DUMPSBOSS.

CompTIA A+ Certification Exam: Core 1

CompTIA 220-1201

Version Demo

Total Demo Questions: 69

Total Premium Questions: 697

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Mobile Devices	83
Topic 2, Networking	198
Topic 3, Hardware	154
Topic 4, Virtualization and Cloud Computing	78
Topic 5, Hardware and Network Troubleshooting	182
Topic 6, Mix Questions	2
Total	697

QUESTION NO: 1

A user ' s laptop experiences intermittent issues during startup. A technician finds that the user has left a corporate flash drive plugged in, which is causing the issues. Which of the following should the technician configure?

A. BitLocker

B. Boot options

C. USB Enable

D. TPM features

ANSWER: B

Explanation:

Boot options should be configured because the laptop's BIOS or UEFI firmware consults its boot configuration during every startup to determine which device it should attempt to start from. When a USB flash drive remains connected, firmware may detect it as a potential boot device. If USB storage has a higher priority than the internal SSD or hard drive, or if removable-media boot is enabled in a way that affects normal startup, the system can attempt to boot from the flash drive instead of the installed operating-system drive. This can produce inconsistent startup delays, errors, or failure to reach the expected operating system, depending on how the drive is detected and whether it contains boot-related data.

Configuring Boot options allows the technician to place the internal drive first in the boot order and, where organizational policy permits, lower the priority of USB devices or disable booting from external media. This resolves the startup problem at the firmware level while allowing the corporate flash drive to remain usable for ordinary file access after the operating system loads. Boot order and device startup behavior are standard UEFI/BIOS configuration functions, as described in Microsoft's UEFI documentation and the CompTIA exam-objectives resources.

QUESTION NO: 2

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 indicated by the report that one or more disks are degraded. A degraded RAID state means that an array has lost normal redundancy or member-disk availability, commonly because a drive has failed or become inaccessible. Although some RAID configurations can continue operating in a degraded state, the RAID controller or firmware must still be able to present a valid logical volume to the server for normal startup.

Bootable device not found directly accounts for the subsequent missing-OS message. Firmware displays this type of condition when it cannot locate a device or logical volume containing valid boot information and an operating system. In this scenario, the degraded RAID condition can prevent the server from accessing the logical volume that normally contains the OS, or the boot device may no longer be available in the configured boot path. The technician should therefore investigate

the RAID array's status and confirm that the expected logical boot volume is detected and selected for booting. Microsoft's recovery guidance describes startup failures when Windows cannot access required boot or system-device information, while Dell's RAID documentation describes degraded virtual disks and their operational state. See Microsoft's INACCESSIBLE_BOOT_DEVICE troubleshooting guidance and Dell's guidance on degraded virtual disks.

QUESTION NO: 3

A technician is replacing a failed power supply in a desktop computer. Which of the following should the technician verify before installing the replacement? (Select TWO).

A. Wattage rating

B. Form factor

C. Monitor resolution

D. Operating system edition

E. Printer driver version

ANSWER: A B

Explanation:

Wattage rating is correct because the replacement PSU must provide sufficient continuous power for the computer's CPU, graphics card, storage devices, memory, fans, and connected peripherals. Installing an undersized PSU can cause instability, shutdowns, or reboots when the system is under load.

Form factor is also correct because the new PSU must physically fit the computer case and align with its mounting points. For example, an ATX power supply may not fit a small-form-factor chassis that requires an SFX unit. The technician should also confirm that the replacement includes the necessary motherboard, CPU, SATA, and PCIe power connectors. See Intel's power supply selection guidance for related considerations.

QUESTION NO: 4

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 hands-on diagnostic technique because these sounds can indicate a mechanical fault in a hard disk, such as problems with the spindle motor, bearings, actuator assembly, or read/write heads. In a degraded SAS RAID array, identifying a disk with obvious mechanical symptoms helps the administrator isolate a likely failed member without performing destructive actions or making configuration changes before the cause is known.

"Check the historical SMART data" is also appropriate because Self-Monitoring, Analysis, and Reporting Technology records drive-health attributes and error history. Reviewing values and trends such as reallocated sectors, pending sectors,

uncorrectable errors, read/write error rates, and interface error counts can reveal a disk that was deteriorating before the array went offline. Historical data is particularly useful when the current status alone does not make the failing component apparent. These two techniques provide evidence that supports identifying a failed or failing physical drive and planning safe replacement or further RAID-controller diagnostics. See the smartmontools SMART FAQ and Seagate's SMART overview.

QUESTION NO: 5

A user ' s computer can connect to internal network resources but cannot access websites on the internet. Other users on the same network do not have this issue. Which of the following should a technician do first to troubleshoot the issue?

A. Verify the computer ' s DNS settings.

B. Replace the network cable.

C. Restart the DHCP server.

D. Adjust the firewall rules on the router.

ANSWER: A

Explanation:

Verify the computer ' s DNS settings. The workstation has already demonstrated that its network adapter, local network connection, and access to internal resources are functioning. Because the symptom is isolated to one computer while other users on the same network can browse the internet, the technician should first check a workstation-specific configuration that commonly prevents access to websites without necessarily preventing local connectivity.

DNS resolves website host names, such as *www.example.com*, to IP addresses that a computer can use for network communication. A manually configured, unavailable, or incorrect DNS server can therefore prevent the user from opening websites by name. The technician can inspect the configured DNS server addresses with `ipconfig /all`, verify whether DNS is obtained automatically or configured statically as required by the network, and test name resolution with tools such as `nslookup`. This is a focused, low-impact first step that follows standard troubleshooting practice: confirm the most likely configuration issue on the affected endpoint before making changes that affect shared network infrastructure.

Microsoft describes DNS as the service that resolves names to IP addresses and documents DNS client troubleshooting tools and behavior in its DNS client troubleshooting guidance. The applicable A+ networking objectives are available from CompTIA Exam Objectives.

QUESTION NO: 6

A user ' s new computer is exhibiting issues after a couple hours of use. The screen freezes and typed characters do not appear for several seconds, if at all. The computer unexpectedly restarts while the user is reading an email. A technician runs diagnostics and verifies that no components show any errors. All hardware meets or exceeds recommendations. Which of the following should the technician do next?

A. Check for swollen capacitors.

B. Replace the power supply with a higher wattage rating.

C. Increase the amount of RAM.

D. Change the CMOS battery.

ANSWER: A

Explanation:

Check for swollen capacitors. The combination of intermittent system freezing, delayed input response, and unexpected restarts can result from unstable power delivery on the motherboard. Capacitors smooth and regulate voltage supplied to sensitive components, including the processor, memory, and chipset. A capacitor that is swollen or leaking is physically

failing and may no longer provide reliable filtering or voltage regulation. Because this fault can become more evident after the computer has been running for a period and components have warmed up, it fits the reported pattern of problems occurring after several hours of use.

A visual inspection is an appropriate next diagnostic action when standard hardware diagnostics report no errors and the installed hardware already meets the system's requirements. The technician should power off and disconnect the system, observe appropriate electrostatic-discharge precautions, open the case, and inspect the motherboard for capacitors with bulging tops, leakage, or other visible damage. This follows the CompTIA troubleshooting approach of gathering evidence and testing a likely cause before making a repair decision. See CompTIA's troubleshooting methodology guide and DigiKey's capacitor-life resource.

QUESTION NO: 7

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 is an appropriate connection type because many Android tablets use a USB-C port that can provide USB On-The-Go (OTG) or USB host functionality. With host support, the tablet can recognize a compatible wired USB keyboard as an input device. Depending on the keyboard's connector, the client may connect it directly through USB-C or use an appropriate USB-C adapter. Android supports standard USB human interface device (HID) keyboards, so this is a common wired peripheral connection method.

Bluetooth is also appropriate because Android tablets can pair with Bluetooth keyboards wirelessly through the device's Bluetooth settings. A paired Bluetooth keyboard functions as an HID input device and does not require a physical data cable or adapter. This is often the most convenient choice for portable use because it allows the keyboard to remain separate from the tablet while providing normal text-entry functionality. The keyboard must be compatible, powered, and placed in pairing mode before the tablet can discover and connect to it.

For Android guidance on connecting physical input devices, see Google Accessibility Help: Use a physical keyboard with your Android device. For the USB host and accessory model used by Android devices, see Android Developers: USB host and accessory overview.

QUESTION NO: 8

A technician installs a new printer for a workstation and tries to print a test page, but the page does not print. The technician looks at the print queue and notices that the printer is called 'Generic Printer." Which of the following BEST describes what the technician should do to fix this issue?

A. Connect the printer with a USB cable rather than over the network.

B. Install the appropriate printer drivers for the OS.

C. Install the correct toner in the printer.

D. Set the printer trays to allow duplex printing

ANSWER: B

Explanation:

Install the appropriate printer drivers for the OS. A printer appearing as “Generic Printer” commonly indicates that the operating system has assigned a generic or incomplete driver rather than the device-specific driver required to communicate fully with that printer. Although a generic driver can sometimes provide limited basic printing, it may not correctly support the printer’s command language, ports, print processor, or device capabilities. This can prevent even a test page from being processed and printed successfully.

The technician should identify the printer’s exact manufacturer and model, obtain the current driver that matches the workstation’s operating system and architecture, and install it through the manufacturer’s supported installation package or the operating system’s printer-management tools. After installation, the technician should verify the correct printer driver is associated with the printer queue and then print a new test page. Device-specific drivers also enable model-dependent functionality such as paper-source selection, finishing features, status reporting, and appropriate print-quality settings. Microsoft’s guidance on adding printers and drivers is available at Install a printer in Windows. CompTIA’s official exam objectives also include installing and configuring printer drivers as a Core 1 hardware support skill: CompTIA exam objectives.

QUESTION NO: 9

An administrator for a wireless network is planning the company ' s floor plan using a heat map. Which of the following types of networks is the administrator configuring?

A. SAN

B. PAN

C. MAN

D. WLAN

ANSWER: D

Explanation:

WLAN is correct because a wireless local area network provides Wi-Fi connectivity within a limited physical area, such as an office floor, building, or campus. When planning WLAN deployment, an administrator uses a wireless heat map to visualize expected or measured radio-frequency coverage across the floor plan. This helps determine appropriate access-point locations, estimate signal strength and overlap, identify dead zones, and support reliable connectivity for users as they move through the workspace. Heat-map planning also accounts for building materials, walls, furniture, and other physical features that can attenuate or reflect wireless signals. The scope described—a company floor plan and its wireless coverage—is therefore characteristic of a WLAN design. CompTIA includes wireless-network configuration and deployment concepts in its A+ Core 1 networking domain, including the placement and configuration of wireless access points. For further background on WLAN planning and RF coverage visualization, see the Cisco overview of WLANs and the Cisco Meraki wireless monitoring documentation.

QUESTION NO: 10

The IT department issued a corporate smartphone to a user, but the user returned the device stating it had connectivity Issues. The user claimed the device functioned on WI-FI but all connectivity to cloud services was lost as soon as the device was taken off site. Which of the following issues was MOST likely affecting the device?

A. MDM was never properly set up on the device.

B. S/MIME certificates were corrupted and needed to be reloaded.

C. Bluetooth on the device was disabled by mistake.

D. The device never had a proper SIM card installed.

ANSWER: D

Explanation:

The device never had a proper SIM card installed. The key diagnostic detail is that the smartphone can reach cloud services while connected to Wi-Fi but loses that connectivity after leaving the site. This indicates the device's applications and cloud-service access are functional; what is missing is an alternative internet connection when Wi-Fi is no longer available. On a corporate smartphone, that connection is ordinarily provided through a cellular carrier plan, authenticated by a SIM card or eSIM configuration. Without an active, properly provisioned SIM, the phone cannot register for cellular data service and therefore cannot establish an internet connection off site. As a result, cloud-based email, collaboration tools, storage, and other online services will appear unavailable away from Wi-Fi coverage. A SIM stores subscriber identity information used by the carrier to associate the device with an authorized mobile subscription. IT should verify that a physical SIM is present and correctly seated, or that an eSIM profile is installed and active, then confirm the assigned carrier plan includes mobile data service. Apple describes how cellular service requires an active SIM or eSIM plan in its Use dual SIM with an eSIM guidance. Android Enterprise also documents carrier and eSIM deployment considerations in its zero-touch enrollment resources.

QUESTION NO: 11

A user submitted a support ticket that states all of the printouts from a laser printer appear to have double images imposed on them. A review of past printer support tickets shows that maintenance kit has not been installed in more than a year. Which of the following printer consumables is MOST likely causing the issue?

A. Separation pad

B. Transfer roller

C. Ink cartridge

D. Fuser

ANSWER: D

Explanation:

Fuser is correct because a laser printer's fuser assembly uses heat and pressure to permanently bond toner to the paper. When the fuser is worn, contaminated, damaged, or no longer reaching and maintaining the required temperature, toner may not be fully fused during its first pass through the assembly. The remaining heat and contact with the rollers can then cause toner residue or a repeated "ghost" image to appear, which users commonly describe as double images on printed pages.

