Network+ (N10-009) Practice Exam #1

Questions

1. What is the purpose of Router Advertisement (RA) Guard in a network?

A) Encrypting data
B) Preventing rogue router advertisements
C) Managing IP addresses
D) Configuring VLANs

2. In which part of an IP packet are IP Precedence markings found?

A) Source IP address
B) Destination IP address
C) Type of Service (ToS) field
D) Data payload

3. Which of the following methods is commonly used to secure data in transit?

A) Using strong passwords
B) Implementing encryption protocols
C) Configuring VLANs
D) Enabling DHCP snooping

4. Why is a site survey important before deploying a wireless network?

A) To increase network speed
B) To assess coverage and potential interference
C) To simplify configuration
D) To reduce hardware costs

5. What is a key characteristic of Direct Attach Copper (DAC) cables?

A) They use fiber optic technology
B) They are used for long-distance connections
C) They provide high-speed, short-distance connectivity
D) They are used for wireless connections

6. Which type of transceiver is commonly used in Ethernet networks?

A) SCSI
B) SATA
C) NVMe
D) SFP

7. Which of the following is a valid IPv4 address?

A) 192.168.1.1
B) 256.256.256.256
C) 123.456.78.90
D) 192.168.1.256

8. Which of the following is a characteristic of an MPO connector?

A) Used for single-mode fiber only
B) Connects multiple fibers in a single connector
C) Limited to low-speed applications
D) Requires proprietary hardware

9. You are integrating multiple smart devices into your network. Which term best describes this collection of devices?

A) SCADA
B) VPN
C) IoT
D) DMVPN

10. What is a common use case for a CAN?

A) Connecting personal devices at home
B) Networking an entire metropolitan area
C) Connecting buildings on a university campus
D) Providing public Internet access

11. Which of the following best describes an ARP poisoning attack?

A) Disrupting DNS resolution
B) Spoofing ARP messages to associate the attacker's MAC address with a target IP address
C) Overloading a switch's MAC address table
D) Blocking network traffic

12. Which of the following represents an IPv6 unspecified address?

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

13. Which of the following is a general networking troubleshooting issue?

A) Misconfigured devices
B) Weak passwords
C) Outdated software
D) All of the above

14. Which of the following is a primary benefit of implementing voice VLANs?

A) Enhanced data encryption
B) Prioritization of voice traffic
C) Increased bandwidth for data traffic
D) Simplified network management

15. What is a potential consequence of a network loop in an Ethernet network?

A) Increased network speed
B) Improved security
C) Reduced latency
D) Broadcast storm

16. You need to provide directional coverage for a long corridor. Which type of WLAN antenna would you use?

A) Omnidirectional
B) Dipole
C) Yagi
D) Parabolic

17. Which safety procedure is important for network engineers to follow?

A) Using default passwords
B) Configuring VLANs
C) Wearing ESD (electrostatic discharge) protection
D) Disabling firewalls

18. Which of the following best describes the purpose of network forensics?

A) Encrypting network data
B) Controlling network traffic
C) Managing IP addresses
D) Investigating network security incidents

19. Why is key management important for network security?

A) To simplify configuration
B) To ensure the secure generation, storage, and distribution of cryptographic keys
C) To reduce hardware costs
D) To increase network speed

20. Which protocol is commonly used for transporting voice over IP networks?

A) ICMP
B) RTP
C) SMTP
D) SNMP

21. Which of the following is a characteristic of an IPv6 link-local address?

A) Routable on the Internet
B) Unique across the entire network
C) Used for communication within a single network segment
D) Requires a global prefix

22. What is a common symptom of network bottlenecking?

A) Increased throughput
B) Reduced signal strength
C) Enhanced security
D) Slow network performance

23. Which of the following is a primary function of a cable modem?

A) Encrypting data
B) Providing high-speed Internet access via cable television networks
C) Managing IP addresses
D) Converting fiber optic signals

24. Which of the following best describes NAT64?

A) Translating IPv6 addresses to IPv4 addresses
B) Assigning IP addresses
C) Providing DNS resolution
D) Encrypting network traffic

25. Which of the following best describes the function of a load-balancer?

A) Increases network security
B) Distributes network traffic across multiple servers
C) Converts IP addresses
D) Filters email spam

26. Which wireless security protocol introduced 192-bit AES encryption for enterprise Wi-Fi networks?

A) WEP
B) WPA
C) WPA2
D) WPA3

27. What is the purpose of a host file in domain resolution?

A) Encrypting data
B) Manually mapping domain names to IP addresses
C) Managing DNS servers
D) Assigning IP addresses

28. Which of the following IPv6 addresses is a global unicast address?

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

29. What is the primary function of a wireless range extender in a network?

A) Encrypting wireless traffic
B) Increasing the coverage area of a wireless network
C) Providing wired connections
D) Managing IP addresses

30. What is a common issue that can affect a wireless LAN (WLAN)?

A) Interference from other devices
B) Cable damage
C) Network loops
D) IP address exhaustion

31. Which of the following is a characteristic of cloud computing?

A) On-premises infrastructure
B) Static resource allocation
C) Limited scalability
D) Pay-as-you-go pricing model

32. Which of the following is an example of a social engineering attack?

A) Phishing email
B) SQL injection
C) Port scanning
D) Man-in-the-Middle

33. Which of the following is a benefit of Infrastructure as Code (IaC)?

A) Manual configuration
B) Consistent and repeatable deployments
C) Increased physical hardware requirements
D) Limited automation

34. Which feature can help secure the Spanning Tree Protocol (STP) in a network?

A) Port security
B) BPDU Guard
C) VLAN tagging
D) Link aggregation

35. Which of the following is a method used by Extensible Authentication Protocol (EAP) for network access authentication?

