CERTKILLERS

Cisco

100-105 Exam

Cisco Interconnecting Cisco Networking Devices Part 1 Exam

Thank you for Downloading 100-105 exam PDF Demo

You can Buy Latest 100-105 Full Version Download

https://www.certkillers.net/Exam/100-105

https://www.certkillers.net

Version: 15.0

Question: 1

Which three statements are true about the operation of a full-duplex Ethernet network? (Choose three.)

A. There are no collisions in full-duplex mode.
B. A dedicated switch port is required for each full-duplex node.
C. Ethernet hub ports are preconfigured for full-duplex mode.
D. In a full-duplex environment, the host network card must check for the availability of the network media before transmitting.
E. The host network card and the switch port must be capable of operating in full-duplex mode.

Answer: A, B, E

Explanation:
Half-duplex Ethernet is defined in the original 802.3 Ethernet and Cisco says you only use one wire pair with a digital signal running in both directions on the wire. It also uses the CSMA/CD protocol to help prevent collisions and to permit retransmitting if a collision does occur. If a hub is attached to a switch, it must operate in half-duplex mode because the end stations must be able to detect collisions. Half-duplex Ethernet—typically 10BaseT—is only about 30 to 40 percent efficient as Cisco sees it, because a large 10BaseT network will usually only give you 3- to 4Mbps—at most.
Full-duplex Ethernet uses two pairs of wires, instead of one wire pair like half duplex. Also, full duplex uses a point-to-point connection between the transmitter of the transmitting device and the receiver of the receiving device, which means that with full-duplex data transfer, you get a faster data transfer compared to half duplex. And because the transmitted data is sent on a different set of wires than the received data, no collisions occur. The reason you don't need to worry about collisions is because now Full-duplex Ethernet is like a freeway with multiple lanes instead of the single-lane road provided by half duplex. Full-duplex Ethernet is supposed to offer 100 percent efficiency in both directions; this means you can get 20Mbps with a 10Mbps Ethernet running full duplex, or 200Mbps for FastEthernet.
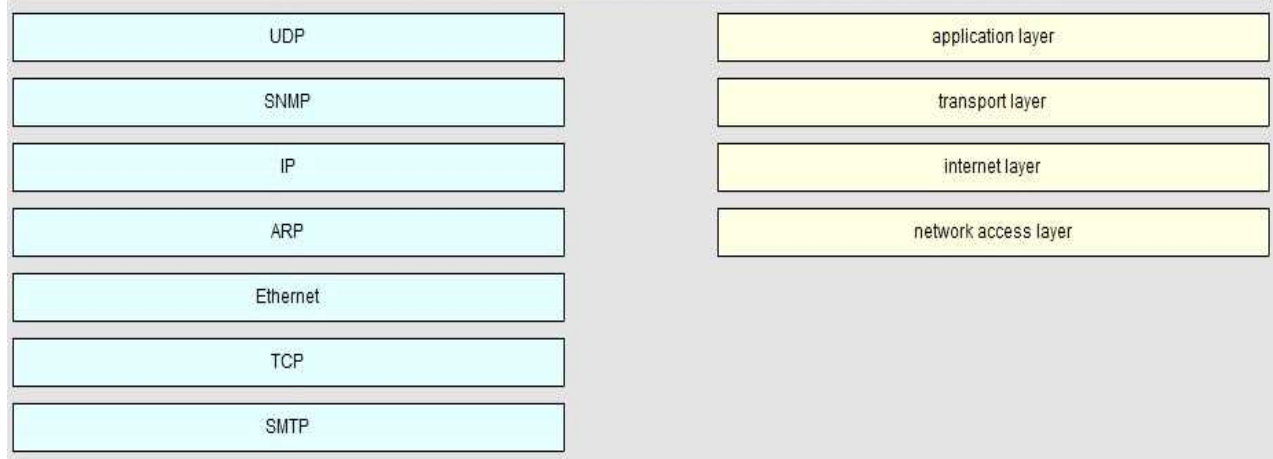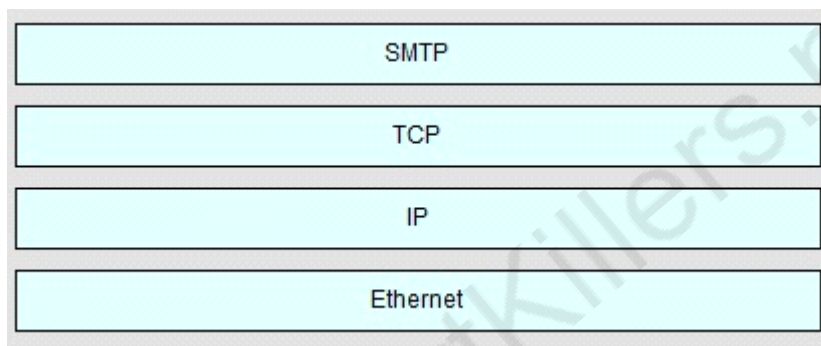
Question: 2

DRAG DROP
On the left are various network protocols. On the right are the layers of the TCP/IP model. Assuming a reliable connection is required, move the protocols on the left to the TCP/IP layers on the right to show the proper encapsulation for an email message sent by a host on a LAN. (Not all options are used.)

On the left are various network protocols. On the right are the layers of the TCP/IP model. Assuming a reliable connection is required, move the protocols on the left to the TCP/IP layers on the right to show the proper encapsulation for an email message sent by a host on a LAN. (Not all options are used.)

