NCTI Field Tech V to VI Practice Exam (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Sample study guide. Visit https://nctifieldtech5to6.examzify.com

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

Questions

1. Which of the following is a unique address assigned to hardware devices such as modems and network interface cards?

A. IP Address

B. MAC Address

C. DNS Address

D. Gateway Address

2. What does 'signal propagation delay' indicate?

A. The delay caused by network encryption

B. The time it takes for a signal to travel from sender to receiver

C. The time required to establish a connection

D. The time needed for data to process in a terminal

3. What does 'QoS' stand for, and why is it important in networking?

A. Quality of Service; it ensures performance for specific applications

B. Quality of Signal; it enhances signal strength

C. Quantity of Service; it measures the number of users

D. Quality of Security; it protects user data

4. What is the function of ephemeral port numbers?

A. They are used for permanent server applications

B. They define static connections between devices

C. They serve as temporary communication channels

D. They are assigned to protocol services

5. Which network type does the Intermediate System to Intermediate System (IS-IS) protocol support?

A. Only point-to-point (P2P) networks

B. Virtual private networks (VPN)

C. Broadcast networks and point-to-point (P2P) networks

D. Only broadcast networks

6. What is a key difference between IPv4 and IPv6?

A. IPv4 uses 64-bit addresses, while IPv6 uses 128-bit addresses

B. IPv4 can support fewer devices than IPv6

C. IPv4 has better security features than IPv6

D. IPv4 is more commonly used than IPv6

7. How is 'attenuation' defined in relation to signal strength?

A. It is the delay in signal transmission

B. It refers to the reduction in signal strength as it travels through a medium

C. It measures the amplification of a signal

D. It indicates the clarity of the transmitted signal

8. What does electrical interference from wiring or electric motors cause on telephone wiring?

A. Static noise issues

B. Noise on the line

C. Disconnected lines

D. Intermittent dialing issues

9. What can notify Simple Network Management Protocol (SNMP) network management stations of multicast problems?

A. Multicast Alerts

B. Multicast Traps

C. Multicast Logs

D. Multicast Messages

10. In Synchronous Optical Networks (SONET), how much faster is the data rate of an electrical level STS-192 compared to an STS-1?

A. 192 times

B. 96 times

C. 48 times

D. 24 times

Answers

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

Explanations

1. Which of the following is a unique address assigned to hardware devices such as modems and network interface cards?

A. IP Address

B. MAC Address

C. DNS Address

D. Gateway Address

A MAC address is a unique identifier assigned to hardware devices, such as modems, network interface cards, and other networked hardware. This address is essential for network communication within a local area network (LAN) because it enables the identification and differentiation of devices on the network. The MAC address is a physical address that operates at the data link layer of the OSI model, allowing devices to communicate with each other on the same physical network segment. It is typically presented in hexadecimal format and is hardcoded into the hardware during manufacturing. Understanding the roles of other addresses helps clarify why the MAC address is the correct answer. An IP address, while it is also unique, serves a different purpose on broader networks such as the Internet. It works at the network layer and can change depending on the device's connection to different networks. Similarly, a DNS address is associated with domain name resolution rather than hardware identification, while a gateway address refers to the device that acts as an access point for forwarding traffic between different networks. Each of these serves a distinct function within network communications, reinforcing the uniqueness and significance of the MAC address for hardware identification.

2. What does 'signal propagation delay' indicate?

A. The delay caused by network encryption

B. The time it takes for a signal to travel from sender to receiver

C. The time required to establish a connection

D. The time needed for data to process in a terminal

Signal propagation delay is a critical concept in networking that describes the time it takes for a signal to travel from the sender to the receiver. This delay is influenced by the distance between the two points and the medium through which the signal travels, such as copper wire, fiber optics, or wireless channels. Understanding signal propagation delay is essential for evaluating the performance and efficiency of a network, especially in systems where response time is crucial, such as real-time communication or streaming applications. The other options address different aspects of network performance. Network encryption may introduce latency, but this is not what signal propagation delay specifically refers to. Connection establishment time relates to the process required to set up a session for communication, which is separate from the actual travel time of a signal. Data processing time in a terminal involves the delay caused by hardware and software processing, rather than the physical distance a signal must travel. Thus, the definition provided in option B accurately captures the essence of signal propagation delay.

