



Free Questions for **220-1101**
Shared by **Mcintyre** on **12-12-2023**

For More Free Questions and Preparation Resources

[Check the Links on Last Page](#)



Question 1

Question Type: MultipleChoice

Which of the following network types is used for pairing a Bluetooth device to a smartphone?

Options:

- A- PAN
- B- WAN
- C- LAN
- D- MAN



Answer:

A

Explanation:

A PAN, or Personal Area Network, is the network type that is used for pairing a Bluetooth device to a smartphone. A PAN is a network that connects personal devices, such as phones, tablets, laptops, headphones, speakers, or printers, over a short distance, usually less than 10 meters or 33 feet. A PAN can use wireless technologies, such as Bluetooth, Wi-Fi, or infrared, to enable communication and data exchange between the devices. A Bluetooth PAN, also known as a piconet, can consist of up to eight devices, one of which acts as the master and the others as slaves. The master device initiates the pairing process with the other devices and controls the data transmission. The devices use radio waves in the 2.4 GHz frequency band to communicate with each other. Bluetooth is a low-power, low-cost, and secure technology that is widely used for creating PANs.



[What Is Bluetooth Wireless Networking?1](#)

[Bluetooth - GeeksforGeeks2](#)

[Bluetooth | Institute of Physics3](#)

[6 Different Types of Bluetooth Devices - TechJeny4](#)

Question 2

Question Type: MultipleChoice

A user's mobile device can back up classified files to an external hard drive at work but cannot save pictures to an external drive at home. Which of the following is most likely the issue?

Options:

- A- The pictures do not have a classification flag set.
- B- The drive permissions are insufficient.
- C- Peripherals are managed via MDM.
- D- Drivers are incorrectly installed.

Answer:

C

Explanation:

The most likely issue that prevents the user's mobile device from saving pictures to an external drive at home is that the peripherals are managed via MDM (mobile device management). MDM is a software solution that allows an organization to remotely control, secure, and enforce policies on mobile devices, such as smartphones, tablets, or laptops. MDM can also restrict the access and functionality of the peripherals, such as external drives, cameras, microphones, or printers, that are connected to the mobile devices.

One of the possible reasons why the user's mobile device can back up classified files to an external hard drive at work but not save pictures to an external drive at home is that the MDM policy allows only authorized peripherals to be used with the mobile device. For example, the MDM policy may require the external drive to have a certain encryption level, a specific serial number, or a valid certificate to be recognized by the mobile device. The external drive at work may meet these criteria, while the external drive at home may not. Therefore, the mobile device can back up the classified files to the external drive at work, but it cannot save the pictures to the external drive at home.

To resolve this issue, the user may need to contact the IT administrator or the MDM provider and request permission to use the external drive at home. Alternatively, the user may need to use a different method to transfer the pictures from the mobile device to the external drive, such as using a cloud service, a wireless network, or a USB cable.

[What is Mobile Device Management \(MDM\)?1](#)

[How to Manage Mobile Devices With MDM2](#)

[How to Connect an External Hard Drive to Your Phone3](#)

Question 3

Question Type: MultipleChoice

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

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

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

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

Wireless Name: HomeWiFi

Shared Key: CompTIA

Router Password: Secure\$1

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

Laptop: IP Address 192.168.1.100

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

Smartphone: IP Address 192.168.1.101

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

INSTRUCTIONS

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

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

Laura's Wireless Configuration

WIRELESS SETUP
NETWORK FILTER
ADMINISTRATOR TOOLS

Wireless Network Settings

Enable Wireless:

Wireless Network Name: (Also called the SSID)

Wireless Channel:

Disable SSID Broadcast:

802.11g Only Mode:

Wireless Security Mode


Security Mode:


WPA2


Passphrase:


Confirmed Passphrase:

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

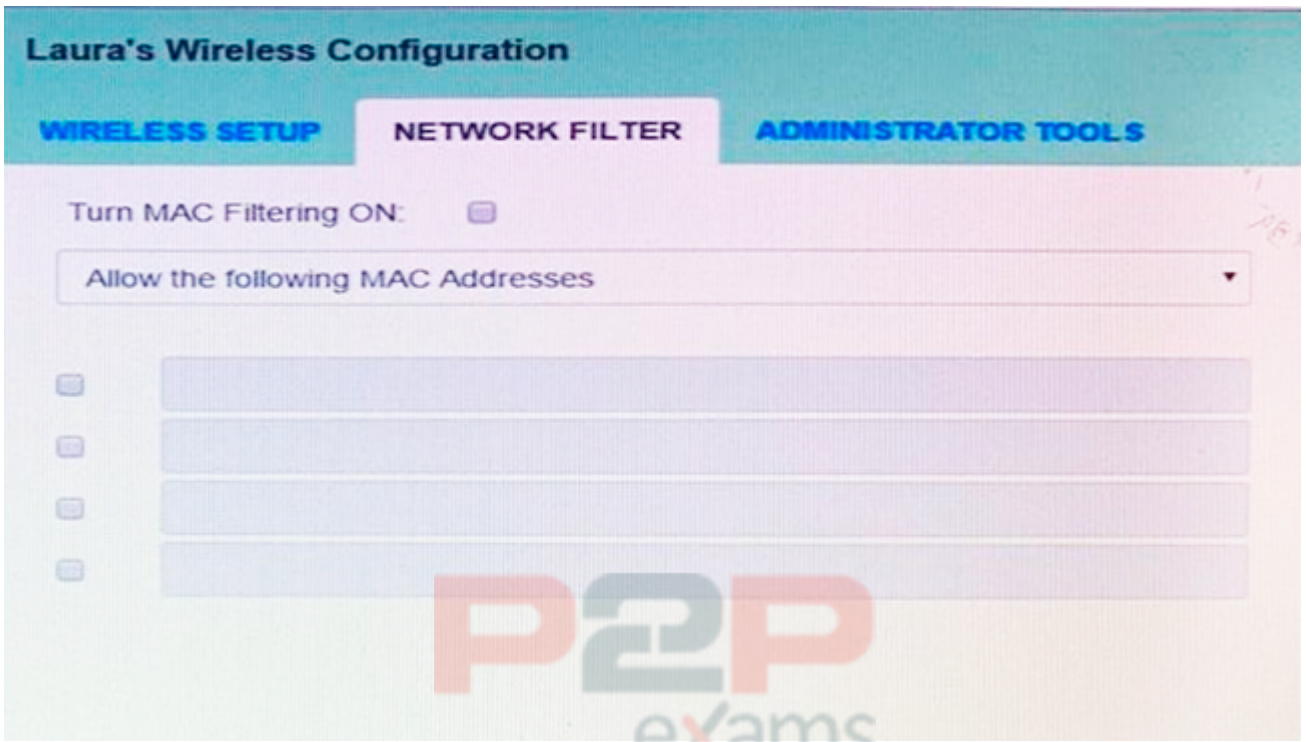
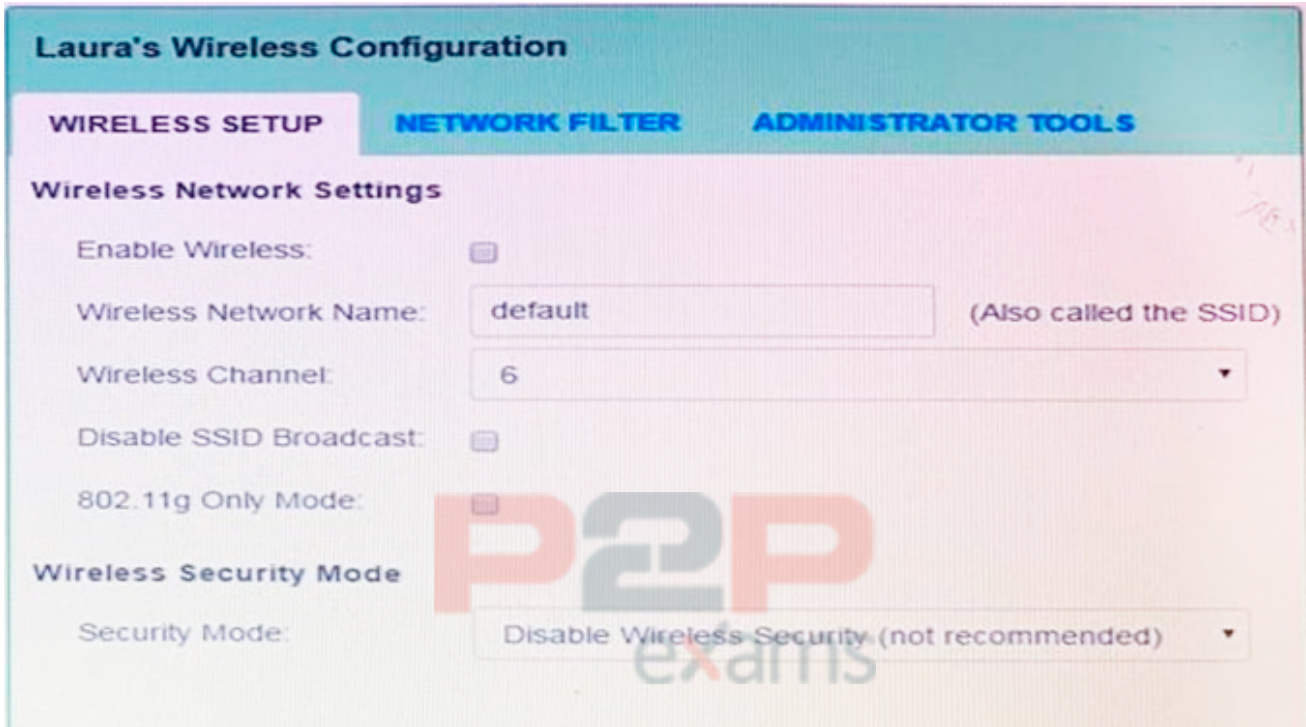
Laura's Wireless Configuration

