➢ Vendor: Cisco

➢ Exam Code: 200-125

➢ Exam Name: Cisco Certified Network Associate (v3.0)

➢ Question 1 – Question 50

QUESTION 1
Refer to the exhibit. What will Router1 do when it receives the data frame shown? (Choose three.)

Router1# **show ip arp**

Protocol	Address	Age(min)	Hardware Adddr	Type	Interface
Internet	192.168.20.5	9	0000.0c07.f892	ARPA	FastEthernet0/0
Internet	192.168.60.5	8	0000.0c07.ac00	ARPA	FastEthernet0/1
Internet	192.168.20.1	-	0000.0c63.ae45	ARPA	FastEthernet0/0
Internet	192.168.40.5	9	0000.0c07.4320	ARPA	FastEthernet0/2
Internet	192.168.60.1	-	0000.0c63.1300	ARPA	FastEthernet0/1
Internet	192.168.40.1	-	0000.0c36.6965	ARPA	FastEthernet0/2

Data Frame:

Source MAC	Source IP	Destination MAC	Destination IP
0000.0c07.f892	192.168.20.5	0000.0c63.ae45	192.168.40.5

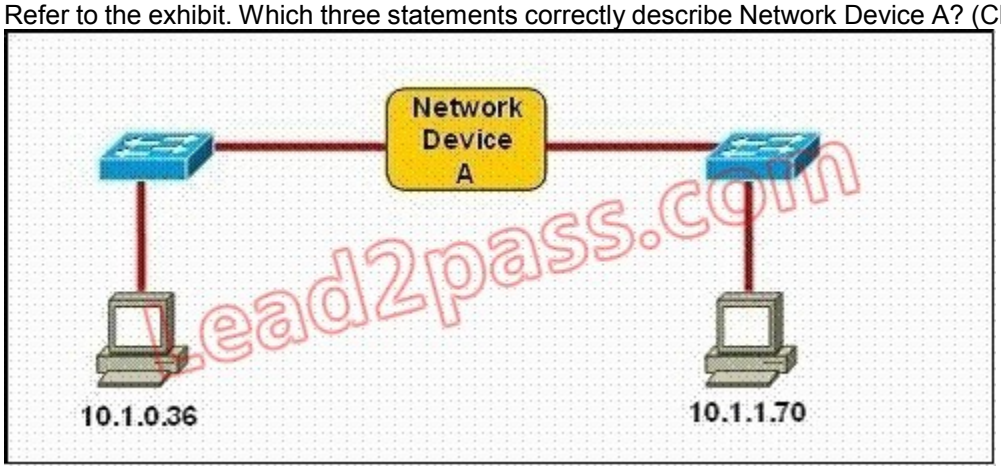
A. Router1 will strip off the source MAC address and replace it with the MAC address 0000.0c36.6965.
B. Router1 will strip off the source IP address and replace it with the IP address 192.168.40.1.
C. Router1 will strip off the destination MAC address and replace it with the MAC address 0000.0c07.4320.
D. Router1 will strip off the destination IP address and replace it with the IP address of 192.168.40.1.
E. Router1 will forward the data packet out interface FastEthernet0/1.
F. Router1 will forward the data packet out interface FastEthernet0/2.

Answer: ACF
Explanation:

Remember, the source and destination MAC changes as each router hop along with the TTL being decremented but the source and destination IP address remain the same from source to destination.

QUESTION 2

Refer to the exhibit. Which three statements correctly describe Network Device A? (Choose three.)



A. With a network wide mask of 255.255.255.128, each interface does not require an IP address.
B. With a network wide mask of 255.255.255.128, each interface does require an IP address on a unique IP subnet.
C. With a network wide mask of 255.255.255.0, must be a Layer 2 device for the PCs to communicate with each other.
D. With a network wide mask of 255.255.255.0, must be a Layer 3 device for the PCs to communicate with each other.
E. With a network wide mask of 255.255.254.0, each interface does not require an IP address.

Answer: BDE

Explanation:

If Subnet Mask is 255.255.255.128 the hosts vary from x.x.x.0 - x.x.x.127 & x.x.x.128- x.x.x.255,so the IP Addresses of 2 hosts fall in different subnets so each interface needs an IP an address so that they can communicate each other.
If Subnet Mask is 255.255.255.0 the 2 specified hosts fall in different subnets so they need a Layer 3 device to communicate.
If Subnet Mask is 255.255.254.0 the 2 specified hosts are in same subnet so are in network address and can be accommodated in same Layer 2 domain and can communicate with each other directly using the Layer 2 address.

QUESTION 3

Which layer in the OSI reference model is responsible for determining the availability of the receiving program and checking to see if enough resources exist for that communication?

A. transport
B. network
C. presentation
D. session
E. application

Answer: E

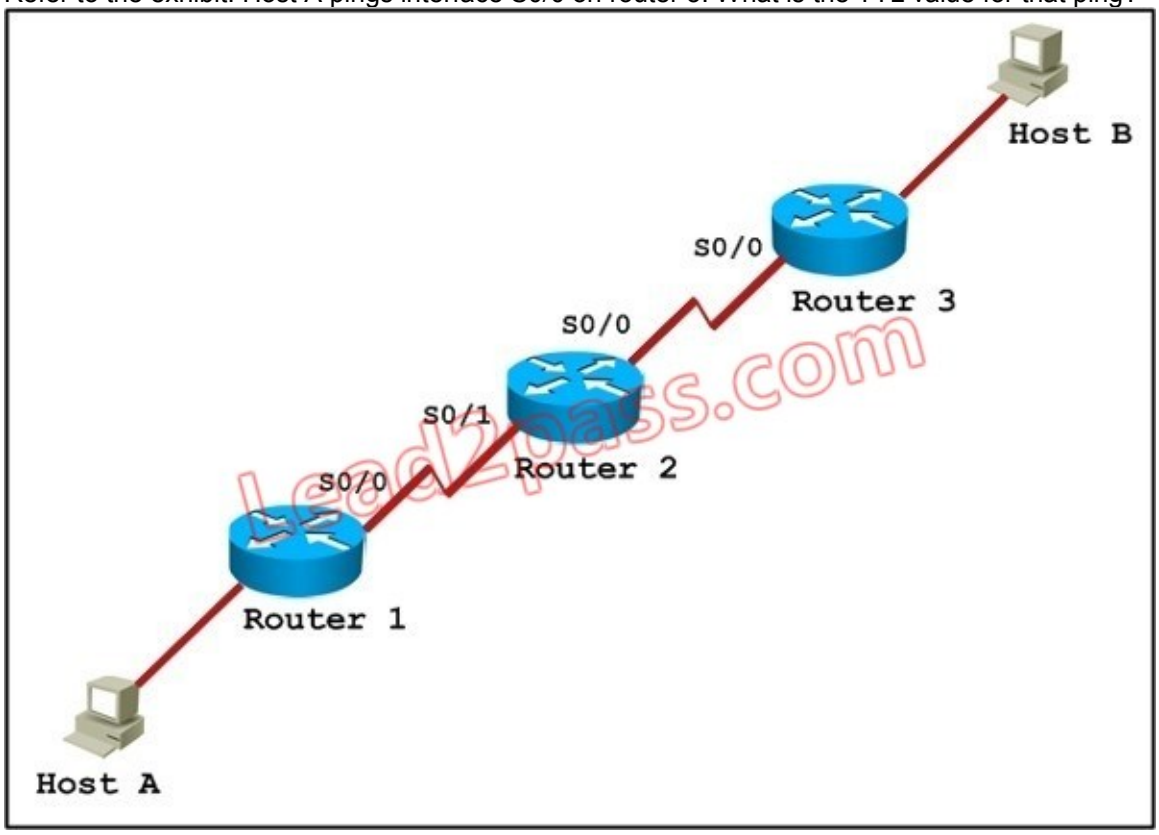
Explanation:

This question is to examine the OSI reference model. The Application layer is responsible for

identifying and establishing the availability of the intended communication partner and determining whether sufficient resources for the intended communication exist.