The fact that the printer has gone more than a year without a maintenance-kit replacement strongly supports this diagnosis. On many laser printers, the fuser is a key maintenance-kit component with a rated service life. Replacing the maintenance kit, including the fuser where applicable for the printer model, restores the heat-and-pressure stage that produces clean, permanent printed output. CompTIA's Core 1 exam objectives include diagnosing printer image-quality issues and identifying replaceable laser-printer maintenance components. See the CompTIA exam objectives and HP's laser printer print-quality troubleshooting guidance.

QUESTION NO: 12

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 because both problems began after an in-place operating-system upgrade and affect hardware features that depend on OS configuration and driver support. An upgrade can preserve the device while resetting, changing, or restricting feature settings. For example, Bluetooth may be turned off or blocked by a radio/airplane-mode setting, while camera access can be disabled through the operating system's privacy permissions. Restoring the relevant Bluetooth and camera settings is an appropriate early troubleshooting step. Microsoft documents that camera troubleshooting includes checking camera privacy permissions and allowing apps to access the camera; see Camera doesn't work in Windows.

Outdated drivers are also especially likely after an OS upgrade. The previous camera and Bluetooth drivers may not fully support the upgraded OS, or the upgrade may have replaced vendor-specific drivers with generic or incomplete versions. Updating the Bluetooth and camera/chipset drivers from the laptop manufacturer or through the operating system's update mechanism helps restore device communication and functionality. Microsoft's Bluetooth guidance specifically includes checking for and installing driver updates through Device Manager; see Fix Bluetooth problems in Windows.

QUESTION NO: 13

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 port numbers are **25** and **110**. Port 25 is the well-known TCP port for Simple Mail Transfer Protocol (SMTP). SMTP is the protocol used to relay outgoing email, particularly between mail servers, and it is a foundational service to recognize when troubleshooting or configuring email delivery. Modern client submission commonly uses authenticated SMTP on other ports, but TCP 25 remains the standard port associated with SMTP relay traffic.

Port 110 is the well-known TCP port for Post Office Protocol version 3 (POP3). POP3 allows an email client to retrieve messages from a mail server, traditionally by downloading them to the client. Therefore, it is directly associated with inbound email retrieval. These port-to-protocol associations are part of the networking and common-port knowledge expected for CompTIA A+ Core 1. The Internet Assigned Numbers Authority lists SMTP under port 25 and POP3 under port 110 in its service-name and port-number registry. See the IANA Service Name and Transport Protocol Port Number Registry and CompTIA's exam objectives resource page.

QUESTION NO: 14

A user is researching hard drives to upgrade a PC and has decided to purchase a NVMe drive. Which of the following Should the user confirm are available on the PC before making the purchase? (Select TWO).

A. SATA

B. M.2

C. PCIe

D. SAS

E. SCSI

F. DRAM

ANSWER: B C

Explanation:

An NVMe solid-state drive communicates over the PCIe bus, so the PC must provide a compatible PCIe-based storage connection. An available **M.2** slot is the common physical connector used by consumer NVMe SSDs. The user should verify not merely that an M.2 socket exists, but that it supports PCIe/NVMe operation; some M.2 sockets support only SATA devices. The physical size and keying of the socket should also match the intended drive, with 2280 being a common M.2 module length.

PCIe availability is equally necessary because NVMe is a storage protocol designed to operate across PCI Express lanes. Motherboard documentation or BIOS/UEFI specifications can identify whether an M.2 slot is wired for PCIe, the supported PCIe generation, and the available lane count. This verification helps ensure both compatibility and expected performance. In systems without an appropriate M.2 socket, an NVMe drive may sometimes be installed through a compatible PCIe expansion-card adapter, provided that an appropriate PCIe slot and platform support are available.

For additional technical background, see the NVM Express specifications and Crucial's PCIe and NVMe SSD overview.

QUESTION NO: 15

A technician needs to select PC components with a minimal number of visible internal cables. Which of the following should the technician use?

A. SATA drive connections

B. Liquid cooling

C. Modular power supply

D. Wireless NIC

ANSWER: C

Explanation:

A modular power supply is the appropriate choice because it allows the technician to connect only the power cables required by the installed components. Unlike a non-modular unit, which has a fixed bundle of unused leads attached to the power supply, a modular design has detachable cables for motherboard, CPU, PCIe, SATA, and peripheral power as needed. Eliminating unnecessary power leads reduces cable clutter in the case and makes it easier to route the remaining cables behind the motherboard tray or through cable-management openings. This produces a cleaner internal appearance with fewer visible cables while also improving access for later component installation, troubleshooting, and maintenance. Proper cable management can also help maintain unobstructed airflow through the chassis, supporting effective cooling. The required motherboard and CPU power cables will still be present, but the technician avoids having extra unused cables visible inside the system. Corsair describes modular power supplies and their detachable-cable design at Corsair Explorer: What Is a Modular Power Supply?. General guidance on component selection and PC assembly is available from CompTIA's IT careers and certifications resources.