WIRELESS SETUP
NETWORK FILTER
ADMINISTRATOR TOOLS

Please enter the same password into both boxes for confirmation.

Password:

Verify Password:



Options:

A- See the explanation below

Answer:

A

Explanation:

solution as



The screenshot shows a 'Wireless Configuration' window with three tabs: 'Wireless Setup', 'Network Filter', and 'Administrator Tools'. The 'Wireless Setup' tab is active. Under 'WIRELESS NETWORK SETTINGS:', 'Enable Wireless' is checked, 'Wireless Network Name' is 'HomeWiFi', 'Wireless Channel' is '1', 'Disable SSID Broadcast' is unchecked, and '802.11g Only Mode' is unchecked. Under 'WIRELESS SECURITY MODE:', 'Security Mode' is 'Enable WPA2 Wireless Security (enhanced)'. Under 'WPA2:', 'Passphrase' and 'Confirmed Passphrase' are both 'CompTIA'. A 'Save Settings' button is at the bottom right.

Wireless Configuration

Wireless Setup | Network Filter | Administrator Tools

Turn MAC Filtering ON

Allow the following MAC Addresses

MAC Address	
<input checked="" type="checkbox"/>	00:0A:BF:03:C4:54
<input checked="" type="checkbox"/>	09:2C:D0:22:3F:11
<input type="checkbox"/>	
<input type="checkbox"/>	

Save Settings

Wireless Configuration

Wireless Setup Network Filter Administrator Tools

ADMIN PASSWORD

Please enter the same password into both boxes for confirmation.

