# Cisco

(200-301)

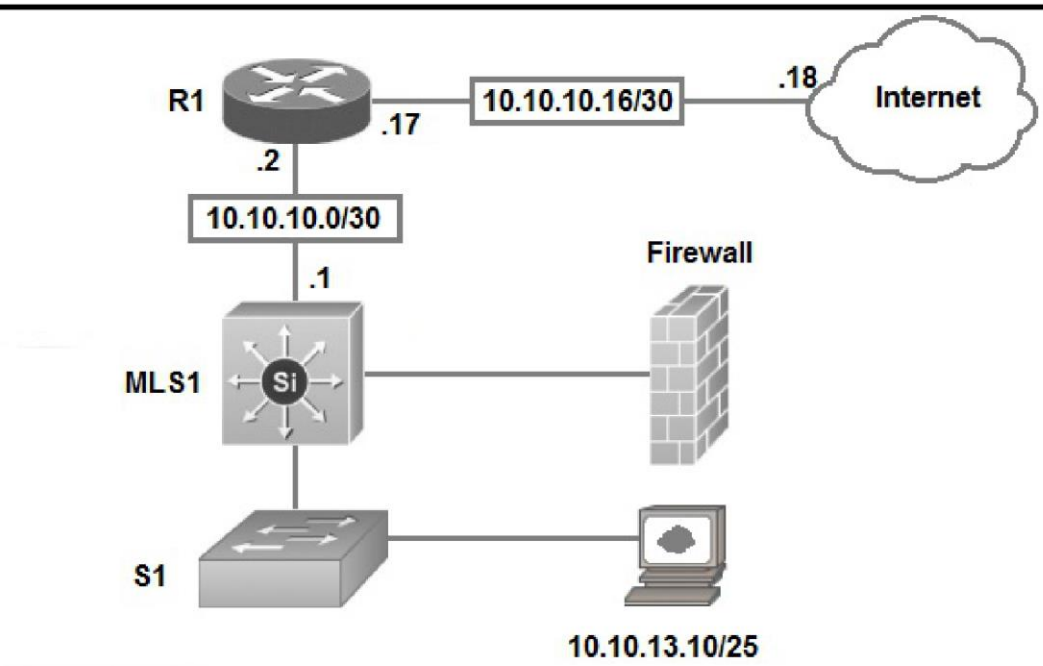
Cisco Certified Network Associate (CCNA)



Total: **1401 Questions**

Link:

**Question: 1**




```
R1#sh ip ro
Gateway of last resort is 10.10.10.18 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
C       10.10.10.0/30 is directly connected, FastEthernet0/1
O       10.10.13.0/25 [110/6576] via 10.10.10.1, 06:58:21, FastEthernet0/1
C       10.10.10.16/30 is directly connected, FastEthernet0/24
O       10.10.13.144/28 [110/110] via 10.10.10.1, 06:58:21, FastEthernet0/1
B*   0.0.0.0/0 [20/0] via 10.10.10.18, 01:17:58
```

Refer to the exhibit. Which type of route does R1 use to reach host 10.10.13.10/32?

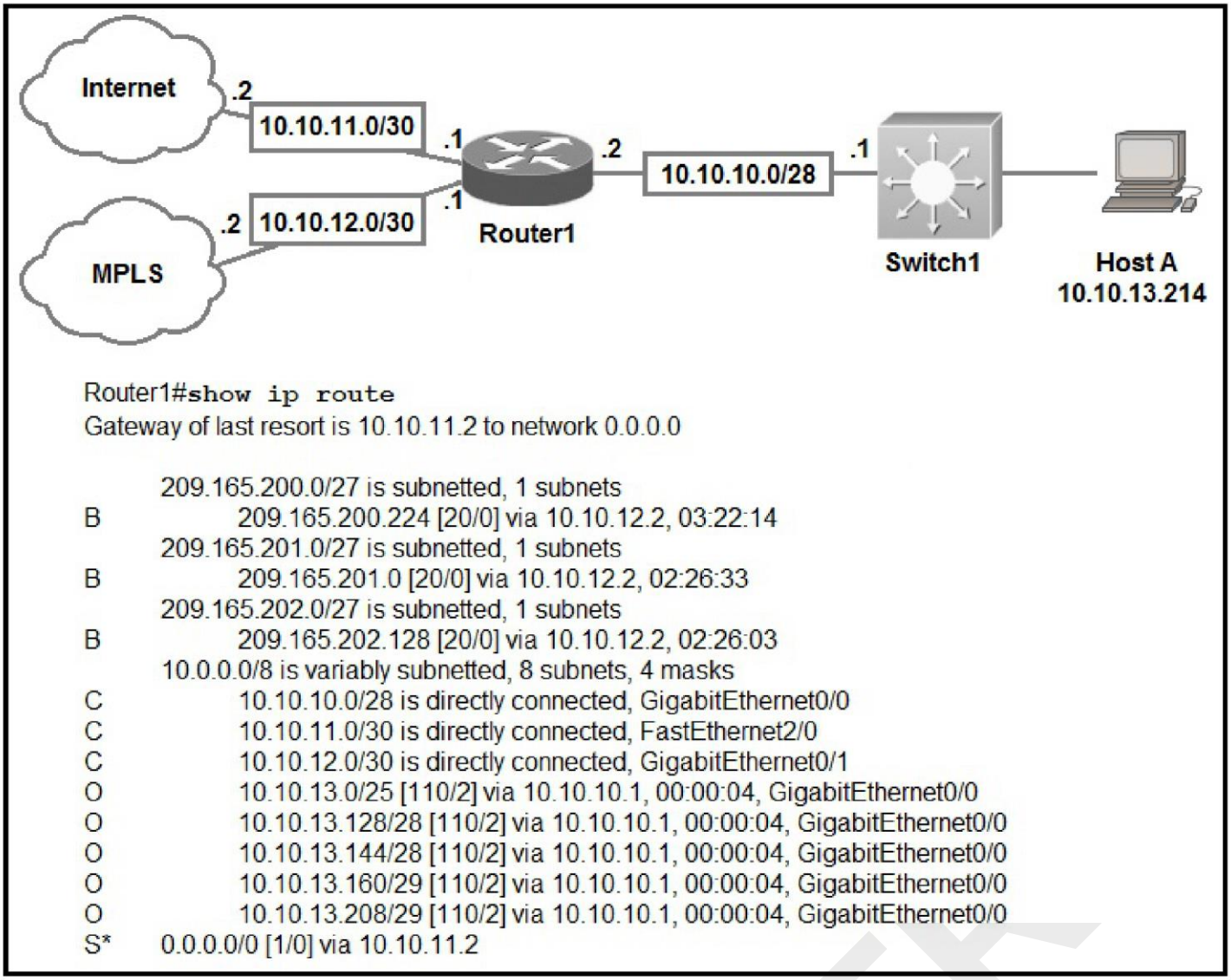
A. default route
B. network route
C. host route
D. floating static route

**Answer: B**

**Explanation:**

The host - 10.10.13.10 is in the host range of 10.10.13.0/25. This subnet is a learned route, a learned 'network' route

**Question: 2**




```
Router1#show ip route
Gateway of last resort is 10.10.11.2 to network 0.0.0.0

      209.165.200.0/27 is subnetted, 1 subnets
B        209.165.200.224 [20/0] via 10.10.12.2, 03:22:14
      209.165.201.0/27 is subnetted, 1 subnets
B        209.165.201.0 [20/0] via 10.10.12.2, 02:26:33
      209.165.202.0/27 is subnetted, 1 subnets
B        209.165.202.128 [20/0] via 10.10.12.2, 02:26:03
      10.0.0.0/8 is variably subnetted, 8 subnets, 4 masks
C        10.10.10.0/28 is directly connected, GigabitEthernet0/0
C        10.10.11.0/30 is directly connected, FastEthernet2/0
C        10.10.12.0/30 is directly connected, GigabitEthernet0/1
O        10.10.13.0/25 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
O        10.10.13.128/28 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
O        10.10.13.144/28 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
O        10.10.13.160/29 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
O        10.10.13.208/29 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
S*    0.0.0.0/0 [1/0] via 10.10.11.2
```

Refer to the exhibit. Which prefix does Router1 use for traffic to Host A?

A. 10.10.10.0/28
B. 10.10.13.0/25
C. 10.10.13.144/28
D. 10.10.13.208/29

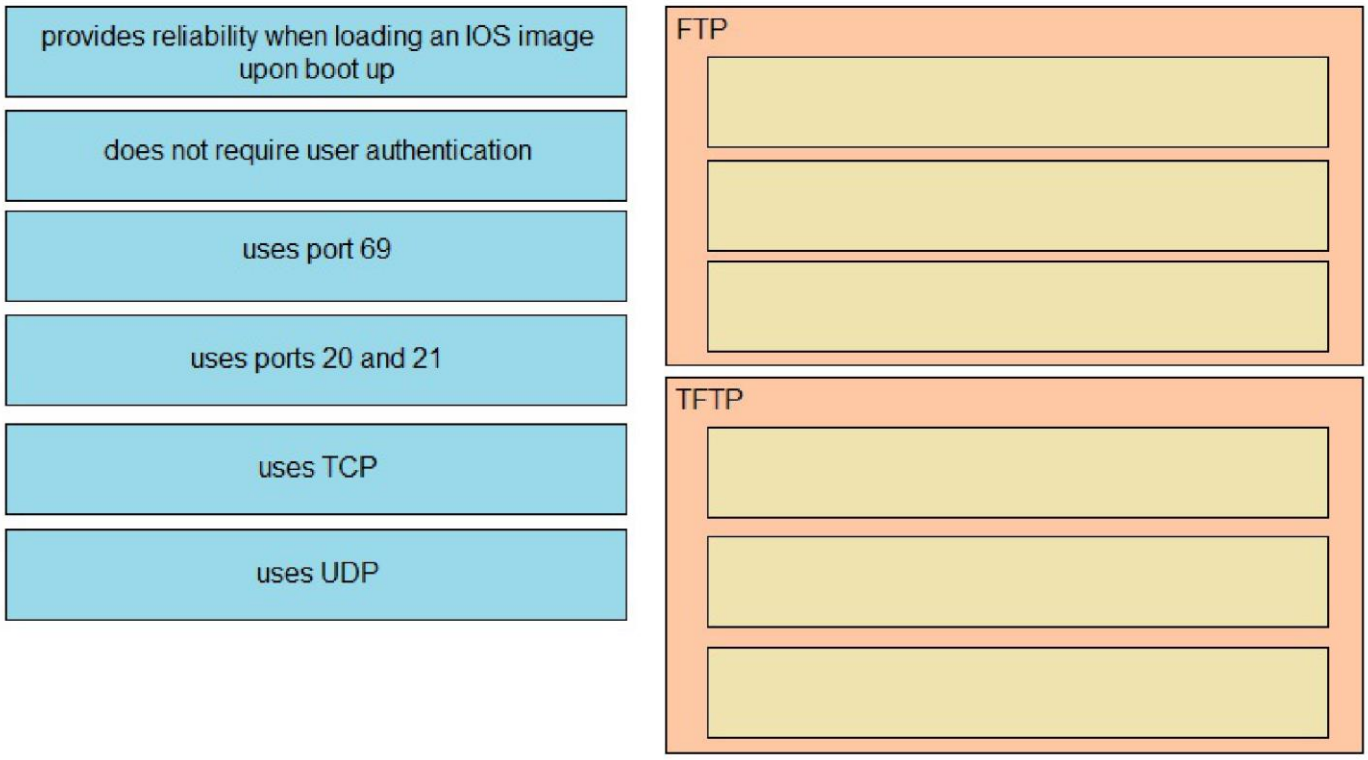
**Answer: D**

**Explanation:**
The prefix with longest prefix will be matched first, in this case is /29.

**Question: 3**

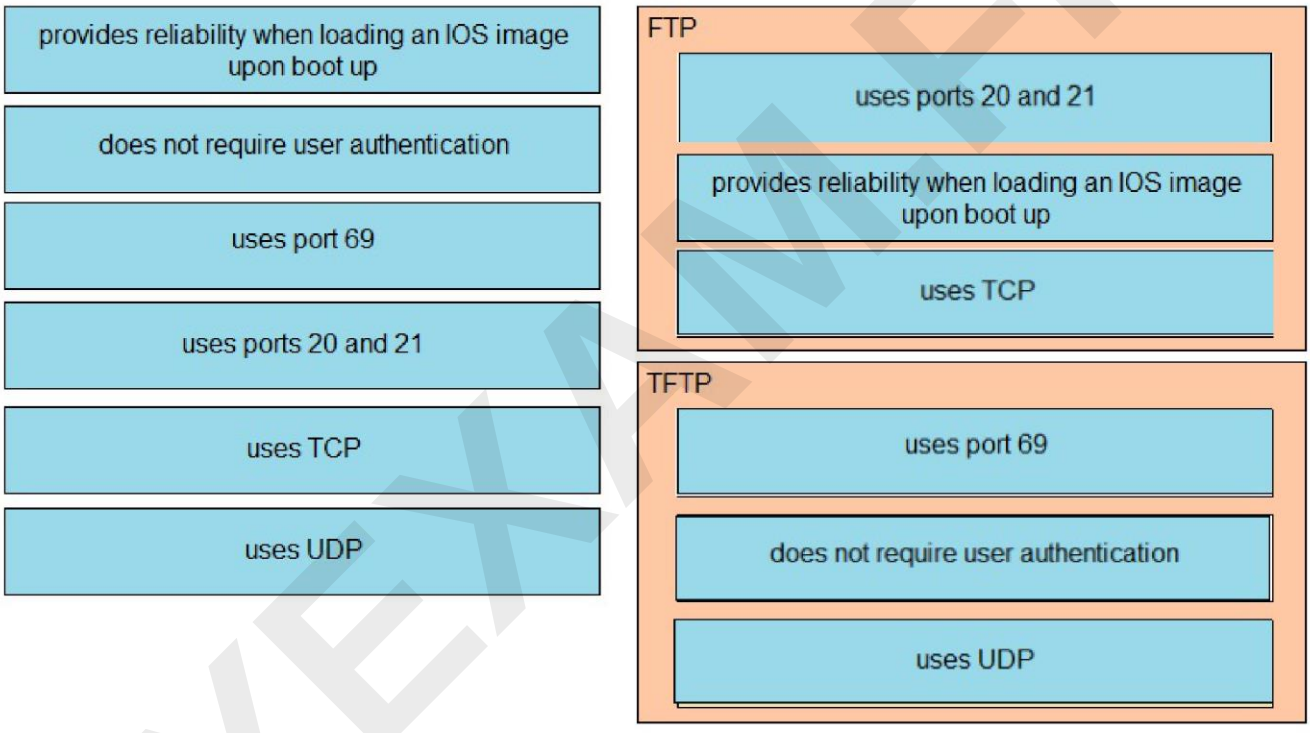
DRAG DROP -
Drag and drop the descriptions of file-transfer protocols from the left onto the correct protocols on the right.
Select and Place:

**Answer Area**




**Answer:**

**Answer Area**






**Question: 4**

A frame that enters a switch fails the Frame Check Sequence. Which two interface counters are incremented?

(Choose two.)

A. input errors
B. frame
C. giants
D. CRC
E. runts

**Answer: AD**

**Explanation:**

Here's the justification for why options A (input errors) and D (CRC) are the correct counters incremented when a frame fails the Frame Check Sequence (FCS) on a switch:

A Frame Check Sequence (FCS) is a critical part of data link layer protocols like Ethernet, used to detect errors that may have occurred during frame transmission. When a frame arrives at a switch, the switch recalculates the FCS based on the received data and compares it to the FCS field within the frame. If these values don't match, it means the frame was corrupted during transit.

The "input errors" counter is a general counter that tracks any errors encountered when receiving a frame on an interface. A failed FCS check falls squarely under this category of input-related errors. Essentially, the switch detected that it did not get the data as it should have.

The specific "CRC" counter directly records the number of frames that failed the Cyclic Redundancy Check, which is the actual algorithm used to generate the FCS. This provides a more specific indicator of FCS-related errors than just 'input errors'. Therefore, this counter will also be incremented when a frame fails the FCS test.

Counters like "frame" would usually track total frames received, not errors. "Giants" are frames exceeding the maximum allowed size, and "runts" are frames that are too small, so neither are relevant to FCS failures. Therefore, only "input errors" and "CRC" are relevant for the given scenario.

Essentially, a corrupted frame triggers the increase of both 'input error' and the more specific 'CRC' counter.

Further research:

1. **Cisco's documentation on interface counters:**https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-i1.html - This link leads to Cisco's documentation on interface counters and will allow you to explore detailed explanations of what each counter measures.
2. **Wikipedia - Frame Check Sequence:**https://en.wikipedia.org/wiki/Frame_check_sequence - This provides a good overview of what the Frame Check Sequence is used for and how it functions. 3.

**Understanding Ethernet CRC errors:**https://community.fs.com/blog/understanding-ethernet-crc-errors.html - This link offers a good overview of CRC errors in the context of Ethernet networks.

## Question: 5

DRAG DROP -
Drag and drop the IPv4 network subnets from the left onto the correct usable host ranges on the right.
Select and Place:

**Answer Area**

| | |
|---|---|
| 172.28.228.144/18 | 172.28.228.1 - 172.28.229.254 |
| 172.28.228.144/21 | 172.28.224.1 - 172.28.231.254 |
| 172.28.228.144/23 | 172.28.228.129 - 172.28.228.254 |
| 172.28.228.144/25 | 172.28.228.145 - 172.28.228.150 |
| 172.28.228.144/29 | 172.28.192.1 - 172.28.255.254 |

**Answer:**

**Answer Area**

| | |
|---|---|
| 172.28.228.144/18 | 172.28.228.144/23 |
| 172.28.228.144/21 | 172.28.228.144/21 |
| 172.28.228.144/23 | 172.28.228.144/25 |
| 172.28.228.144/25 | 172.28.228.144/29 |
| 172.28.228.144/29 | 172.28.228.144/18 |

**Explanation:**
This subnet question requires us to grasp how to subnet very well. To quickly find out the subnet range, we have to find out the increment and the network address of each subnet. Let's take an example with the subnet 172.28.228.144/18: From the /18 (= 1100 0000 in the 3rd octet), we find out the increment is 64. Therefore the network address of this subnet must be the greatest multiple of the increment but not greater than the value in the 3rd octet (228). We can find out the 3rd octet of the network address is 192 (because 192 = 64 * 3 and 192 < 228) -> The network address is 172.28.192.0. So the first usable host should be 172.28.192.1 and it matches with the 5th answer on the right. In this case we don't need to calculate the broadcast address because we found the correct answer.

Let's take another example with subnet 172.28.228.144/23 -> The increment is 2 (as /23 = 1111 1110 in 3rd octet) -> The 3rd octet of the network address is 228
(because 228 is the multiply of 2 and equal to the 3rd octet) -> The network address is 172.28.228.0 -> The first usable host is 172.28.228.1. It is not necessary but if we want to find out the broadcast address of this subnet, we can find out the next network address, which is 172.28.(228 + the increment number).0 or 172.28.230.0 then reduce 1 bit -> 172.28.229.255 is the broadcast address of our subnet. Therefore the last

usable host is 172.28.229.254.

**Question: 6**

How do TCP and UDP differ in the way that they establish a connection between two endpoints?

A. TCP uses the three-way handshake, and UDP does not guarantee message delivery.
B. TCP uses synchronization packets, and UDP uses acknowledgment packets.
C. UDP provides reliable message transfer, and TCP is a connectionless protocol.
D. UDP uses SYN, SYN ACK, and FIN bits in the frame header while TCP uses SYN, SYN ACK, and ACK bits.

**Answer: A**

**Explanation:**

The correct answer is A: TCP uses the three-way handshake, and UDP does not guarantee message delivery.

TCP (Transmission Control Protocol) is a connection-oriented protocol. Before data transfer begins, TCP establishes a reliable connection using a three-way handshake. This process involves the sender sending a SYN (synchronization) packet, the receiver responding with a SYN-ACK (synchronization-acknowledgment) packet, and the sender completing the handshake with an ACK (acknowledgment) packet. This handshake ensures both sides are ready to exchange data and establishes sequence numbers and window sizes for reliable data flow. UDP (User Datagram Protocol), on the other hand, is a connectionless protocol. It does not use any handshake mechanism. UDP simply sends data packets without establishing a connection or guaranteeing delivery, ordering, or avoiding duplicates. This makes it faster but also less reliable than TCP.

Option B incorrectly states that UDP uses acknowledgment packets. While TCP employs acknowledgments for reliability, UDP does not. Option C reverses the roles of UDP and TCP in terms of reliability and connection-orientation. Option D mixes up TCP and UDP headers incorrectly; both utilize SYN flags, but TCP uses ACK, and neither uses FIN flags in this initial connection phase. Hence, option A is the only accurate comparison.

The three-way handshake is pivotal for TCP's reliable, ordered data delivery, which differentiates it fundamentally from UDP's connectionless, best-effort approach.

For further reading on TCP and UDP:

1. **Cisco's Official CCNA Study Guide:**https://www.ciscopress.com/store/ccna-200-301-official-cert-guide-library-9780136895770 (Search for TCP/UDP topics)
2. **Cloudflare's Learning Center:**https://www.cloudflare.com/learning/ddos/glossary/tcp-handshake/ (Specifically on the TCP handshake)
3. **Wikipedia:**https://en.wikipedia.org/wiki/Transmission_Control_Protocol and https://en.wikipedia.org/wiki/User_Datagram_Protocol (General overview of both protocols).

**Question: 7**

Which 802.11 frame type is Association Response?

A. management
B. protected frame
C. action
D. control

**Answer: A**

**Explanation:**

The correct answer is **A. management**.

802.11 frames are categorized into three main types: management, control, and data. Management frames are responsible for the establishment and maintenance of communication between wireless devices and access points (APs). The Association Response frame, specifically, is a subtype of a management frame. It is sent by an access point to a wireless client in response to an Association Request frame from the client. This response signifies whether the AP has accepted or rejected the client's request to join the wireless network. Key functions of Association Response include communication of association ID, capabilities supported, and other information that is necessary for the client to establish a connection. Control frames assist in medium access control, such as RTS/CTS, ACKs and power save mode handling. Action frames are a subtype of management frames used for extended capabilities like radio measurements. Protected frames aren't a frame type but rather an indication of frame encryption. Therefore, the Association Response frame falls squarely within the domain of management frames, making option A the accurate choice.

For deeper understanding, refer to the following resources:

**IEEE 802.11 Standard:** The official standard detailing all aspects of 802.11. (IEEE Standards Association: https://standards.ieee.org/ieee/802/11/)
**Cisco's Documentation on Wireless LAN:** Cisco provides comprehensive information on 802.11 and its associated protocols. (Cisco: https://www.cisco.com/c/en/us/solutions/wireless/index.html ) - Search for 802.11 frame types specifically.
**Wireshark Documentation on 802.11:** Provides details on frame structure and dissection. (Wireshark: https://www.wireshark.org/docs/dfref/) - search for 802.11 frames.

## Question: 8

In which way does a spine-and-leaf architecture allow for scalability in a network when additional access ports are required?

A.A spine switch and a leaf switch can be added with redundant connections between them.
B.A spine switch can be added with at least 40 GB uplinks.
C.A leaf switch can be added with connections to every spine switch.
D.A leaf switch can be added with a single connection to a core spine switch.