QUESTION NO: 16 - (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

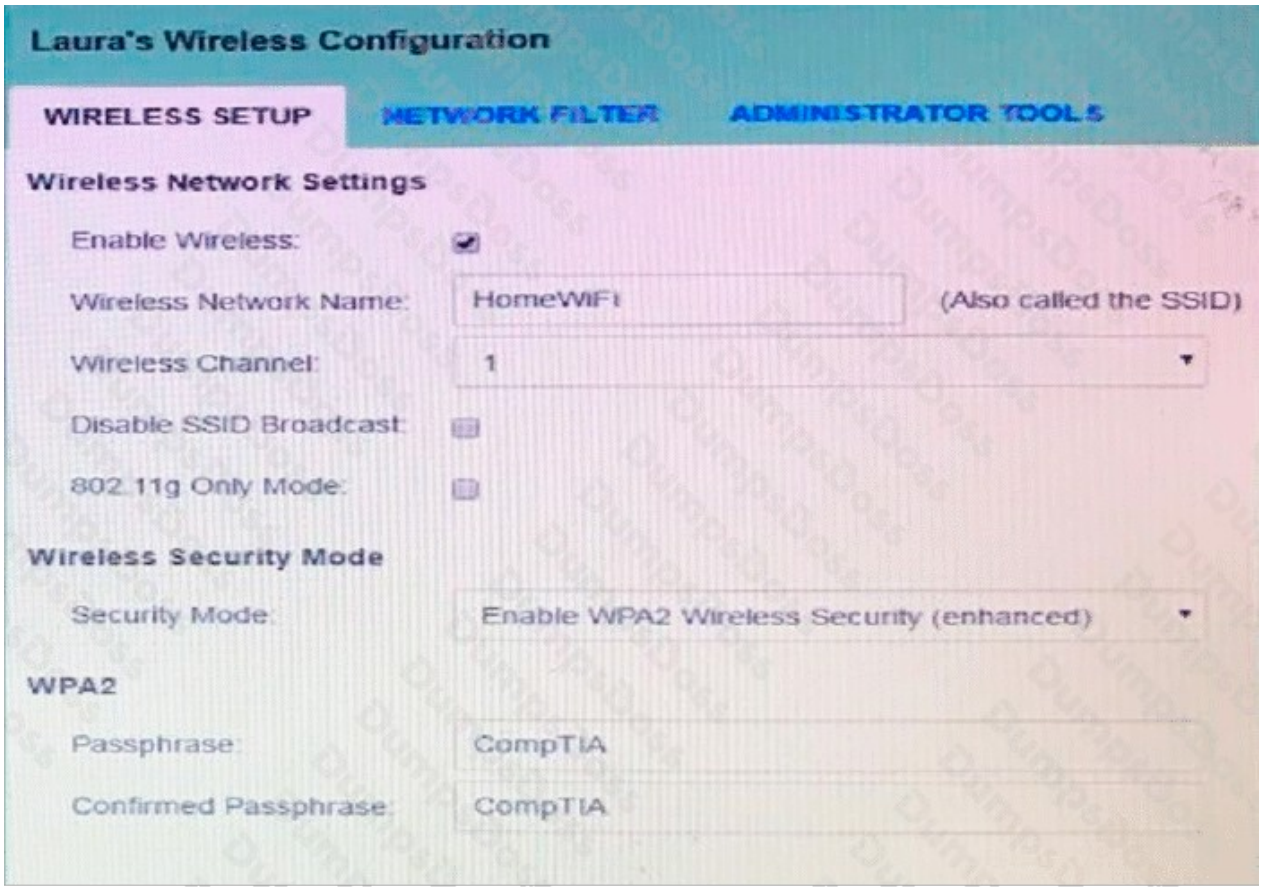
Smartphone: IP Address 192.168.1.101

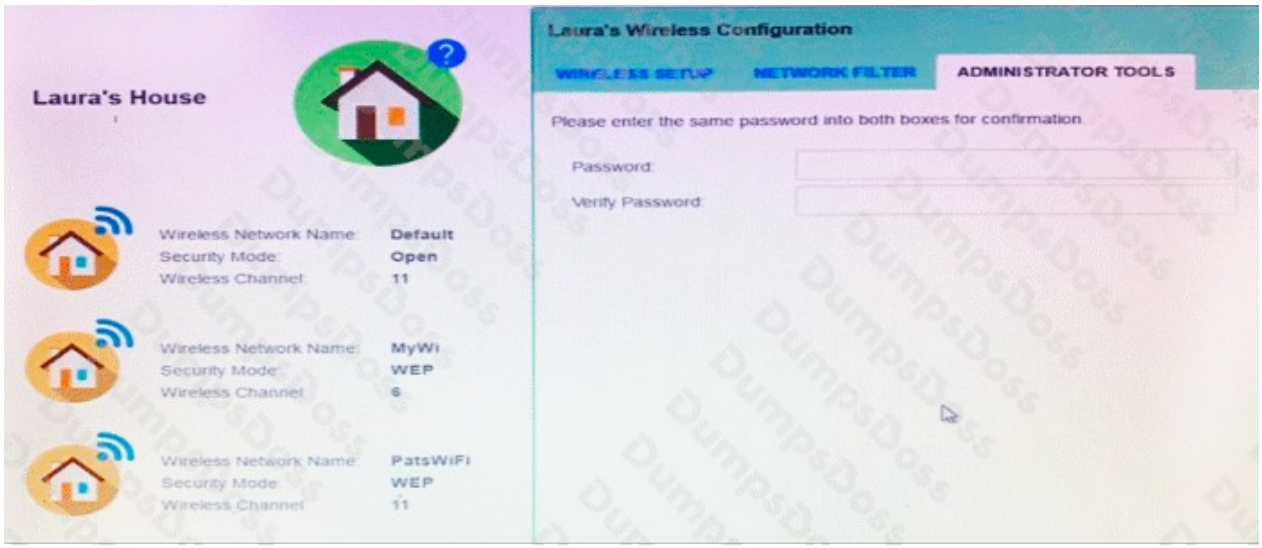
Hardware Address: 09:2C:D0:22:3F:11

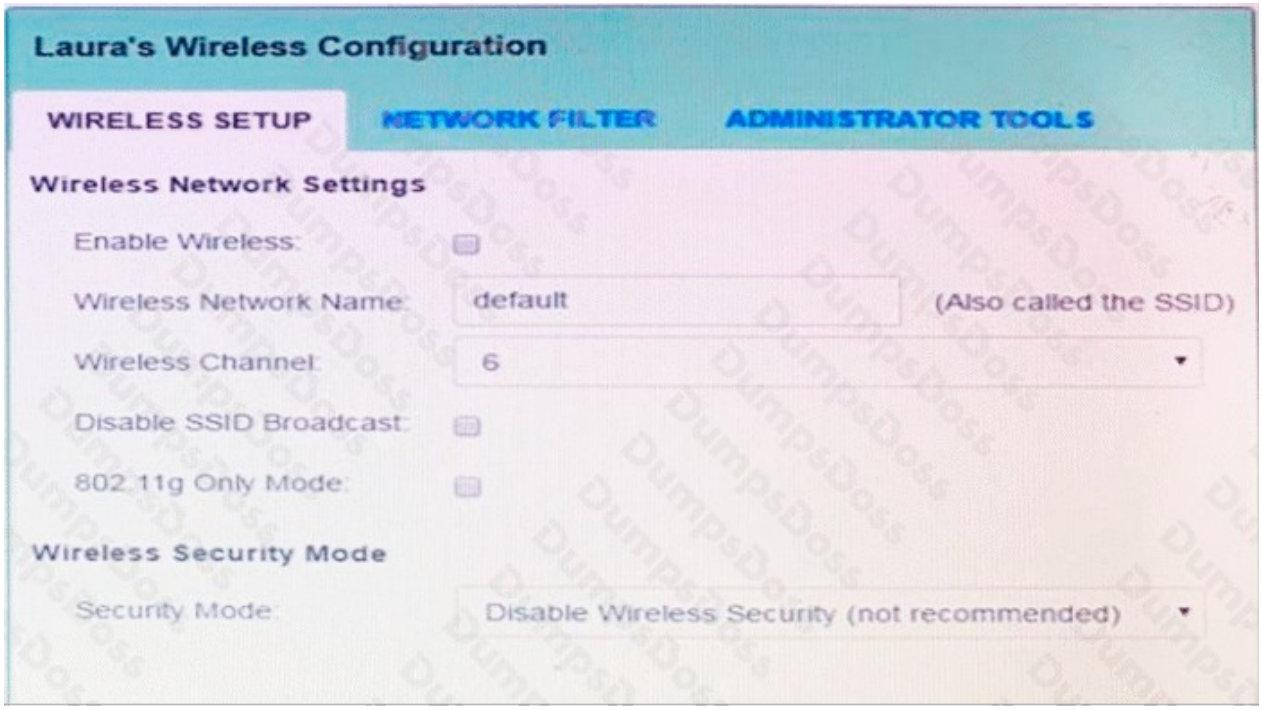
INSTRUCTIONS

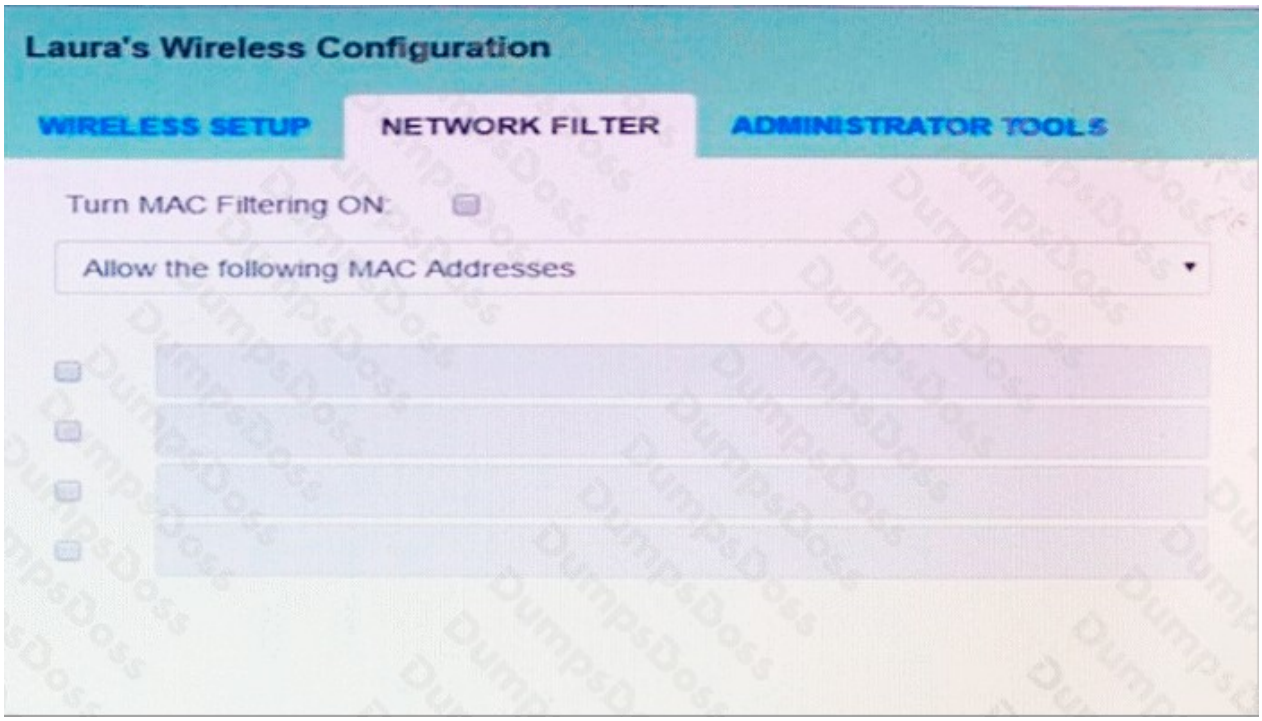
Configure Laura's wireless network using the network adapter window.

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




Laura's House
Wireless Network Name: Default
Security Mode: Open
Wireless Channel: 11
Wireless Network Name: MyWi
Security Mode: WEP
Wireless Channel: 6
Wireless Network Name: PatsWiFi
Security Mode: WEP
Wireless Channel: 11
Laura's Wireless Configuration
ADMINISTRATOR TOOLS
Please enter the same password into both boxes for confirmation.
Password:
Verify Password:


Laura's Wireless Configuration
WIRELESS SETUP
NETWORK FILTER
ADMINISTRATOR TOOLS
Wireless Network Settings
Enable Wireless:
Wireless Network Name:
default
(Also called the SSID)
Wireless Channel:
6
Disable SSID Broadcast:
802.11g Only Mode:
Wireless Security Mode
Security Mode:
Disable Wireless Security (not recommended)



ANSWER: See the explanation for the answer

Explanation:

Configure the access point as follows:

On **Wireless Setup**, leave **Enable Wireless** enabled.
Set **Wireless Network Name (SSID)** to `HomeWiFi`.
Set the wireless channel to **1**. The neighboring networks use channels 6 and 11, so channel 1 is the non-overlapping choice that avoids their interference.
Set **Security Mode** to **Enable WPA2 Wireless Security (enhanced)**.
Enter `CompTIA` for both the passphrase and confirmed passphrase fields.
Leave SSID broadcast enabled and do not enable 802.11g-only mode unless the simulation explicitly requires it.

On **Network Filter**:

Enable **MAC Filtering**.
Select **Allow the following MAC Addresses**.
Enable two filter-entry rows and enter `00:0A:BF:03:C4:54` for Laura's laptop.
Enter `09:2C:D0:22:3F:11` for Laura's smartphone.

The listed IP addresses are not used for MAC filtering; use the hardware (MAC) addresses so that only those two devices are allowed to associate with the wireless network.

On **Administrator Tools**, change the router administrator password and confirmation to `Secure$1`.

QUESTION NO: 17

A technician just finished assembling a new PC for a client. Upon POST, the device presents an unspecified beep code and turns off automatically after five seconds. The technician double-checks the bill of materials for the new build and confirms all items have been installed. Which of the following should the technician do NEXT?

A. Ensure thermal paste is being used on the CPU.

B. Check to make sure that any video cards have auxiliary power cabling connected.

C. Verify the header panel connector is properly connected.

D. Spot-check that the I/O shield for the motherboard is properly installed.

ANSWER: A

Explanation:

Ensure thermal paste is being used on the CPU. In a newly assembled PC that begins POST but powers off within a few seconds, the technician should prioritize verifying that the processor can transfer heat effectively to its heatsink. Thermal interface material fills microscopic gaps between the CPU heat spreader and the cooler's contact plate, allowing heat to move into the heatsink. Without it, or if the cooler is not properly seated, CPU temperature can rise extremely rapidly. Modern systems include thermal protection that can shut the computer down to prevent processor damage, making an immediate or near-immediate shutdown a strong indicator to inspect the CPU cooling installation. The reported beep code indicates that POST detected a hardware-related condition, but because the specific code is unspecified, the repeatable five-second shutdown is the more actionable symptom. The technician should power down, disconnect AC power, remove and inspect the cooler, confirm appropriate thermal paste application, and reinstall the cooler securely before retesting. CPU installation and cooling verification are part of the hardware-installation and troubleshooting skills covered in the CompTIA A+ Core 1 objectives. See CompTIA exam objectives and Intel's guidance on applying thermal paste.

QUESTION NO: 18

A student configures a wireless SOHO network to connect four laptops and one multifunction printer. All laptops must have internet access and be able to use the printer. Which of the following settings ensures the printer is always available?

A. Configure dynamic IPs for the laptops and a static IP for the printer on the same subnet.

B. Manually assign IP addresses to the laptops and printer based on the public IP from the ISP.

C. Use APIPA for laptops and connect the printer to the ISP router.

D. Use dynamic IP addresses from the ISP router for all the devices.

ANSWER: A

Explanation:

Configure dynamic IPs for the laptops and a static IP for the printer on the same subnet. This configuration gives the printer a predictable private IPv4 address, allowing every laptop to consistently locate the printer at the same network address. A printer that obtains a different address after a DHCP lease renewal, reboot, or router restart can become unavailable to devices configured to print to its former address. Assigning a stable address prevents that disruption while keeping the printer on the same local subnet as the wireless laptops, which is necessary for normal LAN communication and printer discovery.

Using DHCP for the laptops is appropriate in a small office/home office network because client devices can receive their IP address, default gateway, DNS servers, and other settings automatically. The router provides network address translation so these private-addressed devices can share the internet connection. In practice, the static printer address should be selected outside the router's DHCP allocation pool, or the router should be configured with a DHCP reservation for the printer's MAC address. A DHCP reservation provides the same consistent-address result while centrally managing the assignment. Microsoft also documents that network printing depends on reaching a printer through its configured network address: Add or install a printer in Windows. For DHCP reservation guidance, see Microsoft DHCP overview.

QUESTION NO: 19

A technician is troubleshooting internet connectivity issues after a firewall update. Users report that they can access local network resources, such as printers and shares, but cannot access the internet. Which of the following settings is most likely causing the issue?

A. Static IP assignments

B. Default gateway

C. Subnet mask

D. VLANs

ANSWER: B

Explanation:

Default gateway is the most likely setting causing this symptom. A host uses its local IP address and subnet mask to determine whether a destination is on the same local network. Resources such as local printers and file shares are reached directly on that local subnet, so they can remain available even when the path to outside networks is disrupted. For destinations outside the local subnet, including public internet addresses, the host sends traffic to its configured default gateway. The gateway, typically a router or firewall interface, then forwards that traffic toward external networks.

Following a firewall update, a changed, removed, unreachable, or incorrectly assigned gateway configuration can therefore leave local communications working while preventing users from reaching the internet. The technician should verify that client devices have the expected gateway address, confirm that the firewall's LAN interface is available at that address, and test reachability by pinging the gateway before testing an external IP address and DNS resolution. This troubleshooting approach aligns with CompTIA's networking objective covering configuration and diagnosis of connectivity issues. Microsoft also describes the default gateway as the router used to reach networks beyond the local subnet: Microsoft Learn: IP address management. For background on IP routing and default routes, see RFC 1812.

QUESTION NO: 20

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, **A failing battery**, and **Too many open applications** are the most likely causes of a phone becoming unusually hot. Operating a Wi-Fi hotspot makes the phone's cellular and Wi-Fi radios work continuously to maintain an internet connection and serve connected devices. This sustained radio activity increases power consumption and can generate noticeable heat, particularly where cellular signal strength is poor.

A failing battery is also a significant heat concern. Lithium-ion batteries can generate excessive heat when damaged, degraded, defective, or unable to charge and discharge normally. Heat accompanied by swelling, rapid battery drain, charging problems, or an unexpected shutdown should be treated as a potential battery-safety issue; the device should be powered off and evaluated or serviced rather than continually charged or used.

Too many open applications can keep the processor, graphics hardware, memory, and network interfaces active. Resource-intensive background activity, synchronization, streaming, navigation, or a misbehaving app can prevent the device from entering lower-power states, causing sustained workload and elevated temperature. Closing unneeded applications and checking for an app consuming abnormal battery power are appropriate initial troubleshooting steps. Apple notes that intensive use, setup, restoration, and charging can make devices warm, while battery safety guidance emphasizes avoiding use of damaged batteries. See Apple Support: If your iPhone or iPad gets too hot or too cold and U.S. CPSC lithium-ion battery safety guidance.

QUESTION NO: 21

A technician is securing a newly installed wireless router in a small office. Which of the following actions should the technician perform? (Select TWO).

