Network+ (N10-009) Practice Exam #2

Questions

1. Which QoS technique is used to control the rate of traffic being sent into a network?

A) Queuing
B) Policing
C) Classification
D) Congestion Avoidance

2. What is a primary benefit of using a Content Delivery Network (CDN)?

A) Increased network congestion
B) Improved content delivery speed
C) Reduced security
D) Higher latency

3. You need to power a network device without using an external power supply. Which technology would you use?

A) Ethernet trunking
B) Power over Ethernet (PoE)
C) Link aggregation
D) VLAN tagging

4. Which practice can help improve wiring management in a network?

A) Labeling cables and connections
B) Using long, uncoiled cables
C) Avoiding cable ties
D) Running cables loosely across the floor

5. How many usable host addresses are available in a subnet with a subnet mask of 255.255.255.240?

A) 4
B) 6
C) 14
D) 30

6. What is a key difference between active-active and active-passive network device configurations?

A) Active-active requires manual failover
B) Active-passive improves network performance
C) Active-active provides load balancing and failover
D) Active-passive offers higher availability

7. Which of the following is a key component of IT risk management?

A) Increasing network speed
B) Identifying and mitigating risks
C) Simplifying network configuration
D) Reducing hardware costs

8. You need to connect a fiber optic network to an existing copper network. Which device should you use?

A) Switch
B) Router
C) Hub
D) Media converter

9. Which of the following is an effective method for securing DHCP in a network?

A) Implementing IPsec
B) Using DHCP snooping
C) Enabling port mirroring
D) Configuring BPDU Guard

10. What is a primary advantage of using InfiniBand in SANs?

A) Low cost
B) Compatibility with older technologies
C) Simplified configuration
D) High bandwidth and low latency

11. Which of the following is an impact of the 802.11h amendment on wireless networks?

A) Increased data rates
B) Enhanced security
C) Dynamic frequency selection and transmit power control
D) Simplified configuration

12. What is the purpose of a Switch Virtual Interface (SVI) in a VLAN configuration?

A) Assigning IP addresses
B) Encrypting data
C) Managing domain names
D) Providing Layer 3 routing capabilities

13. Which of the following is a characteristic of Secure Access Secure Edge (SASE)?

A) Centralized on-premises security
B) Integration of networking and security functions in the cloud
C) Limited scalability
D) Manual configuration of security policies

14. Why is network segmentation important for operational technology (OT) environments?

A) To increase network speed
B) To enhance security by isolating critical systems
C) To simplify configuration
D) To reduce hardware costs

15. What type of information is typically shown in a Layer 3 network diagram?

A) Physical cable connections
B) Logical IP addressing and routing
C) MAC address mapping
D) Device power requirements

16. Which of the following strategies helps achieve high availability in a network?

A) Redundant systems and failover mechanisms
B) Single points of failure
C) Using non-standard equipment
D) Manual configuration

17. What is the purpose of Ethernet port flow control in a network?

A) Increasing data transmission speed
B) Encrypting network traffic
C) Assigning IP addresses
D) Managing traffic congestion

18. What is the primary function of a Network Security Group (NSG) in a cloud environment?

A) Encrypting data
B) Assigning IP addresses
C) Controlling inbound and outbound traffic
D) Managing domain names

19. Which of the following is a primary function of a proxy server?

A) Encrypting data transmissions
B) Caching web content
C) Creating virtual networks
D) Managing IP addresses

20. What is the IPv6 loopback address?

A) fe80::1
B) ff02::1
C) ::1
D) 2001:db8::1

21. Which of the following is a best practice for network documentation?

A) Documenting only major network changes
B) Keeping network diagrams and configurations up-to-date
C) Avoiding documentation of temporary changes
D) Limiting access to network documentation

22. What is a key characteristic of a wide area network (WAN)?

A) Connects devices within a single building
B) Covers a large geographic area
C) Uses Bluetooth technology
D) Is limited to short distances

23. By default, which of the following metrics does EIGRP use to determine the best path?

A) Hop count
B) Cost
C) Bandwidth and delay
D) Administrative distance

24. Which of the following is the first step in CompTIA's 7-step network troubleshooting methodology?

A) Establish a theory of probable cause
B) Implement a solution
C) Identify the problem
D) Verify full system functionality

25. Which factor is commonly used to determine the best route in a routing table?

A) Hop count
B) Prefix length and metric
C) IP address
D) MAC address

26. What is the hexadecimal representation of the decimal number 255?

A) FF
B) 100
C) 0x10
D) AA

27. Which type of attack aims to make a network service unavailable to its intended users?

A) Phishing
B) Man-in-the-middle
C) Denial of Service (DoS)
D) SQL injection

28. What is the primary function of an Internet Gateway in a cloud environment?

A) Encrypting data transmissions
B) Providing a connection to the Internet
C) Managing domain names
D) Assigning IP addresses

29. Which of the following best describes a Virtual Private Cloud (VPC)?

A) A private network within a public cloud
B) A physical data center
C) A local area network
D) A dedicated physical server

30. What is the primary benefit of using DNS over TLS (DoT)?

A) Assigning IP addresses
B) Encrypting DNS traffic to protect against eavesdropping
C) Managing domain names
D) Reducing latency

31. Which of the following is a primary benefit of deploying a WLAN?

A) Increased wired connections
B) Mobility and flexibility for users
C) Simplified cabling
D) Enhanced security

