7.6 Module Quiz

Date: 12/6/2025, 10:14:44 AM

Time Spent: 39:28

Score: 73%

Passing Score: 80%

Question 1 ✓ Correct

A user reports that they are unable to connect to the office Wi-Fi network.

Upon investigation, you find that the network name (SSID) is not visible in the list of available wireless networks on their device. Other users in the same area are able to connect to the Wi-Fi without any issues.

What is the MOST appropriate action to resolve this issue?

○ Move the user's device closer to the wireless access point.

○ Upgrade the user's device to support the latest wireless standards.

● Manually configure the connection to the Wi-Fi network on the user's device. ✓ Correct

○ Restart the wireless router to refresh the network settings.

Explanation

If the SSID broadcast is suppressed (hidden), the network name will not appear in the list of available networks. In this case, the user must manually configure the connection by entering the SSID, security type, and password on their device. This is the most appropriate action based on the scenario described.

While moving closer to the access point can help if the issue is related to weak signal strength, this is not relevant in this scenario because other users in the same area are able to connect without issues. The problem here is related to the SSID not being visible, not signal strength.

Restarting the router might resolve network-wide issues, but in this case, the problem is isolated to one user. Since other users are able to connect without issues, restarting the router is unnecessary and would disrupt the network for others.

Upgrading the device might be necessary if there is a standards mismatch (e.g., the device does not support the Wi-Fi standard used by the network). However, this is not the issue here because the SSID is hidden, and the user's device is not detecting it. Upgrading the device would not resolve this specific problem.

Related Content

- 5.4.11 Long-Range Fixed Wireless
- 7.3.4 Troubleshoot Wireless Issues

7.3.6 Troubleshoot Limited Connectivity

resources\questions\q_troubleshoot_wireless_issues_03.question.xml

Question 2 ✕ Incorrect

A network technician securely connects to a remote server on port 3389. What protocol does the technician use?

○ SSH

○ Telnet

● LDAP ✕ Incorrect

○ RDP ✓ Correct

Explanation

Remote Desktop Protocol (RDP) is Microsoft's protocol for operating remote graphical user interface (GUI) connections to a Windows machine. RDP uses port TCP/3389.

The Lightweight Directory Access Protocol (LDAP) is a TCP/IP protocol used to query and update an X.500 directory, and current directory products widely support it.

Secure Shell (SSH) is the principal means of obtaining secure remote access to UNIX and Linux servers and most types of network appliances (switches, routers, and firewalls).

Telnet is both a protocol and a terminal emulation software tool that transmits shell commands and output between a client and the remote host.

Related Content

6.3.6 Well-Known Ports

7.1.1 File/Print Servers

7.1.9 Remote Terminal Access Servers

14.2.1 Remote Desktop Tools

resources\questions\q_remote_terminal_access_servers_01.question.xml

Question 3 ✓ Correct

As a network analyst, you are tasked with evaluating the email setup for a company that requires employees to access their emails from multiple devices, ensuring that changes made on one device are reflected across all others.

Which protocol would you analyze as the most suitable for this requirement, and why?

○ Post Office Protocol (POP3), because it downloads emails to a single device, ensuring all emails are stored locally.

● Internet Message Access Protocol (IMAP), because it synchronizes email messages across multiple devices. ✓ Correct

○ Simple Mail Transfer Protocol (SMTP), because it allows for the sending and receiving of emails across devices.

○ File Transfer Protocol (FTP), because it allows for the transfer of files, including emails, between devices.

Explanation

IMAP is specifically designed to allow access to emails from multiple devices while keeping them synchronized. It ensures that any changes made (such as reading, deleting, or moving emails) are updated across all devices, making it the most suitable protocol for the company's requirement.

SMTP is primarily used for sending emails, not for retrieving or synchronizing them across multiple devices. It does not provide the functionality needed to ensure that changes made on one device are reflected on others, making it unsuitable for the requirement.

POP3 is designed for downloading emails to a single device and does not support synchronization across multiple devices. Once emails are downloaded, they are typically removed from the server, which does not meet the requirement of reflecting changes across devices.

FTP is used for transferring files between systems and is not related to email synchronization or management. It does not provide the necessary functionality to keep emails synchronized across multiple devices, making it irrelevant to the scenario.

Related Content

- 7.1.5 Mail Servers
- 7.1.6 Mailbox Servers

resources\questions\q_mailbox_servers_04.question.xml

Question 4 ✕ Incorrect

What is the first step in troubleshooting a limited connectivity issue for a single host in a wired network?