A. Change the default administrator password.

B. Enable WPA3-Personal.

C. Disable SSID broadcasting.

D. Configure WEP encryption.

E. Enable DMZ hosting.

F. Use the default wireless passphrase.

ANSWER: A B

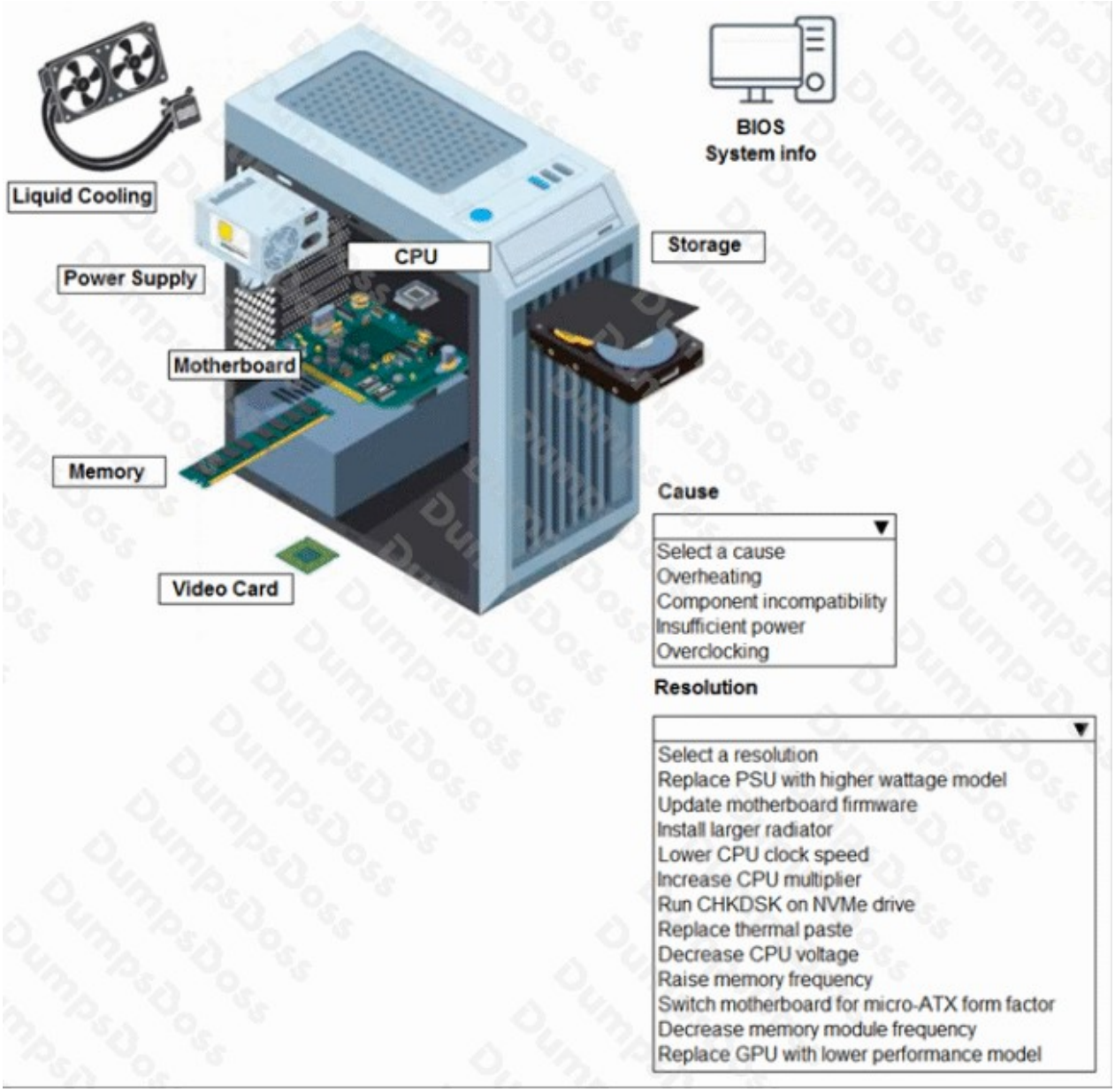
Explanation:

Changing the default administrator password is correct because default router credentials are widely known and can allow an unauthorized person to modify wireless, firewall, DHCP, and other network settings. The technician should configure a unique, strong administrative password and store it according to organizational procedures.

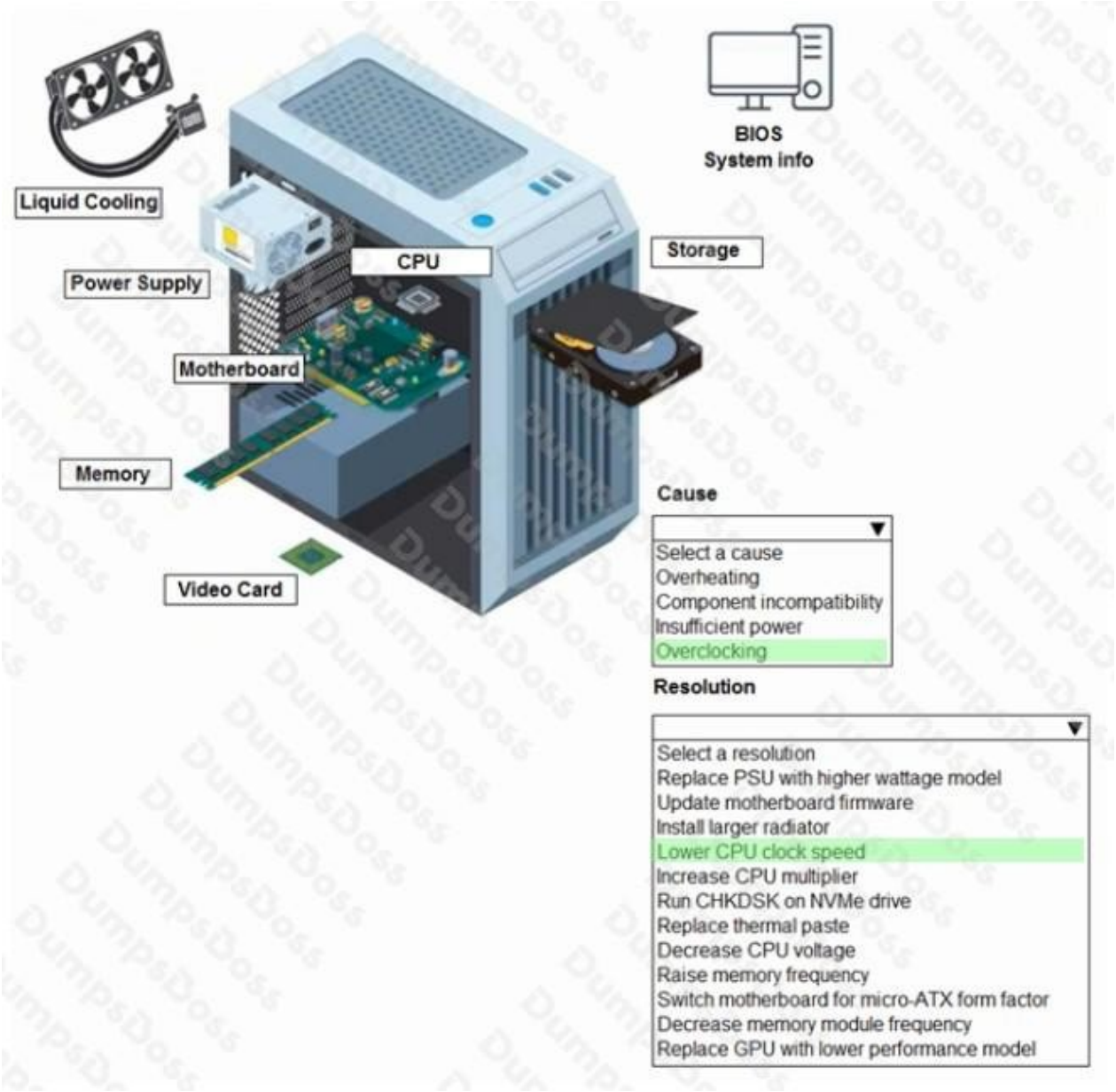
Enabling WPA3-Personal is also correct because WPA3-Personal provides modern Wi-Fi authentication and encryption protections for a small-office wireless network. Where all client devices support it, WPA3-Personal should be preferred over older protocols such as WEP and WPA. The Wi-Fi Alliance describes WPA3 security features at Wi-Fi Security, and CISA provides wireless-network security guidance at CISA: Securing Wireless Networks.

QUESTION NO: 22 - (HOTSPOT)

A customer built a computer for gaming, sourcing individual components and then assembling the system. The OS starts up, but within a few minutes the machine locks up. The customer brought the computer to a technician to diagnose the issue.


Liquid Cooling
Power Supply
CPU
Motherboard
Memory
Video Card
BIOS
System info
Storage
Cause
Select a cause
Overheating
Component incompatibility
Insufficient power
Overclocking
Resolution
Select a resolution
Replace PSU with higher wattage model
Update motherboard firmware
Install larger radiator
Lower CPU clock speed
Increase CPU multiplier
Run CHKDSK on NVMe drive
Replace thermal paste
Decrease CPU voltage
Raise memory frequency
Switch motherboard for micro-ATX form factor
Decrease memory module frequency
Replace GPU with lower performance model

ANSWER:



Explanation:

The correct diagnosis is overclocking, with the corrective action of lowering the CPU clock speed. The system can initially boot because an overclock does not necessarily prevent startup; however, a processor that is configured to run beyond a stable frequency can become unreliable once Windows begins loading drivers, background services, and normal workloads. That instability commonly appears as intermittent freezes, lockups, crashes, or unexpected restarts shortly after boot.

The BIOS system information indicates that the CPU is operating at a clock speed higher than its standard value. In a newly assembled gaming computer, this points to a firmware configuration that is pushing the processor beyond its validated operating settings. Lowering the CPU clock speed removes that excessive frequency setting and returns the processor closer to a known stable configuration. This is an appropriate first corrective step because it directly addresses the detected configuration condition while preserving the rest of the hardware installation.

CPU overclocking requires stable frequency, voltage, power-delivery, and cooling conditions. A setting that appears to work briefly is not necessarily stable over time or under changing workloads. Returning the clock speed to stock settings, or otherwise lowering it until stability is restored, allows the technician to confirm whether the system lockups were caused by the CPU operating frequency. Intel also notes that overclocking changes processor operating parameters and requires stability testing after configuration changes. See Intel's CPU overclocking guide and Intel's guidance on testing overclock stability.

QUESTION NO: 23

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. An optical drive adds another device that must receive power from the PSU. Although its demand is most noticeable while the drive motor is spinning and media is being read or written, that additional load contributes to the system's total power requirement and may exceed the available capacity or connector provisioning of an already marginal PSU.

A graphics-card upgrade is especially likely to require a higher-capacity PSU because modern discrete GPUs can consume substantially more power than an entry-level or older card. Many graphics cards also require one or more dedicated PCIe auxiliary power connectors in addition to the power provided by the motherboard's PCIe slot. The technician should compare the replacement card manufacturer's recommended PSU wattage and required PCIe power connections with the installed PSU's rated output and available connectors before installation. This aligns with Core 1 hardware troubleshooting and installation knowledge, including identifying appropriate power requirements for internal components. See the CompTIA exam objectives and Intel's guidance on graphics-card power requirements.

QUESTION NO: 24

An organization upgrades all desktops to Windows 11 and must ensure protection from malicious software at startup. Which option should be enabled?

A. Trusted Platform Module

B. Hardware security module

C. Secure Boot

D. BIOS password

ANSWER: C

Explanation:

Secure Boot should be enabled because it is a UEFI firmware security capability designed to establish a trusted boot process. Before starting the operating system, UEFI Secure Boot checks the digital signatures of boot components, including the bootloader and associated firmware drivers, against trusted keys stored in the firmware. This validation helps ensure that only trusted, properly signed components run during startup, reducing the risk that bootkits, rootkits, or other unauthorized pre-operating-system malware can load before Windows security protections are active.

This is particularly relevant for Windows 11 deployments. Microsoft lists UEFI firmware that is Secure Boot capable as a minimum system requirement, and Windows uses the UEFI boot environment as part of its platform security model. Enabling Secure Boot provides startup integrity protection at the firmware-to-operating-system handoff, which directly addresses the requirement to defend systems against malicious software at startup. For implementation details and Windows 11 requirements, see Microsoft's Windows 11 requirements and Microsoft Learn: Secure Boot.

QUESTION NO: 25

A small-business owner purchases a building and wants to establish an internet connection. A technician examines the target network room and discovers a coaxial wall jack. Which of the following internet connection types would the technician most likely recommend?

A. Fiber

B. Satellite

C. DSL

D. Cable

ANSWER: D

Explanation:

Cable is the appropriate recommendation because a coaxial wall jack is the standard in-building connection point used for cable television and cable broadband service. A cable internet provider delivers its service over the existing hybrid fiber-coaxial network, and the customer premises typically connects a cable modem or cable gateway to the wall jack with a coaxial cable. The modem communicates with the provider using Data Over Cable Service Interface Specification (DOCSIS), the industry standard for transmitting high-speed data over cable-TV infrastructure. In a small-business environment, the technician would first confirm that a cable provider serves the building's address and that the coaxial run is active or can be activated. The provider can then provision compatible DOCSIS equipment and establish the internet service. This recommendation directly matches the physical media already identified in the network room and can reduce the need for a new access-medium installation. For further technical background, see CableLabs' DOCSIS technology overview and the FCC's guide to obtaining broadband service.

QUESTION NO: 26

Which of the following network services allows a networked device to always be assigned the same IP address based on the device's MAC address?

A. DHCP

B. LDAP

C. UTM

D. DNS

ANSWER: A

Explanation:

DHCP is correct because a DHCP server can be configured with a reservation, also called a static DHCP assignment. The administrator creates a reservation that associates a device's unique MAC address (its hardware address) with a specific IP address. Whenever that device sends a DHCP request, the server recognizes its MAC address and leases the reserved address to it. This delivers a consistent address while retaining centralized DHCP administration for settings such as the subnet mask, default gateway, DNS servers, lease duration, and other DHCP options. DHCP reservations are commonly used for infrastructure and devices that benefit from a predictable address, including printers, servers, access points, cameras, and network appliances. The client remains configured to obtain its address automatically; the fixed assignment is managed on the DHCP server rather than manually configured on the endpoint. RFC 2131 describes DHCP's use of client identifiers and hardware addresses during address allocation: RFC 2131. Microsoft's DHCP documentation also describes reservations as permanent address leases assigned to specified clients: DHCP subnet and reservation configuration.

QUESTION NO: 27

A technician is evaluating how to connect a power-redundant server to the outlets of a rack. Which of the following is the best way to provide electricity to the server?