32. Why is maintaining an asset inventory important in network management?

A) To increase network speed
B) To track and manage hardware, software, licensing, and warranty support
C) To simplify configuration
D) To reduce hardware costs

33. Which of the following best describes the purpose of a MAC address in a network?

A) Logical addressing
B) Physical addressing
C) Routing decisions
D) Domain name resolution

34. What is the primary purpose of Network Time Security (NTS)?

A) Encrypting network traffic
B) Managing domain names
C) Assigning IP addresses
D) Securing time synchronization protocols

35. Why is performance monitoring important in a network?

A) To simplify configuration
B) To ensure optimal network performance and identify issues
C) To reduce hardware costs
D) To manage domain names

36. What is the primary goal of availability monitoring in a network?

A) To track IP address allocations
B) To ensure network services are accessible and operational
C) To manage domain names
D) To encrypt data transmissions

37. In a bus topology, what happens if the main cable fails?

A) Only the connected devices are affected
B) The entire network fails
C) Traffic is rerouted
D) Network speed decreases

38. Which of the following best describes the purpose of Quality of Service (QoS)?

A) Encrypting data
B) Prioritizing network traffic
C) Routing packets based on destination
D) Managing IP addresses

39. Which of the following best describes a screened subnet zone (DMZ)?

A) A network segment isolated from both the internal network and the Internet
B) A secure internal network
C) A public-facing network
D) A private network

40. You need to allow multiple VLANs to communicate across a single link. Which feature would you use?

A) Link aggregation
B) Port mirroring
C) Spanning Tree Protocol
D) Trunking

41. Which of the following best describes a client-server network?

A) All devices have equal roles
B) Centralized server provides resources to clients
C) Devices connect directly to each other
D) Communication is peer-to-peer

42. What does the term 'dual stack' refer to in networking?

A) Using two separate networks
B) Running both IPv4 and IPv6 on the same network
C) Having redundant network devices
D) Utilizing dual processors for networking tasks

43. What is the purpose of a change control process in network management?

A) Increasing network speed
B) Documenting and approving changes to the network
C) Simplifying network configuration
D) Reducing hardware costs

44. What is a common method for securing data at rest?

A) Encrypting the data
B) Using VLANs
C) Assigning IP addresses
D) Implementing DHCP

45. What is the primary purpose of URL filtering in network security?

A) Encrypting data
B) Controlling access to websites based on their URLs
C) Assigning IP addresses
D) Managing domain names

46. Which of the following best describes the purpose of configuration monitoring?

A) Encrypting data
B) Tracking and validating device configurations
C) Assigning IP addresses
D) Managing domain names

47. Why is disaster recovery testing important?

A) To increase network speed
B) To ensure the effectiveness of the disaster recovery plan
C) To simplify configuration
D) To reduce hardware costs

48. Which tool would you use to insert wires into a patch panel?

A) Crimper
B) Punch-down tool
C) Wire stripper
D) Multimeter

49. Which tool is commonly used for managing IP address allocations and usage in a network?

A) DHCP
B) IPAM
C) DNS
D) SNMP

50. You need to resolve domain names to IP addresses for a network application. Which service would you configure?

A) DHCP
B) DNS
C) FTP
D) SNMP

51. What is the principle of least privilege in network security?

A) Allowing all users full access
B) Using default passwords
C) Avoiding user authentication
D) Granting users the minimum access necessary for their roles

52. What is the primary goal of a DNS spoofing attack?

A) To redirect traffic to malicious sites by altering DNS responses
B) To encrypt DNS traffic
C) To assign IP addresses
D) To manage domain names

53. Which switch port security feature can help prevent unauthorized devices from connecting to the network?

A) Spanning Tree Protocol
B) Link aggregation
C) Port security
D) VLAN trunking

54. Which of the following is a characteristic of self-signed certificates?

A) Issued by a trusted certificate authority
B) Used only for internal purposes
C) Validated by third parties
D) Automatically trusted by all devices

55. What is the primary purpose of identity and access management (IAM)?

A) Encrypting data
B) Managing and controlling user access to resources
C) Assigning IP addresses
D) Monitoring network performance

56. Which of the following is a primary use case for SIP trunks?

A) Connecting devices in a LAN
B) Establishing VoIP communication with the public switched telephone network
C) Providing wireless connectivity
D) Encrypting email communications

57. You want to increase the bandwidth and provide redundancy between two switches. Which feature would you use?

A) VLAN tagging
B) Link aggregation
C) Port mirroring
D) Trunking

58. Which of the following best describes a static route?

A) A route automatically added by routing protocols
B) A route manually configured by an administrator
C) A route with the highest priority in the routing table
D) A route used for default traffic

59. Which of the following best describes an IPv6 unique local address?

A) Routable on the Internet
B) Used for private, internal communication
C) Always starts with fe80::
D) Used for multicast communication

60. Which of the following is a key characteristic of the Industrial Internet of Things (IIoT)?

A) Consumer-focused applications
B) Integration of industrial equipment with network connectivity
C) Limited scalability
D) Manual configuration

61. Which device is specifically designed to handle a large number of VPN connections?

A) Router
B) Switch
C) VPN Concentrator
D) Firewall

62. Which of the following is a common security concern associated with IoT devices?

A) High bandwidth usage
B) Limited processing power
C) Weak default passwords
D) Complex configuration

63. What is a key consideration in power management for network equipment?

A) Using non-standard power supplies
B) Disabling power backups
C) Avoiding power monitoring
D) Implementing redundant power sources

64. You are a network engineer tasked with connecting several branch offices within the same city. Which technology might you use?

