www.atmicnetworks.com

ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

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

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

www.atmicnetworks.com

Question: 1

A technician is troubleshooting a connectivity issue on a network computer. The technician runs ipconfig in a command prompt and receives the following IP address:169.254.0.6. Which of the following is most likely the type of IP address being assigned?

A. DHCP reservation assignment

B. Dynamic assignment

C. Self-assignment

D. Static assignment

Answer: C

Explanation:

An IP address starting with169.254.x.xis aself-assigned address(also calledAPIPA– Automatic Private IP Addressing). It's used when a client device cannot contact a DHCP server. This address allows limited communication on the local network segment butno internet access.

Option A:DHCP reservations assign specific IPs from the DHCP server they don't result in APIPA.

Option B:Dynamic assignment from DHCP assigns valid IPs in the proper subnet, not 169.254.x.x.

Option D:Static IPs are manually set and would not fall in the 169.254.x.x range unless set incorrectly.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 2.6: Given a scenario, configure and troubleshoot network connectivity.

www.atmicnetworks.com

Question: 2

A recently installed printer is incorrectly aligning printed documents Which of the following should the technician do first to fix this issue?

A. Run the maintenance application.

B. Clean the rollers

C. Upgrade the firmware

D. Reinstall the drivers

Answer: A

Explanation:

A . Run the maintenance application:

Most modern printers include a built-in maintenance application that can calibrate the print heads and correct alignment issues. Running this tool is the first step to address misalignment.

Incorrect Options:

B . Clean the rollers: Cleaning rollers is typically done to resolve paper feed or jamming issues, not alignment problems.

C . Upgrade the firmware: While updating firmware is beneficial for performance improvements, it is not the first step for fixing alignment.

D . Reinstall the drivers: Misaligned printing is usually hardware-related, not a driver issue.

Key Takeaway: The maintenance application should be run first to resolve alignment issues in a newly

installed printer.

Reference: CompTIA A+ Core 1 Exam Objectives (220-1201), Domain 5.5 – Printer troubleshooting.

Question: 3

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 (Near-Field Communication)operates atvery short ranges usually less than 4cm, and is ideal for quick, secure transactions like contactless payments.Bluetoothsupportslonger ranges (up to 10 meters or 32 feet)and is suited for ongoing connections like wireless headsets or file transfers.

Option A:Bluetooth is faster for large file transfers.

Option B:NFC usesless power, not more.

Option C:NFC doesnotrequire pairing Bluetooth does.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 1.5: Given a scenario, connect and configure accessories and ports of mobile devices.

www.atmicnetworks.com

Question: 4

Which of the following is an advantage of using VDI?

A. Authentication is not required on a domain.

B. Licensing costs are minimized.

C. Less manual configuration is needed for each workstation.

D. A virus is automatically contained locally.

Answer: C

Explanation:

Virtual Desktop Infrastructure (VDI)hosts desktop environments on centralized servers.

Thisallowsrapid deployment and consistent configurationacross multiple users, minimizing manual setup and easing IT management.

Option A:VDI still uses standard authentication methods.

Option B:Licensing can actually be more expensive due to virtualization software and backend servers.

Option D:VDI centralizes the desktop environment viruses would affect the virtual session, not be "contained locally."

CompTIA A+ Core 1 Exam Objective Reference:

Objective 4.1: Compare and contrast cloud computing concepts.

www.atmicnetworks.com

Question: 5

A technician wants to monitor network statistics for devices communicating with one another on the local subnet Which of the following devices should the technician install.

A. Managed switch

B. Router

C. Access point

D. Firewall

Answer: A

Explanation:

A managed switch provides advanced features such as traffic monitoring and VLAN configuration, allowing a technician to view network statistics for devices on the local subnet.

Why Not B (Router): A router connects different networks and directs traffic between them but does not provide detailed subnet-level statistics.

Why Not C (Access point): Access points provide wireless connectivity but lack traffic monitoring features.

Why Not D (Firewall): A firewall filters traffic but is not used for monitoring detailed statistics on a local subnet.

CompTIA A+ Exam Reference: Core 1 (220-1201), Section 2.6, network monitoring tools.

www.atmicnetworks.com

Question: 6

Which of the following provides electricity to devices through network cables?

A. Edge router

B. PoE switch

C. Access point

D. Patch panel

Answer: B

Explanation:

A PoE (Power over Ethernet) switch transmits both data and electrical power over Ethernet cables to devices like wireless access points or VoIP phones. This is especially useful in areas where separate power sources are not available.

Reference: "CompTIA A+ Complete Study Guide" by Quentin Docter – Chapter 5, pages 319–321.

Question: 7

Which of the following DNS record types is used to direct email to a mail server?

A. CNAME

B. SRV

C. MX

D. SOA

Answer: C

Explanation:

An MX (Mail Exchange) record specifies the mail server responsible for receiving email for a domain.

Why Not A (CNAME): CNAME is used for domain aliasing, not for email delivery.

Why Not B (SRV): SRV records are used to locate specific services, not mail servers.

Why Not D (SOA): SOA records provide domain information but do not handle email.

CompTIA A+ Exam Reference: Core 1 (220-1201), Section 2.6, DNS record types.

Question: 8

Which of the following cloud models exclusively utilizes a local data center?

A. Private

B. Public

C. Hybrid

D. Community

www.atmicnetworks.com

Answer: A

Explanation:

APrivate Cloudis operated solely for a single organization. It ishosted on-premises or in a dedicated off-site data center, giving the company full control over data, security, and compliance often hosted in theorganization's own local data center.

Option B (Public):Hosted by third-party providers and shared by multiple clients.

Option C (Hybrid):Combines private and public cloud resources.

Option D (Community):Shared by several organizations with similar goals.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 4.1: Compare and contrast cloud computing concepts.

Question: 9

Which of the following types of RAM is typically used in servers?

A. SODIMM

B. Rambus

C. DDR3

D. ECC

www.atmicnetworks.com

Answer: D

Explanation:

ECC (Error-Correcting Code) RAM is commonly used in servers to provide error detection and correction, improving reliability in critical systems. It is designed to detect and correct single-bit errors, ensuring data integrity in environments where stability is paramount.

Option A (SODIMM): Incorrect. SODIMM is typically used in laptops, not servers.

Option B (Rambus): Incorrect. Rambus is an outdated RAM type and not commonly used today.

Option C (DDR3): Incorrect. While DDR3 is a type of RAM, it is not specific to servers and does not provide error correction.

Reference:

CompTIA A+ Core 1 Objectives: 3.2 (RAM types and their uses)

Question: 10

A user is unable to access secure applications on their tablet when working from home a couple days per week, but the applications work when in the office. Which of the following services most likely needs to be reconfigured to allow for remote work?

A. Global Positioning System

B. Mobile device management

C. Wi-Fi Protected Access

D. Near-field communication

www.atmicnetworks.com

Answer: B

Explanation:

Mobile Device Management (MDM)software often controls access to corporate resources based onlocation, network, or VPN status. If the MDM is not configured to allow access from outside the office or via home networks, the apps may be blocked. This is the most probable cause if apps work only on-premises.

Option A:GPS is used for location services, not access control.

Option C:WPA is a Wi-Fi security protocol, not related to access restrictions.

Option D:NFC enables close-range communication irrelevant to app access.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 1.6: Given a scenario, configure basic mobile device network connectivity and application support.

Question: 11

A user wants to print files from an overseas office using a shared network folder. The user's laptop has no public-facing internet connectivity. Which of the following can be used to print from the shared network folder?

A. ADF

B. USB

C. PCL

D. SMB

www.atmicnetworks.com

Answer: D

Explanation:

SMB (Server Message Block)is a protocol used to access files and printers over a network, including across shared network folders. It enables the user to access and print files stored remotely on a shared directory.

Option A (ADF):Automatic Document Feeder hardware, not a network protocol.

Option B (USB):Used for direct physical connections, not for printing over networks.

Option C (PCL):Printer Command Language relates to printer drivers, not file sharing or access.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 3.4: Given a scenario, install and configure printers.

Question: 12

An SAS RAID array has severely degraded and gone ofline 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

www.atmicnetworks.com

Answer: C,F

Explanation:

Clicking and grinding noises indicate mechanical drive failure.

SMART data provides insights into the health and status of drives, helping identify failing components in the RAID array.

Why Not A (Run a magnet): This would damage drives.

Why Not B (Check if one drive is not level): Physical leveling is irrelevant.

Why Not D (Check OS logs): OS logs may provide limited information for RAID arrays.

Why Not E (Update RAID controller firmware): While important, it does not diagnose drive failure.

CompTIA A+ Exam Reference: Core 1 (220-1201), Section 3.3, storage troubleshooting.

Question: 13

A user reports that a software application functioned as expected the previous day, but this morning, the user is unable to launch the application. Which of the following describe what the technician should do next?

A. Research the symptoms

B. Identify any changes the user has made

C. Determine which steps need to be performed.

D. Check the vendor's website for guidance.

www.atmicnetworks.com

Answer: B

Explanation:

Identifying changes made to the system is the next step to troubleshoot why an application no longer launches, as recent changes often cause such issues.

Why Not A (Research the symptoms): Research is broader and should come after identifying changes.

Why Not C (Determine which steps need to be performed): This comes after identifying the issue.

Why Not D (Check the vendor's website): This is a later step if further guidance is needed.

CompTIA A+ Exam Reference: Core 2 (220-1102), Section 3.1, troubleshooting methodology.

Question: 14

A user's wireless headset shows a "connected" status when turned on, but the Bluetooth list on the user's phone shows that the headset is "not connected." Which of the following should the technician do?

A. Enter the PIN.

B. Turn off Wi-Fi.

C. Re-pair the devices.

D. Enable Bluetooth.

Answer: C

Explanation:

When a device shows asnot connectedeven though it previously paired, the most effective action is tore-pair the devices. This resets the Bluetooth connection, clears any corruption in pairing profiles, and re-establishes communication.

Option A:Entering a PIN is only relevant during initial pairing and may not be prompted again.

Option B:Turning off Wi-Fi doesn't typically affect Bluetooth; they operate on similar frequencies but don't conflict this way in normal use.

Option D:If Bluetooth were disabled, the device wouldn't appear at all, not just show as "not connected."

CompTIA A+ Core 1 Exam Objective Reference:

Objective 1.5: Given a scenario, connect and configure accessories and ports of mobile devices.

Question: 15

Which of the following connectors can be used to charge most modern mobile devices and may have the capacity to send data audio and video?

A. Lightning

B. USB-C

C. MicroUSB

D. MiniUSB

Answer: B

Explanation:

www.atmicnetworks.com

B . USB-C:

USB-C is a versatile connector that supports charging, high-speed data transfer, and the ability to send audio and video signals (e.g., DisplayPort over USB-C).

It is used by most modern mobile devices and laptops because of its fast transfer speeds and power delivery capabilities.

Incorrect Options:

A . Lightning: Lightning is proprietary to Apple devices and does not natively support video output.

C . MicroUSB: MicroUSB is outdated and does not support video output.

D . MiniUSB: MiniUSB is an older standard and does not support modern features like video output or fast charging.

Key Takeaway: USB-C is the most versatile connector for charging and transferring data, audio, and video.

Reference: CompTIA A+ Core 1 Exam Objectives (220-1201), Domain 3.1 – Cable types and features.

Question: 16

Which of the following DNS records would an administrator change to redirect email flow?

A. MX

B. TXT

C. SPF

D. CNAME

Answer: A

Explanation:

AnMX (Mail Exchange)record defineswhich mail servers are responsible for receiving emailfor a domain. If you want to change or redirect email traffic, theMX recordmust be updated with the correct server information.

Option B (TXT):Stores text-based info used for SPF, DKIM, etc.

Option C (SPF):Part of email authentication stored in a TXT record; doesn't redirect traffic.

Option D (CNAME):Alias for another domain name not used for email routing.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 2.4: Compare and contrast common networking hardware.

Question: 17

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

A. Malfunctioning power supply
B. Damaged charge port
C. Deprecated battery
D. Broken screen

Answer: C

Explanation:

Abulging tablet casingis a classic sign of aswollen lithium-ion battery, often caused by age, overheating, or overcharging. This is adangerous condition, as swollen batteries can rupture or catch fire. It also explains why the tablet only works when plugged in the battery is no longer holding a charge.

Option A:Power supply issues wouldn't cause physical bulging.

Option B:A bad charge port wouldn't cause screen damage or physical distortion.

Option D:A broken screen could cause display issues, but not the bulging chassis.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 1.4: Given a scenario, configure settings and use cases for laptops and mobile devices.

Question: 18

A technician is replacing a failed power supply in a ten-year-old computer When installing the customer-provided power supply, the technician discovers the ATX connector would not plug into the motherboard. The customer wants a cost-effective solution. Which of the following should the technician do next?

A. Adjust the input voltage.

B. Install a modular power supply.

C. Rebuild the failed power supply.

D. Use a 20-pin to 24-pin adapter.

Answer: D

Explanation:

Older motherboards use 20-pin connectors, while newer power supplies use 24-pin connectors. An adapter resolves the compatibility issue cost-effectively.

Why Not A (Adjust the input voltage): Input voltage adjustment is unrelated to connector compatibility.

Why Not B (Install a modular power supply): While modular supplies are versatile, this doesn't address the connector issue directly.

www.atmicnetworks.com

Why Not C (Rebuild the failed power supply): Rebuilding is costly and complex compared to using an adapter.

CompTIA A+ Exam Reference: Core 1 (220-1201), Section 3.4, power supply compatibility.

Question: 19

A technician is troubleshooting a PoE phone that will not turn on. When a laptop is plugged directly into the switchport for the phone the technician sees a data link LED and activity. Which of the following tools should the technician use to verify PoE availability to the phone?

A. Network tap

B. Cable tester

C. Loopback plug

D. Toner probe

Answer: B

Explanation:

Reasoning: A cable tester capable of testing Power over Ethernet (PoE) functionality can verify whether the switchport is providing the required power to the phone. This tool measures both the presence of data and the voltage or wattage being provided through the Ethernet cable.

This is the most effective way to confirm that PoE is available on the port.

Why the Other Options Are Incorrect:

A . Network tap:

A network tap is primarily used to monitor network traffic, not to test for PoE availability. It cannot verify if power is being supplied through the Ethernet cable.

C . Loopback plug:

A loopback plug is used to test the functionality of a network port by creating a loop for transmitted and received signals. It does not measure or verify PoE availability.

D . Toner probe:

A toner probe is used for tracing and identifying network cables. It cannot test for PoE functionality.

Practical Example:

A PoE phone might not turn on due to a misconfigured or faulty switchport. Using a cable tester capable of measuring PoE would help the technician determine if the switchport is supplying sufficient power to the phone.

CompTIA A+ Exam Objective Alignment:

Objective 2.1: Identify common networking hardware and tools, including PoE-enabled devices and cable testers.

Question: 20

A technician has discovered that some users are connected to a network that is not available on the user interface. Which of the following is the most effective tool the technician can use to identify networks that are not broadcasting SSIDs?

A. Cable tester

B. Toner probe

C. Wi-Fi analyzer

D. Loopback plug

Answer: C

Explanation:

www.atmicnetworks.com

Comprehensive and Detailed Step-by-Step

Wi-Fi Analyzer:

A Wi-Fi analyzer is a tool used to detect and analyze wireless networks, even those that are not broadcasting their SSIDs (hidden networks).

It provides detailed information about nearby networks, including signal strength, channel usage, and security protocols.

In this case, the Wi-Fi analyzer can identify the hidden networks that users are connected to, which are not visible on the standard user interface.

Incorrect Options:

A . Cable tester: A cable tester is used to test the integrity of physical network cables. It does not detect wireless networks or SSIDs.

B . Toner probe: A toner probe is used to trace and identify cables within a wiring system. It is not applicable to wireless network analysis.

D . Loopback plug: A loopback plug is used to test the functionality of a network port or NIC. It is unrelated to identifying hidden wireless networks.

Key Takeaway:

The most effective tool for identifying hidden wireless networks is a Wi-Fi analyzer, as it can detect networks that are not broadcasting their SSIDs.

Reference: CompTIA A+ Core 1 Exam Objectives (220-1201), Domain 2.5 – Explain basic wired and wireless networking concepts, including Wi-Fi tools and protocols.

Question: 21

When installing a network printer, a technician needs to ensure the printer is available after a network is restarted. Which of the following should the technician set up on the printer to meet this requirement?

A. Static IP address

B. Private address

C. Wi-Fi on the printer

www.atmicnetworks.com

D. Dynamic addressing

Answer: A

Explanation:

Assigning astatic IP addressto a network printer ensures it always retains the same address, allowing users and print servers to consistently reach it even after a reboot or network refresh.

Option B (Private address):Refers to address ranges (e.g., 192.168.x.x) doesn't guarantee address persistence.

Option C (Wi-Fi):Is a connection method, not a method of IP assignment.

Option D (Dynamic addressing):Via DHCP, which can change over time unless reservations are made (less reliable).

CompTIA A+ Core 1 Exam Objective Reference:
Objective 3.4: Given a scenario, install and configure printers.

Question: 22

A user experiences a random BSOD while using a computer, but the operating system recovers as expected Which of the following symptoms would indicate the issue is related to RAM?

A. Wrong BIOS configurations

B. Continuous reboots

C. Distended capacitors

D. POST code beeps

www.atmicnetworks.com

Answer: D

Explanation:

E. POST Code Beeps:

During the Power-On Self-Test (POST), the BIOS performs checks on system hardware, including RAM. If the RAM is faulty, POST may produce a series of beep codes indicating memory issues.

These beep codes are often the first sign of RAM-related problems, especially if the BSOD occurs randomly.

Incorrect Options:

A . Wrong BIOS configurations: Incorrect BIOS settings may cause boot errors, but they are less likely to cause random BSODs.

B . Continuous reboots: Continuous reboots could result from multiple hardware or software issues but do not specifically point to RAM.

C . Distended capacitors: Faulty capacitors typically affect the motherboard, not the RAM.

Key Takeaway: POST beep codes are a common diagnostic tool for identifying RAM-related issues.

Reference: CompTIA A+ Core 1 Exam Objectives (220-1201), Domain 5.2 – Troubleshooting RAM and motherboard issues.

Question: 23

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:

If users canaccess local network resourcesbut not theinternet, the most likely culprit is amisconfigured or missing default gateway. The default gateway routes traffic from the local network to external networks (i.e., the internet). If it's not properly set or was altered during a firewall update, internet traffic won't be forwarded correctly.

Option A:Static IPs could cause conflict, but wouldn't affect only external access if configured correctly.

Option C:An incorrect subnet mask could isolate devices, but local communication would likely be impacted too.

Option D:VLANs segment networks; while misconfigured VLANs could cause access issues, they'd more likely isolate local traffic as well.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 2.6: Given a scenario, configure and troubleshoot network connectivity.

Question: 24

Which of the following cable types is the most suitable for delivering 10Gb speeds for distances over 328ft (100m) but under 1,312ft (400m)?

A. Multimode fiber

B. Single-mode fiber

C. Cat 6a

D. Cat 6

Answer: A

Explanation:

www.atmicnetworks.com

Comprehensive and Detailed Step-by-Step

When delivering 10Gbps speeds over long distances, fiber optic cables are the best choice. Here's the breakdown:

A . Multimode Fiber (Correct Answer):

Multimode fiber is designed for relatively short to medium distances (up to 1,312 feet or 400 meters) while supporting high-speed data transfer (10Gbps and above).

It uses LED light sources and is cost-effective for environments like data centers or within buildings.

For the specified distance of over 328ft but under 1,312ft, multimode fiber is the most suitable option.

Incorrect Options:

B . Single-mode Fiber: While single-mode fiber supports much greater distances (up to several miles or kilometers) and higher speeds, it is more expensive and unnecessary for the specified range.
Single-mode fiber is generally used for long-haul networking or telecommunications.

C . Cat 6a: Cat 6a is capable of 10Gbps speeds but only up to 328ft (100 meters). It cannot reliably handle the specified distance of over 328ft.

D . Cat 6: Cat 6 is also limited to 10Gbps speeds at distances up to 328ft (100 meters). Beyond this range, it is unsuitable.

Key Takeaway:

For delivering 10Gbps speeds over distances longer than 328ft (100m) but under 1,312ft (400m), Multimode Fiber is the best choice due to its ability to support high-speed data over medium distances at a reasonable cost.

Reference: CompTIA A+ Core 1 Exam Objectives (220-1201), Domain 3.1 – Cable types and their characteristics, including fiber optic cables.

Question: 25

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:

The system date/time is maintained by the CMOS battery when the PC is powered off. If this battery fails, time resets will occur. Additionally, since the system is connected to a UPS, ensuring the UPS is functioning correctly (i.e., the backup power source) is essential.

Reference: "CompTIA A+ Complete Study Guide" by Quentin Docter – Chapter 1, page 40.

Question: 26

A technician receives a S.M.A.R.T. error on a PC. When the technician presses the Esc key, the PC continues to turn on without any further issues. Which of the following should the technician do next?

A. Replace the HDD.

B. Update the PC's BIOS.

C. Close the ticket.

D. Change the NIC.

Answer: A

Explanation:

Comprehensive and Detailed Step-by-Step

S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology):

S.M.A.R.T. is a monitoring system integrated into modern HDDs and SSDs that detects and reports on various indicators of drive health and reliability.

A S.M.A.R.T. error indicates that the drive is showing signs of impending failure, even if the PC continues to boot and work normally for the time being.

Next Steps:

The appropriate action is to replace the hard drive (HDD) because a S.M.A.R.T. error is an early warning of possible hardware failure. Ignoring the warning could result in data loss if the drive fails completely.

The technician should also back up the user's data immediately to avoid losing critical information.

Incorrect Options:

B . Update the PC's BIOS: While keeping the BIOS updated is a good practice, it does not address the S.M.A.R.T. error, which is specific to the HDD.

C . Close the ticket: Closing the ticket without resolving the issue would be improper, as the S.M.A.R.T. error is a hardware problem that needs to be addressed to prevent future data loss or downtime.

D . Change the NIC: The NIC (Network Interface Card) is unrelated to the storage system and would not resolve a S.M.A.R.T. error.

Key Takeaway:

A S.M.A.R.T. error is a critical indicator of HDD health issues, and the drive should be replaced as soon as possible. Backing up data is also essential.

Reference: CompTIA A+ Core 1 Exam Objectives (220-1201), Domain 5.1 – Troubleshooting hard drives and RAID arrays.

Question: 27

A company deploys server machines in a public cloud. Which of the following cloud service models is this an example of?

A. Platform as a service

B. Anything as a service

C. Infrastructure as a service

D. Software as a service

Answer: C

Explanation:

Infrastructure as a Service (IaaS) provides virtualized computing resources over the internet. This includes virtual servers, storage, and networking. Deploying server machines falls under IaaS since the organization is responsible for managing the OS and applications on top of the infrastructure.

Reference: "CompTIA A+ Complete Study Guide" by Quentin Docter – Chapter 8, "Virtualization and Cloud Computing", page 488-490. Also found in the220-1201objectives, section 4.1.

Question: 28

Which of the following drive interfaces is typically used in server systems but not in home computers?

A. NVMe

B. SAS

C. SATA

www.atmicnetworks.com

D. PCIe

Answer: B

Explanation:

SAS (Serial Attached SCSI) is a high-performance drive interface commonly found in enterprise environments and servers due to its reliability and speed. While SATA is more common in consumer systems, SAS is specifically designed for mission-critical applications, offering features like full-duplex operation and compatibility with SATA drives.

Reference: "CompTIA A+ Certification All-in-One Exam Guide" by Mike Meyers – Chapter 8, "Mass Storage Technologies", page 288.

Question: 29

A technician is installing a new high-end graphics card that uses a 12VHPWR connector. Which of the following is the maximum wattage supported by this power connector?

A. 400W

B. MOW

C. 600W

D. 700W

Answer: C

Explanation:

The 12VHPWR connector can supply up to 600 watts of power, designed for high-end graphics cards.

Why Not A (400W): This is less than the connector's maximum capability.

www.atmicnetworks.com

Why Not B (MOW): This is an invalid option.

Why Not D (700W): The maximum supported power is 600W.

CompTIA A+ Exam Reference: Core 1 (220-1201), Section 3.4, power supply and connectors.

Question: 30

Which of the following tools would a technician use to connect wires to an RJ45 connector?

A. Crimper

B. Cable stripper

C. Punchdown

D. Loopback plug

Answer: A

Explanation:

A crimper is specifically used to attach RJ45 connectors to the ends of network cables. It pressesthe connector pins into the cable's wires, establishing a secure electrical connection. A punchdown tool is used for wiring patch panels or keystone jacks, not for attaching connectors.

Reference: "CompTIA A+ Complete Study Guide" by Quentin Docter – Chapter 3, "Cables and Connectors", page 162. Also outlined in the220-1201objectives under 3.1.

Question: 31

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:

Outdated drivers: Device functionality issues after an OS upgrade are often caused by incompatible or outdated drivers.

Disabled settings: Some features may be disabled during the upgrade process, requiring reenablement.

Why Not A (Incorrect configuration): This is unlikely given the issues arose only after the upgrade.

Why Not B (OS and device incompatibility): Upgrades check for compatibility before installation.

Why Not D (Full storage): Storage issues typically prevent installation, not device functionality.

Why Not F (Corrupted registry entries): While possible, this is less common than the selected answers.

CompTIA A+ Exam Reference: Core 1 (220-1201), Section 3.5, troubleshooting OS upgrades.

Question: 32

A management team is concerned about enterprise devices that do not have any controls in place. Which of the following should an administrator implement to address this concern?

A. MDM

B. MFA

www.atmicnetworks.com

C. vpn

D. SSL

Answer: A

Explanation:

Mobile Device Management (MDM) enables administrators to enforce controls on enterprise devices, such as restricting apps, ensuring compliance, and remotely managing security policies.

Why Not B (MFA): Multi-Factor Authentication secures user access but does not control device configurations.

Why Not C (VPN): VPN secures communication but does not enforce device controls.

Why Not D (SSL): SSL secures data in transit but does not provide device management.

CompTIA A+ Exam Reference: Core 2 (220-1102), Section 2.7, device management concepts.

Question: 33

A user returns from a trip and discovers a computer that is connected to the LAN times out intermittently Upon investigation, a technician finds the RJ45 pin is not property terminated Which of the following networking tools is most appropriate to fix the issue?

A. Toner probe

B. Cable tester

C. Punchdown

D. Crimper

www.atmicnetworks.com

Answer: D

Explanation:

E. Crimper:

A crimper is used to terminate an RJ45 cable properly by attaching the connector to the twisted-pair wires.

If the termination is not done correctly, the connection will be intermittent or fail entirely.

Incorrect Options:

A . Toner probe: Used to locate cables or trace their path, not for terminating RJ45 connectors.

B . Cable tester: Useful for testing connectivity but does not fix termination issues.

C . Punchdown: Used to connect wires to a patch panel or keystone jack, not for RJ45 connectors.

Key Takeaway: A crimper is the proper tool for fixing an improperly terminated RJ45 connection.

Reference: CompTIA A+ Core 1 Exam Objectives (220-1201), Domain 2.8 – Using appropriate tools for network troubleshooting.

Question: 34

A technician is putting RJ45 connectors on Cat 6 cables. Which of the following tools should the technician use to secure the connectors?

A. Loopback plug

B. Wire cutters

C. Punchdown

D. Crimping

Answer: D

Explanation:

Question: 35

A user joins a conference call with a Bluetooth headset. Which of the following has the user created?

A. MAN

B. PAN

C. SAN

D. WAN

Answer: B

Explanation:

B . PAN (Personal Area Network):

A PAN is a network established between devices in close proximity, such as between a smartphone and a Bluetooth headset.

Bluetooth technology is specifically designed for short-range communication, making it a type of PAN.

Incorrect Options:

A . MAN (Metropolitan Area Network): A MAN covers a city or metropolitan area and is not relevant to Bluetooth connections.

C . SAN (Storage Area Network): A SAN is used for large-scale data storage, unrelated to Bluetooth connections.

D . WAN (Wide Area Network): A WAN spans large geographical areas (e.g., the internet) and is not relevant to this scenario.

Key Takeaway: Bluetooth connections, such as those between a headset and a device, create a Personal Area Network (PAN).

Reference: CompTIA A+ Core 1 Exam Objectives (220-1201), Domain 2.1 – Network types and their features.

Question: 36

A computer displays an error message indicating there is insufficient storage when installing applications. The user reports slow application load times. Which of the following replacement components would best resolve this issue?

A. SSD

B. USB

C. HDD

D. RAM

Answer: A

Explanation:

Upgrading to asolid-state drive (SSD)providesmore storage spaceandfaster read/write speeds, which resolves both the "insufficient storage" error and slow application loads.

Option B (USB):Not intended for permanent application storage or performance improvements.

Option C (HDD):Could solve storage capacity but would not improve speed.

Option D (RAM):Affects multitasking and memory-intensive tasks, not storage capacity directly.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 3.5: Given a scenario, troubleshoot problems related to storage devices.

Question: 37

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

A. Malfunctioning power supply

B. Damaged charge port

C. Swollen battery

D. Broken screen

Answer: C

Explanation:

The most likely cause is a swollen battery, which occurs when the battery's internal components break down, causing a buildup of gas. This results in:

Physical Symptoms: The battery bulges, pushing the screen away.

Operational Symptoms: The device may still power on when connected to a charger but fails to hold a charge due to battery degradation.

Option A (Malfunctioning power supply): Incorrect. Power supply issues affect charging but do not cause physical bulging.

Option B (Damaged charge port): Incorrect. A damaged port can prevent charging but does not explain the bulge.

Option D (Broken screen): Incorrect. A damaged screen does not cause the device to bulge; it is likely a secondary effect of the swollen battery.

Safety Note: A swollen battery poses a risk of fire or explosion and should be replaced immediately following proper disposal procedures.

Reference:

Question: 38

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:

If a desktopfails to power on entirely, the most probable cause is afaulty Power Supply Unit (PSU). If there are no lights, fans, or POST beeps, the PSU may have failed, cutting off all power to the motherboard and components.

Option B (GPU):Could prevent video output, but the system would still power on and beep.

Option C (RAM):Missing or faulty RAM would cause POST errors but not prevent startup entirely.

Option D (CPU):A bad CPU may cause POST failure, but the system would usually at least power on.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 3.5: Given a scenario, troubleshoot problems related to motherboards, RAM, CPU, and power.

Question: 39

A technician is troubleshooting an all-in-one laser printer that prints a vertical line when making copies and scans. When users print or receive faxes, the output from the printer is correct. Which of the following should the technician examine to determine the cause of the issue?

A. The pickup rollers

B. The corona wire

C. The document feeder

D. The drum assembly

Answer: C

Explanation:

Since the issue only occurs during scanning and copying (not printing or faxing), the problem is isolated to the document feeder. A vertical line is typically caused by debris or damage on theglass under the ADF (Automatic Document Feeder), not on components related to printing.

Reference: "CompTIA A+ Complete Study Guide" by Quentin Docter – Chapter 4, page 261.

Question: 40

A customer reports slow network speeds. Which of the following components is most likely failing?

A. CPU

B. NIC

C. HDD

D. RAM

Answer: B

Explanation:

ANetwork Interface Card (NIC)is the hardware responsible for network connectivity. If the NIC is failing or underperforming (e.g., due to a bad driver, hardware fault, or misconfiguration), it can causeslow or unstable network speeds.

Option A (CPU):A failing CPU affects overall system performance but not specifically network speed.

Option C (HDD):A slow hard drive causes application lag, but not poor network performance.

Option D (RAM):Affects multitasking and speed, not network throughput.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 3.5: Given a scenario, troubleshoot problems related to wired and wireless networks.

Question: 41

Which of the following should a technician use to terminate a Cat 6 cable to a patch panel?

A. Punchdown tool

B. Crimper

C. Toner probe

D. Network tap

Answer: A

Explanation:

A punchdown tool is specifically used to insert wires into a punchdown block in patch panels, which is typical for Cat 6

www.atmicnetworks.com

and similar cabling. It ensures a secure and correct connection by pushing the wire into a metal groove that slices the insulation.

Reference: "CompTIA A+ Certification All-in-One Exam Guide" by Mike Meyers – Chapter 18, page 758.

Question: 42

A help desk technician inspects a laptop keyboard because a single key has stopped working. The technician checks the keyboard for debris. Which of the following actions should the technician do next to troubleshoot the issue cost-effectively?

A. Replace the keyboard.

B. Replace the key switch

C. Replace the circuit board.

D. Replace the keycap

Answer: B

Explanation:

If only one key is not functioning and debris has been checked, replacing the individual keycap is the most cost-effective next step. It's a simple, low-cost option before considering more extensive repairs like replacing the entire keyboard.

Reference: "CompTIA A+ Complete Practice Tests" by Jeff T. Parker – Chapter 1, Question 10, page 8.

Question: 43

A technician is troubleshooting issues occurring on a user's mobile device. Applications and the OS have slow response times, even when performing simple tasks, such as writing an email.

Additionally, new applications occasionally fail to launch. Which of the following should the technician do next?

A. Move the device to a room with a colder temperature.

B. Close unnecessary programs.

C. Reset to factory default settings.

D. Check the battery health of the device.

Answer: B

Explanation:

The symptoms slow response and failed app launches indicate that thedevice's memory or processing resources are overutilized. Closing unnecessary apps can free up RAM and CPU resources, improving performance.

Option A:Overheating may cause sluggishness, but that's not indicated here.

Option C:Factory reset is a last resort, not the next logical step.

Option D:Battery health would affect uptime, not system speed.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 1.6: Given a scenario, configure basic mobile device network connectivity and application support.

Question: 44

A customer reports their tablet was recently dropped on the ground. The tablet has a small crack in one corner of the display, and it does not charge when plugged in. Which of the following should a technician do first?

A. Perform a hard restart.

B. Replace the battery

C. Inspect the USB-C port for damage

D. Run diagnostics on the digitizer

Answer: C

Explanation:

Physical damage from dropping a tablet may often affect ports or connectors. Before taking deeper diagnostic or replacement steps, it's important to visually inspect the USB-C charging port for damage or debris. If the port is damaged, charging issues can occur regardless of battery health.

Reference: "CompTIA A+ All-in-One Exam Guide, 11th Edition" by Mike Meyers – Chapter 25, "Maintaining and Securing Mobile Devices", page 879.

Question: 45

A user prints a job from a laser printer. The user wipes the page, and the words and images come off of it. The technician replaces the toner cartridge, but the issue persists. Which of the following components should the technician replace next?

A. Fuser

B. Drum

C. Developer roller

D. Discharge lamp

Answer: A

Explanation:

Inlaser printers, thefuser unitis responsible formelting the toner onto the paperusing heat and pressure. If the toner rubs off easily, it's a clear sign thefuser is failing or not heating properly. Replacing the fuser will ensure the toner bonds correctly to the paper.

Option B (Drum):Transfers the image, but doesn't fuse the toner.

Option C (Developer roller):Applies toner to the drum wouldn't cause toner to rub off.

Option D (Discharge lamp):Prepares the drum for a new image; not related to toner adhesion.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 3.7: Given a scenario, troubleshoot common printer problems.

Question: 46

Which of the following tools is best to track where an Ethernet cable is patched?

A. Crimper

B. Punchdown tool

C. Cable stripper

D. Toner probe

Answer: D

Explanation:

Atoner probe(also known as a tone generator and probe) is the best tool fortracing and identifying cablesin a patch panel or wall jack. The tone generator sends a signal through the wire, and the probe helps locate the cable by detecting the tone.

Option A (Crimper):Used to attach connectors (e.g., RJ-45), not for tracing cables.

Option B (Punchdown tool):Used to terminate cables into patch panels or keystone jacks.

Option C (Cable stripper):Used to remove insulation, not to trace cables.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 5.1: Identify basic cable types, their connectors, and their features.

www.atmicnetworks.com

Question: 47

A small company wants the ability to print in full color but needs to pay a minimal initial purchase price for the printer Which of the following is the best option?

A. Thermal printer

B. Inkjet printer

C. Dot matrix printer

D. Laser printer

Answer: B

Explanation:

Inkjet printers are the best choice for a small company seeking full-color printing with a minimal initial cost. While they have higher operating costs (due to ink), they are affordable and capable of high-quality color output.

Why Not A (Thermal printer): Thermal printers are not designed for color printing and are typically used for labels or receipts.

Why Not C (Dot matrix printer): Dot matrix printers are outdated, noisy, and do not support full-color printing.

Why Not D (Laser printer): Laser printers have lower running costs but a higher initial purchase price, especially for color models.

CompTIA A+ Exam Reference: Core 2 (220-1102), Section 4.6, printer types.

Question: 48

A company wants to save printing costs by restricting network printer use. The company implements a solution that requires employees to authenticate to the printer to release print jobs Which of the following has the company implemented?

www.atmicnetworks.com

A. Access control list

B. Audit logging

C. Badging

D. Print server

Answer: C

Explanation:

Badging is a form of authentication that requires employees to use a badge or ID card to release print jobs. This solution reduces unnecessary printing by ensuring only authorized users print.

Why Not A (Access control list): While ACLs manage permissions, they are not used for physical authentication at printers.

Why Not B (Audit logging): Audit logs track actions but do not restrict printer access.

Why Not D (Print server): A print server manages print jobs but doesn't enforce authentication.

CompTIA A+ Exam Reference: Core 2 (220-1102), Section 2.5, authentication mechanisms.

Question: 49

A user reported performance issues on a computer after a recent OS update A technician is confident that rolling back the system will resolve the issue. Which of the following steps should the technician take next?

A. Document the findings.

B. Investigate any recent infrastructure changes.

C. Initiate the system restore

D. Verify full system functionality.

www.atmicnetworks.com

Answer: C

Explanation:

C . Initiate the system restore:

If the technician is confident that rolling back the system to a previous restore point will resolve the issue, the next logical step is to initiate the System Restore process.

System Restore allows the system to revert to a state before the OS update, which can eliminate the performance issues caused by the update.

Incorrect Options:

A . Document the findings: Documentation is important but should occur after resolving the issue.

B . Investigate any recent infrastructure changes: This is unnecessary if the issue is already attributed to the OS update.

D . Verify full system functionality: This step should be performed after the System Restore is completed.

Key Takeaway: When confident that rolling back will resolve the issue, the technician should proceed with initiating a System Restore to revert the OS.

Reference: CompTIA A+ Core 1 Exam Objectives (220-1201), Domain 5.4 – Troubleshooting OS problems.

Question: 50

A computer is experiencing random shutdowns. A technician notices that the fans on the computer work but are noisy. The CPU temperature is about 122°F (50°C) when the computer is started but rises to 208°F (98°C) when applications are opened. Which of the following would most likely fix this issue?

A. Replacing the power supply

B. Installing a high-performance heat sink

C. Adjusting the fan settings

D. Adding more RAM to the computer

www.atmicnetworks.com

Answer: B

Explanation:

Excessive heat buildup due to insufficient cooling is a primary cause of unexpected shutdowns. A high-performance heat sink improves thermal transfer, dissipates more heat, and helps maintain CPU temperature within safe limits. When CPU temperatures reach levels like 208°F (98°C), the system may shut down to prevent damage.

Reference: "CompTIA A+ Complete Study Guide" by Quentin Docter – Chapter 1, pages 68–71, discusses CPU cooling and heat sink improvements.

Question: 51

Several storms cause mission-critical servers to go ofline unexpectedly A server also goes ofline suddenly due to haroNvare failure Upon assessment the company purchases new UPSs to condition power and allow the OSs to shut down gracefully in the event of a power failure However, the UPSs are delayed due to supply chain issues Which of the following can balance a cost-effective solution with uptime requirements?

A. Purchasing backup generators

B. Increasing input voltage

C. Installing redundant PSUs

D. Activating a hot site

Answer: C

Explanation:

C . Installing redundant PSUs (Power Supply Units):
Redundant PSUs provide fault tolerance by ensuring that if one power supply fails, another will take over seamlessly.

This is a cost-effective way to increase uptime while waiting for the UPSs to arrive.

Incorrect Options:

A . Purchasing backup generators: Generators are costly and are typically used for long-term outages, not as an immediate or cost-effective solution.

B . Increasing input voltage: This is not a practical solution to hardware failures or power issues.

D . Activating a hot site: A hot site is an expensive, fully operational backup facility that would not be a cost-effective solution for this scenario.

Key Takeaway: Installing redundant PSUs is a cost-effective way to balance uptime requirements in case of power or hardware failure.

Reference: CompTIA A+ Core 1 Exam Objectives (220-1201), Domain 5.3 – Power-related troubleshooting.

Question: 52

A customer reports that a text-only document prints with unrecognizable characters. The print preview correctly displays the document. Which of the following is the most likely cause of the issue?

A. Outdated firmware

B. Incorrect driver

C. Bad toner cartridge

D. Corrupted document file

Answer: B

Explanation:

Question: 53

Which of the following best represents the purpose of NFC?

A. Wired connections between several devices

B. Short-distance wireless connections between two devices

C. Wireless connections between multiple devices at once

D. Direct connection of two computers for file sharing

Answer: B

Explanation:

NFC (Near-Field Communication) is a subset of RFID technology designed for very short-range wireless communication, typically within a few centimeters. It is primarily used for contactless transactions, like mobile payments, and can also support peer-to-peer data exchanges. NFC operates at 13.56 MHz and enables devices to communicate when placed near each other.

Reference: "CompTIA A+ Complete Study Guide" by Quentin Docter – Chapter 7, "Wireless and SOHO Networks", page 400.

Question: 54

A company uses vital legacy software that does not run in the current OS version Which of the following will best support the software while keeping the OS current?

A. Shared resources

B. System sandbox

C. Test development

D. Application visualization

Answer: D

Explanation:

Application virtualization allows legacy software to run in a virtualized environment while the operating system remains current. It isolates the application from the OS, ensuring compatibility without downgrading the OS.

Why Not A (Shared resources): This relates to resource sharing, not application compatibility.

Why Not B (System sandbox): Sandboxes isolate applications for security testing, not compatibility.

Why Not C (Test development): Test environments are used for development, not running legacy applications.

CompTIA A+ Exam Reference: Core 1 (220-1201), Section 4.2, virtualization concepts.

Question: 55

While reviewing options in the BIOS/UEFI settings page to fix a laptop issue, a support technician notices an option to clear existing TPM keys. Which of the following would most likely happen if the TPM is cleared?

A. Encrypted hard drives would probably not be accessible.
B. All security certificates would need to be reinstalled from trusted roots.
C. The device would need to be reenrolled in the MDM platform
D. The laptop would need to be registered to the domain as a new client.

Answer: A

Explanation:

The Trusted Platform Module (TPM) is a hardware-based security feature used to store cryptographic keys, such as those used for encryption, authentication, or device identification. It plays a critical role in ensuring secure operations for encrypted drives, BitLocker, and secure boot processes. Clearing TPM keys involves wiping all stored cryptographic data, which can lead to several consequences depending on what the TPM was being used for. Let's break it down:

Correct Answer: A. Encrypted hard drives would probably not be accessible.

Explanation:

Encrypted hard drives, such as those secured with BitLocker encryption, rely on the cryptographic keys stored in the

www.atmicnetworks.com

TPM to unlock data.

Clearing the TPM will erase these keys, making it impossible for the encrypted drive to decrypt its contents unless a recovery key (separate from the TPM) is available. Without this recovery key, the data will likely become inaccessible.

CompTIA A+ Core 1 Exam Objective Reference: This falls under Objective 3.5, which covers understanding BIOS/UEFI configurations, TPM functions, and securing devices.

Why the Other Options Are Incorrect:

B . All security certificates would need to be reinstalled from trusted roots.

Clearing the TPM does not erase security certificates stored in the operating system or other areas. Certificates are generally managed by the OS or specific applications, not the TPM.Clearing the TPM only affects cryptographic keys and data stored in the TPM chip, so this is incorrect.

C . The device would need to be reenrolled in the MDM platform.

Mobile Device Management (MDM) enrollment typically does not rely on the TPM. While certain enterprise security configurations may involve the TPM, clearing it does not inherently trigger MDM reenrollment unless specifically tied to the MDM configuration.

D . The laptop would need to be registered to the domain as a new client.

While domain registrations may sometimes use TPM for authentication or secure operations,

clearing the TPM alone does not require re-registering the device to the domain. The domain registration and authentication process rely more on system-level credentials than the TPM itself.

Practical Example:

A user enables BitLocker on their laptop, which relies on the TPM to store the encryption key. Later, if they clear the TPM via BIOS/UEFI without saving the BitLocker recovery key separately, they will not be able to unlock the hard drive, leading to data loss unless the recovery key is available. This is a common issue when technicians or users inadvertently clear the TPM without understanding its role in encryption.

CompTIA A+ Exam Objective Alignment:

Objective 3.5: Given a scenario, install and configure laptop hardware and components, including UEFI/BIOS security settings (TPM, secure boot, etc.).

This question tests understanding of TPM functionality, encryption technologies, and secure device configurations.

www.atmicnetworks.com

Question: 56

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:

Amodular power supplyallows a technician toconnect only the power cables that are needed, reducing clutter and improving airflow. This is ideal when aiming for a clean build withminimal visible internal cables.

Option A (SATA drive connections):Still require both power and data cables, adding to cable count.

Option B (Liquid cooling):May reduce some bulk from large air coolers, but adds tubing and still needs cabling.

Option D (Wireless NIC):Adds wireless capability but has no relation to internal cabling cleanliness.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 3.3: Given a scenario, apply the appropriate PC configuration.

Question: 57

Which of the following display characteristics would be most important to ensure screen images appear the same as printed output?

A. Color gamut

B. Pixel density

C. Refresh rate

D. Resolution

Answer: A

Explanation:

Color gamut refers to the range of colors a display can accurately reproduce. For tasks like graphic design or photo editing, ensuring the screen's colors match the printed output is critical. Monitors with wide and accurate color gamuts (e.g., Adobe RGB) are preferred for these applications.

Option B (Pixel density): Incorrect. Pixel density affects image sharpness, not color accuracy.

Option C (Refresh rate): Incorrect. Refresh rate impacts motion smoothness but is unrelated to color matching.

Option D (Resolution): Incorrect. Resolution determines clarity and detail but does not influence color accuracy.

Reference:

CompTIA A+ Core 1 Objectives: 1.2 (Display types and characteristics)

Question: 58

Which of the following cable types can be used to transfer data and video?

A. USB-C

B. HDMI

C. DisplayPort

D. VGA

Answer: A

Explanation:

USB-Cis a versatile connector capable oftransmitting data, video, audio, and power. With standards likeDisplayPort over USB-C or Thunderbolt 3/4, it can be used for external displays, file transfers, charging, and more all through one cable.

Option B (HDMI):Supports video and audio but not general data transfer.

Option C (DisplayPort):Similar to HDMI supports video/audio but not general file transfer.

Option D (VGA):Legacy analog video only no data or audio support.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 3.1: Identify common connector types.

Question: 59

A human resources department uses a network shared with other departments to produce a variety of printed resources for legal retention. The human resources department only wants Its members to have access to these materials. Which of the following should the technician Implement?

A. Security groups

B. Audit logs

C. Time-of-day access

D. Print server

Answer: A

Explanation:

Security groups are used to manage access permissions to network resources, ensuring only authorized HR department members can access the shared materials.

Why Not B (Audit logs): Audit logs monitor activity but do not restrict access.

Why Not C (Time-of-day access): Time-of-day access limits when users can access resources but doesn't specify user permissions.

Why Not D (Print server): A print server manages print jobs but does not control file access.

CompTIA A+ Exam Reference: Core 2 (220-1102), Section 2.5, access control and permissions.

Question: 60

Users are complaining that the audio from a presenter is choppy and unintelligible Which of the following is causing the issue?

A. Webcam

B. Digitizer

C. inverter

D. Microphone

Answer: D

Explanation:

Choppy or unintelligible audio is typically caused by issues with the microphone, such as poor quality, hardware defects, or misconfiguration.

Why Not A (Webcam): The webcam handles video, not audio.

Why Not B (Digitizer): A digitizer relates to touchscreens, not audio.

Why Not C (Inverter): Inverters manage power for displays, not audio.

www.atmicnetworks.com

CompTIA A+ Exam Reference: Core 1 (220-1201), Section 3.6, audio troubleshooting.

Question: 61

A user connects their laptop to a projector in a conference room. Once connected, the userreports the screen is smaller at the bottom than at the top. The user tries restarting the laptop and then disconnecting and reconnecting the cable to the projector. Which of the following should a technician do to resolve the issue?

A. Replace the HDMI cable.

B. Power cycle the projector.

C. Adjust the keystone

D. Increase the resolution.

Answer: C

Explanation:

A distorted image where the screen is not symmetrical (wider at the top or bottom) is typically due to keystone distortion. Adjusting the projector's keystone settings corrects this trapezoidal effect caused by an angled projection.

Reference: "CompTIA A+ Complete Study Guide" by Quentin Docter – Chapter 3, page 152.

Question: 62

Which of the following could a user employ to maximize module bandwidth when selecting memory for a high-end gaming computer?

