DUMPSARENA

CompTIA A+ Certification Exam: Core 1

CompTIA 220-1101

Version Demo

Total Demo Questions: 85

Total Premium Questions: 858

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Mobile Devices	93
Topic 2, Networking	199
Topic 3, Hardware	179
Topic 4, Virtualization and Cloud Computing	93
Topic 5, Hardware and Network Troubleshooting	291
Topic 6, Mix Questions	3
Total	858

QUESTION NO: 1

A technician is setting up a home network with the following requirements:

· Automatic distribution of IP addresses

. Internet access

Which of the following should the technician configure? (Select two).

A. DHCP

B. APIPA

C. VPN

D. Public IP addresses

E. Gateway

F. Static IP addresses

ANSWER: A E

Explanation:

DHCP provides the automatic distribution of IP addressing information required by devices on the home network. A DHCP service leases an IP address to each client and can also deliver essential configuration settings, including the subnet mask, DNS server addresses, and the default gateway. This centralizes client network configuration and avoids the need to manually assign an address to every phone, computer, game console, or smart-home device. Microsoft's DHCP overview describes DHCP as the protocol used to automatically provide hosts with IP configuration information: Microsoft Learn: DHCP overview.

Gateway is also required because it supplies the path from the local home network to external networks, including the Internet. In a typical home installation, the router acts as the default gateway for local clients. Devices send traffic intended for destinations outside their local subnet to that gateway, and the router forwards it toward the ISP. Home routers commonly combine gateway/routing functions with DHCP and network address translation, enabling multiple private-addressed devices to access Internet resources through the home's WAN connection. The default-gateway role in IP routing is documented by Microsoft Learn: Default gateway.

QUESTION NO: 2

A technician is preparing to install a replacement CPU in a desktop computer. Which of the following should the technician do before installing the CPU? (Select TWO).

A. Verify CPU compatibility.

B. Apply thermal paste.

C. Format the system drive.

D. Configure RAID 0.

E. Install a CMOS battery.

ANSWER: A B

Explanation:

The technician should verify CPU compatibility and apply thermal paste. The replacement processor must use a socket supported by the motherboard and be compatible with the motherboard firmware and chipset. Installing an unsupported CPU can prevent the system from completing POST.

Thermal paste should be applied between the CPU heat spreader and the heat sink unless the cooling solution already has thermal material preapplied. The compound fills microscopic gaps between the surfaces and improves heat transfer to the heat sink. The technician should also use ESD precautions and secure the heat sink after the processor is seated. Intel's processor installation guidance describes proper processor and thermal-solution installation.

QUESTION NO: 3

A technician needs to assign an IP address to a Windows PC, but a network connection is unavailable. Which of the following tools would be best for the technician to use?

A. DHCP

B. TFTP

C. APIPA

D. DNS

ANSWER: C

Explanation:

APIPA is correct because Windows can automatically configure an IPv4 address for itself when the network adapter is configured to obtain an address automatically but no DHCP server can be reached. This Automatic Private IP Addressing behavior selects an address from the link-local IPv4 range, 169.254.0.0/16, and uses the 255.255.0.0 subnet mask. Before using an address, Windows checks for conflicts so it does not intentionally duplicate an address already in use on the same local segment. This provides the PC with a usable local address without requiring an available network infrastructure service or a manually configured address. Devices using compatible link-local addresses can communicate on the same local network segment, which can assist with basic local connectivity and troubleshooting while normal addressing is unavailable. APIPA addresses are link-local addresses: they are not intended to be routed beyond the local subnet. When DHCP connectivity becomes available later, Windows can obtain its normal DHCP-provided configuration. Microsoft documents the 169.254.0.0/16 range as IPv4 link-local addressing and describes Windows automatic private addressing behavior in its TCP/IP documentation. See Microsoft Learn: Netsh interface IP and Microsoft Learn: IP address management.

QUESTION NO: 4

A user reports a cell phone is getting hot. Which of the following are MOST likely to be possible causes? (Select THREE).

A. Using the device as a Wi-Fi hotspot

B. A cracked screen

C. A failing battery

D. Less than 15% free storage space on the phone

E. Privileged control

F. Recurring prompts to install OS updates

G. Granting too many application camera permissions

H. Too many open applications

ANSWER: A C H

Explanation:

Using the device as a Wi-Fi hotspot is a likely cause because tethering makes the phone actively maintain a wireless connection for client devices while transferring data, increasing radio and processor activity. That sustained workload consumes power and produces heat, particularly where cellular signal conditions are poor or data use is heavy. Apple notes

that devices can become warm during use of features that require more power, including use as a personal hotspot. See Apple Support: Keeping iPhone, iPad, and iPod touch within acceptable operating temperatures.

A failing battery is also a likely cause. Battery degradation or damage can lead to abnormal power behavior and excessive heat during charging or ordinary use. Heat is a significant battery safety symptom that should prompt the technician to stop charging the device if necessary, inspect for battery swelling or physical damage, and arrange appropriate repair or replacement. The U.S. Consumer Product Safety Commission provides lithium-ion battery safety guidance at Lithium-Ion Battery Safety Tips.

Too many open applications can contribute to overheating when multiple apps continue performing processor-intensive work, network communication, location processing, media tasks, or background synchronization. Closing unneeded apps and identifying unusually resource-intensive applications reduces the workload and helps determine whether application activity is responsible for the elevated temperature.

QUESTION NO: 5

A customer called the help desk to request information about how to increase the volume on a laptop using only a keyboard. Which of the following keys would MOST likely allow this to be done?

A. Alt

B. Fn

C. Tab

D. Ctrl

ANSWER: B

Explanation:

Fn is correct because laptop keyboards commonly use the Function key as a modifier to access hardware-specific controls embedded on the top-row keys. To raise volume, the user typically holds Fn and presses the function-row key displaying a volume-up icon, often a speaker symbol with sound waves or a plus sign. This design lets manufacturers provide media and system controls without adding dedicated keys, which is especially useful on compact laptop keyboards.

The exact key bearing the volume-up symbol varies by laptop model and manufacturer. Some systems may have media actions enabled as the primary function of the top-row keys, in which case the volume key can work without holding Fn; however, Fn remains the key most associated with accessing these alternate laptop-keyboard functions. A support technician should direct the customer to look for the volume-up icon among the function-row keys and use it together with Fn if necessary. Dell documents that the Fn key is used with keys on the keyboard to invoke secondary functions: Dell Support: Using Fn keys. Microsoft also describes using keyboard media controls to manage device volume: Microsoft keyboard shortcuts.

QUESTION NO: 6 - (SIMULATION)

Laura, a customer, has instructed you to configure her home office wireless access point.

She plans to use the wireless network for finances and has requested that the network be setup with the highest encryption possible.

Additionally, Laura knows that her neighbors have wireless networks and wants to ensure that her network is not being interfered with by the other networks.

She requests that the default settings be changed to the following.

Wireless Name: HomeWiFi

Shared Key: CompTIA

Router Password: Secure$1

Finally, Laura wants to ensure that only her laptop and Smartphone can connect to the network.

Laptop: IP Address 192.168.1.100

Hardware Address: 00:0A:BF:03:C4:54

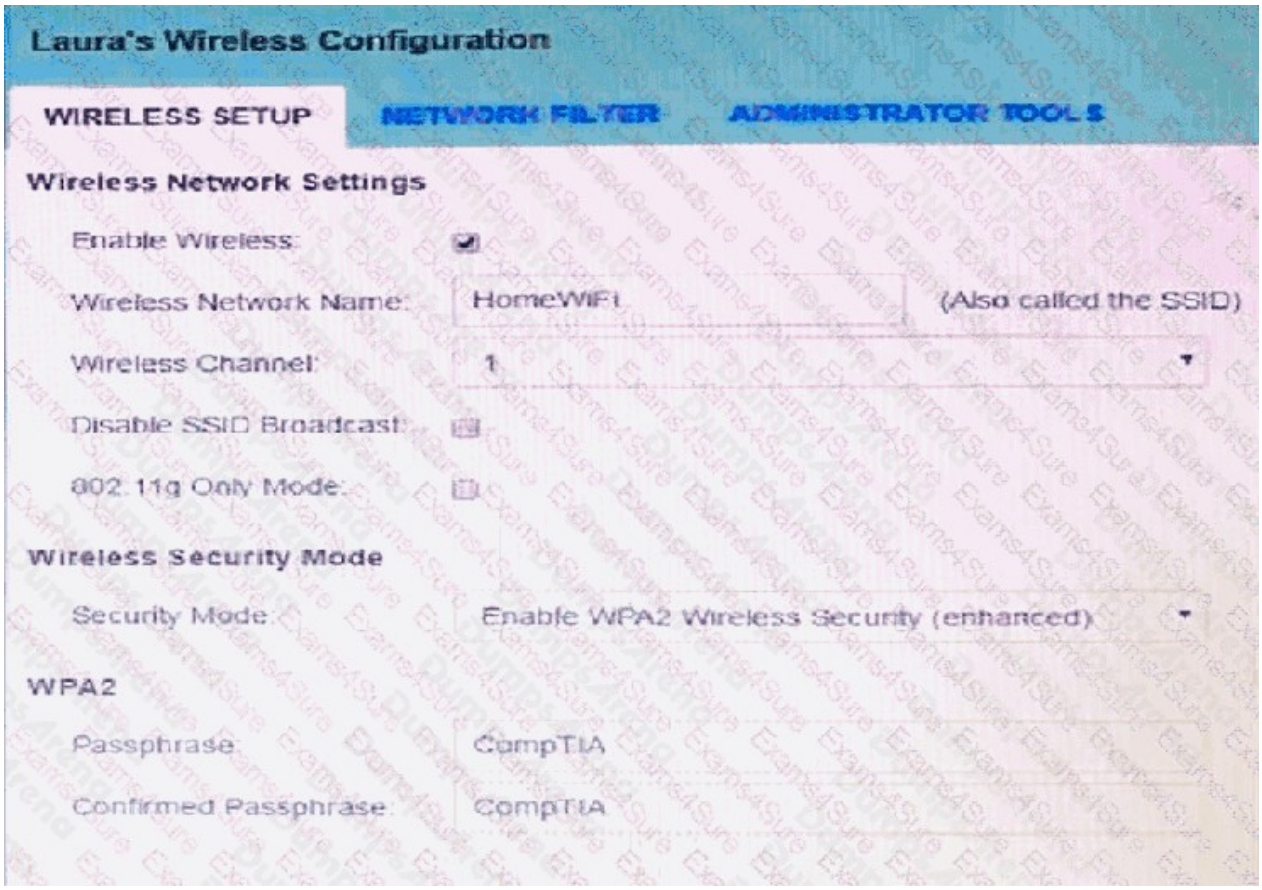
Smartphone: IP Address 192.168.1.101

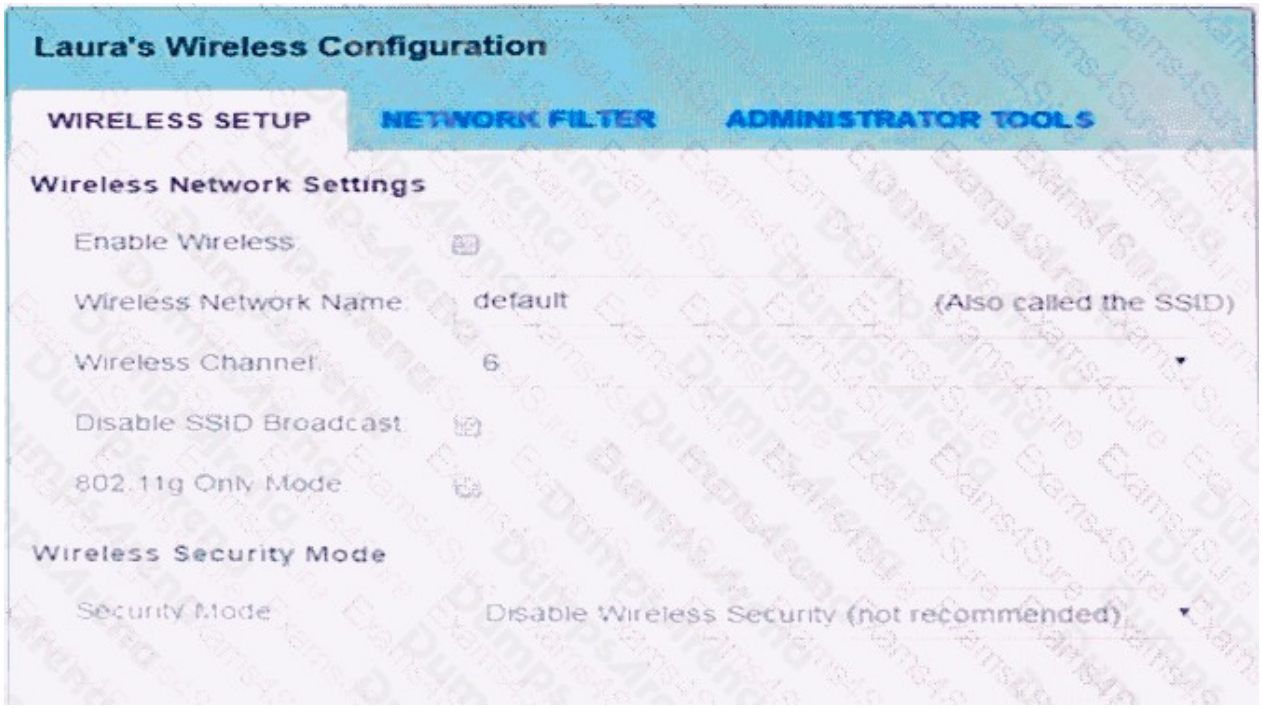
Hardware Address: 09:2C:D0:22:3F:11

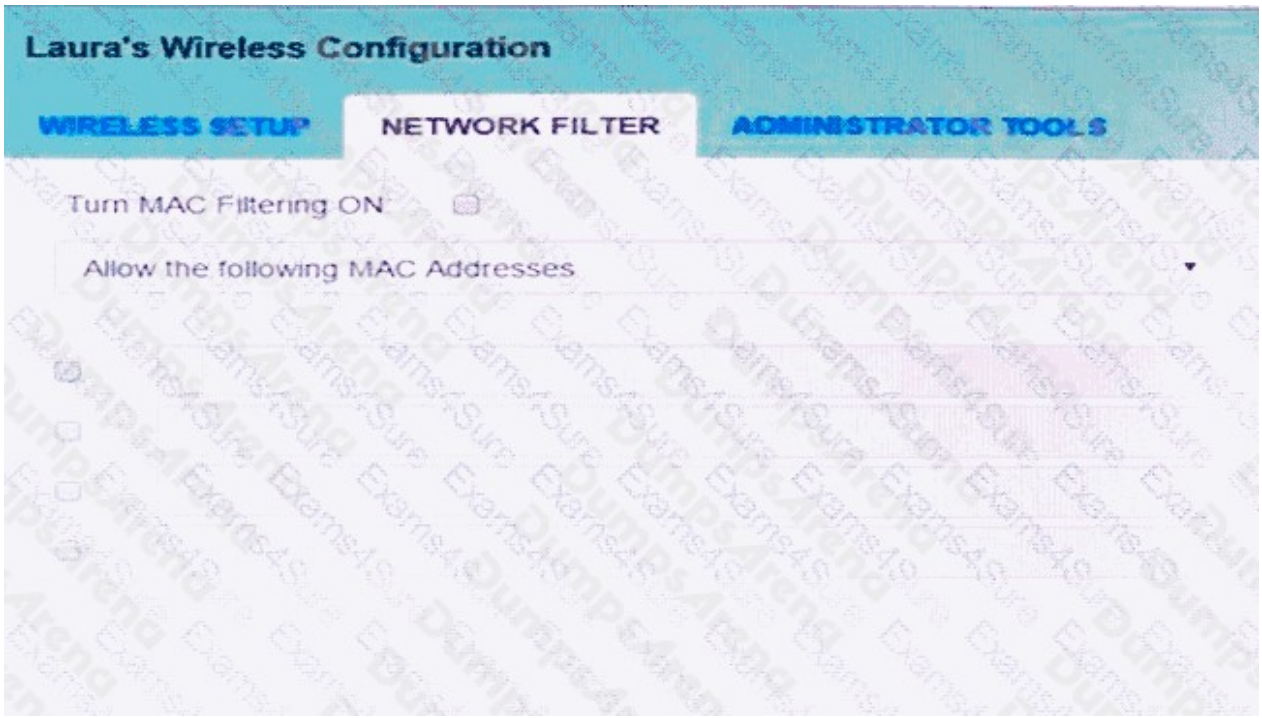
INSTRUCTIONS

Configure Laura's wireless network using the network adapter window.

