# M01B_Midterm1_Ch1-6_Fall_2024_Net_Learn

**Candidate:** Richard Habib (richard_habib1)
**Date:** 10/17/2024, 12:26:27 PM • **Time Spent:** 01:38:07

**Score: 88%**

Passing Score: 70%

Question 1. ✓ Correct

What does the Start of Authority (SOA) record identify?

- The secondary name servers in the zone
- → The primary authoritative name server for the zone
- The dynamic resource records in the zone
- The most frequently visited domain in the zone

**Explanation**

The SOA record identifies the primary authoritative name server that maintains complete resource records for the zone, including modifications.

The SOA record does not track domain visitation frequency.

The SOA record specifies the primary, not secondary, name servers.

The SOA record does not specifically identify dynamic resource records.

**References**

**6.5.3 Name Resolution Using DNS**
**6.5.4 Resource Record Types**
**6.5.6 Mail Exchange, Service, and Text Records**
**6.5.8 DNS Server Configuration**
**6.5.9 Internal vs External DNS**

q_dns_resource_soa_record_identifry_n09.question.fex

Question 2. ✓ Correct

Consider the following IPv6 address: FE80:0000:0000:0055:0000:0000:000A:AB00

Which of the following are valid shortened forms of this address? (Select two.)

- [ ] FE80::55::A:AB
- [x] FE80::55:0000:0000:A:AB00
- [ ] FE80::55::A:AB00
- [x] FE80:0000:0000:0055::000A:AB00
- [ ] FE80::0055::000A:AB

**Explanation**

Valid shortened forms of this IPv6 address are:

- FE80::55:0000:0000:A:AB00
- FE80:0000:0000:0055::000A:AB00 (FE80:0000:0000:55::A:AB00 could also be used)

Leading 0s within a quartet can be omitted. For example, 0055 can be shortened to 55. Addresses with consecutive 0s can be expressed more concisely by substituting a double colon (::) for the group of 0s. However, you can only omit one set of consecutive 0s.

**References**

**4.5.2 IPv6 Address Format**

q_ipv6_format_correct_address_03_n09.question.fex

Question 3. ✓ Correct

What actions does the use of Uninterruptible Power Supplies (UPSs) allow for during power anomalies in enterprise sites? (Select two.)

- [ ] Automatically repair damaged network cables.
- [ ] Increase the processing power of servers.
- [x] Switch to a secondary power source.
- [ ] Permanently replace the main power source.
- [x] Shut down the system gracefully.

**Explanation**

The following are actions that UPSs allow for during power anomalies:

- Switching to a secondary power source. UPSs provide temporary power during outages, allowing time to switch to a secondary power source like a generator. This ensures continuity of operations and prevents data loss.
- Shutting down the system gracefully. UPSs also allow for a graceful shutdown of systems in the event of a power failure. This helps in avoiding data corruption and loss by ensuring that all processes are properly closed before the system powers down.

UPSs are designed for temporary power provision during short-term outages, not as a permanent replacement for the main power source. They provide a bridge to more stable solutions or allow for safe shutdowns.

The purpose of UPSs is to maintain power during outages, not to increase the processing power of servers. They have no direct impact on the computational capabilities of network devices.

UPSs provide power backup; they do not have the capability to automatically repair physical damages such as those to network cables. Their function is purely related to power continuity.

**References**

**2.5.3 Power Management**

q_hard_fail_power_anomaly_actions_n09.question.fex

Question 4. ✓ Correct

When subnetting the network address 172.30.0.0/16 to support 12 subnets, what is the new subnet mask in dotted decimal format?

- 255.255.255.0
- 255.255.248.0
- → 255.255.240.0
- 255.255.0.0

**Explanation**

To support 12 subnets, you round up to the nearest power of 2, which is 16. This requires 4 bits (2^4 = 16). Adding 4 bits to the default /16 mask results in a /20 mask, which in dotted decimal format is 255.255.240.0.

255.255.255.0 represents a /24 mask, which would not provide enough subnets for the requirement.

255.255.248.0 represents a /21 mask, which would provide more subnets than needed and fewer hosts per subnet.

255.255.0.0 is the original /16 mask and does not account for any subnetting.

**References**

**4.3.4 IPv4 Address Scheme Design**

q_ipv4_design_subnet_mask_example_n09.question.fex

Question 5. ✓ Correct

Which of the following best describes the function of subnetting?

→ ◉ Logically dividing an IP network into smaller subnetworks

○ Increasing the broadcast domain size

○ Physically dividing a network into smaller segments

○ Combining multiple IP networks into a single network

**Explanation**

Subnetting allows network administrators to divide a larger IP network into smaller, more manageable segments or subnets. This logical division helps in efficient IP address allocation, reduces broadcast traffic, and can improve network security.

Subnetting is about dividing networks, not combining them.

Subnetting is a logical process, not a physical one, so it doesn't physically divide networks.

Subnetting actually reduces the size of broadcast domains by creating smaller, distinct subnets.

**References**

**5.6.1 Virtual LANs and Subnets**

q_vlans_subnetting_function_n09.question.fex

Question 6. ✓ Correct

What can cause convergence problems in a dynamic routing network?

- A stable network with no changes
- → A flapping interface
- The use of static routing protocols
- Consistent routing information across all routers

**Explanation**

A flapping interface, which frequently changes its state from up to down and back again, can cause convergence problems. This is because each state change can trigger the routers to recalculate routes, leading to instability and inconsistent routing information across the network.

A stable network with no changes would actually facilitate convergence, not cause problems.

Consistent routing information is the goal of convergence, not a cause of its problems.

Static routing protocols do not participate in convergence; they are manually configured and do not adapt to network changes.

**References**

**5.2.1 Dynamic Routing Protocols**

q_dyroute_flapping_interface_n09.question.fex

Question 7. ✓ Correct

What is typically indicated when a host can ping a server by its IP address but not by its name?

→ ◉ Incorrect DNS configuration

○ Incorrect subnet mask configuration

○ Faulty network cable

○ The server is offline.

**Explanation**

When a host can ping a server by its IP address but not by its name, it indicates an issue with DNS configuration. DNS is responsible for translating human-readable domain names into IP addresses. If DNS is not correctly configured, the host cannot resolve the name to an IP address, though direct IP connectivity remains unaffected.

The server being offline would prevent both name and IP address pinging.

An incorrect subnet mask would affect all network communications, not just name resolution.

A faulty network cable would prevent any form of communication, including pinging by IP address.

**References**

**6.5.1 Host Names and Domain Names**
**6.5.2 DNS Hierarchy**
**6.5.3 Name Resolution Using DNS**
**6.5.4 Resource Record Types**
**6.5.5 Host Address and Canonical Name Records**
**6.5.6 Mail Exchange, Service, and Text Records**
**6.5.7 Pointer Records**
**6.5.8 DNS Server Configuration**
**6.5.9 Internal vs External DNS**
**6.5.10 DNS Security**
**6.5.11 Lab: Configure DNS Addresses**
**6.5.12 Lab: Create Standard DNS Zones**
**6.5.13 Lab: Create Host Records**

**6.5.14 Lab: Create CNAME Records**

**6.5.15 Lab: Troubleshoot DNS Records**

**6.5.16 Configuring DNS Caching on Linux**

**6.6.1 Client DNS Issues**

**6.6.2 Name Resolution Issues**

**6.6.3 nslookup**

**6.6.4 dig**

**6.6.5 Lab: Explore nslookup**

**6.6.6 Lab: Use nslookup**

q_trouble_dns_ping_ip_address_n09.question.fex

Question 8. ✓ Correct

What is a scope in the context of DHCP server configuration?

- ◯ The physical range a wireless DHCP server can cover
- ◯ A tool for monitoring network traffic
- ◯ A set of rules for filtering packets
- → ◉ A range of IP addresses and options configured for a single subnet

**Explanation**

A scope is essential for defining the range of IP addresses that the DHCP server can assign within a specific subnet, along with other configuration options.

A tool for monitoring network traffic does not relate to DHCP scopes, which are about IP address allocation.

A set of rules for filtering packets is more akin to firewall functionality, not DHCP scope configuration.

The physical range a wireless DHCP server can cover refers to the signal coverage of a wireless access point, not a DHCP scope.

**References**

**6.2.1 DHCP Process**
**6.2.2 DHCP Server Configuration**
**6.2.5 Lab: Configure a DHCP Server**
**6.2.10 Lab: Configure Client Addressing for DHCP**
**6.3.2 IPv6 Interface Autoconfiguration and Testing**
**6.3.6 Set Up Alternate Addressing**
**6.4.2 DHCP Issues**
**6.4.4 Lab: Configure a DHCP Relay Agent**
**6.4.5 Lab: Add a DHCP Server on Another Subnet**

q_dhcp_config_scope_role_n09.question.fex

Question 9. ✓ Correct

You have a network with 50 workstations. You want to automatically configure the workstations with the IP address, subnet mask, and default gateway values.

Which device should you use?

→ ◉ DHCP server

○ Gateway

○ Router

○ DNS server

**Explanation**

Use a DHCP server to deliver configuration information to hosts automatically. Using DHCP is easier than configuring each host manually.

Use a gateway to provide access to a different network or a network that uses a different protocol.

Use a router to connect multiple subnets.

Use a DNS server to provide name resolution (for example, to get the IP address associated with a logical hostname).

**References**

**6.2.1 DHCP Process**

**6.2.2 DHCP Server Configuration**

**6.2.3 DHCP Options**

**6.2.4 DHCP Reservations and Exclusions**

**6.2.5 Lab: Configure a DHCP Server**

**6.2.6 Lab: Configure DHCP Server Options**

**6.2.7 Lab: Create DHCP Exclusions**

**6.2.8 Lab: Create DHCP Client Reservations**

**6.2.9 Configure Client Addressing**

**6.2.10 Lab: Configure Client Addressing for DHCP**

**6.3.2 IPv6 Interface Autoconfiguration and Testing**

**6.3.3 DHCPv6 Server Configuration**

**6.3.6 Set Up Alternate Addressing**

**6.4.1 DHCP Relay and IP Helper**

**6.4.2 DHCP Issues**

**6.4.3 Troubleshooting DHCP Exhaustion**

**6.4.4 Lab: Configure a DHCP Relay Agent**

**6.4.5 Lab: Add a DHCP Server on Another Subnet**

**6.4.6 Lab: Troubleshoot Address Pool Exhaustion**

**6.4.7 Lab: Explore DHCP Troubleshooting**

**6.4.8 Lab: Troubleshoot IP Configuration 1**

**6.4.9 Lab: Troubleshoot IP Configuration 2**

**6.4.10 Lab: Troubleshoot IP Configuration 3**

**6.6.1 Client DNS Issues**

q_dhcp_overview_example_n09.question.fex

Question 10. ✓ Correct

What is the purpose of applying a unicast address to DHCP frames by the DHCP relay?

- To broadcast the frames across multiple subnets
- To encrypt the DHCP frames for security
- → To directly communicate with the DHCP server without broadcasting
- To assign IP addresses to the frames

**Explanation**

The correct answer is to directly communicate with the DHCP server without broadcasting. By converting broadcast DHCP requests into unicast frames directed to the DHCP server's IP address, DHCP relays facilitate efficient communication between clients and servers across different subnets.

The conversion to unicast is for routing purposes, not encryption.

DHCP frames are not assigned IP addresses; they are forwarded to obtain them from a DHCP server.

The purpose is to avoid broadcasting across multiple subnets, not to enable it.

**References**

**6.2.1 DHCP Process**

**6.2.10 Lab: Configure Client Addressing for DHCP**

**6.3.2 IPv6 Interface Autoconfiguration and Testing**

**6.4.1 DHCP Relay and IP Helper**

**6.4.4 Lab: Configure a DHCP Relay Agent**

q_dhcp_relay_unicast_address_n09.question.fex

Question 11. ✓ Correct

What is the function of the Protocol field in the IPv4 header?

- ◯ Indicates the size of the header
- ◯ Indicates the version of Internet Protocol in use
- ◯ Specifies the total packet size
- → ◉ Specifies the type of data encapsulated in the payload

**Explanation**

The Protocol field in the IPv4 header specifies the type of data encapsulated in the payload, allowing the receiving host to know how to process it. This is crucial for the correct interpretation and handling of the data by the destination.

The version of Internet Protocol in use is indicated by the Version field.

The size of the header is indicated by the Length fields.

The total packet size is also indicated by the Length fields, not the Protocol field.