3. What does 'QoS' stand for, and why is it important in networking?

- A. Quality of Service; it ensures performance for specific applications
- B. Quality of Signal; it enhances signal strength
- C. Quantity of Service; it measures the number of users
- D. Quality of Security; it protects user data

The term 'QoS' stands for Quality of Service, and it is crucial in networking because it refers to the overall performance level of a service, particularly in terms of bandwidth, latency, and the reliability of data connections. QoS is especially important for applications that require high performance, such as voice over IP (VoIP), video conferencing, and online gaming. These applications are sensitive to delays and fluctuations in service, and QoS helps to prioritize certain types of traffic over others to ensure that critical services function smoothly under varying network conditions. By implementing QoS, network administrators can manage network resources effectively to guarantee that essential applications receive the necessary bandwidth and are less affected by network congestion. This prioritization is vital to enhance user experience, ensuring that essential communication and business processes remain uninterrupted.

4. What is the function of ephemeral port numbers?

- A. They are used for permanent server applications
- B. They define static connections between devices
- C. They serve as temporary communication channels
- D. They are assigned to protocol services

Ephemeral port numbers are utilized to establish temporary communication channels between devices during a network session. When a client device initiates a connection to a server, it typically uses an ephemeral port number to identify the specific session on its side. This allows for multiple sessions to occur simultaneously without interference, as each session can be differentiated by its unique port number. The nature of these ports being "ephemeral" or temporary is essential for dynamic network applications where multiple connections may be established and terminated frequently. This characteristic enables efficient use of network resources and helps manage connections effectively. The other options do not accurately describe ephemeral port numbers' function. Permanent server applications typically use well-known, static port numbers to ensure reliable access; static connections are usually defined by fixed port assignments, and protocol services are associated with those well-known ports, rather than ephemeral ones which are dynamic.

5. Which network type does the Intermediate System to Intermediate System (IS-IS) protocol support?

A. Only point-to-point (P2P) networks

B. Virtual private networks (VPN)

C. Broadcast networks and point-to-point (P2P) networks

D. Only broadcast networks

The Intermediate System to Intermediate System (IS-IS) protocol supports both broadcast networks and point-to-point (P2P) networks. This capability is crucial for its operation within different types of network architectures. In broadcast networks, IS-IS efficiently handles the dynamic nature of network topology changes, allowing multiple routers to communicate over a shared medium. This is commonly seen in Ethernet networks, where IS-IS can utilize Link State Protocols to share routing information among all nodes in the broadcast domain. Conversely, in point-to-point networks, IS-IS can establish direct connections between two endpoints. This effectiveness is essential in various scenarios, such as WAN links where routers connect directly over dedicated circuits. By accommodating both network types, IS-IS provides flexibility in deployment, making it suitable for diverse networking environments. This adaptability is one of the reasons IS-IS is widely used in large-scale and complex network infrastructures.

6. What is a key difference between IPv4 and IPv6?

A. IPv4 uses 64-bit addresses, while IPv6 uses 128-bit addresses

B. IPv4 can support fewer devices than IPv6

C. IPv4 has better security features than IPv6

D. IPv4 is more commonly used than IPv6

The choice indicating that IPv4 can support fewer devices than IPv6 is indeed correct because of the fundamental differences in address space. IPv4 uses 32-bit addresses, allowing for approximately 4.3 billion unique IP addresses. In contrast, IPv6 employs 128-bit addresses, which exponentially increases the number of possible addresses to about 340 undecillion (that's 340 followed by 36 zeros). This vast address space of IPv6 was designed specifically to accommodate the ever-growing number of internet-connected devices. The expansion to IPv6 is essential not only for providing unique addresses to every device but also for enabling the Internet of Things (IoT) and the future of online connectivity. As the digital landscape continues to evolve, the limitations of IPv4 become more apparent, emphasizing the need for a protocol that can handle a significantly larger number of devices.