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







ANSWER: See the explanation for the answer

Explanation:

Configure the access point with the following settings:

Use channel **1** because the neighboring networks shown use channels 6 and 11; channels 1, 6, and 11 are the non-overlapping 2.4 GHz choices. WPA2 (enhanced) is the strongest security option available in this simulator, and MAC allow-listing limits wireless access to Laura's two specified devices.

QUESTION NO: 7

A technician needs to install a printer on the network. Which of the following must the technician configure? (Select THREE).

A. PCL

B. Dots per inch

C. Gateway

D. Subnet mask

E. MAC address

F. MB

G. IP address

ANSWER: C D G

Explanation:

A network printer requires valid IPv4 network settings so hosts and print services can address and communicate with it predictably. **IP address** is required to identify the printer as a host on the network. Assigning a static address, or reserving an address through DHCP, prevents the printer's address from changing unexpectedly and allows clients, print servers, and management tools to reliably locate it. The **subnet mask** defines which addresses are local to the printer's network segment. With this value, the printer can determine whether a destination is on its own LAN or requires routing. The **gateway**, usually the local router's address, supplies the route for traffic destined for other subnets. This is necessary when users, print servers, DNS services, or management systems are located outside the printer's local subnet. Together, the IP address, subnet mask, and gateway form the essential IPv4 configuration used for a network-connected printer. Microsoft's printer deployment guidance also identifies an IP address or hostname as the network endpoint used when adding a TCP/IP printer port. See Microsoft PrintUI documentation and Cisco's IPv4 addressing and default-gateway overview.

QUESTION NO: 8

An end user discovered that the touch-screen features on a Windows device have stopped working. Which of the following should a technician check?

A. Performance monitor

B. Tablet/PC settings

C. System configuration

D. Display settings

ANSWER: B

Explanation:

Tablet/PC settings is the appropriate Windows configuration area to check for a touch-input problem. Windows provides the Tablet PC Settings control-panel applet specifically for configuring pen and touch input. It includes options to set up the display used for pen or touch input and to calibrate the screen, ensuring that Windows correctly associates touch input with the intended display and accurately maps physical touch points to on-screen locations. This is particularly relevant when touch capability has stopped functioning as expected after a display change, docking configuration change, or an issue with touch-input alignment.

A technician should open Tablet PC Settings and verify the touch configuration, then use its setup or calibration functionality when appropriate. This focuses troubleshooting on the Windows feature area designed for touch-enabled hardware, rather than on general system monitoring or unrelated display personalization. Microsoft documents Tablet PC Settings as a canonical Control Panel item named *Microsoft.TabletPCSettings*, confirming its role in configuring tablet pen and touch behavior. See Microsoft's Control Panel canonical names documentation and its Pen and Windows Ink support guidance for Windows input configuration context.

QUESTION NO: 9

A user is selecting a display for editing high-resolution photographs. Which of the following display characteristics should the user prioritize? (Select TWO).

A. High refresh rate

B. High resolution

C. Accurate color reproduction

D. Low response time

E. Integrated speakers

ANSWER: B C

Explanation:

A higher resolution and accurate color reproduction are the most appropriate characteristics for photo editing. Higher resolution provides more pixels for viewing image detail and allows more workspace for editing tools. Accurate color reproduction helps ensure that the colors displayed during editing more closely match the intended output.

Refresh rate is most important for motion clarity in gaming and other fast-moving content, while response time primarily measures how quickly pixels change states. Those characteristics are less important than resolution and color accuracy for photographic work. See Adobe guidance on monitors for photo editing.

QUESTION NO: 10

A user wants to confirm that all necessary hardware is functional for a webinar. Which of the following should the user test and configure in the webinar application prior to joining? (Select three).

A. Keyboard

B. Digital pen

C. Speakers

D. Mouse

E. Camera

F. Docking station

G. Microphone

ANSWER: C E G

Explanation:

Speakers, a camera, and a microphone are the hardware devices that webinar applications commonly provide dedicated pre-join controls to test and configure. The user should select the correct speaker or headset output and use the application’s test-sound feature, where available, to confirm that webinar audio will be audible. The camera should be selected from the available video devices and previewed so the user can verify that the application receives an image and that framing, lighting, and video quality are appropriate. The microphone should likewise be selected and tested through the application’s input meter or test feature, allowing the user to confirm that speech is captured at a usable level before entering the webinar. These checks address the core audiovisual functions needed to listen, be seen, and speak during an online session. Microsoft’s guidance for Teams describes choosing and testing speaker, microphone, and camera devices before a meeting through device settings and the pre-join screen: Microsoft Support: Manage your device settings in Teams. Zoom also documents testing audio and video before joining a meeting: Zoom Support: Testing audio before joining a meeting.

QUESTION NO: 11

A colleague has a laptop that has been working as expected for several years wall outlet. The MOST likely component that needs to be replaced is the:

A. power adapter.

B. battery.

C. system fan.

D. hard drive.

ANSWER: B

Explanation:

The battery is the appropriate replacement component when an older laptop operates normally while connected to its AC power source but can no longer provide usable runtime away from the wall outlet. Rechargeable lithium-ion batteries are consumable components: their capacity decreases through normal age, charge/discharge cycles, and heat exposure. After several years of service, a battery may no longer retain sufficient charge even though the rest of the laptop continues to function as expected. Replacing it with a compatible battery restores the laptop's ability to operate portably, subject to normal battery-health and charging checks. Microsoft notes that battery capacity naturally declines over time and provides battery reporting tools that can help assess installed versus design capacity. For safe replacement, technicians should follow the manufacturer's service guidance and use an approved battery model, since laptop batteries and their connectors are device-specific. See Microsoft's battery-care guidance and Microsoft's powercfg battery-report documentation.

QUESTION NO: 12

When a user touches or swipes across an external touch screen, the image flickers but no input is registered on the presentation laptop. Atechnician verifies that the external touch screen appears free from physical damage. Which of the following should the technician do next?

A. Reboot the LCD touch panel and laptop.

B. Check the cables connecting to the laptop.

C. Verify the correct input source is set on the laptop.

D. Replace the laptop with a new device that is known to work.OE.

E. Inspect the LCD touch panel for dead pixels or burn-in.

ANSWER: B

Explanation:

Check the cables connecting to the laptop. An external touch display commonly relies on separate connections: a video cable, such as HDMI, DisplayPort, or USB-C, to render the image, and a USB upstream connection or a full-featured USB-C connection to carry touch input data to the laptop. A loose, damaged, incorrectly connected, or incompatible cable can therefore produce both symptoms described: unstable video that flickers and absent touch events at the laptop. Since the technician has already completed a basic visual inspection of the panel and found no physical damage, examining and reseating the connections is the appropriate next troubleshooting action. The technician should verify that each connector is fully seated at both ends, inspect cables for bent pins or visible wear, confirm that the display's USB touch/upstream port is connected to an appropriate laptop USB port, and, if necessary, test with known-good compatible cables. This follows a methodical troubleshooting approach: validate the physical connectivity needed for the display's separate video-output and touch-input functions before progressing to software or device replacement actions. Microsoft's touch-screen guidance describes touch hardware as an input device integrated with the operating system: Microsoft touch-screen guidance. CompTIA publishes the applicable A+ exam objectives and troubleshooting domains at CompTIA Exam Objectives.

QUESTION NO: 13

A technician has just installed a new SSD into a computer, but the drive is not appearing. Which of the following is most likely the reason's?

A. The SSD is faulty and should be replaced by the manufacturer

B. The SSD has not been properly formatted and is not readable

C. The SSD is incompatible with the motherboard

D. The SSD has not been installed properly and should be reseated

ANSWER: D

Explanation:

The SSD has not been installed properly and should be reseated is the most likely reason immediately after a new drive installation. A drive that is not fully seated in its M.2 socket, has an improperly connected SATA data cable, or lacks a secure SATA power connection may not be detected by the firmware or operating system at all. The technician should power the system down, observe appropriate ESD precautions, remove and reinstall the SSD securely, and verify any required data and power connections. For an M.2 SSD, this includes confirming that the module is inserted fully at the correct angle and held in place with its retaining screw. After reseating, the technician should check whether the SSD is detected in UEFI/BIOS before proceeding with operating-system-level configuration. Microsoft's storage documentation notes that newly attached disks may then need to be initialized and formatted before they can be used in Windows: Initialize new disks. Guidance on checking physical connections and system firmware detection is also available from Crucial SSD support.

QUESTION NO: 14

A systems administrator is attempting to resolve a ticket regarding an issue with an email server. The administrator is covering for a coworker who was previously working on the ticket. The coworker already gathered facts about the issue and spoke with users concerning their missing emails. The coworker also discovered the email server's retention policy was updated shortly before users first noticed the issue. Which of the following should the systems

administrator do NEXT to resolve the email issue?

A. Escalate the ticket to a higher level to resolve the email server issue.

B. Test a theory to determine the cause of the email server issue.

C. Establish a theory of probable cause for the email server issue.

D. Create a plan of action to resolve the email server issue.

ANSWER: C

Explanation:

Establish a theory of probable cause for the email server issue. is the appropriate next step in the CompTIA troubleshooting methodology. The administrator has already completed the initial information-gathering activities: facts were collected, affected users were interviewed, and the issue was correlated with a recent change to the email server. The retention-policy update is a meaningful symptom correlation because retention settings can determine when messages are deleted, archived, or otherwise become unavailable to users.

At this point, the administrator should form a probable-cause theory that the revised retention policy is causing the missing-email reports. This creates a focused, evidence-based hypothesis that can subsequently be tested in a controlled manner. Establishing the theory before acting helps ensure that remediation is directed at the most likely source of the problem and follows a disciplined change-management process. CompTIA's troubleshooting model sequences the work as identifying the problem, establishing a theory of probable cause, testing that theory, establishing a plan of action, implementing the solution, verifying functionality, and documenting findings. The official CompTIA exam-objectives resources describe the skills and troubleshooting concepts assessed for the A+ certification: CompTIA Exam Objectives. CompTIA also outlines the value of structured troubleshooting practices in its IT troubleshooting guide.

QUESTION NO: 15

A technician needs to install a printer on the network. Which of the following must the technician configure? (Select THREE).

A. PCL

B. Dots per inch

C. Gateway

D. Subnet mask

E. MAC address

F. MB

G. IP address

H. Drivers

ANSWER: C D G

Explanation:

For a network printer to communicate reliably using IPv4, it needs an **IP address**, a **subnet mask**, and a **gateway**. The IP address uniquely identifies the printer on its local network and provides the destination that workstations, print servers, and management tools use when sending print jobs or accessing the printer's web interface. A static address or a DHCP reservation is commonly used so the printer remains reachable at a consistent address.

The subnet mask defines the boundaries of the local IP network. It enables the printer to determine whether another device is on the same subnet and can be contacted directly. The gateway is the router address used when the printer must communicate with devices outside its own subnet, such as a print server, DNS server, cloud-print service, or administrative workstation located on another network. Configuring these three values correctly establishes the essential IPv4 network settings needed for normal network connectivity. Microsoft's guidance on TCP/IP configuration describes the role of IP addresses, subnet masks, and default gateways: TCP/IP addressing and subnetting. See also DHCP overview for how these settings can be assigned automatically.

QUESTION NO: 16

A technician is replacing the toner cartridge in a laser printer. Which of the following steps should the technician complete first? (Select two).

A. Check the expiration date of the cartridge.

B. Ensure the cartridge is the correct model.

C. Open the toner compartment.

D. Remove the sealing tape.

E. Run the cleaning utility.

F. Calibrate the printer.

ANSWER: B C

Explanation:

Before beginning a toner replacement, the technician should confirm that the replacement cartridge matches the printer's required model. Laser-printer toner cartridges are designed for specific printer families, and using the correct consumable protects print quality, ensures physical and electrical compatibility, and avoids interrupting the replacement procedure after the existing cartridge has been removed. This aligns with the CompTIA A+ hardware objective covering installation and maintenance of printer consumables.

After confirming the correct cartridge is available, opening the toner compartment is an initial physical-access step. The compartment or front access door provides access to the installed cartridge and is necessary before the technician can remove the old unit or install the new one. Manufacturer installation procedures consistently begin by opening the printer's cartridge-access area before handling the installed toner. The replacement cartridge should remain protected until it is ready to be installed, helping prevent toner spills and avoiding unnecessary exposure of cartridge components.

For related exam coverage, review the printer-maintenance objectives in the CompTIA A+ exam objectives. A representative manufacturer procedure is available in HP's toner-cartridge replacement guidance.

QUESTION NO: 17

The output from a dot matrix printer has become lighter over time. Which of the following should a technician do to fix the issue?

A. Clean the printhead.

B. Replace the ribbon.

C. Install a maintenance kit.

D. Calibrate the alignment.

ANSWER: B

Explanation:

Replace the ribbon. Dot matrix printers are impact printers: a printhead containing small pins strikes an inked fabric ribbon, transferring ink onto the paper to create characters and images. As the printer is used, the ribbon's available ink is depleted or dries out. This produces output that gradually becomes faded or lighter across the page while the printer otherwise continues to feed paper and print normally. Installing a compatible replacement ribbon restores the ink source that the printhead transfers to the paper, returning output density to normal. This is a standard consumable-maintenance task for dot matrix hardware and directly addresses a progressive reduction in print darkness. The technician should also ensure the replacement ribbon is installed correctly in its cartridge and advances freely during printing so that fresh inked ribbon passes in front of the printhead. Epson's support documentation identifies the ribbon cartridge as the replaceable supply for its dot matrix printers and provides installation procedures: Epson: Replacing the Ribbon Cartridge. For general context on the impact-printing mechanism, see Encyclopaedia Britannica: computer printer.