A) Password-based
B) Certificate-based
C) Token-based
D) All of the above

36. Which of the following best describes a threat in network security?

A) A weakness that can be exploited
B) An action that takes advantage of a vulnerability
C) A potential danger to network security
D) The likelihood of a security breach

37. Which type of IPv4 address is used for a single device on a network?

A) Multicast
B) Broadcast
C) Anycast
D) Unicast

38. Which of the following is a key feature of virtual IP addresses used with First Hop Redundancy Protocols (FHRPs)?

A) Port mapping
B) High availability
C) Fixed routing
D) Requires DNS AAAA records

39. Which of the following connectors is typically used with twisted pair copper cabling?

A) LC
B) SC
C) RJ-45
D) ST

40. Which of the following can cause network congestion?

A) High bandwidth usage
B) Low latency
C) Limited device compatibility
D) Increased encryption

41. Which of the following is a primary use case for IPv4 multicast addresses?

A) Sending data to a single device
B) Broadcasting to all devices
C) Sending data to a group of devices
D) Connecting to remote networks

42. What is the primary purpose of using version control in IaC?

A) Encrypting data
B) Managing and tracking changes to code
C) Assigning IP addresses
D) Monitoring network performance

43. You want to detect and respond to network threats in real-time. Which device is best suited for this purpose?

A) Intrusion Detection System (IDS)
B) Firewall
C) Intrusion Prevention System (IPS)
D) Router

44. What tool can be used to measure network bandwidth and throughput capacity?

A) SolarWinds
B) Wireshark
C) iperf
D) Nessus

45. Which of the following is true about a Local Area Network (LAN)?

A) It spans multiple cities
B) It connects devices within a limited area
C) It uses satellite communication
D) It relies on the public Internet

46. Which of the following best describes the purpose of port mirroring in a network?

A) Increasing data transmission speed
B) Monitoring network traffic for analysis
C) Assigning IP addresses
D) Encrypting network traffic

47. Which of the following is a best practice for rack management in a data center?

A) Installing equipment without airflow considerations
B) Using rack units to organize equipment
C) Avoiding cable management systems
D) Placing heavy equipment on top racks

48. Which measure can help enhance physical network security?

A) Using strong encryption protocols
B) Implementing firewall rules
C) Securing network equipment in locked rooms
D) Configuring VLANs

49. Which of the following best describes a vulnerability in network security?

A) A tool used by attackers
B) A weakness that can be exploited
C) A security policy
D) A type of malware

50. You are in a remote location without a traditional network infrastructure. Which technology can provide Internet access?

A) Ethernet
B) Fiber optic
C) Satellite data
D) DSL

51. Which of the following frequency bands is not commonly used for WLANs?

A) 900 MHz
B) 2.4 GHz
C) 6 GHz
D) 5 GHz

52. What is the goal of a MAC flooding attack?

A) To encrypt network traffic
B) To overwhelm a switch's MAC address table
C) To assign IP addresses
D) To manage domain names

53. Which of the following could be accomplished using a transceiver?

A) Encrypting data transmissions
B) Converting electrical signals to optical signals and vice versa
C) Managing IP addresses
D) Filtering network traffic

54. Which strategy is most effective in defending against network attacks?

A) Using default passwords
B) Implementing strong access control policies
C) Applying monthly software updates
D) Allowing open access to network resources

55. Why are standards, policies, and rules important in network management?

A) They increase network complexity
B) They reduce network performance
C) They limit network scalability
D) They ensure consistency and compliance

56. SCADA systems are commonly used in which of the following environments?

A) Personal computing
B) Industrial control
C) Office automation
D) Home networking

57. Which of the following is a benefit of using APIs for network management?

A) Automation and programmability
B) Compatibility with legacy devices
D) Increased complexity
D) Limited scalability

58. What is a key principle of Zero Trust Architecture (ZTA)?

A) Trusting internal network traffic
B) Providing open access to network resources
C) Using single-factor authentication
D) Enforcing least privilege access

59. Which of the following is a private IPv4 address?

A) 8.8.8.8
B) 172.16.0.1
C) 192.0.2.1
D) 203.0.113.1

60. What is the usable IP address range for a subnet with a network address of 192.168.1.0/27?

A) 192.168.1.1 - 192.168.1.14
B) 192.168.1.1 - 192.168.1.30
C) 192.168.1.1 - 192.168.1.62
D) 192.168.1.1 - 192.168.1.126

61. Which CLI utility is used to test the reachability of a host on a network?

A) netstat
B) traceroute
C) ping
D) ifconfig

62. How many subnets can be created with a subnet mask of 255.255.255.192 in a Class C network?

A) 2
B) 4
C) 8
D) 16

63. What is the primary use of a jump box in network management?

A) Encrypting data transmissions
B) Providing a secure entry point for remote management
C) Assigning IP addresses
D) Managing domain names

64. Which of the following describes a primary function of Network Address Translation (NAT)?

A) Assigning IP addresses
B) Encrypting data transmissions
C) Managing email traffic
D) Mapping private IP addresses to public IP addresses

65. Which of the following is a key characteristic of Precision Time Protocol (PTP)?

A) Providing high-accuracy time synchronization
B) Encrypting data transmissions
C) Managing IP addresses
D) Assigning domain names

66. Which type of attack involves intercepting and/or altering communications between two parties without their knowledge?