**Answer: C**

**Explanation:**

The correct answer is C, which states: "A leaf switch can be added with connections to every spine switch." This accurately describes the horizontal scalability mechanism inherent in a spine-and-leaf architecture. In this design, leaf switches connect directly to end devices (servers, clients, etc.) and provide access ports. When more access ports are needed, simply adding another leaf switch and connecting it to every existing spine switch maintains non-blocking bandwidth across the network.

This design avoids the limitations of traditional hierarchical networks where adding more switches can introduce bottlenecks. Each leaf switch has a direct path to every other leaf switch through the spine layer. By connecting each new leaf to every spine, you ensure that traffic from that new leaf can be routed through all available spine resources, optimizing throughput and preventing any single point of congestion. Adding new leaf switches in this manner does not require changes to the existing network topology beyond the new connections, thus enhancing scalability and reducing complexity. Options A, B, and D offer limited approaches and lack the key scalability element seen in option C. The "every spine" connection is fundamental for maintaining a consistent, scalable and predictable network performance.

Here are some authoritative links for further research:

1. **Cisco's Explanation of Spine-Leaf Architecture:**https://www.cisco.com/c/en/us/solutions/data-center-virtualization/what-is-spine-leaf-architecture.html
2. **Arista Networks' Explanation of Spine-Leaf:**https://www.arista.com/en/solutions/data-center-networking/spine-leaf-architecture
3. **Juniper Networks' Explanation of Spine-Leaf:**https://www.juniper.net/us/en/research-library/webinars/transforming-data-center-networking-spine-leaf-architecture.html

## Question: 9

What identifies the functionality of virtual machines?

A. The hypervisor communicates on Layer 3 without the need for additional resources.
B. Each hypervisor supports a single virtual machine and a single software switch.
C. The hypervisor virtualizes physical components including CPU, memory, and storage.
D. Virtualized servers run efficiently when physically connected to a switch that is separate from the hypervisor.

**Answer: C**

**Explanation:**

The correct answer is C because it accurately describes the core function of a hypervisor in virtualization. A hypervisor, which can be either type 1 (bare-metal) or type 2 (hosted), is responsible for abstracting physical hardware resources such as the CPU, memory (RAM), and storage devices. This abstraction creates virtualized versions of these components, allowing multiple operating systems and applications to run simultaneously on a single physical machine, each within its own isolated virtual machine (VM). The hypervisor's primary role is to manage and allocate these virtualized resources to the VMs, ensuring they function independently and without conflict.

Option A is incorrect because while hypervisors can use Layer 3 networking for VM communication, they don't do so "without the need for additional resources". Virtual networking within a hypervisor still requires resource allocation. Option B is also incorrect as hypervisors are designed to support many VMs and typically utilize virtual switches to connect multiple VMs. Option D is incorrect because virtualized servers can run efficiently whether or not they're connected to a separate physical switch; the location of the physical switch does not dictate efficiency. The hypervisor's ability to virtualize hardware resources is fundamental to the operation of all VMs.

**Authoritative Links for Further Research:**

1. **VMware: What is a Hypervisor?** - This link provides a comprehensive explanation of hypervisors and their functions.https://www.vmware.com/topics/glossary/content/hypervisor
2. **Microsoft: Hypervisor Concepts** - This resource from Microsoft details the technical aspects of hypervisors and virtualization.https://learn.microsoft.com/en-us/virtualization/hyper-v-on-windows/about/
3. **Red Hat: What is a hypervisor?** - This article offers an overview of different hypervisor types and their uses in virtualized environments.https://www.redhat.com/en/topics/virtualization/what-is-a-hypervisor

## Question: 10

Which command automatically generates an IPv6 address from a specified IPv6 prefix and MAC address of an interface?

A. ipv6 address dhcp
B. ipv6 address 2001:DB8:5:112::/64 eui-64
C. ipv6 address autoconfig
D. ipv6 address 2001:DB8:5:112::2/64 link-local

**Answer: B**

**Explanation:**

The correct answer is **B. ipv6 address 2001:DB8:5:112::/64 eui-64**. This command configures the IPv6 address on an interface using the EUI-64 (Extended Unique Identifier 64-bit) method.

EUI-64 is a mechanism that automatically generates an IPv6 interface ID (the last 64 bits of the IPv6 address) using the interface's MAC address. The command ipv6 address 2001:DB8:5:112::/64 eui-64 instructs the router to take the provided IPv6 prefix (2001:DB8:5:112::/64) and combine it with an interface ID derived from the interface's MAC address using the EUI-64 algorithm.

Option A (ipv6 address dhcp) configures the interface to obtain an IPv6 address through DHCPv6, which involves a server assigning the address. This doesn't automatically generate an address from the MAC address using EUI-64.

Option C (ipv6 address autoconfig) enables stateless address autoconfiguration (SLAAC), but it relies on Router Advertisements (RAs) to obtain the prefix. While SLAAC also uses EUI-64 to generate the interface ID, it doesn't combine a specified prefix with the MAC address through a direct command like in option B. The router learns the prefix from RAs.

Option D (ipv6 address 2001:DB8:5:112::2/64 link-local) manually configures a specific IPv6 address. This option doesn't use EUI-64 at all; it explicitly defines the entire IPv6 address. Link-local addresses also are not generated from the global prefix and MAC address.

Therefore, only option B utilizes the EUI-64 process with a given prefix to automatically create the IPv6 address from the MAC address. The eui-64 keyword is crucial for enabling this automatic generation.

For further research, refer to the Cisco documentation on IPv6 addressing:

**Cisco IPv6 Configuration Guide:**https://www.cisco.com/c/en/us/td/docs/ios-xml/15_7/ipv6/configuration/157-ipv6-config/ipv6-addr-cfg.html (Specifically, the sections on EUI-64 address configuration.)
**Understanding IPv6 EUI-64 Address:**https://networklessons.com/ipv6/ipv6-eui-64-address

## Question: 11

DRAG DROP -

```
[root#HostTime =]# ip route
default via 192.168.1.193 dev eth1 proto static
192.168.1.0/26 dev sth1 proto kernel scope link src 192.168.1.200 metric 1

[root#HostTime =]# ip addr show eth1
eth1:mtu 1500 qdisc pfifo_fast qlan 1000
   link/ether 00:0C:22:83:79:A3 brd ff:ff:ff:ff:ff:ff
   inet 192.168.1.200/26 hrd 192.168.1.255 scope global eth1
   inet6 fe80::20c::29ff:fe89:79b3/64 scope link
   valid_lft forever preferred_lft forever
```

Refer to the exhibit. Drag and drop the networking parameters from the left onto the correct values on the right. Select and Place:

**Answer Area**

| | |
|---|---|
| default gateway | 00:0C:22 |
| host IP address | 00:0C:22:83:79:A3 |
| NIC MAC address | 192.168.1.193 |
| NIC vendor OUI | 192.168.1.200 |
| subnet mask | 255.255.255.192 |

**Answer:**

**Answer Area**

| | |
|---|---|
| default gateway | NIC vendor OUI |
| host IP address | NIC MAC address |
| NIC MAC address | default gateway |
| NIC vendor OUI | host IP address |
| subnet mask | subnet mask |

**Explanation:**

Default Gateway: 192.168.1.193Host IP: 192.168.1.200NIC MAC Address: 00:0C:22:83:79:A3NIC Vendor OUI: 00:0C:22 - Subnet Mask: 255.255.255.192 (/26)

**Question: 12**

DRAG DROP -

```
[root@HostTest ~]# ip route
default via 192.168.1.193 dev eth1  proto static
192.168.1.0/26 dev eth1  proto kernel  scope link  src 192.168.1.200  metric 1

[root@HostTest ~]# ip addr show eth1
eth1:  mtu 1500 qdisc pfifo_fast qlen 1000
   link/ether 00:0C:22:83:79:A3 brd ff:ff:ff:ff:ff:ff
   inet 192.168.1.200/26 brd 192.168.1.255 scope global eth1
   inet6 fe80::20c:29ff:fe89:79b3/64 scope link
   valid_lft forever preferred_lft forever
```

Refer to the exhibit. Drag and drop the networking parameters from the left onto the correct values on the right.
Select and Place:

**Answer Area**

| | |
|---|---|
| default gateway | 00:0C:22 |
| host IP address | 00:0C:22:83:79:A3 |
| NIC MAC address | 192.168.1.193 |
| NIC vendor OUI | 192.168.1.200 |
| subnet mask | 255.255.255.192 |

**Answer:**

**Answer Area**

| | |
|---|---|
| default gateway | NIC vendor OUI |
| host IP address | NIC MAC address |
| NIC MAC address | default gateway |
| NIC vendor OUI | host IP address |
| subnet mask | subnet mask |

**Explanation:**
The ip route and ip addr show eth1 are Linux commands.

¢ip route: display the routing table
¢ip addr show eth1: get depth information (only on eth1 interface) about your network interfaces like IP Address, MAC Address information

## Question: 13

What is the default behavior of a Layer 2 switch when a frame with an unknown destination MAC address is received?

A.The Layer 2 switch forwards the packet and adds the destination MAC address to its MAC address table.
B.The Layer 2 switch sends a copy of a packet to CPU for destination MAC address learning.
C.The Layer 2 switch floods packets to all ports except the receiving port in the given VLAN.
D.The Layer 2 switch drops the received frame.

**Answer: C**

**Explanation:**

The correct answer is C: The Layer 2 switch floods packets to all ports except the receiving port in the given VLAN.

Layer 2 switches operate at the Data Link Layer of the OSI model, primarily using MAC addresses to forward frames. When a switch receives a frame, it examines the destination MAC address. If the destination MAC address is not present in its MAC address table (also known as the CAM table), the switch doesn't know which port to forward the frame to. In this situation, the switch employs a process known as "flooding." Flooding involves sending a copy of the frame out of every port in the same VLAN except for the port where the frame was received. This ensures that the frame reaches its intended destination, even though the switch doesn't know the destination's location yet. Once the destination device responds, its source MAC address is learned by the switch and added to the MAC address table, mapping the MAC address to the port it was received on.

Subsequent frames destined for that MAC address will be forwarded directly through the specific port. Option A is incorrect because while the switch learns source MAC addresses, it doesn't learn destination MAC addresses upon receiving a frame. Option B is incorrect; the CPU isn't typically involved in learning destination addresses for a regular frame. Option D is incorrect because a switch doesn't drop frames with unknown destinations; instead, it floods them. Flooding is fundamental for proper network operation as it enables devices to discover each other initially, allowing them to communicate even before the switch has learned all the relevant MAC addresses. This process ensures that connectivity is maintained and new devices can join the network smoothly.

Relevant resource:

**Cisco - Understanding How Switches Learn and Forward MAC Addresses:**
https://www.cisco.com/c/en/us/support/docs/lan-switching/ethernet/10569-3.html

## Question: 14

An engineer must configure a /30 subnet between two routes. Which usable IP address and subnet mask combination meets this criteria?

A.interface e0/0 description to XX-AXXX:XXXXX ip address 10.2.1.3 255.255.255.252
B.interface e0/0 description to XX-AXXX:XXXXX ip address 192.168.1.1 255.255.255.248
C.interface e0/0 description to XX-AXXX:XXXXX ip address 172.16.1.4 255.255.255.248

D.interface e0/0 description to XX-AXXX:XXXXX ip address 209.165.201.2 225.255.255.252

**Answer: D**

**Explanation:**

Here's the justification for why option D is the correct answer:

A /30 subnet mask is crucial for point-to-point links between routers, as it provides only two usable IP addresses, one for each end of the connection. This minimizes IP address wastage. The mask 255.255.255.252 represents a /30 subnet because its binary representation has 30 ones, leaving 2 bits for host addresses. Options B and C use the mask 255.255.255.248, which is a /29 subnet, and provides 6 usable addresses, unsuitable for a /30 requirement.

Option A includes the correct /30 mask but has an address (10.2.1.3) in the 10.0.0.0/8 network, which is not specified as a necessity for the address assignment. Option D, with the address 209.165.201.2 using the /30 mask (255.255.255.252), aligns perfectly with the given requirement. The address 209.165.201.2, with a /30 subnet allows for only two usable IP's (209.165.201.1 and 209.165.201.2), making it a valid solution.

Therefore, option D is the correct answer as it uses the right subnet mask and does not violate any given conditions of question.

Authoritative links for further research:

1. **Cisco Subnetting Basics:**https://www.cisco.com/c/en/us/support/docs/ip/subnetting/13953-subnet.html
2. **Understanding IP Addressing and Subnetting:**https://www.cloudflare.com/learning/network-layer/what-is-subnetting/

## Question: 15

Which network allows devices to communicate without the need to access the Internet?

A.172.9.0.0/16
B.172.28.0.0/16
C.192.0.0.0/8
D.209.165.201.0/24

**Answer: B**

**Explanation:**

The question asks which listed IP address range facilitates communication between devices without internet access. This implies a private network context. Private IP addresses are specifically designed for internal use within a network, not for public internet routing. The ranges reserved for private networks are defined in RFC 1918. They include 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. Option B, 172.28.0.0/16, falls within the 172.16.0.0/12 private address range. This means devices configured with IP addresses in this range can communicate with each other within a local network without needing to go through a router connected to the public internet. Option A (172.9.0.0/16) does not fall within a reserved private range; it is within the public address space. Option C (192.0.0.0/8) is not a private address. Option D (209.165.201.0/24) is also a public address, commonly used for examples. Therefore, only addresses from private ranges are suitable for local network communication without requiring internet access, making B the correct choice.

https://datatracker.ietf.org/doc/html/rfc1918https://www.cisco.com/c/en/us/support/docs/ip/ip-

addressing/13850-ipadd.html

**Question: 16**

```
Router(config)#interface GigabitEthernet 1/0/1
Router(config-if)#ip address 192.168.16.143 255.255.255.240
Bad mask /28 for address 192.168.16.143
```

Refer to the exhibit. Which statement explains the configuration error message that is received?

A.It belongs to a private IP address range.
B.The router does not support /28 mask.
C.It is a network IP address.
D.It is a broadcast IP address.

**Answer: D**

**Explanation:**

D is correct because the next subnet address is 192.168.16.144

**Question: 17**

Which IPv6 address type provides communication between subnets and cannot route on the Internet?

A.link-local
B.unique local
C.multicast
D.global unicast

**Answer: B**

**Explanation:**

The correct answer is B, Unique Local IPv6 addresses. These addresses, defined by the prefix fc00::/7, are intended for local communications within a site or a limited set of sites. They are analogous to private IPv4 addresses (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) and are not globally routable on the public internet. This design prevents direct exposure of internal networks to the outside world, enhancing security. Unique local addresses are routable within an organization's infrastructure, enabling communication between different subnets within that administrative domain. Conversely, link-local addresses (fe80::/10) are only used for communication within the same physical network segment and cannot be routed beyond that link. Multicast addresses (ff00::/8) are used for group communication, not unicast routing. Global unicast addresses, on the other hand, are globally routable on the internet, corresponding to public IPv4 addresses, and are not suitable for private internal network communications without Network Address Translation (NAT). Unique local addresses offer a scalable solution for private networking in IPv6 without the need for NAT, promoting end-to-end reachability within an organization. Their scope is explicitly limited to a defined administrative domain, making them ideal for private networks requiring routing between internal subnets.

Authoritative Links:

RFC 4193: Unique Local IPv6 Unicast Addresses: https://datatracker.ietf.org/doc/html/rfc4193
RFC 4291: IP Version 6 Addressing Architecture: https://datatracker.ietf.org/doc/html/rfc4291
Cisco: IPv6 Addressing: https://www.cisco.com/c/en/us/support/docs/ip/ip-version-6-ipv6/113328-ipv6-addr-plan.html

## Question: 18

Which IPv6 address block sends packets to a group address rather than a single address?

A.2000::/3
B.FC00::/7
C.FE80::/10
D.FF00::/8

**Answer: D**

**Explanation:**

The correct answer is D. FF00::/8 signifies the multicast address range in IPv6. Unlike unicast addresses which are assigned to a single interface, and anycast which is assigned to multiple interfaces, multicast addresses are used to send packets to a group of interfaces simultaneously. In IPv6, addresses beginning with "FF" represent multicast addresses, and the "/8" indicates that the first 8 bits (or one byte) are fixed as '11111111', defining the scope for multicast.

Option A, 2000::/3, represents the global unicast address range, primarily used for public internet addressing.
Option B, FC00::/7, refers to unique local addresses meant for private networks, similar to private IPv4 addresses but with a global scope within a limited administrative domain. Option C, FE80::/10, identifies link-local unicast addresses. These addresses are automatically assigned to interfaces within the same link and are non-routable; they are used for local network communication and neighbor discovery. These address types are all unicast and meant for singular interfaces.

Only option D's prefix, FF00::/8, indicates multicast functionality which sends a packet to all interfaces subscribed to that specific multicast group, making it distinct from singular addressing. This group addressing capability is crucial for efficient delivery to multiple recipients on a network segment without requiring individual transmissions.

RFC 4291 offers a deep dive into IPv6 addressing architecture, specifically covering multicast addresses.Cisco's explanation on IPv6 addressing also supports the answer.

## Question: 19

What are two reasons that cause late collisions to increment on an Ethernet interface? (Choose two.)

A.when Carrier Sense Multiple Access/Collision Detection is used
B.when one side of the connection is configured for half-duplex
C.when the sending device waits 15 seconds before sending the frame again
D.when a collision occurs after the 32nd byte of a frame has been transmitted
E.when the cable length limits are exceeded

**Answer: BE**

**Explanation:**

Okay, let's break down why options B and E are the correct reasons for late collisions on an Ethernet interface.

**Late Collisions Explained:**

Late collisions occur when a collision happens after the first 64 bytes (or 512 bits) of a frame have been transmitted. This is abnormal and points to a significant problem within the network. Standard collisions, handled by CSMA/CD, happen within this initial window.

**Why Option B is Correct: Half-Duplex Configuration**

In a half-duplex connection, devices take turns transmitting and receiving data. They listen before transmitting, but collisions can still happen if two devices transmit simultaneously. However, the system is built to quickly detect those and re-transmit. A major problem is that a cable length exceeding the standard length will cause a device to transmit longer than it should before it detects a signal. When one end of a connection is incorrectly forced to half-duplex while the other end runs at full-duplex, the full-duplex end has no mechanism to tell the half-duplex end to back off, resulting in collisions that continue past the initial window of standard collision detection. This commonly occurs when one interface fails to auto-negotiate correctly. This leads to late collisions. This is a severe mismatch that causes problems with the collision detection mechanism, resulting in late collisions.

**Why Option E is Correct: Exceeding Cable Length Limits**

Ethernet has strict cable length limits. Exceeding these limits introduces signal degradation and timing issues. When a signal takes too long to propagate along the cable, a device may not detect a collision within the standard collision window. It would thus transmit longer than it normally should while the other device also transmits leading to a late collision. This delay is outside the normal time frame expected by collision detection.

**Why the Other Options are Incorrect:**

**A:** CSMA/CD (Carrier Sense Multiple Access with Collision Detection) is a mechanism for detecting and handling collisions, it's not a cause of late collisions.

**C:** The sending device does not wait 15 seconds before retransmitting a frame; it’s a much shorter time frame. It is called the backoff algorithm.

**D:** A collision happening after 32 bytes (not 64 bytes) is not defined as a late collision. A late collision happens after the first 64 bytes of transmission.

**In summary, late collisions are caused by configuration mismatches (half-duplex) and physical media issues (excessive cable length) that interfere with the normal operation of collision detection.**

**Authoritative Links for Further Research:**

**Cisco Documentation on Ethernet Collisions:**https://www.cisco.com/c/en/us/support/docs/lan-switching/ethernet/41519-41.html
**Wikipedia on Ethernet:**https://en.wikipedia.org/wiki/Ethernet
**CompTIA Network+ Study Guide** for comprehensive networking information.

These resources offer additional in-depth explanations on Ethernet operations and troubleshooting techniques for network issues.

## Question: 20

What is a benefit of using a Cisco Wireless LAN Controller?

A.It eliminates the need to configure each access point individually.

B.Central AP management requires more complex configurations.

C.Unique SSIDs cannot use the same authentication method.

D.It supports autonomous and lightweight APs.

**Answer: A**

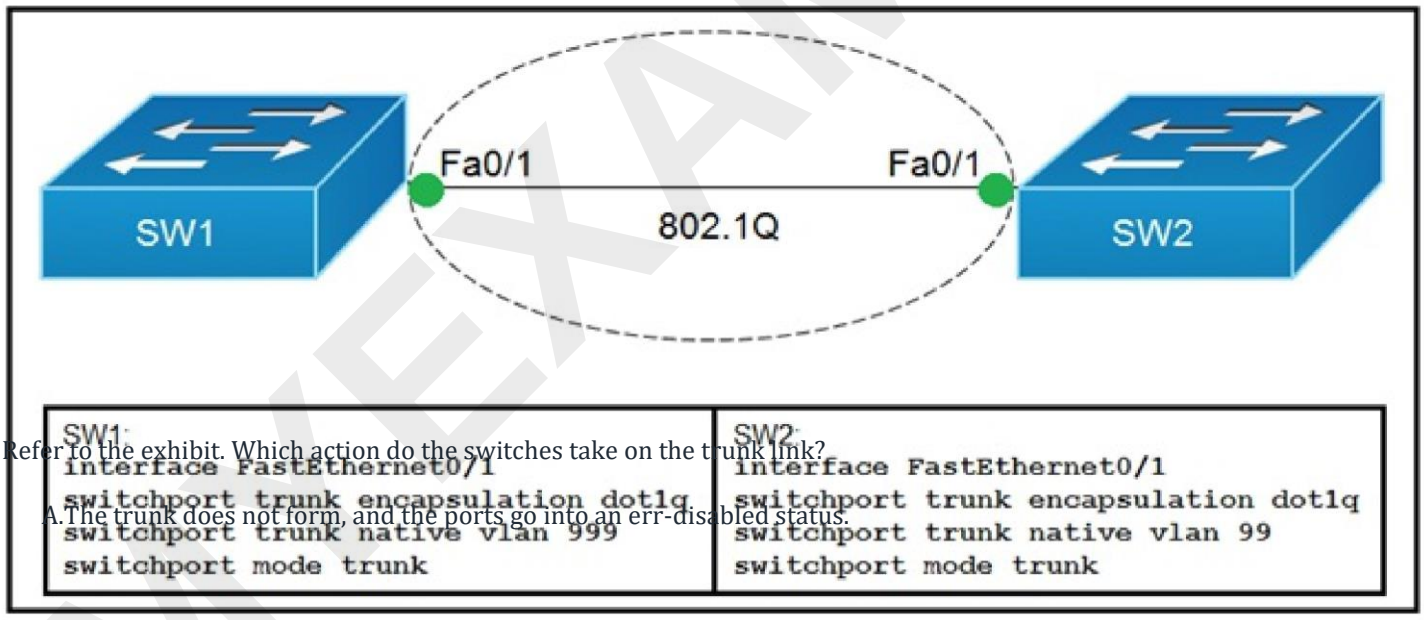
**Explanation:**

The correct answer, **A. It eliminates the need to configure each access point individually**, highlights a key advantage of using a Cisco Wireless LAN Controller (WLC). WLCs provide centralized management of wireless access points (APs). Instead of configuring each AP separately, which can be time-consuming and error-prone, especially in large deployments, administrators configure settings such as SSIDs, security policies, and radio parameters on the WLC. These configurations are then pushed down to all associated APs. This centralized approach simplifies network management, ensures consistency across the wireless network, and reduces administrative overhead. By leveraging a WLC, changes to the wireless environment can be implemented quickly and easily across the entire network, leading to more efficient resource utilization and operational cost reduction. Option B is incorrect because central management, while more sophisticated, generally simplifies configurations by offering a single pane of glass. Option C is incorrect as it is possible, and common practice, to utilize the same authentication method across multiple SSIDs. Option D is incorrect because a WLC is specifically designed to manage lightweight APs (also known as controller-based APs), not autonomous APs. Autonomous APs function as individual units, without needing a WLC for basic operations.