QUESTION NO: 18

In a SOHO environment, a user wants to make sensitive, scanned documents available to other users on the domain. The logs need to indicate who accessed the documents and at what time they were accessed. Which of the following settings should a technician set up on the MFP device?

A. Scan to email

B. ADF tray

C. PCL

D. SMB share

ANSWER: D

Explanation:

SMB share is correct because it lets a multifunction printer scan documents directly to a shared folder hosted on a domain-connected computer or file server. The share can be protected with domain user or group permissions, so access to sensitive documents is controlled through authenticated accounts rather than simply distributing copies of the files. When users open, modify, or otherwise access the scanned files, the file server can record the associated account and the access

time through its auditing configuration. This provides a central, manageable location for the documents and supports the requested accountability.

On the MFP, the technician configures a Scan to SMB destination using the server name or IP address, share path, and an authorized service account or user credentials. The destination folder should use appropriate share and NTFS permissions, while auditing must be enabled on the hosting Windows system and folder to capture object-access events. Microsoft documents SMB as its network file-sharing protocol and describes how advanced audit policy and file-system auditing can record access to file and folder objects. This arrangement is particularly suitable for a small office because users can retrieve the same centrally stored scans while access records remain available to an administrator. See Microsoft's SMB overview and Microsoft's Audit File System policy documentation.

QUESTION NO: 19

A user routinely connects and disconnects multiple devices from a laptop. Which of the following options should a technician recommend to facilitate ease of user mobility?

A. Serial interfaces

B. Docking station

C. Network switch

D. USB hub

ANSWER: B

Explanation:

Docking station is the appropriate recommendation because it consolidates a laptop's common desk connections into one device. The user can leave peripherals such as an external display, keyboard, mouse, Ethernet connection, speakers, and USB storage connected to the docking station, then connect or disconnect the laptop using a single cable or docking connector. This significantly reduces setup and teardown time when moving between a desk, meeting room, and remote location, while also minimizing repeated handling of individual peripheral cables and ports.

Modern USB-C and Thunderbolt docking stations can provide data connectivity, video output, wired networking, and laptop charging through one connection, provided that the laptop and dock support the required capabilities. This arrangement directly supports user mobility: the laptop remains portable, but it can quickly become a full workstation when returned to the primary work area. A technician should verify compatibility with the laptop's USB-C or Thunderbolt implementation, power-delivery requirements, display resolution needs, and operating-system support before selecting a dock. Microsoft provides guidance on connecting and troubleshooting external displays at Microsoft Support, and USB-IF describes USB Type-C capabilities at USB-IF.

QUESTION NO: 20

A cloud engineer, who is designing a cloud architecture, needs to ensure the solution is able to immediately fail over to another region in case of an outage and also scale up in the event of high utilization. Which of the following should the engineer Implement? (Select two).

A. High availability

B. Elasticity

C. Cold storage

D. Machine learning

E. Metered utilization

F. Virtualization

ANSWER: A B

Explanation:

High availability is required because the architecture must continue providing service when a regional outage occurs. In a cloud design, this is achieved by placing redundant workloads and data in separate regions and configuring health monitoring, traffic routing, replication, and automated failover. A secondary regional deployment that is ready to receive traffic enables the service to remain available, or recover with minimal interruption, when the primary region cannot operate. This aligns with the availability and resiliency concepts assessed in CompTIA A+ Core 1 cloud-computing objectives.

Elasticity is required because the solution must scale up when utilization becomes high. Elastic cloud resources can automatically provision additional compute capacity in response to defined demand signals, such as CPU utilization, request volume, memory pressure, or queue depth. When demand later declines, capacity can also be reduced, maintaining appropriate performance without permanently allocating resources for peak load. Together, high availability addresses continuity across a regional failure, while elasticity addresses changing workload demand during normal operation. See the CompTIA exam objectives page and the AWS guidance on reliability and resilient workload design.

QUESTION NO: 21

Which of the following virtualization technologies allows Linux and Windows operating system to run concurrently?

A. Test environment

B. Sandbox

C. Legacy OS

D. Cross-platform

ANSWER: D

Explanation:

Cross-platform is correct because cross-platform virtualization enables operating systems with different architectures and software ecosystems, such as Linux and Windows, to operate concurrently on the same physical computer. A hypervisor abstracts the underlying hardware and allocates virtualized CPU, memory, storage, and network resources to separate virtual machines. Each virtual machine runs its own guest operating system independently, so a user can use Windows-specific applications in one virtual machine while running Linux tools or services in another without needing to reboot the host computer. This capability is particularly useful for application compatibility, development, testing, training, and supporting software that requires a different operating system than the primary workstation environment. CompTIA includes cross-platform virtualization as a virtualization use case because it permits multiple distinct operating systems to coexist while maintaining separation between their individual environments. Microsoft describes virtual machines as isolated computing environments that can run different operating systems on shared hardware, and the Linux Kernel documentation explains the hardware virtualization support used by hypervisors. See Microsoft Hyper-V overview and Linux Kernel KVM documentation.

QUESTION NO: 22

A user plugs in a laptop to the corporate network and the laptop is automatically assigned an IP address. Which of the following server types was used to assign the IP address?

A. DNS

B. AAA

C. DHCP

D. Web

ANSWER: C

Explanation:

DHCP is the server type that automatically provides IP configuration to devices when they connect to a network. Dynamic Host Configuration Protocol uses a client-server process in which the laptop requests network settings and the DHCP server supplies an available IP address from its configured scope or address pool. In addition to the IP address, DHCP commonly delivers other essential configuration values, such as the subnet mask or prefix length, default gateway, DNS server addresses, and lease duration. This centralizes address management and helps administrators avoid the manual configuration burden and duplicate-address problems that can occur when every client is statically configured. The address is normally leased for a defined period, and the client renews that lease as needed while it remains connected. Therefore, an automatically assigned address after connecting a laptop to the corporate network indicates use of a DHCP server. Microsoft's overview of DHCP describes DHCP as a standards-based protocol that dynamically assigns IP addresses and related configuration information to clients. The Internet Engineering Task Force's RFC 2131 defines the DHCP protocol and its mechanisms for allocating network addresses and configuration parameters.

QUESTION NO: 23

A support technician receives a call stating that a user has added a device to the network. The user used the same configurations from another workstation. When both workstations are turned on, neither can access the network reliably. Which of the following is the most likely cause of the issue?

A. The new computer has a duplicate IP address.

B. The DNS server is registering both hostnames.

C. The network cable was improperly terminated.

D. The security on the switchport needs to be reset.

ANSWER: A

Explanation:

The new computer has a duplicate IP address. Copying the network configuration from an existing workstation can copy its manually assigned IPv4 address as well as settings such as the subnet mask, default gateway, and DNS server. Each active host on a given IP network must use a unique IP address. When two workstations use the same address, devices on the local network can receive conflicting Address Resolution Protocol (ARP) information associating that one IP address with different MAC addresses. As ARP entries update, traffic intended for the shared address may be sent to one workstation and then the other. This produces the intermittent or unreliable connectivity described when both systems are powered on. The problem may appear to disappear when either workstation is turned off because only one device then responds for that address. A technician should assign the new device an unused static address that is outside the DHCP scope or, where appropriate, configure it to obtain an address automatically through DHCP. Microsoft documents that duplicate IP addressing can cause network connectivity problems and provides guidance for detecting address conflicts. See Microsoft's duplicate IP address troubleshooting guidance and the CompTIA exam objectives resource.

QUESTION NO: 24

A technician is setting up storage in a server that only has SAS connectors for storage. The technician wants the server to utilize RAID 10 for increased performance. Which of the following storage types should the technician install?

A. NVMe M.2

B. Mechanical

C. mSATA

D. Optical

ANSWER: B

Explanation:

Mechanical is correct because a server limited to Serial Attached SCSI (SAS) storage connectors requires drives that use the SAS interface. Mechanical hard disk drives are commonly manufactured with SAS interfaces for enterprise server deployments, where SAS provides a robust, high-performance storage connection and supports multiple drives through a SAS controller or backplane. RAID 10 combines disk striping and mirroring: data is striped across mirrored drive pairs, improving read and write performance while maintaining redundancy. It requires at least four physical drives, so the technician should install a sufficient number of SAS mechanical hard drives to create the RAID 10 array. In practice, the selected drives must match the server's SAS backplane/controller specifications and should generally have compatible capacities and performance characteristics for efficient array operation. CompTIA's Core 1 objectives include identifying RAID types and storage-device interfaces, including SAS: CompTIA exam objectives. Seagate also describes SAS as an enterprise storage interface used with hard drives and server environments: What is SAS?.

QUESTION NO: 25

Atechnician is replacing all RJ45 cables in a customer environment. Which of the following are the BEST tools to execute the task? (Select TWO).

A. Optical fiber tester

B. Scissors

C. Cable tester

D. Crimper

E. Coaxial cable

F. Screwdriver

ANSWER: C D

Explanation:

Cable tester and **Crimper** are the appropriate tools for replacing RJ45 terminated copper Ethernet cabling. A crimper is used to secure an RJ45 modular plug onto the individual conductors of a properly prepared twisted-pair cable. This is necessary when the technician is building replacement cables to the required length or replacing a damaged connector. Proper crimping helps ensure that each conductor is seated in the plug's contacts and that the connector's strain-relief tab holds the cable jacket securely.

A cable tester is used after termination and installation to validate the new cable. It can check basic wiremap and continuity conditions, helping confirm that the conductors are connected end-to-end in the expected order and identifying common installation faults before the cable is put into service. Using the tester as part of the replacement workflow supports reliable Ethernet connectivity and efficient troubleshooting. These tools align with the CompTIA A+ Core 1 hardware and networking skills covering cable types, connectors, and appropriate networking tools. See the CompTIA exam objectives resources and the CompTIA Ethernet guide for related cabling and Ethernet context.

QUESTION NO: 26

Which of the following handles touch-screen operation on a mobile device?

A. Stylus

B. Liquid crystal display

C. Processor

D. Digitizer

ANSWER: D

Explanation:

Digitizer is correct because it is the hardware layer or component that detects touch input on a mobile device's screen. When a user touches the display with a finger or compatible stylus, the digitizer senses the location and characteristics of that input and converts it into electrical signals and coordinate data the device can interpret. The operating system and applications then use that data to perform the requested action, such as selecting an icon, scrolling a page, or drawing. In many mobile devices, the digitizer is integrated closely with the display assembly, which is why damage to a screen can affect both image output and touch responsiveness. Touchscreens commonly use capacitive sensing, in which a conductive finger changes the device's electrical field; some digitizers also support active stylus input for additional precision and pressure-related features. The display itself presents visual content, while the digitizer provides the touch-input capability that makes the display interactive. For an overview of touchscreen operation and capacitive touch technology, see Explain That Stuff: How Touchscreens Work and Encyclopaedia Britannica: Touch Screen.

QUESTION NO: 27

A technician is troubleshooting a computer that powers on but shuts down after several minutes of use. The issue occurs more quickly when the computer is running demanding applications. Which of the following are MOST likely causes? (Select TWO).

A. A failed CPU fan

B. Dried thermal paste

C. A depleted CMOS battery

D. An incorrect keyboard layout

E. A full print queue

ANSWER: A B

Explanation:

A failed CPU fan and dried thermal paste are likely causes because both can prevent heat from being transferred away from the processor. Under a demanding workload, CPU temperature rises quickly. Modern systems may reduce performance or shut down to prevent hardware damage when temperatures exceed safe limits.

The technician should inspect the fan operation, remove accumulated dust as appropriate, verify that the heat sink is securely attached, and renew thermal compound if it has dried out or is improperly applied. A depleted CMOS battery may reset firmware settings, but it does not normally cause heat-related shutdowns. Intel describes the importance of proper thermal management in its processor cooling guidance.

QUESTION NO: 28

Following a scheduled power outage, users report they cannot access the local intranet. A technician is able to ping the IP address of the server that is hosting the website. Which of the following serves is MOST likely offline?

A. Web

B. DNS

C. File

D. DHCP

ANSWER: B

Explanation:

DNS is the most likely service to be offline. The successful ping to the web server's IP address establishes that a network path to that host is available and that the server's IP configuration is reachable at the network layer. Users generally access an intranet by entering a hostname or fully qualified domain name, rather than memorizing and entering the server's numeric

IP address. Before a browser can connect to a named intranet site, the client must resolve that name to the correct IP address through the Domain Name System.

Following a power outage, a DNS server or its DNS service may fail to restart, may not have completed recovery, or may no longer be reachable by clients. In that situation, users cannot translate the intranet hostname into the web server's already-reachable IP address, producing an apparent inability to access the site. Testing the intranet directly by IP address and then using name-resolution tools such as `nslookup` would help validate this diagnosis. Microsoft documents that DNS provides name resolution for locating network resources and that DNS clients query DNS servers to resolve names. See Microsoft Learn: DNS overview and CompTIA A+ Core 1 study guide.

QUESTION NO: 29

An administrator is using an RJ45 connector to terminate a network cable. Which of the following cables is the administrator terminating?

A. Optical

B. Serial

C. Cat 6

D. USB

ANSWER: C

Explanation:

Cat 6 is correct because it is a balanced twisted-pair Ethernet cabling type that is commonly field-terminated with an eight-position, eight-contact modular plug, conventionally called an RJ45 connector in IT and CompTIA terminology. A Cat 6 horizontal cable contains four twisted copper pairs, and its eight individual conductors are placed into the connector in a recognized Ethernet pinout, such as T568A or T568B. A crimping tool secures the connector's contacts onto the conductors, producing a cable suitable for an Ethernet network interface, switch, router, or patch-panel connection.

Category 6 cabling is designed for high-performance Ethernet installations and is specified for frequencies up to 250 MHz. It supports 1000BASE-T over the standard 100-meter channel and can support 10GBASE-T over shorter, standards-defined distances, depending on the overall channel design and installation conditions. The Telecommunications Industry Association's cabling guidance identifies Category 6 as twisted-pair structured cabling, while Ethernet installation references describe terminating its four pairs using modular eight-contact connectors. See Fluke Networks' Category 6 cabling overview and Cisco's Ethernet cabling reference.

QUESTION NO: 30

A user reports a cell phone is getting hot. Which of the following are MOST likely to be possible causes? (Select THREE).

A. Using the device as a Wi-Fi hotspot

B. A cracked screen

C. A failing battery

D. Less than 15% free storage space on the phone

E. Privileged control

F. Recurring prompts to install OS updates

G. Granting too many application camera permissions

H. Too many open applications

ANSWER: A C H

Explanation:

Using the device as a Wi-Fi hotspot is a likely cause because tethering keeps the cellular and Wi-Fi radios active while the phone routes traffic for other devices. That sustained radio activity and data processing increase power draw, which produces heat. A failing battery is also a significant hardware concern: degraded or damaged lithium-ion batteries can develop abnormal internal resistance, generate excess heat during charging or discharge, and may present a safety risk. The device should be stopped from charging or heavy use and assessed if overheating is persistent, severe, or accompanied by swelling. Too many open applications can contribute when multiple applications are actively using processor time, memory, location services, networking, or background synchronization. Greater CPU/GPU workload and battery consumption naturally raise device temperature, particularly during demanding use or in a warm environment. These causes align with standard mobile-device troubleshooting: identify unusually power-intensive workloads, close unneeded apps, disable unnecessary tethering, and investigate potential battery failure. Apple's guidance on acceptable operating temperatures and overheating behavior is available in Keeping iPhone, iPad, and iPod touch within acceptable operating temperatures. Android users can also review Google's Help keep your Android device from overheating guidance.

