DUMPSARENA

CompTIA Network+ Certification Exam

CompTIA N10-009

Version Demo

Total Demo Questions: 63

Total Premium Questions: 701

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Networking Concepts	93
Topic 2, Network Implementation	177
Topic 3, Network Operations	81
Topic 4, Network Security	180
Topic 5, Network Troubleshooting	169
Topic 6, Mix Questions	1
Total	701

QUESTION NO: 1

Network administrators are using the Telnet protocol to administer network devices that are on the 192.168.1.0 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 is the appropriate tool because it is designed for network discovery and service enumeration across an IP address range. An administrator can scan the 192.168.1.0 subnet—for example, as 192.168.1.0/24—to identify responsive hosts and determine which TCP or UDP services they expose. Since the devices are administered using Telnet, a scan can specifically check TCP port 23, helping identify systems that are likely to be reachable through Telnet. A command such as `nmap -p 23 192.168.1.0/24` checks the subnet for hosts with the Telnet port available, while a host-discovery scan can first identify active addresses. Nmap also provides useful service-detection capabilities when deeper validation is appropriate and authorized. This makes it well suited to inventorying network devices on a defined subnet and locating systems offering a particular management service. Administrators should ensure that scans are authorized and scheduled appropriately, because discovery and port-scanning traffic can trigger monitoring alerts or affect fragile devices. Nmap's official documentation describes host discovery methods and port scanning behavior at Nmap Network Discovery and Nmap Port Scanning Basics.

QUESTION NO: 2

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:

Inspect the connectors for any wires that are touching or exposed. is the appropriate first troubleshooting action because near-end crosstalk is frequently introduced at cable termination points. Twisted-pair cabling relies on each pair's twist rate and physical separation to limit electromagnetic coupling between pairs. When installing passthrough plugs, excessive untwisting near the connector, poor conductor positioning, exposed copper, or an uneven trim can degrade that separation at exactly the point where the pairs enter the plug.

A visual inspection is the least disruptive first step and can quickly identify workmanship issues that are directly relevant to the reported symptom. The electrician should verify that conductors are fully seated in their intended channels, that no bare conductor is exposed outside the plug, that the cable jacket is brought sufficiently into the connector and strain relief, and that pair twists have been maintained as close to the termination as practicable. Correct connector preparation is especially important for Category 8, whose higher operating frequencies make it more sensitive to termination quality. This inspection can identify an immediately correctable source before more invasive remediation is performed. Fluke Networks describes crosstalk as unwanted signal coupling between cable pairs and notes the importance of cabling performance measurements: Fluke Networks: What Is Crosstalk?. For Category 8 cabling requirements and performance context, see TIA Standards.

QUESTION NO: 3

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

E. Link Aggregation Control Protocol (LACP)

ANSWER: E

Explanation:

Link Aggregation Control Protocol (LACP) is correct because it combines multiple physical Ethernet links into one logical aggregated link, commonly called a link aggregation group or port channel. For 100 Mbps switch uplinks, this allows traffic to be distributed across the member links, increasing the aggregate bandwidth available between the switches while also providing resiliency if an individual member link fails. LACP is the standards-based dynamic negotiation protocol for Ethernet link aggregation, defined by IEEE 802.1AX. Both switches must be configured with compatible aggregation settings, and member ports should have matching operational characteristics such as speed and duplex. Traffic distribution is normally based on a hash of fields such as source and destination MAC or IP addresses, so a single flow does not necessarily exceed the speed of one physical member link; however, multiple flows can use the combined capacity of the bundle. The logical treatment of the grouped interfaces also enables the switching topology to use the aggregate connection without treating each member as an independent redundant path. Cisco's overview of EtherChannel and LACP is available in Cisco's EtherChannel configuration guide, and the IEEE standards listing for 802.1AX is available from the IEEE 802.1AX standard page.

QUESTION NO: 4

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 D

Explanation:

5GHz frequency is an appropriate mitigation because it moves WLAN communications away from the congested 2.4 GHz industrial, scientific, and medical band. Industrial equipment and other unlicensed devices may generate energy in that spectrum, so using 5 GHz-capable access points and clients can avoid the affected band entirely. The 5 GHz band also provides substantially more usable Wi-Fi channels, enabling more flexible RF design and channel separation. Cisco's wireless design guidance discusses the greater channel availability in 5 GHz: Cisco 802.11ac Wireless LAN Design Guide.

Non-overlapping channel is also a valid mitigation when devices must continue to use 2.4 GHz. Selecting a non-overlapping Wi-Fi channel reduces adjacent-channel interference caused by overlapping channel assignments. In common

North American 2.4 GHz WLAN deployments, channels 1, 6, and 11 are the standard non-overlapping channel plan. This allows the wireless network to use the available spectrum more efficiently and limits interference between nearby access points and clients, improving reliability in an already challenging RF environment. The channel allocations are documented in Cisco's overview of WLAN radio-frequency basics.

QUESTION NO: 5

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:

Jump box is correct because it is a secured, tightly controlled intermediary system used to administer hosts that reside in isolated or otherwise restricted network segments. An authorized user first establishes a connection to the jump box, then uses that host as the managed access point to reach the isolated device. This design avoids exposing administrative interfaces on sensitive systems directly to broader user networks and centralizes access enforcement.

In practice, a jump box is hardened and configured with strict authentication, authorization, network filtering, session controls, and audit logging. It may have one interface or permitted route toward the administrative network and another toward the protected stand-alone segment, allowing only the specifically approved management traffic to traverse that boundary. Administrators can therefore access a device that is not intended to be directly reachable from their workstation, while security teams gain a single chokepoint for monitoring and controlling privileged activity.

This architecture aligns with NIST guidance to use managed, secure remote-access paths and to restrict access to organizational systems. NIST's Guide to Enterprise Telework, Remote Access, and BYOD Security discusses securing remote-access solutions, while the NIST glossary definition of a bastion host describes a strongly protected host exposed to untrusted networks, a role commonly associated with jump-box deployments.

QUESTION NO: 6

Which of the following are commonly used in Windows-based environments to facilitate file transfers between clients and network shares? Select two.

A. Port 21

B. Port 443

C. Port 445

D. HTTPS

E. SMB

ANSWER: C E

Explanation:

SMB and port 445 are the standard pairing for Windows clients accessing files on network shares. Server Message Block (SMB) is the application-layer protocol Windows uses to provide shared-folder access across a network. When a user opens a Universal Naming Convention path such as `\\fileserver\department`, browses folders, reads or saves a document, or applies share and NTFS permissions, those operations are typically handled through SMB. Modern SMB implementations use direct hosting over TCP, for which TCP port 445 is the well-known listening port. Thus, identifying both SMB and port

445 demonstrates knowledge of the protocol itself and the port normally used to reach the service. SMB also supports related Windows network-sharing capabilities, including authenticated access, file locking, and printer sharing, making it central to file services in Windows-based enterprise networks. Microsoft's SMB documentation describes SMB as the protocol used for network file sharing and notes its role in client-server file operations. Microsoft's networking guidance also identifies TCP 445 as the port used by SMB directly over TCP/IP. See Microsoft's SMB overview and Microsoft's service and port requirements.

QUESTION NO: 7

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:

802.11ac wireless bridge is the most appropriate solution because a point-to-point wireless bridge can connect the LANs of two separate buildings without requiring a physical cable route beneath or above a public street. Bridge devices are installed at each building, typically using directional antennas with clear line of sight, and form a dedicated wireless link that carries Ethernet traffic between the sites. This approach is especially practical for nearby facilities because it avoids the civil work, right-of-way coordination, permitting, and installation costs commonly associated with deploying an interbuilding cable path. An 802.11ac-based bridge operates in the 5 GHz band and can provide substantial throughput for normal office connectivity when it is properly planned, aligned, secured, and protected from environmental exposure. Network+ objectives include selecting appropriate wireless technologies and connectivity solutions based on site requirements. Cisco describes wireless bridges as devices that connect networks at different physical locations over wireless links in its wireless bridge documentation. The current Network+ exam objectives are available from CompTIA Exam Objectives.

QUESTION NO: 8

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 is traffic transmitted by one device to every device within the same Layer 2 broadcast domain. A sender uses a broadcast destination address, causing switches to flood the frame through applicable ports on the local network segment. Each receiving host examines the frame, and the host for which the request is relevant can respond. Broadcasts are therefore used when a sender needs to reach an unknown or not-yet-identified local recipient. For example, an IPv4 host commonly uses an ARP request to discover the MAC address associated with a known local IPv4 address. The ARP request is sent using the Ethernet broadcast MAC address, FF:FF:FF:FF:FF:FF, so all nodes in that broadcast domain receive it. IPv4 DHCP clients also use broadcast communication during initial address configuration because they may not yet have an IP address or know the DHCP server's address. Routers normally do not forward Layer 2 broadcasts between networks, which limits the scope of broadcast traffic to the local broadcast domain. This behavior is central to network segmentation:

placing hosts in separate VLANs or routed subnets creates separate broadcast domains. Cisco's overview of Ethernet frame fields describes the broadcast MAC address and its use for delivering frames to all devices on a LAN, while the IETF ARP specification defines ARP request behavior on local networks. See Cisco Ethernet technology resources and RFC 826: Address Resolution Protocol.

QUESTION NO: 9

A company is connecting its network to two different ISPs. The company needs to advertise its public network prefix and influence the path used for Internet traffic. Which of the following should the network administrator configure? (Select two.)

A. BGP

B. Autonomous system number

C. OSPF area

D. DHCP scope

E. Spanning Tree priority

ANSWER: A B

Explanation:

BGP is the appropriate routing protocol because it is used to exchange reachability information between autonomous systems on the Internet. An organization with connections to multiple ISPs can use BGP to advertise its public prefixes and apply routing policy to influence inbound and outbound traffic paths.

An **autonomous system number** is also required to identify the organization as a distinct routing domain when establishing external BGP sessions. BGP uses AS-path information to support routing-policy decisions and help prevent loops between autonomous systems. The protocol is defined in RFC 4271: A Border Gateway Protocol 4 (BGP-4).

QUESTION NO: 10

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 appropriate technology for a high-density university wireless LAN because it combines the capacity and efficiency enhancements of Wi-Fi 6 (IEEE 802.11ax) with access to the 6 GHz spectrum. The additional spectrum provides more non-overlapping channels than the traditionally congested 2.4 GHz and 5 GHz bands, enabling a campus to design for greater aggregate capacity and reduced co-channel contention. This is particularly valuable in lecture halls, libraries, residence buildings, and student common areas where many clients may concurrently use video conferencing, cloud applications, streaming, and large downloads.

