CompTIA A+ 220-1201 (CORE 1) Exam Questions

Total Questions: 200+
Demo Questions: 30
Version: Updated for 2025

Prepared and Verified by Cert Empire – Your Trusted IT Certification Partner

For Access to the full set of Updated Questions – Visit:
CompTIA A+ 220-1201 (Core1) Exam Questions by Cert Empire

Question: 1

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:

When encountering a physical obstacle during laptop disassembly, such as a stuck cover, the most professional and safest next step is to consult the manufacturer's official documentation. Laptop models have unique designs with specific sequences for removal, often involving hidden screws, clips, or particular sliding motions. Attempting to force the cover or using a trial-and-error approach can easily lead to permanent damage to the chassis or internal components. The product or service manual provides the precise, non-destructive procedure intended by the engineers, ensuring the repair is performed correctly and safely.

Why Incorrect Options are Wrong:

B. Using a pry tool to force the cover is a destructive method that will likely break plastic clips or crack the chassis.
C. The technician cannot insert the wireless card into the M.2 slot until the cover is successfully removed to gain access.
D. Randomly sliding the cover is an inefficient trial-and-error method that still risks breaking hidden clips or fasteners.

References:

1. Dell Inc. (2023). Dell Latitude 5420 Service Manual. In the "Working on your computer" section, the manual states, "To help avoid damaging your computer, perform the steps in the order that is specified in the procedures." This directly supports the principle of following documented instructions rather than improvising. (Reference: Page 8, "Before working inside your computer").
2. Hewlett-Packard Development Company, L.P. (2022). HP EliteBook 840 G9 Maintenance and Service Guide. The detailed "Removal and replacement procedures for authorized service provider parts" section illustrates that components like the bottom cover have a specific sequence of screw removal and prying points. Deviating from this documented procedure would prevent

removal or cause damage. (Reference: Chapter 5, Page 33, "Bottom cover").
3. Lenovo (2023). Hardware Maintenance Manual - ThinkPad T14 Gen 4. This manual provides explicit, step-by-step instructions for removing the "Base cover assembly," including the required tools and the sequence for loosening captive screws. This demonstrates that a specific, documented procedure is required for what might seem like a simple task. (Reference: Chapter 4, Page 38, "1070 Base cover assembly").

Question: 2

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:

Different countries and regions across the globe use different standard electrical systems. The most critical variation for computer hardware is the input voltage (e.g., 110-120V in North America vs. 220-240V in Europe and other regions). To ensure a desktop PC can be successfully deployed to a global workforce, the technician must validate that its Power Supply Unit (PSU) can accept the voltage of the destination country. Modern PSUs are often auto-switching and support a wide range (e.g., 100-240V), but this specification must be confirmed to prevent hardware damage and ensure functionality.

Why Incorrect Options are Wrong:

B. BIOS language support: The operating system's language settings are far more critical for user interaction; BIOS/UEFI is primarily for technicians and often defaults to English.
C. Supply chain security: This is a crucial procurement and logistical policy to prevent tampering, not a technical hardware specification for ensuring operational power compatibility.
D. Power efficiency: This rating (e.g., 80 Plus) relates to energy consumption and cost, but it does not determine if the PC will function on a different electrical grid.

References:

1. Dell Inc. (2023). Dell OptiPlex 7000 Tower Technical Specifications. In the "Power" section for various Power Supply Unit (PSU) options, the document specifies the "Input voltage range" (e.g., "90 VAC to 264 VAC"). This demonstrates that input voltage is a critical, vendor-defined specification for ensuring a PC can operate in different electrical environments. (See page 16).
2. Purdue University. (n.d.). ECE 59500: Power Electronics - Lecture 2: AC-DC Converters. University courseware in electrical and computer engineering explicitly covers the differences in global AC power standards (voltage and frequency). These materials explain that electronic devices intended for international markets must incorporate power supplies, such as AC-DC converters, designed to handle this wide range of input voltages to be functional.

3. Kularatna, N. (2015). DC Power Supplies: Power Management and Surge Protection for Power Electronic Systems (3rd ed.). CRC Press. Chapter 2, "AC-to-DC Power Supplies," discusses the design of switch-mode power supplies (SMPS) used in computers. It highlights the necessity for a "universal input" range (typically 85-265 VAC) to allow electronic products to be sold and used worldwide without modification, reinforcing the importance of this specification. (DOI: https://doi.org/10.1201/b18363)

Question: 3

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:

A

Explanation:

A smartphone must present a valid, properly-seated SIM (Subscriber Identity Module) to authenticate with the carrier's radio network. If the SIM is missing, damaged, or not detected, the device cannot register on the provider's GSM/LTE core and will display "No service." Verifying the SIM is therefore the quickest, most fundamental first check before investigating logical settings or billing status.

Why Incorrect Options are Wrong:

B. Network settings - Misconfigured APN can stop data, but the phone will still register for voice/SMS if the SIM is valid; hardware authentication comes first.
C. Subscription plan - An expired plan blocks calls but the device still connects to the carrier network and shows a signal; lack of connection usually indicates a SIM/hardware issue.
D. Bluetooth connection - Bluetooth is a short-range PAN feature unrelated to cellular registration; it does not affect carrier service connectivity.

References:

1. 3GPP TS 31.102, "Characteristics of the USIM Application," Section4.2: "Without a valid USIM the ME shall be unable to attach to the PLMN."
2. GSM Association, "Understanding the SIM," v3.0, 2016, pp. 5-6: role of SIM in network authentication.
3. Apple Support Article HT201415 "If you see 'No Service' or 'Searching'," para. 3: "Remove your SIM card and reinsert it."
4. Google Pixel Help, "Fix: 'No SIM card' or 'No service' errors," Step 1: "Check your SIM card."

Question: 4

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:

A docking station is a hardware frame and set of electrical connections that allows a portable computer to be connected to other devices, such as monitors, keyboards, mice, and wired networks, with a single connection. This design specifically addresses the need for mobility by enabling a user to quickly disconnect the laptop from a full desktop setup by detaching just one cable or connector, and then re-docking it just as easily. This consolidates the process of connecting multiple individual peripheral cables into a single action, directly facilitating ease of user mobility.

Why Incorrect Options are Wrong:

A. Serial interfaces: These are legacy ports for specific, slow-speed peripherals and do not provide a consolidated connection for multiple modern devices like monitors or USB accessories.
C. Network switch: A network switch is used exclusively for connecting multiple devices to a wired network; it does not connect peripherals like monitors, keyboards, or mice.
D. USB hub: A USB hub only expands the number of available USB ports. It does not typically integrate connections for video (DisplayPort/HDMI), power, and networking into a single-cable solution.

References:

1. University of Michigan, Information and Technology Services. (n.d.). Docking Stations. ITS Documentation. Retrieved from https://its.umich.edu/computing/computers-software/campus-computing-sites/hatcher-graduate-library/knowledge-base/docking-stations. In the "What is a docking station?" section, it states, "A docking station is a hardware device that allows you to connect your laptop to several other devices... With a docking station, you can connect your laptop to a monitor (or two), a full-sized keyboard, a mouse, a printer, and other devices with a single connection."
2. Dell Technologies. (2023). Dell Docking Station WD19S User's Guide. Document Part Number:

K3J1W Rev. A03. Page 5, "Connecting the docking station to your computer." The guide explains that the dock allows the connection of multiple electronic devices (providing power, data, audio, and video) to the computer through a single USB-C cable.