Authoritative links for further research:

**Cisco Wireless LAN Controller Configuration Guide:**
https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/m_configuring_access_points.html
**Cisco Lightweight Access Points Overview:**https://www.cisco.com/c/en/us/products/wireless/access-points/index.html
**Cisco Wireless Technology:**https://www.cisco.com/c/en/us/solutions/small-business/networking/wireless.html

**Question: 21**




Refer to the exhibit. Which action do the switches take on the trunk link?

A.The trunk does not form, and the ports go into an err-disabled status.

B.The trunk forms, but the mismatched native VLANs are merged into a single broadcast domain.

C.The trunk forms, but VLAN 99 and VLAN 999 are in a shutdown state.

D.The trunk does not form, but VLAN 99 and VLAN 999 are allowed to traverse the link.

**Answer: B**

**Explanation:**

802.1q trunking inserts a four-byte 802.1q tag field into frames sent over the trunk, which contain VLAN information. The 802.1q tag is inserted into each frame transferred over the trunk except for frames transmitted on the native VLAN, which are sent untagged. In most cases, the native VLAN has to match on both sides of the trunk unless there is a specific unusual configuration requirement, which is outside the scope of this document. If the native VLANs do not match, the switch will log Cisco Discovery Protocol (CDP) messages stating the mismatch. While not catastrophic, this setup effectively causes the two different native VLANs to be merged into one larger L2 broadcast domain (VLAN). These two VLANs will attempt to calculate one common Spanning-Tree Protocol (STP) topology for such bridged native VLANs, with the risk of eventually exceeding the maximum supported STP diameter

## Question: 22

What occurs to frames during the process of frame flooding?

A.Frames are sent to all ports, including those that are assigned to other VLANs.

B.Frames are sent to every port on the switch that has a matching entry in MAC address table.

C.Frames are sent to every port on the switch in the same VLAN except from the originating port.

D.Frames are sent to every port on the switch in the same VLAN.

**Answer: C**

**Explanation:**

Frame flooding occurs when a switch receives a frame with a destination MAC address it doesn't have recorded in its MAC address table (also called the CAM table). This indicates the switch doesn't know which port to forward the frame to. In this situation, to ensure the frame reaches its destination, the switch sends a copy of the frame out of every port associated with the same VLAN except the port it was received on. This process is known as flooding. Option C correctly describes this behavior: "Frames are sent to every port on the switch in the same VLAN except from the originating port."

Options A, B, and D are incorrect. Option A is wrong because switches don't flood frames to ports in other VLANs; this would violate VLAN segmentation. Option B is incorrect because if the destination MAC address was present in the MAC address table, the frame would be unicast, not flooded. Option D is incorrect because, while the switch does send the frame to all ports in the same VLAN, it excludes the originating port to prevent unnecessary looping.

Flooding is a fundamental process in Ethernet switching that allows unknown destinations to be discovered and the MAC address table to be populated. It ensures that a frame reaches the intended destination even when the switch initially lacks the necessary mapping between MAC addresses and ports. Once the destination device replies to the flooded frame, the switch learns its MAC address and the associated port, allowing for more efficient unicast forwarding in future communications. This process is essential to the operation of a Layer 2 Ethernet network.

For further research, consider these resources:

**Cisco Documentation on Switching:**https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24062-146.html (While this link is on Spanning Tree, it touches on the concept of Layer 2 forwarding and flooding)
**Network Engineering StackExchange:**https://networkengineering.stackexchange.com/ (Search for "frame flooding" for a wealth of community discussions).
**Search for "Ethernet Frame Flooding"** using a search engine for more resources.

## Question: 23

Which function does the range of private IPv4 addresses perform?

A. allows multiple companies to each use the same addresses without conflicts
B. provides a direct connection for hosts from outside of the enterprise network
C. ensures that NAT is not required to reach the Internet with private range addressing
D. enables secure communications to the Internet for all external hosts

**Answer: A**

**Explanation:**

The correct answer is **A. allows multiple companies to each use the same addresses without conflicts**.
Private IPv4 addresses, as defined in RFC 1918, are specifically designated for internal networks. These address ranges (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16) are not routable on the public internet. This allows organizations to use them freely within their local networks without fear of conflicts with public IP addresses or other private networks. Each organization can utilize the same private address ranges independently, because these addresses are not intended for direct internet routing. Network Address Translation (NAT) is then employed at the boundary of a private network, typically the router, to translate these private addresses to public addresses when communicating with external networks like the internet. Option B is incorrect as private addresses are not routable on the internet without NAT. Option C is false, as NAT is specifically required to enable communication with the internet using private addresses. Option D is incorrect since private addresses do not provide direct secure communications to the internet; this is handled via NAT and other security mechanisms. Thus, the primary purpose of private IP address ranges is to avoid public address depletion and enable efficient private networking by allowing re-use of the address space.

Authoritative links for further research:

RFC 1918: https://datatracker.ietf.org/doc/html/rfc1918
Cisco - Understanding IP Addressing and Subnetting:
https://www.cisco.com/c/en/us/support/docs/ip/addressing/10450-13.html

## Question: 24

Which action must be taken to assign a global unicast IPv6 address on an interface that is derived from the MAC address of that interface?

A.explicitly assign a link-local address
B.disable the EUI-64 bit process
C.enable SLAAC on an interface
D.configure a stateful DHCPv6 server on the network

**Answer: C**

**Explanation:**

The correct answer is **C. enable SLAAC on an interface**. Here's why:

Stateful address configuration using DHCPv6 (option D) relies on a server assigning addresses, not deriving them from the MAC. Options A and B are not related to deriving addresses from the MAC address. A link-local address is automatically configured in IPv6, and disabling EUI-64 (option B) would prevent the desired MAC-derived address generation.

**SLAAC (Stateless Address Autoconfiguration)**, when enabled on an interface, utilizes the EUI-64 process to generate the interface ID portion of a global unicast IPv6 address. It combines the network prefix (advertised by a router) with the modified MAC address to create a unique global unicast address. This is exactly what the question describes. The EUI-64 process takes the 48-bit MAC address, inserts FFFE in the middle and then inverts the 7th bit making it a 64 bit interface ID. This interface ID is then combined with the network prefix (typically learned through router advertisements) to create the global IPv6 address. Therefore, by enabling SLAAC, the interface is instructed to participate in this process and self-configure its IPv6 address based on the MAC address and the advertised prefix, thus providing a self-configured global unicast IPv6 address.

**Authoritative links for further research:**

**Cisco Documentation on IPv6 Addressing:**https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-e/ipv6-15-e-book/ipv6-addr-config.html (Focus on Stateless Autoconfiguration) **RFC 4862 - IPv6 Stateless Address Autoconfiguration:**https://datatracker.ietf.org/doc/html/rfc4862 (Original RFC detailing SLAAC)
**Understanding IPv6 EUI-64:**https://networklessons.com/ipv6/ipv6-eui-64-address-calculation (Explanation of how the EUI-64 process works)

## Question: 25

Several new coverage cells are required to improve the Wi-Fi network of an organization. Which two standard designs are recommended? (Choose two.)

A.5GHz provides increased network capacity with up to 23 nonoverlapping channels.
B.5GHz channel selection requires an autonomous access point.
C.Cells that overlap one another are configured to use nonoverlapping channels.
D.Adjacent cells with overlapping channels use a repeater access point.
E.For maximum throughput, the WLC is configured to dynamically set adjacent access points to the channel.

**Answer: AC**

**Explanation:**

Here's a breakdown of why options A and C are the correct choices for improving Wi-Fi coverage with new cells:

**Option A: 5GHz provides increased network capacity with up to 23 nonoverlapping channels.**

This is a crucial point for enhancing Wi-Fi in denser environments. The 5GHz band offers significantly more non-overlapping channels compared to the 2.4GHz band. This means less interference between access points (APs), allowing more devices to connect without experiencing reduced performance. Utilizing the 5GHz band is vital for expanding network capacity and accommodating the increasing number of users and devices. The 2.4GHz band, with only three non-overlapping channels, can quickly become congested when multiple APs are present. Therefore, focusing on the 5GHz band is a key design principle for improving coverage and throughput.

**Option C: Cells that overlap one another are configured to use nonoverlapping channels.**

This design principle, often called channel reuse, is essential in any multi-AP environment. When neighboring Wi-Fi cells operate on the same or overlapping channels, they interfere with each other, leading to reduced performance and coverage. By assigning non-overlapping channels to neighboring cells, we minimize this interference and ensure that devices can connect to the closest AP with a clear signal. This maximizes throughput and coverage across the network. The implementation of non-overlapping channels prevents signal degradation and packet loss, ultimately creating a more efficient and reliable wireless network. This is particularly important in dense environments where numerous overlapping cells are required to achieve comprehensive coverage.

**Why the other options are incorrect:**

**Option B: 5GHz channel selection requires an autonomous access point.** This is incorrect. Centralized management using a Wireless LAN Controller (WLC) is often recommended for managing channel selection. Autonomous APs can lead to management difficulties and less effective channel selection.

**Option D: Adjacent cells with overlapping channels use a repeater access point.** This approach exacerbates interference issues. Using repeaters can extend the range, but it does not address the root problem of overlapping channels. Repeaters also halve the bandwidth, so they are not typically recommended.

**Option E: For maximum throughput, the WLC is configured to dynamically set adjacent access points to the channel.** While dynamic channel assignment by WLCs can be beneficial, it's not one of the foundational standard designs recommended for Wi-Fi cell deployment. The standard design principles include using the 5GHz band and configuring non-overlapping channels. Dynamic channel assignment comes after the basic design principles are implemented.

**Authoritative Links for Further Research:**

**Cisco Wireless LAN Design Guide:**
https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/emob73dg/emob73_DG.html(This Cisco guide provides in-depth information on wireless design best practices.)
**CWNP (Certified Wireless Network Professional):**https://www.cwnp.com/(CWNP is a valuable resource for wireless networking education and certifications.)

In summary, options A and C present foundational standard designs for improving Wi-Fi coverage using new cells. They focus on utilizing the 5GHz band for increased capacity and configuring non-overlapping channels to minimize interference and optimize performance. These practices are key to achieving a reliable and high-performing wireless network in modern organizations.

## Question: 26

How do TCP and UDP differ in the way they provide reliability for delivery of packets?

A. TCP does not guarantee delivery or error checking to ensure that there is no corruption of data, UDP provides message acknowledgement and retransmits data if lost.

B. TCP provides flow control to avoid overwhelming a receiver by sending too many packets at once, UDP sends packets to the receiver in a continuous stream without checking.

C. TCP is a connectionless protocol that does not provide reliable delivery of data; UDP is a connection-oriented protocol that uses sequencing to provide reliable delivery.

D. TCP uses windowing to deliver packets reliably; UDP provides reliable message transfer between hosts by establishing a three-way handshake.

**Answer: B**

**Explanation:**

Okay, let's break down why option B is the correct answer regarding TCP and UDP's reliability mechanisms.

TCP (Transmission Control Protocol) is a connection-oriented protocol designed for reliable data transfer. It achieves this through several mechanisms, most notably flow control. TCP's flow control employs a sliding window mechanism to regulate the rate of data transmission. This window indicates how much data a sender can transmit without receiving an acknowledgment. By adjusting this window size, TCP prevents the receiver from being overwhelmed, ensuring data is not dropped due to buffer overflow at the receiving end. Furthermore, TCP provides other features like error detection and correction.

Conversely, UDP (User Datagram Protocol) is a connectionless protocol, prioritizing speed over reliability. It simply sends packets without establishing a connection or implementing flow control mechanisms. UDP transmits data in a continuous stream, effectively "fire and forget," and does not check if packets reach their destination or are received in order. This approach makes UDP faster but more susceptible to packet loss and out-of-order delivery.

Option B accurately contrasts these approaches. TCP's flow control prevents overwhelming the receiver, while UDP sends packets continuously without checks. Other options misrepresent core functions or mix characteristics of the protocols. For instance, TCP does guarantee delivery using sequence numbers, acknowledgements and retransmissions (not mentioned directly by this option), and it is connection oriented. UDP is connectionless.

In summary, TCP focuses on reliability via flow control, and data delivery mechanisms, while UDP focuses on speed and is less concerned about delivery reliability, making B the correct answer.

Authoritative links for further research:

**TCP:**https://www.cloudflare.com/learning/tcp/what-is-tcp/
**UDP:**https://www.cloudflare.com/learning/tcp/tcp-vs-udp/ **Flow Control:**https://www.geeksforgeeks.org/tcp-flow-control/

## Question: 27

What are two differences between optical-fiber cabling and copper cabling? (Choose two.)

A.A BNC connector is used for fiber connections
B.The glass core component is encased in a cladding
C.The data can pass through the cladding
D.Light is transmitted through the core of the fiber
E.Fiber connects to physical interfaces using RJ-45 connections

**Answer: BD**

**Explanation:**

Here's a detailed justification for why options B and D are the correct differences between optical-fiber and copper cabling:

**B. The glass core component is encased in a cladding:** This statement accurately describes a fundamental characteristic of fiber optic cable. Unlike copper cables which use conductive materials, fiber optic cables transmit data as light pulses. The core, a thin strand of glass or plastic, is where the light travels. This core is then surrounded by a cladding, a layer of material with a different refractive index. This difference in refractive indices ensures that light is confined to the core through total internal reflection, minimizing signal loss and allowing the light to travel long distances. Copper cables, conversely, do not have a core and

cladding structure; their signal is transmitted through electrical conductivity across the copper conductor.

**D. Light is transmitted through the core of the fiber:** This highlights the core operational difference between the two cable types. Fiber optic cables use light to carry data, which, as mentioned above, travels through the core of the fiber. This method allows for significantly higher bandwidth and longer transmission distances compared to copper cabling, which uses electrical signals. Electrical signals in copper are prone to signal degradation and interference over long distances. The use of light in fiber optics eliminates many of these challenges, offering superior performance in data transmission.

Options A, C, and E are incorrect:

**A. A BNC connector is used for fiber connections:** BNC connectors are typically associated with coaxial copper cables, not fiber optic cables. Fiber uses connectors like SC, LC, ST, and MTRJ.

**C. The data can pass through the cladding:** Data is transmitted through the core of the fiber, not the cladding. The cladding's purpose is to confine the light within the core via total internal reflection.

**E. Fiber connects to physical interfaces using RJ-45 connections:** RJ-45 connectors are standard for copper Ethernet cables. Fiber optic connections utilize different connector types, as mentioned above.

In summary, the presence of a core and cladding, and the use of light transmission through the core are key distinctions between fiber optic and copper cables. These characteristics lead to the superior bandwidth and distance capabilities of fiber optic cabling.

**Authoritative Links:**

**Fiber Optic Association:**https://foa.org/ (Provides extensive information on fiber optic technology) **Wikipedia: Optical Fiber:**https://en.wikipedia.org/wiki/Optical_fiber (Comprehensive overview of optical fiber technology) **Cisco Networking Academy:**https://www.netacad.com/ (Offers courses on networking concepts including cabling)

## Question: 28

How does CAPWAP communicate between an access point in local mode and a WLC?

A.The access point must not be connected to the wired network, as it would create a loop

B.The access point must be connected to the same switch as the WLC

C.The access point must directly connect to the WLC using a copper cable

D.The access point has the ability to link to any switch in the network, assuming connectivity to the WLC

**Answer: D**

**Explanation:**

The correct answer is **D**. CAPWAP (Control and Provisioning of Wireless Access Points) allows access points (APs) in local mode to communicate with a Wireless LAN Controller (WLC) regardless of their physical switch connection, as long as IP connectivity to the WLC is established. The AP doesn't need to be directly connected to the same switch or directly cabled to the WLC, which makes options B and C incorrect. Option A is also incorrect, as APs in local mode absolutely need to be connected to the wired network to function. CAPWAP encapsulates control and data traffic between the AP and the WLC using UDP ports 5246 (control) and 5247 (data). This encapsulation allows the traffic to traverse different network segments, provided the underlying network supports IP communication between the AP and the WLC. This design provides deployment flexibility, enabling APs to be placed strategically based on coverage requirements, independent of the WLC's specific switch connection. The AP will discover the WLC using methods like DHCP option 43, DNS, or broadcast, allowing it to establish a CAPWAP tunnel. Once the tunnel is established, the WLC centrally

manages the AP, handling configuration, security policies, and client traffic. The underlying switching infrastructure essentially acts as a transport mechanism for the CAPWAP communication.

Authoritative links for further research:

**Cisco - CAPWAP Discovery and Join Process:**https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/capwap_discovery_join_process.html
**Cisco - Understanding CAPWAP:**https://www.cisco.com/c/en/us/support/docs/wireless/wireless-lan-controller-software/115779-capwap-understanding-1100.html

**Question: 29**

Which IPv6 address block forwards packets to a multicast address rather than a unicast address?

A. 2000::/3
B. FC00::/7
C. FE80::/10
D. FF00::/12

**Answer: D**

**Explanation:**

The correct answer is **D. FF00::/12**. This IPv6 address block is specifically reserved for multicast addresses. In IPv6, multicast communication allows a single packet to be sent to multiple recipients simultaneously. Unlike unicast, where a packet is sent to a single destination, multicast uses a single address to reach a group of devices subscribed to that particular multicast group.

Option A, **2000::/3**, represents global unicast addresses, the most common type used for general internet communication. Option B, **FC00::/7**, designates unique local unicast addresses, designed for private networks and not routable on the public internet. Option C, **FE80::/10**, signifies link-local unicast addresses, used for communication within a single network segment.

The FF00::/12 prefix guarantees that any address starting with 'FF' will be a multicast address, as defined by IETF standards. The subsequent bits following the '/12' determine the specific multicast group the address represents. This design facilitates efficient distribution of data to multiple recipients, a core concept in network management and cloud computing environments. For example, in cloud environments, multicast is used for service discovery and resource replication.

In contrast, global, unique local, and link-local addresses are designed to ensure packets are sent to a single network interface, not to a collection of interfaces. Using these for multicast would be illogical and inefficient, hence the dedicated multicast range.

Authoritative Links:

1. **RFC 4291 - IP Version 6 Addressing Architecture:**https://www.rfc-editor.org/rfc/rfc4291 - This RFC outlines the fundamental aspects of IPv6 addressing, including multicast addressing.
2. **Cisco Documentation on IPv6 Addressing:**https://www.cisco.com/c/en/us/support/docs/ip/ip-version-6-ipv6/113328-ipv6-address-types.html - This provides detailed information on IPv6 address types and their functions.
3. **Juniper Networks - Understanding IPv6 Multicast:** https://www.juniper.net/documentation/en_US/junos/topics/concept/ipv6-multicast-understanding.html - This resource offers insights into multicast in IPv6 from a Juniper perspective.

**Question: 30**

What is the difference regarding reliability and communication type between TCP and UDP?

A.TCP is reliable and is a connectionless protocol; UDP is not reliable and is a connection-oriented protocol.
B.TCP is not reliable and is a connectionless protocol; UDP is reliable and is a connection-oriented protocol.
C.TCP is not reliable and is a connection-oriented protocol; UDP is reliable and is a connectionless protocol.
D.TCP is reliable and is a connection-oriented protocol; UDP is not reliable and is a connectionless protocol.

**Answer: D**

**Explanation:**

The correct answer is **D. TCP is reliable and is a connection-oriented protocol; UDP is not reliable and is a connectionless protocol.**

Here's the breakdown:

**TCP (Transmission Control Protocol):**

**Reliable:** TCP ensures that data packets arrive at their destination in the correct order and without loss or corruption. It achieves this through mechanisms like acknowledgments, sequence numbers, and retransmission timeouts. If a packet is lost or damaged, TCP will resend it. This is critical for applications where data integrity is paramount.

**Connection-Oriented:** Before data transfer begins, TCP establishes a connection using a three-way handshake. This allows for a persistent virtual circuit between the sending and receiving applications, enabling reliable data delivery. This overhead makes TCP slightly slower than UDP.

**UDP (User Datagram Protocol):**

**Not Reliable:** UDP does not guarantee that packets will arrive or arrive in the correct order. It lacks the reliability mechanisms of TCP. If a packet is lost, corrupted, or arrives out of order, UDP doesn't handle it. This makes UDP suitable for applications where speed and low overhead are more important than guaranteed delivery.

**Connectionless:** UDP does not establish a connection before sending data. It sends data in independent datagrams, each routed separately. This lack of overhead makes UDP faster and more lightweight than TCP.

**In Summary:** TCP prioritizes data integrity and delivery order, making it appropriate for applications like web browsing, file transfers, and email. UDP prioritizes speed and low latency, making it suitable for real-time applications like video streaming, online gaming, and VoIP. TCP handles packet loss, order, and error detection, whereas UDP simply transmits packets without these mechanisms. The differences in reliability and connection types make each protocol suitable for different needs within a network.

**Authoritative links for further research:**

1. **Cisco: Understanding TCP/IP**: https://www.cisco.com/c/en/us/support/docs/ip/transmission-control-protocol-tcp/21868-tcp-ip.html
2. **Cloudflare: TCP vs. UDP: What's the Difference?**: https://www.cloudflare.com/learning/network-layer/tcp-vs-udp/
3. **Wikipedia: Transmission Control Protocol**: https://en.wikipedia.org/wiki/Transmission_Control_Protocol
4. **Wikipedia: User Datagram Protocol**: https://en.wikipedia.org/wiki/User_Datagram_Protocol

## Question: 31

What are two descriptions of three-tier network topologies? (Choose two.)

A.The distribution layer runs Layer 2 and Layer 3 technologies
B.The network core is designed to maintain continuous connectivity when devices fail
C.The access layer manages routing between devices in different domains
D.The core layer maintains wired connections for each host
E.The core and distribution layers perform the same functions

**Answer: AB**

**Explanation:**

The correct options are A and B. Three-tier network topologies are hierarchical, typically consisting of the access, distribution, and core layers. Option A accurately describes the distribution layer's function. This layer acts as an intermediary, often running both Layer 2 (data link layer for switching) and Layer 3 (network layer for routing) protocols. It aggregates traffic from the access layer and directs it to the core. Option B accurately describes the core layer's objective. The core layer is designed for high-speed data transfer and resilience; it focuses on maintaining continuous connectivity, minimizing disruptions even if a device fails.

Options C, D, and E are incorrect. The access layer provides endpoints with network access, while routing between different network domains is typically handled by the distribution layer, not the access layer (Option C is incorrect). The access layer maintains wired connections for each host, not the core (Option D is incorrect). The core and distribution layers have distinct roles; the core layer is designed for high-speed transit, while the distribution layer provides policies and controls (Option E is incorrect).

**Authoritative Links:**

**Cisco Documentation on Hierarchical Network Design:**
https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Aug2014/CVD-CampusLANDesign-AUG14.html
**TechTarget Definition of Three-Tier Architecture:**
https://www.techtarget.com/searchnetworking/definition/three-tier-architecture

## Question: 32

Which type of IPv6 address is publicly routable in the same way as IPv4 public addresses?