A) VPN
B) DSL
C) Metro Ethernet
D) Satellite

65. Which of the following protocols automatically assigns IP addresses to devices on a network?

A) DNS
B) HTTP
C) DHCP
D) SMTP

66. Which of the following is an example of a Personal Area Network (PAN)?

A) Office LAN
B) Home Wi-Fi network
C) Bluetooth connection between a phone and headset
D) Corporate intranet

67. How does an Ethernet switch determine where to forward a frame?

A) By IP address
B) By MAC address
C) By protocol type
D) By port number

68. Which command would you use on a Cisco switch to display the MAC address table?

A) show arp
B) show vlan
C) show mac address-table
D) show power

69. What is the primary function of Access Control Lists (ACLs) in a network?

A) Encrypting data
B) Controlling network traffic
C) Assigning IP addresses
D) Managing domain names

70. Which of the following best describes multi-tenancy in cloud computing?

A) Each user has a dedicated physical server
B) Multiple users share the same physical resources
C) Users have isolated networks
D) Cloud services are available only to a single organization

71. Which of the following best describes wireless band steering?

A) Directing traffic to the least congested channel
B) Using only the 2.4 GHz band
C) Avoiding interference from other devices
D) Automatically guiding devices to the most appropriate frequency band

72. Which of the following is a key benefit of using playbooks in IaC automation?

A) Manual configuration
B) Automated and repeatable tasks
C) Increased configuration drift
D) Reduced compliance

73. Which of the following is an important aspect of disaster recovery planning?

A) Increasing network bandwidth
B) Regularly testing and updating the disaster recovery plan
C) Simplifying network configuration
D) Reducing hardware costs

74. Which of the following best describes a Metropolitan Area Network (MAN)?

A) Limited to a single home
B) Covers a city or large campus
C) Connects international offices
D) Uses fiber optic technology exclusively

75. Which issue might occur if a PoE device exceeds the switch's power budget?

A) Increased bandwidth
B) Device overheating
C) Decreased signal strength
D) Loss of power to PoE devices

76. Which of the following is a primary use case for VXLAN?

A) Encrypting network traffic
B) Providing Layer 2 connectivity over Layer 3 networks
C) Assigning IP addresses
D) Managing domain names

77. Which of the following best describes DNS over HTTPS (DoH)?

A) Encrypting DNS traffic to enhance privacy and security
B) Assigning IP addresses
C) Managing domain names
D) Providing a backup for DNS servers

78. What is a primary function of a VPN?

A) Increase Internet speed
B) Encrypt data transmissions
C) Convert IP addresses
D) Cache web content

79. Which protocol is commonly used to access cloud services securely over the Internet?

A) HTTP
B) FTP
C) HTTPS
D) Telnet

80. What is the purpose of a solicited-node multicast address in IPv6?

A) Routing data to all nodes on a network
B) Assisting in neighbor discovery
C) Providing a loopback mechanism
D) Offering a unique local address

81. What is a key benefit of using the 6 GHz band for wireless communication?

A) Increased interference
B) Reduced signal strength
C) Limited device compatibility
D) Greater available bandwidth

82. What is the key difference between in-band and out-of-band network management?

A) In-band management uses a separate network for control traffic
B) Out-of-band management uses the same network as data traffic
C) In-band management uses the same network as data traffic
D) Out-of-band management does not provide remote access

Questions and Answers

1. Which QoS technique is used to control the rate of traffic being sent into a network?

A) Queuing
B) Policing
C) Classification
D) Congestion Avoidance

Answer: B) Policing

Explanation: Both Policing and Shaping mechanisms can be used to limit the rate of traffic being sent into a network. Shaping delays excess packets, while Policing (by default) drops excess packets.

2. What is a primary benefit of using a Content Delivery Network (CDN)?

A) Increased network congestion
B) Improved content delivery speed
C) Reduced security
D) Higher latency

Answer: B) Improved content delivery speed

Explanation: A Content Delivery Network (CDN) improves content delivery speed by caching content at multiple locations closer to end users, reducing latency and load times.

3. You need to power a network device without using an external power supply. Which technology would you use?

A) Ethernet trunking
B) Power over Ethernet (PoE)
C) Link aggregation
D) VLAN tagging

Answer: B) Power over Ethernet (PoE)

Explanation: Power over Ethernet (PoE) allows network devices to receive power through Ethernet cables, eliminating the need for external power supplies.

4. Which practice can help improve wiring management in a network?

A) Labeling cables and connections
B) Using long, uncoiled cables
C) Avoiding cable ties
D) Running cables loosely across the floor

Answer: A) Labeling cables and connections

Explanation: Labeling cables and connections improves wiring management by making it easier to identify and trace connections, reducing the risk of errors and simplifying maintenance.

5. How many usable host addresses are available in a subnet with a subnet mask of 255.255.255.240?

A) 4
B) 6
C) 14
D) 30

Answer: B) 6

Explanation: A subnet mask of 255.255.255.240 (or /28) has 28 network bits and 4 host bits (i.e., 32 – 28 = 4). To calculate the number of assignable host IP addresses, we can use the formula: #_OF_HOSTS = 2^h – 2 where "h" is the number of hosts bits. In this example, the number of hosts = 2^4 – 2 = 16 – 2 = 14. Note that we subtract 2, because we cannot assign the network address or the directed broadcast address to a host.