QUESTION 4

Refer to the exhibit. Host A pings interface S0/0 on router 3. What is the TTL value for that ping?



A. 252
B. 253
C. 254
D. 255

Answer: B

Explanation:

From the CCNA ICND2 Exam book: "Routers decrement the TTL by 1 every time they forward a packet; if a router decrements the TTL to 0, it throws away the packet. This prevents packets from rotating forever." I want to make it clear that before the router forwards a packet, the TTL is still remain the same. For example in the topology above, pings to S0/1 and S0/0 of Router 2 have the same TTL.

QUESTION 5

Which of the following describes the roles of devices in a WAN? (Choose three.)

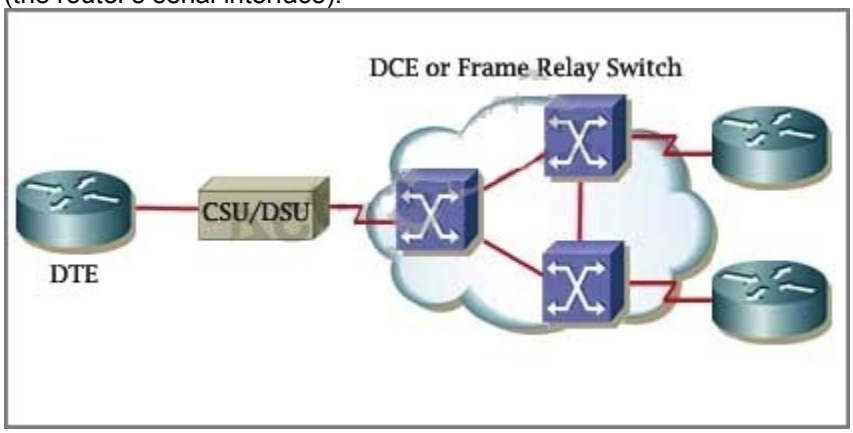
A. A CSU/DSU terminates a digital local loop.
B. A modem terminates a digital local loop.
C. A CSU/DSU terminates an analog local loop.
D. A modem terminates an analog local loop.
E. A router is commonly considered a DTE device.

F. A router is commonly considered a DCE device.

Answer: ADE

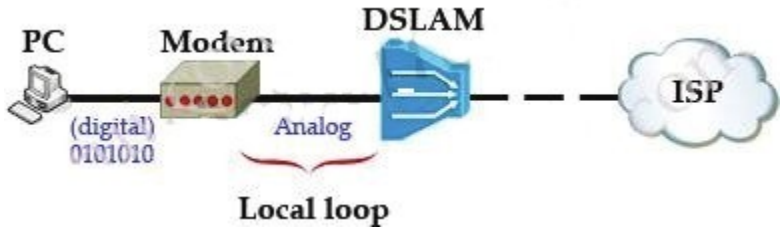
Explanation:

The idea behind a WAN is to be able to connect two DTE networks together through a DCE network. The network's DCE device (includes CSU/DSU) provides clocking to the DTE-connected interface (the router's serial interface).



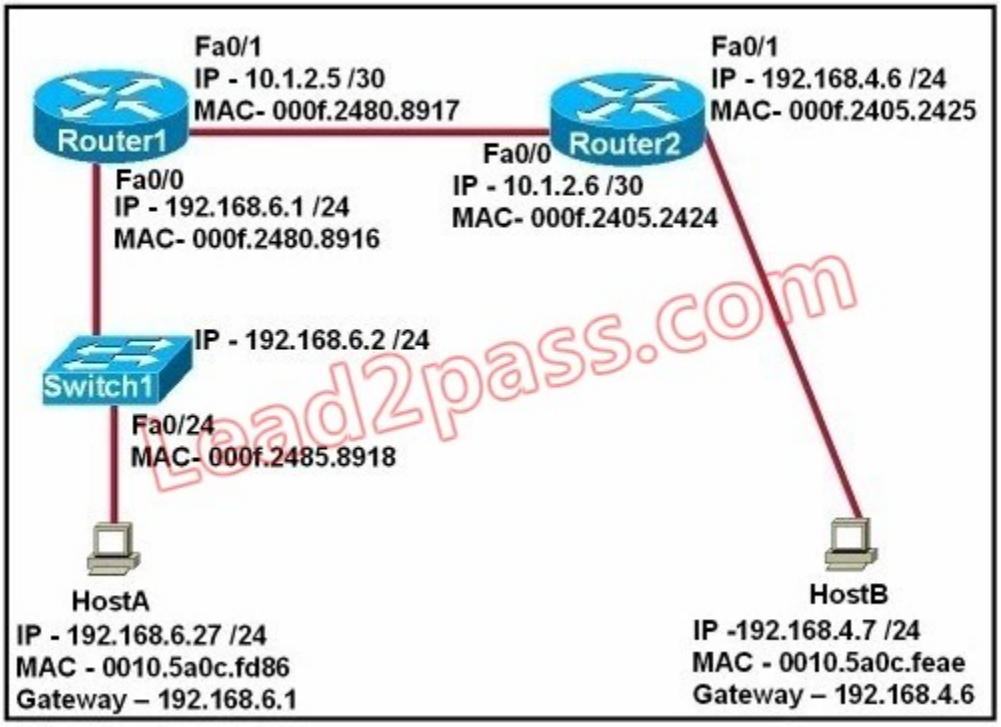
A modem modulates outgoing digital signals from a computer or other digital device to analog signals for a conventional copper twisted pair telephone line and demodulates the incoming analog signal and converts it to a digital signal for the digital device. A CSU/DSU is used between two digital lines -

For more explanation of answer D, in telephony the local loop (also referred to as a subscriber line) is the physical link or circuit that connects from the demarcation point of the customer premises to the edge of the carrier or telecommunications service provider's network. Therefore a modem terminates an analog local loop is correct.



QUESTION 6

Refer to the exhibit. Refer to the exhibit. After HostA pings HostB, which entry will be in the ARP cache of HostA to support this transmission?



A.

Interface Address	Physical Address	Type
192.168.4.7	000f.2480.8916	dynamic

B.

Interface Address	Physical Address	Type
192.168.4.7	0010.5a0c.feae	dynamic

C.

Interface Address	Physical Address	Type
192.168.6.1	0010.5a0c.feae	dynamic

D.

Interface Address	Physical Address	Type
192.168.6.1	000f.2480.8916	dynamic

E.

Interface Address	Physical Address	Type
192.168.6.2	0010.5a0c.feae	dynamic

F.

Interface Address	Physical Address	Type
192.168.6.2	000f.2485.8918	dynamic

Answer: A
Explanation:
When a host needs to reach a device on another subnet, the ARP cache entry will be that of the Ethernet address of the local router (default gateway) for the physical MAC address. The destination IP address will not change, and will be that of the remote host (HostB).

QUESTION 7
A network administrator is verifying the configuration of a newly installed host by establishing an FTP connection to a remote server. What is the highest layer of the protocol stack that the network administrator is using for this operation?