**References**

**4.1.1 IPv4 Datagram Header**

q_ipv4_header_protocol_purpose_n09.question.fex

Question 12. ✕ Incorrect

Under what condition is link aggregation considered to provide full redundancy?

→ ○ When the aggregated link's bandwidth matches the sum of all individual links

○ When all physical links in the aggregation are wireless connections

○ When the business function depends on the full speed of the bonded link and one port fails

◉ ~~When only two network interfaces are combined~~

**Explanation**

Full redundancy in the context of link aggregation is achieved when the total bandwidth of the aggregated link equals the sum of the bandwidths of all individual links. This ensures that even if one link fails, the remaining links can still provide the required bandwidth to maintain network operations without degradation in performance. This scenario represents an ideal state of redundancy where the network can sustain the loss of a link without impacting the overall functionality.

When the business function depends on the full speed of the bonded link and one port fails actually describes a condition where full redundancy is not achieved. If the business function requires the full speed of the bonded link and one port fails, leading to insufficient bandwidth, then the system lacks full redundancy because it cannot maintain its required operational level in the event of a failure.

The number of network interfaces combined (in this case, two) does not directly determine whether full redundancy is achieved. Full redundancy is more about the capacity to maintain required operational levels despite a failure, not the specific number of links aggregated.

The medium of the physical links (wireless or wired) does not determine the full redundancy of link aggregation. Full redundancy is concerned with the ability to sustain operational performance despite the failure of one or more links, regardless of whether the connections are wireless or wired.

**References**

**3.3.1 Link Aggregation and NIC Teaming**

**3.3.6 Lab: Configure Port Aggregation**

q_lag_full_redundancy_n09.question.fex

Question 13. ✓ Correct

What does flipping the 7th bit of the first octet in a MAC address to form an EUI-64 address accomplish?

- It converts the address to a link-local address.
- It indicates that the address is multicast.
- It signifies that the address is now private.
- → It differentiates the modified address from the original MAC address.

**Explanation**

Flipping the 7th bit (U/L bit) of the first octet in a MAC address when forming an EUI-64 address serves to differentiate the modified, globally unique address from the original MAC address. This bit manipulation is part of the process to ensure that the resulting IPv6 address is unique and can be distinguished from the hardware MAC address.

Flipping the 7th bit does not indicate that the address is multicast; it's part of creating a unique unicast address.

The process does not signify that the address is now private; it's about ensuring global uniqueness.

This process does not specifically convert the address to a link-local address; it's about forming a unique global or local unicast address.

**References**

**4.1.4 Unicast and Broadcast Addressing**

**4.5.4 IPv6 Unicast Addressing**

q_ipv6_unicast_flip_7th_bit_n09.question.fex

Question 14. ✓ Correct

You've implemented an ad hoc wireless network that doesn't employ a wireless access point. Every wireless network card can communicate directly with any other wireless network card on the network.

Which type of physical network topology have you implemented in this network?

→ (•) Mesh

( ) Bus

( ) Ring

( ) Star

**Explanation**

This type of network uses a physical mesh topology. A mesh topology has two key characteristics, which are that there's no central connecting point, and any host can communicate directly with any other host on the network.

A mesh network is usually impractical on a wired network. Each host would require a separate dedicated network interface and cable. But you can implement a mesh topology with relative ease on a wireless network because wires aren't an issue.

A ring topology connects neighboring nodes until they form a ring. Signals travel in one direction around the ring.

A star topology uses a hub or switch to connect all network connections to a single physical location.

A bus topology consists of a trunk cable with nodes either inserted directly into the trunk or tapped in with offshoot cables called drop cables.

**References**

**1.1.5 Mesh Topology**

q_mesh_topo_02_n09.question.fex

Question 15. ✓ Correct

What does the **show startup-config** command display?

- ◯ The switch's current operational status
- ◯ The list of errors logged by the switch
- → ◉ The switch's configuration upon the next reboot
- ◯ The switch's temporary configuration

**Explanation**

The **show startup-config** command is used to display the switch's configuration that will be used upon the next reboot. This is important for verifying changes that are saved but not yet applied.

The switch's temporary configuration is typically referred to as the running configuration, not the startup configuration.

The switch's current operational status is typically shown with commands like **show system status**, not show **startup-config**.

The list of errors logged by the switch can be viewed with commands like **show logging**, not show **startup-config**.

**References**

**3.4.3 Switch Show Commands**

q_int_config_show_startup-config_n09.question.fex

Question 16. ✓ Correct

You have purchased a solar backup power device to provide temporary electrical power to critical systems in your data center should the power provided by the electrical utility company go out. The solar panel array captures sunlight, converts it into direct current (DC), and stores it in large batteries.

The power supplies on the servers, switches, and routers in your data center require alternating current (AC) to operate.

Which electrical device should you implement to convert the DC power stored in the batteries into AC power that can be used in the data center?

- Transistor
- → Inverter
- Capacitor
- Transformer

**Explanation**

A power inverter changes direct current (DC) power to alternating current (AC) power. In this scenario, you can use a power inverter to convert the DC power stored in the batteries to AC power that your servers, switches, and routers can use in an emergency.

A transformer is typically used to increase or decrease AC power voltage.

A capacitor temporarily stores an electrical charge. Capacitors are used with the chips on a computer memory module that store data.

A transistor is used to amplify and switch electrical signals.

**References**

**2.5.3 Power Management**

q_power_inverter_n09.question.fex

Question 17. ✓ Correct

An administrator ran a command and determined that the FQDN of a client is forbes.sales.realty.com.

What is the hostname of the client?

- com
- sales
- realty
- → forbes

**Explanation**

A fully qualified domain name (FQDN) consists of the hostname and a domain suffix. In this domain, forbes is the hostname and the domain suffix is sales.realty.com.

A fully qualified domain name (FQDN) consists of the hostname and a domain suffix. In this domain, the suffix .com is the top-level domain.

A fully qualified domain name (FQDN) consists of the hostname and a domain suffix. In this domain, sales is a domain name within the top-level domain .com.

A fully qualified domain name (FQDN) consists of the hostname and a domain suffix. In this domain, realty is a domain name within the top-level domain .com.

**References**

**6.5.1 Host Names and Domain Names**
**6.5.2 DNS Hierarchy**
**6.5.3 Name Resolution Using DNS**
**6.5.4 Resource Record Types**
**6.5.5 Host Address and Canonical Name Records**
**6.5.6 Mail Exchange, Service, and Text Records**
**6.5.7 Pointer Records**
**6.5.8 DNS Server Configuration**
**6.5.9 Internal vs External DNS**
**6.5.10 DNS Security**
**6.5.11 Lab: Configure DNS Addresses**

- **6.5.12 Lab: Create Standard DNS Zones**
- **6.5.13 Lab: Create Host Records**
- **6.5.14 Lab: Create CNAME Records**
- **6.5.15 Lab: Troubleshoot DNS Records**
- **6.5.16 Configuring DNS Caching on Linux**
- **6.6.1 Client DNS Issues**
- **6.6.2 Name Resolution Issues**
- **6.6.3 nslookup**
- **6.6.4 dig**
- **6.6.5 Lab: Explore nslookup**
- **6.6.6 Lab: Use nslookup**

q_dns_overview_hostname_example_n09.question.fex

Question 18. ✓ Correct

What does a hierarchical star-mesh topology involve?

- A single central device connecting all other nodes
- A decentralized network without any hierarchical structure
- A direct connection between every pair of nodes in the network
- → Nodes at the top of the hierarchy configured in a mesh for redundancy

**Explanation**

A hierarchical star-mesh topology, the top-level nodes are configured in a mesh to provide redundancy, while lower levels may use star configurations.

A single central device connecting all other nodes describes a basic star topology, not a hierarchical star-mesh topology.

A direct connection between every pair of nodes in the network describes a full mesh topology. A hierarchical star-mesh involves specific nodes in a mesh, not all nodes.

A decentralized network without any hierarchical structure is incorrect because a hierarchical star-mesh topology does have a hierarchical structure.

**References**

**5.5.1 Hybrid Topology**

q_hybrid_star-mesh_n09.question.fex

Question 19. ✓ Correct

In RIP, what happens when a router receives an update that includes a route to a network it already knows about?

- It increments the hop count of its existing route by 1.
- It always replaces its existing route with the new one.
- It ignores the update.
- → It replaces its existing route with the new one only if the hop count is lower.

**Explanation**

The correct answer is that it replaces its existing route with the new one only if the hop count is lower. When a router in a RIP network receives an update that includes a route to a network it already knows about, it will compare the hop count of the new route with the existing one. If the new route has a lower hop count, the router will replace its existing route with the new one, as RIP aims to use the path with the lowest hop count.

It ignores the update is incorrect because the router evaluates the hop count of the new route before deciding to ignore or replace the existing route.

It always replaces its existing route with the new one is incorrect because replacement only occurs if the new route has a lower hop count.

It increments the hop count of its existing route by 1 is incorrect because the hop count is adjusted based on the received update, not arbitrarily incremented.

**References**

**5.2.2 Routing Information Protocol**

q_rip_already_known_n09.question.fex

Question 20. ✕ Incorrect

In a high-rise office building, the fire alarm system detects smoke on one of the floors. The building is equipped with a sophisticated fire suppression system that includes automatic smoke detectors, manual alarm points, and a combination of wet-pipe and pre-action sprinkler systems.

The fire is located in a storage room filled with paper products, which is adjacent to the server room.

Given the situation, which immediate action should the building's fire safety team prioritize to effectively manage the fire while minimizing potential damage to the server room?

- Immediately release the clean agent fire suppression system in the server room.
- → Use portable Class A fire extinguishers to control the fire in the storage room.
- Activate the wet-pipe sprinkler system throughout the entire building.
- ~~Manually activate the pre-action sprinkler system in the storage room only.~~

**Explanation**

Using portable Class A fire extinguishers to control the fire in the storage room is correct because Class A extinguishers are suitable for fires involving ordinary combustibles like paper, allowing for targeted suppression with minimal risk of water damage to the server room.

Activating the wet-pipe system throughout the entire building could cause unnecessary water damage, especially in areas not affected by the fire.

Because the fire is not in the server room. Prematurely releasing the clean agent could disrupt server operations unnecessarily.

The pre-action system is designed to fill with water upon detection of a fire, but manual activation without confirmation of heat could delay fire suppression efforts. Portable extinguishers provide immediate, targeted response.

**References**

**2.5.4 Fire Suppression**

q_fire_supp_class_a_scenario_n09.question.fex

Question 21. ✕ Incorrect

What does a blinking amber LED on a switch port signify?

- The link is connected but there is no traffic.
- → A fault has been detected.
- The link is operating normally with traffic.
- ~~The port is blocked by the spanning tree algorithm.~~

**Explanation**

A blinking amber LED signifies that a fault has been detected, which could be due to a duplex mismatch, excessive collisions, or redundancy check errors, among other issues.

A solid green LED, not a blinking amber one, indicates that the link is connected but there is no traffic.

A flickering green LED, not a blinking amber one, indicates that the link is operating normally with traffic.

A solid amber LED, not a blinking amber one, indicates that the port is blocked by the spanning tree algorithm.

**References**

**3.3.3 Spanning Tree Protocol**

**3.3.4 Spanning Tree Protocol Configuration**

**3.4.2 Port Status Indicators**

q_loopback_blinking_amber_led_n09.question.fex

Question 22. ✓ Correct

Routing data between computers on a network requires several mappings between different addresses.

Which of the following statements is true?

- Routers use DNS to resolve MAC addresses of diskless workstations into IP addresses based on the information contained in other routers' routing tables.
- Diskless workstations use ARP to ask a server for an IP address.
- ICMP lets routers bypass the general network broadcast by providing a dynamic table of IP-to-MAC address mappings.
- → Hosts use ARP to resolve known IP addresses into MAC addresses.

**Explanation**

ARP lets hosts resolve known IP addresses into MAC addresses by broadcasting requests to the network.

DNS is used to map hostnames to IP addresses. ARP is used to map IP addresses to MAC addresses.

Diskless workstations use BOOTP to discover their IP address, the server's IP address, and the boot files they should use.

ICMP notifies routers of problems on the network and undeliverable packets.

**References**

**4.1.3 Address Resolution Protocol**

q_arp_ip_to_mac_n09.question.fex

Question 23. ✓ Correct

What is the preferred route selection when there are paths to the same destination with different prefix lengths?

- The path with the shortest prefix length
- The path with the highest administrative distance
- The path with the highest metric value
- → The path with the longest prefix length

**Explanation**

The most specific path, which is the one with the longest prefix length, is preferred in route selection.

