CCNA Introduction to Networks (ITN) Practice Test (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Notice: Examzify makes every reasonable effort to obtain from reliable sources accurate, complete, and timely information about this product.

Questions

1. **Which tool would a technician use to trace the path that a packet takes through a network?**

   A. ping

   B. nslookup

   C. tracert

   D. netstat

2. **When monitoring network performance, what key indicator is essential to establish adjustments?**

   A. Network performance baseline

   B. Current bandwidth usage

   C. Type of network topology

   D. Number of active users

3. **What are two problems caused by a large number of ARP request and reply messages?**

   A. Slow down the switching process

   B. Flood the subnet with excessive broadcasts

   C. Enhance network performance

   D. Both A and B

4. **Which protocol is used for secure file transfer over a network?**

   A. FTP

   B. SFTP

   C. HTTP

   D. SMTP

5. **What service is provided by Internet Messenger?**

   A. File sharing among users

   B. An application for live streaming

   C. Real-time chatting among remote users

   D. A platform for video conferencing

6. Which network devices will receive the ARP request sent by Host A in a default switch configuration?

A. Router R1 only

B. Hosts B and C only

C. Only hosts B, C, and router R1

D. All devices on the network

7. What characteristic describes spyware?

A. Software that protects against viruses

B. Software that collects information about the user

C. Software that speeds up computer performance

D. Software that encrypts files for security

8. What are two features of the Address Resolution Protocol (ARP)?

A. It translates IPv6 addresses to MAC addresses

B. It generates an ARP broadcast when the MAC address is unknown

C. It maintains a persistent connection with destination devices

D. It handles data fragmentation and reassembly

9. Which two network addresses can be assigned to a network containing 10 hosts, within the 10.18.10.0/24 range? (Choose two.)

A. 10.18.10.128/28

B. 10.18.10.208/28

C. 10.18.10.224/28

D. 10.18.10.0/25

10. What type of IP addressing allows multiple devices to share the same IP address?

A. Static IP addressing

B. Dynamic IP addressing

C. Private IP addressing

D. Network Address Translation (NAT)

Answers

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

Explanations

1. Which tool would a technician use to trace the path that a packet takes through a network?

A. ping

B. nslookup

C. tracert

D. netstat

The correct answer involves the use of a specific tool known for its ability to track the journey of packets through different routers and network devices in a given network. This tool sends out packets from a source and records the intermediate hops, allowing users to see each router's IP address along the way, as well as the round-trip time for packets to reach those routers. This capability is vital for diagnosing network issues, such as where delays or failures may be occurring within the path to a destination. Users can interpret the resulting output to identify specific problems in the network path, including potential misconfigurations or connectivity issues. The "ping" tool, while useful for checking the reachability of a host, simply measures round-trip time to a specified destination and does not provide details about the intermediary hops taken by the packets. Similarly, "nslookup" is focused solely on querying domain name system (DNS) to obtain information about hostnames or IP addresses, and does not perform any tracing of packet routes across a network. "Netstat" serves a different purpose, providing information about active connections, routing tables, interface statistics, and more on the local device, but does not trace packet paths like the tool in question does. Thus, the tool used to effectively trace

2. When monitoring network performance, what key indicator is essential to establish adjustments?

A. Network performance baseline

B. Current bandwidth usage

C. Type of network topology

D. Number of active users

Establishing a network performance baseline is crucial because it provides a reference point against which current performance can be measured. This baseline is built by collecting data on various performance metrics, such as throughput, latency, and error rates, during normal operating conditions. By having this established baseline, network administrators can identify deviations from expected performance, diagnose issues, and determine whether adjustments are necessary to optimize network functionality. Monitoring current bandwidth usage is important but is often only part of the overall assessment. It provides insights into how much of the available bandwidth is being utilized at any given time. However, without a baseline, it is difficult to discern whether current usage is typical or problematic. The type of network topology influences network design and layout but does not directly provide insights into performance metrics or necessary adjustments. Understanding topology is essential for network design and implementation, but it is not a key performance indicator. The number of active users can provide some context about network demand and performance pressure. However, this data alone does not inform whether the network is performing effectively. Without a baseline, it's challenging to understand how the number of users impacts performance or what adjustments might be required.   Thus, the network performance baseline is essential for continual assessment and adjustment of network performance, making it the key indicator