A. application
B. presentation
C. session
D. transport
E. internet
F. data link

Answer: A
Explanation:
FTP belongs to Application layer and it is also the highest layer of the OSI model.

QUESTION 8
A network interface port has collision detection and carrier sensing enabled on a shared twisted pair network. From this statement, what is known about the network interface port?

A. This is a 10 Mb/s switch port.
B. This is a 100 Mb/s switch port.
C. This is an Ethernet port operating at half duplex.
D. This is an Ethernet port operating at full duplex.
E. This is a port on a network interface card in a PC.

Answer: C
Explanation:
Modern Ethernet networks built with switches and full-duplex connections no longer utilize CSMA/CD. CSMA/CD is only used in obsolete shared media Ethernet (which uses repeater or hub).

QUESTION 9
A receiving host computes the checksum on a frame and determines that the frame is damaged. The frame is then discarded. At which OSI layer did this happen?

A. session
B. transport
C. network
D. data link
E. physical

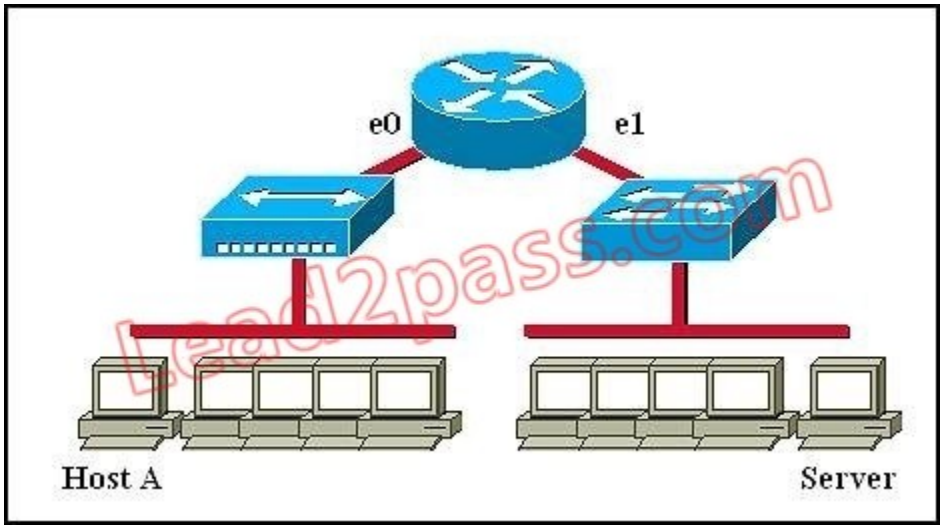
Answer: D
Explanation:
The Data Link layer provides the physical transmission of the data and handles error notification, network topology, and flow control. The Data Link layer formats the message into pieces, each called a data frame, and adds a customized header containing the hardware destination and source address. Protocols Data Unit (PDU) on Datalink layer is called frame. According to this question the frame is damaged and discarded which will happen at the Data Link layer.

QUESTION 10
Which of the following correctly describe steps in the OSI data encapsulation process? (Choose two.)

A. The transport layer divides a data stream into segments and may add reliability and flow control information.
B. The data link layer adds physical source and destination addresses and an FCS to the segment.
C. Packets are created when the network layer encapsulates a frame with source and destination host addresses and protocol-related control information.
D. Packets are created when the network layer adds Layer 3 addresses and control information to a segment.
E. The presentation layer translates bits into voltages for transmission across the physical link.

Answer: AD
Explanation:
The Application Layer (Layer 7) refers to communications services to applications and is the interface between the network and the application. Examples include. Telnet, HTTP, FTP, Internet browsers, NFS, SMTP gateways, SNMP, X.400 mail, and FTAM.
The Presentation Layer (Layer 6) defining data formats, such as ASCII text, EBCDIC text, binary, BCD, and JPEG. Encryption also is defined as a presentation layer service. Examples include. JPEG, ASCII, EBCDIC, TIFF, GIF, PICT, encryption, MPEG, and MIDI.
The Session Layer (Layer 5) defines how to start, control, and end communication sessions. This includes the control and management of multiple bidirectional messages so that the application can be notified if only some of a series of messages are completed. This allows the presentation layer to have a seamless view of an incoming stream of data. The presentation layer can be presented with data if all flows occur in some cases. Examples include. RPC, SQL, NFS, NetBios names, AppleTalk ASP, and DECnet SCP
The Transport Layer (Layer 4) defines several functions, including the choice of protocols. The most important Layer 4 functions are error recovery and flow control. The transport layer may provide for retransmission, i.e., error recovery, and may use flow control to prevent unnecessary congestion by attempting to send data at a rate that the network can accommodate, or it might not, depending on the choice of protocols. Multiplexing of incoming data for different flows to applications on the same host is also performed. Reordering of the incoming data stream when packets arrive out of order is included. Examples include. TCP, UDP, and SPX.
The Network Layer (Layer 3) defines end-to-end delivery of packets and defines logical addressing to accomplish this. It also defines how routing works and how routes are learned; and how to fragment a packet into smaller packets to accommodate media with smaller maximum transmission unit sizes. Examples include. IP, IPX, AppleTalk DDP, and ICMP. Both IP and IPX define logical addressing, routing, the learning of routing information, and end-to-end delivery rules. The IP and IPX protocols most closely match the OSI network layer (Layer 3) and are called Layer 3 protocols because their functions most closely match OSI's Layer 3.
The Data Link Layer (Layer 2) is concerned with getting data across one particular link or medium. The data link protocols define delivery across an individual link. These protocols are necessarily concerned with the type of media in use. Examples includE. IEEE 802.3/802.2, HDLC, Frame Relay, PPP, FDDI, ATM, and IEEE 802.5/802.2.

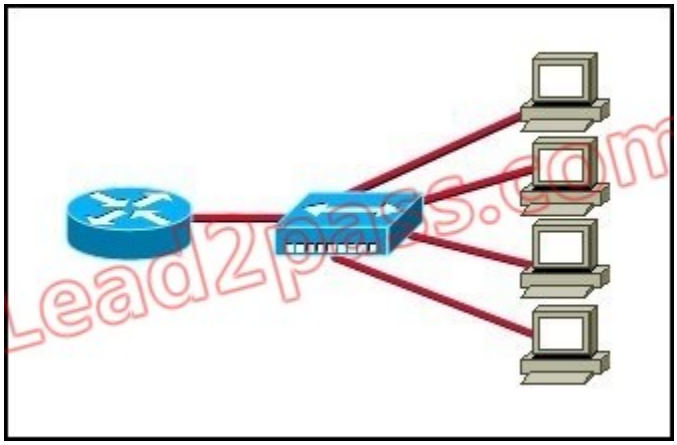
QUESTION 11
Refer to the graphic. Host A is communicating with the server. What will be the source MAC address of the frames received by Host A from the server?



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.)