6. What is a key difference between active-active and active-passive network device configurations?

A) Active-active requires manual failover
B) Active-passive improves network performance
C) Active-active provides load balancing and failover
D) Active-passive offers higher availability

Answer: C) Active-active provides load balancing and failover

Explanation: Active-active configurations provide load balancing and failover, with all devices actively handling traffic, while active-passive configurations have one active device and one standby for failover.

7. Which of the following is a key component of IT risk management?

A) Increasing network speed
B) Identifying and mitigating risks
C) Simplifying network configuration
D) Reducing hardware costs

Answer: B) Identifying and mitigating risks

Explanation: IT risk management involves identifying potential risks and implementing measures to mitigate or eliminate them, ensuring the security and reliability of IT systems.

8. You need to connect a fiber optic network to an existing copper network. Which device should you use?

A) Switch
B) Router
C) Hub
D) Media converter

Answer: D) Media converter

Explanation: A media converter is used to connect different types of media, such as fiber optic and copper, allowing networks with different cabling to communicate.

9. Which of the following is an effective method for securing DHCP in a network?

A) Implementing IPsec
B) Using DHCP snooping
C) Enabling port mirroring
D) Configuring BPDU Guard

Answer: B) Using DHCP snooping

Explanation: DHCP snooping helps secure DHCP by monitoring DHCP messages and filtering out malicious or unauthorized DHCP server responses, preventing DHCP-related attacks.

10. What is a primary advantage of using InfiniBand in SANs?

A) Low cost
B) Compatibility with older technologies
C) Simplified configuration
D) High bandwidth and low latency

Answer: D) High bandwidth and low latency

Explanation: InfiniBand offers high bandwidth and low latency, making it an ideal choice for high-performance SANs (Storage Area Networks).

11. Which of the following is an impact of the 802.11h amendment on wireless networks?

A) Increased data rates
B) Enhanced security
C) Dynamic frequency selection and transmit power control
D) Simplified configuration

Answer: C) Dynamic frequency selection and transmit power control

Explanation: The 802.11h amendment introduces dynamic frequency selection (DFS) and transmit power control (TPC) to mitigate interference with radar systems and comply with regulatory requirements.

12. What is the purpose of a Switch Virtual Interface (SVI) in a VLAN configuration?

A) Assigning IP addresses
B) Encrypting data
C) Managing domain names
D) Providing Layer 3 routing capabilities

Answer: D) Providing Layer 3 routing capabilities

Explanation: An SVI (Switch Virtual Interface) provides Layer 3 routing capabilities for VLANs, allowing inter-VLAN communication and routing within a switch.

13. Which of the following is a characteristic of Secure Access Secure Edge (SASE)?

A) Centralized on-premises security
B) Integration of networking and security functions in the cloud
C) Limited scalability
D) Manual configuration of security policies

Answer: B) Integration of networking and security functions in the cloud

Explanation: SASE (Secure Access Secure Edge) integrates networking and security functions in the cloud, providing scalable and flexible security services at the network edge.

14. Why is network segmentation important for operational technology (OT) environments?

A) To increase network speed
B) To enhance security by isolating critical systems
C) To simplify configuration
D) To reduce hardware costs

Answer: B) To enhance security by isolating critical systems

Explanation: Network segmentation enhances security in OT environments by isolating critical systems from other network segments, reducing the risk of unauthorized access and attacks.

15. What type of information is typically shown in a Layer 3 network diagram?

A) Physical cable connections
B) Logical IP addressing and routing
C) MAC address mapping
D) Device power requirements

Answer: B) Logical IP addressing and routing

Explanation: A Layer 3 network diagram typically shows logical IP addressing and routing information, detailing how data is routed across the network.

16. Which of the following strategies helps achieve high availability in a network?

A) Redundant systems and failover mechanisms
B) Single points of failure
C) Using non-standard equipment
D) Manual configuration

Answer: A) Redundant systems and failover mechanisms

Explanation: High availability is achieved by implementing redundant systems and failover mechanisms, ensuring continuous operation and minimal downtime in case of failures.

17. What is the purpose of Ethernet port flow control in a network?

A) Increasing data transmission speed
B) Encrypting network traffic
C) Assigning IP addresses
D) Managing traffic congestion

Answer: D) Managing traffic congestion

Explanation: Ethernet port flow control manages traffic congestion by regulating the flow of data, preventing packet loss and ensuring smooth communication.

18. What is the primary function of a Network Security Group (NSG) in a cloud environment?

A) Encrypting data
B) Assigning IP addresses
C) Controlling inbound and outbound traffic
D) Managing domain names

Answer: C) Controlling inbound and outbound traffic

Explanation: A Network Security Group (NSG) controls inbound and outbound traffic in a cloud environment by defining rules that permit or deny traffic based on IP addresses, protocols, and ports.

19. Which of the following is a primary function of a proxy server?

A) Encrypting data transmissions
B) Caching web content
C) Creating virtual networks
D) Managing IP addresses

Answer: B) Caching web content

Explanation: A proxy server acts as an intermediary between a client and a server, caching web content to improve load times and reduce bandwidth usage.

20. What is the IPv6 loopback address?

A) fe80::1
B) ff02::1
C) ::1
D) 2001:db8::1

Answer: C) ::1

Explanation: The IPv6 loopback address is ::1, used for testing and diagnostics on the local device.