Wi-Fi 6E access points also use Wi-Fi 6 capabilities such as orthogonal frequency-division multiple access (OFDMA), multi-user MIMO, and improved scheduling efficiency. These features allow an access point to serve numerous clients more effectively and reduce latency under heavy load. A university would still perform an RF site survey and capacity-based

access-point design, but Wi-Fi 6E is a strong technology choice when device density and bandwidth requirements are central concerns. The Wi-Fi Alliance describes Wi-Fi 6E and its use of the 6 GHz band at Wi-Fi 6E. Cisco also outlines the capacity and spectrum benefits at What Is Wi-Fi 6E?

QUESTION NO: 11

A network administrator needs a monitoring solution that records network-device events centrally and provides immediate notification when an interface changes state. Which of the following should the administrator configure? (Select two.)

A. Syslog

B. SNMP traps

C. NAT

D. ARP inspection

E. DHCP relay

ANSWER: A B

Explanation:

Syslog is appropriate for central event recording because network devices can send log messages to a centralized syslog server. These messages can include authentication events, configuration changes, interface errors, and system failures.

SNMP traps provide asynchronous notifications from managed devices to a monitoring system. Rather than waiting for the monitoring platform to poll a device, a switch or router can send a trap when an important event occurs, such as an interface transition. Together, syslog and SNMP traps provide centralized logging and timely event notification. See RFC 5424 for syslog and RFC 3418 for SNMP notification definitions.

QUESTION NO: 12

A network engineer is designing a secure wireless network for employees. The company requires strong encryption and individual user authentication through a centralized identity service. Which of the following should the engineer implement? (Select two.)

A. WPA3-Enterprise

B. RADIUS

C. WEP

D. MAC filtering

E. A pre-shared key

F. An open SSID

ANSWER: A B

Explanation:

WPA3-Enterprise and **RADIUS** meet the requirements. WPA3-Enterprise is designed for enterprise WLAN environments and supports strong security with authentication based on IEEE 802.1X. Unlike a shared pre-shared key deployment, enterprise authentication can validate users individually.

RADIUS provides the centralized authentication service used by the wireless infrastructure to validate credentials and return authorization information. This gives administrators centralized identity management, individual accountability, and the ability to revoke access for a specific user without changing a shared wireless password. The Wi-Fi Alliance describes WPA3 Enterprise security capabilities in its Wi-Fi security overview, and RADIUS is specified in RFC 2865.

QUESTION NO: 13

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 are assigned to an incorrect VLAN.

C. Ports are having an MDIX issue.

D. Ports are trunk ports.

ANSWER: B

Explanation:

Ports are assigned to an incorrect VLAN is the most likely reason because the workspaces were previously occupied and their switch ports may still retain the former occupants' access-VLAN assignments. A switch access port places untagged traffic from a connected workstation into its configured VLAN. If a moved user connects to a port assigned to a different department, subnet, or security zone, the workstation can be placed on the wrong Layer 2 broadcast domain. Consequently, it may be unable to obtain an appropriate DHCP address, reach its expected default gateway, or access resources intended for its assigned network.

The timing and scope strongly support a retained port-configuration issue: connectivity problems affect the users specifically after they connect at previously used locations. Administrators should verify the access VLAN configured on each affected switch interface, compare it with the VLAN required for the users' network, and update the interface configuration where necessary. On Cisco switches, the access VLAN is configured per interface with the `switchport access vlan` command. Cisco's VLAN configuration guidance describes assigning a switch port to an access VLAN: Cisco VLAN Configuration Guide. CompTIA's Network+ exam objectives also include configuring and verifying VLANs: CompTIA Exam Objectives.

QUESTION NO: 14

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:

Incorrect QoS settings and network congestion are the most likely causes because the symptoms began immediately after deployment of a bandwidth-intensive, real-time application. Videoconferencing produces sustained traffic streams and is highly sensitive to delay, jitter, and packet loss. If available WAN, internet, switch-uplink, or wireless capacity is insufficient for the added video workload, traffic queues fill and packets wait longer to be transmitted. This congestion affects all applications sharing the constrained link, resulting in slow internet access and reduced overall network performance.

Correct quality-of-service configuration helps control this impact by classifying and marking real-time traffic, then applying appropriate queuing and bandwidth policies at congestion points. Proper QoS allows latency-sensitive videoconference traffic to receive predictable treatment while preventing it from consuming all available capacity needed by other business services. In particular, traffic markings such as DSCP provide a standard mechanism for communicating forwarding treatment across a network, although the network must also have sufficient capacity; QoS manages contention rather than creating additional bandwidth. These causes align directly with the timing, high-bandwidth workload, and network-wide performance symptoms described. See Cisco's DSCP and QoS guidance and RFC 2474: Differentiated Services Field.

QUESTION NO: 15

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 C

Explanation:

Fire suppression system and **Humidity control** are environmental considerations for network-equipment installations. Fire detection and suppression affect both personnel safety and the protection of network infrastructure. Equipment rooms, telecommunications spaces, and areas containing concentrated power and cabling should be evaluated for appropriate fire protection as part of facility planning. The selected suppression approach must align with the room's use, local building requirements, and the need to limit damage and downtime during an incident.

Humidity control is equally important because electronic equipment operates most reliably within an appropriate, stable environmental range. Excessive humidity can contribute to condensation and corrosion, while insufficient humidity increases the likelihood of electrostatic discharge. Both conditions can damage components, reduce reliability, and create intermittent faults that are difficult to diagnose. Maintaining controlled humidity, along with suitable temperature and airflow, helps preserve equipment availability and service life.

These considerations fit Network+ installation planning because they address physical conditions in the building that directly affect the safety and dependable operation of installed network devices. See the CISA data center security guidance and the EPA data center energy-efficiency resources for facility-environment planning guidance.

QUESTION NO: 16

A company permits employees to use personally owned mobile devices to access email and internal applications. Which of the following should the company implement to control device access and enforce security policies? (Select two.)

A. Network access control

B. Mobile device management

C. Port forwarding

D. Link aggregation

E. DHCP reservation

ANSWER: A B

Explanation:

Network access control can evaluate a device before granting network access. NAC policies can verify factors such as device identity, authentication status, security posture, and authorization requirements before placing the endpoint on an appropriate network segment.

Mobile device management allows the organization to apply and enforce security policies on enrolled mobile devices. MDM capabilities can include screen-lock requirements, encryption enforcement, application controls, configuration management, and remote removal of organizational data when appropriate. Together, NAC and MDM provide network-level access enforcement and device-level policy management. NIST discusses mobile-device security controls in SP 800-124 Rev. 2.

QUESTION NO: 17

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:

tracert and **route print** are the most appropriate commands for investigating loss of access to an external server immediately after a VPN connection is established. A VPN client can alter the endpoint's routing behavior by installing routes for protected networks, changing the default gateway, or applying a full-tunnel policy that sends all nonlocal traffic through the VPN gateway. These changes can prevent traffic from following the expected path to an external destination.

route print displays the Windows IP routing table. A support agent can use it to verify the active default route, identify VPN-added routes, check route metrics, and determine whether a more-specific route is directing traffic for the external server into the tunnel. This directly evaluates the client-side forwarding decision made after the VPN connects.

tracert identifies the sequence of Layer 3 hops toward the external server. Comparing a trace before and after the VPN connection helps reveal whether traffic is being sent to the VPN gateway, reaches an unexpected network boundary, or stops at a particular hop. Together, the routing-table view and path trace provide an effective way to isolate a VPN-related routing or reachability issue. See Microsoft's route command documentation and Microsoft's tracert command documentation.

QUESTION NO: 18

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 is correct because an EIGRP process is associated with an autonomous system number, and that number is a fundamental part of establishing an EIGRP neighbor relationship in classic EIGRP operation. On directly connected routers, EIGRP Hello packets advertise the autonomous system information. To become neighbors and exchange routing information, the routers must be configured to participate in the same EIGRP autonomous system on the shared network. The autonomous system value identifies the EIGRP routing domain and ensures that routers form adjacencies only with devices intended to participate in that same EIGRP domain. This configuration is commonly entered when enabling the EIGRP routing process, such as with the Cisco IOS command `router eigrp <autonomous-system-number>`. Once matching EIGRP parameters are in place and Hello packets are successfully exchanged, the devices can establish an adjacency, exchange topology information, and calculate routes using the Diffusing Update Algorithm. Cisco's EIGRP documentation describes the autonomous system number as an EIGRP configuration requirement and explains its role in neighbor operation. See Cisco: EIGRP Overview and Cisco IOS EIGRP Overview.

QUESTION NO: 19

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:

Protocol analyzer is correct because inconsistent delay in Real-time Transport Protocol packet arrival is jitter, a primary cause of degraded VoIP audio. A protocol analyzer such as Wireshark captures packets and examines the RTP stream at the packet level, including sequence numbers, timestamps, arrival-time variation, packet loss, and packets received out of order. These measurements enable the administrator to validate whether jitter is present, quantify its severity, and correlate it with the time period in which the caller experienced distorted, choppy, or intermittent audio. Wireshark's Telephony features can identify RTP streams and provide RTP stream analysis, including calculated jitter and loss information. This makes packet capture and RTP analysis an appropriate troubleshooting method when the observed symptom is inconsistent packet arrival timing rather than a physical-cable or signal-location problem. RTP is specifically designed for real-time media transport, and its sequence numbers and timestamps support monitoring delivery characteristics that affect real-time audio quality. Reviewing the captured stream can also provide the evidence needed to continue troubleshooting QoS handling, congestion, routing changes, or an unreliable network segment. See the Wireshark User's Guide: Telephony and RFC 3550: RTP—A Transport Protocol for Real-Time Applications.

QUESTION NO: 20

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

Explanation:

QoS is the appropriate feature because voice over IP is highly sensitive to latency, packet loss, and especially jitter—the variation in packet arrival time. QoS lets the engineer classify voice packets and apply policies that give them preferential

treatment when a link or device is congested. In practice, voice traffic can be marked with an appropriate Differentiated Services Code Point value and placed into a low-latency or priority queue. This helps ensure that time-sensitive RTP voice packets are transmitted promptly instead of waiting behind large data transfers, reducing delay variation and making packet delivery more consistent. QoS policies can also reserve or manage bandwidth and use queueing mechanisms designed to protect real-time traffic. These measures improve perceived call clarity and reduce symptoms such as choppy audio, gaps, and distorted speech. QoS must be configured consistently across relevant network paths, particularly at WAN links and other congestion points, so that traffic markings and priority treatment are preserved end to end. Cisco's QoS overview describes QoS as a means to manage network resources and provide preferential handling for selected traffic types, including delay-sensitive voice traffic: Cisco QoS documentation. CompTIA's Network+ exam objectives also include configuring QoS to support voice, video, and other real-time services: CompTIA exam objectives.

