6.4.8 Lesson Review

Date: 11/30/2025, 9:22:24 AM

Time Spent: 30:06

Score: 87%

Passing Score: 80%

Question 1

Correct

What is the primary purpose of a Virtual LAN (VLAN)?

- To physically separate devices on a network
- To logically segment a network into smaller, isolated broadcast domains ✓ Correct
- To assign static IP addresses to devices on a network
- To replace the need for a Domain Name System (DNS)

Explanation

VLANs are designed to logically divide a network into separate broadcast domains, even if the devices are connected to the same physical switch. This helps improve network performance and security by isolating traffic.

VLANs do not involve physical separation of devices. Instead, VLANs achieve logical separation, allowing devices to communicate as if they are on separate physical networks without requiring additional hardware.

VLANs are not responsible for assigning IP addresses. Assigning static or dynamic IP addresses is typically managed by DHCP or manual configuration, not VLANs.

VLANs and DNS serve entirely different purposes. DNS resolves hostnames to IP addresses, while VLANs are used for network segmentation and traffic isolation.

Related Content

6.4.6 Virtual LANs

resources\questions\q_virtual_lans_01.question.xml

Question 2 ✓ Correct

A company has acquired another business and wants to redirect traffic from the acquired company's website to its own without maintaining two separate websites.

Which DNS record type should they use to achieve this?

- (●) CNAME Record ✓ Correct
- ( ) AAAA Record
- ( ) MX Record
- ( ) A Record

Explanation

A CNAME Record (Canonical Name Record) is used to alias one domain name to another. In this scenario, the company can create a CNAME record to redirect traffic from the acquired company's domain (e.g., www.companyB.com) to its own domain (e.g., www.companyA.com). This simplifies management and ensures users are directed to the correct website.

An A Record resolves a host name to an IPv4 address. While it is essential for mapping domain names to IP addresses, it does not provide the functionality to alias one domain name to another.

An AAAA Record resolves a host name to an IPv6 address. Like the A Record, it does not allow for aliasing one domain name to another, which is the requirement in this scenario.

An MX Record (Mail Exchange Record) is used to specify the mail server responsible for receiving email for a domain. It is unrelated to redirecting or aliasing domain names for web traffic.

Related Content

6.4.4 DNS Record Types
resources\questions\q_dns_record_types_02.question.xml

Question 3

Correct

A company has a single physical switch connecting all its devices, including accounting, HR, and IT departments. The IT manager notices that broadcast traffic from one department is affecting the performance of other departments.

To address this issue, the IT manager decides to implement VLANs.

Which configuration would BEST solve the problem?

- Enable a single VLAN for all devices to centralize traffic management.
- Configure the switch to assign IP addresses dynamically to reduce broadcast traffic.
- Create separate VLANs for each department and assign devices to their respective VLANs. ✓ Correct
- Use VLANs to physically separate the devices by connecting each department to a different switch.

Explanation

VLANs allow logical segmentation of the network. By creating separate VLANs for accounting, HR, and IT, broadcast traffic is confined to each VLAN, preventing it from affecting other departments and improving overall network performance.

Assigning IP addresses dynamically (via DHCP) does not reduce broadcast traffic. VLANs are specifically designed to isolate broadcast domains, which is the issue described in the scenario.

VLANs do not require physical separation of devices. VLANs achieve logical separation on the same physical switch, making this approach unnecessary and inefficient.

Using a single VLAN for all devices would not solve the problem. A single VLAN would still allow broadcast traffic to affect all devices, defeating the purpose of isolating traffic between departments.

Related Content

6.4.6 Virtual LANs

resources\questions\q_virtual_lans_03.question.xml

Question 4 ✓ Correct

A user reports that they cannot access a specific website (e.g., www.example.com), but other websites are working fine.

You perform a DNS query for the domain and receive a "Non-Existent Domain" (NXDOMAIN) response.

What is the MOST likely cause of the issue?

- The user's device has an incorrect subnet mask configured in its TCP/IP settings.
- The user's local DNS cache is corrupted and needs to be cleared.
- The domain name (e.g., www.example.com) does not exist or is not registered in the DNS hierarchy. ✓ Correct
- The DNS server is down and not responding to any queries.

Explanation

An NXDOMAIN response from a DNS query indicates that the queried domain name does not exist in the DNS hierarchy. This could mean the domain name is not registered, expired, or incorrectly configured in the DNS system.

If the DNS server were down, you would not receive an NXDOMAIN response. Instead, you would likely encounter a timeout or no response at all. The NXDOMAIN response specifically indicates that the queried domain name does not exist.

The subnet mask is used for local network communication and routing, not DNS resolution. An incorrect subnet mask would prevent the device from communicating with the network properly but would not result in an NXDOMAIN response for a specific domain.