A.multicast
B.unique local
C.link-local
D.global unicast

**Answer: D**

**Explanation:**

The correct answer is D, global unicast. Global unicast addresses in IPv6 are analogous to public IPv4 addresses. They are designed to be globally routable across the internet, enabling communication between devices located anywhere worldwide. Unlike other IPv6 address types, global unicast addresses are uniquely assigned to individual network interfaces and are not constrained by a local network or specific link. They adhere to a hierarchical structure, allowing for efficient routing across the internet. Multicast addresses (A) are used for one-to-many communication within a network, not for general internet routing. Unique local addresses (B) function similarly to private IPv4 addresses, providing routing within private network domains

but not publicly. Link-local addresses (C) are confined to a single link and aren't routable beyond that. Therefore, only global unicast addresses offer the same public, internet-routable characteristic as IPv4 public addresses. They enable direct, publicly routable, end-to-end communication.

Further Research:

**Cisco's official documentation on IPv6 addressing:**https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-sy/ipv6-15-sy-book/ip6-addr-overview.html
**RFC 4291 - IP Version 6 Addressing Architecture:**https://www.rfc-editor.org/rfc/rfc4291

## Question: 33

What is the expected outcome when an EUI-64 address is generated?

A.The interface ID is configured as a random 64-bit value
B.The characters FE80 are inserted at the beginning of the MAC address of the interface
C.The seventh bit of the original MAC address of the interface is inverted
D.The MAC address of the interface is used as the interface ID without modification

**Answer: C**

**Explanation:**

The correct answer is **C. The seventh bit of the original MAC address of the interface is inverted.**

EUI-64 (Extended Unique Identifier-64) is a method used to generate a 64-bit interface ID, often for IPv6 addresses. The process begins with the 48-bit MAC address of a network interface. To expand it to 64 bits, a specific pattern is followed. First, the 24-bit Organizationally Unique Identifier (OUI) portion of the MAC address (first three bytes) is kept unchanged. Then, "FFFE" (or hexadecimal 0xFFFE) is inserted in the middle, splitting the MAC address into two 24-bit parts. The remaining 24-bit part of the MAC address is then appended. Crucially, the seventh bit of the original MAC address, often referred to as the "universal/local" bit, is inverted. This bit, when set to 0, signifies a universally administered address, and when set to 1, indicates a locally administered one. EUI-64 modifies this bit to ensure uniqueness and differentiate the generated interface ID from the original MAC address. This ensures that the generated ID is unlikely to conflict with other interface IDs on the network. Option A is incorrect as EUI-64 does not use a random value. Option B is incorrect because FE80 is the link-local address prefix, not part of the EUI-64 process, and is prepended to the generated interface ID to create a link-local IPv6 address. Option D is incorrect because it doesn't modify the MAC address, a necessary step in EUI-64.

Further Research:

**Cisco Documentation on IPv6 Address Configuration:**https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-mt/ipv6-15-mt-book/ip6-addr-config.html
**Wikipedia on EUI-64:**https://en.wikipedia.org/wiki/EUI-64

## Question: 34

A corporate office uses four floors in a building.
☞ Floor 1 has 24 users.
☞ Floor 2 has 29 users.
Floor 3 has 28 users.
☞ Floor 4 has 22 users.
Which subnet summarizes and gives the most efficient distribution of IP addresses for the router configuration?

▪

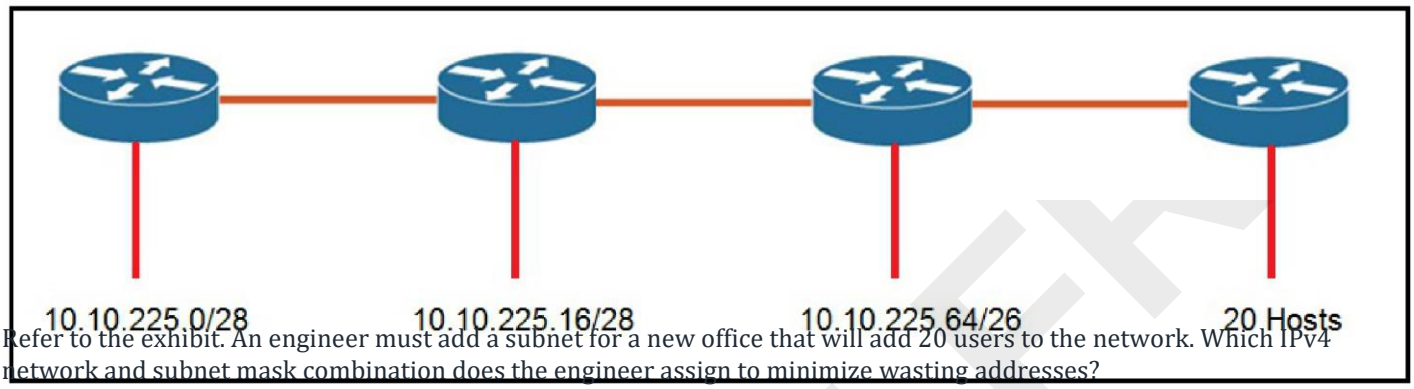
A.192.168.0.0/24 as summary and 192.168.0.0/28 for each floor
B.192.168.0.0/23 as summary and 192.168.0.0/25 for each floor
C.192.168.0.0/25 as summary and 192.168.0.0/27 for each floor
D.192.168.0.0/26 as summary and 192.168.0.0/29 for each floor

**Answer: C**

**Explanation:**

4 floors = 4 subnets. And you have a total of 103 users.How many bits do you need to have 103 addresses? You need 7 bits: (2^7 – 2) = 126 addresses.Starting from the 192.168.0.0 subnet that you're given, you must use a /25 subnet mask:255.255.255.1xxxxxxx = 255.255.255.128How many bits do you need to configure 4 subnets? You need 2 bits: (2^2) = 4 subnets. You have to borrow the two bits from the host ID. This way, the subnet mask, which is a /25 now, becomes a /27:255.255.255.111xxxxx = 255.255.255.224There are 5 bits remaining on the host ID. You have (2^5 – 2) = 30 addresses, and it fits the subnet on which you have the most users (floor 2).You started with a 192.168.0.0/25 subnet and you ended up with a 192.168.0.0/27
subnet.Answer C is correct.

## Question: 35




Refer to the exhibit. An engineer must add a subnet for a new office that will add 20 users to the network. Which IPv4 network and subnet mask combination does the engineer assign to minimize wasting addresses?

A. 10.10.225.48 255.255.255.240
B. 10.10.225.32 255.255.255.240
C. 10.10.225.48 255.255.255.224
D. 10.10.225.32 255.255.255.224

**Answer: D**

**Explanation:**

D is correct!Find the subnet mask*To have 20 User in a subnet We have to use /27 prefix * So Host count for /27 prefix is (2^5-2)=30* Subnet Mask for /27 prefix is (sum of Network bits (128+64+32)=224 , so
255.255.255.224Find the network ID*As per the /27 prefix each subnet has 30 host and 32 including network ID & Broadcast ID* so first network ID is 10.10.255.0 and the second will be 10.10.255.32

## Question: 36

What is a characteristic of spine-and-leaf architecture?

A.Each link between leaf switches allows for higher bandwidth.

B.It provides greater predictability on STP blocked ports.

C.It provides variable latency.

D.Each device is separated by the same number of hops.

**Answer: D**

**Explanation:**

The correct answer, D, highlights a core characteristic of spine-and-leaf architecture: each device is separated by the same number of hops. This architecture, commonly used in modern data centers, employs a two-layer design. Leaf switches, which connect directly to endpoints (servers, storage), are all interconnected to spine switches. The spine switches form the backbone. Crucially, any path between two leaf switches always traverses through exactly one spine switch. This consistent hop count provides predictable and low-latency communication. Option A is incorrect because individual links don't necessarily have higher
bandwidth; the aggregate bandwidth across all links is what's optimized. Option B is wrong since spine-leaf architectures often replace Spanning Tree Protocol (STP) with routing protocols for loop prevention, hence STP is less relevant. Finally, Option C is inaccurate; variable latency isn't a feature of spine-leaf which aims for consistent latency. The consistent one-hop distance ensures predictable performance and simplifies network design, facilitating scalability and minimizing complexities. This architecture contrasts with traditional three-tier designs where hop counts could vary considerably, impacting performance and troubleshooting.

For further research:

Cisco's Design Zone on Spine-Leaf Architecture: https://www.cisco.com/c/en/us/solutions/data-center-virtualization/design-zone/index.html (Look for relevant sections on spine-leaf)
Juniper Networks' explanation of Clos fabrics: https://www.juniper.net/us/en/research-library/webinars/building-modern-data-center-fabric.html (Clos architecture is often synonymous with spine-leaf).

## Question: 37

An office has 8 floors with approximately 30-40 users per floor. One subnet must be used. Which command must be configured on the router Switched Virtual
Interface to use address space efficiently?

A.ip address 192.168.0.0 255.255.0.0

B.ip address 192.168.0.0 255.255.254.0

C.ip address 192.168.0.0 255.255.255.128

D.ip address 192.168.0.0 255.255.255.224

**Answer: B**

**Explanation:**

The correct answer is **B. ip address 192.168.0.0 255.255.254.0**. This choice utilizes the subnet mask 255.255.254.0, which translates to a /23 CIDR notation. This subnet provides 512 total IP addresses (2^(32-23) = 2^9 = 512). Considering that there are approximately 30-40 users per floor across 8 floors, a single subnet needs to support roughly 240-320 users (8 floors * 30-40 users/floor). A /24 subnet (255.255.255.0) with 256 usable addresses would be insufficient for the entire office, thus requiring multiple subnets which the question excludes. A /23 subnet is the smallest subnet that can accommodate the required number of users. Option C's mask (255.255.255.128) translates to a /25, offering only 128 addresses; and Option D's mask (255.255.255.224) is a /27 offering only 32 addresses, both of which are inadequate for even a single floor, let alone the entire office. Option A's mask (255.255.0.0) or /16 would provide over 65,000 addresses

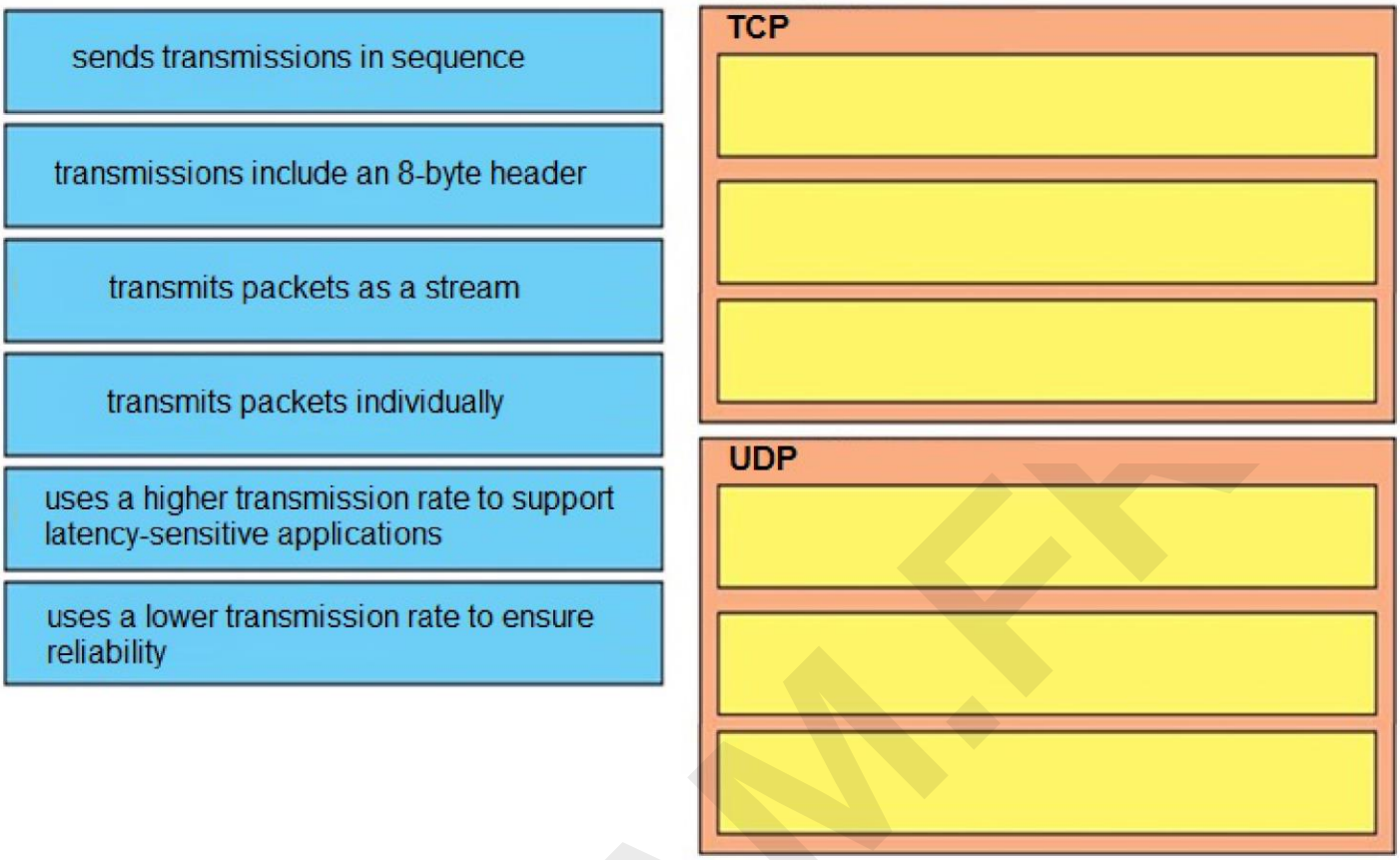
which is excessive and wasteful address space. Efficiency dictates using the smallest subnet mask that meets the need, and a /23 accomplishes this for the described scenario.

For further information on subnetting, CIDR, and IP addressing, you can explore these resources:

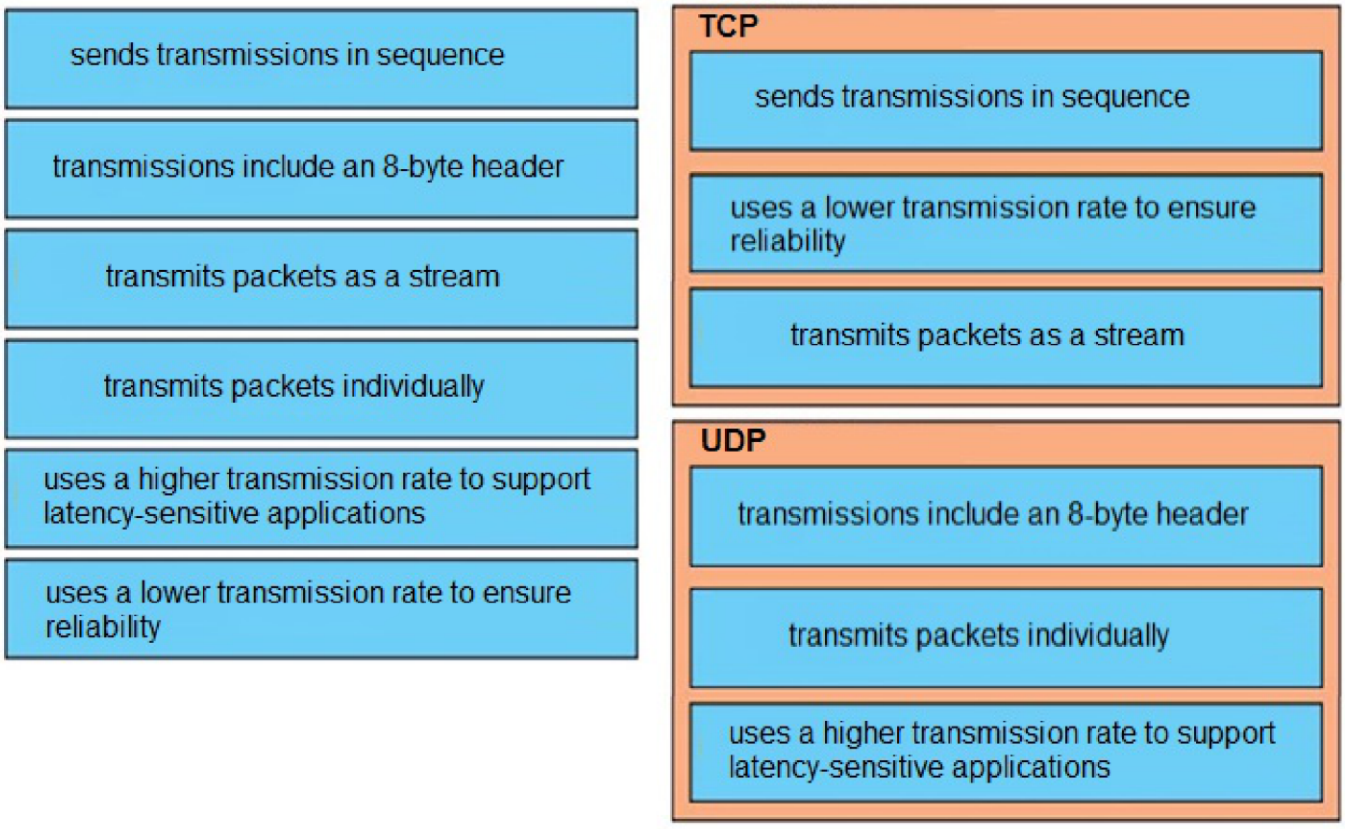
**Cisco's IP Addressing and Subnetting documentation:**
https://www.cisco.com/c/en/us/support/docs/ip/addressing/10715-subnet.html
**TechTarget's Subnet Mask Guide:**https://www.techtarget.com/searchnetworking/definition/subnet-mask
**Cloudflare's explanation on CIDR Notation:**https://www.cloudflare.com/learning/network-layer/what-is-cidr/

**Question: 38**

DRAG DROP -
Drag and drop the descriptions of IP protocol transmissions from the left onto the IP traffic types on the right.
Select and Place:




**Answer:**




**Question: 39**

A device detects two stations transmitting frames at the same time. This condition occurs after the first 64 bytes of the frame is received. Which interface counter increments?

A.runt
B.collision
C.late collision
D.CRC

**Answer: C**

**Explanation:**

The correct answer is **C. late collision**. Here's why:

In Ethernet networks, a collision occurs when two or more devices transmit simultaneously, causing signal interference. Collisions are normal in shared media environments (like older Ethernet hubs), but they need to be managed to ensure successful data transmission. There are two types of collisions: regular collisions and late collisions.

A regular collision occurs within the first 64 bytes (or the preamble + the first 64 bytes) of a frame transmission. This is within the 'collision window' and is expected in shared environments. A 'runt' frame is a frame smaller than the minimum size (64 bytes including FCS), often caused by early termination due to these collisions.

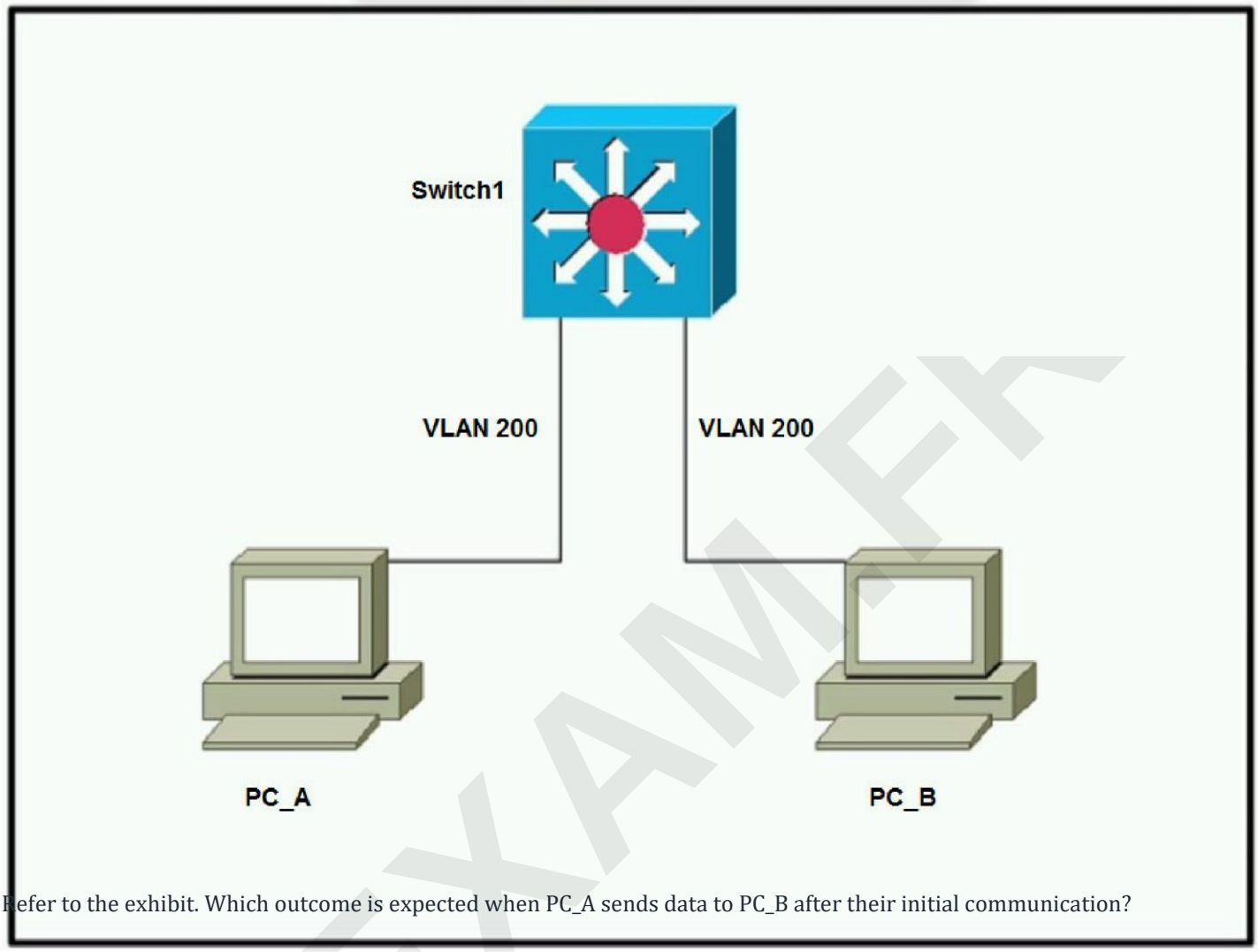
A **late collision**, however, happens after the first 64 bytes of the frame have been transmitted. This indicates a more severe problem, often stemming from issues like excessive cable length, faulty cabling, incorrect duplex settings, or hardware malfunctions. A late collision implies that the sending devices might not be "hearing" each other correctly, leading to transmissions colliding even though they should have been aware of ongoing activity and waited.

Because the problem states the collision happens after the first 64 bytes have been transmitted, it is a **late collision**. The "collision" counter, option B, would be incremented for a regular collision that occurs during the preamble and the first 64 bytes of a transmission. A CRC error (option D) indicates data corruption issues during transmission and is a different scenario.

**Authoritative Links:**

**Cisco Documentation on Ethernet Collisions:** [Search on Cisco.com for "Ethernet collision types" or consult their documentation related to networking fundamentals and troubleshooting.]
**Wikipedia on Ethernet:** [https://en.wikipedia.org/wiki/Ethernet](Specifically sections on Collision and Collision Domain)
**Techopedia on Late Collision:** [https://www.techopedia.com/definition/19594/late-collision](This gives a good overview of what a late collision means).

