2.

INSTRUCTIONS

Click on each router to review output, identify any issues, and configure the appropriate solution.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Router A

Routing Table | Routing Configuration

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S*    0.0.0.0/0 is directly connected, GigabitEthernet3
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.0.4.0/22 is directly connected, GigabitEthernet2
C        10.0.6.0/24 is directly connected, GigabitEthernet2
L        10.0.6.1/32 is directly connected, GigabitEthernet2
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.27.0/30 is directly connected, GigabitEthernet3
L        172.16.27.1/32 is directly connected, GigabitEthernet3
```

Reset to Default | Save | Close

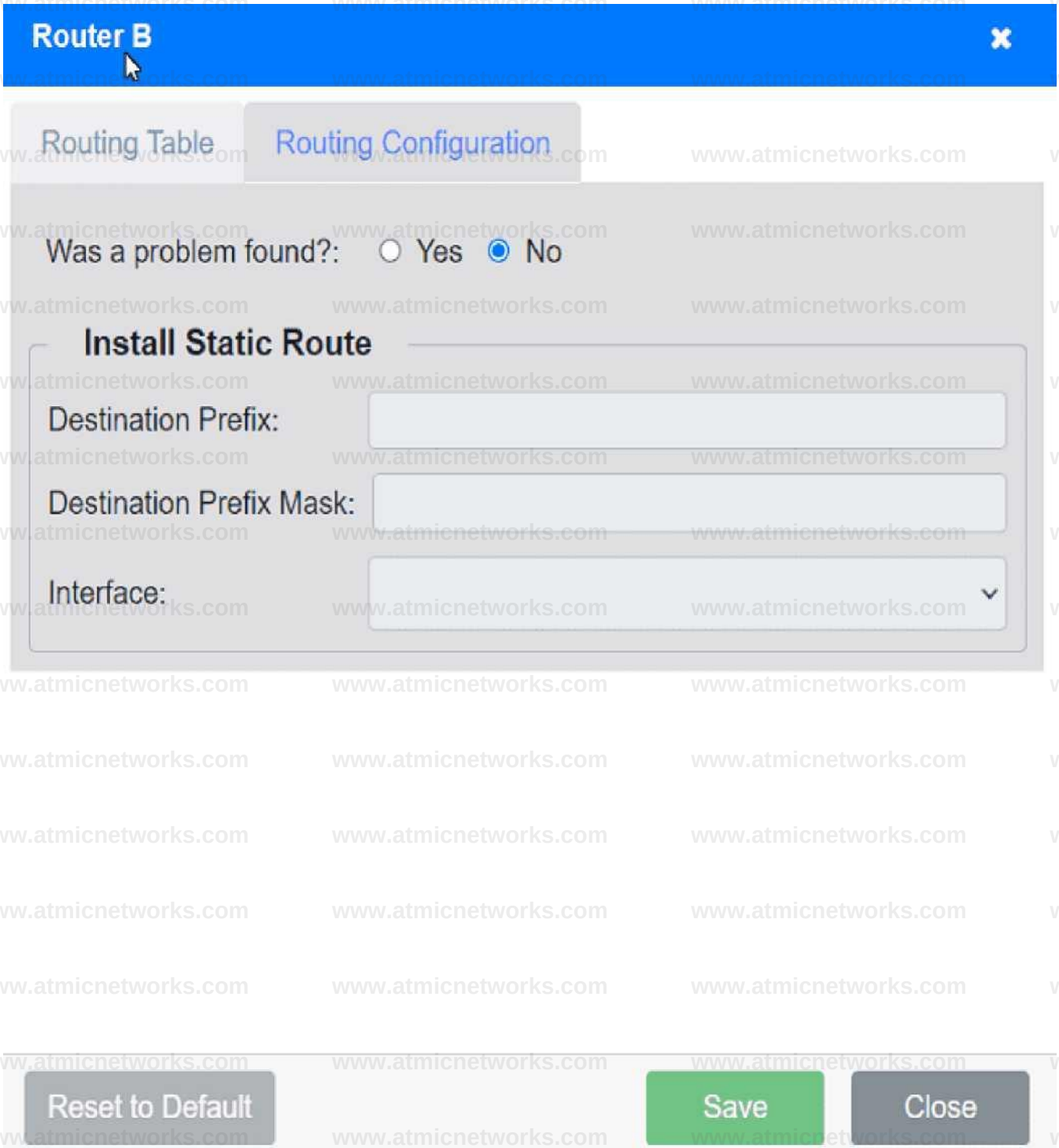
Router C

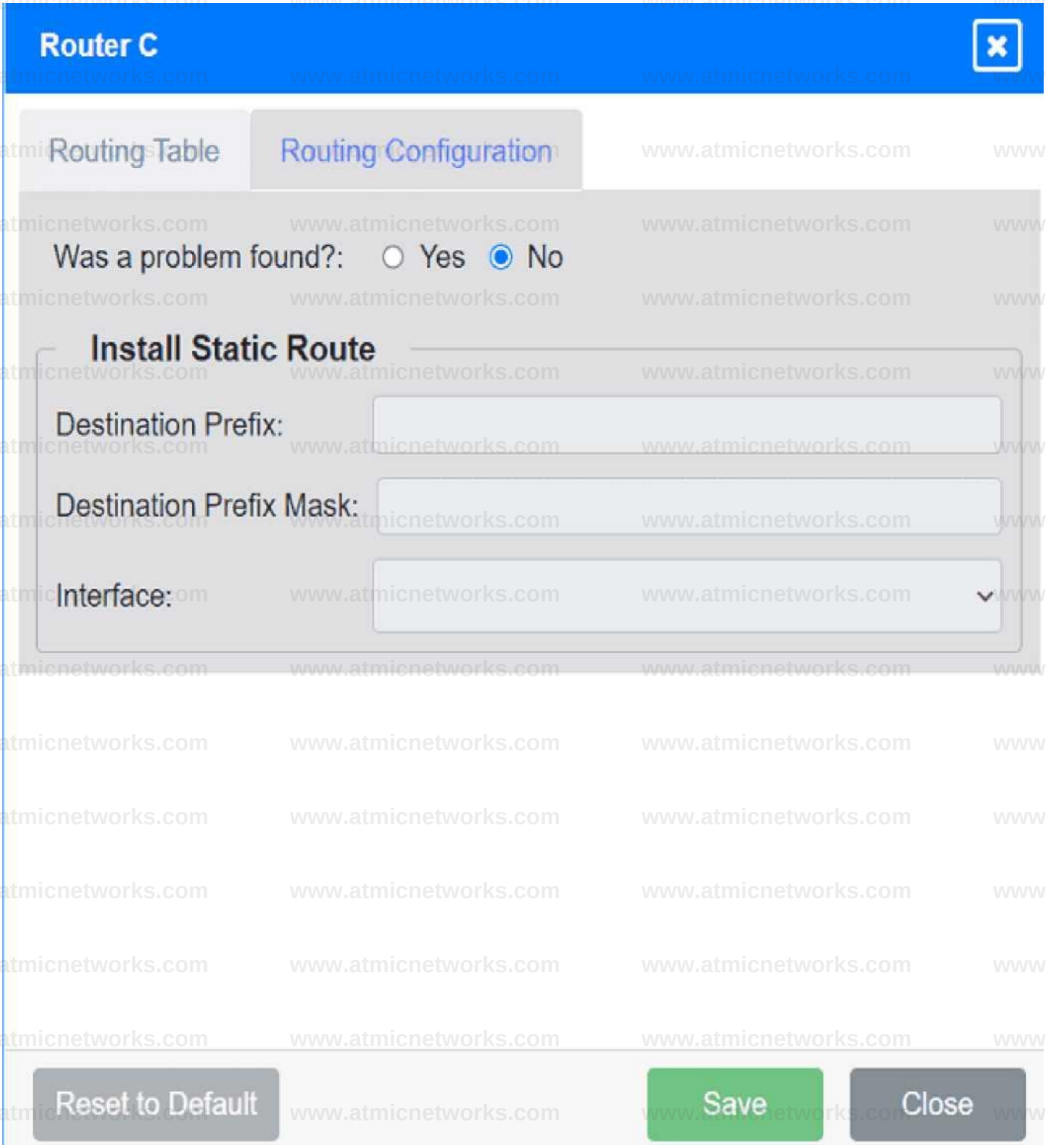
Routing Table Routing Configuration

```
Router-C# show ip route

Codes: L -    local,    C - connected, S - static, R -          RIP,   M - mobile, B - BGP
       D -    EIGRP,EX - EIGRP external, 0 - OSPF,     IA -   OSPF inter area
       N1 - OSPF N5SA external type 1, N2 - OSPF N5SA external type 2 El - OSPF external
       type 1, E2 - OSPF external type 2, m - OHP n -              NAT, Ni -    NAT inside, No -
       NAT outside, Nd- NAT DIA
       i -     IS-IS,    su  - ISIS sunnary, LI - IS-IS          level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route H - NHRP, G - NHRP
       registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, 1 - LISP a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

     10   .0.0.0/8 is variably subnetted, 4 subnets, 2 masks
S         10.0.0.0/22 [1/0] via GigabitEthernetl
S         10.0.4.0/22 [1/0] via GigabitEthernet2
     11   2.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C         172.16.27.0/30    is    directly connected,   GigabitEthernet2
L         172.16.27.2/32    is    directly connected,   GigabitEthernet2
C         172.16.27.4/30    is    directly connected,   GigabitEthernetl
L         172.16.27.6/32    is    directly connected,   GigabitEthernetl
```

Reset to Default

Save ■ Close





Answer: See the solution in Explanation.

Explanation:

To validate routing between networks hosting Workstation A and File Server 2, follow these steps: Review Routing Tables:

Check the routing tables of Router A, Router B, and Router C to identify any missing routes.

Identify Missing Routes:

Ensure that each router has routes to the networks on which Workstation A and File Server 2 are located.

Add Static Routes:

If a route is missing, add a static route to the relevant destination network via the correct interface. Routing Table:

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S* 0.0.0.0/0 is directly connected, GigabitEthernet3 10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks

C 10.0.4.0/22 is directly connected, GigabitEthernet2

C 10.0.6.0/24 is directly connected, GigabitEthernet2

L 10.0.6.1/32 is directly connected, GigabitEthernet2 172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks

C 172.16.27.0/30 is directly connected, GigabitEthernet3

L 172.16.27.1/32 is directly connected, GigabitEthernet3

Routing Table:

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S* 0.0.0.0/0 is directly connected, GigabitEthernet1 10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks

C 10.0.0.0/22 is directly connected, GigabitEthernet1

L 10.0.0.1/32 is directly connected, GigabitEthernet1 172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks

C 172.16.27.4/30 is directly connected, GigabitEthernet1

L 172.16.27.5/32 is directly connected, GigabitEthernet1

Routing Table:

B. .0.0.0/8 is variably subnetted, 4 subnets, 2 masks

S 10.0.0.0/22 [1/0] via GigabitEthernet1

S 10.0.4.0/22 [1/0] via GigabitEthernet2

C. 2.16.0.0/16 is variably subnetted, 2 subnets, 2 masks

C 172.16.27.0/30 is directly connected, GigabitEthernet2

L 172.16.27.2/32 is directly connected, GigabitEthernet2

C 172.16.27.4/30 is directly connected, GigabitEthernet1

L 172.16.27.6/32 is directly connected, GigabitEthernet1

Install Static Route to 10.0.0.0/22 via 172.16.27.1 (assuming Router C's IP is 172.16.27.1):

Destination Prefix: 10.0.0.0

Destination Prefix Mask: 255.255.252.0

Interface: GigabitEthernet3

Install Static Route to 10.0.4.0/22 via 172.16.27.5 (assuming Router C's IP is 172.16.27.5):

Destination Prefix: 10.0.4.0

Destination Prefix Mask: 255.255.252.0

Interface: GigabitEthernet1

Install Static Route to 10.0.6.0/24 via 172.16.27.2 (assuming Router A's IP is 172.16.27.2):

Destination Prefix: 10.0.6.0

Destination Prefix Mask: 255.255.255.0

Interface: GigabitEthernet2

Install Static Route to 10.0.0.0/22 via 172.16.27.1 (assuming Router B's IP is 172.16.27.1):
Destination Prefix: 10.0.0.0
Destination Prefix Mask: 255.255.252.0
Interface: GigabitEthernet1

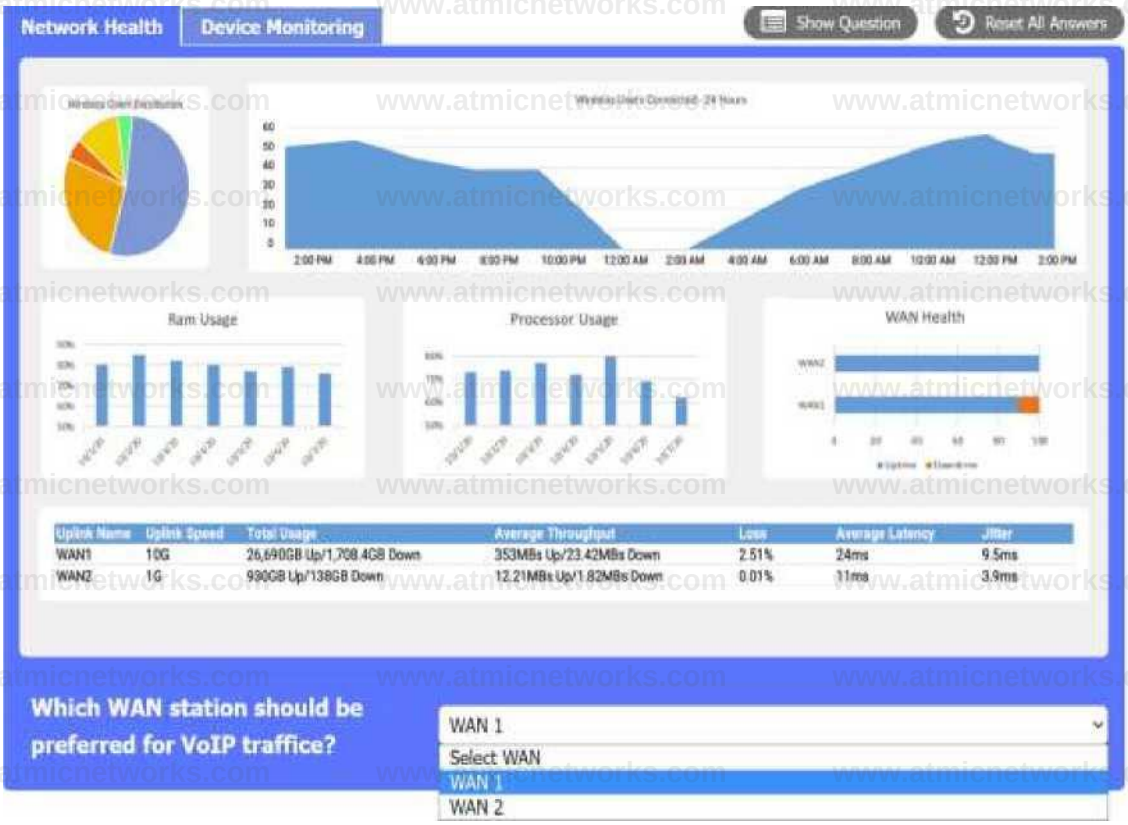
Summary of Static Routes:
Router A:
ip route 10.0.0.0 255.255.252.0 GigabitEthernet3
Router B:
ip route 10.0.4.0 255.255.252.0 GigabitEthernet1
Router C:
ip route 10.0.6.0 255.255.255.0 GigabitEthernet2
ip route 10.0.0.0 255.255.252.0 GigabitEthernet1
These configurations ensure that each router knows the correct paths to reach Workstation A and File Server 2, resolving the connectivity issue.

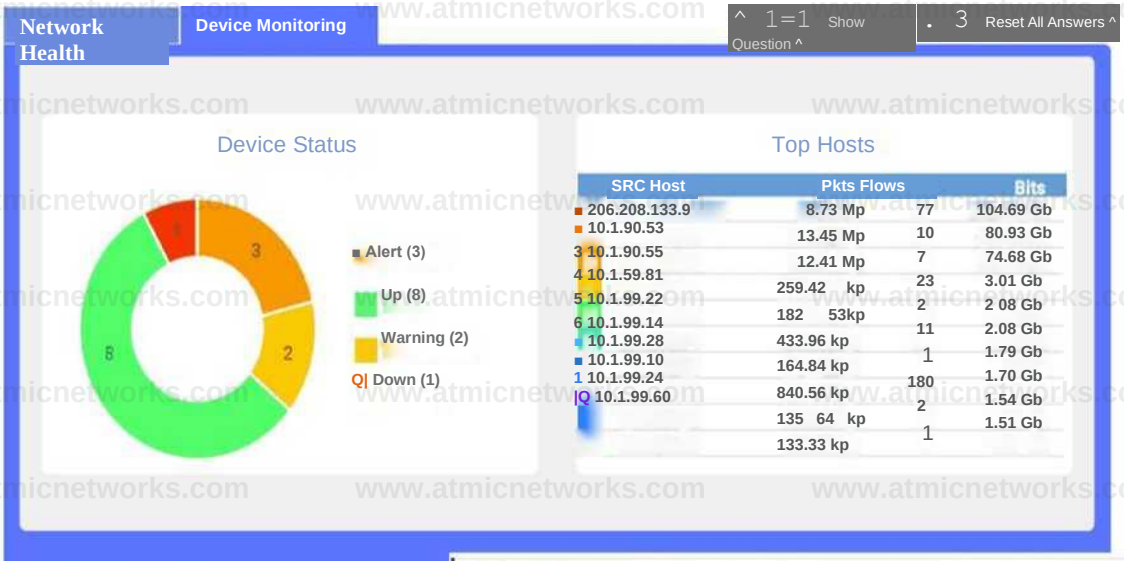
Question: 136

SIMULATION

After a recent power outage, users are reporting performance issues accessing the application servers. Wireless users are also reporting intermittent Internet issues.

INSTRUCTIONS
Click on each tab at the top of the screen. Select a widget to view information, then use the drop-down menus to answer the associated questions. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.





Which device is experiencing connectivity issues?

Select Answer
Router A
Router B
WAP1
WAP2
WirelessController
Switch A
Switch B DHCP
Server Web Server
APP Server

Router A

Which workstation IP is generating the MOST traffic?

Select Answer
10.1.99.28
10.1.99.14
10.1.99.10
10.1.99.22
10.1.99.24
206.208.133.10
206.208.133.9
10.1.50.14
10.1.50.13
10.1.59.81
10.1.90.53
10.1,90.55

206.208.133.9

Answer: See the answer and solution below.

Explanation:

Network Health:

WAN 2 appears to have a lower average latency and loss percentage, which would make it the preferred WAN station for VoIP traffic. VoIP traffic requires low latency and packet loss to ensure good voice quality and reliability. WAN 1 seems to have higher RAM and processor usage, which could also affect the performance of VoIP traffic.

Here's the summary of the key metrics for WAN 1 and WAN 2 from the image provided:

WAN 1:

Uplink Speed: 10G

Total Usage: 26.969GB Up / 1.748GB Down

Average Throughput: 353MBps Up / 23.42MBps Down

Loss: 2.51%

Average Latency: 24ms

Jitter: 9.5ms

WAN 2:

Uplink Speed: 1G

Total Usage: 930GB Up / 138GB Down

Average Throughput: 12.21MBps Up / 1.82MBps Down

Loss: 0.01%

Average Latency: 11ms

Jitter: 3.9ms

For VoIP traffic, low latency and jitter are particularly important to ensure voice quality. While WAN 1 has higher bandwidth and throughput, it also has higher latency and jitter compared to WAN 2.

However, WAN 2 has much lower loss, lower latency, and lower jitter, which are more favorable for VoIP traffic that is sensitive to delays and variation in packet arrival times.

Given this information, WAN 2 would generally be preferred for VoIP traffic due to its lower latency, lower jitter, and significantly lower loss percentage, despite its lower bandwidth compared to WAN 1. The high bandwidth of WAN 1 may be more suitable for other types of traffic that are less sensitive to latency and jitter, such as bulk data transfers.

Device Monitoring:

the device that is experiencing connectivity issues is the APP Server or Router 1, which has a status of Down. This means that the server is not responding to network requests or sending any dat a. You may want to check the physical connection, power supply, and configuration of the APP Server to troubleshoot the problem.

A screenshot of a computer AI-generated content may be incorrect.

Question: 137

Which of the following routing protocols needs to have an autonomous system set in order to establish communication with neighbor devices?

A. OSPF

B. EIGRP

C. FHRP

D. RIP

Answer: B

Explanation:

EIGRP (Enhanced Interior Gateway Routing Protocol) is a Cisco proprietary advanced distance-vector routing protocol. While it operates within an Autonomous System (AS), it requires the AS number to be configured for routers to recognize each other as EIGRP neighbors.

OSPF (Open Shortest Path First) uses areas and routers must be in the same area to form adjacencies, but it doesn't require AS numbers in the same way.

FHRP (First Hop Redundancy Protocol) is not a routing protocol but a group of protocols (e.g., HSRP, VRRP) to ensure high availability at the default gateway level.

RIP (Routing Information Protocol) does not use autonomous system numbers.

Reference:
CompTIA Network+ N10-009 Official Objectives: 3.1 – Compare and contrast various routing technologies.

Question: 138

A network administrator changed an external DNS to point customers to a new server. Which of the following tools should the administrator use to test the new server's configuration?

A. ping
B. tracert
C. tcpdump
D. nslookup

Answer: D

Explanation:

- nslookup allows querying DNS records to verify if the new server is correctly resolving domain names.
- ping (A) tests basic connectivity, not DNS configuration.
- tracert (B) shows network path latency but doesn't test DNS.
- tcpdump (C) captures packets but isn't ideal for DNS verification.

Reference: CompTIA Network+ N10-009 Official Documentation – DNS Testing Tools.

Question: 139

Which of the following is a company most likely enacting if an accountant for the company can only see the financial department's shared folders?

A. General Data Protection Regulation
B. Least privilege network access
C. Acceptable use policy
D. End user license agreement

Answer: B

Explanation:

Least privilege network access is a principle that restricts users' access rights to only what is necessary for them to perform their job functions. In this case, the accountant's access is limited to only the financial department's shared folders, ensuring that they cannot access other parts of the network unnecessarily. This reduces the risk of unauthorized access and potential data breaches. Reference: CompTIA Network+ Exam Objectives and official study guides.

Question: 140

A network administrator is notified that a user cannot access resources on the network. The network administrator checks the physical connections to the workstation labeled User 3 and sees the Ethernet is properly connected. However, the network interface's indicator lights are not blinking on either the computer or the switch. Which of the following Is the most likely cause?

A. Theswitch failed.
B. Thedefault gateway is wrong.
C. Theport Is shut down.
D. TheVLAN assignment is incorrect.

Answer: C

Explanation:

When a network interface's indicator lights are not blinking on either the computer or the switch, it suggests a physical layer issue. Here is the detailed reasoning:

Ethernet Properly Connected: The Ethernet cable is correctly connected, eliminating issues related to a loose or faulty cable.

No Indicator Lights: The absence of blinking indicator lights on both the computer and the switch typically points to the port being administratively shut down.

Switch Port Shut Down: In networking, a switch port can be administratively shut down, disabling it from passing any traffic. This state is configured by network administrators and can be verified and changed using the command-line interface (CLI) of the switch.

Command to Check and Enable Port:

bash

Copy code

```
Switch> enable
Switch# configure terminal
Switch(config)# interface [interface id]
Switch(config-if)# no shutdown
```

The command no shutdown re-enables the interface if it was previously disabled. This will restore the link and the indicator lights should start blinking, showing activity.

Basic Configuration Commands PDF, sections on interface configuration (e.g., shutdown, no shutdown).

Question: 141

A technician needs to identify a computer on the network that is reportedly downloading unauthorized content. Which of the following should the technician use?

A. Anomaly alerts
B. Port mirroring
C. Performance monitoring
D. Packet capture

Answer: D

Explanation:

Packet Capture: This method captures and inspects network traffic to identify unauthorized downloads or malicious behavior. It provides detailed insight into the data being transmitted, making it the best tool for this scenario.
Anomaly alerts (A): Alerts may indicate unusual activity but do not provide detailed traffic analysis. Port mirroring (B): Port mirroring can redirect traffic for analysis but requires a packet capture tool for deeper inspection.
Performance monitoring (C): Focuses on system performance metrics, not detailed traffic content.
Reference: CompTIA Network+ Official Study Guide, Domain 4.3 (Network Monitoring Tools).

Question: 142

A small company has the following IP addressing strategy:

A user is unable to connect to the company fileshare server located at 192.168.10.1. The user's networking configuration is:

Which of the following will most likely correct the issue?

A. Changing the IPv4 address to 192.168.10.1
B. Changing the subnet mask to 255.255.255.0
C. Changing the DNS servers to internet IPs
D. Changing the physical address to 7A-01-7A-21-01-50

Answer: B

Explanation:

If the user cannot communicate with 192.168.10.1, they might be on a different subnet. Changing the subnet mask to 255.255.255.0 ensures the user and the file server are in the same subnet.
Breakdown of Options:
A . Changing the IPv4 address to 192.168.10.1 – This would conflict with the server's IP.
B . Changing the subnet mask to 255.255.255.0 – Q Correct answer. Ensures both the user and the server are on the same subnet.
C . Changing the DNS servers – DNS does not affect local network connectivity.
D . Changing the physical address – The MAC address does not impact subnet communication.
Reference:
CompTIA Network+ (N10-009) Official Study Guide – Domain 2.4: Explain subnetting and addressing concepts.

Question: 143

A network administrator is configuring access points for installation in a dense environment where coverage is often overlapping. Which of the following channel widths should the administrator choose to help minimize interference in the 2.4GHz spectrum?

A. 11MHz
B. 20MHz
C. 40MHz
D. 80MHz
E. 160MHz

Answer: B

Explanation:

Reference: CompTIA Network+ Certification Exam Objectives - Wireless Networks section.

Question: 144

Which of the following VPN types provides secure remote access to the network resources through a web portal?

A. Proxy
B. Clientless
C. Site-to-site
D. Direct connect

Answer: B

Explanation:

Clientless VPNs allow users to access network resources through a secure web portal using a browser, with no VPN software needed. This is ideal for occasional access to internal resources via HTTPS.

A . Proxy is a gateway for accessing web content, not a VPN.

C . Site-to-site VPN connects entire networks, not individual users.

D . Direct Connect usually refers to dedicated cloud connections, not VPNs.

Reference:

CompTIA Network+ N10-009 Official Objectives: 3.3 – Given a scenario, configure and deploy common VPN technologies.

Question: 145

During a recent security assessment, an assessor attempts to obtain user credentials by pretending to be from the organization's help desk. Which of the following attacks is the assessor using?

A. Social engineering
B. Tailgating
C. Shoulder surfing
D. Smishing
E. Evil twin

Answer: A

Explanation:

This is a classic example of social engineering, where an attacker manipulates individuals into giving up confidential information, such as credentials, by pretending to be someone trustworthy (like help desk staff).

B . Tailgating involves physical access without authentication.

C . Shoulder surfing is spying over someone's shoulder to steal info.

D . Smishing is phishing via SMS.

E . Evil twin involves a rogue Wi-Fi access point impersonating a legitimate one.

Reference:

CompTIA Network+ N10-009 Official Objectives: 4.2 – Identify common security threats and vulnerabilities.

Question: 146

Which of the following devices can operate in multiple layers of the OSI model?

A. Hub
B. Switch
C. Transceiver
D. Modem

Answer: B

Explanation:

Understanding Switches:

Layer 2 (Data Link Layer): Traditional switches operate primarily at Layer 2, where they use MAC addresses to forward frames within a local network.

Layer 3 (Network Layer): Layer 3 switches, also known as multilayer switches, can perform routing functions using IP addresses to forward packets between different networks.

Capabilities of Multilayer Switches:

VLANs and Inter-VLAN Routing: Multilayer switches can handle VLAN (Virtual Local Area Network) configurations and perform inter-VLAN routing, enabling communication between different VLANs. Routing Protocols: They can run routing protocols like OSPF (Open Shortest Path First) and EIGRP (Enhanced Interior Gateway Routing Protocol) to manage traffic between networks.

Comparison with Other Devices:

Hub: Operates only at Layer 1 (Physical Layer) and simply repeats incoming signals to all ports.

Transceiver: Also operates at Layer 1, converting electrical signals to optical signals and vice versa.

Modem: Primarily operates at Layer 1 and Layer 2, modulating and demodulating signals for transmission over different types of media.

Practical Application:

Multilayer switches are commonly used in enterprise networks to optimize performance and manage complex routing and switching requirements within a single device.

Reference:

CompTIA Network+ study materials on network devices and the OSI model.

Question: 147

A network engineer is troubleshooting connectivity for a newly installed server on an existing VLAN.
The engineer reviews the following output:

```
C:\> ipconfig
IP Address: 192.168.100.225
Mask: 255.255.255.224
Gateway: 192.168.100.254

Router# show ip route
C 192.168.100.0/24 is directly connected, GigabitEthernet0/0
```

Which of the following describes the issue?

A. The server has an incorrect subnet mask
B. There is a duplicate IP address on the network
C. The DHCP address pool is exhausted
D. The router is missing a default route

Answer: A

Explanation:

The server's subnet mask is 255.255.255.224 (/27), which covers IPs from 192.168.100.224 to 192.168.100.255. However, the router only recognizes 192.168.100.0/24, indicating a mismatch between the server's subnet and the router's network.

Correct mask for the /24 network is 255.255.255.0, allowing 256 IPs from 192.168.100.0 to 192.168.100.255.
This mismatch would result in routing issues, especially with the gateway outside of the subnet range.

Reference:

CompTIA Network+ N10-009 Official Objectives: 5.2 – Given a scenario, troubleshoot common wired connectivity issues.

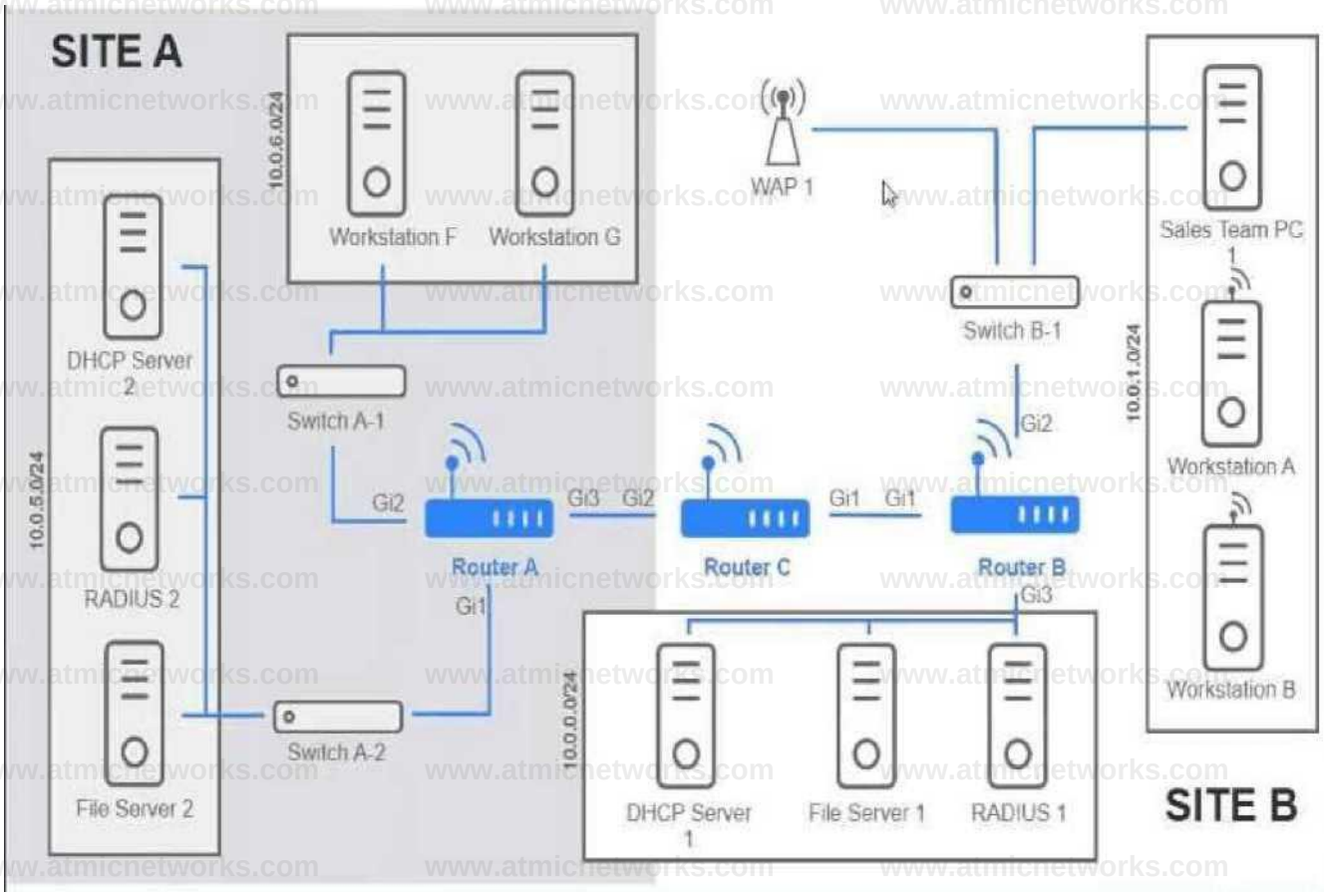
Question: 148

SIMULATION

Users are unable to access files on their department share located on flle_server 2. The network administrator has been tasked with validating routing between networks hosting workstation A and file server 2.

INSTRUCTIONS

Click on each router to review output, identity any Issues, and configure the appropriate solution If at any time you would like to bring back the initial state of trie simulation, please click the reset All button;



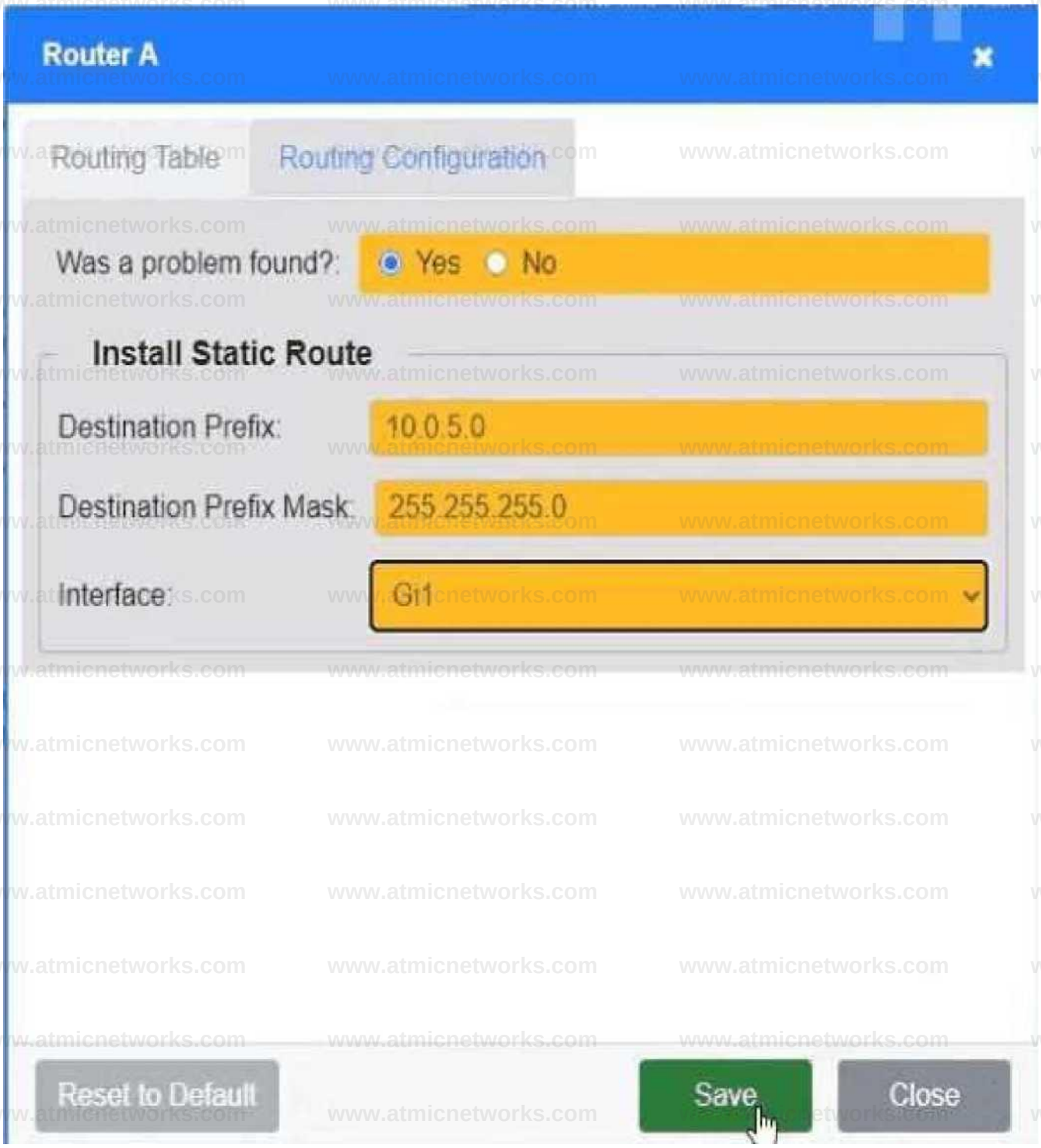
Routine T&315 Routine Confiouraboi

```
Router B# show ip route

Codes: L - localsC - connected, S - static, R -  RIP,  M - mobile, B - BGP
       D -  EIGRP,EX  - EIGRP external, 0 - OSPF,  IA -  OSPF inter area

       MI - OSPF USSA external type 1, K2 - OSPF NSSA external type 2 El • OSPF external
       type 1, E2 OSPF external type 2, m - OMP n -NAT, Ni -HAT inside, No - NAT outside,
       Nd  - NAT DIA

       i -  ISIS,  su  - ISIS summary, LI - IS-IS  level 1, L2 - ISIS level-2
       ia - IS-IS inter area, ♦ - candidate default, U - per-user static route H - NHRP, 6 - NHRP
       registered, g - NHRP registration summary o - OOR, P - periodic downloaded static
       route, 1 • LISP a - application route ♦ - replicated route, X - next hop override, p
       overrides from PfR