3. What are two problems caused by a large number of ARP request and reply messages?

A. Slow down the switching process

B. Flood the subnet with excessive broadcasts

C. Enhance network performance

D. Both A and B

A large number of ARP (Address Resolution Protocol) requests and replies can lead to significant issues in a network. One of the primary problems is that it can flood the subnet with excessive broadcasts. Since ARP operates through broadcast messages, excessive requests can overwhelm the network and lead to congestion, making it difficult for devices to communicate effectively. Additionally, this flooding can slow down the switching process. Switches, while designed to handle a certain amount of traffic efficiently, can become bogged down when they are inundated with numerous ARP messages. This can lead to increased latency for legitimate traffic, as the devices on the network spend precious resources processing these ARP broadcasts rather than forwarding user data. Therefore, both the slowing of the switching process and the flooding of the subnet with excessive broadcasts are accurate problems caused by a high volume of ARP messages, making the combination of these two impacts the correct choice in this scenario.

4. Which protocol is used for secure file transfer over a network?

A. FTP

B. SFTP

C. HTTP

D. SMTP

The use of SFTP, or Secure File Transfer Protocol, for secure file transfer over a network is well justified. SFTP is specifically designed to provide secure file transfer capabilities by leveraging the SSH (Secure Shell) protocol. This includes features such as encryption, which ensures that both the data being transferred and the authentication credentials are securely protected during the transit. Unlike standard FTP (File Transfer Protocol), which transmits data in plaintext, making it vulnerable to interception, SFTP encrypts the entire connection, offering a higher level of security that is crucial for sensitive data exchanges. The other mentioned protocols serve different purposes: FTP is primarily for basic file transfers without security measures. HTTP (Hypertext Transfer Protocol) is used for transferring web pages but does not provide secure transfer on its own, though it can be secured with HTTPS. SMTP (Simple Mail Transfer Protocol) is used for sending emails rather than for file transfers. Hence, SFTP stands out as the correct choice for secure file transfer over a network.

5. What service is provided by Internet Messenger?

A. File sharing among users

B. An application for live streaming

C. Real-time chatting among remote users

D. A platform for video conferencing

The service provided by Internet Messenger is primarily focused on real-time chatting among remote users. This type of application allows individuals to communicate instantly with one another over the internet, facilitating text-based conversations that happen in a live environment. Users can send messages back and forth quickly, often including features like notifications when messages are delivered or read, enabling dynamic and immediate communication. This function is essential in both personal and business contexts, as it allows for continuous interaction without the delays associated with traditional methods of communication, such as email. The emphasis on real-time chatting highlights its role in enhancing interpersonal communication, making it distinct from file sharing or video conferencing platforms, which serve different specific purposes.

6. Which network devices will receive the ARP request sent by Host A in a default switch configuration?

A. Router R1 only

B. Hosts B and C only

C. Only hosts B, C, and router R1

D. All devices on the network

In a default switch configuration, when Host A sends an ARP (Address Resolution Protocol) request, it is designed to discover the MAC address associated with a specific IP address on the local network. The switch operates at Layer 2 of the OSI model and uses a process called flooding to deliver the ARP request. When Host A sends out the ARP request, the switch will indeed send the broadcast frame to all devices connected to that switch port. This means that the frame will reach all devices within the same broadcast domain, including Hosts B and C, as well as any other devices connected to the switch, such as Router R1, if it is within the same broadcast domain. The ARP request typically asks: "Who has IP address X? Tell Host A." Since the request is broadcast, all devices that receive this request will check if they recognize the IP address in question. If the IP belongs to either Host B, Host C, or Router R1, they will respond with their MAC address. Therefore, in this scenario, the correct response includes Hosts B and C, as well as Router R1, assuming Router R1 has an IP address in the same subnet as Host A. This makes option C correct,