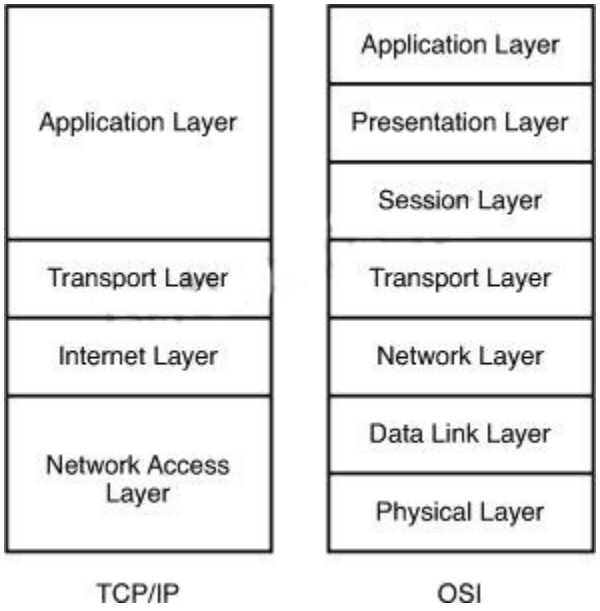
A. Spanning Tree Protocol allows switches to automatically share VLAN information.
B. Establishing VLANs increases the number of broadcast domains.
C. Switches that are configured with VLANs make forwarding decisions based on both Layer 2 and Layer 3 address information.
D. Microsegmentation decreases 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.

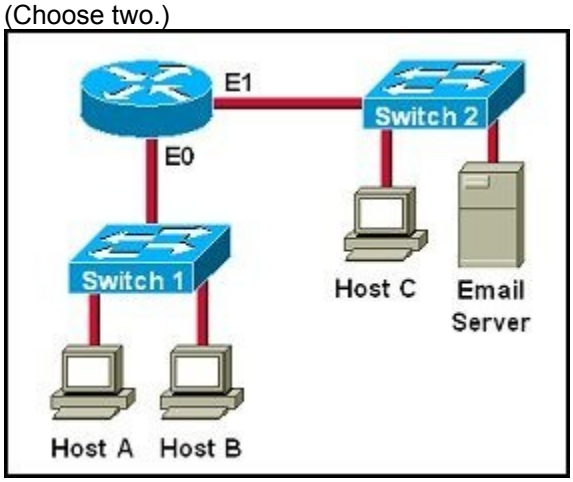
QUESTION 14
Where does routing occur within the DoD TCP/IP reference model?

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

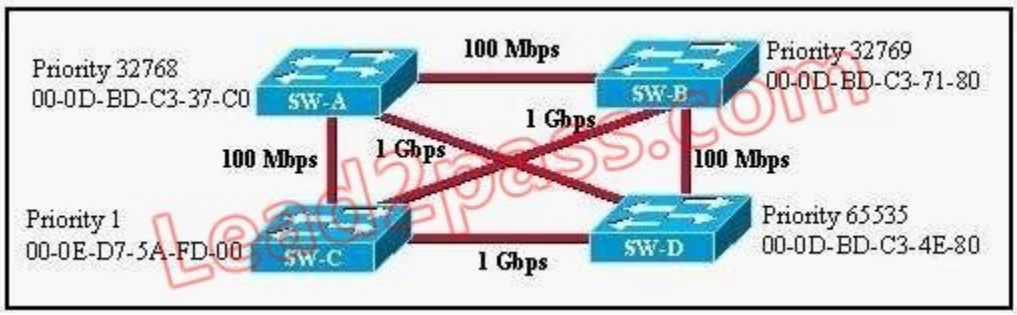
Answer: CF
Explanation:
While transferring data through many different networks, the source and destination IP addresses are not changed. Only the source and destination MAC addresses are changed. So in this case Host A will use the IP address of Host C and the MAC address of E0 interface to send data. When the router receives this data, it replaces the source MAC address with it 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:               41
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.

QUESTION 21
Which two protocols are used by bridges and/or switches to prevent loops in a layer 2 network? (Choose two.)

A. 802.1d
B. VTP
C. 802.1q
D. STP
E. SAP

Answer: AD
Explanation:
This question is to examine the STP protocol.
STP (802.1d) is used to prevent Layer 2 loops.
802.1q is a Frame Relay protocol which belongs to VLAN.
SAP is a concept of the OSI model.

QUESTION 22
Which switch would STP choose to become the root bridge in the selection process?

A. 32768: 11-22-33-44-55-66
B. 32768: 22-33-44-55-66-77
C. 32769: 11-22-33-44-55-65
D. 32769: 22-33-44-55-66-78

Answer: A

QUESTION 23
A switch is configured with all ports assigned to vlan 2 with full duplex FastEthernet to segment existing departmental traffic. What is the effect of adding switch ports to a new VLAN on the switch?

A. More collision domains will be created.
B. IP address utilization will be more efficient.
C. More bandwidth will be required than was needed previously.
D. An additional broadcast domain will be created.

Answer: D
Explanation:
Each VLAN creates its own broadcast domain. Since this is a full duplex switch, each port is a separate collision domain.

QUESTION 24

What are three benefits of implementing VLANs? (Choose three.)

A. A higher level of network security can be reached by separating sensitive data traffic from other network traffic.
B. A more efficient use of bandwidth can be achieved allowing many physical groups to use the same network infrastructure.
C. A more efficient use of bandwidth can be achieved allowing many logical networks to use the same network infrastructure.
D. Broadcast storms can be mitigated by increasing the number of broadcast domains, thus reducing their size.
E. Broadcast storms can be mitigated by decreasing the number of broadcast domains, thus increasing their size.
F. VLANs make it easier for IT staff to configure new logical groups, because the VLANs all belong to the same broadcast domain.
G. Port-based VLANs increase switch-port use efficiency, thanks to 802.1Q trunks.

Answer: ACD
Explanation:
Benefits of VLANs
VLAN is a network structure which allows users to communicate while in different locations by sharing one multicast domain and a single broadcast. They provide numerous networking benefits and have become popular in the market. For instance, it helps reduce administrative costs when users are geographically dispersed.
1. Inexpensive
The popularity of VLANs is due to the fact that changes, adds, and moves can be attained simply by making necessary configurations on the VLAN port. Time-consuming, re-addressing, and host reconfigurations is now a thing of the past, because network configuration can be made at ease when need arises.
2. Better management
A VLAN typically solve the scalability issues that exist in a large network by breaking the main domain into several VLAN groups or smaller broadcast configurations, thereby encourage better control of multicast traffic as well as broadcast domains.
3. Improves network security
High-security can be positioned in different VLAN groups to ensure that non-members cannot receive their broadcasts. On the other hand, a router is added and workgroups relocated into centralized locations.
4. Enhances performance
A more efficient use of bandwidth can be achieved allowing many logical networks to use the same network infrastructure.
5. Segment multiple networks
VLANs are typically used to achieve multiple purposes. They are popularly used to reduce broadcast traffic. Each VLAN creates a separate, smaller broadcast domain.
6. Better administration
VLANs facilitate grouping of multiple geographical stations. When VLAN users move to another physical location, the network does not have to be configured.

QUESTION 25
Which IEEE standard protocol is initiated as a result of successful DTP completion in a switch over Fast Ethernet?

A. 802.3ad
B. 802.1w
C. 802.1D

D. 802.1Q

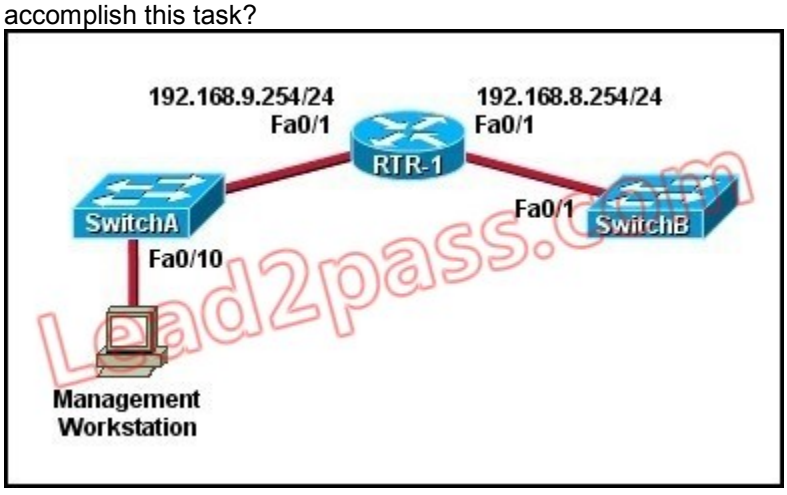
Answer: D
Explanation:
Dynamic Trunking Protocol (DTP) is a Cisco proprietary protocol for negotiating trunking on a link between two devices and for negotiating the type of trunking encapsulation (802.1Q) to be used.