The shortest prefix length represents a less specific route.

The lowest metric value is preferred, not the highest.

The lowest administrative distance is preferred, indicating a more trustworthy source.

**References**

**5.2.1 Dynamic Routing Protocols**

**5.2.6 Route Selection**

q_route_missing_perferred_route_selection_n09.question.fex

Question 24. ✓ Correct

Your company has a network where all devices can communicate with each other as if they were directly connected, regardless of the physical connections.

What type of network topology does this describe?

- ○ Star topology
- → ◉ Logical topology
- ○ Mesh topology
- ○ Ring topology

**Explanation**

Logical topology is the correct answer. A logical topology describes the flow of data through the network. In the scenario, each device can send messages to any other device on the network, which is a characteristic of a logical topology.

A star topology is a type of physical topology where each device on the network is connected to a central node or switch. While the scenario describes a network that physically resembles a star topology, the question is asking for the type of network topology that describes the flow of data, which is a logical topology.

In a mesh topology, every device is connected to every other device on the network. This is not the case in the scenario described.

In a ring topology, each device is connected to exactly two other devices, forming a ring. This is not the case in the scenario described.

**References**

**1.1.2 Network Types**

**1.1.3 Network Topology**

**1.1.4 Star Topology**

**1.1.7 Lab: Create Network Topologies**

q_network_topo_logical_n09.question.fex

Question 25. ✓ Correct

What does ingress and egress traffic filtering refer to?

→ ◉ Controlling both inbound and outbound network traffic

○ Monitoring internet usage and bandwidth

○ Encrypting data entering and leaving a network

○ Filtering both internal and external emails

**Explanation**

The correct answer is to control both inbound and outbound network traffic. Ingress filtering controls incoming traffic to the network, while egress filtering controls outgoing traffic, together ensuring comprehensive traffic management for security purposes.

Ingress and egress filtering apply to all network traffic, not just emails.

The focus is on controlling traffic flow, not encrypting data.

The primary goal is to manage traffic for security reasons, not to monitor usage or bandwidth.

**References**

**1.3.5 Transport and Application Layer and Security Functions**

**5.4.1 Firewall Uses and Types**

**5.4.2 Firewall Selection and Placement**

**10.5.1 Security Rules and ACL Configuration**

**10.5.4 Misconfigured Firewall and ACL Issues**

**10.5.5 Creating Firewall ACLs**

**10.5.7 Lab: Configure a Security Appliance**

**10.5.8 Lab: Configure a Perimeter Firewall**

**14.3.5 Cloud Firewall Security**

q_firewalls_ingress_egress_n09.question.fex

Question 26. ✓ Correct

Which of the following best describes packet filtering firewalls?

- They inspect the content of each data packet.
- They encrypt each data packet.
- → They inspect the headers of IP packets and filter based on rules.
- They only filter outgoing traffic from a network.

**Explanation**

Packet filtering firewalls analyze the headers of IP packets, applying rules to either allow or block the packets based on source and destination IP addresses, protocol types, and port numbers.

Packet filtering firewalls focus on inspecting and filtering packets, not encrypting them.

Packet filtering firewalls inspect packet headers, not the content or payload of the packets.

Packet filtering firewalls can filter both incoming and outgoing traffic.

**References**

**1.3.5 Transport and Application Layer and Security Functions**
**5.4.1 Firewall Uses and Types**
**5.4.2 Firewall Selection and Placement**
**10.5.1 Security Rules and ACL Configuration**
**10.5.4 Misconfigured Firewall and ACL Issues**
**10.5.5 Creating Firewall ACLs**
**10.5.7 Lab: Configure a Security Appliance**
**10.5.8 Lab: Configure a Perimeter Firewall**
**14.3.5 Cloud Firewall Security**

q_firewalls_packet_filtering_description_n09.question.fex

Question 27. ✓ Correct

Which of the following are elements of an IPv6 packet? (Select two.)

→ ☑ Main header

☐ Options field

☐ TTL (Time to Live)

→ ☑ Extension headers

☐ Checksum

**Explanation**

The following are elements of an IPv6 packet:

- Main header. The main header is an essential part of every IPv6 packet, containing important information such as the source and destination addresses, and the version of the IP protocol being used (IPv6).
- Extension headers. Extension headers are used in IPv6 to provide optional features and functionalities such as routing, fragmentation, and security (IPSec), which are not included in the main header.

Checksum is incorrect because IPv6 packets do not include a checksum in the header. Error detection for the header is assumed to be handled by the link layer, and error detection for the payload is handled by the transport layer protocols like TCP or UDP.

The Options field is incorrect because the options field present in IPv4 headers is replaced by extension headers in IPv6. The extension headers provide a more flexible and extensible mechanism for supporting additional functionalities.

TTL (Time to Live) is incorrect because in IPv6, the concept of TTL (Time to Live) from IPv4 is replaced by the Hop Limit field. The Hop Limit serves a similar purpose to TTL, decrementing by one at each hop, but it is part of the main header in IPv6, not a separate element.

**References**

**4.5.1 IPv4 vs IPv6**

q_ipv4_ipv6_elements_n09.question.fex

Question 28. ✓ Correct

Which of the following best describes a directly connected route in a routing table?

→ ◉ A route that is automatically added for each active router interface, representing subnets for which the router has a local interface

○ A special type of static route that serves as the gateway of last resort

○ A route for subnets and IP networks that are not directly attached to the router

○ A route that is manually added and requires manual updates

**Explanation**

Directly connected routes are automatically added to the routing table for each active router interface, indicating the subnets for which the router has a local interface. This ensures that the router can directly forward packets to these subnets without needing to learn these routes through other means.

A route that is manually added and requires manual updates describes a static route, which is manually added to the routing table by an administrator and does not automatically update.

A route for subnets and IP networks that are not directly attached to the router describes remote routes, which are for subnets and IP networks not directly attached to the router.

A special type of static route that serves as the gateway of last resort describes a default route, which is a special type of static route used when an exact match for a network or host route is not found in the routing table.

**References**

**5.1.2 Static and Default Routes**

**5.1.3 Routing Table Example**

**5.1.4 Packet Forwarding**

q_route_route_directly_connected_route_n09.question.fex

Question 29. ✓ Correct

During an audit of external DNS records, you need to verify the mail servers configured for your public domain example.com.

Which **nslookup** command would you use to find this information?

- **nslookup example.com**
- **nslookup -type=a example.com**
- **nslookup -type=ns example.com**
- → **nslookup -type=mx example.com**

**Explanation**

The **nslookup -type=mx example.com** command is correct because the -type=mx option specifically queries for mail exchange (MX) records, which are used to identify mail servers for a domain.

The **-type=a** option queries for A records, which map hostnames to IPv4 addresses, not mail servers.

Running **nslookup** without specifying a type will primarily return A and AAAA records, which are not directly relevant to finding mail server configurations.

The **-type=ns** option queries for name server records, which identify DNS servers for the domain, not mail servers.

**References**

**6.5.16 Configuring DNS Caching on Linux**

**6.6.2 Name Resolution Issues**

**6.6.3 nslookup**

**6.6.5 Lab: Explore nslookup**

**6.6.6 Lab: Use nslookup**

**10.3.5 Lab: Scan for Unsecure Protocols**

q_nslookup_type_mx_scenario_n09.question.fex

Question 30. ✓ Correct

Your company has recently expanded its operations and opened a new branch office. As the IT manager, you are tasked with setting up the network infrastructure for this new location. The office will connect to the company's main data center via the Internet for access to centralized resources.

You need to select a router that will manage the traffic between the branch office's local area network (LAN) and the wide area network (WAN) internet access efficiently.

Which type of router would be most suitable for this purpose?

→ (●) Edge router

( ) Core router

( ) Virtual router

( ) Wireless router

**Explanation**

An edge router is the most suitable choice for managing traffic between a branch office's LAN and the WAN internet access. It is specifically designed to serve as the boundary between internal networks and external networks, handling data entering and exiting the network. This makes it ideal for connecting the branch office to the company's main data center over the internet.

Core routers are used within the backbone of the Internet or within large enterprise networks to route traffic within the network core. They are not designed for direct connection to external networks, making them less suitable for the described scenario.

While a wireless router provides Wi-Fi connectivity, its primary function is not to manage traffic between a LAN and WAN. In a business environment, especially for connecting a branch office to a main data center, a more robust solution like an edge router is needed.

Virtual routers can be used in various scenarios, including as part of a virtualized network infrastructure. However, for the specific task of managing traffic between a branch office's LAN and the WAN with a physical connection, a physical edge router is more appropriate. Virtual routers are more suited for environments where routing capabilities need to be dynamically adjusted or where physical space and hardware are limited.

**References**

**5.3.1 Edge Routers**

q_edge_route_example_scenario_n09.question.fex

Question 31. ✓ Correct

You manage a network that has multiple internal subnets. You connect a workstation to the 192.168.1.0/24 subnet.

This workstation cannot communicate with any other host on the network. You run **ipconfig /all** and see the following:

```
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix. : mydomain.local
Description . . . . . : Broadcom network adapter
Physical Address . . . . . : 00-AA-BB-CC-74-EF
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . : Yes
IPv4 Address. . . . . : 192.168.2.102(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway. . . . . : 192.168.1.1
DNS Servers . . . . . : 192.168.2.20
```

What is the MOST likely cause of the problem?

- ○ Incorrect default gateway
- ○ Incorrect subnet mask
- ○ Incorrect DNS server address
- → ◉ Incorrect IP address

**Explanation**

In this example, the IP address assigned to the host is on the wrong subnet. The host address is on the 192.168.2.0/24 subnet, but the other devices are using addresses on the 192.168.1.0 subnet (the scenario states that you're connecting the workstation to this subnet).

**References**

**4.4.1 ipconfig**
**4.4.2 ifconfig and ip**
**4.4.5 Lab: IPv4 Troubleshooting Tools**
**4.4.6 Lab: IPv4 Troubleshooting tools for Linux**
**4.4.7 Lab: Use IPv4 Test Tools**
**6.4.6 Lab: Troubleshoot Address Pool Exhaustion**
**6.4.8 Lab: Troubleshoot IP Configuration 1**
**6.4.9 Lab: Troubleshoot IP Configuration 2**
**6.4.10 Lab: Troubleshoot IP Configuration 3**

**6.6.1 Client DNS Issues**

**6.6.2 Name Resolution Issues**

q_ipconfig_incorrect_address_scenario_n09.question.fex

Question 32. ✓ Correct

Which organizations have created categories of cable standards for twisted pair to simplify the selection of a suitable quality cable?

→ ◉ ANSI and TIA/EIA

○ ITU and ETSI

○ ISO and IEC

○ IEEE and IETF

**Explanation**

The American National Standards Institute (ANSI) and the Telecommunications Industry Association (TIA)/Electronic Industries Alliance (EIA) are responsible for creating categories of cable standards for twisted pair cables. This simplifies the process of selecting a suitable quality cable for telecommunications purposes.

IEEE and IETF are organizations involved in setting standards for various technologies, but they are not the ones responsible for creating categories of cable standards for twisted pair cables.

ISO and IEC maintain similar standards but are not the primary organizations mentioned in the document for creating categories of cable standards for twisted pair cables.

ITU and ETSI are involved in telecommunications and standardization but are not the organizations mentioned in the document for this specific task.

**References**

**2.2.3 Cat Cable Standards**

q_cat_ansi_tia_eia_n09.question.fex

Question 33. ✓ Correct

What is a runt frame error?

- A frame larger than the maximum permissible size
- → A frame that is smaller than the minimum size
- A frame transmitted with high signal quality
- A frame with no CRC errors

**Explanation**

A frame that is smaller than the minimum size is the correct answer. A runt frame is a frame that is smaller than the minimum size required for Ethernet frames (64 bytes), often caused by collisions.

A frame larger than the maximum permissible size is referred to as a giant frame, not a runt frame.

The presence or absence of CRC errors is unrelated to the definition of a runt frame.

The signal quality does not determine whether a frame is considered a runt.

**References**

**3.4.4 Interface Error Counters**

q_int_error_runt_frame_error_n09.question.fex

Question 34. ✓ Correct

What advantage does a stackable switch offer over a non-stackable switch?

- It offers fewer ports.
- It cannot be managed as a single unit.
- It allows for physical stacking only, without any management benefits.
- → It simplifies network management by allowing multiple switches to be managed as a single unit.

