Cyber Support Journeyman Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. **Which discipline focuses on protecting data in computer systems against unauthorized access?**

   A. OPSEC

   B. EMSEC

   C. COMSEC

   D. COMPUSEC

2. **Which center is typically aligned under the base communications squadron, provides Tier 3 (local level) on-site, and implements technical and physical network changes?**

   A. Area Processing Center (APC)

   B. Network Control Center (NCC)

   C. Air Force Network Operations Center (AFNOC)

   D. Integrated Network Operations and Security Center (I-NOSC)

3. **What IPv4 class address is used for networks with about 250 nodes?**

   A. Class A

   B. Class D

   C. Class C

   D. Class E

4. **Which organization assigns COMMSEC incident report case numbers?**

   A. Air Force Communications Agency

   B. Air Force Office of Record

   C. Central Office of Records

   D. National Security Agency

5. **What concerns slowed the military's adoption of wireless network technology?**

   A. Speed and reliability.

   B. Security and reliability.

   C. Reliability and maintenance.

   D. Certification and interoperability.

6. An optical communications system is comprised of which components?

A. Transmitter, cable, and receiver

B. Transmitter, cable, and logic analyzer

C. Transmitter, transmission medium, and logic analyzer

D. Transmitter, transmission medium, and protocol analyzer

7. At which NETOPS level is global management of the defense information infrastructure overseen?

A. Tier 1

B. Tier 2

C. Tier 3

D. Tier 4

8. The ability to move about without being tethered by wires in wireless technology is referred to as what?

A. Mobility

B. Ease of installations

C. War driving

D. Motion capture technology

9. What is the difference between a hub router and a premise router?

A. Operated and managed as a base communications asset.

B. Considered one of the primary components of the Defense Information Systems Network.

C. Interconnected via the Defense Information Systems Agency Asynchronous Transfer Mode network.

D. Completely protected by encryption devices.

10. What topology defines the way in which devices communicate, and data is transmitted throughout the network?

A. Physical

B. Logical

C. Star

D. Hybrid

Answers

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

Explanations

1. Which discipline focuses on protecting data in computer systems against unauthorized access?

A. OPSEC

B. EMSEC

C. COMSEC

D. COMPUSEC

The correct choice centers on COMPUSEC, which stands for Computer Security. This discipline is specifically dedicated to safeguarding the integrity, availability, and confidentiality of data stored on computer systems. COMPUSEC encompasses various practices and measures designed to prevent unauthorized access to both physical hardware and the data it contains. This includes the implementation of access controls, encryption, user authentication, and various security policies that aim to protect sensitive information from threats. Understanding the protection of data in computer systems is fundamental in the realm of cybersecurity. The principles of COMPUSEC apply to all aspects of computing, from securing networked environments to protecting individual workstations. This makes it an essential area of focus for anyone involved in maintaining the security and integrity of information processed through technological systems.

2. Which center is typically aligned under the base communications squadron, provides Tier 3 (local level) on-site, and implements technical and physical network changes?

A. Area Processing Center (APC)

B. Network Control Center (NCC)

C. Air Force Network Operations Center (AFNOC)

D. Integrated Network Operations and Security Center (I-NOSC)

The Network Control Center (NCC) is the correct choice because it is specifically designed to provide Tier 3 support at the local level. This encompasses on-site assistance and the implementation of technical and physical changes to the network. The NCC plays a crucial role in managing and overseeing the operational aspects of the network, ensuring that it runs smoothly and efficiently while addressing any issues that arise. While other centers have important functions, they do not primarily focus on local-level on-site support in the same manner as the NCC. The Area Processing Center (APC), for instance, typically manages data processing tasks and does not handle on-site technical support directly. The Air Force Network Operations Center (AFNOC) operates at a higher level, dealing with broader network operations and oversight rather than localized issues. The Integrated Network Operations and Security Center (I-NOSC) focuses on integrating network operations and security at a more strategic level but does not provide the hands-on local support that the NCC is tasked with. Therefore, the NCC's role encompasses the essential responsibilities of providing local technical support and managing network changes, making it the appropriate choice in this context.