UDP	application layer
SNMP	transport layer
IP	internet layer
ARP	network access layer
Ethernet	
TCP	
SMTP	

Answer:

SMTP
TCP
IP
Ethernet

Question: 3

Which OSI layer header contains the address of a destination host that is on another network?

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

Answer: D

Explanation:
Only network address contains this information. To transmit the packets the sender uses network address and datalink address. But the layer 2 address represents just the address of the next hop device on the way to the sender. It is changed on each hop. Network address remains the same.
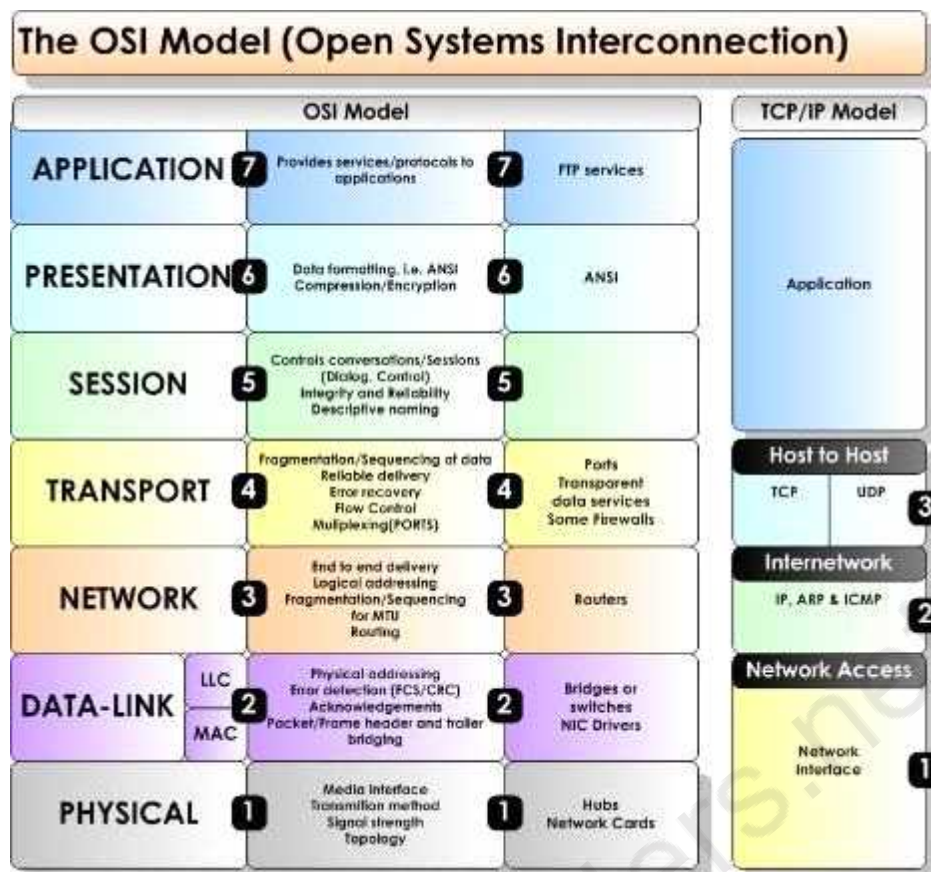
Question: 4

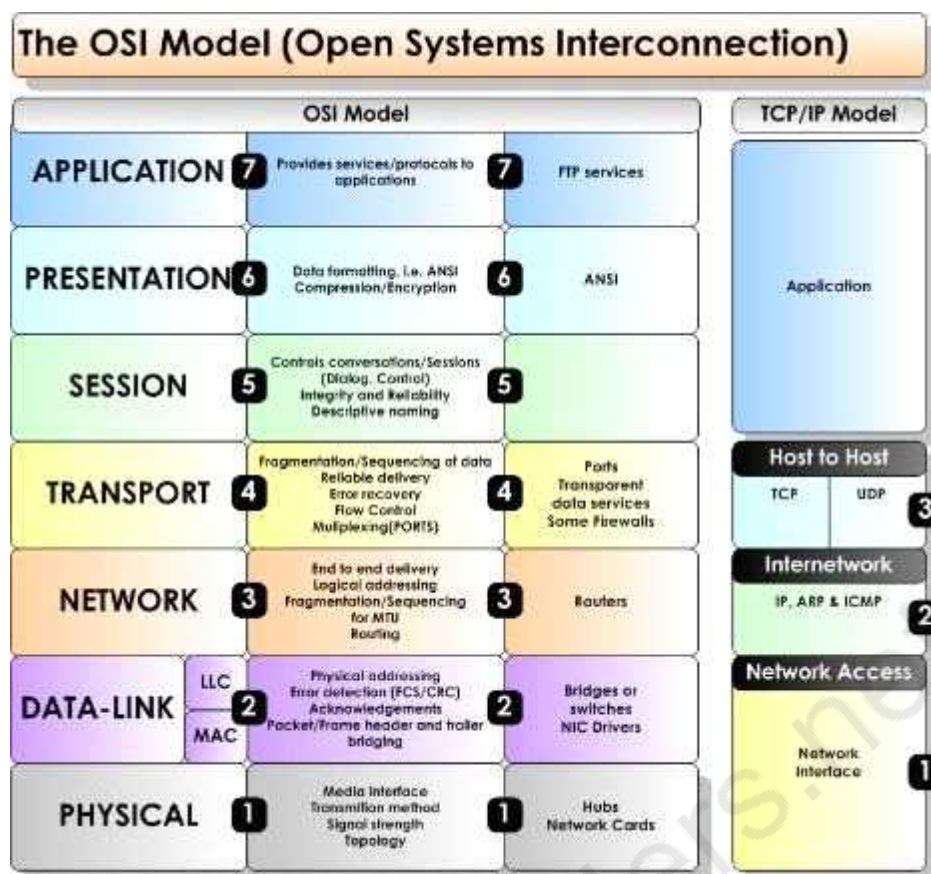Which layer of the TCP/IP stack combines the OSI model physical and data link layers?