QUESTION 26
Which of the following are benefits of VLANs? (Choose three.)

A. They increase the size of collision domains.
B. They allow logical grouping of users by function.
C. They can enhance network security.
D. They increase the size of broadcast domains while decreasing the number of collision domains.
E. They increase the number of broadcast domains while decreasing the size of the broadcast domains.
F. They simplify switch administration.

Answer: BCE
Explanation:
When using VLAN the number and size of collision domains remain the same -> VLANs allow to group users by function, not by location or geography -> . VLANs help minimize the incorrect configuration of VLANs so it enhances the security of the network -> .
VLAN increases the size of broadcast domains but does not decrease the number of collision domains ->
VLANs increase the number of broadcast domains while decreasing the size of the broadcast domains which increase the utilization of the links. It is also a big advantage of VLAN -> . VLANs are useful but they are more complex and need more administration ->

QUESTION 27
Refer to the exhibit. A technician has installed SwitchB and needs to configure it for remote access from the management workstation connected to SwitchA . Which set of commands is required to accomplish this task?



A.
```
SwitchB(config)# interface FastEthernet 0/1
SwitchB(config-if)# ip address 192.168.8.252 255.255.255.0
SwitchB(config-if)# no shutdown
```
B.
```
SwitchB(config)# interface vlan 1
SwitchB(config-if)# ip address 192.168.8.252 255.255.255.0
```

```
SwitchB(config-if)# ip default-gateway 192.168.8.254 255.255.255.0
SwitchB(config-if)# no shutdown
```

C.
```
SwitchB(config)# ip default-gateway 192.168.8.254
SwitchB(config)# interface vlan 1
SwitchB(config-if)# ip address 192.168.8.252 255.255.255.0
SwitchB(config-if)# no shutdown
```

D.
```
SwitchB(config)# ip default-network 192.168.8.254
SwitchB(config)# interface vlan 1
SwitchB(config-if)# ip address 192.168.8.252 255.255.255.0
SwitchB(config-if)# no shutdown
```

E.
```
SwitchB(config)# ip route 192.168.8.254 255.255.255.0
SwitchB(config)# interface FastEthernet 0/1
SwitchB(config-if)# ip address 192.168.8.252 255.255.255.0
SwitchB(config-if)# no shutdown
```

Answer: C
Explanation:
To remote access to SwitchB, it must have a management IP address on a VLAN on that switch. Traditionally, we often use VLAN 1 as the management VLAN (but in fact it is not secure). In the exhibit, we can recognize that the Management Workstation is in a different subnet from the SwitchB. For intersubnetwork communication to occur, you must configure at least one default gateway. This default gateway is used to forward traffic originating from the switch only, not to forward traffic sent by devices connected to the switch.

QUESTION 28
In an Ethernet network, under what two scenarios can devices transmit? (Choose two.)

A. when they receive a special token
B. when there is a carrier
C. when they detect no other devices are sending
D. when the medium is idle
E. when the server grants access

Answer: CD
Explanation:
Ethernet network is a shared environment so all devices have the right to access to the medium. If more than one device transmits simultaneously, the signals collide and can not reach the destination.
If a device detects another device is sending, it will wait for a specified amount of time before attempting to transmit.
When there is no traffic detected, a device will transmit its message. While this transmission is occurring, the device continues to listen for traffic or collisions on the LAN. After the message is sent, the device returns to its default listening mode.

QUESTION 29
Which two states are the port states when RSTP has converged? (Choose two.)

A. discarding
B. listening
C. learning
D. forwarding
E. disabled

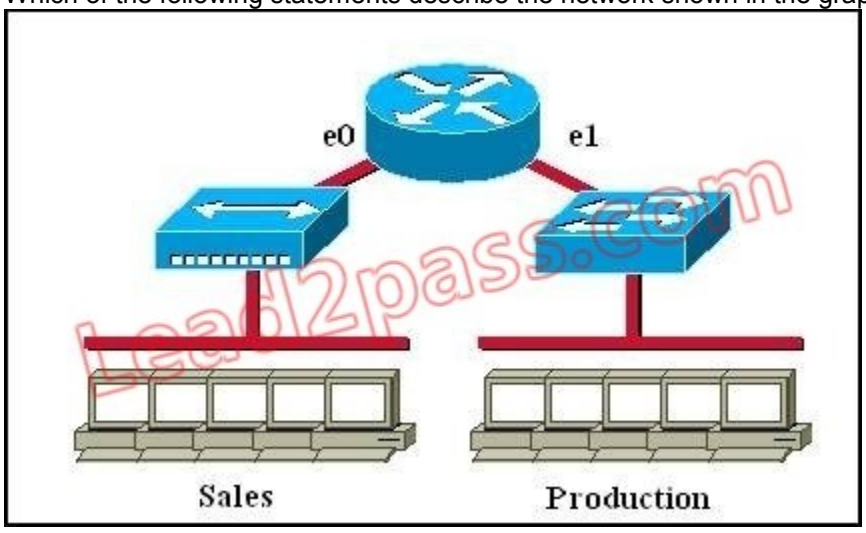
Answer: AD
Explanation:
http://www.cisco.com/en/US/tech/tk389/tk621/technologies_white_paper09186a0080094cfa.shtml#states

QUESTION 30
Which two commands can be used to verify a trunk link configuration status on a given Cisco switch interface? (Choose two.)

A. show interface trunk
B. show interface interface
C. show ip interface brief
D. show interface vlan
E. show interface switchport

Answer: AE

QUESTION 31
Which of the following statements describe the network shown in the graphic? (Choose two.)



A. There are two broadcast domains in the network.
B. There are four broadcast domains in the network.
C. There are six broadcast domains in the network.
D. There are four collision domains in the network.
E. There are five collision domains in the network.
F. There are seven collision domains in the network.

