NCTI Field Tech III to IV Practice Exam (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. What is the function of an access point in a wireless network?

A. To transmit data over fiber optic lines

B. To extend a wired network for wireless devices

C. To encrypt data being transmitted

D. To serve as a backup for network security

2. What is an example of a stateful protocol?

A. Post Office Protocol version 3 (POP3)

B. Transmission Control Protocol (TCP)

C. Hypertext Transfer Protocol (HTTP)

D. Domain Name System (DNS)

3. What type of network topology connects all devices to a central hub?

A. Bus topology

B. Ring topology

C. Mesh topology

D. Star topology

4. What type of delivery method uses an email server between the sender and the receiver of messages?

A. Direct delivery

B. Store-and-forward

C. Instant messaging

D. Client-server

5. Which one of the following protocols allows email clients to download their messages from an email server?

A. Internet Message Access Protocol version 4 (IMAP4)

B. Post Office Protocol version 3 (POP3)

C. Simple Mail Transfer Protocol (SMTP)

D. Hypertext Transfer Protocol (HTTP)

6. What results when a router's routing information is outdated but it still receives data packets?

A. Improved router performance

B. Packet loss and inefficiency

C. Immediate routing table updates

D. Consistent traffic flow

7. Where does Red Hat store its networking parameters?

A. /etc/passwd

B. /etc/sysconfig directory

C. /usr/local/bin

D. /var/log

8. What is the correct destination UDP port number for a DHCPDISCOVER message?

A. 53

B. 67

C. 68

D. 80

9. What is the most commonly used dense wavelength division multiplexing (DWDM) channel in broadband cable networks?

A. A-band (1,490 to 1,530 nm)

B. C-band (1,530 to 1,565 nm)

C. D-band (1,565 to 1,590 nm)

D. W-band (1,590 to 1,620 nm)

10. What is an intrusion detection system (IDS)?

A. A system for backing up data

B. A software that monitors network activities for threats

C. A device that encrypts data packets

D. A protocol for secure data transmission

Answers

1. B
2. B
3. D
4. B
5. B
6. B
7. B
8. B
9. B
10. B

Explanations

1. What is the function of an access point in a wireless network?

A. To transmit data over fiber optic lines

B. To extend a wired network for wireless devices

C. To encrypt data being transmitted

D. To serve as a backup for network security

An access point plays a crucial role in a wireless network by serving as a bridge that connects wireless devices to a wired network. It acts as a central hub that allows mobile devices such as laptops, smartphones, and tablets to access network resources, such as the internet and shared files, via a wireless connection. Essentially, an access point extends the coverage of a network, enabling devices that do not have the capability to connect directly to a wired network to communicate and function within that environment. For instance, in an office setting, when a user wants to connect their laptop to the company's network, the access point facilitates this wireless connection, ensuring that data can be transmitted between the laptop and the server or other network resources. This function is vital in expanding network accessibility to areas where running cables might be difficult or impractical. The other options focus on elements not central to the primary role of an access point. Transmitting data over fiber optic lines relates to the infrastructure of the network rather than wireless connectivity. Encrypting data being transmitted deals with data security, which is important but not the main function of the access point itself. Lastly, serving as a backup for network security does not align with the purpose of an access point, as its primary role is connection rather

2. What is an example of a stateful protocol?

A. Post Office Protocol version 3 (POP3)

B. Transmission Control Protocol (TCP)

C. Hypertext Transfer Protocol (HTTP)

D. Domain Name System (DNS)

A stateful protocol is one that maintains information about the state of a connection or session over time, allowing it to manage and track the data exchanged between systems. In this context, the Transmission Control Protocol (TCP) exemplifies a stateful protocol because it establishes a connection between a sender and receiver and maintains that connection throughout the data transmission process. TCP uses a three-way handshake to initiate a connection, tracks the order of packets, manages retransmission of lost packets, and ensures that data is received in the correct sequence. This capability to maintain and manage state information through the session is what defines it as stateful. In comparison, other options like Post Office Protocol version 3 (POP3) and Hypertext Transfer Protocol (HTTP) are considered stateless protocols. They do not retain session information between requests. Each request is treated independently, with no awareness of previous interactions. The Domain Name System (DNS) also acts statelessly, resolving domain names to IP addresses without maintaining information about past queries or sessions. Thus, in the realm of networking protocols, TCP stands out as the quintessential example of stateful communication, enabling reliable and ordered delivery of data through a sustained connection.