QUESTION NO: 21

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:

Least privilege network access is a foundational security control because it grants each user, device, service, or application only the permissions needed to perform its approved task. Following a breach, reducing excessive privileges limits an attacker's ability to move laterally, access sensitive systems, or expand a compromised account's impact. This approach should be applied consistently to administrative access, shared resources, applications, and network segmentation decisions.

Central policy management is also an effective organization-wide improvement because it provides a consistent way to define, distribute, enforce, review, and update security policies across network infrastructure. Centralized management helps ensure that access rules, authentication requirements, device configurations, and security baselines are applied uniformly rather than relying on separate, potentially inconsistent local settings. It also supports faster remediation after an incident by allowing administrators to implement approved policy changes broadly and verify compliance. Together, these controls reduce unnecessary access and improve the consistency and governance of security enforcement. NIST's access-control guidance describes limiting system access according to authorized permissions, while CISA provides practical guidance for applying least privilege as part of a stronger security posture. See NIST SP 800-53, Least Privilege and CISA's Least Privilege Security Model.

QUESTION NO: 22

A network engineer wants to implement an 802.1X architecture in which BYOD devices must access a trusted wireless network securely. Which of the following should the engineer implement?

A. ACL

B. MAC filtering

C. Port security

D. NAC

ANSWER: D

Explanation:

NAC is the appropriate implementation because Network Access Control provides the policy-driven framework needed to admit and manage personally owned devices on an 802.1X-protected wireless network. In this architecture, a wireless client acts as the supplicant, the access point or wireless controller acts as the authenticator, and a RADIUS server commonly provides the authentication service. NAC extends this authentication workflow by evaluating device and user context against organizational access policies before, or as part of, granting network access.

For BYOD, NAC can support device registration or onboarding, certificate provisioning, identity-based authentication, endpoint posture assessment, and role-based authorization. Following a successful assessment, it can apply an appropriate access level, such as assigning the device to a trusted VLAN, placing it in a restricted role, or directing it to remediation resources. This allows the organization to permit secure access while retaining control over devices it does not fully own or manage. The IEEE 802.1X standard defines port-based network access control and supports EAP-based authentication, while NAC supplies the broader visibility and enforcement capabilities useful for BYOD policy decisions. See the IEEE 802.1X standard overview and Cisco's NAC overview.

QUESTION NO: 23

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:

No more patches or bug fixes are available indefinitely indicates that the computer's operating system or other vendor-supported software has reached end-of-support. End-of-support is a lifecycle milestone at which the vendor no longer provides ongoing maintenance, including security updates, reliability fixes, technical support, or feature updates. Although the physical computer may still start and operate, it is no longer maintained against newly discovered vulnerabilities. This creates an increasing security and compliance risk over time, particularly if the device connects to organizational networks or processes sensitive data.

In practical network administration, systems at end-of-support should be identified through asset and lifecycle management, then upgraded, replaced, isolated, or retired according to organizational policy and risk requirements. A vendor's lifecycle documentation is the authoritative source for determining whether a particular operating system or product version remains supported. Microsoft defines end of support as the point at which a product no longer receives security updates, non-security updates, bug fixes, technical support, or online technical content updates. CISA likewise emphasizes planning for replacement or migration before software reaches its end-of-support date. See Microsoft Lifecycle FAQ: What does end of support mean? and CISA: Understanding Software Lifecycle and End of Support.

QUESTION NO: 24

Which of the following is the best example of implementing role-based access control?

A. Granting data center access only to server and network administrators

B. Providing the entire IT department access to an application development server

C. Requiring all employees to use multifactor authentication when accessing the network

D. Allowing the human resources director to determine who can access human resources files

ANSWER: A

Explanation:

Granting data center access only to server and network administrators is the best example of role-based access control (RBAC) because access is assigned according to defined job functions. In this case, the server administrator and network administrator roles have a legitimate operational need to enter the data center in order to install, maintain, troubleshoot, or secure infrastructure. Rather than evaluating permissions separately for every individual employee, an organization can associate physical-access permissions with these roles and grant membership to personnel who perform those duties. This makes authorization more consistent, simplifies onboarding and role changes, and supports the principle of least privilege by limiting access to personnel whose responsibilities require it. RBAC can govern both logical resources, such as applications and files, and physical resources, such as secured facilities and equipment rooms. When an employee changes positions or leaves the organization, changing their role membership appropriately updates the access they receive. NIST describes RBAC as a model in which permissions are associated with roles and users acquire permissions through assignment to those roles. This approach also supports auditing because access can be reviewed against documented responsibilities. See NIST's Role-Based Access Control project and NIST SP 800-162 for access-control concepts and terminology.

QUESTION NO: 25

An administrator wants to ensure coverage when implementing a wireless solution in a new office building. Which of the following is the most useful for this scenario?

A. Building layout

B. IDF location

C. Cable diagram

D. Heat map

ANSWER: D

Explanation:

Heat map is correct because it provides a visual representation of predicted or measured Wi-Fi radio-frequency coverage across the office floor plan. During wireless design for a new building, an administrator can use a predictive heat map with the building's dimensions, wall materials, room layout, and proposed access point placements to identify areas likely to have weak signal, excessive overlap, or insufficient capacity. This allows access point locations, antenna choices, transmit power, and channel plans to be refined before deployment. After installation, a validation survey can produce an updated heat map based on real measurements, confirming that the design delivers the required coverage and signal quality throughout workspaces, meeting rooms, corridors, and other required areas. Coverage is not merely whether a client can detect a wireless network; it must support a usable signal level and reliable connectivity in the intended service areas. Heat maps are therefore a central planning and verification tool for wireless site surveys, especially when implementing a wireless solution in a previously unserved office environment. CompTIA includes wireless planning and deployment concepts within its Network+ exam objectives; see CompTIA exam objectives. Additional wireless RF design guidance is available from Cisco's wireless coverage design documentation.

QUESTION NO: 26

A network administrator needs to reduce the risk of unauthorized management access to a switch. Which of the following should the administrator configure? (Select two.)

A. SSH

B. An access control list

C. Telnet

D. A captive portal

E. An open SNMP community string

F. A hub

ANSWER: A B

Explanation:

SSH and **an access control list** are appropriate controls. SSH encrypts remote command-line management sessions and protects credentials and commands from disclosure while they traverse the network. It should be used instead of Telnet, which transmits session data in cleartext.

An ACL can limit management-plane access to approved administrative hosts or subnets. Restricting SSH access to a dedicated management network reduces the number of systems that can attempt to connect to the switch. These controls are complementary: SSH protects the management session, and the ACL restricts which sources can initiate one. SSH protocol architecture is defined in RFC 4251. CISA also recommends restricting management access and using secure protocols in its network infrastructure device security guidance.

QUESTION NO: 27

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:

Access point is correct because an access point extends a wired network into a wireless local area network (WLAN) and provides radio coverage, often called the wireless footprint or coverage area, for multiple Wi-Fi client devices. The access point advertises a wireless network name (SSID), accepts associations from authorized clients, and bridges their wireless traffic onto the connected wired LAN. Deploying additional access points, with appropriate channel planning and roaming configuration, expands coverage across a larger area while allowing users to remain connected to the same organizational WLAN. This is the core infrastructure role of an AP in an enterprise or small-office wireless deployment. An AP may be a standalone device or centrally managed through a wireless LAN controller or cloud-management platform, but in either form it is the component that supplies WLAN connectivity to laptops, phones, tablets, and other wireless endpoints. Cisco describes wireless access points as devices that create a wireless local area network and connect Wi-Fi devices to a wired network: Cisco: What Is a Wireless Access Point?. For terminology concerning WLANs and access points, see IEEE 802.11 Working Group.

QUESTION NO: 28

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:

Power budget is the first item to investigate. A Power over Ethernet switch has a finite total amount of power available for all PoE-capable ports, commonly expressed in watts. Although each individual port may support the required PoE standard, the switch cannot power another device once the combined demand of the already connected access points reaches the switch's available PoE budget. The fact that five access points start successfully and the next one does not is a strong indicator that cumulative power consumption, rather than a configuration issue specific to wireless service, is the immediate concern.

The engineer should check the switch's PoE status, total power capacity, current allocated and consumed wattage, and the power class requested by the new access point. The switch interface or management platform can also show whether the port has been denied power because insufficient wattage remains. This is especially relevant because AP consumption can vary based on radio count, radio transmit power, USB accessories, and features enabled during startup. CompTIA Network+ objectives include identifying PoE requirements and power limitations when deploying network devices. See the Cisco PoE troubleshooting guide and the IEEE 802.3af PoE standard information.

QUESTION NO: 29

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

0 lost carrier, 0 no carrier

0 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:

The NIC is set to half duplex is the most likely cause because the interface counters strongly indicate an Ethernet duplex mismatch. The switchport has recorded 89,920 collisions, together with 65,335 runts and a substantial number of input errors. Ethernet collisions occur when devices use a shared, half-duplex transmission method and attempt to transmit at the same time. A modern switched connection operating correctly at full duplex does not use CSMA/CD and should not accumulate collision counters.

A mismatch can occur when one side of a link operates at half duplex while the connected switch interface operates at full duplex. The half-duplex side detects and handles collisions, while the full-duplex side continues transmitting without collision

handling. This produces poor throughput, retransmissions, and small, incomplete frames reported as runts. The timing of the switch firmware update also makes a changed speed/duplex negotiation setting plausible.

The appropriate remediation is to verify the negotiated speed and duplex at both link ends, then configure both ends for auto-negotiation where supported or explicitly set identical speed and duplex settings. Cisco documents duplex mismatches as a common source of collisions, runts, and performance degradation: Cisco: Troubleshooting Ethernet Duplex and Speed Mismatch. See also the Ethernet duplex overview in Cisco support documentation.