**Explanation**

Simplifying network management by allowing multiple switches to be managed as a single unit is a key benefit of stackable switches, enhancing network scalability and simplifying management by treating multiple switches as a single entity.

The primary advantage of stackable switches is precisely that they can be managed as a single unit.

Stackable switches do not inherently offer fewer ports; the stacking feature is about management and scalability rather than limiting port availability.

Stackable switches offer more than just physical stacking; they allow for simplified management and scalability by operating as a group.

**References**

**1.3.3 Data Link Layer Functions**
**3.2.1 Hubs**
**3.2.3 Switches**
**3.2.4 Ethernet Switch Types**
**3.2.5 Switch Interface Configuration**
**3.2.7 Lab: Install a Switch in the Rack**
**3.2.8 Lab: Secure a Switch**

q_switch_types_stackable_vs_nonstackable_n09.question.fex

Question 35. ✓ Correct

What is the purpose of a socket in the context of network communications?

- ◯ To provide a physical connection between two devices
- ◯ To act as a firewall between the client and server
- → ◉ To serve as a unique identifier for a network connection
- ◯ To encrypt data being sent over the network

**Explanation**

A socket serves as a unique identifier for a network connection, combining the IP address and port number to uniquely identify each end of a communication link.

A socket does not encrypt data; it's used for identifying connections.

A socket is not a physical connection but a logical concept used in networking.

A socket does not act as a firewall; it's used for identifying and managing connections.

**References**

**6.1.2 Transmission Control Protocol**

**6.1.3 TCP Handshake and Teardown**

**6.1.7 Lab: Explore Three-Way Handshake in Wireshark**

q_transport_socket_purpose_n09.question.fex

Question 36. ✓ Correct

What is the maximum theoretical size of an IPv4 packet?

→ ◉ 65,535 bytes

○ 1500 bits

○ 32 bits

○ 1,500 bytes

**Explanation**

The maximum theoretical size of an IPv4 packet is 65,535 bytes. This limit is set by the total length field in the IPv4 header, which specifies the total size of the packet including the header and the payload.

1,500 bytes is typically the MTU for Ethernet frames, not the maximum size for an IPv4 packet.

32 bits refers to the size of the source and destination address fields, not the total packet size.

The size is measured in bytes, not bits, and 1500 bits is not the maximum size for an IPv4 packet.

**References**

**4.1.1 IPv4 Datagram Header**

q_ipv4_header_packet_size_n09.question.fex

Question 37. ✓ Correct

Can the same domain name be registered within different top-level domains?

- ○ No, domain names are globally unique and cannot be duplicated.
- ○ Yes, but only if they are in different countries.
- → ◉ Yes, the same domain name can be registered within different TLDs.
- ○ No, once a domain name is registered, it cannot be used elsewhere.

**Explanation**

The correct answer is that the same domain name can be registered within different TLDs. This allows organizations to use the same domain name across different TLDs, catering to various purposes or regions.

Country restriction is not a factor; the same name can be registered under any TLDs.

Domain names can be duplicated across TLDs, ensuring they are unique within each TLD.

Global uniqueness applies within a TLD, not across all TLDs.

**References**

- **6.5.1 Host Names and Domain Names**
- **6.5.2 DNS Hierarchy**
- **6.5.3 Name Resolution Using DNS**
- **6.5.4 Resource Record Types**
- **6.5.5 Host Address and Canonical Name Records**
- **6.5.6 Mail Exchange, Service, and Text Records**
- **6.5.7 Pointer Records**
- **6.5.8 DNS Server Configuration**
- **6.5.9 Internal vs External DNS**
- **6.5.10 DNS Security**
- **6.5.11 Lab: Configure DNS Addresses**
- **6.5.12 Lab: Create Standard DNS Zones**
- **6.5.13 Lab: Create Host Records**
- **6.5.14 Lab: Create CNAME Records**

**6.5.15 Lab: Troubleshoot DNS Records**

**6.5.16 Configuring DNS Caching on Linux**

**6.6.1 Client DNS Issues**

**6.6.2 Name Resolution Issues**

**6.6.3 nslookup**

**6.6.4 dig**

**6.6.5 Lab: Explore nslookup**

**6.6.6 Lab: Use nslookup**

q_dns_overview_different_top-level_n09.question.fex

Question 38. ✓ Correct

Which fiber optic connector is known for its small form factor and is widely adopted for Gigabit Ethernet and 10/40 GbE?

→ ◉ Local Connector (LC)

○ Subscriber Connector (SC)

○ Mini-MT

○ Straight Tip (ST)

**Explanation**

The correct answer is Local Connector (LC). The Local Connector is known for its small form factor, which allows for higher port density. Its tabbed push/pull design makes it similar to the SC connector but smaller in size. This connector is widely adopted for use in Gigabit Ethernet and 10/40 GbE networks due to its compact size and reliability.

The Straight Tip (ST) connector, while an early popular choice for multimode networks, is not specifically known for its use in Gigabit Ethernet and 10/40 GbE. Its larger size and bayonet-style locking mechanism differ from the requirements of high-density networking applications.

The Subscriber Connector (SC) is indeed used for single- or multimode fibers and is common in Gigabit Ethernet. However, it is not specifically highlighted for its small form factor or widespread adoption in 10/40 GbE networks as the LC connector is.

Mini-MT is not a standard or widely recognized type of fiber optic connector in the context provided. The question focuses on connectors known for their small form factor and widespread adoption in specific Ethernet standards, which applies to the LC connector.

**References**

**2.4.3 Fiber Optic Connector Types**

q_fiber_con_local_connector_n09.question.fex

Question 39. ✓ Correct

What is the primary difference between dynamic learning and static configuration in network devices?

- Dynamic learning assigns IP addresses to devices, while static configuration is used for assigning MAC addresses.
- → Dynamic learning allows network devices to automatically learn and store MAC addresses, while static configuration requires manual entry of MAC addresses.
- Static configuration allows for automatic updates to device firmware, while dynamic learning does not.
- Dynamic learning encrypts network traffic, while static configuration does not.

**Explanation**

Dynamic learning refers to the capability of network devices, such as switches, to automatically identify and store MAC addresses as devices communicate across the network, facilitating efficient packet forwarding. Static configuration, on the other hand, involves manually specifying MAC addresses in a device's configuration, which can be useful for security or specific networking requirements but is less flexible and more labor-intensive.

Dynamic learning and static configuration pertain to how MAC addresses are learned or configured, not to the encryption of network traffic. Encryption is handled by separate protocols and configurations.

Both static configuration and dynamic learning are related to MAC address handling and have no direct impact on firmware updates. Firmware updates are managed through different mechanisms and are unrelated to how MAC addresses are learned or configured.

Dynamic learning is specifically about learning MAC addresses, not assigning IP addresses. IP address assignment is typically handled by DHCP (Dynamic Host Configuration Protocol) or manual configuration, not by the process of dynamic learning in switches. Static configuration of MAC addresses is a manual process for specific networking needs and does not involve IP address assignment.

**References**

**4.4.5 Lab: IPv4 Troubleshooting Tools**

**4.4.7 Lab: Use IPv4 Test Tools**

**6.4.7 Lab: Explore DHCP Troubleshooting**

q_arp_cache_static_vs_dynamic_n09.question.fex

Question 40. ✓ Correct

Why might pinging remote hosts fail even if the network configuration is correct?

- The local host's IP address is incorrectly configured.
- The default gateway is down.
- The loopback address is not responding.
- → ICMP is blocked by a firewall or other security software.

**Explanation**

Pinging remote hosts might fail due to ICMP packets being blocked by a firewall or other security software, especially in environments with strict security policies, even if the network configuration is correct.

The loopback address not responding would indicate an issue with the TCP/IP stack, not with pinging remote hosts specifically.

An incorrectly configured local host's IP address would more likely affect local communication, not specifically pinging remote hosts.

If the default gateway is down, it would prevent communication with the local network or Internet, but the question implies that the network configuration, including the gateway, is correct.

**References**

**4.4.3 arp**
**4.4.4 ping**
**4.4.5 Lab: IPv4 Troubleshooting Tools**
**4.4.7 Lab: Use IPv4 Test Tools**
**6.4.7 Lab: Explore DHCP Troubleshooting**
**6.4.9 Lab: Troubleshoot IP Configuration 2**
**6.4.10 Lab: Troubleshoot IP Configuration 3**
**6.5.15 Lab: Troubleshoot DNS Records**
**6.6.1 Client DNS Issues**
**6.6.2 Name Resolution Issues**

q_prob_iso_icmp_blocked_n09.question.fex

Question 41. ✓ Correct

What happens if a Windows host does not receive a response from a DHCP server within a given time frame?

- It will prompt the user to manually enter an IP address.
- → It will select an address at random from the APIPA range.
- It will broadcast a request for manual configuration assistance.
- It will shut down to prevent network conflicts.

**Explanation**

If a Windows host does not receive a DHCP offer within a certain time frame, it will automatically select an IP address from the APIPA range (169.254.1.1 to 169.254.254.254). This allows the host to continue communicating on the local network despite the absence of DHCP server communication.

The host does not shut down; it seeks an alternative method to configure its IP address.

While users can manually enter an IP address, this is not the automatic response when a DHCP server cannot be contacted.

The host does not broadcast for manual configuration assistance; it automatically selects an APIPA address.

**References**

**4.5.5 IPv6 Link Local Addressing**

**6.3.1 Automatic Private IP Addressing**

**6.3.4 Lab: Explore APIPA Addressing**

**6.3.5 Lab: Explore APIPA Addressing in Network Modeler**

**6.3.6 Set Up Alternate Addressing**

q_apipa_dhcp_response_n09.question.fex

Question 42.

Incorrect

| Router B Routing Table | | |
|---|---|---|
| Network | Interface | Source |
| 10.0.1.0/24 | G0 | Static |
| 10.0.2.0/24 | G0 | Connected |
| 10.0.3.0/24 | G1 | Connected |
| 10.0.4.0/24 | G1 | Static |


| Router A Routing Table | | |
|---|---|---|
| Network | Interface | Source |
| 10.0.1.0/24 | G0 | Connected |
| 10.0.2.0/24 | G1 | Connected |
| 10.0.3.0/24 | G1 | Static |
| 10.0.4.0/24 | G1 | Static |

| Router C Routing Table | | |
|---|---|---|
| Network | Interface | Source |
| 0.0.0.0/0 | G0 | Static |
| 10.0.3.0/24 | G0 | Connected |
| 10.0.4.0/24 | G1 | Connected |

Considering the example below of three routers connected in a series, which static routes is Router A configured with? (Select two.)

- [ ] 10.0.4.0/24
- [x] ~~10.0.2.0/24~~
- [ ] 10.0.3.0/24
- [x] ~~10.0.1.0/24~~
- [ ] 0.0.0.0/0

**Explanation**

Router A has been configured with static routes to 10.0.3.0/24 and 10.0.4.0/24, both of which are reachable via interface G1.

None of the routers have been configured with a static route of 10.0.2.0/24.

Router B has been configured with a static route to 10.0.1.0/24, which is reachable via interface G0.

Router C has been configured with static route 0.0.0.0/0, which is reachable via interface G0.

**References**

**5.1.2 Static and Default Routes**

**5.1.3 Routing Table Example**

### 5.1.4 Packet Forwarding

q_routing_char_router_a_02.question.fex

Question 43. ✓ Correct

You have a network address of 132.66.0.0 and a subnet mask of 255.255.224.0.

Which of the following are valid subnet addresses? (Select two.)

- → ☑ 132.66.96.0
- ☐ 132.98.0.0
- → ☑ 132.66.192.0
- ☐ 132.130.0.0
- ☐ 132.66.255.0

**Explanation**

To determine the valid subnet addresses, complete the following steps:

1. Convert the custom subnet mask value to binary (224 = 11100000).
2. Select the rightmost masked bit (100000).
3. Convert this bit to decimal. This is the increment value (32).
4. Add the increment value to the network address, up to the subnet mask value. In this example, the possible subnet addresses are:

- 132.66.0.0
- 132.66.32.0
- 132.66.64.0
- 132.66.96.0
- 132.66.128.0
- 132.66.160.0
- 132.66.192.0
- 132.66.224.0

**References**

**4.2.3 Subnet Masks**

q_subnets_valid_subnet_addresses_n09.question.fex

Question 44. ✓ Correct

What is the first step in the DHCP lease process?

- DHCPOFFER
- DHCPREQUEST
- → DHCPDISCOVER
- DHCPACK

**Explanation**

The first step in the DHCP lease process is the DHCPDISCOVER message, where the client broadcasts to find a DHCP server.