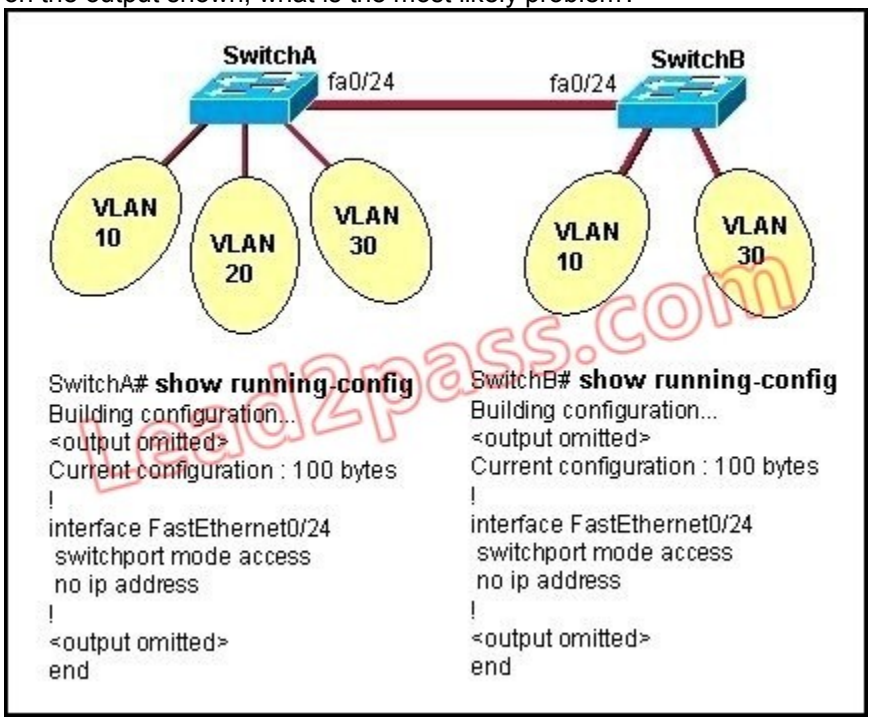
Answer: AF
Explanation:
Only router can break up broadcast domains so in the exhibit there are 2 broadcast domains: from e0 interface to the left is a broadcast domain and from e1 interface to the right is another broadcast domain ->.
Both router and switch can break up collision domains so there is only 1 collision domain on the left of the router (because hub doesn't break up collision domain) and there are 6 collision domains on the right of the router (1 collision domain from e1 interface to the switch + 5 collision domains for 5 PCs in Production) ->

QUESTION 32
Which command enables RSTP on a switch?

A. spanning-tree uplinkfast
B. spanning-tree mode rapid-pvst
C. spanning-tree backbonefast
D. spanning-tree mode mst

Answer: B
Explanation:
Ethernet network is a shared environment so all devices have the right to access to the medium. If more than one device transmits simultaneously, the signals collide and can not reach the destination.
If a device detects another device is sending, it will wait for a specified amount of time before attempting to transmit.
When there is no traffic detected, a device will transmit its message. While this transmission is occurring, the device continues to listen for traffic or collisions on the LAN. After the message is sent, the device returns to its default listening mode.

QUESTION 33
Refer to the exhibit. All switch ports are assigned to the correct VLANs, but none of the hosts connected to SwitchA can communicate with hosts in the same VLAN connected to SwitchB. Based on the output shown, what is the most likely problem?



A. The access link needs to be configured in multiple VLANs.
B. The link between the switches is configured in the wrong VLAN.
C. The link between the switches needs to be configured as a trunk.
D. VTP is not configured to carry VLAN information between the switches.
E. Switch IP addresses must be configured in order for traffic to be forwarded between the switches.

Answer: C
Explanation:
In order to pass traffic from VLANs on different switches, the connections between the switches must be configured as trunk ports.

QUESTION 34
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.

QUESTION 35
Refer to the exhibit. Given the output shown from this Cisco Catalyst 2950, what is the reason that interface FastEthernet 0/10 is not the root port for VLAN 2?

```
Switch# show spanning-tree interface fastethernet 0/10
Vlan             Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
VLAN0001         Root FWD 19        128.1    P2p
VLAN0002         Altn BLK 19        128.2    P2p
VLAN0003         Root FWD 19        128.2    P2p
```


A. This switch has more than one interface connected to the root network segment in VLAN 2.
B. This switch is running RSTP while the elected designated switch is running 802.1d Spanning Tree.
C. This switch interface has a higher path cost to the root bridge than another in the topology.
D. This switch has a lower bridge ID for VLAN 2 than the elected designated switch.

Answer: C
Explanation:
Since the port is in the blocked status, we must assume that there is a shorter path to the root bridge elsewhere.

QUESTION 36
Why will a switch never learn a broadcast address?

A. Broadcasts only use network layer addressing.
B. A broadcast frame is never forwarded by a switch.
C. A broadcast address will never be the source address of a frame.
D. Broadcast addresses use an incorrect format for the switching table.
E. Broadcast frames are never sent to switches.

Answer: C
Explanation:
Switches dynamically learn MAC addresses based on the source MAC addresses that it sees, and since a broadcast is never the source, it will never learn the broadcast address.

QUESTION 37
Refer to the exhibit. Why has this switch not been elected the root bridge for VLAN1?

```
Switch# show spanning-tree vlan 1
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority    20481
              Address     0008.217a.5800
              Cost        38
              Port        1 (FastEthernet0/1)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0008.205e.6600
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/4            Desg FWD 38        128.1    P2p
Fa0/11           Altn BLK 57        128.1    P2p
Fa0/13           Desg FWD 38        128.1    P2p
```


A. It has more than one interface that is connected to the root network segment.
B. It is running RSTP while the elected root bridge is running 802.1d spanning tree.
C. It has a higher MAC address than the elected root bridge.
D. It has a higher bridge ID than the elected root bridge.

Answer: D
Explanation:
The root bridge is determined by the lowest bridge ID, and this switch has a bridge ID priority of 32768, which is higher than the roots priority of 20481.

QUESTION 38
Which two link protocols are used to carry multiple VLANs over a single link? (Choose two.)

A. VTP
B. 802.1q
C. IGP
D. ISL
E. 802.3u

Answer: BD
Explanation:
Cisco switches can use two different encapsulation types for trunks, the industry standard 802.1q or the Cisco proprietary ISL. Generally, most network engineers prefer to use 802.1q since it is standards based and will interoperate with other vendors.

QUESTION 39
Assuming the default switch configuration, which VLAN range can be added, modified, and removed on a Cisco switch?

A. 1 through 1001
B. 2 through 1001
C. 1 through 1002
D. 2 through 1005

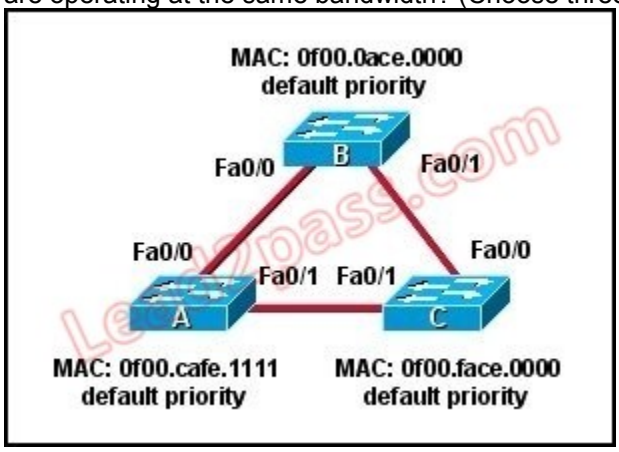
Answer: B
Explanation:
VLAN 1 is the default VLAN on Cisco switch. It always exists and can not be added, modified or removed.
VLANs 1002-1005 are default VLANs for FDDI & Token Ring and they can't be deleted or used for Ethernet.

QUESTION 40
Which statement about VLAN operation on Cisco Catalyst switches is true?

A. When a packet is received from an 802.1Q trunk, the VLAN ID can be determined from the source MAC address and the MAC address table.
B. Unknown unicast frames are retransmitted only to the ports that belong to the same VLAN.
C. Broadcast and multicast frames are retransmitted to ports that are configured on different VLAN.
D. Ports between switches should be configured in access mode so that VLANs can span across the ports.

Answer: B
Explanation:
Each VLAN resides in its own broadcast domain, so incoming frames with unknown destinations are only transmitted to ports that reside in the same VLAN as the incoming frame.