A. Using only one power outlet, as the system will provide energy to the redundant source

B. Leaving one of the power supplies disconnected for use in case the other fails

C. Identifying available power outlets in different UPSs and distributing the connection between them

D. Connecting the device to one dedicated battery backup to provide continuous energy

ANSWER: C

Explanation:

Identifying available power outlets in different UPSs and distributing the connection between them is the best way to support a server with redundant power supplies. Each server power supply should receive power through an independent path—for example, one supply connected to a power distribution unit backed by one UPS and the other supply connected to a separate power distribution unit backed by another UPS. This design protects server availability if a UPS, PDU, circuit, or power feed fails or requires maintenance. The remaining power supply can continue operating the server, assuming it has adequate capacity for the load. Redundant power supplies are intended to eliminate a single point of failure, but that resilience is achieved only when their upstream power sources are also separate. Connecting both supplies to the same UPS or power path would leave the server exposed to a shared infrastructure failure. Before deployment, the technician should also verify that each UPS and circuit has sufficient load capacity and that the server supports continued operation on a single power supply. CompTIA's A+ Core 1 objectives include configuring redundant power supplies and UPS devices, while CISA guidance describes the value of separate, redundant power paths for critical systems. See the CompTIA exam objectives and CISA resilience resources.

QUESTION NO: 28

A company policy change requires all computers to be encrypted. Which of the following technologies should a technician configure to meet this new requirement?

A. NVMe

B. RISC

C. ARM

D. TPM

ANSWER: D

Explanation:

TPM is the appropriate technology to configure because a Trusted Platform Module is a dedicated hardware-based security component that securely generates, protects, and stores cryptographic keys. For a Windows full-disk encryption deployment such as BitLocker, the TPM can protect the volume encryption key and validate measured boot components before allowing the operating system to access the protected drive. This hardware-backed key protection helps ensure that encryption keys are not simply exposed in software or stored unprotected on the disk.

In practice, a technician should verify that a TPM is present, enabled in UEFI/BIOS, activated as needed, and available to the operating system before enabling the organization's chosen full-disk encryption product. TPM 2.0 is the modern standard commonly used with current Windows security and BitLocker configurations. Although the encryption software performs the drive encryption, TPM configuration provides the secure hardware root of trust that supports transparent, system-wide encryption and boot-integrity protection. Microsoft describes TPM use with BitLocker in its BitLocker documentation. TPM is also a security hardware topic within CompTIA A+ Core 1 coverage; see CompTIA's A+ certification overview.

QUESTION NO: 29

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 a practical centralized solution for making Ethernet-connected printers available to users throughout each floor without requiring the printers themselves to be domain joined. A print server hosts the printer queues, receives print jobs from client devices, applies the appropriate printer drivers and settings, and forwards jobs to the physical network printers over their RJ45 Ethernet connections. This centralizes administration, queue monitoring, driver deployment, permissions, and troubleshooting rather than requiring every user to configure every printer individually by its network address.

Printer shares are the published, user-accessible printer queues that clients connect to. Users can add a shared printer from the print server and submit jobs through that shared queue. The server can be joined to the organization's domain for authentication and access control even though the physical printers are standalone network devices and are not domain members. This design supports consistent access and management for a corporate environment with multiple printers per floor. Microsoft describes how Windows print servers manage shared printer queues and client connections in its Print Management documentation. These tasks align with CompTIA A+ networking and printer-configuration concepts covered in the CompTIA exam objectives.

QUESTION NO: 30

A technician is troubleshooting a desktop PC that powers on but does not display an image on the monitor. Which of the following should the technician check FIRST? (Select TWO).

A. Verify the monitor is set to the correct input source.

B. Check that the video cable is securely connected.

C. Replace the CPU.

D. Reinstall the operating system.

E. Replace the motherboard.

ANSWER: A B

Explanation:

Verifying that the monitor is set to the correct input source is appropriate because a powered monitor can show no image when it is configured for a different input than the one connected to the PC. For example, a monitor set to DisplayPort will not show video received through its HDMI connection.

Checking that the video cable is securely connected is also an appropriate first step. A loose, damaged, or disconnected cable prevents the monitor from receiving a usable video signal. These checks are quick, noninvasive, and directly related to the reported symptom before the technician considers replacing internal components. Dell provides display troubleshooting guidance at Dell Support.

QUESTION NO: 31

Which of the following types of connectors does an IDE hard drive use for power?

A. F type

B. SC

C. Molex

D. Lightning

ANSWER: C

Explanation:

Molex is correct. Traditional IDE, also called Parallel ATA (PATA), hard drives commonly use the four-pin peripheral power connector generally known as a Molex connector. This connector comes directly from the computer's power supply and provides the voltages required by the drive: +5 V for the drive's logic circuitry and +12 V for the spindle motor and related mechanical components. The connector is keyed with beveled edges so that it is installed in the proper orientation; it should not be forced. In a legacy IDE/PATA installation, the drive normally has both a wide 40-pin ribbon cable for data transfer and a separate four-pin Molex connector for power. This contrasts with SATA drives, which use a flat 15-pin SATA power connector rather than the older four-pin peripheral connector. Recognizing the Molex connector is useful when servicing older desktop systems, connecting legacy optical drives, or selecting a suitable power adapter. See the Molex connector overview and Seagate's PATA documentation for additional background on legacy PATA/IDE hardware.

QUESTION NO: 32

A user cannot access any local or remote resources. A technician runs a command to find the configuration information and gets the following results:

IPv4 Address: 192.168.1.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.1

The technician checks with the NOC, and it verifies that the upstream router is configured correctly. The next hop given to the technician matches the value in the output. Which of the following should the technician change in order for the userâ€™s connection to work fully?

A. DNS settings

B. Gateway

C. Lease time

D. Firewall rules

E. Subnet mask

ANSWER: E

Explanation:

Subnet mask is the required change. The configured IPv4 address, 192.168.1.10, with a 255.255.255.0 mask, belongs to the 192.168.1.0/24 network. Under that mask, the verified default gateway address, 192.168.2.1, is in a separate 192.168.2.0/24 network. Before a host can send traffic to a default gateway, it must be able to reach that gateway over its local Layer 2 network. Because the NOC has confirmed that 192.168.2.1 is the correct next-hop router address, the client configuration must be adjusted so that both the client address and gateway address are treated as members of the same subnet. For example, a 255.255.254.0 (/23) mask defines the 192.168.0.0 through 192.168.1.255 range, so it would not include 192.168.2.1; a suitable mask must instead be selected according to the network's intended addressing design, such as one that encompasses both addresses. A subnet mask determines which portion of an IPv4 address identifies the local

network and therefore whether a destination is reached directly or through the default gateway. See Microsoft's TCP/IP addressing and subnetting guidance and RFC 1812 for IPv4 routing requirements.

QUESTION NO: 33

Which of the following internet connection types provides the fastest speeds and greatest coverage in less populated areas with minimal infrastructure?

A. Fiber

B. Cable

C. DSL

D. Cellular

E. Satellite

ANSWER: E

Explanation:

Satellite is the best answer because it can deliver broadband service to remote and sparsely populated locations without requiring terrestrial last-mile cabling or nearby cellular towers. A customer needs a satellite dish, modem, clear view of the sky, and electrical power at the installation site; the connection is then carried through a satellite network to a ground gateway. This makes satellite service available across very large geographic areas, including rural properties, temporary worksites, and other locations where deploying local network infrastructure would be impractical. Modern satellite broadband, particularly low-Earth-orbit services, can provide substantially improved throughput and responsiveness compared with traditional geostationary satellite offerings. For an exam question that emphasizes wide coverage in areas with minimal local infrastructure, satellite is the connection type whose service footprint is least dependent on local population density. CompTIA includes satellite among the Internet connection technologies candidates must compare, including their availability and performance characteristics. The FCC also identifies satellite as a broadband technology capable of serving locations where terrestrial options may not be available. See the CompTIA exam objectives resource and the FCC's Getting Broadband guide.

QUESTION NO: 34

Which of the following describes an advantage of mini-LED displays over OLED displays?

A. Increased contrast

B. No backlight

C. Improved viewing angle

D. Decreased burn-in

ANSWER: D

Explanation:

Decreased burn-in is an advantage of mini-LED displays compared with OLED displays. A mini-LED display is an LCD panel illuminated by a backlight containing many very small LEDs arranged into local-dimming zones. The LCD pixels modulate that backlight rather than producing light through self-emissive organic pixel materials. As a result, mini-LED displays avoid the differential aging of individual self-emissive pixels that can cause persistent image retention, commonly called burn-in, after static interface elements such as logos, taskbars, or HUDs have been shown for long periods.

OLED technology delivers excellent image quality because each pixel emits its own light, but the organic emissive materials can age at different rates depending on how intensively particular screen areas are used. Manufacturers use pixel shifting, screen savers, and brightness-management features to mitigate this behavior, but the risk remains a practical consideration for displays used with long-lived static content. Mini-LED therefore offers an especially useful durability benefit in

productivity, signage, and other static-content scenarios while still enabling strong brightness and localized backlight control. Apple notes that its Liquid Retina XDR mini-LED display uses individually controlled LEDs for local dimming, while RTINGS documents the distinct permanent-burn-in behavior associated with OLED panels. See Apple Support and RTINGS OLED burn-in longevity test.

QUESTION NO: 35

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 successful single POST beep commonly indicates that the firmware has completed its initial hardware self-test and has progressed to the boot-device discovery stage. At that point, boot configuration and attached removable media are especially relevant. **Boot order** is correct because UEFI/BIOS uses its configured boot priority to select a device containing a valid boot loader. If the internal system drive is not first in the sequence, is omitted, or an unavailable device is prioritized, the computer can complete POST and then display a boot-related error.

USB flash drive is also correct because firmware may attempt to boot from an inserted USB device before the internal drive. A flash drive that is nonbootable, improperly prepared, or contains an incompatible boot configuration can cause the system to stop with an error after POST. Removing the USB device or adjusting the boot order allows the firmware to attempt the intended internal boot device. Microsoft's recovery guidance specifically identifies removing external drives as a relevant step for startup problems, and its UEFI guidance describes the firmware boot manager and boot entries: Microsoft Support; Microsoft Learn.

QUESTION NO: 36

A technician is preparing to install a replacement laser printer cartridge. Which of the following components are typically associated with the laser printing process? (Select TWO).

A. Imaging drum

B. Fuser

C. Ink cartridge

D. Print ribbon

E. Platen glass

ANSWER: A B

Explanation:

The imaging drum is correct because it receives the electrostatic image created by the laser and transfers toner to the paper. Depending on the printer model, the drum may be integrated into the toner cartridge or installed as a separate replaceable component.

The fuser is also correct because it applies heat and pressure to permanently bond toner to the paper after the toner image has been transferred. A fuser is a core component of the laser printing process, although it is normally a maintenance component rather than part of a standard toner-cartridge replacement. HP provides laser printer maintenance and print-quality information at HP Support.

QUESTION NO: 37

A technician needs to fix a Cat 5 cable issue. The cable, which is connected to a network jack, fails when it is moved around. Which of the following items must the technician use to fix the issue? (Select TWO).

A. Scissors

B. Network tap

C. Magnetized screwdriver

D. Tone generator

E. RJ45 connector

F. Crimper

ANSWER: E F

Explanation:

An RJ45 connector and a crimper are the appropriate items for repairing a twisted-pair Ethernet patch cable when an intermittent connection occurs as the cable or plug is moved. This symptom commonly indicates a worn, damaged, or poorly terminated modular plug, or conductors that no longer maintain reliable contact inside that plug. The technician can cut off the faulty termination, arrange the Cat 5 conductors according to the required Ethernet pinout, insert them fully into a replacement RJ45 connector, and use a crimper to press the connector contacts into the conductors and secure the strain-relief tab around the cable jacket. This creates a new physical termination capable of maintaining stable electrical contact during normal movement. Proper termination is a core practical networking skill covered by CompTIA A+ objectives, including recognizing networking cable types and their associated tools. After replacing the connector, the technician should verify continuity and correct wire mapping with an appropriate cable tester before returning the cable to service. See CompTIA's exam-objectives resource page and Fluke Networks' overview of copper cable terminations for related cabling and termination guidance.

QUESTION NO: 38

Which of the following wireless frequency ranges involves the use of channels 1, 6, and 11?

A. 2.4GHz

B. 5GHz

C. 6GHz

D. 60GHz

ANSWER: A

Explanation:

The correct answer is **2.4GHz**. In common Wi-Fi deployments using the 2.4 GHz band, channels 1, 6, and 11 are the standard non-overlapping channel choices in regions that permit those channels. Each 2.4 GHz Wi-Fi channel occupies more spectrum than the 5 MHz spacing between adjacent channel center frequencies. As a result, nearby channels overlap and can create co-channel or adjacent-channel interference. Separating access points onto channels 1, 6, and 11 provides sufficient spacing for typical 20 MHz channels, allowing multiple nearby wireless networks or access points to operate with substantially less overlap.

This channel-planning convention is particularly important in homes, offices, classrooms, and other dense wireless environments. A technician performing a wireless survey or configuring several access points should use these channel assignments strategically, while also considering neighboring networks, signal strength, and client density. Channel availability can vary by regulatory domain, but 1, 6, and 11 are the familiar non-overlapping 2.4 GHz channels used in North American Wi-Fi planning. Cisco provides an overview of 2.4 GHz channel overlap at Cisco Wireless LAN Channel Deployment Guide. The Wi-Fi Alliance also describes Wi-Fi bands and operation at Wi-Fi Alliance: Discover Wi-Fi.