QUESTION NO: 31

A technician is troubleshooting a computer that displays an incorrect date and time after being disconnected from power. Which of the following should the technician check FIRST? (Select TWO).

A. CMOS battery

B. Date and time settings in UEFI/BIOS

C. Operating system drive

D. Network cable

E. Video card

ANSWER: A B

Explanation:

The CMOS battery and the date/time settings in UEFI/BIOS are the appropriate items to check. The CMOS battery supplies low-level power that preserves firmware settings, including the system clock, while the computer is disconnected from external power. A depleted battery can cause the date, time, and other firmware settings to reset.

The technician should also verify the configured date and time in UEFI/BIOS after replacing the battery if necessary. The operating system drive, network cable, and video card do not maintain firmware clock settings. Dell documents that a depleted coin-cell battery can cause system date and time settings to reset. See Dell CMOS battery troubleshooting guidance.

QUESTION NO: 32

Each floor at a new corporate facility will have four printers available for all users to print from AH of the printers will be connected with RJ45 and not joined to a domain Which of the following needs to be set up to accomplish this task? (Select two).

A. Printer shares

B. DHCP server

C. Print server

D. Printer subnet

E. SMB configuration

F. Printer Wi-Fi settings

ANSWER: A C

Explanation:

Printer shares and a **Print server** provide the appropriate shared-printing design for this scenario. A print server centrally hosts and manages the printer queues for the Ethernet-connected printers. Users send documents to the server's shared queues rather than requiring separate, locally managed printer installations on every workstation. This centralizes driver deployment, queue configuration, job scheduling, monitoring, and administrative controls for each floor's printers. It also provides a consistent network path for all authorized users, which is especially helpful in a corporate facility with many workstations.

Printer shares make each configured queue discoverable and usable by client devices across the network. Sharing does not require the printers themselves to be members of an Active Directory domain; the print server can publish or otherwise make available the printer queues according to the organization's access and network configuration. Together, a print server and printer shares meet the need to provide common access to wired printers for multiple users while reducing per-device setup and simplifying ongoing support. Microsoft's documentation describes how Windows print servers manage shared printer queues and client connections: Print Management overview. CompTIA includes network and shared-printer configuration among the Core 1 printer-installation skills: CompTIA exam objectives.

QUESTION NO: 33

Which of the following scenarios best illustrate a need for VDI? (Select two).

A. An employee needs the ability to work remotely on a non-company-provided computer

B. A company that needs to store 10PB worth of data

C. An employee has latency-sensitive workflow requirements

D. A bank that has security concerns regarding employee activity

E. A payment processor that is planning on implementing virtual currency

F. An application developer who needs to configure network settings for an application

ANSWER: A D

Explanation:

"An employee needs the ability to work remotely on a non-company-provided computer" is an appropriate VDI use case because the user can connect from a personally owned endpoint while the managed desktop session, applications, and business data remain hosted centrally. This provides a consistent corporate workspace without requiring the organization to store sensitive data directly on the non-company device. Administrators can maintain the desktop image centrally, apply updates and policies consistently, and limit the exposure of data if the endpoint is lost, shared, or otherwise not under company management.

"A bank that has security concerns regarding employee activity" also illustrates a strong need for VDI. Centralized virtual desktops allow the bank to apply uniform security controls, restrict local storage or clipboard redirection when necessary, maintain controlled application configurations, and support centralized logging and auditing of user activity. Keeping the primary desktop environment and its data in the data center helps organizations with sensitive financial information reduce endpoint-data risk while improving administrative oversight. Microsoft describes Azure Virtual Desktop as enabling secure remote desktop access and centralized management of virtualized desktops: Microsoft Learn: What is Azure Virtual Desktop?. NIST also discusses virtual desktop infrastructure as a technology that can support centralized security management: NIST SP 800-125.

QUESTION NO: 34

Which of the following are default ports for HTTP and HTTPS traffic? (Select TWO).

A. 23

B. 25

C. 80

D. 143

E. 389

F. 443

ANSWER: C F

Explanation:

The default port for HTTP traffic is 80, and the default port for HTTPS traffic is 443. HTTP uses TCP port 80 for standard unencrypted web communications between a client, such as a browser, and a web server. When a user enters a web address with the `http://` scheme and no port is specified, the browser attempts a connection using port 80. HTTPS is HTTP protected with TLS encryption and, by default, uses TCP port 443. A browser similarly selects port 443 when connecting to an `https://` address without an explicit port number. Recognizing these well-known ports is important for troubleshooting web connectivity, configuring host-based or network firewalls, validating web-server listener settings, and identifying traffic during network analysis. Port assignments are maintained in the IANA Service Name and Transport Protocol Port Number Registry, which lists `http` as port 80 and `https` as port 443. Although a web service can be configured to listen on a nondefault port, 80 and 443 remain the conventional defaults used by clients unless a different port is included in the URL or connection configuration. See the IANA Service Name and Port Number Registry and RFC 9110: HTTP Semantics.

QUESTION NO: 35

In which of the following connection types would receiving power be a major factor? (Select two).

A. Fiber

B. Satellite

C. Cable

D. Cellular

E. DSL

F. Ethernet

ANSWER: D F

Explanation:

Cellular is correct because cellular connectivity depends on a powered client device, such as a smartphone, tablet, hotspot, or cellular modem. Unlike a wired access method that may be used by a stationary system with conventional AC power, cellular is frequently used in portable and mobile scenarios. Battery capacity, charging availability, and power-saving behavior directly affect whether the device can remain connected to the carrier network, so power reception and management are important practical considerations.

Ethernet is correct because Ethernet can deliver both data and electrical power through the same twisted-pair cable when Power over Ethernet is implemented. A powered device, such as an IP phone, wireless access point, IP camera, or some networked sensors, can receive operating power from Power Sourcing Equipment such as a PoE-capable switch or injector. This can eliminate the need for a local AC outlet at the device location. The applicable IEEE PoE standards define this power-delivery capability over Ethernet cabling. CompTIA includes Ethernet and cellular among the network connection technologies candidates must understand; see the CompTIA exam objectives. For PoE operation and terminology, see Cisco's Power over Ethernet overview.

QUESTION NO: 36

A technician is installing multiple plain old telephone service lines for a client. Which of the following tools should the technician use to attach the cables? (Select two).

A. Punchdown tool

B. Multimeter

C. Toner probe

D. Wi-Fi analyzer

E. Loopback plug

F. Network tap

ANSWER: A C

Explanation:

Punchdown tool is used to terminate individual POTS conductors onto insulation-displacement connections, such as 66 blocks, 110 blocks, telephone patch panels, and compatible keystone jacks. The tool seats the conductor securely in the terminal and trims excess wire where applicable, making it the primary termination tool for this type of cabling work. **Toner probe** is used with a tone generator to identify and trace the correct telephone pair among multiple installed or unterminated cables. In a multi-line POTS installation, accurately identifying each pair before placing it on its assigned terminal is necessary for orderly, reliable line attachment and documentation. Together, these tools support the practical workflow of tracing the intended pair and then terminating it on the appropriate punchdown hardware. CompTIA's exam-objectives resources include cabling tools and their appropriate uses as Core 1 knowledge areas; see CompTIA Exam Objectives. For additional technical background on tracing cable pairs using tone and probe equipment, see Fluke Networks' tone generator and probe overview.

QUESTION NO: 37

When trying to print, a is offline. Other users can print to the same printer without error. Which of the following is the first step the technician should take to resolve this issue?

A. Check the user's print queue settings.

B. Check the printer's IP address.

C. Check the user's network settings.

D. Check the printer's firmware version.

ANSWER: A

Explanation:

Check the user's print queue settings. Because other users can print successfully to the same device, the printer itself, its shared connection, and its general availability are working. The issue is therefore isolated to the affected user's workstation or user-specific print configuration. A technician should first open that user's print queue and verify that the queue is not paused, that an offline status has not been selected, and that no stuck or failed job is preventing subsequent jobs from processing. Clearing a problematic job, resuming the queue, or taking the queue out of offline mode can restore printing without changing shared printer infrastructure. This follows efficient troubleshooting practice: identify the scope of the issue and begin with the component unique to the affected user before making broader changes. Windows provides controls for viewing and managing queued documents and printer status through the printer queue. Microsoft documents printer queue management at View the print queue in Windows. For general diagnostic guidance on Windows printing problems, including checking the selected printer and print queue, see Fix printer connection and printing problems.

QUESTION NO: 38

A user's Windows computer started running slowly after the installation of a CAD program. The computer has intermittent timeouts and often has to be rebooted to restore functionally. The computer seems to work correctly if the application is not running. Which of the following should the technician do NEXT to help troubleshoot the issue? (Select TWO).

A. Replace the video card.

B. Research the requirements of the application.

C. Install a new case fun.

D. Run chkdsk on the HD

E. Check the Event Viewer logs.

F. Reinstall the application.

ANSWER: B E

Explanation:

Research the requirements of the application is an appropriate next step because the symptoms began after installing a resource-intensive CAD application and disappear when that application is not running. CAD software commonly has specific minimum and recommended requirements for processor capability, installed memory, graphics hardware and driver support, available storage, and supported operating-system versions. Comparing those requirements with the computer's actual configuration helps the technician determine whether the application is exceeding available system resources or whether an update or upgrade is needed. CompTIA's troubleshooting process emphasizes identifying the problem and establishing a probable cause before making changes; reviewing documented application requirements supports that evidence-based approach. See the CompTIA A+ Core 1 study guide.

Check the Event Viewer logs is also a correct next diagnostic action. Windows event logs can provide time-correlated evidence of application crashes, driver faults, storage errors, low-resource conditions, or unexpected shutdowns occurring while the CAD software runs. Reviewing these entries allows the technician to narrow the cause using recorded system data rather than guessing. Microsoft documents how to access and use Event Viewer at Open Event Viewer.

QUESTION NO: 39

A company is testing the latest model of a laptop. After turning on the laptop, there is a noticeable burning smell. Which of the following steps should a technician take to troubleshoot the laptop issue? (Select two).

A. Turn it off and disconnect all power sources.

B. Submit an emergency request to the local facilities manager.

C. Check for foreign objects, liquid spills, and internal damage.

D. Contact the vendor and submit a return request.

E. Remove the device from the MDM.

F. Try an alternate AC adapter.

ANSWER: A C

Explanation:

Turn it off and disconnect all power sources. is the immediate first step because a burning smell can indicate overheating, an electrical short, damaged insulation, or a failing battery or power component. Shutting the laptop down and removing external power stops electrical energy from continuing to feed a potential fault, limits additional component damage, and reduces the risk of burns, smoke, or fire. The technician should avoid further operation until the device can be safely inspected.

Check for foreign objects, liquid spills, and internal damage. is an appropriate next troubleshooting action after power has been removed. A visual inspection can identify debris blocking vents or contacting circuitry, evidence of a spill or corrosion, melted connectors, swollen battery components, damaged cables, or discoloration around internal parts. These observations help isolate the likely source of the odor while following safe hardware-handling practices. Electrical-safety guidance emphasizes de-energizing equipment before inspecting or servicing it. See OSHA electrical safety resources. These actions also align with the CompTIA A+ Core 1 focus on safe hardware troubleshooting and operational procedures; see the CompTIA A+ certification page.

QUESTION NO: 40

A user reports that a laser printer is producing faded output on every page. Which of the following actions should a technician take to resolve the issue? (Select TWO).

A. Replace the toner cartridge.

B. Disable toner-save mode.

C. Replace the ink cartridge.

D. Clean the platen glass.

E. Replace the pickup rollers.

ANSWER: A B

Explanation:

Replacing the toner cartridge and disabling toner-save mode are appropriate actions. A low or depleted toner cartridge may not supply enough toner to the imaging process, resulting in light or faded text and images. Replacing the cartridge restores the printer's toner supply.

Toner-save or economy mode intentionally reduces the amount of toner applied to each page to conserve consumables. If this setting is enabled, print output can appear lighter than expected. Disabling the setting returns the printer to normal print density. HP provides print-quality troubleshooting information in its laser printer image-defect guidance.

QUESTION NO: 41

A company issued smartphones to users who work from home. The devices are enrolled and configured within the company's MDM, and hardening profiles were deployed to each device for greater security. Which of the following services best enhances security for remote users accessing company resources? (Select two).

A. Two-factor authentication

B. Managed corporate applications

C. Cloud data synchronization

D. Automated device setup

E. GPS location tracking

F. PIN code enforcement

ANSWER: A F

Explanation:

Two-factor authentication and PIN code enforcement provide complementary protections for company-issued smartphones used remotely. Two-factor authentication strengthens access to company resources by requiring a user to prove identity with more than one authentication factor. This means that a stolen or guessed password alone is insufficient to sign in, substantially reducing the risk of unauthorized access to corporate applications, data, and remote services. NIST’s digital

identity guidance describes the value of multi-factor authentication and the use of distinct authentication factors for stronger assurance: NIST SP 800-63B.

PIN code enforcement protects the device itself by requiring a local unlock secret before its contents, managed applications, and stored authentication material can be accessed. In an MDM deployment, enforcing a sufficiently strong device PIN is a practical baseline control that helps protect a phone if it is lost, stolen, or temporarily left unattended. It also supports broader mobile security policies, such as requiring a compliant device before granting access to organizational resources. Microsoft documents device-compliance policies that can require password or PIN settings on managed devices: Microsoft Intune device compliance policies.

QUESTION NO: 42

Which of the following connectors can be plugged into a Thunderbolt 3 port on a laptop?

A. miniUSB

B. microUS3

C. USB-A

D. USB-C

ANSWER: D

Explanation:

USB-C is correct because Thunderbolt 3 uses the USB Type-C connector and receptacle shape. Therefore, a USB-C plug can be inserted directly into a Thunderbolt 3 port without needing a physical adapter. Thunderbolt 3 combines high-speed data capabilities with the reversible USB-C connector design, allowing the port to support Thunderbolt devices as well as compatible USB data devices. The connector's reversible design also means it can be inserted in either orientation, which is a defining physical characteristic of USB-C. Although the capabilities available after connecting a device depend on the laptop, cable, device, and supported protocols, USB-C is the connector type that physically fits a Thunderbolt 3 port. Intel's Thunderbolt documentation identifies Thunderbolt 3 as using the USB-C connector, and the USB Implementers Forum describes USB Type-C as the connector and cable specification used for modern USB connections. See Intel Thunderbolt Technology FAQ and USB-IF USB Type-C information.

QUESTION NO: 43

A technician made several upgrades to a computer and then determined the power supplied by the PSU is insufficient. Which of the following would MOST likely cause the insufficiency? (Select TWO).