A. Internet layer
B. transport layer
C. application layer
D. network access layer

Answer: D

Explanation:
The Internet Protocol Suite, TCP/IP, is a suite of protocols used for communication over the internet. The TCP/ IP model was created after the OSI 7 layer model for two major reasons. First, the foundation of the Internet was built using the TCP/IP suite and through the spread of the World Wide Web and Internet, TCP/IP has been preferred. Second, a project researched by the Department of Defense (DOD) consisted of creating the TCP/IP protocols. The DOD's goal was to bring international standards which could not be met by the OSI model.
Since the DOD was the largest software consumer and they preferred the TCP/IP suite, most vendors used this model rather than the OSI. Below is a side by side comparison of the TCP/IP and OSI models.

The OSI Model (Open Systems Interconnection)

OSI Model				TCP/IP Model
APPLICATION 7	Provides services/protocols to applications	7	FTP services	Application
PRESENTATION 6	Data formatting, i.e. ANSI Compression/Encryption	6	ANSI	
SESSION 5	Controls conversations/Sessions (Dialog. Control) Integrity and Reliability Descriptive naming	5		
TRANSPORT 4	Fragmentation/Sequencing of data Reliable delivery Error recovery Flow Control Multiplexing(PORTS)	4	Ports Transparent data services Some Firewalls	Host to Host TCP UDP 3
NETWORK 3	End to end delivery Logical addressing Fragmentation/Sequencing for MTU Routing	3	Routers	Internetwork IP, ARP & ICMP 2
DATA-LINK LLC MAC 2	Physical addressing Error detection (FCS/CRC) Acknowledgements Packet/Frame header and trailer bridging	2	Bridges or switches NIC Drivers	Network Access Network Interface 1
PHYSICAL 1	Media interface Transmition method Signal strength Topology	1	Hubs Network Cards	

Question: 5

Which protocol uses a connection-oriented service to deliver files between end systems?

A. TFTP
B. DNS
C. FTP
D. SNMP
E. RIP

Answer: C

Explanation:
TCP is an example of a connection-oriented protocol. It requires a logical connection to be established between the two processes before data is exchanged. The connection must be maintained during the entire time that communication is taking place, then released afterwards. The process is much like a telephone call, where a virtual circuit is established--the caller must know the person's telephone number and the phone must be answered--before the message can be delivered.
TCP/IP is also a connection-oriented transport with orderly release. With orderly release, any data remaining in the buffer is sent before the connection is terminated. The release is accomplished in a three-way handshake between client and server processes. The connection-oriented protocols in the OSI protocol suite, on the other hand, do not support orderly release. Applications perform any
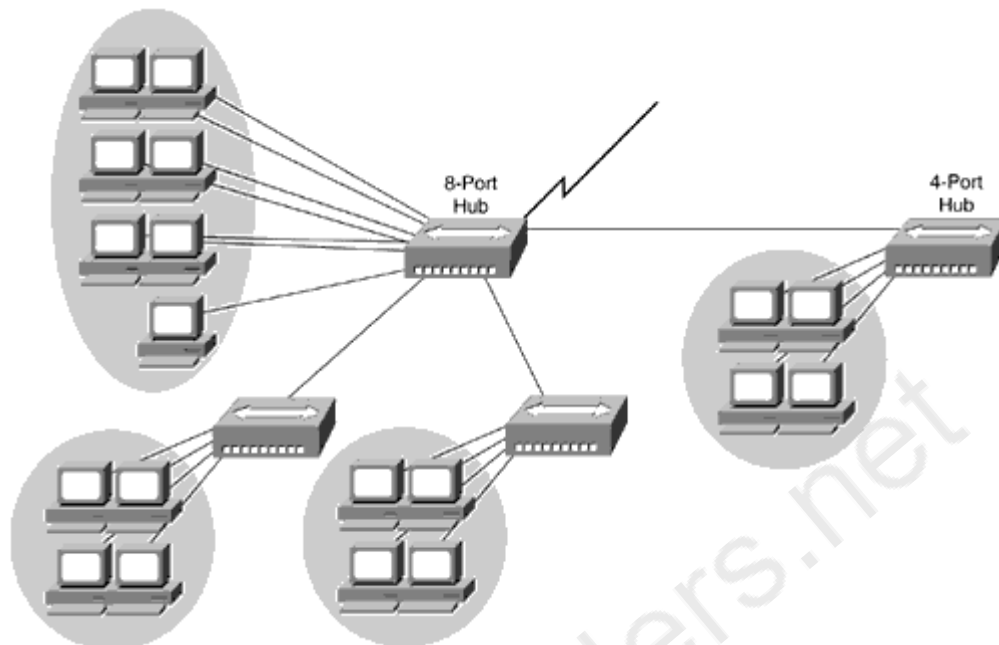
handshake necessary for ensuring orderly release.
Examples of services that use connection-oriented transport services are telnet, rlogin, and ftp.

Question: 6

Refer to the exhibit.

If the hubs in the graphic were replaced by switches, what would be virtually eliminated?