QUESTION NO: 39

Which of the following technologies can allow multiple networks to traverse a switch?

A. VLAN

B. VRRP

C. VPN

D. DHCP

ANSWER: A

Explanation:

VLAN is correct because a virtual LAN logically segments a switched network into separate Layer 2 broadcast domains. A managed switch assigns access ports to a particular VLAN, allowing devices connected to ports in the same VLAN to communicate as though they are on the same physical LAN, even when those ports are distributed across the switch. More importantly for carrying multiple networks, an IEEE 802.1Q trunk link adds a VLAN tag to Ethernet frames so traffic from multiple VLANs can traverse one physical switch-to-switch or switch-to-router connection while remaining logically separated. For example, a switch can carry an employee VLAN, a guest VLAN, and a voice VLAN over the same trunk while preserving the identity and isolation of each network. VLANs therefore enable network segmentation without requiring separate physical switches and dedicated cabling for every network. Inter-VLAN communication, when needed, is handled by a Layer 3 device such as a router or multilayer switch. CompTIA's networking objectives include configuring VLANs and recognizing trunking as a mechanism for transporting traffic for multiple VLANs. Cisco's overview of VLANs and trunking is available at Cisco VLAN technology overview, and the IEEE 802.1Q standard is described by the IEEE 802.1Q standard page.

QUESTION NO: 40

Which of the following describes an environment in which virtual machines are hosted on premises and in a cloud?

A. Hybrid

B. Public

C. Private

D. SaaS

ANSWER: A

Explanation:

Hybrid is the correct description for an environment that hosts virtual machines both on premises and in a cloud provider's infrastructure. A hybrid cloud architecture combines local resources, such as organization-owned servers and virtualization hosts, with cloud-based compute resources. This approach lets an organization retain workloads locally when required by latency, data-residency, operational, or legacy-application needs while also using cloud capacity for scalability, disaster recovery, testing, or variable demand.

For example, an organization might run a line-of-business virtual machine in its own server room but replicate data to cloud-hosted virtual machines for resilience. It could also extend network connectivity between its on-premises environment and a

cloud virtual network, allowing selected systems and users to access resources across both locations. The defining characteristic is the intentional use and integration of both deployment locations—not simply using a cloud service independently of local systems.

This terminology aligns with common cloud-computing definitions: the National Institute of Standards and Technology describes hybrid cloud as a composition of two or more distinct cloud infrastructures that remain unique entities but are bound together to enable data and application portability. See NIST SP 800-145 and Microsoft's hybrid networking guidance.

QUESTION NO: 41

A developer wants to protect critical data from hard drive failure. Their workstation has two hard drives. Which RAID level should they use?

A. RAID 0

B. RAID 1

C. RAID 5

D. RAID 10

ANSWER: B

Explanation:

RAID 1 is the appropriate choice because it mirrors data between two physical drives. Each write is duplicated onto both disks, so the workstation maintains an identical copy of its data on each drive. If either hard drive fails, the system can continue operating from the surviving member of the mirror, and the failed drive can be replaced and rebuilt to restore redundancy. This directly meets the goal of protecting critical data from a single hard-drive failure while using exactly two drives. The usable capacity of a two-drive RAID 1 array is equivalent to the capacity of the smaller drive, since the second drive is dedicated to the mirrored copy. RAID is intended to improve availability and fault tolerance, but it is not a substitute for maintaining separate backups; accidental deletion, corruption, ransomware, and site-wide events can affect both members of a mirror. For additional context on Windows software RAID/storage resiliency concepts, see Microsoft Learn: Storage Spaces overview. CompTIA's official A+ certification page also identifies storage technologies as part of Core 1 exam coverage: CompTIA A+ certification.

QUESTION NO: 42

A programmer needs to run a virtual machine on their laptop to test an application. Which of the following virtualization technologies is the best way to accomplish this goal?

A. Containerization

B. Hypervisor

C. Virtual desktop infrastructure

D. Emulation

ANSWER: B

Explanation:

Hypervisor is the correct technology because it creates and runs virtual machines (VMs) on a physical host, such as the programmer's laptop. A hypervisor abstracts the laptop's hardware resources—including processor capacity, memory, storage, and networking—and presents virtualized hardware to each guest operating system. This lets the programmer install an isolated operating system and application environment for testing without replacing or substantially changing the laptop's primary operating system. For a laptop-based development or test scenario, a hosted (Type 2) hypervisor is commonly used. It runs as an application on top of the existing operating system and supports VMs through products such as VMware Workstation, Oracle VirtualBox, or Microsoft Hyper-V where supported. The VM can be checkpointed, configured

with specific resource allocations, and reset to a known state, which is especially useful for repeatable application testing. Hypervisors are the core platform technology behind virtual machines, as described in Microsoft's Hyper-V overview. The National Institute of Standards and Technology also defines a virtual machine monitor, or hypervisor, as the software layer that enables multiple operating systems to share a host's hardware resources: NIST Hypervisor glossary.

QUESTION NO: 43

The owner of a restaurant reports that wireless network connections are lost intermittently throughout the day. Which of the following steps should a technician take to troubleshoot the issue? (Select TWO).

A. Identify the location of devices that utilize 2.4GHz.

B. Check to see if the phones are IJTP or STP lines.

C. Test to see if the copper electrical Wires are causing interference.

D. Map all of the wireless signals in the restaurant.

E. Verify T568B is being used in the wiring closet patch panel.

F. Schedule timed router reboots throughout the day.

ANSWER: A D

Explanation:

"Identify the location of devices that utilize 2.4GHz." is an appropriate first troubleshooting step because intermittent Wi-Fi drops can result from radio-frequency interference and congestion in the 2.4 GHz band. In a restaurant, potential sources include Bluetooth equipment, wireless peripherals, microwave ovens, cordless devices, and neighboring wireless networks. Locating these devices helps the technician correlate connection losses with physical areas, operating times, or equipment use.

"Map all of the wireless signals in the restaurant." is also correct because a wireless survey or signal map provides evidence about the RF environment. It can reveal overlapping access-point coverage, excessive signal strength from nearby networks, co-channel contention, channel overlap, dead zones, and areas where interference is most significant. With this information, the technician can make an informed remediation decision, such as adjusting access-point placement, selecting less-congested channels, or moving compatible clients to the 5 GHz or 6 GHz bands where available. These actions align with the CompTIA A+ networking objective area covering wireless troubleshooting, including interference, signal issues, and wireless configuration considerations. See the CompTIA exam objectives resource page and the CISA wireless-network guidance.

QUESTION NO: 44 - (SIMULATION)

A user reports poor performance on the application server.

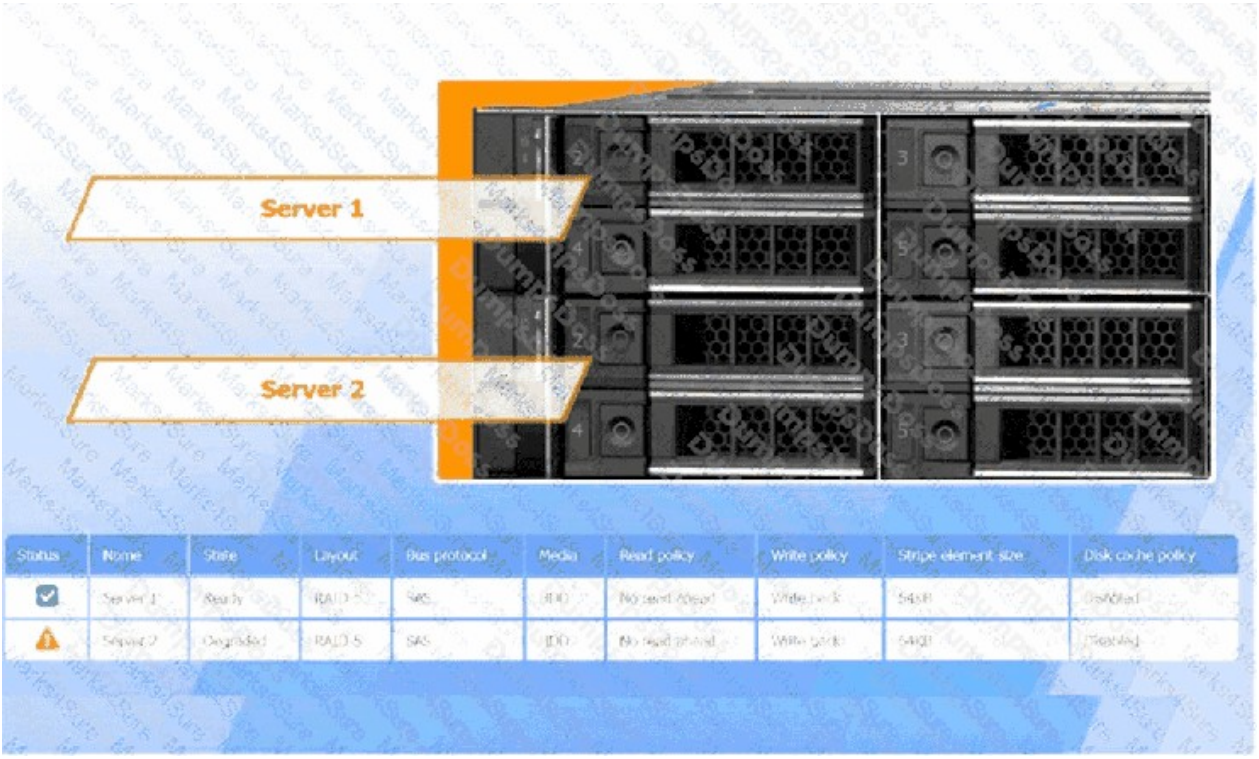
INSTRUCTIONS

Click on Server 1 and Server 2 and review the information presented in each chart to

determine which drives need to be replaced.

Select the appropriate replacement drive that should be used, for the least performance degradation to the server.

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



ANSWER: See the explanation for the answer

Explanation:

Replace the failed drive in Server 2 (the server reporting **Degraded** status). Select a **SAS HDD** replacement drive.

Server 2 is a RAID-5 array and its configuration shows:

Use the SAS HDD replacement in the failed/alerted Server 2 bay, matching the existing array drive capacity/specification. Do not replace Server 1 drives; Server 1 is **Ready**. Replacing Server 2's failed SAS HDD restores the RAID-5 array from degraded operation and minimizes further performance loss.

QUESTION NO: 45

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 and appropriate safety action when a laptop emits a burning smell. A burning odor can indicate overheating, a failed battery, damaged wiring, a short circuit, or another electrical fault. Removing power stops normal operation, reduces the risk of additional component damage, and helps prevent an electrical

or fire hazard before any physical investigation begins. The technician should avoid continuing to operate or charge the device until it has been assessed safely.

“Check for foreign objects, liquid spills, and internal damage.” is the appropriate next troubleshooting step once the laptop is powered down and disconnected. A careful visual inspection can identify evidence of a thermal or electrical event, such as liquid residue, debris obstructing ventilation, discoloration, melted insulation, scorched components, swollen battery cells, or damaged connectors. Documenting observable damage also supports an accurate repair, warranty, or replacement decision. These actions align with CompTIA’s troubleshooting emphasis on identifying hazards, protecting equipment, and inspecting for physical causes before proceeding with deeper diagnostics. See the CompTIA exam objectives resource page and the OSHA electrical safety guidance.

QUESTION NO: 46

Which of the following can carry data and electricity to network devices? (Select two).

A. Router

B. Injector

C. Cable modem

D. Access point

E. PoE

F. Unmanaged switch

ANSWER: B E

Explanation:

Injector and **PoE** are correct because Power over Ethernet delivers DC power and Ethernet data through the same twisted-pair Ethernet cabling to a compatible powered device. PoE is the networking technology and standards framework that permits this combined delivery, commonly supporting devices such as wireless access points, IP cameras, VoIP phones, and some networked sensors without requiring a separate local power adapter.

An injector is a device used when the Ethernet switch does not provide PoE. It accepts an Ethernet data connection, adds the appropriate electrical power to that connection, and sends the resulting powered Ethernet link onward to the network device. This enables one cable run to provide both network connectivity and electrical power. In a typical installation, the injector connects between the non-PoE switch and the powered device; the injector supplies the power while preserving Ethernet data communication.

CompTIA’s current Core 1 objectives include PoE and PoE injectors within networking hardware knowledge. For additional technical context, see the CompTIA exam objectives and the IEEE overview of 802.3af Power over Ethernet.

QUESTION NO: 47

Which of the following are characteristics of cloud computing? (Select TWO).

A. Rapid elasticity

B. Measured service

C. Dedicated physical hardware for every customer

D. Manual allocation of all resources by the customer

E. Local-only network access

ANSWER: A B

Explanation:

Rapid elasticity is correct because cloud resources can be provisioned and released quickly as demand changes. For example, an organization can increase compute capacity during a busy period and reduce it afterward.

Measured service is also correct because cloud providers monitor resource consumption, such as storage capacity, processing use, or network traffic. This metering supports usage reporting and billing models. NIST identifies both rapid elasticity and measured service as essential characteristics of cloud computing in SP 800-145.