A) Phishing
B) Denial of Service
C) Man-in-the-Middle
D) SQL injection

67. What is the purpose of network discovery in network management?

A) Encrypting data
B) Assigning IP addresses
C) Managing domain names
D) Identifying and mapping network devices and topology

68. Which of the following is a key feature of Security Assertion Markup Language (SAML)?

A) Assigning IP addresses
B) Providing single sign-on (SSO) capabilities
C) Managing domain names
D) Encrypting network traffic

69. Which type of IPv4 address is used to send data to all devices on a network segment?

A) Unicast
B) Multicast
C) Broadcast
D) Anycast

70. Which of the following is a distance-vector routing protocol?

A) OSPF
B) EIGRP
C) BGP
D) RIP

71. What is a potential consequence of packet loss in a network?

A) Improved data accuracy
B) Increased latency
C) Enhanced security
D) Reduced throughput

72. What does it mean when a network port is in an 'error disabled' state?

A) The port is manually disabled by an administrator
B) The port is suspended due to a configuration issue or security violation
C) The port is operational but underutilized
D) The port is receiving excessive traffic

73. What is a primary benefit of virtualized servers?

A) Increased physical space requirements
B) Improved resource utilization
C) Enhanced complexity
D) Fixed resource allocation

74. What is a key feature of DMVPNs?

A) Static tunnels
B) Dynamic, multipoint connectivity
C) Manual configuration
D) Limited scalability

75. What is a primary advantage of using fiber optic cables over copper cables?

A) Lower cost
B) Greater resistance to electromagnetic interference
C) Easier installation
D) Longer transmission delays

76. You need to synchronize the clocks of all devices on your network. Which protocol could you use?

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

77. Which of the following describes the function of MPLS in a network?

A) Assigning IP addresses
B) Providing a mechanism for routing packets based on labels
C) Encrypting data
D) Managing domain names

78. Which of the following is a valid IPv6 address?

A) 2001:0db8:85a3:0000:0000:8a2e:0370:7334
B) 2001:db8:85a3::8a2e:370:7334
C) ::1
D) All of the above

79. What is the primary purpose of DNS Security Extensions (DNSSEC)?

A) Encrypting data transmissions
B) Securing DNS queries and responses
C) Assigning IP addresses
D) Managing domain names

80. Which of the following is a common issue that can affect a Local Area Network (LAN)?

A) IP address conflicts
B) High latency
C) Signal attenuation
D) All of the above

81. Which protocol provides secure remote access to network devices?

A) Telnet
B) FTP
C) SSH
D) TFTP

82. Which command would you use on a Cisco router to display the routing table?

A) show ip route
B) show interfaces
C) show running-config
D) show version

Questions and Answers

1. What is the purpose of Router Advertisement (RA) Guard in a network?

A) Encrypting data
B) Preventing rogue router advertisements
C) Managing IP addresses
D) Configuring VLANs

Answer: B) Preventing rogue router advertisements

Explanation: RA Guard prevents rogue router advertisements on a network, protecting against unauthorized devices attempting to act as routers and potentially disrupting network traffic.

2. In which part of an IP packet are IP Precedence markings found?

A) Source IP address
B) Destination IP address
C) Type of Service (ToS) field
D) Data payload

Answer: C) Type of Service (ToS) field

Explanation: IP Precedence markings are found in the Type of Service (ToS) field of an IP packet header, indicating priority levels for traffic.

3. Which of the following methods is commonly used to secure data in transit?

A) Using strong passwords
B) Implementing encryption protocols
C) Configuring VLANs
D) Enabling DHCP snooping

Answer: B) Implementing encryption protocols

Explanation: Implementing encryption protocols, such as Advanced Encryption Standard (AES), secures data in transit by encrypting the data being transmitted, preventing unauthorized access.

4. Why is a site survey important before deploying a wireless network?

A) To increase network speed
B) To assess coverage and potential interference
C) To simplify configuration
D) To reduce hardware costs

Answer: B) To assess coverage and potential interference

Explanation: A site survey assesses coverage and potential interference, ensuring optimal placement of access points and reliable wireless network performance.

5. What is a key characteristic of Direct Attach Copper (DAC) cables?

A) They use fiber optic technology
B) They are used for long-distance connections
C) They provide high-speed, short-distance connectivity
D) They are used for wireless connections

Answer: C) They provide high-speed, short-distance connectivity

Explanation: DAC (Direct Attach Copper) cables provide high-speed, short-distance connectivity, typically used for connecting servers and switches within a data center.

6. Which type of transceiver is commonly used in Ethernet networks?

A) SCSI
B) SATA
C) NVMe
D) SFP

Answer: D) SFP
Explanation: SFP (Small Form-factor Pluggable) transceivers are commonly used in Ethernet networks to provide modular interfaces for network devices, supporting various media types and speeds.