A corrupted local DNS cache might cause issues with resolving domain names, but it would not result in an NXDOMAIN response from the DNS server. Clearing the cache might resolve other issues, but it would not fix a problem where the domain name does not exist in the DNS hierarchy.

Related Content

6.4.2 Domain Name System

6.4.3 DNS Queries

7.1.1 File/Print Servers

resources\questions\q_domain_name_system_04.question.xml

Question 5 Correct

An organization has implemented VLANs to separate traffic for its Sales, Finance, and IT departments. However, the IT team notices that devices in the Sales VLAN cannot communicate with devices in the Finance VLAN, even though some applications require inter-department communication.

What is the MOST likely cause of this issue, and how can it be resolved?

- (●) The switch is not configured with a router or Layer 3 device to enable inter-VLAN communication. ✓ Correct
- ( ) VLANs are designed to block all inter-VLAN communication, and the network must be reconfigured to use a single VLAN.
- ( ) The VLANs are misconfigured, and all devices should be assigned to the same VLAN to allow communication.
- ( ) The devices in the Sales VLAN and Finance VLAN are using different IP address ranges, which prevents communication.

Explanation

VLANs inherently isolate traffic between different VLANs. To enable communication between VLANs, a router or Layer 3 switch must be configured to route traffic between them. Without this configuration, devices in separate VLANs cannot communicate.

VLANs do not block inter-VLAN communication permanently. Inter-VLAN communication is possible with the proper configuration of a router or Layer 3 switch. Reconfiguring the network to use a single VLAN would negate the benefits of VLANs, such as traffic isolation and improved security.

Different IP address ranges are expected in separate VLANs. The issue is not the IP address ranges but the lack of a routing mechanism to enable communication between the VLANs.

Assigning all devices to the same VLAN would eliminate the logical segmentation provided by VLANs. The problem is not a misconfiguration of VLANs but the absence of a routing solution for inter-VLAN communication.

Related Content

6.4.6 Virtual LANs

resources\questions\q_virtual_lans_04.question.xml

Question 6 ✓ Correct

A network administrator needs to configure a DNS record to ensure that users typing www.companyB.com are redirected to www.companyA.com after a recent acquisition.

Which DNS record type should the administrator use?

- ○ PTR Record
- ○ AAAA Record
- ◉ CNAME Record ✓ Correct
- ○ A Record

Explanation

A CNAME Record (Canonical Name Record) is used to alias one domain name to another. In this case, the administrator can configure a CNAME record to redirect traffic from www.companyB.com to www.companyA.com, ensuring users are seamlessly redirected to the new website.

An A Record resolves a host name to an IPv4 address. While it is essential for mapping domain names to IP addresses, it does not provide the functionality to alias one domain name to another.

An AAAA Record resolves a host name to an IPv6 address. Like the A Record, it does not allow aliasing one domain name to another.

A PTR Record (Pointer Record) is used for reverse DNS lookups, mapping an IP address to a host name. It is not used tor redirect domain names.

Related Content

6.4.4 DNS Record Types
resources\questions\q_dns_record_types_03.question.xml

Question 7 Correct

A remote employee needs to securely access their company's internal network while working from a coffee shop's public Wi-Fi.

Which solution should the employee use to ensure their data is protected during transmission?

- Set up a Virtual LAN (VLAN) on the coffee shop's Wi-Fi network.
- Configure their device to use a static IP address assigned by the company.
- Connect to the company's network using a Virtual Private Network (VPN). ✓ Correct
- Use the coffee shop's DNS server to resolve company domain names securely.

Explanation

The correct solution is to use a VPN, which creates a secure and encrypted connection between the employee's device and the company's internal network. This ensures that sensitive data transmitted over the public Wi-Fi is protected from potential eavesdropping or interception.

While a static IP address might be useful for certain network configurations, it does not provide encryption or secure communication over an untrusted network like public Wi-Fi. This does not address the need for data protection.

Using the coffee shop's DNS server does not ensure secure communication. DNS servers are used to resolve domain names into IP addresses, but they do not encrypt data or protect against interception on public networks.

A VLAN is used to segment a network into smaller, isolated sub-networks for traffic management. However, it is not a practical or feasible solution for a remote employee working on a public Wi-Fi network, nor does it provide encryption or secure communication.

Related Content

6.4.7 Virtual Private Networks

resources\questions\q_virtual_private_networks_03.question.xml

Question 8 ✓ Correct

What is the primary purpose of a DHCP server in a network?