A. Error correction

B. RAM voltage

www.atmicnetworks.com

C. Channel configuration

D. Physical module size

Answer: C

Explanation:

Channel configuration(e.g.,dual-channel,quad-channel) determines how memory modules communicate with the memory controller. Usingmatched pairs in dual- or quad-channel setupscan significantlyincrease memory bandwidth, improving performance especially for gaming and videointensive tasks.

Option A (Error correction):ECC RAM is used in servers for reliability, not performance or gaming.

Option B (RAM voltage):Affects compatibility and overclocking but not bandwidth.

Option D (Physical size):Refers to module form factor (e.g., DIMM, SO-DIMM) and does not impact bandwidth.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 3.2: Given a scenario, install RAM types.

Question: 63

Which of the following is used primarily for archiving data?

A. PAN

B. MAN

C. SAN

D. LAN

E. WAN

Answer: C

Explanation:

A Storage Area Network (SAN) is primarily used for data archiving and large-scale storage. SANs provide high-speed, block-level storage for enterprise environments.

Why Not A (PAN): Personal Area Networks are for connecting personal devices like phones and smartwatches.

Why Not B (MAN): Metropolitan Area Networks are for city-wide data communication, not storage.

Why Not D (LAN): Local Area Networks are for general connectivity, not dedicated storage.

Why Not WAN: Wide Area Networks are for connecting geographically dispersed networks, not storage.

CompTIA A+ Exam Reference: Core 1 (220-1201), Section 2.7, network types and purposes.

Question: 64

A user prints a spreadsheet in duplex mode. The spreadsheet is difficult to read because some of the columns spill onto the second side of the page. Which of the following should the user do to prevent the issue but still print on both sides of the page?

A. Turn off duplex printing.

B. Try a smaller font size in the spreadsheet.

C. Change the page orientation.

D. Use a different print driver.

Answer: C

Explanation:

Changing the page orientation(e.g., fromportrait to landscape) allows wider columns to fit on one side of the page. This maintains readability while continuing to use duplex printing.

Option A:Disabling duplex defeats the goal of printing on both sides.

Option B:May help, but could make the document harder to read if the font is too small.

Option D:Unlikely to resolve formatting issues related to layout and dimensions.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 3.7: Given a scenario, troubleshoot common printer problems.

Question: 65

A customer needs to install a new printer in their network. The customer reports that users had intermittent connectivity issues with previous printers. Which of the following should the technician configure on the new printer to prevent this issue?

A. Gateway IP address
B. DHCP IP address
C. Static IP address
D. Public IP address

Answer: C

Explanation:

Intermittent connectivity issues with network printers are commonly caused by changing IP addresses when using DHCP. Assigning a static IP address ensures that the printer is always reachable at the same IP address by client machines.

Reference: "CompTIA A+ Complete Study Guide" by Quentin Docter – Chapter 4, "Printers and Multifunction Devices", page 241.

www.atmicnetworks.com

Question: 66

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:

Comprehensive and Detailed Step-by-Step

To answer this question, we need to identify the port numbers associated with email protocols used in client-server communication.

Port 25 (SMTP - Simple Mail Transfer Protocol):

This port is primarily used for sending emails between mail servers and from mail clients to mail servers (sending outbound mail).

SMTP is an essential protocol for email traffic.

Reference: CompTIA A+ Core 1 Exam Objectives (220-1201), Domain 2.5 – Explain basic wired and wireless networking concepts, including ports and protocols.

Port 110 (POP3 - Post Office Protocol v3):

POP3 is used for retrieving emails from a mail server. It is commonly used for downloading email messages to a local client, after which the messages are deleted from the server.

www.atmicnetworks.com

While not as commonly used today (due to IMAP being preferred), POP3 is still a recognized email protocol, and its association with port 110 makes it a valid answer.

Reference: CompTIA A+ Core 1 Exam Objectives (220-1201), Domain 2.5 – Explain basic wired and wireless networking concepts, including ports and protocols.

Incorrect Options:

A . Port 23: This is the Telnet protocol used for remote terminal access. It is not related to email traffic.

C . Port 67: This port is associated with the DHCP (Dynamic Host Configuration Protocol) server-to- client communications. It is unrelated to email.

E . Port 137: This port is part of NetBIOS, used for name resolution in legacy Windows environments. It is not relevant to email traffic.

F . Port 443: This port is used for HTTPS (secure web traffic) and is unrelated to email protocols.

Key Takeaway:The two correct port numbers associated with email traffic are B. 25 (SMTP) for sending emails and D. 110 (POP3) for retrieving emails.

Question: 67

Which of the following storage options would a technician most likely recommend to have large amounts of affordable capacity without concern for read times on a desktop computer?

A. 750GB NVMe M.2 SSD

B. 2x 1TB PCIe SSD in RAID 1

C. 2TB SATA 3.5" 5,400rpm HDD

D. 4TB SAS 2.5" 15,000rpm HDD

Answer: C

Explanation:

If performance isnot a primary concernand the user requireslarge, cost-effective storage, a2TB

5400rpm SATA HDDis ideal. It offers high capacity at a lower price point than SSDs and faster HDDs.

Option A:NVMe drives offer exceptional speed but are significantly more expensive per GB and not necessary when read/write speed is not a concern.

Option B:RAID 1 improves redundancy but cuts usable capacity in half and uses expensive SSDs.

Option D:SAS drives are fast and reliable but are enterprise-grade and expensive overkill for desktop use.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 1.3: Given a scenario, install and configure storage devices.

Question: 68

Which of the following resolutions is commonly known as Ultra HD?

A. 1920x1080

B. 2048x1080

C. 3840x2160

D. 7680x4320

Answer: C

Explanation:

Ultra HD (UHD), also referred to as4K UHD, has a resolution of3840x2160. It's four times the resolution of standard 1080p (Full HD), offering more screen real estate and sharper images.

Option A (1920x1080):Full HD (FHD), not UHD.

Option B (2048x1080):DCI 2K used in cinema, not common for Ultra HD.

Option D (7680x4320):Known as 8K UHD, not standard Ultra HD.

www.atmicnetworks.com

CompTIA A+ Core 1 Exam Objective Reference:

Objective 1.7: Compare and contrast display technologies and their features.

Question: 69

Which of the following is a benefit of using a VLAN?

A. It minimizes collision domains.

B. It provides private access to cloud resources.

C. It increases network address space.

D. It enables secure network segmentation.

Answer: D

Explanation:

A VLAN (Virtual Local Area Network) segments a physical network into separate logical networks, enhancing security by isolating traffic.

Why Not A (Minimizes collision domains): VLANs manage broadcast domains, not collision domains.

Why Not B (Provides private access to cloud resources): VLANs operate within a local network, not cloud-specific.

Why Not C (Increases network address space): VLANs do not affect address space.

CompTIA A+ Exam Reference: Core 1 (220-1201), Section 2.6, VLAN concepts.

Question: 70

Which of the following would prevent a virtual machine from communicating with any endpoints on a network or the

www.atmicnetworks.com

internet?

A. VDI

B. Private cloud

C. Sandbox

D. Type 1 hypervisor

Answer: C

Explanation:

Asandboxis an isolated virtual environment used totest or run applications securelywithout risk to the host or network. It prevents the VM from communicating with external systems, making it ideal for testing malware or suspicious software.

Option A (VDI):Virtual Desktop Infrastructure allows network communication; it does not restrict it.

Option B (Private cloud):Refers to a cloud deployment model, not a communication barrier.

Option D (Type 1 hypervisor):Runs VMs directly on hardware and doesnotinherently block communication.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 4.1: Compare and contrast cloud computing concepts.

Question: 71

A projector has been shutting down after 30 minutes of use, and it has a strange smell The technician confirms the power source is not the cause of the issue Which of the following steps should the technician take next to resolve this issue?

A. Replace the bulb

www.atmicnetworks.com

B. Check the projector configuration.

C. Clean the filter

D. Adjust the gamma settings.

Answer: C

Explanation:

Reasoning: Projectors have air filters that prevent dust from entering the internal components. A clogged filter can cause the projector to overheat, resulting in shutdowns and even strange smells due to overheating components. Cleaning the filter is a standard troubleshooting step when projectors exhibit overheating symptoms.

Why the Other Options Are Incorrect:

A . Replace the bulb:

While a failing bulb may eventually cause issues, it would not typically result in a strange smell or repeated shutdowns after a fixed period. Bulb issues usually manifest as dim or flickering images.

B . Check the projector configuration:

Configuration settings, such as resolution or input options, would not cause overheating or shutdowns. This option does not address the described symptoms.

D . Adjust the gamma settings:

Gamma settings affect display brightness and contrast but have no impact on overheating or strange smells.

Practical Example:

Dust accumulation in projectors is a common issue, especially in environments with poor air

circulation. A clogged filter causes restricted airflow, leading to overheating and automatic shutdowns to protect internal components. Cleaning the filter typically resolves this issue.

CompTIA A+ Exam Objective Alignment:

Objective 5.5: Troubleshoot common video, projector, and display issues.

Question: 72

A customer is able to print most documents with their USB inkjet printer, but the system is unresponsive when printing a certain report from a custom application. Nothing will print until the computer is restarted and the printer is power cycled. A technician remotes into the PC and confirms that the spooler stops working when this report is sent. After cleaning the spooler and reinstalling the drivers from the manufacturer's website, the issue persists. No other sites using the application report similar issues. Which of the following is most likely causing the issue?

A. The manufacturer is curating content before it reaches the device to preserve ink.

B. The application has a bug that the developer needs to address.

C. The system is using the PostScript language instead of the PCL.

D. Personal preferences have changed and documents with graphics are now online-only

Answer: B

Explanation:

If a print spooler crashes specifically with one application and no issue occurs on other systems, the most likely root cause is a bug within that specific application. Restarting the spooler and reinstalling drivers resolves system-wide or hardware-related issues not app-specific failures. This indicates the application may be sending malformed print data.

Reference: "CompTIA A+ Certification All-in-One Exam Guide" by Mike Meyers – Chapter 26, page 1144.

Question: 73

A technician needs to move a workstation to a different logical network segment. Which of the following technologies should the technician use?

A. DHCP

B. VLAN

C. DNS

D. VPN

Answer: B

Explanation:

AVLAN (Virtual LAN)is used to logically segment a network without requiring physical separation. It enables grouping devices based on function or department regardless of their physical location.

Option A (DHCP):Assigns IP addresses dynamically but doesn't create network segments.

Option C (DNS):Resolves domain names to IP addresses, not used for network segmentation.

Option D (VPN):Provides secure remote access but does not relate to logical segmentation within a local network.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 2.3: Explain common logical networking concepts.

Question: 74

Which of the following connectors is found on an optical networking cable?

A. RJ45

B. LC

C. USB-C

D. Lightning

Answer: B

Explanation:

Comprehensive and Detailed Step-by-Step

LC Connector (Lucent Connector):

LC is a type of fiber optic connector commonly used in optical networking cables. It is small, compact, and widely used for high-speed data transfer over fiber optic networks.

LC connectors are specifically designed for fiber optic cables, making them the correct answer.

Incorrect Options:

A . RJ45: RJ45 connectors are used for Ethernet cables (twisted-pair copper cabling) and are not compatible with optical networking cables.

C . USB-C: USB-C is a connector type used for general-purpose data transfer, charging, and video output, not for optical networking.

D . Lightning: Lightning connectors are proprietary to Apple devices and are not used in optical networking.

Key Takeaway:

The LC connector is specifically designed for fiber optic cables, making it the correct answer for optical networking.

Reference: CompTIA A+ Core 1 Exam Objectives (220-1201), Domain 3.1 – Cable and connector types, including fiber optic cables.

Question: 75

Which of the following is designed to be used in commercial spaces?

A. USB 3.1 Gen 2
B. Straight tip fiber connector
C. Plenum cabling
D. Cat 8

Answer: C

Explanation:

Plenum cabling is designed for use in commercial spaces where cables run through air ducts or plenum spaces, as it has fire-resistant properties and emits less toxic smoke.

Why Not A (USB 3.1 Gen 2): USB is for peripheral connections, not large-scale commercial installations.

Why Not B (Straight tip fiber connector): Fiber connectors are for high-speed connections but are not specifically for commercial spaces.

Why Not D (Cat 8): While Cat 8 is high-speed, it is not uniquely suited for commercial spaces like plenum cabling.

CompTIA A+ Exam Reference: Core 1 (220-1201), Section 3.1, cabling standards.

Question: 76

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:

An IDE hard drive uses a Molex connector for power. This 4-pin connector is a standard for older drives.

Why Not A (F type): F type connectors are used for coaxial cables in video and internet applications.

Why Not B (SC): SC connectors are for fiber optic cables.

Why Not D (Lightning): Lightning connectors are for Apple devices.

CompTIA A+ Exam Reference: Core 1 (220-1201), Section 3.1, cable types and connectors.

Question: 77

Which of the following printing initiatives would be best to accomplish environmentally friendly objectives?

A. Requiring user authentication for printing

B. Locking down printing to only certain individuals

C. Modifying duplex settings to double-sided

D. Changing the print quality settings to best

Answer: C

Explanation:

Comprehensive and Detailed Step-by-Step

Modifying duplex settings to double-sided:

Printing on both sides of the paper (duplex printing) reduces paper usage, making it one of the most effective environmentally friendly printing initiatives.

It directly minimizes waste and supports sustainability goals in the workplace.

Incorrect Options:

A . Requiring user authentication for printing: While this can reduce unnecessary or unauthorized printing, it does not directly address environmental objectives like saving resources.

B . Locking down printing to only certain individuals: Limiting access may reduce printing overall, but it does not actively contribute to environmentally friendly practices like duplex printing.

D . Changing the print quality settings to best: Using the "best" print quality increases toner or ink usage, which is counterproductive to environmentally friendly objectives.

Key Takeaway:

Modifying duplex settings to enable double-sided printing is the best initiative to achieve environmentally friendly goals by reducing paper consumption.

Reference: CompTIA A+ Core 1 Exam Objectives (220-1201), Domain 3.8 – Implementing best practices for environmental impact.

Question: 78

Which of the following networking devices will most likely need to be installed in between the ISP running DOCSIS and the LAN in a SOHO environment?

A. Switch

B. Firewall

C. Cable modem

D. Router

E. Access point

Answer: C

Explanation:

Comprehensive and Detailed Step-by-Step

To determine the correct device, we need to understand how a DOCSIS (Data Over Cable Service Interface Specification) network functions in a Small Office/Home Office (SOHO) environment:

C . Cable Modem:

A cable modem is required to convert the signal provided by the ISP (Internet Service Provider) over a DOCSIS network into a format that is usable by the local area network (LAN).

DOCSIS is a standard for high-speed internet over cable television infrastructure, and the cable modem acts as the gateway between the ISP's coaxial network and the LAN.

Without the cable modem, devices in the LAN would not be able to access the internet.

Reference: CompTIA A+ Core 1 Exam Objectives (220-1201), Domain 2.2 – Compare and contrast Internet connection types, network types, and their features.

Incorrect Options:

A . Switch:

A switch is used to connect multiple devices within the LAN. It does not connect the LAN to the ISP's DOCSIS network.

B . Firewall:

While firewalls provide security by managing inbound and outbound traffic, they do not serve as the interface between the ISP and LAN.

D . Router:

A router directs traffic between different networks (e.g., between a LAN and the internet). However, in a DOCSIS network, the cable modem is the device that first connects to the ISP. Many modern cable modems also include built-in routers, but the modem is the primary device needed.

E . Access Point:

An access point provides wireless connectivity within the LAN. It does not connect directly to the ISP or handle DOCSIS signals.

Key Takeaway:The correct device required to interface between the ISP's DOCSIS network and the SOHO LAN is the cable modem.

Question: 79

A technician needs to ensure all data communications on all network devices are encrypted when logging in to the console. Which of the following protocols should the technician enable?

A. SSH

B. LDAP

C. FTPS

D. SMTP

Answer: A

Explanation:

SSH (Secure Shell) encrypts data communications for secure remote login and management of network devices, ensuring all console connections are encrypted.

Why Not B (LDAP): LDAP is used for directory services and does not encrypt by default.

Why Not C (FTPS): FTPS encrypts file transfers, not console communications.

Why Not D (SMTP): SMTP is used for email transmission, not for securing login sessions.

CompTIA A+ Exam Reference: Core 1 (220-1201), Section 2.7, network security protocols.

Question: 80

A financial institution needs a secure way to protect encryption keys used for unlocking chips on its credit cards Which of the following should the institution use?

A. TLS

B. AMD

C. HSM

D. ARM

Answer: C

Explanation:

A Hardware Security Module (HSM) securely manages cryptographic keys, including those used to protect credit card chips.

www.atmicnetworks.com

Why Not A (TLS): TLS secures data in transit, not encryption key storage.

Why Not B (AMD): AMD refers to processors, not security modules.

Why Not D (ARM): ARM is a processor architecture, not a cryptographic security solution.

CompTIA A+ Exam Reference: Core 2 (220-1102), Section 2.5, cryptographic hardware.

Question: 81

A salesperson is unable to use a personal device to access emails and calendar features at a client site but was able to use the device while at the office. Which of the following policies has been enforced on the salesperson's mobile device?

A. MOW

B. MAN

C. MFA

D. MAM

Answer: D

Explanation:

Mobile Application Management (MAM) enforces policies restricting access to apps and services based on location, ensuring security at external sites.

Why Not A (MOW): "Mobile Only Workplace" (MOW) is not a recognized term in this context.

Why Not B (MAN): Metropolitan Area Network (MAN) is unrelated to mobile device policies.

Why Not C (MFA): Multi-Factor Authentication secures user accounts but does not enforce app restrictions.

CompTIA A+ Exam Reference: Core 2 (220-1102), Section 2.7, mobile device security policies.

Question: 82

A help desk technician needs to work on a high-volume printer. Users have reported occasional paper jams and smudges appearing on printed documents. Which of the following steps should the technician do next to address these issues?

A. Perform a full factory reset.

B. Check and clean the rollers.

C. Change all the ink or toner cartridges.

D. Replace the fuser.

Answer: B

Explanation:

Paper jams and smudging in high-volume printers are often caused bydirty or worn rollers. Rollers are responsible for feeding the paper through the printer. Over time, they accumulate dust, toner residue, or wear out, resulting in misfeeds or jams. Cleaning or replacing them typically resolves this issue.

Option A (Factory reset):A full reset does not directly address mechanical issues like dirty rollers or smudging. It's a last resort and more relevant to configuration or software-related issues.

Option C (Change toner cartridges):While toner quality can affect print quality, it won't usually cause jams or widespread smudging unless the cartridge is leaking which is less likely across multiple users.

Option D (Replace the fuser):A damaged fuser could cause smudging, but this is typically after extensive use and is not the first thing to check. Fuser issues also usually present more persistent, uniform smudges.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 3.7: Given a scenario, troubleshoot common printer problems.

Question: 83

After a technician installs a new motherboard, the computer will not start and fails POST. The technician verifies the power supply is functioning as expected, and the CPU is installed correctly. Which of the following steps should the technician complete next?

A. Flash the BIOS.

B. Check the CMOS battery.

C. Reseat the RAM.

D. Reinstall the old motherboard.

Answer: C

Explanation:

A common reason for aPOST failureafter a motherboard installation isimproperly seated RAM. The system requires working memory to successfully complete POST. Reseating (removing and reinserting) the RAM ensures it's making proper contact with the motherboard.

Option A:Flashing the BIOS is not possible if the system won't POST.

Option B:A dead CMOS battery can cause BIOS settings to reset, but it usually won't prevent POST entirely.

Option D:Reinstalling the old motherboard is premature basic troubleshooting steps should be completed first.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 3.5: Given a scenario, troubleshoot problems related to motherboards, RAM, CPU, and power.

Question: 84

A user brings a laptop to work every morning, correctly seats it in the docking station and then opens the laptop to begin work with no issues After the user left the laptop at home during a two-week vacation the laptop is no longer working.

Upon returning to the office, the user reports that the keyboard and display are no longer working Which of the following should the technician ask the user to do first?

A. Ensure the docking station is plugged in.

B. Press and release the laptop power button.

C. Plug the laptop in and let it charge overnight

D. Connect the laptop directly to the network.

Answer: B

Explanation:

Reasoning: Many docking stations provide power and functionality only when the laptop is properly powered on. If the laptop was powered off (e.g., during the vacation), docking it will not automatically turn it on. The technician should first ensure the laptop is powered on by pressing the power button.

This is a common troubleshooting step when laptops in docking stations appear non-functional.

Relevance to CompTIA A+ Core 1: This falls under Objective 5.2, which covers diagnosing and resolving common laptop and mobile device issues.

Why the Other Options Are Incorrect:

A . Ensure the docking station is plugged in:

While ensuring power to the docking station is important, the scenario specifies that the issue occurred after a vacation. The likelihood of the docking station losing power coincidentally during the vacation is low. Verifying the laptop's power state should be the first step.

C . Plug the laptop in and let it charge overnight:

There is no indication the laptop's battery is drained. While charging could resolve a dead battery, the user is more likely experiencing an issue where the laptop is powered off but docked, so charging overnight is not the best first step.

D . Connect the laptop directly to the network:

www.atmicnetworks.com

A network connection will not resolve the primary issue of the keyboard and display not working. Addressing the laptop's power state is a higher priority.

Practical Example:

If a user returns from a vacation and places a powered-off laptop into a docking station, it may not automatically power on. Pressing the power button ensures the laptop is operational and communicating with the docking station.

CompTIA A+ Exam Objective Alignment:

Objective 5.2: Troubleshooting common laptop issues, including power, display, and peripheral connectivity.

Question: 85

An end user's domain password expires while they are working from home. The end user tries to reset the password using Ctrl+Alt+Delete and then receives the following message:

Configuration information could not be read from the domain controller, either because the machine is unavailable or because access is denied.

Which of the following will resolve this issue?

A. Restart the computer.

B. Connect to the VPN.

C. Reset the account in Active Directory.

D. Join the Wi-Fi network.

Answer: B

Explanation:

To change adomain passwordfrom a remote location, the system must communicate with thedomain controller. Since the user is working from home, they need toconnect to the corporate VPNto

www.atmicnetworks.com

establish that secure connection. Without it, the password change cannot be authenticated.

Option A:Restarting will not resolve the lack of connection to the domain controller.

Option C:Resetting the password in AD could help, but doesn't let the user reset it themselves.

Option D:The user may already be on Wi-Fi; the issue is with connecting to thecorporate network, not local.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 1.6: Given a scenario, configure basic mobile device network connectivity and application support.

Question: 86

The display in a conference room has a ghost image that does not match the presentation Which of the following would test resolve the issue?

A. Adjust the color settings.

B. Correct the keystone.

C. Increase the brightness levels

D. Replace the monitor.

Answer: B

Explanation:

B . Correct the keystone:

A keystone correction adjusts the image shape when a projector is angled either up or down. When a projector is not positioned directly perpendicular to the screen, the image becomes distorted or

offset. Correcting the keystone will resolve alignment issues, ensuring that the presentation matches the display.

Incorrect Options:

A . Adjust the color settings: This is used for improving color balance and has no impact on ghosting or mismatched images.

C . Increase the brightness levels: Brightness changes the visibility of the image but does not address ghosting or alignment.

D . Replace the monitor: Replacing the monitor is unnecessary unless there is hardware failure, which is not indicated here.

Key Takeaway: Keystone correction is essential to resolve alignment and distortion issues in projected images.

Reference: CompTIA A+ Core 1 Exam Objectives (220-1201), Domain 3.4 – Display troubleshooting.

Question: 87

A security team wants to implement compliance controls that only permits the installation of company-approved software on user laptops. Which of the following should the IT department deploy?

A. EDR

B. VPN

C. MDM

D. SaaS

Answer: C

Explanation:

Mobile Device Management (MDM) allows IT departments to enforce compliance controls, such as restricting the installation of unapproved software, on laptops and mobile devices.

Why Not A (EDR): Endpoint Detection and Response focuses on detecting and mitigating security threats, not compliance controls.

Why Not B (VPN): Virtual Private Networks provide secure connections but do not enforce software installation policies.

Why Not D (SaaS): Software as a Service refers to software delivery models and does not enforce compliance controls.

CompTIA A+ Exam Reference: Core 2 (220-1102), Section 2.7, device management and security.

Question: 88

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

A. The new computer has a duplicate IP address.

B. The DNS server is registering both hostnames.

C. The network cable was improperly terminated.

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

Answer: A

Explanation:

If two devices have thesame static IP address, anIP conflictoccurs. This results in both devices being intermittently disconnected or unable to communicate on the network. It's a common mistake when copying configurations manually.

Option B:DNS conflicts wouldn't cause total disconnection and wouldn't occur just from copying IP settings.

Option C:A cable issue would only affect one workstation.

Option D:Switchport security issues wouldn't affect both machines simultaneously unless port security was configured very specifically.

CompTIA A+ Core 1 Exam Objective Reference:

www.atmicnetworks.com

Objective 2.6: Given a scenario, configure and troubleshoot network connectivity.

Question: 89

A user reports slow internet browsing. The technician finds high CPU and memory usage, and pop- ups occur every minute. Which of the following should the technician do next?

A. Escalate to the network team to check end-to-end connectivity.

B. Download and install the latest drivers.

C. Update the anti-malware signatures and scan the system.

D. Check the wireless settings and validate the DHCP configuration.

Answer: C

Explanation:

High resource usage along with frequentpop-upsare strong signs of amalware infection. The next logical step is toupdate anti-malware definitionsandrun a full scanto detect and remove threats.

Option A:Network performance is likely not the root cause local system behavior points to malware.

Option B:Drivers affect hardware functionality; they don’t resolve malware-related slowness.

Option D:DHCP issues usually cause IP conflicts or no network access, not CPU spikes or pop-ups.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 4.2: Given a scenario, detect, remove, and prevent malware using appropriate tools and methods.

Question: 90

Which of the following involves installing an application on a server so several users can run the application

concurrently without the need for local installation?

A. Client virtualization

B. Software as a service

C. Sandboxing

D. Embedded software

Answer: A

Explanation:

Client virtualization involves installing an application on a server and enabling multiple users to run the application simultaneously via virtualized sessions. This eliminates the need for individual installations on local machines.

Why Not B (Software as a Service): SaaS delivers software over the internet and does not require local installations but is managed by a third party, not the organization itself.

Why Not C (Sandboxing): Sandboxing is for isolating applications for security testing, not for concurrent user access.

Why Not D (Embedded software): Embedded software is installed on hardware devices, not shared across multiple users.

CompTIA A+ Exam Reference: Core 1 (220-1201), Section 4.2, virtualization concepts.

Question: 91

Which of the following is a Bluetooth network an example of?

A. PAN

B. LAN

C. WAN

D. SAN

Answer: A

Explanation:

Bluetooth is a wireless technology designed for short-range communication between devices. It is a classic example of a Personal Area Network (PAN), which supports communication between devices like smartphones, headsets, keyboards, and mice within a few meters. PANs are smaller in scope compared to LANs or WANs.

Reference: "CompTIA A+ Complete Study Guide" by Quentin Docter – Chapter 5, "Networking Fundamentals", page 275.

Question: 92

A technician is working on a RAID 1 array that is apparently degraded. The technician verifies the RAM and power are both operating as expected. Which of the following can the technician do to further isolate the issue?

A. Perform individual drive diagnostics.
B. Run the chkdsk /i command.
C. Rebuild the RAID array.
D. Reconfigure the array as RAID 0.

Answer: A

Explanation:

Adegraded RAID 1array usually meansone of the drives has failed or is failing. The correctnext step is torun diagnostics on each driveto identify the faulty one. RAID 1 uses mirroring, so one good drive should still contain all the data.

www.atmicnetworks.com

Option B:chkdsk checks file system integrity, not hardware drive health.

Option C:Rebuilding should only occurafteridentifying and replacing a faulty drive.

Option D:RAID 0 offers no redundancy and would destroy data in this context.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 3.5: Given a scenario, troubleshoot problems related to storage devices.

Question: 93

A user is receiving many unsolicited emails. Which of the following controls can be configured to best reduce these types of emails?

A. Load balancer

B. Spam gateway

C. Mail forwarding

D. Proxy servers

Answer: B

Explanation:

A spam gateway filters unsolicited emails at the server level, significantly reducing spam before it reaches user inboxes.

Why Not A (Load balancer): Load balancers distribute traffic but don't filter spam.

Why Not C (Mail forwarding): Forwarding doesn't filter spam.

Why Not D (Proxy servers): Proxies control web traffic, not email filtering.

CompTIA A+ Exam Reference: Core 2 (220-1102), Section 2.10, email security controls.

Question: 94

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

A. Public

B. Hybrid

C. Community

D. Private

Answer: C

Explanation:

ACommunity Cloudis designed for use by several organizations with shared concerns (e.g., security, compliance, jurisdiction). It's common in industries like healthcare or finance where multiple entities benefit from a common infrastructure with shared policies.

Option A (Public):Open to general public or large industry group less secure.

Option B (Hybrid):Mix of public and private does not imply industry collaboration.

Option D (Private):Dedicated to a single organization.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 2.1: Compare and contrast cloud computing concepts.

Question: 95

A systems administrator deploys BitLocker to all devices. However, one of the desktop PCs is not able to encrypt the boot drive. Which of the following should the administrator check?

A. TPM

B. CPU

C. RAM

D. HDD

Answer: A

Explanation:

BitLocker Drive Encryption in Windows requires aTrusted Platform Module (TPM)to encrypt the boot drive securely. The TPM is a dedicated microcontroller designed to secure hardware through integrated cryptographic keys. It validates system integrity during boot and securely stores the encryption keys. If BitLocker cannot find a TPM or it is disabled in BIOS/UEFI, drive encryption cannot proceed.

BitLocker can function without TPM using a USB startup key, but this compromises some security and is not recommended for managed enterprise environments.

Reference:

"CompTIA A+ Certification All-in-One Exam Guide, Eleventh Edition" by Travis Everett and Andrew Hutz – Chapter 13, page 536–537.

"CompTIA A+ Guide to Managing and Troubleshooting PCs" by Mark Soper – Chapter 13, page 446– 447.

"CompTIA A+ Complete Study Guide" by Quentin Docter – Chapter 1, page 36–38.

Question: 96

Which of the following network services is used to assign an IP address to a network host?

A. DHCP

B. DNS

C. LDAP

D. SMTP

Answer: A

Explanation:

DHCP (Dynamic Host Configuration Protocol) is the service used to automatically assign IP addresses to network hosts. It dynamically manages the distribution of IP addresses and configuration details (like subnet mask, gateway, and DNS servers), ensuring no two devices are assigned the same address on the network.

Option B (DNS): Incorrect. DNS translates domain names into IP addresses but does not assign them.

Option C (LDAP): Incorrect. LDAP is a protocol used for accessing and maintaining directory services, such as user information and permissions.

Option D (SMTP): Incorrect. SMTP is used for sending and receiving email, not for IP address

assignment.

Reference:

CompTIA A+ Core 1 Objectives: 2.5 (Network configuration)

Question: 97

A technician is experimenting with network configurations and has connected two laptops to an unmanaged switch. The technician configured one of the laptops with a static IP address of 192.168.1.1 and the other with a static IP address of 192.168.2.2. The laptops are not communicating with each other. Which of the following is the most likely explanation for this issue?

A. The technician needs to use a hub instead of a switch.

B. The wireless NICs are malfunctioning.

C. PoE interferes with intersubnet communication.

www.atmicnetworks.com

D. The laptops do not have access to a router.

Answer: D

Explanation:

Question: 98

Which of the following utilizes specialized ports on a laptop to expand the local connection options?

A. NFC adapter

B. Docking station

C. Port replicator

D. USB dongle

Answer: B

Explanation:

Adocking stationconnects to a laptop'sproprietary port or USB-C/Thunderbolt, providing access tomultiple additional ports(USB, Ethernet, video, audio, etc.). It allows users to transform a laptop into a full desktop workstation.

Option A (NFC adapter):Used for short-range communication, not port expansion.

Option C (Port replicator):Similar to a dock but usually less powerful and often lacks charging or video output.

Option D (USB dongle):Adds a single function (like Wi-Fi or storage), not full port expansion.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 1.4: Given a scenario, configure settings and use cases for laptops and mobile devices.

Question: 99

Which of the following devices is designed to monitor and filter incoming and outgoing network traffic?

A. Switch

B. Access point

C. Firewall

D. Hub

Answer: C

Explanation:

A firewall monitors and filters incoming and outgoing network traffic based on security rules, protecting the network from unauthorized access and threats.

Why Not A (Switch): A switch connects devices within a network but does not monitor or filter traffic.

Why Not B (Access point): An access point provides Wi-Fi connectivity but does not filter traffic.

Why Not D (Hub): A hub simply broadcasts data to all connected devices without filtering traffic.

CompTIA A+ Exam Reference: Core 1 (220-1201), Section 2.2, network security concepts.

Question: 100

Which of the following can a user utilize to share their mobile phone connection with their laptop?

A. IR

B. NFC

C. Wi-Fi Direct

D. Tethering

Answer: D

Explanation:

Tethering refers to sharing a mobile phone's internet connection with another device, such as a laptop, either through USB, Bluetooth, or Wi-Fi. Tethering effectively turns the mobile phone into a personal hotspot for internet access.

Option A (IR): Incorrect. Infrared (IR) is used for short-range communication, such as remote controls, but it does not support internet sharing.

Option B (NFC): Incorrect. Near-field communication (NFC) is used for close-proximity data transfer, not for internet sharing.

Option C (Wi-Fi Direct): Incorrect. Wi-Fi Direct enables device-to-device communication but does not inherently provide internet sharing.

Reference:

CompTIA A+ Core 1 Objectives: 1.4 (Configure basic mobile-device network connectivity)

Question: 101

A technician is having issues replacing a laptop's wireless card because the cover seems to be stuck Which of the following should the technician do next to troubleshoot this issued

A. Check the product manual for the procedure

B. Use a pry tool to force the cover open

C. Insert the wireless card into the M.2 slot

D. Try to move the cover by sliding it in all directions.

Answer: A

Explanation:

A . Check the product manual for the procedure:

When hardware is not easily accessible, always consult the product manual for proper disassembly procedures. Forcing the cover can damage the laptop or void the warranty.

Product manuals often provide step-by-step instructions for safely accessing internal components.

Incorrect Options:

B . Use a pry tool to force the cover open: Forcing the cover can cause physical damage to the device.

C . Insert the wireless card into the M.2 slot: This step cannot be performed until the cover is properly removed.

D . Try to move the cover by sliding it in all directions: Randomly sliding the cover can cause damage if the correct removal method is not followed.

Key Takeaway: Always refer to the product manual to ensure safe and proper disassembly of laptop components.

Reference: CompTIA A+ Core 1 Exam Objectives (220-1201), Domain 4.1 – Best practices for laptop hardware installation.

Question: 102

A technician needs to confirm that desktop PCs can be deployed to a global, remote workforce. Which of the following specifications should the technician validate?

A. Input voltage

B. BIOS language support

C. Supply chain security

D. Power efficiency

Answer: A

Explanation:

Input voltage must be validated to ensure desktop PCs can operate in different regions with varying power standards (e.g., 110V in North America vs. 220V in Europe). Failure to verify input voltage compatibility can lead to hardware damage or operational issues.

Option B (BIOS language support): Incorrect. While language support may be helpful, it is not critical for hardware deployment across regions.

Option C (Supply chain security): Incorrect. This refers to ensuring secure sourcing of components but does not directly impact deployment.

Option D (Power efficiency): Incorrect. Power efficiency may be important for energy savings but is not relevant to regional compatibility.

Reference:

CompTIA A+ Core 1 Objectives: 3.5 (Power supply requirements)

Question: 103

A technician needs to troubleshoot a user's smartphone that will not connect to its wireless provider's service. Which of the following should the technician check first?

A. SIM card

B. Network settings

C. Subscription plan

D. Bluetooth connection

Answer: C

Explanation:

Question: 104

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

A. Serial interfaces

B. Docking station

C. Network switch

D. USB hub

Answer: B

Explanation:

Reasoning: A docking station is designed to provide a central connection point for multiple peripherals, such as monitors, keyboards, mice, and network cables. It allows users to quickly connect or disconnect all devices by simply docking or undocking their laptop, improving mobility and reducing wear and tear on individual ports.

Why the Other Options Are Incorrect:

A . Serial interfaces:

Serial interfaces are outdated and rarely used in modern laptops or peripherals. They are not practical for facilitating the connection of multiple devices.

C . Network switch:

A network switch is used to connect multiple devices to a network, but it does not simplify the connection of

peripherals to a laptop.

D . USB hub:

A USB hub can extend the number of available USB ports but lacks the full functionality of a docking station, such as video output or Ethernet connectivity.

Practical Example:

A user with a laptop, external monitors, keyboard, and mouse can use a docking station to connect all devices with a single action, instead of plugging in each device manually.

CompTIA A+ Exam Objective Alignment:

Objective 5.2: Explain device interfaces, connection types, and usage of docking stations.

Question: 105

Which of the following best characterizes the use of a virtual machine as a sandbox?

A. Run an application on multiple workstations without installation.

B. Explore how an application behaves in a different environment

C. Migrate a currently used legacy application from physical to virtual

D. Create a firewall where the sandbox acts as a perimeter network.

Answer: B

Explanation:

A sandbox in virtualization allows testing an application in an isolated environment to observe its behavior without

affecting the host system.

Why Not A (Run an application on multiple workstations): This describes application virtualization, not sandboxing.

Why Not C (Migrate a legacy application): This is about virtualization for legacy support, not testing.

Why Not D (Create a firewall): A firewall does not act as a sandbox for application testing.

CompTIA A+ Exam Reference: Core 1 (220-1201), Section 4.2, virtualization and sandboxing.

Question: 106

An employee who travels worldwide wants a workstation to perform the same whether the workstation is in the corporate office environment or elsewhere. Which of the following should a technician implement?

A. Public cloud

B. VDI

C. SSH

D. SaaS

Answer: B

Explanation:

Question: 107

When turning on a workstation, a technician observes the following message:

"Bootable device not found."

The technician verifies the correct boot order in the BIOS. Which of the following steps should the technician take next?

A. Reformat the HDD.

B. Run HDD diagnostics.

C. Reseat the RAM.

D. Replace the HDD.

Answer: B

Explanation:

If the system reports“Bootable device not found”, and the BIOS is configured correctly, the next step is torun diagnostics on the hard driveto check for physical or logical failure. It could be a sign of afailing drive or corrupt boot sector.

Option A:Reformatting the drive would erase data not a diagnostic step.

Option C:RAM does not affect whether a drive is bootable.

Option D:Replacing the drive should only be doneafter diagnostics confirm failure.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 3.5: Given a scenario, troubleshoot problems related to storage devices.

Question: 108

Which of the following is an advantage of using a hybrid cloud instead of a public cloud?

A. Ability to reduce management overhead

B. Ability to use cross-platform virtualization

C. Ability to meet data residency requirements

D. Ability to leverage IaaS and PaaS

Answer: C

Explanation:

A hybrid cloud combines on-premises infrastructure with public cloud services. One significant advantage is that it allows organizations to keep sensitive data in a private environment to meet regulatory or data residency requirements, while still utilizing the scalability and cost-efficiency of the public cloud for other workloads. This ensures compliance with legal mandates about data location.

Reference: "CompTIA A+ Complete Study Guide" by Quentin Docter – Chapter 8, "Virtualization and Cloud Computing", page 488. Also supported in CompTIA A+ Exam Objectives220-1201under section 4.1.

Question: 109

A group of friends is gathering in a room to play video games. One of the friends has a game server. Which of the following network types should the group use so they can all connect to the same server and the internet?

A. SAN

B. MAN

C. LAN

D. PAN

Answer: C

Explanation:

The appropriate network type for this scenario is a Local Area Network (LAN), which is designed for small, localized networks, such as within a single building or room. LANs are ideal for gaming because they provide high-speed, low-latency connections.

Option A (SAN): Incorrect. A Storage Area Network is used for data storage, not for gaming or general networking.

Option B (MAN): Incorrect. A Metropolitan Area Network covers a city or campus, far exceeding the scope needed for a gaming setup in a single room.

Option D (PAN): Incorrect. A Personal Area Network is designed for a single user, such as Bluetooth devices, and would not support multiple devices connecting to a game server.

Reference:

CompTIA A+ Core 1 Objectives: 2.7 (Compare and contrast network types and features)

Question: 110

A technician is troubleshooting a computer that has random BSOD alerts and intermittently freezes during normal use. Performance degrades as the day goes on. No new software or hardware changes have been implemented. Freezing occurs under performance-intensive operations. Which of the following hardware components is most likely at fault?

A. Video card

B. HDD

C. RAM module

D. TPM

Answer: C

Explanation:

Comprehensive and Detailed Step-by-Step

Random BSODs (Blue Screen of Death), intermittent freezing, and degraded performance under load are common symptoms of failing or faulty RAM (Random Access Memory). Here's the reasoning:

RAM Module (Correct Answer):

Faulty or failing RAM can cause random BSODs due to memory errors when the system attempts to read or write to corrupted memory locations.

Intermittent freezing, especially under performance-intensive operations, can occur because the CPU relies heavily on RAM for active processing tasks.

Over time, heat generated during usage can exacerbate RAM instability, leading to progressively worse performance throughout the day.

Solution: The technician should run a memory diagnostic tool, such as Windows Memory Diagnostic or MemTest86, to confirm if the RAM is at fault.

Incorrect Options:

A . Video Card: A faulty video card can cause graphical glitches, screen artifacts, or crashes, but it is unlikely to cause system-wide performance degradation and random freezing under normal operations unless the issue is specific to GPU-intensive tasks (e.g., gaming or video rendering).

B . HDD: A failing hard drive can cause system slowdowns and freezing, but it typically produces other symptoms such as read/write errors, boot failures, or clicking sounds. HDD issues do not usually cause BSODs unless critical system files are corrupted.

D . TPM (Trusted Platform Module): A TPM is a hardware-based security module used for encryption and secure authentication. It does not affect performance or cause BSODs or freezing under normal operation.

Key Takeaway:

The symptoms described (random BSODs, intermittent freezing, and degraded performance under load) are most likely caused by faulty or failing RAM. Memory diagnostic tools should be used to confirm the issue.

Reference: CompTIA A+ Core 1 Exam Objectives (220-1201), Domain 5.2 – Troubleshooting problems related to motherboards, RAM, CPUs, and power.

Question: 111

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

www.atmicnetworks.com

C. Print server

D. Printer subnet

E. SMB configuration

F. Printer Wi-Fi settings

Answer: A,C

Explanation:

To allow multiple users to print to networked printers:

Printer shares enable users to access printers shared on the network.

Print servers manage print jobs and provide centralized control of printing.

Why Not B (DHCP server): DHCP is unrelated to print management.

Why Not D (Printer subnet): Subnets group devices but don't manage printing.

Why Not E (SMB configuration): SMB is for file sharing, not specifically print management.

Why Not F (Printer Wi-Fi settings): These settings are irrelevant since the printers use Ethernet.

CompTIA A+ Exam Reference: Core 2 (220-1102), Section 4.6, printer configuration.

Question: 112

Which of the forming connector types would best suit a company that experiences a large volume of internet traffic?

A. USB 3.1

B. Quad-shielded RG11 coax

C. SATA3.0

D. Unshielded plenum RJ45

Answer: B

Explanation:

RG11 coaxial cable with quad shielding is designed to handle large volumes of internet traffic, providing excellent resistance to interference and high bandwidth capacity.

Why Not A (USB 3.1): USB 3.1 is used for connecting peripherals, not for high-volume internet traffic.

Why Not C (SATA3.0): SATA is used for internal data storage connections, not for network traffic.

Why Not D (Unshielded plenum RJ45): While RJ45 cables are commonly used, unshielded cables are prone to interference and are not ideal for high-volume traffic.

CompTIA A+ Exam Reference: Core 1 (220-1201), Section 3.1, cable types and their characteristics.

Question: 113

A technician is troubleshooting stylus issues on identical, company-provided tablets. Users can purchase their own accessories. Some users have no issues, but others report that their styluses charge intermittently and die frequently. Which of the following is the most likely cause of this issue?

A. Certain cases are causing charging issues.

B. The tablets need to be updated.

C. Some of the tablets have manufacturing defects.

D. The malfunctioning styluses need firmware updates.

Answer: A

Explanation:

The most likely cause isthird-party or ill-fitting casesobstructing the contact between the stylus and the tablet charging mechanism. Some cases may not be designed with stylus charging in mind, particularly if users are purchasing

www.atmicnetworks.com

their own accessories.

Option B:A software update might fix OS-related issues, but would not typically affect physical charging.

Option C:If some devices had defects, the issue would likely be consistent, not isolated to some users.

Option D:Firmware issues could be a factor but are less likely than physical obstructions when users are using different accessories.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 1.4: Given a scenario, configure settings and use cases for laptops and mobile devices.

Question: 114

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

A. The SSD is faulty and should be replaced by the manufacturer
B. The SSD has not been properly formatted and is not readable
C. The SSD is incompatible with the motherboard
D. The SSD has not boon installed properly and should be reseated

Answer: D

Explanation:

Improper seating is the most common reason an SSD isn’t recognized. Ensuring it is correctly connected resolves the issue.

Why Not A (Faulty SSD): A faulty SSD is possible but less likely than an installation issue.

Why Not B (Not formatted): Formatting affects data usability, not drive detection.

Why Not C (Incompatibility): SSD compatibility issues are rare with modern hardware.

CompTIA A+ Exam Reference: Core 1 (220-1201), Section 3.3, storage troubleshooting.

www.atmicnetworks.com

Question: 115

A salesperson is unable to reach the internet from a home office PC A support technician wants to verify the router is receiving a valid public IP address Which of the Wowing is a valid public IP address in this scenario?

A. 10.254.128.11

B. 66.157.195.20

C. 172.16.0.30

D. 192.168 1.50

Answer: B

Explanation:

A valid public IP address must fall outside the private IP address ranges:

A. .0.0.0 to 10.255.255.255

B. 2.16.0.0 to 172.31.255.255

C. 2.168.0.0 to 192.168.255.255

66.157.195.20 is outside these ranges, making it a public IP address.

Why Not A, C, D: These IPs fall within private IP address ranges.

CompTIA A+ Exam Reference: Core 1 (220-1201), Section 2.6, IP addressing.

Question: 116

A customer reports a problem connecting to network resources. After asking open-ended questions, the technician determines the issue likely exists on the remote server. Which of the following should the technician do next?

A. Document the findings.

B. Test the theory

C. Gather information

D. Establish a plan of action

Answer: B

Explanation:

After determining the issue is likely on the remote server, the technician should test the theory to confirm the root cause before proceeding.

Why Not A (Document the findings): Documentation comes after confirming the issue.

Why Not C (Gather information): Information gathering is already completed.

Why Not D (Establish a plan of action): This is done after confirming the issue.

CompTIA A+ Exam Reference: Core 2 (220-1102), Section 3.1, troubleshooting methodology.

Question: 117

Which of the following technologies best allows a phone to connect to a point-of-sale terminal for wireless payments?

A. Bluetooth

B. NFC

C. Wi-Fi

D. Cellular

Answer: B

Explanation:

Near-field communication (NFC) is a short-distance wireless communication method widely used in mobile payment systems like Apple Pay and Google Pay. Simply placing the device near a compatible terminal initiates the payment process.

Reference: "Mike Meyers' CompTIA A+ Certification All-in-One Exam Guide" – Chapter 24, page 1022.

Question: 118

A new directive mandates the use of a security component to securely allow users to authenticate to systems, access sensitive data, and enter the office. The component must provide an additional factor of authentication alongside user accounts and cannot be something the user o Which of the Mowing components best meets these requirements?

A. Fingerprint reader
B. Smart card
C. Secure token
D. NFC scanner

Answer: B

Explanation:

A smart card provides an additional factor of authentication by storing secure credentials, such as certificates, that cannot be guessed or replicated. It complements user accounts and is "something you have".

Why Not A (Fingerprint reader): This is "something you are", but the scenario specifically requires a physical token.

Why Not C (Secure token): Secure tokens are also valid but may not integrate as seamlessly into multi-factor

authentication for physical and system access.

Why Not D (NFC scanner): An NFC scanner is a device and not a token itself; it reads cards or other credentials.

CompTIA A+ Exam Reference: Core 2 (220-1102), Section 2.5, access controls.

Question: 119

A network administrator must ensure that a printer will still be assigned a specific IP address even if all addresses are depleted. Which of the following network configuration concepts is this describing?

A. VLAN

B. Lease

C. Reservation

D. Exclusion

Answer: C

Explanation:

A DHCP reservation binds a specific MAC address to an IP address so the device always receives the same IP from the DHCP server. This ensures network devices like printers maintain consistent connectivity and availability even when the IP pool is low.

Reference: "CompTIA A+ Complete Study Guide" by Quentin Docter – Chapter 18, page 1252.

Question: 120

A company needs to develop a disaster recovery solution based on virtual machines. Which of the following service models is the most suitable?

A. Infrastructure as a Service

www.atmicnetworks.com

B. Security as a Service

C. Platform as a Service

D. Software as a Service

Answer: A

Explanation:

Infrastructure as a Service (IaaS)providesvirtualized computing resources over the internetsuch as servers, storage, and networking. It allows a business to quickly spin up virtual machines and is ideal fordisaster recoveryand scalable IT infrastructure needs.

