TestOut Network 009 Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. **How does a switch enhance network performance over a hub in a Fast Ethernet environment?**
   - A. By reducing the number of devices on the network
   - B. By allowing for half-duplex transmissions
   - C. By facilitating full-duplex transmissions and eliminating contention
   - D. By increasing overall bandwidth available

2. **Which of the following are typical uses of RG-59 coax cable?**
   - A. High-speed internet access
   - B. Closed circuit TV (CCTV) and audio/video applications
   - C. Telephone lines
   - D. Long-distance data transmission

3. **When troubleshooting cable connectivity issues, which OSI model layer is primarily focused on?**
   - A. Layer 2 - Data Link
   - B. Layer 3 - Network
   - C. Layer 1 - Physical
   - D. Layer 4 - Transport

4. **What does the term "crosstalk" refer to in UTP cabling?**
   - A. Physical damage to cables
   - B. Interference from external sources
   - C. Signal leakage between adjacent pairs
   - D. Data speed loss due to distance

5. **Which steps are involved in transmitting a signal using electromagnetic radiation? (Select two)**
   - A. Encoding and Modulation
   - B. Transmission and Reception
   - C. Decoding and Filtering
   - D. Sampling and Amplification

6. Which of the following is a typical use of twinaxial cables?

- **A. Residential internet connections**
- **B. Home theater audio systems**
- **C. Data center interconnects**
- **D. Long-distance telephone lines**

7. What is the main difference between TCP and UDP?

- **A. TCP is asynchronous while UDP is synchronous**
- **B. TCP is connection-oriented and reliable, while UDP is connectionless and faster**
- **C. TCP provides encryption while UDP does not**
- **D. TCP is used for local networks while UDP is used for the internet**

8. Which factors can adversely affect network throughput?

- **A. Link distance and interference**
- **B. More devices and increased bandwidth**
- **C. Reduced latency and upgraded hardware**
- **D. Improved signal strength and better cables**

9. In a contention-based MAC system, what are the consequences of adding more nodes to the network?

- **A. Collisions become more frequent**
- **B. Data transfer speeds improve**
- **C. Network devices require more power**
- **D. Latency decreases**

10. What is a subnet mask?

- **A. A number that divides an IP address into network and host portions**
- **B. A unique identifier for a device on a local network**
- **C. A protocol for data transmission**
- **D. A firewall setting for network traffic**

Answers

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

Explanations

1. How does a switch enhance network performance over a hub in a Fast Ethernet environment?

A. By reducing the number of devices on the network

B. By allowing for half-duplex transmissions

C. By facilitating full-duplex transmissions and eliminating contention

D. By increasing overall bandwidth available

A switch enhances network performance over a hub in a Fast Ethernet environment by facilitating full-duplex transmissions and eliminating contention. Unlike hubs, which operate using a shared medium and only allow one device to transmit at a time, switches create a dedicated communication path between devices. In a hub configuration, when one device sends data, it must wait for any ongoing transmissions to finish before it can transmit again. This can lead to collisions, especially when multiple devices attempt to communicate simultaneously, resulting in contention for the shared bandwidth. As a result, the overall network efficiency decreases, and performance suffers. Switches, on the other hand, manage data packets more efficiently. They can operate in full-duplex mode, allowing devices to send and receive data simultaneously without interference. This eliminates potential collisions and contention issues, which significantly improves throughput and reduces latency. The enhanced ability of switches to provide dedicated bandwidth to each connected device allows networks to scale better and handle larger amounts of data traffic more effectively. Therefore, the use of switches is crucial in modern networking to maintain high performance in environments that require fast and reliable data communication.

2. Which of the following are typical uses of RG-59 coax cable?

A. High-speed internet access

B. Closed circuit TV (CCTV) and audio/video applications

C. Telephone lines

D. Long-distance data transmission

RG-59 coax cable is commonly used in closed circuit television (CCTV) systems and various audio/video applications. This type of coaxial cable has a characteristic impedance of 75 ohms, which makes it ideal for transmitting video signals over short distances with minimal signal loss. In CCTV setups, RG-59 is particularly favored for connecting cameras to monitors or DVRs, as it can effectively carry video signals while also allowing for accompanying power transmission in some configurations. This suitability for video surveillance systems is what makes it a typical choice for such applications, as it ensures reliable performance without the need for extensive amplification or signal boosting. In contrast, RG-59 is not the right choice for high-speed internet access, telephone lines, or long-distance data transmission, where other types of cables, such as RG-6 for television and internet services or fiber optic cables for data transmission, are preferred due to their superior bandwidth capabilities and reduced attenuation over longer runs.