DHCPOFFER is incorrect because it is the second step, where the server offers an IP address to the client.

DHCPREQUEST is incorrect because it is the third step, where the client requests to use the offered IP address.

DHCPACK is incorrect because it is the fourth step, where the server acknowledges the client's request to use the IP address.

**References**

**6.2.1 DHCP Process**
**6.2.2 DHCP Server Configuration**
**6.2.3 DHCP Options**
**6.2.4 DHCP Reservations and Exclusions**
**6.2.5 Lab: Configure a DHCP Server**
**6.2.6 Lab: Configure DHCP Server Options**
**6.2.7 Lab: Create DHCP Exclusions**
**6.2.8 Lab: Create DHCP Client Reservations**
**6.2.9 Configure Client Addressing**
**6.2.10 Lab: Configure Client Addressing for DHCP**
**6.3.2 IPv6 Interface Autoconfiguration and Testing**
**6.3.3 DHCPv6 Server Configuration**
**6.3.6 Set Up Alternate Addressing**

**6.4.1 DHCP Relay and IP Helper**

**6.4.2 DHCP Issues**

**6.4.3 Troubleshooting DHCP Exhaustion**

**6.4.4 Lab: Configure a DHCP Relay Agent**

**6.4.5 Lab: Add a DHCP Server on Another Subnet**

**6.4.6 Lab: Troubleshoot Address Pool Exhaustion**

**6.4.7 Lab: Explore DHCP Troubleshooting**

**6.4.8 Lab: Troubleshoot IP Configuration 1**

**6.4.9 Lab: Troubleshoot IP Configuration 2**

**6.4.10 Lab: Troubleshoot IP Configuration 3**

**6.6.1 Client DNS Issues**

q_dhcp_overview_lease_first_step_n09.question.fex

Question 45. ✓ Correct

What should you suspect if you cannot ping a local host and the error is "destination unreachable"?

- The network protocol stack needs to be reinstalled
- The default gateway parameter on the local host is incorrect
- → Incorrect IP address or netmask in the IP configuration
- ICMP is blocked by a firewall or other security software

**Explanation**

If a local host cannot be pinged and the error is "destination unreachable," it suggests an issue with the local configuration, such as an incorrect IP address or netmask.

The need to reinstall the network protocol stack is suggested by an inability to ping the loopback address, not by a "destination unreachable" error when pinging a local host.

An incorrect default gateway parameter would affect the ability to communicate with remote hosts, not local hosts.

ICMP being blocked would not typically result in a "destination unreachable" error for local hosts, as this involves local network communication that doesn't pass through firewalls or security software configured to block ICMP.

**References**

**4.6.3 IP Forwarding Issues**

q_prob_iso_destination_unreachable_n09.question.fex

Question 46. ✕ Incorrect

You are monitoring network traffic and notice that ARP requests for a specific IP address are receiving responses from two different MAC addresses.

What is the MOST likely cause of this issue, and how should you proceed to troubleshoot it?

→ ○ There may be a duplicate MAC address issue; use a protocol analyzer to examine ARP traffic more closely.

◉ ~~The IP address is configured on a virtual machine and its host; reassign the IP address to only one device.~~

○ The network switch is malfunctioning; replace the switch immediately.

○ This is a normal occurrence in networks with multiple access points; no action is needed.

**Explanation**

When ARP requests for a specific IP address receive responses from two different MAC addresses, it indicates a potential duplicate MAC address issue. Using a protocol analyzer to examine ARP traffic more closely allows you to identify which devices are claiming the same MAC address, facilitating further investigation and resolution of the conflict.

While networks with multiple access points may have complex ARP behaviors, receiving ARP responses from two different MAC addresses for a single IP address is indicative of an issue, not a normal occurrence.

A malfunctioning network switch could cause various network issues, but duplicate MAC addresses responding to ARP requests for a single IP address suggest a problem with the devices themselves, not necessarily the switch.

While IP address conflicts can occur with virtual machines and their hosts, the scenario describes a MAC address conflict, which requires a different approach to troubleshooting.

**References**

**8.5.3 Protocol Analyzers**

**8.5.4 Using Wireshark to Troubleshoot Network Issues**

**8.5.5 Lab: Troubleshoot with Wireshark**

**9.3.7 Lab: Poison ARP and Analyze with Wireshark**

q_ip_duplicate_protocol_analyzer_scenario_n09.question.fex

Question 47. ✓ Correct

Consider the following IP addresses:

1. 124.77.8.5
2. 131.11.0.9
3. 190.66.250.10
4. 196.5.89.44

Which of the following represents (in order) the IP address class of each listed IP address?

- Class A, Class B, Class C, Class C
- → Class A, Class B, Class B, Class C
- Class B, Class B, Class C, Class C
- Class B, Class C, Class C, Class D
- Class B, Class B, Class C, Class D

**Explanation**

The IP addresses listed are of the following classes: Class A, Class B, Class B, Class C. You can identify the IP address class by memorizing the range of values for the first octet.

- 0-126 = Class A
- 128-191 = Class B
- 192-223 = Class C
- 223-239 = Class D
- 240-255 = Class E

**References**

**4.3.1 Classful Addressing**

q_class_addr_class_order_n09.question.fex

Question 48. ✕ Incorrect

What is a recommended action before reconfiguring DHCP server scopes?

→ ◯ Lower the lease duration.

◯ Disable the DHCP server temporarily.

◉ ~~Inform all network users about the change.~~

◯ Increase the lease duration.

**Explanation**

Lowering the lease duration before making changes to DHCP server scopes forces all clients to renew their leases more frequently. This ensures that clients' IP configurations are updated more quickly once the changes are made, minimizing potential connectivity issues.

Increasing the lease duration would delay clients from obtaining updated IP configurations after the server scopes are edited.

Disabling the DHCP server temporarily would prevent all clients from obtaining or renewing IP leases, causing network connectivity issues.

While informing users about changes is good practice, it does not technically facilitate the update of clients' IP configurations in response to DHCP scope changes.

**References**

**6.2.1 DHCP Process**

**6.2.2 DHCP Server Configuration**

**6.2.5 Lab: Configure a DHCP Server**

**6.2.10 Lab: Configure Client Addressing for DHCP**

**6.3.2 IPv6 Interface Autoconfiguration and Testing**

**6.3.6 Set Up Alternate Addressing**

**6.4.2 DHCP Issues**

**6.4.4 Lab: Configure a DHCP Relay Agent**

**6.4.5 Lab: Add a DHCP Server on Another Subnet**

q_dhcp_issues_lower_lease_duration_n09.question.fex

Question 49. ✓ Correct

What solution addresses the inflexibility of using whole octet boundaries for subnet masks in IP networking?

→ ◉ Dividing networks into subnetworks or subnets

○ Using dynamic IP addressing

○ Increasing the number of IP addresses with IPv6

○ Applying Quality of Service (QoS) protocols

**Explanation**

The inflexibility of using whole octet boundaries for subnet masks is addressed by dividing networks into subnetworks or subnets. This approach allows for more efficient use of IP address space by creating smaller, logically separated portions of a larger network. It enables the allocation of IP addresses based on the specific needs of different parts of a network, rather than adhering to the rigid structure imposed by whole octet boundaries.

Dynamic IP addressing involves automatically assigning IP addresses to devices on a network. While it helps manage IP addresses efficiently, it does not solve the problem of inflexibility in subnetting based on whole octet boundaries. Dynamic IP addressing is more about the allocation and management of IP addresses rather than structuring networks into smaller, more manageable segments.

Transitioning to IPv6 significantly increases the pool of available IP addresses, addressing the limitation of IP address availability in IPv4. However, it does not directly address the issue of inflexibility in subnetting with whole octet boundaries. IPv6 does offer more flexibility in addressing and subnetting, but the specific solution to the mentioned problem is dividing networks into smaller subnetworks or subnets.

Quality of Service (QoS) protocols are used to prioritize network traffic, ensuring that critical applications receive the bandwidth they need. However, QoS does not address the structural division of networks into subnetworks or the flexibility of subnetting. It is focused on managing and optimizing network traffic rather than organizing the network into more efficient subnetworks.

**References**

**4.2.3 Subnet Masks**

q_subnets_dividing_networks_subnets_n09.question.fex

Question 50. ✓ Correct

What happens when a routing protocol's database contains more than one route to the same destination prefix?

- All routes are used simultaneously to balance the load.
- The router selects the route with the highest cost metric.
- The router randomly selects one of the routes for use.
- → The path with the lowest cost metric is used.

**Explanation**

When multiple routes to the same destination are available, the routing protocol evaluates them based on their cost metrics. The route with the lowest cost metric is considered the most efficient and is therefore selected for use in the IP routing table. This ensures optimal use of network resources and efficient data transmission.

Selecting the route with the highest cost metric would lead to less efficient data transmission, which contradicts the goal of dynamic routing protocols to find the best path.

Routing decisions are not made randomly. They are based on specific criteria, such as the cost metric, to ensure the most efficient path is chosen.

While some routing protocols can support load balancing across multiple paths, the question specifically refers to the selection process when multiple routes are available. The primary criterion for selection is the cost metric, not load balancing.

**References**

**5.2.1 Dynamic Routing Protocols**

**5.2.6 Route Selection**

q_dyroute_same_destination_prefix_n09.question.fex

Question 51. ✓ Correct

What factor is considered when there are identical paths with equal administrative distances to a destination?

- The path with the most recent update
- The path with the highest metric value
- → The path with the lowest metric value
- The path with the shortest prefix length

**Explanation**

When there are identical paths with equal administrative distances, the path with the lowest metric value is preferred, as it represents the most efficient route.

The highest metric value indicates a less efficient route.

Prefix length is considered before comparing metric values when paths are not identical.

The timing of updates does not directly influence route selection in this context.

**References**

**5.2.1 Dynamic Routing Protocols**

**5.2.6 Route Selection**

q_route_missing_identical_paths_n09.question.fex

Question 52. ✓ Correct

When referencing network topologies, what distinguishes half-duplex from full-duplex communication in a point-to-point link?

- Half-duplex communication can only occur in one direction, while full-duplex allows for data transmission in both directions but not at the same time.
- Full-duplex communication is limited to one direction at a time, similar to half-duplex, but it operates at higher speeds.
- → Half-duplex allows for data transmission in both directions, but not simultaneously; full-duplex permits simultaneous two-way data transmission.
- Half-duplex communication uses a single cable for data transmission, whereas full-duplex requires separate cables for each direction.

**Explanation**

The correct answer is half-duplex allows for data transmission in both directions, but not simultaneously; full-duplex permits simultaneous two-way data transmission.

Half-duplex communication can only occur in one direction, while full-duplex allows for data transmission in both directions but not at the same time is incorrect. It inaccurately states that half-duplex communication can only occur in one direction. Half-duplex does allow for two-way communication, but with the limitation that it cannot happen simultaneously.

Full-duplex communication is limited to one direction at a time, similar to half-duplex, but it operates at higher speeds is incorrect. It confuses the capabilities of full-duplex communication. Full-duplex systems can indeed transmit data in both directions simultaneously, not just one direction at a time. The speed of the communication is not the defining difference between half-duplex and full-duplex.

Half-duplex communication uses a single cable for data transmission, whereas full-duplex requires separate cables for each direction is incorrect. It suggests that the use of separate cables is what differentiates half-duplex from full-duplex communication. The distinction between half-duplex and full-duplex is not about the number of cables used but about whether data transmission can occur simultaneously in both directions.

**References**

**1.1.3 Network Topology**

**1.1.7 Lab: Create Network Topologies**

q_network_topo_half_vs_full_duplex_n09.question.fex

Question 53. ✓ Correct

Which command can be used on Windows to display the FQDN of the local host?

- nslookup -type=fqdn
- hostname --fqdn
- resolve-hostname
- → **ipconfig /all**

**Explanation**

On Windows, the command **ipconfig /all** is used to display detailed information about the network configuration of the host, including the FQDN (Fully Qualified Domain Name).

**hostname --fqdn** is a command used in Linux to display the FQDN of the host, not Windows.

**nslookup -type=fqdn** is not a valid command for displaying the FQDN of the local host. nslookup is used for querying DNS servers.