7. Which of the following is a valid IPv4 address?

A) 192.168.1.1
B) 256.256.256.256
C) 123.456.78.90
D) 192.168.1.256

Answer: A) 192.168.1.1

Explanation: A valid IPv4 address consists of four octets, each ranging from 0 to 255. 192.168.1.1 is a valid IPv4 address.

8. Which of the following is a characteristic of an MPO connector?

A) Used for single-mode fiber only
B) Connects multiple fibers in a single connector
C) Limited to low-speed applications
D) Requires proprietary hardware

Answer: B) Connects multiple fibers in a single connector

Explanation: An MPO (Multi-Fiber Push On) connector is used to connect multiple fibers in a single connector, simplifying cabling and supporting high-density, high-speed fiber optic connections.

9. You are integrating multiple smart devices into your network. Which term best describes this collection of devices?

A) SCADA
B) VPN
C) IoT
D) DMVPN

Answer: C) IoT

Explanation: IoT (Internet of Things) refers to a network of interconnected smart devices that can communicate and share data with each other.

10. What is a common use case for a CAN?

A) Connecting personal devices at home
B) Networking an entire metropolitan area
C) Connecting buildings on a university campus
D) Providing public Internet access

Answer: C) Connecting buildings on a university campus

Explanation: A Campus Area Network (CAN) connects multiple buildings within a campus, such as a university or business complex, providing centralized network services.

11. Which of the following best describes an ARP poisoning attack?

A) Disrupting DNS resolution
B) Spoofing ARP messages to associate the attacker's MAC address with a target IP address
C) Overloading a switch's MAC address table
D) Blocking network traffic

Answer: B) Spoofing ARP messages to associate the attacker's MAC address with a target IP address

Explanation: An ARP poisoning attack involves spoofing ARP messages to associate the attacker's MAC address with a target IP address, allowing the attacker to intercept or redirect traffic.

12. Which of the following represents an IPv6 unspecified address?

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

Answer: A) ::

Explanation: The IPv6 unspecified address is ::, used to indicate the absence of an IPv6 address.

13. Which of the following is a general networking troubleshooting issue?

A) Misconfigured devices
B) Weak passwords
C) Outdated software
D) All of the above

Answer: D) All of the above

Explanation: General networking troubleshooting issues can include misconfigured devices, weak passwords, and outdated software, each potentially impacting network performance and security.

14. Which of the following is a primary benefit of implementing voice VLANs?

A) Enhanced data encryption
B) Prioritization of voice traffic
C) Increased bandwidth for data traffic
D) Simplified network management

Answer: B) Prioritization of voice traffic

Explanation: Voice VLANs prioritize voice traffic over other types of traffic, ensuring high-quality voice communication by reducing latency and jitter.

15. What is a potential consequence of a network loop in an Ethernet network?

A) Increased network speed
B) Improved security
C) Reduced latency
D) Broadcast storm

Answer: D) Broadcast storm

Explanation: A network loop can cause a broadcast storm, where broadcast frames are continuously forwarded in the loop, overwhelming the network and degrading performance.

16. You need to provide directional coverage for a long corridor. Which type of WLAN antenna would you use?

A) Omnidirectional
B) Dipole
C) Yagi
D) Parabolic

Answer: C) Yagi

Explanation: A Yagi antenna provides directional coverage, making it suitable for covering long corridors or specific areas with focused signal strength. While a Parabolic antenna also provides directional coverage, it is used for longer range applications.

17. Which safety procedure is important for network engineers to follow?

A) Using default passwords
B) Configuring VLANs
C) Wearing ESD (electrostatic discharge) protection
D) Disabling firewalls

Answer: C) Wearing ESD (electrostatic discharge) protection

Explanation: Wearing ESD protection helps prevent damage to sensitive electronic components from electrostatic discharge, ensuring the safety of network engineers and equipment.

18. Which of the following best describes the purpose of network forensics?

A) Encrypting network data
B) Controlling network traffic
C) Managing IP addresses
D) Investigating network security incidents

Answer: D) Investigating network security incidents

Explanation: Network forensics involves investigating network security incidents to identify the cause, gather evidence, and determine the impact of the incident.

19. Why is key management important for network security?

A) To simplify configuration
B) To ensure the secure generation, storage, and distribution of cryptographic keys
C) To reduce hardware costs
D) To increase network speed

Answer: B) To ensure the secure generation, storage, and distribution of cryptographic keys

Explanation: Key management is crucial for network security as it ensures the secure generation, storage, and distribution of cryptographic keys, protecting sensitive data and communications.

20. Which protocol is commonly used for transporting voice over IP networks?

A) ICMP
B) RTP
C) SMTP
D) SNMP

Answer: B) RTP

Explanation: RTP (Real-time Transport Protocol) is commonly used for transporting voice and video over IP networks, providing end-to-end network transport functions.

21. Which of the following is a characteristic of an IPv6 link-local address?

A) Routable on the Internet
B) Unique across the entire network
C) Used for communication within a single network segment
D) Requires a global prefix

Answer: C) Used for communication within a single network segment

Explanation: IPv6 link-local addresses are used for communication within a single network segment and are not routable beyond that segment. These addresses are similar to APIPA addresses used in IPv4 addressing.