QUESTION NO: 30

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 inventories

C. Central policy management

D. Zero-touch provisioning

E. Configuration drift prevention

F. Subnet range limits

ANSWER: A C

Explanation:

Least privilege network access and **Central policy management** are the best paired improvements because they address both the scope of access available to an attacker and the consistency of security enforcement across the environment. Least privilege grants users, devices, applications, and administrators only the network access and permissions required for their defined functions. Following a breach, this reduces the potential impact of compromised credentials, limits lateral movement, and prevents broad access from being available by default. It should be applied through role-based access controls, network segmentation, and carefully scoped administrative privileges.

Central policy management supports a durable security baseline by enabling administrators to define, distribute, monitor, and enforce access, authentication, and configuration policies from a consistent control point. This helps ensure security requirements are applied across managed systems rather than relying on individually configured devices. It also improves auditability and allows teams to identify and remediate policy deviations more efficiently during recovery and ongoing operations. Together, these practices strengthen identity and access controls, reduce unnecessary exposure, and make the organization's security posture more manageable after an incident. NIST describes least privilege as a fundamental access-control principle in its Least Privilege glossary entry; CISA provides implementation guidance in its Identity and Access Management resources.

QUESTION NO: 31

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:

“Ensure a bottleneck is not coming from other devices on the network” is an appropriate first troubleshooting step because wireless performance depends on the entire end-to-end path, not solely on the access point’s radio capability. The engineer should validate the AP’s Ethernet uplink speed, switch-port configuration, cabling quality, available switch capacity, and upstream network throughput. For example, an AP capable of multi-gigabit wireless service cannot deliver its potential throughput if it is connected through a lower-speed or impaired wired link. Testing with a suitable wired baseline helps isolate whether the AP itself is the limiting component or whether congestion or a physical/link-layer limitation exists elsewhere in the network.

“Install the latest firmware for the device” is also correct because AP firmware contains the vendor’s radio drivers, feature implementations, security fixes, and interoperability improvements. Updating to a supported current release can resolve known throughput, stability, channel-management, and client-compatibility defects. Firmware should be obtained from the AP vendor and applied according to its documented upgrade procedure, with configuration backup and compatibility checks where applicable. These actions follow a structured performance-troubleshooting approach: first verify the network path, then ensure the AP is running maintained software. See Cisco’s wireless LAN troubleshooting guidance and the CompTIA exam objectives resources.

QUESTION NO: 32

Which of the following is the best use case for PAT?

A. Using BGP for internet routing

B. Using a single public IP

C. Using redundant internet service providers

D. Using a dual-stack IP scheme

ANSWER: B

Explanation:

Using a single public IP is the best use case for PAT, or Port Address Translation. PAT enables multiple devices that use private IPv4 addresses on an internal network to access external networks while sharing one public IPv4 address. The NAT device distinguishes simultaneous conversations by translating not only the source IP address but also source-layer port information. This creates unique address-and-port mappings for individual sessions, allowing return traffic to be delivered to the appropriate internal host.

This is a practical and common design where public IPv4 addresses are limited. For example, a small office can use private addressing for its workstations, phones, and other devices while its edge router or firewall presents a single public address to internet services. PAT therefore conserves public IPv4 address space while allowing many internal endpoints to initiate outbound connections. CompTIA includes NAT and PAT among the networking concepts assessed for Network+, including their role in IPv4 connectivity and address translation. RFC 3022 describes traditional NAT behavior, including NAPT, the standards term closely associated with PAT. See the CompTIA exam objectives resource and RFC 3022.

QUESTION NO: 33

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 userâ€™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:

Changing the subnet mask to 255.255.255.0 is the appropriate correction when the workstation's configured mask places it in a different logical IPv4 network from the fileshare server at 192.168.10.1. A subnet mask determines which portion of an IPv4 address identifies the network and which portion identifies an individual host. With a 255.255.255.0 mask (a /24 prefix), the network is 192.168.10.0/24, and usable host addresses include 192.168.10.1 through 192.168.10.254. Therefore, a user device with a 192.168.10.x address and this mask recognizes 192.168.10.1 as a local destination. It can use ARP to resolve the server's MAC address and send Ethernet frames directly on the LAN, assuming the normal physical connectivity and host settings are present. Correct subnetting is fundamental to local communication because hosts use the mask to decide whether traffic is local or must be forwarded to a default gateway. This behavior is described in RFC 1812, and subnet-mask configuration concepts are covered in Cisco's IP addressing and subnetting documentation.

QUESTION NO: 34

A company is implementing a new wireless network in its office building and wants to ensure maximum coverage and signal strength. Which of the following factors should a technician consider to meet these requirements? Select two.

A. Building materials

B. Electrical interference

C. Distance from the server room

D. Type of encryption being used

E. Power over Ethernet

F. Type of client devices

ANSWER: A B

Explanation:

Building materials and **Electrical interference** are essential considerations during a wireless site survey and access point placement design. Radio-frequency signals are affected substantially by the physical environment. Materials such as concrete, brick, metal, low-emissivity glass, walls, elevator shafts, and dense furniture can attenuate, reflect, or scatter Wi-Fi signals. The degree of attenuation varies by material and frequency band, so technicians should survey the actual office environment rather than rely solely on a floor plan. This helps identify likely dead zones and determine suitable AP locations, antenna choices, and AP density.

Electrical interference also directly affects usable signal quality and coverage. Sources of radio-frequency or electromagnetic noise, including microwave ovens, Bluetooth devices, cordless equipment, fluorescent lighting, motors, and nearby wireless networks, can raise the noise floor or create channel contention. A site survey should identify these sources and inform channel planning and AP placement so clients receive an adequate signal-to-noise ratio throughout the building. CompTIA's Network+ objectives specifically include wireless surveys, environmental factors, signal strength, antenna placement, and interference as wireless design considerations. See the CompTIA exam objectives page and the Cisco wireless site-survey guidance.

QUESTION NO: 35

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:

Unreachable gateway is the cause most consistent with this symptom pattern. The successful connection to a local database server demonstrates that the workstation can communicate on its local IP network. Its network interface, local IP configuration, subnet mask, and the LAN path to resources in the same subnet are functioning sufficiently for local traffic. Communication with an internet host, however, requires the workstation to send packets for destinations outside its local subnet to its configured default gateway. The gateway is the router that provides the next hop from the local network toward external networks.

If the configured gateway address is incorrect, the gateway interface is offline, or connectivity between the workstation and that gateway is unavailable, the workstation cannot forward off-subnet traffic. It can therefore continue to reach a database server located locally while being unable to access internet resources. A technician can validate this diagnosis by checking the configured default gateway, attempting to ping that gateway, and tracing the route to an external IP address. Microsoft describes the default gateway as the route used to reach remote networks, and router requirements for forwarding IP traffic are defined in RFC 1812. See also Microsoft guidance on default gateway availability.

QUESTION NO: 36

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:

Enable 802.1Q and **Set up voice VLANs** are required because each IP phone and its attached computer must share one existing physical switch port. A typical VoIP deployment uses the phone's built-in switch: the uplink connects to the access switch and the computer connects through the phone. The switch port provides an untagged data VLAN for the attached computer while the IP phone identifies and sends voice traffic using IEEE 802.1Q VLAN tags.

A dedicated voice VLAN gives voice endpoints their own Layer 2 broadcast domain even though they share cabling and switch ports with data devices. This separation supports appropriate traffic handling for real-time voice, including the ability to classify and prioritize voice traffic through QoS policies. The phone can learn its assigned voice VLAN through switch configuration and then tag its voice frames accordingly; meanwhile, ordinary workstation traffic remains associated with the data VLAN on that same port. This design expands the VoIP deployment without consuming additional switch interfaces and maintains logical segmentation between voice and user data. Cisco's voice VLAN guidance describes carrying voice and data traffic on the same port with distinct VLAN treatment, and its 802.1Q documentation describes the VLAN-tagging mechanism: Cisco Voice VLAN configuration overview and Cisco IEEE 802.1Q VLAN tagging overview.

QUESTION NO: 37

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:

Site-to-site VPN is the most cost-effective solution for maintaining a persistent, secure connection between two facilities. This type of VPN connects entire networks through VPN gateways, such as firewalls or routers, at each location. Once configured, the gateways automatically establish and maintain the tunnel as needed, allowing users and systems at both sites to communicate without requiring each individual device to initiate a VPN session.

For confidentiality and integrity across an untrusted transport network, site-to-site VPNs commonly use IPsec. IPsec provides encryption, peer authentication, and integrity protection for traffic moving between the sites. Because the encrypted tunnel can use an existing business internet connection, the organization avoids the recurring cost of leasing a private carrier circuit while still protecting data in transit. This makes it a practical choice for branch-office connectivity, interoffice access to internal applications, and secure routing between separate LANs.

CompTIA Network+ objectives include selecting appropriate remote-access and site-connectivity technologies based on requirements such as security, availability, and cost. A site-to-site IPsec VPN directly addresses the requirements for an always-available interfacility connection and secure transmission over the internet. See the Cloudflare overview of site-to-site VPNs and Cisco's IPsec VPN documentation.