Gateway of last resort is 0.0.0.0 to network 0.0.0.0
```

```
S* B.e.e.e/e is directly connected, GigabitEthernetl 10.0.0.0/8 is variably subnetted, 4 subnets,
2 masks C                10.0.0.0/22 is      directly connected, GigabitEthernetl
L          10.0.0.1/32 is      directly connected, GigabitEthernet3
          172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks C   172.16.27.4/30          is
directly connected, GigabitEthernetl
L          172.16.27.5/32      is directly connected, GigabitEthernetl
```

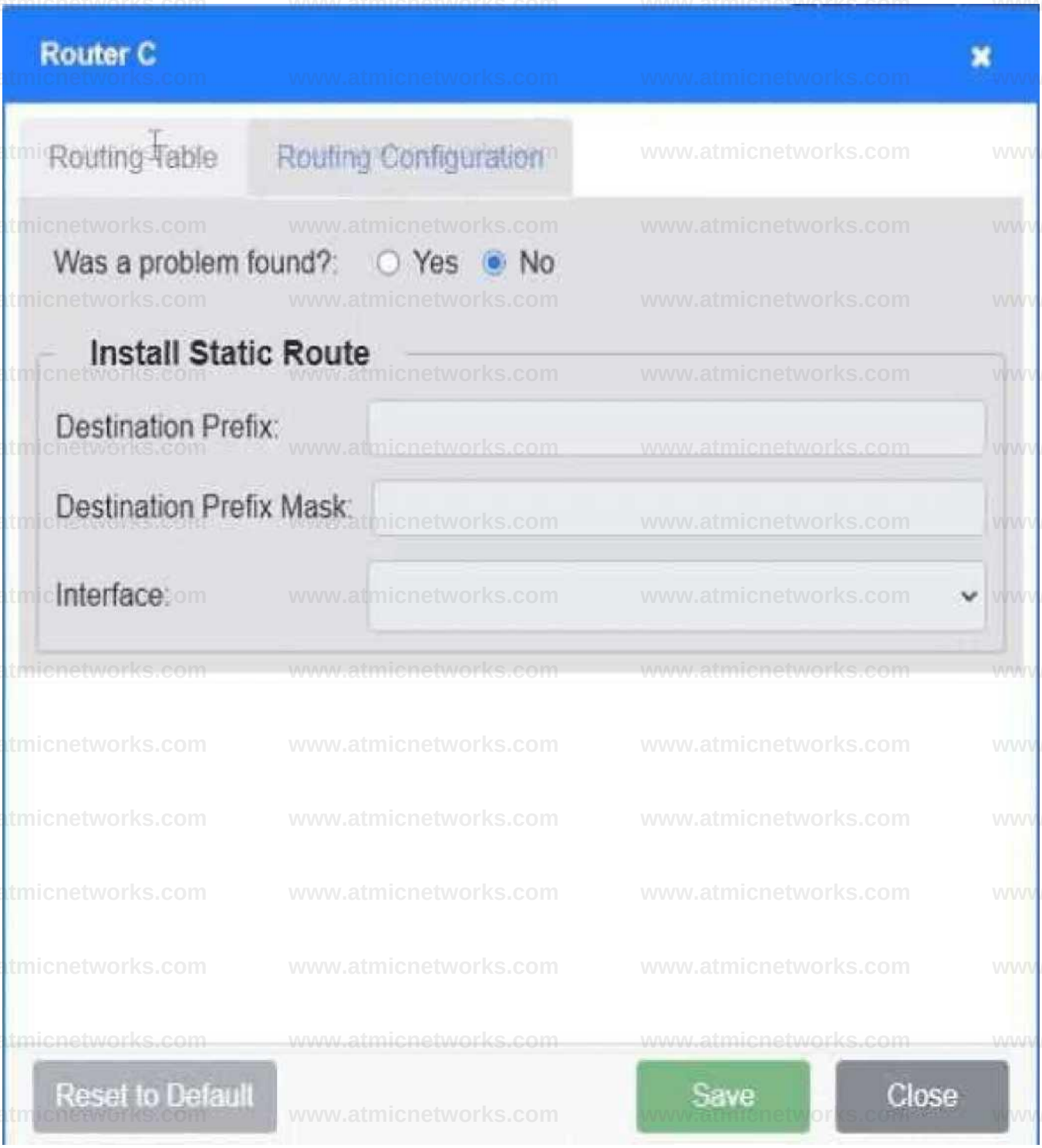
Answer: See the solution configuration below in Explanation.

Explanation:



A screenshot of a computer AI-generated content may be incorrect.

A screenshot of a computer AI-generated content may be incorrect.



A screenshot of a computer AI-generated content may be incorrect.

Question: 149

Which of the following steps in the troubleshooting methodology comes after using a top-to-top buttom examination of the OSI model to determine cause?

A. Test in the theory
B. Establish a plan of action
C. Verify full system functionality
D. Identify the problem

Answer: B

Explanation:

Question: 150

Which of the following network traffic type is sent to all nodes on the network?

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

Answer: B

Explanation:

Broadcast traffic is sent to all nodes on the network. In a broadcast, a single packet is transmitted to all devices in the network segment. This is commonly used for tasks like ARP (Address Resolution Protocol) requests.
Broadcast Domain: All devices within the same broadcast domain will receive broadcast traffic.
Network Types: Ethernet networks commonly use broadcast traffic for certain functions, including network discovery and addressing.
IPv4 Broadcast: An IPv4 broadcast address (e.g., 255.255.255.255) ensures the packet is sent to all devices on the network.
Network Reference:
CompTIA Network+ N10-007 Official Certification Guide: Explains network traffic types, including broadcast, unicast, and multicast.
Cisco Networking Academy: Provides training on network communication methods and traffic types. Network+ Certification All-in-One Exam Guide: Discusses different types of network traffic and their uses in various network scenarios.
Broadcast traffic is essential for network operations that require communication with all nodes, such as ARP requests or DHCP discovery messages.

Question: 151

A network administrator notices interference with industrial equipment in the 2.4GHz range. Which of the following technologies would most likely mitigate this issue? (Select two).

A. Mesh network
B. 5GHz frequency
C. Omnidirectional antenna
D. Non-overlapping channel
E. Captive portal
F. Ad hoc network

Answer: B

Explanation:

Understanding 2.4GHz Interference:
The 2.4GHz frequency range is commonly used by many devices, including Wi-Fi, Bluetooth, and various industrial equipment. This can lead to interference and degraded performance.
Mitigation Strategies:
5GHz Frequency:
The 5GHz frequency band offers more channels and less interference compared to the 2.4GHz band. Devices operating on 5GHz are less likely to encounter interference from other devices, including industrial equipment.
Non-overlapping Channels:
In the 2.4GHz band, using non-overlapping channels (such as channels 1, 6, and 11) can help reduce interference. Non-overlapping channels do not interfere with each other, providing clearer communication paths for Wi-Fi signals.
Why Other Options are Less Effective:
Mesh Network: While useful for extending network coverage, a mesh network does not inherently address interference issues.
Omnidirectional Antenna: This type of antenna broadcasts signals in all directions but does not mitigate interference.
Captive Portal: A web page that users must view and interact with before accessing a network, unrelated to frequency interference.
Ad Hoc Network: A decentralized wireless network that does not address interference issues directly.
Implementation:
Switch Wi-Fi devices to the 5GHz band if supported by the network infrastructure and client devices. Configure Wi-Fi access points to use non-overlapping channels within the 2.4GHz band to minimize interference.
Reference:
CompTIA Network+ study materials on wireless networking and interference mitigation.

Question: 152

A newtwork 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 insufficent.

Answer: C

Explanation:
An SVI (Switched Virtual Interface) is a logical interface on a Layer 3-capable switch used to route traffic between VLANs. This is particularly useful in environments where voice and data traffic need to be separated, as each type of traffic can be assigned to different VLANs and routed accordingly. SVI (Switched Virtual

Interface): A virtual interface created on a switch for inter-VLAN routing.

VLAN Routing: Enables the routing of traffic between VLANs on a Layer 3 switch, allowing for logical separation of different types of traffic, such as voice and data.

Use Case: Commonly used in scenarios where efficient and segmented traffic management is required, such as in VoIP implementations.

Network Reference:

CompTIA Network+ N10-007 Official Certification Guide: Discusses VLANs, SVIs, and their applications in network segmentation and routing.

Cisco Networking Academy: Provides training on VLAN configuration and inter-VLAN routing using SVIs.

Network+ Certification All-in-One Exam Guide: Covers network segmentation techniques, including the use of SVIs for VLAN routing.

Question: 153

A company recently implemented a videoconferencing system that utilizes large amounts of bandwidth. Users start reporting slow internet speeds and an overall decrease in network performance. Which of the following are most likely the causes of the network performance issues? (Select two)

A. DNS misconfiguration
B. Inadequate network security
C. Malware or a virus
D. Outdated software
E. Incorrect QoS settings
F. Network congestion

Answer: E,F

Explanation:

When high-bandwidth services like videoconferencing are introduced, two primary factors may degrade performance:

Incorrect QoS Settings (E):QoS (Quality of Service) is used to prioritize traffic. If not configured correctly, critical services like video may not get the necessary bandwidth and prioritization.

Network Congestion (F):Video services consume large amounts of data. If the network doesn't have sufficient bandwidth or is not segmented properly, congestion will slow down all services.

DNS misconfiguration (A) would affect name resolution, not bandwidth.

Malware (C) could degrade performance, but is not tied to the described scenario.

Outdated software (D) may affect performance in some cases, but not directly linked to network congestion in this case.

Inadequate network security (B) isn't likely to cause general slowness related to video traffic.

Q So, the most likely culprits are E. Incorrect QoS settings and F. Network congestion.

Reference:CompTIA Network+ N10-009 Official Study Guide — Objective 2.5: "Explain common performance concepts and issues."

Question: 154

A network administrator installed a new VLAN to the network after a company added an additional floor to the office. Users are unable to obtain an IP address on the new VLAN, but ports on existing VLANs are working properly. Which of the following configurations should the administrator update?

A. Scope size
B. Address reservations
C. Lease time
D. IP helper

Answer: D

Explanation:

When a new VLAN is created, it typically exists on a different subnet. If DHCP servers are on a different VLAN, the network needs an IP helper address to forward DHCP requests correctly. Without it, clients in the new VLAN won't receive an IP address.

Breakdown of Options:

A . Scope size – Increasing the DHCP scope would not resolve the issue if requests aren't reaching the server.

B . Address reservations – Reservations only assign specific addresses to devices; they do not fix DHCP communication issues.

C . Lease time – Changing the lease time does not impact DHCP functionality across VLANs.

D . IP helper – Correct answer. This forwards DHCP requests across VLANs to the DHCP server.

Reference:

CompTIA Network+ (N10-009) Official Study Guide – Domain 2.4: Explain IP addressing technologies and subnetting.

RFC 1542: BOOTP (Bootstrap Protocol) relay agents

Question: 155

An organization wants to ensure that incoming emails were sent from a trusted source. Which of the following DNS records is used to verify the source?

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

Answer: A

Explanation:

A TXT record can be used to store SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) information, which help verify that an email has been sent from a trusted source.

Question: 156

A small business is deploying new phones, and some of the phones have full HD videoconferencing features. The Chief Information Officer (CIO) is concerned that the network might not be able to handle the traffic if it reaches a certain threshold. Which of the following can the network engineer configure to help ease these concerns?

A. A VLAN with 100Mbps speed limits
B. An IP helper to direct VoIP traffic
C. A smaller subnet mask
D. Full duplex on all user ports

Answer: D

Explanation:

Full duplex mode allows devices to send and receive data simultaneously, improving network performance and reducing congestion, which is critical for VoIP and video conferencing.

Breakdown of Options:

A . A VLAN with 100Mbps speed limits – VLANs segment traffic but limiting speeds to 100Mbps would worsen video performance.

B . An IP helper to direct VoIP traffic – IP helper is used for DHCP relay, not for VoIP optimization. C . A smaller subnet mask – A smaller subnet reduces IP address availability but does not improve network performance.

D . Full duplex on all user ports – Correct answer. Full duplex eliminates collisions, allowing better VoIP and video performance.

Reference:

CompTIA Network+ (N10-009) Official Study Guide – Domain 2.2: Compare and contrast various networking devices.

IEEE 802.3: Ethernet Full Duplex Operation

Question: 157

A user's VoIP phone and workstation are connected through an inline cable. The user reports that the VoIP phone intermittently reboots, but the workstation is not having any network-related issues Which of the following is the most likely cause?

A. The PoE power budget is exceeded.
B. Port security is violated.
C. The signal is degraded
D. The Ethernet cable is not working

Answer: A

Explanation:

Power over Ethernet (PoE) delivers power to devices such as VoIP phones over the same cables used for data. If the total power requirement of connected devices exceeds the PoE power budget of the switch or injector, some devices may not receive adequate power and could intermittently reboot. This issue would not affect the workstation, which is likely receiving power separately. Reference: CompTIA Network+ Exam Objectives and official study guides.

Question: 158

A technician is troubleshooting a computer issue for a user who works in a new annex of an office building. The user is reporting slow speeds and intermittent connectivity. The computer is connected via a Cat 6 cable to a distribution switch that is 492ft (150m) away. Which of the following should the technician implement to correct the issue?

A. Increase the bandwidth allocation to the computer.
B. Install an access switch in the annex and run fiber to the distribution switch.
C. Run a Cat 7 cable from the computer to the distribution switch.
D. Enable the computer to support jumbo frames.

Answer: B

Explanation:

The maximum recommended length for Ethernet cable runs is 100 meters (328 feet). At 150 meters, the Cat 6 cable is too long, causing signal degradation and connectivity issues. Running fiber from the distribution switch to an access switch in the annex will allow for reliable connectivity over longer distances, as fiber can cover greater distances without signal loss. (Reference: CompTIA Network+ Study Guide, Chapter on Network Cable Standards)

Question: 159

A network administrator is deploying a new switch and wants to make sure that the default priority value was set for a spanning tree. Which of the following values would the network administrator expect to see?

A. 4096
B. 8192
C. 32768
D. 36684

Answer: C

Explanation:

Understanding Spanning Tree Protocol (STP):

STP is used to prevent network loops in Ethernet networks by creating a spanning tree that selectively blocks some redundant paths.

Default Priority Value:

Bridge Priority: STP uses bridge priority to determine which switch becomes the root bridge. The default bridge priority value for most switches is 32768.

Priority Range: The bridge priority can be set in increments of 4096, ranging from 0 to 61440.

Configuration and Verification:

When deploying a new switch, the network administrator can verify the bridge priority using commands such as show spanning-tree to ensure it is set to the default value of 32768.

Comparison with Other Values:

4096 and 8192: Lower than the default priority, indicating these would be manually configured for higher preference.

36684: A non-standard value, likely a result of specific configuration changes.

Reference:

CompTIA Network+ study materials on Spanning Tree Protocol and network configuration.

Question: 160

Which of the following most likely determines the size of a rack for installation? (Select two).

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

Answer: B

Explanation:

Understanding Rack Size Determination:

The size of a rack for installation is determined by the dimensions of the equipment to be housed in it, primarily focusing on the depth and height of the devices.

Switch Depth:

Depth of Equipment: The depth of network switches and other rack-mounted devices directly influences the depth of the rack. If the equipment is deeper, a deeper rack is required to accommodate it.

Industry Standards: Most racks come in standard depths, but it is essential to match the depth of the rack to the deepest piece of equipment to ensure proper fit and airflow.

Server Height:

Height of Equipment: The height of servers and other devices is measured in rack units (U), where 1U equals

1.75 inches. The total height of all equipment determines the overall height requirement of the rack.

Rack Units: A rack's height is typically described in terms of the number of rack units it can accommodate, such as 42U, 48U, etc.

Why Other Options are Less Relevant:

KVM Size: While important for management, KVM (Keyboard, Video, Mouse) switches do not typically determine rack size.

Hard Drive Size: Individual hard drives are installed within servers or storage devices, not directly influencing rack dimensions.

Cooling Fan Speed: Fan speed affects cooling but not the physical size of the rack.

Outlet Amperage: Power requirements do not determine rack dimensions but rather the electrical infrastructure supporting the rack.

Reference:

CompTIA Network+ study materials on rack installation and equipment sizing.

Question: 161

Which of the following technologies is the best choice to listen for requests and distribute user traffic across web servers?

A. Router
B. Switch
C. Firewall
D. Load balancer

Answer: D

Explanation:

A load balancer is designed to distribute user requests across multiple servers to ensure high availability and performance.

Breakdown of Options:

A . Router – Directs traffic between networks, not between web servers.

B . Switch – Works at Layer 2, does not distribute web traffic.

C . Firewall – Secures network traffic, but does not distribute load.

D . Load balancer – Q Correct answer. Optimizes web traffic distribution across multiple servers.

Reference:

CompTIA Network+ (N10-009) Official Study Guide – Domain 1.5: Explain load balancing and redundancy concepts.

Question: 162

Users usually use RDP to connect to a terminal server with hostname TS19 that points to 10.0.100.19. However, users recently have been unable to connect to TS19. The technician pings 10.0.100.19 and gets an unreachable error. Which of the following is the most likely cause?

A. The users are on the wrong subnet.
B. The DHCP server renewed the lease.

C. The IP address was not reserved.
D. The hostname was changed.

Answer: A

Explanation:

If a ping to 10.0.100.19 is unreachable, the most likely issue is that users are on the wrong subnet and cannot communicate with the server.

Breakdown of Options:

A . The users are on the wrong subnet. Q Correct answer. If users are on a different subnet without proper routing, they won't reach the server.

B . The DHCP server renewed the lease. – Would change the client's IP, but the server's static IP should remain unchanged.

C . The IP address was not reserved. – DHCP reservations matter for dynamic IPs, but RDP servers typically have static IPs.

D . The hostname was changed. – Would affect DNS resolution, but pinging the IP directly would still work.

Reference:

CompTIA Network+ (N10-009) Official Study Guide – Domain 2.4: Explain subnetting concepts.

Question: 163

An IT department asks a newly hired employee to use a personal laptop until the company can provide one. Which of the following policies is most applicable to this situation?

A. IAM
B. BYOD
C. DLP
D. AUP

Answer: B

Explanation:

BYOD (Bring Your Own Device) policies define rules for using personal devices on the company network. Since the new employee is using a personal laptop, this policy applies.

Breakdown of Options:

A . IAM (Identity and Access Management) – Governs user permissions, not device policies.

B . BYOD (Bring Your Own Device) – Q Correct answer. Covers using personal devices for work.

C . DLP (Data Loss Prevention) – Focuses on preventing sensitive data leaks, not device usage policies.

D . AUP (Acceptable Use Policy) – Covers internet and system usage, but not personal device rules.

Reference:

CompTIA Network+ (N10-009) Official Study Guide – Domain 3.6: Explain security policies and best practices.

Question: 164

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

A. Implementingenterprise authentication
B. Requiring theuse of PSKs
C. Configuring acaptive portal for users
D. Enforcing wired equivalent protection

Answer: A

Explanation:

Enterprise authentication (such as WPA2-Enterprise) utilizes unique credentials for each user, typically integrating with an authentication server like RADIUS. This allows for tracking and logging user activity, ensuring that all connections can be traced back to individual users. PSKs (Pre-Shared Keys) are shared among users and do not provide individual accountability. Captive portals can identify users but are less secure than enterprise authentication, and Wired Equivalent Privacy (WEP) is outdated and not recommended for security purposes.

Reference:

CompTIA Network+ materials highlight enterprise authentication methods as the preferred solution for secure and accountable wireless network access.

Question: 165

Which of the following can be implemented to add an additional layer of security between a corporate network and network management interfaces?

A. Jump box
B. Console server
C. API interface
D. In-band management

Answer: A

Explanation:

A jump box is a hardened, isolated system that provides secure access to critical infrastructure devices like routers and firewalls.

Reference:

CompTIA Network+ (N10-009) Official Study Guide – Domain 4.3: Explain network security techniques.

Question: 166

Which of the following is used to stage copies of a website closer to geographically dispersed users?

A. VPN
B. CDN
C. SAN
D. SDN

Answer: B

Explanation:

A Content Delivery Network (CDN) caches website content across multiple geographically distributed servers to reduce latency and improve load times for users worldwide.

Breakdown of Options:

A . VPN – Encrypts network connections, does not distribute website content.

B . CDN – Q Correct answer. A network of caching servers that delivers web content faster.

C . SAN – Storage Area Network, not related to web content distribution.

D . SDN – Software-defined networking, which controls network flows but does not stage website content.

Reference:

CompTIA Network+ (N10-009) Official Study Guide – Domain 1.5: Compare and contrast different networking services.

Question: 167

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

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

Answer: A

Explanation:

Importance of Proper Termination:

Cat 8 cabling requires precise termination practices to ensure signal integrity and reduce interference. One common requirement is to wrap the end connections in copper tape to maintain shielding and reduce electromagnetic interference (EMI).

Interference Troubleshooting:

Interference in high-frequency cables like Cat 8 can be caused by improper shielding or grounding.

Checking the end connections for proper wrapping in copper tape is a crucial step.

Why Other Options are Less Likely:

Passthrough modular crimping plugs: Not specifically related to interference issues and are typically used for ease of cable assembly.
Connecting RX/TX wires to different pins: Would likely result in no connection or incorrect data transmission rather than interference.
Running a speed test on a device that can only achieve 100Mbps speeds: This would not diagnose interference and would not provide relevant information for Cat 8 cabling rated for higher speeds. Corrective Actions:
Verify that all end connections are properly wrapped with copper tape before termination.
Ensure that the shielding is continuous and properly grounded throughout the installation.
Retest the cabling for interference after making corrections.
Reference:
CompTIA Network+ study materials and structured cabling installation guides.

Question: 168

A network engineer is testing a website to ensure it is compatible with IPv6. After attempting to ping the website by its IPv6 address, the engineer determines that the DNS has not been set up properly. Which of the following should the network engineer complete to resolve this issue?

A. Enable a PTR record.
B. Update the existing TXT record.
C. Add a new AAAA record.
D. Configure a secondary NS record.

Answer: C

Explanation:

- AAAA records map domain names to IPv6 addresses, enabling proper resolution.
- PTR records (A) are for reverse DNS lookups.
- TXT records (B) store text-based information, not IP addresses.
- NS records (D) define authoritative name servers but don't directly affect IPv6 resolution.

Reference: CompTIA Network+ N10-009 Official Documentation – DNS Configuration & IPv6.

Question: 169

A network administrator is configuring a network for a new site that will have 150 users. Within the next year, the site is expected to grow by ten users. Each user will have two IP addresses (one for a computer and one for a phone). Which of the following classful IPv4 address ranges will be best- suited for the network?

A. Class D B. Class B C. Class A D. Class C

Answer: B

Explanation:

- The total number of devices = (150 + 10) users × 2 IPs per user = 320 devices
- Class C (D) supports a maximum of 254 hosts (2^8 - 2), which is too small.

- Class B (B) supports 65,534 hosts (2^16 - 2), making it the best choice.
- Why not the other options?
- Class A (C): Supports millions of addresses, which is overkill for 320 devices.
- Class D (A): Used for multicast, not for device addressing.

Reference:
CompTIA Network+ (N10-009) Official Guide – Chapter 7: IP Addressing and Subnetting

Question: 170

Which of the following requires network devices to be managed using a different set of IP addresses?

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

Answer: D

Explanation:

Out-of-band (OOB) management refers to using a dedicated management network that is physically separate from the regular data network. This management network uses a different set of IP addresses to ensure that management traffic is isolated from user data traffic, providing a secure way to manage network devices even if the main network is down or compromised.Reference: CompTIA Network+ study materials.

Question: 171

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:

Understanding VoIP and VLANs:

VoIP (Voice over IP) phones often use VLANs (Virtual Local Area Networks) to separate voice traffic from data traffic for improved performance and security.

Tagging Traffic to Voice VLAN:

Voice VLAN Configuration: The port on the switch needs to be configured to tag traffic for the specific voice VLAN. This ensures that voice packets are prioritized and handled correctly.

VLAN Tagging: VLAN tagging allows the switch to identify and separate voice traffic from other types of traffic

on the network, reducing latency and jitter for VoIP communications.

Comparison with Other Options:

Trunk all VLANs on the port: Trunking all VLANs is typically used for links between switches, not for individual device ports.

Configure the native VLAN: The native VLAN is for untagged traffic and does not address the need for separating and prioritizing voice traffic.

Disable VLANs: Disabling VLANs would mix voice and data traffic, leading to potential performance issues and lack of traffic separation.

Implementation:

Configure the switch port connected to the VoIP phone to tag the traffic for the designated voice VLAN, ensuring proper network segmentation and quality of service.

Reference:

CompTIA Network+ study materials on VLAN configuration and VoIP implementation.

Question: 172

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

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

Answer: A

Explanation:

Introduction to OSI Model:

The OSI model is a conceptual framework used to understand network interactions in seven layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.

Application Layer:

The application layer (Layer 7) is the topmost layer in the OSI model. It provides network services directly to end-user applications. This layer facilitates communication between software applications and lower layers of the network protocol stack.

Reliance on Other Layers:

The application layer relies on the transport layer (Layer 4) for data transfer across the network. The transport layer ensures reliable data delivery through protocols like TCP and UDP.

The network layer (Layer 3) is responsible for routing packets to their destination.

The data link layer (Layer 2) handles node-to-node data transfer and error detection.

The physical layer (Layer 1) deals with the physical connection between devices.

Explanation of the Options:

A . It relies upon other layers for packet delivery: This is correct. The application layer depends on the lower layers (transport, network, data link, and physical) for the actual delivery of data packets.

B . It checks independently for packet loss: This is incorrect. Packet loss detection is typically handled by the transport layer (e.g., TCP).

C . It encrypts data in transit: This is incorrect. Encryption is typically handled by the presentation layer or at the transport layer (e.g., TLS/SSL).

D . It performs address translation: This is incorrect. Address translation is performed by the network layer

(e.g., NAT).

Conclusion:

The application layer's primary role is to interface with the end-user applications and ensure that data is correctly presented to the user. It relies on the underlying layers to manage the actual data transport and delivery processes.

Reference:

CompTIA Network+ guide covering the OSI model and the specific roles and functions of each layer (see page Ref 10†How to Use Cisco Packet Tracer).

Question: 173

A network engineer is now in charge of all SNMP management in the organization. The engineer must use a SNMP version that does not utilize plaintext dat

a. Which of the following is the minimum version of SNMP that supports this requirement?

A. v1
B. v2c
C. v2u
D. v3

Answer: D

Explanation:

SNMPv3 is the version of the Simple Network Management Protocol that introduces security enhancements, including message integrity, authentication, and encryption. Unlike previous versions (v1 and v2c), SNMPv3 supports encrypted communication, ensuring that data is not transmitted in plaintext. This provides confidentiality and protects against eavesdropping and unauthorized access.Reference: CompTIA Network+ study materials.

Question: 174

Which of the following steps in the troubleshooting methodology would be next after putting preventive measures in place?

A. Implement the solution.
B. Verify system functionality.
C. Establish a plan of action.
D. Test the theory to determine cause.

Answer: B

Explanation:

After implementing a solution and putting preventive measures in place, the next step is to verify that the

system is functioning correctly. This ensures that the issue has been fully resolved.

Question: 175

A network analyst is installing a wireless network in a corporate environment. Employees are required to use their domain identities and credentials to authenticate and connect to the WLAN. Which of the following actions should the analyst perform on the AP to fulfill the requirements?

A. Enable MAC security.
B. Generate a PSK for each user.
C. Implement WPS.
D. Set up WPA3 protocol.

Answer: D

Explanation:

WPA3-Enterprise provides strong security and supports authentication using domain identities through a RADIUS server and 802.1X authentication. This is the best choice for a corporate environment requiring user-based authentication.
WPA3-Enterprise Benefits:
Uses 802.1X with EAP (Extensible Authentication Protocol) to authenticate users via a directory service (e.g., Active Directory).
Eliminates shared passwords (PSK) for authentication.
Provides strong encryption and resistance to brute-force attacks.

Incorrect Options:
A . Enable MAC Security:
MAC filtering is not secure because MAC addresses can be spoofed.
B . Generate a PSK for Each User:
Pre-shared keys (PSK) are used in WPA-Personal, not in an enterprise setting.
Does not scale well in corporate environments.
C . Implement WPS:
Wi-Fi Protected Setup (WPS) is a vulnerable security method meant for home users.
Not suitable for enterprise authentication.
Reference:
CompTIA Network+ N10-009 Official Study Guide – Chapter on Wireless Security and Authentication

Question: 176

Which of the following network topologies contains a direct connection between every node in the network?

A. Mesh
B. Hub-and-spoke
C. Star
D. Point-to-point

Answer: A

Explanation:

In a mesh topology, every node is directly connected to every other node. This provides high redundancy and reliability, as there are multiple paths for data to travel between nodes. This topology is often used in networks where high availability is crucial.Reference: CompTIA Network+ study materials.

Question: 177

A network administrator needs to create a way to redirect a network resource that has been on the local network but is now hosted as a SaaS solution. Which of the following records should be used to accomplish the task?

A. TXT
B. AAA
C. PTR
D. CNAME

Answer: D

Explanation:

To redirect a network resource that has moved from a local network to a Software-as-a-Service (SaaS) solution, the network administrator needs to configure a DNS record that maps an alias to the new canonical name (hostname) of the SaaS provider's server. The CNAME (Canonical Name) record is used to alias one domain name to another, effectively redirecting requests to the new hostname without needing to update the IP address directly. This is ideal for SaaS solutions, where the provider's server hostname is used, and the IP address may change dynamically.

Why not TXT? A TXT record is used to store arbitrary text data, such as SPF records for email authentication or verification strings, not for redirecting resources.

Why not AAA? There is no such thing as an "AAA" record in DNS. This might be a typo for AAAA (IPv6 address record), but AAAA maps a hostname to an IPv6 address, not an alias.

Why not PTR? A PTR record is used for reverse DNS lookups (mapping an IP address to a hostname), not for redirecting a resource to a new hostname.

Reference:CompTIA Network+ N10-009 Objective 1.5: Compare and contrast common network services and ports. The CNAME record is discussed under DNS configuration in the CompTIA Network+ Certification Study Guide (e.g., Mike Meyers' CompTIA Network+ Guide, Chapter 7: TCP/IP Applications). The guide explains that CNAME records are used to create aliases for hostnames, particularly useful for redirecting services to external providers like SaaS solutions.

Question: 178

A wireless technician wants to implement a technology that will allow user devices to automatically navigate to the best available frequency standard. Which of the following technologies should the technician use?

A. Band steering

B. Wireless LAN controller
C. Directional antenna
D. Autonomous access point

Answer: A

Explanation:

Band Steering: This technology enables wireless devices to connect to the most optimal frequency band (2.4 GHz or 5 GHz) by encouraging capable devices to switch to the less congested 5 GHz band. This improves overall network performance and prevents overcrowding on the 2.4 GHz band. Wireless LAN controller (B): This manages multiple access points in a network but does not handle frequency optimization.
Directional antenna (C): This focuses the signal in a specific direction but does not affect frequency selection.
Autonomous access point (D): This operates independently but lacks advanced features like band steering.
Reference: CompTIA Network+ Official Study Guide, Domain 1.6 (Wireless Standards and Technologies).

Question: 179

A research facility is expecting to see an exponential increase in global network traffic in the near future. The offices are equipped with 2.5Gbps fiber connections from the ISP, but the facility is currently only utilizing 1Gbps connections. Which of the following would need to be configured in order to use the ISP's connection speed?

A. 802.1Q tagging
B. Network address translation
C. Port duplex
D. Link aggregation

Answer: D

Explanation:

Understanding Link Aggregation:
Definition: Link aggregation combines multiple network connections into a single logical link to increase bandwidth and provide redundancy.
Usage in High-Bandwidth Scenarios:
Combining Links: By aggregating multiple 1Gbps connections, the facility can utilize the full 2.5Gbps bandwidth provided by the ISP.
Benefits: Enhanced throughput, load balancing, and redundancy, ensuring better utilization of available bandwidth.
Comparison with Other Options:
802.1 Q Tagging: Used for VLAN tagging, which does not affect the physical bandwidth utilization. Network Address Translation (NAT): Used for IP address translation, not related to link speed or bandwidth aggregation.
Port Duplex: Refers to the mode of communication (full or half duplex) on a port, not the aggregation of

bandwidth.

Implementation:

Configure link aggregation (often referred to as LACP - Link Aggregation Control Protocol) on network devices to combine multiple physical links into one logical link.

Reference:

CompTIA Network+ study materials on network configuration and link aggregation.

Question: 180

An organizatin is struggling to get effective coverage using the wireless network. The organization wants to implement a solution that will allow for continous connectivity anywhere in the facility.

Which of the following should the network administ rator suggest to ensure the best coverage?

A. Implementing additional ad hoc access points
B. Providing more Ethernet drops for user connections
C. Deploying a mesh network in the building
D. nl Changing the current frequency of the WI-FI

Answer: C

Explanation:

Question: 181

Several users in an organization report connectivity issues and lag during a video meeting. The network administrator performs a tcpdump and observes increased retransmissions for other nonvideo applications on the network. Which of the following symptoms describes the users' reported issues?

A. Latency
B. Packet loss
C. Bottlenecking
D. Jitter

Answer: B

Explanation:

Packet loss occurs when network packets fail to reach their destination, leading to disruptions in connectivity and performance issues. In this scenario:

Users report connectivity issues and lag during video meetings.

The administrator detects increased retransmissions in tcpdump, which is a strong indicator of lost packets that must be resent.

Video meetings are particularly sensitive to packet loss, leading to buffering, frozen screens, and dropped calls.

Latency (Option A) refers to delayed data transmission but does not necessarily cause retransmissions.

Bottlenecking (Option C) happens when a network component (e.g., router, switch) cannot handle the traffic load, but packet retransmissions are more directly related to packet loss.

Jitter (Option D) affects the consistency of packet arrival times, but the symptoms described here are more aligned with packet loss rather than timing variations.

? Reference: CompTIA Network+ (N10-009) Official Study Guide – Section: Troubleshooting Connectivity Issues

Question: 182

After a company installed a new IPS, the network is experiencing speed degradation. A network administrator is troubleshooting the issue and runs a speed test. The results from the different network locations are as follows:

Location	Speed Down	Speed Up
Wireless laptop	4.8 Mbps	47.1 Mbps
Wired desktop	5.2 Mbps	49.3 Mbps
Firewall	48.8 Mbps	49.5 Mbps

Which of the following is the most likely issue?

A. Packet loss
B. Bottlenecking
C. Channel overlap
D. Network congestion

Answer: B

Explanation:

Bottlenecking occurs when a device in the network (such as an IPS) cannot process traffic efficiently, resulting in a dramatic drop in throughput. The significant difference between the firewall's speed (48.8 Mbps down) and the end-user devices' speeds (4.8 - 5.2 Mbps down) indicates a bottleneck caused by the IPS.

- Why not the other options?
- Packet loss (A) – Would typically cause connection timeouts, not just slow speeds.
- Channel overlap (C) – Affects only wireless networks, but the wired desktop is also experiencing slow speeds.
- Network congestion (D) – Would show fluctuations in both upload and download speeds, but upload speeds remain unaffected.

Reference:

CompTIA Network+ (N10-009) Official Guide – Chapter 13: Network Performance Optimization

Question: 183

A company is implementing a wireless solution in a high-density environment. Which of the following 802.11 standards is used when a company is concerned about device saturation and converage?