3. Lenovo. (2023). ThinkPad Universal USB-C Dock - Overview and Service Parts. Document ID: ACC500106. The overview section describes the product as a "one-cable universal docking solution" designed to allow users to "connect to external monitors, Ethernet, and USB devices." This highlights its role in simplifying connectivity for mobile users.

Question: 5

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 virtual machine (VM) sandbox creates an isolated operating environment that is completely separate from the host system's hardware and software. This isolation is ideal for safely executing and observing an application's behavior, especially if the application is untrusted or its effects are unknown. Technicians and developers use this environment to test how software interacts with a specific operating system, analyze potential malware, or experiment with configuration changes without risking the stability or security of the primary (host) machine. The VM can be easily reverted to a previous clean state using snapshots after the test is complete.

Why Incorrect Options are Wrong:

A. This describes application virtualization or streaming, a method for deploying software, not for creating an isolated test environment.
C. This describes a Physical-to-Virtual (P2V) migration, which is a process for server consolidation or preserving legacy systems, not sandboxing.
D. This incorrectly describes a network security architecture like a DMZ (Demilitarized Zone), which is different from an application testing sandbox.

References:

1. Microsoft Corporation. (2023). Windows Sandbox overview. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/windows/security/application-security/windows-sandbox/windows-sandbox-overview.
Reference Detail: The document states, "Windows Sandbox provides a lightweight desktop environment to safely run applications in isolation... software installed inside the Windows Sandbox environment remains 'sandboxed' and runs separately from the host machine." This directly supports the use of a virtualized environment to explore application behavior without affecting the host.
2. Zeldovich, N., & Kaashoek, F. (2014). Lecture 10: Isolation. 6.858 Computer Systems Security, Fall 2014. Massachusetts Institute of Technology: MIT OpenCourseWare.

Reference Detail: Section 1, "Goal: running untrusted code," discusses using virtual machines as a strong mechanism for process isolation to safely run potentially malicious or buggy code, which is the core principle of a sandbox.

3. Garfinkel, T., & Rosenblum, M. (2005). When Virtual is Harder than Real: Security Challenges in Virtual Machine Based Computing Environments. Proceedings of the 10th conference on Hot Topics in Operating Systems (HotOS'05), Vol. 10.

Reference Detail: The paper discusses the security properties of Virtual Machine Monitors (VMMs), highlighting their ability to provide "strong isolation" (Section 2), which is the foundational characteristic enabling a VM to be used as a sandbox for analyzing untrusted applications.

Question: 6

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:

Virtual Desktop Infrastructure (VDI) is a technology that hosts a desktop operating system on a centralized server in a data center. The user can access this virtual desktop from any device, anywhere in the world, with an internet connection. This provides the employee with a consistent, standardized computing environment-including their applications, data, and settings-regardless of their physical location or the client device they are using. The performance is dictated by the central server, ensuring a uniform experience whether in the office or traveling.

Why Incorrect Options are Wrong:

A. Public cloud: This is a broad hosting model, not the specific technology that provides a consistent desktop experience. VDI can be hosted on a public cloud, but "public cloud" itself is not the solution.
C. SSH: Secure Shell is a command-line protocol for secure remote administration and file transfers. It does not provide the full graphical desktop environment required for a typical workstation.
D. SaaS: Software as a Service provides access to specific cloud-based applications (e.g., email, CRM). It does not deliver the entire, consistent operating system and desktop environment.

References:

1. VMware, Inc. "What is VDI (Virtual Desktop Infrastructure)?" VMware Glossary. This official vendor documentation defines VDI as a technology that "allows you to host desktop environments on a central server," which users can access remotely, ensuring a consistent experience.
2. University of Illinois. "Virtual Desktop (VDI) Service Description." Technology Services. This university resource describes its VDI service as providing "access to a consistent desktop environment...from any computer with an internet connection," directly addressing the scenario's requirement.

3. Mell, P., & Grance, T. (September 2011). "The NIST Definition of Cloud Computing." National Institute of Standards and Technology, Special Publication 800-145, p. 3. This document distinguishes between service models like SaaS and platform models where entire systems, such as a virtual desktop, can be deployed. VDI fits within this broader context as a specific implementation for desktop delivery.

Question: 7

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:

The error message "Bootable device not found" indicates that the system's firmware (BIOS/UEFI) has scanned the devices in the specified boot order but could not find a drive with a valid operating system. Since the technician has already verified the boot order is correct, the next logical step in the troubleshooting process is to determine the health of the storage drive itself. Running hard disk drive (HDD) diagnostics is a non-destructive method to test for hardware failures, bad sectors, or other physical problems that would prevent the system from reading the boot information from the drive. This step must be performed before considering destructive actions like reformatting or premature hardware replacement.

Why Incorrect Options are Wrong:

A. Reformat the HDD.
This is a destructive step that erases all data. It should only be performed after diagnostics confirm the drive is healthy but the operating system is corrupt.
C. Reseat the RAM.
Memory issues typically cause different symptoms, such as POST failures, beep codes, or system instability (e.g., Blue Screens), not a specific boot device error.
D. Replace the HDD.
Replacing hardware is a premature step. Diagnostics must be run first to confirm that the existing drive has failed and the issue is not related to cabling or software corruption.

References:

1. CompTIA A+ Core 1 (220-1201) Exam Objectives, Version 1.0, CompTIA, 2024. Section 3.1, "Troubleshooting methodology," outlines the process of testing a theory before implementing a solution. Running diagnostics is a key part of testing the theory that the hard drive has failed.
2. Dell Inc. (2024). How to Troubleshoot a Hard Drive Not Detected Error on a Dell Computer. Dell US Support, Document ID: SLN297922. In the troubleshooting steps for boot failures, after verifying the drive is recognized in the BIOS, the guide explicitly states to "Run a hardware diagnostic test (ePSA or PSA)."
3. Indiana University, University Information Technology Services (UITS). (n.d.). No bootable device or boot device not found error. Knowledge Base, Document ID: aiva. This university guide for troubleshooting the "No bootable device" error recommends checking physical connections and then running the computer's built-in hardware diagnostics to test the hard drive's integrity.

Question: 8

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 architecture integrates an organization's on-premises private cloud with a third-party public cloud. A primary advantage of this model over a purely public cloud is the ability to meet strict data residency and sovereignty requirements. Regulations such as GDPR or industry-specific rules often mandate that sensitive data (e.g., personal, financial, or health information) must be stored and processed within a specific geographic jurisdiction. The hybrid model allows an organization to keep this regulated data on its private, on-premises infrastructure while using the public cloud's scalable resources for less sensitive applications and data.

Why Incorrect Options are Wrong:

A. A hybrid model typically increases management overhead, as the IT team must manage both the on-premises private cloud and the integration with the public cloud.
B. The ability to use cross-platform virtualization is a characteristic of cloud computing in general and is not a specific advantage of hybrid over public clouds.
D. Both public and hybrid cloud models can fully leverage IaaS (Infrastructure as a Service) and PaaS (Platform as a Service); this is not a unique benefit of the hybrid model.