3. What IPv4 class address is used for networks with about 250 nodes?

A. Class A

B. Class D

C. Class C

D. Class E

The correct choice of Class C addresses is based on the capacity they provide for network devices. Class C IP addresses are designed to accommodate smaller networks, typically allowing for up to 254 usable host addresses, as each Class C network has a default subnet mask of 255.255.255.0. This range is ideal for networks that require around 250 nodes, as it fits the requirement very well while also providing enough address space for additional devices if necessary. In contrast, Class A addresses are meant for very large networks and offer a significantly larger range of host addresses—over 16 million—far more than what is necessary for a typical small network. Class D addresses are designated for multicast groups and do not serve as typical host addresses for standard networks. Class E addresses are reserved for experimental purposes and are not used for general networking, making them unsuitable for the described scenario. Therefore, Class C is the most appropriate choice for a network with approximately 250 nodes.

4. Which organization assigns COMMSEC incident report case numbers?

A. Air Force Communications Agency

B. Air Force Office of Record

C. Central Office of Records

D. National Security Agency

The correct answer highlights that the Air Force Communications Agency is responsible for assigning COMMSEC incident report case numbers. This organization plays a pivotal role in managing communications security (COMMSEC) within the Air Force, including logging and tracking security incidents related to communications systems. By creating a systematic way to assign case numbers, the agency ensures a consistent approach to handling security incidents and facilitates effective reporting, documentation, and follow-up. In contrast, the other options are associated with different functions or responsibilities. The Air Force Office of Record primarily deals with the archiving and maintenance of official records but does not handle COMMSEC incident reports specifically. The Central Office of Records is not directly involved in COMMSEC matters and typically pertains to overarching record management functions. The National Security Agency focuses on national security and intelligence but does not assign case numbers for Air Force-specific COMMSEC incidents. Thus, the Air Force Communications Agency is the most relevant organization for this function.

5. What concerns slowed the military's adoption of wireless network technology?

A. Speed and reliability.

B. Security and reliability.

C. Reliability and maintenance.

D. Certification and interoperability.

The slow adoption of wireless network technology by the military can primarily be attributed to concerns over security and reliability. Security is a paramount issue, especially for military operations, as wireless communications can be more susceptible to interception, hacking, and other malicious activities compared to wired connections. The potential vulnerabilities inherent in wireless networks necessitate robust encryption and security measures to protect sensitive information and maintain operational integrity. Reliability is equally crucial, as military operations often require constant and uninterrupted communication. The adverse effects of environmental factors, such as interference or signal degradation, can impact the effectiveness of operations. Ensuring that wireless technology can deliver consistent and reliable communication, particularly in critical situations, is essential for mission success. While other concerns such as speed, maintenance, certification, and interoperability are important in assessing network technology, the unique demands of military applications place heightened emphasis on security and reliability as fundamental priorities that must be addressed before widespread adoption can be realized.

6. An optical communications system is comprised of which components?

A. Transmitter, cable, and receiver

B. Transmitter, cable, and logic analyzer

C. Transmitter, transmission medium, and logic analyzer

D. Transmitter, transmission medium, and protocol analyzer

The correct answer highlights the fundamental components of an optical communications system. It includes a transmitter, which is responsible for converting electrical signals into optical signals for transmission. The cable, or optical fiber, serves as the transmission medium, allowing these optical signals to travel from the transmitter to the receiver with minimal signal loss and interference. Finally, the receiver is essential for converting the received optical signals back into electrical signals that can be utilized by devices or systems. The inclusion of a logic analyzer or protocol analyzer in the other options lacks relevance to the basic structure of an optical communication system. While these tools are useful for analyzing and troubleshooting data for various types of communications, they do not form the core components necessary for the system's operation.