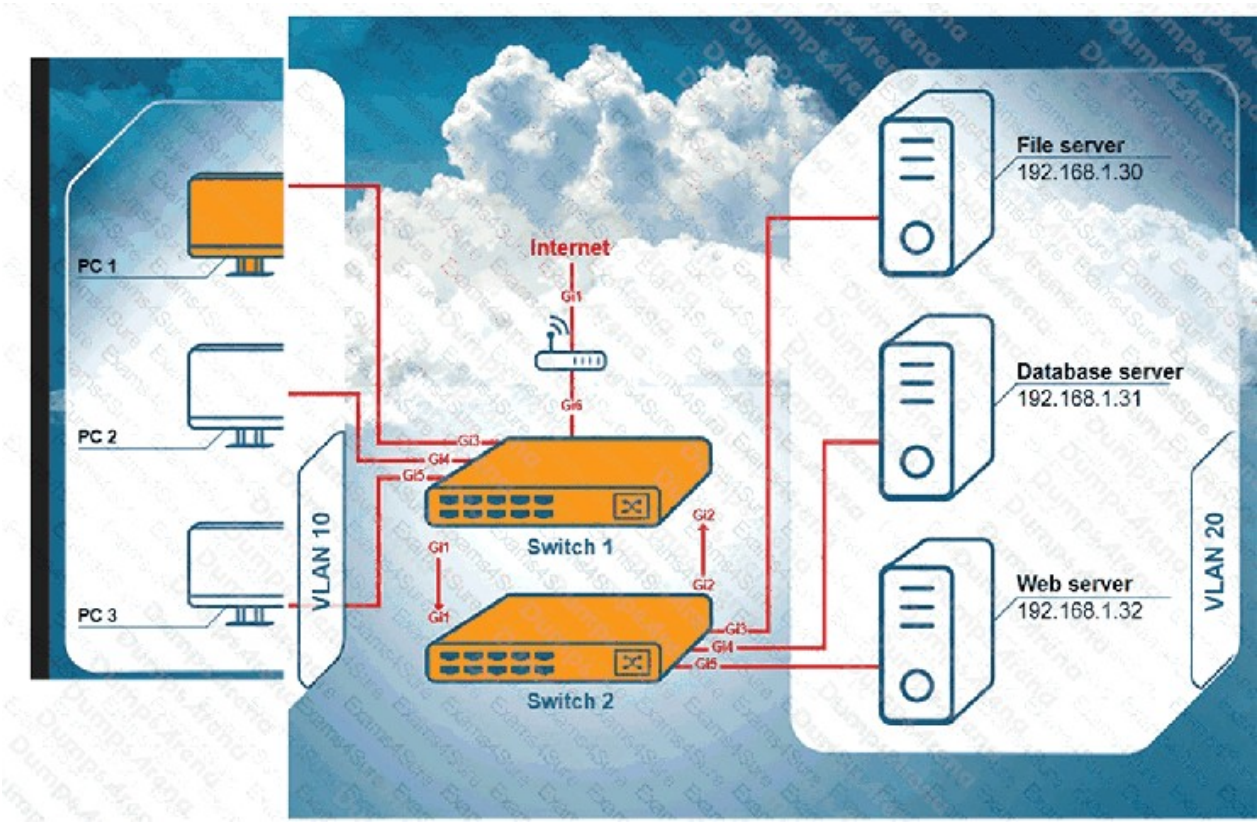
QUESTION NO: 38 - (SIMULATION)

A network technician receives a ticket from an employee who is working on PC 1 but is unable to connect to the database server. The technician pings the database server from PC 1, but the request times out. After reviewing the utilization of Switch 1 and Switch 2, the technician finds high CPU utilization and sees that the MAC table is continuously changing.

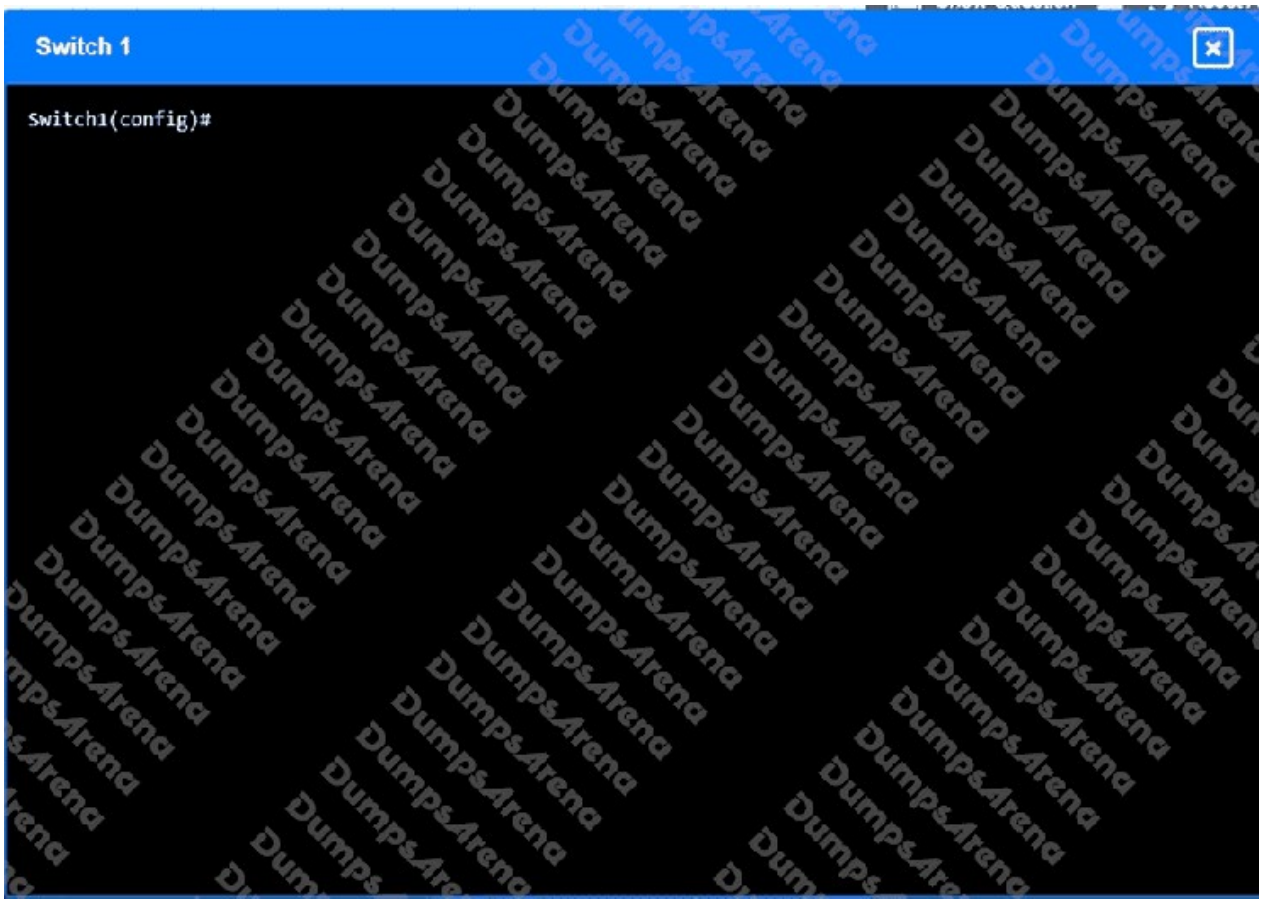
INSTRUCTIONS

Configure Switch 1 and Switch 2 to remediate the employee ' s issue. Then, validate connectivity between PC 1 and the database server.

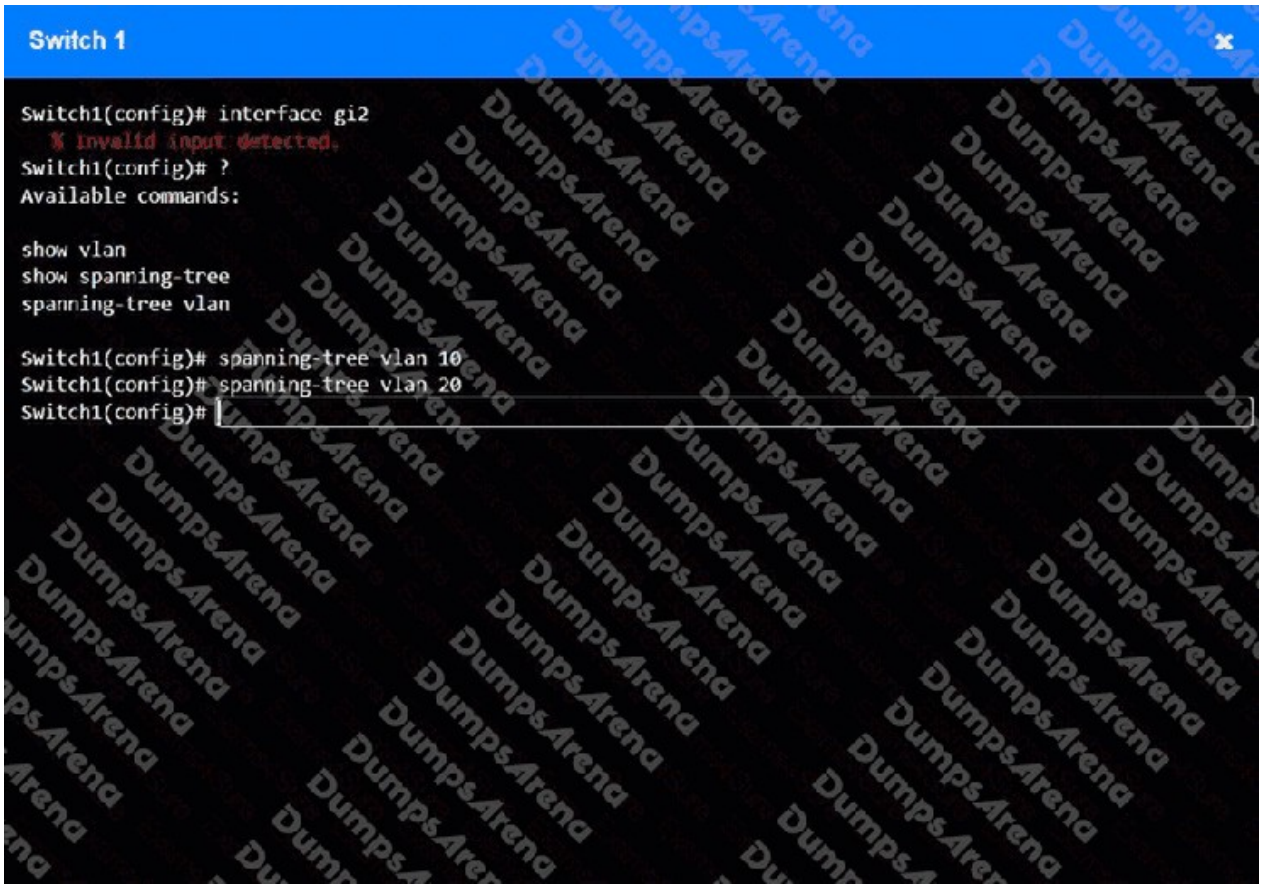
Switch 1 and Switch 2 are already in configuration mode. Type help to view a list of available commands.


PC 1
PC 2
PC 3
VLAN 10
Internet
Gi1
Gi6
Gi3
Gi4
Gi5
Switch 1
Gi2
Gi1
Gi2
Gi1
Gi3
Gi4
Gi5
Switch 2
File server
192.168.1.30
Database server
192.168.1.31
Web server
192.168.1.32
VLAN 20


PC 1
>ping 192.168.1.30
Pinging 192.168.1.30 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.30:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC 1
PC 2
PC 3
Switch 2
File server
192.168.1.30
Database server
192.168.1.31
Web server
192.168.1.32
VLAN 20


Switch 1
switch1(config)#


Switch 2
Switch2(config)#





ANSWER: See the explanation for the answer

Explanation:

The changing MAC table and high switch CPU indicate a Layer 2 switching loop. Configure STP root bridges per VLAN so STP can block the redundant loop path while retaining redundancy.