**Question: 40**




Refer to the exhibit. Which outcome is expected when PC_A sends data to PC_B after their initial communication?

A.The source MAC address is changed.
B.The destination MAC address is replaced with ffff.ffff.ffff.
C.The source and destination MAC addresses remain the same.
D.The switch rewrites the source and destination MAC addresses with its own.

**Answer: C**

**Explanation:**

You have a TCP/IP network. This means that PC A and PC B have an IP address each. PC A knows PC B's address and creates an IP packet for PC B. Then, the packet (Layer 3) becomes an Ethernet frame (Layer 2): PC A gets PC B's MAC address and uses it as the destination L2 address.When the frame arrives at SW1, the switch looks at the destination MAC address and controls (in its MAC table) to which port that address is associated. Then, the switch sends the frame to PC B through that port (forwarding phase).The switch leaves unchanged BOTH the source and the destination MAC addresses inside the frame.Answer C is correct.

**Question: 41**

Using direct sequence spread spectrum, which three 2.4-GHz channels are used to limit collisions?

A.5, 6, 7
B.1, 2, 3
C.1, 6, 11
D.1, 5, 10

**Answer: C**

**Explanation:**

The correct answer is C: 1, 6, and 11. Direct Sequence Spread Spectrum (DSSS), used in 2.4 GHz Wi-Fi, divides the available bandwidth into channels. To minimize interference and collisions between overlapping wireless networks, it's crucial to use non-overlapping channels. In the 2.4 GHz band, each channel is 22 MHz wide, but channels are spaced 5 MHz apart. This means channels directly adjacent to each other significantly overlap.
Therefore, using channels 1, 6, and 11 provides the maximum separation and avoids substantial overlap.
Channel 1, using center frequency 2412 MHz, when active will overlap with channel 2, 3 and parts of 4.
Channel 6 using center frequency 2437 MHz overlaps with channel 4, 5, 7 and 8. Channel 11 using center frequency 2462 MHz overlaps with 9, 10, parts of 8 and 12.

Choosing channels 1, 6, and 11 ensures that each signal has minimal interference from the others. Using channels like 1, 2, and 3 would cause significant overlap. This leads to increased packet collisions, resulting in slower throughput and unreliable wireless performance. The spacing between these non-overlapping channels is typically sufficient for most environments to maintain good signal quality and minimize interference.

Authoritative Link 1: 802.11 Wireless LAN - WikipediaAuthoritative Link 2: Understanding Wireless Channels

**Question: 42**

How do TCP and UDP differ in the way they guarantee packet delivery?

A. TCP uses retransmissions, acknowledgment, and parity checks, and UDP uses cyclic redundancy checks only
B. TCP uses two-dimensional parity checks, checksums, and cyclic redundancy checks, and UDP uses retransmissions only
C. TCP uses checksum, acknowledgements, and retransmissions, and UDP uses checksums only
D. TCP uses checksum, parity checks, and retransmissions, and UDP uses acknowledgements only

**Answer: C**

**Explanation:**

The correct answer is C. TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) handle packet delivery reliability differently. TCP is a connection-oriented protocol that prioritizes reliable data transfer. It achieves this through a combination of mechanisms: a checksum for error detection, acknowledgments (ACKs) to confirm successful packet reception, and retransmissions to resend packets that are lost or corrupted. When a sender doesn't receive an ACK for a sent packet within a specified time, it assumes loss and retransmits. This ensures that data reaches its destination in the correct order and without loss. In contrast, UDP is a connectionless protocol that emphasizes speed over reliability. It primarily uses a checksum to detect errors, but does not implement acknowledgments or retransmissions. UDP is therefore "best-effort", making it suitable for applications where minor data loss is tolerable and low latency is important, like real-time streaming or online gaming. Because TCP ensures order and reliable transmission, it has higher overhead than UDP.**Authoritative Links:**

TCP Overview: Cloudflare's explanation of TCP, including reliability mechanisms.
UDP Overview: Cloudflare's explanation of UDP, including its lack of reliability mechanisms.
Computer Networking: A Top-Down Approach (Kurose & Ross): A well-known networking textbook that dives into the intricacies of TCP and UDP (look for chapters on transport protocols).

This clear distinction between TCP's reliable mechanisms and UDP's lack of these explains why option C accurately describes the differences in their packet delivery guarantees.

## Question: 43

A wireless administrator has configured a WLAN; however, the clients need access to a less congested 5-GHz network for their voice quality. What action must be taken to meet the requirement?

A.enable Band Select
B.enable DTIM
C.enable RX-SOP
D.enable AAA override

**Answer: A**

**Explanation:**

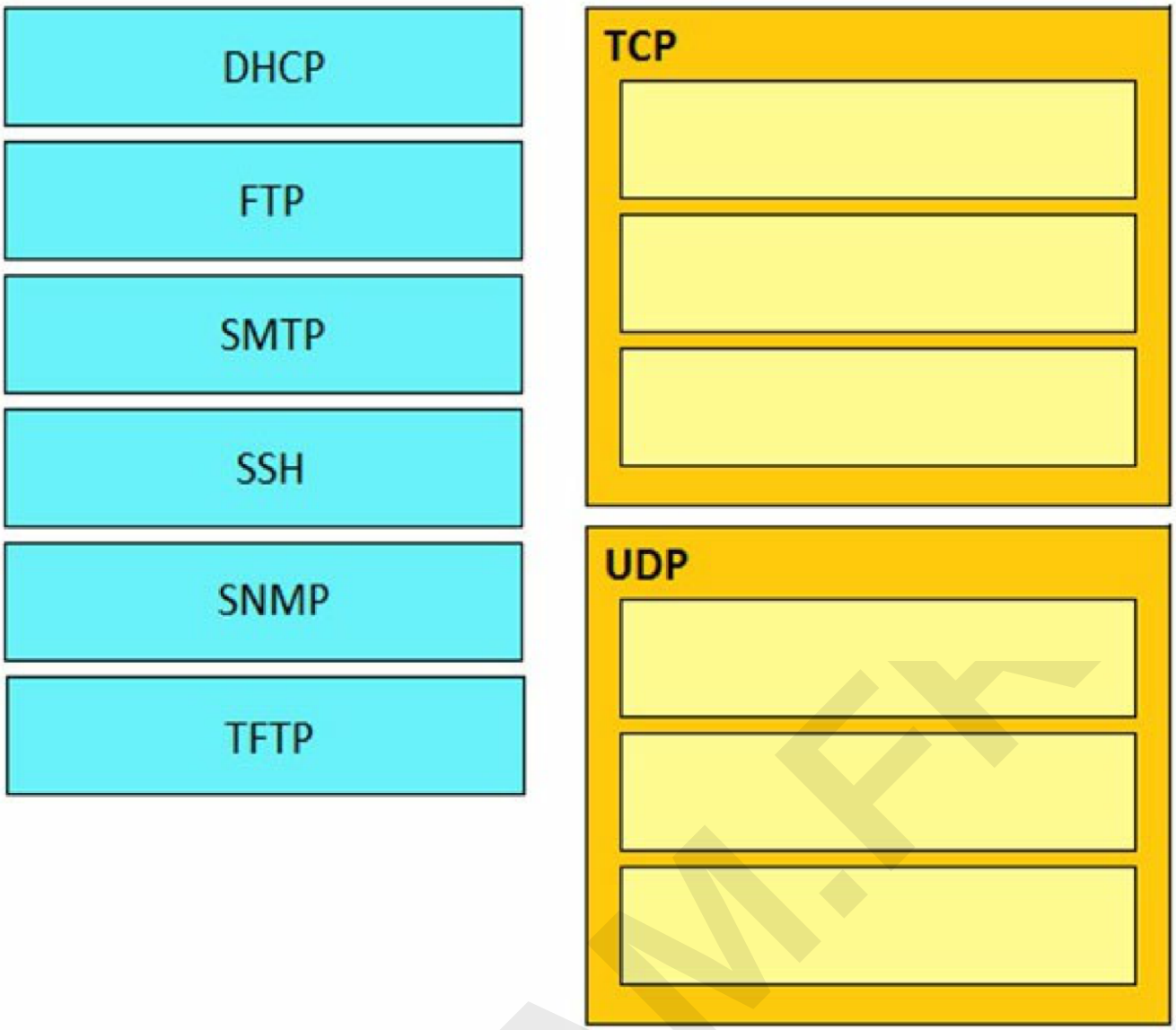
The correct answer is **A. enable Band Select**. Band Select is a feature that encourages dual-band (2.4 GHz and 5 GHz) wireless clients to connect to the less congested 5 GHz band. This mechanism operates by delaying or suppressing beacon transmissions on the 2.4 GHz band, effectively steering capable clients toward the 5 GHz band. This is beneficial because the 5 GHz band generally experiences less interference and offers more channels, leading to better performance, particularly for latency-sensitive applications like voice. DTIM (Delivery Traffic Indication Message) is related to power saving and has no direct impact on band preference. RX-SOP (Receive Start-of-Packet) is a sensitivity threshold, adjusting the range and throughput, but doesn't prioritize bands. AAA override relates to authentication, authorization, and accounting parameters, and also does not control band selection. Band Select is explicitly designed for the task of prioritizing the 5 GHz band for suitable devices, thereby improving voice quality.

For more information, refer to:

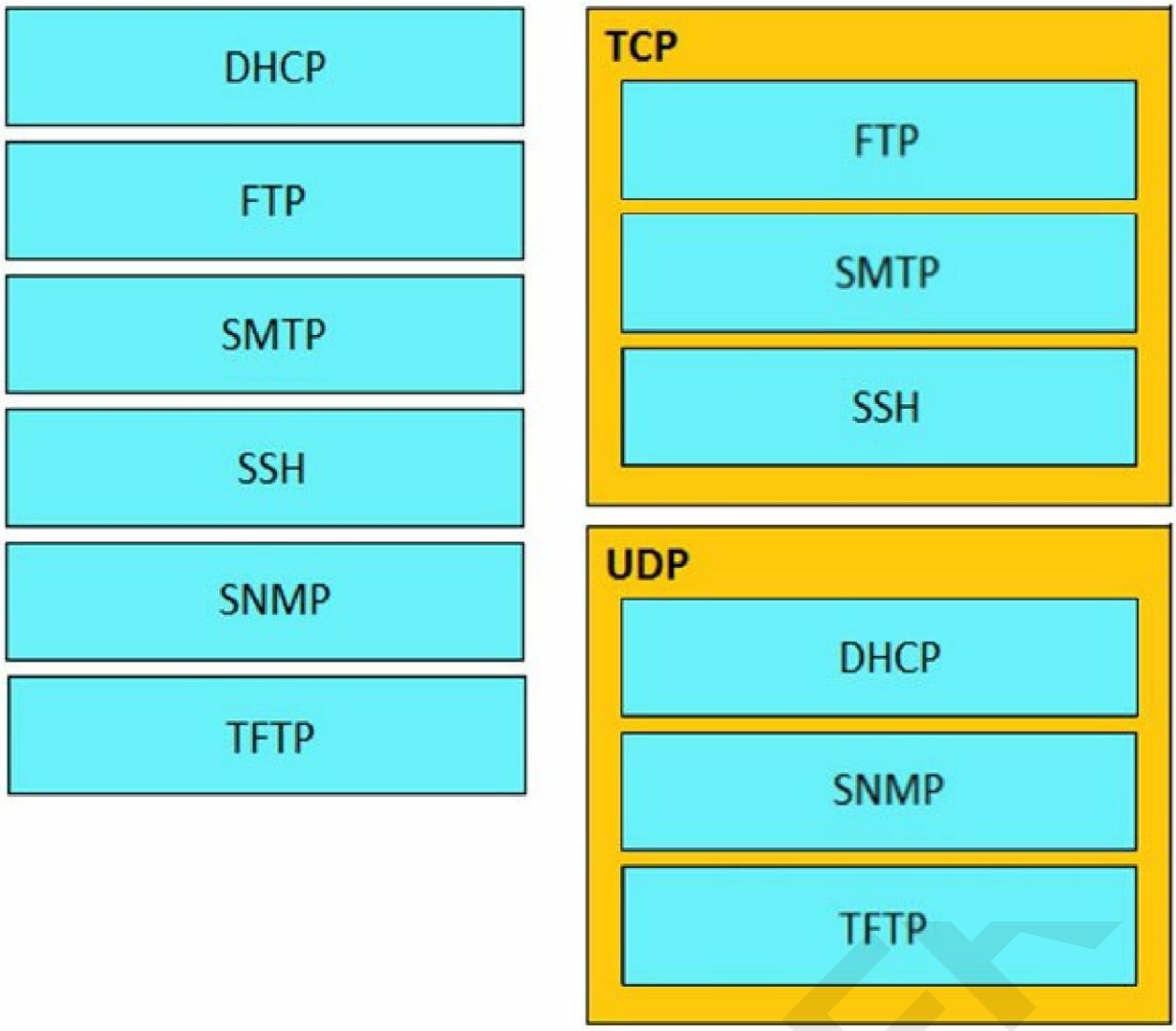
**Cisco Wireless LAN Controller Configuration Guide:**
https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/m_wlan_adv_features.html#concept_F1EE85E9E0854AD9A753FEF72C8A730C (search for "band select")
**Cisco Tech Blog on Band Select:**https://blogs.cisco.com/networking/band-steering-better-wireless-experience

**Question: 44**

DRAG DROP -
Drag and drop the application protocols from the left onto the transport protocols that it uses on the right.
Select and Place:




**Answer:**




**Question: 45**

What is the destination MAC address of a broadcast frame?

A. 00:00:0c:07:ac:01
B. ff:ff:ff:ff:ff:ff
C. 43:2e:08:00:00:0c
D. 00:00:0c:43:2e:08
E. 00:00:0c:ff:ff:ff

**Answer: B**

**Explanation:**

The correct answer is B, ff:ff:ff:ff:ff:ff, because this is the universally recognized MAC address for a broadcast. MAC addresses are 48-bit (6-byte) hexadecimal identifiers assigned to network interfaces for layer 2 (data link layer) communication. A broadcast frame is intended to be received by every device on the local network segment, also known as the broadcast domain. Therefore, a special MAC address is required that all devices recognize as a signal that the frame should be processed by them. The MAC address consisting of all ones in binary (or all 'f's in hexadecimal) is precisely that address. It signals that the frame is not destined for a

specific device but rather all devices within the broadcast domain. Options A, C, D, and E are examples of unicast MAC addresses, which are intended for specific destinations, and are not used for broadcast traffic.

When a device transmits a broadcast frame, it sets the destination MAC address to ff:ff:ff:ff:ff:ff. Every network interface on the same Ethernet segment that receives the frame will process it. This differs from a unicast frame, where the destination MAC address identifies a single device. Understanding broadcast MAC addresses is fundamental to understanding how local area networks function and how devices discover each other and communicate. For further research, you can refer to the following:

IEEE 802 Standards: This is the official page for the IEEE 802 standards, particularly 802.3 (Ethernet) which defines MAC addressingCisco Documentation: Cisco's documentation provides in-depth explanations of MAC addresses in networking contexts.Computer Networking: A Top-Down Approach: This is a highly recommended textbook for deep dives into computer networking concepts like MAC addressing.

## Question: 46

For what two purposes does the Ethernet protocol use physical addresses?

A.to uniquely identify devices at Layer 2
B.to allow communication with devices on a different network
C.to differentiate a Layer 2 frame from a Layer 3 packet
D.to establish a priority system to determine which device gets to transmit first
E.to allow communication between different devices on the same network
F.to allow detection of a remote device when its physical address is unknown

**Answer: AE**

**Explanation:**

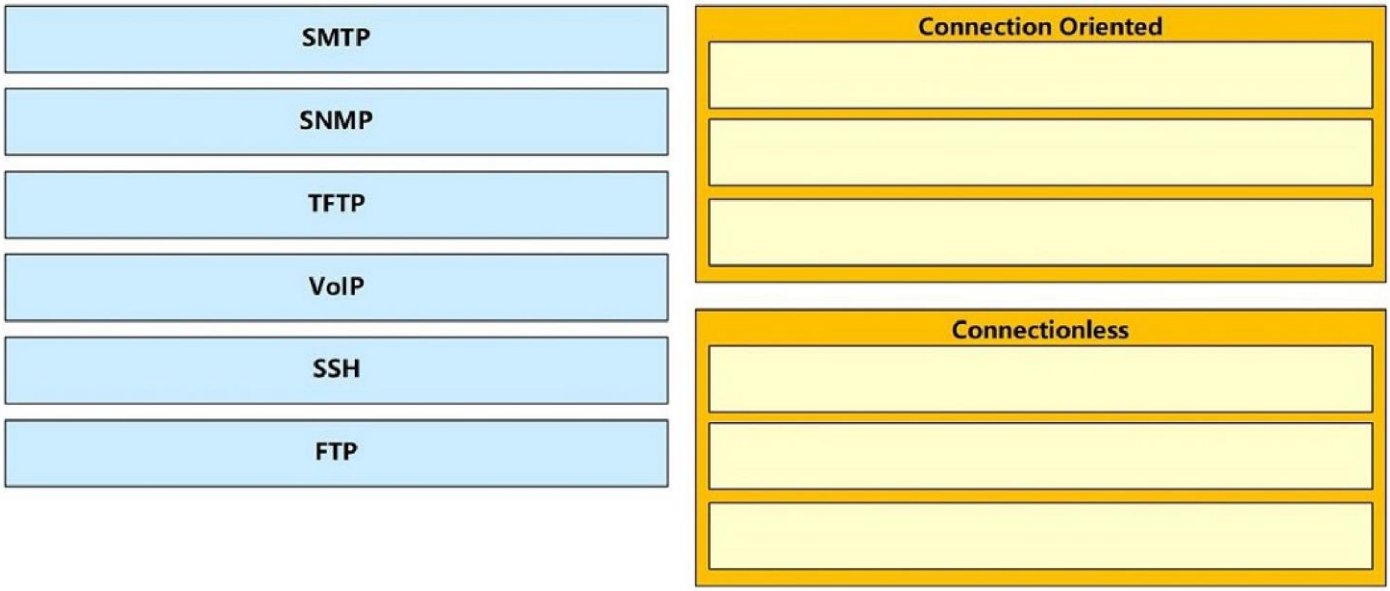
The Ethernet protocol, at Layer 2 of the OSI model (the Data Link Layer), primarily uses physical addresses, also known as MAC addresses, for two fundamental purposes. Option A is correct because MAC addresses provide a unique identifier for each network interface card (NIC). This uniqueness allows devices to be distinguished from one another on the local network. Option E is also correct as MAC addresses are crucial for enabling communication between devices residing on the same network segment or local area network (LAN). When a device needs to send data, it encapsulates the data into an Ethernet frame, including the destination MAC address. Switches use these MAC addresses to learn the locations of devices on the network and then forward frames only to the intended recipient. Options B, C and D are not correct because those are not the primary purposes of physical addressing at the Ethernet level.

Further Research:

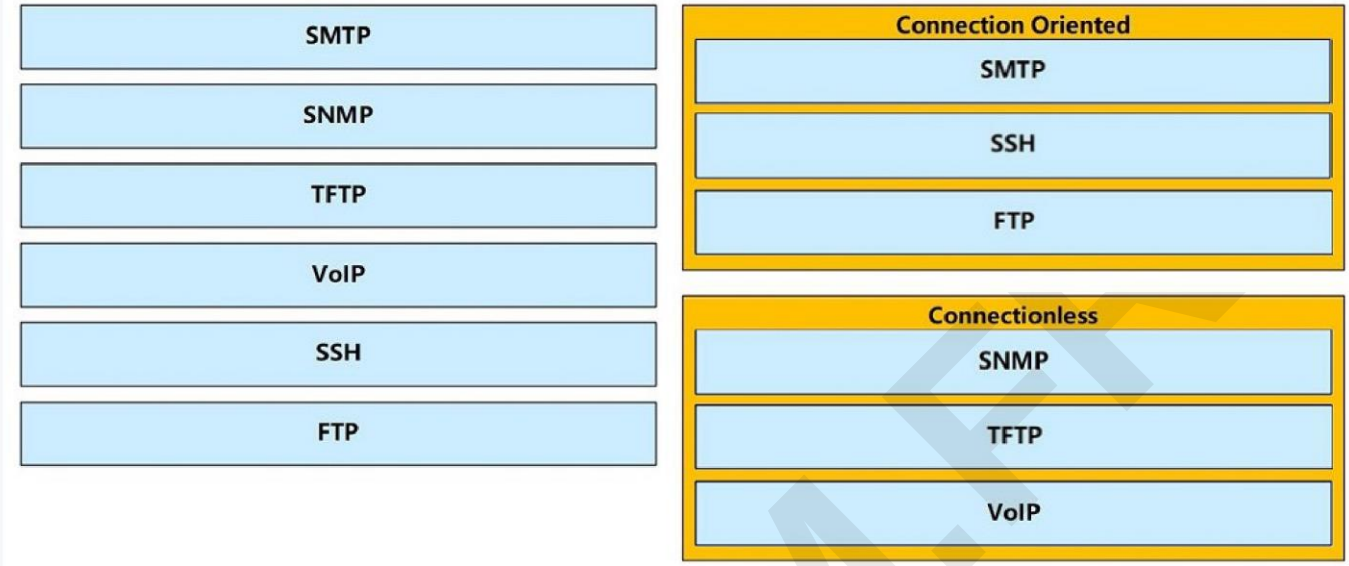
**Cisco - Understanding Ethernet Addressing:**https://www.cisco.com/c/en/us/support/docs/lan-switching/ethernet/12186-addressing.html
**TechTarget - MAC Address:**https://www.techtarget.com/searchnetworking/definition/MAC-address
**Wikipedia - MAC Address:**https://en.wikipedia.org/wiki/MAC_address

## Question: 47

DRAG DROP -
Drag and drop the networking parameters from the left on to the correct values on the right.
Select and Place:




**Answer:**




**Explanation:**
SSH uses TCP port 22 while SNMP uses UDP port 161 and 162.

## Question: 48

Which component of an Ethernet frame is used to notify a host that traffic is coming?

A. start of frame delimiter
B. Type field
C. preamble
D. Data field

**Answer: C**

**Explanation:**

The correct answer is **C. preamble**. The preamble is a crucial component of an Ethernet frame, acting as a synchronization signal for receiving hosts. It's a sequence of alternating 1s and 0s (typically 7 bytes or 56 bits)

that precedes the Start Frame Delimiter (SFD). This rhythmic pattern allows the receiving network interface card (NIC) to lock onto the incoming signal's timing and prepare for data reception. The NIC uses this time to synchronize its clock with the sending device's clock, thus ensuring accurate data capture and interpretation.

Think of it as a "wake-up" call; the receiving NIC isn't constantly listening but needs a signal to initiate the process of processing the subsequent data. Without a preamble, the receiver would have difficulty determining the beginning of the frame and could easily misinterpret the data.

While the Start of Frame Delimiter (SFD, answer choice A) marks the end of the preamble and the beginning of the actual data frame, it doesn't perform the initial synchronization role. It's the preamble that gets the receiver ready for the rest of the frame. The Type field (B) indicates the type of protocol encapsulated in the data field, and the Data field (D) carries the actual information being transmitted. Therefore, neither B nor D are involved in the initial notification of incoming traffic.