7. At which NETOPS level is global management of the defense information infrastructure overseen?

A. Tier 1

B. Tier 2

C. Tier 3

D. Tier 4

The correct answer reflects that global management of the defense information infrastructure is overseen at Tier 1. This tier deals with the highest level of oversight within NETOPS (Network Operations) and is responsible for managing the entire scope of operations and strategic direction across the defense information networks. Tier 1 focuses on global resource management, strategic planning, and coordination of services and capabilities necessary to ensure the efficient functioning and security of the defense information infrastructure. This includes maintaining awareness of the operational status, security posture, and overall health of the networks. In contrast, the other tiers such as Tier 2 and Tier 3 tend to focus on more localized management and operational execution, dealing with specific segments of the network and tactical level responses. Tier 4, while also involved in operational aspects, generally pertains to more granular, technical management and troubleshooting rather than overarching global strategies. Therefore, Tier 1 stands out as the correct level for global oversight.

8. The ability to move about without being tethered by wires in wireless technology is referred to as what?

A. Mobility

B. Ease of installations

C. War driving

D. Motion capture technology

The concept of moving about without the restriction of being tethered by wires in wireless technology is defined as "mobility." This term encompasses the freedom and flexibility that wireless systems provide to users, allowing them to connect to networks and communicate without being bound by physical connections. Mobility is a fundamental aspect of many modern technologies, including smartphones, laptops, and tablet devices, which utilize wireless technologies such as Wi-Fi, Bluetooth, and cellular networks to enable users to access information and connect with others from virtually anywhere. While ease of installations is also relevant to wireless technology, it primarily deals with how straightforward it is to set up these networks and devices rather than the movement aspect. War driving refers to the act of searching for open or unsecured wireless networks, and motion capture technology involves tracking movement, often for applications in gaming or animation, which do not directly relate to the concept of being untethered in wireless communication. Thus, mobility stands out as the most accurate and relevant term in describing this capability.

9. What is the difference between a hub router and a premise router?

A. Operated and managed as a base communications asset.

B. Considered one of the primary components of the Defense Information Systems Network.

C. Interconnected via the Defense Information Systems Agency Asynchronous Transfer Mode network.

D. Completely protected by encryption devices.

The distinction between a hub router and a premise router primarily relates to their functions and contexts in networking, particularly when considering how they interact within larger systems like the Defense Information Systems Network (DISN). The correct choice emphasizes that a hub router is interconnected via networks such as the Defense Information Systems Agency (DISA) Asynchronous Transfer Mode (ATM) network. This highlights the role of hub routers in facilitating communication within a wide area network (WAN) framework, allowing routing and management of network traffic between various locations and nodes. In contrast, premise routers typically serve as local devices that manage service delivery within a specific physical location, such as an office or building. They are not designed for the same level of inter-connection across a wide area network like hub routers. This means that while both types of routers play critical roles in network infrastructure, their applications and the scale at which they operate differ significantly. Therefore, this understanding of interconnectivity via ATM networks encapsulates why this option reflects an accurate differentiation.

10. What topology defines the way in which devices communicate, and data is transmitted throughout the network?

A. Physical

B. Logical

C. Star

D. Hybrid

The logical topology refers to the way in which data flows on the network and how devices communicate with one another, regardless of their physical arrangement. This concept is crucial because it determines the actual path that data takes and how it is handled by the network protocols. For instance, even if devices are physically connected in a certain way, the logical topology defines how the network appears from a functional perspective. In contrast, the physical topology describes the specific physical layout of devices and cables in the network, which does not always represent how the data is transmitted or how devices communicate logically. While star, hybrid, and other specific topologies may depict certain physical arrangements, they do not inherently address the logical pathways and data flow. Thus, when considering how data moves and devices interact on the network, the logical topology is the accurate descriptor. This reinforces the understanding that communication and data transmission dynamics are dictated by the logical arrangement rather than merely the physical configuration of network components.