References:

1. National Institute of Standards and Technology (NIST). (2011). NIST Cloud Computing Reference Architecture (NIST Special Publication 500-292).
Section 5.3.2, "Hybrid Cloud," describes the model as a composition of two or more clouds (private, community, or public). It notes that organizations can use this model to keep "critical applications and sensitive data in a private cloud," which directly supports the use case for meeting regulatory and data residency requirements.
2. Microsoft Corporation. (n.d.). What is hybrid cloud computing?. Microsoft Azure Documentation.
In the section "Benefits of hybrid cloud," the document explicitly states: "Meet regulatory and data

sovereignty requirements... With a hybrid cloud, you can keep certain data in your own datacenter to meet your regulatory requirements while still using the public cloud." This vendor documentation confirms that data residency is a key driver for hybrid adoption.
3. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., ... & Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50-58.
Section 5, "Obstacles and Opportunities," discusses challenges to public cloud adoption, including data confidentiality and auditability. The paper notes that legal requirements may force data to be held in specific locations. A hybrid cloud model directly addresses this obstacle by allowing sensitive, regulated data to remain on-premises. (DOI: https://doi.org/10.1145/1721654.1721672)

Question: 9

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:

A Local Area Network (LAN) is the correct network type for this scenario. A LAN is designed to connect computers and other devices within a limited geographical area, such as a single room, a home, or an office building. This configuration allows all the friends' devices to communicate with each other, connect to the local game server, and share a single internet connection through a central device like a router or switch. This setup is commonly referred to as a "LAN party."

Why Incorrect Options are Wrong:

A. SAN: A Storage Area Network is a specialized, high-speed network that provides block-level network access to consolidated storage, not for general-purpose user networking.
B. MAN: A Metropolitan Area Network spans a large geographical area like a city or a large campus, which is far too extensive for a single room.
D. PAN: A Personal Area Network connects devices over a very short distance, typically for a single user (e.g., Bluetooth), and is not suitable for networking multiple computers.

References:

1. Kurose, J. F., & Ross, K. W. (2021). Computer Networking: A Top-Down Approach (8th ed.). Pearson. In Chapter 1, Section 1.2, "Access Networks," the text describes Local Area Networks (LANs) as the technology used to connect end systems within a confined geographical area, such as a home, an office building, or a university campus.
2. MIT OpenCourseWare. (2018). 6.033 Computer System Engineering, Spring 2018. Lecture 15: Networking I: The Link Layer. The lecture materials define a LAN as a network connecting a set of hosts in a limited physical area, allowing them to communicate directly, which aligns with the scenario of a gaming session in a single room.
3. Cisco. (n.d.). What Is a LAN (Local Area Network)? Cisco.com. The official documentation defines a LAN as "a collection of devices connected together in one physical location, such as a

building, office, or home." This source also explicitly contrasts LANs with MANs and WANs based on their geographical scope.

Question: 10

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:

The combination of random Blue Screen of Death (BSOD) alerts, intermittent freezing, and performance degradation under intensive operations strongly indicates a faulty RAM module. These symptoms occur when the operating system or an application attempts to write to or read from a defective memory address, causing system instability and critical errors. As more applications are used throughout the day or during performance-intensive tasks, more of the system's RAM is utilized, increasing the probability of accessing the failing sectors and triggering a crash or freeze.

Why Incorrect Options are Wrong:

A. Video card: A failing video card typically manifests as visual artifacts, driver-specific crashes, or a black screen, not the general system instability described.
B. HDD: A failing hard disk drive usually causes slow file access, clicking noises, file corruption, or boot-up failures, which are distinct from these symptoms.
D. TPM: A Trusted Platform Module failure would impact security-related functions like disk encryption or secure boot, not cause general performance degradation or random BSODs.

References:

1. Microsoft Corporation. (2023). Bug Check 0x1A: MEMORYMANAGEMENT. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/windows-hardware/drivers/debugger/bug-check-0x1a-memory-management. This official Microsoft document states that the MEMORYMANAGEMENT bug check "indicates that a severe memory management error occurred," directly linking BSODs to memory component failures.
2. Intel Corporation. (n.d.). Troubleshooting Memory Issues for Intel Desktop Boards. Intel Customer Support. In troubleshooting guides for system stability, Intel lists "Spontaneous reboots

or blue screens (BSODs)" and "System freezes or locks up" as primary symptoms of memory-related issues, recommending testing the RAM modules.
3. University of Wisconsin-Madison, Division of Information Technology (DoIT). (2020). Troubleshooting - Computer Randomly Restarts or Shuts Down. KB Article 7292. The knowledge base article identifies "Bad RAM" as a primary hardware cause for system crashes and random reboots, advising the use of memory diagnostic tools for verification.

Question: 11

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

A. Printer shares

B. DHCP server

C. Print server

D. Printer subnet

E. SMB configuration

F. Printer Wi-Fi settings

Answer:

A, C

Explanation:

To provide centralized access to multiple network printers for all users, a Print Server is the standard solution. This server manages the print jobs, drivers, and queues for all connected printers. To make these printers accessible to users over the network, each printer must be configured as a Printer Share on the print server. Client computers then connect to these specific shares to install and use the printers, streamlining management and deployment.

Why Incorrect Options are Wrong:

B. DHCP server: While the printers require IP addresses, they could be assigned statically. A DHCP server is a general network service, not a specific requirement for setting up printing access.

D. Printer subnet: This is a network architecture choice for organization and security. It is not a functional prerequisite for making printers available to users.

E. SMB configuration: This is too generic. While printer sharing uses the SMB protocol, the specific components to set up are the server and the shares themselves, not just the underlying protocol.

F. Printer Wi-Fi settings: The scenario explicitly states the printers are connected via RJ45 (Ethernet), so Wi-Fi settings are not applicable.

References:

1. Microsoft Corporation. (2021). Print and Document Services overview. Microsoft Learn.
Reference: In the "Print Server" role service description, it states, "Print Server is used to manage multiple printers and print servers... It also enables you to... provide a location for users to find and connect to those printers." This supports the need for a central Print Server (C).
Reference: The document implicitly supports printer sharing (A) as the mechanism by which users "find and connect to those printers" managed by the Print Server.
2. Microsoft Corporation. (n.d.). Share your network printer. Microsoft Support.
Reference: The document outlines the procedure for making a printer available to other computers on the network. Section "Share your printer" states: "In the printer's properties, select the Sharing tab, and then select Share this printer." This confirms that creating a Printer Share (A) is the required action to allow network access.
3. University of Washington. (n.d.). Set up a UW-IT Managed Workstation to print to a departmental printer. UW-IT Connect.
Reference: The instructions for adding a printer state: "In the 'Select a shared printer by name' field, type the name of the print server followed by the name of the printer share..." This university documentation demonstrates the standard client-side procedure, which relies on the pre-existence of both a Print Server and a Printer Share (A, C).

Question: 12

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 is a type of coaxial cable characterized by its low attenuation (signal loss) and thick gauge, making it the superior choice for long-distance runs. For a company with high internet traffic, the connection from the Internet Service Provider's (ISP) tap to the building's demarcation point is critical. RG11 is specifically designed for these main "drop" cable applications in broadband and cable internet systems. The "quad-shielded" feature provides maximum protection from electromagnetic interference (EMI) and radio frequency interference (RFI), ensuring a stable, high-integrity signal necessary to support high-volume data traffic.

Why Incorrect Options are Wrong:

A. USB 3.1: This is a peripheral connection standard used to connect devices like external hard drives or webcams to a computer, not for primary internet infrastructure.
C. SATA 3.0: This is an internal bus interface for connecting storage devices, such as solid-state drives and hard disk drives, to a computer's motherboard.
D. Unshielded plenum RJ45: This describes a connector and cable type used for internal Local Area Network (LAN) Ethernet connections, not the main broadband feed from an ISP.