To illustrate, if a radio station doesn't provide a 'station is starting now' signal and just plays music straight away, it would be hard for listeners to tune in precisely. In the same way, the preamble ensures the receiver can correctly receive an incoming packet of data.

For further research, consider these authoritative sources:

**Cisco's official documentation on Ethernet frames:**https://www.cisco.com/c/en/us/support/docs/lan-switching/ethernet/10985-ethernet-frames.html
**Wikipedia's page on Ethernet Frame:**https://en.wikipedia.org/wiki/Ethernet_frame
**IEEE 802.3 Standard:**https://standards.ieee.org/ieee/802/3/ (This is the technical specification of Ethernet but might be quite dense)

## Question: 49

You are configuring your edge routers interface with a public IP address for Internet connectivity. The router needs to obtain the IP address from the service provider dynamically.
Which command is needed on interface FastEthernet 0/0 to accomplish this?

A.ip default-gateway
B.ip route
C.ip default-network
D.ip address dhcp
E.ip address dynamic

**Answer: D**

**Explanation:**

The correct command is **D. ip address dhcp**. This command configures the interface to obtain its IP address, subnet mask, and default gateway information automatically from a DHCP server. In this scenario, the service provider's network is expected to have a DHCP server that will assign these parameters to the router's interface.

Option A, ip default-gateway, is used to specify a gateway of last resort for networks not explicitly defined in the routing table, but not for obtaining an IP address. Option B, ip route, is for manually configuring static routes, not dynamic IP assignment. Option C, ip default-network, is related to classful routing and is not used for DHCP. Option E, ip address dynamic, is not a valid command in Cisco IOS for DHCP configuration.

DHCP (Dynamic Host Configuration Protocol) is a network management protocol used on IP networks. It allows network devices to automatically obtain IP addresses and other network configuration parameters from a DHCP server, reducing the manual configuration burden on network administrators. In this case, the

router's FastEthernet 0/0 interface acts as a DHCP client, requesting an IP configuration from the service provider's DHCP server. By using ip address dhcp, the router will broadcast a DHCP Discover message, which the service provider's DHCP server will respond to, assigning an available IP address to the router's interface.

This dynamic allocation is common in scenarios where public IP addresses are provided by internet service providers. This dynamic approach also simplifies network configuration and improves scalability. The use of DHCP is fundamental for modern network deployments where manual IP address configuration would be inefficient and error-prone.

**Authoritative Links:**

**Cisco Documentation on IP Addressing:**https://www.cisco.com/c/en/us/support/docs/ip/address-management/13708-dhcp-server.html
**Cisco Command Reference for "ip address dhcp":**https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr/command/ipaddr-cr-book/ipaddr-i1.html#wp1009611

## Question: 50

Which two statements about the purpose of the OSI model are accurate? (Choose two.)

A.Defines the network functions that occur at each layer
B.Facilitates an understanding of how information travels throughout a network
C.Changes in one layer do not impact other layer
D.Ensures reliable data delivery through its layered approach

**Answer: AB**

**Explanation:**

The correct answers are A and B. The OSI (Open Systems Interconnection) model is a conceptual framework that standardizes how different networking systems should communicate. Option A, "Defines the network functions that occur at each layer," is accurate. The OSI model divides network communication into seven distinct layers, each with specific responsibilities. These range from the physical transmission of bits at the Physical layer to application-specific protocols at the Application layer. Understanding these layer-specific functions is crucial for troubleshooting and designing networks. Option B, "Facilitates an understanding of how information travels throughout a network," is also correct. By following the path of data as it moves up and down the layers of the OSI model, one can gain a clear picture of how data is prepared for transmission, transmitted, and received and processed. This step-by-step view is foundational to comprehending network communication. Option C, "Changes in one layer do not impact other layer," is incorrect. While the goal is to promote modularity and minimize dependencies, a change in one layer, especially in lower layers, often necessitates changes or adjustments in higher layers. For example, a change in the Physical layer's transmission medium may influence the Data Link layer's framing process. Option D, "Ensures reliable data delivery through its layered approach," is partly true, but it's not the primary purpose of the OSI model. Some layers, like the Transport layer, do have mechanisms for reliability (e.g., error checking and retransmission), but the OSI model's purpose is primarily about structuring communication, not dictating specific reliability mechanisms at all layers. The OSI model's primary goals are to provide a standardized way to understand network communications and a structure for developing networking protocols.

For further reading and confirmation, see:

Cisco's explanation of the OSI Model
TechTarget's definition of the OSI Model

**Question: 51**

Which three statements about MAC addresses are correct? (Choose three.)

A. To communicate with other devices on a network, a network device must have a unique MAC address

B. The MAC address is also referred to as the IP address

C. The MAC address of a device must be configured in the Cisco IOS CLI by a user with administrative privileges

D. A MAC address contains two main components, the first of which identifies the manufacturer of the hardware and the second of which uniquely identifies the hardware

E. An example of a MAC address is 0A:26:B8:D6:65:90

F. A MAC address contains two main components, the first of which identifies the network on which the host resides and the second of which uniquely identifies the host on the network

**Answer: ADE**

**Explanation:**

Here's a detailed justification for why options A, D, and E are correct regarding MAC addresses, and why B, C, and F are incorrect:

**A. To communicate with other devices on a network, a network device must have a unique MAC address.** This is fundamentally true. MAC addresses (Media Access Control addresses) serve as unique identifiers at the data link layer of the OSI model. They are crucial for devices to communicate within a local network because they are used to direct frames between devices on the same broadcast domain. Without a unique MAC address, devices wouldn't be able to distinguish each other, leading to communication failures.

**D. A MAC address contains two main components, the first of which identifies the manufacturer of the hardware and the second of which uniquely identifies the hardware.** This statement accurately describes the structure of a MAC address. The first 24 bits (or 3 bytes) constitute the Organizationally Unique Identifier (OUI), which identifies the manufacturer of the network interface card (NIC). The remaining 24 bits are assigned by the manufacturer to uniquely identify each device they produce, ensuring no two devices share the same MAC address.

**E. An example of a MAC address is 0A:26:B8:D6:65:90.** This is correct. MAC addresses are typically represented in hexadecimal format, using colon, hyphen, or period as separators. The example provided adheres to this standard and is a valid representation of a MAC address.

**Why B is incorrect:** The MAC address is not the same as the IP address. IP addresses operate at the network layer and are used for logical addressing across networks. MAC addresses are physical addresses tied to the hardware.**Why C is incorrect:** MAC addresses are typically burned into the hardware and aren't configured by users. While some NICs may allow MAC address spoofing in certain cases, they are not routinely set via the Cisco IOS CLI.**Why F is incorrect:** A MAC address identifies the manufacturer of the hardware and a specific instance of that hardware. It does not identify the network the host resides on or the specific host within that network. That is the role of an IP address.

**Authoritative links for further research:**

1. **IEEE Standards Association:** The IEEE manages the OUI registry for MAC addresses. You can find detailed information about the OUI assignments here: https://standards.ieee.org/products-services/regauth/oui/
2. **Cisco - Understanding MAC Addresses:** Cisco provides detailed documentation on how MAC addresses function within networks. You can find relevant materials on their website by searching for "Understanding MAC Addresses" on Cisco.com
3. **Wikipedia: MAC address:**https://en.wikipedia.org/wiki/MAC_addressThis is a good starting point for understanding the concept of MAC addresses.

In summary, MAC addresses are fundamental to local network communication, uniquely identifying devices based on manufacturer-assigned values. Options A, D, and E correctly reflect their properties, while B, C, and F are based on misconceptions about MAC addresses.

## Question: 52

Which technique can you use to route IPv6 traffic over an IPv4 infrastructure?

A.NAT
B.6 to 4 tunneling
C.L2TPv3
D.dual-stack

**Answer: B**

**Explanation:**

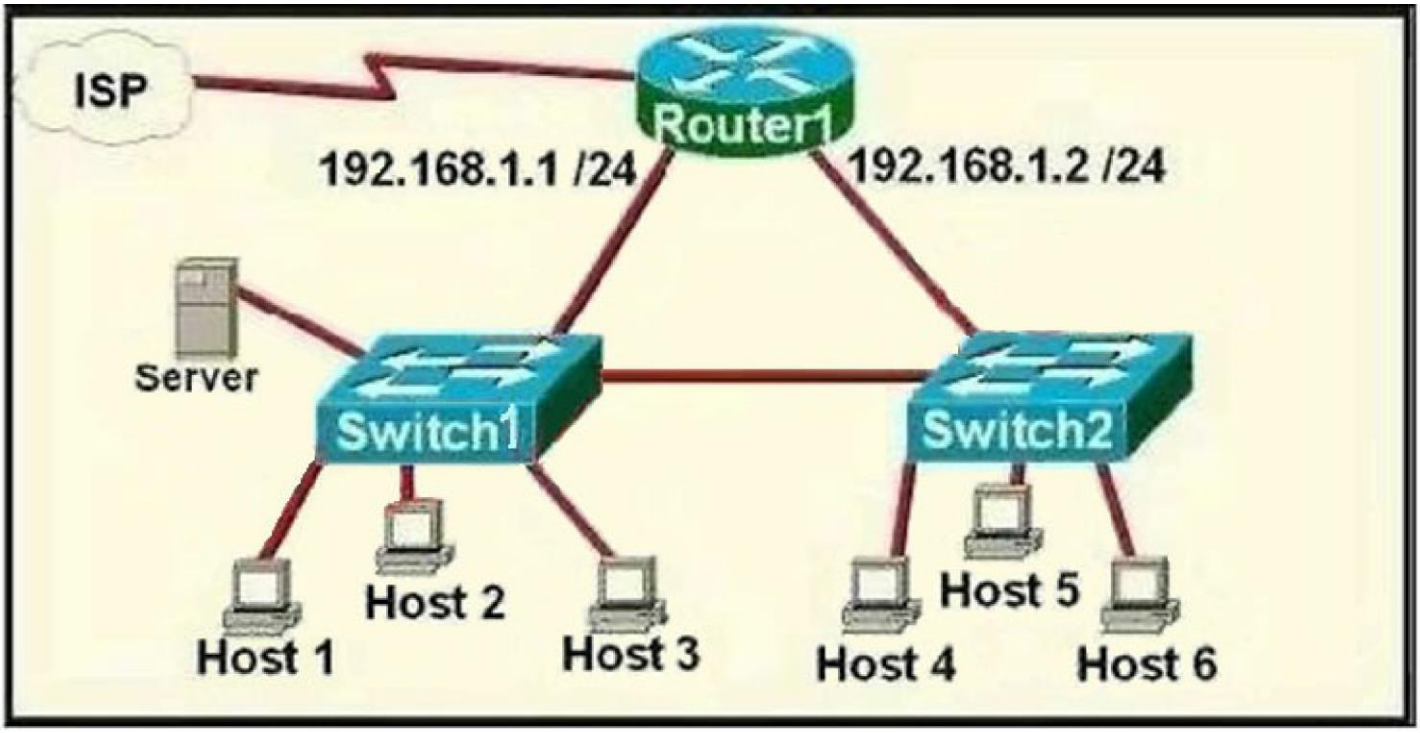
The correct answer is B, **6to4 tunneling**. 6to4 tunneling is a mechanism that allows IPv6 packets to be transmitted over an IPv4 network. It achieves this by encapsulating IPv6 packets within IPv4 headers, effectively creating a tunnel through the IPv4 infrastructure. This enables IPv6-enabled devices to communicate even when connected via IPv4-only networks. The IPv4 address of the tunnel endpoint is embedded into the IPv6 address, creating the mapping between IPv6 and IPv4. NAT (A) translates IP addresses but doesn't inherently facilitate IPv6 routing over IPv4. L2TPv3 (C) is a tunneling protocol used primarily for VPNs and not for IPv6 over IPv4 routing. Dual-stack (D) refers to running both IPv4 and IPv6 simultaneously on a device, but it doesn't solve the specific problem of routing IPv6 across an IPv4 infrastructure. 6to4 tunneling is explicitly designed for that purpose by dynamically creating IPv6 tunnels based on the IPv4 addressing of the tunnel endpoints. The tunnel endpoints are usually public IP addresses and the IPv6 addresses are derived from the IPv4 addresses. It is a straightforward way of transitioning to IPv6 networks without requiring complete replacement of IPv4 infrastructure.

Authoritative links:

RFC 3056 - Connection of IPv6 Domains via IPv4 Clouds
Cisco: Understanding IPv6 Tunneling

## Question: 53

Refer to the exhibit. A network technician is asked to design a small network with redundancy. The exhibit represents this design, with all hosts configured in the same VLAN. What conclusions can be made about this design?




A. This design will function as intended.

B. Spanning-tree will need to be used.

C. The router will not accept the addressing scheme.

D. The connection between switches should be a trunk.

E. The router interfaces must be encapsulated with the 802.1Q protocol.

**Answer: C**

**Explanation:**
Each interface on a router must be in a different network. If two interfaces are in the same network, the router will not accept it and show error when the administrator assigns it.

**Question: 54**

Which two statements are true about the command ip route 172.16.3.0 255.255.255.0 192.168.2.4? (Choose two.)

A. It establishes a static route to the 172.16.3.0 network.

B. It establishes a static route to the 192.168.2.0 network.

C. It configures the router to send any traffic for an unknown destination to the 172.16.3.0 network. D. It configures the router to send any traffic for an unknown destination out the interface with the address 192.168.2.4.

E. It uses the default administrative distance.

F. It is a route that would be used last if other routes to the same destination exist.

**Answer: AE**

**Explanation:**

Okay, let's break down why options A and E are the correct answers for the ip route 172.16.3.0 255.255.255.0 192.168.2.4 command, and why the others are incorrect.

**Explanation:**

The ip route command in Cisco IOS is used to configure static routes. The syntax generally follows the pattern:

ip route [destination_network] [subnet_mask] [next_hop_address or exit_interface].

**Option A: "It establishes a static route to the 172.16.3.0 network."** This is correct. The first part of the command, 172.16.3.0 255.255.255.0, explicitly defines the destination network as 172.16.3.0 with a subnet mask of 255.255.255.0 (a /24 network). The command tells the router that any traffic destined for this specific network should be forwarded according to the rest of the command's configuration.

**Option B: "It establishes a static route to the 192.168.2.0 network."** This is incorrect. The 192.168.2.4 is not a network. It represents the IP address of the next hop router, which is the immediate interface the current router needs to send packets toward to reach the destination.

**Option C: "It configures the router to send any traffic for an unknown destination to the 172.16.3.0 network."** This is incorrect. This describes a default route (often configured as 0.0.0.0 0.0.0.0), not a static route to a specific network like 172.16.3.0. The router will only use this route for traffic destined specifically to 172.16.3.0/24.

**Option D: "It configures the router to send any traffic for an unknown destination out the interface with the address 192.168.2.4."** This is incorrect. The command specifies that traffic destined to 172.16.3.0 should be forwarded to the router at 192.168.2.4. It does not indicate the router will forward any unknown traffic to this interface. A gateway of last resort would use the ip default-gateway or the ip route 0.0.0.0 0.0.0.0 <next_hop> to achieve that.

**Option E: "It uses the default administrative distance."** This is correct. Static routes have a default administrative distance of 1. Administrative distance is a measure of the trustworthiness of a route; lower values are preferred. If there is a dynamic route (e.g., from routing protocols like OSPF or EIGRP) to the same network, the static route (with AD of 1) is given priority over these dynamic routes which have a higher AD.

**Option F: "It is a route that would be used last if other routes to the same destination exist."** This is incorrect. As explained in Option E, a static route has an AD of 1, making it more preferred than dynamic routes to the same destination.

**In summary:** The ip route 172.16.3.0 255.255.255.0 192.168.2.4 command creates a static route to network 172.16.3.0 via the router at 192.168.2.4, and it uses the default administrative distance of 1.

**Authoritative Links:**

**Cisco Documentation on IP Routing:**https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_pi/configuration/15-sy/iproute-pi-15-sy-book/ip-static-rt.html
**Cisco on Administrative Distance:**https://www.cisco.com/c/en/us/support/docs/ip/routing/15939-admndist.html

These links will provide further detailed information regarding Cisco IP routing and the usage of the ip route command, along with explanations of administrative distance.

## Question: 55

What are two benefits of private IPv4 IP addresses? (Choose two.)

A. They are routed the same as public IP addresses.
B. They are less costly than public IP addresses.
C. They can be assigned to devices without Internet connections.
D. They eliminate the necessity for NAT policies.
E. They eliminate duplicate IP conflicts.

**Answer: BC**

**Explanation:**

Private IPv4 addresses offer distinct advantages related to cost and network scope. Option B is correct because private IP addresses are free to use within a private network; unlike public IP addresses which require registration and can incur costs. This cost-effectiveness makes private IP addressing ideal for internal networks. Option C is also correct as private addresses are not intended for routing on the public internet. This means they can be assigned to devices that do not require direct internet connectivity, such as servers within a data center or local network devices like printers. The absence of public internet routing makes them suitable for internal use and avoids the depletion of public IPv4 address space. Option A is incorrect; private IP addresses require Network Address Translation (NAT) to communicate with the public internet as they are not routable across it directly. Option D is incorrect because NAT policies are essential when using private IP addresses to connect to the internet. NAT translates private addresses into public addresses for internet communication. Option E is incorrect; private IP address ranges can be re-used across different private networks, leading to potential conflicts if not properly managed within a single private network. Therefore, careful planning and administration are still required.

Further Research:

**RFC 1918:**https://www.rfc-editor.org/rfc/rfc1918 - This document specifies the address allocation for private internets.

**Cisco Documentation on IP Addressing:**https://www.cisco.com/c/en/us/support/docs/ip/addressing/13882-private-ip.html - Cisco's guide on private IP addressing, usage and benefits.

## Question: 56

What are two benefits that the UDP protocol provide for application traffic? (Choose two.)

A. UDP traffic has lower overhead than TCP traffic
B. UDP provides a built-in recovery mechanism to retransmit lost packets
C. The CTL field in the UDP packet header enables a three-way handshake to establish the connection
D. UDP maintains the connection state to provide more stable connections than TCP
E. The application can use checksums to verify the integrity of application data

**Answer: AE**

**Explanation:**

Here's a detailed justification for the correct answer choices, A and E:

**Choice A: UDP traffic has lower overhead than TCP traffic.** This is a core characteristic of UDP. Unlike TCP, which includes sequence numbers, acknowledgments, and flow control mechanisms, UDP has a much simpler header. This minimal overhead translates to less data being transmitted, resulting in faster transmission speeds and reduced bandwidth consumption. This efficiency is especially beneficial for applications that prioritize speed over reliability, such as streaming video or real-time gaming. The absence of connection establishment also contributes to this lower overhead.

**Choice E: The application can use checksums to verify the integrity of application data.** While UDP itself doesn't provide robust data recovery, it does include a checksum field in its header. This checksum allows the receiving application to detect if any data corruption occurred during transmission. If a checksum mismatch is detected, the receiving application can choose to discard the damaged data and, if necessary, request retransmission from the sending application (though UDP does not handle this itself). This provides a basic level of data integrity verification.

**Why the other choices are incorrect:**

**B: UDP provides a built-in recovery mechanism to retransmit lost packets.** This is incorrect. UDP does not have a built-in mechanism to retransmit lost packets. It's a connectionless protocol, meaning it sends data without establishing a session or tracking delivery. If packets are lost, UDP does not handle this, it's up to the application layer to implement retransmission if necessary.

**C: The CTL field in the UDP packet header enables a three-way handshake to establish the connection.**

There's no CTL field in UDP header and furthermore, UDP does not use a three-way handshake. UDP is connectionless and doesn't establish a session before transmitting data.

**D: UDP maintains the connection state to provide more stable connections than TCP.** This is incorrect. UDP is connectionless and does not maintain any connection state, which makes it inherently less stable in terms of guaranteeing data delivery compared to TCP.

**Authoritative Links for Further Research:**

**Cisco - TCP and UDP:**https://www.cisco.com/c/en/us/support/docs/ip/transmission-control-protocol-tcp/27612-tcp-udp.html
**Cloudflare - UDP Protocol Explained:**https://www.cloudflare.com/learning/ddos/glossary/udp-protocol/
**Wikipedia - User Datagram Protocol:**https://en.wikipedia.org/wiki/User_Datagram_Protocol

In summary, UDP's primary advantages stem from its low overhead and the inclusion of a checksum for data integrity verification. These features make it a suitable choice for applications where speed is paramount and some data loss can be tolerated or handled by higher layers.

## Question: 57

Which two goals reasons to implement private IPv4 addressing on your network? (Choose two.)

A. Comply with PCI regulations
B. Conserve IPv4 address
C. Reduce the size of the forwarding table on network routers
D. Reduce the risk of a network security breach
E. Comply with local law

**Answer: BD**

**Explanation:**

Private IPv4 addressing, as defined by RFC 1918, offers several key benefits in networking. Primarily, it addresses the finite nature of publicly routable IPv4 addresses. By using private IP ranges (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16), organizations can significantly conserve IPv4 addresses (B), as these addresses are not globally unique and can be reused across different private networks. This is crucial because it reduces the strain on the limited pool of public IPv4 addresses.

Furthermore, deploying private IP addresses alongside Network Address Translation (NAT) enhances security. While NAT doesn't inherently offer security, it does obscure the internal network topology by using a public IP address when communicating with the outside world. This means internal machines with private IP addresses aren't directly exposed on the Internet, reducing the risk of a network security breach (D). However, it's essential to note that NAT is not a replacement for a robust security strategy, but it is a contributing factor to overall network security. Choices A and C, are not primary reasons. PCI compliance (A) isn't achieved through private IPs; it requires a range of security controls. Similarly, While reducing forwarding table size (C) is a positive side effect of subnetting, not its primary goal for utilizing private IP addresses. Therefore, the correct answer aligns with conservation and security.

RFC 1918 - Address Allocation for Private InternetsNetwork Address Translation (NAT)

## Question: 58

Which WAN access technology is preferred for a small office / home office architecture?

A. broadband cable access
B. frame-relay packet switching
C. dedicated point-to-point leased line
D. Integrated Services Digital Network switching

**Answer: A**

**Explanation:**

Broadband cable access is the preferred WAN technology for small office/home office (SOHO) environments due to its cost-effectiveness and widespread availability. SOHO users typically require sufficient bandwidth for everyday tasks like web browsing, email, video conferencing, and cloud application access, which cable broadband adequately provides. Its asymmetrical download and upload speeds cater well to the typical usage pattern of SOHO users, who consume more data than they upload. Options like frame relay and dedicated leased lines are more expensive and often require complex configurations, making them unsuitable for small offices. These technologies are primarily used in larger enterprise environments demanding high reliability and dedicated bandwidth. ISDN, while offering digital connectivity, is considered outdated and lacks the speed and cost-effectiveness of modern broadband options. Cable's shared infrastructure model allows providers to offer competitive pricing. Furthermore, its plug-and-play nature simplifies setup and
management, reducing the technical overhead for SOHO users. Cloud services, SaaS, and telecommuting have further driven the reliance on reliable and affordable broadband, making cable access ideal. For more information, you can explore resources on WAN technologies and their applications from Cisco, a major networking vendor, and independent IT publications.

https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/wan-technologies.htmlhttps://www.techtarget.com/searchnetworking/definition/WAN

## Question: 59

Which two WAN architecture options help a business scalability and reliability for the network? (Choose two.)

A.asychronous routing
B.single-homed branches
C.dual-homed branches
D.static routing
E.dynamic routing

**Answer: CE**

**Explanation:**

The correct answers are **C. dual-homed branches** and **E. dynamic routing**.