A. broadcast domains
B. repeater domains
C. Ethernet collisions
D. signal amplification
E. Ethernet broadcasts

Answer: C

Explanation:
Modern wired networks use a network switch to eliminate collisions. By connecting each device directly to a port on the switch, either each port on a switch becomes its own collision domain (in the case of half duplex links) or the possibility of collisions is eliminated entirely in the case of full duplex links.

Question: 7

Refer to the exhibit.
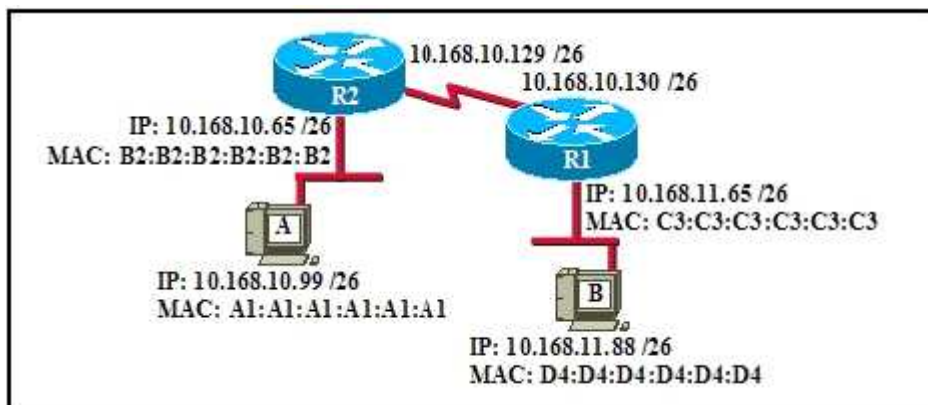
If host A sends an IP packet to host B, what will the source physical address be in the frame when it reaches host B?

A. 10.168.10.99
B. 10.168.11.88
C. A1:A1:A1:A1:A1:A1
D. B2:B2:B2:B2:B2:B2
E. C3:C3:C3:C3:C3:C3
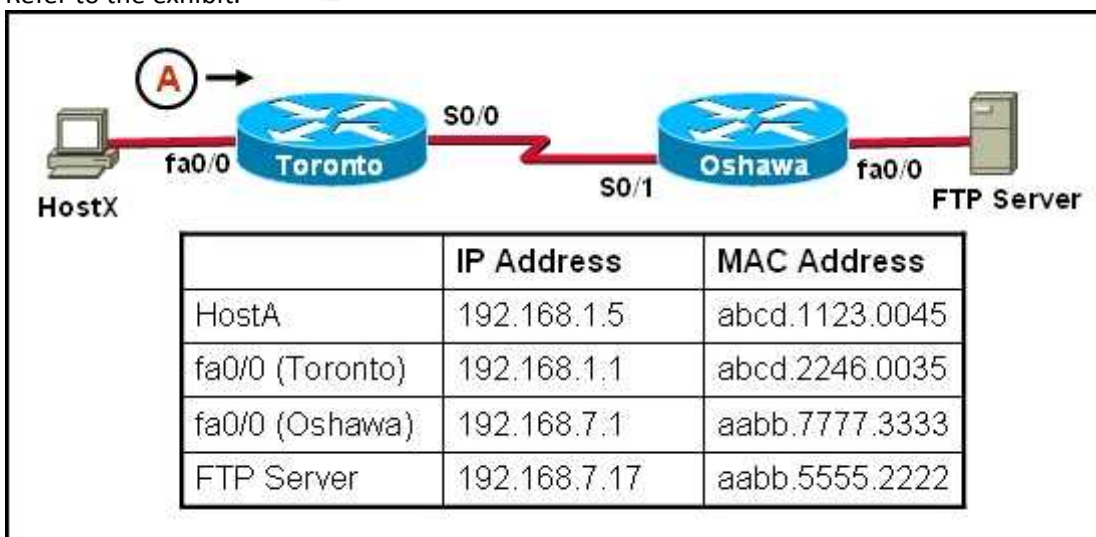F. D4:D4:D4:D4:D4:D4

Answer: E

Explanation:
When packets transfer from one host to another across a routed segment, the source IP address always remains the same source IP address, and the source physical (MAC) address will be the existing router's interface address. Similarly, the destination IP address always remains the same and the destination physical (MAC) address is the destination router's interface address.

Question: 8

Refer to the exhibit.

	IP Address	MAC Address
HostA	192.168.1.5	abcd.1123.0045
fa0/0 (Toronto)	192.168.1.1	abcd.2246.0035
fa0/0 (Oshawa)	192.168.7.1	aabb.7777.3333
FTP Server	192.168.7.17	aabb.5555.2222

HostX is transferring a file to the FTP server. Point A represents the frame as it goes toward the Toronto router. What will the Layer 2 destination address be at this point?

A. abcd.1123.0045
B. 192.168.7.17
C. aabb.5555.2222
D. 192.168.1.1
E. abcd.2246.0035

Answer: E

Explanation:
For packets destined to a host on another IP network, the destination MAC address will be the LAN interface of the router. Since the FTP server lies on a different network, the host will know to send the frame to its default gateway, which is Toronto.

Question: 9

Which network device functions only at Layer 1 of the OSI model?

A)
bridge

B)
hub

C)
NIC

D)
router

E)
switch

A. Option A

B. Option B
C. Option C
D. Option D
E. Option E

Answer: B

Explanation:
Most hubs are amplifying the electrical signal; therefore, they are really repeaters with several ports. Hubs and repeaters are Layer 1 (physical layer) devices.