**resolve-hostname** is not a valid Windows command for displaying the FQDN of the local host.

**References**

**4.4.1 ipconfig**
**4.4.2 ifconfig and ip**
**4.4.5 Lab: IPv4 Troubleshooting Tools**
**4.4.6 Lab: IPv4 Troubleshooting tools for Linux**
**4.4.7 Lab: Use IPv4 Test Tools**
**6.4.6 Lab: Troubleshoot Address Pool Exhaustion**
**6.4.8 Lab: Troubleshoot IP Configuration 1**
**6.4.9 Lab: Troubleshoot IP Configuration 2**
**6.4.10 Lab: Troubleshoot IP Configuration 3**
**6.6.1 Client DNS Issues**
**6.6.2 Name Resolution Issues**

q_nslookup_local_host_fqdn_n09.question.fex

Question 54. ✓ Correct

A network engineer is troubleshooting an issue where a specific workstation cannot access network resources. Preliminary checks show that the workstation's network adapter is functioning correctly, and the cable has been tested and verified to work with another device.

The workstation is connected to port Gi1/0/24 on a switch. The engineer suspects a configuration issue on the switch port might be the root cause.

To analyze the situation, which command should the engineer use to view both the current operational status and the configuration of port Gi1/0/24?

→ ◉ **show interface Gi1/0/24**

○ **show running-config interface Gi1/0/24**

○ **show mac address-table interface Gi1/0/24**

○ **show vlan brief**

**Explanation**

The **show interface Gi1/0/24** command provides detailed information about the specific port's operational status, including line protocol status, speed, duplex settings, and any error statistics, which are crucial for diagnosing connectivity issues.

The **show mac address-table interface Gi1/0/24** command would display the MAC addresses learned by the specified interface, which helps in tracking devices but does not provide operational status or configuration details of the port.

The **show running-config interface Gi1/0/24** command would display the configuration of the specified interface as it currently exists in the running configuration. While useful, it does not provide real-time operational status.

The **show vlan brief** command would provide a summary of all VLANs and their assigned ports on the switch, which is useful for VLAN troubleshooting but does not offer detailed information about the operational status or configuration of a specific port.

**References**

**3.4.3 Switch Show Commands**

**3.4.8 Lab: Troubleshoot Disabled Ports**

q_int_config_show_interface_gil_scenario_n09.question.fex

Question 55. ✕ Incorrect

Which of the following are components of the 18-byte header in a standard Ethernet frame? (Select three.)

- → ☑ Destination MAC address
- → ☐ Error checking field
- ☐ Preamble
- ☐ Payload size indicator
- ☐ Frame sequence number
- → ☑ Source MAC address
- ☑ ~~EtherType field~~

**Explanation**

The following are components of a standard Ethernet frame header:

- Destination MAC address. The destination MAC address is a 6-byte field in the Ethernet frame header that specifies the intended recipient of the frame.
- Source MAC address. The source MAC address is a 6-byte field in the Ethernet frame header that identifies the sender of the frame.
- Error checking field. The error checking field, also known as the Frame Check Sequence (FCS), is a 4-byte field used to detect errors in the transmitted frame.

The Ethernet frame header does not include a payload size indicator. The size of the payload is determined by the MTU and is not specified in the header.

Ethernet frames do not include a sequence number in their header. Sequence numbers are used in other protocols for ordering and reliability but not in the Ethernet frame structure.

The preamble is not considered part of the Ethernet frame header. It is a sequence of bits used for synchronization and is not included in the 18-byte header calculation.

**References**

**3.3.2 Maximum Transmission Unit**

q_frame_ethernet_frame_components_n09.question.fex

Question 56. ✓ Correct

How are communications between VLANs facilitated?

- Through a network firewall
- By configuring VLANs with the same ID
- Through direct connection
- → Through an IP router or layer 3 capable switch

**Explanation**

Routing between VLANs requires an IP router or a layer 3 switch capable of understanding and processing IP packets. This is necessary to facilitate communication between different VLANs, which are otherwise isolated.

Direct connections do not facilitate communication between VLANs without routing.

Configuring VLANs with the same ID would not create separate VLANs; it would merge them into a single broadcast domain.

While firewalls can control traffic between VLANs, they do not route traffic. Routing is required for VLANs to communicate.

**References**

**5.6.2 Virtual LAN IDs and Membership**

q_vlan_id_router_or_switch_n09.question.fex

Question 57. ✓ Correct

What role does a router play in a network with multiple subnets?

- It switches frames within a subnet.
- It encrypts data for all subnets.
- → It forwards packets between subnets.
- It assigns MAC addresses to devices.

**Explanation**

A router facilitates communication between different subnets by forwarding packets based on IP addresses, acting as a gateway between broadcast domains.

Switching within a subnet is performed by Layer 2 devices, such as switches, not routers.

The primary role of a router is not to encrypt data. While routers can support encryption for secure routing, their main function is packet forwarding.

Routers do not assign MAC addresses. MAC addresses are hardware addresses assigned to network interfaces by manufacturers.

**References**

**1.2.1 Open Systems Interconnection Model**
**1.2.5 Layer 3 - Network**
**1.2.8 OSI Model Summary**
**1.3.4 Network Layer Functions**
**1.3.6 The Internet**
**1.3.7 Binary and Hexadecimal**
**1.3.8 Lab: Explore a Single Location in a Lab**
**4.1.2 Layer 2 vs. Layer 3 Addressing and Forwarding**
**13.1.1 Wide Area Networks and the OSI Model**
**14.3.5 Cloud Firewall Security**

q_addressing_router_multiple_subnets_n09.question.fex

Question 58. ✕ Incorrect

A network administrator notices that the data transfer rates between devices in a 100BASE-TX Fast Ethernet network are not reaching the expected 100 Mbps. The network uses switches, and all devices support Fast Ethernet.

What could the network administrator enable to improve the data transfer rates to the expected 100 Mbps?

- ◯ Replace switches with hubs
- → ◯ Full-duplex mode on all devices
- ◉ ~~Autonegotiation on all devices~~
- ◯ Replace all Cat 5 cables with fiber optic cables

**Explanation**

Enabling full-duplex mode on all devices allows for simultaneous transmission and reception of data, effectively allowing each node to use the full 100 Mbps bandwidth of the cable link to the switch port. This can improve data transfer rates to the expected 100 Mbps.

While autonegotiation is important for compatibility, it does not directly address the issue of not reaching the expected data transfer rates if all devices already support Fast Ethernet.

While fiber optic cables offer higher data transfer rates and longer distances, simply replacing Cat 5 cables with fiber optic cables does not address the specific issue in a 100BASE-TX Fast Ethernet network.

Replacing switches with hubs would likely degrade network performance further, as hubs do not manage collision domains as effectively as switches and do not support full-duplex transmissions.

**References**

**2.1.3 Media Access Control and Collision Domains**

**2.1.4 100BASE-TX Fast Ethernet Standards**

**3.2.5 Switch Interface Configuration**

q_fast_full-duplex_scenario_n09.question.fex

Question 59. ✓ Correct

Which IPv6 autoconfiguration method allows a host to generate a link-local address and verify its uniqueness?

- DHCPv6
- Manual configuration
- ARP
- → SLAAC

**Explanation**

Stateless Address Autoconfiguration (SLAAC) enables a host to automatically generate a link-local address and use Neighbor Discovery Protocol messages to ensure that the address is unique on the network.

DHCPv6 is used for stateful autoconfiguration, not for generating link-local addresses.

Manual configuration involves manually assigning IP addresses, not automatically generating them.

ARP is used in IPv4 for address resolution and does not apply to IPv6 link-local address generation.

**References**

**6.3.2 IPv6 Interface Autoconfiguration and Testing**

q_apipa6_slaac_definition_n09.question.fex

Question 60. ✓ Correct

Which of the following networking topologies connects each network device to a central forwarding appliance?

- Bus
- → Star
- Mesh
- Ring

**Explanation**

Star topologies connect each device on a network to a central forwarding appliance.

In ring topologies, each device connects to a neighboring device so that a ring is formed.

A bus topology connects all devices to a trunk cable.

A mesh topology exists when there are multiple paths between any two nodes on a network.

**References**

**1.1.2 Network Types**

**1.1.3 Network Topology**

**1.1.4 Star Topology**

**1.1.7 Lab: Create Network Topologies**

q_star_topo_star_03_n09.question.fex

Question 61. ✓ Correct

Which type of laser is typically used with single mode fiber transceivers?

- VCSEL
- LED
- → Laser diodes
- Incandescent bulbs

**Explanation**

Single mode fiber transceivers typically use laser diodes because they can provide the narrow beam and high power necessary for the long-distance transmission that single mode fibers support. Laser diodes are capable of transmitting data over longer distances with less signal loss compared to LEDs or VCSELs, which are more commonly used with multimode fibers.

LEDs are used with multimode fiber transceivers, not single mode, due to their wider beam and lower power.

VCSELs are also used with multimode fibers for similar reasons as LEDs, offering benefits in cost and power usage but not suited for the long distances covered by single mode fibers.

Incandescent bulbs are not used in fiber optic communications; they do not have the properties necessary for transmitting data over optical fibers.

**References**

**3.1.3 Transceiver Mismatch Issues**

q_transceiver_laser_diodes_n09.question.fex

Question 62. ✓ Correct

Kate, a network administrator, has been tasked with staying within the company budget. She has a large network and doesn't want to spend more than she needs to on purchasing and registering multiple public IP addresses for each of the hosts on her network.

Which of the following methods could help her provide internet access but also keep costs low and limit the number of registered IP addresses her organization needs to purchase?

- Use Layer 2 switches.
- Use Layer 3 switches.
- Use PoE devices.
- → Use Network Address Translation.

**Explanation**

Using NAT will allow the hosts on Kate's network to be private and to utilize just one registered public IP address.

Using Layer 2 switches will not impact the public IP address situation.

Using Layer 3 switches would only improve the public IP address situation if NAT were implemented on them.

Using PoE (Power over Ethernet) devices will not impact the public IP address situation.

**References**

**5.3.2 Network Address Translation Types**

**5.3.4 Lab: Configure NAT**

q_nat_scenario_n09.question.fex

Question 63. ✓ Correct

Which optical wavelengths are typically supported by different transceivers?

- 700 nm, 950 nm, and 1450 nm
- 650 nm, 850 nm, and 1300 nm
- 900 nm, 1200 nm, and 1600 nm
- → 850 nm, 1300 nm, and 1550 nm

**Explanation**

Transceivers are designed to work at specific optical wavelengths to match the transmission characteristics of the optical fiber they are used with. The typical wavelengths supported are 850 nm, 1300 nm, and 1550 nm. These wavelengths are chosen based on their transmission properties, including minimal loss and dispersion over fiber optic cables.

650 nm is not a typical wavelength used in standard fiber optic communications.

900 nm, 1200 nm, and 1600 nm are not standard wavelengths for fiber optic transceivers.

700 nm, 950 nm, and 1450 nm are not commonly used wavelengths in fiber optic networks.

**References**

**3.1.3 Transceiver Mismatch Issues**

q_transceiver_optical_wavelengths_n09.question.fex

Question 64. ✓ Correct

How is a connection uniquely identified in a TCP/IP network?

→ (●) By the combination of server port and IP address and client port and IP address

( ) By the client port and IP address only

( ) By the server port and IP address only

( ) By the MAC addresses of the communicating devices

**Explanation**

A connection in a TCP/IP network is uniquely identified by the combination of both the server's and client's port numbers and IP addresses, ensuring precise identification of each end of the connection.

By the server port and IP address only or the client port and IP address only are incorrect because both the server and client port and IP addresses are needed to uniquely identify a connection.

MAC addresses identify devices at the Data Link layer, not connections at the Transport layer.

**References**

**6.1.2 Transmission Control Protocol**

**6.1.3 TCP Handshake and Teardown**

**6.1.7 Lab: Explore Three-Way Handshake in Wireshark**

q_transport_connection_identification_n09.question.fex

Question 65. ✓ Correct

What is the primary purpose of trunking in a network?

- To connect a computer to the Internet
- → To interconnect multiple switches and build the network fabric
- To increase the security of the network
- To replace wireless connections with wired connections

**Explanation**

Trunking is used to connect multiple network switches together, allowing for the creation of a larger network infrastructure. This is essential in environments where a single switch cannot provide enough ports to connect all devices, thereby necessitating the use of multiple switches to form a cohesive network fabric.

Connecting a computer to the Internet is a function of routers and modems, not trunking. Trunking specifically refers to the practice of linking switches to expand the network.

Trunking does not specifically aim to replace wireless connections; it is a method used in wired networks to interconnect switches. Both wired and wireless connections have their own applications and are used based on different criteria.