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

Answer: B

Explanation:

802.11ax, also known as Wi-Fi 6, is designed for high-density environments and improves device saturation and coverage compared to previous standards.

802.11ac: While it offers high throughput, it is not optimized for high-density environments as effectively as 802.11ax.

802.11ax (Wi-Fi 6): Introduces features like OFDMA, MU-MIMO, and BSS Coloring, which enhance performance in crowded environments, reduce latency, and increase the number of devices that can be connected simultaneously.

802.11g and 802.11n: Older standards that do not offer the same level of efficiency or support for high device density as 802.11ax.

Network Reference:

CompTIA Network+ N10-007 Official Certification Guide: Covers the 802.11 standards and their capabilities.

Cisco Networking Academy: Provides training on Wi-Fi technologies and best practices for high- density deployments.

Network+ Certification All-in-One Exam Guide: Discusses the various 802.11 standards and their applications in different environments.

Question: 184

Which of the following is used to describe the average duration of an outage for a specific service?

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

Answer: B

Explanation:

MTTR (Mean Time to Repair) is the average time it takes to repair a system or service after a failure. It helps in measuring the downtime and planning recovery processes.

Question: 185

A critical infrastructure switch is identified as end-of-support. Which of the following is the best next step to ensure security?

A. Apply the latest patches and bug fixes.
B. Decommission and replace the switch.
C. Ensure the current firmware has no issues.

D. Isolate the switch from the network.

Answer: B

Explanation:

Understanding End-of-Support:
End-of-Support Status: When a vendor declares a device as end-of-support, it means the device will no longer receive updates, patches, or technical support. This poses a security risk as new vulnerabilities will not be addressed.
Risks of Keeping an End-of-Support Device:
Security Vulnerabilities: Without updates, the switch becomes susceptible to new security threats. Compliance Issues: Many regulatory frameworks require that critical infrastructure be maintained with supported and secure hardware.
Best Next Step - Replacement:
Decommission and Replace: The most secure approach is to replace the end-of-support switch with a new, supported model. This ensures the infrastructure remains secure and compliant with current standards.
Planning and Execution: Plan for the replacement by evaluating the network's needs, selecting a suitable replacement switch, and scheduling downtime for the hardware swap.
Comparison with Other Options:
Apply the Latest Patches: While helpful, this does not address future vulnerabilities since no further patches will be provided.
Ensure the Current Firmware Has No Issues: This is only a temporary measure and does not mitigate future risks.
Isolate the Switch from the Network: Isolating the switch may disrupt network operations and is not a viable long-term solution.
Reference:
CompTIA Network+ study materials on network maintenance and security best practices.

Question: 186

Which of the following must be implemented to securely connect a company's headquarters with a branch location?

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

Answer: D

Explanation:

Site-to-Site VPN: A site-to-site VPN is used to securely connect two networks, such as a company's

headquarters and a branch location, over the internet. This type of VPN creates a secure tunnel for data transmission, ensuring confidentiality and integrity.

Split-tunnel VPN (A): Allows some traffic to bypass the VPN tunnel, which may not secure all communications.

Clientless VPN (B): Used for individual users to access the network without VPN client software.

Full-tunnel VPN (C): Typically used for individual user traffic rather than connecting two networks.

Reference: CompTIA Network+ Official Study Guide, Domain 1.3 (Secure Network Connections).

Question: 187

A network engineer wants to implement a new IDS between the switch and a router connected to the LAN. The engineer does not want to introduce any latency by placing the IDS in line with the gateway. The engineer does want to ensure that the IDS sees all packets without any loss. Which of the following is the best way for the engineer to implement the IDS?

A. Use a network tap.
B. Use Nmap software.
C. Use a protocol analyzer.
D. Use a port mirror.

Answer: D

Explanation:

Reference: CompTIA Network+ Certification Exam Objectives - Network Security section.

Question: 188

Which of the following steps of the troubleshooting methodology would most likely include checking through each level of the OSI model after the problem has been identified?

A. Establish a theory.
B. Implement the solution.
C. Create a plan of action.
D. Verify functionality.

Answer: A

Explanation:

The CompTIA troubleshooting methodology includes steps like identifying the problem, establishing a theory of probable cause, testing the theory, creating a plan of action, implementing the solution, verifying functionality, and documenting findings. Establishing a theory involves analyzing the problem and considering possible causes, often by systematically checking each level of the OSI model (Physical, Data Link, Network, etc.) to pinpoint the root cause.

Why not Implement the solution? This step involves applying the fix, not analyzing the OSI model. Why not

Create a plan of action? This step focuses on planning the solution, not diagnosing the cause.
Why not Verify functionality? This step confirms the solution worked, not analyzing the OSI model.
Reference:CompTIA Network+ N10-009 Objective 5.2: Explain the troubleshooting methodology. The CompTIA Network+ Study Guide (e.g., Chapter 13: Network Troubleshooting) details the troubleshooting steps, noting that establishing a theory often involves using the OSI model to systematically identify the cause of network issues.

Question: 189

Which of the following is created to illustrate the effectiveness of wireless networking coverage in a building?

A. Logical diagram
B. Layer 3 network diagram
C. Service-level agreement
D. Heat map

Answer: D

Explanation:

Definition of Heat Maps:
A heat map is a graphical representation of data where individual values are represented by colors. In the context of wireless networking, a heat map shows the wireless signal strength in different areas of a building.
Purpose of a Heat Map:
Heat maps are used to illustrate the effectiveness of wireless networking coverage, identify dead zones, and optimize the placement of access points (APs) to ensure adequate coverage and performance.
Comparison with Other Options:
Logical Diagram: Represents the logical connections and relationships within the network.
Layer 3 Network Diagram: Focuses on the routing and IP addressing within the network.
Service-Level Agreement (SLA): A contract that specifies the expected service levels between a service provider and a customer.
Creation and Use:
Heat maps are created using specialized software or tools that measure wireless signal strength throughout the building. The data collected is then used to generate a visual map, guiding network administrators in optimizing wireless coverage.
Reference:
CompTIA Network+ certification materials and wireless network planning guides.

Question: 190

After changes were made to a firewall, users are no longer able to access a web server. A network administrator wants to ensure that ports 80 and 443 on the web server are still accessible from the user IP space. Which of the following commands is best suited to perfom this testing?

A. Dig

B. Ifconfig
C. Ping
D. nmap

Answer: D

Explanation:

Question: 191

A network administrator needs to assign IP addresses to a newly installed network. They choose 192.168.1.0/24 as their network address and need to create three subnets with 30 hosts on each subnet. Which of the following is a valid subnet mask that will meet the requirements?

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

Answer: C

Explanation:

Understanding the Requirements
Network Address: 192.168.1.0/24
The /24 notation means a subnet mask of 255.255.255.0, providing 256 total addresses (192.168.1.0–192.168.1.255).
Usable hosts: 256 – 2 (network and broadcast) = 254.
Goal: Create 3 subnets, each with 30 hosts.
Each subnet needs enough addresses to accommodate 30 hosts, plus 2 reserved addresses (network and broadcast) per subnet.
Total addresses per subnet = 30 (hosts) + 2 (network/broadcast) = 32 addresses.
Subnetting Basics (Networking Fundamentals)
Subnet Mask: Determines how many bits are borrowed from the host portion to create subnets.
Original Mask: /24 (255.255.255.0) = 24 network bits, 8 host bits.
Formulae:
Number of subnets = 2^(number of borrowed bits).
Number of addresses per subnet = 2^(remaining host bits).
Usable hosts per subnet = 2^(remaining host bits) – 2.
We need:
At least 3 subnets.
At least 32 addresses per subnet (to fit 30 hosts + 2 reserved).
Step-by-Step Analysis
Determine Addresses Needed per Subnet:
32 addresses is a power of 2 (2^5 = 32).
This means each subnet requires 5 host bits (since 2^5 = 32 total addresses, and 32 – 2 = 30 usable hosts).
Calculate Remaining Bits:

Original network has 8 host bits (/24).

If 5 bits are left for hosts, we borrow: 8 – 5 = 3 bits for subnetting.

New Subnet Mask:

Original mask: /24 (24 network bits).

Borrow 3 bits: 24 + 3 = /27.

/27 = 255.255.255.224 (binary: 11111111.11111111.11111111.11100000).

Verify Requirements:

Number of Subnets: 2^3 = 8 subnets (meets the requirement of at least 3).

Addresses per Subnet: 2^5 = 32 addresses.

Usable Hosts per Subnet: 32 – 2 = 30 hosts (exactly meets the requirement).

Subnet Breakdown:

Increment: 256 – 224 = 32 (each subnet increments by 32 in the fourth octet).

Subnets:

192.168.1. 0–192.168.1.31 (Network: .0, Broadcast: .31, Hosts: .1–.30)

192.168.1.32 –192.168.1.63 (Network: .32, Broadcast: .63, Hosts: .33–.62)

192.168.1.64 –192.168.1.95 (Network: .64, Broadcast: .95, Hosts: .65–.94)

(And 5 more subnets up to 192.168.1.255.)

Three subnets fit perfectly with 30 hosts each.

Evaluating the Options

A . 255.255.255.128 (/25):

Borrow 1 bit: 24 + 1 = /25.

Subnets: 2^1 = 2 (not enough, need 3).

Host bits: 7 (2^7 = 128 addresses, 126 hosts).

Why Not: Only 2 subnets, fails the requirement.

B . 255.255.255.192 (/26):

Borrow 2 bits: 24 + 2 = /26.

Subnets: 2^2 = 4 (meets 3).

Host bits: 6 (2^6 = 64 addresses, 62 hosts).

Why Not: 62 hosts exceeds 30, but it’s overkill; /27 is more efficient and still valid.

C . 255.255.255.224 (/27):

Borrow 3 bits: 24 + 3 = /27.

Subnets: 2^3 = 8 (meets 3).

Host bits: 5 (2^5 = 32 addresses, 30 hosts).

Why Yes: Perfectly fits 3 subnets with exactly 30 hosts each.

D . 255.255.255.240 (/28):

Borrow 4 bits: 24 + 4 = /28.

Subnets: 2^4 = 16 (meets 3).

Host bits: 4 (2^4 = 16 addresses, 14 hosts).

Why Not: Only 14 hosts per subnet, fails the 30-host requirement.

Why /27 (255.255.255.224) is Best

It provides exactly 30 usable hosts per subnet, avoiding waste while meeting the minimum requirement.

It allows 8 subnets, exceeding the need for 3, ensuring flexibility.

The study guide emphasizes efficient subnet design, and /27 balances host count and subnet availability.

CompTIA Network+ Context

Networking Fundamentals: Subnetting is a core skill, requiring understanding of CIDR, binary conversion, and address allocation.

Example from Study Guide: Similar problems calculate subnet masks for specific host counts, reinforcing /27 as a common solution for ~30 hosts.

Question: 192

Which of the following is the most cost-effective way for a network administrator to establish a persistent, secure connection between two facilities?

A. Site-to-site VPN
B. GRE tunnel
C. VXLAN
D. Dedicated line

Answer: A

Explanation:

A Site-to-site VPN (Virtual Private Network) is the most cost-effective solution for establishing a persistent, secure connection between two facilities. It uses the public internet to create an encrypted tunnel, leveraging existing internet connections without requiring expensive dedicated infrastructure. This makes it ideal for organizations looking to securely connect remote sites while minimizing costs.

Why not GRE tunnel? Generic Routing Encapsulation (GRE) tunnels encapsulate traffic but do not provide encryption natively, requiring additional protocols (e.g., IPsec) for security. This adds complexity and is less cost-effective than a site-to-site VPN, which integrates encryption. Why not VXLAN? Virtual Extensible LAN (VXLAN) is used for overlay networks in data centers to extend Layer 2 networks, not for secure site-to-site connectivity.

Why not Dedicated line? A dedicated line (e.g., leased line or MPLS) provides high reliability but is significantly more expensive due to the need for dedicated infrastructure.

Reference:CompTIA Network+ N10-009 Objective 1.7: Explain the use cases for virtual private networks (VPNs) and tunneling protocols. The CompTIA Network+ Study Guide (e.g., Chapter 12: Network Security) explains that site-to-site VPNs are a cost-effective, secure method for connecting geographically separate networks over the internet.

Question: 193

Which of the following can support a jumbo frame?

A. Access point
B. Bridge
C. Hub
D. Switch

Answer: D

Explanation:

Definition of Jumbo Frames:

Jumbo frames are Ethernet frames with more than 1500 bytes of payload, typically up to 9000 bytes. They are

used to improve network performance by reducing the overhead caused by smaller frames. Why Switches Support Jumbo Frames:

Switches are network devices designed to manage data packets and can be configured to support jumbo frames. This capability enhances throughput and efficiency, particularly in high-performance networks and data centers.

Incompatibility of Other Devices:

Access Point: Primarily handles wireless communications and does not typically support jumbo frames.

Bridge: Connects different network segments but usually operates at standard Ethernet frame sizes. Hub: A simple network device that transmits packets to all ports without distinguishing between devices, incapable of handling jumbo frames.

Practical Application:

Enabling jumbo frames on switches helps in environments where large data transfers are common, such as in storage area networks (SANs) or large-scale virtualized environments.

Reference:

CompTIA Network+ course materials and networking hardware documentation.

Question: 194

After providing a username and password, a user must input a passcode from a phone application. Which of the following authentication technologies is used in this example?

A. SSO
B. LDAP
C. MFA
D. SAML

Answer: C

Explanation:

This is an example of Multi-Factor Authentication (MFA) because it requires:

Something you know (username/password)

Something you have (a phone-generated passcode)

Breakdown of Options:

A . SSO (Single Sign-On) – Allows one login for multiple services, but does not add a second authentication factor.

B . LDAP (Lightweight Directory Access Protocol) – Used for directory authentication, not MFA.

C . MFA (Multi-Factor Authentication) – Q Correct answer. Uses multiple authentication factors for better security.

E. SAML (Security Assertion Markup Language) – Used for federated identity management, not multi-factor authentication.

Reference:

CompTIA Network+ (N10-009) Official Study Guide – Domain 3.5: Implement authentication and authorization methods.

Question: 195

Which of the following best explains the role of confidentiality with regard to data at rest?

A. Datacanbe accessedby anyone on the administrative network.
B. Datacanbe accessedremotely with proper training.
C. Datacanbe accessedafter privileged access Is granted.
D. Datacanbe accessedafter verifying the hash.

Answer: C

Explanation:

Confidentiality with Data at Rest: Confidentiality is a core principle of data security, ensuring that data stored (at rest) is only accessible to authorized individuals. This protection is achieved through mechanisms such as encryption, access controls, and permissions.
Privileged Access: The statement "Data can be accessed after privileged access is granted" aligns with the confidentiality principle, as it restricts data access to users who have been granted specific permissions or roles. Only those with the appropriate credentials or permissions can access the data. Incorrect Options:
A . "Data can be accessed by anyone on the administrative network." This violates the principle of confidentiality by allowing unrestricted access.
B . "Data can be accessed remotely with proper training." This focuses on remote access rather than restricting access based on privileges.
D . "Data can be accessed after verifying the hash." This option relates more to data integrity rather than confidentiality.
CompTIA Network+ materials on data security principles, particularly sections on confidentiality and access control mechanisms.

Question: 196

A network administrator needs to connect a department to a new network segment. They need to use a DHCP server located on another network. Which of the following can the administrator use to complete this task?

A. IP Helper
B. Reservation
C. Exclusion
D. Scope

Answer: A

Explanation:

An IP Helper (IP Helper Address) allows DHCP requests to pass through routers and reach a DHCP server on another network.

DHCP broadcasts are not forwarded across routers by default, so an IP Helper Address is needed to relay the request.

This is crucial for large networks where a single DHCP server serves multiple subnets.

Option B (Reservation): Ensures a specific IP address is assigned to a MAC address but does not relay DHCP across networks.

Option C (Exclusion): Prevents specific IP addresses from being assigned, but does not help with DHCP relay.

Option D (Scope): Defines the range of IP addresses available for DHCP clients but does not assist in cross-network communication.

? Reference: CompTIA Network+ (N10-009) Official Study Guide – Section: DHCP and IP Addressing

Question: 197

While troubleshooting a VoIP handset connection, a technician's laptop is able to successfully connect to network resources using the same port. The technician needs to identify the port on the switch. Which of the following should the technician use to determine the switch and port?

A. LLDP
B. IKE
C. VLAN
D. netstat

Answer: A

Explanation:

Link Layer Discovery Protocol (LLDP) is a network protocol used for discovering devices and their capabilities on a local area network, primarily at the data link layer (Layer 2). It helps in identifying the connected switch and the specific port to which a device is connected. When troubleshooting a VoIP handset connection, the technician can use LLDP to determine the exact switch and port where the handset is connected. This protocol is widely used in network management to facilitate the discovery of network topology and simplify troubleshooting.

Other options such as IKE (Internet Key Exchange), VLAN (Virtual LAN), and netstat (network statistics) are not suitable for identifying the switch and port information. IKE is used in setting up secure IPsec connections, VLAN is used for segmenting networks, and netstat provides information about active connections and listening ports on a host but not for discovering switch port details. Reference: CompTIA Network+ Certification Exam Objectives - Network Troubleshooting and Tools section.

Question: 198

A group of users cannot connect to network resources. The technician runs ipconfig from one user's

device and is able to ping the gateway shown from the command. Which of the following is most likely preventing the users from accessing network resources?

A. VLAN hopping

B. Rogue DHCP
C. Distributed DoS
D. Evil twin

Answer: B

Explanation:

A rogue DHCP server occurs when an unauthorized or misconfigured DHCP server assigns incorrect IP addresses, default gateways, or DNS settings to clients.

- In this scenario:
- The user can ping the gateway, meaning local network communication is working.
- However, they cannot access network resources, which suggests incorrect IP configuration (likely due to a rogue DHCP server assigning the wrong gateway or DNS).
- Why not the other options?
- VLAN hopping (A): This is an attack that exploits VLAN configurations to gain access to unauthorized VLANs. It would not typically cause multiple users to lose network access.
- Distributed DoS (C): A DDoS attack floods a network or service with traffic, but this issue is more likely misconfigured IP settings than an actual attack.
- Evil twin (D): This refers to a fraudulent Wi-Fi network mimicking a legitimate one. Since the users are on a wired network (ipconfig output checked), this is not applicable.

Reference:
CompTIA Network+ (N10-009) Official Guide – Chapter 11: Network Security Threats

Question: 199

A network administrator is implementing security zones for each department. Which of the following should the administrator use to accomplish this task?

A. ACLs
B. Port security
C. Content filtering
D. NAC

Answer: A

Explanation:

Understanding ACLs:
Access Control Lists (ACLs): A set of rules used to control network traffic and restrict access to network resources by filtering packets based on IP addresses, protocols, or ports.
Implementing Security Zones:
Defining Zones: ACLs can be used to create security zones by applying specific rules to different departments, ensuring that only authorized traffic is allowed between these zones.
Control Traffic: ACLs control inbound and outbound traffic at network boundaries, enforcing security policies and preventing unauthorized access.

Comparison with Other Options:

Port Security: Limits the number of devices that can connect to a switch port, preventing MAC address flooding attacks, but not used for defining security zones.

Content Filtering: Blocks or allows access to specific content based on predefined policies, typically used for web filtering rather than network segmentation.

NAC (Network Access Control): Controls access to the network based on the security posture of devices but does not define security zones.

Implementation Steps:

Define ACL rules based on the requirements of each department.

Apply these rules to the appropriate network interfaces or firewall policies to segment the network into security zones.

Reference:

CompTIA Network+ study materials on network security and access control methods.

Question: 200

Which of the following is a cost-effective advantage of a split-tunnel VPN?

A. Web traffic is filtered through a web filter.
B. More bandwidth is required on the company's internet connection.
C. Monitoring detects insecure machines on the company's network.
D. Cloud-based traffic flows outside of the company's network.

Answer: D

Explanation:

A split-tunnel VPN allows some traffic to be routed through the VPN while other traffic goes directly to the internet. This setup offers several advantages, with a primary one being cost-effectiveness due to cloud-based traffic not consuming company bandwidth.

Bandwidth Utilization: Split-tunnel VPNs reduce the amount of traffic passing through the company's network, freeing up bandwidth for other uses.

Performance: By allowing internet-bound traffic to bypass the VPN, it can reduce latency and improve the performance for users accessing cloud services directly.

Cost Savings: Reduced load on the company's VPN infrastructure can lead to lower costs in terms of both hardware and bandwidth.

Network Reference:

CompTIA Network+ N10-007 Official Certification Guide: Covers VPN types, including split-tunnel configurations and their advantages.

Cisco Networking Academy: Discusses VPN technologies and the benefits of split-tunneling.

Network+ Certification All-in-One Exam Guide: Provides detailed information on VPN setups, including the cost-effectiveness of split-tunnel VPNs.

By allowing cloud-based traffic to flow outside the company's network, a split-tunnel VPN optimizes resource usage and enhances the overall network performance without incurring extra costs for bandwidth.

Question: 201

A company wants to implement data loss prevention by restricting user access to social media platforms and personal cloud storage on workstations. Which of the following types of filtering should the company deploy to achieve these goals?

A. Port
B. DNS
C. MAC
D. Content

Answer: D

Explanation:
Reference: CompTIA Network+ Certification Exam Objectives - Network Security section.

Question: 202

A company recently rearranged some users' workspaces and moved several users to previously used workspaces. The network administrator receives a report that all of the users who were moved are having connectivity issues. Which of the following is the MOST likely reason?

A. Ports are error-disabled.
B. Ports have an incorrect native VLAN.
C. Ports are having an MDIX issue.
D. Ports are trunk ports.

Answer: B

Explanation:

The most likely cause is that the switch ports were previously configured for a different VLAN than the one the users' computers are on. If the native VLAN on the port doesn't match the end device's VLAN, communication fails.

A . Ports are error-disabled: Would result in no link at all, not common across multiple ports unless a violation occurred.

C . MDIX issue: Auto-MDIX eliminates most crossover problems on modern switches.

D . Ports are trunk ports: While possible, typical user devices should be on access ports, but if the port is incorrectly trunked, it can cause similar issues. However, "incorrect VLAN" is more precise here.

Reference:

CompTIA Network+ N10-009 Official Objectives: 2.3 – Given a scenario, configure and verify VLANs.

Question: 203

As part of an attack, a threat actor purposefully overflows the content-addressable memory (CAM) table on a switch. Which of the following types of attacks is this scenario an example of?

A. ARP spoofing
B. Evil twin
C. MAC flooding
D. DNS poisoning

Answer: C

Explanation:

Definition of MAC Flooding:
MAC flooding is an attack where a malicious actor sends numerous fake MAC addresses to a switch, overwhelming its CAM table. The CAM table stores MAC addresses and their associated ports for efficient traffic forwarding.
Impact of MAC Flooding:
CAM Table Overflow: When the CAM table is full, the switch cannot learn new MAC addresses and is forced to broadcast traffic to all ports, leading to a degraded network performance and potential data interception.
Switch Behavior: The switch operates in a fail-open mode, treating the network as a hub, which can be exploited for eavesdropping on traffic.
Comparison with Other Attacks:
ARP Spoofing: Involves sending false ARP (Address Resolution Protocol) messages to associate the attacker's MAC address with the IP address of another device.
Evil Twin: Involves creating a rogue wireless access point that mimics a legitimate one to intercept data.
DNS Poisoning: Involves corrupting the DNS cache with false information to redirect traffic to malicious sites.
Preventive Measures:
Port Security: Configure port security on switches to limit the number of MAC addresses per port, preventing CAM table overflow.
Network Segmentation: Use VLANs to segment network traffic and limit the impact of such attacks.
Reference:
CompTIA Network+ study materials on network security threats and mitigation techniques.

Question: 204

A network engineer is completing a wireless installation in a new building. A requirement is that all clients be able to automatically connect to the fastest supported network. Which of the following best supports this requirement?

A. Enabling band steering
B. Disabling the 5GHz SSID
C. Adding a captive portal
D. Configuring MAC filtering

Answer: A

Explanation:

Band steering is a feature in wireless networks that encourages dual-band capable devices to connect to the 5GHz band instead of the 2.4GHz band.

Why Band Steering?

The 5GHz band supports higher speeds and less interference compared to 2.4GHz.

If a device supports both bands, the access point (AP) can "steer" it to connect to 5GHz instead of 2.4GHz.

This helps ensure users always connect to the fastest available network.

Incorrect Options:

B . Disabling the 5GHz SSID: Would force devices onto 2.4GHz, which is slower and more congested.

C . Adding a Captive Portal: Used for guest authentication, not for speed optimization.

D . Configuring MAC Filtering: Used for security, not for optimizing network speed.

Reference:

CompTIA Network+ N10-009 Official Study Guide – Chapter on Wireless Technologies and Optimization

Question: 205

Which of the following does a full-tunnel VPN provide?

A. Lower bandwidth requirements
B. The ability to reset local computer passwords
C. Corporate Inspection of all networktraffic
D. Access to blocked sites

Answer: C

Explanation:

A full-tunnel VPN routes all of a user's network traffic through the corporate network. This means that the organization can inspect all network traffic for security and compliance purposes, as all data is tunneled through the VPN, allowing for comprehensive monitoring and inspection.Reference: CompTIA Network+ study materials.

Question: 206

A virtual machine has the following configuration:

- IPv4 address: 169.254.10.10
- Subnet mask: 255.255.0.0

The virtual machine can reach colocated systems but cannot reach external addresses on the Internet.

Which of the following Is most likely the root cause?

A. Thesubnet mask is incorrect.
B. TheDHCP server is ofline.
C. TheIP address is an RFC1918 private address.
D. TheDNS server is unreachable.

Answer: B

Explanation:

Understanding the 169.254.x.x Address:

An IPv4 address in the range of 169.254.x.x is an Automatic Private IP Addressing (APIPA) address, assigned when a DHCP server is unavailable.

DHCP Server Ofline:

APIPA Assignment: When a device cannot obtain an IP address from a DHCP server, it assigns itself an APIPA address to enable local network communication. This allows communication with other devices on the same local subnet but not with external networks.

Resolution: Ensure the DHCP server is operational. Check for connectivity issues between the virtual machine and the DHCP server, and verify the DHCP server settings.

Comparison with Other Options:

The subnet mask is incorrect: The subnet mask 255.255.0.0 is appropriate for the 169.254.x.x range and does not prevent external access by itself.

The IP address is an RFC1918 private address: RFC1918 addresses are private IP ranges (10.x.x.x, 172.16.x.x-172.31.x.x, 192.168.x.x) but 169.254.x.x is not one of them.

The DNS server is unreachable: While this could affect name resolution, it would not prevent the assignment of a non-APIPA address or local network communication.

Troubleshooting Steps:

Verify the DHCP server's status and connectivity.

Restart the DHCP service if necessary.

Renew the IP lease on the virtual machine using commands such as ipconfig /renew (Windows) or dhclient (Linux).

Reference:

CompTIA Network+ study materials on IP addressing and DHCP troubleshooting.

Question: 207

Which of the following provides an opportunity for an on-path attack?

A. Phishing
B. Dumpster diving
C. Evil twin
D. Tailgating

Answer: C

Explanation:

An evil twin is a rogue Wi-Fi access point that mimics a legitimate network. Attackers use it to intercept and manipulate traffic, making it an on-path (formerly MITM) attack opportunity. Breakdown of Options:

A . Phishing – Tries to steal credentials through fake emails/websites but does not intercept network traffic.

B . Dumpster diving – Involves physical security breaches, not network interception.

C . Evil twin – Q Correct answer. A rogue Wi-Fi AP impersonates a real network, allowing traffic interception.

D . Tailgating – Involves physical access security, not network interception.

Reference:

CompTIA Network+ (N10-009) Official Study Guide – Domain 3.3: Explain common network security threats.

Question: 208

A network engineer needs to order cabling to connect two buildings within the same city. Which of the following media types should the network engineer use?

A. Coaxial
B. Twinaxial
C. Single-mode fiber
D. Cat 5

Answer: C

Explanation:

Single-mode fiber is best suited for long-distance communication, often exceeding 10 km (6.2 miles). It's immune to EMI and offers high bandwidth — making it the ideal choice for connecting buildings across a city.

Coaxial (A) and Twinaxial (B) are used for shorter distances and specific use cases (e.g., storage or legacy systems).

Cat 5 (D) is limited to 100 meters and is not suitable for city-level interconnects.

Q For long-distance, high-speed, and reliable communication between buildings, Single-mode fiber is the professional choice.

Reference:CompTIA Network+ N10-009 Official Study Guide — Objective 3.4: "Summarize the properties and purposes of physical network topologies and network types."

Question: 209

SIMULATION

SIMULATION

You have been tasked with setting up a wireless network in an office. The network will consist of 3 Access Points and a single switch. The network must meet the following parameters:

The SSIDs need to be configured as CorpNet with a key of S3cr3t!

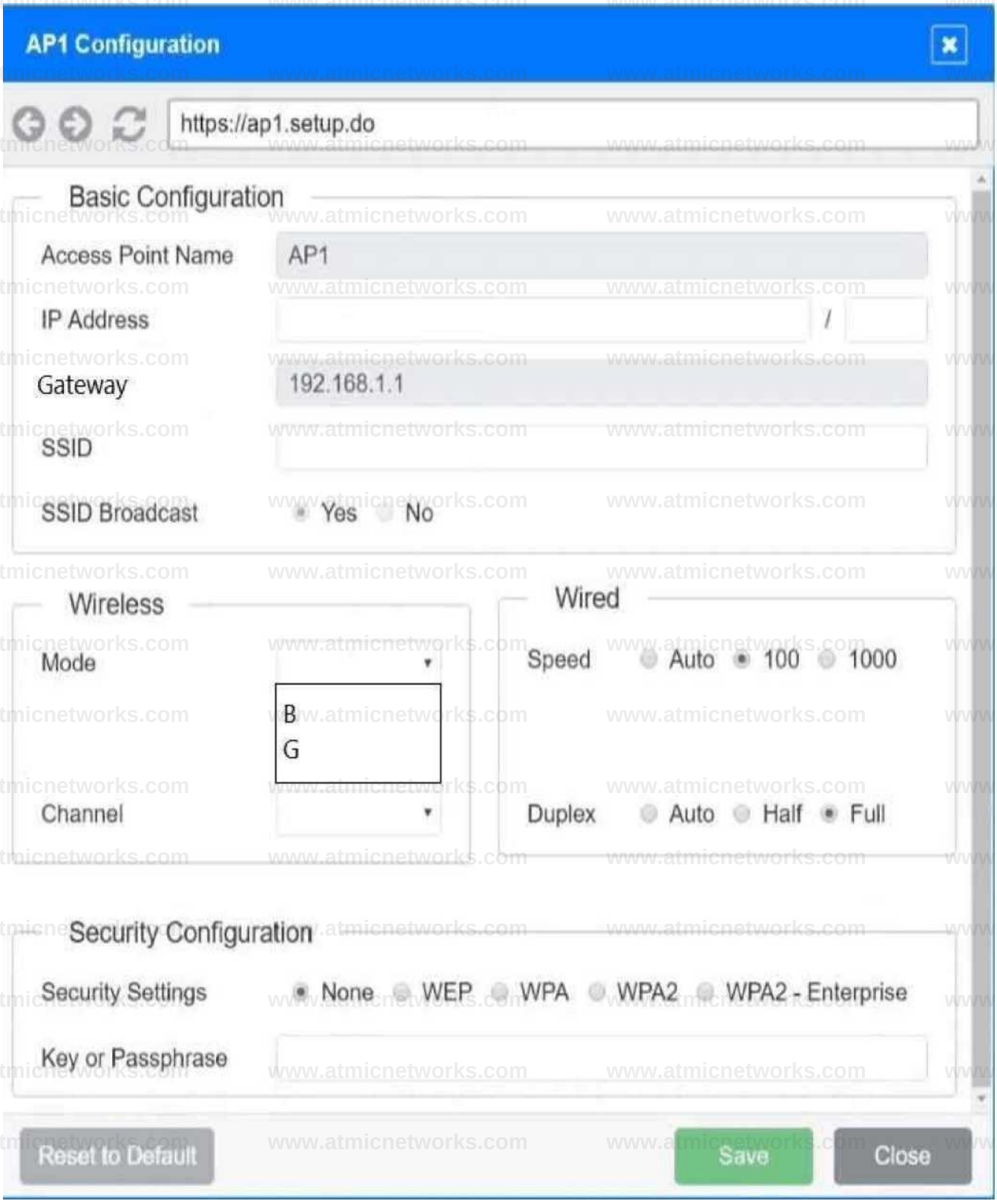
The wireless signals should not interfere with each other

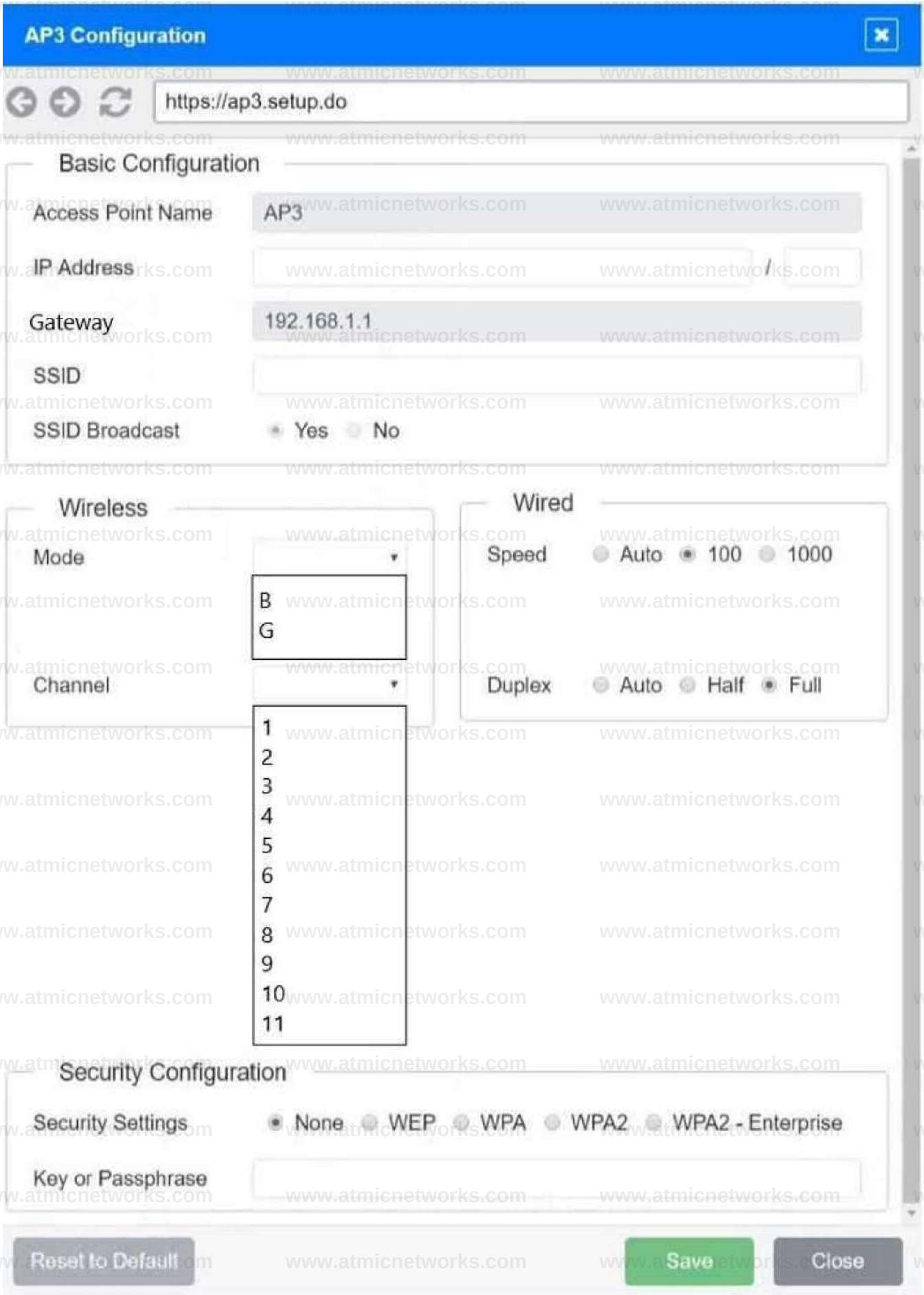
The subnet the Access Points and switch are on should only support 30 devices maximum

The Access Points should be configured to only support TKIP clients at a maximum speed INSTRUCTONS

Click on the wireless devices and review their information and adjust the settings of the access points to meet the given requirements.

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

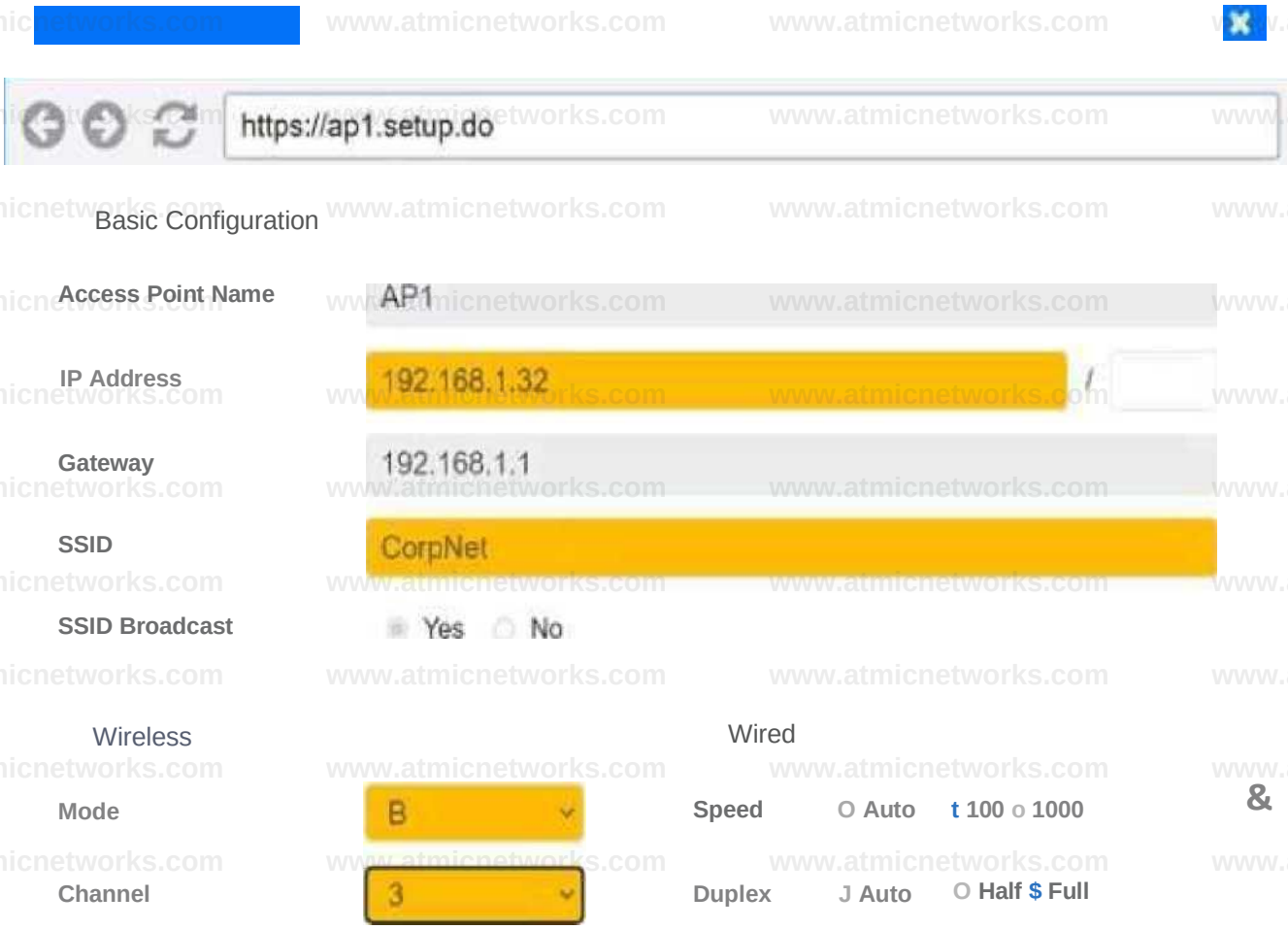




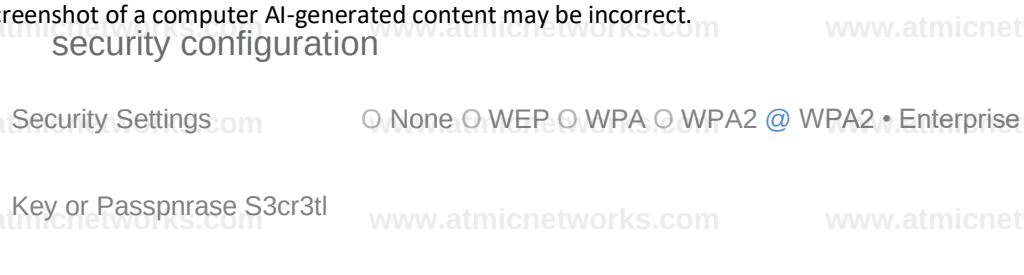
Answer: See explanation below.

Explanation:

On the first exhibit, the layout should be as follows



A screenshot of a computer AI-generated content may be incorrect.



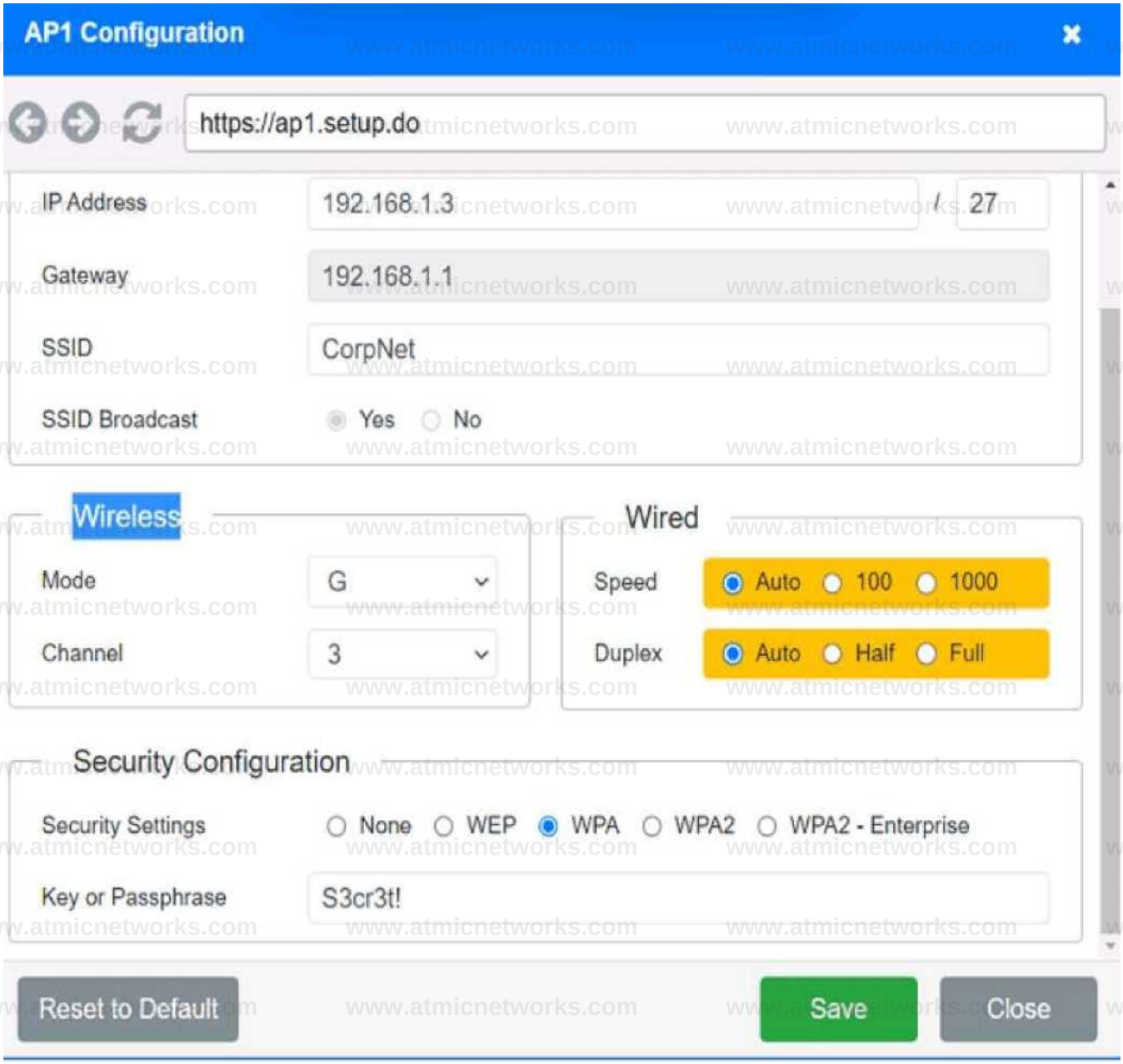
A screenshot of a computer AI-generated content may be incorrect.
A screenshot of a computer AI-generated content may be incorrect.

security configuration

Security Settings 0 None O WEP O WPA O WPA2 @ WPA2 • Enterprise

Key or Passpnrase S3cr3tl

A screenshot of a computer AI-generated content may be incorrect.



A screenshot of a computer AI-generated content may be incorrect.

Exhibit 2 as follows

Access Point Name AP2

00 https//sp2 setup do

Basic Configuration

Access Point Name	AP2
IP Address	192.168.1.64 / 27
Gateway	192.168.1.1
SSID	CorpNet
SSID Broadcast	Yes No

Wireless

Mode	B
Channel	6

Wired

Speed	0 Auto 100 1000
Duplex	Auto Half Full

Security Configuration

Reset to Default Save Close

A screenshot of a computer AI-generated content may be incorrect.
A screenshot of a computer AI-generated content may be incorrect.
A screenshot of a computer AI-generated content may be incorrect.

AP? Configuration

Exhibit 3 as follows

Access Point Name AP3

AP3 Configuration

. ; https://ap3.setup.do

Wireless

Mode B

Channel 9

Wired

Speed o Auto #100 3 1000

Duplex G Auto Hall • Full

A screenshot of a computer AI-generated content may be incorrect.

security configuration

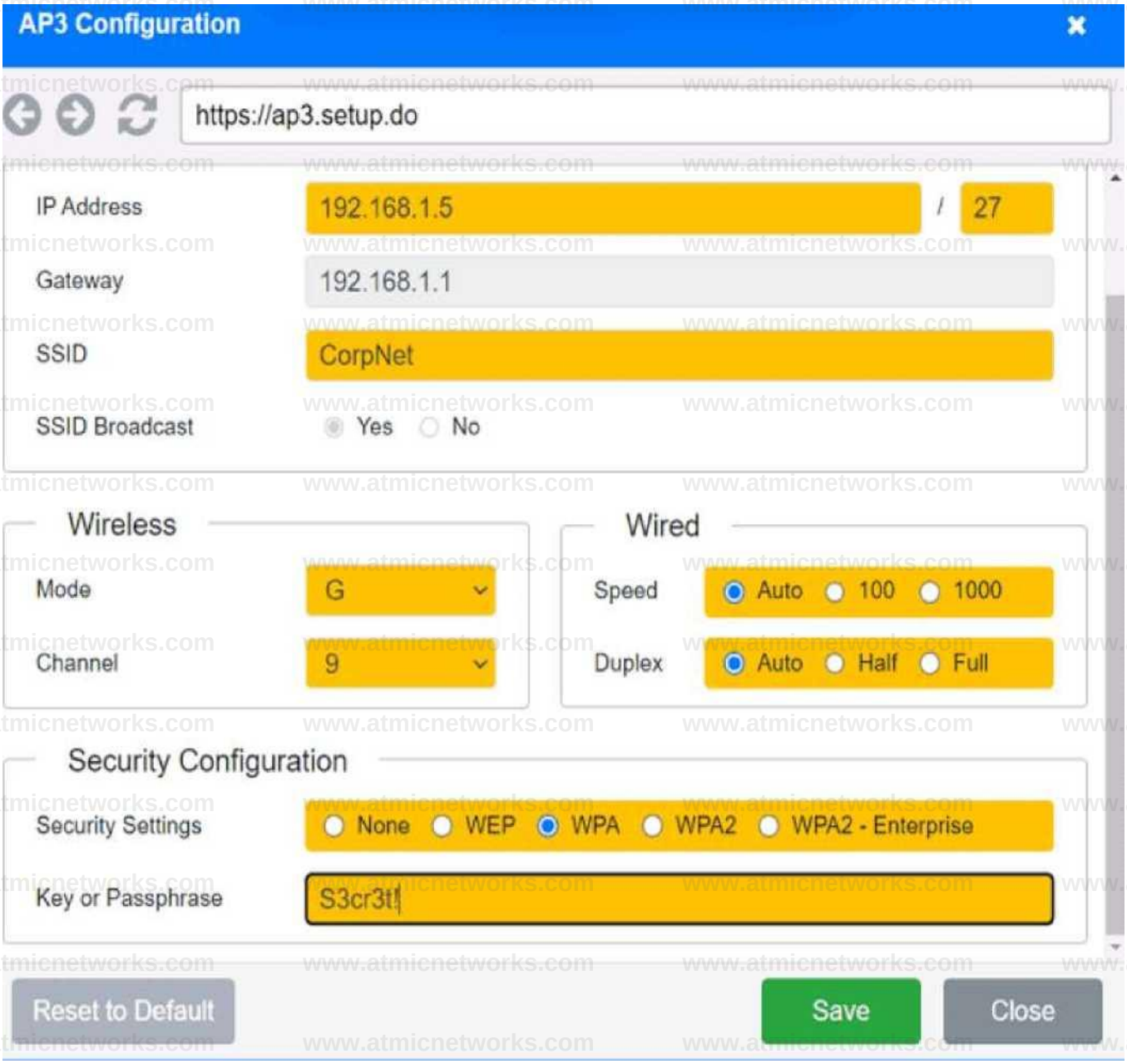
Basic Configuration

Access Point Name	AP3
IP Address	192.168 J .96 / 27
Gateway	192.168 1 1
SSID	CorpNei
SSID Broadcast	Yes No

Security Settings O None O WEP O WPA O WPA2 @ WPA2 • Enterprise

Key or Passphrase S3cr3tl

A screenshot of a computer AI-generated content may be incorrect.



A screenshot of a computer AI-generated content may be incorrect.

Question: 210

Which of the following should be used to obtain remote access to a network appliance that has failed to start up properly?

A. Crash cart
B. Jump box
C. Secure Shell (SSH)
D. Out-of-band management

Answer: D

Explanation:

If a network appliance fails to start, standard remote access methods like SSH won't work. Instead, Out-of-Band (OOB) management provides a dedicated access path (e.g., a console port or iDRAC/iLO), allowing administrators to troubleshoot devices even when the network is down. Breakdown of Options:

A . Crash cart – A physical monitor/keyboard setup, not a remote solution.

B . Jump box – A hardened system used for secure remote access but requires the device to be operational.

C . Secure Shell (SSH) – Requires the device to be fully booted and network-connected.

D . Out-of-band management – Q Correct answer. Provides independent access for troubleshooting failed network devices.

Reference:

CompTIA Network+ (N10-009) Official Study Guide – Domain 4.3: Explain network device management concepts.

Question: 211

A network administrator needs to set up a multicast network for audio and video broadcasting.
Which of the following networks would be the most appropriate for this application?

A. 172.16.0.0/24
B. 192.168.0.0/24
C. 224.0.0.0/24
D. 240.0.0.0/24

Answer: C

Explanation:

Understanding Multicast:

Multicast IP Address Range: The multicast address range is from 224.0.0.0 to 239.255.255.255, designated for multicast traffic.

Multicast Applications:

Use Case: Multicast is used for one-to-many or many-to-many communication, suitable for applications like audio and video broadcasting where the same data is sent to multiple recipients simultaneously.

Appropriate Network Selection:

192.1. 0.0/24 Network: This range is reserved for multicast addresses, making it the appropriate choice for setting up a multicast network.

Comparison with Other Options:

172.16. 0.0/24: Part of the private IP address space, used for private networks, not designated for multicast.

192.168. 0.0/24: Another private IP address range, also not for multicast.

240.0.0.0/24: Reserved for future use, not suitable for multicast.

Reference:

CompTIA Network+ study materials on IP address ranges and multicast.

Question: 212

A technician is troubleshooting a user's laptop that is unable to connect to a corporate server. The technician thinks the issue pertains to routing. Which of the following commands should the technician use to identify the issue?

A. tcpdump

B. dig
C. tracert
D. arp

Answer: C

Explanation:

The tracert (Traceroute) command is used to determine the path packets take from the source to the destination. It helps in identifying routing issues by showing each hop the packets pass through, along with the time taken for each hop. This command can pinpoint where the connection is failing or experiencing delays, making it an essential tool for troubleshooting routing issues.Reference: CompTIA Network+ study materials and common network troubleshooting commands.