21. Which of the following is a best practice for network documentation?

A) Documenting only major network changes
B) Keeping network diagrams and configurations up-to-date
C) Avoiding documentation of temporary changes
D) Limiting access to network documentation

Answer: B) Keeping network diagrams and configurations up-to-date

Explanation: Keeping network diagrams and configurations up-to-date is a best practice for network documentation, ensuring accurate and current information is available for troubleshooting and management.

22. What is a key characteristic of a wide area network (WAN)?

A) Connects devices within a single building
B) Covers a large geographic area
C) Uses Bluetooth technology
D) Is limited to short distances

Answer: B) Covers a large geographic area

Explanation: A WAN spans a large geographic area, connecting multiple LANs across cities, regions, or even countries, often using leased telecommunication lines.

23. By default, which of the following metrics does EIGRP use to determine the best path?

A) Hop count
B) Cost
C) Bandwidth and delay
D) Administrative distance

Answer: C) Bandwidth and delay

Explanation: EIGRP (Enhanced Interior Gateway Routing Protocol) uses a composite metric based on bandwidth and delay by default to determine the best path.

24. Which of the following is the first step in CompTIA's 7-step network troubleshooting methodology?

A) Establish a theory of probable cause
B) Implement a solution
C) Identify the problem
D) Verify full system functionality

Answer: C) Identify the problem

Explanation: The first step in CompTIA's 7-step network troubleshooting methodology is to identify the problem, gathering information to understand the issue at hand.

25. Which factor is commonly used to determine the best route in a routing table?

A) Hop count
B) Prefix length and metric
C) IP address
D) MAC address

Answer: B) Prefix length and metric

Explanation: The best route in a routing table is typically determined by prefix length (longest match) and metric (cost), ensuring the most efficient path is selected.

26. What is the hexadecimal representation of the decimal number 255?

A) FF
B) 100
C) 0x10
D) AA

Answer: A) FF

Explanation: The hexadecimal representation of the decimal number 255 is FF, which each represent a series of eight binary ones.

27. Which type of attack aims to make a network service unavailable to its intended users?

A) Phishing
B) Man-in-the-middle
C) Denial of Service (DoS)
D) SQL injection

Answer: C) Denial of Service (DoS)

Explanation: A Denial of Service (DoS) attack aims to make a network service unavailable to its intended users by overwhelming it with traffic or exploiting vulnerabilities.

28. What is the primary function of an Internet Gateway in a cloud environment?

A) Encrypting data transmissions
B) Providing a connection to the Internet
C) Managing domain names
D) Assigning IP addresses

Answer: B) Providing a connection to the Internet
Explanation: An Internet Gateway provides a connection between a cloud network and the Internet, enabling external access to cloud-based resources.

29. Which of the following best describes a Virtual Private Cloud (VPC)?

A) A private network within a public cloud
B) A physical data center
C) A local area network
D) A dedicated physical server

Answer: A) A private network within a public cloud

Explanation: A Virtual Private Cloud (VPC) is a private network within a public cloud, providing isolated resources and enhanced security for cloud-based applications.

30. What is the primary benefit of using DNS over TLS (DoT)?

A) Assigning IP addresses
B) Encrypting DNS traffic to protect against eavesdropping
C) Managing domain names
D) Reducing latency

Answer: B) Encrypting DNS traffic to protect against eavesdropping

Explanation: DNS over TLS (DoT) encrypts DNS traffic, protecting against eavesdropping and ensuring the privacy and integrity of DNS queries and responses.

31. Which of the following is a primary benefit of deploying a WLAN?

A) Increased wired connections
B) Mobility and flexibility for users
C) Simplified cabling
D) Enhanced security

Answer: B) Mobility and flexibility for users

Explanation: A WLAN (Wireless Local Area Network) provides mobility and flexibility for users, allowing them to connect to the network without the constraints of wired connections.

32. Why is maintaining an asset inventory important in network management?

A) To increase network speed
B) To track and manage hardware, software, licensing, and warranty support
C) To simplify configuration
D) To reduce hardware costs

Answer: B) To track and manage hardware, software, licensing, and warranty support

Explanation: Maintaining an asset inventory is important for tracking and managing hardware, software, licensing, and warranty support, ensuring efficient resource management and compliance.

33. Which of the following best describes the purpose of a MAC address in a network?

A) Logical addressing
B) Physical addressing
C) Routing decisions
D) Domain name resolution

Answer: B) Physical addressing

Explanation: A MAC (Media Access Control) address provides a unique physical identifier for a network interface, used for data link layer communication within a network.

34. What is the primary purpose of Network Time Security (NTS)?

A) Encrypting network traffic
B) Managing domain names
C) Assigning IP addresses
D) Securing time synchronization protocols

Answer: D) Securing time synchronization protocols

Explanation: Network Time Security (NTS) secures time synchronization protocols, protecting against attacks and ensuring the integrity of time information.

35. Why is performance monitoring important in a network?

A) To simplify configuration
B) To ensure optimal network performance and identify issues
C) To reduce hardware costs
D) To manage domain names

Answer: B) To ensure optimal network performance and identify issues

Explanation: Performance monitoring ensures optimal network performance by tracking metrics such as bandwidth usage, latency, and packet loss, helping to identify and address issues proactively.

36. What is the primary goal of availability monitoring in a network?

A) To track IP address allocations
B) To ensure network services are accessible and operational
C) To manage domain names
D) To encrypt data transmissions

Answer: B) To ensure network services are accessible and operational

Explanation: Availability monitoring aims to ensure that network services are accessible and operational, minimizing downtime and ensuring continuous service availability.