While trunking can contribute to network security by segregating traffic into VLANs, its primary purpose is not security but rather the expansion and interconnection of the network infrastructure.

**References**

**5.6.3 Trunking and IEEE 802.1Q**

q_trunking_primary_purpose_n09.question.fex

Question 66. ✓ Correct

What is the default probe message type used by the **tracert** command on Windows systems?

- TCP SYN
- → ICMP Echo Request
- ARP Request
- UDP

**Explanation**

The **tracert** command on Windows systems uses ICMP Echo Request probes by default to trace the path to a target host. This method helps in identifying the route and diagnosing any issues along the path.

TCP SYN is incorrect because **tracert** does not use TCP SYN packets by default for its probes.

UDP is incorrect as this is the default probe type used by the **traceroute** command on Linux and router OSes, not **tracert** on Windows.

ARP Request is incorrect because ARP Requests are used for resolving IP addresses to MAC addresses within a local network, not for tracing the path between two nodes over the Internet or a large network.

**References**

**5.1.8 tracert and traceroute**
**5.1.10 Lab: Cisco Troubleshooting Tools**
**6.4.7 Lab: Explore DHCP Troubleshooting**
**6.4.9 Lab: Troubleshoot IP Configuration 2**
**6.4.10 Lab: Troubleshoot IP Configuration 3**
**13.3.9 Lab: Use PowerShell Remote**

q_tracert_icmp_echo_request_n09.question.fex

Question 67. ✓ Correct

What does IPv6 use to replace the Options field found in IPv4 headers?

- Hop Limit
- → Extension headers
- Flow Label
- Traffic Class

**Explanation**

In IPv6, the Options field from IPv4 headers is replaced by extension headers. These headers provide a flexible method to extend the protocol and support features like fragmentation and reassembly, security (IPSec), and source routing.

Traffic Class is used in IPv6 for QoS purposes but does not replace the Options field.

Hop Limit replaces the TTL field from IPv4, not the Options field.

Flow Label is used for identifying packet flows in IPv6 and does not replace the Options field.

**References**

**4.5.1 IPv4 vs IPv6**

q_ipv4_ipv6_option_field_replace_n09.question.fex

Question 68. ✓ Correct

What does the Time to Live (TTL) header field represent in a packet?

- ◯ The maximum time the packet can exist on the network
- ◯ The maximum distance the packet can travel
- → ◉ The maximum number of routers the packet can pass through
- ◯ The priority assigned to the packer for data transmission

**Explanation**

The maximum number of routers the packet can pass through is the correct answer. TTL effectively limits the number of hops a packet can make, preventing it from circulating indefinitely in the network.

TTL is not measured in physical distance but in hops.

While TTL stands for Time to Live, it is used as a hop count rather than a time limit.

TTL does not indicate priority; it controls the packet's lifespan in terms of hops.

**References**

**5.1.4 Packet Forwarding**

**6.5.8 DNS Server Configuration**

q_pack_forw_ttl_header_field_n09.question.fex

Question 69. ✕ Incorrect

Which command outputs the active routing table and includes details such as destination, gateway, and the source of the route?

- ip route show
- → show route
- ~~route print~~
- show arp

**Explanation**

The **show route** command is used on routers to output the active routing table, including comprehensive details such as destination, gateway, AD/metric, interface, and the source of the route, identified by letter codes.

The **route print** command is specific to Windows hosts and, while it does show the routing table, it is not the command that provides the detailed output described, especially regarding the source of the route.

The **ip route show** Linux command displays the routing table but the question specifically describes the output format typical of router commands like **show route**.

The **show arp** command is used to view the ARP cache, not the routing table, and does not provide information on destinations, gateways, or route sources.

**References**

**5.1.7 Routing Table Tools**

**5.1.10 Lab: Cisco Troubleshooting Tools**

q_route_show_route_command_n09.question.fex

Question 70. ✓ Correct

What is the primary purpose of link aggregation/NIC teaming?

- To replace wireless connections with wired connections
- To increase the cost of network infrastructure
- To decrease the network speed
- → To combine multiple network connections into a single logical connection

**Explanation**

The correct answer is to combine multiple network connections into a single logical connection. Link aggregation, also known as NIC teaming, is the process of combining two or more network connections into a single logical connection to increase bandwidth and provide redundancy.

Link aggregation/NIC teaming is used to increase the network speed by combining multiple network connections, not to decrease it.

The purpose of link aggregation/NIC teaming is to combine multiple wired network connections for increased bandwidth and redundancy, not to replace wireless connections with wired ones.

While implementing link aggregation/NIC teaming might involve some initial costs for additional hardware, its primary purpose is to enhance network performance and reliability, not to increase overall infrastructure costs.

**References**

**3.3.1 Link Aggregation and NIC Teaming**

**3.3.6 Lab: Configure Port Aggregation**

q_lag_primary_purpose_n09.question.fex

Question 71. ✓ Correct

Which layer in the three-tiered network hierarchy is responsible for providing fault-tolerant interconnections between different access blocks?

- Wireless Access Layer
- Access Layer
- Core Layer
- → Distribution Layer

**Explanation**

The distribution layer provides fault-tolerant interconnections between different access blocks and either the core or other distribution blocks. It is also used to implement traffic policies, such as routing boundaries, filtering, or quality of service (QoS).

The access layer connects end-user devices to the network.

The core layer provides a high-speed backbone for the network.

The Wireless Access Layer is not a standard layer in the three-tiered network hierarchy. The access layer includes both wired and wireless connections for end-user devices, but the "Wireless Access Layer" as a separate entity does not exist within this context.

**References**

**5.5.2 Three-Tiered Network Hierarchy**

**5.5.4 Lab: Create a Three-Tier Network**

q_3tier_distribution_layer_function_n09.question.fex

Question 72. ✓ Correct

Which of the following is a multicast frame that contains spanning tree protocol information about switch ports that allows switches to exchange information?

- Bus
- Lowest ID
- DPs
- → BPDU

**Explanation**

The spanning tree protocol (STP) information gets packaged as bridge protocol data unit (BPDU) multicast frames. Each switch then determines the shortest path to the root bridge by exchanging information with other switches.

A bus is a topology that is not part of the traditional three-tiered network. A physical bus topology with more than two nodes is a shared access topology, meaning that all nodes share the media's bandwidth.

The root bridge has two designated ports (DP) connected to Bridge A and Bridge B. There are also root ports (RP) connected back to the interfaces on the root bridge.

The switch with the lowest ID, comprising a priority value and the MAC address, will be selected as the root.

**References**

**3.3.3 Spanning Tree Protocol**

**3.3.4 Spanning Tree Protocol Configuration**

q_stp_bpdu_description_n09.question.fex

Question 73. ✓ Correct

What is the role of Router Advertisements (RAs) in the IPv6 address configuration process?

→ ◉ To inform hosts of network prefixes and autoconfiguration options

○ To request an IP address from a DHCPv6 server

○ To assign static IP addresses to devices

○ To encrypt data packets sent between hosts and routers

**Explanation**

Router Advertisements (RAs) are sent by routers to inform hosts on the network about available network prefixes and autoconfiguration options (stateless or stateful). This information is crucial for hosts to configure their IPv6 addresses properly.

RAs do not request IP addresses; they provide information necessary for address configuration.

RAs are not involved in encrypting data packets; they are used for network configuration.

RAs do not assign static IP addresses; they provide information for automatic configuration.

**References**

**4.5.5 IPv6 Link Local Addressing**

**6.3.1 Automatic Private IP Addressing**

**6.3.4 Lab: Explore APIPA Addressing**

**6.3.5 Lab: Explore APIPA Addressing in Network Modeler**

**6.3.6 Set Up Alternate Addressing**

q_apipa6_ra_role_n09.question.fex

Question 74. ✓ Correct

What is the main advantage of using VLSM over traditional fixed-length subnet masking?

- It allows for the use of the same subnet mask throughout the network.
- → It reduces the number of wasted IP addresses.
- It simplifies the routing table.
- It increases the total number of available IP addresses.

**Explanation**

The main advantage of VLSM is its ability to reduce IP address wastage by allowing subnets of different sizes within the same network. This flexibility ensures that each subnet gets just the right amount of IP addresses, minimizing unused addresses.

VLSM can actually increase the complexity of the routing table due to the presence of subnets with different masks.

VLSM, by definition, allows for different subnet masks to be used within the same network, not the same one.

VLSM does not increase the total number of available IP addresses; it just allocates them more efficiently.

**References**

**4.3.1 Classful Addressing**

**4.3.6 Variable Length Subnet Masks**

q_vlsm_main_advantage_n09.question.fex

Question 75. ✓ Correct

What is the maximum size of the data payload in a standard Ethernet frame?

- ○ 1518 bytes
- → ◉ 1500 bytes
- ○ 9018 bytes
- ○ 18 bytes

**Explanation**

The maximum size of the data payload in a standard Ethernet frame is 1500 bytes. This is referred to as the maximum transmission unit (MTU) for Ethernet.

The other answers are incorrect because 1518 bytes is the total length of a standard Ethernet frame excluding the preamble, 9018 bytes is a possible size for a jumbo frame's data payload, and 18 bytes is the size of the Ethernet frame header.

**References**

**3.3.2 Maximum Transmission Unit**

q_frame_data_payload_size_n09.question.fex

Question 76. ✓ Correct

Multi-mode fiber is designed to operate at which of the following wavelengths?

→ ◉ 850 nm and 1300 nm

○ 850 nm and 1310 nm

○ 1300 nm and 1550 nm

○ 1310 nm and 1550 nm

**Explanation**

Multi-mode fiber is designed to operate at 850 nm and 1300 nm.

Single-mode fiber is optimized for 1310 nm and 1550 nm.

**References**

**2.1.6 Fiber Ethernet Standards**

**2.4.2 Single Mode Fiber and Multimode Fiber**

q_fiber_cables_multi_n09.question.fex

Question 77. ✓ Correct

What distinguishes a collision domain from a broadcast domain?

- Collision domains are established by routers, while broadcast domains are established by switches.
- → Collision domains are about physically shared media, and their borders are established by bridges and switches.
- Collision domains can span multiple routers, while broadcast domains are limited to a single switch.
- Broadcast domains require a layer 2 broadcast address to be established.

**Explanation**

Collision domains refer to network segments where data packets can collide due to shared media access. Bridges and switches segment networks into separate collision domains by providing dedicated paths for data packets, thus reducing collisions. Broadcast domains, on the other hand, are defined by routers at layer 3 and determine the reach of broadcast traffic within a network.

Collision domains are not established by routers; they are segmented by bridges and switches. Broadcast domains are defined by routers, not switches.

While broadcast domains involve layer 3 devices and protocols, the requirement for a layer 2 broadcast address is not what distinguishes them from collision domains.

Collision domains are segmented by bridges and switches, not routers, and do not span multiple routers. Broadcast domains can span multiple switches and are limited by routers.

**References**

**1.3.3 Data Link Layer Functions**
**3.2.1 Hubs**
**3.2.3 Switches**
**3.2.4 Ethernet Switch Types**
**3.2.5 Switch Interface Configuration**
**3.2.7 Lab: Install a Switch in the Rack**
**3.2.8 Lab: Secure a Switch**

q_bridges_collision_vs_broadcast_n09.question.fex

Question 78. ✓ Correct

How can you identify machines with duplicate IP addresses?

- By restarting the router
- → Using **ping** and then **arp -a** to examine the ARP cache table
- Checking the physical connections of all network devices
- Assigning new IP addresses to all devices on the network

**Explanation**

To identify machines with duplicate IP addresses, you can use the **ping** command to communicate with the IP address in question and then use **arp -a** to examine the ARP (Address Resolution Protocol) cache table. This method helps in identifying the MAC addresses of the interfaces that are contending for the same IP address.

Restarting the router will not specifically help in identifying machines with duplicate IP addresses.

Assigning new IP addresses to all devices is a broad approach and does not directly identify which devices had the duplicate IP addresses.

Checking the physical connections of network devices does not provide information about IP address conflicts.

**References**

**4.6.2 Duplicate IP and MAC Address Issues**

q_ip_duplicate_arp_a_n09.question.fex

Question 79. ✓ Correct

Which statement BEST describes the use of port numbers in TCP/IP networking?

- Port numbers are used to identify the physical location of devices on a network.
- Port numbers are used exclusively for encrypting network communications.
- Port numbers are optional and rarely used in modern networking.
- → Port numbers are used in conjunction with IP addresses to direct packets to specific services or applications.