QUESTION NO: 48

An IT specialist compares Bluetooth and NFC technologies for mobile device connectivity. Which of the following statements accurately describes a key difference between the two?

A. NFC is faster than Bluetooth when transferring large files between devices.

B. NFC consumes more power than Bluetooth, making it less suitable for devices in which battery conservation is crucial.

C. NFC requires pairing with the receiving host, whereas Bluetooth just needs the available connection.

D. NFC works best within a few centimeters, but Bluetooth can connect devices that are up to 32ft (10m) apart.

ANSWER: D

Explanation:

NFC works best within a few centimeters, but Bluetooth can connect devices that are up to 32ft (10m) apart. This reflects the fundamental intended use of each wireless technology. Near Field Communication uses very short-range radio communication, typically requiring devices to be brought extremely close together—often within about 4 cm—for actions such as contactless payments, access badges, and quickly initiating a connection. Its deliberate proximity requirement is useful when an interaction should occur only between devices physically near one another.

Bluetooth is designed for wireless personal-area networking over a substantially longer distance. A commonly cited Bluetooth range for many consumer devices is approximately 10 meters (33 feet), although real-world range varies with Bluetooth version, radio class, transmit power, antenna design, obstacles, and interference. This longer operating distance supports connections to peripherals such as headsets, keyboards, speakers, and wearable devices without requiring direct contact or near-contact placement. NFC can also assist with connection setup in some situations, but its defining connectivity distinction is its very short operating range compared with Bluetooth. See the NFC Forum overview of NFC and the Bluetooth SIG technology overview.

QUESTION NO: 49

The Chief Information Security Officer asks a technician to inventory desktop PCs to determine which ones meet the requirements for Secure Boot. The technician must also configure the PCs for non-user-controllable keys. Which of the following are necessary to meet the enhanced security requirements? (Select two).

A. VDI

B. BIOS password

C. TPM

D. UEFI

E. Disabled boot drive

F. USB permissions

ANSWER: B D

Explanation:

UEFI is necessary because Secure Boot is implemented by Unified Extensible Firmware Interface firmware. During startup, UEFI Secure Boot validates the signature of preboot components, such as the boot manager and operating-system loader, against trusted certificates and keys held in the firmware's Secure Boot databases. This establishes a trusted boot path before the operating system begins loading. Microsoft describes Secure Boot as a security standard developed for PCs using UEFI firmware: Microsoft Secure Boot documentation.

BIOS password is also necessary for the stated enhanced requirement that the Secure Boot keys not be user-controllable. More accurately called a UEFI administrator or setup password on modern systems, this firmware-level credential restricts access to firmware configuration. It helps ensure that an end user cannot simply enter the setup utility and alter Secure Boot state, delete trusted keys, enroll unauthorized keys, or change relevant boot settings. The technician should use a strong administrative firmware password and manage it according to organizational policy. NIST's firmware-resilience guidance recognizes the importance of protecting firmware configuration and update functions from unauthorized modification: NIST SP 800-193.

QUESTION NO: 50

An IT specialist sets up a new computer for a user who requires a high-end video card and the fastest hard drive possible. Which of the following connectors should the specialist verify are available on the motherboard? (Select two).

A. Molex

B. NVMe

C. SATA

D. FireWire

E. USB-C

F. PCIe

ANSWER: B F

Explanation:

PCIe is required because a high-end discrete video card installs in a motherboard PCI Express expansion slot—typically a full-length, high-bandwidth x16 slot. PCIe provides the direct system interconnect and throughput needed by modern graphics adapters. The specialist should confirm that a suitable physical slot is present and available before selecting the video card.

NVMe identifies the high-performance storage interface/protocol used by the fastest consumer solid-state drives. In a motherboard installation, an NVMe SSD is commonly fitted to an M.2 socket that carries PCIe lanes, though NVMe drives can also be provided through a PCIe expansion card. Therefore, verifying motherboard support for NVMe-capable PCIe/M.2 storage ensures that the system can use an SSD with substantially higher throughput and lower latency than conventional disk-based storage. CompTIA's current Core 1 objectives include PCIe expansion slots and storage interfaces such as M.2 and NVMe among the motherboard and storage technologies technicians must recognize. See the CompTIA exam objectives page and Microsoft's NVMe overview.

QUESTION NO: 51

A technician is troubleshooting a desktop PC that is plugged into a UPS. The PC loses the system date/time after every power outage. Which of the following should the technician do to resolve the issue? (Select two).

A. Run a BIOS update.

B. Swap out the RAM.

C. Disable NTP in the OS.

D. Repair the backup power source.

E. Replace the CMOS battery

F. Install a surge protector.

ANSWER: D E

Explanation:

“Replace the CMOS battery” is appropriate because the CMOS/RTC battery provides standby power for the real-time clock and firmware configuration when the desktop has no external power. A depleted battery can no longer preserve the clock state during a loss of utility power, causing the system date and time to reset. Replacing it restores the independent low-power source required to retain those settings while the computer is shut down or disconnected.

“Repair the backup power source” is also appropriate because the UPS is intended to supply temporary battery power when utility power fails. A functional UPS prevents an outage from immediately removing power from the desktop, allowing the system to remain powered long enough for an orderly shutdown or to continue operating through a brief interruption. Verifying and repairing the UPS—including its battery and output capability—addresses the stated condition that the computer is connected to backup power but still experiences the effects of every outage. These actions align with CompTIA’s hardware troubleshooting focus on resolving power-related symptoms and maintaining system configuration. See the CompTIA A+ exam objectives and Dell’s guidance on replacing a CMOS battery.

QUESTION NO: 52

A customer wants a new desktop computer that can run recently released, popular video games. Which of the following should a desktop technician consider when building the computer? (Select two.)

A. A low-wattage power supply unit

B. An integrated GPU

C. A high amount of RAM

D. A dedicated graphics card

E. A Linux operating system

F. A TPM 2.0 module

ANSWER: C D

Explanation:

A high amount of RAM and **A dedicated graphics card** are appropriate considerations for a desktop intended to run current, popular games. Modern games keep substantial quantities of game assets in memory, including textures, maps, audio, shaders, and object data. Sufficient system memory also lets the operating system and supporting applications run alongside the game without excessive paging to storage, which can produce stuttering and longer loading times. The exact capacity should be selected according to the game publishers’ recommended specifications, with additional capacity considered for streaming, content creation, or other concurrent workloads.

A dedicated graphics card supplies a discrete graphics processing unit and dedicated video memory. This hardware is designed to render demanding three-dimensional graphics workloads, including high-resolution textures, lighting, shadows, visual effects, and high frame rates. When selecting the card, the technician should also plan for compatible motherboard expansion, adequate case clearance and cooling, suitable display connections, and a power supply sized for the complete system’s peak load. These hardware considerations align with the A+ Core 1 hardware focus on choosing components that meet a customer’s stated requirements. See the CompTIA exam objectives resource and Microsoft’s GPU overview.

QUESTION NO: 53

Which of the following technologies is the best way to reduce hardware costs in a data center by allowing multiple operating systems to run on a single physical server?

A. Containerization

B. Cloud computing

C. Virtualization

D. Remote desktop services

ANSWER: C

Explanation:

Virtualization is correct because it uses a hypervisor to abstract a physical server's hardware resources—such as CPU, memory, storage, and networking—and allocate them to multiple isolated virtual machines. Each virtual machine can run its own complete guest operating system and applications while sharing the same underlying physical host. Consolidating workloads in this manner reduces the number of separate servers an organization must buy, power, cool, rack, maintain, and replace. It also improves utilization because workloads with different resource demands can share a host rather than leaving capacity idle on multiple underused physical systems. Virtualization platforms can further simplify management through capabilities such as virtual-machine provisioning, snapshots, resource allocation, and migration between hosts. These capabilities make virtualization a foundational data-center technology for server consolidation and for providing distinct operating-system environments without requiring one physical server per operating system. Microsoft describes Hyper-V virtual machines as isolated computing environments that can run their own operating systems and applications on a physical host: Hyper-V overview. NIST also defines virtualization as using a virtual abstraction layer to enable multiple operating systems and applications to run on the same physical hardware: NIST Virtualization glossary entry.

QUESTION NO: 54

Which of the following is used to prevent unwanted emails from reaching an inbox?

A. Proxy server

B. Intrusion detection system

C. Firewall

D. Spam gateway

ANSWER: D

Explanation:

A **spam gateway** is designed to inspect email traffic and stop or divert unsolicited, malicious, or otherwise unwanted messages before they are delivered to a user's primary inbox. Positioned in the email-delivery path, it evaluates messages using techniques such as sender and domain reputation, blocklists and allowlists, message-content analysis, attachment scanning, URL inspection, and authentication results from technologies such as SPF, DKIM, and DMARC. Based on the organization's policy and the gateway's analysis, a message can be rejected during delivery, quarantined for administrative or user review, tagged as spam, or routed to a junk-email folder. This provides centralized protection for an organization's mailboxes and reduces exposure to phishing, malware-bearing attachments, business email compromise attempts, and bulk unsolicited email. In the CompTIA A+ Core 1 exam objectives, spam gateways are included among network-based internet appliances that support secure and managed network services. Microsoft also describes anti-spam protection as filtering messages to identify and separate unwanted bulk email and spam from legitimate mail. See the CompTIA exam objectives resource and Microsoft's anti-spam protection documentation.

QUESTION NO: 55

A user reports that a printer is leaving streaks on printed pages. The paper type and the toner have been replaced. Which of the following should the technician check NEXT to resolve the issue?

A. System board

B. Paper tray

C. Memory

D. Fuser

ANSWER: D

Explanation:

Fuser is the correct component to check next. In a laser printer, the fuser assembly applies heat and pressure to permanently bond toner to the paper after the image has been transferred. A worn, contaminated, or damaged fuser roller or film can leave repetitive streaks, lines, smears, or areas where toner is not properly fused. Since the technician has already addressed two common consumable-related contributors—paper and toner—the fuser is the most appropriate remaining component among the choices to inspect. The technician should look for toner buildup, damage to the fuser sleeve or pressure roller, and signs that the assembly is not reaching or maintaining its normal operating temperature. Following the printer manufacturer's service procedure is important because fusers operate at high temperatures and may need time to cool before they can be safely handled. If cleaning does not resolve the print defect or visible wear is present, replacing the fuser maintenance kit or fuser assembly is the appropriate corrective action. HP's laser-printer troubleshooting guidance discusses print-quality defects and maintenance components: HP LaserJet Support. For general laser-printer operating and troubleshooting information, see Brother Support.

QUESTION NO: 56 - (DRAG DROP)

An office manager reports that a printer is experiencing performance issues. Printouts are smudging when they are handled, and. recently, whenever the manager tries to print oversized documents, the paper jams before anything is printed on it.

ANSWER:

Explanation:

A laser printer creates an image by placing toner on the paper and then passing that sheet through the fuser. The fuser uses a heated roller and a pressure roller to melt and press toner into the paper fibers, producing a durable image. Therefore, the upper printer-engine location is correctly identified as the fuser. This relationship also fits the reported smudging: if toner can be rubbed or smeared after printing, it has not been sufficiently bonded to the page during the fusing stage. HP describes laser-printer toner as being fused to paper through heat and pressure in its laser printing support documentation.

The main front section of the printer is the toner-cartridge access area. The toner cartridge holds the powdered imaging material used by the laser-print process and is replaced through the printer body rather than through a paper tray. The letter-size input tray contains the feed mechanism, including the rollers that grip and advance sheets into the print path. Proper paper feeding starts there before a page reaches the imaging and fusing assemblies. HP's paper-feed troubleshooting guidance explains the role of paper pickup and feed in avoiding jams.

The lower legal-size position corresponds to the duplexer area. A duplexer reverses or redirects a printed sheet through a secondary paper path so the printer can place an image on the other side. It is part of the printer's paper-handling path and is associated with the lower paper-path assembly in this diagram. The correct completed matching is: FUSER to the upper printer position; TONER to the main printer-body position; ROLLERS to Tray 2 - Letter; and DUPLEXER to Tray 3 - Legal. The ink cartridge is not used because this is a laser-printer configuration that uses toner.

QUESTION NO: 57

Which of the following services are typically provided by a networked host to facilitate file sharing across different OSs? (Select two).

A. NTP

B. SMB

C. IMAP

D. FTP

E. ROP

F. LDAP

ANSWER: B D

Explanation:

SMB and FTP are services a networked host can provide to make files available to clients running different operating systems. SMB (Server Message Block) is the standard Windows network file-sharing protocol and supports access to shared folders and printers. It is also interoperable with macOS and Linux systems; Linux hosts commonly use Samba to implement SMB-compatible file and print sharing. This makes SMB a typical choice where users need to browse and use shared network folders across a mixed-OS environment. FTP (File Transfer Protocol) provides a broadly supported client-server method for transferring files between hosts. An FTP server can accept connections from compatible clients on Windows, macOS, and Linux, making it useful for cross-platform upload and download workflows. In the CompTIA A+ Core 1 objectives, SMB/CIFS and FTP are included among common ports and protocols technicians must recognize, with SMB/CIFS associated with network file sharing and FTP associated with file transfer. Although secure alternatives such as SFTP are generally preferred when sensitive data is involved, FTP remains a recognized file-transfer service and is the correct selection in this question. See the CompTIA exam objectives resource and Microsoft's SMB overview.