Question: 10

Refer to the exhibit.
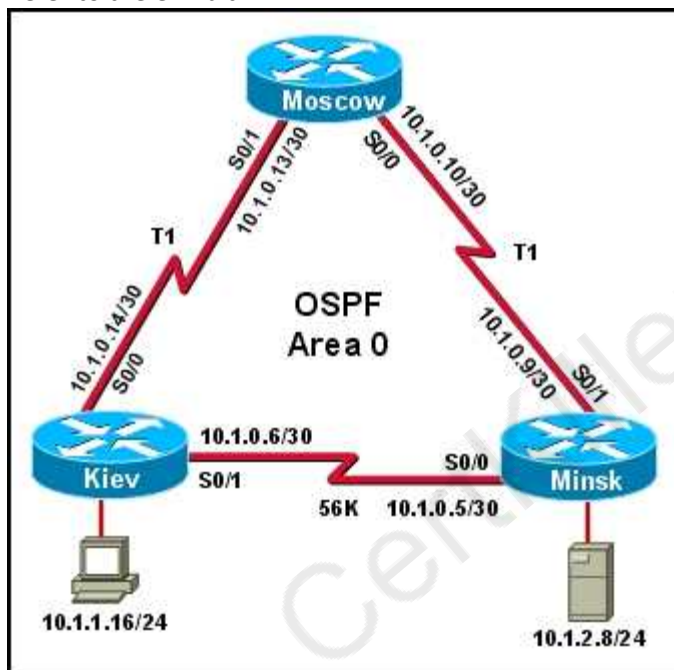
The host in Kiev sends a request for an HTML document to the server in Minsk. What will be the source IP address of the packet as it leaves the Kiev router?

A. 10.1.0.1
B. 10.1.0.5
C. 10.1.0.6
D. 10.1.0.14
E. 10.1.1.16
F. 10.1.2.8

Answer: E

Explanation:
Although the source and destination MAC address will change as a packet traverses a network, the source and destination IP address will not unless network address translation (NAT) is being done,
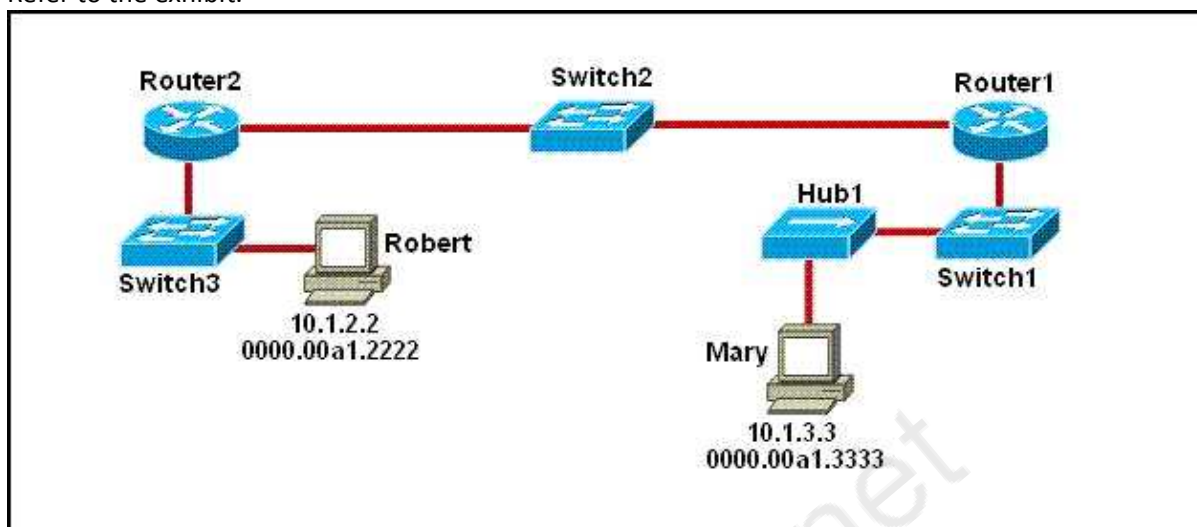
which is not the case here.

Question: 11

Refer to the exhibit.

As packets travel from Mary to Robert, which three devices will use the destination MAC address of the packet to determine a forwarding path? (Choose three.)

A. Hub1
B. Switch1
C. Router1
D. Switch2
E. Router2
F. Switch3

Answer: B, D, F

Explanation:
Switches use the destination MAC address information for forwarding traffic, while routers use the destination IP address information.
Local Area Networks employ Layer 2 Switches and Bridges to forward and filter network traffic. Switches and Bridges operate at the Data Link Layer of the Open System Interconnect Model (OSI). Since Switches and Bridges operate at the Layer 2 they operate more intelligently than hubs, which work at Layer 1 (Physical Layer) of the OSI. Because the switches and bridges are able to listen to the traffic on the wire to examine the source and destination MAC address. Being able to listen to the traffic also allows the switches and bridges to compile a MAC address table to better filter and forward network traffic.
To accomplish the above functions switches and bridges carry out the following tasks:
MAC address learning by a switch or a bridge is accomplished by the same method. The switch or bridge listens to each device connected to each of its ports and scan the incoming frame for the source MAC address. This creates a MAC address to port map that is cataloged in the switches/bridge MAC database. Another name for the MAC address table is content addressable memory or CAM table.

When a switch or bridge is listening to the network traffic, it receives each frame and compares it to the MAC address table. By checking the MAC table the switch/ bridge are able o determine which port the frame came in on. If the frame is on the MAC table the frame is filtered or transmitted on only that port. If the switch determines that the frame is not on the MAC table, the frame is forwarded out to all ports except the incoming port.