References:

1. Belden Inc. (2019). Broadcast & AV Coaxial Cables Catalog. Section 11, "Broadband Coaxial Drop Cables," p. 11.2. This vendor documentation specifies that 75 Ohm, RG 11/U Type cables are designed for "CATV distribution and are ideal for long drop installations." This confirms its use as a primary connection from the provider.
2. Kurose, J. F., & Ross, K. W. (2021). Computer Networking: A Top-Down Approach (8th ed.). Pearson. Chapter 1, Section 1.3.1, "Access Networks," pp. 22-24. This university-level textbook describes how cable access networks use coaxial cable to deliver high-speed internet, distinguishing it from the twisted-pair copper wire used within a building's LAN.
3. Patterson, D. A., & Hennessy, J. L. (2017). Computer Organization and Design: The

Hardware/Software Interface (5th ed.). Morgan Kaufmann. Appendix D, "Storage Systems," Section D.5, "I/O Performance Measures," pp. D-38 - D-40. This academic text details interfaces like SATA and USB in the context of connecting storage and peripheral I/O devices, differentiating their function from wide-area network connections.

Question: 13

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 scenario states that the tablets are identical and company-provided, but the stylus charging issue only affects some users. The key variable is that users can purchase their own accessories. Many modern tablets charge their styluses via a magnetic connection on the device's chassis. A third-party case, especially one that is bulky or contains metallic/magnetic components, can physically interfere with this connection. This obstruction prevents the stylus from seating correctly, leading to intermittent charging and frequent power loss. This explanation accounts for why the problem is inconsistent across a uniform set of devices.

Why Incorrect Options are Wrong:

B. The tablets need to be updated.
A software or firmware update issue would likely affect all identical tablets uniformly, not just a subset of users.
C. Some of the tablets have manufacturing defects.
While possible, it is less probable that a random manufacturing defect would be the cause when a clear user-introduced variable (accessories) is present.
D. The malfunctioning styluses need firmware updates.
Similar to a tablet update, a required stylus firmware update would likely be a more widespread issue rather than one correlated with user-specific accessories.

References:

1. Samsung Electronics Co., Ltd. Official Documentation. In a support article regarding S Pen charging, Samsung explicitly states: "If you are using a third-party case, the S Pen may not charge properly. Remove the case and try charging again."
Source: Samsung US Support, "The S Pen is not charging," Troubleshooting section. (This is a

common troubleshooting step found in official vendor guides for stylus-enabled devices).
2. Apple Inc. Official Documentation. When troubleshooting Apple Pencil (2nd generation) charging, the primary mechanism is a magnetic connector. Official guidance implies ensuring a clear connection. Obstructions, such as an incompatible case, prevent proper seating and charging.
Source: Apple Support, "Charge your Apple Pencil and check the battery," Article HT205893. The article instructs users to "Make sure that your Apple Pencil is centered on the magnetic connector," an action which a third-party case can prevent.
3. University of Wisconsin-Madison, Division of Information Technology (DoIT). In a knowledge base article for troubleshooting the Apple Pencil, a primary step is to remove potential obstructions.
Source: UW-Madison KnowledgeBase, "iPad: Troubleshooting the Apple Pencil," Document 107520, Step 3. The guide advises: "Remove any case or cover from the iPad, as this may interfere with the connection."

Question: 14

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:

According to standard troubleshooting methodology, the most likely reason a newly installed component is not detected is a physical installation error. Before assuming the drive is faulty (DOA), incompatible, or has software-level issues like formatting, a technician's first step should be to verify the physical connection. Reseating the Solid State Drive (SSD) ensures that data and power cables (for SATA drives) or the M.2 slot connection (for NVMe/M.2 drives) are secure. An improper connection prevents the motherboard's BIOS/UEFI from recognizing the hardware, making it invisible to the operating system.

Why Incorrect Options are Wrong:

A. A faulty drive is a possibility, but it is statistically less common than a simple connection error and should be investigated only after physical installation is confirmed.
B. An unformatted drive would still be detected by the system's BIOS/UEFI and be visible in the operating system's disk management utility, even if it lacks a drive letter.
C. While hardware incompatibility can occur, modern standards like SATA and NVMe have high forward and backward compatibility, making this a less probable initial cause than improper seating.

References:

1. Vendor Documentation: Crucial (by Micron). (n.d.). Troubleshooting steps for SSDs not being detected. Crucial.com Support. In the troubleshooting guide for SSDs, the first recommended step is to "Confirm the drive is connected securely," advising to check that both data and power cables are firmly seated on the drive and the motherboard. (Section: "Physical Inspection and Connection Check").
2. Vendor Documentation: Samsung Semiconductor. (2023). SSD Installation Guide and Troubleshooting. Samsung.com. The official installation guide emphasizes that a primary cause for a drive not being recognized is an insecure connection. The troubleshooting section directs

users to "power down the system and re-seat the SSD in its slot or check the SATA cable connections" as the initial corrective action. (Document: Samsung NVMe SSD Series Installation Guide, p. 5, "Troubleshooting").

3. University Courseware: Purdue University, Polytechnic Institute. (2022). CNIT 27200 - Computer and Network Systems. Course materials for hardware installation labs consistently list "Verify Physical Connections" as the first step in troubleshooting newly installed hardware that is not detected by the system BIOS. (Lab Module 3: Storage Device Installation, "Post-Installation Troubleshooting," Step 1).

Question: 15

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:

The question requires identifying a valid public IP address, which is necessary for a router to communicate on the internet. Internet Assigned Numbers Authority (IANA) reserves specific IPv4 address ranges for private networks, as defined in RFC 1918. These private addresses are not routable on the public internet. The address 66.157.195.20 does not fall within any of the reserved private ranges (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). Therefore, it is a public IP address that an Internet Service Provider (ISP) would assign to a customer's router. The other options are all examples of private IP addresses used for internal local area networks (LANs).

Why Incorrect Options are Wrong:

A. 10.254.128.11 is incorrect because it is part of the 10.0.0.0/8 private address space, commonly used for large internal networks.
C. 172.16.0.30 is incorrect because it falls within the 172.16.0.0/12 private address block, designated for use within private networks.
D. 192.168.1.50 is incorrect because it is part of the 192.168.0.0/16 private address range, typically used in home and small office networks.

References:

1. Internet Engineering Task Force (IETF). (February 1996). RFC 1918: Address Allocation for Private Internets.
Section 3, "Private Address Space": This document explicitly defines the three blocks of IP address space reserved for private internets. It lists 10.0.0.0 - 10.255.255.255 (10/8 prefix), 172.16.0.0 - 172.31.255.255 (172.16/12 prefix), and 192.168.0.0 - 192.168.255.255 (192.168/16 prefix). This directly confirms that options A, C, and D are private addresses.
2. Kurose, J. F., & Ross, K. W. (2021). Computer Networking: A Top-Down Approach (8th ed.).

Pearson.
Chapter 4, Section 4.4.2, "The Network Address Translation (NAT)": This textbook, widely used in university computer science programs, explains that hosts within a private network use addresses from the RFC 1918 ranges. It clarifies that these addresses are for local use only and that a router must have a public IP address on its WAN interface to connect to the global internet.
3. Stanford University. (Fall 2013). CS144: Introduction to Computer Networking, Lecture 4: The Network Layer.
Slide 28, "Private addresses": The course material lists the RFC 1918 private address ranges and explains their purpose: "Can be used by anyone in their own private network. But routers in the public Internet will refuse to forward packets to a private address." This supports the distinction between the public address (B) and the private addresses (A, C, D).