Dual-homed branches enhance scalability and reliability by connecting a branch office to the WAN through two separate links. This redundancy ensures that if one link fails, the other provides continuous connectivity,

minimizing downtime and improving the network's overall resilience. This approach is crucial for maintaining business operations, especially for critical applications.

Dynamic routing protocols like OSPF or BGP contribute to scalability and reliability by automatically adjusting network paths based on changing network conditions. When a link fails or becomes congested, dynamic routing protocols can quickly reroute traffic through alternative paths, preventing disruptions and ensuring optimal bandwidth usage. Moreover, these protocols enable the network to adapt to growth without requiring manual reconfiguration, which simplifies management as the network expands. Static routing, while simpler, lacks this adaptability and is not suitable for dynamic environments that require efficient path selection.

Asynchronous routing and single-homed branches do not provide the needed scalability or reliability compared to the correct answers.

**Authoritative Links for Further Research:**

**Cisco Documentation on Dual-Homed WAN Connections:**
https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/Dual_Homed/DHDG_v02.html **Cisco Documentation on Dynamic Routing Protocols:**
https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/19685-bgp-faq.html (While this link pertains to BGP, it provides a good overview of dynamic routing principles.)
**TechTarget Article on Dynamic Routing:**https://www.techtarget.com/searchnetworking/definition/dynamic-routing

## Question: 60

What is the binary pattern of unique ipv6 unique local address?

A. 00000000
B. 11111100
C. 11111111
D. 11111101

**Answer: B**

**Explanation:**

The correct binary pattern for the prefix of an IPv6 Unique Local Address (ULA) is indeed **11111100**, corresponding to option **B**. ULAs are defined in RFC 4193 and are intended for private addressing within a limited site or organization. The first seven bits of the IPv6 address, known as the Global Routing Prefix, are used to identify the address type. For ULAs, these seven bits are fixed as 1111110, which in decimal is 254, or in hexadecimal FC. The subsequent bit within the prefix is the 'L' bit, which indicates that an IPv6 address is a local address; and for ULAs this is '1'. Therefore, the fixed prefix is 11111101 which is FC00::/7, in hexadecimal. After that /7 prefix we get the /8 prefix 11111100, representing the binary representation for FD. The remaining bits are then used for the subnet ID and interface ID. Consequently, the binary pattern 11111100 (or FD in hexadecimal) is the crucial identifier for the ULA address range. This contrasts with Global Unicast addresses which start with 001 and other multicast addresses which begin with a different bit pattern. The binary pattern 00000000 (option A) is not specific to any IPv6 address type and neither is 11111111 (option C). The binary pattern 11111101 (option D) denotes a prefix of FC which is combined with the 'L' bit to create ULA prefix of FD. Option B, i.e. 11111100, is specifically the binary representation for prefix FD which is used for ULAs.

For authoritative information on IPv6 Unique Local Addresses, refer to:

**RFC 4193:**https://datatracker.ietf.org/doc/html/rfc4193
**IPv6 Addressing Overview:**https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-sy/ipv6-

15-sy-book/ipv6-addr-over.html

**Question: 61**

Which two options are the best reasons to use an IPV4 private IP space? (Choose two.)

A. to enable intra-enterprise communication
B. to implement NAT
C. to connect applications
D. to conserve global address space
E. to manage routing overhead

**Answer: AD**

**Explanation:**

The correct answers are A and D. Let's explore why.

**A. To enable intra-enterprise communication:** Private IPv4 addresses are designed for use within private networks, such as homes, offices, or enterprise networks. They allow devices within these networks to communicate with each other without requiring globally unique public IP addresses. This facilitates local network interactions and data sharing, forming the backbone of internal communication infrastructures.

**D. To conserve global address space:** IPv4 addresses are a finite resource. The use of private IP address spaces significantly reduces the demand for public addresses. Instead of assigning a public IP to every device within an organization, only edge devices (e.g., firewalls, routers) require one. This conservation strategy was crucial in prolonging the viability of IPv4 before the widespread adoption of IPv6.

**Why B, C, are incorrect:**

**B. To implement NAT:** While Network Address Translation (NAT) is often used in conjunction with private IP addressing, it's not a primary reason for using private IPs. NAT allows devices with private IP addresses to access the internet via a public IP address, but this is a consequence of private IP usage, not its primary justification.

**C. To connect applications:** Application connectivity is facilitated by network protocols and addressing schemes in general, not specifically by using private IP addresses. Private IPs enable communication between devices, and thereby applications that are running on those devices within a private network. However, it's the network communication that is enabled, not directly application connectivity itself.

In summary, the fundamental purpose of private IP address spaces is to enable internal communication and to conserve globally routable IPv4 addresses. These two aspects make private IP addressing a core component of modern network architectures, allowing organizations to establish private and secure local networks without consuming vast quantities of the public address space.

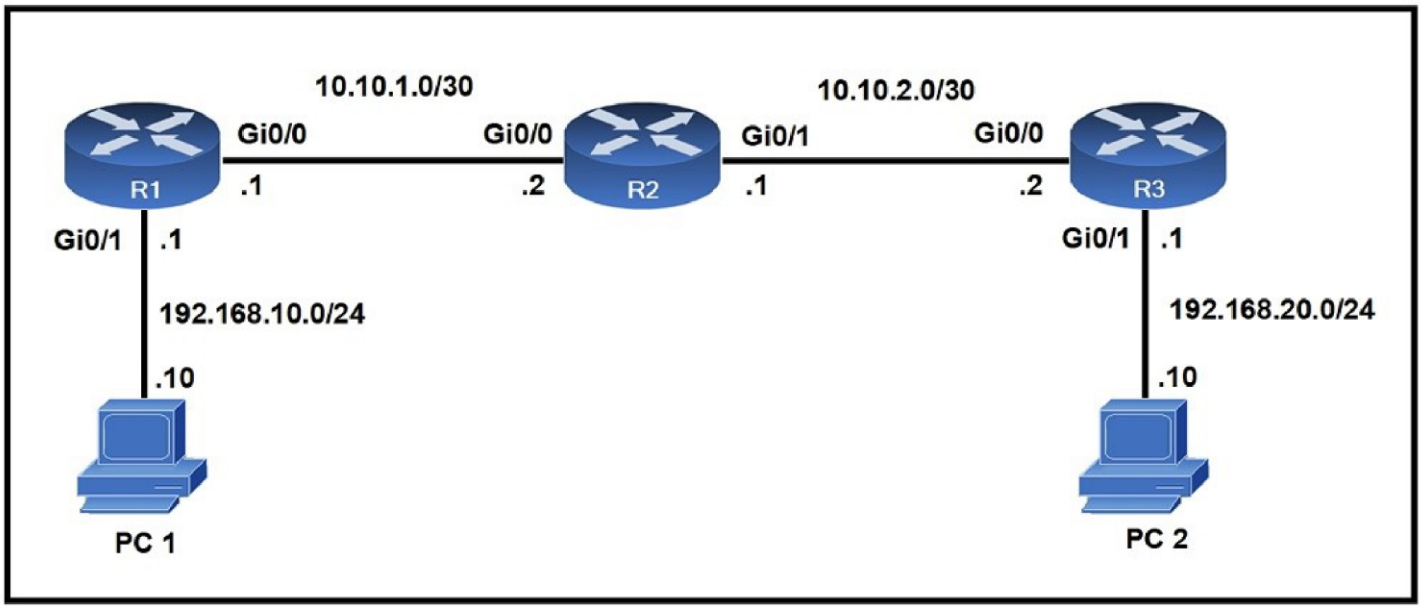
**Authoritative Links for Further Research:**

**RFC 1918 - Address Allocation for Private Internets:**https://datatracker.ietf.org/doc/html/rfc1918 This is the original document defining private IP address ranges.

**Cisco on Private IP Addressing:**https://www.cisco.com/c/en/us/support/docs/ip/addressing/13863-private-ip.html This provides a detailed explanation from a networking equipment vendor.

**Question: 62**

Refer to the exhibit. When PC1 sends a packet to PC2, the packet has which source and destination IP address when it arrives at interface Gi0/0 on router R2?




A.source 192.168.10.10 and destination 10.10.2.2
B.source 192.168.20.10 and destination 192.168.20.1
C.source 192.168.10.10 and destination 192.168.20.10
D.source 10.10.1.1 and destination 10.10.2.2

**Answer: C**

**Explanation:**
The source and destination IP addresses of the packets are unchanged on all the way. Only source and destination MAC addresses are changed.

## Question: 63

What is the same for both copper and fiber interfaces when using SFP modules?

A.They support an inline optical attenuator to enhance signal strength
B.They accommodate single-mode and multi-mode in a single module
C.They provide minimal interruption to services by being hot-swappable
D.They offer reliable bandwidth up to 100 Mbps in half duplex mode

**Answer: C**

**Explanation:**

The correct answer is **C. They provide minimal interruption to services by being hot-swappable.** This characteristic is a key advantage of using Small Form-factor Pluggable (SFP) modules, regardless of whether they are copper or fiber based. Hot-swappability means that these modules can be inserted or removed while the networking device (like a switch or router) remains powered on and operational, minimizing downtime. This feature allows for flexible upgrades, repairs, and replacements without requiring a complete system shutdown. While copper and fiber SFP modules differ greatly in their physical transmission medium, data encoding, and the technology used for sending and receiving signals, their shared interface standard (the SFP cage) is designed for this hot-swappable functionality. The other options are incorrect. Option A is specific to fiber optics, as attenuators are used to reduce signal strength to avoid overloading receivers, and copper interfaces do not require this. Option B is incorrect because SFPs are designed for a specific media type (single or multi-mode fiber or copper). Option D is also incorrect as both fiber and copper SFPs can support

speeds much higher than 100 Mbps in half-duplex mode; SFP speeds can range from 100Mbps to 100Gbps and beyond, supporting full-duplex operation as well. Hot-swapping is a significant benefit in network management, allowing for less disruptive maintenance and a quicker mean time to repair (MTTR).

**Supporting Links:**

**Wikipedia - Small Form-factor Pluggable:**https://en.wikipedia.org/wiki/Small_form-factor_pluggable **Cisco - Understanding SFP and SFP+ Transceiver Modules:**
https://www.cisco.com/c/en/us/products/interfaces-modules/transceiver-modules/index.html

## Question: 64

What are two functions of a server on a network? (Choose two.)

A. handles requests from multiple workstations at the same time

B. achieves redundancy by exclusively using virtual server clustering

C. housed solely in a data center that is dedicated to a single client achieves redundancy by exclusively using virtual server clustering

D. runs the same operating system in order to communicate with other servers

E. runs applications that send and retrieve data for workstations that make requests

**Answer: AE**

**Explanation:**

Let's break down why options A and E are the correct functions of a server on a network.

**Option A: "handles requests from multiple workstations at the same time"** This is a core function of a server. Servers are designed to be powerful enough to manage simultaneous connections and requests from numerous client devices (workstations). They achieve this using techniques like multithreading and multiprocessing, allowing them to efficiently respond to requests for data, services, or applications from multiple users concurrently. This is fundamental to how networks operate, as users aren't typically working in isolation.

**Option E: "runs applications that send and retrieve data for workstations that make requests"** This accurately reflects the server's role in providing services. Servers host and execute applications (like web servers, databases, email servers, etc.). When a workstation needs a specific service or data, it sends a request to the appropriate server. The server then processes the request, retrieves the necessary information or runs the application, and sends the response back to the workstation. This interaction forms the basis of client-server architecture, a cornerstone of network operations.

**Why the other options are incorrect:**

**Option B: "achieves redundancy by exclusively using virtual server clustering"** While virtual server clustering is a common redundancy technique, it's not the exclusive method for redundancy. Redundancy can also be achieved through physical server replication, load balancers, and other methods. This option's absolute language ("exclusively") makes it incorrect.

**Option C: "housed solely in a data center that is dedicated to a single client"** Servers can be located in data centers, but it is not a rule that it will be dedicated to a single client. Servers can also be located in local offices or even on-premises, and they can be shared between multiple clients.

**Option D: "runs the same operating system in order to communicate with other servers"** Servers do not need to run on the same operating system to communicate with other servers, they use standardized protocols to send data between each other.

**In Conclusion:** The correct options (A and E) describe the fundamental roles of a server in a network environment: handling simultaneous requests and providing services by running applications and managing data.

**Authoritative Links for Further Research:**

**Cisco:**https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/what-is-server.html
**Microsoft:**https://learn.microsoft.com/en-us/windows-server/get-started/what-is-windows-server
**TechTarget:**https://www.techtarget.com/searchnetworking/definition/server

## Question: 65

Which function is performed by the collapsed core layer in a two-tier architecture?

A.enforcing routing policies
B.marking interesting traffic for data policies
C.applying security policies
D.attaching users to the edge of the network

**Answer: A**

**Explanation:**

Okay, let's break down why option A, "enforcing routing policies," is the correct function of a collapsed core layer in a two-tier network architecture.

In a two-tier design, the network is simplified into an access layer and a collapsed core. The access layer is where end-user devices connect, and the collapsed core combines the distribution and core functionalities of a more traditional three-tier model. The primary responsibility of the collapsed core is to efficiently route traffic between different parts of the network.

Option A directly addresses this core function. Routing policies define how traffic is directed based on destination, source, or other criteria. Enforcing these policies is vital for ensuring packets reach their intended location and for optimizing network performance. The collapsed core layer is the central point for making these routing decisions.

Options B, C, and D, while important network functions, are not the primary role of the collapsed core in this specific architecture. Marking traffic (B) is often done at the access or edge layer. Applying security policies (C), is also commonly done at the network edge or firewall locations, though security can be implemented in layers and enforced in the core to a certain degree, but the primary focus for a collapsed core remains routing. Attaching users to the network edge (D) is specifically the function of the access layer.

The collapsed core's key task is to provide a high-speed, reliable, and scalable routing infrastructure. This ensures data can move efficiently between access layer segments and onward to other networks. Therefore, enforcing routing policies is a defining characteristic of the collapsed core in a two-tier model.

**Authoritative Links for further research:**

**Cisco Documentation on Network Design:**
https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Dec2014/CVD-EnterpriseCampusDesign1-0.html (This is a comprehensive overview of Cisco's campus network design best practices, including two-tier model explanations.)
**Network Layering Concepts:**https://networklessons.com/cisco/ccna-routing-switching-icnd1-100-105/network-layering-access-distribution-core-layer (This explains the differences between the three-tier

architecture and how it relates to a two-tier design.)
**Wikipedia: Collapsed Core:** While Wikipedia is not a definitive source, it provides a quick overview and a good starting point. https://en.wikipedia.org/wiki/Core_layer (Look for the collapsed core section.)

## Question: 66

What is the primary function of a Layer 3 device?

A.to transmit wireless traffic between hosts
B.to analyze traffic and drop unauthorized traffic from the Internet
C.to forward traffic within the same broadcast domain
D.to pass traffic between different networks

**Answer: D**

**Explanation:**

The correct answer is **D. to pass traffic between different networks**. Layer 3 devices, also known as network layer devices, operate at the network layer of the OSI model. This layer is primarily concerned with logical addressing (IP addresses) and routing of data packets across networks. Unlike Layer 2 devices (like switches) that forward traffic within the same network segment (broadcast domain) using MAC addresses, Layer 3 devices (typically routers) make routing decisions based on IP addresses and routing tables. They examine the destination IP address of incoming packets and determine the best path to forward the packet to its destination network. This process enables communication between different networks, which is the core function of a Layer 3 device. Options A and B are incorrect. While wireless access points can operate at layer 2, they do not inherently work at Layer 3 and therefore do not define primary function of L3 devices. Furthermore, although firewalls, which often operate at Layer 3, can analyze and drop traffic, this is not their primary function, but rather an additional functionality focused on security. Option C describes a Layer 2 function of switches. In summary, Layer 3 devices facilitate internetworking by intelligently routing data packets across different network segments, enabling communication beyond the boundaries of a single broadcast domain.

**Supporting Links:**

**Cisco's Overview of the Network Layer:**https://www.cisco.com/c/en/us/support/docs/ip/routing/15995-layer3.html
**Techopedia Explanation of Layer 3:**https://www.techopedia.com/definition/24072/layer-3
**GeeksforGeeks on Network Layer:**https://www.geeksforgeeks.org/network-layer-in-computer-network/

## Question: 67

Which two functions are performed by the core layer in a three-tier architecture? (Choose two.)

A. Provide uninterrupted forwarding service
B. Inspect packets for malicious activity
C. Ensure timely data transfer between layers
D. Provide direct connectivity for end user devices
E. Police traffic that is sent to the edge of the network

**Answer: AC**

**Explanation:**

The core layer in a three-tier network architecture is primarily responsible for high-speed data transfer and reliable, uninterrupted forwarding. Its primary function is to provide a robust and efficient backbone for the network. Option A, "Provide uninterrupted forwarding service," directly aligns with this core responsibility. The core layer is designed for speed and reliability, minimizing any disruptions to data flow. It does not handle traffic inspection or security functions; those are typically the responsibility of other layers. Therefore, option B, "Inspect packets for malicious activity," is incorrect.

Option C, "Ensure timely data transfer between layers," also accurately reflects a core function. The core layer must facilitate quick and efficient data movement between the distribution and access layers, preventing bottlenecks and ensuring smooth overall network operation. The core layer acts as the central switching hub for the network, and its timely data handling is crucial for effective communication between different parts of the network. Option D, "Provide direct connectivity for end user devices," is incorrect as that is the job of the access layer. Lastly, option E, "Police traffic that is sent to the edge of the network," is incorrect as this is a function of the distribution layer, not the core.

In summary, the core layer's main jobs are high-speed data switching and timely data transfer, making options A and C the correct choices.

For further research, consider the following links:

**Cisco's Three-Tier Hierarchical Model**: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Aug2011/CVD-CampusNetworkDesign-AUG11.html This Cisco document gives an overview of network design models. **Techopedia's definition of core layer:**https://www.techopedia.com/definition/23561/core-layer This provides a simplified explanation of the core layer.

## Question: 68

What is a recommended approach to avoid co-channel congestion while installing access points that use the 2.4 GHz frequency?

A.different nonoverlapping channels
B.one overlapping channel
C.one nonoverlapping channel
D.different overlapping channels

**Answer: A**

**Explanation:**

**Justification for Answer A: Different Nonoverlapping Channels**

Co-channel interference, a significant problem in 2.4 GHz Wi-Fi networks, occurs when multiple access points (APs) operate on the same or overlapping channels. This interference degrades performance, leading to slower speeds, higher latency, and reduced network reliability. The 2.4 GHz band has a limited number of non-overlapping channels – specifically, channels 1, 6, and 11 are typically used as they minimize signal collisions. Selecting different nonoverlapping channels (Answer A) for nearby access points is the most effective way to mitigate co-channel congestion. This ensures each AP has a dedicated frequency space with minimal overlap with neighboring APs. Utilizing non-overlapping channels reduces the likelihood of APs interfering with each other, resulting in better throughput and a more stable connection. Deploying neighboring APs on overlapping channels, as suggested in options B and D, exacerbates the co-channel interference problem, severely degrading network performance. Option C (one non-overlapping channel) is unsuitable for multiple access points since it leads to interference and it doesn't leverage the available channel space. By carefully planning and assigning different non-overlapping channels, network administrators can establish a robust and performant wireless environment, maximizing efficiency and minimizing the negative impacts of interference.

Proper channel planning is a fundamental aspect of wireless network design, especially in dense deployments.

**Authoritative Links:**

**Cisco - Wireless LAN (WLAN) Best Practices:**
https://www.cisco.com/c/en/us/td/docs/wireless/technology/wlan/bestpractices/Cisco_WLAN_Best_Practices.htm (Focus on the "Channel Management" section)
**Wi-Fi Alliance:**https://www.wi-fi.org/ (General information on Wi-Fi technology)
**IEEE 802.11 Standard:**https://www.ieee.org/ (Technical specifications for Wi-Fi networks)

## Question: 69

A manager asks a network engineer to advise which cloud service models are used so employees do not have to waste their time installing, managing, and updating software that is only used occasionally. Which cloud service model does the engineer recommend?

A.infrastructure-as-a-service
B.platform-as-a-service
C.business process as service to support different types of service
D.software-as-a-service

**Answer: D**

**Explanation:**

The correct answer is Software-as-a-Service (SaaS). SaaS provides ready-to-use applications over the internet, eliminating the need for users to install, manage, or update software on their devices. This aligns perfectly with the manager's request to avoid employees wasting time on such tasks for occasionally used software. Instead of managing the underlying infrastructure, operating systems, or middleware (as in IaaS and PaaS), users simply access and use the application directly. SaaS solutions handle all backend tasks like patching, upgrades, and maintenance, significantly reducing administrative overhead. This contrasts with IaaS where users manage the operating system, storage, and deployed applications and PaaS where users manage applications and data, which would both still require some level of management effort from the employees.

Common examples of SaaS applications include email services (like Gmail), CRM systems (like Salesforce), and project management tools (like Asana), which do not require any software installation on the end user's machine. Therefore, for the given scenario, SaaS best fits the requirements of providing software directly to users with minimal management overhead.

https://www.salesforce.com/solutions/cloud-computing/saas/https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-saas/

## Question: 70

What are two functions of a Layer 2 switch? (Choose two.)

A. acts as a central point for association and authentication servers
B. selects the best route between networks on a WAN
C. moves packets within a VLAN
D. moves packets between different VLANs
E. makes forwarding decisions based on the MAC address of a packet

**Answer: CE**

**Explanation:**

The correct answers are C and E. Layer 2 switches operate at the Data Link Layer of the OSI model and primarily deal with MAC addresses. Option C is correct because switches learn MAC addresses associated with connected devices and use this information to forward frames to the correct destination within a VLAN. This ensures that data only reaches its intended recipient in the same VLAN. Option E is also correct; Layer 2 switches can move packets (specifically, frames) between different VLANs, however, this is achieved using a router on a stick configuration or Layer 3 switch to route between the VLANS.