22. What is a common symptom of network bottlenecking?

A) Increased throughput
B) Reduced signal strength
C) Enhanced security
D) Slow network performance

Answer: D) Slow network performance

Explanation: Network bottlenecking occurs when a particular component or resource limits overall network performance, resulting in slow network speeds and delays.

23. Which of the following is a primary function of a cable modem?

A) Encrypting data
B) Providing high-speed Internet access via cable television networks
C) Managing IP addresses
D) Converting fiber optic signals

Answer: B) Providing high-speed Internet access via cable television networks

Explanation: A cable modem provides high-speed Internet access by connecting to cable television networks.

24. Which of the following best describes NAT64?

A) Translating IPv6 addresses to IPv4 addresses
B) Assigning IP addresses
C) Providing DNS resolution
D) Encrypting network traffic

Answer: A) Translating IPv6 addresses to IPv4 addresses

Explanation: NAT64 is a protocol that translates IPv6 addresses to IPv4 addresses, enabling communication between IPv6-only and IPv4-only devices.

25. Which of the following best describes the function of a load-balancer?

A) Increases network security
B) Distributes network traffic across multiple servers
C) Converts IP addresses
D) Filters email spam

Answer: B) Distributes network traffic across multiple servers

Explanation: A load-balancer distributes incoming network traffic across multiple servers (or other network devices) to ensure no single server is overwhelmed, enhancing performance and reliability.

26. Which wireless security protocol introduced 192-bit AES encryption for enterprise Wi-Fi networks?

A) WEP
B) WPA
C) WPA2
D) WPA3

Answer: D) WPA3

Explanation: WPA3 provides the highest level of security for Wi-Fi networks, offering stronger encryption and improved protection against brute force attacks compared to earlier protocols.

27. What is the purpose of a host file in domain resolution?

A) Encrypting data
B) Manually mapping domain names to IP addresses
C) Managing DNS servers
D) Assigning IP addresses

Answer: B) Manually mapping domain names to IP addresses

Explanation: A host file manually maps domain names to IP addresses, providing a local method for domain resolution without querying a DNS server.

28. Which of the following IPv6 addresses is a global unicast address?

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

Answer: C) 2001:db8::1

Explanation: The address 2001:db8::1 is a global unicast address, which is globally routable and unique across the entire Internet.

29. What is the primary function of a wireless range extender in a network?

A) Encrypting wireless traffic
B) Increasing the coverage area of a wireless network
C) Providing wired connections
D) Managing IP addresses

Answer: B) Increasing the coverage area of a wireless network

Explanation: A wireless range extender increases the coverage area of a wireless network by receiving and retransmitting wireless signals, helping eliminate dead spots.

30. What is a common issue that can affect a wireless LAN (WLAN)?

A) Interference from other devices
B) Cable damage
C) Network loops
D) IP address exhaustion

Answer: A) Interference from other devices

Explanation: Interference from other devices, such as microwaves and cordless phones, can affect a wireless LAN (WLAN), causing connectivity and performance issues.

31. Which of the following is a characteristic of cloud computing?

A) On-premises infrastructure
B) Static resource allocation
C) Limited scalability
D) Pay-as-you-go pricing model

Answer: B) Pay-as-you-go pricing model

Explanation: Cloud computing typically uses a pay-as-you-go pricing model, allowing organizations to pay for only the resources they use, and scale as needed.

32. Which of the following is an example of a social engineering attack?

A) Phishing email
B) SQL injection
C) Port scanning
D) Man-in-the-Middle

Answer: A) Phishing email

Explanation: A phishing email is an example of a social engineering attack, where attackers deceive individuals into divulging confidential information by posing as a trustworthy entity.

33. Which of the following is a benefit of Infrastructure as Code (IaC)?

A) Manual configuration
B) Consistent and repeatable deployments
C) Increased physical hardware requirements
D) Limited automation

Answer: B) Consistent and repeatable deployments

Explanation: Infrastructure as Code (IaC) provides consistent and repeatable deployments by using code to define and manage infrastructure, reducing manual errors and improving efficiency.

34. Which feature can help secure the Spanning Tree Protocol (STP) in a network?

A) Port security
B) BPDU Guard
C) VLAN tagging
D) Link aggregation

Answer: B) BPDU Guard

Explanation: BPDU Guard helps secure STP by disabling ports that receive unexpected Bridge Protocol Data Units (BPDUs), preventing potential STP attacks and misconfigurations.

35. Which of the following is a method used by Extensible Authentication Protocol (EAP) for network access authentication?

A) Password-based
B) Certificate-based
C) Token-based
D) All of the above

Answer: D) All of the above
Explanation: EAP supports various methods for network access authentication, including password-based, certificate-based, and token-based methods.

36. Which of the following best describes a threat in network security?

A) A weakness that can be exploited
B) An action that takes advantage of a vulnerability
C) A potential danger to network security
D) The likelihood of a security breach

Answer: C) A potential danger to network security

Explanation: A threat is a potential danger to network security that could exploit vulnerabilities and cause harm or unauthorized access.

37. Which type of IPv4 address is used for a single device on a network?

A) Multicast
B) Broadcast
C) Anycast
D) Unicast

Answer: D) Unicast

Explanation: A unicast IPv4 address is assigned to a single device on a network, allowing direct communication with that device.