Option B:SecaaS focuses on cloud-delivered security, not infrastructure.

Option C:PaaS offers development environments, not full virtual infrastructure.

Option D:SaaS delivers applications over the internet (e.g., email, CRM) not for disaster recovery.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 4.1: Compare and contrast cloud computing concepts.

Question: 121

Each lime a user ties to print, the paper becomes stuck at the last stage of the print job and the user has to poll me paper out of the printer. Which of the following is me most likely cause?

A. Rollers

B. Tray assembly

C. Toner

D. Printhead

Answer: A

Explanation:

If paper gets stuck at the last stage of printing, the rollers responsible for moving the paper through the printer are likely worn out or dirty.

Why Not B (Tray assembly): The tray assembly manages paper loading, not feeding during the print process.

Why Not C (Toner): Toner is unrelated to paper jams.

Why Not D (Printhead): Printheads manage ink/toner distribution, not paper movement.

CompTIA A+ Exam Reference: Core 2 (220-1102), Section 4.6, printer troubleshooting.

Question: 122

Users working with large files back up the files to external hard drives. One user's files take longer to back up than other users' files. The user has tried backing up the files to other users' drives with the same results. Which of the following steps should the technician take first to correct this issue?

A. Replace the hard drive's USB cable.

B. Defragment the user's external hard drive.

C. Update the storage drivers on the user's system.

D. Instruct the user to compress the files.

Answer: B

Explanation:

If a hard drive is heavily fragmented, file read/write operations can take significantly longer, causing slow backup speeds. Defragmenting the drive organizes the data for more efficient access.

Why Not A (Replace the hard drive's USB cable): A faulty cable would typically cause disconnections or errors, not just slower speeds.

Why Not C (Update the storage drivers): This might help if the issue is with system drivers, but the described symptoms point to a fragmentation issue.

Why Not D (Compress the files): Compression reduces file size but does not address the root cause of the slow backups.

CompTIA A+ Exam Reference: Core 2 (220-1102), Section 3.1, storage troubleshooting.

Question: 123

Which of the following devices is used to implement ACL polices for an environment?

A. Managed switch

B. Gateway

C. Repeater

D. Firewall

Answer: D

Explanation:

A firewall implements ACLs (Access Control Lists) to filter traffic and enforce policies based on rules such as IP address, port, or protocol.

Why Not A (Managed switch): A managed switch supports VLANs and QoS but does not enforce ACLs at the network perimeter.

Why Not B (Gateway): Gateways connect networks and translate protocols but don't typically implement ACLs.

Why Not C (Repeater): Repeaters extend signal range but don't enforce policies.

CompTIA A+ Exam Reference: Core 1 (220-1201), Section 2.2, firewall concepts.

Question: 124

A customer reports that the output from their thermal receipt printer has vertical white lines. Which of the following would most likely resolve this issue?

A. Replacing the ink cartridge

B. Using the correct paper type

C. Installing a maintenance kit

D. Cleaning the heating element

Answer: D

Explanation:

Thermal printerscreate images using aheated print headon specially coated thermal paper. Vertical white lines indicate thatpart of the heating element is dirty or blocked, preventing heat transfer to the paper. Cleaning the print head (heating element) will restore full functionality.

Option A:Thermal printers donot use ink or toner, so this is not applicable.

Option B:Wrong paper could cause blank output, but consistent vertical lines point to the print head.

Option C:Maintenance kits are typically for laser printers, not thermal printers.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 3.7: Given a scenario, troubleshoot common printer problems.

Question: 125

Which of the following describes the function of an injector?

A. To provide only data connectivity

B. To supply power across a cable

C. To improve wireless performance

D. To extend a network connection

Answer: B

Explanation:

A PoE injector is used to add power to an Ethernet cable, enabling the cable to deliver both power and data. This is crucial when connecting to PoE-enabled devices like IP cameras or wireless access points that are far from power outlets.

Reference: "CompTIA A+ Complete Practice Tests" by Jeff T. Parker – Chapter 10, Question 77, page 585.

Question: 126

Which of the following is the best to use when testing a file for potential malware?

A. Multitenancy

B. Test development

C. Cross-platform virtualization

D. Sandbox

Answer: D

Explanation:

A sandbox is a secure, isolated environment used to test potentially harmful software or code. It prevents the software from affecting the main system, allowing safe malware testing. Thismethod is standard in cybersecurity best practices.

Reference: "CompTIA A+ Certification All-in-One Exam Guide" by Mike Meyers – Chapter 28, page 1230.

Question: 127

A technician wants to upgrade a computer to a new Windows version. The Windows Upgrade Advisor states that the computer is not compatible with the new Windows version due to a lack of TPM 2.0 support. Which of the following should the technician do next?

A. Enable the module in the UEFI BIOS.

B. Install an HSM in the computer.

C. Perform a clean Install of the new Windows version.

D. Implement BitLocker on the computer.

Answer: A

Explanation:

TPM 2.0 (Trusted Platform Module) is often disabled by default in the UEFI BIOS. Enabling it is necessary to meet the requirements for certain Windows installations, including Windows 11.

Why Not B (Install an HSM): A Hardware Security Module (HSM) is a separate device used for cryptographic functions and is not related to TPM on the motherboard.

Why Not C (Perform a clean install): A clean installation will not bypass the TPM 2.0 requirement.

Why Not D (Implement BitLocker): BitLocker requires TPM but does not resolve its absence or lack of activation.

CompTIA A+ Exam Reference: Core 1 (220-1201), Section 3.4, BIOS/UEFI configuration.

Question: 128

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

A. Fuser

B. Maintenance kit

C. Corona wire

D. Toner cartridge

Answer: B

Explanation:

Amaintenance kitfor a laser printer often includesrollers, fuser, and other partsthat wear out over time. If the printer issmudging and misfeeding, it's a sign thatmultiple components are failing, which a maintenance kit is designed to resolve.

Option A (Fuser):May cause smudging if it's not heating correctly, but it won't resolve paper misfeeds alone.

Option C (Corona wire):Can cause poor image quality if dirty but doesn't affect paper feeding.

Option D (Toner cartridge):Can cause streaks if defective, but not paper feed issues.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 3.4: Given a scenario, install and configure printers.

Question: 129

Which of the following services is used to allocate IP addresses in an enterprise-wide environment?

A. DNS

www.atmicnetworks.com

B. Syslog

C. Telnet

D. DHCP

Answer: D

Explanation:

Dynamic Host Configuration Protocol (DHCP) is a network service used to automatically assign IP addresses and other network configuration details (such as subnet masks and default gateways) to devices on an enterprise-wide network.

Why Not A (DNS): DNS resolves domain names to IP addresses but does not allocate IP addresses.

Why Not B (Syslog): Syslog is used for logging system events, not IP address management.

Why Not C (Telnet): Telnet is a protocol for remote access, not for IP allocation.

CompTIA A+ Exam Reference: Core 1 (220-1201), Section 2.6, DHCP concepts.

Question: 130

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

A. Clean the printhead.

B. Replace the ribbon.

C. Install a maintenance kit.

D. Calibrate the alignment.

Answer: B

Explanation:

Dot matrix printersuse aninked ribbonthat physically contacts the paper through tiny pins. Over time, the ribbon wears out or dries up, resulting infaded or light print output. Replacing the ribbon restores print quality.

Option A:Cleaning helps with image clarity, not ink density.

Option C:Maintenance kits apply to laser printers, not dot matrix.

Option D:Calibration affects print position, not darkness.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 3.7: Given a scenario, troubleshoot common printer problems.

Question: 131

A company needs to keep a record of tasks performed by an application. Which of the following should the company most likely implement as part of a solution?

A. Fileshare

B. Syslog

C. Database

D. SAN

Answer: B

Explanation:

Syslog is used to log system events and tasks performed by applications, providing a centralized record of activity.

Why Not A (Fileshare): Fileshares store files but are not designed for event logging.

Why Not C (Database): Databases can store logs but are not a logging mechanism themselves.

Why Not D (SAN): A SAN is a storage solution, not a logging tool.

CompTIA A+ Exam Reference: Core 1 (220-1201), Section 2.6, system monitoring and logging.

Question: 132

A technician recently updated the firmware on a dual-BIOS motherboard. Following the update, the system has been stuck in a boot loop and cannot start an OS from any internal or external device. The technician cannot access the UEFI menu either. Which of the following should the technician do next?

A. Enable the secondary configuration.

B. Downgrade the firmware via USB.

C. Start a warranty repair of the motherboard.

D. Reapply thermal paste to the CPU.

Answer: A

Explanation:

Dual-BIOS motherboards contain two firmware chips. If theprimary BIOS becomescorrupted, the system canfailover to the secondary BIOS. Most boards allow manual enabling of the secondary BIOS via a physical switch or jumper.

Option B:Downgrading firmware may not be possible if the system won't POST or access UEFI.

Option C:Not necessary until both BIOS chips are non-functional.

Option D:Thermal paste affects heat dissipation, not BIOS/boot behavior.

www.atmicnetworks.com

CompTIA A+ Core 1 Exam Objective Reference:

Objective 3.5: Given a scenario, troubleshoot problems related to motherboards, RAM, CPU, and power.

Question: 133

A customer reports that a workstation has no internet connectivity. A technician confirms the port is disabled. Which of the following is most likely responsible for the issue?

A. Patch panel

B. Physical NIC

C. Managed switch

D. Stand-alone firewall

Answer: C

Explanation:

A managed switch allows an administrator to enable or disable individual ports as part of network security and management. If a port on a managed switch has been disabled, the device connected to that port will lose connectivity, which matches the scenario described.

Reference: CompTIA A+ Certification Exam Core 1 Objectives – Domain 2.0 Networking – Objective 2.2: Compare and contrast common networking hardware devices.

Question: 134

A user is having issues when charging a device with a Lightning cable. The cable is not recognized when it is plugged into the device. This issue is usually resolved by flipping the cable over. This issue does not occur with other devices of the same type. Which of the following would most likely cause the issue?

A. The device needs to be restarted.

B. The battery may be swelling and needs inspection.

C. The cable is failing and needs to be replaced

D. The charging port is dirty or damaged

Answer: D

Explanation:

If flipping the cable helps but the problem is isolated to this device (not others of the same type), the most likely cause is a dirty or damaged charging port on the device itself. Dirt or debris inside the port can prevent a good electrical connection, causing the cable to work intermittently.

Reference: CompTIA A+ Certification Exam Core 1 Objectives – Domain 1.0 Mobile Devices – Objective 1.6: Troubleshoot common mobile device issues.

Question: 135

A technician is setting up a scan-to-SMB function on a multifunction printer. Which of the following connection types should the technician configure?

A. Email server

B. SFTP connection

C. Network share

D. Print services

Answer: C

Explanation:

The scan-to-SMB feature allows the printer to send scanned documents to a shared folder (SMB share) on the network. Setting up a network share enables the device to securely and conveniently save files for user access.

Reference: CompTIA A+ Certification Exam Core 1 Objectives – Domain 2.0 Networking – Objective 2.7: Compare and contrast internet connection types, network types, and their features.

Question: 136

Which of the following internet connection types is the best for extremely high data transfer with symmetrical upload and download speeds?

A. DSL

B. Cellular

C. Fiber

D. Satellite

Answer: C

Explanation:

Fiber optic connections provide the highest data transfer rates and symmetrical upload and download speeds. This makes fiber the ideal choice for applications requiring high-speed connectivity, such as video conferencing, large file transfers, and cloud-based workflows.

Reference: CompTIA A+ Certification Exam Core 1 Objectives – Domain 2.0 Networking – Objective 2.7: Compare and contrast internet connection types, network types, and their features.

Question: 137

Which of the following networking devices is used to create a mesh network?

A. Modem

B. DSL

C. Access point

D. ONT

Answer: C

Explanation:

Mesh networks rely on multiple access points (or mesh nodes) to create a seamless, self-healing network. Each access point communicates with others to extend coverage and improve reliability without requiring a wired backbone for each AP.

Reference: CompTIA A+ Certification Exam Core 1 Objectives – Domain 2.0 Networking – Objective 2.4: Compare and contrast wireless networking protocols.

Question: 138

A user purchases a new mobile phone and tries to connect it to the corporate communications and email applications without success. Which of the following should a technician do to allow the phone to connect?

A. Configure biometric security settings.

B. Turn on LTE hotspot connectivity.

C. Enroll the device in the MDM software.

D. Complete the company's BYOD training process.

Answer: C

Explanation:

Mobile Device Management (MDM) enrollment ensures that mobile devices meet security and access policies required by the corporate network. By enrolling the device in MDM, the technician can apply necessary configurations and enable corporate app access.

Reference: CompTIA A+ Certification Exam Core 1 Objectives – Domain 1.0 Mobile Devices – Objective 1.5: Compare and contrast methods for securing mobile devices.

Question: 139

Which of the following is the ability to automatically increase and decrease instances based on demand?

A. Availability
B. Scalability
C. Multitenancy
D. Elasticity

Answer: D

Explanation:

Elasticity in cloud computing refers to the ability of a system to automatically allocate and release resources (such as CPU, RAM, or virtual machines) as workload demands change. This feature is key to ensuring that resources are used efficiently without manual intervention.

Reference: CompTIA A+ Certification Exam Core 1 Objectives – Domain 4.0 Virtualization and Cloud Computing – Objective 4.2: Summarize cloud computing concepts.

Question: 140

A user is having trouble with the location services on their smartphone. Location-based applications show incorrect positions when the user is traveling. This issue affects the user's ability to navigate and use location-dependent applications. Which of the following is the best way to resolve this issue?

A. Downloading a third-party mapping application

B. Resetting the network settings

C. Enabling Wi-Fi to assist GPS

D. Restarting the smartphone

Answer: C

Explanation:

Wi-Fi assistance in mobile devices helps improve location accuracy by using nearby wireless networks to triangulate the device's position, even when GPS signals are weak (like indoors or in dense areas).

Reference: CompTIA A+ Certification Exam Core 1 Objectives – Domain 1.0 Mobile Devices – Objective 1.6: Troubleshoot common issues with mobile devices.

Question: 141

Which of the following is related to the creation of a secured communication channel between workstations in different locations and is supported by credentials for authentication?

A. DHCP

B. CNAME

C. VLAN

D. VPN

Answer: D

Explanation:

A Virtual Private Network (VPN) creates an encrypted, secure tunnel across a public or untrusted network. It uses authentication credentials to ensure that only authorized users can connect, keeping data safe from interception.

Reference: CompTIA A+ Certification Exam Core 1 Objectives – Domain 2.0 Networking – Objective 2.3: Compare and contrast various types of networks.

Question: 142

Which of the following ports is commonly used for remote desktop connections?

A. 137
B. 445
C. 3389
D. 4443

Answer: C

Explanation:

Port 3389 is used by the Remote Desktop Protocol (RDP) for remote desktop connections in Windows environments. This port allows remote control and management of systems across the network.

Reference: CompTIA A+ Certification Exam Core 1 Objectives – Domain 2.0 Networking – Objective 2.2: Compare and contrast common networking hardware devices and ports.

www.atmicnetworks.com

Question: 143

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:

When a technician encounters a burning smell, it is a critical safety issue. The first response must be to immediately power down and disconnect the device from all power sources to prevent electric shock, fire, or further hardware damage.

From the CompTIA A+ 220-1101 Official Study Guide, Objective 4.1 – Troubleshoot common hardware problems:

"Signs of electrical issues such as burning smells, smoke, or sparks require an immediate shutdown of the system and disconnection from any power source."

After ensuring safety, the technician should inspect the hardware for visible signs of damage:

From the same Objective (4.1):

"Inspect for foreign objects, liquid damage, or burnt components. These can cause short circuits or thermal events that may damage the motherboard or other internal components."

These steps are standard practice in the industry to ensure safe and accurate diagnosis of faulty devices. Trying a different adapter (Option F) may make the problem worse, and contacting vendors (Option D) comes after initial safety and inspection.

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 4: Troubleshooting Hardware Problems

CompTIA Exam Objectives 220-1101, Domain 4.0 – Hardware and Network Troubleshooting

Question: 144

A technician needs to figure out why a laser printer is intermittently not feeding paper to print. The technician verifies the issue by running several copy-and-print tests. Which of the following should the technician do next?

A. Update the printer drivers.
B. Select the correct paper size.
C. Clean the pickup rollers.
D. Replace the toner cartridge.

Answer: C

Explanation:

When a laser printer intermittently fails to feed paper, the most common hardware cause is worn or dirty pickup rollers. These rollers grab the paper from the tray and move it into the printer. Over time, dust, paper debris, or worn rubber reduces their effectiveness, causing feeding issues.

From the CompTIA A+ 220-1101 Official Study Guide, Objective 4.3 – Troubleshoot printing problems:
"If the printer is not picking up paper correctly or is experiencing paper jams, check and clean or replace the pickup rollers and separation pads as these are responsible for feeding paper into the print path."

Other options like updating drivers, selecting paper size, or replacing toner will not resolve a mechanical paper feed problem.

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 4: Troubleshooting Printing Problems

www.atmicnetworks.com

CompTIA Exam Objectives 220-1101, Domain 4.3

Question: 145

Which of the following has the best penetration through physical objects, such as walls?

A. 2.4GHz

B. 5GHz

C. 6GHz

D. NFC

Answer: A

Explanation:

2.4GHz Wi-Fi signals have better penetration through walls and other obstacles compared to 5GHz and 6GHz. Lower frequency waves (like 2.4GHz) travel farther and are less absorbed by physical barriers.

From the CompTIA A+ 220-1101 Official Study Guide, Objective 2.5 – Compare and contrast wireless networking protocols:

"The 2.4GHz frequency band offers greater range and better penetration through walls and obstacles than higher frequencies like 5GHz and 6GHz. Higher frequencies provide faster speeds but are more easily absorbed by walls."

NFC (Near Field Communication) is not a Wi-Fi technology and works only over very short distances (a few centimeters).

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 2: Wireless Networking

CompTIA Exam Objectives 220-1101, Domain 2.5

www.atmicnetworks.com

Question: 146

Which of the following can be used to logically segment networks?

A. MAC

B. VLAN

C. NIC

D. DSL

Answer: B

Explanation:

A VLAN (Virtual Local Area Network) is a network technology used to logically segment a physical network into multiple distinct broadcast domains, even if they share the same hardware.

From the CompTIA A+ 220-1101 Official Study Guide, Objective 2.2 – Compare and contrast common networking hardware:

"VLANs allow network administrators to segment a network logically, isolating broadcast traffic and improving security and management, regardless of the physical network layout."

Other options explained:

MAC (Media Access Control) is a hardware address, not a segmentation method.

NIC (Network Interface Card) is network hardware, not for logical segmentation.

DSL (Digital Subscriber Line) is an internet connection type.

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 2: Networking Concepts

CompTIA Exam Objectives 220-1101, Domain 2.2

Question: 147

After troubleshooting a computer's connectivity, the network team determines there is a portmapping issue. After plugging the patch cable into a different port, the issue persists. Which of the following troubleshooting steps should a technician take next to resolve the issue?

A. Convert the patch cable to a crossover cable.

B. Test the patch cable from the computer to the network closet.

C. Verify the length of the patch cable meets current standards.

D. Replace the patch cable from the device to the wall.

Answer: B

Explanation:

When port issues persist after moving to a different switch port, the next logical troubleshooting step is to test the patch cable. Faulty or damaged cables are a common cause of network connectivity problems. Using a cable tester between the computer and the network closet verifies the integrity of the cable and rules out a physical layer issue.

From CompTIA A+ 220-1101 Official Study Guide, Objective 4.2 – Troubleshoot wired and wireless networks:

"If a device continues to experience connectivity issues after switching ports, test the cabling with a cable tester to check for continuity, shorts, or pinout issues before replacing hardware."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 4: Troubleshooting Network Connectivity

CompTIA Exam Objectives 220-1101, Domain 4.2

Question: 148

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

www.atmicnetworks.com

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 require no configuration they simply need to be plugged in and start working immediately, making them ideal for simple network setups.

Managed switches provide advanced features such as VLANs, SNMP monitoring, port security, and traffic management, but require configuration.

From CompTIA A+ 220-1101 Official Study Guide, Objective 2.2 – Compare and contrast common networking hardware:

"Unmanaged switches operate out of the box with no configuration and are designed for simple connectivity. Managed switches allow for configuration, monitoring, and management of network traffic and security."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 2: Networking Hardware

CompTIA Exam Objectives 220-1101, Domain 2.2

Question: 149

A user is testing a new OS that is contained on a USB drive. The user wants the new OS to load automatically when the computer is turned on. Which of the following should the user configure?

A. BIOS password

B. Trusted Platform Module

C. USB permissions

D. Boot options

Answer: D

Explanation:

To boot from a USB drive, the user must configure the boot order in the system BIOS/UEFI to prioritize the USB device. This setting tells the computer to load the operating system from the USB device on startup.

From CompTIA A+ 220-1101 Official Study Guide, Objective 3.5 – Configure BIOS/UEFI settings:

"The boot order determines the sequence in which the system firmware attempts to find an OS to boot. Setting USB as the first boot device allows the computer to boot from a USB drive."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 3: BIOS/UEFI Configuration

CompTIA Exam Objectives 220-1101, Domain 3.5

Question: 150

A technician is setting up a locally hosted environment for internal developers who need concurrent access to a wide array of test OSs. Which of the following would best fulfill this requirement?

A. Hypervisor

B. SaaS platform

C. Multiboot server computer

D. Sandbox

Answer: A

Explanation:

A hypervisor allows multiple operating systems to run simultaneously on a single physical host, making it the ideal solution for providing concurrent access to different test environments.
Developers can use virtual machines (VMs) for testing and development.

From CompTIA A+ 220-1101 Official Study Guide, Objective 3.7 – Compare and contrast cloud computing concepts:

"A hypervisor is software that enables multiple operating systems to run on a single host as virtual machines. This is commonly used in development and testing environments for flexibility and isolation."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 3: Virtualization

CompTIA Exam Objectives 220-1101, Domain 3.7

Question: 151

An employee's screen keeps flashing. Sometimes the picture goes out and comes back. The employee checks the power cord and confirms the device is plugged in fully. Which of the following should a technician check for first?

A. Loose video cable

B. Failing graphics card

C. Conflicting drivers

D. Swollen motherboard capacitor

Answer: A

Explanation:

Intermittent display issues, such as a screen flashing on and off, are most commonly caused by a loose or faulty video

cable connection. If the power cable is confirmed secure, the next logical step is to check the video (data) cable between the monitor and the computer.

From the CompTIA A+ 220-1101 Official Study Guide, Objective 4.1 – Troubleshoot common hardware problems:

"Common video issues include intermittent display or loss of picture. The most likely causes are a loose or faulty video cable or connector. Check all cable connections before troubleshooting internal components."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 4: Troubleshooting Hardware Problems

CompTIA Exam Objectives 220-1101, Domain 4.1

Question: 152

A user reports that the print quality of their desk printer is poor. A technician replaces the ink cartridge, but this does not resolve the issue. Which of the following should the technician do next?

A. Replace the pickup rollers

B. Clean the printheads

C. Switch the paper type

D. Change the ribbon

Answer: B

Explanation:

If print quality remains poor after replacing the ink cartridge, the next step is to clean the printheads. Printheads can become clogged with dried ink, especially in inkjet printers, causing streaks or faded output.

From the CompTIA A+ 220-1101 Official Study Guide, Objective 4.3 – Troubleshoot printing problems:

www.atmicnetworks.com

"Poor print quality after replacing cartridges is commonly caused by clogged or dirty printheads. Use the printer's cleaning cycle or manually clean the printheads as needed."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 4: Printer Troubleshooting

CompTIA Exam Objectives 220-1101, Domain 4.3

Question: 153

An end user reports that their laptop shuts down when they undock it. Even when using a new charging cable, the issue persists. Which of the following should the technician do next?

A. Flash the BIOS

B. Update the drivers

C. Try a different charger

D. Replace the battery

Answer: D

Explanation:

If a laptop shuts down when undocked and remains powered off even with a new charging cable, the internal battery is likely faulty and cannot hold a charge. Replacing the battery is the next troubleshooting step.

From the CompTIA A+ 220-1101 Official Study Guide, Objective 4.1 – Troubleshoot common hardware problems:

"If a laptop only works when docked or connected to AC power, and a replacement cable does not resolve the issue, the internal battery may need to be replaced."

Verified Source:

CompTIA Exam Objectives 220-1101, Domain 4.1

Question: 154

A company provides cell phones to employees who travel internationally. An employee brings their phone to the help desk so the necessary equipment can be installed. However, the technician cannot install any new hardware on the phone. Which of the following will the technician require so the phone can connect to a different provider?

A. USB-C

B. SD card

C. eSIM

D. MDM

Answer: C

Explanation:

An eSIM (embedded SIM) allows users to change carriers and provision new cellular service without installing any physical hardware. It is managed via software and is ideal for international travelers who need to switch providers quickly.

From the CompTIA A+ 220-1101 Official Study Guide, Objective 3.3 – Install and configure mobile device network connectivity:

"eSIMs provide carrier flexibility by enabling remote provisioning and profile switching, making it possible to connect to different networks without a physical SIM card."

Verified Source:

www.atmicnetworks.com

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 3: Mobile Devices

CompTIA Exam Objectives 220-1101, Domain 3.3

Question: 155

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

Answer: D

Explanation:

Cellular networks offer broad coverage in rural or less populated areas where laying fiber, cable, or DSL lines may not be feasible or cost-effective. Cellular broadband (4G LTE/5G) provides fast speeds using existing mobile network infrastructure.

From CompTIA A+ 220-1101 Official Study Guide, Objective 2.7 – Compare and contrast Internet connection types:

"Cellular connections offer high speed and extensive coverage, especially in areas where other wired infrastructure may not exist or be practical."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 2: Internet Connections

CompTIA Exam Objectives 220-1101, Domain 2.7

www.atmicnetworks.com

Question: 156

Which of the following ports should a technician disable to increase the security of remote connectivity?

A. 22

B. 23

C. 25

D. 53

Answer: B

Explanation:

Port 23 is used by Telnet, an unencrypted remote connection protocol that poses significant security risks. Disabling Telnet and using secure alternatives like SSH (port 22) is best practice.

From CompTIA A+ 220-1101 Official Study Guide, Objective 2.1 – Common ports and protocols:

"Port 23 (Telnet) provides unencrypted remote access and should be disabled to increase security.

Use SSH (port 22) for secure remote connections."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 2: Ports and Protocols

CompTIA Exam Objectives 220-1101, Domain 2.1

Question: 157

A network operations analyst receives an automated alert regarding a server with an array. The analyst walks over to the server and sees a blinking orange light at the hard disk bay. The server is configured for RAID 1. Which of the following should the analyst do to resolve this issue?

www.atmicnetworks.com

A. Change the array to RAID 0.

B. Undo the array and create a new one.

C. Update RAID card firmware.

D. Replace the hard disk and rebuild the array.

Answer: D

Explanation:

A blinking orange light typically indicates a failed hard drive in the RAID array. In RAID 1 (mirroring), you can replace the failed drive and rebuild the array without data loss.

From CompTIA A+ 220-1101 Official Study Guide, Objective 3.4 – RAID configuration and troubleshooting:

"In the event of a hard drive failure in RAID 1, replace the failed disk and allow the array to rebuild using the remaining mirrored disk."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 3: RAID and Storage

CompTIA Exam Objectives 220-1101, Domain 3.4

Question: 158

A technician upgrades a PC with two DIMMs, for a total of 32GB. After installing the two DIMMs, the user notices the OS is reporting only 16GB. Which of the following tasks should the technician perform to resolve the issue in the most rapid, cost-effective way possible?

A. Roll back recent system updates

B. Reinstall RAM in different slots.

C. Update the OS to the latest version

www.atmicnetworks.com

D. Replace the faulty motherboard

Answer: B

Explanation:

If newly installed RAM is not fully recognized, the most likely cause is incorrect installation or incompatible slots. Reseating or reinstalling the RAM modules in the correct slots can quickly resolve the issue without extra cost.

From CompTIA A+ 220-1101 Official Study Guide, Objective 3.2 – Install and configure PC components:

"If memory is not detected, check installation and reseat modules. Ensure they are placed in the correct, matched slots for dual-channel operation."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 3: Memory Installation

CompTIA Exam Objectives 220-1101, Domain 3.2

Question: 159

A company wants to have fast read speeds for its locally stored dat

a. Which of the following configurations has the lowest cost to fulfill this requirement?

A. RAID 0

B. RAID 1

C. RAID 5

D. RAID 10

www.atmicnetworks.com

Answer: A

Explanation:

RAID 0 (striping) provides the fastest read (and write) speeds at the lowest cost, as all disk capacity is used for storage and performance. However, it offers no redundancy.

From CompTIA A+ 220-1101 Official Study Guide, Objective 3.4 – RAID types:

"RAID 0 stripes data across multiple disks, offering the best performance and lowest cost but no fault tolerance."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 3: RAID Levels

CompTIA Exam Objectives 220-1101, Domain 3.4

Question: 160

Which of the following devices has ACL capabilities?

A. PoE injector

B. DSL

C. Firewall

D. Unmanaged switch

Answer: C

Explanation:

Firewalls are specifically designed to monitor, filter, and control network traffic using Access Control Lists (ACLs). ACLs define which traffic is allowed or denied based on parameters like IP address, protocol, or port.

From CompTIA A+ 220-1101 Official Study Guide, Objective 2.2 – Networking hardware and security:

www.atmicnetworks.com

"Firewalls use access control lists (ACLs) to allow or deny traffic based on rules. Unmanaged switches and PoE injectors do not support ACLs."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 2: Networking Security Devices

CompTIA Exam Objectives 220-1101, Domain 2.2

Question: 161

A user would like to connect a laptop to a monitor, keyboard, and mouse when in the office. The user prefers to use as few cables as possible. Which of the following would best achieve that goal?

A. Bluetooth

B. Managed switch

C. Docking station

D. Near-field communication

Answer: C

Explanation:

A docking station allows users to connect multiple peripherals (monitor, keyboard, mouse, etc.) to a laptop with a single connection, reducing cable clutter and improving convenience.

From CompTIA A+ 220-1101 Official Study Guide, Objective 3.1 – Laptop hardware and connections:

"A docking station enables the use of multiple external devices with a laptop using only one or two connections, making it ideal for office environments."

Verified Source:

www.atmicnetworks.com

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 3: Laptop Hardware

CompTIA Exam Objectives 220-1101, Domain 3.1

Question: 162

A user keeps getting an error message when trying to print a letter. The printer is normally used to print cards and invitations. The user tries printing from a different computer, but the issue persists. Which of the following should the user do to resolve the issue?

A. Print fewer pages.

B. Print on card stock

C. Replace the rollers.

D. Change the paper tray setting.

Answer: D

Explanation:

If a printer is set to use a special tray (for cards/invitations) but a different type of print job is attempted (like a letter), a paper tray setting mismatch can cause errors. Changing the tray setting to match the print media resolves the issue.

From CompTIA A+ 220-1101 Official Study Guide, Objective 4.3 – Troubleshooting printers:

"If print jobs fail when media type changes, verify and adjust the paper tray settings to match the required output."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 4: Printer Troubleshooting

CompTIA Exam Objectives 220-1101, Domain 4.3

www.atmicnetworks.com

Question: 163

Which of the following should a company use to implement automatic time synchronization?

A. DHCP

B. UTM

C. NTP

D. AAA

Answer: C

Explanation:

NTP (Network Time Protocol) is specifically designed to synchronize the clocks of networked computers and devices automatically.

From CompTIA A+ 220-1101 Official Study Guide, Objective 2.6 – Network services and protocols:

"NTP is used to automatically synchronize system clocks on network devices, ensuring all systems have accurate time."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 2: Networking Protocols

CompTIA Exam Objectives 220-1101, Domain 2.6

Question: 164

An end user reports that their laptop has a blank screen. A technician observes the keyboard lights are on, and the fan is running. Which of the following should the technician do next?

www.atmicnetworks.com

A. Check the display ribbon cable.

B. Contact vendor support

C. Replace the inverter

D. Connect to an external monitor

Answer: D

Explanation:

When a laptop powers on but the screen is blank, the quickest way to isolate the problem is to connect to an external monitor. This helps determine if the issue is with the laptop display or with the graphics subsystem.

From CompTIA A+ 220-1101 Official Study Guide, Objective 4.1 – Troubleshoot common hardware problems:

"A blank screen on a laptop with power indicators lit should be tested with an external display first to rule out a faulty screen or ribbon cable."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 4: Laptop Display Troubleshooting

CompTIA Exam Objectives 220-1101, Domain 4.1

Question: 165

Which of the following minimizes the time it takes to connect a display, keyboard, mouse, and network cable to a laptop?

A. Lightning interface

B. Port replicator

C. USB hub

www.atmicnetworks.com

D. Bluetooth

Answer: B

Explanation:

A port replicator is designed to allow a user to quickly connect a laptop to multiple peripherals (display, keyboard, mouse, network, etc.) using a single interface, reducing setup time.

From CompTIA A+ 220-1101 Official Study Guide, Objective 3.1 – Laptop hardware and connections:

"Port replicators offer quick connections for multiple peripherals, streamlining the process of docking and undocking a laptop."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 3: Laptop Hardware

CompTIA Exam Objectives 220-1101, Domain 3.1

Question: 166

A multifunction printer in a small office recently had issues with scan-to-email functionality. The manufacturer has an update ready to fix the printer issues. Which of the following would a technician most likely deploy to remediate the issue?

A. Firmware

B. Driver

C. OS update

D. HSM

Answer: A

Explanation:

Firmware is the embedded software on a device such as a printer. Manufacturers often release firmware updates to resolve hardware-specific functionality issues, such as scan-to-email or security vulnerabilities.

From CompTIA A+ 220-1101 Official Study Guide, Objective 3.4 – Printer installation and maintenance:

"Firmware updates provide bug fixes and add new features for multifunction printers. Apply firmware updates to resolve device-specific issues."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 3: Printer Maintenance

CompTIA Exam Objectives 220-1101, Domain 3.4

Question: 167

A technician is setting up a new SOHO wireless router. According to security best practices, which of the following should the technician do first?

A. Enable encryption.

B. Assign a static IP.

C. Change the default password.

D. Reset the router.

Answer: C

Explanation:

The first security step after deploying a new router is to change the default administrative password. Default credentials are well known and pose a security risk if left unchanged.

From CompTIA A+ 220-1101 Official Study Guide, Objective 2.3 – Secure a wireless network:

"Always change default administrative credentials before further configuration to prevent unauthorized access."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 2: Wireless Security

CompTIA Exam Objectives 220-1101, Domain 2.3

Question: 168

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:

PoE (Power over Ethernet) allows both data and electrical power to be delivered over the same Ethernet cable. A PoE injector adds power to Ethernet cables for devices that need it.

From CompTIA A+ 220-1101 Official Study Guide, Objective 2.2 – Networking hardware:

"Power over Ethernet (PoE) technology and PoE injectors enable both power and data transmission to compatible network devices like access points and IP cameras."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 2: Network Hardware

CompTIA Exam Objectives 220-1101, Domain 2.2

Question: 169

A company deploys its infrastructure in self-operated data centers. The company recently migrated some of its applications to a public cloud. Which of the following most accurately describes the cloud model the company is following?

A. Public

B. Hybrid

C. Community

D. Private

Answer: B

Explanation:

A hybrid cloud combines private infrastructure (on-premises, self-operated data centers) with public cloud services, providing flexibility and scalability.

From CompTIA A+ 220-1101 Official Study Guide, Objective 3.7 – Cloud concepts:

"A hybrid cloud model integrates private and public cloud infrastructure to allow applications and data to be shared between them."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 3: Cloud Computing

CompTIA Exam Objectives 220-1101, Domain 3.7

www.atmicnetworks.com

Question: 170

A technician is setting up a new multifunction device to be used over a shared network connection. Copier functions need to be restricted to only office employees. Which of the following should the technician perform after configuring the device to use a print server that exists on the domain?

A. SMTP implementation

B. Firmware update

C. User authentication

D. SMB configuration

Answer: C

Explanation:

User authentication allows access to device functions (like printing and copying) to be restricted to authorized personnel. This is typically implemented on networked multifunction devices for security and auditing.

From CompTIA A+ 220-1101 Official Study Guide, Objective 3.4 – Printer and device security:

"Enable user authentication on shared multifunction devices to restrict access to specific features for authorized users only."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 3: Printer Security

CompTIA Exam Objectives 220-1101, Domain 3.4

Question: 171

A technician observes slow startup times on a laptop. Which of the following is most likely causing the issue?

A. HDD

B. RAM

C. NIC

D. BIOS

Answer: A

Explanation:

A hard disk drive (HDD), especially if it's older or nearly full, is the most common cause of slow startup times in laptops. HDDs are much slower than SSDs and can significantly bottleneck the boot process.

From CompTIA A+ 220-1101 Official Study Guide, Objective 4.1 – Troubleshoot common hardware problems:

"A slow startup or sluggish system performance is commonly due to a failing or fragmented hard disk drive (HDD). Replacing with an SSD can greatly improve boot times and overall system responsiveness."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 4: Troubleshooting PC Hardware

CompTIA Exam Objectives 220-1101, Domain 4.1

Question: 172

Which of the following display technologies typically provides the highest contrast?

A. IPS

B. OLED

C. TN

www.atmicnetworks.com

D. VA

Answer: B

Explanation:

OLED (Organic Light-Emitting Diode) technology can turn off individual pixels completely, producing “true black” and resulting in the highest contrast ratios compared to other display types.

From CompTIA A+ 220-1101 Official Study Guide, Objective 3.1 – Display types and features:

“OLED displays provide superior contrast by emitting light per pixel, allowing perfect black and extremely high contrast ratios.”

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 3: Display Technologies

CompTIA Exam Objectives 220-1101, Domain 3.1

Question: 173

Which of the following types of RAM would most likely be used in a server?

A. SODIMM

B. ECC

C. Unbuffered

D. DDR3

Answer: B

Explanation:

ECC (Error-Correcting Code) RAM is commonly used in servers because it can detect and correct memory errors, providing greater stability and reliability for mission-critical environments.

From CompTIA A+ 220-1101 Official Study Guide, Objective 3.2 – Types of RAM:

"Servers often require ECC memory, which can detect and correct single-bit errors, preventing data corruption and increasing system reliability."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 3: Memory Technologies

CompTIA Exam Objectives 220-1101, Domain 3.2

Question: 174

A company migrates a local application to an internal cloud platform. Which of the following best describes this cloud platform?

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

Answer: A

Explanation:

An internal cloud platform operated exclusively for a single organization is a private cloud, providing dedicated resources and enhanced control.

From CompTIA A+ 220-1101 Official Study Guide, Objective 3.7 – Cloud models:

"A private cloud is provisioned for exclusive use by a single organization, typically managed internally or by a third party, and may be hosted on-premises."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 3: Cloud Concepts

CompTIA Exam Objectives 220-1101, Domain 3.7

Question: 175

A technician sets up secure print and configures an NFC device that will authenticate users for access. Which of the following will the NFC device most likely use to authenticate?

A. Badging

B. Password

C. Passcode

D. Biometrics

Answer: A

Explanation:

Badging refers to the use of NFC-enabled ID badges or cards that authenticate users when tapped against a reader for secure print or access control.

From CompTIA A+ 220-1101 Official Study Guide, Objective 3.4 – Secure printing and authentication:

"NFC authentication is commonly implemented using employee badges, allowing secure and convenient access to devices and functions."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 3: Secure Print Solutions

CompTIA Exam Objectives 220-1101, Domain 3.4

Question: 176

A customer recently lost data due to several unexpected shutdowns. Data integrity is important to the customer. Which of the following features should the technician choose to prevent data loss?

A. Redundant power supply

B. Uninterruptible power supply

C. Modular power supply

D. High-efficiency power supply

Answer: B

Explanation:

An uninterruptible power supply (UPS) protects systems against power outages by providing temporary backup power, giving users time to save data and safely shut down.

From CompTIA A+ 220-1101 Official Study Guide, Objective 3.3 – Power protection:

"A UPS supplies backup power to prevent data loss and hardware damage during outages or surges, ensuring system integrity."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 3: Power Protection

CompTIA Exam Objectives 220-1101, Domain 3.3

www.atmicnetworks.com

Question: 177

Which of the following allows a physical server to host multiple virtual machines?

A. Cross-platform virtualization

B. Hypervisor

C. Sandbox

D. SaaS

Answer: B

Explanation:

A hypervisor is software or firmware that allows multiple operating systems (virtual machines) to run on a single physical host. It manages the allocation of resources and isolation of each VM.

From CompTIA A+ 220-1101 Official Study Guide, Objective 3.7 – Virtualization concepts:

"A hypervisor is the key component of virtualization, enabling a physical server to host multiple virtual machines (VMs), each with its own OS and resources."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 3: Virtualization

CompTIA Exam Objectives 220-1101, Domain 3.7

Question: 178

Which of the following virtualization technologies is best suited for running microservices?

A. Containers

B. VDI

C. Type 2 hypervisors

D. Type 1 hypervisors

Answer: A

Explanation:

Containers provide lightweight virtualization, ideal for deploying microservices because they are isolated, portable, and require fewer resources than traditional VMs.

From CompTIA A+ 220-1101 Official Study Guide, Objective 3.7 – Virtualization and cloud computing:

"Containers package applications and their dependencies, making them ideal for running microservices efficiently and independently."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 3: Cloud and Virtualization

CompTIA Exam Objectives 220-1101, Domain 3.7

Question: 179

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 (Peripheral Component Interconnect Express) is required for high-end video cards.

NVMe (Non-Volatile Memory Express) utilizes the M.2 or PCIe interface for the fastest SSD performance.

From CompTIA A+ 220-1101 Official Study Guide, Objective 3.2 – Motherboard expansion slots and storage interfaces:

"High-end video cards require a PCIe slot, while NVMe drives use M.2 (PCIe) slots for the highest data transfer rates."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 3: Motherboard and Storage

CompTIA Exam Objectives 220-1101, Domain 3.2

Question: 180

A user's phone does not respond to touch. A technician inspects the phone but does not see any evidence of physical damage. The technician restarts the device, which does not fix the issue. Which of the following components should the technician examine next?

A. Battery

B. Screen

C. Stylus

D. Digitizer

Answer: D

Explanation:

The digitizer is the component responsible for detecting touch input on a screen. If touch is not registering and there's no physical damage, the digitizer may be faulty.

From CompTIA A+ 220-1101 Official Study Guide, Objective 3.1 – Mobile device hardware:

"If a touchscreen device does not respond to input and the screen is intact, the digitizer (touch sensor) may be defective."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 3: Mobile Hardware

CompTIA Exam Objectives 220-1101, Domain 3.1

Question: 181

A user can connect their laptop to the internet in the main office. However, when the user places the laptop on top of a motor on the factory floor, there is no internet connectivity. Which of the following is the most likely cause of this issue?

A. Jitter

B. Insufficient power levels

C. External interference

D. High latency

Answer: C

Explanation:

Large electrical motors can emit electromagnetic interference (EMI), which can disrupt wireless signals and prevent connectivity.

From CompTIA A+ 220-1101 Official Study Guide, Objective 2.4 – Wireless troubleshooting:

"Sources of external interference such as motors or other electrical equipment can disrupt wireless network connectivity."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 2: Networking Troubleshooting

CompTIA Exam Objectives 220-1101, Domain 2.4

Question: 182

Which of the following is a characteristic of an NVMe drive?

A. M.2 interface

B. 3.5in (8.9cm) external

C. 7,200rpm

D. Molex connector

Answer: A

Explanation:

NVMe (Non-Volatile Memory Express) drives commonly use the M.2 interface and provide the highest performance for SSDs.

From CompTIA A+ 220-1101 Official Study Guide, Objective 3.2 – Storage devices:

"NVMe drives connect via the M.2 slot and provide the fastest data transfer rates available for storage devices."

Verified Source:

www.atmicnetworks.com

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 3: Storage Technologies

CompTIA Exam Objectives 220-1101, Domain 3.2

Question: 183

Which of the following connector types is associated with coaxial terminations serving cable internet deployments?

A. DB9

B. ST

C. F-type

D. RJ45

Answer: C

Explanation:

F-type connectors are commonly used to terminate coaxial cables in cable internet, cable TV, and satellite connections.

From CompTIA A+ 220-1101 Official Study Guide, Objective 3.1 – Network cables and connectors:

"F-type connectors are used for coaxial cable terminations in cable modem and TV installations."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 3: Networking Cables and Connectors

CompTIA Exam Objectives 220-1101, Domain 3.1

Question: 184

A technician receives several complaints from the same office about VoIP calls sounding broken up, being difficult to hear, and having lagging audio. The technician arrives on-site and runs an internet speed test on several wired and wireless computers. Internet speed seems normal throughout the office. Which of the following should the technician do to fix the call issues?

A. Enable QoS in the router

B. Configure PoE on the switch

C. Change the encryption from WPA3 to WPA2

D. Turn on MAC address filtering

Answer: A

Explanation:

Quality of Service (QoS) prioritizes VoIP traffic on the network, reducing jitter, latency, and packet loss to improve call quality.

From CompTIA A+ 220-1101 Official Study Guide, Objective 2.4 – Network troubleshooting:

"Enabling QoS in the router ensures time-sensitive traffic, like VoIP, receives network priority, reducing dropped or lagging calls."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 2: Network Troubleshooting

CompTIA Exam Objectives 220-1101, Domain 2.4

www.atmicnetworks.com

Question: 185

A technician needs to update a web server's IPv4 address in a DNS server. Which of the following records should the technician update?

A. AAAA

B. MX

C. CNAME

D. A

Answer: D

Explanation:

An A record maps a domain name to an IPv4 address in a DNS server.

From CompTIA A+ 220-1101 Official Study Guide, Objective 2.6 – DNS records:

"A records map hostnames to IPv4 addresses, while AAAA records map to IPv6 addresses."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 2: DNS Records

CompTIA Exam Objectives 220-1101, Domain 2.6

Question: 186

A technician needs to prepare a conference room for a meeting. The technician connects the laptop to the LCD projector and audio system, and then verifies the connectivity of each device. The meeting begins, but the visual presentation suddenly cuts off 30 minutes later. The audio continues to play without interruption. The technician brings in a backup laptop and connects it to the projector. The meeting continues without issue for 15 minutes until the presentation suddenly cuts off again. Which of the following should the technician do to resolve this issue?

A. Check the laptop's audio output

B. Verify the input source

C. Examine the display for burn-in

D. Inspect the cables for damage

E. Clean or replace the filter

Answer: E

Explanation:

Overheating is a common cause of projectors shutting down after extended use. A clogged air filter can cause overheating, resulting in intermittent shutdowns.

From CompTIA A+ 220-1101 Official Study Guide, Objective 4.1 – Troubleshooting displays:

"If a projector shuts down after running for a period, clean or replace the filter to prevent overheating and automatic shutdown."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 4: Display Troubleshooting

CompTIA Exam Objectives 220-1101, Domain 4.1

Question: 187

A technician installs an upgraded wireless access point. The technician then notices the activity light comes on briefly and turns off. The access point continues to exhibit this behavior repeatedly and does not come online. Which of the following is the most likely cause of this issue?

A. High latency

B. Port flapping

C. External interference

www.atmicnetworks.com

D. Channel conflict

Answer: B

Explanation:

Port flapping refers to a network port continuously going up and down, which can prevent the access point from fully coming online.

From CompTIA A+ 220-1101 Official Study Guide, Objective 2.4 – Wired and wireless troubleshooting:

"Repeated loss and restoration of network link is called port flapping and may result in network devices, such as access points, not coming online."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 2: Network Troubleshooting

CompTIA Exam Objectives 220-1101, Domain 2.4

Question: 188

A technician is setting up a workstation. Which of the following settings should the technician configure to ensure that users can connect to the network? (Select three).

A. APIPA

B. Gateway

C. IP address

D. Subnet mask

E. Static routes

F. UPnP settings

G. NAT rules

H. MAC filters

Answer: B,C,D

Explanation:

For a device to communicate on a network, it must have a valid IP address, subnet mask, and default gateway configured.

From CompTIA A+ 220-1101 Official Study Guide, Objective 2.2 – Network configuration:

"A valid IP address, subnet mask, and gateway are required for network connectivity and communication outside the local network."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 2: Network Configuration

CompTIA Exam Objectives 220-1101, Domain 2.2

Question: 189

A major retailer is moving its online shopping website to the cloud and wants to expand its server resources as needed during busier shopping days. Which of the following should the retailer consider?

A. Location

B. Elasticity

C. Availability

D. Multitenancy

Answer: B

Explanation:

Elasticity in cloud computing refers to the ability to automatically scale resources up or down based on demand,

making it ideal for businesses with fluctuating workloads.

From CompTIA A+ 220-1101 Official Study Guide, Objective 3.7 – Cloud characteristics:

"Elasticity allows cloud customers to quickly and automatically scale computing resources in response to changing demand."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 3: Cloud Concepts

CompTIA Exam Objectives 220-1101, Domain 3.7

Question: 190

A network printer does not release a user's final print job from the queue, but the user's other print jobs successfully printed a few moments before. Other users can print without issues. Which of the following should the user check first to solve the issue?