**Explanation**

Port numbers, when used with IP addresses, play a crucial role in ensuring that data packets are directed to the correct service or application on a host, facilitating the multiplexing of network communications.

Port numbers are essential for identifying services and applications in TCP/IP networking.

Port numbers do not identify physical locations but logical endpoints.

Port numbers are not used for encryption but for directing traffic to specific services or applications.

**References**

**6.1.2 Transmission Control Protocol**

**6.1.3 TCP Handshake and Teardown**

**6.1.7 Lab: Explore Three-Way Handshake in Wireshark**

q_transport_port_number_use_n09.question.fex

Question 80. ✓ Correct

What is the primary purpose of a network mask (netmask) in IPv4 addressing?

- To increase the speed of network packet delivery
- To encrypt the IP address for security purposes
- → To distinguish between the network ID and the host ID within an IP address
- To identify the device's hardware address

**Explanation**

A network mask is crucial for identifying which part of an IP address refers to the network and which part refers to the specific host within that network. This separation is essential for routing and addressing within IP networks.

A netmask does not identify a device's hardware address; that's the role of a MAC address.

Netmasks are not used for encryption or security purposes; they are used for IP address segmentation.

The speed of network packet delivery is influenced by various factors, but the primary purpose of a netmask is not to increase this speed.

**References**

**4.2.2 Network Masks**

q_netmask_primary_purpose_n09.question.fex

Question 81. ✓ Correct

For a rack containing equipment that draws 2000 watts in total on a 240 VAC circuit, what is the amperage?

→ ◉ 8.3 Amps

○ 4.2 Amps

○ 16.6 Amps

○ 12.5 Amps

**Explanation**

Using the formula for calculating amperage (Amps = Watts / Voltage), if a rack's equipment draws 2000 watts on a 240 VAC circuit, the amperage would be 2000 / 240 = 8.3 Amps. This calculation is essential for ensuring that the circuit can handle the load without being overloaded.

16.6 Amps is incorrect because this would imply a total wattage of 4000 watts on a 240 VAC circuit, not 2000 watts.

4.2 Amps is incorrect because this would suggest a much lower total wattage or a higher voltage than 240 VAC.

12.5 Amps is incorrect because this would indicate a total wattage of 3000 watts on a 240 VAC circuit, which is not the case here.

**References**

**2.5.3 Power Management**

q_power_amperage_example_n09.question.fex

Question 82. ✓ Correct

What is the role of the Gateway/next hop parameter in a routing table?

- It determines the speed at which the packet is forwarded.
- It specifies the final destination of the packet.
- It identifies the router's physical location.
- → It indicates the next router or gateway along the path to the destination.

**Explanation**

The Gateway/next hop parameter is crucial for indicating the immediate next stop (router or gateway) a packet should be forwarded to on its journey towards the final destination. It helps in making hop-by-hop decisions to efficiently route the packet.

The final destination of the packet is determined by the Destination parameter, not the Gateway/next hop, which only indicates the next immediate stop.

The Gateway/next hop parameter does not provide information about the physical location of routers; it simply points to the next device in the path.

The forwarding speed of packets is influenced by the network's bandwidth and the router's processing capabilities, not the Gateway/next hop parameter.

**References**

**1.3.1 SOHO Routers**
**1.3.2 Physical Layer Functions**
**1.3.3 Data Link Layer Functions**
**1.3.4 Network Layer Functions**
**1.3.5 Transport and Application Layer and Security Functions**
**1.3.6 The Internet**
**1.3.9 Lab: Create a Home Wireless Network**
**1.3.10 Lab: Create a SOHO Network**
**5.1.1 Routing Tables and Path Selection**
**5.1.4 Packet Forwarding**
**5.1.5 Fragmentation**

**5.1.6 Router Configuration**

**5.1.9 Lab: Install an Enterprise Router**

**10.5.9 Lab: Restrict Telnet and SSH Access**

**10.5.10 Lab: Permit Traffic**

**10.5.11 Lab: Block Source Hosts**

q_route_table_gateway_parameter_n09.question.fex

Question 83. ✓ Correct

You are troubleshooting a connectivity problem on a Linux server. You're able to connect to another system on the local network but not to a server on a remote network.

You suspect that the default gateway information for the system may be configured incorrectly.

Which of the following would you use to view the default gateway information on the Linux server?

- Telnet
- **ipconfig**
- **dig**
- → **ifconfig**

**Explanation**

Use the **ifconfig** command on systems running Linux to view information on the TCP/IP configuration for network adapters.

Use **ipconfig** to view network configuration information on Windows systems.

Use the **dig** command on Linux and Unix systems to query Domain Name Service (DNS) servers.

Telnet is a remote console that allows access to devices within a network.

**References**

- **4.4.1 ipconfig**
- **4.4.2 ifconfig and ip**
- **4.4.5 Lab: IPv4 Troubleshooting Tools**
- **4.4.6 Lab: IPv4 Troubleshooting tools for Linux**
- **4.4.7 Lab: Use IPv4 Test Tools**
- **6.4.6 Lab: Troubleshoot Address Pool Exhaustion**
- **6.4.8 Lab: Troubleshoot IP Configuration 1**
- **6.4.9 Lab: Troubleshoot IP Configuration 2**
- **6.4.10 Lab: Troubleshoot IP Configuration 3**

**6.6.1 Client DNS Issues**

**6.6.2 Name Resolution Issues**

q_ifconfig_troubleshoot_n09.question.fex

Question 84.

Incorrect

What is the primary difference between tagged and untagged ports regarding VLAN tags?

- Tagged ports strip VLAN tags from incoming frames.
- Untagged ports can transport traffic for multiple VLANs.
- ~~Tagged ports add a VLAN tag to all outgoing frames.~~
- → Untagged ports do not add or remove VLAN tags from frames within the same VLAN.

**Explanation**

Untagged ports, being configured for a single VLAN, do not need to add or remove VLAN tags when forwarding traffic within the same VLAN. The traffic is inherently part of that VLAN.

Tagged ports add a VLAN tag only when necessary, such as when forwarding traffic over a trunk link.

Untagged ports are designed for a single VLAN, not multiple VLANs.

Tagged ports do not strip VLAN tags from incoming frames; they forward frames with the tags to appropriate VLANs.

**References**

**5.6.4 Tagged and Untagged Ports**

q_tagged_vs_untagged_ports_n09.question.fex

Question 85. ✓ Correct

What is the primary purpose of twisting the pairs in an unshielded twisted pair (UTP) cable?

→ ◉ To reduce external interference and crosstalk

○ To increase the cable's thickness

○ To color-code the cable for easier identification

○ To make the cable more flexible

**Explanation**

The pairs in a UTP cable are twisted at different rates to reduce external interference from electromagnetic sources and crosstalk, which is interference from adjacent pairs within the same cable.

Twisting the pairs does not primarily aim to make the cable more flexible. Flexibility is more related to the type of conductor (solid or stranded) used in the cable.

The twisting of pairs does not increase the cable's thickness. The thickness is determined by the gauge of the wire used.

While the pairs are color-coded for identification, the primary reason for twisting them is not for color-coding but to reduce interference and crosstalk.

**References**

**2.2.1 Unshielded Twisted Pair Cable**

**2.2.2 Shielded and Screened Twisted Pair Cable**

q_twisted_pair_primary_purpose_n09.question.fex

Question 86. ✓ Correct

Which cable category is recommended by TIA/EIA for use in healthcare facilities?

- Cat 5e
- → Cat 6A
- Cat 7
- Cat 6

**Explanation**

TIA/EIA standards recommend Cat 6A for use in healthcare facilities due to its ability to support 10 Gbps over 100 meters and its suitability for Power over Ethernet (PoE) 802.3bt installations, which are common in healthcare settings for devices like VoIP phones and wireless access points.

While Cat 5e supports Gigabit Ethernet, it's not recommended for environments requiring high-speed data transfer and PoE capabilities like healthcare facilities.

Although Cat 6 can support 10 Gbps, it's limited to 55 meters and not specifically recommended for healthcare facilities.

Despite the high performance of Cat 7, it's not recognized by TIA/EIA and thus not specifically recommended for healthcare facilities.

**References**

**2.6.3 Cable Category Issues**

q_cable_category_cat_6a_healthcare_n09.question.fex

Question 87. ✓ Correct

What is the primary purpose of a wire map tester?

→ ◉ To detect improper termination issues

○ To measure the length of a cable

○ To identify the type of cable used

○ To increase the signal strength in a cable

**Explanation**

A wire map tester is specifically designed to detect improper termination issues by checking for continuity, shorts, and incorrect pin-outs/terminations, making it an essential tool for ensuring cable integrity.

While some advanced cable testers can measure cable length, the primary function of a basic wire map tester is not to measure length but to detect wiring and termination issues.

A wire map tester does not have the capability to increase signal strength. Its purpose is to test the physical wiring and termination of cables, not to enhance signal transmission.

Identifying the type of cable used is not a function of a wire map tester. This device focuses on detecting wiring and termination problems, not on identifying cable materials or categories.

**References**

**2.6.4 Cable Testers**

**2.6.5 Wire Map Testers and Tone Generators**

q_wire_map_primary_purpose_n09.question.fex

Question 88.

Incorrect

Which of the following is a valid IPv6 address compression?

- 2001:db8:0000:0000:0abc:0000:def0:1234
- ~~2001:db8::abc::def0:1234~~
- → 2001:db8::abc:0:def0:1234
- 2001:db8:0abc::def0:1234

**Explanation**

The 2001:db8::abc:0:def0:1234 address correctly uses the double colon (::) to compress consecutive 16-bit blocks of zeros only once, adhering to the rules of IPv6 address notation.

2001:db8::abc::def0:1234 is incorrect because it uses double colon compression more than once, which violates the rule that it can only be used once to avoid ambiguity.

2001:db8:0000:0000:0abc:0000:def0:1234 is incorrect in this context because it is fully expanded and does not demonstrate compression.

2001:db8:0abc::def0:1234 is incorrect because it suggests an incorrect structure by misplacing the compression, potentially leading to confusion about the original address structure.

**References**

**4.5.2 IPv6 Address Format**

q_ipv6_format_valid_compression_n09.question.fex

Question 89. ✓ Correct

What happens when VLANs are configured on a switch?

- The switch's performance is significantly reduced.
- The switch can only support legacy network cards.
- → The switch divides the network into multiple broadcast domains.
- The switch operates in half-duplex mode.

**Explanation**

When VLANs (Virtual Local Area Networks) are configured on a switch, it divides the network into multiple broadcast domains. This allows for better traffic management and increases network security by segregating different parts of the network at the data link layer. VLANs do not cause the switch to operate in half-duplex mode, support only legacy network cards, or significantly reduce the switch's performance.

Configuring VLANs on a switch does not affect its duplex mode. Duplex mode (full or half) is determined by the capability of the switch port and the connected device, not by VLAN configuration.

The ability of a switch to support legacy network cards is not influenced by VLAN configuration. Switches can support a variety of devices, including modern and legacy ones, regardless of VLAN settings.

Configuring VLANs does not inherently reduce a switch's performance. In fact, by segmenting a network into VLANs, traffic can be more efficiently managed, potentially improving overall network performance by reducing unnecessary broadcast traffic.

**References**

**1.3.3 Data Link Layer Functions**
**3.2.1 Hubs**
**3.2.3 Switches**
**3.2.4 Ethernet Switch Types**
**3.2.5 Switch Interface Configuration**
**3.2.7 Lab: Install a Switch in the Rack**
**3.2.8 Lab: Secure a Switch**

q_switches_vlans_n09.question.fex

Question 90. ✓ Correct

A network administrator wants to use a subnet mask containing 62 usable addresses.

Which of the following subnet masks should the administrator use?

- 255.255.255.224
- 255.255.255.240
- → 255.255.255.192
- 255.255.255.128

**Explanation**

A subnet mask of 255.255.255.192 has 62 usable addresses. Subnet addressing has three hierarchical levels: a network ID, subnet ID, and host ID.

A subnet mask of 255.255.255.240 has 16 addresses. To create logical subnets, the network administrator must allocate the bits from the host portion of the IP address as a subnetwork address, rather than part of the host ID.

A subnet mask of 255.255.255.224 has 32 addresses. The mask will always have one of these values in the least significant octet: 128, 192, 224, 240, 248, 252, 254, 255.

A subnet mask of 255.255.255.128 has 128 addresses. It is important to understand that only one mask is ever applied to the IP address on each interface.

**References**

**4.2.2 Network Masks**

q_netmask_62_addresses_n09.question.fex