38. Which of the following is a key feature of virtual IP addresses used with First Hop Redundancy Protocols (FHRPs)?

A) Port mapping
B) High availability
C) Fixed routing
D) Requires DNS AAAA records

Answer: B) High availability

Explanation: Virtual IP addresses used with FHRPs (First Hop Redundancy Protocols) provide high availability by allowing multiple routers to share a virtual IP address, helping provide continuous network service.

39. Which of the following connectors is typically used with twisted pair copper cabling?

A) LC
B) SC
C) RJ-45
D) ST

Answer: C) RJ-45

Explanation: The RJ45 connector is commonly used with twisted pair copper cabling for Ethernet networking.

40. Which of the following can cause network congestion?

A) High bandwidth usage
B) Low latency
C) Limited device compatibility
D) Increased encryption

Answer: A) High bandwidth usage

Explanation: High bandwidth usage can cause network congestion, leading to slower network performance and increased contention for available resources.

41. Which of the following is a primary use case for IPv4 multicast addresses?

A) Sending data to a single device
B) Broadcasting to all devices
C) Sending data to a group of devices
D) Connecting to remote networks

Answer: C) Sending data to a group of devices

Explanation: Multicast addresses are used to send data to a group of devices, allowing efficient communication with multiple recipients.

42. What is the primary purpose of using version control in IaC?

A) Encrypting data
B) Managing and tracking changes to code
C) Assigning IP addresses
D) Monitoring network performance

Answer: B) Managing and tracking changes to code

Explanation: Version control in IaC is used to manage and track changes to infrastructure code, ensuring that modifications are documented, reversible, and easily manageable.

43. You want to detect and respond to network threats in real-time. Which device is best suited for this purpose?

A) Intrusion Detection System (IDS)
B) Firewall
C) Intrusion Prevention System (IPS)
D) Router

Answer: C) Intrusion Prevention System (IPS)

Explanation: An IPS not only detects but also prevents network threats in real-time by taking actions such as blocking or dropping malicious traffic.

44. What tool can be used to measure network bandwidth and throughput capacity?

A) SolarWinds
B) Wireshark
C) iperf
D) Nessus

Answer: C) iperf

Explanation: iperf is a tool used to measure network bandwidth and throughput capacity, providing insights into the network's performance capabilities.

45. Which of the following is true about a Local Area Network (LAN)?

A) It spans multiple cities
B) It connects devices within a limited area
C) It uses satellite communication
D) It relies on the public Internet

Answer: B) It connects devices within a limited area

Explanation: A LAN connects devices within a limited geographic area, such as a home, office, or building, allowing for high-speed local communication.

46. Which of the following best describes the purpose of port mirroring in a network?

A) Increasing data transmission speed
B) Monitoring network traffic for analysis
C) Assigning IP addresses
D) Encrypting network traffic

Answer: B) Monitoring network traffic for analysis

Explanation: Port mirroring copies network traffic from one port to another for monitoring and analysis, helping administrators diagnose and troubleshoot network issues.

47. Which of the following is a best practice for rack management in a data center?

A) Installing equipment without airflow considerations
B) Using rack units to organize equipment
C) Avoiding cable management systems
D) Placing heavy equipment on top racks

Answer: B) Using rack units to organize equipment

Explanation: Using rack units to organize equipment helps maintain an orderly and efficient data center environment, facilitating easier management and maintenance.

48. Which measure can help enhance physical network security?

A) Using strong encryption protocols
B) Implementing firewall rules
C) Securing network equipment in locked rooms
D) Configuring VLANs

Answer: C) Securing network equipment in locked rooms

Explanation: Securing network equipment in locked rooms helps protect against physical tampering and unauthorized access, enhancing physical network security.

49. Which of the following best describes a vulnerability in network security?

A) A tool used by attackers
B) A weakness that can be exploited
C) A security policy
D) A type of malware

Answer: B) A weakness that can be exploited

Explanation: A vulnerability is a weakness in a network or system that can be exploited by attackers to gain unauthorized access or cause harm.

50. You are in a remote location without a traditional network infrastructure. Which technology can provide Internet access?

A) Ethernet
B) Fiber optic
C) Satellite data
D) DSL

Answer: C) Satellite data

Explanation: Satellite data technology provides Internet access in remote locations where traditional network infrastructure, such as cable modem access, is unavailable.

51. Which of the following frequency bands is not commonly used for WLANs?

A) 900 MHz
B) 2.4 GHz
C) 6 GHz
D) 5 GHz

Answer: A) 900 MHz

Explanation: Most Wi-Fi standards support 2.4 GHz and/or 5 GHz frequency bands, with support for the 6 GHz band being added in Wi-Fi 6e.

52. What is the goal of a MAC flooding attack?

A) To encrypt network traffic
B) To overwhelm a switch's MAC address table
C) To assign IP addresses
D) To manage domain names

Answer: B) To overwhelm a switch's MAC address table

Explanation: A MAC flooding attack aims to overwhelm a switch's MAC address table, causing the switch to flood traffic to all ports and potentially allowing attackers to intercept data.

53. Which of the following could be accomplished using a transceiver?

A) Encrypting data transmissions
B) Converting electrical signals to optical signals and vice versa
C) Managing IP addresses
D) Filtering network traffic

Answer: B) Converting electrical signals to optical signals and vice versa

Explanation: Some transceivers can convert electrical signals to optical signals (and vice versa), enabling communication between devices using different media types.