- ● Use a cable tester to verify the structured cabling. ✕ Incorrect
- ○ Verify that the patch cords are properly terminated and connected to the network ports. ✓ Correct
- ○ Update the NIC's device driver software.
- ○ Check the switch configuration for port security settings.

Explanation

The first step in troubleshooting limited connectivity for a single host is to check the physical connections, such as ensuring that the patch cords are properly terminated and securely connected to the network ports. This is a basic but essential step to rule out simple physical issues before moving on to more complex troubleshooting.

While port security settings on the switch can cause connectivity issues, this is not the first step in troubleshooting. Physical connections should be checked before investigating switch configurations.

Using a cable tester to verify structured cabling is a more advanced step in troubleshooting. It is performed after confirming that the patch cords and physical connections are not the source of the problem.

Updating the NIC's device driver software is a potential solution for connectivity issues caused by driver problems. However, this is not the first step in troubleshooting. Physical connections should be checked before addressing software-related issues.

Related Content

- 7.3.1 Troubleshoot Wired Connectivity
- 7.3.6 Troubleshoot Limited Connectivity

resources\questions\q_troubleshoot_limited_connectivity_01.question.xml

Question 5 ✓ Correct

A network technician is configuring an email connection that will have a permanent connection to the mail server. What kind of email connection is the technician configuring?

○ POP3

○ SMTP

○ HTML

● IMAP ✓ Correct

Explanation

The Internet Message Access Protocol (IMAP) is a mail retrieval protocol that supports permanent connections to a server and connecting multiple clients to the same mailbox simultaneously.

In Simple Mail Transfer Protocol (SMTP), the SMTP server of the sender discovers the IP address of the recipient SMTP server by using the domain name part of the recipient's email address.

HyperText Markup Language (HTML) web pages are plain text files with coded tags describing how to format the document.

The Post Office Protocol (POP) is an early example of a mailbox access protocol. POP is generally known as POP3 because the active version of the protocol is version 3.

Related Content

7.1.5 Mail Servers

7.1.6 Mailbox Servers

resources\questions\q_mailbox_servers_01.question.xml

Question 6 ✓ Correct

After several new computers are connected to a network device, every computer connected to the device begins to experience slow transfer speeds.

Which of the following is the FIRST step to troubleshoot this problem?

- ● Determine whether the network device is a hub or a switch. ✓ Correct
- ○ Use a cable tester to determine whether all cables between each computer and the device are good.
- ○ Use a loopback plug to determine whether the NIC in each computer is good.
- ○ Use a loopback plug to determine whether each port on the network device is good.

Explanation

When troubleshooting slow speeds, you need first to determine which device is running slowly (such as a hub or switch). If a specific resource is experiencing slow speeds, you need to focus your efforts on that resource.

The problem is unlikely to be a bad port on the network device, which would only affect one computer.

If the problem is a bad NIC, already knowing whether the network device is a hub or switch would help isolate the problem.

A bad cable would only affect the computer it was connected to, but all computers are experiencing slow transfer speeds in this scenario.

Related Content

7.3.2 Troubleshoot Network Speed Issues

resources\questions\q_troubleshoot_network_speed_issues_01.question.xml

Question 7 ✓ Correct

Which of the following internet appliances filters specific internet content categories and also keeps internal users anonymous?

○ Unified Threat Management

● Proxy server ✓ Correct

○ Content filter

○ Spam gateway

Explanation

A proxy server is an appliance that typically monitors all incoming and outgoing network traffic and determines if the traffic is allowed or not. The network administrator can configure the proxy server to block specific content categories, such as gambling websites. The proxy server also keeps internal users anonymous since all outgoing traffic shows as coming from the proxy server.

Content filtering is a service that a UTM appliance can handle but will not keep internal users anonymous.

A firewall is responsible for monitoring and controlling all incoming and outgoing traffic. A firewall does not filter based on content, nor does it keep users anonymous.

A spam gateway monitors incoming and outgoing emails to reduce the amount of spam affecting the network.

Related Content

7.2.1 Proxy Servers

7.2.4 Load Balancers

resources\questions\q_proxy_servers_02.question.xml

Question 8 ✕ Incorrect

You are an IT manager at a company that relies on a legacy system to run critical business operations. Recently, a security vulnerability was discovered in the system, but the vendor no longer provides support or updates.

What is the BEST course of action to mitigate the security risk while maintaining the system's functionality?

○ Wait for the vendor to release a patch, as they might still provide occasional updates.

○ Continue using the legacy system without any changes, as it has been reliable so far.