3. When troubleshooting cable connectivity issues, which OSI model layer is primarily focused on?

A. Layer 2 - Data Link

B. Layer 3 - Network

C. Layer 1 - Physical

D. Layer 4 - Transport

When troubleshooting cable connectivity issues, the primary focus is on the Physical layer of the OSI model, which is Layer 1. This layer is responsible for the actual transmission of data over physical media, such as cables and connectors. It encompasses the electrical and physical specifications of the network devices, including voltage levels, timing of signals, and physical characteristics of the hardware. Connectivity issues commonly arise from problems at this layer, such as faulty cables, loose connections, or damaged ports. Ensuring that the physical connection is intact and functioning correctly is essential for establishing a reliable network connection. Therefore, when diagnosing connectivity problems, checking the cables and physical connections is the first step, emphasizing the importance of Layer 1 in this context. In contrast, the Data Link layer, which deals with node-to-node data transfer and error detection, is pertinent but typically comes into play after confirming that the physical connection is operational. The Network layer is concerned with routing and forwarding of packets, while the Transport layer addresses end-to-end communication and data flow control, neither of which directly addresses the physical issues associated with cables.

4. What does the term "crosstalk" refer to in UTP cabling?

A. Physical damage to cables

B. Interference from external sources

C. Signal leakage between adjacent pairs

D. Data speed loss due to distance

Crosstalk in UTP (Unshielded Twisted Pair) cabling specifically refers to the phenomenon where signals from one cable pair interfere with signals in an adjacent pair. This typically happens because the twisted pairs are placed close together within the cable, and the electromagnetic fields that are generated when electrical signals pass through a pair can inadvertently affect nearby pairs. The design of twisted pairs aims to minimize crosstalk by twisting the wires in pairs, which helps to cancel out electromagnetic interference generated by each wire. However, if the crosstalk is significant, it can lead to data transmission errors and degradation of network performance. Understanding crosstalk is crucial in network design and troubleshooting, as it can significantly impact the reliability and efficiency of data transmission over UTP cabling.

5. Which steps are involved in transmitting a signal using electromagnetic radiation? (Select two)

A. Encoding and Modulation

B. Transmission and Reception

C. Decoding and Filtering

D. Sampling and Amplification

Transmitting a signal using electromagnetic radiation involves several key steps, among which encoding and modulation are fundamental. Encoding is the process of transforming information into a format suitable for transmission. This ensures that the data can be effectively sent over a medium and interpreted correctly upon reception. For example, encoding converts digital data into a form that can be handled by the modulation process. Modulation is the technique used to impose the encoded signal onto a carrier wave. This allows the signal to be transmitted over long distances without significant loss or interference. By varying the properties of the carrier wave—such as its amplitude, frequency, or phase—modulation facilitates the effective transmission of data over electromagnetic waves. These two processes are essential in preparing a signal for propagation through space, enabling it to travel from the transmitter to the receiver effectively.

6. Which of the following is a typical use of twinaxial cables?

A. Residential internet connections

B. Home theater audio systems

C. Data center interconnects

D. Long-distance telephone lines

Twinaxial cables are commonly used for data center interconnects due to their design and capabilities. They are known for their ability to support high-speed data transmission with low latency over relatively short distances, which makes them ideal for connecting servers, storage devices, and network switches within a data center environment. The cables' construction includes a central conductor, an insulating layer, a shielding layer, and an outer jacket, allowing them to minimize interference and maintain signal integrity even in environments with significant electromagnetic interference (EMI), such as data centers. Their typically short range—effective for distances up to about 30 meters—aligns well with the requirements of data centers, where connections need to be made between closely located devices. In contrast, twinaxial cables are not typically utilized for residential internet connections, home theater audio systems, or long-distance telephone lines, as those applications tend to favor other types of cabling solutions that are better suited for those specific needs.