37. In a bus topology, what happens if the main cable fails?

A) Only the connected devices are affected
B) The entire network fails
C) Traffic is rerouted
D) Network speed decreases

Answer: B) The entire network fails

Explanation: In a bus topology, all devices are connected to a single central cable. If this cable fails, the entire network is disrupted.

38. Which of the following best describes the purpose of Quality of Service (QoS)?

A) Encrypting data
B) Prioritizing network traffic
C) Routing packets based on destination
D) Managing IP addresses

Answer: B) Prioritizing network traffic

Explanation: QoS (Quality of Service) prioritizes network traffic to ensure that critical applications receive the necessary bandwidth and performance levels.

39. Which of the following best describes a screened subnet zone (DMZ)?

A) A network segment isolated from both the internal network and the Internet
B) A secure internal network
C) A public-facing network
D) A private network

Answer: A) A network segment isolated from both the internal network and the Internet

Explanation: A screened subnet zone, or DMZ (Demilitarized Zone), is a network segment isolated from both the internal network and the Internet, providing an additional layer of security for public-facing services.

40. You need to allow multiple VLANs to communicate across a single link. Which feature would you use?

A) Link aggregation
B) Port mirroring
C) Spanning Tree Protocol
D) Trunking

Answer: D) Trunking

Explanation: Ethernet trunking allows multiple VLANs to communicate across a single link by tagging frames with VLAN identifiers, allowing inter-VLAN communication.

41. Which of the following best describes a client-server network?

A) All devices have equal roles
B) Centralized server provides resources to clients
C) Devices connect directly to each other
D) Communication is peer-to-peer

Answer: B) Centralized server provides resources to clients

Explanation: In a client-server network, a centralized server provides resources and services to client devices, managing and controlling access.

42. What does the term 'dual stack' refer to in networking?

A) Using two separate networks
B) Running both IPv4 and IPv6 on the same network
C) Having redundant network devices
D) Utilizing dual processors for networking tasks

Answer: B) Running both IPv4 and IPv6 on the same network

Explanation: Dual stack refers to running both IPv4 and IPv6 protocols simultaneously on the same network, allowing for smooth transition and compatibility.

43. What is the purpose of a change control process in network management?

A) Increasing network speed
B) Documenting and approving changes to the network
C) Simplifying network configuration
D) Reducing hardware costs

Answer: B) Documenting and approving changes to the network

Explanation: A change control process documents and approves changes to the network, ensuring that modifications are planned, tested, and implemented in a controlled manner.

44. What is a common method for securing data at rest?

A) Encrypting the data
B) Using VLANs
C) Assigning IP addresses
D) Implementing DHCP

Answer: A) Encrypting the data

Explanation: Encrypting data at rest ensures that stored data is protected from unauthorized access, providing an additional layer of security.

45. What is the primary purpose of URL filtering in network security?

A) Encrypting data
B) Controlling access to websites based on their URLs
C) Assigning IP addresses
D) Managing domain names

Answer: B) Controlling access to websites based on their URLs

Explanation: URL filtering controls access to websites based on their URLs, allowing administrators to block or allow access to specific web content for security and productivity reasons.

46. Which of the following best describes the purpose of configuration monitoring?

A) Encrypting data
B) Tracking and validating device configurations
C) Assigning IP addresses
D) Managing domain names

Answer: B) Tracking and validating device configurations

Explanation: Configuration monitoring tracks and validates device configurations, ensuring that settings remain consistent and compliant with defined policies.

47. Why is disaster recovery testing important?

A) To increase network speed
B) To ensure the effectiveness of the disaster recovery plan
C) To simplify configuration
D) To reduce hardware costs

Answer: B) To ensure the effectiveness of the disaster recovery plan

Explanation: Disaster recovery testing is important to ensure that the disaster recovery plan is effective and can be executed successfully in case of an actual disaster.

48. Which tool would you use to insert wires into a patch panel?

A) Crimper
B) Punch-down tool
C) Wire stripper
D) Multimeter

Answer: B) Punch-down tool

Explanation: A punch-down tool is used to insert wires into a patch panel, ensuring a secure and reliable connection.

49. Which tool is commonly used for managing IP address allocations and usage in a network?

A) DHCP
B) IPAM
C) DNS
D) SNMP

Answer: B) IPAM

Explanation: IPAM (IP Address Management) tools are used for managing IP address allocations, tracking usage, and ensuring efficient IP address space management.

50. You need to resolve domain names to IP addresses for a network application. Which service would you configure?

A) DHCP
B) DNS
C) FTP
D) SNMP

Answer: B) DNS

Explanation: DNS (Domain Name System) translates domain names into IP addresses, allowing users to access websites using human-readable names.

51. What is the principle of least privilege in network security?

A) Allowing all users full access
B) Using default passwords
C) Avoiding user authentication
D) Granting users the minimum access necessary for their roles

Answer: D) Granting users the minimum access necessary for their roles

Explanation: The principle of least privilege grants users the minimum access necessary for their roles, reducing the risk of unauthorized access and potential security breaches.

52. What is the primary goal of a DNS spoofing attack?

A) To redirect traffic to malicious sites by altering DNS responses
B) To encrypt DNS traffic
C) To assign IP addresses
D) To manage domain names

Answer: A) To redirect traffic to malicious sites by altering DNS responses

Explanation: A DNS spoofing attack aims to redirect traffic to malicious sites by altering DNS responses, tricking users into visiting fake or harmful websites.