On **Switch 1**, enter:

On **Switch 2**, enter:

This makes Switch 1 the preferred STP root for VLAN 10 and Switch 2 the preferred STP root for VLAN 20, with the other switch serving as the backup root for each VLAN. STP will then place the appropriate redundant port into a blocking/discarding state, stopping the MAC flapping and excessive CPU utilization.

After STP converges, validate from PC 1 with:

The ping to the database server should succeed.

QUESTION NO: 39

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:

IDS is correct because an intrusion detection system can inspect and analyze network traffic passively, without being placed inline between internet-facing traffic and its destination. A network administrator commonly deploys an IDS using a network TAP or a switch SPAN/port-mirroring configuration. These methods send the IDS a copy of packets while the original packets continue on their normal forwarding path. The IDS can then compare observed activity against known attack signatures, suspicious behavior patterns, or policy rules and generate alerts for investigation. Because the IDS is observing copied traffic rather than making a forwarding or blocking decision for each packet, its processing does not add latency to the production traffic flow. This makes it appropriate when visibility into internet-originated attacks is needed while preserving application and network performance. The administrator can use IDS alerts to investigate malicious scans, exploit attempts, malware communications, or anomalous traffic, then make informed response decisions through other security controls. Cisco describes IDS as monitoring and alerting on suspicious activity, while inline prevention systems actively intervene in traffic. NIST also identifies intrusion detection as the process of monitoring events to identify signs of security incidents. See Cisco IDS and IPS overview and NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems.

QUESTION NO: 40

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:

When no additional switchports are available, an IP phone can share the existing physical switch connection with a workstation. The phone connects to the switch and provides a pass-through Ethernet port for the workstation, allowing both devices to use one switchport while retaining separate logical network segments. Setting up voice VLANs places VoIP endpoints in a dedicated VLAN, separate from the workstation data VLAN. This separation supports appropriate voice-focused policies, including quality of service classification and prioritization, as well as distinct security and addressing controls.

Enabling 802.1Q provides the VLAN frame-tagging mechanism needed to identify traffic belonging to the voice VLAN versus the ordinary data VLAN across the shared connection. A typical IP phone tags its own voice frames for the configured voice VLAN while forwarding workstation traffic on the access or data VLAN. The switch can therefore associate each frame with the intended logical network despite both traffic types using the same physical infrastructure. This design is a standard switched-LAN VoIP deployment model and directly addresses the constraint that additional physical ports cannot be allocated. Cisco's voice-VLAN configuration guidance describes the use of a switchport data VLAN together with a voice VLAN, and IEEE 802.1Q defines VLAN bridging and tagging behavior. See Cisco voice VLAN configuration guidance and IEEE 802.1Q standard information.

QUESTION NO: 41

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:

TLS is the protocol used by HTTPS to provide encryption in transit between a client, such as a web browser, and a web server. HTTPS combines HTTP, which defines how web requests and responses are exchanged, with TLS, which establishes a protected communication session. During the TLS handshake, the client and server negotiate a supported TLS version and cryptographic parameters, validate the server's digital certificate, and establish shared session keys. Those keys are then used to protect the confidentiality and integrity of the HTTP data while it crosses potentially untrusted networks.

In practical terms, TLS prevents passive observers from reading sensitive information transmitted to an HTTPS site, such as credentials, session cookies, form submissions, and application data. It also provides authentication of the server when certificate validation succeeds, helping the client confirm it is communicating with the intended service. Current security practice is to use modern TLS configurations, particularly TLS 1.2 or TLS 1.3, and to disable obsolete SSL and early TLS versions. The MDN overview of Transport Layer Security describes TLS as the mechanism that encrypts and authenticates HTTPS connections. The IETF's TLS 1.3 specification defines the current protocol standard.

QUESTION NO: 42

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 F

Explanation:

Rack selection is primarily based on the physical dimensions of the equipment that must be installed. **Server height** determines the required vertical capacity of the rack. Rack-mounted equipment is measured in rack units, or U, with one rack unit equal to 1.75 inches (44.45 mm). An administrator totals the rack-unit requirements of servers and other equipment to select a rack with sufficient usable height, while normally reserving additional space for future growth, cable management, airflow, and maintenance.

Switch depth determines the rack's required front-to-rear depth. Network switches vary substantially in chassis depth, and the rack must accommodate the equipment's deepest device as well as power connections, network cabling, cable bend radius, and appropriate clearance for ventilation. A rack that is physically deep enough helps ensure that doors can close properly and that rear connections are not compressed or obstructed.

These two measurements correspond directly to the standardized physical dimensions used when planning a 19-inch equipment rack: vertical rack-unit capacity and usable equipment depth. CompTIA Network+ installation planning expects technicians to account for equipment fit alongside related operational considerations such as cooling, power, and cable routing. See the rack-unit and mounting-hole specifications in EIA-310-E and the equipment-rack planning guidance from Cisco.

QUESTION NO: 43

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:

The RJ45 cables were replaced with unshielded cables and the wrong transceiver type was used for the new termination are the most likely cabling-related causes following replacement work. Data centers contain potential sources of electromagnetic interference, including power distribution equipment, generators, motors, and cooling infrastructure. Where a cabling design requires shielded twisted-pair cable, replacing it with unshielded cable can reduce noise immunity and result in intermittent connectivity, increased errors, retransmissions, or reduced link reliability. Shielding must also be correctly terminated and bonded as part of the overall cabling system.

Optical and direct-attach links require compatible transceivers at both ends. The selected module must match the switch interface and the installed medium, including the supported Ethernet speed, connector type, optical wavelength, reach, and fiber mode when fiber is used. For example, multimode and single-mode fiber deployments require optics designed for the applicable fiber type. A mismatched transceiver can prevent a link from establishing or produce unreliable operation after equipment is restored. These checks are especially appropriate when the symptoms begin immediately after cable and termination replacement. CompTIA's Network+ exam objectives include identifying cabling characteristics and transceiver types: CompTIA exam objectives. Cisco also documents optical compatibility considerations in its transceiver module guide.

QUESTION NO: 44

A company is preparing a network device for a remote-site deployment. The device must continue operating during a brief utility-power failure and must shut down safely during an extended outage. Which of the following should be implemented? (Select two.)

A. An uninterruptible power supply

B. Automated shutdown software

C. A cable tester

D. A KVM switch

E. A layer 2 loop guard

F. A wireless controller

ANSWER: A B

Explanation:

An uninterruptible power supply and **automated shutdown software** are the best solutions. A UPS provides short-term battery power when utility power fails, allowing the network device to remain available through brief interruptions. It can also protect equipment from certain power irregularities, depending on the UPS design.

For a prolonged outage, automated shutdown software or an equivalent management function can monitor the remaining battery capacity and initiate an orderly shutdown before power is exhausted. This helps avoid abrupt power loss and reduces the risk of configuration or file-system corruption on supported devices. CISA includes backup power among important resilience considerations in its Infrastructure Resilience Planning Framework.

QUESTION NO: 45

A company is upgrading its wireless network. Currently, each AP broadcasts a wireless LAN name depending on the location in the building. Which of the following configurations allows a single wireless LAN name to be broadcast across the entire building?

A. ESSID

B. Wireless mesh

C. Band steering

D. WPA3

ANSWER: A

Explanation:

ESSID is correct because an Extended Service Set consists of multiple access points configured to provide one logical wireless LAN across a broader physical area, such as an entire building. In this deployment, the access points advertise the same network name (SSID) and are connected to the same underlying distribution system. A user therefore sees one consistent WLAN name rather than location-specific network names as they move through the facility.

For roaming to work effectively, the participating access points normally use the same SSID, compatible authentication and encryption settings, and appropriate VLAN or network access configuration. Their radios should also be planned to provide overlapping coverage while using suitable nonoverlapping channels to reduce co-channel interference. As a client moves away from one access point and toward another, it can reassociate with the stronger AP while remaining on the same logical wireless network. This design improves usability because employees do not need to select a different wireless network manually when changing rooms or floors.

CompTIA's Network+ exam objectives include configuring wireless networks and distinguishing WLAN concepts such as SSIDs and wireless deployment types. See the CompTIA exam objectives resource page and Cisco's overview of wireless LANs.

QUESTION NO: 46

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:

Isolate smart devices to their own network segment and change the default credentials. Network segmentation is the primary control because a guest SSID must not have Layer 3 access to internal resources or IoT equipment such as the clinic's speaker system. Placing the speakers on a dedicated IoT VLAN or SSID and applying firewall or access-control rules prevents guest clients from discovering, connecting to, or sending control traffic to those devices. The guest network should be restricted to Internet access only, while authorized staff devices can be granted only the specific access required to manage the speakers.

Changing the default credentials is also an essential hardening measure for IoT devices and any associated management interface or application account. Default usernames, passwords, PINs, or administrative settings may be publicly known or easily guessed. Replacing them with unique, strong credentials ensures that only authorized clinic personnel can administer the speaker system, including from permitted internal network segments. These controls provide both network-level separation and device-level access protection, which is appropriate for an environment handling guests and potentially sensitive clinical operations. CISA recommends changing default passwords and securing smart devices, while Cisco describes segmentation as a means to limit communication between network zones. See CISA: Secure Your Smart Devices and Cisco: What Is Network Segmentation?.

QUESTION NO: 47

A company is hosting a customer-facing application in the cloud. The application must remain available if a single virtual server fails and must distribute incoming client connections across available servers. Which of the following should the company implement? (Select two.)

A. Load balancing

B. High availability

C. Port security

D. Jumbo frames

E. MAC filtering

ANSWER: A B

Explanation:

Load balancing distributes incoming client connections across multiple application instances. This prevents a single server from receiving all requests and allows traffic to be directed to healthy servers when one instance becomes unavailable.

High availability provides redundancy so that the application can continue operating after a component failure. In this scenario, deploying multiple virtual servers as redundant application instances supports continued service if one server fails. These controls improve availability but should be paired with health checks and appropriate capacity planning. NIST describes availability as ensuring timely and reliable access to information and systems in its Availability glossary entry.