3. What type of network topology connects all devices to a central hub?

A. Bus topology

B. Ring topology

C. Mesh topology

D. Star topology

In a star topology, all devices in the network are connected to a central hub or switch. This central device acts as a point of communication, managing data traffic between the connected devices. Because each device has a direct point of connection to the hub, it allows for easier management and isolation of devices. If one connection fails, it does not impact the entire network, allowing for better fault tolerance compared to other topologies. In contrast, the bus topology connects all devices along a single communication line (the bus), meaning that if the bus fails, the entire network goes down. The ring topology connects devices in a circular formation, where each device is connected to two others, which can complicate troubleshooting and maintenance. Mesh topology, while providing more redundancy due to multiple connections between devices, does not typically utilize a central hub but instead connects multiple devices to one another, increasing complexity and cost. Thus, the characteristic of connecting all devices to a single central point is what specifically defines the star topology.

4. What type of delivery method uses an email server between the sender and the receiver of messages?

A. Direct delivery

B. Store-and-forward

C. Instant messaging

D. Client-server

The store-and-forward delivery method involves utilizing an email server to facilitate the transmission of messages between the sender and the recipient. In this method, when an email is sent, it does not go directly from the sender to the receiver. Instead, it first travels to an email server, which temporarily stores the message until it can be forwarded to the recipient's email server. This allows for the handling of situations where the recipient's email server might not be immediately available, ensuring that messages are queued and successfully delivered once the server is reachable. This process is essential for managing emails, especially in scenarios where network connections may fluctuate or where email servers are experiencing downtime. The other methods mentioned do not utilize the email server in the same manner. Direct delivery sends messages straight to the recipient with no intermediary server, instant messaging typically involves a real-time communication protocol without storing messages on a server, and client-server refers to a model where client devices communicate with a server, which can encompass various types of data transmission but not necessarily with the store-and-forward method specifically used in email communications.

5. Which one of the following protocols allows email clients to download their messages from an email server?

A. Internet Message Access Protocol version 4 (IMAP4)

B. Post Office Protocol version 3 (POP3)

C. Simple Mail Transfer Protocol (SMTP)

D. Hypertext Transfer Protocol (HTTP)

The protocol that allows email clients to download their messages from an email server is Post Office Protocol version 3 (POP3). POP3 is specifically designed to enable users to retrieve emails from their mail servers and store them locally on their devices. When using POP3, emails are typically downloaded and stored locally, allowing users to access their messages without the need for a continuous connection to the internet. POP3 works by connecting to the mail server and downloading messages to the email client, often removing the emails from the server in the process unless configured otherwise. This simplicity makes it effective for users who prefer to manage their emails offline. In contrast, Internet Message Access Protocol version 4 (IMAP4) also allows email retrieval but is designed for users who want to manage their emails directly on the server. IMAP4 enables multiple devices to access the same mailbox, keeping messages synchronized across devices and allowing for better management of folders and message states. Simple Mail Transfer Protocol (SMTP) is primarily used for sending emails rather than retrieving them. It works alongside POP3 or IMAP4 rather than functioning as a retrieval protocol. Hypertext Transfer Protocol (HTTP) is unrelated as it is used for transferring web pages rather than managing email.

6. What results when a router's routing information is outdated but it still receives data packets?

A. Improved router performance

B. Packet loss and inefficiency

C. Immediate routing table updates

D. Consistent traffic flow

When a router's routing information is outdated but it continues to receive data packets, the result is typically packet loss and inefficiency. Outdated routing information means that the router may not have the most current pathways to forward the incoming data packets effectively. Consequently, packets can be sent to incorrect destinations or even dropped if there are no valid routes available in the routing table at the time of transmission. This situation can lead to increased latency as the router struggles to process packets that it can't properly route. Additionally, packets may be retransmitted from the source due to timeouts or errors, which adds further inefficiency to the network. In summary, when routing information is not current, the overall performance of the network can degrade significantly, leading to problems such as packet loss, longer delivery times, and inefficient use of network resources.