- ○ To manually assign static IP addresses to all devices on the network
- ◉ To allocate IP addresses dynamically to devices on the network ✓ Correct
- ○ To resolve domain names into IP addresses for devices on the network
- ○ To act as a firewall and block unauthorized access to the network

Explanation

The primary purpose of a DHCP (Dynamic Host Configuration Protocol) server is to dynamically assign IP addresses, subnet masks, and other configuration settings (e.g., default gateway, DNS server) to devices on the network. This eliminates the need for manual configuration and reduces the risk of errors such as duplicate IP addresses.

DHCP is specifically designed to automate the process of assigning IP addresses dynamically. Manually assigning static IP addresses is the opposite of what DHCP is intended to do, and it is prone to errors and inefficiencies.

Resolving domain names into IP addresses is the function of a DNS (Domain Name System) server, not a DHCP server. While both DHCP and DNS are important for network functionality, they serve different purposes.

Acting as a firewall is not a function of a DHCP server. Firewalls are separate devices or software designed to monitor and control incoming and outgoing network traffic based on security rules. DHCP servers are focused on IP address allocation and configuration.

Related Content

6.4.1 DHCP Functions
resources\questions\q_dhcp_functions_01.question.xml

Question 9 Correct

Which port is used by a client to communicate with a DNS server during a DNS query?

- (●) Port 53 ✓ Correct
- ( ) Port 80
- ( ) Port 67
- ( ) Port 443

Explanation

DNS servers use port 53 to communicate with clients and resolve queries for hostnames or Fully Qualified Domain Names (FQDNs) into IP addresses.

Port 67 is used by DHCP servers to listen for client requests, not for DNS queries. While both DNS and DHCP are network services, they serve different purposes and operate on different ports.

Port 80 is used for HTTP (Hypertext Transfer Protocol), which is the standard port for web traffic, not for DNS queries. DNS operates independently of HTTP.

Port 443 is used for HTTPS (Hypertext Transfer Protocol Secure), which is the secure version of HTTP for encrypted web traffic. It is unrelated to DNS queries.

Related Content

6.4.2 Domain Name System

6.4.3 DNS Queries

7.1.1 File/Print Servers

resources\questions\q_dns_queries_01.question.xml

Question 10 ✓ Correct

An IT administrator is troubleshooting an issue where legitimate emails from their domain are being marked as spam by recipient mail servers.

Upon investigation, the administrator finds that the recipient servers cannot verify the authenticity of the sender's domain.

What is the MOST likely cause of this issue?

- (●) The domain does not have an SPF record configured. ✓ Correct
- ( ) The domain's DNS server is down.
- ( ) The domain's A record is missing.
- ( ) The domain's MX record is pointing to the wrong mail server.

Explanation

If the domain does not have an SPF record, recipient mail servers cannot verify whether the email was sent from an authorized mail server. This can lead to legitimate emails being marked as spam.

MX records are used to direct incoming emails to the correct mail server. While an incorrect MX record can cause issues with receiving emails, it does not affect the verification of outgoing emails.

If the DNS server were down, it would cause broader issues, such as the inability to resolve the domain name entirely. However, this is not specific to SPF record verification.

An A record maps a domain name to an IP address and is unrelated to the verification of outgoing emails or SPF functionality.

Related Content

6.4.5 DNS Spam Management Records
resources\questions\q_dns_spam_management_records_04.question.xml

Question 11 ✕ Incorrect

What is the primary purpose of a DNS query in a network?

- ○ To encrypt communication between a client and a server
- ○ To establish a secure connection for web traffic
- ○ To resolve a hostname or FQDN to an IP address ✓ Correct
- ◉ To assign IP addresses dynamically to devices on the network ✕ Incorrect

Explanation

The purpose of a DNS query is to resolve a hostname or Fully Qualified Domain Name (FQDN) into an IP address. This process allows users to access resources on the network or the internet using human-readable names instead of numerical IP addresses.

Assigning IP addresses dynamically is the role of the DHCP (Dynamic Host Configuration Protocol), not DNS. DNS is responsible for name resolution, not IP address allocation.

DNS does not handle encryption of communication. Encryption is typically handled by protocols like HTTPS (using SSL/TLS) or other security mechanisms. DNS is focused on resolving names to IP addresses.

Establishing secure connections for web traffic is the role of HTTPS (port 443) or other secure protocols, not DNS. DNS is not involved in securing connections but rather in resolving names to IP addresses.

Related Content

6.4.2 Domain Name System

6.4.3 DNS Queries

7.1.1 File/Print Servers

resources\questions\q_dns_queries_02.question.xml

Question 12 ✕ Incorrect

You are troubleshooting a network issue where users cannot access a website by typing its domain name (e.g., www.example.com) into their browsers, but they can access it by entering their IP address directly.

What is the MOST likely cause of the issue?

- ○ The VLAN configuration on the network switch is incorrect.
- ◉ The DHCP server is not assigning IP addresses to client devices. ✕ Incorrect
- ○ The DNS server is not resolving the domain name to its corresponding IP address. ✓ Correct
- ○ The MAC address of the client devices is not registered with the network.