QUESTION NO: 48

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 is the appropriate tool because it collects and displays the actual packets traversing a network interface. By examining captured traffic, a technician can identify source and destination IP addresses, MAC addresses, DNS requests, protocols, connection timing, and traffic volumes. Those details can be correlated with DHCP leases, switch port information, or endpoint inventory records to identify the specific computer generating the suspected downloads.

A capture can also reveal the remote hosts or services contacted by that endpoint and provide evidence of the traffic pattern involved. Although encrypted connections generally prevent inspection of the downloaded file contents without appropriate decryption capabilities and authorization, the metadata in the capture—such as DNS lookups, TLS server names where available, destination addresses, and session behavior—can still establish which system is communicating with suspicious destinations. Captures should be performed in accordance with organizational policy, authorization requirements, and applicable privacy rules. Wireshark provides documentation on capturing and analyzing packets at Wireshark Documentation. For an overview of packet-capture concepts and analysis, see the CISA guidance on network traffic analysis.

QUESTION NO: 49

A network engineer is troubleshooting poor VoIP call quality over a WAN connection. Monitoring shows that the link is saturated during business hours. Which of the following should the engineer review first? (Select two.)

A. Jitter

B. Packet loss

C. MAC address aging

D. DHCP lease duration

E. DNS zone transfer

F. Cable jacket type

ANSWER: A B

Explanation:

Jitter and **packet loss** should be reviewed because both directly affect real-time voice traffic. Jitter is variation in packet-arrival time. Excessive jitter can cause voice packets to arrive too late for playback, resulting in gaps or distorted audio. Packet loss can also produce missing audio because real-time applications generally cannot wait for retransmissions without increasing delay.

WAN saturation can cause queues to build and packets to be dropped, making these metrics especially relevant. The engineer should also validate QoS classification and queuing policies after confirming the condition of the constrained link. RFC 3550 describes RTP, which is commonly used for real-time media and includes mechanisms for monitoring packet loss and jitter: RFC 3550.

QUESTION NO: 50

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:

MTBF (mean time between failures) is the reliability metric used to estimate the average operating time between failures for repairable equipment, such as network switches, routers, servers, and power supplies. Manufacturers derive MTBF from reliability testing, field data, or statistical models across a population of devices. A higher MTBF generally indicates that failures are expected less frequently under stated operating conditions. For Network+ purposes, MTBF is the appropriate metric when the question concerns anticipated hardware reliability or the average time a device operates before a failure event occurs.

MTBF is an estimate rather than a guaranteed service life for one individual device. It helps IT teams assess equipment reliability, compare hardware models, plan maintenance, maintain appropriate spare inventory, and make replacement decisions. The value is commonly expressed in hours and represents a population-level average interval between failures; it should be interpreted along with the manufacturer's environmental, workload, and maintenance assumptions. The U.S. National Institute of Standards and Technology identifies mean time between failures as a commonly used reliability measure for repairable systems, while IBM describes its use in evaluating system availability and failure behavior. See NIST reliability, maintainability, and availability engineering and IBM documentation on MTBF.

QUESTION NO: 51

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:

Client device compatibility should be checked because a Wi-Fi 6E router does not automatically provide Wi-Fi 6E performance to every connected endpoint. Wi-Fi 6E extends Wi-Fi operation into the 6 GHz band, but a client must have a compatible wireless adapter, driver, and operating-system support to use that band. Clients that support only earlier Wi-Fi generations, or that lack support for relevant channel widths and features, may associate using 2.4 GHz or 5 GHz and negotiate lower PHY rates. The technician should verify each affected device's adapter capabilities, connected band, negotiated link rate, signal quality, and channel width. The Wi-Fi Alliance describes Wi-Fi 6E and its use of 6 GHz spectrum at Wi-Fi 6E.

Interference levels should also be evaluated because radio-frequency conditions directly affect wireless throughput. Although 6 GHz generally offers additional spectrum and less legacy-device contention, clients may be using 2.4 GHz or 5 GHz, where neighboring WLANs, Bluetooth devices, and other RF sources can reduce signal-to-noise ratio and increase retransmissions. A wireless site survey or analyzer can identify channel utilization, co-channel contention, overlapping coverage, and weak-signal areas. Cisco provides an overview of Wi-Fi 6E spectrum and deployment considerations at What Is Wi-Fi 6E?.

QUESTION NO: 52

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 appropriate because they increase the Ethernet maximum transmission unit (MTU) beyond the standard 1500-byte payload size, commonly to approximately 9000 bytes. A storage network often transfers large volumes of data, so carrying more payload in each frame reduces the total number of frames required for a given transfer. This lowers the proportional Ethernet, IP, and TCP/UDP header overhead and can reduce processing demands on network interfaces, switches, and hosts. The resulting reduction in per-frame processing can improve throughput and efficiency, particularly for high-bandwidth storage traffic such as iSCSI or network-attached storage workloads. Jumbo frames must be configured consistently end to end: the storage system, host NICs, switches, routed interfaces where applicable, and any intervening network devices must all support the selected MTU. An MTU mismatch can cause fragmentation issues or dropped traffic, so validation across the complete storage traffic path is essential. Cisco describes jumbo frames as frames larger than the conventional 1500-byte Ethernet payload and documents their use and MTU considerations in its configuration guidance: Cisco: MTU and Jumbo Frames. Additional Ethernet frame and MTU background is available from the IEEE 802.3 Ethernet standards overview: IEEE 802.3 Ethernet.

QUESTION NO: 53

A user reports issues connecting to the network via an Ethernet Cat 6 cable. A network technician examines the cable and notices that it is terminated properly, but the color code is incorrect. Which of the following steps should the technician take next to troubleshoot this issue?

A. Implement a fiber cable.

B. Replace the Ethernet cable.

C. Change the switchport speed.

D. Use a cable tester.

ANSWER: D

Explanation:

Use a cable tester. An Ethernet cable can appear physically well terminated because each conductor is seated in the connector, yet still fail to provide a reliable network link if the conductors do not follow a valid pinout and pair arrangement. For Cat 6 twisted-pair Ethernet, the conductors must be positioned according to an applicable wiring scheme, such as T568A or T568B, and the twisted pairs must remain correctly mapped end to end. An incorrect color sequence can indicate a wire-map issue, including a reversed conductor, crossed conductors, or a split pair. These faults may prevent link establishment or cause intermittent connectivity and poor performance.

A cable tester is the appropriate next troubleshooting tool because it objectively checks continuity and pin mapping across the cable. More capable cable certification testers can additionally evaluate characteristics relevant to Cat 6 performance, such as length, attenuation, and crosstalk. The test results let the technician identify whether the observed color-code discrepancy produces an actual cabling fault and determine the required corrective action based on evidence. This follows a structured troubleshooting practice: validate the physical-layer condition with the tool designed for copper cabling before making configuration changes or replacing components. Cisco also describes Ethernet twisted-pair wiring and pin assignments in its Ethernet cable guide; Fluke Networks provides an overview of copper cable certification.

QUESTION NO: 54

Which of the following best describes a characteristic of a DNS poisoning attack?

A. DNS address records are edited and changed on a DNS server.

B. An attacker sets up a malicious DNS server in place of a legitimate server.

C. DNS client requests are intercepted and false responses are returned.

D. False DNS records are injected into cache on a DNS server.

ANSWER: D

Explanation:

False DNS records are injected into cache on a DNS server is correct because DNS poisoning, also called DNS cache poisoning, corrupts the cached DNS data that a recursive resolver uses to answer future queries. The attacker causes the resolver to store a forged resource record, such as an incorrect IP address associated with a legitimate domain name. While that cache entry remains valid for its time-to-live (TTL), users who request the targeted domain can be directed to an attacker-controlled destination even though they entered the correct domain name. This can facilitate credential theft, malware delivery, or interception of traffic through a convincing fraudulent site. DNS poisoning is particularly impactful because recursive DNS servers provide answers for many clients, so one successful cache injection can affect numerous users until the cache is cleared or the forged record expires. DNS Security Extensions (DNSSEC) help mitigate this threat by enabling DNS resolvers to validate digitally signed DNS data and reject unauthenticated responses. The U.S. Cybersecurity and Infrastructure Security Agency describes DNS cache poisoning and related protective practices at CISA's DNS cache poisoning guidance. Additional technical background on DNSSEC validation is available from ICANN's DNSSEC overview.

QUESTION NO: 55

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 establish Internet connectivity using the ISP-provided static addressing, the firewall needs **One static IP address** assigned to its external/WAN interface. This address identifies the firewall on the ISP-facing network and provides a valid source address for traffic leaving the organization. Although the ISP supplied five public addresses, only one is required for the firewall itself to establish basic outbound connectivity; the remaining addresses can be assigned to other public-facing interfaces, services, or NAT mappings as needed.

The firewall also needs the **Default gateway**, which is the ISP router's reachable next-hop address on the WAN subnet. The firewall uses its default route to forward traffic destined for networks outside its directly connected WAN network, including Internet destinations. Together, the WAN static address and a default route pointing to the ISP gateway provide the fundamental Layer 3 configuration needed for Internet access. This is consistent with standard IPv4 host configuration, in which an address, subnet information, and a default-router setting allow off-network traffic to be forwarded. See Cisco's routing fundamentals documentation and the IETF's IPv4 router requirements.

QUESTION NO: 56

Which of the following OSI model layers manages the exchange of HTTP information?

A. Session

B. Data link

C. Network

D. Application

ANSWER: D

Explanation:

The Application layer is correct because HTTP (Hypertext Transfer Protocol) is an application-layer protocol in the OSI model. HTTP specifies the structure and semantics of communication between web clients and web servers, including request methods such as GET and POST, response status codes, headers, and message bodies. These functions directly support application software, including browsers, web services, and APIs, so they belong to OSI Layer 7.

Although an HTTP exchange depends on lower-layer services to reach its destination, HTTP itself defines the web-oriented information being exchanged. For example, TCP commonly provides dependable transport for HTTP traffic, while IP provides logical addressing and routing between networks. Those underlying services enable the connection and delivery, but they do not define the meaning or format of an HTTP request or response. In CompTIA Network+ OSI-model mappings, HTTP is therefore associated with the Application layer. The Internet Engineering Task Force defines HTTP as an application-layer protocol in its HTTP Semantics specification: RFC 9110: HTTP Semantics. For additional background on the OSI model and its seven layers, see ISO/IEC 7498-1.

QUESTION NO: 57

A network administrator is deploying IPv6 on a new user VLAN. Client devices must automatically receive an IPv6 address and the address of a default gateway without using DHCPv6. Which of the following are required? (Select two.)