7. What characteristic describes spyware?

A. Software that protects against viruses

B. Software that collects information about the user

C. Software that speeds up computer performance

D. Software that encrypts files for security

Spyware is characterized primarily by its function to collect information about the user without their knowledge or consent. It operates by monitoring user activity, gathering personal data, and often transmitting that information back to the creator of the spyware or other third parties for various purposes, such as targeted advertising, identity theft, or other malicious intents. This capability to stealthily observe and gather detailed data about a person's habits or personal information is what defines spyware, making it distinct from other types of software such as antivirus programs, performance enhancers, or encryption tools, which serve different purposes relating to protection, speed, and security.

8. What are two features of the Address Resolution Protocol (ARP)?

A. It translates IPv6 addresses to MAC addresses

B. It generates an ARP broadcast when the MAC address is unknown

C. It maintains a persistent connection with destination devices

D. It handles data fragmentation and reassembly

The Address Resolution Protocol (ARP) serves a critical function in networking by mapping IP addresses to their corresponding MAC addresses, which are necessary for devices within a local network to communicate effectively. One of its primary features is the generation of an ARP broadcast when a device needs to discover the MAC address associated with a specific IP address but does not have that information in its ARP cache. This broadcast allows all devices on the local network segment to receive the request, and the device that owns the queried IP address responds with its MAC address. This fundamental mechanism enables seamless communication within Ethernet networks. The other options present features that do not align with the core functionality of ARP. For instance, ARP does not deal with IPv6 addresses, persistent connections, or the management of data fragmentation. Instead, ARP is specifically designed for IPv4 address resolution and does not maintain any sort of connection, nor does it engage in the fragmentation and reassembly of data packets, which are functions handled at higher layers of the OSI model.

9. Which two network addresses can be assigned to a network containing 10 hosts, within the 10.18.10.0/24 range? (Choose two.)

A. 10.18.10.128/28

B. 10.18.10.208/28

C. 10.18.10.224/28

D. 10.18.10.0/25

To determine which addresses can be assigned to a network containing 10 hosts in the range of 10.18.10.0/24, it’s essential to understand the implications of subnetting and host requirements. The CIDR notation of /24 indicates that this network has a subnet mask of 255.255.255.0, which means it can support up to 256 IP addresses total (0-255), but only 254 can be assigned to hosts (the lowest address is reserved as the network address and the highest for the broadcast address). To support 10 hosts, you require a subnet that offers at least 10 valid IPs. The closest subnet that meets this requirement would be a /28 subnet, which provides 16 IP addresses (14 usable for hosts, because it reserves 2 addresses — one for the network and one for the broadcast). Address 10.18.10.208/28 is valid as it falls within the /24 network range and allows for 14 usable IP addresses, accommodating the requirement for 10 hosts. Address 10.18.10.224/28 is also valid and similarly allows for sufficient IPs for the 10 hosts requirement. On the other hand,

10. What type of IP addressing allows multiple devices to share the same IP address?

A. Static IP addressing

B. Dynamic IP addressing

C. Private IP addressing

D. Network Address Translation (NAT)

Network Address Translation (NAT) is a crucial technology that enables multiple devices on a local network to share a single public IP address when accessing external networks, such as the internet. This is particularly useful in conserving the limited supply of public IP addresses and enhancing security by allowing internal devices to remain hidden behind the NAT device. NAT works by modifying the IP address information in the packets as they pass through the NAT router. When an internal device sends a request to the internet, the NAT device replaces the private IP address of the device with its own public IP address. It keeps a translation table that maps the internal IP address and port to the public IP address and an external port number. When replies come back from the external network, the NAT device uses this table to forward the packets to the correct internal device. This method not only facilitates efficient use of IP addresses but also provides a layer of security by concealing internal IP addresses from the outside world. Overall, NAT is widely employed in home routers and enterprise networks to manage IP addressing effectively.