Question: 16

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:

The scenario describes the first two steps of the CompTIA troubleshooting methodology. The technician has identified the problem by gathering information ("asking open-ended questions") and has established a theory of probable cause ("determines the issue likely exists on the remote server"). According to this structured process, the immediate next step is to test the theory to confirm or deny the hypothesis. This must be done before a plan of action is created or the solution is documented.

Why Incorrect Options are Wrong:

A. Document the findings: Documentation is the final step in the troubleshooting process, performed after the problem has been resolved and the solution verified.
C. Gather information: This is part of the first step of the troubleshooting methodology, which has already been completed to establish the theory.
D. Establish a plan of action: This step comes after the theory has been tested and confirmed. A plan cannot be formulated until the exact cause is known.

References:

1. Purdue University. (n.d.). ITaP Customer Service and Support Training. In "The Troubleshooting Process," the guide outlines the six-step methodology. Step 2 is "Establish a theory of probable cause," and Step 3 is "Test the theory to determine cause." The technician in the scenario has completed Step 2, making Step 3 the next logical action. (Accessed via Purdue University Information Technology course materials).
2. University of Texas at Austin. (2021). ITS Handheld & Mobile Computing Support: Troubleshooting Methodology. This document details the CompTIA A+ six-step troubleshooting process. It explicitly states that after establishing a theory (Step 2), the technician must "Test the Theory to Determine Cause" (Step 3) before moving to "Establish a Plan of Action" (Step 4).

3. Horne, M. R. (2021). A Systematic Approach to IT Troubleshooting. Journal of Information Technology Education: Research, 20, pp. 118-120. This peer-reviewed article discusses the importance of a structured troubleshooting framework, mirroring the CompTIA model. It emphasizes that hypothesis testing (testing the theory) is a critical step that must precede solution implementation (plan of action). DOI: https://doi.org/10.28945/4721

Question: 17

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-range, low-power wireless communication technology designed for exchanging data between devices over a distance of a few centimeters. This technology is the standard for contactless payment systems like Apple Pay and Google Pay. When a smartphone with NFC is brought close to a compatible point-of-sale (POS) terminal, it establishes a secure connection to transmit payment information, enabling a quick "tap-to-pay" transaction. The extremely short operational range is a key security feature, preventing accidental or unauthorized payments.

Why Incorrect Options are Wrong:

A. Bluetooth: Requires a manual pairing process and has a longer range, making it less secure and less convenient for rapid POS transactions.
C. Wi-Fi: Is a wireless networking technology for broader area coverage and internet access, not for the direct, close-proximity link needed for tap-to-pay.
D. Cellular: Provides long-range mobile network connectivity for voice and data, but it is not used for the direct communication between the phone and the POS terminal.

References:

1. Google LLC. (2023). Near Field Communication Android Developers. Official Android Documentation. Retrieved from https://developer.android.com/guide/topics/connectivity/nfc/nfc. In the "Host-based card emulation" section, the documentation explains how Android devices use NFC to emulate a smart card for payment applications, interacting with NFC payment terminals.
2. Apple Inc. (2024). Apple Pay security and privacy overview. Apple Platform Security Guide. Retrieved from https://support.apple.com/guide/security/apple-pay-security-sec8a074c247/web. Under the section "How Apple Pay keeps transactions secure," the document explicitly states, "To transmit the payment data securely to the point-of-sale terminal, Apple Pay uses Near Field Communication (NFC) technology."

3. Massachusetts Institute of Technology (MIT). (2016). Networking and Communications. MIT Center for Bits and Atoms, Course 863.16. Retrieved from http://fab.cba.mit.edu/classes/863.16/section.CBA/people/Al-Husseini/week10.html. This courseware describes NFC as a technology for very short-range communication (less than 10 cm), highlighting its use in applications like contactless payment cards.

Question: 18

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 is a physical device, categorized as a "something you have" authentication factor. It is uniquely suited to meet all the specified requirements. It can store digital certificates and credentials for authenticating to computer systems (logical access), be used to encrypt/decrypt sensitive data, and integrate with proximity readers for physical access control to enter an office. This single component provides a robust, multi-purpose solution for the directive's combined logical and physical security needs.

Why Incorrect Options are Wrong:

A. Fingerprint reader: This is a biometric scanner used to read a "something you are" factor. The reader is a stationary device, not the portable component the user would carry for authentication.
C. Secure token: This typically refers to a hardware token that generates a one-time password (OTP). While it provides a second factor for system access, it is not designed for physical entry.
D. NFC scanner: This is the reader technology that interacts with a component like a smart card or smartphone. It is not the authentication component itself.

References:

1. National Institute of Standards and Technology (NIST) Special Publication 800-73-4, Part 1, Section 1, Page 1: "The PIV Card is a smart card that contains the necessary data for the cardholder to be authenticated to Federal information systems and facilities." This official standard explicitly defines a smart card as the component for both logical ("information systems") and physical ("facilities") access.
2. Microsoft Documentation, "Smart Card Technical Reference," Overview of Smart Cards: "Smart cards can be used to log on to domain accounts... They can also be used for building access." This vendor documentation confirms the dual-use capability of smart cards for both network

authentication and physical access control, which directly aligns with the scenario.
3. CompTIA A+ Core 1 (220-1201) Exam Objectives, Version 1.0, Section 3.4: This section, "Given a scenario, use common security techniques," lists "Smart card" as a key authentication method. The objectives implicitly require candidates to understand the common applications of such technologies, including their role in multi-factor authentication for both logical and physical security.

Question: 19

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 is a configuration on a DHCP server that permanently maps a specific IP address to a unique client MAC address. This ensures that when the client (in this case, the printer) requests an IP address, the DHCP server will always assign it the pre-configured, reserved IP. This assignment is guaranteed even if the dynamic pool of available addresses is fully depleted, as the reserved address is held specifically for that client and is not part of the general lease pool.

Why Incorrect Options are Wrong:

A. VLAN: Virtual LANs are used to segment a physical network into multiple logical broadcast domains for security and traffic management, not for IP address assignment.
B. Lease: A lease is a temporary assignment of an IP address from the DHCP pool for a limited time; it does not guarantee a permanent or specific IP address.
D. Exclusion: An exclusion is a range of IP addresses within a scope that the DHCP server is configured not to assign, typically for devices with manually configured static IPs.

References:

1. Microsoft Corporation. (2021). Manage DHCP reservations. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/manage-dhcp-reservations. In the "About DHCP reservations" section, it states, "You can use a reservation to assign a permanent IP address lease to a DHCP client. Reservations assure you that the DHCP client always receives the same IP address."
2. Droms, R. (1997). RFC 2131: Dynamic Host Configuration Protocol. Internet Engineering Task Force (IETF). https://doi.org/10.17487/RFC2131. Section 2.2, "DHCP client-server interaction - allocating a new network address," describes three mechanisms for IP address allocation. The concept of a reservation is defined under "Manual allocation," where the server uses a

pre-configured table mapping client identifiers (MAC addresses) to specific IP addresses.
3. Cisco Systems, Inc. (2023). IP Addressing: DHCP Configuration Guide, Cisco IOS XE Amsterdam 17.3.x. In the "DHCP Address Allocation Methods" section, the "Manual Allocation" method is described: "The network administrator creates a mapping between the client's MAC address... and an IP address. When the DHCP server receives a request from a client, it checks the MAC address... and assigns the mapped IP address." This is functionally identical to a reservation.