Question: 213

A medical clinic recently configured a guest wireless network on the existing router. Since then, guests have been changing the music on the speaker system. Which of the following actions should the clinic take to prevent unauthorized access? (Select two).

A. Isolate smart devices to their own network segment.
B. Configure IPS to prevent guests from making changes.
C. Install a new AP on the network.
D. Set up a syslog server to log who is making changes.
E. Change the default credentials.
F. Configure GRE on the wireless router.

Answer: A,E

Explanation:

- A. Isolate smart devices to their own network segment: Network segmentation using VLANs or separate SSIDs ensures that smart devices (like speakers) are not on the same network as guests, preventing unauthorized control.
- E. Change the default credentials: Many IoT devices (e.g., smart speakers) come with default usernames and passwords. If these are not changed, unauthorized users can easily take control.
- Why not the other options?
- B. Configure IPS: IPS (Intrusion Prevention System) detects threats but cannot block specific guest

actions on an IoT device.

- C. Install a new AP: A new access point does not solve the unauthorized control issue.
- D. Set up a syslog server: Helps with logging, but does not prevent unauthorized access.
- F. Configure GRE: Generic Routing Encapsulation (GRE) is used for VPN tunneling, which is irrelevant in this case.

Reference:
CompTIA Network+ (N10-009) Official Guide – Chapter 11: Network Security

Question: 214

A network administrator recently upgraded a wireless infrastructure with new APs. Users report that when stationary, the wireless connection drops and reconnects every 20 to 30 seconds. While reviewing logs, the administrator notices the APs are changing channels.

Which of the following is the most likely reason for the service interruptions?

A. Channel interference
B. Roaming misconfiguration
C. Network congestion
D. Insufficient wireless coverage

Answer: A

Explanation:

If APs are changing channels frequently, it indicates automatic channel selection due to interference.

This can cause temporary disconnections as the APs switch frequencies.

Breakdown of Options:

A . Channel interference – Q Correct answer. APs change channels automatically to avoid interference, causing disconnections.

B . Roaming misconfiguration – Roaming only affects moving users, but users report issues while stationary.

C . Network congestion – Causes slow speeds, not frequent disconnects.

D . Insufficient wireless coverage – Would cause weak signals, but not channel switching issues.

Reference:

CompTIA Network+ (N10-009) Official Study Guide – Domain 1.6: Explain wireless troubleshooting techniques.

Question: 215

Which of the following routing protocols is most commonly used to interconnect WANs?

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

Answer: C

Explanation:

Border Gateway Protocol (BGP): BGP is the most commonly used routing protocol for interconnecting WANs, especially across the internet. It is used for exchanging routing information between autonomous systems (AS), making it the backbone protocol for large-scale WANs.

IGP (A): Interior Gateway Protocols like OSPF and EIGRP are typically used within a single AS, not between them.

EIGRP (B): While it is efficient, EIGRP is primarily used for intra-domain routing and not ideal for WAN interconnection.

OSPF (D): While OSPF can be used for WANs, it is not as common as BGP for inter-AS communication. Reference: CompTIA

Network+ Official Study Guide, Domain 1.3 (WAN Concepts), Domain 2.5 (Routing Protocols).

Question: 216

Which of the following will allow secure, remote access to internal applications?

A. VPN
B. CDN
C. SAN
D. IDS

Answer: A

Explanation:

A Virtual Private Network (VPN) creates an encrypted connection between a remote user and an internal network, ensuring secure access to internal applications.
VPNs use encryption protocols like IPSec and SSL/TLS to protect data during transmission.
They are widely used for secure remote work, accessing company resources, and bypassing geographic restrictions.
Option B (CDN - Content Delivery Network): Used for speeding up website content delivery, not for remote access security.
Option C (SAN - Storage Area Network): Used for high-speed storage, unrelated to remote access. Option D (IDS - Intrusion Detection System): Monitors for malicious activities but does not provide secure access to applications.
? Reference: CompTIA Network+ (N10-009) Official Study Guide – Section: Secure Remote Access Technologies

Question: 217

A company implements a video streaming solution that will play on all computers that have joined a particular group, but router ACLs are blocking the traffic. Which of the following is the most
appropriate IP address that will be allowed in the ACL?

A. 127.0.0.1
B. 172.17.1.1
C. 224.0.0.1
D. 240.0.0.1

Answer: C

Explanation:

224.0.0.1 is a multicast address that allows packets to be sent to all hosts within a multicast group. Since video streaming often uses multicast to efficiently distribute data to multiple clients without unnecessary duplication, this is the correct answer.

- Why not the other options?

- 127.0.0.1 (A) – This is the loopback address used for internal device testing, not for multicast traffic.
- 172.17.1.1 (B) – This is a private unicast address, meaning it can only send packets to one specific host.
- 240.0.0.1 (D) – This falls within the reserved experimental IP address range and is not used for multicast.

Reference:
CompTIA Network+ (N10-009) Official Guide – Chapter 7: IP Addressing and Subnetting

Question: 218

A network technician is examining the configuration on an access port and notices more than one VLAN has been set. Which of the following best describes how the port is configured?

A. With a voice VLAN
B. With too many VLANs
C. With a default VLAN
D. With a native VLAN

Answer: A

Explanation:

It is common for an access port to have both a voice VLAN and a data VLAN. A voice VLAN separates voice traffic from regular data traffic, ensuring better quality and security for voice communications.

==========

Question: 219

Which of the following routing protocols uses an autonomous system number?

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

Answer: D

Explanation:

BGP (Border Gateway Protocol) uses an Autonomous System (AS) number for its operations. An AS is a collection of IP networks and routers under the control of a single organization that presents a common routing policy to the Internet. BGP is used to exchange routing information between different ASes on the Internet, making it the only protocol among the listed options that uses an AS number.Reference: CompTIA Network+ study materials and RFC 4271.

Question: 220

Which of the following best describes a group of devices that is used to lure unsuspecting attackers and to study the

attackers' activities?

A. Geofencing
B. Honeynet
C. Jumpbox
D. Screened subnet

Answer: B

Explanation:

A honeynet is a network of honeypots designed to attract and study attackers. Honeypots are decoy systems set up to lure cyber attackers and analyze their activities. A honeynet, being a collection of these systems, provides a broader view of attack methods and patterns, helping organizations improve their security measures. Reference: CompTIA Network+ Exam Objectives and official study guides.

Question: 221

A network administrator suspects users are being sent to malware sites that are posing as legitimate sites. The network administrator investigates and discovers that user workstations are configured with incorrect DNS IP addresses. Which of the following should the network administrator implement to prevent this from happening again?

A. Dynamic ARP inspection
B. Access control lists
C. DHCP snooping
D. Port security

Answer: C

Explanation:

DHCP snooping is a security feature on network switches that helps to prevent unauthorized (rogue) DHCP servers from assigning IP addresses to clients. By implementing DHCP snooping, the network administrator can restrict DHCP responses to authorized servers only, preventing unauthorized DHCP configurations, such as incorrect DNS IPs, from being assigned to clients. This helps prevent man-in- the-middle attacks where malicious actors misconfigure DNS to redirect users to fraudulent sites. (Reference: CompTIA Network+ Study Guide, Chapter on Network Security)

Question: 222

Which of the following appliances provides users with an extended footprint that allows connections from multiple devices within a designated WLAN?

A. Router

B. Switch
C. Access point
D. Firewall

Answer: C

Explanation:

An access point (AP) provides users with an extended footprint that allows connections from multiple devices within a designated Wireless Local Area Network (WLAN).
Router: Typically used to connect different networks, not specifically for extending wireless coverage.
Switch: Used to connect devices within a wired network, not for providing wireless access.
Access Point (AP): Extends wireless network coverage, allowing multiple wireless devices to connect to the network.
Firewall: Primarily used for network security, controlling incoming and outgoing traffic based on security rules, not for providing wireless connectivity.
Network Reference:
CompTIA Network+ N10-007 Official Certification Guide: Explains the roles and functions of network appliances, including access points.
Cisco Networking Academy: Provides training on deploying and managing wireless networks with access points.
Network+ Certification All-in-One Exam Guide: Covers network devices and their roles in creating and managing networks.

Question: 223

Which of the following is used to estimate the average life span of a device?

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

Answer: C

Explanation:

Understanding MTBF:
Mean Time Between Failures (MTBF): A reliability metric that estimates the average time between successive failures of a device or system.
Calculation and Importance:
Calculation: MTBF is calculated as the total operational time divided by the number of failures during that period.
Usage: Used by manufacturers and engineers to predict the lifespan and reliability of a device, helping in maintenance planning and lifecycle management.
Comparison with Other Metrics:
RTO (Recovery Time Objective): The maximum acceptable time to restore a system after a failure. RPO (Recovery Point

Objective): The maximum acceptable amount of data loss measured in time. MTTR (Mean Time to Repair): The average time required to repair a device or system and return it to operational status.

Application:

MTBF is crucial for planning maintenance schedules, spare parts inventory, and improving the overall reliability of systems.

Reference:

CompTIA Network+ study materials on reliability and maintenance metrics.

Question: 224

Which of the following should be configured so users can authenticate to a wireless network using company credentials?

A. SSO
B. SAML
C. MFA
D. RADIUS

Answer: D

Explanation:

RADIUS (Remote Authentication Dial-In User Service) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service. RADIUS is often used to manage access to wireless networks, enabling users to authenticate with their company credentials, ensuring secure access to the network.Reference: CompTIA Network+ study materials.

Question: 225

A company upgrades its network and PCs to gigabit speeds. After the upgrade, users are not getting the expected performance. Technicians discover that the speeds of the endpoint NICs are inconsistent. Which of the following should be checked first to troubleshoot the issue?

A. Speed mismatches
B. Load balancer settings
C. Flow control settings
D. Infrastructure cabling grade

Answer: A

Explanation:

Speed Mismatches: If NICs are set to different speeds (e.g., 100 Mbps on one side and 1 Gbps on the other), performance will degrade. Ensuring consistent speed settings between devices is crucial for optimal performance.

Load balancer settings (B): Applies to server load distribution, not endpoint speed.
Flow control settings (C): Can affect performance but is secondary to speed mismatches.
Infrastructure cabling grade (D): Relevant if the cables are unsuitable for gigabit speeds, but speed settings should be checked first.
Reference: CompTIA Network+ Official Study Guide, Domain 2.5 (Troubleshooting Network Issues).

Question: 226

An organization moved its DNS servers to new IP addresses. After this move, customers are no longer able to access the organization's website. Which of the following DNS entries should be updated?

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

Answer: D

Explanation:

When an organization moves its DNS servers to new IP addresses, the NS (Name Server) records must be updated. The NS record defines which DNS servers are authoritative for a domain. Ifthese

records still point to the old IP addresses, clients will continue to query the outdated servers, leading to connectivity issues.
Breakdown of Options:
A . AAAA – This record maps a domain name to an IPv6 address. Since the issue is with DNS resolution, not IP versioning, this is incorrect.
B . CNAME – A CNAME (Canonical Name) record is used for domain aliasing, not for defining authoritative name servers.
C . MX – Mail Exchange (MX) records direct email traffic to the correct mail server, which does not impact general website accessibility.
D . NS – Correct answer. NS records must be updated to reflect the new authoritative DNS servers. Reference:
CompTIA Network+ (N10-009) Official Study Guide – Domain 1.3: Explain the purpose and properties of DNS records.
RFC 1035: Domain Names - Implementation and Specification

Question: 227

A network administrator is configuring a wireless network with an ESSID. Which of the following is a user benefit of ESSID compared to SSID?

A. Stronger wireless connection
B. Roaming between access points
C. Advanced security
D. Increased throughput

Answer: B

Explanation:

An Extended Service Set Identifier (ESSID) allows multiple access points to share the same SSID, enabling seamless roaming for users. This means that users can move between different access points within the same ESSID without losing connection or having to reauthenticate. This provides a better user experience, especially in large environments such as office buildings or campuses.Reference: CompTIA Network+ study materials.

Question: 228

A network engineer performed a migration to a new mail server. The engineer changed the MX record, verified the change was accurate, and confirmed the new mail server was reachable via the IP address in the A record. However, users are not receiving email. Which of the following should the engineer have done to prevent the issue from occurring?

A. Change the email client configuration to match the MX record.
B. Reduce the TTL record prior to the MX record change.
C. Perform a DNS zone transfer prior to the MX record change.
D. Update the NS record to reflect the IP address change.

Answer: B

Explanation:

Understanding TTL (Time to Live):

TTL is a value in a DNS record that tells how long that record should be cached by DNS servers and clients. A higher TTL value means that the record will be cached longer, reducing the load on the DNS server but delaying the propagation of changes.

Impact of TTL on DNS Changes:

When an MX record change is made, it may take time for the change to propagate across all DNS servers due to the TTL setting. If the TTL is high, old DNS information might still be cached, leading to email being directed to the old server.

Best Practice Before Making DNS Changes:

To ensure that changes to DNS records propagate quickly, it is recommended to reduce the TTL value to a lower value (such as 300 seconds or 5 minutes) well in advance of making the changes. This ensures that any cached records will expire quickly, and the new records will be used sooner.

Verification of DNS Changes:

After reducing the TTL and making the change to the MX record, it is important to verify the propagation using tools like dig or nslookup.

Comparison with Other Options:

Change the email client configuration to match the MX record: Email clients generally do not need to match the MX record directly; they usually connect to a specific mail server specified in their settings. Perform a DNS zone transfer prior to the MX record change: DNS zone transfers are used to replicate DNS records between DNS servers, but they are not related to the propagation of individual record changes.

Update the NS record to reflect the IP address change: NS records specify the DNS servers for a domain and are not related to MX record changes.

Reference:

CompTIA Network+ study materials and DNS best practices.

Question: 229

Which of the following protocols has a default administrative distance value of 90?

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

Answer: B

Explanation:

EIGRP (Enhanced Interior Gateway Routing Protocol) has a default administrative distance (AD) value of 90 for internal routes. The administrative distance is used to rate the trustworthiness of routing information received from different routing protocols. EIGRP, developed by Cisco, has an AD of 90, which is lower than that of RIP (120) and OSPF (110), making it more preferred if multiple protocols provide a route to the same destination.Reference: CompTIA Network+ study materials.

Question: 230

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 probe, often referred to as a toner and probe kit, is the easiest and most effective tool for identifying individual cables in a bundle, especially in situations where the patch panel is not labeled. The toner sends an audible tone through the cable, and the probe detects the tone at the other end, allowing the technician to quickly identify the correct cable.

Functionality: The toner generates a tone that travels along the cable. When the probe is placed near the correct cable, it detects the tone and emits a sound.

Ease of Use: Toner probes are straightforward to use, even in environments with many cables, making them ideal for identifying cables in unlabeled patch panels.

Efficiency: This method is much faster and more reliable than manual tracing, especially in complex setups.

Network Reference:

CompTIA Network+ N10-007 Official Certification Guide: Details tools used for cable identification and troubleshooting. Cisco Networking Academy: Provides training on using toner probes and other cable testing tools. Network+ Certification All-in-One Exam Guide: Explains the use of different tools for network cable identification and management.

Question: 231

Which of the following disaster recovery concepts is calculated by dividing the total hours of operation by the total number of units?

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

Answer: B

Explanation:

Introduction to Disaster Recovery Concepts:
Disaster recovery involves strategies and measures to ensure business continuity and data recovery in the event of a disaster.
Mean Time Between Failures (MTBF):
MTBF is a reliability metric used to predict the time between failures of a system during operation. It is calculated by dividing the total operational time by the number of failures.
Formula: MTBF=Total Operational TimeNumber of Failures\text{MTBF} = \frac{\text{Total Operational Time}}{\text{Number of Failures}}MTBF=Number of FailuresTotal Operational Time This metric helps in understanding the reliability and expected lifespan of systems and components. Example Calculation:
If a server operates for 1000 hours and experiences 2 failures, the MTBF is:
MTBF=1000 hours2=500 hours\text{MTBF} = \frac{1000 \text{ hours}}{2} = 500 \text{ hours}MTBF=21000 hours=500 hours
Explanation of the Options:
A . MTTR (Mean Time to Repair): The average time required to repair a system after a failure.
B . MTBF (Mean Time Between Failures): The correct answer, representing the average time between failures.
C . RPO (Recovery Point Objective): The maximum acceptable amount of data loss measured in time. D . RTO (Recovery Time Objective): The target time set for the recovery of IT and business activities after a disaster.
Conclusion:
MTBF is a crucial metric in disaster recovery and system reliability, helping organizations plan maintenance and predict system performance.
Reference:
CompTIA Network+ guide explaining MTBF, MTTR, RPO, and RTO concepts and their calculations (see page Ref 10†How to Use Cisco Packet Tracer).

Question: 232

An ISP provided a company with a pre-configured modem and five public static IP addresses. Which of the following does the company's firewall require to access the internet? (Select TWO).

A. NTP server
B. Default gateway
C. The modem's IP address
D. One static IP address
E. DNS servers
F. DHCP server

Answer: B,D

Explanation:

To access the internet using static IPs, the firewall (or router) must be configured correctly:

B . Default gateway: This is essential because it tells the firewall where to send outbound traffic destined for outside the local network.

D . One static IP address: The firewall must be assigned one of the static IPs to communicate over the public internet.

The other options are not essential for basic internet connectivity in this context:

A . NTP server: Useful for time synchronization but not required for internet access.

C . The modem's IP address: Irrelevant unless doing modem-level configuration.

E . DNS servers: Important for name resolution but not for basic layer 3 connectivity.

F . DHCP server: Not used when static IPs are assigned.

Reference:

CompTIA Network+ N10-009 Official Objectives: 2.2 – Compare and contrast addressing technologies.

Question: 233

Which of the following network ports is used when a client accesses an SFTP server?

A. 22
B. 80
C. 443
D. 3389

Answer: A

Explanation:

SFTP (Secure File Transfer Protocol) operates over port 22, using SSH (Secure Shell) encryption for secure file transfers.

Breakdown of Options:

A . 22 – Correct answer. SFTP runs over SSH (port 22) for secure file transfers.

B . 80 – Used for HTTP, not SFTP.

C . 443 – Used for HTTPS (secure web traffic).

D . 3389 – Used for RDP (Remote Desktop Protocol).

Reference:

CompTIA Network+ (N10-009) Official Study Guide – Domain 3.1: Compare and contrast network protocols.

RFC 4253: SSH Transport Layer Protocol

Question: 234

A network administrator is troubleshooting a connectivity issue between two devices on two different subnets. The administrator verifies that both devices can successfully ping other devices on the same subnet. Which of the following is the most likely cause of the connectivity issue?

A. Incorrect default gateway
B. Faulty Ethernet cable
C. Wrong duplex settings
D. VLAN mismatch

Answer: A

Explanation:

When two devices on different subnets are unable to communicate, but can communicate with other devices on their own subnet, the issue is most often related to routing. Devices on different subnets require a default gateway to route traffic between networks.

If the default gateway is incorrectly configured, the device won't know how to reach other subnets. Faulty cables (Option B) or duplex mismatches (Option C) would likely cause connectivity issues even within the local subnet, which is not the case here.

VLAN mismatches (Option D) are typically issues with switch port configurations and would likely cause total loss of connectivity, including within the same subnet.

Q So, the most probable and logical cause is an incorrect default gateway.

Reference:CompTIA Network+ N10-009 Official Study Guide — Objective 2.4: "Compare and contrast routing technologies."

Question: 235

SIMULATION

A network administrator has been tasked with configuring a network for a new corporate office. The office consists of two buildings, separated by 50 feet with no physical connectivity. The configuration must meet the following requirements:

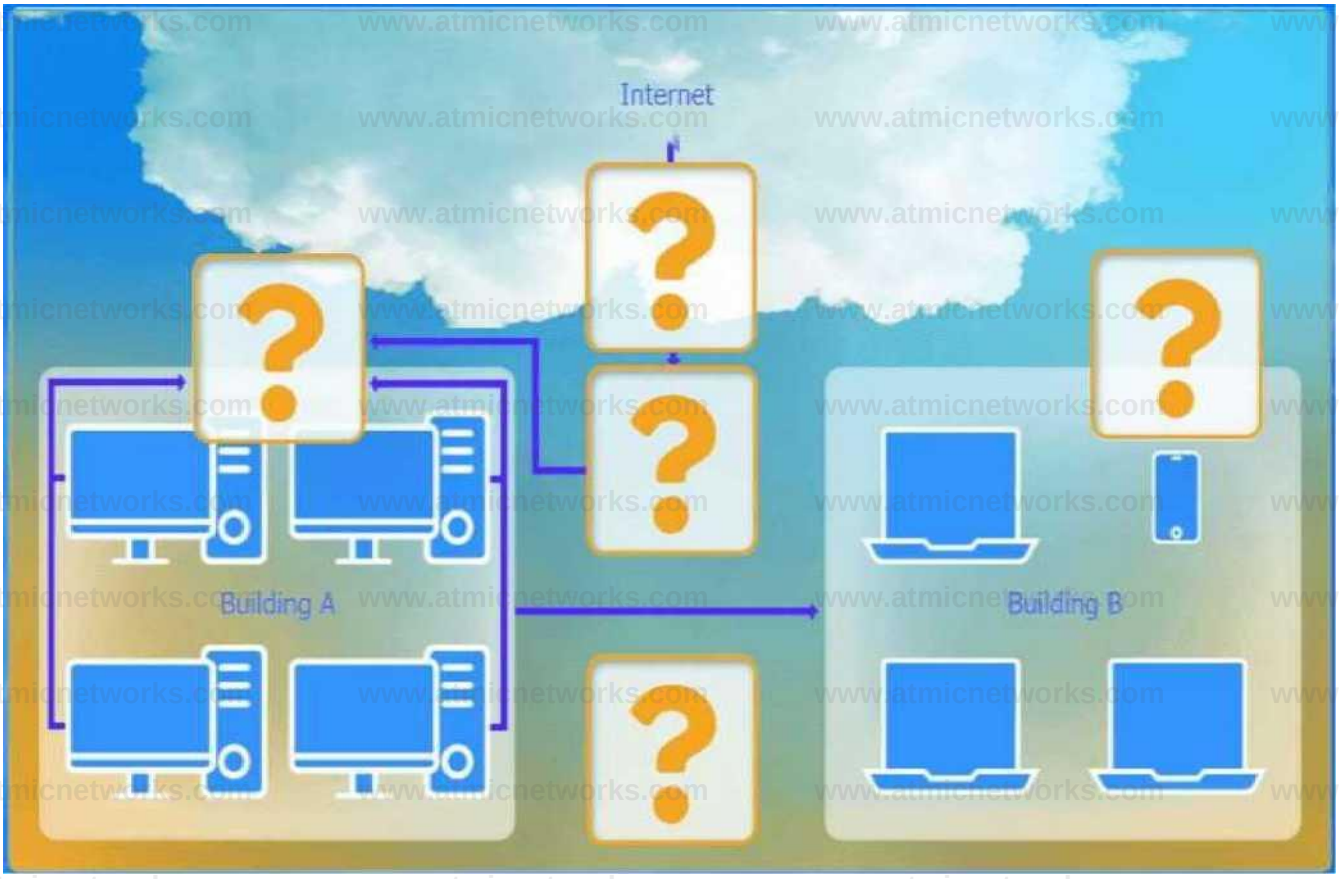
. Devices in both buildings should be able to access the Internet.
. Security insists that all Internet traffic be inspected before entering the network.
. Desktops should not see traffic destined for other devices.

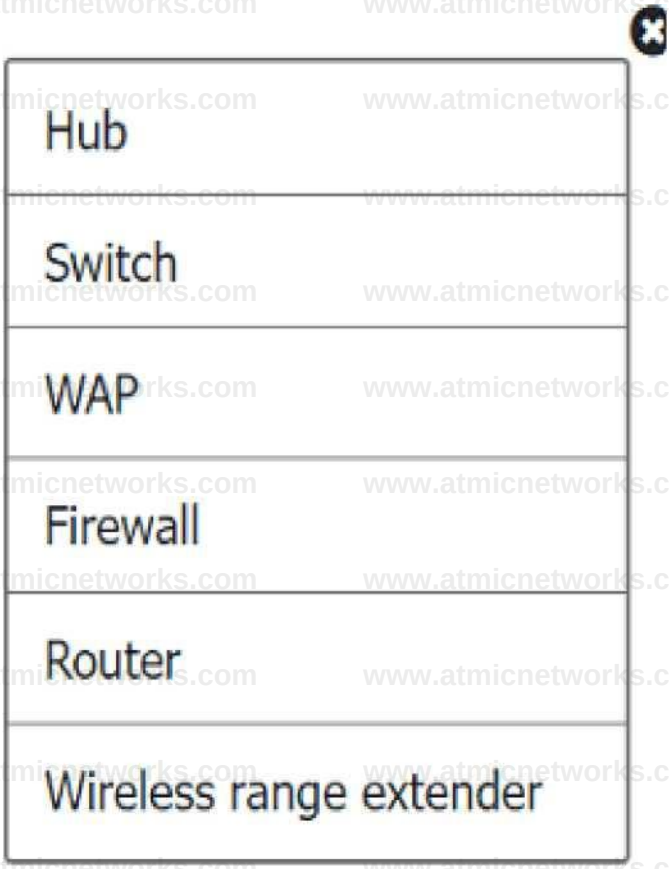
INSTRUCTIONS

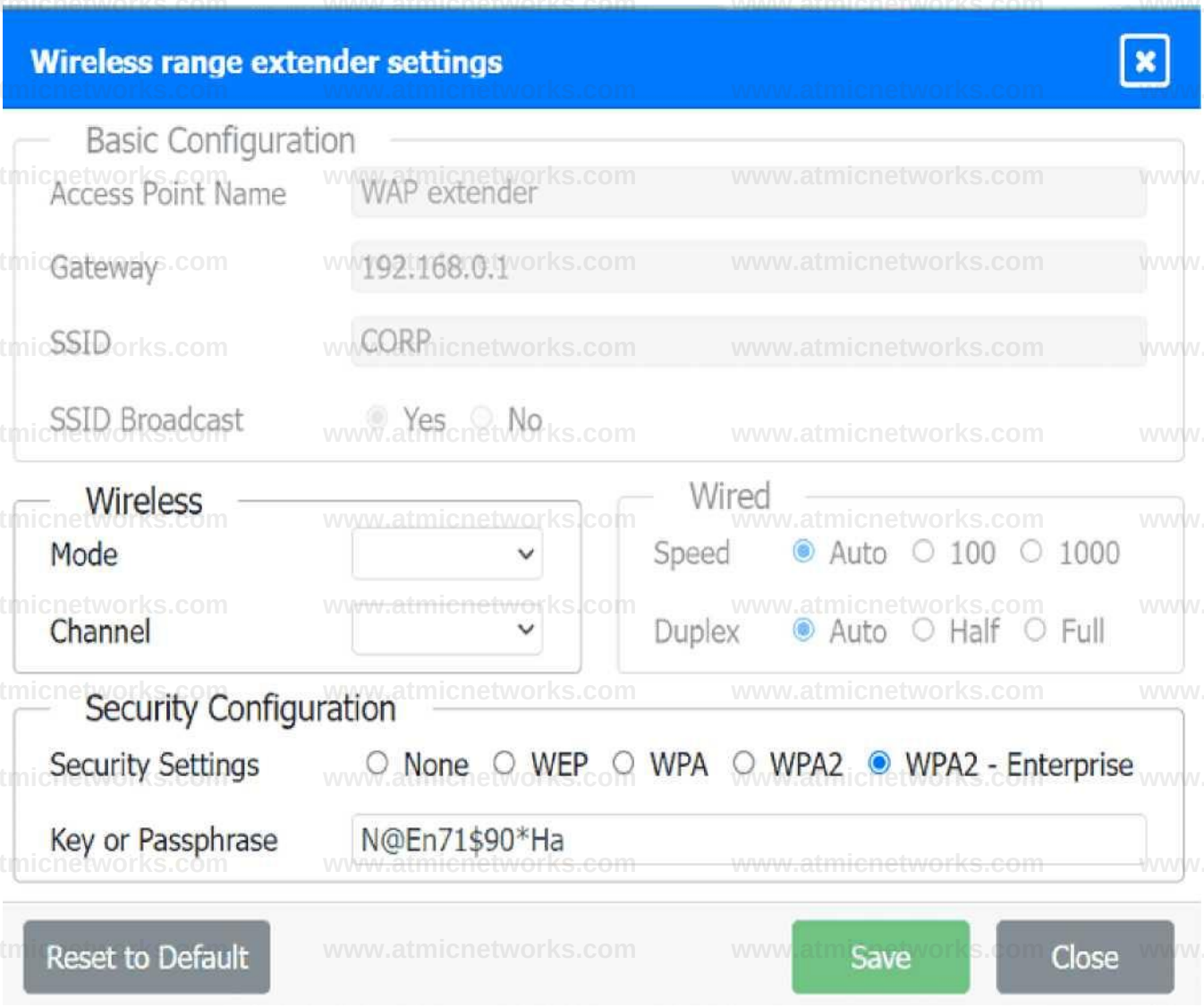
Select the appropriate network device for each location. If applicable, click on the magnifying glass next to any device which may require configuration updates and make any necessary changes.

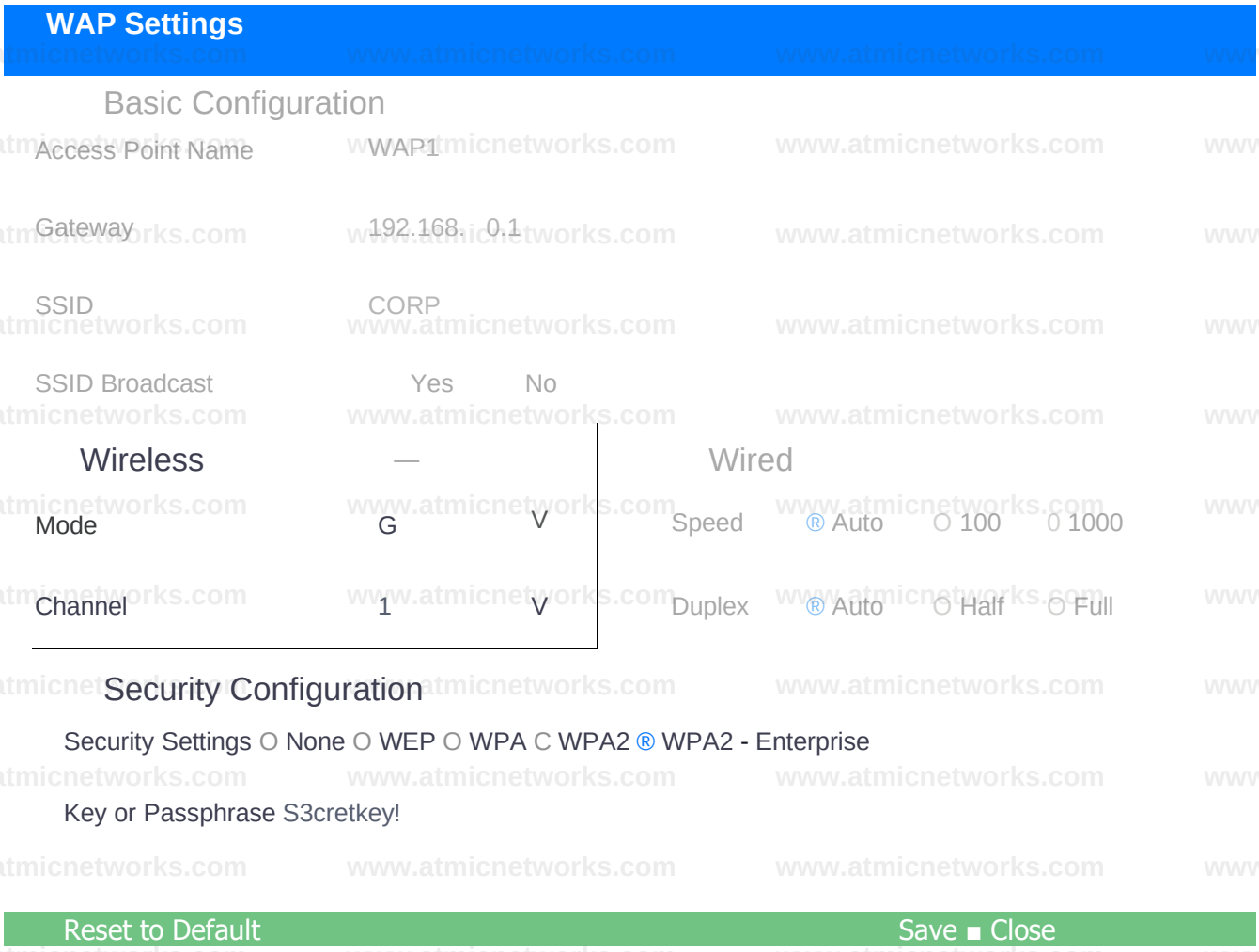
Not all devices will be used, but all locations should be filled.

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




Hub
Switch
WAP
Firewall
Router
Wireless range extender





Answer: See the step by step complete solution below.

Explanation:

Devices in both buildings should be able to access the Internet.

Security insists that all Internet traffic be inspected before entering the network.

Desktops should not see traffic destined for other devices.

Here is the corrected layout with explanation:

Building A:

Switch: Correctly placed to connect all desktops.

Firewall: Correctly placed to inspect all incoming and outgoing traffic.

Building B:

Switch: Not needed. Instead, place a Wireless Access Point (WAP) to provide wireless connectivity for laptops and mobile devices.

Between Buildings:

Wireless Range Extender: Correctly placed to provide connectivity between the buildings wirelessly.

Connection to the Internet:

Router: Correctly placed to connect to the Internet and route traffic between the buildings and the Internet.

Firewall: The firewall should be placed between the router and the internal network to inspect all traffic before it enters the network.

Corrected Setup:

Top-left (Building A): Switch

Bottom-left (Building A): Firewall (inspect traffic before it enters the network)

Top-middle (Internet connection): Router

Bottom-middle (between buildings): Wireless Range Extender

Top-right (Building B): Wireless Access Point (WAP)

In this corrected setup, the WAP in Building B will connect wirelessly to the Wireless Range Extender, which is connected to the Router. The Router is connected to the Firewall to ensure all traffic is inspected before it enters the network.

Configuration for Wireless Range Extender:

SSID: CORP

Security Settings: WPA2 or WPA2 - Enterprise

Key or Passphrase: [Enter a strong passphrase]

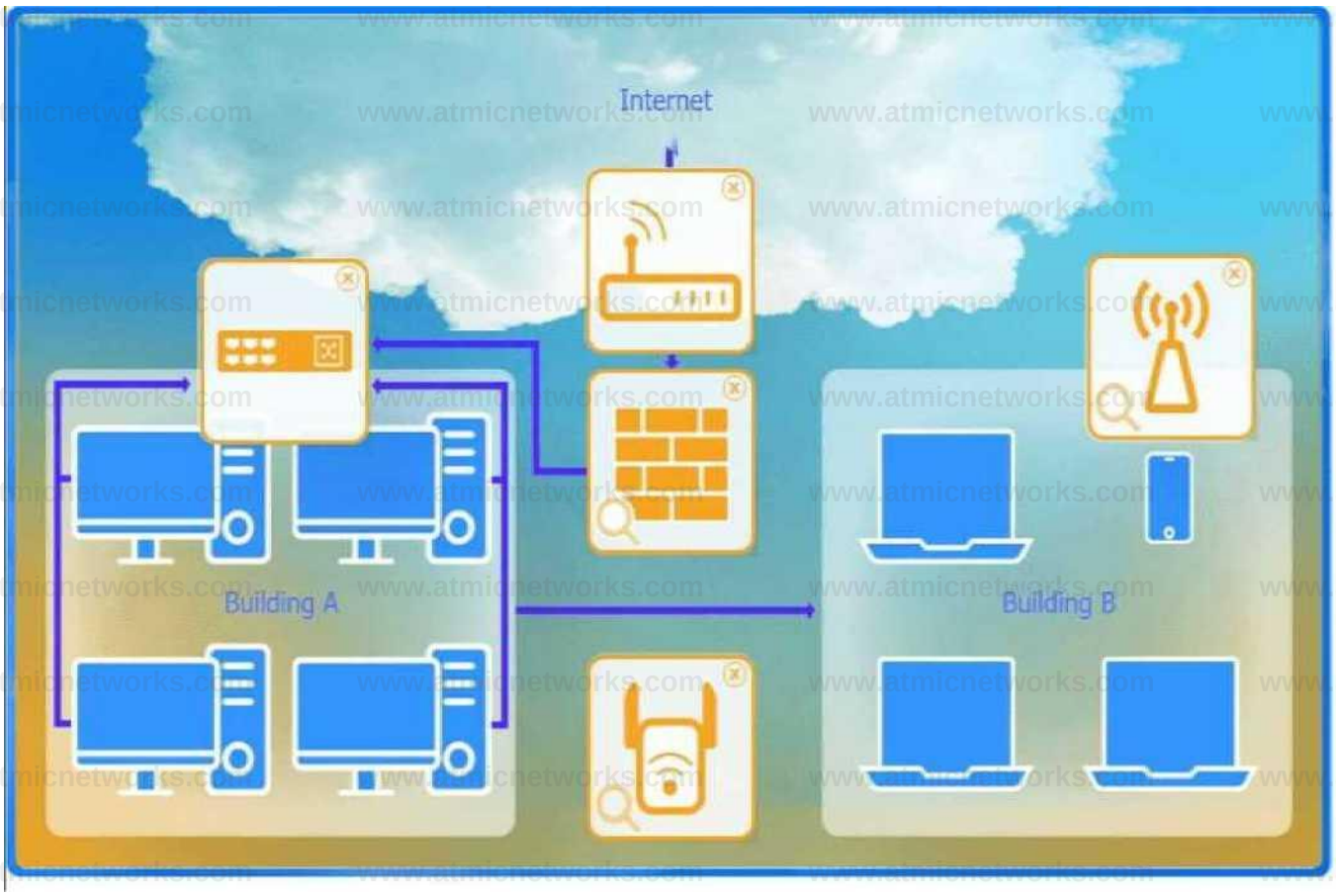
Mode: [Set based on your network plan]

Channel: [Set based on your network plan]

Speed: Auto

Duplex: Auto

With these settings, both buildings will have secure access to the Internet, and all traffic will be inspected by the firewall before entering the network. Desktops and other devices will not see traffic intended for others, maintaining the required security and privacy.



To configure the wireless range extender for security, follow these steps:

SSID (Service Set Identifier):

Ensure the SSID is set to "CORP" as shown in the exhibit.

Security Settings:

WPA2 or WPA2 - Enterprise: Choose one of these options for stronger security. WPA2-Enterprise provides more robust security with centralized authentication, which is ideal for a corporate environment.

Key or Passphrase:

If you select WPA2, enter a strong passphrase in the "Key or Passphrase" field.

If you select WPA2 - Enterprise, you will need to configure additional settings for authentication servers, such as RADIUS, which is not shown in the exhibit.

Wireless Mode and Channel:

Set the appropriate mode and channel based on your network design and the environment to avoid interference. These settings are not specified in the exhibit, so set them according to your network plan.

Wired Speed and Duplex:

Set the speed to "Auto" unless you have specific requirements for 100 or 1000 Mbps.

Set the duplex to "Auto" unless you need to specify half or full duplex based on your network equipment.

Save Configuration:

After making the necessary changes, click the "Save" button to apply the settings.

Here is how the configuration should look after adjustments:

SSID: CORP

Security Settings: WPA2 or WPA2 - Enterprise

Key or Passphrase: [Enter a strong passphrase]

Mode: [Set based on your network plan]

Channel: [Set based on your network plan]

Speed: Auto

Duplex: Auto

Once these settings are configured, your wireless range extender will provide secure connectivity for devices in both buildings.

Firewall setting to to ensure complete compliance with the requirements and best security practices, consider the following adjustments and additions:

DNS Rule: This rule allows DNS traffic from the internal network to any destination, which is fine. HTTPS Outbound: This rule allows HTTPS traffic from the internal network (assuming 192.169.0.1/24 is a typo and should be 192.168.0.1/24) to any destination, which is also good for secure web browsing.

Management: This rule allows SSH access to the firewall for management purposes, which is necessary for administrative tasks.

HTTPS Inbound: This rule denies inbound HTTPS traffic to the internal network, which is good unless you have a web server that needs to be accessible from the internet.

HTTP Inbound: This rule denies inbound HTTP traffic to the internal network, which is correct for security purposes.

Suggested Additional Settings:

Permit General Outbound Traffic: Allow general outbound traffic for web access, email, etc.

Block All Other Traffic: Ensure that all other traffic is blocked to prevent unauthorized access.

Firewall Configuration Adjustments:

Correct the Network Typo:

Ensure that the subnet 192.169.0.1/24 is corrected to 192.168.0.1/24.

Permit General Outbound Traffic:

Rule Name: General Outbound

Source: 192.168.0.1/24

Destination: ANY

Service: ANY
Action: PERMIT
Deny All Other Traffic:
Rule Name: Block All
Source: ANY
Destination: ANY
Service: ANY
Action: DENY
Here is how your updated firewall settings should look:

Rule Name	Source	Destination	Service	Action
DNS Rule	192.168.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	192.168.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	192.168.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	192.168.0.1/24	HTTPS	DENY
HTTP Inbound	ANY	192.168.0.1/24	HTTP	DENY
General Outbound	192.168.0.1/24	ANY	ANY	PERMIT
Block All	ANY	ANY	ANY	DENY

These settings ensure that:
Internal devices can access DNS and HTTPS services externally.

Management access via SSH is permitted.
Inbound HTTP and HTTPS traffic is denied unless otherwise specified.
General outbound traffic is allowed.
All other traffic is blocked by default, ensuring a secure environment.
Make sure to save the settings after making these adjustments.

Question: 236

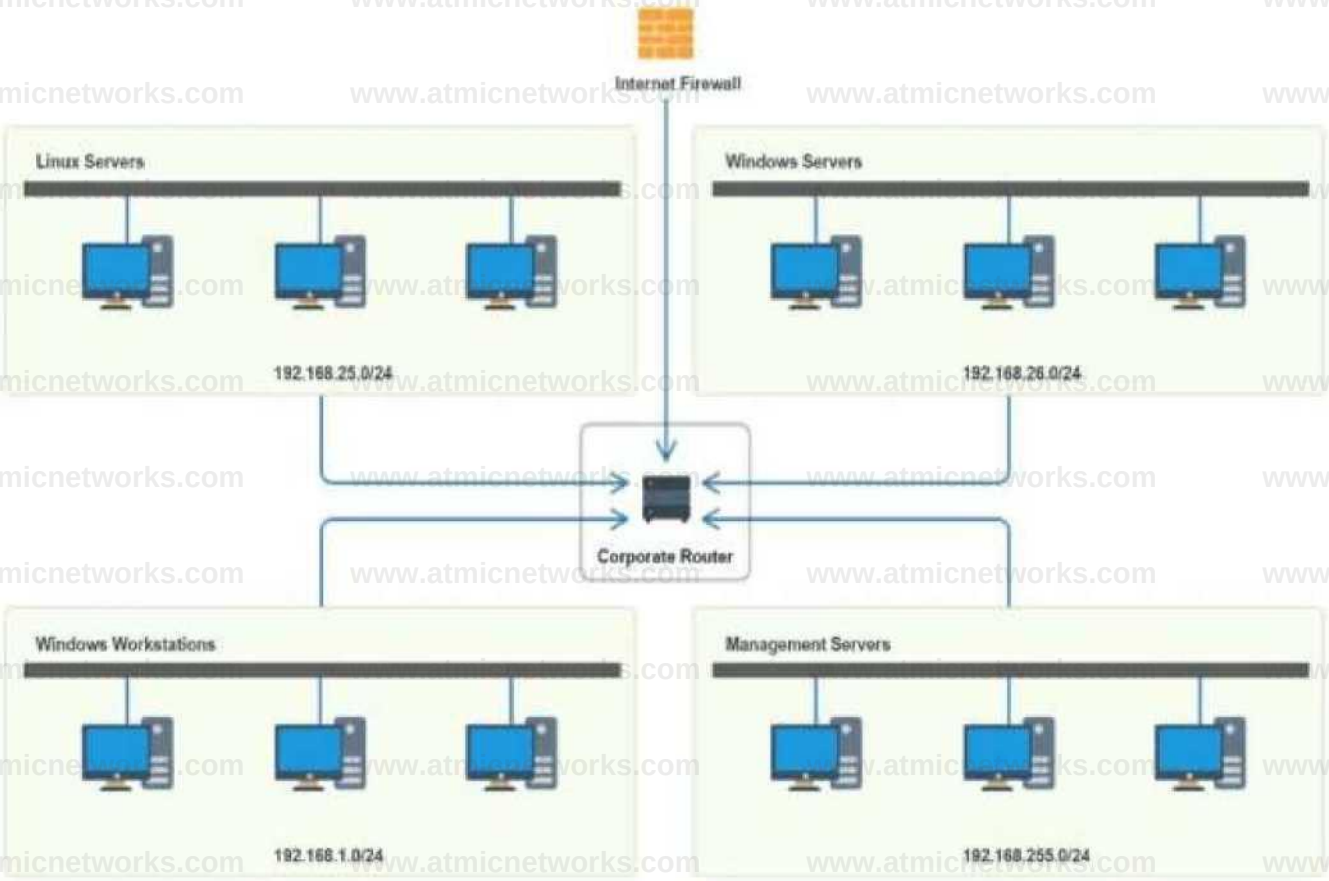
SIMULATION

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.



Answer: See the answer and solution below.

Explanation:

Router Access Control List X'

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	1921681 0	Any	TCP	VNC	Deny
8	192 168 1 0	Any	Any	Any	Allow
9	Any	Any	Any	Any	Deny

A screenshot of a computer screen AI-generated content may be incorrect.

Question: 237

Which of the following is a major difference between an IPS and IDS?

A. An IPS needs to be installed in line with traffic and an IDS does not.
B. An IPS is signature-based and an IDS is not.
C. An IPS is less susceptible to false positives than an IDS.
D. An IPS requires less administrative overhead than an IDS.

Answer: A

Explanation:

The key difference is that an Intrusion Prevention System (IPS) is installed in line with network traffic, allowing it to actively block threats. In contrast, an Intrusion Detection System (IDS) only monitors and alerts without actively blocking traffic.

Breakdown of Options:

A . An IPS needs to be installed in line with traffic and an IDS does not. Q Correct answer. IPS actively prevents threats, while IDS only detects them.

B . An IPS is signature-based and an IDS is not. – False, both can use signature-based detection.

C . An IPS is less susceptible to false positives than an IDS. – False, both can produce false positives, depending on configurations.

D . An IPS requires less administrative overhead than an IDS. – False, IPS requires more administrative effort due to

real-time blocking decisions.

Reference:

CompTIA Network+ (N10-009) Official Study Guide – Domain 3.4: Explain network security devices.

Question: 238

Which of the following is the most likely reason an insurance brokerage would enforce VPN usage?

A. To encrypt sensitive data in transit
B. To secure the endpoint
C. To maintain contractual agreements
D. To comply with data retentin requirements

Answer: A

Explanation:

The most likely reason an insurance brokerage would enforce VPN usage is to encrypt sensitive data in transit. VPNs (Virtual Private Networks) create a secure tunnel between the user's device and the corporate network, ensuring that data is encrypted and protected from interception.

Encryption: VPNs encrypt data, preventing unauthorized access and ensuring data privacy during transmission over public or unsecured networks.

Data Protection: Essential for industries handling sensitive information, such as insurance brokerages, to protect customer data and comply with regulatory requirements.

Security: Enhances overall network security by providing secure remote access for employees. Network Reference:

CompTIA Network+ N10-007 Official Certification Guide: Discusses the role of VPNs in securing data in transit.

Cisco Networking Academy: Provides training on VPN technologies and their importance in data security.

Network+ Certification All-in-One Exam Guide: Explains VPN usage and its benefits in protecting sensitive information.

Question: 239

Which of the following connector types would most likely be used to connect to an external antenna?

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

Answer: A

Explanation:

BNC connectors are commonly used for coaxial cables, including those connecting to external antennas in Wi-Fi, radio, and surveillance systems.

Breakdown of Options:

A . BNC – Correct answer. Used for coaxial cables in wireless and antenna connections.
B . ST – Used for fiber optic cables, not antennas.
C . LC – A fiber optic connector, not for antennas.
D . MPO – Used for multi-fiber optic cables, not RF antennas.

Reference:
CompTIA Network+ (N10-009) Official Study Guide – Domain 1.1: Compare and contrast physical network connectors.
IEEE 802.11: Wireless standards and antenna connectors

Question: 240

A network administrator needs to add 255 useable IP addresses to the network. A /24 is currently in use. Which of the following prefixes would fulfill this need?

A. /23
B. /25
C. /29
D. /32

Answer: A

Explanation:

A /23 subnet provides 512 total addresses, of which 510 are usable (subtracting 2 for network and broadcast addresses). This would satisfy the need for 255 additional addresses.

Question: 241

A network administrator has been monitoring the company's servers to ensure that they are available. Which of the following should the administrator use for this task?

A. Packet capture
B. Data usage reports
C. SNMP traps
D. Configuration monitoring

Answer: C

Explanation:

To monitor server availability, SNMP traps are the best choice. SNMP (Simple Network Management Protocol) allows devices to send alerts (traps) when certain conditions are met, such as server downtime or high resource usage.
Breakdown of Options:
A . Packet capture – Capturing packets provides insights into network traffic but does not actively monitor server availability.

B . Data usage reports – These analyze network traffic consumption but do not indicate whether a server is available or not.

C . SNMP traps – Correct answer. SNMP traps notify administrators of server issues in real time.

D . Configuration monitoring – This tracks configuration changes rather than availability.

Reference:

CompTIA Network+ (N10-009) Official Study Guide – Domain 2.3: Explain network monitoring concepts.

RFC 1157: Simple Network Management Protocol (SNMP)

Question: 242

A user is unable to navigate to a website because the provided URL is not resolving to the correct IP address. Other users are able to navigate to the intended website without issue. Which of the following is most likely causing this issue?

A. Hosts file
B. Self-signed certificate
C. Nameserver record
D. IP helperANS

Answer: A

Explanation:

Role of the Hosts File:

The hosts file is a local file on a computer that maps hostnames to IP addresses. It can be used to override DNS resolution by providing a static mapping of a hostname to an IP address.

Common Issues with the Hosts File:

If an incorrect IP address is mapped to a hostname in the hosts file, it can cause the computer to resolve the hostname to the wrong IP address. This can lead to navigation issues for specific websites while other users, relying on DNS, do not face the same problem.

Why Other Options are Less Likely:

Self-signed certificate: Relates to SSL/TLS and would cause a security warning, not a navigation failure.

Nameserver record: Affects all users, not just one.

IP helper: Used to forward DHCP requests and is unrelated to DNS resolution issues.

Troubleshooting Steps:

Check the hosts file on the affected user's computer (C:\Windows\System32\drivers\etc\hosts on Windows or /etc/hosts on Unix/Linux).

Look for entries that map the problematic hostname to an incorrect IP address and correct or remove them.

Reference:

CompTIA Network+ study materials and system administration documentation.

Question: 243

A network administrator needs to fail over services to an off-site environment. This process will take four weeks to become fully operational. Which of the following DR (Disaster Recovery) concepts does this describe?

A. Hot site
B. Warm site
C. Cold site
D. Active-active approach

Answer: C

Explanation:

A cold site is a backup facility that provides infrastructure (such as power, cooling, and space) but does not have active IT resources installed. When a disaster occurs, IT teams must bring in and configure all necessary hardware and software before services can resume. This process can take weeks or longer—which matches the scenario described.

- Why not the other options?
- Hot site (A) – A hot site is a fully operational backup facility with up-to-date data and pre-configured hardware, allowing almost instant failover (minutes to hours).
- Warm site (B) – A warm site has pre-installed hardware and some software/configurations, but it requires some setup before becoming fully operational (hours to a few days).
