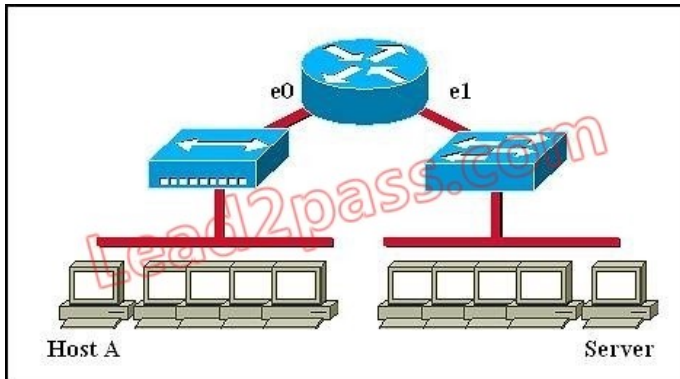


Free Download Cisco CCNA 200-120 Practice Exams with PDF & VCE (11-20)

QUESTION 11

Refer to the graphic. Host A is communicating with the server. What will be the source MAC address of the frames received by Host A from the server?



- A. the MAC address of router interface e0
- B. the MAC address of router interface e1
- C. the MAC address of the server network interface
- D. the MAC address of host A

Answer: A

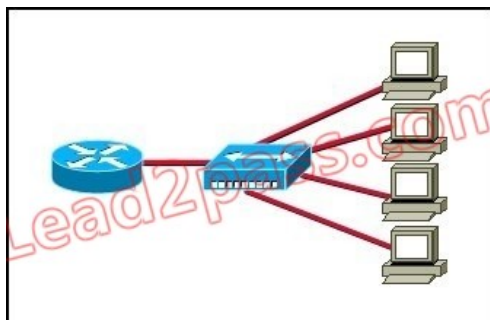
Explanation:

Whereas switches can only examine and forward packets based on the contents of the MAC header, routers can look further into the packet to discover the network for which a packet is destined. Routers make forwarding decisions based on the packet's network-layer header (such as an IPX header or IP header). These network-layer headers contain source and destination network addresses. Local devices address packets to the router's MAC address in the MAC header. After receiving the packets, the router must perform the following steps:

1. Check the incoming packet for corruption, and remove the MAC header. The router checks the packet for MAC-layer errors. The router then strips off the MAC header and examines the network-layer header to determine what to do with the packet.
2. Examine the age of the packet. The router must ensure that the packet has not come too far to be forwarded. For example, IPX headers contain a hop count. By default, 15 hops is the maximum number of hops (or routers) that a packet can cross. If a packet has a hop count of 15, the router discards the packet. IP headers contain a Time to Live (TTL) value. Unlike the IPX hop count, which increments as the packet is forwarded through each router, the IP TTL value decrements as the IP packet is forwarded through each router. If an IP packet has a TTL value of 1, the router discards the packet. A router cannot decrement the TTL value to 1 and then forward the packet.
3. Determine the route to the destination. Routers maintain a routing table that lists available networks, the direction to the desired network (the outgoing interface number), and the distance to those networks. After determining which direction to forward the packet, the router must build a new header. (If you want to read the IP routing tables on a Windows 95/98 workstation, type ROUTE PRINT in the DOS box.)
4. Build the new MAC header and forward the packet. Finally, the router builds a new MAC header for the packet. The MAC header includes the router's MAC address and the final destination's MAC address or the MAC address of the next router in the path.

QUESTION 12

Refer to the exhibit. What two results would occur if the hub were to be replaced with a switch that is configured with one Ethernet VLAN? (Choose two.)



- A. The number of collision domains would remain the same.
- B. The number of collision domains would decrease.
- C. The number of collision domains would increase.
- D. The number of broadcast domains would remain the same.
- E. The number of broadcast domains would decrease.
- F. The number of broadcast domains would increase.

Answer: CD

Explanation:

Basically, a collision domain is a network segment that allows normal network traffic to flow back and forth. In the old days of hubs, this meant you had a lot of collisions, and the old CSMA/CD would be working overtime to try to get those packets re-sent every time there was a collision on the wire (since ethernet allows only one host to be transmitting at once without there being a traffic jam). With switches, you break up collision domains by switching packets bound for other collision domains. These days, since we mostly use switches to connect computers to the network, you generally have one collision domain to a PC.

Broadcast domains are exactly what they imply: they are network segments that allow broadcasts to be sent across them. Since switches and bridges allow for broadcast traffic to go unswitched, broadcasts can traverse collision domains freely. Routers, however, don't allow broadcasts through by default, so when a broadcast hits a router (or the perimeter of a VLAN), it doesn't get forwarded. The simple way to look at it is this way: switches break up collision domains, while routers (and VLANs) break up collision domains and broadcast domains. Also, a broadcast domain can contain multiple collision domains, but a collision domain can never have more than one broadcast domain associated with it.