7. Where does Red Hat store its networking parameters?

A. /etc/passwd

B. /etc/sysconfig directory

C. /usr/local/bin

D. /var/log

The correct answer is the /etc/sysconfig directory because this is where Red Hat-based systems typically store configuration files for system services and networking parameters. The /etc/sysconfig directory contains various scripts and configuration files that can define system environment variables, network interface configurations, and specific settings for services that run during system startup. In particular, files within this directory are used to customize settings such as network settings for interfaces, firewall configurations, and other system service parameters, making it a central place for managing network and system configurations. This understanding is crucial for administering and troubleshooting Red Hat systems effectively. The other options refer to different directories that serve distinct purposes. The /etc/passwd file is responsible for storing user account information. The /usr/local/bin directory is typically used for executable programs that are locally installed, while the /var/log directory is where system log files are stored. These directories do not contain networking parameters, which highlights the specific role of /etc/sysconfig in managing network configurations in Red Hat systems.

8. What is the correct destination UDP port number for a DHCPDISCOVER message?

A. 53

B. 67

C. 68

D. 80

The correct destination UDP port number for a DHCPDISCOVER message is 67. This is part of the Dynamic Host Configuration Protocol (DHCP), which operates on the client-server model to dynamically assign IP addresses and other network configuration parameters to devices on a network. When a client wants to discover available DHCP servers, it sends a DHCPDISCOVER message as a broadcast on its local subnet. The message is directed to port 67 on the DHCP server, which is designated for handling DHCP requests from clients. To elaborate, while port 68 is used by the client to receive messages from the DHCP server, port 67 is specifically the listening port for the server to process incoming requests. This distinction is critical in the DHCP process, as proper port allocation ensures that messages reach the correct destination and that the communication between the client and server occurs seamlessly. The other options represent different services or mechanisms: port 53 is used for DNS (Domain Name System) traffic, port 80 is for HTTP (Hypertext Transfer Protocol) web traffic, and although port 68 is relevant to DHCP, it is not the port that a DHCPDISCOVER message is aimed at. Thus, understanding the function of port 67 is essential in DHCP operations.

9. What is the most commonly used dense wavelength division multiplexing (DWDM) channel in broadband cable networks?

A. A-band (1,490 to 1,530 nm)

B. C-band (1,530 to 1,565 nm)

C. D-band (1,565 to 1,590 nm)

D. W-band (1,590 to 1,620 nm)

The C-band, which ranges from 1,530 to 1,565 nm, is the most commonly used dense wavelength division multiplexing (DWDM) channel in broadband cable networks for several reasons. This wavelength range is particularly efficient for fiber optic transmission because it allows for a higher number of densely packed channels. The efficiency of the C-band stems from its lower attenuation and higher capacity for data transmission compared to other bands. Fiber optics operating within this range can support long-distance communication without requiring frequent signal boosting, which is crucial for maintaining quality in broadband services. Moreover, equipment such as lasers and optical amplifiers have been optimized to operate effectively within the C-band. This standardization facilitates compatibility and interoperability among different network components, making the deployment of broadband services more straightforward and cost-effective. While other bands like the A-band, D-band, and W-band are available, they are not as widely utilized in broadband cable networks due to factors like higher attenuation and less established technology support. The dominance of the C-band in existing infrastructure and equipment further solidifies its role as a key player in maximizing data capacity and network performance in modern communications.

10. What is an intrusion detection system (IDS)?

A. A system for backing up data

B. A software that monitors network activities for threats

C. A device that encrypts data packets

D. A protocol for secure data transmission

An intrusion detection system (IDS) is a critical component of network security that serves to monitor network activities for potential threats or malicious behavior. This system analyzes traffic patterns and data flows to detect unauthorized access or breaches, which can indicate security incidents. The importance of an IDS lies in its ability to provide real-time alerts concerning abnormal activities that could compromise network integrity, thereby allowing organizations to respond quickly to those threats. The other options do not align with the primary function of an IDS. A system for backing up data focuses on preserving data rather than actively monitoring for security threats. A device that encrypts data packets is concerned with protecting data through encryption, ensuring confidentiality, but does not involve monitoring or detection of intrusions. Similarly, a protocol for secure data transmission pertains to the methods used to transmit data securely over existing networks but does not involve threat detection or monitoring functionalities. Therefore, the essence of an IDS is accurately captured by identifying it as a software that specifically monitors network activities for threats.