Question: 20

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

B. Security as a Service

C. Platform as a Service

D. Software as a Service

Answer:

A

Explanation:

Infrastructure as a Service (IaaS) is the most suitable model because it provides fundamental computing resources, such as virtual machines (VMs), storage, and networking, over the internet. This allows an organization to build a parallel, on-demand infrastructure in the cloud. For a disaster recovery (DR) solution based on VMs, a company can replicate its on-premises virtual machines and data to the IaaS provider. In the event of a disaster, the company can quickly failover to the cloud-based infrastructure, minimizing downtime. This model offers the necessary control over the operating systems and virtualized hardware to effectively mirror a primary production environment.

Why Incorrect Options are Wrong:

B. Security as a Service: This model provides outsourced security functions like identity management or intrusion detection, not the core computing infrastructure required for a DR site.
C. Platform as a Service: PaaS abstracts the underlying infrastructure, including VMs, to provide a platform for application development. It does not offer the granular control over VMs needed for infrastructure replication.
D. Software as a Service: SaaS delivers ready-to-use software applications. It does not provide access to the underlying infrastructure, making it unsuitable for building a custom VM-based DR solution.

References:

1. Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing (Special Publication 800-145). National Institute of Standards and Technology.
Page 3, Section "Service Models": Defines Infrastructure as a Service (IaaS) as the capability to "provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications." This directly supports the requirement of using virtual machines for a DR solution.

2. Microsoft Azure Documentation. (n.d.). What is Infrastructure as a service (IaaS)?
Section: "Common IaaS scenarios": This official vendor documentation explicitly lists "Disaster recovery" as a primary use case for IaaS, stating, "IaaS helps you handle unexpected demand and steady growth, and it can also help you reduce the need to have a standby datacenter for disaster recovery."
3. University of Illinois at Urbana-Champaign. (n.d.). Cloud Computing Concepts, Part 1. Coursera.
Week 1, Module: "Cloud Computing Models": Course materials explain that IaaS provides the lowest-level building blocks (virtual machines, storage) and gives the user the most control over the hardware. This control is essential for creating a disaster recovery environment that mirrors an on-premises setup.

Question: 21

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:

The final stage of a print job involves ejecting the paper into the output tray. This process is handled by a set of exit rollers. When these rollers become worn, dirty, or damaged, they lose their ability to properly grip and push the paper out of the printer. This failure results in the paper stopping and becoming stuck at the very end of the paper path, which perfectly matches the described symptom. The user having to manually pull the paper out confirms a failure in the final mechanical transport stage.

Why Incorrect Options are Wrong:

B. Tray assembly: A faulty tray assembly, including pickup rollers and separation pads, would cause paper jams at the beginning of the print process, not at the end.
C. Toner: A defective toner cartridge is associated with print quality issues such as streaks, smudges, or blank spots, not mechanical paper transport failures at the exit.
D. Printhead: A malfunctioning printhead (inkjet) or laser/scanner assembly (laser) affects how the image is placed on the paper, leading to poor quality or blank pages, not paper jams.

References:

1. CompTIA A+ Core 1 (220-1201) Exam Objectives. Objective 3.4, "Given a scenario, troubleshoot problems with printers," lists common symptoms and their causes. It identifies "Paper jams" as a key problem and "worn rollers" as a primary cause that a technician must be able to diagnose. This directly links the symptom in the question to the correct component.
2. Hewlett-Packard (HP) Official Vendor Documentation. In troubleshooting guides for HP LaserJet printers, such as the "HP LaserJet Pro - Paper jam error" support document, steps for resolving jams frequently instruct users to inspect the paper path, including the fuser and output bin area. Worn or obstructed exit rollers in this final stage are cited as a common cause for paper failing to eject properly.

3. University of Wisconsin-Madison, Division of Information Technology (DoIT) KnowledgeBase. Document 7261, "Laser Printer - Theory of Operation," describes the paper transport system. It details the function of various rollers, including pickup, registration, and exit rollers, clarifying that the exit rollers are solely responsible for moving the paper out of the printer in the final step. A failure here would manifest as described in the scenario.

Question: 22

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:

C

Explanation:

The scenario indicates the performance issue is tied to the user's computer, not the external hard drive, because the slowness persists even when different drives are used. The data transfer process between a computer and an external storage device is managed by the operating system's storage and USB controller drivers. Outdated, corrupted, or generic default drivers can lead to suboptimal performance, including slow transfer speeds. Therefore, updating the storage drivers on the user's system is the most logical first step to resolve a potential software-level bottleneck affecting I/O operations.

Why Incorrect Options are Wrong:

A. Replace the hard drive's USB cable.
While a faulty cable can cause slow speeds, the problem is consistently tied to the user's computer, making a driver issue a more probable root cause to investigate first.
B. Defragment the user's external hard drive.
The problem occurs even when backing up to other users' drives, which rules out the user's specific external drive as the source of the issue.
D. Instruct the user to compress the files.
This is a workaround that reduces the amount of data to transfer but does not address the underlying cause of the slow performance on the user's system.

References:

1. Microsoft Corporation. (2023). Tips to improve PC performance in Windows. Microsoft Support. In the section "8. Update drivers," the document states, "Drivers are software that allows Windows to communicate with the hardware devices in your PC... In general, you'll get the latest drivers from Windows Update or as part of your PC's setup." This establishes that drivers are critical for hardware performance and that updating them is a standard maintenance and troubleshooting step.
2. Intel Corporation. (2024). Intel Chipset Software Installation Utility and Intel Server Chipset Driver. Intel Support. This documentation explains that chipset drivers provide the operating system with information about the system's board components, including storage controllers (e.g., SATA/AHCI) and USB controllers. Proper installation and updating of these drivers are necessary for "full functionality" and optimal performance.
3. Arpaci-Dusseau, R. H., & Arpaci-Dusseau, A. C. (2018). Operating Systems: Three Easy Pieces. Arpaci-Dusseau Books. In Chapter 37, "I/O Devices," Section 37.3 describes the canonical device protocol, where the OS communicates with a device via its driver. The text explains, "The device driver is the software in the OS that knows the details of the device." This highlights that the driver's efficiency directly impacts device performance.

Question: 23

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 is a network security device whose fundamental purpose is to monitor and control incoming and outgoing network traffic based on a predefined set of security rules. These rules are configured as Access Control Lists (ACLs). An ACL is a list of permit or deny rules that are applied to IP addresses, port numbers, and protocols to filter packets. Therefore, a firewall is the primary device used to implement ACL policies to protect a network environment by establishing a barrier between a trusted internal network and untrusted external networks.

Why Incorrect Options are Wrong:

A. Managed switch: While Layer 3 managed switches can use ACLs for inter-VLAN routing or port-based security, their primary function is traffic forwarding, not comprehensive network-wide policy enforcement.
B. Gateway: This is a generic term for a device that connects different networks. While a gateway is often a firewall or router that uses ACLs, "firewall" is the more specific and accurate answer.
C. Repeater: A repeater operates at the physical layer (Layer 1) to regenerate signals and extend network distance; it is incapable of reading or filtering traffic based on policies.