QUESTION 41
Refer to the topology shown in the exhibit. Which ports will be STP designated ports if all the links are operating at the same bandwidth? (Choose three.)

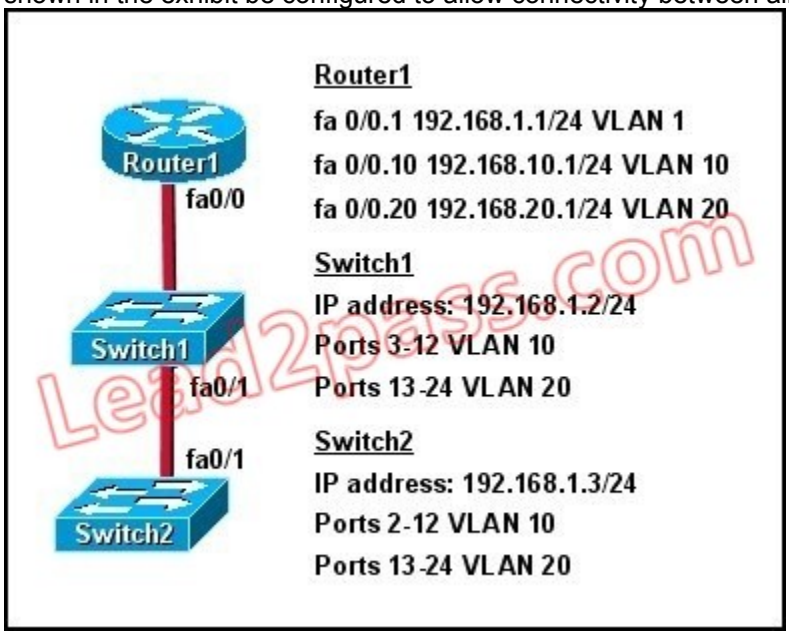


A. Switch A - Fa0/0
B. Switch A - Fa0/1
C. Switch B - Fa0/0
D. Switch B - Fa0/1

E. Switch C - Fa0/0
F. Switch C - Fa0/1

Answer: BCD
Explanation:
This question is to check the spanning tree election problem.
1. First, select the root bridge, which can be accomplished by comparing the bridge ID, the smallest will be selected. Bridge-id= bridge priority + MAC address. The three switches in the figure all have the default priority, so we should compare the MAC address, it is easy to find that SwitchB is the root bridge.
2. Select the root port on the non-root bridge, which can be completed through comparing root path cost. The smallest will be selected as the root port.
3. Next, select the Designated Port. First, compare the path cost, if the costs happen to be the same, then compare the BID, still the smallest will be selected. Each link has a DP. Based on the exhibit above, we can find DP on each link. The DP on the link between SwitchA and SwitchC is SwitchA'Fa0/1, because it has the smallest MAC address.

QUESTION 42
Refer to the exhibit. How should the FastEthernet0/1 ports on the 2950 model switches that are shown in the exhibit be configured to allow connectivity between all devices?



A. The ports only need to be connected by a crossover cable.
B.
```
SwitchX(config)# interface fastethernet 0/1
SwitchX(config-if)# switchport mode trunk
```
C.
```
SwitchX(config)# interface fastethernet 0/1
SwitchX(config-if)# switchport mode access
SwitchX(config-if)# switchport access vlan 1
```
D.
```
SwitchX(config)# interface fastethernet 0/1
SwitchX(config-if)# switchport mode trunk
SwitchX(config-if)# switchport trunk vlan 1
SwitchX(config-if)# switchport trunk vlan 10
SwitchX(config-if)# switchport trunk vlan 20
```

Answer: B

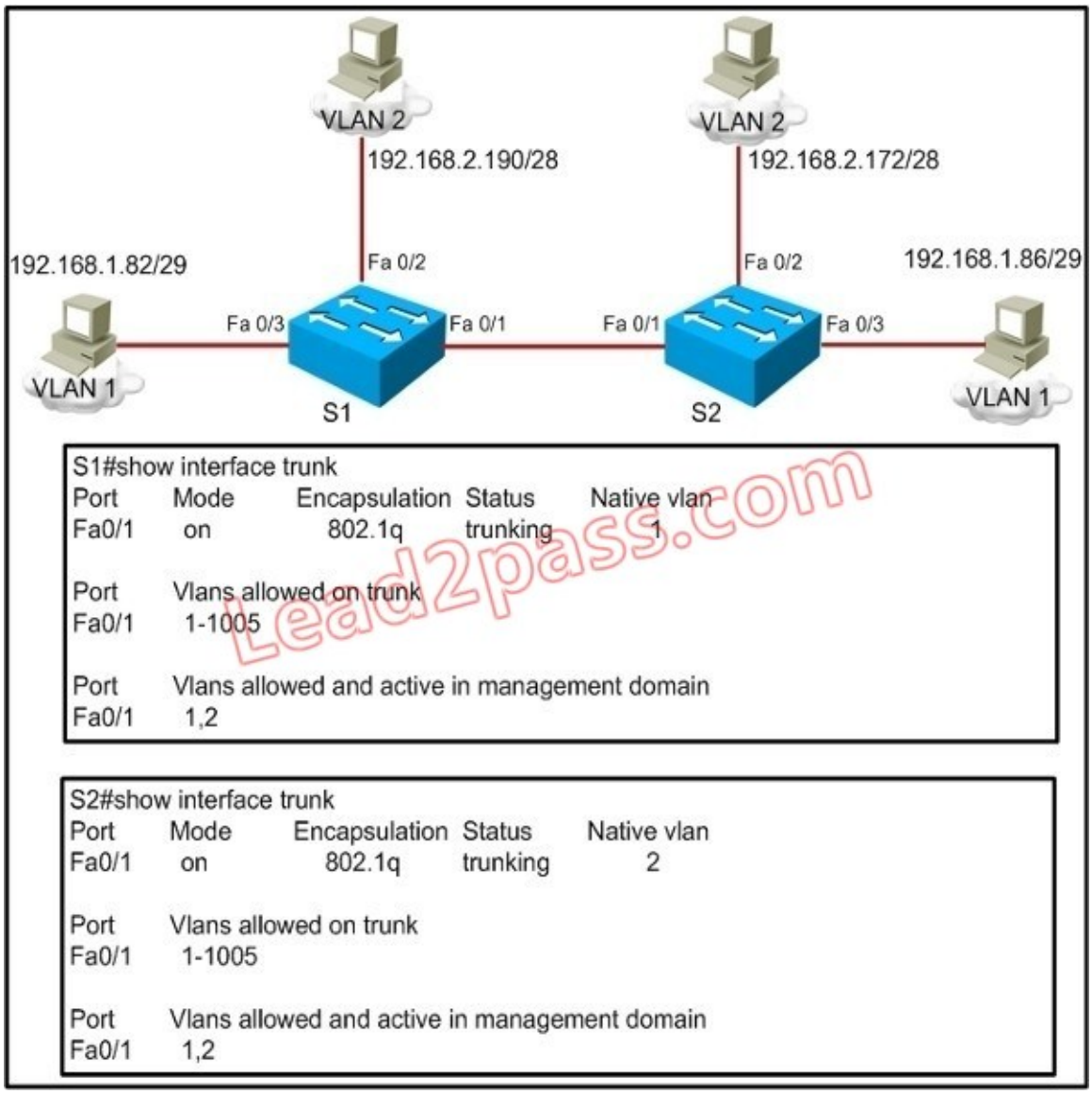
Explanation:
IN order for multiple VLANs to cross switches, the connection between the switches must be a trunk. The "switchport mode trunk" command is all that is needed, the individual VLANs should not be listed over that trunk interface.