A. Replacing the HDD with an SSD

B. Upgrading the firmware

C. Adding an optical drive

D. Adding more RAM

E. Adding a CMOS battery

F. Upgrading the graphics card

ANSWER: C F

Explanation:

Adding an optical drive and upgrading the graphics card are the upgrades most likely to make an existing PSU inadequate. A graphics-card upgrade can substantially increase total system demand because the card draws power through the motherboard slot and, for many performance cards, one or more dedicated PCIe power connectors. Its demand can rise

sharply during gaming, rendering, or other GPU-intensive workloads, so PSU capacity must be evaluated against the card manufacturer's recommended system-power requirement.

An added optical drive also increases the system's load by requiring power from the PSU for its motor, laser, and drive electronics. Although its sustained draw may be modest, startup and disc-spin activity add load to the available power budget. When several components are added or upgraded, the technician should calculate combined component requirements, account for peak demand, and retain sufficient capacity for stable operation and future expansion. Corsair's PSU guidance discusses sizing a unit according to component power requirements and headroom, while NVIDIA publishes board-power and system-power recommendations for its graphics products: Corsair PSU selection guidance and NVIDIA graphics-card specifications.

QUESTION NO: 44

Which of the following cloud models would multiple organizations in the same industry most likely use?

A. Public

B. Hybrid

C. Community

D. Private

ANSWER: C

Explanation:

Community is correct because a community cloud is intended for use by multiple organizations that have shared requirements, such as common security controls, regulatory obligations, mission objectives, or data-handling policies. Organizations in the same industry frequently have these common concerns. For example, healthcare organizations may need infrastructure and services designed around privacy requirements for patient information, while financial organizations may need to meet similar governance, audit, and risk-management expectations. A community cloud lets participating organizations share an environment that is purpose-built and governed for those collective needs, rather than each organization building and operating a completely separate environment. It may be managed by one or more member organizations or by a third party, and it can be hosted on or off premises. This model is distinct in that access and design are focused on a defined community with shared concerns. CompTIA includes community cloud among the cloud deployment models candidates should understand under the cloud-computing concepts objective. The National Institute of Standards and Technology defines a community cloud as infrastructure provisioned for exclusive use by a specific community of consumers with shared concerns. See NIST Special Publication 800-145 and the CompTIA exam objectives resource page.

QUESTION NO: 45

A mechanical engineer's PC has started randomly shutting off whenever the engineer attempts to render a design. The mechanical engineer states that the PC has worked for three years without issue. Which of the following should the technician perform first to diagnose the issue? (Select two).

A. Listen for POST beeps when turning on the PC.

B. Check if the computer is overheating.

C. Run chkdsk.

D. Reinstall the operating system.

E. Check if the graphics card is compatible with the motherboard.

F. Replace the HDD.

G. Test the power supply unit for stable power delivery under load.

ANSWER: B G

Explanation:

Checking whether the computer is overheating is an appropriate first diagnostic step because rendering places sustained, heavy demand on the CPU and often the GPU. After three years of operation, accumulated dust, degraded thermal compound, failed or obstructed fans, and reduced airflow can prevent adequate cooling. A system may then shut down abruptly through thermal-protection mechanisms when component temperatures exceed safe operating limits. The technician should inspect fans and heatsinks, verify airflow, and monitor CPU and GPU temperatures while reproducing the rendering workload.

Testing the power supply unit is also an appropriate first step. Rendering can substantially increase total system power draw, and an aging or failing power supply may be unable to maintain stable voltage under that load. The technician should inspect power connections and use an appropriate PSU tester, multimeter, or known-good replacement power supply to evaluate power stability. These are targeted, non-destructive hardware diagnostics that directly address shutdowns occurring only during high-load operation, consistent with CompTIA's hardware troubleshooting focus. See the CompTIA exam objectives resource and Intel's guidance on processor temperature and thermal behavior.

QUESTION NO: 46

Which of the following port numbers are associated with email traffic? (Select two).

A. 23

B. 25

C. 67

D. 110

E. 137

F. 443

ANSWER: B D

Explanation:

The correct email-related ports are **25** and **110**. Port 25 is the well-known port for Simple Mail Transfer Protocol (SMTP). SMTP is used to transfer email messages, particularly for server-to-server mail delivery; it may also be used for message submission in some configurations. The Internet Assigned Numbers Authority registers SMTP on TCP port 25, making it a fundamental port to recognize for email transport and a core networking fact tested at the CompTIA A+ level.

Port 110 is the well-known port for Post Office Protocol version 3 (POP3). A mail client uses POP3 to retrieve messages from a mailbox on a mail server. POP3 traditionally downloads messages to the client, enabling users to access received email locally. IANA's service-name registry identifies port 110 as POP3, while its registry identifies port 25 as SMTP. Together, these ports represent two distinct, common functions in traditional email systems: SMTP handles sending and relaying messages, and POP3 handles receiving messages from a server. See the IANA SMTP service registration and the IANA POP3 service registration.

QUESTION NO: 47 - (HOTSPOT)

A customer has contacted you about building two new desktops. The first desktop will be a gaming workstation. The customer requirements include:

Playing the newest games at a high frame rate

Fast game load times

Enough storage to have several games installed at once

High-end audio

No concern about cost

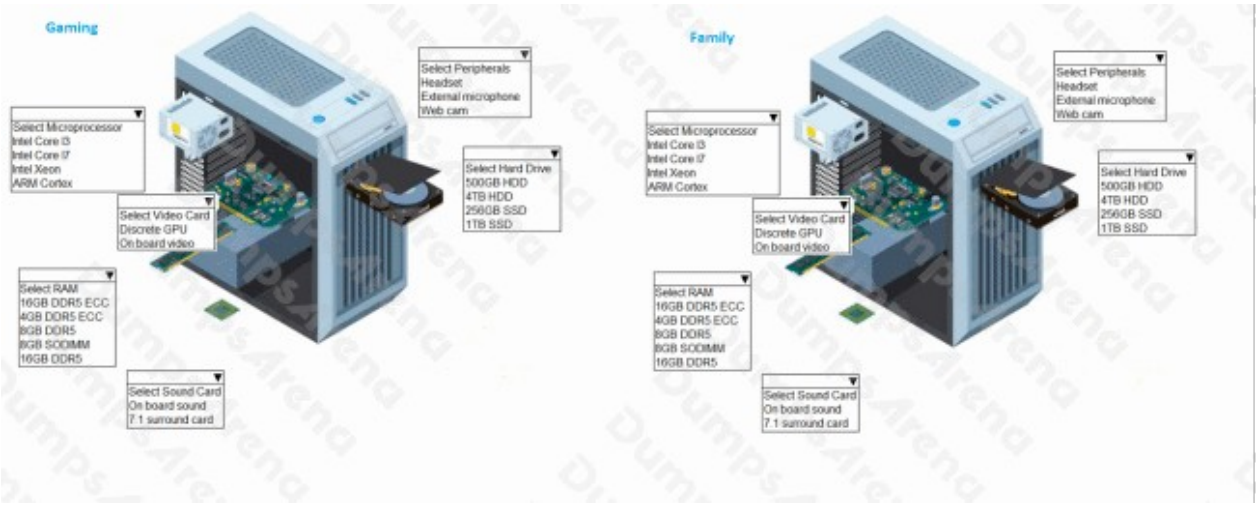
Running the current Windows OS

The second workstation will be a family workstation. The requirements include:

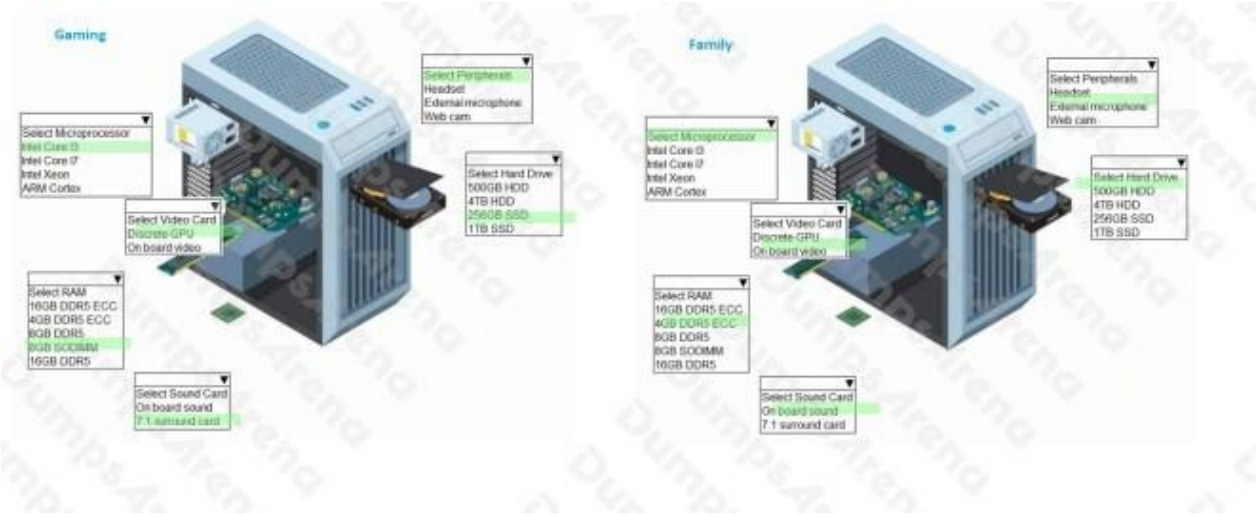
Capability for word processing, videoconferencing, and basic web surfing

Minimal cost, as long as it meets the requirements

Running the current Windows OS



ANSWER:



Explanation:

The correct configurations balance each computer's components with its stated purpose. The gaming system needs an Intel Core i7 processor and a discrete GPU to provide the CPU and graphics performance needed for current games at high frame rates. Installing 16GB of DDR5 memory gives the system sufficient modern memory capacity for games, Windows, and background applications. A 1TB SSD supplies both the storage capacity needed for several installed games and the fast read performance that reduces game and operating-system loading times. A headset and a 7.1 surround sound card provide the requested high-end audio experience. These are appropriate performance-focused selections when cost is not a constraint.

The family system should use an Intel Core i3 processor, 8GB of DDR5 RAM, onboard video, and onboard sound. This level of hardware is suitable for everyday productivity software, web use, and video calls without adding unnecessary component cost. A webcam is the needed peripheral for videoconferencing. The family system should use the 500GB HDD, since it provides more than enough room for the current Windows operating system, common office files, web-browser data, and normal household use while supporting the requirement to keep costs as low as possible. Microsoft lists a minimum of 64GB of storage for Windows 11, so a 500GB drive comfortably exceeds the operating-system requirement. See Microsoft's Windows 11 specifications. SSD storage is especially appropriate in the gaming configuration because solid-state storage

improves loading responsiveness; the Microsoft PC performance guidance also identifies storage and system resources as factors that affect performance.

QUESTION NO: 48

A user with an older laptop is unable to connect to the office network after new access points were installed. The user confirms that from home the laptop can connect wirelessly to the network. Which of the following should the user to do to quickly resolve the issue?

A. Connect a new USB wireless adapter.

B. Install a new SSD

C. Connect a new biometric device.

D. Install a new Bluetooth card.

ANSWER: A

Explanation:

Connect a new USB wireless adapter is the appropriate rapid resolution because the laptop's existing wireless hardware is likely incompatible with the radio band, Wi-Fi generation, or security capabilities used by the newly installed office access points. An older internal adapter may support only legacy 2.4 GHz Wi-Fi, while newer access points may be configured primarily or exclusively for 5 GHz or newer standards. The fact that the laptop still connects from home shows that its general wireless functionality is intact; the problem is most likely compatibility with the office wireless environment rather than a failed laptop component. A USB wireless adapter that supports the office network's required Wi-Fi standard and bands can be attached without disassembling the laptop or replacing its internal wireless card. This makes it a practical, low-impact troubleshooting and remediation step. CompTIA's A+ Core 1 exam coverage includes wireless networking technologies and client connectivity considerations; see the CompTIA A+ certification page and CompTIA's exam objectives resource page. In practice, the replacement adapter should support the access points' configured band and authentication requirements.

QUESTION NO: 49

A user contacted the help desk about files that disappeared from a laptop. The technician discovered during troubleshooting that the drive was corrupt due to a possible mechanical failure, but the files were still readable. Which of the following actions did the technician take during troubleshooting?

(Select two).

A. Checked S.M.A.R.T. information

B. Made sure the replacement drive was compatible

C. Ran CHKDSK

D. Reseated the HDD connector

E. Increased the page file size

F. Updated the firmware

ANSWER: A B

Explanation:

Checking S.M.A.R.T. information is an appropriate diagnostic action when a hard drive shows corruption and possible mechanical failure. Self-Monitoring, Analysis, and Reporting Technology exposes health indicators collected by the drive, such as reallocated-sector counts, pending sectors, read-error rates, and spin-related attributes. Reviewing these indicators helps the technician substantiate a suspected physical drive problem and determine that the disk should be treated as

unreliable. This aligns with the hardware-troubleshooting knowledge assessed in the CompTIA A+ Core 1 objectives; see CompTIA Exam Objectives and the drive-health guidance from Seagate.

Making sure the replacement drive is compatible is also necessary once the evidence indicates a failing laptop drive. The technician must select a replacement that works with the laptop's supported storage interface and physical form factor, such as an appropriate SATA or M.2 device and the correct size. Compatibility verification supports a successful repair and enables the user's readable files to be copied or recovered to dependable storage before the failing drive becomes inaccessible. In a potential mechanical-failure situation, protecting accessible data and preparing compatible replacement storage are key parts of resolving the incident safely.

QUESTION NO: 50

A user reports that a printer pulls multiple sheets of paper from the paper tray instead of a single sheet. Which of the following should a technician

investigate to resolve this issue? (Select two).

A. Toner cartridge

B. Tractor feed

C. Pickup roller

D. Separation pad

E. Duplexer

F. Fuser

ANSWER: C D

Explanation:

"Pickup roller" and "Separation pad" are the appropriate components to investigate when a printer feeds multiple sheets from an input tray. The pickup roller is the rubberized feed component that contacts the top sheet and advances it into the paper path. Over time, its surface can accumulate paper dust or become smooth and worn, reducing its ability to feed media consistently. The separation pad works with the pickup mechanism to create enough friction and resistance that only the top sheet proceeds while additional sheets remain in the tray. A worn, dirty, glazed, or damaged separation pad commonly permits more than one sheet to enter the paper path, producing multi-feeds and often subsequent paper jams. A technician should inspect these components for wear and contamination, clean them only according to the printer manufacturer's service guidance, and replace them when they no longer provide reliable paper handling. The technician should also confirm that supported paper is loaded correctly, since paper condition and tray setup affect feed performance. These items align with CompTIA A+ Core 1 printer troubleshooting objectives concerning paper-feed issues and printer maintenance. See CompTIA Exam Objectives and HP paper-feed troubleshooting guidance.

QUESTION NO: 51

A user's laptop has been slow to respond for the past few days. The user has run a virus scan, deleted temporary files, closed unnecessary programs, and rebooted the laptop, but the issue persists. Which of the following steps should the technician take next?