A. If the print job is configured to a tray or manual feed

B. If the computer and printer are connected to the same network

C. If the print queue is full and will not allow additional jobs

D. If the printer has stopped due to empty trays

Answer: A

Explanation:

If only one print job fails and others succeed, it is often due to a paper type or tray selection mismatch for that specific job. If a print job is configured to use a tray that is empty or set to manual feed, it will not be released until resolved.

From CompTIA A+ 220-1101 Official Study Guide, Objective 4.3 – Printer troubleshooting:

"If a specific print job stalls while others succeed, check the job settings for specific tray or paper type configurations that do not match the printer's current setup."

www.atmicnetworks.com

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 4: Printer Troubleshooting

CompTIA Exam Objectives 220-1101, Domain 4.3

Question: 191

A technician is troubleshooting a workstation that repeatedly shuts down within ten minutes of being turned on. The technician notices a loud clicking sound coming from inside the case. Which of

the following components should the technician check first?

A. Exhaust fan

B. Capacitors

C. CPU fan

D. Intake fan

Answer: C

Explanation:

A failing CPU fan may make unusual noises (including clicking) and, if it is not cooling the CPU, the system will quickly overheat and shut down to prevent damage.

From CompTIA A+ 220-1101 Official Study Guide, Objective 4.1 – Troubleshooting hardware problems:

"Overheating due to a failed or obstructed CPU fan can cause frequent shutdowns. Loud noises are a sign the fan should be checked first."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 4: PC Hardware Troubleshooting

www.atmicnetworks.com

CompTIA Exam Objectives 220-1101, Domain 4.1

Question: 192

Which of the following allows for a beam of light to transmit data through a flexible cable?

A. Coaxial

B. HDMI

C. Thunderbolt

D. Single-mode fiber

Answer: D

Explanation:

Single-mode fiber (as well as multi-mode fiber) transmits data using beams of light, allowing for high-speed data transfer over flexible fiber-optic cables.

From CompTIA A+ 220-1101 Official Study Guide, Objective 2.1 – Networking media:

"Fiber optic cables transmit data using light. Single-mode fiber is used for long-distance, high-speed communication."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 2: Networking Media

CompTIA Exam Objectives 220-1101, Domain 2.1

www.atmicnetworks.com

Question: 193

An IT specialist is setting up a new, custom computer. The specialist wants to minimize the number of power cables to keep the internal components organized and uncluttered. Which of the following power supply types should the specialist use?

A. Modular

B. Redundant

C. Linear

D. External

Answer: A

Explanation:

A modular power supply allows the user to connect only the cables needed, reducing clutter and improving organization inside the case.

From CompTIA A+ 220-1101 Official Study Guide, Objective 3.3 – Power supplies:

"Modular power supplies provide detachable cables, allowing users to use only the required connections for a neater build."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 3: Power Supplies

CompTIA Exam Objectives 220-1101, Domain 3.3

www.atmicnetworks.com

Question: 194

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:

A Trusted Platform Module (TPM) is a hardware chip used to enable encryption technologies such as BitLocker, providing secure key storage for system-wide encryption.

From CompTIA A+ 220-1101 Official Study Guide, Objective 3.5 – Security features:

"A TPM chip is required for system encryption, storing encryption keys securely on the hardware."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 3: Security Hardware

CompTIA Exam Objectives 220-1101, Domain 3.5

Question: 195

A company wants to use cloud services with the requirement that data will reside on physical hardware that will not be shared with other companies. Which of the following meets this requirement?

A. Dedicated resources

B. Elasticity

C. Hybrid cloud

D. SaaS

Answer: A

Explanation:

Dedicated resources (sometimes called single-tenant or bare metal) guarantee that physical hardware is allocated exclusively to one customer and not shared.

From CompTIA A+ 220-1101 Official Study Guide, Objective 3.7 – Cloud deployment models:

"Dedicated resources ensure data isolation at the hardware level for compliance and security."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 3: Cloud Deployment

CompTIA Exam Objectives 220-1101, Domain 3.7

Question: 196

A user connects a company-issued laptop to a 4K TV but can only get 1080p resolution on the TV. The technician confirms that the laptop is capable of producing a 4K output. Which of the following is the most likely cause of the issue?

A. The TV firmware is out of date

B. The HDMI cable version is incorrect

C. The laptop firmware is not current

D. The CPU cannot keep up with the transcoding

Answer: B

Explanation:

An older HDMI cable version may not support 4K resolution. For 4K output, both the device and the cable must support HDMI 2.0 or higher.

From CompTIA A+ 220-1101 Official Study Guide, Objective 3.1 – Display troubleshooting:

"Ensure the correct version of HDMI cable is used for high-resolution outputs like 4K. Older cables may be limited to 1080p."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 3: Display and Video

CompTIA Exam Objectives 220-1101, Domain 3.1

Question: 197

Which of the following is an isolated virtual machine?

A. Sandbox

B. Hypervisor

C. Container

D. VDI

Answer: A

Explanation:

A sandbox is an isolated virtual environment, often used for testing code or software safely without affecting the host system.

From CompTIA A+ 220-1101 Official Study Guide, Objective 3.7 – Virtualization:

"A sandbox provides an isolated environment, often implemented as a virtual machine, to safely test applications or code."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 3: Virtualization

CompTIA Exam Objectives 220-1101, Domain 3.7

Question: 198

A user cannot see the office multifunction printer in their laptop's print options. They have printed to the device in the past successfully. The user's laptop is connected to the guest wireless network. Other users on both wireless and wired computers can see and print to the printer. Which of the following will fix the issue?

A. Power cycle the printer to refresh connectivity.

B. Reset the closest wireless AP.

C. Download the printer driver from the manufacturer's website.

D. Connect the laptop to the corporate Wi-Fi.

Answer: D

Explanation:

If the user is on a guest network and cannot access internal resources like printers, connecting to the corporate Wi-Fi will place the device on the correct subnet to access the printer.

From CompTIA A+ 220-1101 Official Study Guide, Objective 2.2 – Network segmentation:

www.atmicnetworks.com

"Guest networks are isolated from internal resources for security. Connect to the main corporate WiFi to access shared devices."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 2: Wireless Networking

CompTIA Exam Objectives 220-1101, Domain 2.2

Question: 199

A technician receives a notification after a network outage that indicates the printer is not reachable. Which of the following printer settings should the technician implement to prevent this issue in the future?

A. Gateway

B. Static IP

C. APIPA

D. DHCP

Answer: B

Explanation:

Assigning a static IP to network printers ensures the printer's address does not change after outages or DHCP lease expirations, preventing connectivity issues.

From CompTIA A+ 220-1101 Official Study Guide, Objective 3.4 – Printer network configuration:

"Printers should use static IPs to ensure they remain reachable and do not change addresses after network events."

Verified Source:

CompTIA Exam Objectives 220-1101, Domain 3.4

Question: 200

Which of the following cloud models allows customers to connect to company resources from their laptops with the least amount of infrastructure?

A. PaaS

B. IaaS

C. SaaS

D. FaaS

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

SaaS (Software as a Service) is a cloud model that allows users to access applications over the Internet without managing the infrastructure or platform. Users can log in via a browser or app on any device, such as a laptop, with minimal configuration required.

Reference: CompTIA A+ Core 1 220-1201 Official Study Guide, Section: Virtualization and Cloud Computing ConceptsSaaS provides "ready-to-use" applications and is ideal for organizations looking to minimize local infrastructure needs.

Question: 201

Employees are concerned about sensitive data being printed on a shared multifunction printer located in a high-traffic hallway. Which of the following should a technician do to address this concern?

www.atmicnetworks.com

A. Set up a PIN for user authentication at the printer
B. Relocate the printer to an unused office space
C. Configure printing of sensitive data through a specific tray
D. Schedule print jobs to be released at certain times

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

PIN printing (also known as secure printing) ensures that documents are held in a queue until the authorized user enters a PIN directly at the printer. This prevents unauthorized viewing of confidential documents.

Reference: CompTIA A+ Core 1 220-1201 Official Study Guide, Section: Printer SecuritySecure printing with PIN authentication ensures only the document owner can release sensitive print jobs.

Question: 202

An office manager wants to block all outbound internet traffic but continue to enable all inbound traffic. Which of the following should a technician configure to achieve this goal?

A. MAC filtering
B. Network interface card
C. Firewall
D. Switch

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

A firewall allows for detailed traffic control, including blocking outbound connections while allowing inbound ones. This is contrary to typical security setups, but it can be configured via advanced firewall rules.

Reference: CompTIA A+ Core 1 220-1201 Official Study Guide, Section: Firewall ConfigurationFirewalls can allow inbound traffic and deny outbound connections based on configured rules.

Question: 203

A thief stole a company phone and successfully extracted confidential company information from the device. Which of the following should have been used to prevent the extraction?

A. GPS

B. EPS

C. eSIM

D. MDM

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

MDM (Mobile Device Management) enforces security policies, such as encryption, remote wipe, and access control. It could have remotely wiped the device or locked it down to prevent data theft.

Reference: CompTIA A+ Core 1 220-1201 Official Study Guide, Section: Mobile Device SecurityMDM tools provide remote

wipe and security policy enforcement, essential for protecting mobile data.

Question: 204

Which of the following RAID configurations can lose two drives without data loss?

A. RAID 0

B. RAID 1

C. RAID 5

D. RAID 6

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

RAID 6 uses two parity blocks, allowing it to tolerate the failure of two drives without losing data.

Reference: CompTIA A+ Core 1 220-1201 Official Study Guide, Section: RAID TypesRAID 6 supports dual-drive failure tolerance with dual parity, making it more fault-tolerant than RAID 5.

Question: 205

An IT support specialist needs to configure several laptops to access local resources wherever the employees are while in the office. Which of the following would best meet this requirement?

A. Configure cellular location services to facilitate device identification

B. Set up a Wi-Fi connection with a common SSID

www.atmicnetworks.com

C. Enable Bluetooth connectivity in all laptops

D. Create roaming profiles for each laptop

Answer: B

Explanation:

Comprehensive and Detailed Explanation (From CompTIA A+ 220-1201 Concepts):

A consistent Wi-Fi SSID across all APs allows users to roam throughout the office while maintaining access to local resources without reconnecting manually.

CompTIA Core 1 Study Guide Concept Reference:

Wireless networking configuration

SSID broadcast and roaming

WLAN infrastructure

The study guide explains that a common SSID enables seamless roaming and uninterrupted access to network resources.

Question: 206

A technician replaces a laptop's failed motherboard. During validation testing, the wireless is slow and shows a weak signal. Which of the following should the technician do first to verify the source of the issue?

A. Contact the manufacturer

B. Reseat antenna connections

C. Restart the access point

D. Install a new wireless adapter

Answer: B

Explanation:

Comprehensive and Detailed

Laptop Wi-Fi antennas run through the display bezel and connect via small coaxial clips. After motherboard replacement, these are often not fully seated, causing weak or unstable Wi-Fi.

CompTIA Concepts:

Laptop hardware troubleshooting

Antenna connector checks after repair

WLAN performance issues caused by antenna misalignment

Question: 207

Which of the following will a company most likely use to control which websites a user can access?

A. Proxy server

B. Spam gateway

C. DHCP server

D. RADIUS server

Answer: A

Explanation:

Comprehensive and Detailed Explanation (100–150 Words):

A proxy server acts as an intermediary between client devices and the internet. One of its primary functions is URL

filtering, web-content restriction, and logging user activity. When a user attempts to connect to a website, the request first goes to the proxy, where filtering rules determine whether the site is allowed or blocked. CompTIA A+ 220-1201 emphasizes that proxies help organizations control outbound traffic, enforce browsing policies, block malicious or inappropriate content, and improve security through caching.

Spam gateways only filter email, DHCP assigns IP addresses, and RADIUS handles authentication, none of which enforce website restriction. Therefore, the correct solution for content control is a proxy server, as stated in the Networking domain of the A+ curriculum.

Question: 208

Which of the following technologies is most used in portable devices?

A. ECC

B. RAID

C. SATA

D. SODIMM

Answer: D

Explanation:

Portable devices such as laptops, small-form-factor computers, and mini-PCs use SODIMM (Small Outline DIMM) memory modules. CompTIA A+ explains that SODIMMs are physically smaller and consume less power than standard DIMMs, making them ideal for mobile systems where space and
energy efficiency are critical. Unlike ECC memory, which is primarily used in servers, or RAID which is a storage redundancy methodology rather than a memory type SODIMM is specifically designed for compact computing devices. SATA is a storage interface, not a memory form factor.

The A+ study guide clearly lists SODIMM as the standard laptop memory type because of its compact footprint and compatibility with mobile motherboard layouts. This makes SODIMM the most widely implemented memory technology in portable devices.

www.atmicnetworks.com

Question: 209

Which of the following is commonly affected by high latency?

A. Satellite

B. Fiber

C. Cable

D. DSL

Answer: A

Explanation:

CompTIA A+ emphasizes that satellite internet connections inherently suffer from extremely high latency because the data must travel from the user's antenna to satellites orbiting tens of thousands of miles above Earth and back. Although satellite systems offer broad geographic coverage, this long travel distance introduces noticeable delays often 500ms or more.

Fiber, cable, and DSL operate through terrestrial wiring and have far lower latency due to short signal paths. Fiber, in particular, is the fastest and lowest-latency connection type.

Satellite delay significantly impacts VoIP calls, video conferencing, online gaming, and real-time applications. The A+ exam specifically notes latency as a major performance characteristic of satellite service, distinguishing it from other broadband technologies.

Question: 210

Which of the following connectors supports High-bandwidth Digital Content Protection (HDCP)?

A. DVI-A

B. F-type

C. VGA

D. DisplayPort

Answer: D

Explanation:

DisplayPort is a fully digital video interface that supports HDCP (High-bandwidth Digital Content Protection), a digital rights-management protocol used to protect copyrighted content such as movies, streaming video, and Blu-ray playback. The CompTIA A+ study guide notes that DisplayPort and HDMI support HDCP, while analog connections like VGA and DVI-A do not support HDCP because analog signals cannot enforce digital content protection.

F-type connectors are used for coaxial cabling (cable TV, satellite), not digital video output. DisplayPort's support for encrypted high-definition video streams makes it the correct answer and aligns with CompTIA's coverage of display connectors and digital content protection technologies.

Question: 211

Which of the following is used to confirm that a physical port is working?

A. Network tap

B. Crimper

C. Patch panel

D. Loopback plug

Answer: D

Explanation:

A loopback plug is a diagnostic tool used to test whether a physical port such as an Ethernet NIC port or serial port is capable of sending and receiving its own signal. When inserted, it "loops" outgoing signals back into the device, confirming the port's transmit/receive functionality.

CompTIA A+ emphasizes loopback plugs as essential tools during hardware and network troubleshooting, especially when isolating physical port or NIC failures.

Network taps passively monitor traffic, crimpers attach RJ45 connectors to cables, and patch panels organize cabling none of these verify port-level functionality. Therefore, only a loopback plug can confirm that a port is working correctly by testing signal integrity and hardware responsiveness.

Question: 212

Which of the following allows an organization to provide remote desktop resources without providing physical workstations to its users?

A. RMM

B. SaaS

C. VDI

D. Containers

Answer: C

Explanation:

Virtual Desktop Infrastructure (VDI) hosts user desktops on centralized servers rather than physical PCs. Users access a virtual desktop session remotely through thin clients, laptops, or web browsers. The CompTIA A+ cloud-computing domain explains that VDI improves manageability, security, and resource efficiency by allowing IT to centralize OS images, apps, and updates.

SaaS provides applications not desktops. RMM is for monitoring and managing devices. Containers virtualize applications, not full desktops.

VDI enables organizations to avoid purchasing physical desktops while still delivering full computing environments to users, which aligns with the A+ virtualization objectives and remote-access concepts.

www.atmicnetworks.com

Question: 213

A student configures a wireless SOHO network to connect four laptops and one multifunction printer. Which setting ensures the printer is always available?

A. Dynamic IPs for laptops, static IP for printer on same subnet

B. Manually assign public IPs to laptops and printer

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

D. Use dynamic IP addressing for all devices

Answer: A

Explanation:

Printers in SOHO environments must maintain a consistent IP address so devices can regularly locate them for scanning and printing tasks. CompTIA A+ emphasizes assigning static IPs to network printers to prevent address changes that occur with DHCP.

Laptops can remain DHCP clients because their address consistency is less critical. APIPA cannot communicate across networks and therefore should not be used. Assigning public IPs is incorrect and unsafe.

By giving the printer a static IP within the same subnet, all laptops can reliably access it, and the network remains organized and functional exactly as the A+ objectives recommend.

Question: 214

A user on the edge of a building reports slow Wi-Fi and intermittent drops. Which action will solve the issue?

A. Enable the 5GHz band

B. Run ipconfig /flushdns

C. Upgrade laptop to Wi-Fi 6 NIC

D. Install additional wireless APs around the location

Answer: D

Explanation:

Wireless coverage issues at the physical edges of a building are typically caused by weak RF signal strength. The CompTIA A+ study material says the best solution is to add additional wireless access points (APs) or implement a mesh system to extend coverage and eliminate dead zones.

Enabling 5GHz often worsens the issue because 5GHz has shorter range. Wi-Fi 6 NIC upgrades improve performance but do not increase signal reach. Flushing DNS does not affect wireless coverage.

Installing more APs ensures stronger coverage, better signal-to-noise ratio, and stable connectivity

aligning with CompTIA's wireless troubleshooting best practices.

Question: 215

A user replaces their PC power supply and connects it to the components, but the PC fails to start. What is the most likely cause?

A. The computer requires additional RAM

B. The wattage is insufficient

C. The 4-pin CPU power connector is not connected

D. The PSU only works in redundant setups

Answer: C

Explanation:

Modern motherboards require both the 24-pin ATX connector and a 4-pin or 8-pin CPU power connector. If the CPU power connector is not attached, the motherboard will receive power but the system will not boot. CompTIA A+ specifically lists this as a common mistake after replacing a power supply.

Insufficient wattage may cause instability, but usually the system still attempts to start. RAM does not prevent power-on if missing; instead, the system produces beep codes. Redundant PSUs are used in servers, not standard desktops.

Therefore, the missing CPU power connector is the most likely cause, and this scenario reflects typical troubleshooting steps outlined in A+ hardware diagnostics.

Question: 216

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, also known as disk mirroring, duplicates data identically to two drives, ensuring full redundancy if one drive fails. Because the workstation only has two drives, RAID 1 is the only RAID level that provides fault tolerance under this constraint, exactly as described in the CompTIA A+ study guide.

RAID 0 offers no redundancy, RAID 5 requires at least three drives, and RAID 10 requires at least four drives.

RAID 1 is the recommended configuration for small environments or workstations that rely on data integrity and quick recovery, matching CompTIA's guidance for redundancy in systems with limited drive availability.

Question: 217

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:

Comprehensive and Detailed Explanation (100–150+ Words):

CompTIA A+ stresses that printers must use static IP addresses to remain consistently reachable on a LAN. When using DHCP, the printer's IP address may change, causing laptops to lose access. By assigning a static IP within the same subnet, the printer becomes a stable, discoverable network resource for all laptops.

Using dynamic IPs for the laptops is perfectly acceptable in SOHO environments, because clients don't require permanent IPs. Assigning public IPs (Option B) is incorrect and unsafe. APIPA (169.254.x.x) does not route and cannot reach the internet or a standard printer. Using dynamic ISP- assigned IPs for all devices (Option D) is also incorrect because ISP routers typically give only one public IP, not multiple internal ones.

Therefore, to ensure the printer is always reachable, the correct configuration is: DHCP for laptops, static IP for printer a best practice detailed in CompTIA's networking and SOHO setup guidelines.

Question: 218

A Wi-Fi router is set up in a central room. A user on the outer edge of the building reports slow connections and intermittent internet drops. Which of the following actions will solve the issue?

A. Enabling the 5GHz band

B. Running the flushdns command

C. Upgrading the laptop to a Wi-Fi 6 NIC

D. Installing additional wireless APs around the location

Answer: D

Explanation:

CompTIA A+ explains that Wi-Fi issues at the edges of a building are typically caused by weak signal coverage, not client configuration. The recommended solution is to add additional wireless access points (APs) or mesh extenders to expand coverage and eliminate dead zones.

Enabling 5GHz would worsen the problem because 5GHz has shorter range and penetrates walls less effectively than 2.4GHz. Flushing DNS affects name resolution, not wireless signal strength.

Upgrading the NIC to Wi-Fi 6 improves maximum throughput but still depends on sufficient signal, which the user does not have.

Additional APs ensure strong signal-to-noise ratio, consistent throughput, and stable roaming all solutions emphasized in the A+ wireless troubleshooting section. Therefore, option D is the correct and CompTIA-aligned fix.

Question: 219

The power supply for a user's gaming PC fails. The user installs a new power supply and connects it to the motherboard, GPU, and SSDs, but the computer will not start. What is the most likely cause?

A. The computer requires more RAM

B. The wattage is insufficient

www.atmicnetworks.com

C. The user did not connect the 4-pin CPU connector

D. The power supply only works in redundant configurations

Answer: C

Explanation:

CompTIA A+ repeatedly highlights that modern motherboards require two power connectors:

The 24-pin ATX main power connector

The 4-pin or 8-pin CPU power connector (EPS connector)

If the CPU power connector is missing, the system will not POST, even though other components appear to have power.

This is a very common mistake after replacing PSUs and is specifically noted in CompTIA materials as a frequent cause of “no boot” scenarios.

Insufficient wattage usually causes instability, not a total failure to start. RAM is unrelated to powering on.

Redundant PSUs are used in servers, not gaming PCs.

Thus, the missing CPU power connector is the correct diagnosis and matches A+ hardware troubleshooting guidelines.

Question: 220

A developer wants to ensure their critical data is protected 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 known as mirroring. It duplicates all data to both drives simultaneously, providing redundancy in the event of a single drive failure. CompTIA A+ teaches that RAID 1 is ideal when reliability is the priority and only two drives are available exactly matching this scenario.

RAID 0 offers no redundancy. RAID 5 requires three or more drives. RAID 10 requires four or more drives.

Since the workstation has only two drives, RAID 1 is the only RAID configuration providing data protection and is heavily featured in CompTIA's coverage of RAID technologies, their requirements, and their purposes in fault tolerance.

Question: 221

A user's laptop keyboard is distorted and no longer flat. Which laptop component most likely failed?

A. Battery
B. RAM
C. Keyboard
D. HDD

Answer: A

Explanation:

CompTIA A+ highlights that swollen or expanding batteries especially lithium-ion batteries can physically warp the laptop chassis, keyboard, or trackpad. This happens when internal chemical reactions cause the battery to swell. Distorted keyboards, bulging trackpads, and lifted chassis panels are classic symptoms of battery failure.

RAM and HDD issues do not cause physical deformation. A broken keyboard may malfunction electronically, but it will not bulge upward unless forced by something underneath typically an expanding battery.

www.atmicnetworks.com

The A+ safety domain also warns technicians not to puncture swollen batteries and to replace them immediately due to fire hazards.

Therefore, a failing (swollen) laptop battery is the most likely cause.

Question: 222

Which storage device is best suited for a high-performance gaming laptop requiring fast data access?

A. 1TB SATA 2.5" HDD

B. 512GB NVMe M.2 SSD

C. 750GB SATA III HDD

D. 1TB SAS SSD

Answer: B

Explanation:

Gaming laptops prioritize speed, low latency, fast read/write times, and quick loading. CompTIA A+ explains that NVMe M.2 SSDs provide the fastest consumer storage available due to their use of the PCIe bus, which delivers significantly higher performance compared to SATA-based drives.

HDDs (Options A and C) are mechanical and have slow seek times, making them unsuitable for high- performance gaming. SAS SSDs (Option D) are enterprise-grade, rarely used in laptops, and require SAS controllers not found in consumer systems.

Thus, a 512GB NVMe M.2 SSD offers the best performance, fastest boot times, rapid texture loading, and optimal gaming responsiveness fully aligning with A+ hardware performance recommendations.

Question: 223

A desktop can connect to a file server but cannot access the internet. The ipconfig /all output shows a correct IP and DNS

www.atmicnetworks.com

but no default gateway. What will most likely restore internet access?

A. Flushing the DNS cache

B. Choosing a different IPv6 address

C. Setting the default gateway

D. Disabling NetBIOS

Answer: C

Explanation:

CompTIA A+ teaches that the default gateway is required for any device to communicate with external networks such as the internet. Without a configured default gateway, the computer can communicate only with devices on the same local subnet explaining why the file server is reachable.

DNS and IPv6 settings are not the issue; without a gateway, external routing cannot occur. Flushing DNS affects hostname resolution, not routing. NetBIOS settings have no effect on internet connectivity.

Adding or correcting the default gateway (usually the router's LAN IP, such as 192.168.1.1) will allow the PC to route traffic beyond its local network.

This aligns precisely with CompTIA's troubleshooting steps for missing or incorrect gateway configuration.

Question: 224

A SOHO user cannot connect to the internet. Their configuration shows:

IP: 192.168.223.15

Mask: 255.255.255.0

Gateway: 192.168.233.1

DNS: 8.8.8.8, 4.2.2.1, 4.2.2.2

Baseline documentation shows valid subnet range: 192.168.200.0–192.168.232.255.

Which setting must be changed?

A. Tertiary DNS
B. Secondary DNS
C. Primary DNS
D. IP Address
E. Gateway
F. Subnet mask

Answer: E

Explanation:

The baseline documentation says the valid network range ends at 192.168.232.255, but the user's gateway is 192.168.233.1, which is outside the permitted network range. CompTIA A+ emphasizes that devices must have a gateway inside their own subnet.

Given a mask of 255.255.255.0, the user's subnet is 192.168.223.x, so the gateway must be in 192.168.223.x, not 192.168.233.x.

DNS settings are public and acceptable. The IP address and subnet mask are valid within the documented address space.

Therefore, the incorrect setting is the gateway, which prevents external routing. Correcting it resolves the connection issue, matching CompTIA's routing and TCP/IP troubleshooting procedures.

Question: 225

A technician checks a RAID 5 array and sees a S.M.A.R.T. alert on one disk, but the array still shows healthy. What should the technician do next?

A. Run chkdsk /f

B. Disable write caching

C. Rebuild the RAID array

D. Replace the failing drive

Answer: D

Explanation:

CompTIA A+ teaches that S.M.A.R.T. warnings indicate imminent drive failure. Even if the RAID controller reports the array as "healthy," a S.M.A.R.T. alert means the drive should be replaced immediately.

RAID 5 provides redundancy for one drive failure, but technicians should replace the degrading drive before it fails fully, ensuring the rebuild happens proactively.

Running chkdsk affects file systems, not drive health. Disabling write caching is unrelated. Rebuilding the array should only occur after replacing the faulty drive.

Replacing the drive prevents a catastrophic dual-drive failure scenario, which RAID 5 cannot survive.

This approach aligns with CompTIA troubleshooting guidelines for RAID maintenance and S.M.A.R.T. diagnostics.

Question: 226

A technician receives complaints that a network fileshare is slow and now unavailable. The server is powered on and accessible via RDP. What should the technician check next?

A. RAID array status

B. Data backup integrity

C. Network connectivity

D. Available memory

Answer: A

Explanation:

A fileshare becoming slow over time and then failing completely strongly suggests storage subsystem degradation, often due to a failing RAID array. CompTIA A+ explains that slow file access is an early sign of a degraded array, and eventual unavailability indicates the array may have failed or entered a critical state.

Since the technician can still RDP into the server, the OS is functioning, meaning memory is likely not the issue. Network connectivity is sufficient for remote login. Backup integrity does not affect real-time file availability.

Thus, the next step is to check the RAID array status, which directly controls the server's storage performance and availability precisely what CompTIA identifies as the primary point of failure in such scenarios.

Question: 227

A company is installing a new shared printer for all employees. Some managers need to print sensitive HR material, and the company does not want to purchase separate printers. Which of the following should the company implement?

A. Audit logging

B. Secure printing

C. Wired connectivity

D. Duplex settings

Answer: B

Explanation:

Comprehensive and Detailed Explanation (100–150+ words):

Secure printing ensures that print jobs are not immediately output to the tray but instead held in a secure queue. The user must enter a PIN, password, or badge authentication directly at the printer to release the job. CompTIA A+ emphasizes secure printing as the correct method for environments where sensitive information such as HR files, performance reviews, or confidential reports must not be viewed by unauthorized individuals.

Audit logging tracks usage but does not protect documents from being seen on the printer tray. Wired connectivity has no relation to security or confidentiality. Duplex is simply a printing mode.

Secure printing is widely used in corporate environments so shared devices can remain shared without compromising sensitive data. The A+ curriculum describes this as a security control that ensures confidentiality in shared-print environments, making Secure Printing the proper solution.

Question: 228

A user's laptop is projecting an image upside down when connected to a ceiling-mounted projector. Which of the following should the technician do to best resolve the issue?

A. Change the input source

B. Rotate the image from the laptop

C. Adjust the display frequency

D. Flip the image vertically from the projector

Answer: D

Explanation:

Ceiling-mounted projectors are typically installed upside down, and therefore include a built-in “Ceiling Mount” or “Vertical Flip” setting within their display menu. CompTIA A+ emphasizes that projectors provide their own orientation controls intended specifically for this installation scenario. Adjusting orientation from the laptop rotates the desktop, not the projected output configuration. Changing input sources does not affect image orientation. Display frequency affects refresh rate and flickering, not physical image rotation.

Flipping the image directly from the projector ensures the display is oriented correctly regardless of the device connected. This is the method recommended in A+ material under display configuration and projector troubleshooting, which covers keystone correction, rotation, and mounting modes.

Thus, the correct solution is to flip the image vertically using the projector’s built-in settings.

Question: 229

Which of the following will most likely be used in a testing environment to execute unauthorized or experimental code without affecting production systems?

A. Virtual machines
B. Hybrid cloud
C. Load balancers
D. Application gateways

Answer: A

Explanation:
CompTIA A+ strongly emphasizes that virtual machines (VMs) are ideal for testing potentially unsafe software, malware samples, or experimental code because they isolate the environment from the host system. VMs allow snapshots, cloning, and rollback functionality, which makes them essential in development, QA, and cybersecurity environments where code might be unstable or harmful.

Hybrid cloud refers to infrastructure strategy, not code execution isolation. Load balancers distribute production traffic but have no testing or sandboxing purpose. Application gateways filter traffic but do not provide execution environments.

Virtual machines create a safe sandbox where failure, infection, or corruption is contained. This is covered in the Virtualization and Cloud Computing domain of the CompTIA A+ exam, making VMs the correct tool for executing unauthorized code safely.

Question: 230

A user experiences intermittent Wi-Fi performance issues only in their office. Nearby RJ45 ports do not provide connectivity, but the user connects fine in other campus areas. AP coverage is weak in the user's office. What is the most likely cause?

A. APs are installed too far from the user's office

B. Brute-force attempts are causing drops

C. Ports near the office are disabled

D. The laptop has malware contacting unauthorized sites

Answer: A

Explanation:

The scenario states that the Wi-Fi signal is weak in the user's office, but the laptop works perfectly in other locations. CompTIA A+ stresses that weak signal strength is caused by distance from the access point, physical obstructions, or poor AP placement. Since other users are not affected and the laptop
works elsewhere, the issue is localized signal weakness.

Disabled RJ45 ports (Option C) matter only for wired connections, and the user relies on Wi-Fi.
Malware (Option D) would affect performance everywhere, not just in one office. Brute-force attacks (Option B) would trigger security logs and affect multiple users.

Weak signal caused by AP distance or line-of-sight issues is the cause, as detailed in A+ wireless troubleshooting procedures related to low RSSI, interference, and AP placement.

Question: 231

An administrator is helping a new employee configure email on a smartphone. The employee also needs access to a shared mailbox. Which is the best email client for this situation?

A. Open-source

B. Built-in

C. Corporate

D. Employee preferred

Answer: C

Explanation:

A corporate-provided email client is designed to integrate with enterprise services such as shared mailboxes, MDM policies, and enterprise authentication. CompTIA A+ states that corporate clients support additional management features, secure authentication protocols (such as OAuth or Kerberos), and policy-enforced access control essential for accessing shared or departmental mailboxes.

Open-source clients (Option A) may lack compatibility with enterprise environments. Built-in smartphone clients (Option B) often don't support complex mailbox structures such as shared mailboxes. Employee-preferred apps (Option D) are discouraged because they may not meet security requirements.

Corporate clients ensure full compatibility with organizational mail servers, shared folders, calendars, and enterprise security features, making corporate email clients the correct choice according to CompTIA's mobile device email configuration standards.

Question: 232

An office manager must scan a 300-page contract quickly. They are worried about scanning each page one at a time. Which feature will speed up the process?

A. Flatbed scanner

B. Duplexing

C. Automatic document feeder

D. Orientation configuration

Answer: C

Explanation:

CompTIA A+ details that an Automatic Document Feeder (ADF) allows multi-page documents to be scanned automatically without manually placing each sheet on the flatbed. This drastically increases scanning efficiency for large documents.

Flatbed scanners require manual placement for every page. Duplexing scans both sides of a page but does not feed multiple sheets by itself. Orientation configuration only affects image alignment.

The ADF is explicitly highlighted in the A+ study guide as the primary feature used in business environments when scanning high-volume documents efficiently.

Thus, the ADF is the correct solution because it automates page feeding and dramatically reduces scanning time, especially for hundreds of pages.

Question: 233

Which DNS record is used by DMARC to verify the authenticity of email servers?

A. MX

B. CNAME

C. TXT

D. A

Answer: C

Explanation:

CompTIA A+ explains that DMARC (Domain-based Message Authentication, Reporting, and Conformance) relies on TXT DNS records to define its policies. TXT records allow administrators to publish arbitrary text-based configuration data, including DKIM and SPF policies, which DMARC references.

MX records identify mail servers, A records map IP addresses, and CNAME records create aliases none are used to store DMARC policy rules.

DMARC improves email authenticity by requiring SPF and DKIM alignment and specifying how receiving servers should handle failed validations. The A+ exam explicitly mentions TXT records as the method used for SPF, DKIM, and

DMARC storage.

Therefore, the correct answer is the TXT record, which stores the policy used by DMARC to authenticate senders and prevent spoofing.

Question: 234

A user reports intermittent Wi-Fi issues in an open office. Other users are not affected. What is the most likely cause?

A. Interference from other Wi-Fi signals

B. All users are on the same frequency

C. The laptop's wireless card is malfunctioning

D. The antenna is near a device creating electromagnetic interference

Answer: C

Explanation:

Since only one user experiences the issue in a shared environment where everyone else has stable connectivity, CompTIA A+ suggests that the problem is most likely with the client device, not the network. The wireless card may be failing, overheating, or experiencing intermittent hardware faults.

If other Wi-Fi signals or EMI (electromagnetic interference) were the cause, multiple users would be affected. Frequency congestion (Option B) also impacts groups, not a single device.

CompTIA stresses that isolating whether the issue affects one user or many helps determine whether the fault lies with the network or device. Because the problem is isolated, the most probable cause is a malfunctioning wireless NIC in the user's laptop.

Question: 235

A user reports that scanned or copied pages from an MFP show vertical lines down the page. The printer processes print jobs correctly. What should the technician do?

A. Replace the transfer roller

B. Remove the pickup rollers

C. Clean the glass bed

D. Apply a maintenance kit

Answer: C

Explanation:

CompTIA A+ teaches that vertical lines on scanned or copied documents but not printed documents indicate a dirty or smudged scanner glass or ADF glass strip. Dust, ink smears, or debris create a line because the scanning sensor repeatedly passes over the same contaminated area.

If printing works normally, internal printer components such as the transfer roller or pickup rollers are not at fault. Maintenance kits apply to internal wear components like rollers, belts, or fusers not scanning artifacts.

Cleaning the scanner glass or ADF strip directly addresses this common problem. The A+ exam frequently includes troubleshooting questions about print vs. scan artifacts, and this scenario is a classic example.

Therefore, the correct solution is to clean the glass bed (or ADF strip).

Question: 236

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

A. Cable

B. Satellite

C. DSL

D. Cellular

E. Ethernet

F. Fiber

www.atmicnetworks.com

Answer: B,D

Explanation:

CompTIA A+ explains that radio frequency (RF) connections use electromagnetic waves instead of copper or optical cabling. Satellite uses RF signals transmitted to and from orbiting satellites, while cellular networks (3G/4G/5G) use RF communications via cell towers.

Cable uses coaxial wired infrastructure, DSL uses telephone lines, Ethernet is twisted-pair copper, and fiber uses light instead of RF.

Satellite and cellular are the only technologies in the list that rely on wireless radio frequency transmission as their medium. The A+ networking domain emphasizes understanding the physical media of WAN technologies and distinguishing wired vs. wireless connectivity, making B and D the correct answers.

Question: 237

A company will retire a legacy application in one year but wants to decommission the physical environment now. Which migration method is best?

A. Relocating the server to a colocated data center

B. Performing a physical-to-virtual conversion and hosting on IaaS

C. Deploying all components using PaaS

D. Taking a backup and shutting down the server

Answer: B

Explanation:

CompTIA A+ emphasizes virtualization as an ideal solution during system phase-out or transition periods. The correct approach here is a P2V (physical-to-virtual) conversion and hosting the server in an Infrastructure as

a Service (IaaS) environment. This removes the need for physical hardware while still keeping the application operational for its final year. IaaS provides full control over OS and applications, making it suitable for legacy systems that cannot be rewritten.

Colocation (Option A) still requires physical hardware. PaaS (Option C) is inappropriate because PaaS requires rewriting or replatforming the application. Shutting down the server after a backup (Option D) makes the application immediately unusable.

Thus, the best method is to convert to a virtual machine and host it on IaaS.

Question: 238

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:

CompTIA A+ explains that Secure Boot is a UEFI security feature that prevents unauthorized or malicious bootloaders, rootkits, and unsigned OS loaders from starting during the boot process. Secure Boot verifies digital signatures on the OS and critical boot files before allowing startup, ensuring the system has not been tampered with.

TPM (Option A) provides encryption key storage and is used for BitLocker, but alone does not block malicious bootloaders. HSMs (Option B) are enterprise cryptographic devices, not PC boot protection features. BIOS passwords (Option D) restrict access to configuration but do not protect against

malicious boot-level malware.

Windows 11 specifically requires Secure Boot, making it the correct protection mechanism for preventing startup-level malware.

Thus, Secure Boot is the proper choice.

Question: 239

A company implements a new policy that prohibits users from installing unapproved applications on corporate tablets.

Which of the following should the technician use to enforce this policy?

A. MDM

B. ACL

C. DRM

D. PAM

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract (Aligned With CompTIA A+ 220-1201 Official Study Guide)

Mobile Device Management (MDM) is the technology used by organizations to centrally configure, secure, and control mobile devices such as smartphones and tablets.

The CompTIA A+ Core 1 (220-1201) objectives specify that MDM solutions allow administrators to implement and enforce security and usage policies, including:

Application control (whitelisting and blacklisting)

Restricting installation of unapproved applications

Enforcing corporate compliance requirements

Remotely managing mobile device configurations

This directly applies to the scenario: the company wants to prevent users from installing unapproved apps on

www.atmicnetworks.com

corporate tablets.

MDM enforces this through:

App whitelisting → only approved apps can be installed

App blacklisting → specific apps are blocked

Locked-down app stores → only corporate-approved app stores or catalogs

This is exactly the function MDM is designed for in enterprise mobile security and management.

Why the Other Options Are Incorrect

B . ACL (Access Control List)

ACLs control network or file-system access, such as allowing or denying IP addresses, ports, or file permissions.

They cannot control app installation behavior on mobile devices.

C . DRM (Digital Rights Management)

DRM protects digital content from unauthorized copying or distribution.

It does not restrict which applications can be installed on a mobile device.

D . PAM (Privileged Access Management)

PAM controls administrative or privileged accounts in enterprise environments.

It is unrelated to app-installation restrictions on tablets.

Question: 240

After a user builds their first PC, the user needs to install the operating system from a USB drive.

Which of the following should the user configure next?

A. BIOS password

B. PXE boot

C. Secure Boot

D. Boot order

www.atmicnetworks.com

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract (Aligned With CompTIA A+ 220-1201 Study Guide)

When installing an operating system from external media (USB flash drive), the motherboard firmware must be instructed to check that device before checking the internal storage.

The CompTIA A+ official objectives describe that technicians must know how to access UEFI/BIOS settings and configure boot priority. Installing an OS from USB requires:

Entering UEFI/BIOS setup

Navigating to the Boot or Startup menu

Setting the USB drive as the first boot device

Saving and exiting to allow the computer to boot from the USB installer

This process is specifically referenced in CompTIA A+ material under "BIOS/UEFI settings," where boot sequence / boot order is a fundamental configuration needed for OS installation.

Thus, the next step after assembling the PC is to modify the boot order to allow the system to boot from the USB installation media.

Why the other options are incorrect

A . BIOS password

Used for system access security; has no relevance to installing an OS from USB.

B . PXE boot

Used for network-based installations, not USB installations.

C . Secure Boot

Controls OS signature validation; not required to be changed for USB installation and is not the next required step.

Final Answer: D

Explanation:

www.atmicnetworks.com

Question: 241

An administrator is configuring a SOHO network. The network scope requires static IP addresses for printers. Which of the following must the administrator set manually? (Select two.)

A. DHCP

B. Subnet mask

C. Default gateway

D. DNS

E. Reservations

F. Exclusions

Answer: B, C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract (Aligned With CompTIA A+ 220-1201 Study Guide)

When assigning a static IP address to a network device such as a printer, the administrator must manually enter all information that a DHCP server would normally provide automatically.

CompTIA A+ networking fundamentals explain that a statically assigned host requires:

IP address (set manually)

Subnet mask (must be manually configured to define the network boundary)

Default gateway (must be manually assigned so the device can communicate outside its subnet)

DNS (also typically required, but in SOHO printer configs, it is not always mandatory unless name resolution is needed)

The question asks specifically: Which must be set manually?

The two required components for every static IP assignment in a CompTIA-compliant small office network are:

✓ B. Subnet mask

www.atmicnetworks.com

Defines the network and host portions of the IP address. Must be manually entered for static IPs.

✓ C. Default gateway

Allows communication outside the local network. Must also be manually set for static IP devices.

Why the other options are incorrect

A . DHCP

Not used in static addressing. DHCP is automatic; static addressing bypasses it.

D . DNS

Not always required for printers unless hostname resolution is needed. The question asks for what must be set manually.

E . Reservations

DHCP reservations create “static-like” addresses via DHCP, not manual configuration.

F . Exclusions

Used to prevent DHCP from assigning certain IPs; not part of configuring a static IP on a device.

Question: 242

Which of the following characteristics differentiates DDR4 RAM from DDR3 RAM?

A. Lower operating voltage

B. Higher latency

C. Increased DIMM width

D. Single-sided modules

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract (Aligned With CompTIA A+ 220-1201 Study Guide)

CompTIA A+ Core 1 memory standards describe the differences between DDR generations. One of the key improvements in DDR4 over DDR3 is reduced operating voltage, which allows lower power consumption and increased efficiency.

DDR3 operates at 1.5V (some variants 1.35V)

DDR4 operates at 1.2V (some variants 1.05V LPDDR4)

This lower voltage is a recognized defining characteristic separating DDR4 from DDR3.

Other differences such as increased speed and internal bank structure exist, but the question specifically asks for the characteristic that differentiates DDR4 from DDR3 — and voltage is the correct, primary distinction used in CompTIA A+ materials.

Why the other options are incorrect

B . Higher latency

DDR4 generally has slightly higher CAS latency numbers, but due to increased speed, real latency is similar. This is not the standard differentiator referenced by CompTIA.

C . Increased DIMM width

DDR3 and DDR4 standard DIMMs both have a 64-bit data width.

D . Single-sided modules

Both DDR3 and DDR4 can be single- or double-sided; not a differentiating factor.

Final Answer: A

Explanation:

Question: 243

A company is separating its accounting department's network from its customer service department's network. Which of the following will accomplish this task?

www.atmicnetworks.com

A. VPN

B. DNS

C. VLAN

D. DHCP

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract (Aligned With CompTIA A+ 220-1201 Study Guide)

CompTIA networking fundamentals describe VLANs (Virtual Local Area Networks) as a method to segment network traffic logically, even while using the same physical switch hardware.

A VLAN allows a company to:

Separate traffic by department

Improve security

Reduce broadcast domains

Control inter-department access

To separate accounting and customer service networks, VLANs are the industry-standard and the CompTIA-approved method.

Why the other options are incorrect

A . VPN – Used for secure remote connections, not internal LAN segmentation.

B . DNS – Resolves hostnames to IPs, not used for network separation.

D . DHCP – Assigns IP addresses; does not isolate network groups.

Final Answer: C

Explanation:

www.atmicnetworks.com

Question: 244

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 nonuser-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: C, D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract (Aligned With CompTIA A+ 220-1201 Study Guide)

To run Secure Boot, the system must have:

✓ UEFI firmware (not legacy BIOS)

Secure Boot is a UEFI feature that validates bootloaders using digitally signed keys stored in secure firmware.

✓ TPM (Trusted Platform Module)

The TPM stores cryptographic keys in tamper-resistant hardware, enabling secure key management that cannot be altered by normal users.

CompTIA materials describe TPM as essential for enhanced platform security and for storing validated boot keys when Secure Boot is enabled.

Together, UEFI + TPM provide:

Verified boot loader

www.atmicnetworks.com

Hardware-level key protection

Prevention of unauthorized OS tampering

Non-user-controllable secure key storage

Why the other options are incorrect

A . VDI – Virtual desktops; unrelated to Secure Boot hardware requirements.

B . BIOS password – Helps protect firmware settings but is not required for Secure Boot.

E . Disabled boot drive – Irrelevant to Secure Boot.

F . USB permissions – Not part of Secure Boot requirements.

Final Answer: C, D

Explanation:

Question: 245

Which of the following is an advantage of using the 2.4 GHz wireless frequency?

A. Communication between devices without external power

B. Security for connections in close proximity

C. Minimized structural interference

D. Increased channel options

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract (Aligned With CompTIA A+ 220-1201 Study Guide)

The CompTIA A+ wireless networking section describes key differences between 2.4 GHz and 5 GHz Wi-Fi frequencies.

www.atmicnetworks.com

2.4 GHz provides:

Better range

Better wall penetration

Better performance through structures and obstacles

This means less interference from physical structures, which is the primary advantage of 2.4 GHz over 5 GHz.

This maps directly to:

✓ C . Minimized structural interference

Why the other options are incorrect

A . Communication without external power

Not related to Wi-Fi frequencies.

B . Security for close-proximity connections

No Wi-Fi frequency provides inherent security advantages.

D . Increased channel options

5 GHz has more channels, not 2.4 GHz.

Question: 246

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

www.atmicnetworks.com

E. ROP

F. LDAP

Answer: B, D

Explanation:

Comprehensive and Detailed Explanation

To enable file sharing across different operating systems, CompTIA A+ emphasizes the use of:

✓ SMB (Server Message Block)

The primary file-sharing protocol used by Windows.

Also supported on macOS and Linux (via Samba).

Allows shared folders, printers, and network browsing.

✓ FTP (File Transfer Protocol)

A cross-platform file transfer service supported by all major OSs.

Commonly used to upload/download files between systems of different types.

These two protocols are explicitly listed in CompTIA objectives under network protocols and file services.

Why the other options are incorrect

A . NTP – Time synchronization, not file sharing.

C . IMAP – Email protocol, not related to file sharing.

E . ROP – Not a file-sharing protocol (Return-Oriented Programming = security exploit).

F . LDAP – Directory service for authentication, not file sharing.

Final Answer: B, D

Explanation:

www.atmicnetworks.com

Question: 247

A user reports that they cannot get their laptop to work with a video projector connected with an HDMI cable. The projector is turned on. The HDMI cable is securely connected on both ends, and the laptop displays properly on its own screen. The display mode is set to "Duplicate" on the laptop.

Which of the following is most likely causing the issue?

A. The projector does not support HDMI connections.

B. The laptop display mode should be set to “Extend”.

C. An HDMI port on the projector failed.

D. The input source is incorrect on the projector.

Answer: D

Explanation:

Comprehensive and Detailed Explanation

CompTIA troubleshooting procedures emphasize confirming input source settings on the external display device.

Even if the HDMI cable is connected properly:

The projector must be set to the correct input source (HDMI 1, HDMI 2, etc.).

If the source is incorrect, the laptop will not display, even though the laptop output is functioning normally.

Since the projector is powered on, and the laptop is already set to “Duplicate,” and cables are good, the most likely cause is:

E. The projector is set to the wrong input source.

This is a common real-world issue covered under "video and projector troubleshooting."

Why the other answers are incorrect

A . Projector may support HDMI; this is not the “most likely.”

B . “Extend” is not required — “Duplicate” works for projectors.

C . A failed HDMI port is possible but not the most likely scenario.