Question: 12

Refer to the exhibit.
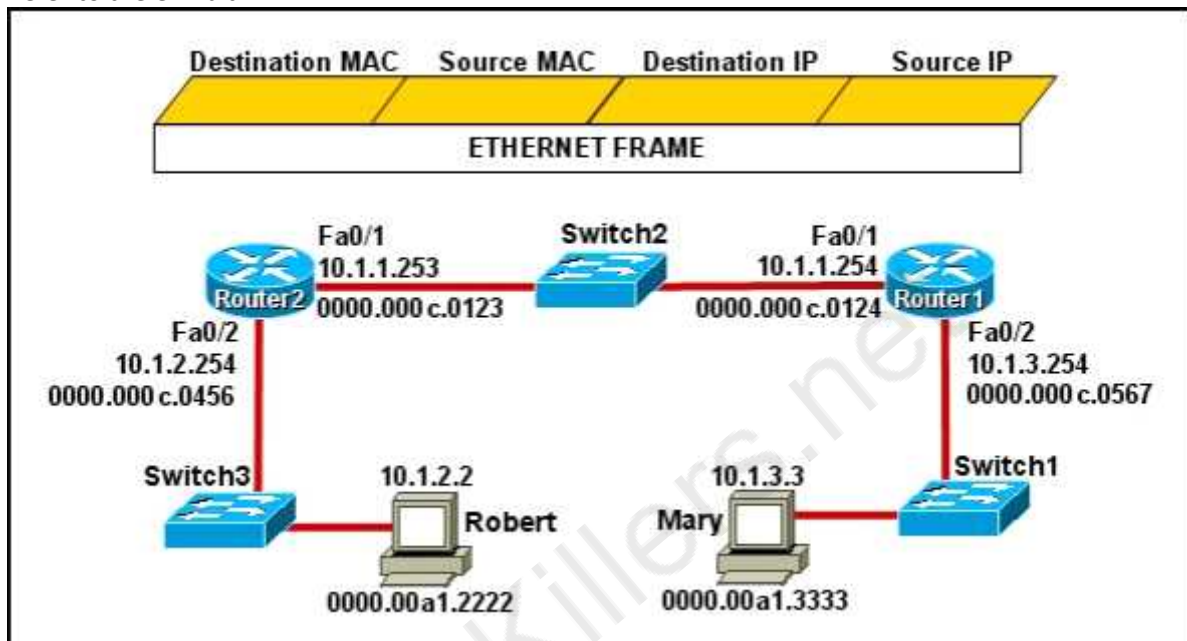
Mary is sending an instant message to Robert. The message will be broken into a series of packets that will traverse all network devices. What addresses will populate these packets as they are forwarded from Router1 to Router2?

A. Option A
B. Option B
C. Option C
D. Option D
E. Option E

Answer: B

Explanation:
The Source and Destination IP address is not going to change. Host 1 IP address will stay as being the source IP and the Host 2 IP address will stay the destination IP address. Those two are not going to change.

For the MAC address it is going to change each time it goes from one hope to another. (Except switches... they don't change anything)

Frame leaving HOST 1 is going to have a source MAC of Host 1 and a destination MAC of Router 1.

Router 1 is going to strip that info off and then will make the source MAC address of Router1's exiting interface, and making Router2's interface as the destination MAC address.
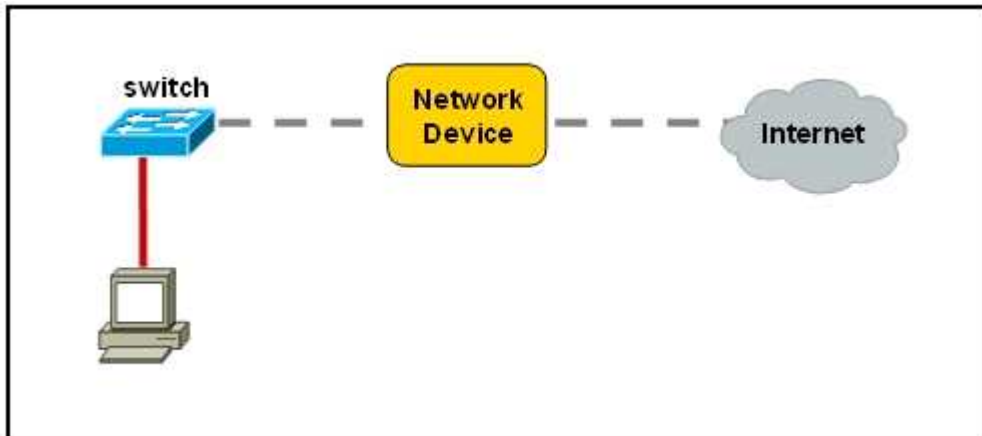
Then the same will happen... Router2 is going to change the source/destination info to the source MAC being the Router2 interface that it is going out, and the destination will be Host2's MAC address.

Question: 13

Refer to the exhibit.

A network device needs to be installed in the place of the icon labeled Network Device to accommodate a leased line attachment to the Internet. Which network device and interface configuration meets the minimum requirements for this installation?

A. a router with two Ethernet interfaces
B. a switch with two Ethernet interfaces
C. a router with one Ethernet and one serial interface
D. a switch with one Ethernet and one serial interface
E. a router with one Ethernet and one modem interface

Answer: C

Explanation:
Only a router can terminate a leased line attachment access circuit, and only a router can connect two different IP networks. Here, we will need a router with two interfaces, one serial connection for the line attachment and one Ethernet interface to connect to the switch on the LAN.