A. Perform a RAM upgrade.

B. Replace the laptop's hard drive.

C. Bench test the laptop.

D. Run a firmware update.

E. Check Task Manager to identify the process or resource causing the slowdown.

ANSWER: E

Explanation:

Check Task Manager to identify the process or resource causing the slowdown is the appropriate next step because the reported symptom is broad and does not yet establish a hardware fault. A technician should first gather measurable evidence and form a theory before making invasive changes such as replacing components or updating device firmware. Task Manager can show whether the processor, memory, storage, network, or a specific process is persistently consuming resources. This helps distinguish, for example, a resource-intensive background process from high disk activity or memory pressure. The technician can then target the corrective action based on the observed bottleneck and verify that performance improves afterward. Microsoft documents that Task Manager provides real-time views of running processes and system resource utilization, including CPU, memory, disk, and network activity. This approach follows CompTIA's troubleshooting methodology: identify the problem, establish a theory of probable cause, test that theory, and only then implement a solution. See Microsoft Support: How to use Task Manager in Windows and CompTIA Exam Objectives.

QUESTION NO: 52

A user requested upgrades to a company-issued laptop to increase its performance while working with a large database stored on drive

C.

Which of the following tasks should a systems administrator complete to BEST meet this goal? (Select TWO).

A. Configure RAID 1.

B. Install a hybrid drive.

C. Upgrade to a 1GB NIC.

D. Increase the RAM.

E. Migrate to an SSD.

F. Upgrade the power supply.

ANSWER: D E

Explanation:

Increasing the RAM and migrating to an SSD directly address the two primary local performance constraints involved in working with a large database: available working memory and storage input/output speed. More RAM allows the operating system and database application to retain a larger amount of actively used data, program code, and file-system cache in memory. This reduces paging and decreases the frequency with which the laptop must retrieve data from the C: drive. An SSD provides substantially lower latency and faster random-read performance than a mechanical hard disk, which is especially valuable when a database performs frequent, nonsequential reads and writes to indexes, tables, temporary files, and transaction data. Together, these upgrades improve responsiveness during searches, queries, updates, and other database-intensive tasks. CompTIA's A+ Core 1 objectives include selecting and installing appropriate storage and memory upgrades as part of hardware support and performance-oriented troubleshooting. See the CompTIA exam objectives resource page and Microsoft's guidance on hardware considerations for performance tuning.

QUESTION NO: 53

A technician receives several error alerts on a server after an unexpected reboot. A message states that one or more disks are in a degraded state. When the technician advances to the next error message, it indicates the OS is missing. Which of the following are the MOST likely causes of these errors? (Choose two.)

A. Missing drives in the OS

B. RAID failure

C. Bootable device not found

D. Data loss

E. Controller failure

F. CMOS corruption

G. TPM malfunction

ANSWER: B C

Explanation:

“RAID failure” is a most likely cause because a degraded-state alert is generated when a RAID array has lost redundancy or cannot fully access one of its member disks. This can occur after a member drive fails, becomes disconnected, or is otherwise no longer available to the RAID controller. The array may remain operational in a degraded state depending on its RAID level, but it requires prompt investigation and replacement or recovery of the affected component to restore fault tolerance. RAID troubleshooting, storage devices, and boot issues are within the hardware and troubleshooting areas covered by the CompTIA A+ Core 1 objectives: CompTIA exam objectives.

“Bootable device not found” is also a most likely cause of an operating-system-missing message. During startup, firmware must identify a valid boot device and locate boot files on the configured boot volume. If the system cannot access the RAID logical volume, the boot device is unavailable, or the boot order no longer points to the correct device, startup can report that no operating system is present. Microsoft documents that startup recovery processes address failures involving the boot environment and the files required to start Windows: Microsoft boot troubleshooting guidance.

QUESTION NO: 54

A company is designing a data center environment where a critical requirement is highly available computing. Which of the following types of memory should an administrator choose to install in the servers?

A. DDR5

B. ECC

C. DDR4

D. Dual-channel

ANSWER: B

Explanation:

ECC is the appropriate choice for servers supporting highly available computing because it adds error-detection and error-correction capability to system memory. Random, transient bit errors can occur in RAM due to electrical interference, component degradation, or environmental factors. In a server environment, an uncorrected memory error can corrupt data being processed, cause an application failure, or lead to an operating-system crash. ECC memory uses additional check bits to identify errors; standard ECC implementations can correct a single-bit error and detect certain multi-bit errors. This lets the system continue operating when a correctable memory error occurs, improving reliability and reducing the likelihood of downtime caused by memory faults. Server-class platforms also commonly report corrected ECC events through hardware-management logs, allowing administrators to identify a degrading DIMM and replace it proactively. The processor and motherboard must both support ECC for this protection to function. Memory generation and channel configuration describe performance or architecture characteristics, but the error-correction feature is the key requirement when availability and data integrity are priorities. See Intel’s ECC memory overview and Micron’s server DRAM information.

QUESTION NO: 55

A technician replaced a failed PSU on a high-end workstation P

C.

Now, the PC fails to POST and does not stay turned on for more than five seconds. Which of the following power connections was most likely forgotten during installation?

A. 5V

B. 12V CPU power connector (ATX12V/EPS12V)

C. 120V

D. 220V

ANSWER: B

Explanation:

The **12V CPU power connector (ATX12V/EPS12V)** is the most likely connection to have been missed. A high-end workstation motherboard requires not only the main motherboard power connector but also dedicated 12 V power for the processor voltage-regulation circuitry. This connection is commonly a four-pin, eight-pin, or additional CPU/EPS connector located near the CPU socket. Workstation-class boards may require more than one CPU power connection, particularly when supporting high-core-count processors or demanding workloads.

Without this dedicated 12 V feed, the board may receive enough standby or initial power to begin its startup sequence, spin fans briefly, or illuminate LEDs. However, it cannot reliably supply the processor with the required regulated power. Firmware or PSU protection behavior can then shut the system down within seconds, preventing successful Power-On Self-Test.

During PSU replacement, technicians should verify that every required motherboard connector is attached securely and that CPU/EPS cables are used for CPU power rather than similarly shaped PCIe power cables. CompTIA's A+ objectives include identifying power-supply connectors and troubleshooting power-related hardware issues: CompTIA exam objectives. Intel also documents the importance of proper processor-platform power connections: Intel Support.

QUESTION NO: 56

A user dropped a laptop while it was turned on. The hard drive now makes a clicking sound, and the laptop will not start up. Which of the following most likely explains this

situation?

A. The hard drive bracket screws are lose.

B. The hard drive jumpers need to be reseated.

C. The hard drive is damaged.

D. The SATA cable is lose.

ANSWER: C

Explanation:

The hard drive is damaged. A traditional hard disk drive contains rapidly spinning magnetic platters and delicate read/write heads that normally float extremely close to the platter surfaces. Dropping a laptop while the drive is operating can cause a head crash or damage the head-positioning mechanism, spindle motor, or platters. A repetitive clicking sound following such an impact is a common symptom of the drive being unable to initialize or accurately locate data, often because its heads or internal mechanical components have failed. Since the laptop cannot start, the damage likely prevents the system from reading the boot files and operating system from the drive. The appropriate response is to stop repeatedly attempting to power on the system, as further operation can worsen physical media damage. The drive should be replaced, and, if the data is important and not backed up, recovery should be evaluated by a qualified data-recovery provider rather than attempting repairs. CompTIA Core 1 troubleshooting expects technicians to recognize clicking or grinding from a mechanical hard drive as an indicator of physical drive failure, particularly after a drop. See Seagate's guidance on clicking hard drives and Microsoft's overview of backing up and restoring files.

QUESTION NO: 57

A user reboots a machine. On rebooting, the user hears one beep, and then an error message is displayed. Which of the following are MOST likely causing this issue? (Select TWO).

A. RAM module

B. Graphics card

C. CPU

D. Boot order

E. USB flash drive

F. Power supply

ANSWER: D E

Explanation:

A single startup beep commonly indicates that the system has completed its initial power-on self-test sufficiently to begin the boot process. Because the error appears after that point, the most likely issue is that firmware is attempting to start from an unavailable or nonbootable device rather than from the intended operating-system drive. **Boot order** is therefore a likely cause: an incorrect firmware boot priority can direct the computer to a device that has no valid boot loader or operating system. **USB flash drive** is also a likely cause because a connected removable drive can be selected before the internal drive when USB boot is enabled or prioritized. Removing the flash drive, or changing the boot priority so that the correct internal boot device is first, typically restores normal startup. This follows the A+ troubleshooting distinction between successful POST indications and failures that occur during operating-system boot selection. Microsoft's boot troubleshooting guidance discusses startup failures after firmware initialization, and CompTIA's exam-objectives resources include hardware and boot-process troubleshooting domains: Microsoft Windows boot diagnostics and CompTIA exam objectives.

QUESTION NO: 58

A client wants to connect an external keyboard to an Android tablet. Which of the following connection types are appropriate for this task? (Select TWO).

A. DVI

B. Infrared

C. Lightning

D. USB-C

E. PS/2

F. Bluetooth

ANSWER: D F

Explanation:

USB-C and Bluetooth are appropriate connection types for an external keyboard used with an Android tablet. A USB-C keyboard can connect directly to a tablet with a USB-C port, or a conventional USB keyboard can be attached through a compatible USB On-The-Go (OTG) adapter. Android supports USB human interface devices, including keyboards, enabling physical-key input without requiring a separate driver in typical supported configurations. Bluetooth is also a standard wireless method for pairing external keyboards with Android devices. After the keyboard is put into pairing mode, the user can pair it from the tablet's Bluetooth settings and use it for typing and navigation. These two methods cover the common wired and wireless keyboard-connection approaches expected for modern Android tablets. The Android documentation describes support for USB host mode and USB accessories, while its Bluetooth documentation covers connecting and

managing Bluetooth peripherals. See the Android Open Source Project USB accessories documentation and Google Android Bluetooth help.

QUESTION NO: 59

The Wi-Fi network in the office is experiencing slow connection speeds. Which of the following should the technician check first on the access point?

A. Transmit power settings

B. Security settings

C. Firmware version

D. Location

ANSWER: A

Explanation:

Transmit power settings is the appropriate first item to check because it directly controls the access point's radio-frequency coverage cell and the signal level received by clients. Wi-Fi clients select data rates based partly on signal quality; when received signal is weak, clients commonly fall back to lower modulation and coding rates, reducing effective connection speed. An incorrectly low transmit-power value can therefore create weak coverage and low throughput, particularly for users farther from the access point. Power that is not appropriately planned can also create an unbalanced wireless cell, making roaming and overall airtime use less efficient. The technician should verify the configured power level, whether automatic radio-resource management is enabled, and whether the setting is appropriate for the office's size, client density, antenna design, and neighboring access points. Cisco's wireless guidance explains that transmit-power management is used to maintain appropriate RF coverage and mitigate changing RF conditions. CompTIA's A+ Core 1 objectives also include wireless networking configuration and troubleshooting concepts, including factors that affect wireless performance. See Cisco's transmit-power management guidance and CompTIA exam objectives resources.

QUESTION NO: 60

A technician identified an issue on a workstation, obtained details from the user, and made a backup of the system. Which of the following should the technician do NEXT?

A. Determine the next steps to resolve the issue and document it.

B. Design a plan of action to resolve the issue and implement the solution.

C. Document the findings, actions, and outcomes.

D. Establish a theory of probable cause, researching internally or externally as needed.

ANSWER: D

Explanation:

Establish a theory of probable cause, researching internally or externally as needed, is the appropriate next step in CompTIA's troubleshooting methodology. The technician has already completed the initial identification phase by gathering user information and identifying the issue. Creating a backup is also a prudent precaution before making changes that could affect user data or system configuration. With the issue identified and the system protected, the technician should develop a likely explanation for the symptoms. This can involve checking event logs, reviewing recent hardware or software changes, consulting internal knowledge bases and documentation, or using reputable vendor resources. The goal is to form a focused, evidence-based hypothesis that can be tested before changes are implemented. Establishing a probable cause helps prevent unnecessary actions and supports an efficient, methodical repair process. After the likely cause has been confirmed, the technician can create and implement an appropriate remediation plan, verify full system functionality, and document the work performed. CompTIA's Core 1 exam objectives explicitly include establishing a theory of probable cause as the second step of the troubleshooting process. See the CompTIA exam objectives resource and the CompTIA A+ certification page.

QUESTION NO: 61

A technician is relocating a router access point farther away from the modem to optimize signal coverage for a SOHO client. Which of the following will the technician most likely use to complete the relocation? (Select two).

A. Punchdown tool

B. Crimper

C. Clamp-style wire stripper

D. Network tap

E. Wi-Fi analyzer

F. Loopback plug

ANSWER: B E

Explanation:

Crimper and **Wi-Fi analyzer** are appropriate tools for this relocation. Moving an access point farther from the modem commonly requires a longer twisted-pair Ethernet run to preserve the wired backhaul connection. A crimper is used to terminate an Ethernet cable with modular connectors when the technician must make a custom-length cable or replace a connector during installation. This supports placing the access point in a better physical location rather than limiting placement to the existing cable length.

A Wi-Fi analyzer supports the coverage-optimization part of the task. Before and after moving the access point, the technician can measure received signal levels, identify competing wireless networks and interference, and observe channel utilization. Those measurements help validate that the new placement improves coverage for the SOHO environment and can guide channel selection if needed. Together, these tools address both the physical wired extension and verification of the wireless result. CompTIA's A+ certification objectives include installing and configuring basic wired and wireless networks and using appropriate networking tools; see the CompTIA A+ certification page. For background on wireless site assessment and signal measurements, see Cisco's wireless network design guidance.

QUESTION NO: 62 - (DRAG DROP)

A natural disaster occurred, and the storage system for the development team is unrecoverable. The technician is preparing replacement storage arrays that include a hypervisor with the capacity to support several virtual machines. Two separate bays are available, and both should be utilized.

Requirements for the primary array include the following:

• No need to be scalable

• Very fast on reads

• Fault tolerance of one drive

• Ability to function with only one drive

• Easily recoverable data

• High redundancy

• Minimum number of drives

Requirements for the secondary array include the following:

• Fault tolerance of one drive

• Total space of 600G3

• Best write performance

• Minimum number of drives

Instructions:

Drag and Drop the appropriate Hard Drives. Then Open each array to complete the configuration.

ANSWER:

Explanation:

The primary array should use two 120 GB SSDs configured as RAID 1. RAID 1 stores the same data on both members of a mirror, so the array can continue operating when one drive fails. This directly provides the requested single-drive fault tolerance, high redundancy, and the ability to function from one remaining disk. Because either mirror member contains a complete copy of the data, recovery is straightforward: after replacing a failed drive, the array rebuilds the replacement from the still-functioning member. RAID 1 also provides strong read performance because reads can be serviced from either mirrored disk. Two drives is the minimum required for this design, and its usable capacity is 120 GB.