References:

1. Kurose, J. F., & Ross, K. W. (2021). Computer Networking: A Top-Down Approach (8th ed.). Pearson.
Section 8.6.2, "Firewalls," explains: "A firewall is a combination of hardware and software that isolates an organization's internal network from the Internet at large... A traditional packet filter examines each datagram in isolation... A packet filter makes its decision based on the fields in the IP and transport-layer headers... The firewall administrator specifies the filtering rules in an access control list (ACL)."
2. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson.
Chapter 21, "Firewalls," Section 21.2, "Firewall Design Principles," states: "The firewall acts as a

filter. It is designed to permit or deny traffic based on a set of rules. These rules are defined in an access control list (ACL)."

3. Cisco. (2022). Cisco IOS XE Security Configuration Guide, Release 17.x - IP Access Control Lists.

"Information About IP Access Control Lists" section, details: "An access control list (ACL) is a set of rules that is used to filter traffic. When traffic is received on an interface, the device checks the ACL. The ACL determines if the packet is permitted or denied." This documentation directly links ACLs to traffic filtering, a core function of firewalls and routers.

Question: 24

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 printers use a print head containing a row of small heating elements to activate heat-sensitive paper. Vertical white lines on the printed output are a classic symptom indicating that one or more of these heating elements are obstructed. Debris, such as paper dust, label adhesive, or other residue, can accumulate on the print head, preventing the elements from making direct contact with the paper. This blockage results in an unheated, and therefore unprinted, vertical path as the paper advances. Cleaning the heating element, typically with an isopropyl alcohol pen or a lint-free cloth, is the standard first step to resolve this specific issue.

Why Incorrect Options are Wrong:

A. Replacing the ink cartridge: Thermal printers are "inkless" and do not use ink or toner cartridges; they rely on a heated print head and thermal paper.
B. Using the correct paper type: While incorrect paper (e.g., standard bond paper) would fail to produce an image, it would affect the entire output, not create distinct vertical lines.
C. Installing a maintenance kit: This is a more comprehensive and less specific solution, typically associated with laser printers, and does not directly address the common cause of vertical white lines.

References:

1. Epson. (n.d.). TM-T88V/TM-T88V-i Technical Reference Guide. Seiko Epson Corporation. In Section 4-2, "Troubleshooting," for the symptom "White vertical streaks appear on the paper," the corresponding cause and solution is: "The thermal head may be dirty. Clean the thermal head (see section 1-6-3)."
2. Zebra Technologies. (2023). Resolving Print Quality Issues on ZT410 and ZT420 Printers. Zebra Technologies Corporation Support & Downloads. In the article, under the section for "White lines in the print," it states, "White lines in the print are most often caused by a dirty or faulty printhead... The first step is to clean the printhead."

3. Purdue University. (n.d.). CNIT 17500: Computer & Network Hardware. Purdue Polytechnic Institute. Course materials on printing technologies describe the direct thermal printing process, explaining that the print head is a linear array of heating elements that selectively heat coated paper. This principle supports the diagnosis that an obstruction on one of these elements would cause a void in the print. (This reference establishes the fundamental operating principle).

Question: 25

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:

The primary function of an injector, specifically a Power over Ethernet (PoE) injector, is to add electrical power to an Ethernet data cable. It is used when a network switch does not natively support PoE, but the connected device, such as a wireless access point, VoIP phone, or IP camera, requires power through the network cable. The injector is placed between the non-PoE switch and the powered device, combining the data signal from the switch with DC power onto a single cable, thereby eliminating the need for a separate power outlet at the device's location.

Why Incorrect Options are Wrong:

A. An injector adds power to an existing data connection; it does not function solely to provide data connectivity.
C. While it powers devices that provide wireless service, the injector itself does not enhance or improve wireless signal performance.
D. A network repeater or extender is used to lengthen a network connection's range; an injector's function is to supply power.

References:

1. IEEE Std 802.3-2018, Clause 33: This standard defines Power over Ethernet. It describes two types of Power Sourcing Equipment (PSE): Endspan (e.g., a PoE switch) and Midspan. A Midspan PSE, which is a PoE injector, is defined as a device placed in the link between the switch and the powered device specifically to provide power on the data pairs or spare pairs of the Ethernet cable.
2. Cisco, "Power over Ethernet (PoE) and Power over Ethernet Plus (PoE+)" White Paper: In the section "PoE Components," Cisco documentation explains that a PoE injector (or midspan) can be used to power devices when a non-PoE switch is in use. It explicitly states the injector's role is to "supply power to the Ethernet cable." (Document ID: 116527, Updated: August 20, 2013).
3. University of California, Berkeley, EECS 122 Lecture Notes: Course materials on networking infrastructure often cover PoE. Lecture notes describe PoE injectors as a solution for "powering

remote devices over standard Ethernet cabling," highlighting their function as a power source integrated into the network link. (Reference to general principles taught in advanced networking courses).

Question: 26

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 an isolated testing environment used to execute and analyze suspicious code without affecting the host system or the production network. When testing a file for potential malware, a sandbox allows security analysts to safely observe the file's behavior, such as its attempts to modify the file system, alter the registry, or establish network connections. This controlled observation is the most effective and secure method for determining if a file is malicious. The isolation prevents any potential damage from spreading beyond the sandbox environment.

Why Incorrect Options are Wrong:

A. Multitenancy: This is a cloud computing architecture where a single software instance serves multiple customers; it is unrelated to malware analysis.
B. Test development: This is the process of creating and implementing software tests, not a specific environment for analyzing malicious files.
C. Cross-platform virtualization: This technology allows running different operating systems on a single host. While a virtual machine can be used as a sandbox, "sandbox" is the more precise term for the security-focused, isolated environment itself.

References:

1. Microsoft Corporation. (2023). Windows Sandbox. Microsoft Learn. In the overview section, it states, "Windows Sandbox provides a lightweight desktop environment to safely run applications in isolation. Software installed inside the Windows Sandbox environment remains 'sandboxed' and runs separately from the host machine." This directly supports the use of a sandbox for isolated testing.
2. University of Washington, Paul G. Allen School of Computer Science & Engineering. (2021). CSE 484 / CSE M 584: Computer Security and Privacy - Malware. Courseware, Lecture 19, Slide 33. The lecture material describes dynamic analysis of malware, stating, "Run malware in a controlled environment and monitor its actions... Sandboxes: Cuckoo, Anubis, Norman Sandbox."

This exemplifies the academic and practical use of sandboxes for malware analysis.
3. Kirat, D., & Vigna, G. (2015). BareCloud: a bare-metal analysis-based sandboxing system. In Proceedings of the 24th USENIX Security Symposium, (pp. 167-182). The introduction (Section 1) defines a sandbox in the context of malware analysis: "A sandbox is a controlled environment where a potentially malicious program is executed and its behavior is monitored." This peer-reviewed publication confirms the definition and purpose of a sandbox in cybersecurity.

Question: 27

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:

The Windows Upgrade Advisor has identified that the Trusted Platform Module (TPM) 2.0 is not available, which is a mandatory system requirement for newer Windows versions like Windows 11. In many modern computer systems, the TPM is integrated into the CPU as a firmware TPM (fTPM) or is a discrete module on the motherboard that is disabled by default in the system's firmware. The most direct and appropriate first step for a technician is to access the UEFI/BIOS settings to verify if the TPM feature is present and, if so, enable it. This action directly addresses the specific compatibility error reported by the upgrade tool.