Question: 14

Which transport layer protocol provides best-effort delivery service with no acknowledgment receipt required?

A. HTTP
B. IP
C. TCP
D. Telnet
E. UDP

Answer: E

Explanation:

UDP provides a connectionless datagram service that offers best-effort delivery, which means that UDP does not guarantee delivery or verify sequencing for any datagrams. A source host that needs reliable communication must use either TCP or a program that provides its own sequencing and acknowledgment services.

Question: 15

Which layer of the OSI model controls the reliability of communications between network devices using flow control, sequencing and acknowledgments?

A. Physical
B. Data-link
C. Transport
D. Network

Answer: C

Explanation:

Layer	Function	Examples
Application (Layer 7)	User interface	Telnet, HTTP
Presentation (Layer 6)	Handles encryption & changes to syntax	ASCII/EBCDIC, JPEG/MP3
Session (Layer 5)	Manages multiple applications and maintains synchronisation points	Operating systems, scheduling
Transport (Layer 4)	Provides reliable or best-effort delivery and (optional) error and flow control	TCP, UDP
Network (Layer 3)	Provides logical end-to-end addressing used by routers and hosts	IP
Data Link (Layer 2)	Creates frames from data bits, uses MAC addresses to access endpoints, and provides error detection but no correction	802.3, 802.2, HDLC, Frame Relay
Physical (Layer 1)	Specifies voltage, wire speed, and cable pin-outs	EIA/TIA, V.35

Question: 16

Which statements are true regarding ICMP packets? (Choose two.)

A. They acknowledge receipt of TCP segments.
B. They guarantee datagram delivery.
C. TRACERT uses ICMP packets.
D. They are encapsulated within IP datagrams.
E. They are encapsulated within UDP datagrams.

https://www.certkillers.net

Answer: C, D

Explanation:
Ping may be used to find out whether the local machines are connected to the network or whether a remote site is reachable. This tool is a common network tool for determining the network connectivity, which uses ICMP protocol instead of TCP/IP and UDP/IP. This protocol is usually associated with the network management tools, which provide network information to network administrators, such as ping and traceroute (the later also uses the UDP/IP protocol).
ICMP is quite different from the TCP/IP and UDP/IP protocols. No source and destination ports are included in its packets. Therefore, usual packet-filtering rules for TCP/IP and UDP/IP are not applicable. Fortunately, a special "signature" known as the packet's Message type is included for denoting the purposes of the ICMP packet. Most commonly used message types are namely, 0, 3, 4, 5, 8, 11, and 12 which represent echo reply, destination unreachable, source quench, redirect, echo request, time exceeded, and parameter problem respectively.
In the ping service, after receiving the ICMP "echo request" packet from the source location, the destination

Question: 17

Which statements accurately describe CDP? (Choose three.)

A. CDP is an IEEE standard protocol.
B. CDP is a Cisco proprietary protocol.
C. CDP is a datalink layer protocol.
D. CDP is a network layer protocol.
E. CDP can discover directly connected neighboring Cisco devices.
F. CDP can discover Cisco devices that are not directly connected.

Answer: B, C, E

Explanation:
CDP (Cisco Discovery Protocol) is a proprietary protocol designed by Cisco to help administrators collect information about both locally attached and remote devices. By using CDP, you can gather hardware and protocol information about neighbor devices containing useful info for troubleshooting and documenting the network.

Question: 18

How does a switch differ from a hub?

A. A switch does not induce any latency into the frame transfer time.
B. A switch tracks MAC addresses of directly-connected devices.
C. A switch operates at a lower, more efficient layer of the OSI model.
D. A switch decreases the number of broadcast domains.
E. A switch decreases the number of collision domains.

	Answer: B

Explanation:

Some of the features and functions of a switch include:

A switch is essentially a fast, multi-port bridge, which can contain dozens of ports.

Rather than creating two collision domains, each port creates its own collision domain.

In a network of twenty nodes, twenty collision domains exist if each node is plugged into its own switch port.

If an uplink port is included, one switch creates twenty-one single-node collision domains.

A switch dynamically builds and maintains a Content-Addressable Memory (CAM) table, holding all of the necessary MAC information for each port.

For a detailed description of how switches operate, and their key differences to hubs, see the reference link below.

Reference: http://www.cisco.com/warp/public/473/lan-switch-cisco.shtml

Question: 19

What must occur before a workstation can exchange HTTP packets with a web server?

A. A UDP connection must be established between the workstation and its default gateway.
B. A UDP connection must be established between the workstation and the web server.
C. A TCP connection must be established between the workstation and its default gateway.
D. A TCP connection must be established between the workstation and the web server.
E. An ICMP connection must be established between the workstation and its default gateway.
F. An ICMP connection must be established between the workstation and the web server.

	Answer: D

Explanation:

HTTP uses TCP port 80, and a TCP port 80 connection must be established for HTTP communication to occur.

http://pentestlab.wordpress.com/2012/03/05/common-tcpiHYPERLINK
"http://pentestlab.wordpress.com/2012/03/05/common-tcpip-ports/#_blank"p-ports/

Question: 20

How does TCP differ from UDP? (Choose two.)

A. TCP provides best effort delivery.
B. TCP provides synchronized communication.
C. TCP segments are essentially datagrams.
D. TCP provides sequence numbering of packets.
E. TCP uses broadcast delivery.