Final Answer: D

Explanation:

Question: 248

Which of the following internet connection types is primarily used for high-speed internet access in rural areas where traditional broadband services are unavailable?

A. Fiber

B. Satellite

C. DSL

D. Cable

Answer: B

Explanation:

Comprehensive and Detailed Explanation

CompTIA A+ describes satellite internet as:

A wireless broadband solution used where wired infrastructure is unavailable.

Most common in rural and remote areas.

Provides high-speed access where DSL, cable, or fiber cannot be deployed.

Thus, satellite internet is the primary option for rural high-speed access.

Why the other answers are incorrect

A . Fiber – Not available in rural regions due to high installation costs.

C . DSL – Requires phone lines and is distance-limited; rarely available in remote areas.

D . Cable – Requires existing cable TV infrastructure; usually not available rurally.

Final Answer: B

Explanation:

Question: 249

A user's laptop keyboard is distorted and is no longer flat. Which of the following components most likely failed?

A. Battery

B. RAM

C. Keyboard

D. HDD

Answer: A

Explanation:

Comprehensive and Detailed Explanation

CompTIA A+ describes swollen or warped laptop chassis components as a classic symptom of a failing or swollen lithium-ion battery.

A swollen battery can:

Warp the keyboard

Push the bottom panel outward

Bend or distort the laptop frame

This is a safety hazard and requires immediate replacement.

Why the other answers are incorrect

B . RAM – Cannot cause physical warping.

C . Keyboard – May fail electronically, but does not physically deform itself.

D . HDD – Located away from the keyboard and cannot distort the chassis.

Final Answer: A

Explanation:

Question: 250

A consultant is assessing the wireless configurations for a small office. The existing equipment uses WEP encryption and operates on the default channel. The office is in a crowded urban area with many nearby networks. Which of the following is the best way to improve the wireless network performance?

A. Replacing the access point

B. Disabling SSID broadcasting

C. Enabling MAC address filtering

D. Updating the firmware

Answer: A

Explanation:

Comprehensive and Detailed Explanation

The wireless environment is crowded, and the office is using:

WEP encryption → obsolete, insecure, and supported only by outdated hardware

Default channel → likely causes interference in a busy area

CompTIA A+ emphasizes:

WEP should be replaced with WPA2 or WPA3

www.atmicnetworks.com

Older APs that only support WEP cannot simply be updated

Newer APs also allow dual-band / multiple channels to avoid interference

Therefore, the best solution is:

✓ Replace the access point with a modern WPA2/WPA3-capable AP that supports improved channel selection.

Why the other options are incorrect

B . Disabling SSID broadcast – Does nothing for performance or security.

C . MAC filtering – Ineffective for performance and easily bypassed.

D . Updating firmware – Cannot upgrade WEP hardware to WPA2/3 if hardware limitations exist.

Final Answer: A

Explanation:

Question: 251

A small company recently added VoIP through its ISP. Users report intermittent call quality issues during peak hours.

Which of the following steps should the IT administrator take to solve the issue?

A. Configure the VLAN to split services.

B. Route calls through a gigabit port.

C. Install a shielded network cable.

D. Increase the VoIP bit rate.

Answer: A

Explanation:

Comprehensive and Detailed Explanation

CompTIA A+ VoIP and network performance topics stress the importance of Quality of Service (QoS) and traffic separation.

Creating a separate VLAN for VoIP:

Reduces congestion

Prioritizes voice traffic

Prevents voice packets from competing with data traffic

Improves latency, jitter, and packet loss issues during peak hours

This directly fixes intermittent VoIP quality issues.

Why the other options are incorrect

B . Route calls through a gigabit port – Internal port speed is not the bottleneck; congestion is.

C . Shielded cable – Does not solve bandwidth or QoS issues.

D . Increase bit rate – Makes the problem worse, requiring more bandwidth.

Question: 252

A customer is using port 110 for email. However, the customer wants to upgrade to a more secure connection that automatically synchronizes with the server. Which of the following should the customer use?

A. IMAP

B. HTTPS

C. SMTP

D. SFTP

Answer: A

Explanation:

Port 110 is used by POP3, a protocol designed for downloading emails from a remote server to a local client. POP3 does not inherently synchronize changes (such as read status, folder organization, or deletions) between devices. The customer wants a more secure connection that automatically synchronizes with the server, which directly aligns with the functions of IMAP (Internet Message Access Protocol).

IMAP typically uses port 143 for unencrypted connections and 993 for secure, encrypted connections (IMAPS). It is designed for modern email usage—supporting multi-device access, live synchronization across clients, and server-stored mail. When a user reads, deletes, or moves an email using IMAP, these changes are reflected on the server and visible on every device logged into the same account.

CompTIA A+ emphasizes that IMAP is preferred for users requiring constant synchronization, mobile access, and cloud-based email management, while POP3 is considered outdated. IMAP also supports secure, encrypted communication when paired with SSL/TLS.

HTTPS and SFTP do not handle email retrieval, and SMTP is a sending protocol, not a retrieval protocol. Therefore, IMAP is the only correct and CompTIA-aligned upgrade option.

Question: 253

A technician must install a printer at a corporate office for all employees to use. Which of the following is the best option?

A. Print server
B. Bluetooth printing
C. Cloud printing
D. Wi-Fi Direct

Answer: A

Explanation:

In a corporate office environment where multiple employees must share a single printer, the most efficient and manageable solution is a print server. A print server centralizes print management, queues print jobs, handles driver distribution, and provides access control. CompTIA A+ highlights print servers as the enterprise-standard method for managing shared printing resources because they ensure reliability, scalability, and better network performance.

Bluetooth printing and Wi-Fi Direct are short-range, peer-to-peer technologies meant for one-to-one or small-scale printing. They lack user authentication management, enterprise security controls, and cannot efficiently support dozens or hundreds of print requests simultaneously. Cloud printing requires internet reliance and external service routing, which introduces latency, potential downtime, and privacy concerns—often unsuitable for corporate networks, especially those with sensitive internal documents.

A print server allows users to connect to the printer through a standard network infrastructure (wired or wireless), and technicians can configure permissions, monitor print loads, and troubleshoot from a central location. It integrates seamlessly with enterprise directory services such as Active Directory, enabling controlled access and auditing. Because of these capabilities, the print server is the best professional-grade solution for corporate-wide printing needs.

Question: 254

Which of the following cable types must be used when running copper network cable through a suspended ceiling that is used for air ventilation?

A. Plenum
B. Multimode
C. Coaxial
D. Twisted pair

Answer: A

Explanation:

When installing copper network cable in spaces that serve as air-handling plenums, safety regulations require the use of plenum-rated cable. Suspended ceilings used for ventilation fall into this category. CompTIA A+ emphasizes that plenum spaces require cable with low-smoke, fireresistant insulation made from specialized materials that limit toxic emissions during combustion.

Plenum-rated cabling (CMP) is designed to meet strict fire codes such as NFPA 70 (National Electrical Code). It prevents smoke-filled ventilation pathways, which could rapidly spread fire or toxic fumes throughout a building. Standard PVC-jacketed twisted pair cables are not permitted in plenum spaces because they produce thick, toxic smoke when burned.

Multimode cable refers to fiber optics, not copper cabling. Coaxial cable is used for broadband and certain RF applications but does not inherently meet plenum safety requirements unless specifically plenum-rated. Twisted pair describes the cable's internal structure (Cat5e, Cat6, etc.), but it does not indicate the type of jacket. Only plenum-rated twisted pair is acceptable.

Therefore, the correct answer is Plenum, as it ensures compliance with safety standards and building codes, prevents hazardous conditions, and aligns with CompTIA best practices for structured cabling installations.

Question: 255

Which of the following DNS records displays the destination of incoming email on a domain?

A. CNAME

B. TXT

C. MX

D. AAAA

Answer: C

Explanation:

DNS contains different record types that serve specific purposes. To determine where incoming email should be delivered for a particular domain, DNS uses an MX (Mail Exchange) record. CompTIA A+ identifies MX records as essential for routing mail from external senders to the appropriate mail server assigned to a domain.

The MX record specifies:

The mail server hostname responsible for receiving messages

Priority values, which determine which server to try first

The server destination for SMTP traffic

When someone sends an email, the sending mail server queries DNS to find the MX record for the recipient's domain. The SMTP server then relays the email to the server listed in that record.

CNAME is used for aliasing hostnames, TXT is used for verification/security (SPF, DKIM), and AAAA maps a hostname to an IPv6 address. None of these direct email delivery. Only MX records are designed to instruct mail servers where to deliver incoming email.

Thus, the correct answer is MX.

Question: 256

A technician upgrades a CPU heat sink with a higher-performing model. While stress testing the computer, the technician finds that the CPU temperatures have drastically increased. Which of the following is most likely causing the issue?

A. Decreased CPU voltage

B. Higher fan RPM

C. Airflow interruption

D. Missing thermal paste

Answer: D

Explanation:

Whenever a CPU heat sink is removed or replaced, thermal paste must be reapplied. Thermal paste fills microscopic gaps between the CPU heat spreader and the heat sink, ensuring efficient heat transfer. Without it, there is a significant air gap, which acts as an insulator, causing CPU temperatures to rise dramatically even under light load. CompTIA A+ stresses thermal compound application as a key step in CPU cooling installation.

The scenario indicates that temperatures increased drastically after upgrading to a better heat sink. A higher-performing heat sink should improve temperatures, not worsen them—unless a critical installation step was missed. Missing thermal paste is the most common cause of this symptom and easily explains the sudden overheating.

Decreased CPU voltage would lower temperatures, not raise them. Higher fan RPM increases cooling efficiency, not reduces it. Airflow interruption is possible but less likely in a simple heat sink upgrade scenario unless the technician installed the CPU cooler incorrectly; however, the most direct and common cause described by CompTIA is

missing thermal paste.

Thus, D is the correct answer.

Question: 257

A technician needs to replace a laptop's display assembly. Which of the following should the technician do to complete this task?

A. Reattach the heat sinks.

B. Reconnect the wireless antennas.

C. Install a new CPU fan.

D. Reset the BIOS to default settings.

Answer: B

Explanation:

Laptop display assemblies typically include not only the LCD panel but also the webcam, microphone, display cable, and critically, the Wi-Fi antennas. In most laptops, Wi-Fi antennas are built into the display bezel, because the elevated position allows for stronger wireless signal reception. When replacing the entire display assembly, the antennas must be carefully disconnected and reconnected during reinstallation.

CompTIA A+ emphasizes proper cable routing and antenna reattachment as essential steps in laptop

hardware disassembly and reassembly. Failing to reconnect these antennas results in weak or nonfunctional wireless connectivity, even though the display replacement itself may be successful.

Heat sinks and CPU fans are located on the motherboard and are unrelated to display assembly replacement. Resetting BIOS settings is unnecessary unless troubleshooting firmware-related issues, not replacing hardware components like a display. Therefore, the only action that aligns with standard laptop design and CompTIA A+ procedures is ensuring that the wireless antennas are reconnected.

Thus, the correct answer is B.

Question: 258

Which of the following best describes a Type 2 hypervisor?

A. It works as a firewall to control network traffic.

B. It interacts directly with the underlying hardware.

C. It runs on a host operating system.

D. It brings higher CPU capabilities to virtual machines.

Answer: C

Explanation:

CompTIA A+ divides hypervisors into two main categories: Type 1 (bare-metal) and Type 2 (hosted).
A Type 2 hypervisor runs on top of an existing host operating system such as Windows, macOS, or Linux. It relies on the host OS for device drivers, hardware interaction, and resource management. Examples include VMware Workstation, Oracle VirtualBox, and Parallels Desktop.

Type 2 hypervisors are ideal for lab environments, testing, learning, and small-scale virtualization because they do not require dedicated hardware or direct hardware control. The host OS loads first, and the hypervisor runs as an application, allowing users to create and manage virtual machines from within the OS environment.

Option B describes a Type 1 hypervisor, which installs directly on hardware without a host OS. Option A is unrelated, as firewalls are separate from virtualization technology. Option D is incorrect because hypervisors do not inherently increase CPU capabilities; they merely allocate existing hardware resources to virtual machines.

Thus, the correct and CompTIA-aligned description of a Type 2 hypervisor is that it runs on a host operating system.

Question: 259

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: B, D

Explanation:

A workstation running three high-end GPUs requires a power supply capable of both high wattage and stable, reliable output. In CompTIA A+ power supply fundamentals, modularity and redundancy are emphasized for high-performance and mission-critical systems.

Modularity (B) allows the technician to connect only the necessary cables, reducing clutter, improving airflow, and enabling proper cable routing to multiple GPUs. High-end graphics cards require multiple PCIe connectors, and modular PSUs provide the flexibility to attach the exact number of required GPU power cables. This is important for systems where space management and cooling efficiency directly affect performance and component longevity.

Redundancy (D) is critical for mission-critical workstations used for 3-D modeling and rendering. A redundant power supply ensures that if one PSU module fails, the system continues running without interruption. CompTIA A+ highlights redundancy as a key feature in professional environments where uptime is essential. These systems typically use dual hot-swappable power modules to guarantee continuous power delivery.

The other options do not meaningfully address the requirements. A 12V output is standard on all PSUs. A 20-pin connector is outdated; modern motherboards use 24-pin. The 3.3V rail is not relevant to GPU loads, and 240 VAC input only refers to wall power compatibility, not PSU capability.

Therefore, modularity and redundancy best meet the workstation's needs.

www.atmicnetworks.com

Question: 260

A shared printer experiences an outage when users submit numerous print jobs at the same time.
Which of the following will an engineer most likely do after verifying network connectivity?

A. Reboot the server.

B. Reinstall the printer drivers.

C. Reset the printer to factory settings.

D. Restart the spooler service.

Answer: D

Explanation:

In networked print environments, print jobs are processed through a system service called the print spooler. CompTIA A+ stresses that when shared printers fail due to job overload, the problem often lies with a hung or overloaded spooler service, especially when multiple jobs are sent simultaneously. The spooler queues, organizes, and processes print jobs; if it becomes overwhelmed or corrupted, printing stops completely even though the network and printer hardware remain functional.

After verifying network connectivity—as the question states— the next logical and CompTIA-aligned troubleshooting step is to restart the spooler service (D). Restarting it clears stuck or corrupt jobs, reinitializes print processing, and restores functionality without requiring a full server reboot or reinstallation of drivers.

Rebooting the server (A) may work but is unnecessarily disruptive and affects multiple services. Reinstalling printer drivers (B) is only warranted for driver corruption issues and is not the first step for spooler congestion. Resetting the printer to factory defaults (C) erases settings and is far too drastic for a simple print queue issue.

Therefore, the most efficient and technically correct action is restarting the print spooler service, restoring printing immediately while maintaining normal server operations.

www.atmicnetworks.com

Question: 261

Which of the following tools will a technician most likely use to identify an unlabeled network connection?

A. Network tap

B. Loopback plug

C. Cable tester

D. Toner probe

Answer: D

Explanation:

To locate or identify an unlabeled network connection, the tool most suited for tracing cables through walls, ceilings, or patch panels is a toner probe (also called a tone generator and probe kit). CompTIA A+ describes this tool as essential for cable identification: the technician attaches the tone generator to one end of the network cable, and the probe detects the signal on the other end, even across long distances or through bundled wiring.

This makes the toner probe ideal for environments where cables are unlabeled, routed through structured cabling systems, or mixed with other wires. It allows the technician to listen for the distinctive tone, confirming the cable's termination point.

A cable tester (C) verifies wiring integrity and pinouts but cannot trace a cable through physical pathways. It is used after identification, not during it. A loopback plug (B) is used for port testing and NIC diagnostics, not cable tracing. A network tap (A) is used for traffic monitoring, security analysis, and packet capture; it does not help locate cables.

Therefore, the toner probe is the correct tool for identifying and tracing an unlabeled network cable, aligning with CompTIA's recommended cable management and troubleshooting procedures.

Question: 262

A healthcare facility is printing government documents on preprinted forms. The output has shifted downward on the paper and the printed data is not aligned with the blank spaces on the forms.

Which of the following should a technician do first?

A. Verify that the correct paper type is loaded into the tray.

B. Make sure that PostScript drivers are being used.

C. Check the orientation settings of the printer.

D. Ensure that the pickup rollers are firmly gripping the paper.

Answer: A

Explanation:

When printing on preprinted forms, precise alignment is critical. If print output shifts downward on the page, the first step is to ensure that the correct paper type and form stock are loaded properly. CompTIA A+ emphasizes verifying media type and tray configuration when dealing with alignment issues, especially in environments using specialized or preformatted paper.

Preprinted forms often require thicker media, specialty settings, or exact tray loading orientation to ensure feeding accuracy. If the wrong paper type is selected on the printer or print driver, the printer may adjust feed rate, roller pressure, or margin expectations incorrectly, causing vertical

misalignment. Thus, confirming the correct paper type is loaded—and that the printer is configured for that type—is the most fundamental starting point.

Orientation settings (C) could affect sideways alignment but not vertical shifting. Pickup rollers (D) can cause skewing or paper jams, but they generally do not cause consistent downward shifts.

PostScript drivers (B) relate to graphic rendering but do not affect form alignment unless dealing with complex images, which is not indicated here.

Therefore, confirming correct paper type and loading aligns with CompTIA's troubleshooting methodology: always check the simplest, most likely physical cause first—especially with form printing.

Question: 263

A computer training institute needs to implement multiple VLANs that must:

- Connect to each other with minimum hardware
- Communicate traffic at wire speed

Which of the following is the most suitable?

A. Web application firewall

B. DDoS appliance

C. Layer 3 switch

D. Router

Answer: C

Explanation:

A Layer 3 switch is the optimal solution when multiple VLANs must intercommunicate while maintaining high performance and minimal hardware complexity. CompTIA A+ explains that Layer 3 switches combine the capabilities of switching (Layer 2) and routing (Layer 3), allowing VLAN traffic to be routed internally at wire speed, without the latency typically associated with traditional

routers.

Layer 3 switches use hardware-based routing, meaning they forward inter-VLAN traffic using ASICs (Application-Specific Integrated Circuits). This allows them to achieve extremely fast throughput, ideal for environments like computer training institutes where multiple VLANs may be used for student labs, instructor networks, and administrative traffic.

A router (D) can route between VLANs but introduces more latency due to software-based routing and typically requires additional equipment. A Web application firewall (A) and DDoS appliance (B) are security devices unrelated to internal VLAN communication.

Because the institute requires minimal hardware and high-speed inter-VLAN communication, the Layer 3 switch is the only CompTIA-supported device that meets both requirements simultaneously.

Question: 264

A technician has built a new computer. On the initial startup, the computer passes POST but will not turn on the operating system. Which of the following components has failed?

A. Audio card

B. CPU

C. Power supply

D. HDD

Answer: D

Explanation:

When a newly built computer successfully passes POST, it indicates that the CPU, RAM, motherboard, video output, and other essential components are functioning at a hardware level. POST will typically fail or display error codes if there are problems with the CPU, RAM, GPU, or power delivery. Therefore, the fact that POST succeeds allows us to eliminate those components from suspicion.

The issue arises after POST, when the system attempts to load an operating system. For the OS to load, the BIOS/UEFI must detect a working storage device—such as an HDD, SSD, or NVMe drive— containing a bootable OS. If the computer cannot locate or read the drive, the system will halt at a boot error, such as “No boot device found,” “Insert boot media,” or similar messages. This is consistent with a failed or improperly connected HDD.

A failed HDD prevents access to boot files, even though the rest of the system hardware functions normally. Audio cards are irrelevant to booting. A failed CPU would cause a POST failure, not an OS loading issue. A faulty power supply would affect system stability during POST, not specifically OS boot failure unless the system is not powering at all.

Thus, the failed component is the HDD.

Question: 265

A user's smartphone frequently disconnects from Wi-Fi networks, particularly in crowded areas like airports and coffee shops. The user also notices that their device shows a lower Wi-Fi signal strength compared to other devices in the same location. Which of the following is likely contributing to the smartphone's Wi-Fi connectivity issues?

A. The smartphone's antenna may be malfunctioning.

B. The smartphone may have an outdated Wi-Fi standard.

C. The smartphone may be experiencing interference from nearby devices.

D. The smartphone's power settings may be affecting performance.

Answer: A

Explanation:

The symptoms clearly point to a hardware-level signal degradation issue, which is most commonly caused by a malfunctioning or damaged Wi-Fi antenna in the smartphone. CompTIA A+ mobile device troubleshooting emphasizes comparing the affected device's signal strength with other nearby devices. In this case, other devices in the same location have stronger Wi-Fi signals, meaning the network itself is functioning normally. The consistent low signal across multiple networks
strongly suggests antenna failure.

Modern smartphones use internal antenna assemblies located along the frame or behind the back cover. If the antenna becomes loose, damaged, or obstructed, the device may show weak or unstable Wi-Fi connectivity, especially in crowded environments where strong, stable reception is required to maintain a connection.

Option B (outdated Wi-Fi standard) would limit speed but not cause significant signal weakness compared to surrounding devices. Option C (interference) affects all devices in an area similarly—not just one device. Option D (power settings) may reduce background activity or scanning frequency, but it does not cause consistently low signal strength.

Therefore, the most likely cause is a malfunctioning Wi-Fi antenna inside the smartphone.

Question: 266

A drive for a RAID 1 array fails. Users are concerned that information could be lost. Which of the following is the best way to manage the situation?

A. Repairing and reinstalling the defective disk to recover any files

B. Discarding the defective disk without further action

C. Replacing the defective disk and syncing the new one so that all files are retained

D. Finding the latest backup of the legacy server and restoring it to transfer the files

Answer: C

Explanation:

A RAID 1 array uses disk mirroring, meaning all data is written identically to two drives. When one drive fails, the other contains a complete, current copy of the data. CompTIA A+ emphasizes that RAID 1 is designed for fault tolerance, allowing continued operation even after a disk failure.

The correct action is to replace the defective drive and allow the RAID controller to rebuild (sync) the mirror onto the new disk. This restores redundancy and ensures ongoing data protection. The system can typically continue running during the rebuild process.

Option A is incorrect because attempting to repair a failed drive is unreliable and unnecessary—RAID 1 already provides a healthy copy. Option B ignores the importance of restoring redundancy, leaving the system vulnerable to data loss if the remaining drive fails. Option D (restore from backup) is unnecessary because RAID 1 already preserves the data.

Therefore, the best solution is to install a new drive and resynchronize the array, preserving all data with minimal disruption.

Question: 267

Which of the following connection methods allows a mobile device to share an LTE connection with other nearby devices?

A. Bluetooth
B. NFC
C. Cellular
D. Hotspot

Answer: D

Explanation:

Mobile devices can share their LTE or cellular data connection using a feature called tethering, more commonly known as hotspot mode. According to CompTIA A+ objectives on mobile networking technologies, a hotspot allows a smartphone or tablet to become a mini wireless router, broadcasting a Wi-Fi signal that nearby devices can connect to. The LTE (or 5G) connection is then shared over Wi-Fi, enabling laptops, tablets, or other phones to access the internet through the mobile device.

Bluetooth is capable of tethering but provides much lower bandwidth and slower speeds—not ideal for sharing LTE widely. NFC is used for close-range data exchange or payment transactions and cannot share internet service. "Cellular" refers to the phone's own mobile network connection, not the mechanism for sharing it with others.

Hotspot functionality is specifically built into modern mobile OSs and supports WPA2/3 encryption,

password protection, and device whitelisting. This makes it the most common and efficient method to share LTE connectivity with multiple nearby devices.

Thus, Hotspot (D) is the correct answer.

Question: 268

Which of the following should a technician create to assign a permanent IP address to a PC using DHCP?

A. Reservation

B. Lease

C. Exclusion

D. Scope option

Answer: A

Explanation:

DHCP normally assigns IP addresses dynamically using timed leases, meaning the address may change after expiration. However, many devices—such as servers, printers, or specialized workstations—require permanent, predictable IP addresses. CompTIA A+ identifies a DHCP reservation as the correct method for assigning a consistent IP while still using DHCP.

A reservation binds a device's MAC address to a specific IP address in the DHCP server. Each time the device requests an address, the DHCP server recognizes the MAC address and issues the same IP. This provides reliability while still allowing centralized management of network addressing.

A lease is temporary and not permanent. An exclusion simply removes certain IP addresses from the assignable pool—it does not assign any device a fixed address. A scope option configures additional network parameters such as DNS, gateway, or WINS settings but does not assign static IPs.

Therefore, a reservation is the correct method to permanently assign an IP address using DHCP without requiring static configuration on the device itself.

Question: 269

A small business is growing and wants to scale its computing capacity. The business wants to continue using on-site equipment until it is EOL. The solution must be able to share data with the local data center. Which of the following models should a technician suggest?

A. Public

B. Community

C. Hybrid

D. Private

E. SaaS

Answer: C

Explanation:

The requirements describe an environment transitioning gradually from on-site hardware to scalable cloud services. The business wishes to continue using its existing local equipment until end of life, while also expanding computing resources beyond what the on-premises infrastructure can handle. Additionally, the cloud environment must be able to share data with the internal data center.

This aligns perfectly with a hybrid cloud model, which CompTIA A+ defines as a combination of private (on-premises) and public cloud resources operating together. Hybrid cloud enables secure data sharing, workload distribution, and scaling without eliminating existing hardware investments. It allows organizations to ofload high-demand processes to the cloud

while maintaining sensitive data or critical services on-site.

A private cloud (D) would not allow scaling into a public provider efficiently. A public cloud (A) replaces internal resources instead of complementing them. A community cloud (B) is shared among organizations with similar compliance requirements—not applicable here. SaaS (E) refers to hosted applications, not infrastructure scalability.

Thus, a Hybrid cloud model fulfills all stated requirements: seamless data sharing, scalable computing, and continued use of on-site equipment.

Question: 270

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:

A hybrid environment combines both on-premises infrastructure and cloud-based resources, allowing virtual machines to operate seamlessly between the two. CompTIA A+ describes hybrid cloud as a deployment model where organizations maintain their own private servers or virtualization hosts while also leveraging public cloud platforms such as AWS, Azure, or Google Cloud. This model supports flexibility, scalability, and gradual migration, making it ideal for businesses not ready to fully abandon local infrastructure.

In this model, workloads can move between the local environment and the cloud depending on performance requirements, cost considerations, or redundancy needs. Additionally, hybrid clouds allow resource sharing, data synchronization, and load balancing across both environments.

A public cloud hosts resources entirely in the provider's data center, offering no on-premises integration. A private cloud exists solely within the organization's infrastructure with no external shared resources. SaaS delivers applications, not infrastructure, meaning it cannot host or manage virtual machines.

Therefore, an environment where VMs exist both on-site and in the cloud is best described as a Hybrid cloud.

www.atmicnetworks.com

Question: 271

A user with a home office wants to add additional devices to the existing internet service while maintaining minimal cost and administration. Which of the following provides the needed functionality?

A. DSL modem

B. Firewall

C. Unmanaged switch

D. Cable modem

Answer: C

Explanation:

To add additional wired network devices in a simple and cost-effective manner, the best solution is an unmanaged switch. CompTIA A+ explains that unmanaged switches require no configuration, provide instant port expansion, and operate using plug-and-play functionality. This makes them ideal for home offices where the user wants more Ethernet ports without dealing with administrative overhead or complex setup.

An unmanaged switch automatically forwards traffic using MAC addresses, expanding the network without altering IP configuration or security settings. It is inexpensive compared to other networking equipment and requires no firmware updates, VLAN management, or routing knowledge.

A DSL modem or cable modem provides internet service but does not increase the number of available network ports beyond the single LAN port commonly offered. A firewall controls traffic but does not expand physical connectivity. Therefore, neither modem nor firewall options meet the requirement of adding more wired devices.

Thus, the unmanaged switch is the simplest, cheapest, and most practical choice for expanding connectivity in a home office environment.

Question: 272

A technician is manually configuring network settings on a user's computer to route network traffic to a newly deployed firewall. Which of the following should the technician change?

A. VPN

B. Gateway

C. Subnet mask

D. VLAN

Answer: B

Explanation:

The default gateway is the network device responsible for routing traffic from a local computer to destinations outside its subnet. When a new firewall is deployed and intended to manage outbound traffic, client devices must be configured to send packets to this firewall. CompTIA A+ identifies the gateway setting as the key parameter that determines where a workstation sends its external-bound traffic.

By updating the gateway address to point to the new firewall's internal interface, all internet-bound and off-subnet traffic will now pass through the firewall for filtering, inspection, and routing. This ensures correct traffic flow and enforces security policies.

Changing the VPN settings (A) does not affect local traffic routing unless a VPN tunnel is active. Subnet mask adjustments (C) determine the network size but do not control routing. VLAN settings (D) require switch configuration, not workstation changes, and do not dictate default routing behavior.

Thus, modifying the gateway is the correct and necessary step to route all traffic through the newly implemented firewall.

Question: 273

Which of the following devices forwards traffic based on MAC addresses?

A. Switch

B. Router

C. Firewall

D. Gateway

Answer: A

Explanation:

A network switch operates at Layer 2 (Data Link Layer) of the OSI model and forwards traffic using MAC addresses. CompTIA A+ teaches that switches maintain a MAC address table, learning which devices reside on each port. When a frame arrives, the switch checks the destination MAC address and forwards it only to the appropriate port, reducing unnecessary traffic and improving performance.

Routers, on the other hand, operate at Layer 3 and forward traffic based on IP addresses, not MAC addresses. Firewalls inspect traffic for security policies and operate across multiple OSI layers but do not perform MAC-based forwarding. A gateway is a broad term that generally refers to a device connecting different networks or protocols, typically involving routing, not MAC-based switching.

Thus, the device specifically responsible for forwarding frames based on MAC address lookup is the switch.

Question: 274

Which of the following will most likely be installed in an NVMe port on the motherboard of a desktop PC?

A. SATA drive

B. Solid-state drive

C. SAS drive

D. Optical drive

Answer: B

Explanation:

An NVMe port, typically implemented through an M.2 slot, is designed specifically for NVMe-based solid-state drives (SSDs). CompTIA A+ explains that NVMe (Non-Volatile Memory Express) is a high- performance storage protocol that communicates directly with the CPU over PCIe lanes, offering significantly faster read/write speeds compared to SATA-based SSDs.

SATA drives (A) connect via SATA ports, not NVMe/M.2 PCIe slots. SAS drives (C) are enterprise-level storage devices requiring SAS controllers and are incompatible with consumer desktop motherboards. Optical drives (D) use SATA or USB interfaces and cannot be installed in an NVMe slot.

Thus, the only device designed for and compatible with an NVMe slot is a solid-state drive (SSD) using the NVMe protocol.

Question: 275

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:
In Wi-Fi, the 2.4GHz band contains 14 total channels (depending on region), but only channels 1, 6, and 11 are considered non-overlapping in most countries. CompTIA A+ highlights the importance of selecting these channels to minimize interference, especially in environments with multiple wireless networks or access points.

The 2.4GHz band is narrower than 5GHz, causing adjacent channels to overlap significantly. Using channels 1, 6, and 11 prevents overlap and reduces signal interference, improving performance and stability.

5GHz (B) has many non-overlapping channels and does not use the 1/6/11 scheme. The 6GHz band (C) is part of Wi-Fi 6E and uses entirely different channel planning. The 60GHz band (D) supports short-range high-speed connections like WiGig, not traditional Wi-Fi channels.

Therefore, the 2.4GHz band is the correct answer.

Question: 276

Which of the following types of RAM is most likely used in data centers and in high-performance machines?

A. ECC

B. Single-channel

C. Unbuffered

D. RDIMM

Answer: A

Explanation:

Data centers and high-performance servers prioritize stability and fault tolerance. CompTIA A+ identifies ECC (Error-Correcting Code) RAM as the standard memory used in such environments. ECC RAM automatically detects and corrects single-bit memory errors, preventing system crashes, data corruption, and downtime—critical requirements for servers running mission-critical workloads.

ECC memory is commonly paired with registered/buffered modules (RDIMM) for additional stability, but ECC itself is the defining feature required in data center environments. Non-ECC, unbuffered memory is used in consumer desktops where minor memory errors pose minimal risk.

Single-channel memory (B) is simply a configuration and does not imply reliability. Unbuffered RAM (C) is not used in enterprise-grade systems because it lacks error correction and electrical stabilization. RDIMM (D) includes buffering but may come with or without ECC; however, ECC is the key requirement highlighted by the question.

Therefore, the correct answer is ECC RAM.

Question: 277

Some users are unable to access their workstations. An administrator runs ipconfig on one of the workstations and sees the following:

IPv4 address! 192.1613.1.27
Subnet mask: 255.255.255.0
Default gateway: 192.169.1.1

The administrator runs the following command and receives this output:

C;XUaptFAlJEer? ping gateway

www.atmicnetworks.com

Pinging gateway <192.168.1.1) with 32 bytes al data:
Request timed out,
Request titled out.
Request timed out.
Request timed out.

Which of the following is the source of issue?

A. Web server
B. Router
C. DNS
D. DHCP

Answer: B

Explanation:

The workstation's IP configuration (192.168.1.27/24 with gateway 192.168.1.1) shows that it has a correct IP address, correct subnet mask, and expected default gateway for a typical small office network. Because the IP is in the correct private range and not an APIPA address (169.254.x.x), this also confirms that DHCP is functioning properly. Therefore, option D (DHCP) cannot be the cause.

The user then pings the default gateway at 192.168.1.1, which should be the router—the device providing routing between local devices and outside networks. The repeated "Request timed out" responses indicate the workstation cannot reach the router at all. This type of failure points directly to a router outage, a powered-off router, a failed router interface, or a physical disconnection of the router from the switch.

If DNS (C) were the issue, the user would still be able to ping the IP address of the gateway because DNS is not required for IP-to-IP connectivity. A web server (A) has no relation to local gateway communication and does not affect workstation access.

Since the workstation has a valid IP but cannot reach its default gateway, the failure point is the router.

Question: 278

Which of the following should a technician check when the display of a computer Is flickering?

A. LCD type

B. Refresh rate

C. Screen resolution

D. Pixel density

Answer: B

Explanation:

Display flickering is most commonly caused by an incorrect or unstable refresh rate setting. The refresh rate is the number of times per second (measured in Hz) that a monitor redraws the image. CompTIA A+ teaches that LCD, LED, and especially older CRT displays can exhibit flickering if the refresh rate is set too low or to a value unsupported by the monitor.

For modern displays, typical refresh rates are 60 Hz, 75 Hz, 120 Hz, 144 Hz, and higher. If the refresh rate is mismatched—such as manually set above the monitor's rated capability—the screen may flicker, blank intermittently, or show instability. Similarly, if the refresh rate is set too low, the user may perceive visible flicker, eye strain, or shimmering on the display.

Checking and adjusting the refresh rate through the operating system's display settings (or GPU control panel) is the first and most direct troubleshooting step for flickering issues.

The LCD type (A) has no bearing on flickering once installed. Screen resolution (C) affects clarity and scaling but does not cause flicker by itself. Pixel density (D) is a hardware characteristic and cannot cause flickering.

Thus, the correct component to check when diagnosing display flicker is the refresh rate.

Question: 279

Marketing department users report network performance degradation in the morning and early afternoon, but sales and customer service department users do not report any issues. All structured cabling Is Cat 5e. All departments are

www.atmicnetworks.com

connected to a core switch. The running network configuration shows the following:

```
Switch#J.'IUA runnltxi-c.'nllg | section interlace
interface ^iqabitEthernetO/1
ip address 192.16B.1.11 255.255.255.0
duplex full
speed 1000
descriptirr - ■=■.=

inter lace giguru lEthex:nclO/2
ip address 92.166.1.12 2 55.2 S'!. 251. c
duplex. Lull
speed ! "'Oil
description CustomerService

i qrerface ST qabi rErhernetO/3
ip addict 192.166.1.13 255.255.255.0
dupl ex s-im
speed uuLu
iescriptinn Marfcetintj
```

Which of the following is the most likely cause of the performance issues?

A. The marketing department subnet has an error.

B. The structured Cat 5e cabling is outdated.

C. The interfaces are configured with Incorrect IP addresses.

D. The marketing department Interface is running at 10/100.

Answer: D

Explanation:

From the configuration, the Sales and Customer Service ports are hard-set to full duplex, 1000 Mbps, while the Marketing interface (GigabitEthernet0/3) is set to duplex auto and speed auto. CompTIA A+ explains that mismatched or lower-negotiated speeds and duplex settings can cause noticeable network slowdowns, collisions, and retransmissions—especially at busy times of the day when utilization is high.

Because all cabling is Cat 5e, it fully supports Gigabit Ethernet, so the cabling is not the limiting factor. The IP addresses are all in the same subnet (192.168.1.0/24) and formatted correctly, so there is no subnet or addressing problem. That rules out options A and C.

With speed auto, the Marketing port may be negotiating only 10/100 Mbps, or even a duplex mismatch (e.g., half duplex vs full). This would severely limit throughput compared to the gigabit links used by the other departments. In peak periods, that slower link would become congested first, which matches the users' reports of performance degradation only in Marketing.

Therefore, the most likely cause is that the Marketing interface is operating at 10/100 instead of 1000 Mbps, making option D correct.

Question: 280

: >i pcor>firj

```
Wireless LAN adapter Wi-Fi:

. •r.recfron-.-.peti f i .* .'NS Suffix . :
Description ......                : Intel(R) Wixeleso-AC 9560 . .   :   7C!H2:7D:74:2?:83
I hysical Address . . , . DHCP    : Yen ;  |7?.n.',|W (Preferred} : 255.255.255.0   :
Enabled ..... :pv4 Address .....  172.17.1.254 ; 172.17.1.1
Subnet HULK .....                 DNS Servers .....  :  9.0.8.S
Default Gateway .... DHCP                            8.8.4.4
Server                            NetBIOS
over TCF/TP                       : Enabled
```

Which of the following is the most likely cause?

A. The subnet mask Is Incorrect.

B. NetBIOS is enabled.

C. DHCP is enabled.

D. DNS servers are manually set.

Answer: D

Explanation:

The key detail in the ipconfig output is that the system is receiving an IP address, subnet mask, default gateway, and DHCP server information via DHCP, but the DNS servers shown are 8.8.8.8 and 8.8.4.4, which are Google's public DNS servers. In most corporate networks, DNS is provided internally by the DHCP server—usually the same device assigning the IP address. When DNS values are different from DHCP-provided defaults, it indicates manual DNS configuration.

CompTIA A+ emphasizes that mismatched DNS settings can cause browsing issues, name-resolution delays, or an inability to access internal resources. DNS is critical because it translates domain names into IP addresses; if manually configured, the device bypasses the organization's DNS server and may not resolve internal hostnames.

The subnet mask is correct for a Class B private network subdivided using /24 (255.255.255.0). NetBIOS being enabled is common and not a cause of connectivity issues here. DHCP being enabled is normal and functioning correctly, as shown by the proper IP lease obtained.

Thus, the anomalous and most likely problematic configuration is manually configured DNS, making Option D correct.

Question: 281

A user receives an error when installing a new email app on their phone. Technician verifies OS is updated and app is supported. What should the technician check next?

A. Storage

B. Battery health

C. SIM card

D. Processor

Answer: A

Explanation:

When an application fails to install on a smartphone despite being supported by the OS and device type, CompTIA A+ stresses that the most common cause is insufficient storage. Mobile devices require not only space for the app itself but also additional temporary space for the installation

process, cached data, and updates. If internal storage is nearly full, the app store will display installation errors—even if the OS and hardware meet requirements.

Battery health has no impact on app installation. A SIM card is unrelated to installing local applications—it only affects cellular connectivity. Processor architecture issues would have been caught during compatibility checking, but the technician already verified the device supports the application.

Therefore, after confirming compatibility, the next logical step is to check available storage space. If storage is low, deleting unused apps, clearing cached data, or transferring media to cloud storage or an SD card typically resolves the installation issue.

Thus, Option A: Storage is the correct answer.

Question: 282

Which internet connection type will most likely experience interference from rain?

A. Fiber

B. Cable

C. Satellite

D. DSL

Answer: C

Explanation:

CompTIA A+ identifies satellite internet as the connection type most susceptible to weather-related interference, particularly rain, snow, and heavy cloud cover. This phenomenon is known as rain fade. Satellite connections rely on high-frequency microwave signals transmitted between a dish antenna at the customer site and an orbiting satellite. Moisture in the atmosphere absorbs and scatters these signals, causing latency spikes, reduced bandwidth, or complete signal loss during storms.

Fiber (A) uses light signals through glass fiber and is immune to electromagnetic and weather interference. Cable internet (B) uses shielded coaxial lines buried or run overhead, but rain does not affect signal quality in normal conditions. DSL (D) uses telephone lines, which may degrade with physical line issues, but not directly due to rain in the same way satellite is affected.

Thus, satellite internet is most likely to experience signal degradation during rain conditions.

Question: 283

While using a laptop and Bluetooth headset for conference calls, a user notices intermittent sound issues. The user frequently walks between office rooms during calls, leaving the laptop in place. The office network uses fiber internet and has two connected APs. What is the MOST likely cause?

A. The number of available APs is inadequate.

B. The user is moving in and out of range.

C. The APs are not in mesh mode.

D. The internet connection is too slow.

Answer: B

Explanation:

Bluetooth audio issues are typically related to distance and signal strength, not internet connectivity or Wi-Fi access points. Bluetooth devices—especially headsets—generally have a limited effective range of around 10 meters (33 feet) for Class 2 Bluetooth, which is common in consumer laptops and headsets. When the user leaves the room and walks into adjacent offices, they are likely moving beyond the optimal Bluetooth range or passing through walls that weaken the signal.

CompTIA A+ highlights that Bluetooth uses low-power radio frequencies easily disrupted by physical obstructions, distance, and interference. Since the laptop remains stationary and the user moves, the headset becomes progressively further from the laptop, causing intermittent audio dropouts, stuttering, or loss of connection.

The number of APs (A) is irrelevant because the headset is not using Wi-Fi. Mesh mode (C) applies only to wireless AP-to-AP communication. The internet connection (D) is high-quality fiber and

conference calls work fine when stationary, so the issue is not bandwidth or WAN throughput.

Thus, the most likely cause is that the user is moving in and out of Bluetooth range.

Question: 284

A company wants to enable access to corporate email on smartphones. Employees must install software that

separates corporate and personal dat

a. Which should the company implement?

A. Encryption

B. Network access control

C. Mobile device management

D. Endpoint protection

Answer: C

Explanation:

The requirement to separate corporate and personal data on employee smartphones is a core function of Mobile Device Management (MDM). CompTIA A+ describes MDM as an enterprise toolset used to enforce security policies, manage applications, configure email profiles, and separate work-related data from personal user data. This separation is typically achieved through features such as containerization, where corporate data is stored in a protected, encrypted workspace that is isolated from the personal side of the device.

This ensures security, prevents data leakage, and enables IT administrators to remotely wipe corporate data without affecting the user's personal information. MDM solutions are widely used in BYOD (Bring Your Own Device) environments and corporate-issued devices.

Encryption (A) protects data but does not create separation. Network access control (B) restricts network access but does not manage mobile apps or data separation. Endpoint protection (D) refers to antivirus/antimalware, not data partitioning.

Thus, Mobile Device Management (MDM) is the correct solution.

Question: 285

A technician installs an external camera on a user's laptop. When loading meeting software, the video preview shows a blank screen. What should the technician do next?

A. Select the correct camera source.

B. Replace the camera.

C. Update the camera software.

D. Check the camera cable.

Answer: A

Explanation:

Most meeting or conferencing applications default to the built-in laptop camera unless manually changed. When an external camera is connected, the software may continue to use the default device, resulting in a blank preview, especially if the internal camera is disabled, covered, or malfunctioning. CompTIA A+ stresses verifying correct device selection when peripherals are installed.

Selecting the correct camera source is a quick, non-invasive test that resolves the issue in the majority of cases. The technician should open the application's video settings and choose the external webcam from the camera dropdown menu.

Replacing the camera (B) is premature without confirming configuration. Updating software (C) is beneficial but will not resolve a simple input-selection error. Checking the cable (D) is a valid step if the preview still fails after selecting the device.

Thus, the correct next step is to select the proper camera source.

Question: 286

Which cloud characteristic allows local folders to contain updates made by users or other devices?

A. Network share

B. Synchronization

C. Availability

D. Metered utilization

www.atmicnetworks.com

Answer: B

Explanation:

Cloud storage platforms—such as OneDrive, Google Drive, and Dropbox—use synchronization to ensure that files updated on one device automatically update on all connected devices. CompTIA A+ defines synchronization as a key cloud characteristic that keeps local folders and cloud-stored versions consistent, enabling seamless multi-device collaboration.

Synchronization allows users to:

Modify files ofline and have them sync once online

Access identical data on laptops, desktops, and mobile devices

Ensure real-time updates across multiple users or clients

Maintain version consistency and conflict resolution

A network share (A) is local to an organization and does not automatically sync across devices. Availability (C) relates to uptime and reliability, not file updates. Metered utilization (D) refers to cloud billing models where usage is tracked, not data syncing.

Thus, synchronization is the capability that ensures local folders update dynamically whenever changes occur.

Question: 287

Which of the following offers access to business productivity applications for a recurring fee?

A. SaaS

B. DaaS

C. PaaS

D. IaaS

Answer: A

Explanation:

Software as a Service (SaaS) provides users access to fully managed applications hosted in the cloud. CompTIA A+ explains that SaaS is subscription-based and typically billed monthly or annually, which aligns perfectly with the phrase "recurring fee." Business productivity applications—such as Microsoft 365, Google Workspace, Zoom, Slack, and Salesforce—are classic examples of SaaS offerings.

SaaS applications run entirely in the provider's cloud environment, eliminating the need for installation, maintenance, or management by the customer. This makes SaaS ideal for businesses that need reliable, scalable tools without maintaining their own infrastructure.

DaaS (Desktop as a Service) provides virtual desktops.

PaaS (Platform as a Service) offers a development framework for building applications.

IaaS (Infrastructure as a Service) provides virtual servers, storage, and networking—not end-user productivity apps.

Thus, SaaS is the correct and only model that matches the description of subscription-based access to productivity applications.

Question: 288

A software developer wants to test a new application in an environment that limits access to the OS. Which of the following should the developer implement?

A. Container

B. Type 2 hypervisor

C. VDI

D. Quarantined PC

Answer: A

Explanation:

A container is the ideal environment for software testing when access to the underlying operating system must be restricted. CompTIA A+ explains that containers isolate applications from the host OS by packaging the app and all its dependencies into a controlled environment. This prevents the application from modifying or interfering with the host system and ensures predictable, consistent behavior across environments.

Unlike virtual machines, containers do not include a full OS installation; they share the host OS kernel but run in isolated user-space environments. This makes them lightweight, fast to deploy, and secure—perfect for developers testing new or potentially unstable applications.

A Type 2 hypervisor hosts full virtual machines but does not inherently limit OS access. A VDI provides remote desktops but is not designed for controlled application testing. A quarantined PC is used for isolating infected or suspicious systems, not structured development testing.

Thus, containers provide the controlled, restricted environment required.

Question: 289

A user cannot access the internet from a corporate laptop. All other employees can. The technician reviews the laptop's configuration:

IP Address: 169.254.2.162

Which explains the reason the user cannot access the internet?

A. The subnet mask is misconfigured.

B. The NIC is not using the latest driver.

C. Network settings are only configured to IPv6.

D. The DHCP server is unable to assign an address.

Answer: D

Explanation:

An IP address beginning with 169.254.x.x is an APIPA address (Automatic Private IP Addressing). CompTIA A+ explains that APIPA is assigned automatically by Windows when the NIC cannot reach a DHCP server. This indicates the laptop requested an IP lease but never received one.

APIPA addresses allow only local subnet communication and cannot access the internet, because no default gateway, DNS, or valid subnet configuration is provided. Since all other employees can access the internet, the DHCP server is functioning generally, but it is not delivering an address to this specific laptop—possibly due to cable issues, Wi-Fi authentication failure, DHCP scope exhaustion, or NIC misconfiguration.

A subnet mask misconfiguration (A) would still show a normal IP, not APIPA. IPv6-only configuration (C) would not

www.atmicnetworks.com

produce a 169.254 address. An outdated NIC driver (B) could cause network instability but does not directly generate APIPA.

Thus, the root cause is that the DHCP server did not assign an IP address.

Question: 290

Which cloud model provides hardware, storage, networking, and virtualization but requires customers to manage the OS and applications?

A. SaaS

B. PaaS

C. IaaS

D. XaaS

Answer: C

Explanation:

Infrastructure as a Service (IaaS) provides the foundational computing components: virtualized hardware, storage, networking, and hypervisor resources. CompTIA A+ explains that customers using IaaS are responsible for installing and maintaining:

The operating system

Applications

Patches, updates, and configurations

This model gives organizations maximum flexibility because they can build custom server environments without purchasing physical hardware.

In contrast:

SaaS (A) provides fully managed applications—users do not manage OS or software.

PaaS (B) provides a development platform and tools but does not allow OS management.

XaaS (D) is a broad term meaning "anything as a service," not a specific model.

Thus, IaaS is the only model where OS-level control remains with the customer.