Why Incorrect Options are Wrong:

B. An HSM (Hardware Security Module) is enterprise-grade cryptographic hardware and is not a standard substitute for the TPM 2.0 requirement for a Windows OS installation.
C. Performing a clean install might bypass the initial check, but it does not resolve the underlying hardware requirement and is not the correct troubleshooting procedure.
D. BitLocker is a Windows feature that uses an enabled TPM for disk encryption; implementing BitLocker does not enable the TPM module itself in the firmware.

References:

1. Microsoft Corporation. (2023). Enable TPM 2.0 on your PC. Microsoft Support. Retrieved from support.microsoft.com. In the section "How to enable TPM," the official guidance states, "If you need to enable TPM, these settings are managed via the UEFI BIOS (PC firmware) and vary based on your device... These settings are commonly found in a sub-menu in the UEFI BIOS labeled Advanced, Security, or Trusted Computing." This directly supports checking and enabling the module in the UEFI BIOS as the correct procedure.
2. Intel Corporation. (2023). Intel Platform Trust Technology (Intel PTT) for Windows 8 and 10 and Windows 11. Intel.com. Retrieved from intel.com. The documentation states, "Intel PTT is a

platform functionality for credential storage and key management used by Windows 8, Windows 10 and Windows 11. Intel PTT supports BitLocker for hard drive encryption and supports all Microsoft requirements for firmware Trusted Platform Module (fTPM) 2.0." It further clarifies that this feature is enabled within the BIOS.

3. Purdue University. (2022). ECE 468: Comp Security - Lecture 21: Trusted Computing. Courseware. The lecture notes discuss the role of the TPM in establishing a root of trust, which is configured and managed at the firmware (BIOS/UEFI) level before the operating system loads. This academic source establishes the principle that TPM functionality is controlled within the system firmware.

Question: 28

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:

The user is experiencing two distinct issues: a print quality problem (lines and smudges) and a paper handling problem (intermittent misfeeds). A laser printer maintenance kit is a collection of user-replaceable parts that wear out over time. These kits typically include a fuser assembly, transfer roller, pickup rollers, and separation pads. Replacing the fuser and transfer roller addresses common causes of smudges and lines, while replacing the pickup rollers and separation pads resolves paper misfeeding issues. Therefore, installing a maintenance kit is the comprehensive solution that addresses all the reported symptoms.

Why Incorrect Options are Wrong:

A. Fuser: Replacing only the fuser might correct the smudging but would not solve the paper misfeeding caused by worn rollers.
C. Corona wire: A faulty corona wire (or transfer roller) affects charge distribution, leading to print quality defects, but it does not cause paper misfeeds.
D. Toner cartridge: While a defective toner cartridge can cause lines and smudges, it plays no role in the paper feeding mechanism and would not fix the misfeeds.

References:

1. Hewlett-Packard (HP) Official Documentation: "HP LaserJet Printers - What is a Maintenance Kit?" HP Customer Support, Knowledge Base Document ID: c00899228. This document states, "Printer maintenance kits include paper pickup rollers, paper feed/separation rollers, a transfer roller, and a fuser assembly... Installing a maintenance kit is a preventative maintenance measure to ensure the printer continues to function properly and to maintain the highest possible print quality."
2. University of Wisconsin-Madison IT KnowledgeBase: "Laser Printer - Maintenance," DoIT KnowledgeBase, Document 6862, Published: 2008-09-09, Revised: 2020-02-19. The article

explains that maintenance kits contain parts that wear out, such as "fusers, transfer rollers, and pickup rollers," and are replaced to maintain "print quality and paper handling reliability."
3. Academic Textbook: Andrews, J., Dark, J., & West, J. (2020). A+ Guide to IT Technical Support (10th ed.). Cengage Learning. In Chapter 11, "Supporting Printers," the section on "Laser Printer Maintenance" describes a maintenance kit as containing parts that routinely wear out, including the fuser, rollers, and separation pads, and is used to solve problems like paper jams and poor print quality (p. 488).

Question: 29

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

A. DNS

B. Syslog

C. Telnet

D. DHCP

Answer:

D

Explanation:

The Dynamic Host Configuration Protocol (DHCP) is the standard network protocol used to automatically assign and manage IP addresses and other related network configuration parameters for devices on a network. In an enterprise setting, a DHCP server maintains a pool of available IP addresses and "leases" them to client devices as they connect. This centralization automates the IP assignment process, prevents duplicate IP address conflicts, and simplifies the administration of a large number of network clients. The process involves a client broadcasting a discovery request, and a server responding with an offer containing an IP address, subnet mask, default gateway, and DNS server information.

Why Incorrect Options are Wrong:

A. DNS (Domain Name System) is used to translate human-readable domain names into numerical IP addresses; it does not allocate or assign them to hosts.
B. Syslog is a protocol for forwarding log messages in an IP network. It is used for network management and security auditing, not IP allocation.
C. Telnet is an older, insecure remote access protocol used to provide a command-line interface to a remote host. It has no function in IP address assignment.

References:

1. Droms, R. (1997). RFC 2131: Dynamic Host Configuration Protocol. Internet Engineering Task Force (IETF). Section 1, "Introduction," states, "The Dynamic Host Configuration Protocol (DHCP) provides a framework for passing configuration information to hosts on a TCP/IP network... DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options."
2. Kurose, J. F., & Ross, K. W. (2021). Computer Networking: A Top-Down Approach (8th ed.). Pearson. In Chapter 4, Section 4.4.2, "The Dynamic Host Configuration Protocol (DHCP)," the text explains, "DHCP allows a host to obtain (be allocated) an IP address automatically."

3. Saltzer, J. H., & Kaashoek, M. F. (2009). Principles of Computer System Design: An Introduction. Morgan Kaufmann. Chapter 9, "Networking," Section 9.4.3, "Getting started," describes the role of DHCP: "When a computer is first attached to a network... it uses the Dynamic Host Configuration Protocol (DHCP) to find a server that can assign it an IP address." This is often covered in university-level computer science curricula based on this text.

Question: 30

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 printers are a type of impact printer. They function by striking a set of pins against an ink-soaked cloth ribbon, which then presses against the paper to form characters. Over time, the ink in the ribbon is depleted through repeated use. This gradual loss of ink is the direct cause of the printed output becoming progressively lighter or faded. Therefore, the standard and correct procedure to resolve this issue is to replace the old ribbon with a new one, which replenishes the ink supply.

Why Incorrect Options are Wrong:

A. Clean the printhead: A dirty or malfunctioning printhead would typically cause specific problems like missing dots, streaks, or incomplete characters, not uniform fading.
C. Install a maintenance kit: This term is more commonly associated with laser printers. For a dot matrix printer, the primary consumable part related to print fading is the ribbon.
D. Calibrate the alignment: Misalignment would result in skewed text or improperly formed characters, affecting their shape and position, not their overall lightness.

References:

1. Epson Corporation. (n.d.). FX-890II/FX-2190II User's Guide. In the "Solving Problems" chapter, section "Print Quality Problems," for the symptom "The printout is faint," the first recommended solution is: "The ribbon may be worn out. Replace the ribbon cartridge." (p. 106).
2. Indiana University. (2021, May 18). Troubleshooting common printer problems. UITS Knowledge Base. In the section discussing dot matrix printers, the document identifies that faint or light printing is a primary symptom of a worn-out ribbon that requires replacement.
3. Purdue University College of Engineering. (n.d.). ECE 362: Microprocessor Systems and Interfacing - Lecture 21: I/O Devices. Courseware documentation describes the mechanism of dot-matrix printers, identifying the ink ribbon as the consumable for transferring images to paper, implying its depletion leads to faded print.