○ Isolate the legacy system from the rest of the network and implement strict access controls. ✓ Correct

● Replace the legacy system immediately with a modern alternative, regardless of cost. ✕ Incorrect

Explanation

Isolating the legacy system from the rest of the network and implementing strict access controls is a practical approach to mitigate security risks. This helps protect the rest of the network from potential vulnerabilities in the legacy system while maintaining its functionality.

Continuing to use the legacy system without addressing the security vulnerability is risky. The lack of vendor support means vulnerabilities will not be patched, increasing the risk of exploitation.

While replacing the legacy system with a modern alternative could solve the security issue, doing so immediately without considering cost and operational impact may not be feasible. A more balanced approach is needed.

Since the legacy system is no longer supported by the vendor, waiting for a patch is not a reliable strategy. Legacy systems are not supported, so relying on vendor updates is not advisable.

Related Content

resources\questions\q_legacy_systems_03.question.xml

Question 9 ✓ Correct

You connect your computer to a wireless network available at the local library. You find that you cannot access several websites on the internet.

Which of the following is the MOST likely cause of this problem?

- ○ The router has not been configured to perform port forwarding.
- ● A proxy server is filtering access to websites. ✓ Correct
- ○ A firewall is blocking ports 80 and 443.
- ○ Port triggering is redirecting traffic to the wrong IP address.

Explanation

A proxy server can block internet access based on a website or URL. Many schools and public networks use proxy servers to prevent access to websites with objectionable content.

Ports 80 and 443 are used by HTTP to retrieve all web content. If a firewall were blocking these ports, access would be denied to all websites.

Port forwarding directs incoming connections to a host on the private network.

Port triggering dynamically opens firewall ports based on applications that initiate contact from the private network.

Related Content

7.2.1 Proxy Servers

7.2.4 Load Balancers

resources\questions\q_proxy_servers_06.question.xml

Question 10 × Incorrect

A company is experiencing slow network speeds, and the issue appears to affect multiple users connected to the same switch.

Upon reviewing the switch's configuration, you notice a high number of damaged frames being reported.

What is the MOST likely cause of the issue?

○ Malware infection on one of the connected hosts

● Mismatched duplex settings on the network adapter and switch port × Incorrect

○ An outdated driver on a single user's network adapter

○ External interference affecting the cabling ✓ Correct

Explanation

External interference, such as from nearby power lines, fluorescent lighting, or motors, can cause issues like damaged frames in the cabling. This is the most likely cause when multiple users connected to the same switch are affected, and the switch reports damaged frames.

Mismatched duplex settings would typically affect the speed of a single connection rather than multiple users connected to the same switch. The issue described in the scenario is broader in scope.

While malware can cause network performance issues, it would not directly result in damaged frames being reported by the switch. Damaged frames are more indicative of physical or environmental issues with the cabling.

An outdated driver would only affect the performance of the specific user's connection. It would not cause network-wide issues or result in damaged frames being reported by the switch.

Related Content

7.3.2 Troubleshoot Network Speed Issues

resources\questions\q_troubleshoot_network_speed_issues_04.question.xml

Question 11 ✓ Correct

Your organization has recently deployed a Network Monitoring Server to address frequent network outages and potential security breaches.

After a week of monitoring, you receive a report indicating a significant increase in network traffic during non-business hours, along with several failed login attempts from an unfamiliar IP address.

As the network analyst, how should you interpret these findings to enhance network security and performance?

○ Conclude that the increased traffic is due to legitimate after-hours work by employees, and no action is needed.

● Analyze the report to identify potential unauthorized access attempts and recommend implementing stricter access controls. ✓ Correct

○ Assume the network monitoring server is malfunctioning and schedule a maintenance check to resolve the issue.

○ Determine that the failed login attempts are likely due to forgotten passwords and advise users to reset their credentials.

Explanation

Analyzing the report to identify potential unauthorized access attempts and recommending the implementation of stricter access controls and monitoring demonstrates an analytical approach by considering the possibility of unauthorized access based on the report's findings.

Concluding that the increased traffic is due to legitimate after-hours work by employees and no action is needed overlooks the potential security threat posed by the unusual traffic patterns and failed login attempts. Analyzing the situation requires considering the possibility of unauthorized access rather than assuming all activity is legitimate.

While forgotten passwords can cause failed login attempts, this explanation does not account for the unusual timing and unfamiliar IP address. A deeper analysis is needed to assess potential security risks.

Assuming a malfunction without further investigation dismisses the potential security threat. Analyzing the data should focus on understanding the traffic patterns and addressing any security vulnerabilities.

Related Content

resources\questions\q_network_monitoring_servers_03.question.xml

Question 12 ✓ Correct

Which of the following statements BEST describes the primary security concern associated with Telnet?