Question: 291

A human resources manager printed a sensitive termination document and forgot to retrieve it from the printer. Which of the following prevents this situation?

A. Badging

B. Duplex

C. Printer share

D. Wireless encryption

Answer: A

Explanation:

Secure badging—often used with "pull printing" or "secure print release"—requires users to authenticate at the printer before documents are printed. CompTIA A+ highlights this feature as critical for protecting sensitive data in corporate environments. With badge-based printing, jobs stay in a secure print queue until the authorized user physically scans their badge.

This prevents confidential documents, like HR termination notices, from sitting unattended in the output tray. It also reduces print waste and ensures accountability for printed materials.

Duplex printing (B) simply prints double-sided pages. Printer sharing (C) allows multiple users to use a printer but does not provide security. Wireless encryption (D) protects network traffic but does not address abandoned print jobs.

Therefore, badging / secure print release is the correct protective measure.

Question: 292

A user ran out of USB ports on their laptop but wants to plug in more devices. What technology is best?

A. Near-field communication

B. Bluetooth

C. USB receiver

D. Port replicator

Answer: D

Explanation:

A port replicator expands the number and types of ports available to a laptop, including additional USB ports, video outputs, Ethernet, and more. CompTIA A+ identifies port replicators as solutions for users needing greater connectivity, especially when docking stations are unnecessary or unavailable.

Port replicators connect through a single USB or proprietary connector and provide multiple expansion ports instantly. This resolves the issue of limited USB availability without requiring hardware replacement.

NFC (A) is used for short-range communication, not peripheral connectivity. Bluetooth (B) only supports wireless peripherals such as mice and headphones, not wired USB devices. A USB receiver (C) adds wireless capability for one specific device, not general expansion.

Thus, the correct solution is a port replicator.

Question: 293

Which connector is used to uplink a new ISP cable modem to its wall jack?

A. F-type

B. LC

C. RJ45

D. Lightning

Answer: A

Explanation:

Cable modems supplied by ISPs connect to the coaxial wall outlet using an F-type connector. CompTIA A+ specifies that F-type connectors are threaded coaxial connectors used in broadband cable internet, cable TV, and some satellite systems. They attach to RG-6 or RG-59 coaxial cable and provide a secure, shielded connection to the cable provider's infrastructure.

The cable modem requires this coaxial uplink to receive downstream and upstream signals from the

ISP before converting them into Ethernet on the LAN side.

LC (B) is for fiber optic connectors, not coaxial. RJ45 (C) is an Ethernet connector and is used on the LAN side of the modem—not on the wall uplink. Lightning (D) is an Apple connector and irrelevant to networking hardware.

Thus, the correct connector for the ISP cable modem uplink is F-type.

Question: 294

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

www.atmicnetworks.com

Answer: B, F

Explanation:

When troubleshooting intermittent latency to a remote internal resource, CompTIA A+ recommends using tools that help identify where latency occurs and whether it is consistent or fluctuating over time. The best tools for this scenario are ping -t and tracert.

Ping -t (B) sends continuous ICMP echo requests, allowing the technician to observe packet loss, fluctuating response times, or timeouts. This helps identify intermittent connectivity problems that occur at specific times, such as bandwidth congestion, routing instability, or wireless interference.

Tracert (F) maps each hop between the local workstation and the remote office. If latency spikes occur only after a particular hop—such as a VPN tunnel, MPLS gateway, or inter-office router—that device becomes the suspected bottleneck. This makes tracert essential for isolating WAN-related slowdowns.

Ipconfig /all (A) only provides local configuration and does not diagnose latency. Nslookup (C) is for DNS testing—not latency to a specific internal host. Examining switchports (D) helps with local issues but not remote latency. QoS (E) is a solution, not a troubleshooting step. Calling ISP (G) may be premature unless testing confirms ISP-related issues.

Thus, ping -t and tracert are the correct diagnostic tools.

Question: 295

A customer has bare-metal servers running Windows, Linux, and Unix. They want consolidation while maintaining isolation and compatibility. What should the technician recommend?

A. IaaS

B. Containers

C. Type 2 hypervisor

D. VDI

Answer: A

Explanation:

The customer wants to consolidate multiple physical servers running different operating systems, including Windows, Linux, and Unix, while maintaining strong isolation between systems. CompTIA A+ identifies Infrastructure as a Service (IaaS) as the best model for hosting fully isolated virtual machines in a cloud environment, allowing each OS to run independently on its own virtual hardware.

IaaS provides virtualized computing resources—CPU, RAM, networking, and storage—while allowing the customer full control over the OS and application layer. This means Windows, Linux, and Unix VMs can coexist without compatibility concerns because each VM runs its native OS without

modification.

Containers (B) are unsuitable because they share the host OS kernel, meaning they cannot run different OS families. A Type 2 hypervisor (C) is workstation-based and not designed for enterprise server consolidation. VDI (D) provides user desktops, not server workload consolidation.

Thus, IaaS is the correct solution for compatibility, isolation, and consolidation across multiple OS types.

Question: 296

Which RAID type offers double parity?

A. RAID 0

B. RAID 1

C. RAID 5

D. RAID 6

Answer: D

Explanation:

www.atmicnetworks.com

CompTIA A+ teaches that RAID 6 is the RAID level that uses double parity, allowing the array to survive the failure of two drives simultaneously. RAID 6 stripes data across all disks like RAID 5 but stores two independent sets of parity information, making it far more fault-tolerant.

RAID 0 has no parity and provides only performance. RAID 1 mirrors data but uses no parity. RAID 5 uses single parity and can tolerate only one disk failure. Because the question explicitly asks for double parity, only RAID 6 is correct.

Question: 297

A user reports cursor issues on a company laptop. Technician finds a bulge under the trackpad. Which component should be replaced first?

A. Motherboard

B. Heat sink

C. Battery

D. Trackpad

Answer: C

Explanation:

A physical bulge under the trackpad is a classic CompTIA-identified symptom of a swollen lithium-ion battery. As batteries degrade, internal gas buildup expands the casing, pushing upward on the laptop chassis—often distorting the trackpad, keyboard, or bottom shell. This can cause cursor issues, clicking problems, and safety hazards.

Replacing the battery first is essential because swollen batteries can rupture, leak, or ignite. Only after the battery is removed and replaced should the technician evaluate whether the trackpad suffered permanent damage.

Replacing the trackpad (D) without addressing the battery fails to correct the root cause. The motherboard (A) and heat sink (B) are unrelated to the physical bulge.

Thus, the correct first step is replacing the battery.

www.atmicnetworks.com

Question: 298

A user wants scan-to-email functionality on a printer. Which protocol is required?

A. SMS

B. SMTP

C. SFTP

D. SMB

Answer: B

Explanation:

Scan-to-email functions rely on the printer sending scanned documents to an email server. CompTIA A+ identifies SMTP (Simple Mail Transfer Protocol) as the protocol responsible for sending email messages from clients to mail servers.

When configuring scan-to-email, the technician must enter:

SMTP server address

Authentication credentials

Port number (25, 465, or 587)

Encryption type (TLS/SSL)

Without SMTP, the printer cannot transmit emails.

SMS (A) refers to text messaging. SFTP (C) is secure file transfer, common for scan-to-folder workflows, not email. SMB (D) is used for Windows file sharing.

Therefore, the correct protocol is SMTP.

www.atmicnetworks.com

Question: 299

An engineer must implement a solution to facilitate and maintain an organization's legacy application until it is retired. The application is currently hosted on three physical servers. Which of the following is the most suitable concept?

A. SAN

B. FaaS

C. Virtualization

D. Configuration management platform

Answer: C

Explanation:

When a legacy application is running on multiple physical servers, and the organization wants to maintain it until retirement, the best CompTIA-aligned solution is virtualization. Virtualization allows the engineer to convert existing physical servers into virtual machines (VMs), a process known as P2V (Physical-to-Virtual) migration. This reduces hardware footprint, simplifies management, and isolates the application within a controlled environment. CompTIA A+ emphasizes virtualization for legacy support because it eliminates dependence on aging physical hardware while preserving application functionality exactly as before.

Virtual machines also provide snapshots, backups, failover capabilities, and easier resource allocation, making them more reliable than maintaining old hardware. A SAN (A) provides storage, not application hosting. FaaS (B) is a serverless model inappropriate for legacy applications that require full OS environments. A configuration management platform (D) manages software deployments and settings but does not replace or consolidate physical servers.

Thus, virtualization is the most suitable and industry-standard method for sustaining legacy applications.

Question: 300

A company wants to migrate a large amount of data from an on-premises server to a cloud provider. Which connection type is most likely the fastest?

A. Coaxial

B. DSL

C. Fiber

D. SAN

Answer: C

Explanation:

When migrating large volumes of data to a cloud provider, CompTIA A+ notes that the transfer speed is dominated by the WAN (internet) connection speed. Among the given options, fiber-optic internet (C) provides the highest upload and download throughput, often delivering speeds from 1 Gbps to 10 Gbps or more, depending on the service. Fiber supports symmetrical upload speeds, which is critical because data migration requires heavy upstream bandwidth.

Coaxial (A) and DSL (B) offer much lower upstream speeds—often under 30 Mbps—making them too slow for large-scale cloud migration. A SAN (D) is a local storage network that operates within the data center; it does not provide a path to the cloud and cannot replace an internet connection.

Fiber's extremely high capacity, low latency, and resistance to electromagnetic interference make it the best and most efficient option for cloud migration performance.

Question: 301

A user attempts to print diagrams on 11×17 inch (28×43 cm) paper. The correct paper is loaded, but the printer keeps prompting for paper. Another identical printer prints successfully. What is the MOST likely cause?

A. Tray settings

B. Incorrect driver

C. Connectivity issues

D. Insufficient permissions

www.atmicnetworks.com

Answer: A

Explanation:

When a printer refuses to use paper that is physically present in the tray, CompTIA A+ identifies tray configuration settings as the most likely cause. Printers require a match between tray settings (paper size, paper type, orientation) and the incoming print job's specifications. If the tray is incorrectly configured—such as being set to Letter (8.5×11 in) or A4—then the printer will keep prompting for the correct paper even though 11×17 paper is loaded.

The fact that the technician successfully prints the same diagram on another identical printer proves that the driver, print job format, and user permissions are correct. This isolates the issue to the local printer's configuration. Incorrect drivers (B) would affect printing on both printers. Connectivity issues (C) would prevent printing entirely, not cause paper prompts. Permissions (D) do not affect paper-size recognition.

Therefore, the most likely cause is improper tray settings on the user's printer.

Question: 302

A technician is building a high-powered workstation. When the technician attempts to start the workstation, nothing happens. The technician verifies that all power connectors are fully seated. Which of the following is the most likely cause of the issue?

A. The case header pins are not connected.
B. The RAM is not fully seated.
C. The power supply unit's wattage is too low.
D. The CPU fan connector is faulty

Answer: A

Explanation:

When a newly built workstation shows no response at all—no fans spinning, no indicator LEDs, and no POST activity—this indicates that the system is not receiving the signal to power on. Since the technician has already verified that all primary power connectors are fully seated (including the 24- pin ATX motherboard connector and the 4-pin or 8-pin CPU power connector), the most likely cause is that the case header pins are not connected to the motherboard.

According to CompTIA Core 1 (220-1201) hardware installation and troubleshooting concepts, the

power button on the computer case connects to the motherboard via the front-panel (system panel) header, specifically the PWR_SW pins. If this connector is missing, improperly placed, or connected to the wrong pins, pressing the power button will do nothing because the motherboard never receives the power-on signal.

Incorrectly seated RAM typically allows the system to power on but prevents successful POST, often resulting in beep codes or error lights. An underpowered PSU usually causes instability, random shutdowns, or failure under load rather than complete inactivity. A faulty CPU fan connector generally triggers a BIOS warning or shutdown after power-on, not total failure to start.

This scenario directly matches CompTIA's emphasis on checking front-panel connections as a primary step when a system does not power on at all.

Reference:

CompTIA A+ Core 1 (220-1201) Official Study Guide – Hardware Installation, Motherboard Components, and Power Troubleshooting Sections

Question: 303

A user only has access to basic printer functions. A technician notices that the advanced printer features are missing. Which of the following actions will fix this issue?

A. Modifying the printer settings and rebooting the printer

B. Installing the drivers from the printer's manufacturer

C. Restarting the OS and attempting to reprint the document

D. Applying the OS-provided patches for the printer

Answer: B

Explanation:

When a printer only provides basic functionality (such as simple printing without duplexing, color management, stapling, or finishing options), this typically indicates that the system is using a generic or basic printer driver rather than the full-featured driver from the printer manufacturer. According to CompTIA Core 1 (220-1201) printing and troubleshooting

www.atmicnetworks.com

objectives, advanced printer features are enabled through manufacturer-specific drivers, which expose all hardware capabilities to the operating system.

Operating systems often install default or class drivers automatically, especially when printers are connected via USB or discovered on a network. While these drivers allow basic printing, they do not include proprietary features such as high-resolution settings, tray selection, finishing units, or secure printing options. Installing the correct driver package from the printer manufacturer ensures full compatibility and unlocks advanced functionality.

Restarting the OS or modifying printer settings will not add missing features if the correct driver is not installed. OS-provided patches are designed to fix bugs or compatibility issues, not to enable vendor-specific printer capabilities.

CompTIA explicitly emphasizes verifying and installing manufacturer-recommended drivers as a key troubleshooting step when printer features are missing or limited.

Reference:

CompTIA A+ Core 1 (220-1201) Official Study Guide – Printer Installation, Drivers, and Troubleshooting

Question: 304

An administrator selects a new platform that provides the following benefits:

- Shares a host OS
- Shares kernel resources
- Rapid start and deployment
- Limited isolation

Which of the following virtualization options did the administrator select?

A. Type 1 hypervisor

B. Containers

C. Virtual desktop

D. Virtual machine

Answer: B

Explanation:

The virtualization platform described matches the characteristics of containers. According to CompTIA Core 1 (220-1201) virtualization concepts, containers are lightweight virtualization solutions that share the host operating system and kernel, rather than running separate guest operating systems. This design allows containers to start almost instantly and be deployed rapidly, making them highly efficient and scalable.

Because containers share kernel resources, they use significantly fewer system resources compared to traditional virtual machines. However, this also results in limited isolation, since applications are not fully separated at the OS level. This tradeoff is a defining characteristic of container-based virtualization.

A Type 1 hypervisor runs directly on hardware and hosts fully isolated virtual machines, each with its own operating system, which does not align with the shared OS and kernel described. A virtual machine also includes a full guest OS, leading to slower startup times and greater resource usage. A virtual desktop refers to user desktop virtualization, not application-level virtualization.

CompTIA highlights containers as an example of application virtualization that prioritizes speed, efficiency, and portability over complete isolation.

Reference:

CompTIA A+ Core 1 (220-1201) Official Study Guide – Virtualization Concepts, Containers, and Cloud Computing

www.atmicnetworks.com

Question: 305

A technician purchases a device that connects directly to the rear of a laptop and provides a one-to- one match for every peripheral connection. Which of the following best describes this device?

A. USB hub
B. Docking station
C. KVM switch
D. Port replicator

Answer: D

Explanation:

A device that connects directly to a laptop and provides a one-to-one duplication of the laptop's existing ports is known as a port replicator. According to CompTIA Core 1 (220-1201) mobile device and laptop accessories objectives, a port replicator extends the available connections by mirroring the laptop's built-in ports, such as USB, HDMI, Ethernet, and audio. This allows users to quickly connect peripherals like monitors, keyboards, mice, and network cables without plugging each device in individually.

Port replicators are typically passive devices and do not add new functionality beyond duplicating existing ports. They are commonly used in office environments where users frequently dock and undock laptops.

A docking station, by contrast, often provides additional or enhanced functionality, such as extra video outputs, higher-power charging, expansion slots, or proprietary connectors. A USB hub only expands USB connectivity and does not replicate all peripheral connections. A KVM switch is used to
control multiple computers with a single keyboard, video display, and mouse, which is unrelated to laptop port expansion.

CompTIA distinguishes port replicators as simple port-duplication devices, making them the correct answer in this scenario.

Reference:
CompTIA A+ Core 1 (220-1201) Official Study Guide – Mobile Device Accessories and Laptop Hardware

www.atmicnetworks.com

Question: 306

The power supply for a user's gaming computer fails. The user buys a replacement online. The user connects the power supply to the motherboard, the graphics card, and the SSDs, but the computer fails to start and displays a critical error. Which of the following is the most likely cause?

A. The computer requires an additional RAM upgrade.
B. The wattage is insufficient for all the peripherals.
C. The user did not connect the 4-pin connector for the CPU.
D. The power supply only operates in a redundant configuration

Answer: C

Explanation:

Modern motherboards require two separate power connections from the power supply: the 24-pin ATX connector for general motherboard power and a 4-pin or 8-pin CPU (EPS) connector dedicated to powering the processor. According to CompTIA Core 1 (220-1201) power supply installation and troubleshooting guidelines, failing to connect the CPU power connector commonly results in a system that does not boot and may display a critical or CPU-related error.

In this scenario, the user connected power to the motherboard, graphics card, and storage devices, but the system fails to start. This strongly indicates that the CPU power connector was overlooked, which is a frequent mistake during PSU replacement. Without this connection, the processor cannot initialize, preventing POST.

Insufficient wattage typically causes instability, shutdowns, or reboots under load rather than immediate failure with a critical error. RAM upgrades are unrelated to PSU replacement, and

redundant power supplies are used in enterprise systems, not standard gaming PCs.

CompTIA emphasizes verifying all required PSU connectors, especially the CPU power connector, as a critical troubleshooting step when a system will not power on after a PSU replacement.

Reference:

CompTIA A+ Core 1 (220-1201) Official Study Guide – Power Supplies, Connectors, and Troubleshooting

Question: 307

Which of the following is the standard for Wi-Fi 7?

A. 802.1X
B. 802.3at
C. 802.11be
D. 802.15.1

Answer: C

Explanation:

The IEEE standard for Wi-Fi 7 is 802.11be, also known as Extremely High Throughput (EHT). According to CompTIA Core 1 (220-1201) networking standards objectives, each Wi-Fi generation corresponds to a specific IEEE 802.11 amendment. Wi-Fi 7 builds upon Wi-Fi 6/6E by offering significantly higher throughput, lower latency, and improved performance in high-density environments.

Option 802.11be is the only choice that represents a wireless LAN (WLAN) standard. 802.1X is an authentication framework used for network access control, not a Wi-Fi standard. 802.3at defines Power over Ethernet Plus (PoE+), which supplies electrical power over Ethernet cables. 802.15.1 is the IEEE standard for Bluetooth.

CompTIA expects candidates to recognize and differentiate wireless standards and their IEEE designations, especially newer technologies such as Wi-Fi 6, Wi-Fi 6E, and Wi-Fi 7. Identifying 802.11be as Wi-Fi 7 is essential for both exam success and real-world networking scenarios.

Reference:

CompTIA A+ Core 1 (220-1201) Official Study Guide – Networking Standards and Wireless Technologies

Question: 308

Which of the following systems most likely contains ECC memory?

A. A high-end gaming console

www.atmicnetworks.com

B. A file server

C. A smartphone

D. A laptop

Answer: B

Explanation:

Error-Correcting Code (ECC) memory is designed to detect and correct single-bit memory errors, increasing system reliability and data integrity. According to CompTIA Core 1 (220-1201) hardware and memory objectives, ECC memory is most commonly used in servers and enterprise-grade systems where uptime and data accuracy are critical.

A file server is responsible for storing, managing, and serving data to many users simultaneously. Memory errors in such systems could lead to data corruption, crashes, or security issues. For this reason, servers frequently use ECC memory in combination with server-class CPUs and motherboards that support error correction.

High-end gaming consoles prioritize performance and cost efficiency rather than fault tolerance, and they do not use ECC memory. Smartphones rely on low-power mobile RAM without error correction,
and laptops typically use non-ECC memory unless they are specialized workstation-class systems, which is not indicated in this question.

CompTIA emphasizes that ECC memory is associated with mission-critical environments, particularly servers and enterprise systems, making a file server the most appropriate answer.

Reference:

CompTIA A+ Core 1 (220-1201) Official Study Guide – RAM Types, ECC Memory, and Server Hardware

www.atmicnetworks.com

Question: 309

Users in a 200-person call center report that phone calls experience severe performance degradation on busy days. The technician confirms:

- Upload and download speeds are 50Mbps during a speed test.
- VoIP call prioritization settings are properly configured for the VLAN that the call center uses.

Which of the following is most likely the cause of this issue?

A. The QoS is not configured correctly on the router.

B. The switchports dedicated to the call center are flapping.

C. The call center's VLAN is not configured to allow voice traffic.

D. The bandwidth dedicated to the call center is insufficient.

Answer: D

Explanation:

Voice over IP (VoIP) traffic is highly sensitive to latency, jitter, and packet loss, especially in large environments such as a 200-person call center. Although the technician confirms that VoIP prioritization (QoS) is configured correctly and speed tests show 50 Mbps upload and download speeds, overall available bandwidth can still be insufficient during peak usage.

Speed tests measure raw throughput at a point in time and do not reflect real-world congestion caused by hundreds of simultaneous calls, application usage, and data transfers. On busy days, the cumulative bandwidth demand likely exceeds the available capacity, leading to degraded call quality despite correct VLAN and QoS settings.

If QoS were misconfigured or the VLAN did not allow voice traffic, call issues would be consistent at all times, not only during peak periods. Flapping switchports would cause intermittent connectivity drops rather than predictable performance degradation correlated with high usage.

CompTIA highlights that bandwidth limitations are a common root cause of VoIP performance problems in high-density environments, even when prioritization is properly implemented.

Reference:

CompTIA A+ Core 1 (220-1201) Official Study Guide – Networking Performance, QoS, and VoIP

Question: 310

A customer reports that internet browsing on their smartphone is fast at the beginning of the month but significantly slows down toward the end of the month. A technician examines the smartphone and finds multiple free cloud backup services running with several gigabytes of personal data spread across each. Data availability is important to the customer. Which of the following is the best way to resolve the customer's issue?

A. Disabling all cloud backup services except one
B. Installing an additional SD card for photos and videos
C. Expanding the cache storage to consolidate data
D. Configuring data synchronization only over Wi-Fi connections

Answer: D

Explanation:

The described behavior indicates that the customer is likely exceeding their mobile data allowance each month. Multiple cloud backup services continuously synchronizing gigabytes of data consume large amounts of cellular bandwidth, which can trigger data throttling by the mobile carrier near the end of the billing cycle. This results in noticeably slower browsing speeds.

Since data availability is important, disabling backup services entirely is not the best option. Installing an SD card increases local storage but does not reduce cellular data usage. Expanding cache storage does not address network

bandwidth consumption or carrier throttling.

Configuring data synchronization to occur only over Wi-Fi ensures that backups continue uninterrupted when the device is connected to a wireless network, while preventing excessive cellular data usage. This preserves data availability and eliminates unnecessary mobile data consumption, restoring consistent browsing performance throughout the month.

CompTIA Core 1 (220-1201) mobile device troubleshooting objectives emphasize managing background services, synchronization settings, and data usage to resolve performance and connectivity issues on smartphones.

Reference:

CompTIA A+ Core 1 (220-1201) Official Study Guide – Mobile Device Configuration, Data Usage, and Troubleshooting

Question: 311

Which of the following networking technologies allows for high-speed data transmission over short distances between devices like smartphones and tablets?

A. Near-field communication
B. Zigbee
C. Infrared
D. Wi-Fi Direct

Answer: D

Explanation:

Wi-Fi Direct is designed to provide high-speed, short-range wireless communication directly between devices such as smartphones, tablets, laptops, and printers without requiring a traditional wireless access point. According to CompTIA Core 1 (220-1201) networking objectives, Wi-Fi Direct uses standard Wi-Fi radio technology, allowing devices to communicate at speeds comparable to typical wireless LAN connections.

Near-field communication (NFC) operates at extremely short distances (typically a few centimeters) and supports very low data transfer rates, making it unsuitable for high-speed data transmission. Zigbee is a low-power, low-bandwidth protocol commonly used for IoT and home automation devices, not for high-speed data sharing. Infrared requires line-of-sight and offers limited data rates, which restricts its usefulness for modern mobile devices.

Wi-Fi Direct is commonly used for tasks such as file sharing, screen mirroring, and device-to-device printing. CompTIA emphasizes understanding the differences between short-range wireless technologies, particularly distinguishing high-throughput solutions like Wi-Fi Direct from low-power or proximity-based technologies.

Reference:
CompTIA A+ Core 1 (220-1201) Official Study Guide – Wireless Networking Technologies

Question: 312

Which of the following record types is used to create an alias for a domain?

A. CNAME
B. AAAA
C. TXT
D. A

Answer: A

Explanation:

A CNAME (Canonical Name) record is used in DNS to create an alias that maps one domain name to another canonical domain name. According to CompTIA Core 1 (220-1201) DNS objectives, CNAME records allow multiple hostnames to reference the same IP address indirectly by pointing to a single authoritative domain name.

For example, www.example.com can be configured as a CNAME that points to example.com. When DNS queries are made, the resolver follows the alias until it reaches an A or AAAA record that contains the actual IP address.

An A record maps a hostname directly to an IPv4 address, while an AAAA record maps a hostname to an IPv6 address. A TXT record is used to store arbitrary text data, commonly for verification, email security (SPF, DKIM), or policy information, not for aliasing.

CompTIA stresses that CNAME records are specifically intended for aliasing and name redirection within DNS, making them the correct answer.

Reference:
CompTIA A+ Core 1 (220-1201) Official Study Guide – DNS Record Types and Name Resolution

Question: 313

An IP address is automatically assigned to a single workstation in an office, but the technician confirms the IP address is not in the lease pool. This workstation is having issues accessing the internet and internal file shares. Which of the following address types has been automatically assigned?

A. APIPA
B. Static
C. DHCP
D. Public IP

Answer: A

Explanation:

When a workstation automatically assigns itself an IP address that is not part of the DHCP lease pool, the system has most likely configured an APIPA (Automatic Private IP Addressing) address. According to CompTIA Core 1 (220-1201) networking fundamentals, APIPA addresses fall within the range 169.254.0.0/16 and are assigned when a device cannot communicate with a DHCP server.

APIPA allows limited local network communication but does not provide access to the internet or network resources such as internal file shares that require routing or proper IP configuration. This explains why the workstation experiences connectivity issues.

A static IP address is manually configured and would not be automatically assigned. A DHCP address would come from the defined lease pool, which the technician has confirmed is not the case. A public IP address is assigned by an ISP and is not used directly on internal workstations.

CompTIA highlights APIPA as a key troubleshooting indicator of DHCP failure or network connectivity issues, making it the correct answer.

Reference:
CompTIA A+ Core 1 (220-1201) Official Study Guide – IP Addressing, DHCP, and Troubleshooting

Question: 314

A technician is building a home desktop computer. The technician wants to prioritize cable management when considering the type of power supply. Which of the following power supply types should the technician consider?

A. Back-up
B. Modular
C. Standard
D. Redundant

Answer: B

Explanation:

A modular power supply is the best choice when cable management is a priority. According to CompTIA Core 1 (220-1201) power supply objectives, modular PSUs allow technicians to connect only the cables that are needed for the system's components, reducing clutter inside the case.

This improves airflow, simplifies troubleshooting, and creates a cleaner internal layout, which is especially beneficial in home-built desktop systems. Semi-modular and fully modular power supplies offer varying degrees of flexibility, but all modular designs reduce unused cables compared to standard power supplies.

A standard (non-modular) power supply has all cables permanently attached, often resulting in excess unused cables that obstruct airflow. A backup power supply refers to an uninterruptible power supply (UPS), which provides battery backup but does not improve internal cable management. A redundant power supply is typically found in enterprise servers and includes multiple PSUs for fault tolerance, not cable management.

CompTIA emphasizes modular power supplies as a best practice for clean builds and efficient system design, making this the correct answer.

Reference:
CompTIA A+ Core 1 (220-1201) Official Study Guide – Power Supplies, Form Factors, and Cable Management

Question: 315

An administrator is investigating a misuse of printer resources. The administrator suspects an employee. Which of the following will help the administrator verify the source of misuse?

A. Secure printing
B. Print counter
C. Audit logs
D. User authentication

Answer: C

Explanation:

To verify the source of printer misuse, the administrator needs detailed records showing who performed specific actions and when. According to CompTIA Core 1 (220-1201) printer management and security objectives, audit logs provide a historical record of printer activity, including user IDs, timestamps, document names, and print volumes. These logs allow administrators to trace printer usage back to a specific user or device, making them the most effective tool for investigating misuse.

Secure printing requires users to authenticate at the printer before jobs are released, which helps prevent unauthorized access but does not provide historical evidence of past misuse. A print counter tracks the total number of pages printed but does not identify individual users or specific print jobs. User authentication ensures that only authorized users can access the printer, but by itself it does not provide detailed usage tracking unless combined with logging.

CompTIA emphasizes audit logging as a critical component of accountability and security across systems, including printers. When investigating policy violations or misuse, audit logs are the primary source of verifiable evidence.

Reference:
CompTIA A+ Core 1 (220-1201) Official Study Guide – Printer Security, Monitoring, and Management

Question: 316

The computers and IP phones at an office experience degraded performance during the day. The issue does not occur before the start of business. Which of the following will resolve the issue?

A. Changing the switches to ones with higher capacity
B. Using VLANs to segregate data and voice traffic
C. Adding RAM to the PCs and additional VoIP lines
D. Updating the firmware on the switches

Answer: B

Explanation:

Degraded performance that occurs only during business hours strongly suggests network congestion caused by simultaneous data and voice traffic. According to CompTIA Core 1 (220-1201) networking objectives, combining voice (VoIP) and data traffic on the same network without proper segmentation can lead to latency, jitter, and packet loss,

especially during peak usage periods.

Implementing VLANs (Virtual Local Area Networks) allows administrators to logically separate voice and data traffic, enabling better traffic management and prioritization. VLANs also support Quality of Service (QoS) policies that ensure time-sensitive voice traffic is prioritized over standard data traffic, improving call quality and overall performance.

Replacing switches with higher-capacity models is costly and unnecessary if proper traffic segmentation has not yet been implemented. Adding RAM to PCs or VoIP lines does not address network-level congestion. Firmware updates may improve stability but will not resolve sustained performance degradation caused by traffic contention.

CompTIA highlights VLAN implementation as a best practice for environments that use IP phones, especially when performance issues occur during high utilization periods.

Reference:
CompTIA A+ Core 1 (220-1201) Official Study Guide – VLANs, VoIP, and Network Performance

Question: 317

Which of the following is the best to use to stream real-time video from a network camera?

A. UDP
B. TCP
C. FTP
D. RDP

Answer: A

Explanation:

UDP (User Datagram Protocol) is the preferred protocol for real-time video streaming, such as feeds from network cameras. According to CompTIA Core 1 (220-1201) networking protocols objectives, UDP prioritizes speed and low latency over guaranteed delivery, making it ideal for time-sensitive

applications.

Real-time video streaming can tolerate occasional packet loss, but it cannot tolerate delays caused by retransmissions. UDP does not perform error checking or packet retransmission, which reduces overhead and ensures smooth, continuous playback. This is critical for live video feeds where delayed packets are useless.

TCP, while reliable, introduces latency due to acknowledgments and retransmissions, making it unsuitable for real-time streaming. FTP is a file transfer protocol and does not support live streaming. RDP is used for remote desktop access and is not designed for transmitting continuous real-time video streams from cameras.

CompTIA emphasizes understanding protocol selection based on application requirements, particularly distinguishing between reliability and performance needs. For live video, UDP is the optimal choice.

Reference:

CompTIA A+ Core 1 (220-1201) Official Study Guide – Network Protocols and Use Cases

Question: 318

Which of the following is an example of VDI?

A. Streaming a GUI to thin clients from a server
B. Provisioning a sandbox as a test environment
C. Providing high-performance workstations with a local OS
D. Launching a virtual machine server on a hypervisor

Answer: A

Explanation:

Virtual Desktop Infrastructure (VDI) delivers a desktop operating system hosted on a centralized server and streams the graphical user interface (GUI) to endpoint devices such as thin clients, zero clients, or standard PCs. According to CompTIA Core 1 (220-1201) virtualization objectives, VDI allows users to access their desktop environments remotely while all processing and data remain on the server.

Option A accurately describes this model: a GUI streamed from a server to thin clients. This approach improves centralized management, enhances security, and simplifies endpoint hardware requirements.

Provisioning a sandbox is an example of test or development virtualization, not desktop virtualization. High-performance workstations with a local OS are physical desktops, not VDI. Launching a virtual machine server on a hypervisor describes server virtualization, not desktop delivery.

CompTIA highlights VDI as a common enterprise solution that separates the desktop environment from the physical device, enabling flexibility, scalability, and centralized control.

Reference:

Question: 319

A user connects a PC to a projector and configures the projector to use HDMI. However, when the user tries to use the projector, the projector shows a black screen with the message "HDMI2 no signal found." The user reports that the projector worked properly during a previous meeting. Which of the following should the user do to fix the issue?

A. Replace the bulb.
B. Swap the video cable.
C. Change the input source.
D. Update the video drivers.

Answer: C

Explanation:

The error message "HDMI2 no signal found" indicates that the projector is set to an input source that is not currently receiving a video signal. According to CompTIA Core 1 (220-1201) display and troubleshooting objectives, input source selection is one of the first items to verify when an external display shows a black screen but powers on correctly.

Many projectors have multiple HDMI ports (HDMI1, HDMI2, etc.). If the PC is connected to a different HDMI port than the one currently selected, the projector will display a "no signal" message even

though the cable and device are functioning properly. Changing the input source to match the connected HDMI port resolves the issue quickly.

Replacing the bulb would not fix a "no signal" message, as the projector is clearly powered on and displaying text. Swapping the video cable is a valid troubleshooting step, but the explicit HDMI2 message points to an incorrect input selection. Updating video drivers is unnecessary when the device worked previously and the issue is isolated to input detection.

CompTIA emphasizes verifying correct input selection as a primary step when troubleshooting external display issues.

Reference:

Question: 320

A technician must upgrade a computer system to improve its overall processing performance. Which of the following should the technician focus on to ensure maximum system performance?

A. Integrated GPU
B. Power connectors
C. Voltage regulator module
D. Clock frequency

Answer: D

Explanation:

Clock frequency is one of the most significant factors influencing a computer system's processing performance. According to CompTIA Core 1 (220-1201) CPU and performance objectives, clock speed—measured in gigahertz (GHz)—determines how many instruction cycles a processor can perform per second.

Higher clock frequencies generally result in faster execution of instructions, leading to improved performance in both single-threaded and multi-threaded workloads. While modern CPUs also rely on core count, cache size, and architecture efficiency, clock frequency remains a primary metric for evaluating raw processing speed.

An integrated GPU affects graphics performance rather than overall CPU processing capability. Power connectors ensure proper electrical delivery but do not directly improve processing performance. The voltage regulator module (VRM) stabilizes and regulates power supplied to the CPU but does not itself increase processing speed.

CompTIA expects candidates to recognize clock frequency as a key determinant of CPU performance when upgrading or comparing processors.

Reference:
CompTIA A+ Core 1 (220-1201) Official Study Guide – CPU Architecture and Performance

Question: 321

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:

If a computer can access internal network resources but cannot reach external websites, the most likely issue is a DNS configuration problem. According to CompTIA Core 1 (220-1201) networking troubleshooting methodology, DNS should be one of the first items checked when internet access fails but local connectivity remains intact.

DNS translates human-readable domain names into IP addresses. If DNS settings are incorrect, missing, or pointing to an invalid server, the computer will be unable to resolve website names even though it has network connectivity. Since other users on the same network can access the internet, the issue is isolated to the individual workstation.

Replacing the network cable is unnecessary because internal connectivity is already working.
Restarting the DHCP server would impact all users, not just one. Adjusting firewall rules on the router

would affect the entire network rather than a single computer.

CompTIA emphasizes starting with least disruptive and most likely causes when troubleshooting.
Verifying DNS settings aligns with this best-practice approach.

Reference:
CompTIA A+ Core 1 (220-1201) Official Study Guide – Network Troubleshooting and DNS

Topic 2, Simulation Performance Based Questions

www.atmicnetworks.com

Question: 322

SIMULATION

A small ISP has hired a new technician Joe, the new technician, is being trained to configure customers* home networks The trailing instructor gives me technician a starter kit with cables, cable ends, and other network equipment and asks mm to build a working network.

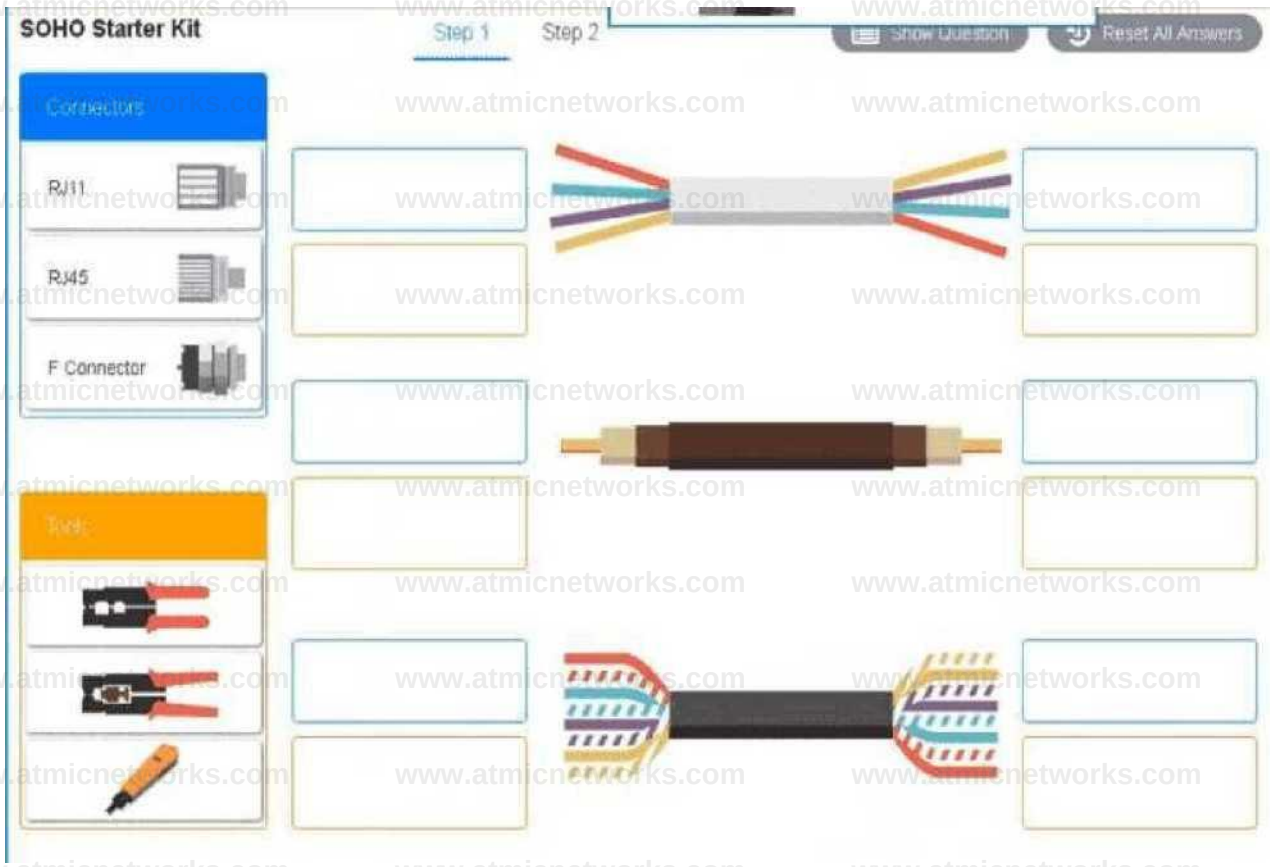
The computer should be connected to have internet connectivity and the phone should be connected to have a dial tone.

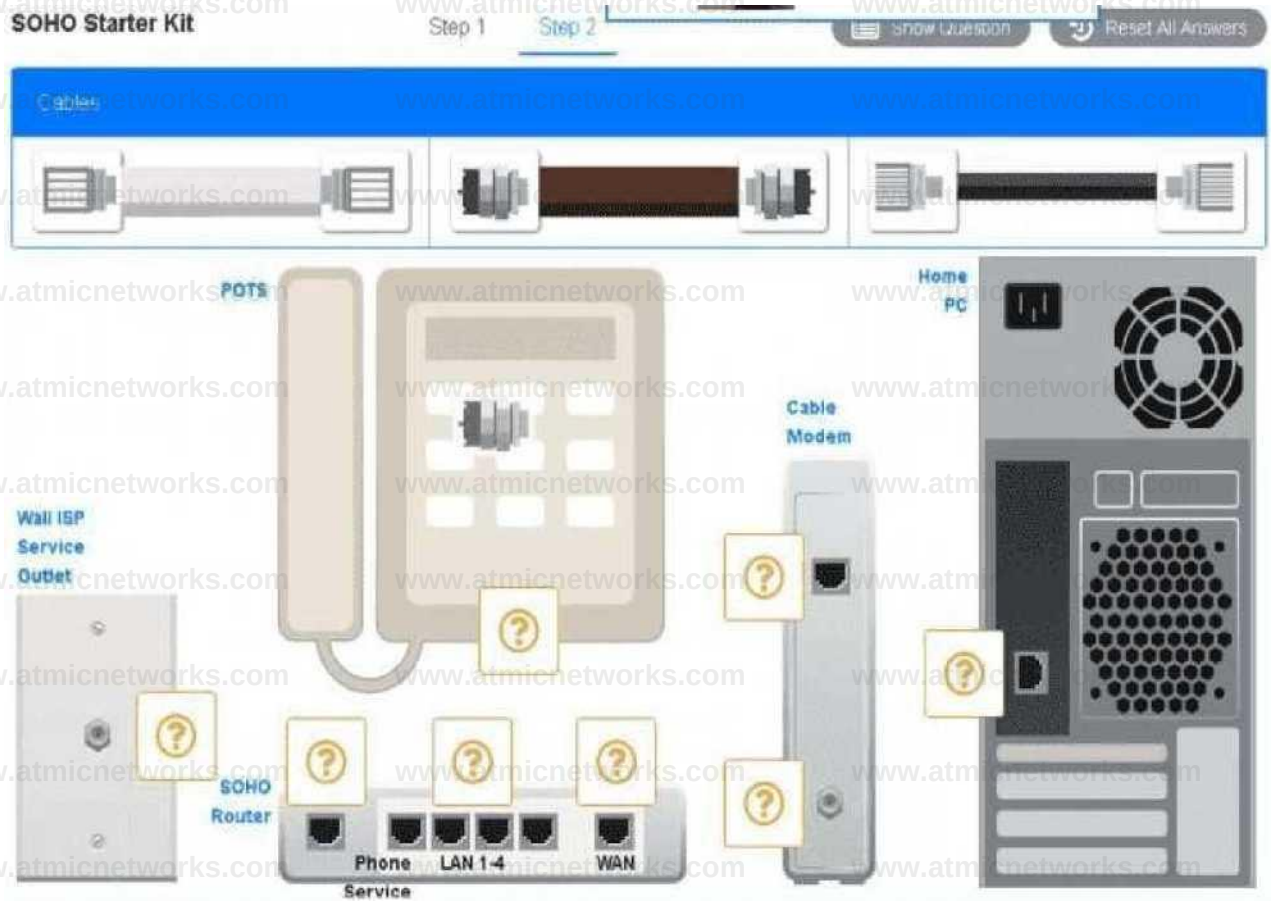
INSTRUCTIONS

Use the appropriate cables. cable ends, tools and equipment to configure the network ana connect an components accordingly

There are 3 steps and the simulation starts on step 1.

www.atmicnetworks.com

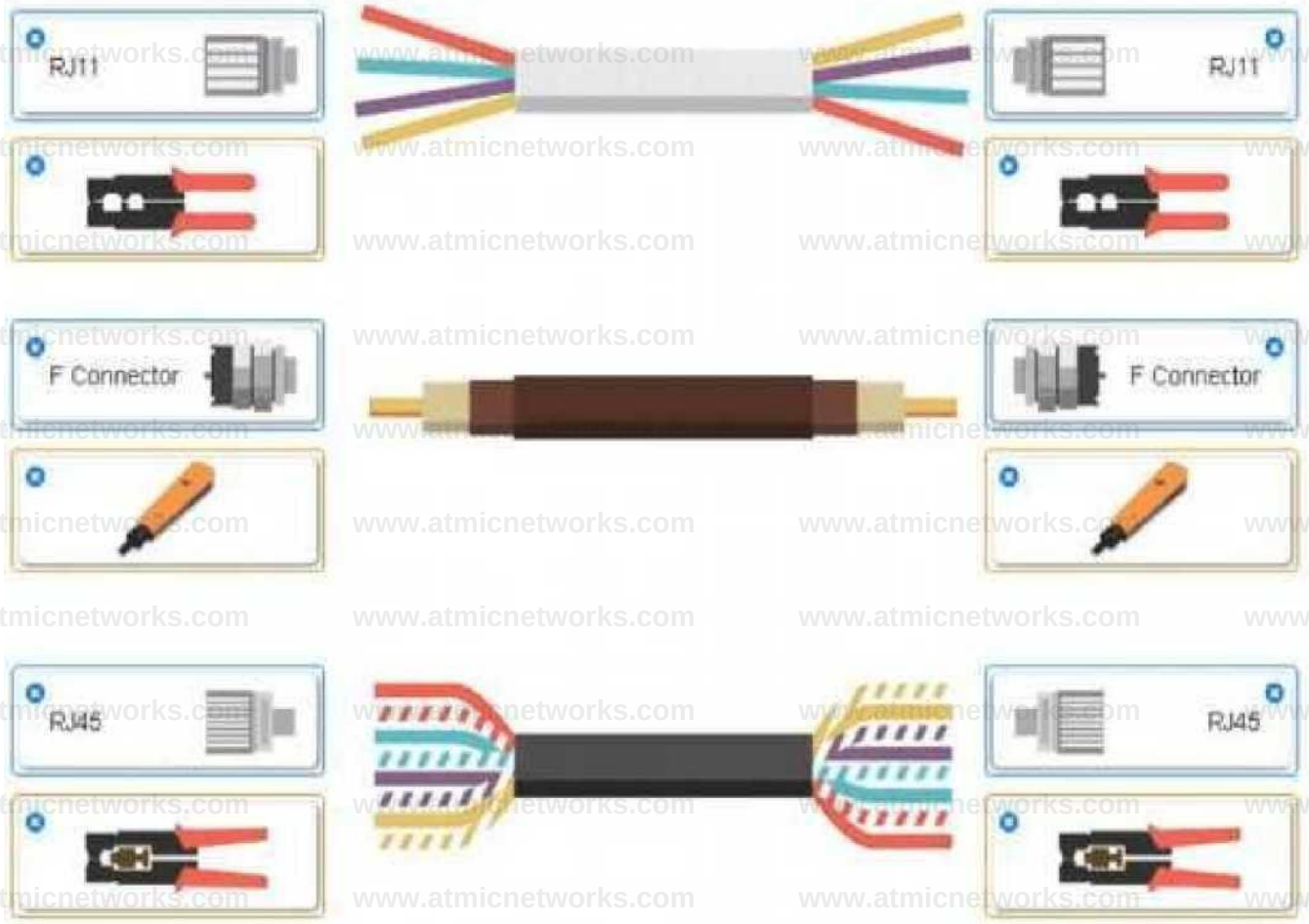




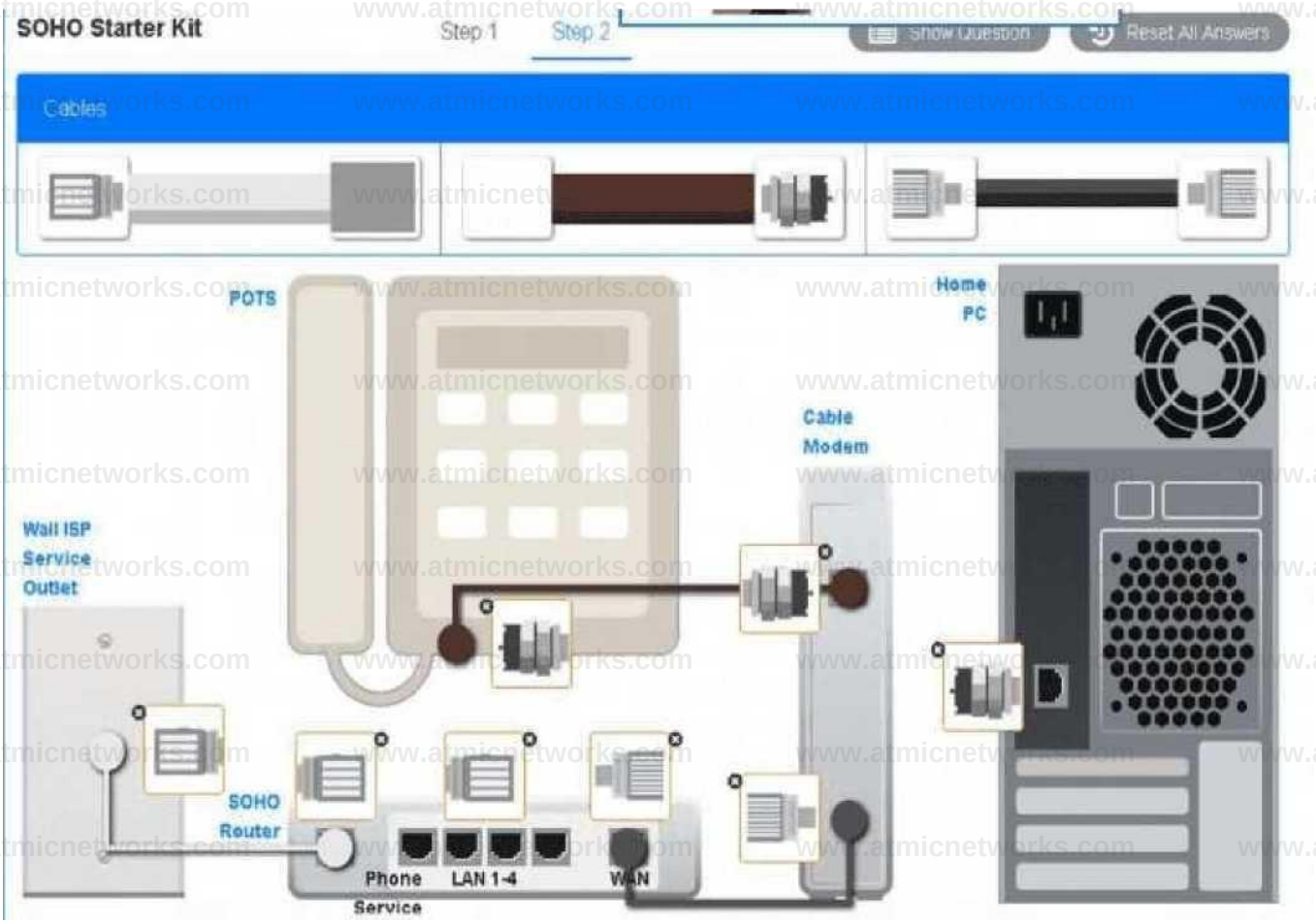
Answer: See the answer below in explanation part.