A. Router advertisements

B. Stateless address autoconfiguration

C. DHCP reservation

D. NAT overload

E. ARP inspection

F. Port forwarding

ANSWER: A B

Explanation:

Router advertisements and **stateless address autoconfiguration** are required for this design. An IPv6 router sends router advertisement messages that provide the network prefix and identify the router as a default gateway. Hosts use the information in the advertisement to configure an IPv6 address and install a default route.

Stateless Address Autoconfiguration (SLAAC) enables the client to create its own interface identifier and combine it with the advertised prefix. This avoids the need for a DHCPv6 server to assign the IPv6 address. DHCPv6 may still be used in some deployments to provide supplementary settings, such as DNS server addresses, but it is not required for the automatic addressing and gateway functions described. See RFC 4861 for IPv6 Neighbor Discovery and router advertisements and RFC 4862 for IPv6 Stateless Address Autoconfiguration.

QUESTION NO: 58

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 and changing default passwords are foundational device-hardening practices because both directly reduce the likelihood of unauthorized access to network infrastructure. Disabling unused ports removes unnecessary physical or logical entry points from switches, routers, firewalls, and similar devices. A port that has no business purpose should not be available for an unknown endpoint, rogue device, or accidental connection. This applies to unused switch interfaces as well as unnecessary management and network services, which should be disabled or restricted when they are not required.

Changing default passwords is equally essential because manufacturer-supplied credentials are frequently documented, predictable, or broadly known. Replacing them with strong, unique administrative credentials prevents attackers from gaining straightforward access to a device's management interface. Device hardening establishes a secure baseline configuration before operational monitoring and broader access-control processes are applied. CISA specifically recommends changing default passwords and disabling unused ports and services when securing network infrastructure devices. These actions follow the principle of minimizing exposed functionality and ensuring that administrative access is protected from the outset. See CISA guidance for securing network infrastructure devices and NIST password guidance.

QUESTION NO: 59

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:

Theport Is shut down. is the most likely cause because an administratively disabled switch interface prevents the Ethernet link from becoming active, even when the cable is securely connected at both ends. A functioning Ethernet connection normally establishes link integrity between the workstation NIC and switch port; the devices then illuminate link LEDs and may blink activity LEDs as frames are transmitted or received. If the switch interface has been placed in a shutdown state, it does not participate in link establishment or forward traffic, so the workstation cannot access network resources and neither end will show normal link/activity behavior.

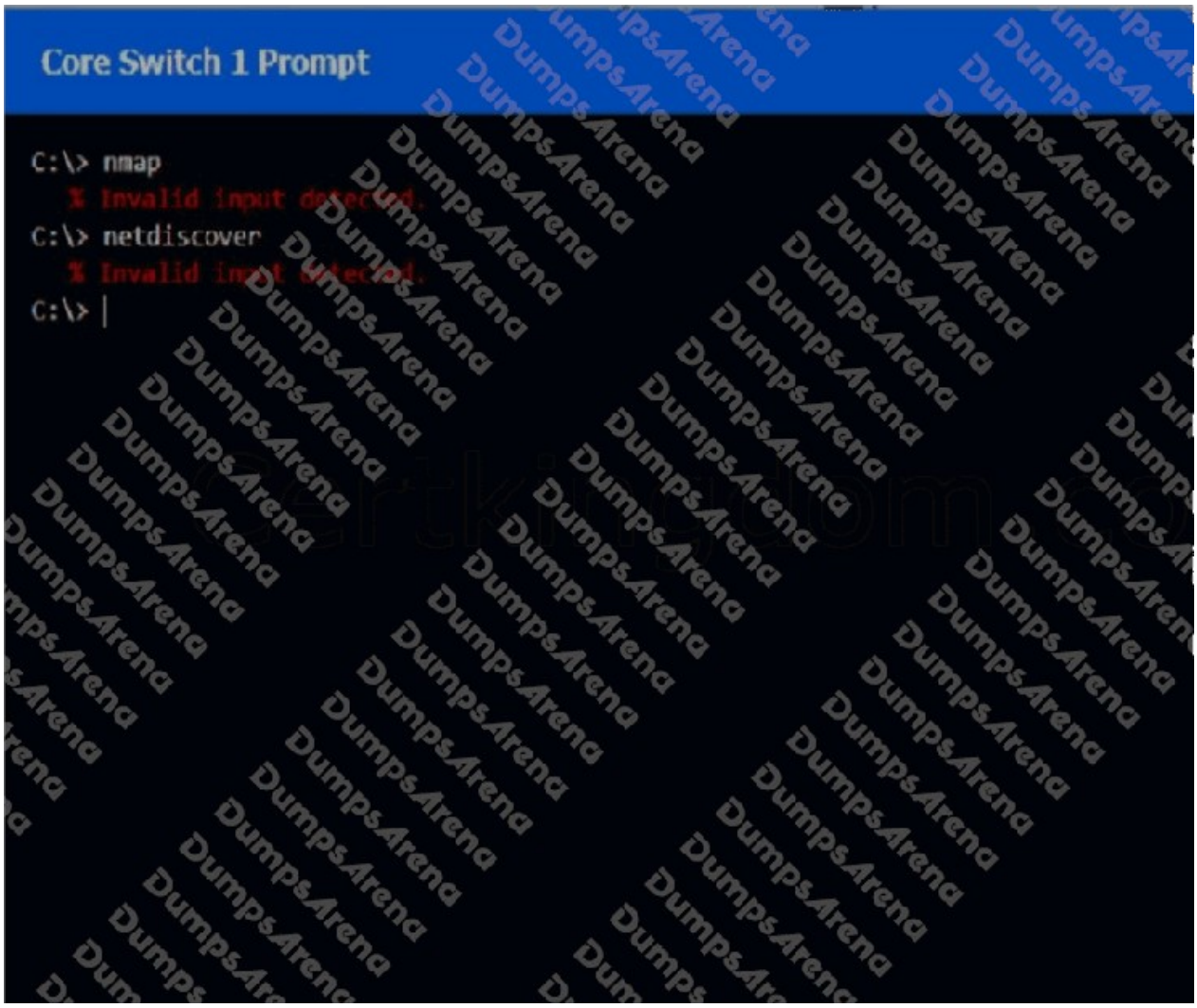
An administrator should inspect the switch interface status and configuration, confirm that the correct physical port is being checked, and enable the interface if it was intentionally or accidentally disabled. On Cisco IOS-based switches, this is commonly done from interface-configuration mode with the `no shutdown` command. Once the interface is enabled and the physical link is negotiated, the link indicators should illuminate and normal network connectivity can be tested. This troubleshooting approach aligns with Network+ objectives covering physical-interface status and switch-port configuration. See CompTIA's exam objectives resources and Cisco's interface command reference.

QUESTION NO: 60 - (SIMULATION)

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



ANSWER: See the explanation for the answer

Explanation:

The commands `nmap` and `netdiscover` are not valid in this switch CLI. On **each switch**, use the switch discovery/show commands below and select the values shown in that switch's output in the diagram drop-downs.

Answer/action: Do not enter `nmap` or `netdiscover`. Run the four `show` commands above on Core Switch 1 and every other switch, then map each CDP entry as *local switch/local interface → neighbor switch/remote interface* and choose the IP/VLAN values exactly as displayed.

The supplied image contains no command output or topology/drop-down values, so the specific IP addresses, interface numbers, and VLAN selections cannot be determined from it. They are simulation-instance values and must be read from the live command output.

QUESTION NO: 61

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:

SIEM is the appropriate solution because Security Information and Event Management platforms are designed to provide centralized visibility across heterogeneous environments. A SIEM ingests event records, logs, alerts, and telemetry from numerous sources, including network infrastructure, security appliances, endpoints, servers, applications, cloud platforms, and operating systems from different vendors. This centralized collection supports the stated multivendor and multi-OS monitoring requirement.

SIEM platforms also collect and normalize incoming data continuously or in near real time. Normalization makes events from otherwise dissimilar products usable in a common format, allowing security and network operations teams to search, monitor, and alert on activity as it occurs. A core SIEM capability is correlation: the platform evaluates related events across multiple sources and over defined time periods to identify patterns, produce meaningful alerts, and provide broader operational visibility. For example, it can associate authentication activity from an endpoint with firewall and server logs to identify a single incident or operational condition. NIST describes the centralized collection, analysis, and correlation functions associated with log management in SP 800-92: Guide to Computer Security Log Management. CISA also identifies SIEM as a capability for aggregating and analyzing security-relevant log data in its SIEM resource.

QUESTION NO: 62

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:

UPS is the best way to keep devices operating during a loss of utility power. An uninterruptible power supply contains batteries and power-conditioning circuitry that can provide immediate temporary power when the normal electrical source fails. Because the transition is effectively instantaneous for connected equipment, a UPS helps prevent network devices, servers, workstations, and storage systems from rebooting or shutting down abruptly during a brief outage. It also provides a limited period in which essential equipment can remain available while power is restored or an administrator performs an orderly shutdown. Selecting an appropriately sized UPS requires considering the connected equipment's total power draw and the required runtime. UPS units are commonly used for critical network infrastructure such as switches, routers, firewalls, and wireless controllers, where even a short interruption can disrupt connectivity. Depending on the model, a UPS may also help protect connected equipment from electrical disturbances such as surges and voltage fluctuations. The U.S. Cybersecurity and Infrastructure Security Agency recommends using uninterruptible power supplies to maintain power for critical systems during outages. See CISA guidance on power outages and NIST's guide to uninterruptible power systems.

QUESTION NO: 63

A network engineer is installing a wireless bridge between two buildings on the same campus. Which of the following should the engineer implement to provide the most reliable connection? (Select two.)

A. Directional antennas

B. Line of sight

C. Captive portal authentication

D. Omnidirectional antennas

E. Ad hoc mode

ANSWER: A B

Explanation:

Directional antennas are appropriate because a building-to-building wireless bridge needs to focus radio-frequency energy toward the remote endpoint. Directional antennas provide higher gain in the intended direction and reduce reception of unwanted signals from other areas.

Line of sight is also required because physical obstructions between bridge endpoints can attenuate, reflect, or block the wireless signal. The engineer should verify an unobstructed path and account for the Fresnel zone when mounting the antennas. These practices improve signal strength and reduce instability on the point-to-point link. Cisco describes the use of directional antennas and line-of-sight planning in its wireless antenna guidance.