○ Telnet uses a secure tunneling protocol to protect data integrity and confidentiality during transmission.

● Telnet transmits data, including passwords, in plaintext. ✓ Correct

○ Telnet requires multi-factor authentication, providing an additional layer of security against unauthorized access.

○ Telnet encrypts all data transmissions, ensuring secure communication between client and server.

Explanation

Because Telnet transmits data in plaintext, it is vulnerable to eavesdropping and interception by malicious actors, which can lead to unauthorized access and data breaches.

Telnet does not encrypt data transmissions. This is a common misconception. The lack of encryption is a significant security flaw, as it allows data to be intercepted in plaintext.

Telnet does not use any secure tunneling protocol. This statement is false because Telnet lacks built-in security features to protect data integrity and confidentiality.

Telnet does not inherently require multi-factor authentication. This statement is misleading, as Telnet's standard implementation does not include advanced authentication mechanisms, making it less secure compared to modern alternatives like SSH.

Related Content

7.1.9 Remote Terminal Access Servers

14.2.1 Remote Desktop Tools

resources\questions\q_remote_terminal_access_servers_02.question.xml

Question 13 ✓ Correct

Which of the following all-in-one security appliance (UTM) functions detects intrusions and alerts the network but does not block traffic?

○ Intrusion protection

○ Anti-spam

○ VPN

● Intrusion detection ✓ Correct

Explanation

Intrusion detection detects intrusions and alerts the network. However, it does not block traffic.

Intrusion protection detects and blocks network traffic that is not recognized by its profile.

Anti-spam is designed to detect and block certain types of email.

A VPN encrypts traffic over a secure network. However, a VPN does not block traffic.

Related Content

resources\questions\q_spam_gateways_and_unified_threat_management_03.question.xml

Question 14 ✓ Correct

A security technician is installing a doorbell/video entry system for a customer so that the customer can see and communicate with people who come to their home when they aren't there.

What kind of device is the doorbell/video entry system?

● Smart device ✓ Correct

○ Zigbee

○ OT

○ Hub and control system

Explanation

The doorbell/video entry system is a smart device, which is a device or appliance that users can configure and monitor over an IoT network.

Zigbee is a wireless technology. While the control system is typically joined to the Wi-Fi network, smart devices may use other wireless technologies, such as Z-Wave or Zigbee, to exchange data via the hub.

A hub and control system are each required by IoT devices. The hub facilitates wireless networking while the control system operates the device.

An embedded system network is known as an operational technology (OT) network, to distinguish it from an IT network.

Related Content

7.2.7 Internet of Things Devices

resources\questions\q_internet_of_things_devices_01.question.xml

Question 15 ✓ Correct

A user reports intermittent connectivity and slow transfer speeds on the office Wi-Fi network. Upon investigation, you find that the user's device is connected to the 2.4 GHz band, while other devices connected to the 5 GHz band are not experiencing any issues.

Additionally, the Wi-Fi analyzer shows that the 2.4 GHz band is heavily congested with multiple overlapping networks.

What is the BEST course of action to resolve the issue?

○ Replace the wireless access point with a newer model that supports higher speeds.

● Configure the user's device to connect to the 5 GHz band instead of the 2.4 GHz band. ✓ Correct

○ Adjust the channel settings on the wireless access point to a less congested channel in the 2.4 GHz band.

○ Move the user's device closer to the wireless access point to improve the signal strength.

Explanation

The 5 GHz band is less congested and offers better performance in terms of speed and reliability compared to the 2.4 GHz band, especially in environments with many overlapping networks. Configuring the user's device to connect to the 5 GHz band will resolve the issue of congestion and improve connectivity. This is the most effective solution based on the analysis of the problem.

While adjusting the channel settings can reduce interference in the 2.4 GHz band, it does not address the fundamental issue of congestion caused by multiple overlapping networks. Switching to the 5 GHz band is a more effective solution in this scenario.

Moving closer to the access point might improve signal strength, but it does not resolve the issue of congestion in the 2.4 GHz band. The problem is not related to signal strength but to interference and congestion.

Replacing the access point is unnecessary in this scenario because the issue is related to the user's device being connected to the congested 2.4 GHz band. The existing access point already supports the 5 GHz band, which is a viable solution. Replacing the hardware would be an excessive and costly approach.

Related Content

- 5.4.11 Long-Range Fixed Wireless
- 7.3.4 Troubleshoot Wireless Issues
- 7.3.6 Troubleshoot Limited Connectivity

resources\questions\q_troubleshoot_wireless_issues_04.question.xml