54. Which strategy is most effective in defending against network attacks?

A) Using default passwords
B) Implementing strong access control policies
C) Applying monthly software updates
D) Allowing open access to network resources

Answer: B) Implementing strong access control policies

Explanation: Implementing strong access control policies is an effective strategy for defending against network attacks by restricting unauthorized access to network resources. Also, while software updates should be regularly applied, a weekly schedule is considered more secure than a monthly schedule.

55. Why are standards, policies, and rules important in network management?

A) They increase network complexity
B) They reduce network performance
C) They limit network scalability
D) They ensure consistency and compliance

Answer: D) They ensure consistency and compliance

Explanation: Standards, policies, and rules ensure consistency and compliance in network management, helping maintain a reliable and secure network environment.

56. SCADA systems are commonly used in which of the following environments?

A) Personal computing
B) Industrial control
C) Office automation
D) Home networking

Answer: B) Industrial control

Explanation: SCADA (Supervisory Control and Data Acquisition) systems are used in industrial control environments to monitor and control industrial processes remotely.

57. Which of the following is a benefit of using APIs for network management?

A) Automation and programmability
B) Compatibility with legacy devices
D) Increased complexity
D) Limited scalability

Answer: A) Automation and programmability

Explanation: Using APIs for network management enables automation and programmability, allowing for more efficient and flexible network operations.

58. What is a key principle of Zero Trust Architecture (ZTA)?

A) Trusting internal network traffic
B) Providing open access to network resources
C) Using single-factor authentication
D) Enforcing least privilege access

Answer: D) Enforcing least privilege access

Explanation: A key principle of Zero Trust Architecture (ZTA) is enforcing least privilege access, ensuring that users and devices have only the minimum permissions needed to perform their tasks.

59. Which of the following is a private IPv4 address?

A) 8.8.8.8
B) 172.16.0.1
C) 192.0.2.1
D) 203.0.113.1

Answer: B) 172.16.0.1

Explanation: Private IPv4 addresses are reserved for internal use within a network. 172.16.0.1 is a private IPv4 address, as defined in RFC 1918.

60. What is the usable IP address range for a subnet with a network address of 192.168.1.0/27?

A) 192.168.1.1 - 192.168.1.14
B) 192.168.1.1 - 192.168.1.30
C) 192.168.1.1 - 192.168.1.62
D) 192.168.1.1 - 192.168.1.126

Answer: B) 192.168.1.1 - 192.168.1.30

Explanation: A subnet with a /27 mask provides 32 IP addresses, with 30 usable addresses ranging from 192.168.1.1 to 192.168.1.30.

61. Which CLI utility is used to test the reachability of a host on a network?

A) netstat
B) traceroute
C) ping
D) ifconfig

Answer: C) ping

Explanation: The `ping` utility tests the reachability of a host on a network by sending ICMP Echo Requests and measuring the response time.

62. How many subnets can be created with a subnet mask of 255.255.255.192 in a Class C network?

A) 2
B) 4
C) 8
D) 16

Answer: B) 4

Explanation: A subnet mask of 255.255.255.192 (or /26) provides 4 subnets in a Class C network, with each subnet having 64 IP addresses. The number of subnets is calculated by raising 2 to the power of the number of "borrowed bits." Since a Class C network has a default subnet mask of /24, and in this instance a subnet mask of /26 is being used, there are 2 borrowed bits (i.e., 26 – 24 = 2). Therefore, the number of created subnets = 2^2 = 4.

63. What is the primary use of a jump box in network management?

A) Encrypting data transmissions
B) Providing a secure entry point for remote management
C) Assigning IP addresses
D) Managing domain names

Answer: B) Providing a secure entry point for remote management

Explanation: A jump box provides a secure entry point for remote management of network devices, acting as a gateway to access and manage network resources.

64. Which of the following describes a primary function of Network Address Translation (NAT)?

A) Assigning IP addresses
B) Encrypting data transmissions
C) Managing email traffic
D) Mapping private IP addresses to public IP addresses

Answer: D) Mapping private IP addresses to public IP addresses

Explanation: NAT (Network Address Translation) can be used to map private IP addresses to public IP addresses. A variation of NAT, called Port Address Translation (PAT), allows multiple devices on a local network to share a single public IP.

65. Which of the following is a key characteristic of Precision Time Protocol (PTP)?

A) Providing high-accuracy time synchronization
B) Encrypting data transmissions
C) Managing IP addresses
D) Assigning domain names

Answer: A) Providing high-accuracy time synchronization

Explanation: PTP (Precision Time Protocol) provides high-accuracy time synchronization for networked devices, ensuring precise timekeeping and coordination.

66. Which type of attack involves intercepting and/or altering communications between two parties without their knowledge?

A) Phishing
B) Denial of Service
C) Man-in-the-Middle
D) SQL injection

Answer: C) Man-in-the-Middle
Explanation: A Man-in-the-Middle (MitM) attack involves intercepting and potentially altering communications between two parties without their knowledge.

67. What is the purpose of network discovery in network management?

A) Encrypting data
B) Assigning IP addresses
C) Managing domain names
D) Identifying and mapping network devices and topology

Answer: D) Identifying and mapping network devices and topology

Explanation: Network discovery identifies and maps network devices and topology, providing an up-to-date view of the network for better management and troubleshooting.