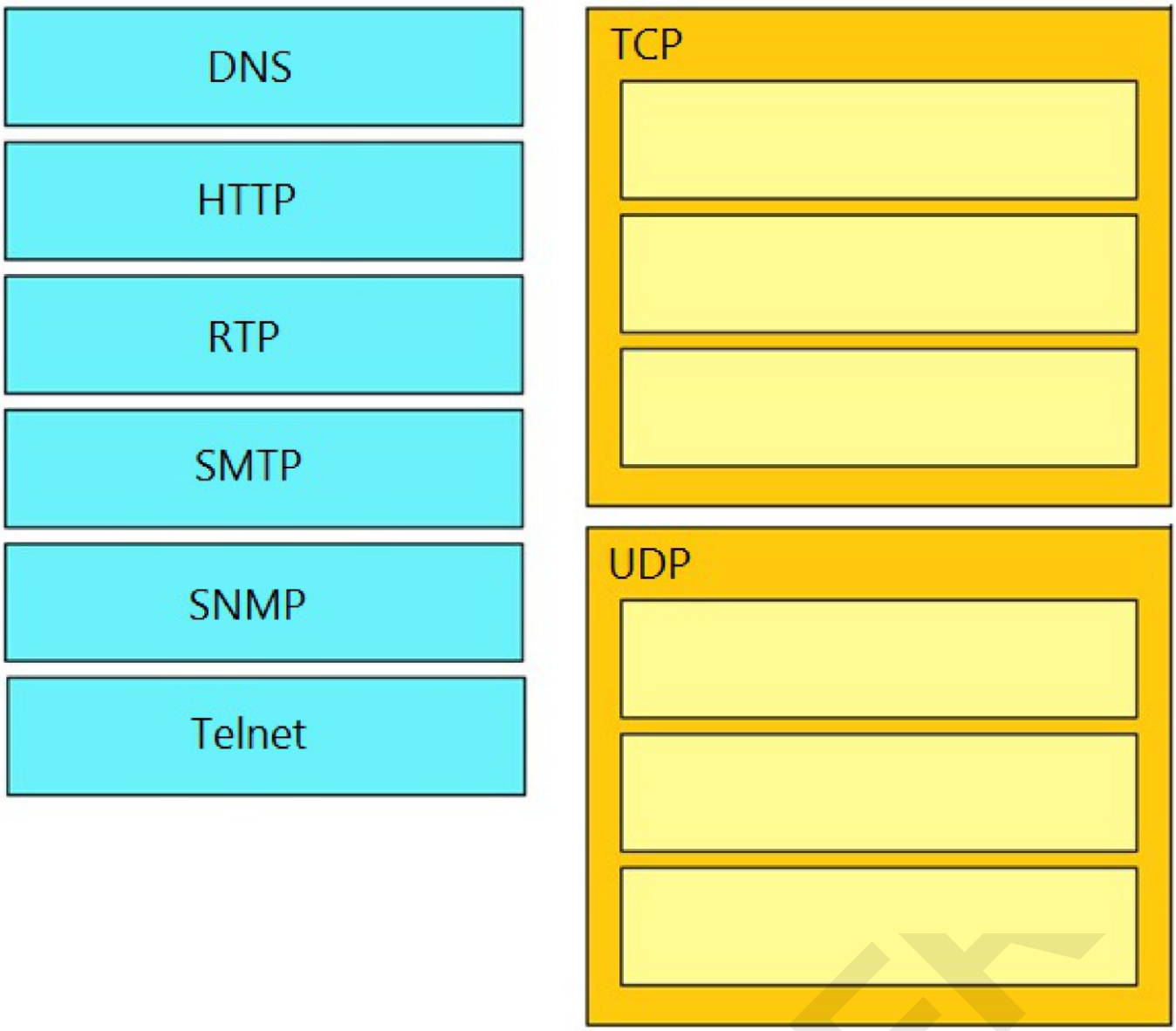
Option A is incorrect because authentication and association servers are typically managed by network devices such as routers or dedicated servers and not Layer 2 switches. Option B is incorrect as route selection on a WAN (Wide Area Network) is the job of Layer 3 routers. Layer 2 switches do not handle routing between different networks; they forward packets within the same broadcast domain. Option D is partially true as a switch with VLAN tagging (802.1Q) can receive frames from different VLANs; however it can't move the packets to other VLANs without Layer 3 routing.

Here are some authoritative links for further research:

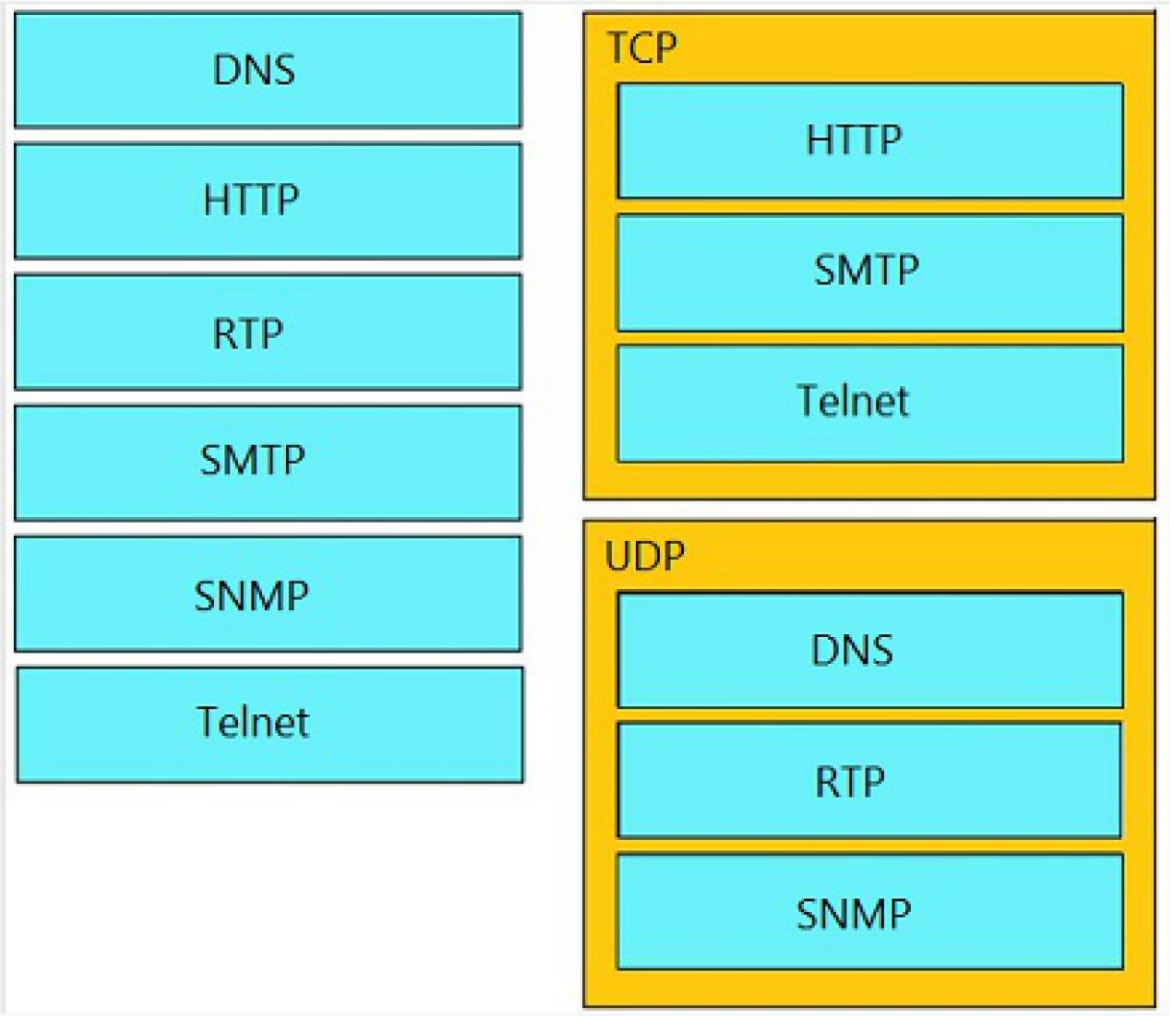
**Cisco - What is a Layer 2 Switch?**https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/layer-2-switch.html
**GeeksforGeeks - Difference between Switch and Router**https://www.geeksforgeeks.org/difference-between-switch-and-router/
**Cloudflare - What is a Layer 2 Switch?**https://www.cloudflare.com/learning/network-layer/what-is-a-layer-2-switch/

## Question: 71

DRAG DROP -
Drag and drop the TCP/IP protocols from the left onto their primary transmission protocols on the right.
Select and Place:




**Answer:**




**Explanation:**

TCP- HTTP, SMTP, TelnetUDP- DNS, RTP, SNMP

**Question: 72**

An engineer observes high usage on the 2.4GHz channels and lower usage on the 5GHz channels. What must be configured to allow clients to preferentially use
5GHz access points?

A.Client Band Select
B.Re-Anchor Roamed Clients
C.OEAP Spilt Tunnel
D.11ac MU-MIMO

**Answer: A**

**Explanation:**

The correct answer is **A. Client Band Select**. Here's why:

Client Band Select is a feature that encourages dual-band wireless clients (those capable of using both 2.4GHz and 5GHz bands) to connect to the 5GHz band whenever possible. 5GHz offers higher bandwidth and lower interference compared to the congested 2.4GHz band. When 2.4GHz is experiencing high usage, directing clients towards 5GHz can significantly improve overall network performance and user experience.

Client Band Select works by subtly "steering" clients towards 5GHz. This is often achieved through

techniques such as delaying the 2.4GHz beacon broadcast or slightly reducing the transmit power of the 2.4GHz radio. By making the 5GHz band appear more attractive to the client, it's more likely to initiate a connection or roam to the 5GHz access point.

Options B, C, and D are incorrect:

**B. Re-Anchor Roamed Clients:** This feature is related to wireless roaming and ensuring seamless transitions between access points, not band preference. It's useful for maintaining consistent connectivity but doesn't address the channel utilization imbalance.

**C. OEAP Spilt Tunnel:** This option pertains to OfficeExtend Access Points (OEAP) and how traffic is routed through a corporate network, not band selection for clients within a standard wireless deployment. **D. 11ac MU-MIMO:** This is a technology that allows an access point to communicate with multiple devices simultaneously, increasing network efficiency. While beneficial for performance, it doesn't specifically address client band preference between 2.4GHz and 5GHz.

Client Band Select is specifically designed to manage this exact scenario where 2.4GHz is congested and promotes the use of the less crowded 5GHz band.

For further information, you can explore these resources:

**Cisco Documentation on Band Select:** (Search Cisco's website for "Client Band Select Configuration" or similar)
**Wi-Fi Alliance:**https://www.wi-fi.org/ This site contains technical information regarding Wi-Fi specifications and features.

**Wireless Networking Basics:** Search for articles on "2.4GHz vs 5GHz Wi-Fi" on reputable technology websites for foundational understanding.

## Question: 73

Which networking function occurs on the data plane?

A.processing inbound SSH management traffic
B.sending and receiving OSPF Hello packets
C.facilitates spanning-tree elections
D.forwarding remote client/server traffic

**Answer: D**

**Explanation:**

The correct answer is **D. forwarding remote client/server traffic**. The data plane is primarily responsible for the actual movement of user data traffic across a network. It focuses on forwarding packets based on routing decisions made by the control plane. This involves looking up destination addresses in forwarding tables and physically moving the data along the determined path. Options A, B, and C all pertain to the control plane.

Processing SSH traffic (A) is about managing the device itself, a function of the control plane. Sending and receiving OSPF Hello packets (B) are part of the routing protocol's process of discovering neighbors and exchanging routing information, another control plane task. Similarly, participating in spanning-tree elections (C) is about managing network loops and is part of the control plane. The key difference is that the data plane handles the actual traffic payload, while the control plane establishes the how and where for that traffic to flow. Option D directly reflects the data plane's function: forwarding user-generated traffic, like requests from clients to servers and responses back.

Further Research:

**Cisco's explanation of Control and Data Plane:**https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mpls/configuration/15-sy/mp-15-sy-book/mp-ctrl-data-plane.html
**Juniper's explanation of Control and Data Plane:**
https://www.juniper.net/documentation/en_US/junos/topics/concept/control-data-planes-understanding.html

## Question: 74

Under which condition is TCP preferred over UDP?

A.UDP is used when low latency is optimal, and TCP is used when latency is tolerable.
B.TCP is used when dropped data is more acceptable, and UDP is used when data is accepted out-of-order.
C.TCP is used when data reliability is critical, and UDP is used when missing packets are acceptable.
D.UDP is used when data is highly interactive, and TCP is used when data is time-sensitive.

**Answer: C**

**Explanation:**

The correct answer is C because it accurately reflects the fundamental differences in design and application between TCP and UDP. TCP (Transmission Control Protocol) is a connection-oriented protocol that prioritizes reliable data delivery. It achieves this through mechanisms such as sequencing, acknowledgments, and retransmission. This guarantees that data arrives in the correct order and without loss. This reliability comes at the cost of overhead in terms of connection setup and maintenance, leading to higher latency compared to UDP.

UDP (User Datagram Protocol), on the other hand, is a connectionless protocol. It does not guarantee reliable delivery, sequence, or retransmission of data. Instead, it focuses on speed and low latency, making it suitable for applications where dropped packets are acceptable or where real-time data delivery is more crucial than perfect accuracy. Think of streaming video where a few dropped frames are less noticeable than a delayed stream.

Option A is incorrect because it reverses the latency characteristics of TCP and UDP. UDP is preferred when low latency is crucial, while TCP is used when a higher degree of latency is acceptable due to its reliability mechanisms. Option B is incorrect because TCP is not used when dropped data is acceptable, but quite the opposite. The strength of TCP lies in its guarantee that data will not be dropped and will be received in order.
UDP, conversely, is tolerant to data loss and out-of-order data. Option D is incorrect because UDP is often favored in real-time applications where interactivity is key, while TCP is more suitable for situations requiring a reliable stream of data, not necessarily time-sensitive.

Therefore, when data reliability is critical, as it is with file transfers, email, and web browsing, TCP is the protocol of choice. UDP is suitable when missing packets are acceptable, such as in streaming video, online games, or VoIP (Voice over Internet Protocol), where speed and low latency are prioritized over data accuracy.

**Authoritative Links:**

**TCP vs UDP:**https://www.cloudflare.com/learning/network-layer/what-is-tcp/
**TCP:**https://en.wikipedia.org/wiki/Transmission_Control_Protocol
**UDP:**https://en.wikipedia.org/wiki/User_Datagram_Protocol

## Question: 75

```
SiteA#show interface TenGigabitEthernet0/1/0
TenGigabitEthernet0/1/0 is up, line protocol is up
  Hardware is BUILT-IN-EPA-8x10G, address is 780c.f02a.db91 (bia 780a.f02b.db91)
  Description: Connection to SiteB
  Internet address is 10.10.10.1/30
  MTU 8146 bytes, BW 10000000 Kbit/sec, DLY 10 usec,
     reliability 166/255, txload 1/255, rxload 1/255
  Full Duplex, 10000Mbps, link type is force-up, media type is SFP-LR
  5 minute input rate 264797000 bits/sec, 26672 packets/sec
  5 minute output rate 122464000 bits/sec, 15724 packets/sec

SiteB#show interface TenGigabitEthernet0/1/0
TenGigabitEthernet0/1/0 is up, line protocol is up
  Hardware is BUILT-IN-EPA-8x10G, address is 780c.f02c.db26 (bia 780c.f02c.db26)
  Description: Connection to SiteA
  Internet address is 10.10.10.2/30
  MTU 8146 bytes, BW 10000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Full Duplex, 10000Mbps, link type is force-up, media type is SFP-LR
  5 minute input rate 122464000 bits/sec, 15724 packets/sec
  5 minute output rate 264797000 bits/sec, 26672 packets/sec
```

Refer to the exhibit. Shortly after SiteA was connected to SiteB over a new single-mode fiber path, users at SiteA report intermittent connectivity issues with applications hosted at SiteB. What is the cause of the intermittent connectivity issue?

A.Interface errors are incrementing.

B.High usage is causing high latency.

C.An incorrect SFP media type was used at SiteA.

D.The sites were connected with the wrong cable type.

**Answer: A**

**Explanation:**

The only indicator of any issues here is the reliability 166/255 on SiteA. When the input and output errors increase, they affect the reliability counter. This indicates how likely it is that a packet can be delivered or received successfully. Reliability is calculated like this: reliability = number of packets / number of total frames.

The value of 255 is the highest value meaning that the interface is very reliable at the moment. The calculation above is done every 5 minutes.

## Question: 76

A network engineer must configure the router R1 GigabitEthernet1/1 interface to connect to the router R2 GigabitEthernet1/1 interface. For the configuration to be applied, the engineer must compress the address 2001:0db8:0000:0000:0500:000a:400F:583B. Which command must be issued on the interface?

A.ipv6 address 2001::db8:0000::500:a:400F:583B

B.ipv6 address 2001:db8:0::500:a:4F:583B

C.ipv6 address 2001:db8::500:a:400F:583B

D.ipv6 address 2001:0db8::5:a:4F:583B

**Answer: C**

**Explanation:**

The correct answer is C: ipv6 address 2001:db8::500:a:400F:583B. This involves IPv6 address compression, a critical concept for managing the lengthy 128-bit IPv6 addresses. IPv6 addresses are composed of eight 16-bit

hexadecimal fields. To simplify them, leading zeros within a field can be omitted. Additionally, a single contiguous sequence of one or more fields containing all zeros can be replaced by a double colon (::). This double colon can only be used once per address.

In the provided IPv6 address (2001:0db8:0000:0000:0500:000a:400F:583B), the leading zeros in "0db8" can be removed, becoming "db8". Two consecutive fields "0000:0000" are all zeros, so they can be replaced by "::". The fields "0500" becomes "500" when leading zeros are removed and "000a" becomes "a". Applying these compressions yields 2001:db8::500:a:400F:583B. This compressed form represents the same IPv6 address. Options A, B and D contain formatting or compression errors. Option A mistakenly uses a double colon in non consecutive zero fields, while options B and D incorrectly compress the leading zeros or apply multiple :: which is illegal. Option C correctly represents the address after applying the valid IPv6 compression rules, making it the only suitable command to apply the correct address to the interface.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-mt/ipv6-15-mt-book/ipv6-addr-config.htmlhttps://www.rfc-editor.org/rfc/rfc4291#section-2.2

**Question: 77**

What is a network appliance that checks the state of a packet to determine whether the packet is legitimate?

A.Layer 2 switch
B.LAN controller
C.load balancer
D.firewall

**Answer: D**

**Explanation:**

The correct answer is **D. firewall**. Firewalls are network security devices that monitor incoming and outgoing network traffic and make decisions about allowing or blocking packets based on pre-defined security rules.

Specifically, a **stateful firewall** examines the context of network connections, tracking the state of active sessions. This allows it to distinguish between legitimate packets belonging to an established connection and unsolicited or potentially malicious traffic. This is crucial for determining if a packet is part of an authorized conversation or a new, suspicious attempt to communicate.

Layer 2 switches (A) operate at the data link layer and make forwarding decisions based on MAC addresses, not packet content or state. LAN controllers (B) manage network access points and wireless devices, focusing on connectivity rather than security at the packet level. Load balancers (C) distribute network traffic across multiple servers to improve performance and availability; they don't analyze the state of individual packets for security purposes.

The primary function of a firewall, especially a stateful one, is to perform deep packet inspection and maintain a "state table" or connection tracking table. This table records details like source and destination IPs and ports, sequence numbers, and flags for active connections. The firewall uses this information to verify that incoming packets are part of an existing, authorized session, which is key for filtering out unauthorized access attempts. This ability to analyze connection state is what makes firewalls the appropriate answer to the original question.

**Authoritative Links:**

**Cisco on Firewalls:**https://www.cisco.com/c/en/us/products/security/firewalls/index.html
**National Institute of Standards and Technology (NIST) on Firewalls:**
https://csrc.nist.gov/glossary/term/firewall

**Fortinet on Stateful Firewalls:**https://www.fortinet.com/resources/cyberglossary/stateful-firewall

## Question: 78

What is a role of access points in an enterprise network?

A.integrate with SNMP in preventing DDoS attacks
B.serve as a first line of defense in an enterprise network
C.connect wireless devices to a wired network
D.support secure user logins to devices on the network

**Answer: C**

**Explanation:**

The correct answer is C: connect wireless devices to a wired network. Access points (APs) are fundamental components of wireless LAN (WLAN) infrastructure, acting as bridges between wireless clients (laptops, smartphones, tablets) and the wired network. They achieve this by receiving wireless signals from client devices and converting them into Ethernet frames for transmission on the wired network, and vice-versa. This allows wireless devices to communicate with resources like servers, printers, and other wired network devices. While some advanced APs may offer security features, their primary function isn't frontline security (eliminating option B). SNMP (Simple Network Management Protocol) is used for monitoring and managing network devices, and though access points may be monitored via SNMP, they don't integrate with it to prevent DDoS attacks, making option A incorrect. Lastly, APs do not directly handle user logins; this is typically done through authentication servers or the network operating system itself (making D incorrect). Instead, APs often utilize security protocols like WPA2/3 to secure the wireless connection. In short, the core functionality of an access point is facilitating wireless connectivity to a wired network infrastructure.

Further Research:

**Cisco Documentation on Access Points:**https://www.cisco.com/c/en/us/products/wireless/index.html (Explore the section on Access Points)
**CWNP Certified Wireless Network Professional (CWNP):**https://www.cwnp.com/ (This website contains resources on wireless networking concepts)
**IEEE 802.11 standards:**https://standards.ieee.org/ieee/802/11/ (For detailed technical understanding of wireless standards)

## Question: 79

An implementer is preparing hardware for virtualization to create virtual machines on a host. What is needed to provide communication between hardware and virtual machines?

A.router
B.hypervisor
C.switch
D.straight cable

**Answer: B**

**Explanation:**

The correct answer is **B. hypervisor**. A hypervisor is the crucial software layer that enables virtualization by managing and allocating hardware resources to virtual machines (VMs). It acts as an intermediary between

the physical hardware and the guest operating systems running within the VMs. Without a hypervisor, the VMs wouldn't have access to the underlying CPU, memory, storage, and networking resources. This software layer creates an abstraction, allowing multiple VMs to operate independently on the same physical hardware. This separation provides resource isolation and ensures that one VM's actions do not affect other VMs. The hypervisor also handles resource scheduling, ensuring efficient utilization of the host's resources. There are two main types of hypervisors: Type 1 (bare-metal) which runs directly on the hardware, and Type 2 (hosted) which runs on top of a host OS. In either case, the core function remains the same: enabling virtualization by providing the essential communication layer between the hardware and VMs. Options A, C, and D are incorrect. Routers (A) are used for network traffic management between networks, not direct hardware access for VMs. Switches (C) provide network connectivity for devices within a network, not hardware virtualization. Straight cables (D) are physical network media used for connecting devices but do not facilitate virtualization.**Authoritative Links:**

**VMware: What is a Hypervisor?**https://www.vmware.com/topics/glossary/content/hypervisor **Microsoft: Hypervisor Technology**https://learn.microsoft.com/en-us/virtualization/hyper-v-on-windows/about/
**Red Hat: What is a Hypervisor?**https://www.redhat.com/en/topics/virtualization/what-is-a-hypervisor

## Question: 80

How does a Cisco Unified Wireless Network respond to Wi-Fi channel overlap?

A.It allows the administrator to assign the channels on a per-device or per-interface basis.
B.It segregates devices from different manufactures onto different channels.
C.It analyzes client load and background noise and dynamically assigns a channel.
D.It alternates automatically between 2.4 GHz and 5 GHz on adjacent access points.

**Answer: C**

**Explanation:**

The correct answer is **C. It analyzes client load and background noise and dynamically assigns a channel.** Cisco Unified Wireless Networks employ a feature called **Radio Resource Management (RRM)**. RRM's primary function is to optimize the wireless network's performance, primarily by mitigating channel interference. Unlike manually configured channel assignments (A), RRM dynamically assesses various parameters, such as client density, data traffic, and the level of non-Wi-Fi interference and noise on each channel. Based on this analysis, RRM automatically selects the optimal channels for each Access Point (AP) to minimize overlap and interference. This dynamic channel assignment ensures that the wireless network is constantly adapting to changing conditions to provide the best performance. The system doesn't isolate devices from different manufacturers (B), and while 5GHz has less interference, the selection is based on channel availability not automatic alternation of AP frequencies (D). RRM also handles power adjustments to further mitigate interference and enhance coverage. By dynamically responding to environmental conditions and load variations, RRM ensures an efficient and reliable wireless experience. Cisco's documentation on RRM reinforces that the intent is channel optimization, not manual configurations or other methods.

Further reading on Cisco RRM can be found at:

Cisco RRM Overview
Understanding Cisco RRM