53. Which switch port security feature can help prevent unauthorized devices from connecting to the network?

A) Spanning Tree Protocol
B) Link aggregation
C) Port security
D) VLAN trunking

Answer: C) Port security

Explanation: Port security features, such as MAC address filtering and limiting the number of allowed MAC addresses, can help prevent unauthorized devices from connecting to the network.

54. Which of the following is a characteristic of self-signed certificates?

A) Issued by a trusted certificate authority
B) Used only for internal purposes
C) Validated by third parties
D) Automatically trusted by all devices

Answer: B) Used only for internal purposes

Explanation: Self-signed certificates are typically used for internal purposes and are not issued by a trusted certificate authority, meaning they must be manually trusted by devices.

55. What is the primary purpose of identity and access management (IAM)?

A) Encrypting data
B) Managing and controlling user access to resources
C) Assigning IP addresses
D) Monitoring network performance

Answer: B) Managing and controlling user access to resources

Explanation: Identity and access management (IAM) manages and controls user access to resources, ensuring that only authorized users can access specific resources.

56. Which of the following is a primary use case for SIP trunks?

A) Connecting devices in a LAN
B) Establishing VoIP communication with the public switched telephone network
C) Providing wireless connectivity
D) Encrypting email communications

Answer: B) Establishing VoIP communication with the public switched telephone network

Explanation: SIP trunks are used to connect VoIP systems to the public switched telephone network (PSTN), allowing VoIP calls to reach traditional phone lines.

57. You want to increase the bandwidth and provide redundancy between two switches. Which feature would you use?

A) VLAN tagging
B) Link aggregation
C) Port mirroring
D) Trunking

Answer: B) Link aggregation

Explanation: Link aggregation combines multiple physical links into a single logical link, increasing bandwidth and providing redundancy between network devices.

58. Which of the following best describes a static route?

A) A route automatically added by routing protocols
B) A route manually configured by an administrator
C) A route with the highest priority in the routing table
D) A route used for default traffic

Answer: B) A route manually configured by an administrator

Explanation: A static route is manually configured by an administrator, providing a fixed path for traffic to follow.

59. Which of the following best describes an IPv6 unique local address?

A) Routable on the Internet
B) Used for private, internal communication
C) Always starts with fe80::
D) Used for multicast communication

Answer: B) Used for private, internal communication

Explanation: IPv6 unique local addresses are used for private, internal communication within an organization and are not routable on the Internet. These addresses are similar to IPv4 RFC 1918 addresses.

60. Which of the following is a key characteristic of the Industrial Internet of Things (IIoT)?

A) Consumer-focused applications
B) Integration of industrial equipment with network connectivity
C) Limited scalability
D) Manual configuration

Answer: B) Integration of industrial equipment with network connectivity

Explanation: The Industrial Internet of Things (IIoT) integrates industrial equipment with network connectivity, enabling remote monitoring, control, and data analysis in industrial environments.

61. Which device is specifically designed to handle a large number of VPN connections?

A) Router
B) Switch
C) VPN Concentrator
D) Firewall

Answer: C) VPN Concentrator

Explanation: A VPN concentrator is designed to manage multiple VPN connections efficiently, providing encryption and secure communication for remote users.

62. Which of the following is a common security concern associated with IoT devices?

A) High bandwidth usage
B) Limited processing power
C) Weak default passwords
D) Complex configuration

Answer: C) Weak default passwords

Explanation: IoT devices often come with weak default passwords, making them vulnerable to unauthorized access and exploitation if not properly secured.

63. What is a key consideration in power management for network equipment?

A) Using non-standard power supplies
B) Disabling power backups
C) Avoiding power monitoring
D) Implementing redundant power sources

Answer: D) Implementing redundant power sources

Explanation: Implementing redundant power sources ensures that network equipment remains operational in case of a primary power source failure, enhancing reliability and uptime.

64. You are a network engineer tasked with connecting several branch offices within the same city. Which technology might you use?

A) VPN
B) DSL
C) Metro Ethernet
D) Satellite

Answer: C) Metro Ethernet

Explanation: Metro Ethernet provides high-speed network connections between multiple locations within a metropolitan area, ideal for connecting branch offices in the same city. Metro Ethernet is an example of a Metropolitan Area Network (MAN) technology.

65. Which of the following protocols automatically assigns IP addresses to devices on a network?

A) DNS
B) HTTP
C) DHCP
D) SMTP

Answer: C) DHCP

Explanation: DHCP (Dynamic Host Configuration Protocol) automatically assigns IP addresses to devices on a network, simplifying the management of IP addresses.

66. Which of the following is an example of a Personal Area Network (PAN)?

A) Office LAN
B) Home Wi-Fi network
C) Bluetooth connection between a phone and headset
D) Corporate intranet

Answer: C) Bluetooth connection between a phone and headset

Explanation: A PAN connects personal devices within a close range, such as a Bluetooth connection between a phone and a headset, typically within a few meters of one another.

67. How does an Ethernet switch determine where to forward a frame?

A) By IP address
B) By MAC address
C) By protocol type
D) By port number

Answer: B) By MAC address

Explanation: An Ethernet switch forwards frames based on destination MAC addresses, using a MAC address table to determine the appropriate egress port for each frame.

68. Which command would you use on a Cisco switch to display the MAC address table?

A) show arp
B) show vlan
C) show mac address-table
D) show power

Answer: C) show mac address-table

Explanation: The `show mac address-table` command displays the MAC address table on a Cisco switch, providing information about MAC addresses and their associated ports.