QUESTION NO: 58

A user reports intermittent latency when accessing an internal website hosted at a remote office. Which of the following should a technician do? (Select two)

A. Run ipconfig /all

B. Run ping -t

C. Run nslookup

D. Examine the physical switchport

E. Configure QoS

F. Run tracert

G. Call ISP

ANSWER: B F

Explanation:

Run ping -t is appropriate because continuous ICMP echo testing provides an ongoing view of reachability and round-trip response times between the workstation and the remote resource or its host. This allows a technician to capture intermittent symptoms as they occur, including variable latency, dropped replies, and timeouts. Recording when response times change also helps correlate the issue with periods of congestion or other recurring network conditions. Microsoft documents that the `-t` switch causes Ping to continue sending echo requests until manually stopped.

Run tracert is also appropriate because it identifies the routed path to the remote office and reports timing information for each network hop. The results help narrow the scope of investigation by showing where delay may begin along the route, such as at an interoffice router, WAN edge, VPN path, or other transit point. Used alongside continuous ping results, traceroute testing supports a structured troubleshooting process: confirm the intermittent behavior, identify the route involved, and gather evidence before escalating or changing network configuration. See Microsoft's command references for ping and tracert.

QUESTION NO: 59

Which of the following statements best summarize managed vs unmanaged switches? (Select two).

A. Unmanaged switches are generally more expensive

B. Unmanaged switches have more security capabilities

C. Unmanaged switches start working as soon as they are plugged in to the network

D. Managed switches have more features

E. Managed switches require no configuration

F. Managed switches consume less power

ANSWER: C D

Explanation:

“Unmanaged switches start working as soon as they are plugged in to the network” is correct because an unmanaged switch is intended for basic Ethernet connectivity with no administrative setup. It uses built-in forwarding behavior to learn device MAC addresses and send frames to the appropriate connected port, making it suitable where simple plug-and-play expansion is needed. “Managed switches have more features” is also correct because these switches offer a management interface that enables administrators to configure and monitor switch operation. Common managed-switch capabilities include creating VLANs to segment networks, configuring port settings, applying port-security controls, monitoring traffic and device status, and using SNMP for centralized management. These administrative and security-related capabilities support more complex business networks where traffic separation, visibility, and policy enforcement are required. CompTIA includes managed and unmanaged switches among the network devices technicians must be able to compare, recognizing unmanaged equipment as simple connectivity hardware and managed equipment as configurable infrastructure. See the CompTIA exam objectives resource page and Cisco’s overview of network switch functions and managed-switch features.

QUESTION NO: 60

A technician connects a WISP modem to a portable router in order to provide an Ethernet connection to a laptop. Which of the following network types has the technician configured?

A. WAN

B. SAN

C. PAN

D. MAN

ANSWER: A

Explanation:

WAN is correct because the WISP modem provides the router’s connection to a Wireless Internet Service Provider. That provider-facing connection is the router’s wide area network interface: it links the local equipment to an external network and ultimately to Internet services over infrastructure that extends beyond the user’s immediate location. The portable router uses this WAN uplink as its source of connectivity, then makes that connectivity available to the attached laptop through its local Ethernet interface. In practical router setup terminology, the cable from an ISP-provided modem or gateway is connected to the router’s Internet/WAN port, while devices such as laptops connect on the local side of the router. CompTIA’s A+ Core 1 objectives include identifying common network types and network-device roles, including WAN connectivity, as part of foundational networking knowledge. A WISP is simply an ISP whose last-mile service is delivered wirelessly; it still functions as the external provider network for the customer router. See the CompTIA exam objectives resource page and Cisco’s overview of wide-area networking.

QUESTION NO: 61

Which of the following connectors will uplink a new ISP cable modem to its wall jack?

A. F-type

B. LC

C. RJ45

D. Lightning

ANSWER: A

Explanation:

F-type is the correct connector for linking a cable modem to the provider's coaxial wall outlet. Cable Internet service is commonly delivered over the same coaxial-cable infrastructure used for cable television, including DOCSIS-based services. An F-type connector is a threaded RF coaxial connector: the cable's center conductor carries the signal, while the outer threaded shell provides a secure mechanical connection and shielding/ground reference. The technician attaches the coaxial cable's F-type connector to the threaded port on the wall plate and to the cable input on the modem, typically labeled *Cable In*, *RF In*, or similar. This physical connection allows the modem to communicate with the ISP's cable network and establish service before the modem provides Ethernet connectivity to a router or local device. CompTIA Core 1 expects candidates to identify connectors by the cable medium and service context; a cable-modem connection to a wall jack indicates coaxial cabling and therefore an F-type connector. The FCC describes cable systems as using coaxial cable infrastructure, and CommScope provides technical details on F connectors used in broadband coaxial installations. See the FCC cable television consumer guide and CommScope coaxial connector information.

QUESTION NO: 62

An employee requires a workstation with three high-end graphics cards to render 3-D models. A technician must choose a power supply that meets the power requirements for the components and takes into consideration the mission-critical nature of the work. Which of the following meet the requirements? (Select two).

A. 12V output

B. Modularity

C. 20-pin motherboard connector

D. Redundancy

E. 3.3V output

F. 240 VAC input

ANSWER: A D

Explanation:

12V output is required because modern graphics cards draw the overwhelming majority of their operating power from the power supply's 12 V rail, delivered through the PCIe expansion slot and supplemental PCIe power connectors. A workstation containing three high-end GPUs therefore needs a power supply with sufficient total wattage and, critically, enough stable 12 V capacity to supply the combined GPU and processor load. The ATX power-supply design specification identifies 12 V as a principal output rail and defines its output and regulation requirements. See the Intel Power Supply Design Guide.

Redundancy addresses the mission-critical requirement. A redundant power supply uses more than one power module so that, when one module fails, the remaining module can continue supplying power without shutting down the workstation. This reduces downtime and supports continuous rendering work, particularly in professional environments where an unexpected interruption can delay work or risk unsaved data. Redundant units are commonly designed with hot-swappable modules, allowing a failed module to be replaced while the system remains online. CompTIA's A+ objectives include selecting power supplies based on features such as redundancy and the power demands of the system. Review the CompTIA exam objectives resources for the current hardware-domain scope.

QUESTION NO: 63

Which of the following RAM characteristics allows for recovery from data faults in memory modules?

A. Capacity

B. Speed

C. ECC

D. DDR

E. Parity

ANSWER: C

Explanation:

ECC is the RAM characteristic that supports recovery from data faults because it adds error-correcting information to the data stored in memory. When a correctable memory error occurs, ECC logic can identify the erroneous bit and restore the intended value, allowing normal operation to continue without the error being passed to the operating system or an application. This capability is especially valuable in systems where data integrity and uptime matter, such as servers, workstations, and systems handling critical workloads.

In common implementations, ECC memory uses a scheme that can correct single-bit errors and detect certain multiple-bit errors. The platform must support ECC end to end: the installed memory modules, motherboard/chipset, processor memory controller, and firmware configuration must all be compatible. ECC does not eliminate every possible hardware failure, but it provides an important protection layer against transient bit errors and helps maintain reliable memory operation.

CompTIA's Core 1 objectives include recognizing ECC as a RAM feature associated with error correction and reliability. For technical background, see Intel's ECC memory overview and IBM documentation on Error Correcting Code memory.

QUESTION NO: 64

A user reports that their desktop PC does not turn on. Which of the following components would most likely cause the issue?

A. PSU

B. GPU

C. RAM

D. CPU

ANSWER: A

Explanation:

PSU is the most likely component because it provides the DC power required by the motherboard, processor, memory, storage devices, cooling fans, and other internal hardware. If the power supply unit has failed, is not receiving AC power, has a switched-off rear rocker switch, or has a loose power connection, the desktop may show no signs of life when the user presses the power button. Typical symptoms include no power LEDs, no fan movement, no startup sounds, and no POST activity. A technician should first verify the external power source and cable, confirm that the PSU's input-voltage setting is correct when applicable, inspect internal power connectors, and test the PSU with an appropriate PSU tester or known-good replacement. The power supply's purpose and output characteristics are described in the Intel desktop power-supply guidance. CompTIA's Core 1 exam objectives include troubleshooting power-related hardware issues as part of hardware support skills; see the CompTIA exam objectives resource. Therefore, for a desktop that does not turn on, PSU is the best answer.

QUESTION NO: 65

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 directly improves the laptop's ability to keep more of the operating system, database application, query data, and file-system cache in memory. This reduces paging to the system drive when the user works with a large local database, which can substantially improve responsiveness during searches, sorting, reporting, and other memory-intensive operations. Windows also uses available physical memory to cache recently accessed disk data, helping repeated database reads complete more quickly. Microsoft describes how memory pressure and paging can affect system performance in its Windows performance troubleshooting guidance.

Migrating to a SSD improves storage performance for the database stored on drive C because solid-state storage provides much lower latency and faster random input/output operations than a mechanical hard disk. Database workloads commonly involve many small, nonsequential reads and writes, so faster random access can reduce the time required to retrieve records, load indexes, write temporary data, and handle paging if memory demand rises. Microsoft's Disk Management overview provides background on managing local storage devices and volumes. Together, additional memory and an SSD address the two key local bottlenecks most likely to affect this workload: memory capacity and drive access speed.

QUESTION NO: 66

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 Hypertext Transfer Protocol traffic is **80**. When a user enters a standard HTTP URL without specifying a port, such as `http://example.com`, the client connects to the web server using TCP port 80 by default. The default port for Hypertext Transfer Protocol Secure traffic is **443**. HTTPS protects web traffic by using TLS to provide encryption, server authentication, and integrity protection; browsers use TCP port 443 when an HTTPS URL does not explicitly include a port number, such as `https://example.com`. These well-known port assignments let clients and servers communicate predictably without users needing to append port information to ordinary web addresses. Port 80 and port 443 are core ports technicians should recognize when configuring web services, reviewing firewall rules, troubleshooting browser connectivity, or identifying traffic during network analysis. The Internet Assigned Numbers Authority service-name and port-number registry lists HTTP as assigned to port 80 and HTTPS as assigned to port 443. For additional context on HTTP's URI scheme and default port behavior, see RFC 9110 and the IANA Service Name and Port Number Registry.

QUESTION NO: 67

Which of the following are radio frequency connections? (Select two.)

A. Cable

B. Satellite

C. DSL

D. Cellular

E. Ethernet

F. Fiber

ANSWER: B D

Explanation:

Satellite and Cellular are radio frequency (RF) connection types because they carry information through electromagnetic radio waves transmitted wirelessly through the air. A satellite connection uses a ground-based dish or terminal to transmit and receive RF signals to and from an orbiting satellite. This enables connectivity in locations where terrestrial wired services may be impractical or unavailable, although latency can be significant depending on the satellite orbit. Cellular connectivity also relies on RF transmissions between a mobile device or cellular modem and nearby cell towers. Modern cellular services, including LTE and 5G, use licensed radio spectrum and cellular infrastructure to provide voice and data access over a wireless wide-area network. In the CompTIA A+ Core 1 networking objectives, recognizing the physical medium used by Internet connection types is important: both satellite and cellular are wireless WAN technologies based on radio transmission. The Federal Communications Commission provides an overview of satellite communications at https://www.fcc.gov/engineering-technology/satellite-communications, and its consumer guidance describes mobile wireless service as communication using radio frequencies at https://www.fcc.gov/consumers/guides/wireless-devices-and-health-concerns.

QUESTION NO: 68

A technician is preparing to recycle several retired laptops. Which of the following actions should the technician take to protect company data before the devices leave the facility? (Select TWO).

A. Remove the storage drives

B. Sanitize the storage drives

C. Update the BIOS

D. Defragment the storage drives

E. Clear the printer queue

ANSWER: A B

Explanation:

Remove the storage drives is correct because drives can contain operating system files, user profiles, browser data, credentials, and business documents. Removing the drives prevents the devices from leaving the facility with accessible local storage installed.

Sanitize the storage drives is also correct because data must be securely erased or otherwise rendered unrecoverable before drives are reused, transferred, or disposed of. The appropriate sanitization method depends on the storage technology, organizational policy, and intended disposition of the drive. NIST describes media sanitization methods and decision factors in NIST SP 800-88 Rev. 1.

QUESTION NO: 69

A technician needs to configure a static IPv4 address on a workstation. Which of the following settings must be configured for the workstation to communicate with devices on other networks? (Select TWO).

A. IP address

B. Default gateway

C. Workgroup name

D. Printer driver

E. MAC address

ANSWER: A B

Explanation:

An IP address is required because it uniquely identifies the workstation on its local IPv4 network. The address must be valid for the assigned subnet and must not duplicate another device's address.

A default gateway is also required for the workstation to send traffic to destinations outside of its local subnet. The default gateway is normally the IP address of the router interface on the workstation's local network. Without a gateway, the workstation can communicate with devices on the same subnet but cannot route traffic to remote networks. Microsoft provides TCP/IP addressing information at Microsoft Learn: TCP/IP addressing and subnetting.