- Active-active approach (D) – This means that multiple sites run simultaneously with load balancing, ensuring no downtime in case of a failure.

Reference:
CompTIA Network+ (N10-009) Official Guide – Chapter 15: Business Continuity and Disaster Recovery

Question: 244

A systems administrator is investigating why users cannot reach a Linux web server with a browser but can ping the server IP. The server is online, the web server process is running, and the link to the switch is up. Which of the following commands should the administrator run on the server first?

A. traceroute
B. netstat
C. tcpdump
D. arp

Answer: B

Explanation:

The netstat command provides information about network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. Running netstat on the server can help the administrator verify that the web server process is listening on the expected port (e.g., port 80 for HTTP or port 443 for HTTPS) and that there are no issues with network connections. This is a crucial first step in diagnosing why the web server is not accessible via a browser.Reference: CompTIA Network+ study materials.

Question: 245

An IT manager needs to connect ten sites in a mesh network. Each needs to be secured with reduced provisioning time.

Which of the following technologies will best meet this requirement?

A. SD-WAN
B. VXLAN
C. VPN
D. NFV

Answer: A

Explanation:

Definition of SD-WAN:
Software-Defined Wide Area Network (SD-WAN) is a technology that simplifies the management and operation of a WAN by decoupling the networking hardware from its control mechanism. It allows for centralized management and enhanced security.
Benefits of SD-WAN:
Reduced Provisioning Time: SD-WAN enables quick and easy deployment of new sites with centralized control and automation.
Security: Incorporates advanced security features such as encryption, secure tunneling, and integrated firewalls.
Scalability: Easily scales to accommodate additional sites and bandwidth requirements.
Comparison with Other Technologies:
VXLAN (Virtual Extensible LAN): Primarily used for network virtualization within data centers.
VPN (Virtual Private Network): Provides secure connections but does not offer the centralized management and provisioning efficiency of SD-WAN.
NFV (Network Functions Virtualization): Virtualizes network services but does not specifically address WAN management and provisioning.
Implementation:
SD-WAN solutions are implemented by deploying edge devices at each site and connecting them to a central controller. This allows for dynamic routing, traffic management, and security policy enforcement.
Reference:
CompTIA Network+ course materials and networking solution guides.

Question: 246

Which of the following is the part of a disaster recovery (DR) plan that identifies the critical systems that should be recovered first after an incident?

A. RTO
B. SLA
C. MTBF
D. SIEM

Answer: A

Explanation:

RTO stands for Recovery Time Objective, which defines the maximum acceptable amount of time that a system, application, or function can be down after a failure or disaster. It helps prioritize which systems need to be recovered first based on their importance to business operations.
SLA (Service Level Agreement) refers to an agreement between a service provider and a customer regarding expected performance and availability, but it does not dictate recovery order.
MTBF (Mean Time Between Failures) is a measure of reliability and time between hardware or system failures.
SIEM (Security Information and Event Management) is a centralized tool for logging and alerting but not relevant to DR recovery prioritization.
Reference:
CompTIA Network+ N10-009 Official Objectives: 4.4 – Summarize business continuity and disaster recovery concepts.

Question: 247

An employee in a corporate office clicks on a link in an email that was forwarded to them. The employee is redirected to a splash page that says the page is restricted. Which of the following security solutions is most likely in place?

A. DLP
B. Captive portal
C. Content filtering
D. DNS sinkholing

Answer: C

Explanation:

Content filtering blocks access to restricted or malicious websites. When a user attempts to visit a site that violates company policies, they are redirected to a restriction page.

This is a common security measure to prevent employees from accessing phishing or malware- infected sites.
Content filters work by scanning URLs, keywords, or categories and blocking inappropriate or harmful content.
Option A (DLP - Data Loss Prevention): Focuses on preventing sensitive data leaks rather than blocking web access.
Option B (Captive portal): Used mainly in public Wi-Fi to authenticate users before granting access, not to restrict sites.
Option D (DNS sinkholing): Redirects malicious domain requests to a safe address but is not responsible for policy-based restrictions on general content.
? Reference: CompTIA Network+ (N10-009) Official Study Guide – Section: Security Solutions

Question: 248

While troubleshooting connectivity issues, a junior network administrator is given explicit instructions to test the host's TCP/IP stack first. Which of the following commands should the network administrator run?

A. ping 127.0.0.1
B. ping 169.254.1.1
C. ping 172.16.1.1

D. ping 192.168.1.1

Answer: A

Explanation:

The loopback address (127.0.0.1) is used to test a host's local TCP/IP stack, ensuring that the networking components of the operating system are functioning properly.

This test does not require network connectivity because it only checks if the local machine's TCP/IP stack is operational.

If the loopback test fails, it indicates a misconfigured TCP/IP stack, corrupt drivers, or an issue with the OS networking components.

Option B (ping 169.254.1.1) – This is an APIPA (Automatic Private IP Addressing) address, which is assigned when DHCP fails. It does not test the local TCP/IP stack.

Option C (ping 172.16.1.1) and Option D (ping 192.168.1.1) – These are private network addresses and test connectivity to other devices, not the local TCP/IP stack.

? Reference: CompTIA Network+ (N10-009) Official Study Guide – Section: Troubleshooting Network Connectivity

Question: 249

After a networking intern plugged in a switch, a significant number of users in a building lost connectivity. Which of the following is the most likely root cause?

A. VTP update
B. Port security issue
C. LLDP misconfiguration
D. Native VLAN mismatch

Answer: D

Explanation:

When a switch is improperly connected to a network, it can cause widespread connectivity issues, especially if there's a misconfiguration in VLAN settings. A Native VLAN mismatch occurs when two switches connected via a trunk link have different native VLANs configured for untagged traffic. This can cause traffic to be sent to the wrong VLAN or dropped, resulting in connectivity loss for users. Scenario Analysis: The intern likely connected the switch without ensuring that the trunk port's native VLAN matched the existing network configuration. This is a common issue in Cisco-based networks when trunk links are misconfigured.

Why not VTP update? VLAN Trunking Protocol (VTP) updates propagate VLAN configurations across switches. While a VTP misconfiguration could cause issues, it's less likely to immediately disrupt connectivity for many users unless the VTP server deleted critical VLANs, which is not implied here. Why not Port security issue? Port security restricts access based on MAC addresses, typically affecting individual ports, not causing widespread outages.

Why not LLDP misconfiguration? Link Layer Discovery Protocol (LLDP) is used for device discovery, and misconfiguration is unlikely to cause a broad loss of connectivity.

Reference:CompTIA Network+ N10-009 Objective 2.2: Explain the purpose of network segmentation and VLAN

configuration. The CompTIA Network+ Study Guide (e.g., Chapter 6: Switching) discusses VLAN trunking and the importance of matching native VLANs on trunk links to prevent connectivity issues. Native VLAN mismatches are highlighted as a common cause of network disruptions.

Question: 250

A network administrator needs to change where the outside DNS records are hosted. Which of the following records should the administrator change the registrar to accomplish this task?

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

Answer: A

Explanation:

To change where the outside DNS records are hosted, the network administrator needs to update the NS (Name Server) records at the domain registrar. NS records specify the authoritative name servers for a domain, directing where DNS queries should be sent.

NS (Name Server) Records: These records indicate the servers that are authoritative for a domain.

Changing the NS records at the registrar points DNS resolution to the new hosting provider.

SOA (Start of Authority): Contains administrative information about the domain, including the primary name server.

PTR (Pointer) Records: Used for reverse DNS lookups, mapping IP addresses to domain names. CNAME (Canonical Name) Records: Used to alias one domain name to another, not relevant for changing DNS hosting.

Network Reference:

CompTIA Network+ N10-007 Official Certification Guide: Discusses DNS records, their purposes, and how to manage them.

Cisco Networking Academy: Provides training on DNS management and the role of different DNS record types.

Network+ Certification All-in-One Exam Guide: Explains DNS records and their configuration for domain management.

Question: 251

A network technician is troubleshooting a web application's poor performance. The office has two internet links that share the traffic load. Which of the following tools should the technician use to determine which link is being used for the web application?

A. netstat
B. nslookup
C. ping
D. tracert

Answer: D

Explanation:

Understanding Tracert:

Traceroute Tool: tracert (Windows) or traceroute (Linux) is a network diagnostic tool used to trace the path that packets take from a source to a destination. It lists all the intermediate routers the packets traverse.

Determining Traffic Path:

Path Identification: By running tracert to the web application's destination IP address, the technician can identify which route the traffic is taking and thereby determine which internet link is being used. Load Balancing Insight: If the office uses load balancing for its internet links, tracert can help verify which link is currently handling the traffic for the web application.

Comparison with Other Tools:

netstat: Displays network connections, routing tables, interface statistics, and more, but does not trace the path of packets.

nslookup: Used for querying DNS to obtain domain name or IP address mapping, not for tracing packet routes.

ping: Tests connectivity and measures round-trip time but does not provide path information.

Implementation:

Open a command prompt or terminal.

Execute tracert [destination IP] to trace the route.

Analyze the output to determine the path and the link being used.

Reference:

CompTIA Network+ study materials on network troubleshooting and diagnostic tools.

Question: 252

Three access points have Ethernet that runs through the ceiling. One of the access points cannot reach the internet.

Which of the following tools can help identify the issue?

A. Network tap
B. Cable tester
C. Visual fault locator
D. Toner and probe

Answer: B

Explanation:

A cable tester is a tool that can help identify issues with the physical cabling, such as breaks or improper terminations, which may prevent the access point from reaching the internet.

Question: 253

A network engineer configures the network settings in a new server as follows:

IP address = 192.163.1.15

Subnet mask = 255.255.255.0

Gateway = 192.163.1.255

The server can reach other hosts on the same subnet successfully, but it cannot reach hosts on different subnets. Which of the following is most likely configured incorrectly?

A. Subnet mask
B. Gateway
C. Default route
D. IP address

Answer: B

Explanation:

The default gateway for a network should be an IP address within the subnet, but not the broadcast address. In this case:

IP: 192.163.1.15

Subnet Mask: 255.255.255.0

This means the network range is: 192.163.1.0 - 192.163.1.255

192.163.1.255 is the broadcast address for this subnet, so it cannot be used as a gateway.

Hence, the device fails to communicate outside its subnet because it's trying to use a broadcast address as its gateway.

Q The issue is clearly with the gateway configuration.

Reference:CompTIA Network+ N10-009 Official Study Guide — Objective 1.4: "Given a scenario, configure and deploy common Ethernet switching features."

Question: 254

An organization has four departments that each need access to different resources that do not overlap. Which of the following should a technician configure in order to implement and assign an ACL?

A. VLAN
B. DHCP
C. VPN
D. STP

Answer: A

Explanation:

VLANs (Virtual Local Area Networks) segment network traffic by department, allowing ACLs (Access Control Lists) to be applied based on VLAN membership, improving security and resource isolation. Breakdown of Options:

A . VLAN – Correct answer. VLANs enable logical network segmentation, allowing ACLs per department.

B . DHCP – Assigns IP addresses but does not control access.

C . VPN – Provides remote access, not segmentation within a network.

D . STP – Prevents switching loops, not related to ACL implementation.

Reference:

CompTIA Network+ (N10-009) Official Study Guide – Domain 1.3: Explain VLANs and network segmentation.

IEEE 802.1Q: VLAN tagging standard

Question: 255

A firewall administrator is mapping a server's internal IP address to an external IP address for public use. Which of the following is the name of this function?

A. NAT
B. VIP
C. PAT
D. BGP

Answer: A

Explanation:

Network Address Translation (NAT) is a process that allows a device, typically a firewall or router, to map private IP addresses to public IP addresses. This enables internal network devices to communicate over the internet using a single or a limited number of public IP addresses.

Static NAT (One-to-One Mapping): Maps a single private IP address to a single public IP address, commonly used for servers that need to be accessible from the internet.

Dynamic NAT (Many-to-Many Mapping): Dynamically assigns a public IP from a pool to internal devices.

PAT (Port Address Translation): A type of NAT where multiple private IPs share a single public IP using different port numbers.

Incorrect Options:

B . VIP (Virtual IP Address): Used in load balancing and high-availability configurations, not for NAT.

C . PAT (Port Address Translation): A specific form of NAT, but the question refers to general NAT, making option A the best choice.

D . BGP (Border Gateway Protocol): A routing protocol used to exchange information between different networks, not related to NAT.

Reference:

CompTIA Network+ N10-009 Official Study Guide – Chapter on Network Address Translation (NAT)

Question: 256

Before using a guest network, an administrator requires users to accept the terms of use Which of the following is the best way to accomplish this goal?

A. Pre-shared key
B. Autonomous access point
C. Captive portal
D. WPA2 encryption

Answer: C

Explanation:

A captive portal is a web page that users must view and interact with before being granted access to a network. It is commonly used in guest networks to enforce terms of use agreements. When a user connects to the network, they are redirected to this portal where they must accept the terms of use before proceeding. This method ensures that users are aware of and agree to the network's policies, making it the best choice for this scenario. Reference: CompTIA Network+ Exam Objectives and official study guides.

Question: 257

Which of the following steps of the troubleshooting methodology should a technician take to confirm a theory?

A. Duplicate the problem.
B. Identify the symptoms.
C. Gather information.
D. Determine any changes.

Answer: A

Explanation:

Troubleshooting Methodology:
Troubleshooting involves a systematic approach to diagnosing and resolving issues. It typically includes steps such as identifying symptoms, gathering information, formulating and testing theories, and implementing solutions.
Confirming a Theory:
Duplicate the Problem: To confirm a theory, the technician should reproduce the problem in a controlled environment. This helps verify that the identified cause actually leads to the observed issue.
Verification: By duplicating the problem, the technician can observe the issue firsthand, validate the hypothesis, and rule out other potential causes.
Comparison with Other Steps:
Identify the Symptoms: Initial step to understand what the problem is, not specifically for confirming a theory.
Gather Information: Involves collecting data and details about the issue, usually done before formulating a theory.
Determine Any Changes: Involves checking for recent changes that could have caused the issue, a part of the information-gathering phase.
Implementation:
Use similar equipment or software in a test environment to recreate the issue.
Observe the results to see if they match the original problem, thereby confirming the theory. Reference:
CompTIA Network+ study materials on troubleshooting methodologies and best practices.

Question: 258

A network architect is implementing an off-premises computing facility and needs to ensure that operations will not be impacted by major outages. Which of the following should the architect consider?

A. Hot site
B. DCI
C. Direct Connect
D. Active-passive approach

Answer: A

Explanation:

A hot site is a fully operational backup facility with hardware, network, and data synchronization already in place. It allows for immediate failover in the event of a disaster, minimizing downtime. B . DCI (Data Center Interconnect) connects data centers but doesn't guarantee availability unless built redundantly.

C . Direct Connect refers to a private link to cloud providers, not disaster recovery.

D . Active-passive can help with failover but may involve delay unless combined with hot site principles.

Reference:

CompTIA Network+ N10-009 Official Objectives: 4.4 – Summarize business continuity and disaster recovery concepts.

Question: 259

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:

Power over Ethernet (PoE) allows devices such as cameras, access points, and VoIP phones to receive both power and data over the same Ethernet cable. If only eight out of twelve cameras turn on, the most likely issue is that the PoE switch has exceeded its power budget (total wattage capacity).

PoE Budget Limitation: PoE switches have a maximum power output, which can limit the number of devices they support simultaneously.

Voltage Check: Different PoE standards exist:

802.3af (PoE): Supplies up to 15.4W per port

802.3at (PoE+): Supplies up to 30W per port

802.3bt (PoE++): Supplies up to 60-100W per port

Power Draw Calculation: If each camera requires 15W and the switch can only provide 120W, then only 8 cameras (8 × 15W = 120W) will turn on.

Incorrect Options:

A . Ethernet Cable Type: Most PoE devices work with Cat5e and above. Cable type could be an issue, but power limitation is the more immediate concern.

C . Transceiver Compatibility: Only relevant if fiber transceivers or modules are in use, but not likely the root cause for power-related issues.

D . DHCP Addressing: DHCP issues affect network connectivity, not power delivery.

Reference:

CompTIA Network+ N10-009 Official Study Guide – Chapter on Power over Ethernet (PoE)

Question: 260

Which of the following is the most secure way to provide site-to-site connectivity?

A. VXLAN
B. IKE
C. GRE
D. IPsec

Answer: D

Explanation:

IPsec (Internet Protocol Security) is the most secure way to provide site-to-site connectivity. It provides robust security services, such as data integrity, authentication, and encryption, ensuringthat data sent across the network is protected from interception and tampering. Unlike other options, IPsec operates at the network layer and can secure all traffic that crosses the IP network, making it the most comprehensive and secure choice for site-to-site VPNs.Reference: CompTIA Network+ study materials and NIST Special Publication 800-77.

Question: 261

A network engineer receives a vendor alert regarding a vulnerability in a router CPU. Which of the following should the engineer do to resolve the issue?

A. Update the firmware.
B. Replace the system board.
C. Patch the OS.
D. Isolate the system.

Answer: A

Explanation:

Understanding the Vulnerability:

Vulnerabilities in the router CPU can be exploited to cause performance degradation, unauthorized access, or other security issues.

Firmware Update:

Firmware Role: The firmware is low-level software that controls the hardware of a device. Updating the firmware can address vulnerabilities by providing patches and enhancements from the manufacturer.

Procedure: Download the latest firmware from the vendor’s website, follow the manufacturer's

instructions to apply the update, and verify that the update resolves the vulnerability.

Comparison with Other Options:

Replace the System Board: This is a costly and often unnecessary step if the issue can be resolved with a firmware update.

Patch the OS: Patching the OS is relevant for devices with a full operating system but not directly applicable to addressing a CPU vulnerability on a router.

Isolate the System: Temporarily isolating the system can mitigate immediate risk but does not resolve the underlying vulnerability.

Best Practice:

Regularly check for and apply firmware updates to ensure that network devices are protected against known vulnerabilities.

Reference:

CompTIA Network+ study materials on network security and device management.

Question: 262

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

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

Answer: D

Explanation:

Multimode fiber optic cables involve the transmission of light signals that bounce off the core's cladding as they travel down the fiber. This characteristic differentiates it from single-mode fiber, where the light travels directly down the fiber without reflecting off the cladding.

Here are some detailed points about multimode fiber cables:

Construction: Multimode fibers have a larger core diameter, typically 50 or 62.5 microns, compared to single-mode fibers, which have a core diameter of about 9 microns.

Light Propagation: The larger core of multimode fiber allows multiple light modes to propagate. These modes travel at different angles, leading to reflections off the core-cladding boundary. Distance and Bandwidth: Due to modal dispersion, where different light modes arrive at the receiver at different times, multimode fibers are suited for shorter distance applications compared to singlemode fibers. Typical distances are up to 550 meters for 10 Gbps Ethernet using OM4 multimode fiber. Applications: Multimode fibers are commonly used in LANs (Local Area Networks), data centers, and for shorter distance data transmission due to their cost-effectiveness and ease of installation.

Network Reference:

CompTIA Network+ N10-007 Official Certification Guide, which covers fiber optic technologies, including the differences between multimode and single-mode fibers.

Cisco Networking Academy: Provides training materials and reference guides on the properties of different fiber optic cables.

Fiber Optic Association (FOA): A professional society dedicated to fiber optics, offering extensive information and certification on fiber optic technologies.

Multimode fibers are specifically designed for short-range communication with higher data rates and are typically used in environments like data centers, where high bandwidth over shorter distances is crucial. The reflections off the cladding, inherent to multimode fiber, facilitate this high-capacity communication.

Question: 263

Which of the following IP transmission types encrypts all of the transmitted data?

A. ESP
B. AH
C. GRE
D. UDP
E. TCP

Answer: A

Explanation:

Definition of ESP (Encapsulating Security Payload):
ESP is a part of the IPsec protocol suite used to provide confidentiality, integrity, and authenticity of data. ESP encrypts the payload and optional ESP trailer, providing data confidentiality.
ESP Functionality:
ESP can encrypt the entire IP packet, ensuring that the data within the packet is secure from interception or eavesdropping. It also provides options for data integrity and authentication.
ESP operates in two modes: transport mode (encrypts only the payload of the IP packet) and tunnel mode (encrypts the entire IP packet).
Comparison with Other Protocols:
AH (Authentication Header): Provides data integrity and authentication but does not encrypt the payload.
GRE (Generic Routing Encapsulation): A tunneling protocol that does not provide encryption.
UDP (User Datagram Protocol) and TCP (Transmission Control Protocol): These are transport layer protocols that do not inherently provide encryption. Encryption must be provided by additional protocols like TLS/SSL.
Use Cases:
ESP is widely used in VPNs (Virtual Private Networks) to ensure secure communication over untrusted networks like the internet.
Reference:
CompTIA Network+ study materials on IPsec and encryption.

Question: 264

A network administrator wants to increase network security by preventing client devices from communicating directly with each other on the same subnet. Which of the following technologies should be implemented?

A. ACL
B. Trunking
C. Port security
D. Private VLAN

Answer: D

Explanation:

Private VLANs (PVLANs) are used to segment devices on the same subnet and switch so they cannot communicate with each other, while still accessing a shared resource like a router or gateway. This is often used in shared hosting or DMZ environments.

A . ACLs (Access Control Lists) control traffic between networks, not within the same VLAN.

B . Trunking carries multiple VLANs between switches but does not isolate devices.

C . Port security limits MAC addresses per port but doesn't isolate communication between ports.

Reference:

CompTIA Network+ N10-009 Official Objectives: 3.4 – Compare and contrast access control methods.

Question: 265

A network administrator for a small office is adding a passive IDS to its network switch for the purpose of inspecting network traffic. Which of the following should the administrator use?

A. SNMP trap
B. Port mirroring
C. Syslog collection
D. API integration

Answer: B

Explanation:

Port mirroring, also known as SPAN (Switched Port Analyzer), is used to send a copy of network packets seen on one switch port (or an entire VLAN) to another port where the IDS is connected. This allows the IDS to passively inspect network traffic without interfering with the actual traffic flow. Port mirroring is an essential feature for implementing IDS in a network for traffic analysis and security monitoring.Reference: CompTIA Network+ study materials.

Question: 266

A network administrator wants users to be able to authenticate to the corporate network using a port-based authentication framework when accessing both wired and wireless devices. Which of the following is the best security feature to accomplish this task?

A. 802.1X
B. Access control list
C. Port security
D. MAC filtering

Answer: A

Explanation:

802.1X is a port-based network access control (PNAC) protocol that provides an authentication mechanism to devices wishing to connect to a LAN or WLAN. It is widely used for secure network access, ensuring that only authenticated devices can access the network, whether they are connecting via wired or wireless means. 802.1X works in conjunction with an authentication server, such as RADIUS, to validate the credentials of devices trying to connect.Reference: CompTIA Network+ study materials.

Question: 267

A network administrator is planning to host a company application in the cloud, making the application available for all internal and third-party users. Which of the following concepts describes this arrangement?

A. Multitenancy
B. VPC
C. NFV
D. SaaS

Answer: A

Explanation:

Multitenancy is a cloud computing architecture where a single instance of software serves multiple customers or tenants. Each tenant's data is isolated and remains invisible to other tenants. Hosting a company application in the cloud to be available for both internal and third-party users fits this concept, as it allows shared resources and infrastructure while maintaining data separation and security. Reference: CompTIA Network+ Exam Objectives and official study guides.

Question: 268

Which of the following troubleshooting steps would provide a change advisory board with the information needed to make a decision?

A. Identify the problem.
B. Develop a theory of probable cause.
C. Test the theory to determine cause.
D. Establish a plan of action.

Answer: D

Explanation:

A Change Advisory Board (CAB) reviews and approves network changes. Before approval, they need a detailed action plan outlining the change, potential impacts, and mitigation strategies.

A Plan of Action includes risk assessments, rollback procedures, and deployment steps, which are critical for decision-

making.
? Reference: CompTIA Network+ (N10-009) Official Study Guide – Section: Network Troubleshooting Methodologies

Question: 269

Which of the following is the most likely benefit of installing server equipment in a rack?

A. Simplified troubleshooting process
B. Decreased power consumption
C. Improved network performance
D. Increased compute density

Answer: D

Explanation:

Installing server equipment in a rack increases compute density by allowing multiple servers to be organized efficiently in a vertical configuration, saving space while housing more devices in a smaller footprint. This is critical for data centers and businesses with high hardware demands.
Simplified troubleshooting process (A): While racks can aid in organizing equipment, this is a secondary benefit, not the primary purpose.
Decreased power consumption (B): Rack installation does not directly reduce power usage; equipment power consumption remains the same.
Improved network performance (C): Racking servers does not inherently improve network performance; that depends on network configurations.
Reference: CompTIA Network+ Official Study Guide, Domain 1.3 (Rack Installations).

Question: 270

Which of the following is the best VPN to use for reducing data bandwidth requirements of the corporate network?

A. Split-tunnel
B. Site-to-site
C. Full-tunnel client
D. GRE tunnel

Answer: A

Explanation:

A split-tunnel VPN allows a device to route some traffic through the VPN (typically corporate traffic) while sending other traffic (like general internet browsing) directly over the local internet connection. This reduces the load on the corporate network because not all traffic is routed through the VPN tunnel.

Site-to-site VPNs are for permanent links between locations.

Full-tunnel VPNs route all traffic through the VPN, increasing the bandwidth usage on the corporate network.

GRE (Generic Routing Encapsulation) is a tunneling protocol that doesn't encrypt and doesn't reduce bandwidth usage by itself.

Reference:

CompTIA Network+ N10-009 Official Objectives: 3.3 – Given a scenario, configure and deploy common VPN technologies.

Question: 271

Which of the following is the most closely associated with segmenting compute resources within a single cloud account?

A. Network security group
B. laaS
C. VPC
D. Hybrid cloud

Answer: C

Explanation:

Reference: CompTIA Network+ Certification Exam Objectives - Cloud Models section.

Question: 272

A company is expanding to another floor in the same building. The network engineer configures a new switch with the same VLANs as the existing stack. When the network engineer connects the new switch to the existing stack, all users lose connectivity. Which of the following is the MOST likely reason?

A. The new switch has unused ports disabled
B. The new switch does not have a default gateway
C. The new switch is connected to an access port
D. The new switch is in a spanning tree loop

Answer: D

Explanation:

This describes a Spanning Tree Protocol (STP) loop. If STP isn't correctly configured or a redundant link is added without STP protection, it causes broadcast storms and network outages.

A . Unused ports disabled would not affect the entire network.

B . Missing default gateway on a switch doesn't cause total network loss.

**C. Connecting a switch to an access port can cause VLAN mismatches, but not total connectivity loss unless a loop

forms.

Reference:

CompTIA Network+ N10-009 Official Objectives: 3.6 – Explain the characteristics of network topologies and types.

Question: 273

An organization wants better network visibility. The organization's requirements include:

Multivendor/OS-monitoring capabilities

Real-time collection

Data correlation

Which of the following meets these requirements?

A. SNMP
B. SIEM
C. Nmap
D. Syslog

Answer: B

Explanation:

A Security Information and Event Management (SIEM) system collects, correlates, and analyzes logs from multiple sources in real-time, providing enhanced visibility across multivendor environments. Breakdown of Options:

A . SNMP – SNMP is used for network device monitoring, but it lacks real-time correlation across multiple vendors.

B . SIEM – Correct answer. SIEM aggregates, analyzes, and correlates logs from multiple sources, providing real-time visibility.

C . Nmap – Nmap is a network scanning tool used for mapping hosts and detecting open ports but does not provide log correlation.

D . Syslog – Syslog collects logs but does not correlate or analyze them in real-time.

Reference:

CompTIA Network+ (N10-009) Official Study Guide – Domain 3.3: Explain network security concepts. NIST Special Publication 800-92: Guide to Computer Security Log Management

Question: 274

A secure communication link needs to be configured between data centers via the internet. The data centers are located in different regions. Which of the following is the best protocol for the network administrator to use?

A. DCI
B. GRE
C. VXLAN
D. IPSec

Answer: D

Explanation:

IPSec (Internet Protocol Security) is the best choice for secure communication over the internet, as it provides encryption, authentication, and data integrity. It is widely used in VPNs and site-to-site secure tunnels.

Breakdown of Options:

A . DCI (Data Center Interconnect) – A general term for linking data centers, but it doesn't specify a secure tunneling protocol.

B . GRE (Generic Routing Encapsulation) – Encapsulates traffic but lacks encryption, making it less secure than IPSec.

C . VXLAN (Virtual Extensible LAN) – Used for Layer 2 network overlays, not for securing communication over the internet.

D . IPSec – Q Correct answer. Provides encryption, authentication, and integrity for data over the internet.

Reference:

CompTIA Network+ (N10-009) Official Study Guide – Domain 3.5: Implement secure remote access methods.

RFC 4301: Security Architecture for the Internet Protocol

Question: 275

A technician is designing a cloud service solution that will accommodate the company's current size, compute capacity, and storage capacity. Which of the following cloud deployment models will fulfill these requirements?

A. SaaS
B. PaaS
C. IaaS
D. IaC

Answer: C

Explanation:

Infrastructure as a Service (IaaS) provides scalable compute power, storage, and networking resources on demand. It is the best choice for a company that needs to customize its cloud solution based on size, compute capacity, and storage needs.

IaaS Benefits:

Provides virtual machines, storage, and networking resources.

Scalable based on company needs.

Reduces the need for physical infrastructure.

Incorrect Options:

A . SaaS (Software as a Service): Delivers software applications (e.g., Google Docs, Microsoft 365) but does not provide compute/storage infrastructure.

B . PaaS (Platform as a Service): Provides a development environment for application deployment but not full infrastructure control.

D . IaC (Infrastructure as Code): A methodology for automating infrastructure, not a cloud deployment model.

Reference:

CompTIA Network+ N10-009 Official Study Guide – Chapter on Cloud Computing Models

Question: 276

A network administrator configured a router interface as 10.0.0.95 255.255.255.240. The administrator discovers that the router is not routing packets to a web server with IP 10.0.0.81/28.

Which of the following is the best explanation?

A. Theweb server Is In adifferent subnet.
B. Therouter interface isa broadcast address.
C. TheIP address spaceis a class A network.
D. Thesubnet is in a private address space.

Answer: B

Explanation:

Understanding Subnetting:

The subnet mask 255.255.255.240 (or /28) indicates that each subnet has 16 IP addresses (14 usable addresses, 1 network address, and 1 broadcast address).

Calculating the Subnet Range:

Subnet Calculation: For the IP address 10.0.0.95 with a /28 subnet mask:

Network address: 10.0.0.80

Usable IP range: 10.0.0.81 to 10.0.0.94

Broadcast address: 10.0.0.95

Router Interface Configuration:

Broadcast Address Issue: The IP address 10.0.0.95 is the broadcast address for the subnet 10.0.0.80/28. Configuring a router interface with the broadcast address will cause routing issues as it is not a valid host address.

Comparison with Other Options:

The web server is in a different subnet: The web server (10.0.0.81) is within the same subnet range (10.0.0.80/28).

The IP address space is a class A network: While 10.0.0.0 is a Class A network, this does not explain the routing issue caused by the broadcast address.

The subnet is in a private address space: The private address space designation (RFC 1918) does not impact the routing issue related to the broadcast address configuration.

Resolution:

Reconfigure the router interface with a valid host IP address within the usable range, such as 10.0.0.94.

Reference:

CompTIA Network+ study materials on subnetting and IP address configuration.

Question: 277

Which of the following can also provide a security feature when implemented?

A. NAT
B. BGP
C. FHRP
D. EIGRP

Answer: A

Explanation:

NAT (Network Address Translation) helps hide internal IP addresses from external networks, adding a layer of security by preventing direct access to internal systems from the outside.

Question: 278

A network administrator deploys several new desk phones and workstation cubicles. Each cubicle has one assigned switchport. The administrator runs the following commands:

```
nginx
CopyEdit
switchport mode access
switchport voice vlan 69
```

With which of the following VLANs will the workstation traffic be tagged?

A. Private VLAN
B. Voice VLAN
C. Native VLAN
D. Data VLAN

Answer: D

Explanation:

When the command switchport voice vlan 69 is used, it tags the voice traffic with VLAN 69, while the workstation traffic continues untagged on the access VLAN, which is typically considered thedata VLAN. This configuration enables both voice and data traffic over the same port while keeping them in separate VLANs for QoS and traffic management.

Reference:Section 2.2 – Switching Technologies and Features – "Switchport Voice VLAN Configuration"

Question: 279

A network administrator needs to connect a multimode fiber cable from the MDF to the server room. The administrator connects the cable to Switch 2, but there is no link light. The administrator tests the fiber and finds it does not have any issues. Swapping the connection to Switch 1 in a working port is successful, but the swapped connection does not work on Switch 2. Which of the following should the administrator verify next?

A. Fiber length
B. Transceiver model
C. Connector type
D. Port speed

Answer: B

Explanation:

The most probable issue is with thetransceiver model. Not all transceivers are compatible with multimode fiber, and the specific type (e.g., SFP, SFP+) and its wavelength must match the fiber cable type. If a port works on one switch but not the other with the same cable, this is a strong indicator of incompatible or faulty transceiver hardware.
Reference:Section 1.5 – Transmission Media and Transceivers – "Transceivers and Compatibility"

Question: 280

A network technician is installing a new switch that does not support STP at the access layer of a network. The technician wants a redundant connection to the distribution switch. Which of the following should the technician use?

A. Link aggregation
B. Subinterfaces
C. Switch virtual interfaces
D. Half-duplex connections

Answer: A

Explanation:

Link aggregation(also known as port channeling or EtherChannel) allows multiple physical connections to act as one logical connection. This avoids loops that would typically be prevented by STP and provides redundancy and increased bandwidth. It's ideal when STP is not available or desirable.
Reference:Section 2.2 – Switching Technologies and Features – "Link Aggregation"

Question: 281

Users are experiencing significant lag while connecting to a cloud-based application during peak hours. An examination of the network reveals that the bandwidth is being heavily utilized. Further analysis shows that only a few users are using the application at any given time. Which of the following is the most cost-effective solution for this issue?

A. Limit the number of users who can access the application.
B. Lease a Direct Connect connection to the cloud service provider.
C. Implement QoS to prioritize application traffic.
D. Use a CDN to service the application.

Answer: C

Explanation:

Quality of Service (QoS)is the best cost-effective solution. It prioritizes traffic based on application criticality. If the bandwidth is limited and only a few users are affected, prioritizing that application traffic can improve performance without needing costly bandwidth upgrades or direct connections. Reference:Section 1.2 – Networking Appliances, Applications, and Functions – "Quality of Service (QoS)"

Question: 282

Which of the following layers in the OSI model is responsible for establishing, maintaining, and terminating connections between nodes?

A. Physical
B. Network
C. Session
D. Transport

Answer: C

Explanation:

TheSession Layer(Layer 5 of the OSI Model) is responsible for setting up, managing, and tearing down sessions between applications. It maintains dialog control and synchronizes data exchange between systems.
Reference:Section 1.1 – OSI Reference Model Concepts – "Layer 5 – Session"

Question: 283

Which of the following is the best way to reduce the likelihood of electrostatic discharge?

A. Uninterruptible power supply
B. Surge protector
C. Power distribution units
D. Temperature and humidity control

Answer: D

Explanation:

Temperature and humidity controlis the best way to reduce the risk of electrostatic discharge (ESD). Dry environments significantly increase the likelihood of static buildup, which can discharge and damage sensitive components. By controlling humidity, the environment becomes less prone to static electricity.
Reference:Section 2.4 – Important Factors of Physical Installations – "Environmental Considerations"

Question: 284

Which of the following can be used when a server at a remote site is physically unreachable?

A. OOB management
B. Crash cart
C. Jump box
D. Console

Answer: A

Explanation:

Out-of-band (OOB) managementallows administrators to manage devices remotely even if the primary network is down. This is especially useful when physical access to the server is not possible. OOB management often uses a separate management interface, ensuring access regardless of the server's operational state.
Reference:Section 3.5 – Network Access and Management Methods – "OOB Management"

Question: 285

A network engineer is designing an internal network that needs to support both IPv4 and IPv6 routing. Which of the following routing protocols is capable of supporting both IPv4 and IPv6?

A. OSPFv3
B. RIPv2
C. BGP
D. EIGRP

Answer: D

Explanation:

EIGRP(Enhanced Interior Gateway Routing Protocol) supports bothIPv4 and IPv6. While OSPFv3 is specific to IPv6 and RIPv2 only supports IPv4, EIGRP was extended to handle dual-stack environments efficiently.
Reference:Section 2.1 – Characteristics of Routing Technologies – "EIGRP"

Question: 286

A network engineer is deploying switches at a new remote office. The switches have been preconfigured with hostnames and STP priority values. Based on the following table: Switch Name
Priority
core-sw01
24576

access-sw01
28672
distribution-sw01
32768
access-sw02
36864
Which of the following switches will become the root bridge?

A. core-sw01
B. access-sw01
C. distribution-sw01
D. access-sw02

Answer: A

Explanation:

The switch with the lowest STP priority becomes the root bridge.In the given table, core-sw01 has the lowest priority value of 24576. Therefore, it will be elected as the root bridge in the Spanning Tree Protocol topology.
Reference:Section 2.2 – Switching Technologies and Features – "Spanning Tree Protocol (STP)"

Question: 287

Which of the following is enforced through legislation?

A. AUP
B. GDPR
C. Code of conduct
D. EULA

Answer: B

Explanation:

GDPR (General Data Protection Regulation)is alegal frameworkenforced by the European Union to protect personal data and privacy. Unlike internal organizational policies such as AUPs or codes of conduct, GDPR is alegislated regulation, and organizations must comply or face legal consequences. Reference:Section 4.1 – Basic Network Security Concepts – "GDPR and Compliance Regulations"

Question: 288

A network administrator wants to restrict inbound traffic to allow only HTTPS to the company website, denying all other inbound traffic from the internet. Which of the following would best accomplish this goal?

A. ACL on the edge firewall
B. Port security on an access switch
C. Content filtering on a web gateway
D. URL filtering on an outbound proxy

Answer: A

Explanation:

AnAccess Control List (ACL)configured on theedge firewallis the correct and most effective solution tofilter inbound traffic. The administrator can allow TCP port 443 (HTTPS) and deny all other traffic. This is a classic firewall configuration for securing public-facing servers.

Reference:Section 4.3 – Network Security Features, Defense Techniques, and Solutions – "ACLs (Access Control Lists)"

Question: 289

Which of the following indicates a computer has reached end-of-support?

A. The computer does not have any users.
B. The antivirus protection is expired.
C. The operating system license is expired.
D. No more patches or bug fixes are available indefinitely.

Answer: D

Explanation:

A system has reachedend-of-supportwhen thevendor no longer provides patches, updates, or bug fixes. This significantly increases the risk of security vulnerabilities and is a major operational concern.

Reference:Section 3.3 – Disaster Recovery Concepts – "End-of-Support Considerations"

Question: 290

Which of the following source control features allows an administrator to test a new configuration without changing the primary configuration?

A. Central repository
B. Conflict identification
C. Branching
D. Version control

Answer: C

Explanation:

Branchingallows developers and administrators tocreate an isolated copyof the main configuration so they can test changes independently. This avoids impacting the primary environment and allows for safer testing and development.

Reference:Section 3.5 – Network Access and Management Methods – "Source Control: Branching"

Question: 291

A network engineer needs to add a boundary network to isolate and separate the internal network from the public-facing internet. Which of the following security defense solutions would best accomplish this task?

A. Trusted zones
B. URL filtering
C. ACLs
D. Screened subnet

Answer: D

Explanation:

Ascreened subnet, also known as aDMZ (Demilitarized Zone), is aboundary networkthat separates an organization's internal network from external-facing systems. It is used to host public services like web or email servers while protecting internal systems from exposure.

Reference:Section 4.3 – Network Security Features, Defense Techniques, and Solutions – "Screened Subnet (DMZ)"

Question: 292

Which of the following is the greatest advantage of maintaining a cold DR site compared to other DR sites?

A. Redundancy
B. Availability
C. Security
D. Cost

Answer: D

Explanation:

Acold disaster recovery (DR) siteis a backup facility equipped withminimal infrastructure, often lacking active systems or

real-time data replication. Itsgreatest advantage is cost-efficiency. Cold sites aremuch cheaperto maintain than warm or hot sites, which require continuous synchronization and operational readiness. They are used when low cost is more important than recovery speed. Reference:Section 3.3 – Disaster Recovery Concepts – "Cold, Warm, and Hot Sites Comparison"

Question: 293

Which of the following allows for interactive, secure remote management of a network infrastructure device?

A. SSH
B. VNC
C. RDP
D. SNMP

Answer: A

Explanation:

SSH (Secure Shell) is a cryptographic network protocol that enables secure remote management and operation of network devices, including routers and switches. SSH encrypts traffic, making it more secure than alternatives like Telnet, which sends data in plaintext. The document states: "SSH (Secure Shell) is the recommended protocol for secure, interactive remote management of network devices. It provides a secure channel over an unsecured network by encrypting the traffic between the administrator's workstation and the managed device."

Question: 294

A data center administrator is evaluating the use of jumbo frames within a storage environment.
Which of the following describes the best reason to use jumbo frames in the storage environment?

A. To reduce device overhead
B. To report on the current root switch in the STP
C. To improve routing convergence
D. To increase drive throughput

Answer: A

Explanation:

Jumbo frames are Ethernet frames with a payload greater than the standard 1,500 bytes. Using jumbo frames reduces the number of frames transmitted over the network, thereby reducing the overhead associated with frame headers and processing. The document explains:
"Jumbo frames are used in storage networks to reduce device overhead by lowering the number of frames required for data transfer, which can increase overall throughput and performance."

Question: 295

Which of the following should a company implement in order to share a single IP address among all the employees in the office?

A. STP
B. BGP
C. PAT
D. VXLAN

Answer: C

Explanation:

PAT (Port Address Translation) allows multiple devices on a local network to share a single public IP address when accessing the internet. It translates the private IP addresses to a single public IP with different port numbers for each session. The document states:
"PAT (Port Address Translation) allows multiple devices on a LAN to share a single public IP address by assigning unique port numbers to each session, enabling internet connectivity for all devices."

Question: 296

Which of the following OSI model layers can utilize a connectionless protocol for data transmission?

A. Physical
B. Network
C. Transport
D. Application

Answer: B

Explanation:

The Network layer (Layer 3 of the OSI model) can utilize the connectionless protocol IP (Internet Protocol) to send data packets independently without establishing a connection. This approach is typical for protocols like IP, which provide best-effort delivery rather than guaranteed delivery. The document explains:
"The OSI Network Layer is responsible for logical addressing and routing, and it can utilize connectionless protocols like IP to send packets without requiring a session setup. This layer does not guarantee packet delivery, relying on higher layers for error detection or correction if needed."

Question: 297

A network engineer runs ipconfig and notices that the default gateway is 0.0.0.0. Which of the following address types is in use?

A. APIPA
B. Multicast
C. Class C
D. Experimental

Answer: A

Explanation:

APIPA (Automatic Private IP Addressing) assigns an IP address in the range 169.254.x.x when a DHCP server cannot be contacted, and it sets the default gateway to 0.0.0.0 because APIPA is designed only for local communication within the same subnet. The document states:
"APIPA allows for automatic, ad hoc network communication within a single subnet when a DHCP server is not available. In this state, the default gateway is typically set to 0.0.0.0 because APIPA does not provide routing to other networks."

Question: 298

A network administrator needs to monitor data from recently installed firewalls in multiple locations. Which of the following solutions would best meet the administrator's needs?

A. IDS
B. IPS
C. SIEM
D. SNMPv2

Answer: C

Explanation:

SIEM (Security Information and Event Management) systems are used to aggregate and analyze log data from various sources, including firewalls, to detect potential security incidents and assist in regulatory compliance. The document explains:
"SIEM solutions aggregate and analyze log and event data from multiple devices, including firewalls, across different locations. They help in real-time monitoring, incident response, and ensuring compliance with security policies."

Question: 299

Which of the following allows a standard user to log in to multiple resources with one account?

A. RADIUS
B. MFA
C. TACACS+
D. SSO

Answer: D

Explanation:

Single Sign-On (SSO) enables a user to access multiple resources or applications with one set of credentials, improving usability and security. The document confirms:
"Single Sign-On (SSO) allows a user to authenticate once and gain access to multiple resources or applications without needing to log in again for each. It streamlines the login process and improves security by reducing the number of passwords that need to be managed."

Question: 300

Which of the following should an installer orient a port-side exhaust to when installing equipment?

A. The patch panel
B. The front of the IDF
C. The warm aisle
D. The administrator console

Answer: C

Explanation:

In data centers, hot aisle/cold aisle configurations are used to manage airflow and cooling efficiency. Port-side exhausts should be oriented towards the warm aisle to expel hot air and maintain optimal cooling. The document clarifies:
"Equipment with port-side exhausts should be oriented towards the warm aisle to ensure that hot air is properly directed away from the cold air intake areas. This alignment supports effective cooling in data center environments."

Question: 301

Which of the following kinds of targeted attacks uses multiple computers or bots to request the same resource repeatedly?

A. On-path
B. DDoS
C. ARP spoofing
D. MAC flooding

Answer: B

Explanation:

A Distributed Denial of Service (DDoS) attack leverages multiple computers or bots (botnet) to flood a target system with requests, overwhelming its resources and making it unavailable to legitimate users. This is a common tactic used by attackers to disrupt services. The document explains:

"A DDoS (Distributed Denial of Service) attack involves multiple computers (often called bots) simultaneously sending requests to a single resource, overwhelming the system and causing a denial of service to legitimate users."

Question: 302

A network technician is troubleshooting the connection to the company website. The traceroute command produces the following output:

Traceroute towww.mysite.com(8.8.8.8) over a maximum of 30 hops

10.1.1.1 <1 ms 2. * <1 ms <1 ms

k k

k kTraceroute completeWhich of the following should the technician do to identify the path to the server?

A. Review the router's ACL.
B. Execute netstat.
C. Perform an nslookup.
D. Enable LLDP.

Answer: C

Explanation:

When traceroute shows asterisks (timeouts) instead of IP addresses or hostnames, it may indicate that intermediate routers are dropping ICMP packets. However, performing an nslookup will reveal the IP address associated with the domain name, confirming that DNS resolution is correct and helping identify the path to the target server. The document states:

"nslookup is used to query DNS servers to retrieve IP address information associated with a domain name, which helps confirm DNS resolution is working correctly even when traceroute results show timeouts."

Question: 303

A technician is deploying new networking hardware for company branch offices. The bridge priority must be properly set. Which of the following should the technician configure?

A. Spanning tree protocol
B. Jumbo frames
C. Perimeter network
D. Port security

Answer: A

Explanation:

Spanning Tree Protocol (STP) uses bridge priority values to determine the root bridge in a switched network topology.

Correctly configuring bridge priority helps in maintaining a loop-free and efficient network. The document explains:

"Spanning Tree Protocol (STP) uses bridge priority values to determine which switch will be the root bridge, ensuring loop prevention and efficient path selection within the network."

Question: 304

Which of the following is the most cost-effective way to safely expand outlet capacity in an IDF?

A. PDU
B. Surge protector
C. UPS
D. Power strip

Answer: A

Explanation:

A Power Distribution Unit (PDU) provides multiple power outlets in a data center or IDF (Intermediate Distribution Frame), while offering features like surge protection, load balancing, and sometimes remote monitoring, making it a cost-effective and reliable solution. The document confirms:

"PDUs (Power Distribution Units) are a cost-effective way to expand outlet capacity in a structured cabling environment like an IDF. They ensure safe power delivery to networking equipment and often include monitoring features."

Question: 305

Which of the following ports is a secure protocol?

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

Answer: C

Explanation:

Port 443 is used by HTTPS (Hypertext Transfer Protocol Secure), a secure version of HTTP that uses SSL/TLS to encrypt the communication between a client and server. This ensures confidentiality and integrity of data in transit. The document states:

"Port 443 is the default port for HTTPS, which secures HTTP traffic using SSL/TLS, providing encryption and secure identification of web servers."

Question: 306

Which of the following connector types is most commonly associated with Wi-Fi antennas?

A. BNC
B. SFP
C. MPO
D. RJ45

Answer: A

Explanation:

BNC (Bayonet Neill–Concelman) connectors are commonly used with coaxial cables in RF and wireless applications, including some older Wi-Fi antennas and specialized networking equipment. The document says:
"BNC (Bayonet Neill–Concelman) connectors are typically used with coaxial cables, especially in radio frequency (RF) and some Wi-Fi antenna applications, providing a secure and quick connect/disconnect."

Question: 307

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 fundamental step in device hardening, as default credentials are widely known and published online, posing a significant security risk if not updated. The document notes:
"Default passwords are often known by attackers and published on the internet. Changing them to unique, strong passwords is a critical first step in securing network devices against unauthorized access."

Question: 308

A network administrator upgraded the wireless access points and wants to implement a configuration that will give users higher speed and less channel overlap based on device compatibility. Which of the following will accomplish this goal?

A. 802.1X
B. MIMO

C. ESSID
D. Band steering

Answer: D

Explanation:

Band steering allows wireless access points to automatically direct capable devices to the 5GHz band, which typically has higher throughput and less interference than the 2.4GHz band, improving performance. The document confirms:
"Band steering helps balance wireless client loads by steering dual-band capable devices to the 5GHz band, which offers higher speeds and less channel congestion than 2.4GHz."

Question: 309

An employee has a new laptop and reports slow performance when using the wireless network.
Switch firmware was updated the previous night. A network administrator logs in to the switch and sees the following statistics on the switch interface for that employee:
98469 packets input, 1681937 bytes, 0 no buffer
Received 1548 broadcasts (25285 multicasts)
65335 runts, 0 giants, 0 throttles
11546 input errors, 5 CRC, 0 frame, 0 overrun, 0 ignored
0 input packets with dribble condition detected
22781 packets output, 858040 bytes, 0 underruns
0 output errors, 89920 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
E. lost carrier, 0 no carrier
F. output buffer failures, 0 output buffers swapped out
Which of the following is most likely the cause of the issue?

A. The patch cord from the wall jack is faulty.
B. The switchport bandwidth needs to be increased.
C. Multicast is not configured correctly on the switch.
D. The NIC is set to half duplex.

Answer: D

Explanation:

A large number of collisions and input errors typically indicates a duplex mismatch, such as when one device is set to full duplex and the other to half duplex. This leads to communication issues and poor performance. The document explains:
"Collisions and input errors are clear signs of duplex mismatches… typically caused when one device operates in half duplex while the other is in full duplex, causing performance and connectivity issues."

Question: 310

Which of the following uses the longest prefix match to determine an exit interface?

A. ARP table
B. MAC address table
C. Routing table
D. Netstat table

Answer: C

Explanation:

The longest prefix match is a routing concept used to find the most specific route to a destination IP address. The routing table performs this calculation to determine the exit interface for a packet, ensuring the most accurate delivery.
The document explains:
"Routers use the longest prefix match when searching the routing table to determine the best path for an IP packet. This ensures that the most specific (and thus optimal) route is chosen, based on the destination IP address."

Question: 311

Which of the following is the best way to keep devices on during a loss of power?

A. UPS
B. Power load
C. PDU
D. Voltage

Answer: A

Explanation:

A UPS (Uninterruptible Power Supply) provides backup power to devices during a power outage, allowing for continuous operation and protecting against sudden shutdowns that could cause data loss or equipment damage. The document confirms:
"A UPS (Uninterruptible Power Supply) is essential for maintaining power to critical devices during an outage, protecting data and ensuring continuous operation until power is restored or a safe shutdown can be performed."

Question: 312

A major natural disaster strikes a company's headquarters, causing significant destruction and data loss. The company needs to quickly recover and resume operations. Which of the following will a network administrator need to do first?

A. Conduct a damage assessment
B. Migrate to the cold site
C. Notify customers of the disaster
D. Establish a communication plan

Answer: A

Explanation:

In disaster recovery, the first step after an incident is to conduct a thorough damage assessment to understand the extent of the damage and determine the next appropriate steps. This allows for informed decision-making during the recovery process. The document says:
"The first step after a disaster is to conduct a damage assessment. This involves evaluating the extent of damage to equipment, infrastructure, and data, forming the foundation for recovery efforts and prioritizing response actions."

Question: 313

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

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

Answer: A, B

Explanation:

Troubleshooting poor performance of a newly installed access point involves multiple steps.
Checking for network bottlenecks and ensuring the device firmware is up to date are crucial first

steps. The document confirms:"Network bottlenecks can severely limit the performance of even the fastest wireless access points, so it's essential to verify that no other devices are causing a slowdown. In addition, keeping firmware updated ensures optimal performance and security."

Question: 314

A junior network administrator is auditing the company network and notices incrementing input errors on a long-range microwave interface. Which of the following is the most likely reason for the errors?

A. The parabolic signal is misaligned.
B. The omnidirectional signal is being jammed.
C. The omnidirectional signal is not strong enough to receive properly.
D. The parabolic signal uses improper routing protocols.

Answer: A

Explanation:

A misaligned parabolic antenna can cause a significant increase in input errors because the signal is not properly focused or directed towards the receiving antenna, resulting in poor reception and data corruption. The document confirms:

"Misalignment of parabolic microwave antennas can lead to weak or incorrect signal reception, causing an increase in input errors and connectivity issues on the link."

Question: 315

A network manager connects two switches together and uses two connecting links. Which of the following configurations will prevent Layer 2 loops?

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

Answer: C

Explanation:

Link aggregation (also known as port trunking or EtherChannel) combines multiple network connections in parallel to increase throughput and provide redundancy. When two switches are connected with multiple links without any additional configuration, a Layer 2 loop may occur. Link aggregation prevents these loops by treating the multiple connections as a single logical link, using a protocol such as LACP (Link Aggregation Control Protocol).

From Andrew Ramdayal's guide:

"Link aggregation allows you to combine multiple network connections to increase the bandwidth

and provide redundancy. It helps prevent Layer 2 loops when connecting switches with multiple links by making them operate as a single logical interface."

Question: 316

A network engineer is setting up a new VoIP network for a customer. The current network is segmented only for computers and servers. No additional switchports can be used in the new network. Which of the following does the engineer need to do to configure the network correctly? (Select two).

A. Change network translation definitions
B. Enable 802.1Q
C. Implement a routing protocol
D. Set up voice VLANs
E. Reconfigure the DNS
F. Place devices in the perimeter network

Answer: B, D

Explanation:

To support VoIP on a network with limited switchports, the engineer should configure voice VLANs and enable 802.1Q tagging. Voice VLANs allow VoIP traffic to be prioritized and isolated from data traffic even when sharing the same physical port. 802.1Q is used for VLAN tagging, enabling multiple VLANs over a single physical link.
From Andrew Ramdayal's guide:
"Voice VLANs allow IP phones and computers to share the same physical switch port while keeping their traffic separate. 802.1Q is used to tag VLAN traffic so that it can be appropriately routed and prioritized."

Question: 317

A user reports having intermittent connectivity issues to the company network. The network configuration for the user reveals the following:
IP address: 192.168.1.10
Subnet mask: 255.255.255.0
Default gateway: 192.168.1.254
The network switch shows the following ARP table:

MAC address	IP address	Interface	VLAN
0c00.1134.0001	192.168.1.10	eth4	10
0c00.1983.210a	192.168.2.13	eth5	11
0c00.1298.d239	192.168.1.10	eth6	10
0c00.a291.c113	192.168.2.12	eth7	11
0c00.923b.2391	192.168.1.11	eth8	10
feff.2391.1022	192.168.1.254	eth1	10

Which of the following is the most likely cause of the user's connection issues?

A. A port with incorrect VLAN assigned
B. A switch with spanning tree conflict
C. Another PC with manually configured IP D. A router with overlapping route tables

Answer: C

Explanation:
This scenario describes a duplicate IP address. The ARP table shows two different MAC addresses (0c00.1134.0001 and 0c00.1298.d239) associated with the same IP address (192.168.1.10), which leads to ARP table conflicts and intermittent connectivity.
From Andrew Ramdayal's guide:
"Duplicate IP addresses occur when two devices on the same network are assigned the same IP address, causing network conflicts. Common issues include manual configuration errors or DHCP lease issues. Resolution includes using IP management tools and avoiding overlaps in DHCP and static IP assignments."

Question: 318

Which of the following is associated with avoidance, acceptance, mitigation, and transfer?

A. Risk
B. Exploit
C. Threat
D. Vulnerability

Answer: A

Explanation:

These four terms—avoidance, acceptance, mitigation, and transfer—are strategies used in risk management.
From Andrew Ramdayal's guide:

"Risk in security refers to the potential for loss, damage, or destruction of assets or data due to a threat exploiting a vulnerability. Risk management strategies include avoidance, acceptance, mitigation, and transfer."

Question: 319

Which of the following routing technologies uses an attribute list for path selection?

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

Answer: A

Explanation:

BGP (Border Gateway Protocol) uses attributes like AS path, origin, and MED (multi-exit discriminator) to determine the best path among multiple available routes.
From Andrew Ramdayal's guide:
"BGP is the protocol underlying the global routing system of the internet. It is used for routing data between autonomous systems (ASes)... BGP uses a path vector mechanism and maintains a list of attributes for route selection."

Question: 320

Which of the following is the step that a troubleshooter should take immediately after implementing a solution?

A. Review lessons learned during the process.
B. Establish a plan of action.
C. Verify full system functionality.
D. Document actions and outcomes.

Answer: C

Explanation:

After implementing the solution, the immediate next step is to verify full system functionality. This confirms that the problem has been resolved and helps ensure no new issues have been introduced. From Andrew Ramdayal's guide:
"After the solution is implemented, test the system to ensure that it is fully operational, and the original problem has been resolved. Also, put in place any measures that could prevent the issue from recurring."

Question: 321

Which of the following protocols uses the Dijkstra's Link State Algorithm to establish routes inside its routing table?

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

Answer: A

Explanation:

OSPF (Open Shortest Path First) is a link-state routing protocol that uses the Dijkstra algorithm, also known as the shortest path first (SPF) algorithm, to determine the most efficient routes.
From Andrew Ramdayal's guide:
"OSPF is a link-state routing protocol that provides fast, efficient path selection using the shortest path first (SPF) algorithm."

Question: 322

After a recent security awareness phishing campaign, the cybersecurity team discovers that additional security measures need to be set up when users access potentially malicious websites. Which of the following security measures will best address this concern?

A. Implement DNS filtering.
B. Update ACLs to only allow HTTPS.
C. Configure new IPS hardware.
D. Deploy 802.1X security features.

Answer: A

Explanation:

DNS filtering blocks access to known malicious websites by comparing domain requests against a list of allowed or blocked URLs. It is an effective defense against phishing and other web-based attacks. From Andrew Ramdayal's

guide:

"URL filtering restricts access to specific websites or web content by comparing URLs against a predefined list of allowed or blocked sites…commonly used to prevent users from accessing malicious sites."

Question: 323

Which of the following offers the ability to manage access at the cloud VM instance?

A. Security group
B. Internet gateway
C. Direct Connect
D. Network ACL

Answer: A

Explanation:

Security groups in cloud environments act as virtual firewalls for VM instances, controlling inbound and outbound traffic based on specified rules.

From Andrew Ramdayal's guide:

"Network security groups are used to control inbound and outbound traffic to cloud resources within a VPC. They act as a virtual firewall for associated instances..."

Question: 324

A network administrator is creating a subnet that will include 45 separate hosts on a small private network within a large network architecture. Which of the following options is the most efficient use of network addresses when assigning this network?

A. 10.0.50.128/25
B. 10.7.142.128/27
C. 10.152.4.192/26
D. 10.192.1.64/28

Answer: C

Explanation:

For 45 hosts, the minimum subnet size must allow at least 46 usable addresses (1 each for network and broadcast addresses).

A /26 subnet provides 64 addresses, 62 usable — suitable.

A /27 subnet gives only 30 usable — insufficient.

A /25 offers 126 usable — more than needed.

A /28 provides just 14 — too small.

So, the most efficient subnet with minimal wastage is /26.

From Andrew Ramdayal's guide:

"When designing subnets, always choose the smallest subnet mask that still accommodates all hosts.
A /26 provides 62 usable host addresses, suitable for networks with about 50 hosts."

Question: 325

A network engineer needs to deploy an access point at a remote office so that it will not

communicate back to the wireless LAN controller. Which of the following deployment methods must the engineer use to accomplish this task?

A. Lightweight
B. Autonomous
C. Mesh
D. Ad hoc

Answer: B

Explanation:

Autonomous access points operate independently without needing to communicate with a central wireless LAN controller. This is ideal for remote deployments.
From Andrew Ramdayal's guide:
"Autonomous access points are stand-alone devices that manage their own configurations and operations. They do not require a WLC and are ideal for small or remote office deployments."

Question: 326

Which of the following is used to store and deliver content to clients in a geographically distributed manner using edge servers?

A. Load balancer
B. CDN
C. DNS server
D. SAN

Answer: B

Explanation:

A Content Delivery Network (CDN) stores cached versions of content in edge locations to deliver data faster and more reliably to users based on geographical proximity.
From Andrew Ramdayal's guide:
"CDNs distribute content to multiple, geographically dispersed servers. This enhances performance and reliability for end-users by reducing latency and load times."

Question: 327

Which of the following ports should a network administrator enable for encrypted login to a network switch?

A. 22
B. 23
C. 80
D. 123

Answer: A

Explanation:

Port 22 is used for Secure Shell (SSH), which enables encrypted remote login and command execution on network devices.
Port 23 = Telnet (unencrypted)
Port 80 = HTTP
Port 123 = NTP
From Andrew Ramdayal's guide:
"SSH uses port 22 to provide secure command-line access to devices such as switches and routers. Unlike Telnet (port 23), SSH encrypts session traffic, making it the preferred method for remote administration."

Question: 328

Which of the following would allow a network administrator to analyze attacks coming from the internet without affecting latency?

A. IPS
C. IDS
D. Load balancer
E. Firewall

Answer: B

Explanation:

An Intrusion Detection System (IDS) monitors and analyzes traffic to detect suspicious activity but does not sit in the traffic path, meaning it doesn't affect latency. In contrast, an IPS is in-line and can introduce delay.
From Andrew Ramdayal's guide:
"IDS monitors and alerts on malicious activity but does not block traffic, making it suitable for environments where low latency is critical."

Question: 329

A network engineer needs to change, update, and control APs remotely, with real-time visibility over HTTPS. Which of

the following will best allow these actions?

A. Web interface
B. Command line
C. SNMP console
D. API gateway

Answer: D

Explanation:

API gateways offer programmable control and real-time communication, commonly over HTTPS, which allows administrators to update and manage devices like access points remotely and efficiently.
From Andrew Ramdayal's guide:
"APIs enable automation and real-time interaction with network devices via secure interfaces, often using HTTPS for encrypted communication and control."

Question: 330

A detective is investigating an identity theft case in which the target had an RFID-protected payment card issued and compromised in the same day. The only place the target claims to have used the card was at a local convenience store. The detective notices a video camera at the store is placed in such a way that customers' credentials can be seen when they pay. Which of the following best explains this social engineering technique?

A. Shoulder surfing
B. Impersonation
C. Vishing
D. Tailgating

Answer: A

Explanation:

Shoulder surfing is a social engineering attack where attackers observe someone's private information by looking over their shoulder or using tools like cameras to capture input.
From Andrew Ramdayal's guide:
"Shoulder surfing is the act of watching someone enter confidential information, such as PINs or passwords, often using direct line-of-sight or surveillance equipment."

Question: 331

A user called the help desk after business hours to complain that files on a device are inaccessible and the wallpaper was changed. The network administrator thinks that this issue is an isolated incident, but the security analyst thinks the issue might be a ransomware attack. Which of the following troubleshooting steps should be taken first?

A. Identify the problem

B. Establish a theory
C. Document findings
D. Create a plan of action

Answer: A

Explanation:

The first step in any troubleshooting process is to identify the problem. This includes gathering information from the user, reviewing logs, and observing the symptoms. In this case, identifying the scope and nature of the issue (e.g., signs of ransomware) is critical before forming any theories or plans.
From Andrew Ramdayal's guide:
"The troubleshooting methodology begins with identifying the problem. This step involves questioning users, identifying user changes, and determining the symptoms."

Question: 332

A network technician is designing a LAN for a new facility. The company is expecting more than 300 devices to connect to the network. Which of the following masks will provide the most efficient subnet?

A. 255.255.0.0
B. 255.255.192.0
C. 255.255.254.0
D. 255.255.255.254

Answer: C

Explanation:

The requirement is to support over 300 hosts. The subnet mask 255.255.254.0 (or /23) provides 512 addresses, 510 of which are usable — ideal for around 300 devices.
255.255.0.0 (/16) provides too many addresses.
255.255.192.0 (/18) gives 16384 addresses — overkill.
255.255.255.254 is invalid for host assignments (only 2 addresses, 0 usable).
From Andrew Ramdayal's guide:
"To support 300 hosts, a /23 subnet (255.255.254.0) offers 510 usable addresses — the most efficient choice without excessive overhead."

Question: 333

After installing a new 6E wireless router in a small office, a technician notices that some wireless devices are not able to achieve the rated speeds.

Which of the following should the technician check to troubleshoot the issue? (Select two)

A. Client device compatibility

B. Back-end cabling

C. Weather phenomena

D. Voltage source requirements

E. Interference levels

F. Processing power

Answer: A, E

Explanation:

Question: 334

A network engineer receives a new router to use for WAN connectivity. Which of the following best describes the layer the network engineer should connect the new router to?

A. Access

B. Core

C. Leaf

D. Spine

Answer: C

Explanation:

Comprehensive and Detailed Explanation (paraphrased, aligned to N10-009):

In a spine–leaf architecture, endpoints (including servers, firewalls, and WAN/edge routers) connect to leaf switches. Leaf switches then uplink to spine switches; spine switches do not have endpoints connected directly to them. Therefore, a WAN router (an external/edge device) should connect to the leaf layer—often specifically to a "border leaf" that handles external connectivity.

Why not B. Core or D. Spine? In spine–leaf, "core" isn't a formal layer, and spines are designed only to interconnect leafs, not to terminate endpoints.

Why not A. Access? "Access" is a term from the traditional three-tier model (access–distribution– core). In modern spine–leaf language, the analogous layer for endpoint attachment is the leaf.

Reference (CompTIA Network+ N10-009):

Domain: Network Infrastructure — Data center and campus architectures (spine–leaf vs. three-tier), roles of leaf/spine, WAN/edge connectivity points.

Question: 335

A customer wants to cache commonly used content to reduce the number of full page downloads from the internet.
Which of the following should the network administrator recommend?

A. Proxy server
B. Load balancer
C. Open relay
D. Code repository

Answer: A

Explanation:

Comprehensive and Detailed Explanation (paraphrased, aligned to N10-009):