QUESTION 43
Which three statements about RSTP are true? (Choose three.)

A. RSTP significantly reduces topology reconverging time after a link failure.
B. RSTP expands the STP port roles by adding the alternate and backup roles.
C. RSTP port states are blocking, discarding, learning, or forwarding.
D. RSTP provides a faster transition to the forwarding state on point-to-point links than STP does.
E. RSTP also uses the STP proposal-agreement sequence.
F. RSTP uses the same timer-based process as STP on point-to-point links.

Answer: ABD
Explanation:
One big disadvantage of STP is the low convergence which is very important in switched network. To overcome this problem, in 2001, the IEEE with document 802.1w introduced an evolution of the Spanning Tree Protocol: Rapid Spanning Tree Protocol (RSTP), which significantly reduces the convergence time after a topology change occurs in the network. While STP can take 30 to 50 seconds to transit from a blocking state to a forwarding state, RSTP is typically able to respond less than 10 seconds of a physical link failure.
RSTP works by adding an alternative port and a backup port compared to STP. These ports are allowed to immediately enter the forwarding state rather than passively wait for the network to converge.
RSTP bridge port roles:
* Root port - A forwarding port that is the closest to the root bridge in terms of path cost
* Designated port - A forwarding port for every LAN segment
* Alternate port - A best alternate path to the root bridge. This path is different than using the root port. The alternative port moves to the forwarding state if there is a failure on the designated port for the segment.
* Backup port - A backup/redundant path to a segment where another bridge port already connects. The backup port applies only when a single switch has two links to the same segment (collision domain). To have two links to the same collision domain, the switch must be attached to a hub.
* Disabled port - Not strictly part of STP, a network administrator can manually disable a port

QUESTION 44
Refer to the exhibit. A frame on VLAN 1 on switch S1 is sent to switch S2 where the frame is received on VLAN 2. What causes this behavior?



A. trunk mode mismatches
B. allowing only VLAN 2 on the destination
C. native VLAN mismatches
D. VLANs that do not correspond to a unique IP subnet

Answer: C
Explanation:
Untagged frames are encapsulated with the native VLAN. In this case, the native VLANs are different so although S1 will tag it as VLAN 1 it will be received by S2.

QUESTION 45
At which layer of the OSI model is RSTP used to prevent loops?

A. physical
B. data link

C. network
D. transport

Answer: B
Explanation:
RSTP and STP operate on switches and are based on the exchange of Bridge Protocol Data Units (BPDUs) between switches. One of the most important fields in BPDUs is the Bridge Priority in which the MAC address is used to elect the Root Bridge -> RSTP operates at Layer 2 ?Data Link layer -> .

QUESTION 46
What does a Layer 2 switch use to decide where to forward a received frame?

A. source MAC address
B. source IP address
C. source switch port
D. destination IP address
E. destination port address
F. destination MAC address

Answer: F
Explanation:
When a frame is received, the switch looks at the destination hardware address and finds the interface if it is in its MAC address table. If the address is unknown, the frame is broadcast on all interfaces except the one it was received on.

QUESTION 47
Refer to the exhibit. Which statement is true?

```
SwitchA# show spanning-tree vlan 20

VLAN0020
  Spanning tree enabled protocol rstp
  Root ID     Priority    24596
              Address     0017.596d.2a00
              Cost        38
              Port        11 (FastEthernet0/11)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    28692  (priority 28672 sys-id-ext 20)
              Address     0017.596d.1580
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- ---------
Fa0/11           Root FWD 19        128.11   P2p
Fa0/12           Altn BLK 19        128.12   P2p
```


A. The Fa0/11 role confirms that SwitchA is the root bridge for VLAN 20.
B. VLAN 20 is running the Per VLAN Spanning Tree Protocol.

C. The MAC address of the root bridge is 0017.596d.1580.
D. SwitchA is not the root bridge, because not all of the interface roles are designated.

Answer: D
Explanation:
Only non-root bridge can have root port. Fa0/11 is the root port so we can confirm this switch is not the root bridge ->
From the output we learn this switch is running Rapid STP, not PVST -> 0017.596d.1580 is the MAC address of this switch, not of the root bridge. The MAC address of the root bridge is 0017.596d.2a00 ->
All of the interface roles of the root bridge are designated. SwitchA has one Root port and 1 Alternative port so it is not the root bridge.

QUESTION 48
Which two benefits are provided by creating VLANs? (Choose two.)

A. added security
B. dedicated bandwidth
C. provides segmentation
D. allows switches to route traffic between subinterfaces
E. contains collisions

Answer: AC
Explanation:
A VLAN is a switched network that is logically segmented on an organizational basis, by functions, project teams, or applications rather than on a physical or geographical basis.
Security:
VLANs also improve security by isolating groups. High-security users can be grouped into a VLAN, possible on the same physical segment, and no users outside that VLAN can communicate with them
LAN Segmentation
VLANs allow logical network topologies to overlay the physical switched infrastructure such that any arbitrary collection of LAN ports can be combined into an autonomous user group or community of interest. The technology logically segments the network into separate Layer 2 broadcast domains whereby packets are switched between ports designated to be within the same VLAN. By containing traffic originating on a particular LAN only to other LANs in the same VLAN, switched virtual networks avoid wasting bandwidth.

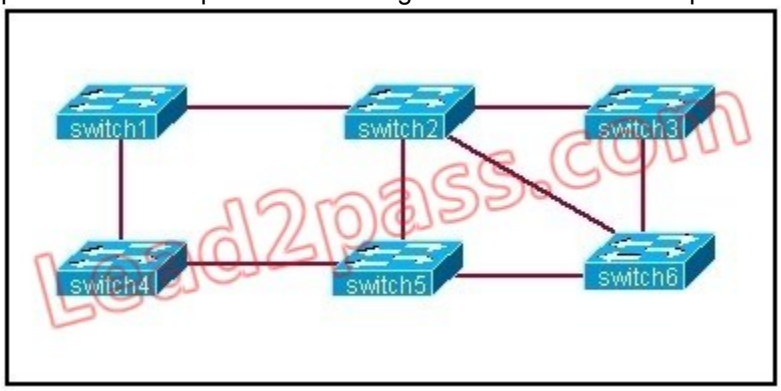
QUESTION 49
Which command can be used from a PC to verify the connectivity between hosts that connect through a switch in the same LAN?

A. pingaddress
B. tracertaddress
C. traceroute address
D. arpaddress

Answer: A
Explanation:
ICMP pings are used to verify connectivity between two IP hosts. Traceroute is used to verify the router hop path traffic will take but in this case since the hosts are in the same LAN there will be no router hops involved.

QUESTION 50

Based on the network shown in the graphic. Which option contains both the potential networking problem and the protocol or setting that should be used to prevent the problem?



A. routing loops, hold down timers
B. switching loops, split horizon
C. routing loops, split horizon
D. switching loops, VTP
E. routing loops, STP
F. switching loops, STP

Answer: F

Explanation:

The Spanning-Tree Protocol (STP) prevents loops from being formed when switches or bridges are interconnected via multiple paths. Spanning-Tree Protocol implements the 802.1D IEEE algorithm by exchanging BPDU messages with other switches to detect loops, and then removes the loop by shutting down selected bridge interfaces. This algorithm guarantees that there is one and only one active path between two network devices.