The secondary array should use four 300 GB SSDs configured as RAID 10. RAID 10 combines mirrored drive pairs with striping across those pairs. Its mirrored component means the array tolerates the loss of one drive while keeping the data available. Its striping component spreads writes across the mirrored pairs, making it the suitable choice where high write

performance is required along with redundancy. RAID 10 has a minimum requirement of four drives. With four 300 GB SSDs, the raw capacity is 1,200 GB, and mirroring reserves half that capacity for duplicate data, leaving exactly 600 GB usable. This fulfills the specified capacity, one-drive fault-tolerance, performance, and minimum-drive requirements in a single array configuration. See the RAID overview in the IBM RAID levels documentation and the RAID 10 capacity and minimum-disk guidance from StarWind.

QUESTION NO: 63

A technician receives a PC that frequently shuts down and has extremely loud fans. When the technician begins a stress test, the PC shuts down almost immediately. Which of the following should the technician do next?

A. Install a liquid cooling unit in the computer.

B. Monitor the core CPU and system temperatures.

C. Reapply thermal paste to the processor heat sink.

D. Clean and test all fans to ensure proper airflow.

ANSWER: B

Explanation:

Monitor the core CPU and system temperatures. is the appropriate next troubleshooting step because the reported symptoms strongly indicate a thermal condition that should be verified before performing a repair. Extremely loud fans generally mean the system's cooling controls are responding to elevated component temperatures by increasing fan speed. A shutdown almost immediately after a stress test starts is also consistent with thermal-protection behavior: the processor or another monitored component can reach its safe operating threshold rapidly, causing the firmware or operating system to power down the computer to prevent damage.

Temperature monitoring provides objective diagnostic evidence while the system is idle and, if it remains stable long enough, during a controlled workload. The technician can compare processor and system readings, observe how quickly temperatures rise, and determine whether the problem is isolated to processor cooling or reflects a broader chassis-airflow or sensor issue. This follows a best-practice troubleshooting process: identify and validate the probable cause before changing hardware or applying corrective maintenance. Intel explains that processors include thermal-monitoring and protective mechanisms designed to respond to excessive temperature conditions in its processor thermal-solution guidance. Microsoft also documents hardware monitoring information available through Windows management instrumentation in its Win32_TemperatureProbe reference.

QUESTION NO: 64

Which of the following options provides correct information about 2.4GHz and 5GHz wireless frequencies? (Select TWO)

A. 2.4GHz has less interference. 5GHz transmits inlower speed.

B. 2.4GHz penetrates solid objects more effectively. 5GHz provides faster data connections.

C. 2.4GHz has a higher data rate. 5GHz has 23 channels.

D. 2.4GHz has II channels. 5GHz has no data interference.

E. 2.4GHz has a higher coverage area. 5GHz has higher bandwidth.

F. 2.4GHz has a higher bandwidth. 5GHz has lower transmit power.

ANSWER: B E

Explanation:

"2.4GHz penetrates solid objects more effectively. 5GHz provides faster data connections." is correct because lower-frequency radio waves generally experience less attenuation through common obstructions such as walls, floors, and

furniture. This gives 2.4 GHz Wi-Fi a practical advantage for maintaining a signal through obstacles, while 5 GHz can support higher throughput when signal conditions are favorable. “2.4GHz has a higher coverage area. 5GHz has higher bandwidth.” is also correct. The 2.4 GHz band generally provides greater range because its lower-frequency signals propagate farther and retain usable strength more effectively over distance. In contrast, 5 GHz Wi-Fi supports wider channel widths, such as 40 MHz, 80 MHz, and 160 MHz where supported, enabling higher potential data rates and greater capacity for demanding traffic. These characteristics are important when selecting an access-point band: 2.4 GHz is useful when coverage and obstacle penetration are priorities, whereas 5 GHz is preferred when devices are nearer to the access point and higher-performance connectivity is needed. Cisco summarizes the propagation and performance trade-offs between the two bands in its Wi-Fi overview, and the Wi-Fi Alliance provides additional wireless technology information.

QUESTION NO: 65

A technician is setting up a SOHO wireless router. Which of the following settings should the technician configure to secure the wireless network? (Select TWO).

A. Enable WPA3-Personal.

B. Configure a strong passphrase.

C. Enable WEP.

D. Disable wireless encryption.

E. Disable SSID broadcasting.

ANSWER: A B

Explanation:

WPA3-Personal and a strong passphrase are appropriate wireless security settings. WPA3-Personal provides modern Wi-Fi authentication and encryption for home and small-office wireless networks. A strong, unique passphrase helps prevent unauthorized users from successfully joining the network through password guessing or reuse of known credentials.

WEP is obsolete and vulnerable. Disabling encryption leaves wireless traffic and access unprotected. SSID broadcasting is not a security control because the network name can still be discovered by wireless monitoring tools. The Wi-Fi Alliance describes WPA3 security features in its Wi-Fi security overview.

QUESTION NO: 66

Which of the following components converts light into a digital signal?

A. Inverter

B. OLED

C. Digitizer

D. Webcam

ANSWER: D

Explanation:

Webcam is correct because its image sensor—commonly a CMOS sensor—detects incoming light and converts it into electrical signals. The webcam’s internal electronics then sample and process those signals into digital image data that the computer can use for video capture, conferencing, or recording. In practical PC hardware troubleshooting and configuration, a webcam is therefore an input device that captures optical information from the physical environment and delivers a digital video stream to the operating system or application. This conversion process is fundamental to digital imaging: individual sensor elements measure the amount of light reaching them, creating pixel data that can be encoded and transmitted over interfaces such as USB. Microsoft describes cameras as devices that provide video frames to applications through the Windows camera platform, while the U.S. National Institute of Standards and Technology explains that digital cameras use

image sensors to convert light into electronic image information. See Microsoft Learn: Camera drivers and the Windows camera platform and NIST: Digital camera imaging systems.

QUESTION NO: 67

A technician is troubleshooting a laptop that has no display on its built-in screen. The laptop works normally when connected to an external monitor. Which of the following are MOST likely causes of the issue? (Select TWO).

A. A damaged display panel

B. A loose display cable

C. A depleted laptop battery

D. A failed Ethernet adapter

E. An incorrect default gateway

ANSWER: A B

Explanation:

A damaged display panel and a loose display cable are likely causes. The successful external display confirms that the laptop can boot and generate video output, which helps isolate the problem to the internal display assembly or its connection. A failed LCD or LED panel can prevent the built-in screen from displaying an image even while an external monitor functions correctly.

A loose or damaged display cable can also interrupt the video signal between the motherboard and the laptop panel. The technician should follow the manufacturer's disassembly procedure, use ESD precautions, inspect the cable and connectors, and test with known-good components when available. Microsoft provides general display troubleshooting guidance in its external display troubleshooting documentation.

QUESTION NO: 68

A home user has purchased a subscription for a service that blocks malicious sites by preventing them from resolving correctly. Which of the following settings MOST likely needs to be changed on the user's router to enable this functionally?

A. DNS server

B. Port forwarding

C. Perimeter network

D. Universal PnP

E. DHCP server

ANSWER: A

Explanation:

The correct setting is **DNS server**. DNS translates human-readable host names, such as *example.com*, into the IP addresses that devices use to establish network connections. A subscription service that prevents known malicious domains from resolving works by providing DNS servers that apply threat-intelligence and domain-filtering policies. When a user attempts to visit a blocked domain, the filtering DNS resolver can return no address, return a safe blocking-page address, or otherwise decline to provide the normal resolution response. Configuring the router to use the subscription provider’s DNS server addresses allows devices that receive their network settings from that router to use the protective resolver automatically. This is especially useful in a home network because the policy can apply broadly to connected devices without configuring each device individually. The router may distribute those DNS server addresses to clients through its DHCP settings, but the setting that enables the subscription’s malicious-domain resolution blocking is the DNS server address itself. DNS name resolution and resolver configuration are described in the IETF Domain Names—Concepts and Facilities

standard. CompTIA also includes configuration of common network settings, including DNS, in the CompTIA A+ exam objectives.

QUESTION NO: 69

A restaurant calls the support line about its 3in (2.5cm) point-of-sale printer that is only printing fully black receipts. Which of the following should the technician check in order to resolve the issue? (Select two).

A. Power supply

B. Humidity

C. Rollers

D. Fuser

E. Heating element

F. Room temperature

ANSWER: C E

Explanation:

Rollers and **Heating element** are the components to check on a thermal point-of-sale receipt printer. This printer type creates an image by selectively applying heat from a thermal printhead, commonly described in basic troubleshooting as the heating element, to heat-sensitive receipt paper. If the heating element or its control circuitry applies heat continuously rather than selectively, the thermal coating can activate across the whole receipt width, producing a solid-black receipt. Inspecting the printhead for contamination, physical damage, and improper operation is therefore an appropriate first diagnostic step.

The rollers, particularly the platen roller that presses and moves paper beneath the printhead, must also be inspected. A worn, dirty, damaged, or improperly seated roller can prevent consistent paper movement and correct pressure at the printhead. Cleaning the roller with an approved method and checking that it turns freely and is correctly installed helps restore the controlled paper feed required for thermal printing. These checks align with the CompTIA A+ Core 1 objective area covering printer troubleshooting and maintenance. See the CompTIA exam objectives and Epson's thermal POS printer technical documentation for thermal-printer operating and maintenance guidance.

QUESTION NO: 70

Which of the following scenarios best illustrate a need for VDI? (Select two).

A. An IT engineer who is designing and showcasing organization user experiences for multiple clients

B. A company that needs to store IOPB worth of data

C. A manufacturing plant that has high turnover

D. A bank that has security concerns regarding employee activity

E. A payment processor that is planning on implementing virtual currency

F. An application developer who needs to configure network settings for an application

ANSWER: C D

Explanation:

VDI is particularly well suited to a manufacturing plant that has high turnover because desktops can be centrally created, standardized, assigned, reset, and reclaimed as workers join, change roles, or leave. Rather than individually preparing and maintaining a separate physical workstation image for every employee, IT can provide a managed virtual desktop from a centralized infrastructure. Nonpersistent desktop configurations can give each new worker a consistent, approved

environment while allowing the desktop to be returned to a known-good state after use. This supports rapid onboarding and reduces the operational burden associated with frequent account and workstation turnover.

A bank that has security concerns regarding employee activity also has a strong need for VDI. With desktop workloads hosted centrally, sensitive business data and applications can remain in the controlled data-center or cloud environment instead of being stored on endpoint devices. Administrators can apply centralized identity, access, session, logging, and policy controls to the virtual desktop environment. This model supports stronger oversight of access to regulated financial information and helps limit exposure when an endpoint is lost, shared, or otherwise not fully trusted. Microsoft describes VDI as hosting desktop environments on centralized servers for remote user access, while AWS notes that managed virtual desktops can centralize administration and help protect organizational data. See Microsoft Learn: Azure Virtual Desktop overview and AWS WorkSpaces.

QUESTION NO: 71

A user requested upgrades to a company-issued laptop to increase its performance while working with a large database stored on drive C. Which of the following tasks should a systems administrator complete to BEST meet this goal? (Select TWO).

A. Configure RAID 1.

B. Install a hybrid drive.

C. Upgrade to 1GB NIC.

D. Increase the RAM.

E. Migrate to a SSD.

F. Upgrade the power supply.

ANSWER: D E

Explanation:

Increasing the RAM and migrating to an SSD directly address the primary hardware constraints that affect a laptop processing a large local database. Increasing the RAM provides more working memory for the operating system, database application, queries, indexes, and cached data. This reduces the need to repeatedly move active data between memory and the storage drive, improving responsiveness when the database workload exceeds the system's available memory. Microsoft describes memory as a key resource for application performance and explains how memory pressure can affect workload behavior: Microsoft Memory Management documentation.

Migrating to an SSD improves storage input/output performance for the database files held on drive C. Database activity commonly involves frequent reads and writes, including loading tables, retrieving records, updating data, and accessing temporary files. SSDs have substantially lower latency and faster random-access performance than mechanical hard drives, so moving the operating system and database storage to an SSD makes these disk-bound operations complete more quickly. This is an appropriate performance-focused upgrade for a laptop with locally stored data. CompTIA's exam-objectives resources cover selecting and installing storage and memory hardware appropriate to stated requirements: CompTIA Exam Objectives.

QUESTION NO: 72

A graphic designer needs a RAID solution for design work. The solution needs to provide speed and redundancy. Which of the following RAID solutions should be installed?

A. 0

B. 1

C. 5

D. 10

ANSWER: D

Explanation:

RAID 10 is the best fit because it combines disk mirroring with striping. Data is first duplicated across mirrored drives, providing redundancy when a drive fails, and then striped across the mirrored sets to improve read and write performance. This combination is especially appropriate for a graphic-design workstation, where large image, video, and project files can create substantial storage I/O demands while the designer also needs protection against a single-drive failure. RAID 10 requires at least four drives and provides usable capacity equal to roughly half of the total raw capacity because each piece of data has a mirrored copy. Its architecture also supports efficient rebuilds: when a disk fails, only its mirror needs to be copied to a replacement drive rather than reconstructing all data from parity information. RAID remains an availability and performance technology, not a substitute for a separate backup strategy; important design assets should also be backed up to independent storage. CompTIA includes RAID levels and their use cases within the storage knowledge assessed by A+ Core 1. See the CompTIA exam objectives and Microsoft's Storage Spaces overview for related storage-resiliency concepts.

QUESTION NO: 73

Recently, users have been reporting quality issues when making internal and external VoIP calls each day around noon. Which of the following Is the most likely cause of the VoIP quality Issues?

A. Bandwidth saturation

B. ISP issues

C. Failing network switch

ANSWER: A

Explanation:

Bandwidth saturation is the most likely cause because the problem occurs predictably at approximately the same time every day. This pattern strongly suggests that network utilization rises around noon, perhaps as users stream media, download updates, participate in video meetings, use cloud applications, or access the internet during lunch. When available link capacity is consumed, real-time VoIP packets can be queued or dropped, and delay can vary as queues fill and empty. These conditions produce the familiar call-quality symptoms of choppy audio, delay, jitter, and dropped calls.

VoIP is particularly sensitive to congestion because voice packets must arrive consistently and in order within a short time window; retransmitting delayed voice traffic is generally not useful during a live conversation. Network QoS can prioritize voice traffic and reserve or manage capacity, but QoS does not create additional bandwidth when the connection is fully utilized. An administrator should confirm the diagnosis by reviewing interface utilization, packet-loss counters, latency, and jitter during the noon period, then identify the traffic responsible and apply capacity planning and QoS controls as appropriate. Cisco explains the relationship between congestion, delay, jitter, and real-time traffic in its Quality of Service overview. Microsoft also describes using QoS policies to manage real-time communication traffic in QoS Policy.

QUESTION NO: 74

A technician needs to configure a printer for network communications Which of the following must the technician configure? (Select THREE).