A proxy server (specifically a caching HTTP/HTTPS proxy) stores frequently accessed web objects and serves them locally to clients, reducing external bandwidth consumption and improving response times.

B . Load balancer distributes traffic across servers but does not inherently cache internet content.

C . Open relay is a misconfigured mail server that permits unauthorized relaying—this is a security issue, not a caching solution.

D . Code repository (e.g., for source control) isn't related to web content caching.

Reference (CompTIA Network+ N10-009):

Domain: Network Standards, Protocols, and Implementations — Application-layer services (HTTP/HTTPS), proxies and caching behavior, performance optimization.

Question: 336

Which of the following types of attacks is most likely to occur after an attacker sets up an evil twin?

A. On-path
B. DDoS
C. ARP spoofing
D. Phishing

Answer: A

Explanation:

Comprehensive and Detailed Explanation (paraphrased, aligned to N10-009):

An evil twin is a malicious wireless access point that impersonates a legitimate SSID. Once victims connect, the attacker can intercept and manipulate traffic, performing an on-path (man-in-the- middle) attack—capturing credentials, injecting content, or downgrading encryption.

B . DDoS overwhelms services with traffic; it's not the typical follow-on from clients joining a rogue AP.

C . ARP spoofing is another way to become on-path on wired segments, but with an evil twin, the wireless association itself enables the on-path position.

D . Phishing is social engineering; while an evil twin could be used to present fake portals, the primary technical posture after connection is on-path.

Reference (CompTIA Network+ N10-009):

Domain: Network Security — Wireless threats (rogue APs/evil twins), traffic interception, on-path attacks.

Question: 337

Which of the following connection methods allows a network engineer to automate configuration deployment for network devices across the environment?

A. RDP

B. Telnet

C. SSH

D. GUI

Answer: C

Explanation:

Comprehensive and Detailed Explanation (paraphrased, aligned to N10-009):

SSH provides secure, scriptable remote access used by automation/orchestration tools (e.g., leveraging CLI, NETCONF over SSH, or Ansible modules) to push configurations at scale.

A . RDP is primarily for Windows GUI sessions and is not commonly used for network device automation.

B . Telnet can be scripted but is insecure (plaintext); modern best practice is to use SSH.

D . GUI access is typically manual and not ideal for scalable, repeatable automation.

Reference (CompTIA Network+ N10-009):

Domain: Network Operations — Configuration management, automation/orchestration, secure

management protocols (SSH vs. Telnet), change at scale.

Question: 338

Which of the following would most likely be used to implement encryption in transit when using HTTPS?

A. SSH

B. TLS

C. SCADA

D. RADIUS

Answer: B

Explanation:

Comprehensive and Detailed Explanation (paraphrased, aligned to N10-009):

HTTPS is HTTP encapsulated in TLS (the successor to SSL), which provides confidentiality, integrity, and server authentication for web traffic.

A . SSH secures remote shell and tunnels, not HTTPS.

C . SCADA refers to industrial control systems, not a transport security protocol.

D . RADIUS is an AAA protocol for authentication/authorization/accounting, not the web encryption layer.

Reference (CompTIA Network+ N10-009):

Domain: Network Standards, Protocols, and Implementations — Web protocols (HTTP/HTTPS), TLS handshake and purpose, encryption in transit.

Question: 339

A network architect of a stock exchange broker is implementing a disaster recovery (DR) high- availability plan. Which of the following approaches would be the best fit?

A. Warm site

B. Active-active

C. Full mesh

D. In-band

Answer: B

Explanation:

In financial institutions such as stock exchanges, downtime or latency can have severe consequences. Active-active high availability ensures multiple sites/systems are running simultaneously, distributing the load and providing immediate failover with minimal or no interruption. This is the best approach for environments that require continuous uptime and resiliency.

A . Warm site: Useful for disaster recovery, but not immediate; systems must be partially configured and brought

online.

C . Full mesh: Refers to topology interconnections, not DR/HA design.

D . In-band: Relates to management methods, not HA/DR strategies.

Reference (CompTIA Network+ N10-009):

Domain: Network Infrastructure — High availability, redundancy strategies, active-active vs. activepassive design.

Question: 340

An organization recently connected a new computer to the LAN. The user is unable to ping the default gateway. The technician examines the configuration and sees a self-assigned IP address.

Which of the following is the most likely cause?

A. The DHCP server is not available
B. An RFC1918 address is being used
C. The TCP/IP stack is disabled
D. A static IP is assigned

Answer: A

Explanation:

When a host fails to obtain an IP address from a DHCP server, it assigns itself an APIPA (Automatic Private IP Addressing) address in the 169.254.x.x range, commonly described as a “self-assigned IP.” This prevents communication outside the local link, including reaching the default gateway.

B . RFC1918 addresses are private ranges (10.x.x.x, 172.16–31.x.x, 192.168.x.x), but these are not self-assigned.

C . If the TCP/IP stack were disabled, the host wouldn’t have any IP at all.

D . If a static IP were assigned, it would show a configured value, not self-assigned.

Reference (CompTIA Network+ N10-009):

Domain: Network Troubleshooting — IP addressing issues, DHCP failures, APIPA behavior.

Question: 341

During a security audit, a consulting firm notices inconsistencies between the documentation and the actual environment. Which of the following can keep a record of who made the changes and what the changes are?

A. Network access control
B. Configuration monitoring
C. Zero Trust

D. Syslog

Answer: B

Explanation:

Configuration monitoring and management tools (often part of network management systems) maintain version-controlled records of device configurations, track changes, and log who made them. This provides accountability and supports compliance audits.

A . Network access control (NAC) manages endpoint access policies but does not track device config changes.

C . Zero Trust is a security framework requiring strict identity verification, not a configuration tracking tool.

D . Syslog collects system logs, but without a config monitoring system, it does not directly compare documentation to device state.

Reference (CompTIA Network+ N10-009):

Domain: Network Operations — Change management, configuration management, auditing.

Question: 342

An attacker gained access to the hosts file on an endpoint and modified it. Now, a user is redirected from the company's home page to a fraudulent website. Which of the following most likely happened?

A. DNS spoofing
B. Phishing
C. VLAN hopping
D. ARP poisoning

Answer: A

Explanation:

When the hosts file is altered, local name resolution is compromised, and domain queries are redirected to malicious IP addresses. This is a form of DNS spoofing/poisoning, where false mappings trick users into visiting fraudulent websites.

B . Phishing typically uses emails or messages to trick users, not local file modification.

C . VLAN hopping is a Layer 2 attack to gain unauthorized network access, unrelated to DNS.

D . ARP poisoning manipulates ARP tables on a LAN to reroute traffic, not name resolution.

Reference (CompTIA Network+ N10-009):

Domain: Network Security — DNS poisoning/spoofing, host file manipulation, endpoint attacks.

Question: 343

Which of the following allows a network administrator to analyze attacks coming from the internet without affecting latency?

A. IPS
B. IDS
C. Load balancer
D. Firewall

Answer: B

Explanation:

An IDS (Intrusion Detection System) is deployed out-of-band, meaning it passively monitors network traffic using a SPAN/mirror port or network tap. It detects and analyzes suspicious traffic without introducing latency since it does not sit in-line.

A . IPS (Intrusion Prevention System) is in-line and can block traffic but may add latency.

C . Load balancer distributes traffic across servers for performance and redundancy, not for threat detection.

D . Firewall filters traffic at the perimeter or internally; it can affect latency but does not provide the same in-depth attack analysis.

Reference (CompTIA Network+ N10-009):

Domain: Network Security — IDS vs. IPS, in-band vs. out-of-band monitoring, passive detection methods.

Question: 344

Which of the following attacks forces a switch to send all traffic out of all ports?

A. ARP poisoning
B. Evil twin
C. MAC flooding
D. DNS spoofing

Answer: C

Explanation:

MAC flooding overwhelms a switch's CAM (Content Addressable Memory) table by sending a flood of frames with spoofed MAC addresses. Once the CAM table overflows, the switch cannot learn legitimate MAC addresses and defaults to flooding all frames out all ports, effectively turning it into a hub. This allows an attacker to capture traffic not originally destined for their port.

A . ARP poisoning corrupts ARP tables to redirect traffic but does not overflow the CAM table.

B . Evil twin is a wireless rogue AP attack, unrelated to switch behavior.

D . DNS spoofing redirects domain queries, not Layer 2 switching.

Reference (CompTIA Network+ N10-009):

Domain: Network Security — Switch security, CAM table attacks, MAC flooding.

Question: 345

A network engineer is installing new PoE wireless APs. The first five APs deploy successfully, but the sixth one fails to start. Which of the following should the engineer investigate first?

A. Signal strength
B. Duplex mismatch
C. Power budget
D. CRC

Answer: C

Explanation:

When deploying multiple Power over Ethernet (PoE) devices, the switch's power budget can be exhausted. If the available wattage on the switch cannot supply the additional AP, it will fail to power on. This is the most likely cause when previous APs worked fine but a new one does not.

A . Signal strength affects wireless connectivity, not whether the AP powers up.

B . Duplex mismatch causes poor throughput, not power failure.

D . CRC errors point to cabling issues but do not prevent booting if no power is available.

Reference (CompTIA Network+ N10-009):

Domain: Network Troubleshooting — PoE power budget considerations, device startup issues.

Question: 346

Which of the following devices functions mainly at the data link layer of the OSI model and is used to connect a fiber-

optic cable to a network interface?

A. SC
B. DAC
C. SFP transceiver
D. Twinaxial cable

Answer: C

Explanation:

An SFP (Small Form-factor Pluggable) transceiver is a modular device that provides the interface between fiber-optic or copper cabling and the networking equipment (e.g., switch or router). It operates primarily at Layer 2 (Data Link), converting optical or electrical signals into frames usable by the network device.

A . SC is a fiber connector type, not the transceiver.

B . DAC (Direct Attach Copper) is a passive copper cable assembly with fixed transceivers, not a general-purpose module.

D . Twinaxial cable is a copper medium, not an interface device.

Reference (CompTIA Network+ N10-009):

Domain: Networking Concepts — Transceivers (SFP, GBIC, QSFP), fiber connectivity, OSI model mapping.

Question: 347

Which of the following steps of the troubleshooting methodology would most likely involve comparing current throughput tests to a baseline?

A. Implement the solution
B. Verify full system functionality
C. Document findings
D. Test the theory

Answer: B

Explanation:

Verifying full system functionality occurs after implementing a fix. This step ensures the solution resolved the issue and that performance is back to expected levels. Comparing current throughput to baseline measurements is part of validation testing to confirm everything is within normal operational parameters.

A . Implement the solution applies the fix but does not confirm results.

C . Document findings happens at the end of troubleshooting.

D . Test the theory comes earlier, when trying to confirm the suspected cause.

Reference (CompTIA Network+ N10-009):

Domain: Network Troubleshooting — Troubleshooting methodology steps, baselines, verification testing.

Question: 348

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

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

Answer: C

Explanation:

Multi-factor authentication (MFA) requires two or more different categories of authentication factors:

Something you know (password, PIN)

Something you have (smart card, hardware token)

Something you are (biometric)

The only valid second factor here is a hard token (e.g., a key fob generating one-time codes).

A . PIN is still "something you know," the same category as a password.

B . Favorite color is a weak knowledge-based factor, not a true second factor.

D . Mother's maiden name is also "something you know" and insecure.

Reference (CompTIA Network+ N10-009):

Domain: Network Security — Authentication methods, MFA factor categories.

Question: 349

A network technician is working on a PC with a faulty NIC. The host is connected to a switch with secured ports. After testing the connection cables and using a known-good NIC, the host is still unable to connect to the network. Which of the following is causing the connection issue?

A. MAC address of the new card

B. BPDU guard settings
C. Link aggregation settings
D. PoE power budget

Answer: A

Explanation:

If a switch has port security enabled (such as sticky MAC or a configured allowed MAC), the port will only allow the original NIC's MAC address. When a new NIC with a different MAC address is installed, the port rejects traffic, preventing network connectivity.

B . BPDU guard protects against rogue switches, not end hosts.

C . Link aggregation applies when bundling multiple uplinks, not a single PC connection.

D . PoE budget applies to powered devices like APs, not PCs.

Reference (CompTIA Network+ N10-009):

Domain: Network Troubleshooting — Port security, MAC address filtering, switch security features.

Question: 350

A network administrator deploys new network hardware. While configuring the network monitoring server, the server could authenticate but could not determine the specific status of the hardware.
Which of the following would the administrator most likely do to resolve the issue?

A. Use the public community string
B. Import the appropriate MIB
C. Set up a switchport analyzer and forward traffic
D. Configure SNMPv3 privacy

Answer: B

Explanation:

MIBs (Management Information Bases) define the variables and objects that SNMP can query on a device. If the monitoring server authenticates but cannot interpret the data, it likely lacks the correct MIB for that vendor or model. Importing the proper MIB allows the monitoring server to correctly display device status and metrics.

A . Using a public community string is insecure and not related to missing MIBs.

C . Switchport analyzer (SPAN) captures traffic for packet analysis, not SNMP monitoring.

D . SNMPv3 privacy adds encryption but doesn't fix missing MIB interpretation.

Reference (CompTIA Network+ N10-009):

Domain: Network Operations — SNMP, MIBs, network monitoring systems.

Question: 351

A company's Chief Information Security Officer requires that servers and firewalls have accurate timestamps when creating log files so that security analysts can correlate events during incident investigations. Which of the following should be implemented?

A. Syslog server
B. SMTP
C. SNMP
D. NTP

Answer: D

Explanation:

NTP (Network Time Protocol) synchronizes clocks across network devices, ensuring accurate timestamps in logs. This is critical for correlating events across different systems during investigations.

A . Syslog collects logs but relies on accurate timestamps already present.

B . SMTP is an email protocol, unrelated to time synchronization.

C . SNMP is for monitoring and management, not time.

Reference (CompTIA Network+ N10-009):

Domain: Network Operations — Time synchronization (NTP), log correlation, security operations.

Question: 352

Two network switches at different locations are connected via fiber-optic cable at a distance of 10 miles (16 km). The duplex fiber-optic patch cord between the patch panel and switch is accidentally pinched, stopping connectivity between the two switches. A network technician replaces the broken cable with a new, single-mode patch cord. However, connectivity between both switches is still down and the link lights are still off. Which of the following actions should the technician perform first?

A. Replace the fiber-optic transceiver in the switch
B. Log in to the switch to shut down and re-enable the switchport
C. Transpose the two fiber connectors at one end of the new patch cord
D. Swap the single-mode fiber patch cord with a multimode fiber patch cord

Answer: C

Explanation:

Fiber connections require Tx on one end to connect to Rx on the other end. If the patch cord is replaced and link lights remain off, the most common cause is that the connectors are reversed. Swapping (transposing) the connectors ensures proper transmit/receive alignment.

A . Replacing the transceiver may eventually be necessary, but only after verifying correct connections.

B . Restarting the switchport won't resolve a physical misconnection.

D . Using multimode fiber would be incorrect here, as the link was designed for single-mode (10 miles/16 km requires SMF).

Reference (CompTIA Network+ N10-009):

Domain: Network Troubleshooting — Fiber connectivity, Tx/Rx alignment, link light diagnostics.

Question: 353

Users are reporting issues with mobile phone connectivity after a cellular repeater was recently installed. Users also note that the phones are rapidly losing battery charge. Which of the following should the technician check first to troubleshoot the issue?

A. WPS configuration
B. Signal strength
C. Channel frequency
D. Power budget

Answer: B

Explanation:

When signal strength is poor, mobile devices constantly boost their transmission power in an attempt to maintain a stable connection. This results in dropped calls/data and rapid battery drain. Since a repeater was installed, misalignment or misconfiguration could be degrading the signal strength.

A . WPS applies to Wi-Fi, not cellular repeaters.

C . Channel frequency might matter for interference, but signal strength is the most direct cause of the described symptoms.

D . Power budget applies to PoE and wired devices, not mobile phones.

Reference (CompTIA Network+ N10-009):

Domain: Network Troubleshooting — Wireless/cellular troubleshooting, signal strength impact, user symptoms (battery drain, poor connectivity).

Question: 354

A network engineer is implementing a new connection between core switches. The engineer deploys the following configurations:

Core-SW01

vlan 100

name

interface Ethernet 1/1

channel-group 1 mode active

interface Ethernet 1/2

channel-group 1 mode active

interface port-channel 1

switchport mode trunk

switchport trunk allow vlan 100

Core-SW02

vlan 100

name

interface Ethernet 1/1

switchport mode trunk

switchport trunk allow vlan 100

interface Ethernet 1/2

switchport mode trunk

switchport trunk allow vlan 100

interface port-channel 1

switchport mode trunk

switchport trunk allow vlan 100

Which of the following is the state of the Core-SW01 port-channel interfaces?

A. Incrementing CRC errors

B. Error disabled

C. Administratively down

D. Suspended

Answer: D

On Core-SW01, the ports are configured with LACP (mode active) for link aggregation. On Core- SW02, the ports are configured as independent trunks, not as part of an LACP group. Because of this mismatch, LACP cannot form the bundle, and the aggregated ports on SW01 will go into a suspended state.

A . CRC errors suggest cabling or signal integrity issues, not config mismatch.

B . Error disabled occurs when a violation (like BPDU guard or port security) disables the port, not

LACP mismatch.

C . Administratively down indicates a shutdown command, not the case here.

Reference (CompTIA Network+ N10-009):

Domain: Network Troubleshooting — Port-channel/LACP configuration issues, interface states.

Question: 355

After a security incident, a technician reveals that company data was stolen. During the investigation, it is discovered that a host disguised itself as a switch. Which of the following best describes the attack that occurred?

A. VLAN hopping

B. Evil twin

C. DNS poisoning

D. ARP spoofing

Answer: A

VLAN hopping occurs when an attacker tricks a switch into believing the host is another switch by generating tagged frames or exploiting trunk negotiation (DTP). This allows the attacker to access traffic from multiple VLANs, potentially stealing sensitive data.

B . Evil twin is a rogue wireless AP attack, unrelated to switch impersonation.

C . DNS poisoning corrupts name resolution, not VLAN access.

D . ARP spoofing is a Layer 2 on-path attack, not masquerading as a switch.

Reference (CompTIA Network+ N10-009):

Domain: Network Security — VLAN hopping attacks, switch spoofing techniques.

Question: 356

Which of the following troubleshooting steps provides a change advisory board with the information needed to make a decision?

A. Identify the problem
B. Develop a theory of probable cause
C. Test the theory to determine cause
D. Establish a plan of action

Answer: D

When dealing with troubleshooting and change management, the plan of action outlines the steps, risks, and mitigation strategies. A change advisory board (CAB) uses this documented plan to decide whether to approve the change.

A . Identify the problem is the first step in troubleshooting, not decision-making for CAB.

B . Develop a theory is diagnostic work, not planning.

C . Test the theory confirms causes but doesn't provide actionable planning information.

Reference (CompTIA Network+ N10-009):

Domain: Network Operations — Change management, troubleshooting methodology, CAB processes.

Question: 357

Voice traffic is experiencing excessive jitter. A network engineer wants to improve call performance and clarity. Which of the following features should the engineer configure?

A. QoS
B. STP

Answer: A

Quality of Service (QoS) prioritizes delay-sensitive traffic such as VoIP by assigning higher priority in queues, reducing jitter, latency, and packet loss. Implementing QoS policies ensures stable and clear voice communication.

B . STP (Spanning Tree Protocol) prevents switching loops, but it does not address jitter or real-time traffic performance.

Reference (CompTIA Network+ N10-009):

Domain: Network Infrastructure — QoS, traffic shaping, prioritization of voice/video.

Question: 358

A user tries to visit a website, but instead of the intended site, the page displays vmw.cba.com.
Which of the following should be done to reach the correct website?

A. Modify the CNAME record
B. Update the PTR record
C. Change the NTP settings
D. Delete the TXT record

Answer: A

A CNAME (Canonical Name) record maps an alias to the correct fully qualified domain name (FQDN). If a user is redirected to the wrong hostname, correcting or updating the CNAME ensures the alias points to the proper domain.

B . PTR record maps IP to hostname (reverse DNS), not forward website resolution.

C . NTP relates to time sync, irrelevant to DNS resolution.

D . TXT record stores metadata like SPF or DKIM info, not used for hostname aliasing.

Reference (CompTIA Network+ N10-009):

Domain: Network Standards, Protocols, and Implementations — DNS record types (A, AAAA, CNAME, PTR, TXT).

Question: 359

Which of the following physical installation factors is the most important when a network switch is installed in a sealed enclosure?

A. Fire suppression
B. Power budget
C. Temperature
D. Humidity

Answer: C

Switches in sealed enclosures are at risk of overheating because airflow is restricted. The temperature factor is critical since heat buildup can damage components, shorten device lifespan, and cause outages. Proper cooling or ventilation must be ensured.

A . Fire suppression is important for data centers but not the primary concern in a sealed box.

B . Power budget applies to PoE allocations, not environmental safety.

D . Humidity matters, but overheating is far more immediate in sealed environments.

Reference (CompTIA Network+ N10-009):

Domain: Network Infrastructure — Environmental considerations, switch installation, temperature control.

Question: 360

A network technician needs to connect a new user to the company's Wi-Fi network called SSID: business. When attempting to connect, two networks are listed as possible choices: SSID: business and SSID: myaccess. Which of the following attacks is occurring?

A. On-path
B. Rogue AP
C. Evil twin
D. Tailgating

Answer: C

An evil twin attack occurs when an attacker creates a fraudulent AP with an SSID very similar (or identical) to the legitimate one. Users may accidentally connect, allowing the attacker to capture traffic and credentials.

A . On-path is the consequence of connecting to the evil twin, not the initial attack itself.

B . Rogue AP is any unauthorized access point, but the key here is the malicious mimicry of a legitimate SSID — specifically an evil twin.

D . Tailgating is a physical social engineering attack, unrelated to Wi-Fi.

Reference (CompTIA Network+ N10-009):

Domain: Network Security — Wireless threats (rogue APs, evil twins).

Question: 361

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

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

Answer: A

Spanning Tree Protocol (STP) is designed to detect and prevent Layer 2 loops by blocking redundant paths. If loops are possible in the design, enabling STP ensures network stability.

B . Port security controls endpoint MAC addresses, not loops.

C . Speed limits address bandwidth, not loop prevention.

D . 802.1Q tagging allows VLAN separation but does not resolve loops.

Reference (CompTIA Network+ N10-009):

Domain: Network Operations — Loop prevention, spanning tree, switch design.

Question: 362

A network engineer connects a business to a new ISP. A simple ping test to 8.8.8.8 is successful.

However, users complain of extreme slowness to any website and periods of no connectivity. Which of the following is the most likely cause?

A. Incorrect default gateway
B. VLAN mismatch
C. Subnet mask configuration
D. Duplicate ISP IP address

Answer: D

If the business shares or duplicates the ISP-assigned public IP address, routing instability and conflicts will occur. Pinging a public IP like 8.8.8.8 may work (since ICMP can bypass certain conflicts), but browsing websites (which requires stable sessions and return traffic) will fail intermittently.

A . If the default gateway were incorrect, no external connectivity would work at all.

B . VLAN mismatch is an internal issue, not affecting ISP routing.

C . Subnet mask misconfiguration would prevent consistent routing but usually blocks ping too.

Reference (CompTIA Network+ N10-009):

Domain: Network Troubleshooting — Internet connectivity issues, ISP IP conflicts.

Question: 363

Which of the following is a type of NAC that uses a set of policies to allow or deny access to the network based on the user's identity?

A. Standard ACL
B. MAC filtering
C. 802.1X
D. SSO

Answer: C

802.1X is a port-based Network Access Control (NAC) method that enforces authentication before allowing access to the network. It uses a RADIUS server for identity verification and policy enforcement, ensuring only authorized users/devices gain access.

A . Standard ACL filters traffic by IP, not identity.

B . MAC filtering controls devices by hardware address but can be spoofed.

D . SSO (Single Sign-On) provides user convenience across services, not network-level access control.

Reference (CompTIA Network+ N10-009):

Domain: Network Security — NAC, 802.1X authentication, identity-based access.

Question: 364

A network administrator recently configured an autonomous wireless AP and performed a throughput test via comptiaspeedtester.com. The result was 75 Mbps. When connected to other APs, the results reached 500 Mbps. Which of the following is most likely the reason for this difference?

A. Channel width configuration
B. DNS server issues
C. Authentication failure
D. Incorrect DHCP settings

Answer: A

Explanation:

The channel width (20 MHz vs. 40 MHz vs. 80 MHz) directly impacts Wi-Fi throughput. If the AP is configured with a narrow channel width (e.g., 20 MHz), maximum data rates will be significantly lower than other APs using wider channels (e.g., 80 MHz). This matches the scenario where one AP achieves only ~75 Mbps, while others reach 500 Mbps.

B . DNS issues affect name resolution, not raw throughput.

C . Authentication failure would prevent connection, not reduce throughput.

D . DHCP issues would prevent obtaining an IP, not cause slower speeds.

Reference (CompTIA Network+ N10-009):

Domain: Network Troubleshooting — Wireless throughput issues, channel width configuration.

Question: 365

Which of the following is an example of a split-tunnel VPN?

A. Only public resources are accessed through the user's internet connection.
B. Encrypted resources are accessed through separate tunnels.
C. All corporate and public resources are accessed through routing to on-site servers.
D. ACLs are used to balance network traffic through different connections.

Answer: A

Explanation:

In a split-tunnel VPN, only corporate traffic is sent through the VPN tunnel, while public internet traffic goes directly through the user's local ISP. This reduces bandwidth use on the corporate VPN concentrator and improves performance for non-work traffic.

B . Separate tunnels for encrypted traffic describes multi-tunnel VPNs, not split tunneling.

C . All traffic routed through on-site servers is a full-tunnel VPN, not split-tunnel.

D . ACLs balancing traffic relates to routing or load balancing, not VPN split tunneling.

Reference (CompTIA Network+ N10-009):

Domain: Networking Concepts — VPN types, split vs. full tunnel, remote access.

Question: 366

Which of the following cable types allows the use of QSFP ports without requiring transceivers?

A. Multimode
B. Twinaxial
C. RG11
D. Category 6

Answer: B

Explanation:

Twinaxial (Direct Attach Copper / DAC) cables can plug directly into QSFP ports without needing separate optical transceivers. They are cost-effective for short-distance, high-speed connections (commonly in data centers).

A . Multimode fiber requires SFP/QSFP transceivers to convert electrical signals to optical.

C . RG11 is coaxial cable for broadband/cable TV, not used in QSFP ports.

D . Category 6 is twisted-pair Ethernet cabling, not directly compatible with QSFP ports.

Reference (CompTIA Network+ N10-009):

Domain: Network Infrastructure — Cable types, QSFP, DAC (Twinaxial), transceiver requirements.

Question: 367

Which of the following protocols is commonly associated with TCP port 443?

A. Telnet
B. SMTP
C. HTTPS
D. SNMP

Answer: C

Explanation:

TCP port 443 is reserved for HTTPS (Hypertext Transfer Protocol Secure), which uses TLS encryption to secure web traffic.

It is the standard port for encrypted web communications.

A . Telnet uses TCP port 23.

B . SMTP commonly uses TCP ports 25, 465, or 587.

D . SNMP typically uses UDP ports 161 (queries) and 162 (traps).

Reference (CompTIA Network+ N10-009):

Domain: Network Standards, Protocols, and Implementations — Common ports and services.

Question: 368

A network administrator is setting up a firewall to protect the organization's network from external threats. Which of the following should the administrator consider first when configuring the firewall?

A. Required ports, protocols, and services
B. Inclusion of a deny all rule
C. VPN access
D. Outbound access originating from customer-facing servers

Answer: A

Explanation:

When configuring a firewall, the first step is identifying which ports, protocols, and services are required for normal business operations. This ensures only legitimate traffic is allowed. After establishing the required rules, a default deny rule is added for security.

B . Deny all rule is important, but it should come after defining required rules.

C . VPN access is a service to configure, but only after determining baseline needs.

D . Outbound traffic policies are part of refinement, not the first consideration.

Reference (CompTIA Network+ N10-009):

Domain: Network Security — Firewall configuration, rule order, least privilege.

Question: 369

A company's VoIP phone connection is cutting in and out. A senior network engineer is recommending the implementation of a voice VLAN. Which of the following should be configured?

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

Answer: A

Explanation:

Voice VLANs rely on 802.1Q tagging to separate voice traffic from data traffic on the same physical link. This separation allows QoS policies to prioritize VoIP, reducing jitter and packet loss.

B . Jumbo frames improve throughput for large data transfers, not voice.

C . Native VLAN is the untagged VLAN, not specifically for voice.

D . Link aggregation bundles links for bandwidth/redundancy, not QoS.

Reference (CompTIA Network+ N10-009):

Domain: Network Infrastructure — VLANs, voice VLANs, 802.1Q tagging, QoS.

Question: 370

A network engineer adds a tunnel for a new branch network. Which of the following ensures that all data is encrypted inside the tunnel?

A. ESP
B. SSH
C. GRE
D. IKE

Answer: A

Explanation:

ESP (Encapsulating Security Payload) is an IPsec protocol that provides encryption, integrity, and authentication for data inside a VPN tunnel. It ensures that all tunneled traffic is encrypted.

B . SSH secures remote terminal sessions, not site-to-site VPN tunnels.

C . GRE (Generic Routing Encapsulation) provides encapsulation but does not encrypt data.

D . IKE (Internet Key Exchange) negotiates keys and establishes the IPsec tunnel but does not encrypt the payload itself.

Reference (CompTIA Network+ N10-009):

Domain: Network Security — VPN protocols, IPsec (AH vs. ESP), encryption in transit.

Question: 371

During a VoIP call, a user notices inconsistent audio and logs an incident ticket. A network administrator notices inconsistent delays in arrival of the RTP packets. Which of the following troubleshooting tools should the network administrator use to determine the issue?

A. Toner and probe
B. Protocol analyzer
C. Cable tester
D. Spectrum reader

Answer: B

Explanation:

Inconsistent arrival of RTP (Real-Time Protocol) packets indicates jitter or latency variation. A protocol analyzer (packet sniffer, e.g., Wireshark) can capture and analyze RTP streams, showing delay, jitter, and packet loss statistics.

A . Toner and probe locates cable runs, not packet analysis.

C . Cable tester checks wiring faults, not packet timing.

D . Spectrum reader is for identifying wireless interference, not analyzing RTP traffic.

Reference (CompTIA Network+ N10-009):

Domain: Network Troubleshooting — Protocol analyzers, VoIP troubleshooting, jitter analysis.

Question: 372

After extremely high temperatures cause a power outage, the servers automatically shut down, even though the UPSs for the servers still have hours of battery life. Which of the following should a technician recommend?

A. Include backup power for air-conditioning units
B. Configure door locks to automatically lock during power outages
C. Increase UPS battery size
D. Add an IoT-enabled thermostat

Answer: A

Explanation:

Servers shut down due to overheating, not loss of electrical power. Although UPS units had battery life, without cooling systems (HVAC/air conditioning) running on backup power, server rooms overheated. Backup power for air-conditioning is essential in data center design.

B . Door locks are unrelated to server shutdown.

C . Increasing UPS capacity won't help cooling.

D . IoT thermostats may monitor temperature but won't prevent overheating.

Reference (CompTIA Network+ N10-009):

Domain: Network Infrastructure — Environmental controls, power redundancy, HVAC systems.

Question: 373

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

root cause?

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

Answer: A

Explanation:

Traffic analysis involves monitoring and inspecting network traffic flows to detect unusual patterns, such as a workstation sending large volumes of outbound SMTP (spam). This process enables identification of malware as the root cause.

B . Availability monitoring checks uptime but doesn't diagnose spam traffic.

C . Baseline metrics show normal usage but don't pinpoint infected hosts.

D . Network discovery identifies devices, not malicious traffic flows.

Reference (CompTIA Network+ N10-009):

Domain: Network Security — Traffic analysis, malware detection, identifying compromised hosts.

Question: 374

After a recent merger, a large number of alerts are coming in regarding extremely high utilization.
Which of the following should be generated to help inform new alerting requirements?

A. SLA
B. Network diagram
C. Baseline
D. Heat map

Answer: C

Explanation:

A baseline establishes normal performance levels for network utilization, latency, jitter, and other metrics. After a merger, traffic patterns change, so a new baseline is needed to recalibrate monitoring thresholds and avoid excessive false alerts.

A . SLA defines performance agreements with customers but doesn't adjust alerting.

B . Network diagrams show topology, not traffic norms.

D . Heat maps show wireless coverage, not utilization baselines.

Reference (CompTIA Network+ N10-009):

Domain: Network Operations — Baselines, monitoring, alerting, performance tuning.

Question: 375

An administrator needs to configure an IoT device with a /21 subnet mask, but the device will only accept dotted decimal notation. Which of the following subnet masks should the administrator use?

A. 255.255.224.0
B. 255.255.240.0
C. 255.255.248.0
D. 255.255.252.0

Answer: B

Explanation:

A /21 subnet mask means 21 bits are network bits:

8 + 8 + 5 = 21 → leaves 11 bits for hosts.

Subnet mask in binary: 11111111.11111111.11111000.00000000

Converted to decimal: 255.255.248.0

Therefore:

A . /19 = 255.255.224.0

B . /20 = 255.255.240.0

Q C . /21 = 255.255.248.0 ← correct

D . /22 = 255.255.252.0

Answer correction: The correct option is C. 255.255.248.0, not B.

Reference (CompTIA Network+ N10-009):

Domain: Networking Concepts — Subnetting, CIDR notation, dotted decimal masks.

Question: 376

A junior network administrator gets a text message from a number posing as the domain registrar of the firm. The administrator is tricked into providing global administrator credentials. Which of the following attacks is taking place?

A. DNS poisoning
B. ARP spoofing
C. Vishing
D. Smishing

Answer: D

Explanation:

Smishing (SMS phishing) occurs when attackers send fraudulent text messages pretending to be a trusted source, tricking the victim into giving up sensitive credentials. Since this came via text message, it qualifies as smishing.

A . DNS poisoning corrupts name resolution.

B . ARP spoofing manipulates MAC-to-IP mappings.

C . Vishing is phishing via voice calls, not text.

Reference (CompTIA Network+ N10-009):

Domain: Network Security — Social engineering, phishing types (smishing, vishing, spear phishing).

Question: 377

Which of the following tools uses ICMP to help determine whether a network host is reachable?

A. tcpdump
B. netstat
C. nslookup
D. ping

Answer: D

Explanation:

Ping sends ICMP Echo Request packets and waits for Echo Replies to verify host reachability and measure round-trip time.

A . tcpdump captures packets but does not test reachability.

B . netstat displays open ports and network sessions.

C . nslookup queries DNS servers for name resolution.

Reference (CompTIA Network+ N10-009):

Domain: Networking Concepts — ICMP operation, troubleshooting tools.

Question: 378

A newly opened retail shop uses a combination of new tablets, PCs, printers, and legacy card readers.
Which of the following wireless encryption types is the most secure and compatible?

A. WPA3
B. WPA2

C. WPA2/WPA3 mixed mode

D. WPA/WPA2 mixed mode

Answer: C

Explanation:

WPA2/WPA3 mixed mode provides compatibility for older devices (that only support WPA2) while allowing newer devices to take advantage of stronger WPA3 encryption. This ensures maximum compatibility and security in a mixed-device environment.

A . WPA3 only is most secure but not compatible with legacy devices.

B . WPA2 only is secure but does not future-proof against WPA3-capable devices.

D . WPA/WPA2 mixed mode is weaker due to WPA (deprecated, insecure).

Reference (CompTIA Network+ N10-009):

Domain: Network Security — Wi-Fi encryption standards, WPA2 vs WPA3, mixed-mode compatibility.

Question: 379

A network technician is configuring the company's network of 100 Mbps Layer 2 switches. The technician wants increased throughput for the uplinks between switches. The technician connects multiple redundant links between the switches. Which of the following should the technician configure?

A. Spanning Tree Protocol

B. Switch Virtual Interfaces

C. Native VLAN

D. First Hop Redundancy Protocol

Answer: A

Explanation:

When multiple redundant links exist between switches, Spanning Tree Protocol (STP) is required to prevent switching

loops. STP blocks redundant paths but can allow aggregation if configured with protocols like LACP.

B . SVIs provide Layer 3 interfaces, not loop prevention.

C . Native VLAN defines the untagged VLAN but does not manage loops.

D . FHRP (VRRP, HSRP, GLBP) provides gateway redundancy, not switch uplink management.

Reference (CompTIA Network+ N10-009):

Domain: Network Infrastructure — STP, redundancy, loop prevention.

Question: 380

Which of the following involves an attacker traversing from one part of a network to another part that should be inaccessible?

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

Answer: C

Explanation:

VLAN hopping allows an attacker to send traffic into another VLAN without authorization, often by impersonating a switch and negotiating a trunk link. This lets the attacker traverse into normally inaccessible VLANs.

A . MAC flooding disrupts switch operations but does not cross VLANs.

B . DNS poisoning corrupts name resolution.

D . ARP spoofing reroutes local traffic but doesn't grant VLAN traversal.

Reference (CompTIA Network+ N10-009):

Domain: Network Security — VLAN attacks, unauthorized lateral movement.