Explanation:

Answer of both steps below.



A group of wires with different colors AI-generated content may be incorrect.



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

Question: 323

SIMULATION

A technician is installing a wireless access point and is required to run all cabling and make patch cords if necessary.

INSTRUCTIONS

Part 1

For each cable type, click the (+) to select the appropriate connector and tool.

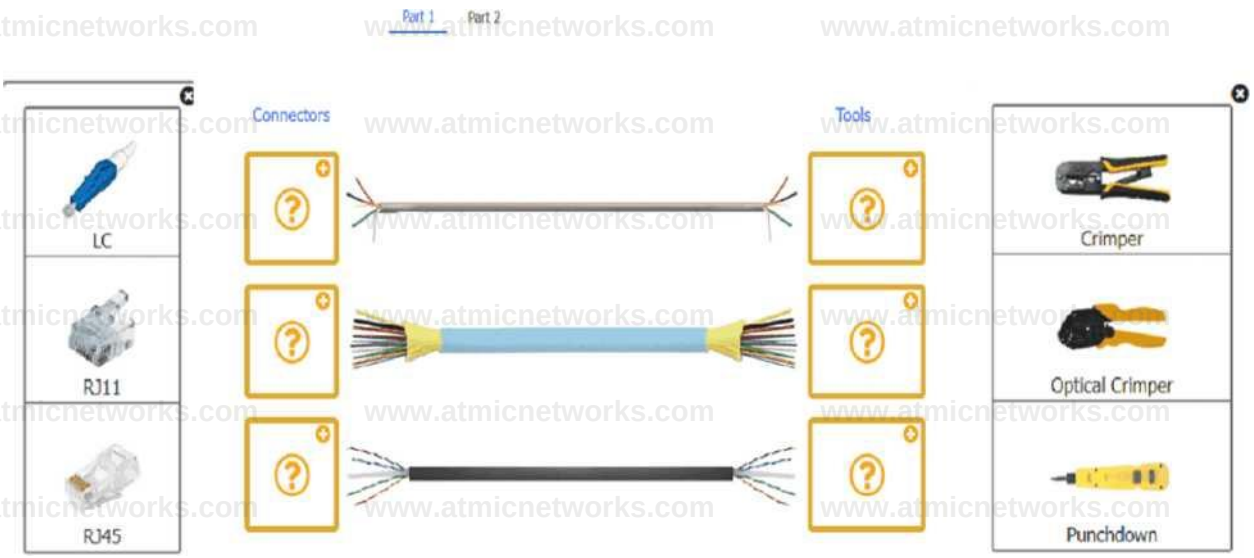
www.atmicnetworks.com

part 2

An access point was moved and no longer has connectivity. Connect the access point, patch panel, and switch by clicking the (+) to select the appropriate cable end for each corresponding location to create a link.

The link will be visible after making the second selection of each pair.

Cable ends may be used multiple times, and all placeholders will be filled.

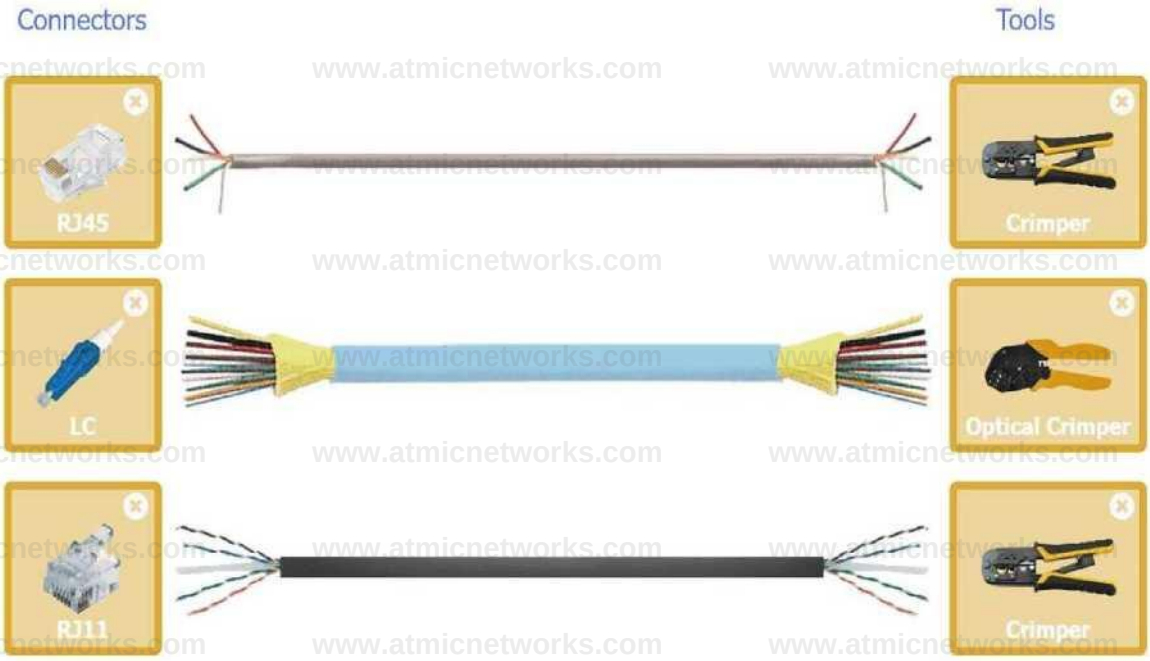


Answer: See the solution below in Explanation.

Explanation:

www.atmicnetworks.com

Check the exhibit diagram for both parts.



A close-up of several cables AI-generated content may be incorrect.

Part 2

A group of different colored rectangular objects AI-generated content may be incorrect.

Question:
324

SIMULATION

A user reports poor performance on the application server.

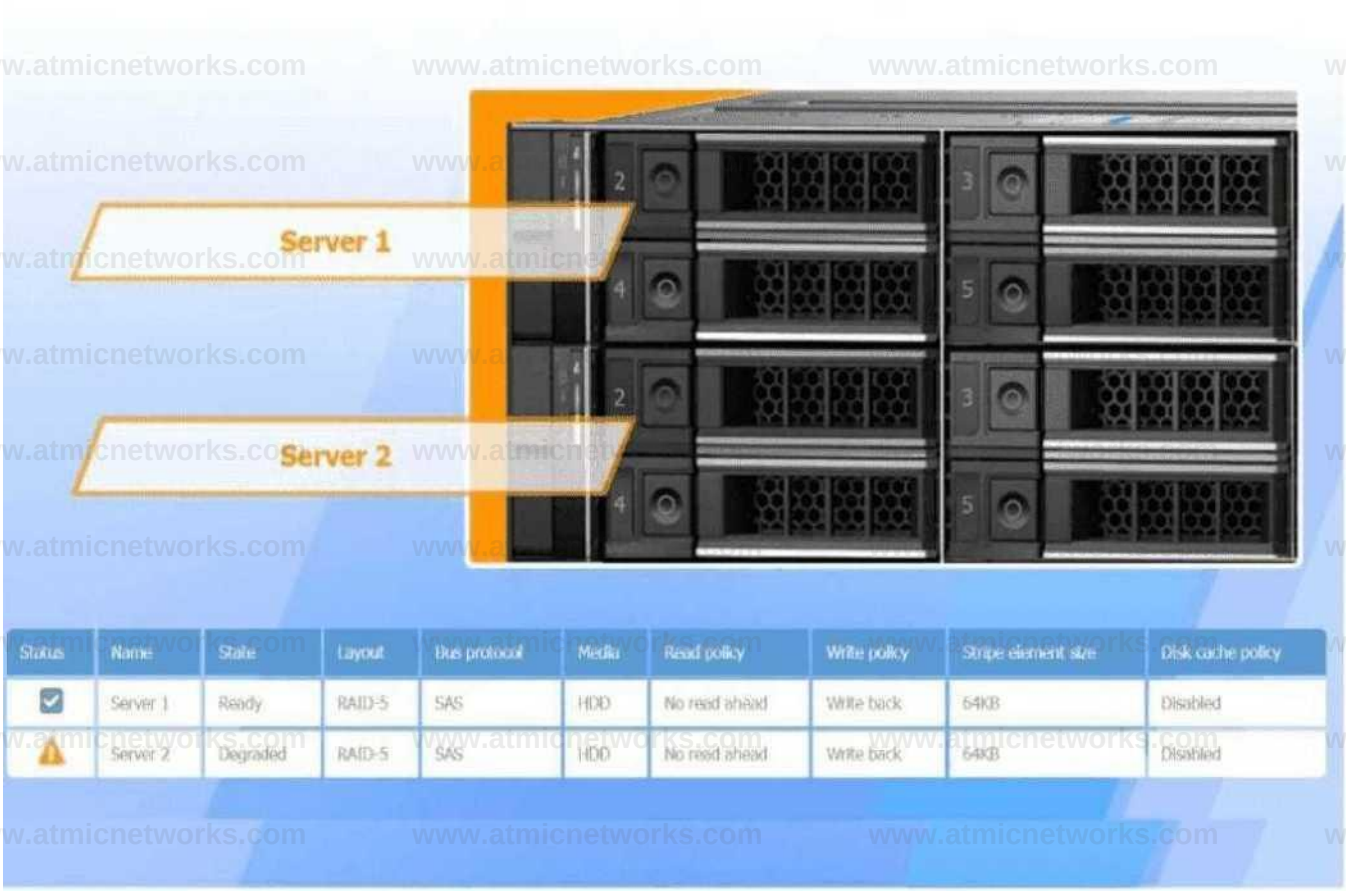
www.atmicnetworks.com

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.



Status	Name	State	Layout	Bus protocol	Media	Read policy	Write policy	Stripe element size	Disk cache policy
☑	Server 1	Ready	RAID-5	SAS	HDD	No read ahead	Write back	64KB	Disabled
⚠	Server 2	Degraded	RAID-5	SAS	HDD	No read ahead	Write back	64KB	Disabled

Answer: See the detailed solution in explanation below.

Explanation:

The degraded status on Server 2 indicates a RAID-5 issue, typically due to a failed or failing drive. In RAID-5 configurations,

when one drive fails, the system can still operate but with reduced performance as parity data is used to rebuild missing data on-the-fly.

Recommended Replacement Drive:

To minimize performance degradation, the replacement drive should be:

SAS HDD with the same specifications (64KB stripe size, no read-ahead, and write-back policy).

Matching the configuration exactly ensures seamless integration and optimizes recovery speed in the RAID-5 array.

In RAID-5, degraded performance is expected when one drive fails, as parity data needs to rebuild missing information during each read/write process. Replacing the failed drive restores the RAID array to optimal status, reducing the load on existing drives and returning the system to normal read/write performance. The write-back policy and disabled disk cache settings are designed to reduce latency and increase efficiency, essential for handling real-time applications.

A user reports poor performance on the

application server.

INSTRUCTIONS

Click on Server 1 and Server 2 and review

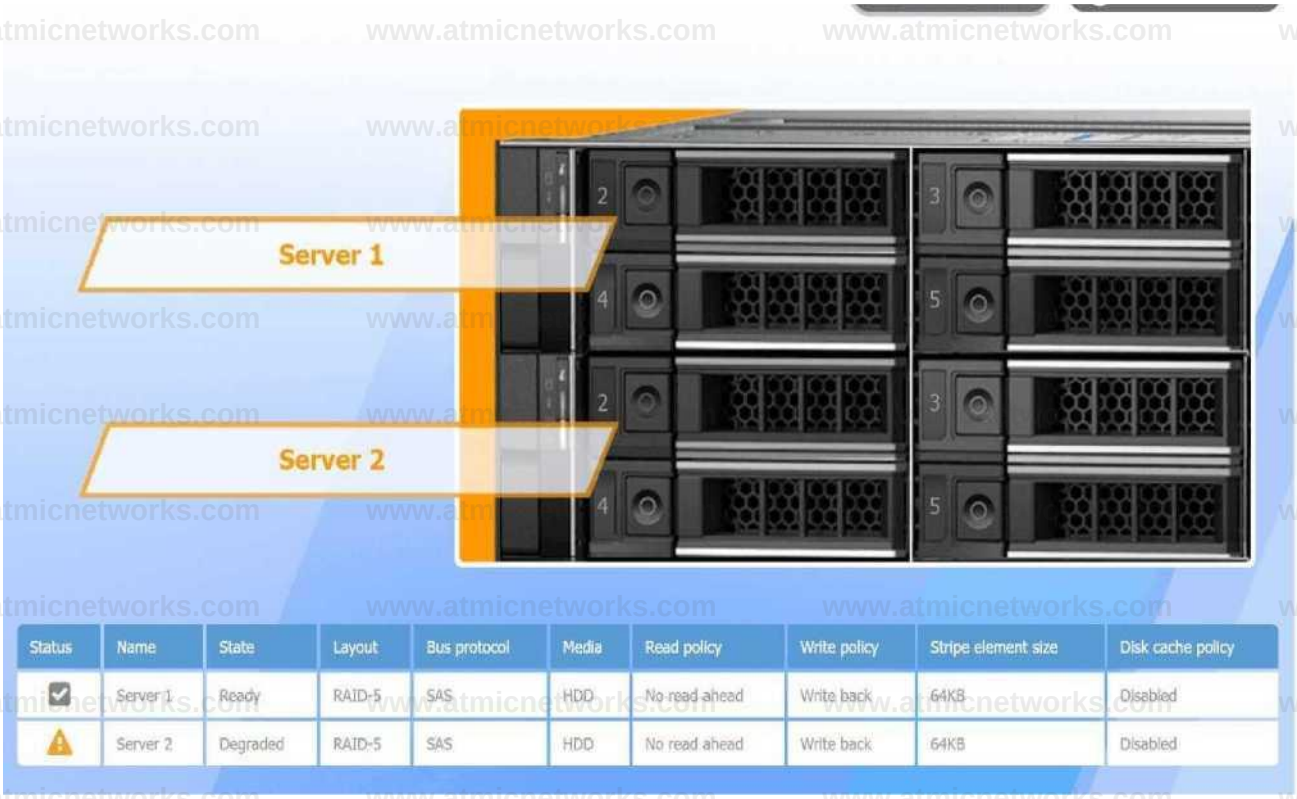
the information presented in each chart to

determine which drives need to be replaced.

Select the appropriate replacement drive

that should be used, for the least

performance degradation to the server.



Status	Name	State	Layout	Bus protocol	Media	Read policy	Write policy	Stripe element size	Disk cache policy
☑	Server 1	Ready	RAID-5	SAS	HDD	No read ahead	Write back	64KB	Disabled
⚠	Server 2	Degraded	RAID-5	SAS	HDD	No read ahead	Write back	64KB	Disabled

A computer server with many black and silver parts AI-generated content may be incorrect.A computer server with many black boxes Description automatically generated with medium confidence

Server 1 X

Status	Name	State	Size	Media	Speed	Failure predicted
Q	Physical disk 1:2	Online	4TB	HDD	15k rpm	Yes
☐	Physical disk 1:3	Online	4TB	HDD	15k rpm	No
Q	Physical disk 1:4	Online	4TB	HDD	15k rpm	No
☐	Physical disk 1:5	Online	4TB	HDD	15k rpm	No

A screen shot of a computer AI-generated content may be incorrect.A screen shot of a computer Description automatically generated

A computer screen shot of a computer AI-generated content may be incorrect.A computer screen shot of a computer Description automatically generated

www.atmicnetworks.com

Server 1, Drive bay 4

Size	Interface	Rotational speed
4TB v	HDD	15k rpm

www.atmicnetworks.com

A computer screen shot of a computer AI-generated content may be incorrect.A computer screen shot of a computer Description automatically generated

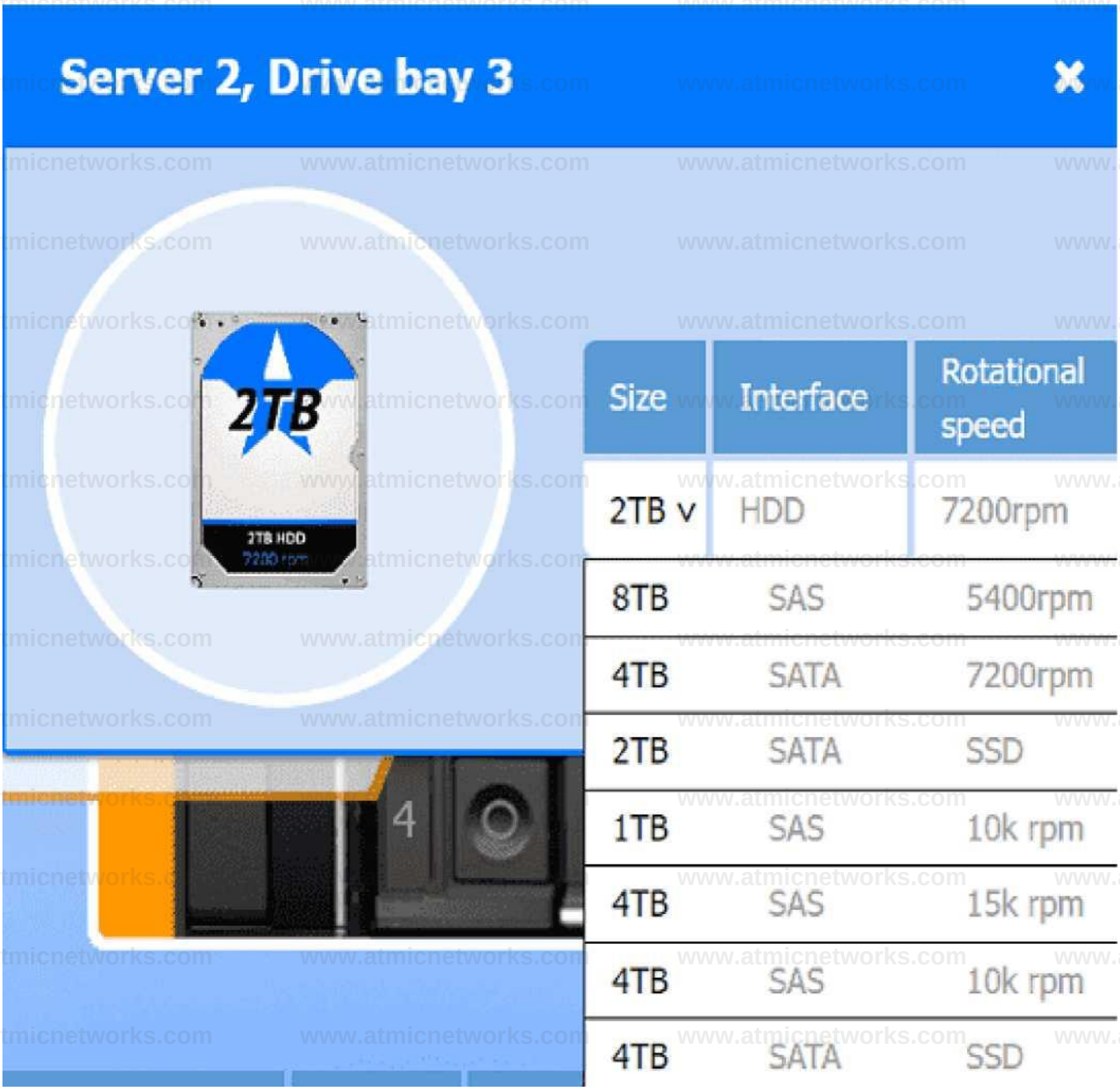
A computer screen shot of a computer AI-generated content may be incorrect.A computer screen shot of a computer Description automatically generated

Server 2, Drive bay 2

Size	Interface	Rotational speed
2TB v	HDD	7200rpm
8TB	SAS	5400rpm
4TB	SATA	7200rpm
2TB	SATA	SSD
1TB	SAS	10k rpm
4TB	SAS	15k rpm
4TB	SAS	10k rpm
4TB		SSD

Layout	Bus protocol	Met
RAID-5	SAS	
RAID-5	SAS	HD

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



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

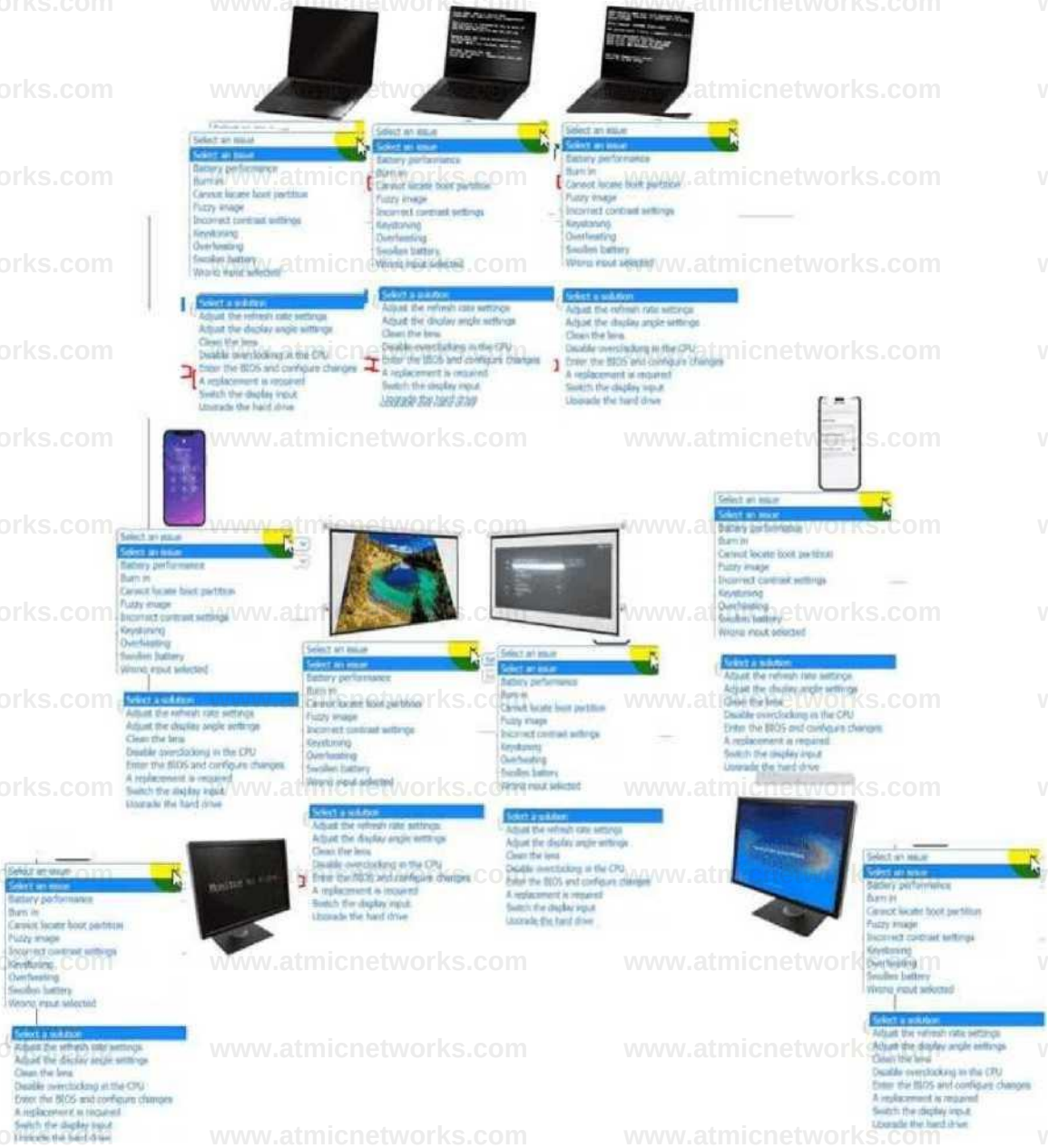
Question: 325

A technician is diagnosing several device issues reported by employees.

INSTRUCTIONS

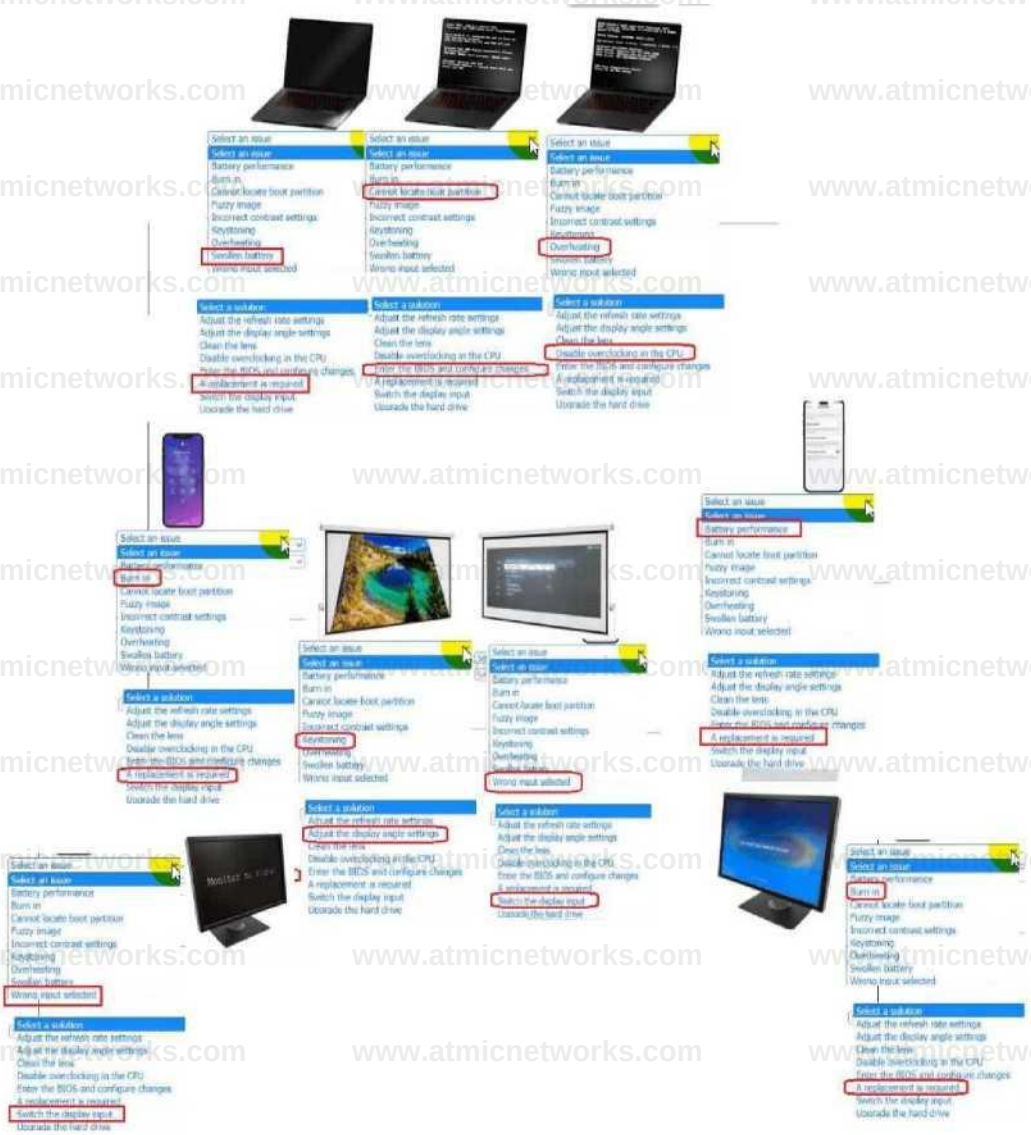
Click on each device to review the issue. Then select the appropriate issue and solution

from the drop-down menu. Each option may be used more than once.



Answer:

Explanation:



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

Question: 326

SIMULATION

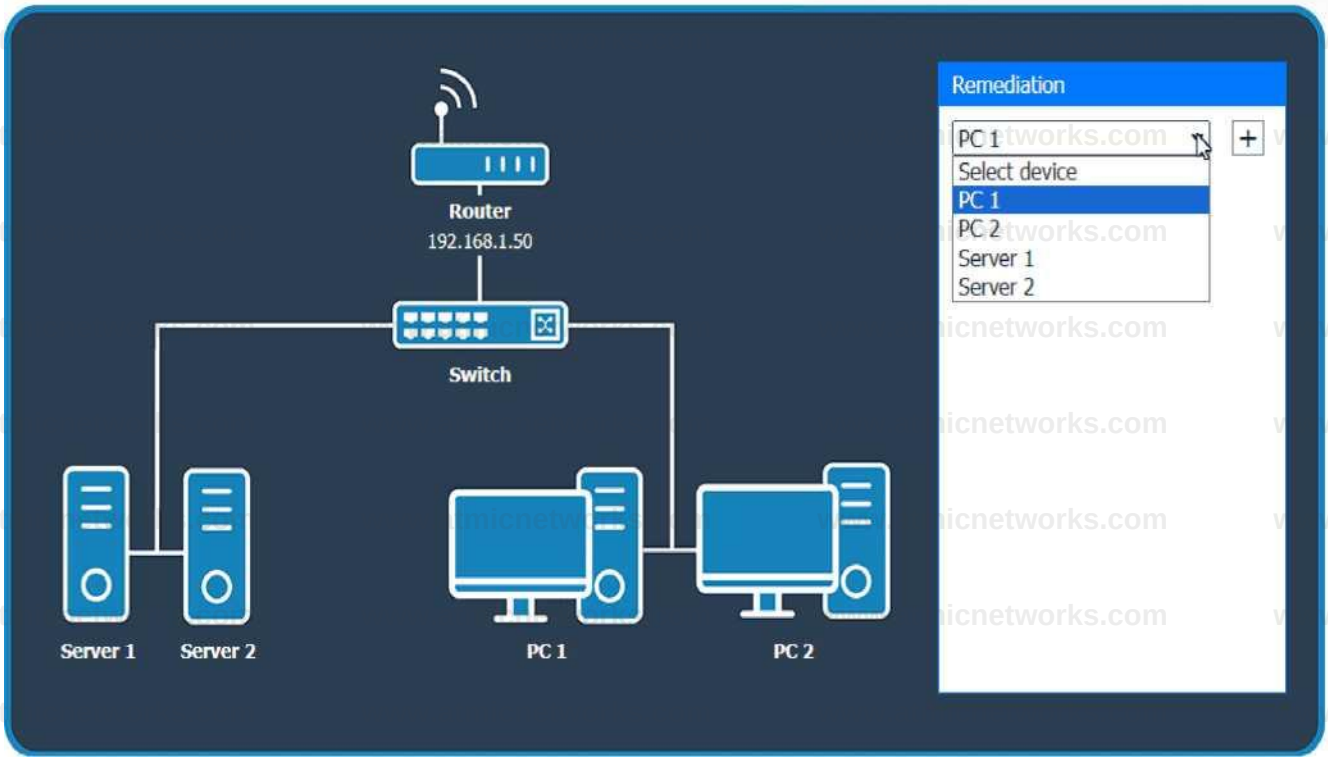
A third-party contractor recently installed a new switch, router, and cabling for a small corporate office. After the installation, users started experiencing issues connecting to resources over the network.

INSTRUCTIONS

Click on each PC and server to review outputs. From the remediation section on

www.atmicnetworks.com

the right, select an issue and solution for each device.



www.atmicnetworks.com

PCI

X

Command terminal IPv4 properties

Internet protocol version 4 (TCP/IPv4) properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

Obtain an IP address automatically

,-- Use the following IP address: ----------

IP address: 192.168.1.1

Subnet mask: 255.255.255.0

Default gateway:

Obtain DNS server address automatically

,-- Use the following DNS server addresses: ----------

Preferred DNS server: 192.168.1.1

Alternate DNS server:

Validate settings upon exit

Advanced...

PCI

Command terminal IPv4 properties

```
ipconfig /all

Windows IP Configuration

   Host Name ..... : PCI
   Primary Dns Suffix ..... :
   Node Type ..... : Peer-Peer
   IP Routing Enabled ..... : No
   WINS Proxy Enabled ..... : No
   DNS Suffix Search List ..... : corp.Ian

Ethernet adapter Ethernet 1:

   Connection-specific DNS Suffix . : corp.Ian Description . . . . . : Realtek
   USB GbE Family Controller
   Physical Address ..... : E1:7C:5C:D4:57:79

   DHCP Enabled ..... : No
   Autoconfiguration Enabled . . . . : No
   IPv4 Address ..... : 192.168.1.1 (Preferred)
   Subnet Mask ..... : 255.255.255.0
```

www.atmicnetworks.com

PCI

X

Command terminal | IPv4 properties

```
   Host Name  ..................
   Primary Dns Suffix  ..........
   Node Type  ..................
   IP Routing Enabled.....
   WINS Proxy Enabled.....
   DNS Suffix Search List. . . .

Ethernet adapter Ethernet 1:

   Connection-specific DNS Suffix
   Description  ..................
   Physical Address.....
   DHCP Enabled..................
   Autoconfiguration Enabled . .
   IPv4 Address..................
   Subnet Mask  ..................
   Default Gateway  .....
   DNS Servers  ..................

   NetBIOS over Tcpip.....
```

```
PCI

Peer-Peer
No
No corp.Ian



corp.Ian
Realtek USB GbE Family Controller
E1:7C:5C:D4:57:79
No
No
192.168.1.1 (Preferred)
255.255.255.0
192.168.1.50
192.168.1.1
192.168.1.50
Enabled
```

www.atmicnetworks.com

PC2

Command terminal IPv4 properties

```
Node Type . . . . . . . . . . . . . IP
Routing Enabled. . . . WINS Proxy
Enabled. . . . DNS Suffix Search
List. .
```

```
: Peer-Peer
: No
. : No
. : corp.Ian
```

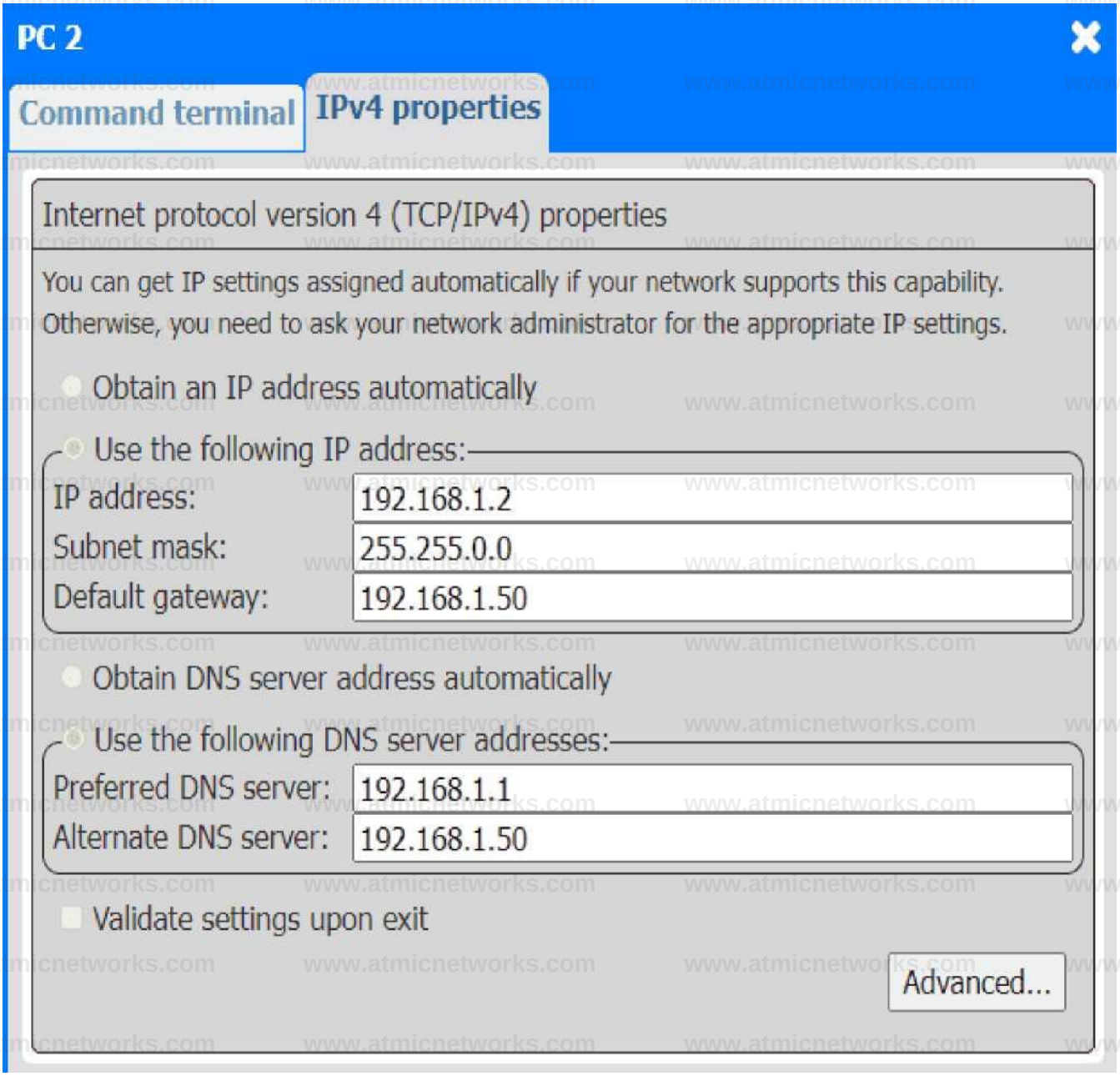
```
Ethernet adapter Ethernet 1:
```

```
Connection-specific DNS Suffix
Description . . . . . . . . . . . . . . .
Physical Address. . . . . . . . . . . . .
DHCP Enabled. . . . . . . . . . . . . . .
Autoconfiguration Enabled . .
IPv4 Address. . . . . . . . . . . . . . .
Subnet Mask . . . . . . . . . . . . . . .
Lease Obtained. . . . . . . . . . . . . .
Lease Expires . . . . . . . . . . . . . .
Default Gateway . . . . . . . . . . . . .
DHCP Server . . . . . . . . . . . . . . .
DNS Servers . .
```

```
: corp.Ian
: Realtek USB GbE Family Controller
: 36:9E:94:F0:59:83
: Yes
: Yes
: 192.168.1.12 (Preferred)
: 255.255.255.0
: August 28, 2028 9:07:46 AM
: August 29, 2023 9:07:46 AM
: 192.168.1.50
: 192.168.1.1
```

```
: 192.168.1.1
192.168.1.50
```

www.atmicnetworks.com



Server 1

Command terminal IPv4 properties

```
    Host Name ..........................:  Serveri
    Primary Dns Suffix  ..............  :
    Node Type ..........................:  Peer-Peer
    IP Routing Enabled .................:  No
    WINS Proxy Enabled .................:  No
    DNS Suffix Search List .............:  corp.Ian
```

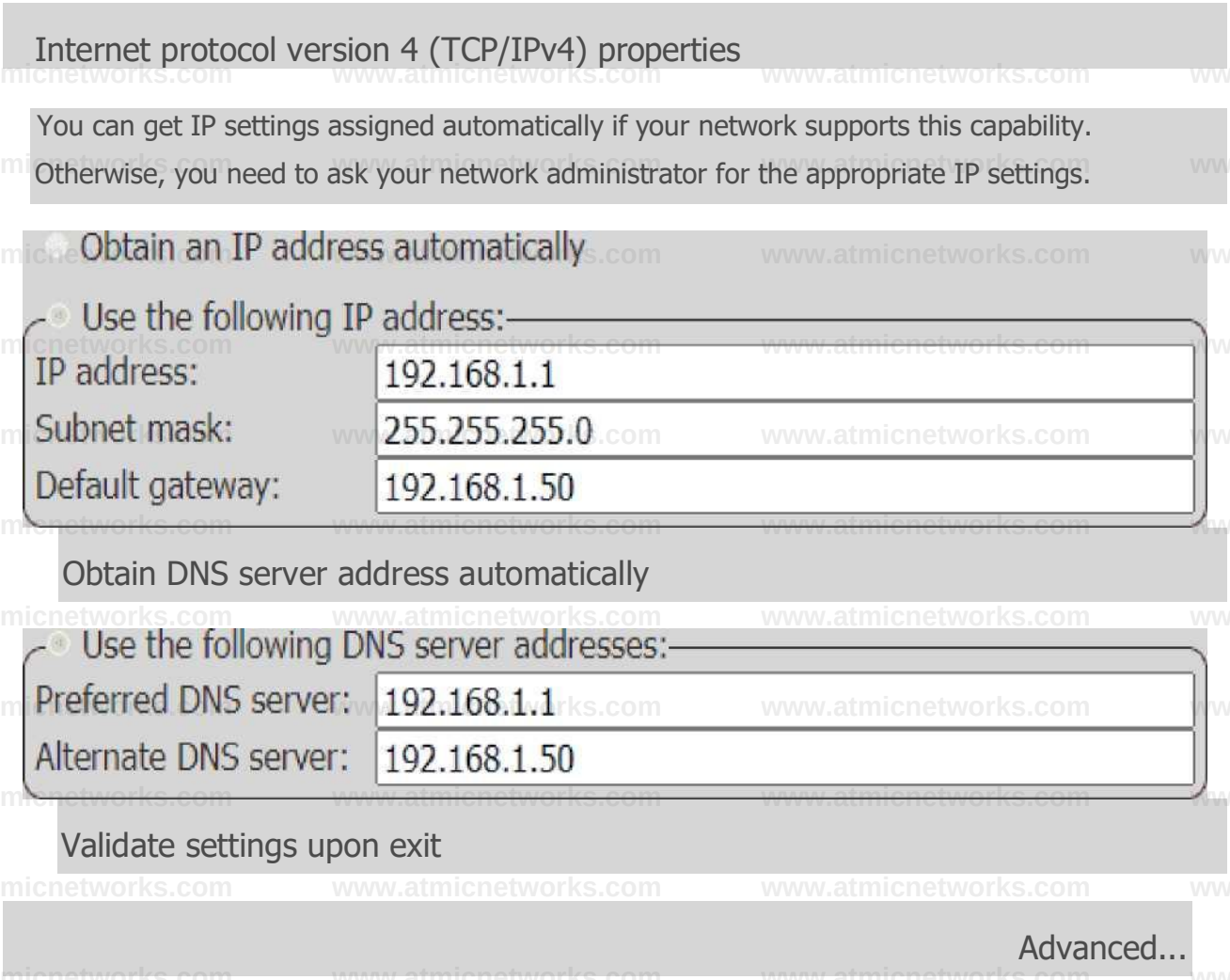
```
  Ethernet adapter Ethernet 1:
```

```
    Connection-specific DNS Suffix . : corp.Ian Description       :    Realtek USB
    GbE Family Controller
    Physical Address ...................:  B2:9F:BB:2C:21:74

    DHCP Enabled .......................:  No
    Autoconfiguration Enabled . . . . :    No
    IPv4 Address .......................:  192.168.1.1 (Preferred)
    Subnet Mask  ..................... :  255.255.255.255
    Default Gateway  .................. :  192.168.1.50

    DNS Servers  ..................... :  192.168.1.1
                                          192.168.1.50
    NetBIOS over Tcpip .................:  Enabled
```

www.atmicnetworks.com

Server 1

Command terminal **IPv4 properties**



www.atmicnetworks.com

Server 2

Command terminal IPv4 properties

```
   Host Name ..................
   Primary Dns Suffix ..........
   Node Type ..................
   IP Routing Enabled ..........
   WINS Proxy Enabled ..........
   DNS Suffix Search List. . . .
```

```
Serveri

Peer-Peer
No
No
corp.Ian
```

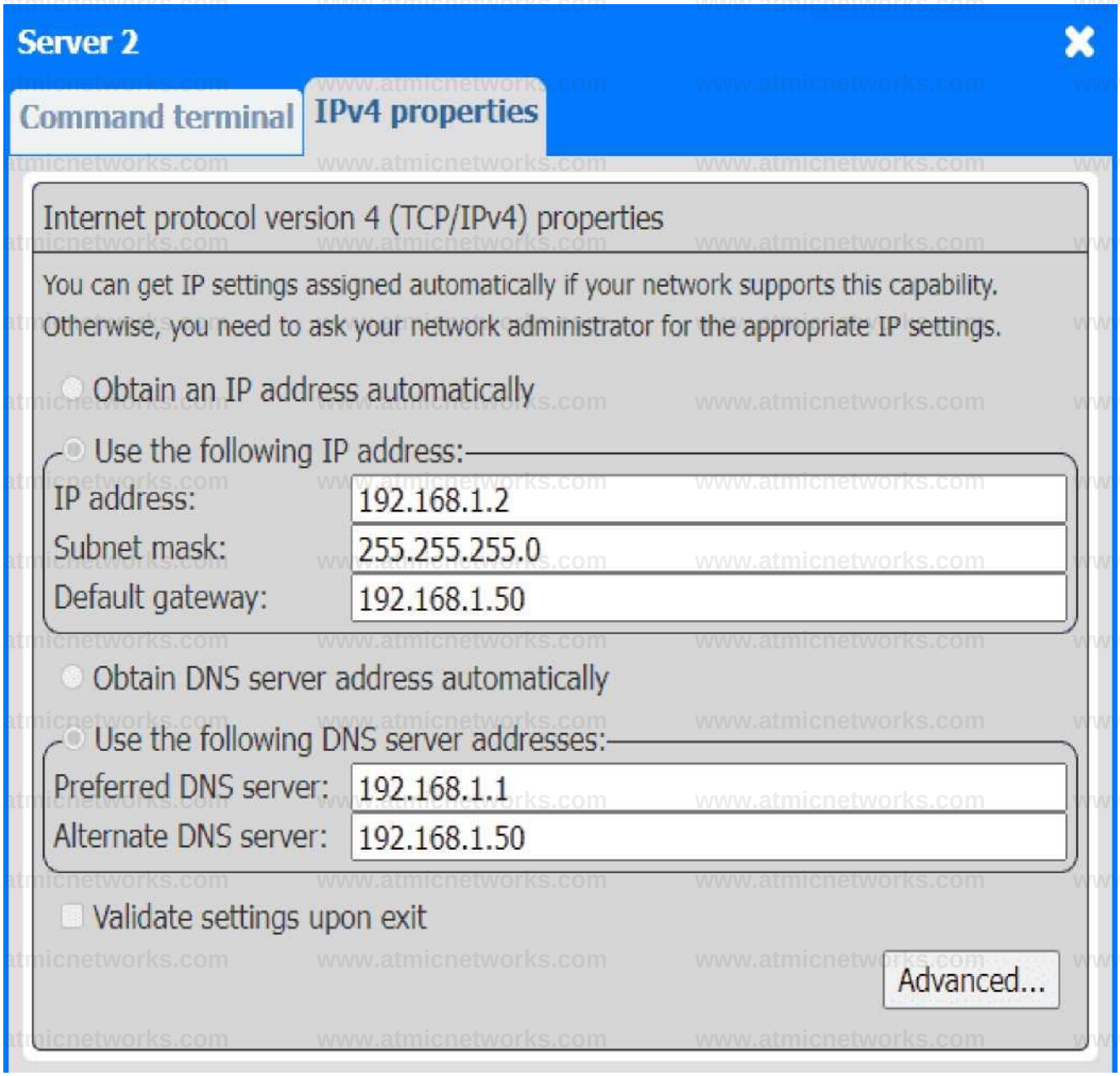
```
Ethernet adapter Ethernet 1:
```

```
   Connection-specific  DNS  Suffix
   Description ................
   Physical Address ...........
   DHCP Enabled ...............
   Autoconfiguration Enabled . .
   IPv4 Address ...............
   Subnet Mask ................
   Default Gateway ............
   DNS Servers ................
```

```
: corp.Ian
: Realtek USB GbE Family Controller
: AC:50:46:09:72:60
: No
: No
: 192.168.1.2 (Preferred)
: 25S.255.255.9
: 192.168.1.5
: 192.168.1.1
  192.168.1.50
```

```
   NetBIOS over Tcpip ..........
```

```
: Enabled
```



Answer: See the Explanation and detailed steps below.