Collision Domain: A group of Ethernet or Fast Ethernet devices in a CSMA/CD LAN that are connected by repeaters and compete for access on the network. Only one device in the collision domain may transmit at any one time, and the other devices in the domain listen to the network in order to avoid data collisions. A collision domain is sometimes referred to as an Ethernet segment.

Broadcast Domain: Broadcasting sends a message to everyone on the local network (subnet). An example for Broadcasting would be DHCP Request from a Client PC. The Client is asking for a IP Address, but the client does not know how to reach the DHCP Server. So the client sends a DHCP Discover packet to EVERY PC in the local subnet (Broadcast). But only the DHCP Server will answer to the Request.

How to count them?

Broadcast Domain:

No matter how many hosts or devices are connected together, if they are connected with a repeater, hub, switch or bridge, all these devices are in ONE Broadcast domain (assuming a single VLAN). A Router is used to separate Broadcast-Domains (we could also call them Subnets

- or call them VLANs).

So, if a router stands between all these devices, we have TWO broadcast domains.

Collision Domain:

Each connection from a single PC to a Layer 2 switch is ONE Collision domain. For example, if 5 PCs are connected with separate cables to a switch, we have 5 Collision domains. If this switch is connected to another switch or a router, we have one collision domain more. If 5 Devices are connected to a Hub, this is ONE Collision Domain. Each device that is connected to a Layer 1 device (repeater, hub) will reside in ONE single collision domain.

QUESTION 13

Which three statements accurately describe Layer 2 Ethernet switches? (Choose three.)

- A. Spanning Tree Protocol allows switches to automatically share VLAN information.
- B. Establishing VLANs increases the number of broadcast domains.
- C. Switches that are configured with VLANs make forwarding decisions based on both Layer 2 and Layer 3 address information.
- D. Microsegmentation decreases the number of collisions on the network.
- E. In a properly functioning network with redundant switched paths, each switched segment will contain one root bridge with all its ports in the forwarding state. All other switches in that broadcast domain will have only one root port.
- F. If a switch receives a frame for an unknown destination, it uses ARP to resolve the address.

Answer: BDE

Explanation:

Microsegmentation is a network design (functionality) where each workstation or device on a network gets its own dedicated segment (collision domain) to the switch. Each network device gets the full bandwidth of the segment and does not have to share the segment with other devices. Microsegmentation reduces and can even eliminate collisions because each segment is its own collision domain -> .

Note: Microsegmentation decreases the number of collisions but it increases the number of collision domains.

QUESTION 14

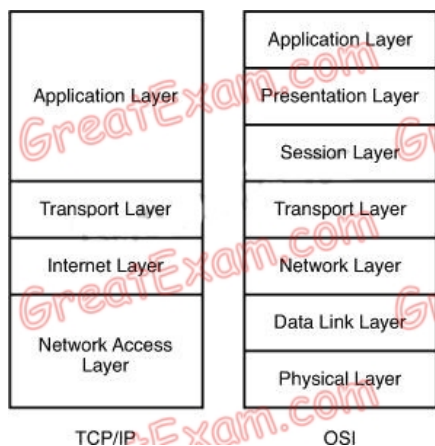
Where does routing occur within the DoD TCP/IP reference model?

- A. application
- B. internet
- C. network
- D. transport

Answer: B

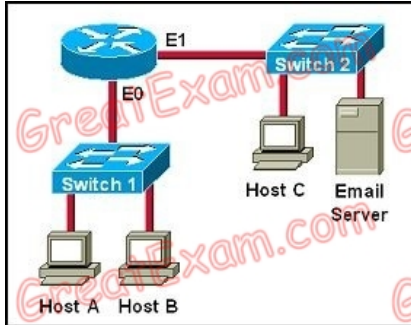
Explanation:

The picture below shows the comparison between TCP/IP model & OSI model. Notice that the Internet Layer of TCP/IP is equivalent to the Network Layer which is responsible for routing decision.



QUESTION 15

Refer to exhibit: Which destination addresses will be used by Host A to send data to Host C? (Choose two.)



- A. the IP address of Switch 1
- B. the MAC address of Switch 1
- C. the IP address of Host C
- D. the MAC address of Host C
- E. the IP address of the router's E0 interface
- F. the MAC address of the router's E0 interface

Answer: CF

Explanation:

While transferring data through many different networks, the source and destination IP addresses are not changed. Only the source and destination MAC addresses are changed. So in this case Host A will use the IP address of Host C and the MAC address of E0 interface to send data. When the router receives this data, it replaces the source MAC address with its own E1 interface's MAC address and replaces the destination MAC address with Host C's MAC address before sending to Host C.