A. PCL

B. Dots per Inch

C. Gateway

D. Subnet mask

E. MAC address

F. IMEI

G. IP address

ANSWER: C D G

Explanation:

“Gateway,” “Subnet mask,” and “IP address” are the core IPv4 settings used to place a network printer on a TCP/IP network and allow hosts to reach it. The IP address uniquely identifies the printer’s network interface so workstations, print servers, and management tools can send traffic to the correct device. The subnet mask defines the local IP network (subnet) to which that address belongs. It lets the printer determine whether a destination, such as a user’s workstation or print server, is on the same local network or must be reached through a router. The gateway setting supplies the IP address of the router used for traffic destined for other networks. This is important when clients, DNS services, print servers, or administrative systems are outside the printer’s local subnet. Together, these values enable correct local addressing, subnet membership decisions, and routed communication. CompTIA’s Core 1 objectives include configuring networked devices using IP addressing, subnet masks, and gateways as fundamental TCP/IP configuration concepts. Microsoft also documents that TCP/IP printing relies on specifying the printer’s IP address when creating a Standard TCP/IP printer port. See the CompTIA exam objectives and Microsoft documentation for TCP/IP printer ports.

QUESTION NO: 75

A technician is troubleshooting a laptop that has a blank LCD panel. The technician shines a flashlight into the LCD and sees a faint image. Which of the following BEST describes the issue?

A. Defective inverter

B. Incomplete video driver

C. Incorrect input source

D. Burned-out bulb

ANSWER: A

Explanation:

Defective inverter is correct because a faint image visible only when an external flashlight is directed at the display is a classic symptom of a failed internal backlight system in a legacy CCFL-backlit laptop LCD. The LCD panel is still receiving video data and is able to form an image, which is why the image can be seen when external light passes through the panel. However, the panel’s normal illumination is absent, making the screen appear blank during ordinary use.

In these older laptop designs, the inverter converts the computer’s low-voltage DC power into the high-voltage AC power required by the cold-cathode fluorescent lamp that illuminates the LCD. A failed inverter prevents that lamp from receiving the power needed to light the display while leaving the panel’s image-forming function intact. This symptom-based diagnosis is consistent with the CompTIA A+ Core 1 hardware troubleshooting domain, which includes diagnosing laptop display and power-component issues. Modern LED-backlit panels generally use an LED driver rather than a separate CCFL inverter, but the terminology and symptom pattern in this question identify the conventional inverter fault. See the CompTIA exam objectives and iFixit’s backlight overview.

QUESTION NO: 76

A network technician needs to connect into the console of a switch. Which of the following connection types should the technician most likely utilize?

A. Serial interface

B. Bluetooth

C. Near-field communication

D. Port replicator

ANSWER: A

Explanation:

Serial interface is correct because a switch console connection is an out-of-band management connection used for initial setup, recovery, and troubleshooting when normal network access may not yet be available. Traditionally, the switch's console port connects to a technician's computer through a console or rollover cable, with the computer providing a serial connection directly or through a USB-to-serial adapter. A terminal-emulation application, such as PuTTY or Tera Term, is then configured with the serial port's communication settings so the technician can access the switch command-line interface.

This type of direct console access does not depend on the switch already having an IP address, a functioning network uplink, or remote-management services enabled. That makes it especially useful when deploying a new switch or diagnosing a connectivity failure. Modern devices may also provide a USB console port, but this still serves the same local console-management purpose; among the listed connection types, a serial interface is the established and most appropriate choice. Cisco documents console access as a direct local connection for configuring and managing network devices. See Cisco Catalyst configuration guidance and PuTTY for terminal-emulation software information.

QUESTION NO: 77

A customer's phone no longer charges fully The phone only charges to 67% and then stops_ Which of the following should be replaced to resolve this issue?

A. The phone

B. The charger

C. The battery

D. The SD card

ANSWER: C

Explanation:

The battery is the appropriate replacement because a phone that consistently stops charging at a substantially reduced percentage commonly has a degraded or failing battery. Rechargeable lithium-ion batteries lose usable capacity as they age and accumulate charge cycles. Their internal chemistry and battery-management circuitry can no longer reliably accept, store, or report a full charge, producing symptoms such as charging that stops at a fixed percentage, unexpectedly short runtime, or a battery percentage that falls rapidly after unplugging. Replacing the battery with a compatible, manufacturer-approved component restores the device's ability to store its intended amount of energy and is the standard hardware remediation for this symptom. Before replacement, a technician should confirm that the issue persists with a known-good charging source and inspect the phone for battery swelling or physical damage. Swollen batteries require prompt professional service and safe handling. On devices with sealed batteries, the repair may require manufacturer service or a qualified technician because the enclosure, adhesive, and internal connectors must be handled correctly. CompTIA's exam-objectives resource covers mobile-device hardware and troubleshooting topics relevant to battery faults: CompTIA Exam Objectives. Apple also explains that lithium-ion batteries are consumable components whose capacity diminishes with chemical age: About iPhone battery health and performance.

QUESTION NO: 78

To which of the following should a technician connect individual pairs of a Cat 6 cable in order to provide a connection to a switch?

A. Access point

B. Patch panel

C. Hub

D. Firewall

E. Wall jack

ANSWER: B

Explanation:

Patch panel is correct. In structured Ethernet cabling, the four twisted pairs within a horizontal Cat 6 cable are permanently terminated—typically by punching each conductor down onto insulation-displacement contacts—at the rear of a patch panel. The front of the panel provides numbered RJ-45 ports. A short, flexible patch cord is then used to connect the appropriate patch-panel port to a port on the network switch. This arrangement creates a reliable, organized, and serviceable transition between fixed in-wall or ceiling cabling and active network equipment. It also allows moves, additions, changes, cable testing, and switch replacement to be handled at the rack without disturbing the permanent cable run. Cat 6 terminations must follow the same recognized pinout at both ends, normally T568A or T568B, while preserving pair twists as close to the termination point as practical to maintain network performance. The Telecommunications Industry Association describes structured cabling components and practices through its ANSI/TIA-568 standards; see the TIA standards overview. For practical Ethernet cabling and termination guidance, see Cisco's Ethernet cable guide.

QUESTION NO: 79

Following a security breach that revealed employee username and password information, an organization would like to implement additional security for users logging in to company devices. Which of the following would be the best solution for the organization to use?

A. Biometric authentication

B. Peer-reviewed log-ins

C. Log-in scripts

D. One-time tokens

ANSWER: D

Explanation:

One-time tokens are the best solution because they add a separate authentication factor to the username-and-password process. A one-time password (OTP) is generated for a specific login attempt and is valid only briefly or for a single use. Therefore, a previously exposed username and password alone are insufficient for an attacker to log in: the attacker would also need access to the current token generated by the user's authenticator application or hardware token. This directly addresses the risk created by the credential breach while providing a practical form of multifactor authentication for device access. Token-based MFA is especially useful because the generated value continually changes and cannot be reused after it expires or has been accepted. Organizations should pair this control with password resets for affected accounts and encourage phishing-resistant authentication methods where feasible. The National Institute of Standards and Technology describes OTP authenticators as devices or applications that generate one-time codes for authentication, and CISA recommends MFA as an important protection when passwords are compromised. See NIST SP 800-63B: Authentication and Authenticator Management and CISA: Implementing Multifactor Authentication.

QUESTION NO: 80

An SAS RAID array has severely degraded and gone offline A systems administrator examines the syslog, and the point of failure is not obvious. Which of the following techniques should the administrator use to identify the issue (Select two).

A. Run a magnet over each drive.

B. Check if one of the drives is not level

C. Listen for clicking and grinding noises

D. Check the OS logs

E. Update the RAID controller firmware.

F. Check the historical SMART data

ANSWER: C F

Explanation:

“Listen for clicking and grinding noises” is an appropriate first diagnostic technique because these sounds can indicate a mechanical problem within a spinning disk, such as head, spindle, or bearing failure. In a degraded SAS RAID array, identifying a drive with physical symptoms helps the administrator isolate a likely failed member before taking further recovery action. The administrator should listen carefully without disturbing drive connections or attempting destructive testing.

“Check the historical SMART data” is also appropriate because Self-Monitoring, Analysis, and Reporting Technology records drive health attributes and error history. Historical values are particularly useful when a current failure is not immediately apparent in the syslog: trends in reallocated sectors, pending sectors, uncorrectable errors, temperature, or read/write error rates can reveal which disk was deteriorating before the array went offline. SMART results should be correlated with the RAID controller’s disk status and slot information so that the correct physical drive is identified for replacement or further testing. This approach aligns with storage troubleshooting practice: gather non-destructive evidence, identify the failing component, and preserve the array’s remaining data before remediation. CompTIA’s exam-objectives resources are available at CompTIA Exam Objectives; SMART monitoring details are documented by smartmontools.

QUESTION NO: 81

A user is experiencing multiple issues with an in-place upgrade of a laptop's operating system. The built-in camera is unresponsive, and the user is unable to pair the device with any Bluetooth accessories. Which of the following ate most likely causing three issues? (Select two).

A. Incorrect configuration of the settings

B. OS and device version incompatibility

C. Disabled settings following the upgrade

D. Full storage

E. Outdated drivers

F. Corrupted registry entries

ANSWER: C E

Explanation:

Disabled settings following the upgrade and **Outdated drivers** are the most likely causes of these post-upgrade hardware symptoms. An in-place operating-system upgrade can retain applications and user data while changing system components, permissions, privacy controls, and device configuration. Camera access can be disabled by an operating-system privacy setting, and wireless functionality can be unavailable when its associated feature, service, or adapter setting is disabled after the upgrade. Restoring the relevant enabled settings is therefore an appropriate first troubleshooting action.

Device drivers provide the operating system with the hardware-specific instructions needed to use integrated components such as a webcam and a wireless adapter. A driver that was suitable before the upgrade may not fully support the newly installed operating-system version. Updating the laptop manufacturer’s chipset, camera, and wireless drivers can restore device detection, normal camera operation, and accessory pairing. Microsoft similarly recommends checking for updated drivers when troubleshooting camera problems and obtaining driver updates through Windows Update or the device manufacturer. See Microsoft camera troubleshooting and Microsoft guidance for updating drivers.

QUESTION NO: 82

A user reports that the printouts from a laser printer have lines and smudges on them. The printer is also intermittently misfeeding the paper. Which of the following components should a technician replace to address this issue?

A. Fuser

B. Maintenance kit

C. Corona wire

D. Toner cartridge

ANSWER: B

Explanation:

Maintenance kit is the correct replacement because the reported symptoms span both the laser printer's imaging/fusing process and its paper-handling path. A laser-printer maintenance kit is a scheduled-service set of commonly worn components, typically including the fuser assembly and paper-feed parts such as pickup rollers and separation rollers; exact contents vary by printer model. Worn rollers can intermittently fail to pick up or separate sheets, causing misfeeds. Meanwhile, a worn or damaged fuser can produce smudging or lines because toner may not be consistently fused to the paper. Replacing the maintenance kit addresses these related wear items together, rather than treating only one symptom in isolation. This is especially appropriate when the printer has had substantial use or has reached its manufacturer-specified maintenance interval. Technicians should use the kit specified for the exact printer model, follow the manufacturer's replacement procedure, reset the maintenance counter if the device requires it, and then print a test page to confirm clean output and reliable paper feeding. HP's support guidance describes maintenance kits as replaceable assemblies for high-use LaserJet printers, while Epson's printer documentation discusses replacing pickup rollers when feed reliability declines. See HP printer maintenance guidance and Epson paper-feed roller replacement documentation.

QUESTION NO: 83

A technician receives a tablet that looks like it has a bulge inside. The bulge is pushing the screen away from the backplate. The tablet still turns on when it is plugged in, but the screen looks damaged and turns off when unplugged. Which of the following is the most likely cause of this issue?

A. Malfunctioning power supply

B. Damaged charge port

C. Swollen battery

D. Broken screen

ANSWER: C

Explanation:

Swollen battery is the most likely cause. Lithium-ion batteries can swell when internal chemical degradation or failure produces gas within the battery cell. Because tablets have tightly packed internal components, a swelling battery can visibly deform the device and force the display assembly away from the rear housing. The screen damage described is consistent with pressure from inside the tablet rather than an isolated display failure.

The power behavior also supports battery failure: the tablet can operate while external power is available but shuts down after it is unplugged because the battery is no longer able to safely store or deliver adequate power. A visibly swollen lithium-ion battery is a safety concern because damage to the cell can increase the risk of overheating, fire, or release of hazardous substances. The technician should stop using and charging the device, avoid puncturing or compressing the battery, and arrange for service and disposal through an appropriate battery-recycling or manufacturer-supported process. The U.S. Environmental Protection Agency provides battery safety and recycling guidance at EPA: Used Household Batteries. Apple also specifically warns that damaged batteries should be handled by trained technicians: Apple: Important safety information for batteries.

QUESTION NO: 84

A user's laptop is running out of disk space and requires a new hard drive. The user wants to replace the existing hard drive with the fastest possible I TB HDD. A technician assesses the user's hardware and determines the connections that are available. Which of the following drive types should the technician recommend as the BEST choice?

A. 1TB NVMe SSD

B. 1TB flash drive

C. 1TB SATA SSD

D. 1TB SAS

ANSWER: A

Explanation:

1TB NVMe SSD is the best choice when the laptop has a compatible NVMe-capable M.2/PCIe connection. Although the question uses the common phrase “hard drive,” its stated priority is the fastest available 1TB replacement drive. An NVMe solid-state drive uses the NVMe protocol over PCIe, providing a much higher-bandwidth, lower-latency storage path than legacy storage interfaces. This improves responsiveness during operating-system startup, application launches, file transfers, multitasking, and other storage-intensive work.

For a laptop upgrade, the technician must verify physical and electrical compatibility before installation. In particular, the system must support an M.2 NVMe drive of the appropriate size and keying, and the firmware must support booting from that device if it will contain the operating system. The scenario explicitly says that the technician has assessed the available connections, so selecting an NVMe drive is appropriate where that compatible connection is present. CompTIA’s Core 1 objectives include identifying common storage-device interfaces and characteristics, including NVMe and SATA: CompTIA exam objectives. For additional technical background, Microsoft describes NVMe as an interface designed for PCIe-connected nonvolatile storage: Microsoft Learn NVMe documentation.

QUESTION NO: 85

A company has a dot matrix printer that uses carbon paper. The company reports that the first page is printing too light, although the following pages are still legible. Which of the following MOST likely needs to be fixed?

A. The print drum is worn and loose causing the printing to be light in places

B. The ribbon is low on ink or missing and must be replaced to get proper output

C. The heating element has failed, and a new one needs to be installed for proper transfer

D. The wrong type of filement is loaded, preventing it from sticking correctly

E. The fuser assembly is not calibrated properly, causing it to impact the paper too hard

ANSWER: B

Explanation:

The ribbon is low on ink or missing and must be replaced to get proper output. A dot matrix printer is an impact printer: its print head contains small pins that strike an inked ribbon against the paper to create characters and images. In a multipart form using carbon paper, the first sheet is the original sheet and depends directly on the ink transferred from the ribbon. If that ribbon is depleted, dry, improperly seated, or absent, the original print will appear faint. The physical impact of the pins can still transfer enough pressure through the carbon paper to make the later copies readable, which matches the reported symptom. Replacing the ribbon cartridge, ensuring it is correctly installed and advances properly, restores the ink source required for a dark, readable first-page print. This reflects the CompTIA A+ Core 1 objective area covering printer technologies and common printer maintenance tasks, including consumable replacement. See the CompTIA exam objectives resource page and Epson’s impact-printer product information for background on impact printing and ribbon-based operation.