69. What is the primary function of Access Control Lists (ACLs) in a network?

A) Encrypting data
B) Controlling network traffic
C) Assigning IP addresses
D) Managing domain names

Answer: B) Controlling network traffic

Explanation: Access Control Lists (ACLs) are ordered lists of Access Control Entries (ACEs). ACLs can be used to control network traffic by defining rules that permit or deny traffic based on information such as IP addresses, protocols, and ports.

70. Which of the following best describes multi-tenancy in cloud computing?

A) Each user has a dedicated physical server
B) Multiple users share the same physical resources
C) Users have isolated networks
D) Cloud services are available only to a single organization

Answer: B) Multiple users share the same physical resources

Explanation: Multi-tenancy in cloud computing means that multiple users share the same physical resources, with logical isolation to ensure privacy and security.

71. Which of the following best describes wireless band steering?

A) Directing traffic to the least congested channel
B) Using only the 2.4 GHz band
C) Avoiding interference from other devices
D) Automatically guiding devices to the most appropriate frequency band

Answer: D) Automatically guiding devices to the most appropriate frequency band

Explanation: Wireless band steering automatically guides devices to the most appropriate frequency band, optimizing performance and reducing congestion.

72. Which of the following is a key benefit of using playbooks in IaC automation?

A) Manual configuration
B) Automated and repeatable tasks
C) Increased configuration drift
D) Reduced compliance

Answer: B) Automated and repeatable tasks

Explanation: Playbooks in IaC automation allow for automated and repeatable tasks, ensuring consistency and reducing the need for manual configuration.

73. Which of the following is an important aspect of disaster recovery planning?

A) Increasing network bandwidth
B) Regularly testing and updating the disaster recovery plan
C) Simplifying network configuration
D) Reducing hardware costs

Answer: B) Regularly testing and updating the disaster recovery plan

Explanation: Regularly testing and updating the disaster recovery plan ensures that it remains effective and up-to-date, providing a reliable response in case of a disaster.

74. Which of the following best describes a Metropolitan Area Network (MAN)?

A) Limited to a single home
B) Covers a city or large campus
C) Connects international offices
D) Uses fiber optic technology exclusively

Answer: B) Covers a city or large campus

Explanation: A MAN covers a city or large campus, providing network connectivity over a metropolitan area, typically larger than a LAN but smaller than a WAN.

75. Which issue might occur if a PoE device exceeds the switch's power budget?

A) Increased bandwidth
B) Device overheating
C) Decreased signal strength
D) Loss of power to PoE devices

Answer: D) Loss of power to PoE devices

Explanation: If a PoE device exceeds the switch's power budget, it can result in the loss of power to PoE devices, causing them to shut down or malfunction.

76. Which of the following is a primary use case for VXLAN?

A) Encrypting network traffic
B) Providing Layer 2 connectivity over Layer 3 networks
C) Assigning IP addresses
D) Managing domain names

Answer: B) Providing Layer 2 connectivity over Layer 3 networks

Explanation: VXLAN (Virtual Extensible LAN) provides Layer 2 connectivity over Layer 3 networks, enabling scalable and flexible data center interconnects and virtualized network segments.

77. Which of the following best describes DNS over HTTPS (DoH)?

A) Encrypting DNS traffic to enhance privacy and security
B) Assigning IP addresses
C) Managing domain names
D) Providing a backup for DNS servers

Answer: A) Encrypting DNS traffic to enhance privacy and security

Explanation: DNS over HTTPS (DoH) encrypts DNS traffic using HTTPS, enhancing privacy and security by preventing DNS queries and responses from being easily intercepted.

78. What is a primary function of a VPN?

A) Increase Internet speed
B) Encrypt data transmissions
C) Convert IP addresses
D) Cache web content

Answer: B) Encrypt data transmissions

Explanation: A VPN (Virtual Private Network) can be used to encrypt data transmissions, providing secure communication over public networks such as the Internet.

79. Which protocol is commonly used to access cloud services securely over the Internet?

A) HTTP
B) FTP
C) HTTPS
D) Telnet

Answer: C) HTTPS

Explanation: HTTPS (Hypertext Transfer Protocol Secure) is commonly used to securely access cloud services over the Internet, encrypting data in transit.

80. What is the purpose of a solicited-node multicast address in IPv6?

A) Routing data to all nodes on a network
B) Assisting in neighbor discovery
C) Providing a loopback mechanism
D) Offering a unique local address

Answer: B) Assisting in neighbor discovery

Explanation: Solicited-node multicast addresses are used in IPv6 for neighbor discovery, allowing a device to verify the reachability of other devices on the same link.

81. What is a key benefit of using the 6 GHz band for wireless communication?

A) Increased interference
B) Reduced signal strength
C) Limited device compatibility
D) Greater available bandwidth

Answer: D) Greater available bandwidth

Explanation: The 6 GHz band provides greater available bandwidth, supporting higher data rates and reducing congestion in wireless networks.

82. What is the key difference between in-band and out-of-band network management?

A) In-band management uses a separate network for control traffic
B) Out-of-band management uses the same network as data traffic
C) In-band management uses the same network as data traffic
D) Out-of-band management does not provide remote access

Answer: C) In-band management uses the same network as data traffic

Explanation: In-band management uses the same network as data traffic for control and management, while out-of-band management uses a separate, dedicated network.