7. How is 'attenuation' defined in relation to signal strength?

A. It is the delay in signal transmission

B. It refers to the reduction in signal strength as it travels through a medium

C. It measures the amplification of a signal

D. It indicates the clarity of the transmitted signal

Attenuation is defined as the reduction in signal strength as it travels through a medium. This phenomenon occurs due to various factors, such as the absorption of the signal by the medium, scattering, and other impedance mismatches. As a signal propagates through cables, water, air, or any other transmission medium, it loses energy, and this energy loss results in a weaker signal at the receiving end. Understanding attenuation is crucial for maintaining optimal signal quality in communication systems, as higher levels of attenuation can lead to significant degradation in performance and usability. In designing and troubleshooting networks, field technicians must consider attenuation to ensure that signal strength remains within acceptable limits for effective communication.

8. What does electrical interference from wiring or electric motors cause on telephone wiring?

A. Static noise issues

B. Noise on the line

C. Disconnected lines

D. Intermittent dialing issues

Electrical interference from wiring or electric motors can indeed lead to noise on the line in telephone systems. This interference can introduce unwanted signals that disrupt the clarity of voice communications, creating a range of unwanted sounds, including hums, buzzes, or static that can be picked up by the phone line. When electrical devices like motors operate, they can generate electromagnetic fields or electrical noise that can couple with the telephone wiring, leading to degradation in the quality of the audio signal. This phenomenon can result in a poor user experience, as the call may become difficult to understand due to the additional noise. The other choices, while potentially related to issues experienced in telecommunication systems, do not specifically encapsulate the nature of the problem caused by electrical interference as accurately as the concept of noise on the line.

9. What can notify Simple Network Management Protocol (SNMP) network management stations of multicast problems?

A. Multicast Alerts

B. Multicast Traps

C. Multicast Logs

D. Multicast Messages

Multicast Traps are specifically designed to notify Simple Network Management Protocol (SNMP) network management stations of issues that arise in a multicast network. Traps are unsolicited messages sent from an SNMP agent to the management station, providing real-time alerts about significant events or problems, such as multicast transmission errors or link failures.   Using traps within the context of SNMP allows for proactive monitoring, as they can be configured to trigger automatically when predefined multicast thresholds or conditions are not met. Instead of relying on periodic polling, which can be resource-intensive, traps provide immediate notification, making them an efficient means of managing network performance and identifying potential issues before they escalate. In contrast, other choices like Multicast Alerts, Multicast Logs, and Multicast Messages do not have specific definitions or established protocols within the context of SNMP that denote their role in notifying management stations. While they may illustrate various means of tracking or relaying information, they do not serve the same function or have the same structured purpose as Multicast Traps in SNMP environments.

10. In Synchronous Optical Networks (SONET), how much faster is the data rate of an electrical level STS-192 compared to an STS-1?

A. 192 times

B. 96 times

C. 48 times

D. 24 times

In Synchronous Optical Networks (SONET), the structure and hierarchy of data rates are clearly defined. An STS-1 (Synchronous Transport Signal level 1) has a data rate of 51.84 Mbps. In the SONET hierarchy, STS-192 is the signal level that corresponds to a data rate of 9.95328 Gbps (or 9,953.28 Mbps). To determine how many times faster STS-192 is compared to STS-1, you can perform a simple calculation: 1. Convert both data rates to the same unit (in this case, Mbps).   - STS-1 = 51.84 Mbps   - STS-192 = 9,953.28 Mbps   2. Divide the data rate of STS-192 by the data rate of STS-1:   - 9,953.28 / 51.84 = 192   This calculation shows that the STS-192 level is indeed 192 times faster than STS-1. Therefore, selecting the first option demonstrates a solid understanding of the hierarchical structure of SONET and the multiplying rates of the different signal levels. Understanding these data rates is crucial for optimizing bandwidth and