Question: 381

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

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

Answer: C

Explanation:

MFA (Multi-Factor Authentication) requires factors from different categories:

Something you know → Password, PIN

Something you have → Smart card, hardware (hard) token

Something you are → Biometric

The correct second factor is a hard token.

A . PIN = something you know (same factor as password).

B . Favorite color = knowledge-based, same factor as password.

D . Mother's maiden name = weak knowledge-based, same factor as password.

Reference (CompTIA Network+ N10-009):

Domain: Network Security — Authentication methods, MFA categories.

Question: 382

A network engineer is configuring network ports in a public office. To increase security, the engineer wants the ports to allow network connections only after authentication. Which of the following security features should the engineer use?

A. Port security
B. 802.1X
C. MAC filtering
D. Access control list

Answer: B

Explanation:

802.1 X provides port-based Network Access Control (NAC). Ports remain in a blocked state until a device authenticates (usually with RADIUS). This is ideal for public or semi-public areas where ports should not be "always on."

A . Port security restricts by MAC addresses but does not authenticate users.

C . MAC filtering is easily spoofed and weaker than 802.1X.

D . ACLs filter traffic but do not enforce port-based authentication.

Reference (CompTIA Network+ N10-009):

Domain: Network Security — NAC, 802.1X authentication, port-based security.

Question: 383

Which of the following would an adversary do while conducting an evil twin attack?

A. Trick users into using an AP with an SSID that is identical to a legitimate network
B. Manipulate address resolution to point devices to a malicious endpoint
C. Present an identical MAC to gain unauthorized access to network resources
D. Capture data in transit between two legitimate endpoints to steal data

Answer: A

Explanation:

An evil twin attack sets up a rogue AP with the same SSID as a legitimate wireless network, tricking users into connecting.

Once connected, the attacker can intercept traffic or harvest credentials.

B . Describes ARP spoofing.

C . Describes MAC spoofing.

D . Describes on-path attacks, which may follow, but the evil twin method begins with SSID impersonation.

Reference (CompTIA Network+ N10-009):

Domain: Network Security — Wireless threats, rogue APs, evil twin.

Question: 384

A user recently moved a workstation to a different part of the office. The user is able to access the internet and print but is unable to access server resources. Which of the following is the most likely cause of the issue?

A. Incorrect default gateway
B. Wrong VLAN assignment
C. Error-disabled port
D. Duplicate IP address

Answer: B

Explanation:

If a workstation can access the internet and printers (likely in another VLAN) but not internal servers, the port was likely placed into the wrong VLAN after the move. VLAN assignment controls Layer 2 segmentation, restricting access to resources on different VLANs.

A . A wrong default gateway would prevent internet access.

C . An error-disabled port would block all connectivity.

D . A duplicate IP would cause general network issues, not just missing server access.

Reference (CompTIA Network+ N10-009):

Domain: Network Troubleshooting — VLAN misconfiguration, connectivity issues.

Question: 385

A network administrator needs to implement a solution to filter access to the internet. Which of the following should the administrator most likely implement?

A. Router
B. Cloud gateway
C. Proxy
D. Intrusion detection system

Answer: C

Explanation:

A proxy server can filter internet access by controlling which websites or services users can reach. It enforces content policies and can provide caching and monitoring.

A . A router directs traffic but doesn't filter internet sites by itself.

B . A cloud gateway could also filter, but the most direct answer is proxy.

D . An IDS detects suspicious activity but doesn't filter browsing access.

Reference (CompTIA Network+ N10-009):

Domain: Network Security — Proxy servers, filtering, access control.

Question: 386

A government entity wants to implement technology that can block websites based on country code. Which of the following will best enable this requirement?

A. URL filtering
B. Content filtering
C. DNS poisoning
D. MAC filtering

Answer: A

Explanation:

URL filtering can block access to websites based on their domain or country code TLDs (e.g., .cn, .ru).
This is the correct method to block by location identifiers in URLs.

B . Content filtering blocks based on keywords or categories within websites, not country code.

C . DNS poisoning is an attack, not a control mechanism.

D . MAC filtering restricts devices, not websites.

Reference (CompTIA Network+ N10-009):

Domain: Network Security — Filtering technologies, URL vs content filtering.

Question: 387

A network technician is requesting a fiber patch cord with a connector that is round and twists to install. Which of the following is the proper name of this connector type?

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

Answer: A

Explanation:

The ST (Straight Tip) fiber connector is round with a bayonet twist-lock mechanism. It is older but still used in some fiber installations.

B . BNC is a coaxial connector.

C . SC (Subscriber Connector) is a square push-pull fiber connector.

D . LC (Lucent Connector) is a small form-factor fiber connector.

Reference (CompTIA Network+ N10-009):

Domain: Networking Concepts — Fiber connectors (ST, SC, LC).

Question: 388

Which of the following actions should be taken as part of the first step of the troubleshooting methodology?

A. Conduct tests to verify ideas
B. Handle multiple problems individually
C. Create a theory about the possible root cause
D. Use a top-down approach

Answer: C

Explanation:

Question: 389

A new backup system takes too long to copy files to the new SAN each night. A network administrator makes a simple change to the network and the devices to decrease backup times. Which of the following does the network administrator change?

A. QoS
B. SDN
C. MTU
D. VXLAN
E. TTL

Answer: C

Explanation:

Increasing the MTU (Maximum Transmission Unit) size allows larger frames to be transmitted, reducing overhead and improving throughput — especially for large file transfers like backups.

A. QoS prioritizes traffic but doesn't reduce backup times directly.

B. SDN is a network management model, not a parameter change.

D. VXLAN encapsulates VLANs, not relevant to backup speeds.

E. TTL is for packet lifetime, not throughput.

Reference (CompTIA Network+ N10-009):

Domain: Network Infrastructure — MTU, jumbo frames, performance tuning.

Question: 390

A network engineer configures an application server so that it automatically adjusts resource allocation as demand changes. This server will host a new application and demand is not predictable. Which of the following concepts does this scenario demonstrate?

A. Scalability
B. Software as a Service
C. Hybrid cloud
D. Elasticity

Answer: D

Explanation:

Elasticity is the ability of a system (often in cloud environments) to automatically scale resources up or down in real time based on demand.

A . Scalability means the ability to grow over time but not necessarily dynamically.

B . SaaS is a service model, not a resource-allocation concept.

C . Hybrid cloud is a deployment model, not a performance behavior.

Reference (CompTIA Network+ N10-009):

Domain: Networking Concepts — Cloud computing, elasticity vs. scalability.

Question: 391

Which of the following allows an organization to map multiple internal devices to a single external-facing IP address?

A. NAT
B. BGP
C. OSPF
D. FHRP

Answer: A

Explanation:

NAT (Network Address Translation) allows multiple private IP addresses to share a single public IP when accessing the internet. This conserves public IPs and provides basic security by hiding internal addresses.

B . BGP is a routing protocol.

C . OSPF is a link-state IGP.

D . FHRP provides redundant gateways, not IP sharing.

Reference (CompTIA Network+ N10-009):

Domain: Networking Concepts — NAT, PAT, private-to-public IP mapping.

Question: 392

A user submits an escalated ticket regarding failed logins on their laptop. The user states that the time displayed on the laptop is incorrect. An administrator thinks the issue is related to the NTP. Which of the following should the administrator do next?

A. Create a plan of action
B. Implement a solution

C. Identify the problem

D. Test the theory

Answer: C

Explanation:

The first step of troubleshooting is always to identify the problem, which includes verifying the symptoms (incorrect time), asking the user clarifying questions, and checking system logs. Only after confirming the problem can the administrator proceed to form a theory and plan.

A . Plan of action is later.

B . Implement solution comes after testing a theory.

D . Test the theory requires a defined problem first.

Reference (CompTIA Network+ N10-009):

Domain: Network Troubleshooting — Troubleshooting methodology (Identify → Theory → Test → Plan → Implement → Verify → Document).

Question: 393

Which of the following most directly secures sensitive information on a network?

A. Data-in-transit encryption

B. Principle of least privilege C. Role-based access controls D. Multifactor authentication

Answer: A

Explanation:

The option that most directly secures sensitive information on the network is data-in-transit encryption. This ensures that data packets are unreadable to attackers who intercept them while moving across the network. Protocols such as TLS, HTTPS, IPsec, and SSH protect confidentiality and integrity of sensitive information.

B . Principle of least privilege (PoLP) secures access control but does not directly protect data in motion.

C . Role-based access control (RBAC) enforces permissions but again does not secure the data while transmitted.

D . Multifactor authentication (MFA) strengthens identity verification but does not directly protect the data itself once transmitted.

Thus, while all options contribute to overall security, encryption of data-in-transit most directly addresses protection of sensitive information on the network.

Reference (CompTIA Network+ N10-009):

Domain: Network Security — Encryption methods, confidentiality, data-in-transit protection.

Question: 394

A Chief Information Officer wants a DR solution that runs only after a failure of the primary site and can be brought online quickly once recent backups are imported. Which of the following DR site solutions meets these requirements?

A. Cold
B. Warm
C. Active
D. Hot

Answer: B

Explanation:

Comprehensive and Detailed Explanation (aligned to N10-009):

A warm site is partially configured with necessary infrastructure and systems, but it requires recent backups to be restored before becoming fully operational. This provides a balance between cost and recovery time.

A . Cold site has only power and space, requiring full setup, which takes too long.

C . Active (active-active) runs simultaneously with the primary site, not only during failure.

D . Hot site is fully operational at all times and can take over immediately, but it’s more expensive.

Reference (CompTIA Network+ N10-009):

Domain: Network Infrastructure — Disaster recovery sites (cold, warm, hot, active).

Question: 395

Which of the following connection methods allows a network engineer to automate the configuration deployment for network devices across the environment?

A. RDP
B. Telnet
C. GUI
D. API

Answer: D

Explanation:

Comprehensive and Detailed Explanation (aligned to N10-009):

APIs (Application Programming Interfaces) allow automation tools and scripts to push configurations to network devices programmatically. Modern network automation platforms rely on APIs to ensure consistency and scalability.

A . RDP is remote desktop for Windows systems, not automation.

B . Telnet is insecure and manual.

C . GUI requires manual configuration, not automation.

Reference (CompTIA Network+ N10-009):

Domain: Network Operations — Automation, orchestration, APIs in network management.

Question: 396

A systems administrator needs to connect two laptops to a printer via Wi-Fi. The office does not have access points and cannot purchase any. Which of the following wireless network types best fulfills this requirement?

A. Mesh
B. Infrastructure
C. Ad hoc
D. Point-to-point

Answer: C

Explanation:

Comprehensive and Detailed Explanation (aligned to N10-009):

An ad hoc wireless network allows devices to connect directly to each other without an access point. This is suitable for small, temporary setups like two laptops and a printer.

A . Mesh requires multiple nodes forming a larger distributed network.

B . Infrastructure requires an AP, which is not available here.

D . Point-to-point is typically for long-distance wireless links between two fixed endpoints.

Reference (CompTIA Network+ N10-009):

Domain: Networking Concepts — Wireless network types: infrastructure, ad hoc, mesh.

Question: 397

Which of the following network traffic types is sent to all nodes on the network?

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

Answer: B

Explanation:

Comprehensive and Detailed Explanation (aligned to N10-009):

A broadcast message is delivered to all nodes in a broadcast domain (e.g., ARP requests).

A . Unicast is one-to-one.

C . Multicast is one-to-many but only to subscribed members.

D . Anycast is one-to-one-of-many, sending to the nearest node.

Reference (CompTIA Network+ N10-009):

Domain: Networking Concepts — Traffic types: unicast, multicast, broadcast, anycast.

Question: 398

Which of the following concepts describes the idea of housing different customers in the same public cloud data center?

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

Answer: D

Explanation:

Comprehensive and Detailed Explanation (aligned to N10-009):

Multitenancy is a cloud concept where multiple customers share the same physical resources (servers, storage, and networks) but remain logically separated for security and privacy.

A . Elasticity is auto-scaling resources.

B . Hybrid cloud combines private and public resources.

C . Scalability is the ability to grow resources but doesn't imply multiple customers.

Reference (CompTIA Network+ N10-009):

Domain: Networking Concepts — Cloud computing models, multitenancy in public cloud.

Question: 399

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:

Comprehensive and Detailed Explanation (aligned to N10-009):

Multimode fiber uses multiple paths (modes) of light that bounce off the cladding to travel through the fiber. This is effective for shorter distances but more prone to dispersion.

A . Twinaxial is copper, not fiber.

B . Coaxial carries electrical signals, not light.

C . Single-mode fiber uses a single light path directly through the core without bouncing.

Reference (CompTIA Network+ N10-009):

Domain: Networking Concepts — Fiber optics: single-mode vs. multimode.

Question: 400

Which of the following standards enables the use of an enterprise authentication for network access control?

A. 802.1Q
B. 802.1X
C. 802.3bt
D. 802.11h

Answer: B

Explanation:

Comprehensive and Detailed Explanation (aligned to N10-009):

802.1 X provides port-based Network Access Control (NAC), requiring authentication (often through RADIUS) before granting access. This is the standard for enterprise authentication on both wired and wireless networks.

A . 802.1Q defines VLAN trunking.

C . 802.3bt defines higher-power PoE.

D . 802.11h deals with spectrum management in wireless.

Reference (CompTIA Network+ N10-009):

Domain: Network Security — NAC, 802.1X authentication.

Question: 401

A Linux server is running a log collector that needs to be hardened. A network administrator executes netstat to find open ports on the server. Which of the following ports should be disabled?

A. 22
B. 80
C. 162
D. 514

Answer: B

Explanation:

Comprehensive and Detailed Explanation (aligned to N10-009):

For a log collector server, the primary needed service is Syslog, which typically uses UDP port 514.

Other ports may be open for management (e.g., 22 for SSH) or SNMP traps (162) if integrated.

However, port 80 (HTTP) should not be open unless required, as it increases attack surface and does not directly serve the log collection purpose. Disabling it hardens the server.

A. 22 (SSH) is needed for secure management.

C. 162 (SNMP trap) may be required for monitoring/log correlation.

D. 514 (Syslog) is essential for log collection.

Reference (CompTIA Network+ N10-009):

Domain: Network Security — Hardening servers, disabling unnecessary services and ports.

Question: 402

A network administrator upgrades the wireless access points and wants to implement a configuration that gives users higher speed and less channel overlap based on device compatibility. Which of the following accomplishes this goal?

A. 802.1X
B. MIMO
C. ESSID
D. Band steering

Answer: D

Explanation:

The best solution here is band steering. Band steering allows modern wireless access points to automatically direct dual-band capable clients toward the 5 GHz band instead of the crowded 2.4 GHz band. The 5 GHz band has more available non-overlapping channels and can provide faster speeds with less interference, especially in dense environments. Devices that only support 2.4 GHz will remain on that band, while compatible devices enjoy the improved performance of 5 GHz.

A . 802.1X is a port-based network access control method for authentication. While important for

security, it does not affect wireless channel utilization or client throughput.

B . MIMO (Multiple Input, Multiple Output) is a technology that improves throughput by using multiple antennas to send/receive simultaneously, but it does not actively steer clients between frequency bands.

C . ESSID (Extended Service Set Identifier) is just the network name for a set of APs in the same WLAN; it has no role in optimizing performance by band.

By implementing band steering, administrators reduce channel overlap on the 2.4 GHz band, improve spectral efficiency, and provide higher performance to capable devices, directly meeting the requirements described in the scenario.

Reference (CompTIA Network+ N10-009):

Domain: Networking Concepts — Wireless optimization, band steering, dual-band client management.

Question: 403

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

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

Answer: B

Explanation:

The correct solution is a Data Center Interconnect (DCI). DCIs extend Layer 2 networks across geographically dispersed data centers, enabling seamless replication of services such as SAN storage, backup synchronization, or VM migrations. This ensures workloads and data can move between sites while maintaining the same VLANs and addressing.

A . Security Service Edge (SSE) provides cloud-delivered security functions like secure web gateways

and CASB, not Layer 2 extension.

C . Infrastructure as code (IaC) automates deployment and management of network infrastructure but is unrelated to extending Layer 2 domains.

D . Zero Trust architecture is a security framework ensuring strict access control but doesn't address network connectivity between sites.

In scenarios where backups need replication between sites, Layer 2 extension is often required so systems can communicate as if they are in the same broadcast domain. DCI is specifically designed to provide this functionality reliably and securely.

Reference (CompTIA Network+ N10-009):

Domain: Network Infrastructure — WAN technologies, data center interconnect, backup replication.

Question: 404

Which of the following types of network architecture typically uses leased lines to provide dedicated, private connections between multiple satellite offices and a head office?

A. Mesh
B. Point to point
C. Hub and spoke
D. Star

Answer: C

Explanation:

The correct answer is hub-and-spoke. In this design, the head office serves as the hub, and all satellite or branch offices (the spokes) connect directly to the hub using leased lines or VPNs. Communication between spokes typically passes through the hub, which centralizes connectivity and simplifies management.

A . Mesh involves every site connecting to every other site, which is more redundant but costly.

B . Point-to-point describes a single dedicated link between two sites, not a multi-site topology.

D . Star is often used in LAN switching, with all devices connecting to a central switch, but it's not the WAN architecture typically used here.

Hub-and-spoke is a cost-effective WAN design, as fewer circuits are needed compared to full mesh. However, its main disadvantage is reliance on the hub site: if the hub goes down, inter-spoke communication fails.

Reference (CompTIA Network+ N10-009):

Domain: Networking Concepts — WAN topologies (hub-and-spoke, mesh, point-to-point).

Question: 405

Which of the following is the best reason to create a golden configuration?

A. To provide configuration consistency

B. To decrease the size of configuration files
C. To increase security by encrypting configurations
D. To set up backup configurations for each device

Answer: A

Explanation:

A golden configuration is a baseline configuration file that contains approved, standardized settings for network devices. The purpose is to ensure configuration consistency across the environment. This prevents misconfigurations, supports compliance with organizational or regulatory standards, and accelerates recovery if a device needs reconfiguration.

B . Reducing file size is not the goal of golden configs.

C . Golden configs can include security settings, but they are not inherently encrypted — they are simply a baseline template.

D . While configs can be backed up, golden configs are more about standardization, not devicespecific backups.

By maintaining a golden configuration, administrators can quickly detect unauthorized changes (by comparing running configs against the golden file) and enforce consistency across devices. This

improves network stability, reduces troubleshooting complexity, and enhances security posture.

Reference (CompTIA Network+ N10-009):

Domain: Network Operations — Configuration management, golden images/configurations.

Question: 406

Developers want to create a mobile application that requires a runtime environment, developer tools, and databases. The developers will not be responsible for security patches and updates. Which of the following models meets these requirements?

A. Container as a service
B. Infrastructure as a service
C. Platform as a service
D. Software as a service

Answer: C

Explanation:

The correct answer is Platform as a Service (PaaS). PaaS provides developers with a ready-to-use platform that includes runtime environments, developer tools, middleware, and database services. Developers can focus on writing code while the provider handles security patches, updates, and infrastructure management.

A . CaaS (Containers as a Service) focuses on deploying and managing containerized applications, not providing full developer platforms.

B . IaaS delivers virtual machines, storage, and networking, but administrators must install and maintain the OS, middleware, and updates.

D . SaaS provides end-user applications (e.g., email, CRM), not platforms for development.

By using PaaS, the developers can build applications quickly and cost-effectively without worrying about underlying infrastructure or system maintenance.

Reference (CompTIA Network+ N10-009):

Domain: Networking Concepts — Cloud service models (IaaS, PaaS, SaaS, CaaS).

Question: 407

Which of the following is the best networking appliance for interconnecting multiple logical networks and forwarding data packets between them while minimizing latency?

A. Firewall
B. Router
C. Layer 2 switch
D. Load balancer

Answer: B

Explanation:

The correct appliance is a router, which is specifically designed to interconnect multiple networks and forward packets based on IP addresses. Routers operate at Layer 3 (Network layer) of the OSI model and make intelligent forwarding decisions to ensure data reaches the correct destination network.

A . Firewall can also forward traffic, but its primary function is security, not routing efficiency.

C . Layer 2 switches connect devices within the same LAN but do not forward packets between different networks without routing capability.

D . Load balancers distribute traffic among servers but are not general-purpose routers.

Modern enterprise routers are optimized to minimize latency by using fast switching and hardware acceleration, making them ideal for interconnecting logical networks securely and efficiently.

Reference (CompTIA Network+ N10-009):

Domain: Network Infrastructure — Routers, Layer 3 devices, inter-network communication.

Question: 408

A network administrator is conducting an assessment and finds network devices that do not meet standards. Which of the following configurations is considered a set of rules that devices should adhere to?

A. Production
B. Backup
C. Candidate
D. Golden

Answer: D

Explanation:

The correct answer is golden configuration. This is a reference standard or baseline that defines the approved settings and rules devices should follow. Any deviation from the golden configuration indicates drift or misconfiguration that must be remediated.

A . Production refers to the live environment but doesn't define a standard.

B . Backup configurations are stored copies, not the standard rules.

C . Candidate configuration is a proposed change being tested, not the final baseline.

By enforcing golden configurations, administrators ensure compliance, maintain security standards, and improve consistency across the enterprise.

Reference (CompTIA Network+ N10-009):

Domain: Network Operations — Configuration standards, golden images/configs.

Question: 409

Which of the following is an XML-based security concept that works by passing sensitive information about users, such as login information and attributes, to providers?

A. IAM
B. MFA
C. RADIUS
D. SAML

Answer: D

Explanation:

The correct answer is SAML (Security Assertion Markup Language). SAML is an XML-based standard used for single sign-on (SSO) and identity federation. It allows identity providers (IdPs) to share authentication and authorization data with service providers (SPs), passing secure tokens containing user attributes and credentials.

A . IAM (Identity and Access Management) is the broader framework, not specifically XML-based.

B . MFA enforces multiple factors for authentication but does not involve XML assertions.

C . RADIUS is an AAA protocol, but it uses UDP, not XML assertions.

SAML is widely used in federated identity systems, enabling secure authentication across different domains and applications without requiring multiple credentials.

Reference (CompTIA Network+ N10-009):

Domain: Network Security — Authentication methods, SAML, SSO.

Question: 410

A company's Chief Information Security Officer requires that servers and firewalls have accurate time stamps when creating log files so that security analysts can correlate events during incident investigations. Which of the following should be implemented?

A. Syslog server
B. SMTP
C. NTP
D. SNMP

Answer: C

Explanation:

The correct solution is NTP (Network Time Protocol). Accurate timestamps across servers, firewalls, and network devices are critical for correlating logs during incident response. NTP synchronizes device clocks to a trusted time source, ensuring consistency across the network.

A . Syslog centralizes logs but does not synchronize time.

B . SMTP is email transfer, unrelated to time.

D . SNMP monitors devices but does not correct time discrepancies.

By implementing NTP, analysts can ensure that logs from different devices are time-aligned, which is essential for reconstructing attack timelines and detecting anomalies.

Reference (CompTIA Network+ N10-009):

Domain: Network Operations — Time synchronization, NTP, log correlation.

Question: 411

Which of the following is used most often when implementing a secure VPN?

A. IPSec
B. GRE

C. BGP

D. SSH

Answer: A

Explanation:

The most common protocol for secure VPNs is IPsec (Internet Protocol Security). IPsec provides confidentiality, integrity, and authentication for VPN traffic, typically using ESP (Encapsulating Security Payload). It is used in both site-to-site and remote access VPNs.

B . GRE encapsulates traffic but does not provide encryption.

C . BGP is a routing protocol, not a VPN technology.

D . SSH can be used for secure tunneling but is not the standard for VPN deployment.

IPsec is the industry standard because it operates at Layer 3, securing IP traffic regardless of the application, making it highly versatile.

Reference (CompTIA Network+ N10-009):

Domain: Network Security — VPN protocols, IPsec, ESP.

Question: 412

A security administrator is creating a new firewall object for a device with IP address 192.168.100.1/25. However, the firewall software only uses dotted decimal notation in configuration fields. Which of the following is the correct subnet mask to use?

A. 255.255.254.0

B. 255.255.255.1

C. 255.255.255.128

D. 255.255.255.192

Answer: C

Explanation:

A /25 subnet mask means 25 bits are reserved for the network portion, leaving 7 bits for host addresses. In dotted decimal, that is:

11111111.11111111.11111111.10000000

Decimal equivalent: 255.255.255.128

A . 255.255.254.0 corresponds to /23.
B . 255.255.255.1 is invalid as a subnet mask.

D . 255.255.255.192 corresponds to /26.

Thus, the correct subnet mask for a /25 network is 255.255.255.128.

Reference (CompTIA Network+ N10-009):
Domain: Networking Concepts — Subnetting, CIDR notation, dotted decimal.

Question: 413

Which of the following cloud deployment models is most commonly associated with multitenancy and is generally offered by a service provider?

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

Answer: C

Explanation:

The correct answer is public cloud. In public cloud models, a provider (such as AWS, Azure, or Google Cloud) hosts

infrastructure and services that are shared across multiple customers, known as multitenancy. Each tenant is logically isolated, but physical infrastructure is shared, allowing providers to achieve economies of scale.

A . Private cloud is dedicated to one organization, not multitenant.

B . Community cloud is shared among organizations with common interests, but it's less common than public multitenancy.

D . Hybrid cloud combines private and public but does not define tenancy alone.

Public cloud services are the most cost-effective and scalable because they spread costs across many customers, but they require strong security and isolation to protect tenants.

Reference (CompTIA Network+ N10-009):

Domain: Networking Concepts — Cloud models, multitenancy, public vs private.

Question: 414

A company recently experienced outages of one of its critical, customer-facing applications. The root cause was an overutilized network router, but the Chief Technology Officer is concerned that the support staff was unaware of the issue until notified by customers. Which of the following is the best way to address this issue in the future?

A. Packet capture
B. SNMP
C. Syslog collector
D. SIEM

Answer: B

Explanation:

The best answer is SNMP (Simple Network Management Protocol). SNMP enables monitoring of network devices (routers, switches, firewalls, servers) and provides performance data such as CPU usage, bandwidth utilization, and interface status. In this scenario, if SNMP monitoring had been in place, administrators would have received alerts that the router was overutilized before customers noticed outages.

A . Packet capture (e.g., Wireshark) is useful for deep troubleshooting but is reactive, not proactive, and not scalable for continuous monitoring.

C . Syslog collects log messages but generally does not provide proactive resource utilization metrics. It is

complementary but not the best fit for this problem.

D . SIEM aggregates logs and security events for analysis, but the primary requirement here is performance and availability monitoring.

By implementing SNMP monitoring (and potentially integrating it with a network monitoring tool such as Nagios, PRTG, or SolarWinds), the organization can track utilization trends, set thresholds, and automatically generate alerts, thereby preventing downtime from going unnoticed.

Reference (CompTIA Network+ N10-009):

Domain: Network Operations — SNMP monitoring, proactive network performance management.

Question: 415

An organization is struggling to get effective coverage using the wireless network. The organization wants to implement a solution that allows for continuous connectivity anywhere in the facility.

Which of the following should the network administrator suggest to ensure the best coverage?

A. Implementing additional ad hoc access points
B. Providing more Ethernet drops for user connections
C. Deploying a mesh network in the building
D. Changing the current frequency of the Wi-Fi

Answer: C

Explanation:

The correct answer is deploying a mesh network. A mesh wireless network uses multiple interconnected access points that automatically route traffic through the best available path. This ensures seamless coverage throughout a facility, even when users move between APs. Mesh APs can extend coverage without requiring each AP to be directly wired, making them ideal for large or hard- to-wire environments.

A . Ad hoc access points are peer-to-peer connections and cannot provide enterprise-grade continuous coverage.

B . Ethernet drops provide wired connectivity but do not solve wireless coverage issues.

D . Changing the frequency (from 2.4 GHz to 5 GHz or vice versa) may reduce interference but will not guarantee building-wide seamless connectivity.

Mesh networks are particularly effective in environments with roaming devices (smartphones, tablets, handheld

scanners) and ensure that there are no dead spots, thereby delivering continuous wireless access.

Reference (CompTIA Network+ N10-009):

Domain: Network Infrastructure — Wireless architectures, mesh networking, seamless connectivity.

Question: 416

A network technician is adding a new switch to increase capacity on the network. The technician connects the two switches using a single cable. Several hosts are moved to the new switch, but none of the hosts can access the network or internet. Which of the following should the technician do to resolve the issue?

A. Configure the connecting ports as trunk ports
B. Install STP cables between the switches
C. Increase the PoE budget for the switches
D. Set up link aggregation on the uplink ports

Answer: A

Explanation:

The correct solution is to configure the connecting ports as trunk ports. When connecting switches, the uplink ports must be configured to carry traffic for multiple VLANs (trunking), not just a single access VLAN. Without trunking, VLAN tags may be dropped, and traffic from hosts will not reach the rest of the network or internet.

B . STP cables is a misnomer — STP refers to Spanning Tree Protocol or Shielded Twisted Pair cables, neither of which solves this logical configuration issue.

C . PoE budget is irrelevant because switches and hosts in this context don't require PoE.

D . Link aggregation (LACP, EtherChannel) is for increasing bandwidth/redundancy across multiple links, not required with a single cable.

By enabling trunking on the uplink ports, the switches can pass VLAN-tagged traffic, ensuring hosts connected to the new switch have access to the same resources as those on the existing switch.

Reference (CompTIA Network+ N10-009):

Domain: Network Troubleshooting — VLAN trunking, inter-switch connectivity.

Question: 417

Which of the following objectives does an evil twin achieve?

A. DNS poisoning
B. Login credentials
C. ARP spoofing
D. Denial of service

Answer: B

Explanation:

An evil twin attack is when an attacker sets up a rogue access point (AP) with the same SSID as a legitimate one to trick users into connecting. Once users connect, attackers often present fake login pages or capture unencrypted session data to steal login credentials.

A . DNS poisoning manipulates DNS resolution but is not inherent to evil twin.

C . ARP spoofing is a Layer 2 attack involving MAC/IP mapping manipulation.

D . Denial of service can be a side effect but is not the primary objective of evil twin attacks.

The main purpose of an evil twin is credential theft, enabling further unauthorized access to networks or systems.

Reference (CompTIA Network+ N10-009):

Domain: Network Security — Wireless attacks, rogue APs, evil twins.

Question: 418

Which of the following internal routing protocols is best characterized as having fast convergence and being loop-free?

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

Answer: C

Explanation:

The correct answer is OSPF (Open Shortest Path First). OSPF is a link-state routing protocol known for its fast convergence and use of the Dijkstra algorithm to calculate the shortest loop-free path. It efficiently scales to large enterprise networks and avoids routing loops by maintaining a complete topology map.

A . BGP is primarily an external routing protocol used between ISPs, not internal.

B . STP is not a routing protocol; it prevents loops at Layer 2.

D . RIP is an older distance-vector protocol with slower convergence and a maximum hop limit of 15.

OSPF's design makes it the preferred internal gateway protocol (IGP) for medium-to-large organizations requiring speed and loop-free reliability.

Reference (CompTIA Network+ N10-009):

Domain: Networking Concepts — IGPs, OSPF, routing protocols.

Question: 419

A support engineer is troubleshooting a network outage that is affecting 3,000 users. The engineer has isolated the issue to the internet firewall. Packet captures confirm that the firewall is blocking the traffic. Which of the following is the next step in troubleshooting?

A. Implement the solution or escalate as necessary
B. Create a plan of action to resolve the issue and identify potential effects
C. Establish a theory of probable cause
D. Document findings, actions, outcomes, and lessons learned throughout the process

Answer: B

Explanation:

The troubleshooting methodology requires following a logical sequence. In this case, the engineer has already identified the problem (firewall blocking traffic) and confirmed it with evidence (packet captures). The next appropriate step is to create a plan of action that outlines how to resolve the issue and considers potential effects.

A . Implementing the solution is premature without planning.

C . Establishing a theory was already completed during problem isolation.

D . Documentation occurs after resolution.

By carefully planning, the engineer ensures that corrective action won't cause additional outages or security issues, especially given the scale of the incident (3,000 users).

Reference (CompTIA Network+ N10-009):

Domain: Network Troubleshooting — Troubleshooting methodology, plan of action.

Question: 420

Which of the following technologies is most appropriate for a business that requires high-speed access to frequently used web content, such as images and videos?

A. CDN
B. SAN
C. Firewall
D. Switch

Answer: A

Explanation:

The correct solution is a Content Delivery Network (CDN). A CDN caches web content (like images, videos, scripts) on distributed servers close to end users. This reduces latency, improves load times, and decreases the load on origin servers. For a business requiring high-speed access to media-rich content, a CDN is the most effective option.

B . SAN (Storage Area Network) is used for storage in a data center, not for distributing web content.

C . Firewall secures traffic but doesn't accelerate content delivery.

D . Switches forward packets within a LAN, not globally distribute content.

By leveraging CDNs, businesses can handle large traffic volumes efficiently while improving user experience.

Reference (CompTIA Network+ N10-009):

Domain: Network Infrastructure — CDNs, caching, performance optimization.

Question: 421

A network technician installs a new 19.7ft (6m), Cat 6, UTP cable for the connection between a server and a switch. Communication to the server is degraded, and the NIC statistics show dropped packets and CRC errors. Which of the following cables would the technician most likely use instead to reduce the errors?

A. Coaxial cable
B. 9.8ft (3m) cable
C. Plenum cable
D. STP cable

Answer: D

Explanation:

The errors described — dropped packets and CRC (Cyclic Redundancy Check) errors — often indicate electromagnetic interference (EMI) on unshielded twisted pair (UTP) cabling. The correct replacement is STP (Shielded Twisted Pair), which has shielding that protects signals from external interference, ensuring better reliability in noisy environments such as data centers or near heavy electrical equipment.

A . Coaxial is not used for modern Ethernet server-switch links.

B . Shorter UTP cable does not solve EMI issues.

C . Plenum cable refers to cable jacket type for fire safety, not electrical shielding.

STP cabling reduces interference and ensures reliable gigabit+ Ethernet connections between servers and switches.

Reference (CompTIA Network+ N10-009):

Domain: Network Troubleshooting — Cabling issues, UTP vs. STP, EMI.

Question: 422

Which of the following best describes the amount of time between a disruptive event and the point that affected

resources need to be back to fully functional status?

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

Answer: A

Explanation:

The correct metric is RTO (Recovery Time Objective). RTO defines the maximum acceptable time to restore services after a disruption, ensuring business continuity. For example, if the RTO is 4 hours, systems must be back online within that timeframe after an outage.

B . MTBF (Mean Time Between Failures) measures reliability by calculating the average time between hardware failures.

C . RPO (Recovery Point Objective) defines how much data loss (in terms of time, such as last backup point) is acceptable.

D . MTTR (Mean Time to Repair) measures the average time taken to fix a failure but is not a predefined business requirement like RTO.

Organizations define RTOs during disaster recovery planning to align IT recovery capabilities with business needs.

Reference (CompTIA Network+ N10-009):

Domain: Networking Concepts — Business continuity metrics (RTO, RPO, MTBF, MTTR).