Password:

Verify Password:

Save Settings

Question 4

Question Type: MultipleChoice

A technician recently reinstalled a previously virtualized application directly to a user's computer. Now, the application is not launching. Which of the following did the technician most likely do to cause this issue?

Options:

- A- Installed the software on the base operating system.
- B- Installed the wrong license type.
- C- Installed the application with administrator rights.
- D- Reset the user's application virtualization session.

Answer:

A

Explanation:

If an application was previously running in a virtualized environment and is not launching after being installed directly on the base operating system, it's possible that the technician did not account for dependencies or configurations specific to the virtualized environment that are not present or are incompatible with the base operating system. This mismatch can prevent the application from launching properly.

CompTIA A+ Core 1 Exam Objectives Section 4.0: Virtualization and Cloud Computing

CompTIA A+ Core 1 Exam Objectives Section 5.0: Hardware and Network Troubleshooting

Question 5

Question Type: MultipleChoice

A user keeps a company-provided camera's battery charger plugged into a docking station at a desk. Company policy requires that USB devices be identified and approved by

installed peripheral security software. A technician is unable to add a unique identifier to the battery charger's security software. Which of the following should the technician do?

Options:

- A- Provide a USB to AC adapter for the battery charger.
- B- Add a powered USB hub to the docking station.
- C- Disable the peripheral security software for this user only.
- D- Replace the battery charger with a USB device that has a unique identifier.

Answer:

A

Explanation:

The problem in this scenario is that the battery charger is not a USB device, but a device that plugs into a USB port to draw power. Therefore, it does not have a unique identifier that can be recognized by the peripheral security software, which is designed to prevent unauthorized USB

devices from accessing the company's network or dat

a. The security software cannot add the battery charger to its whitelist, and may block its power supply or generate alerts.

The best solution for this problem is to provide a USB to AC adapter for the battery charger, which is a device that converts the USB power output to an AC power input that can be plugged into a wall outlet. This way, the battery charger does not need to connect to the docking station or the computer, and does not trigger the peripheral security software. The user can still charge the camera's battery without compromising the company's security policy.

The other options are not advisable because they either do not solve the problem or create new risks. Option B, adding a powered USB hub to the docking station, may not work if the security software also monitors the hub's ports and detects the battery charger as an unknown device. Option C, disabling the peripheral security software for this user only, is a very bad idea because it exposes the user's computer and the company's network to potential attacks from malicious USB devices. Option D, replacing the battery charger with a USB device that has a unique identifier, is unnecessary and costly, and may not be compatible with the camera's battery.

[CompTIA A+ Core 1 \(220-1101\) Certification Study Guide, Chapter 9: Security, Section 9.3: Device Security, Page 419](#)

[CompTIA A+ Core 1 \(220-1101\) and Core 2 \(220-1102\) Pearson uCertify Course and Labs and Textbook Bundle, Chapter 9: Security, Section 9.3: Device Security, Page 420](#)

[CompTIA A+ Core 1 \(220-1101\) and Core 2 \(220-1102\) Exam Cram, Chapter 9: Security, Section 9.3: Device Security, Page 402](#)

Question 6

Question Type: MultipleChoice

Which of the following network devices is needed to direct packets to networks outside of the LAN?

Options:

- A- Hub
- B- Switch
- C- Router
- D- Bridge

Answer:

C

Explanation:

Routers are designed to connect multiple networks and direct packets to their intended destinations across network segments. This makes them essential for directing packets to networks outside of the LAN, such as the internet or other remote networks.

CompTIA A+ Core 1 Exam Objectives Section 2.2: Compare and contrast common networking hardware.



To Get Premium Files for 220-1101 Visit

<https://www.p2pexams.com/products/220-1101>

For More Free Questions Visit

<https://www.p2pexams.com/comptia/pdf/220-1101>

20%
DISCOUNT

P2P
exams