68. Which of the following is a key feature of Security Assertion Markup Language (SAML)?

A) Assigning IP addresses
B) Providing single sign-on (SSO) capabilities
C) Managing domain names
D) Encrypting network traffic

Answer: B) Providing single sign-on (SSO) capabilities

Explanation: SAML (Security Assertion Markup Language) provides single sign-on (SSO) capabilities, allowing users to authenticate once and access multiple services without re-entering credentials.

69. Which type of IPv4 address is used to send data to all devices on a network segment?

A) Unicast
B) Multicast
C) Broadcast
D) Anycast

Answer: C) Broadcast

Explanation: A broadcast IPv4 address is used to send data to all devices on a network segment, typically for announcements or segment-wide messages.

70. Which of the following is a distance-vector routing protocol?

A) OSPF
B) EIGRP
C) BGP
D) RIP

Answer: D) RIP

Explanation: RIP (Routing Information Protocol) is a distance-vector routing protocol that uses hop count as its metric for path selection.

71. What is a potential consequence of packet loss in a network?

A) Improved data accuracy
B) Increased latency
C) Enhanced security
D) Reduced throughput

Answer: D) Reduced throughput

Explanation: Packet loss can result in reduced throughput, as lost packets need to be retransmitted, decreasing overall data transfer rates and network performance.

72. What does it mean when a network port is in an 'error disabled' state?

A) The port is manually disabled by an administrator
B) The port is suspended due to a configuration issue or security violation
C) The port is operational but underutilized
D) The port is receiving excessive traffic

Answer: B) The port is suspended due to a configuration issue or security violation

Explanation: A network port in an 'error disabled' state is suspended due to a configuration issue or security violation, preventing it from forwarding traffic until the issue is resolved. For example, if the Port Security feature only permitted a maximum of 2 MAC addresses to be learnable off of a switch port, the port might go into an error disabled state if a 3rd MAC address were seen (and if the port's violation mode was set to "shutdown").

73. What is a primary benefit of virtualized servers?

A) Increased physical space requirements
B) Improved resource utilization
C) Enhanced complexity
D) Fixed resource allocation

Answer: B) Improved resource utilization

Explanation: Virtualized servers improve resource utilization by allowing multiple virtual machines to run on a single physical server, optimizing hardware usage and reducing costs.

74. What is a key feature of DMVPNs?

A) Static tunnels
B) Dynamic, multipoint connectivity
C) Manual configuration
D) Limited scalability

Answer: B) Dynamic, multipoint connectivity

Explanation: DMVPN (Dynamic Multipoint VPN) allows for dynamic, multipoint connectivity between remote sites, reducing the need for static tunnels and manual configuration.

75. What is a primary advantage of using fiber optic cables over copper cables?

A) Lower cost
B) Greater resistance to electromagnetic interference
C) Easier installation
D) Longer transmission delays

Answer: B) Greater resistance to electromagnetic interference

Explanation: Fiber optic cables are less susceptible to electromagnetic interference compared to copper cables, allowing for cleaner and more reliable data transmission over long distances.

76. You need to synchronize the clocks of all devices on your network. Which protocol could you use?

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

Answer: C) NTP
Explanation: NTP (Network Time Protocol) is used to synchronize the clocks of networked devices to a reference time source, ensuring accurate timekeeping.

77. Which of the following describes the function of MPLS in a network?

A) Assigning IP addresses
B) Providing a mechanism for routing packets based on labels
C) Encrypting data
D) Managing domain names

Answer: B) Providing a mechanism for routing packets based on labels

Explanation: MPLS (Multiprotocol Label Switching) routes packets based on labels instead of IP addresses, improving speed and efficiency in a network.

78. Which of the following is a valid IPv6 address?

A) 2001:0db8:85a3:0000:0000:8a2e:0370:7334
B) 2001:db8:85a3::8a2e:370:7334
C) ::1
D) All of the above

Answer: D) All of the above

Explanation: All listed options are valid IPv6 addresses, with different levels of abbreviation and special use cases (e.g., the ::1 loopback address).

79. What is the primary purpose of DNS Security Extensions (DNSSEC)?

A) Encrypting data transmissions
B) Securing DNS queries and responses
C) Assigning IP addresses
D) Managing domain names

Answer: B) Securing DNS queries and responses

Explanation: DNS Security Extensions (DNSSEC) secure DNS queries and responses by adding cryptographic signatures, ensuring the integrity and authenticity of DNS data.

80. Which of the following is a common issue that can affect a Local Area Network (LAN)?

A) IP address conflicts
B) High latency
C) Signal attenuation
D) All of the above

Answer: D) All of the above

Explanation: Common LAN troubleshooting issues include IP address conflicts, high latency, and signal attenuation, each impacting network performance and connectivity.

81. Which protocol provides secure remote access to network devices?

A) Telnet
B) FTP
C) SSH
D) TFTP

Answer: C) SSH

Explanation: SSH (Secure Shell) provides secure remote access to network devices, encrypting communication and protecting against unauthorized access.

82. Which command would you use on a Cisco router to display the routing table?

A) show ip route
B) show interfaces
C) show running-config
D) show version

Answer: A) show ip route

Explanation: The `show ip route` command displays the routing table on a Cisco router, providing information about the available routes, including information such as the routing information source, metric, cost, and next-hop IP address.