QUESTION 16

For what two purposes does the Ethernet protocol use physical addresses? (Choose two.)

- 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:

Physical addresses or MAC addresses are used to identify devices at layer 2.

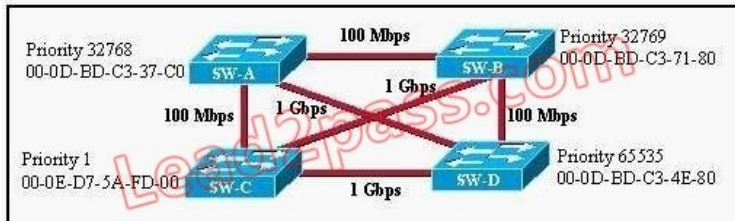
MAC addresses are only used to communicate on the same network. To communicate on different network we have to use Layer 3 addresses (IP addresses) -> B is not correct.

Layer 2 frame and Layer 3 packet can be recognized via headers. Layer 3 packet also contains physical address ->

On Ethernet, each frame has the same priority to transmit by default -> All devices need a physical address to identify itself. If not, they can not communicate ->

QUESTION 17

Refer to the exhibit. Based on the information given, which switch will be elected root bridge and why?



- A. Switch A, because it has the lowest MAC address
- B. Switch A, because it is the most centrally located switch
- C. Switch B, because it has the highest MAC address
- D. Switch C, because it is the most centrally located switch
- E. Switch C, because it has the lowest priority
- F. Switch D, because it has the highest priority

Answer: E

Explanation:

To elect the root bridge in the LAN, first check the priority value. The switch having the lowest priority will win the election process. If Priority Value is the same then it checks the MAC Address; the switch having the lowest MAC Address will become the root bridge. In this case, switch C has the lowest MAC Address so it becomes the root bridge.

QUESTION 18

Refer to the exhibit. Switch-1 needs to send data to a host with a MAC address of 00b0.d056.efa4. What will Switch-1 do with this data?

```
Switch-1# show mac address-table
Dynamic Addresses Count:          3
Secure Addresses (User-defined) Count: 0
Static Addresses (User-defined) Count: 0
System Self Addresses Count:     47
Total Mac addresses:              50
Non-static Address Table:
Destination Address  Address Type  VLAN  Destination Port
-----
0010.0de0.e289      Dynamic      1     FastEthernet0/1
0010.7b00.1540      Dynamic      2     FastEthernet0/3
0010.7b00.1545      Dynamic      2     FastEthernet0/2
```

- A. Switch-1 will drop the data because it does not have an entry for that MAC address.
- B. Switch-1 will flood the data out all of its ports except the port from which the data originated.
- C. Switch-1 will send an ARP request out all its ports except the port from which the data originated.
- D. Switch-1 will forward the data to its default gateway.

Answer: B

Explanation:

This question tests the operating principles of the Layer 2 switch. Check the MAC address table of Switch1 and find that the MAC address of the host does not exist in the table. Switch1 will flood the data out all of its ports except the port from which the data originated to determine which port the host is located in.

Switches work as follows:

In output there is no MAC address of give host so switch floods to all ports except the source port.

QUESTION 19

What value is primarily used to determine which port becomes the root port on each nonroot switch in a spanning-tree topology?

- A. path cost
- B. lowest port MAC address
- C. VTP revision number
- D. highest port priority number
- E. port priority number and MAC address

Answer: A

Explanation:

The path cost to the root bridge is the most important value to determine which port will become the root port on each non-root switch. In particular, the port with lowest cost to the root bridge will become root port (on non-root switch).

QUESTION 20

What is the function of the command switchport trunk native vlan 999 on a Cisco Catalyst switch?

- A. It creates a VLAN 999 interface.
- B. It designates VLAN 999 for untagged traffic.
- C. It blocks VLAN 999 traffic from passing on the trunk.
- D. It designates VLAN 999 as the default for all unknown tagged traffic.

Answer: B

Explanation:

Configuring the Native VLAN for Untagged Traffic

A trunk port configured with 802.1Q tagging can receive both tagged and untagged traffic. By default, the switch forwards untagged traffic in the native VLAN configured for the port. The native VLAN is VLAN 1 by default.

If you want to pass the Cisco CCNA 200-120 exam sucessfully, recommend to read latest Cisco [200-120 dumps](#) full version.