Explanation:

Looking at the network configurations and outputs from both PCs and servers, here are the possible issues and solutions:

1. PC 1

Issue: The IP address for PC1 is 192.168.1.1, which conflicts with Server 1 (which also uses

192.168.1.1).

Solution: Change the IP address on PC1 to a unique one within the range, like 192.168.1.3.

2. PC 2

Issue: PC 2 is configured with 192.168.1.2, which conflicts with Server 2 that has the same IP address.

Solution: Update the IP address on PC 2 to something unique, like 192.168.1.4.

3. Server 1

Issue: The IP address for Server 1 is 192.168.1.1, which conflicts with PC1.

Solution: Since Server 1 and PC1 are using the same IP address, change one of them. For Server 1, you could change the IP address to 192.168.1.5.

4. Server 2

Issue: Server 2 is using the IP address 192.168.1.2, which conflicts with PC2.

Solution: Update Server 2 to use a different IP address, such as 192.168.1.6.

General Remediation:

The primary problem here is overlapping IP addresses, leading to connectivity issues. Each device on the network must have a unique IP address. After making these changes, ensure that all devices can communicate properly by testing the connection between devices and verifying they can access shared resources.

Question: 327

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

The customer requirements include:

Playing the newest games at a high frame rate

Fast game load times

Enough storage to have several games installed at once

High-end audio

No concern about cost

Running the current Windows OS

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

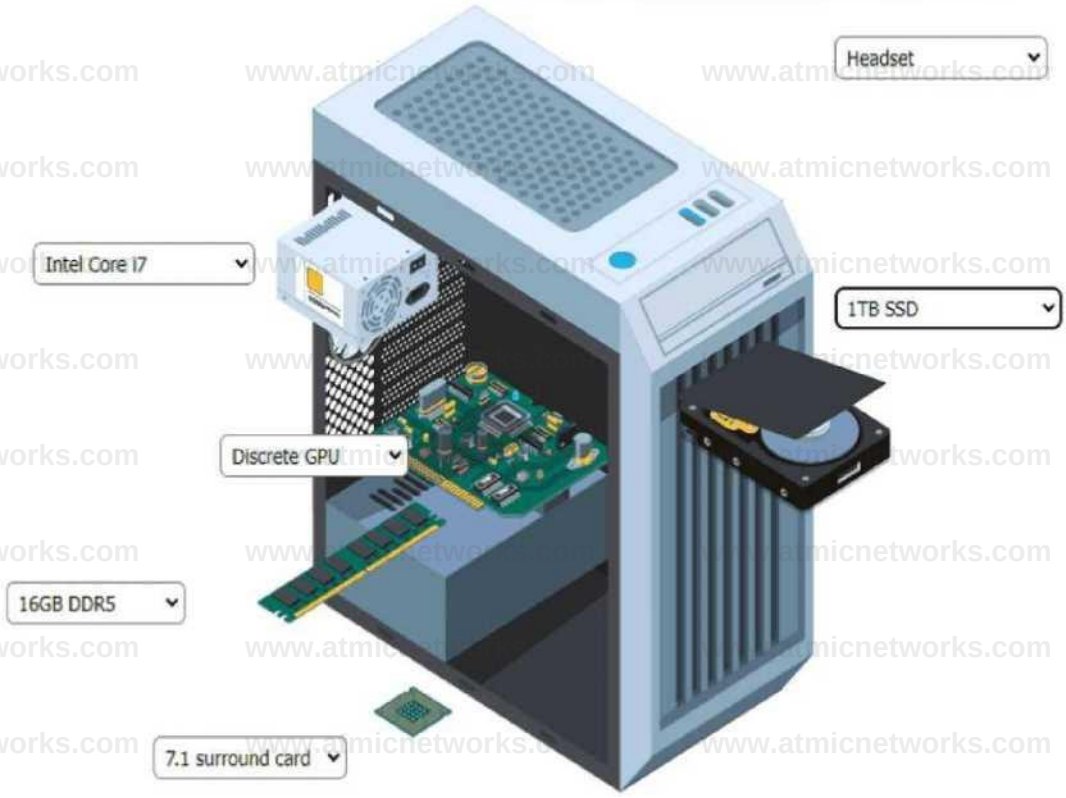
Capability for word processing, videoconferencing, and basic web surfing

Minimal cost, as long as it meets the requirements

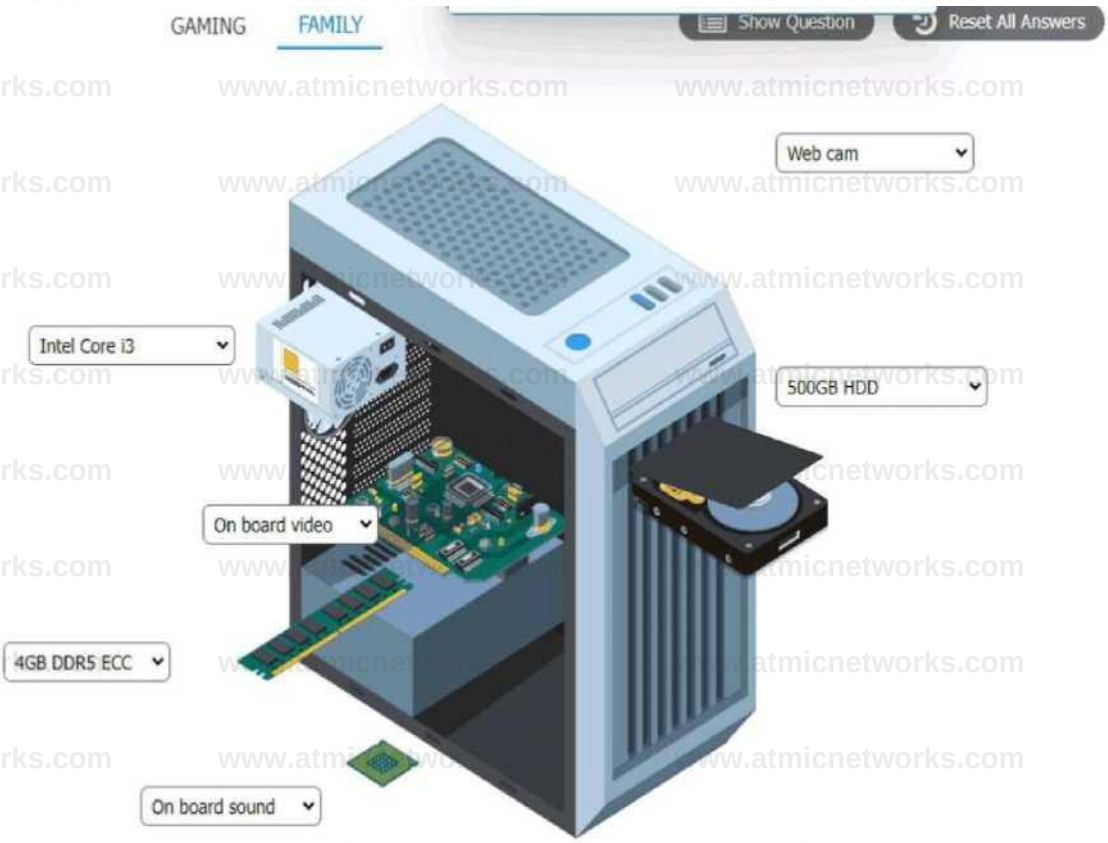
Running the current Windows OS

Answer:

Explanation:



A computer tower with a hard drive and a hard drive AI-generated content may be incorrect.



A computer tower with a computer and a hard drive AI-generated content may be incorrect.

www.atmicnetworks.com

Question: 328

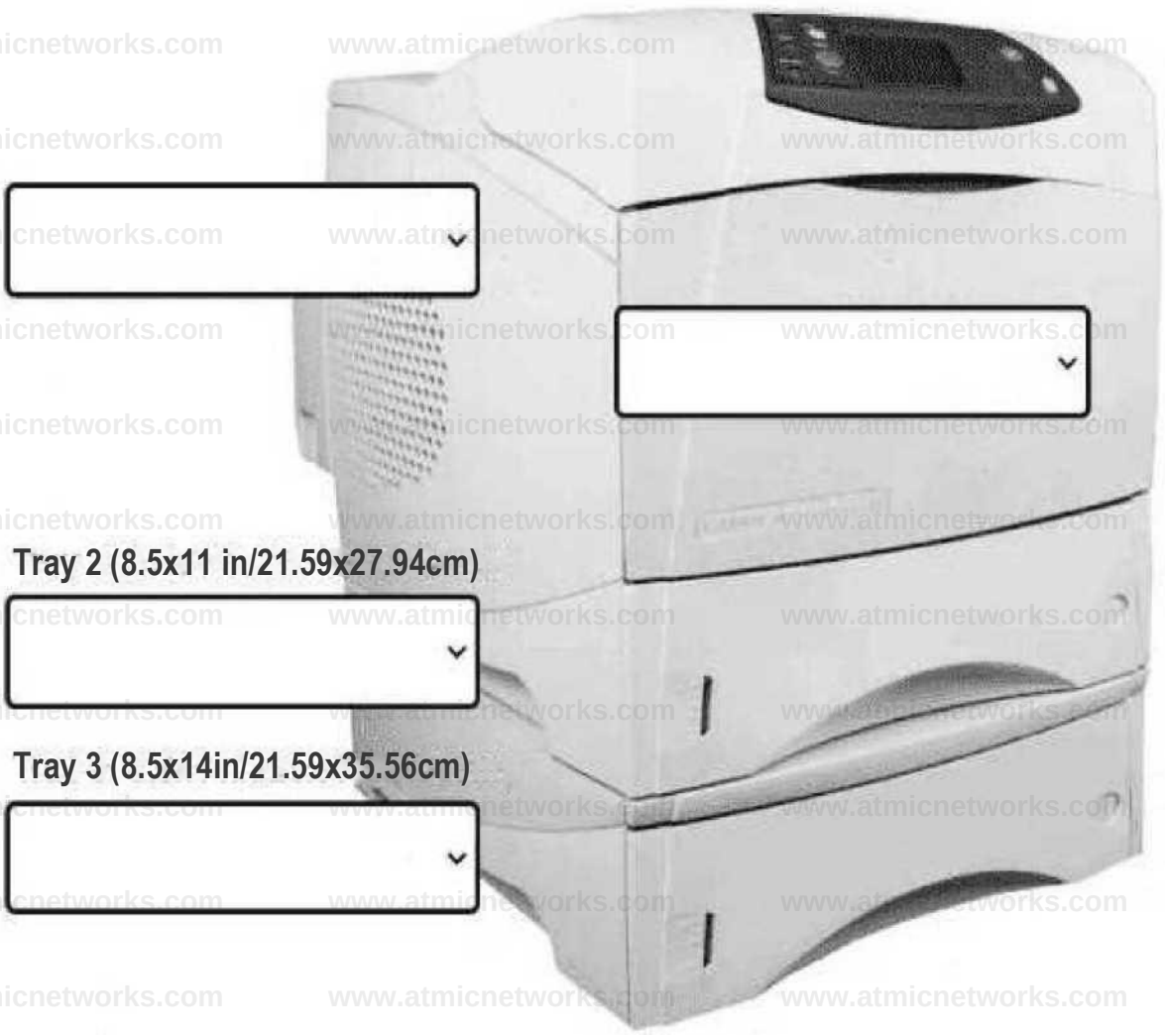
An office manager reports that a printer is experiencing performance issues. Printouts are smudging when they are handled, and, recently whenever they need to print legal sized documents, the paper jams before anything is printed on it.

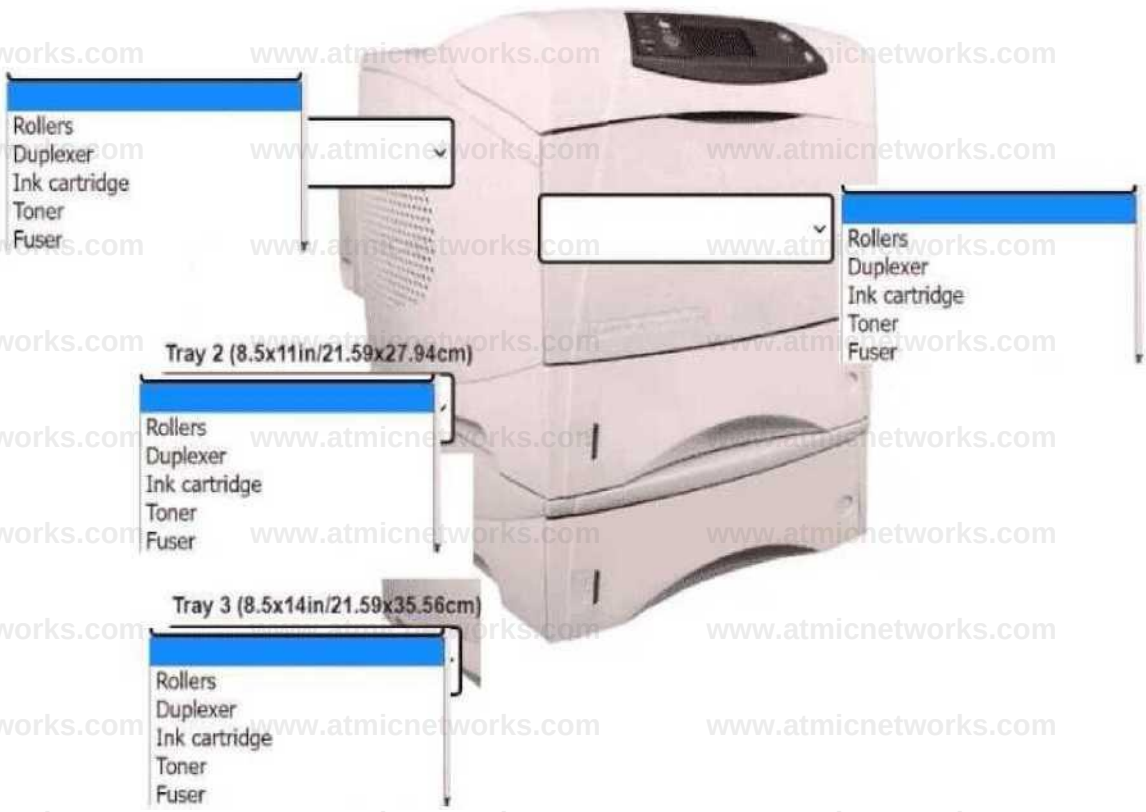
The following paper sizes are used:

Letter (8.5x11in/21.59x27.94cm)

Legal (8.5x14in/21.59x35.56cm)

Oversized (11x17in/27.94x43.18cm)


Tray 2 (8.5x11 in/21.59x27.94cm)
Tray 3 (8.5x14in/21.59x35.56cm)



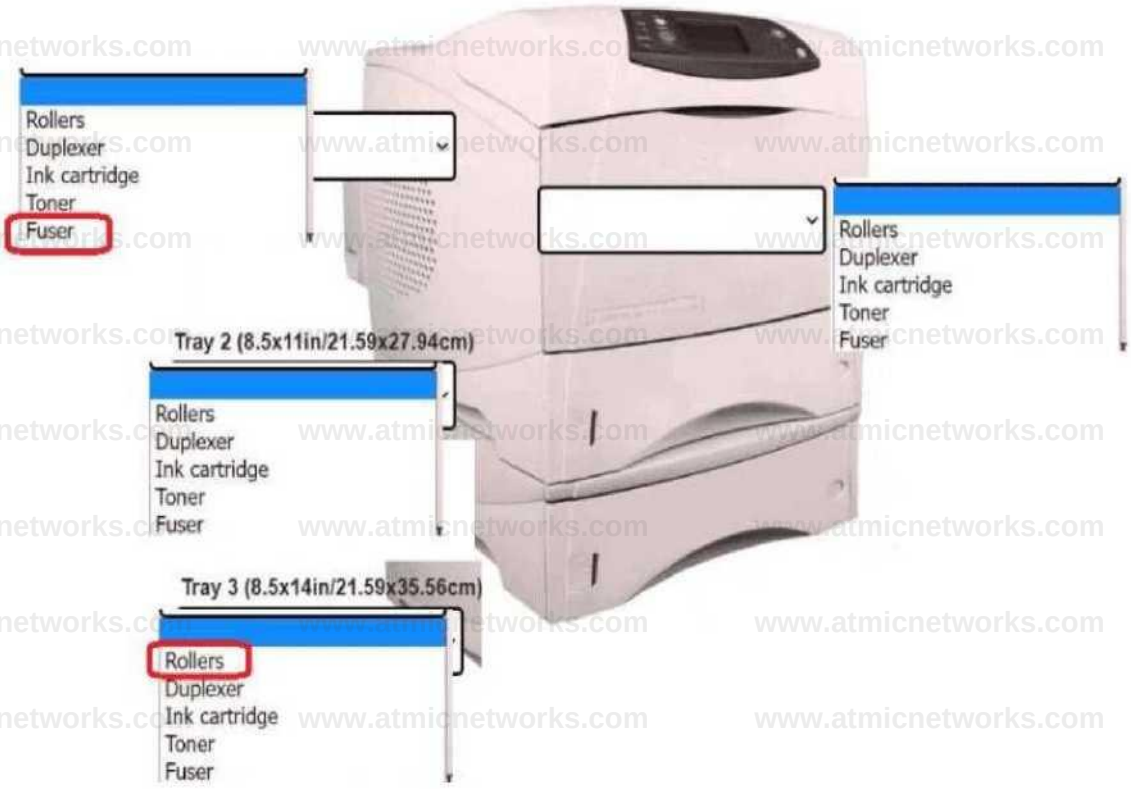
INSTRUCTIONS

Using the dropdown menus, select from the available printer parts to replace only the faulty components on the office printer to resolve the stated issues.

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

Explanation:

Answer:



A printer with text boxes AI-generated content may be incorrect.

Question: 329

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

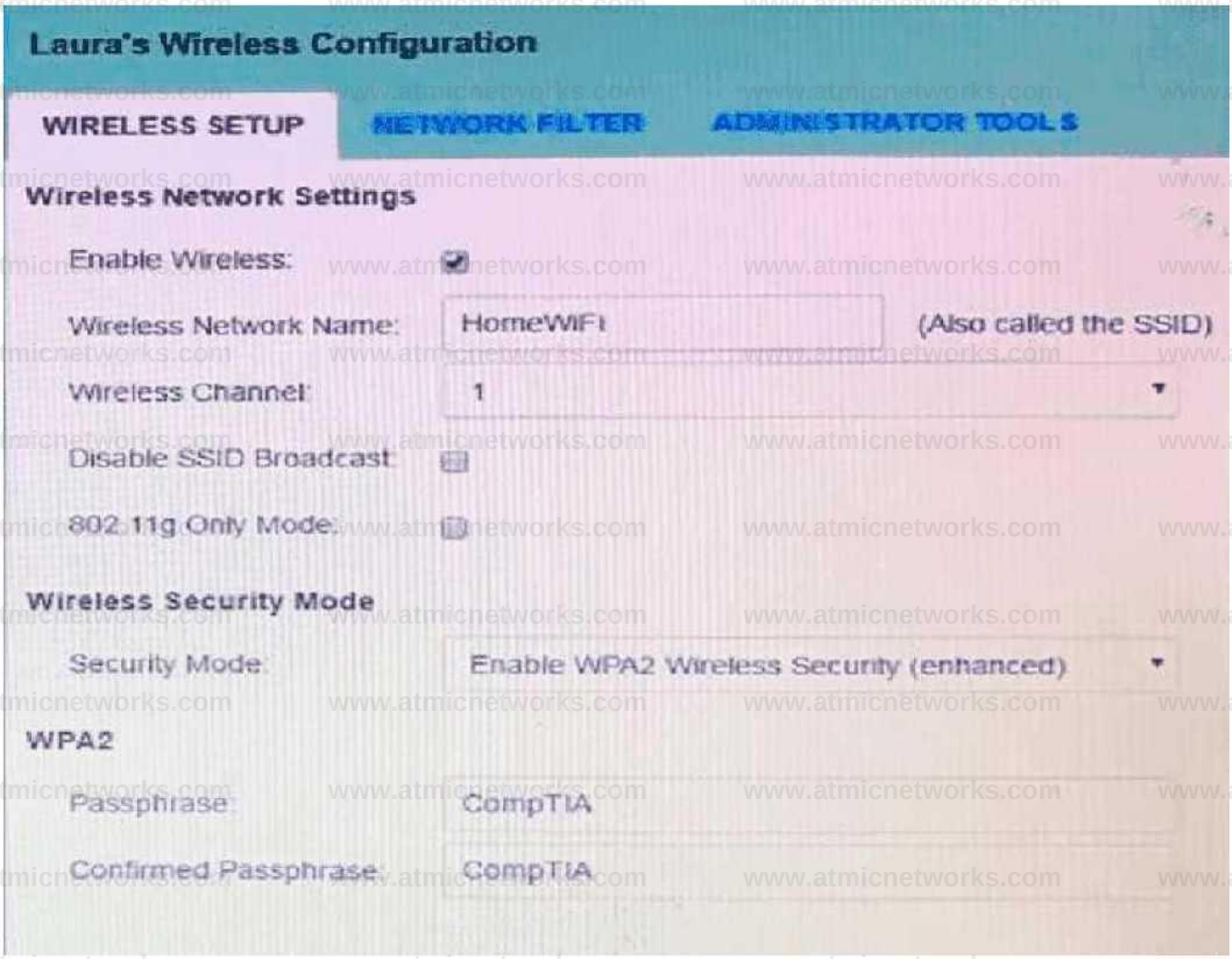
Hardware Address: 09:2C:D0:22:3F:11

INSTRUCTIONS

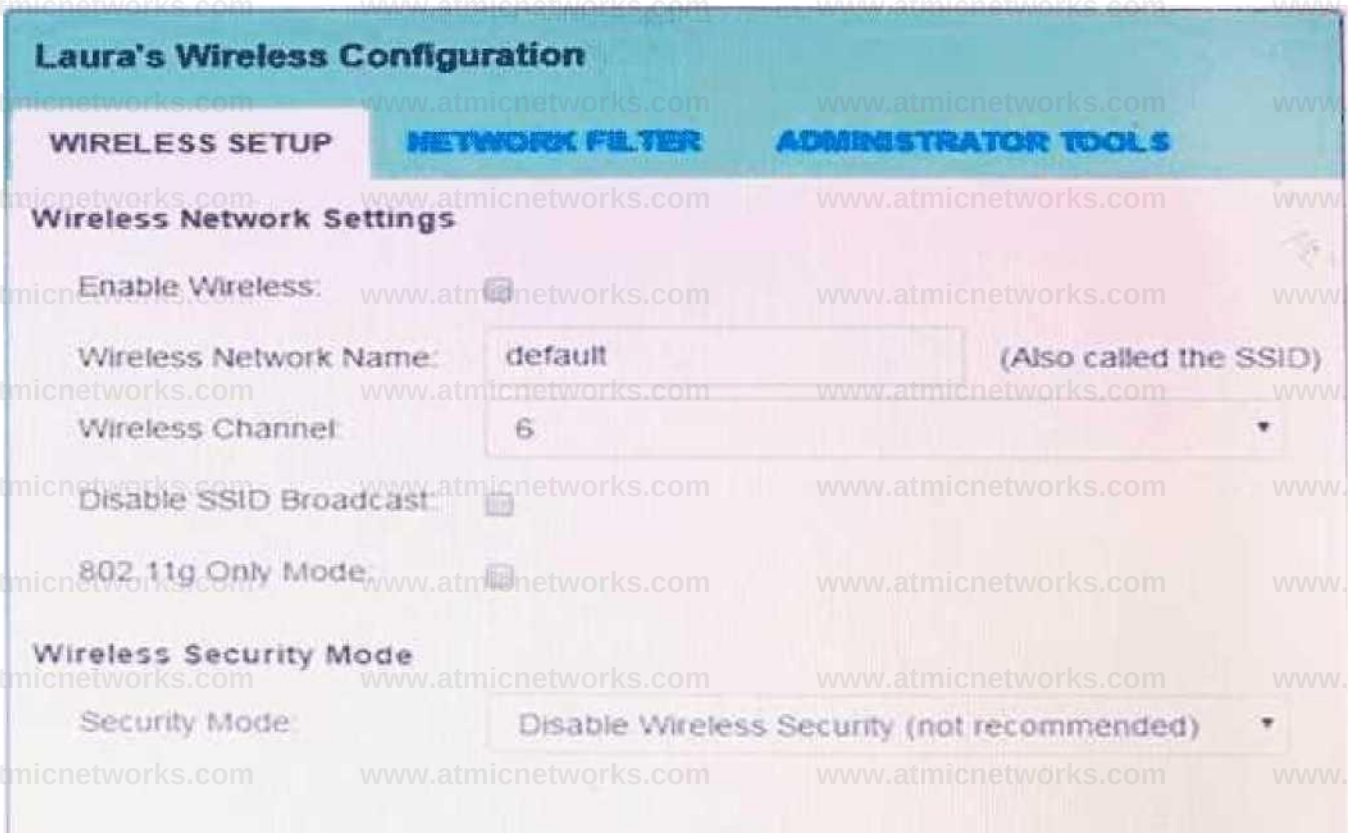
Configure Laura's wireless network using the network adapter window.

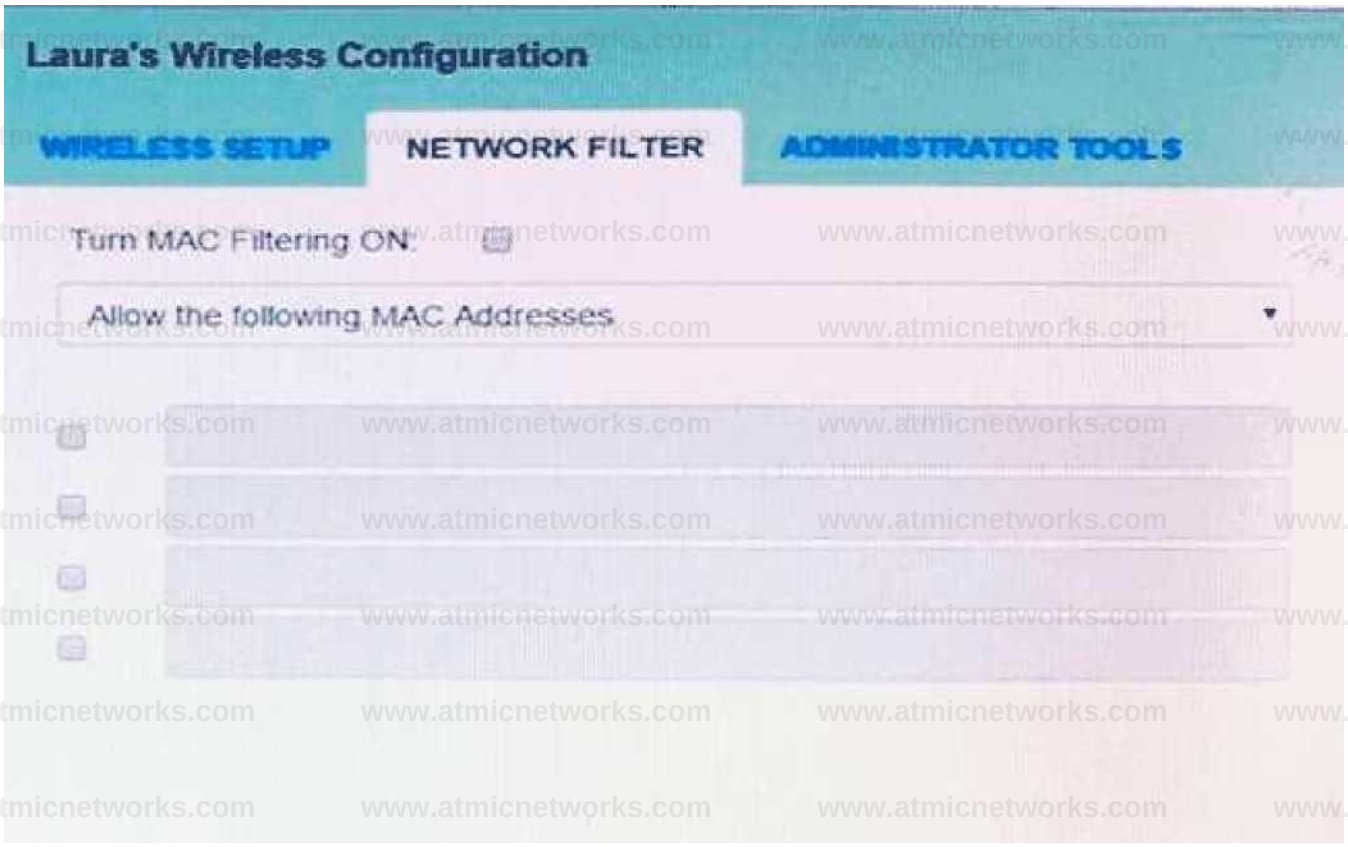
If at any time you would like to bring back the initial state of the situation, please click the Reset All button.

www.atmicnetworks.com


Laura's Wireless Configuration
WIRELESS SETUP
NETWORK FILTER
ADMINISTRATOR TOOLS
Wireless Network Settings
Enable Wireless:
Wireless Network Name:
HomeWiFi
(Also called the SSID)
Wireless Channel:
1
Disable SSID Broadcast:
802.11g Only Mode:
Wireless Security Mode
Security Mode:
Enable WPA2 Wireless Security (enhanced)
WPA2
Passphrase:
CompTIA
Confirmed Passphrase:
CompTIA


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:



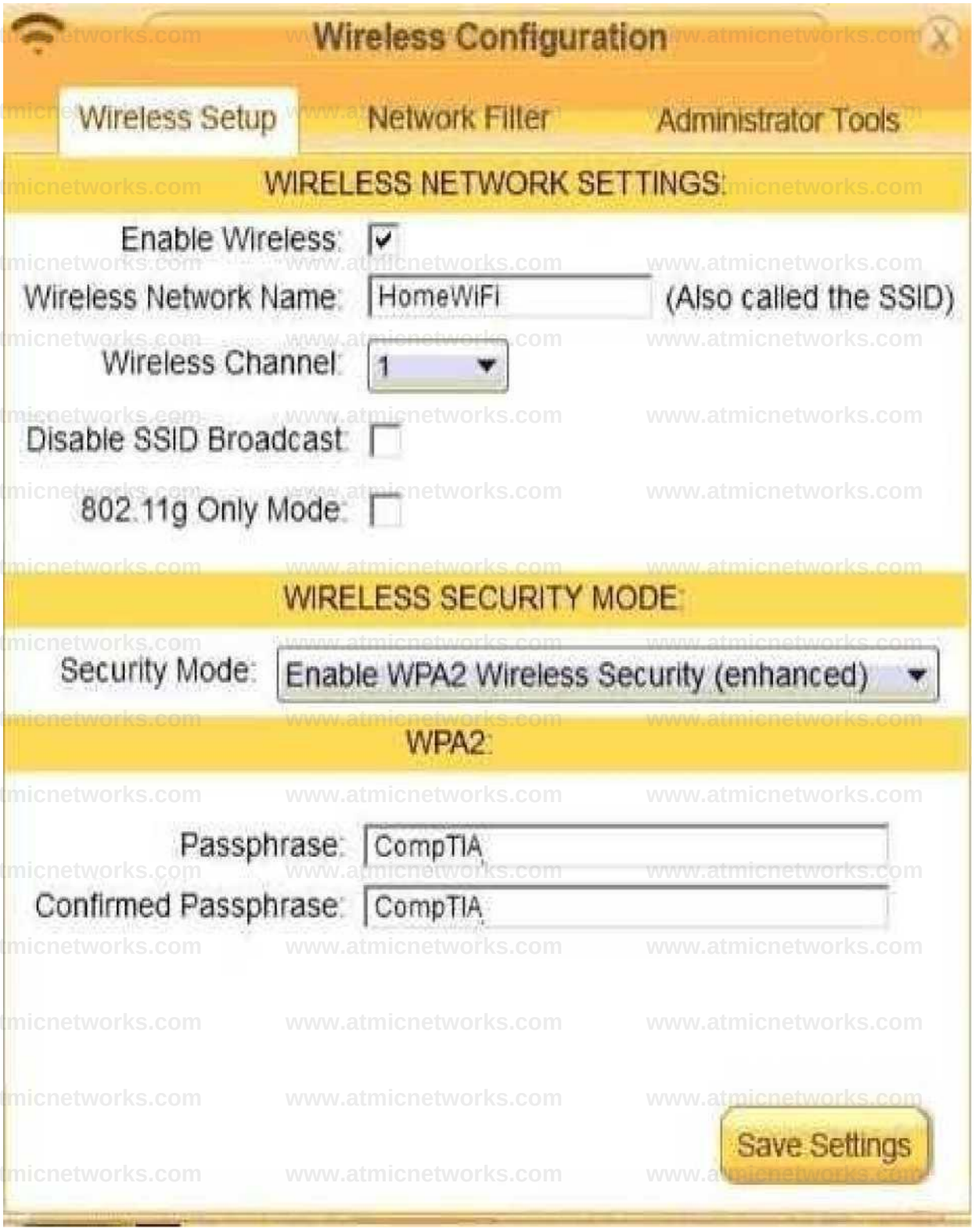


Answer: See the

www.atmicnetworks.com

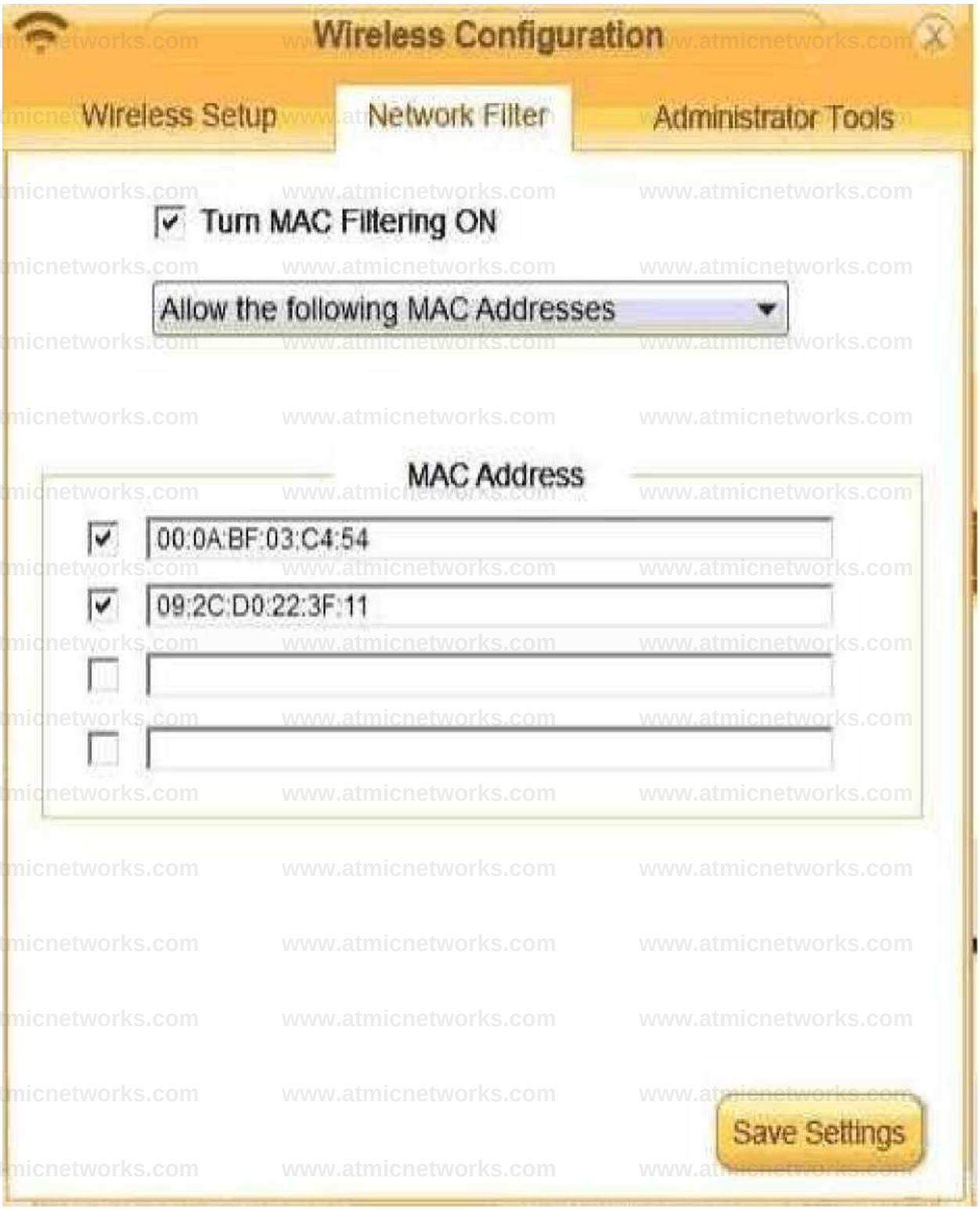
Explanation: **explanation below**

solution as



www.atmicnetworks.com

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

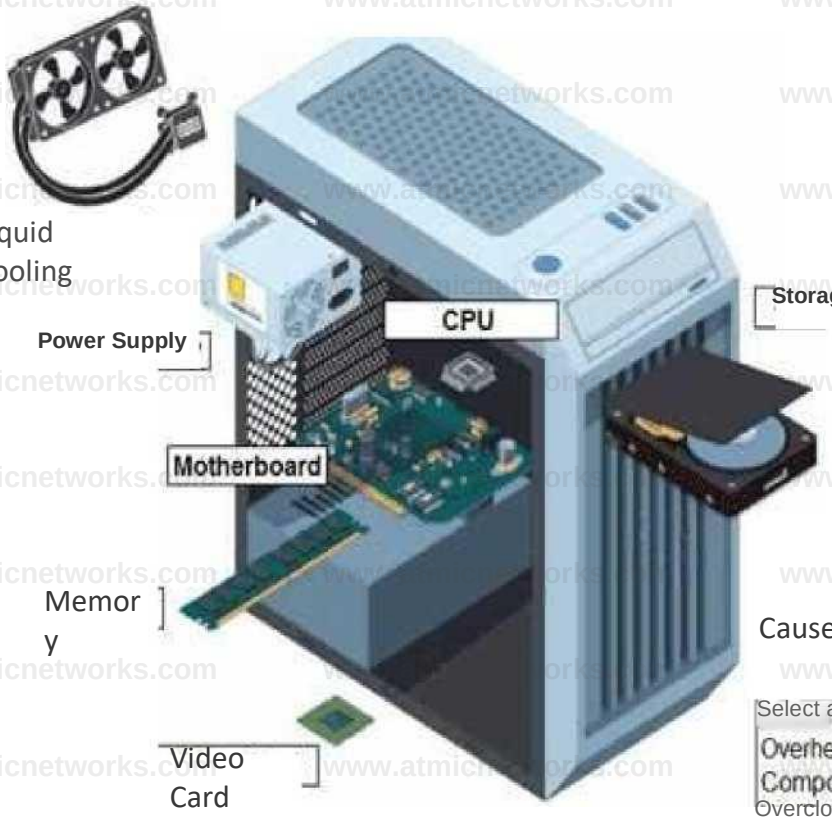


A screenshot of a computer AI-generated content may be incorrect.

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

Question: 330

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.



Answer:

Explanation:

correct answer is "Overclocking" and "Reduce CPU Clock speed" CPU is at 4.5 Ghz when normal is 3.2 Ghz. Overclocking too much can cause freezes, and this is a gaming computer sothe user probably

took it too far. http://blog.logicalincrements.com/2018/12/4-troubleshooting-tips-overclocking-pc/

Question: 331

DRAG DROP

A customer recently experienced a power outage at a SOHO. The customer does not think the components are connected properly. A print job continued running for several minutes after the power failed, but the customer was not able to interact with the computer.

Once the UPS stopped beeping, all functioning devices also turned off.

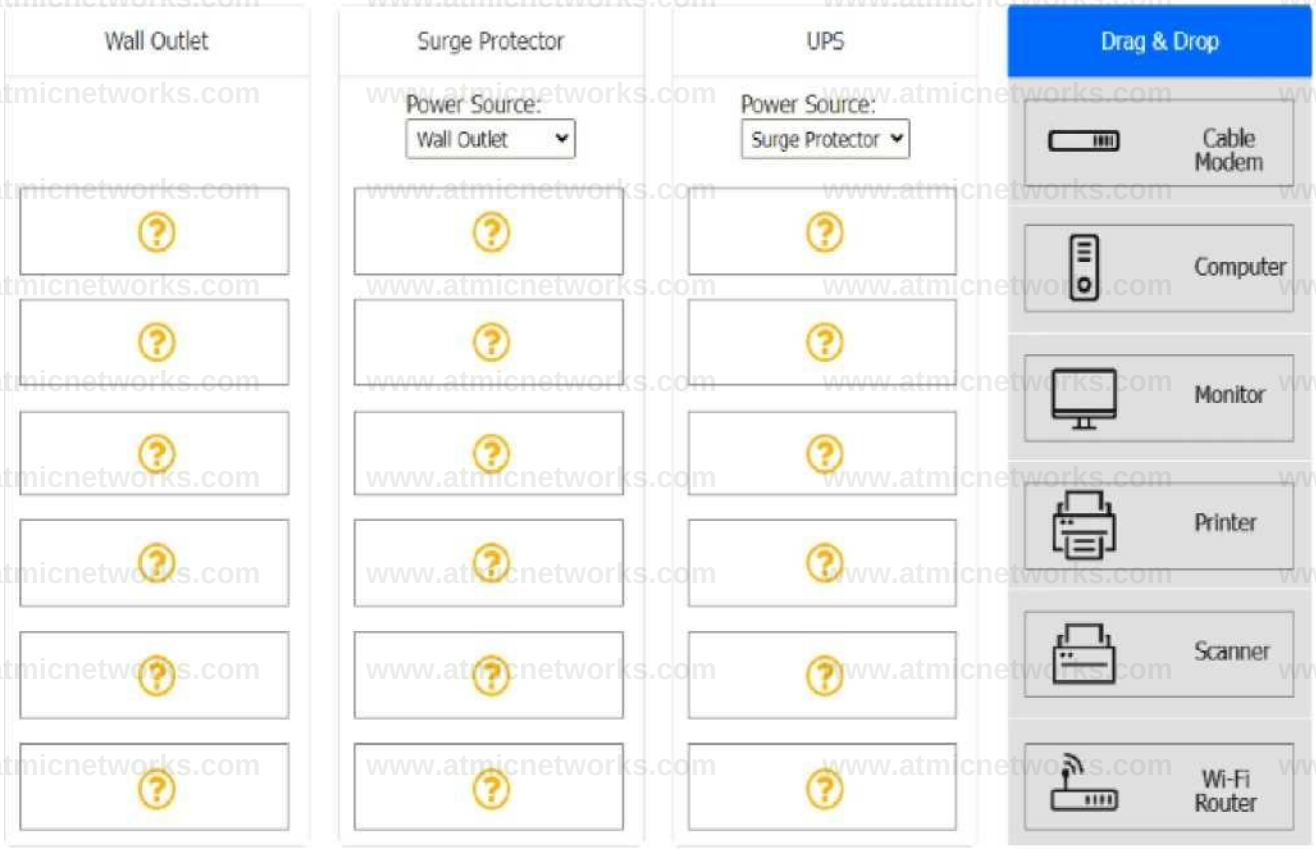
In case of a future power failure, the customer wants to have the most time available to save cloud documents and shut down the computer without losing any data.

INSTRUCTIONS

Based on the customer's requirements, connect the customer's devices to the proper outlets. Select the power source for the Surge Protector and UPS. This may require reselecting dropdowns or removing tokens.

Each token may only be used once.

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



Answer:

Explanation:

Wall Outlet

(empty — nothing goes directly to the wall)

Surge Protector (Power Source: Wall Outlet)

Printer

Scanner

UPS (Power Source: Surge Protector)

Computer

Monitor

Cable Modem

Wi-Fi Router

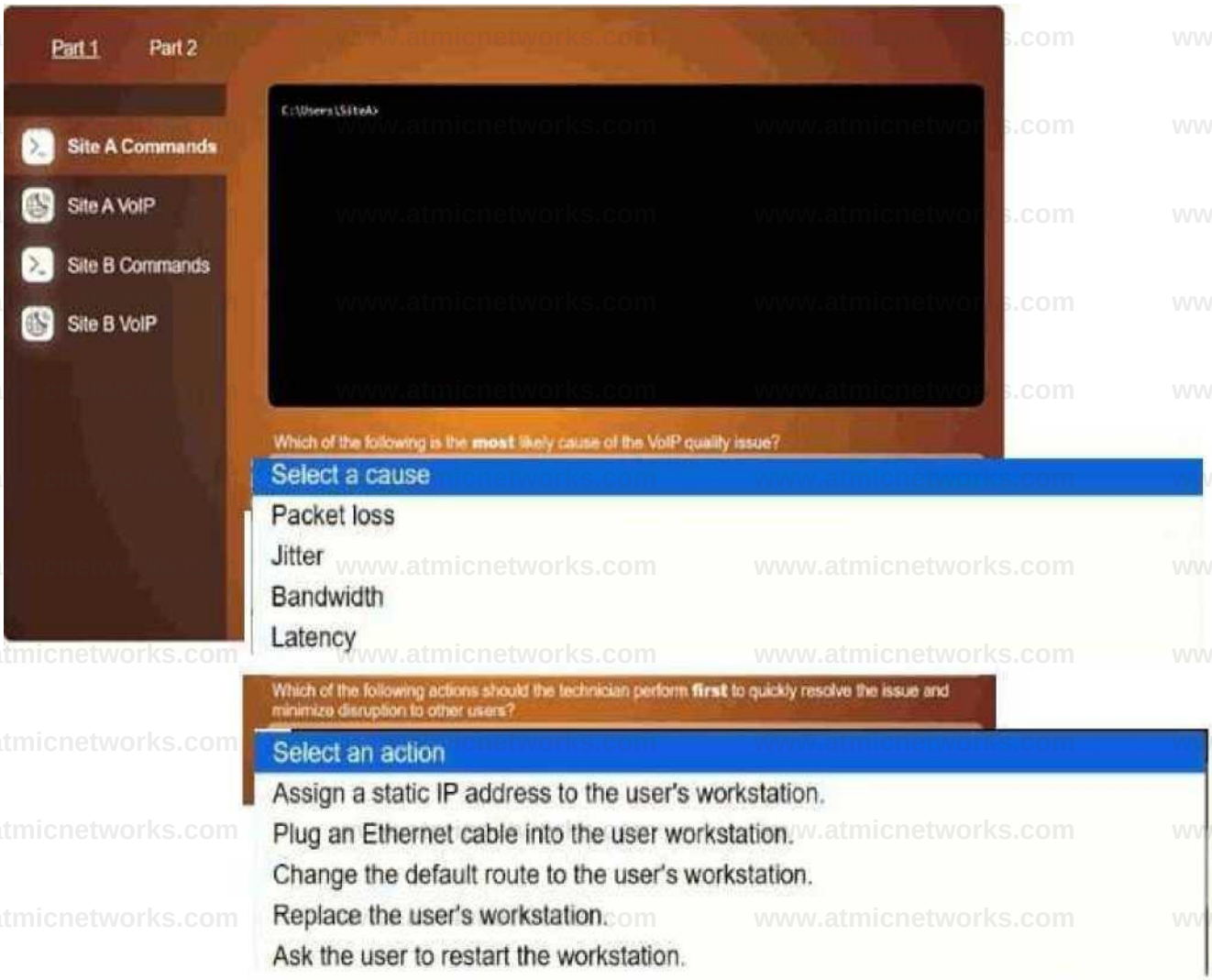
www.atmicnetworks.com

Question: 332

User at site A is reporting dropped VoIP calls when using a softphone application.

However, users at site B are not experiencing any issues. The VoIP provider has a tool to troubleshoot connectivity Issues.

Click on each tab to investigate the cause of the dropped calls. In Part 1, type help in each terminal to view a list of available commands. Then, select the correct answer for each question. In Part 2, make unnecessary network configuration changes to resolve reported issue.



www.atmicnetworks.com

Answer:

Packet loss

Plug an Ethernet cable into the workstation

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