Explanation

The issue described indicates a problem with name resolution. DNS is responsible for translating domain names (e.g., www.example.com) into IP addresses. If users can access the website using the IP address but not the domain name, it suggests that the DNS server is either unavailable or misconfigured.

The users are able to access the website using its IP address, which means their devices already have valid IP addresses. DHCP is not related to the issue of resolving domain names to IP addresses.

MAC addresses are used for local network communication and are not related to DNS or domain name resolution. The ability to access the website using the IP address confirms that MAC addresses are not the issue.

VLAN configurations affect network segmentation and traffic flow but are unrelated to DNS resolution. The ability to access the website using the IP address indicates that the network is functioning, and the issue lies specifically with DNS.

Related Content

- 6.4.2 Domain Name System
- 6.4.3 DNS Queries
- 7.1.1 File/Print Servers

resources\questions\q_domain_name_system_03.question.xml

Question 13 ✓ Correct

A network administrator notices that several devices on the network are unable to connect to the internet. Upon investigation, they find that the affected devices have IP addresses in the 169.254.x.x range.

The DHCP server appears to be running, and other devices on the network are functioning correctly.

What is the MOST likely cause of the issue?

- The affected devices are using static IP addresses that conflict with the DHCP scope.
- The DHCP server is configured with an incorrect subnet mask for the network.
- The DHCP scope does not have enough available IP addresses to assign to new devices. ✓ Correct
- The DNS server is misconfigured, preventing devices from resolving domain names.

Explanation

Devices receiving an IP address in the 169.254.x.x range indicate that they could not obtain an IP address from the DHCP server. If the DHCP scope has run out of available IP addresses, the server cannot assign new addresses to devices, causing them to self-assign an APIPA address. This scenario matches the symptoms described.

The issue described is related to IP address assignment, not domain name resolution. A misconfigured DNS server would cause problems with resolving domain names (e.g., accessing websites), but devices would still have valid IP addresses assigned by the DHCP server.

Devices with static IP addresses would not attempt to contact the DHCP server for an address. Additionally, a conflict with the DHCP scope would not result in the devices receiving an APIPA address (169.254.x.x).

An incorrect subnet mask on the DHCP server would typically cause connectivity issues for all devices on the network, not just a subset. The scenario specifies that other devices are functioning correctly, which rules out this possibility.

Related Content

6.4.1 DHCP Functions

resources\questions\q_dhcp_functions_04.question.xml

Question 14 Correct

How does a Virtual Private Network (VPN) ensure secure communication over an untrusted network?

- By dividing a network into smaller segments to isolate traffic
- By resolving domain names into IP addresses for secure access
- By dynamically assigning IP addresses to devices on the network
- By encrypting data transmitted between the client and the server ✓ Correct

Explanation

A VPN ensures secure communication over an untrusted network, such as the internet, by encrypting the data transmitted between the client and the server. This encryption prevents unauthorized parties from intercepting or accessing sensitive information during transmission.

Dynamically assigning IP addresses to devices on the network describes the function of a DHCP server, not a VPN. DHCP is responsible for assigning IP addresses to devices automatically, but it does not provide encryption or secure communication.

Resolving domain names into IP addresses for secure access is the function of the Domain Name System (DNS), which translates domain names into IP addresses. While DNS is essential for network communication, it does not provide the encryption or secure tunneling that a VPN offers.

Dividing a network into smaller segments to isolate traffic describes the purpose of a Virtual LAN (VLAN), which is used to segment a network for better traffic management. While VLANs improve network efficiency, they do not provide the secure communication features of a VPN.

Related Content

6.4.7 Virtual Private Networks

resources\questions\q_virtual_private_networks_02.question.xml

Question 15 Correct

Which type of DNS record is specifically used to manage email spam by specifying which mail servers are authorized to send emails on behalf of a domain?

- (●) SPF (Sender Policy Framework) Record ✓ Correct
- ( ) A (Address) Record
- ( ) CNAME (Canonical Name) Record
- ( ) AAAA (IPv6 Address) Record

Explanation

SPF records are DNS records used to specify which mail servers are authorized to send emails on behalf of a domain. They help prevent email spoofing and reduce spam by allowing receiving mail servers to verify the authenticity of the sender's domain.

An A record is used to map a domain name to an IPv4 address. It does not have any role in managing email spam or specifying authorized mail servers.

A CNAME record is used to alias one domain name to another. It is not related to email or spam management.

An AAAA record is used to map a domain name to an IPv6 address. Like the A record, it is unrelated to email spam management or sender verification.

Related Content

6.4.5 DNS Spam Management Records
resources\questions\q_dns_spam_management_records_01.question.xml