7. What is the main difference between TCP and UDP?

A. TCP is asynchronous while UDP is synchronous

B. TCP is connection-oriented and reliable, while UDP is connectionless and faster

C. TCP provides encryption while UDP does not

D. TCP is used for local networks while UDP is used for the internet

The distinction between TCP and UDP is fundamentally rooted in their protocols and the way they manage data transmission. TCP, or Transmission Control Protocol, is described as connection-oriented and reliable. This means that before any data is sent, a connection is established between the sender and receiver, ensuring that both parties are ready for data exchange. During transmission, TCP guarantees that all packets arrive in the correct order and that any lost packets are retransmitted, ensuring data integrity and reliability. In contrast, UDP, or User Datagram Protocol, is connectionless and faster. It allows for data to be sent without establishing a dedicated end-to-end connection, which reduces the overhead and potentially speeds up transmission. However, it does not provide the same reliability guarantees as TCP. Packets sent via UDP may arrive out of order, or some may not arrive at all, and there is no mechanism for retransmission or error correction. The characteristics of TCP's reliability and connection-oriented nature make it well-suited for applications where data integrity is critical, such as web browsing or file transfers. UDP's speed and low latency make it ideal for applications where speed is prioritized, such as online gaming or video streaming, where a few lost packets might not significantly impact the user experience. Understanding these differences helps

8. Which factors can adversely affect network throughput?

A. Link distance and interference

B. More devices and increased bandwidth

C. Reduced latency and upgraded hardware

D. Improved signal strength and better cables

Link distance and interference can significantly adversely affect network throughput. When discussing link distance, it refers to how far data must travel from one device to another within the network. The longer the distance, the more potential for signal degradation due to attenuation, which can lead to slower data transmission speeds. Interference can stem from various sources, including physical obstacles, electronic devices, and even environmental factors, which can disrupt signals traveling over the network. This disruption can cause packet loss or the need for retransmissions, both of which contribute to reduced throughput. In contrast, options that mention having more devices, increased bandwidth, reduced latency, upgraded hardware, improved signal strength, or better cables are generally oriented towards enhancing network performance rather than hindering it. More devices can lead to congestion, but increased bandwidth paired with proper network management usually mitigates that issue. Meanwhile, reduced latency and improved hardware are likely to enhance throughput, while better cables and signal strength are associated with optimizing connections for higher speeds.

9. In a contention-based MAC system, what are the consequences of adding more nodes to the network?

A. Collisions become more frequent

B. Data transfer speeds improve

C. Network devices require more power

D. Latency decreases

In a contention-based Medium Access Control (MAC) system, the way nodes share the communication medium is crucial to understanding the impact of adding more nodes to the network. As more nodes are introduced, the likelihood of multiple devices attempting to transmit data simultaneously increases. This leads to an uptick in collisions—instances where two or more nodes transmit at the same time and their signals interfere with each other. When collisions occur, the involved nodes must back off and attempt to resend their data after a random time interval, which not only delays the transmission of the collided packets but can also lead to further collisions as more nodes compete for the same bandwidth. As a result, adding more nodes creates a chaotic environment where the medium becomes congested, amplifying the frequency of these collisions. Therefore, it is clear that in a contention-based MAC system, increasing the number of nodes directly correlates with an increase in collisions. While improving data transfer speeds, changing power requirements, or decreasing latency may be plausible in different networking scenarios, they do not result from simply adding more nodes to a contention-based MAC environment. Instead, they may lead to detrimental effects that make the network less efficient and more prone to issues.

10. What is a subnet mask?

A. A number that divides an IP address into network and host portions

B. A unique identifier for a device on a local network

C. A protocol for data transmission

D. A firewall setting for network traffic

The subnet mask is indeed a number that divides an IP address into its network and host portions. This is essential for IP addressing in networks, as it defines how many bits are used for the network part of the address and how many bits are used for the host part. For example, in IPv4 addressing, a common subnet mask is 255.255.255.0, which indicates that the first three octets (or 24 bits) represent the network address, while the last octet (or 8 bits) is used for host addresses within that network. By differentiating between the network and host portions, devices within the same network can communicate effectively without routing through larger networks. This subdivision is crucial for efficient network management and enables the development of network hierarchies. In contrast, unique identifiers for devices on a local network refer to IP addresses assigned to each device, which should not be confused with the subnet mask's function of defining network boundaries. Data transmission protocols encompass a variety of methods for sending data across networks but do not pertain to the structural division of IP addresses. Lastly, firewall settings relate to security and the control of network traffic, rather than the foundational structure of IP addresses themselves.