	Answer: B, D

Explanation:

Because TCP is a connection-oriented protocol responsible for ensuring the transfer of a datagram from the source to destination machine (end-to-end communications), TCP must receive communications messages from the destination machine to acknowledge receipt of the datagram. The term virtual circuit is usually used to refer to the handshaking that goes on between the two end machines, most of which are simple acknowledgment messages (either confirmation of receipt or a failure code) and datagram sequence numbers.

Rather than impose a state within the network to support the connection, TCP uses synchronized state between the two endpoints. This synchronized state is set up as part of an initial connection process, so TCP can be regarded as a connection-oriented protocol. Much of the protocol design is intended to ensure that each local state transition is communicated to, and acknowledged by, the remote party.

Reference: http://en.wikibooks.org/wiki/Communication_Networks/TCP_and_UDP_Protocols

Question: 21

A workstation has just resolved a browser URL to the IP address of a server. What protocol will the workstation now use to determine the destination MAC address to be placed into frames directed toward the server?

A. HTTP
B. DNS
C. DHCP
D. RARP
E. ARP

Answer: E

Explanation:
The RARP protocol is used to translate hardware interface addresses to protocol addresses. The RARP message format is very similar to the ARP format. When the booting computer sends the broadcast ARP request, it places its own hardware address in both the sending and receiving fields in the encapsulated ARP data packet. The RARP server will fill in the correct sending and receiving IP addresses in its response to the message. This way the booting computer will know its IP address when it gets the message from the RARP server

Question: 22

Refer to the exhibit.

https://www.certkillers.net
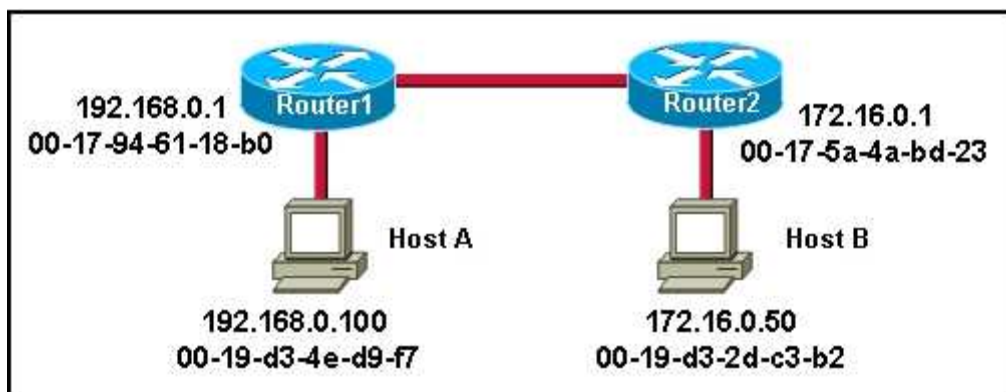
Host A is sending a packet to Host B for the first time. What destination MAC address will Host A use in the ARP request?

A. 192.168.0.1
B. 172.16.0.50
C. 00-17-94-61-18-b0
D. 00-19-d3-2d-c3-b2
E. ff-ff-ff-ff-ff-ff
F. 255.255.255.255

Answer: E

Explanation:
For the initial communication, Host A will send a broadcast ARP (all F's) to determine the correct address to use to reach the destination.
ARP sends an Ethernet frame called an ARP request to every host on the shared link-layer legmen. The Ethernet header includes the source host MAC address and a destination address of all Fs representing a broadcast frame. The ARP request contains the sender's MAC and IP address and the target (destination) IP address. The target's MAC address is set to all 0s.
ARP Request
Reference:
http://www.technicalhowto.com/protocols/arp/arp

Question: 23

What are two common TCP applications? (Choose two.)

A. TFTP
B. SMTP
C. SNMP
D. FTP
E. DNS

Answer: B, D

Explanation:

SMTP uses TCP port 25, while FTP uses TCP ports 20 and 21.
Reference: http://pentestlab.wordpress.com/2012/03/05/common-tcpip-ports/

Question: 24

Refer to the exhibit.

```
SwitchA# show mac-address-table
< non-essential output omitted >
    Destination Address  Address Type  VLAN  Destination Port

    -------------------  ------------  ----  ------------------
    00b0.d056.fe4d       Dynamic        1    FastEthernet0/3
    00b0.d043.ac2e       Dynamic        1    FastEthernet0/4
    00b0.d0fe.ac32       Dynamic        1    FastEthernet0/5
    00b0.d0da.cb56       Dynamic        1    FastEthernet0/6

Frame received by SwitchA:
```

Source MAC	Destination MAC	Source IP	Destination IP
00b0.d056.fe4d	00b0.d0da.cb56	192.168.40.5	192.168.40.6

SwitchA receives the frame with the addressing shown. According to the command output also shown in the exhibit, how will SwitchA handle this frame?

A. It will drop the frame.
B. It will forward the frame out port Fa0/6 only.
C. It will flood the frame out all ports.
D. It will flood the frame out all ports except Fa0/3.

Answer: B

Explanation:
Switches keep the learned MAC addresses in a table, so that when a frame comes in with a destination MAC address that the switch has already learned, it will forward it to that port only. If a frame comes in with a destination MAC that is not already in the MAC address table, then the frame will be flooded to all ports except for the one that it came in on. In this case, Switch A already knows that 00b0.d0da.cb56 resides on port fa0/6, so it will forward the from out that port.

Question: 25

Refer to the exhibit.

```
SwitchA# show mac-address-table
< non-essential output omitted >
        Destination Address  Address Type  VLAN  Destination Port

        -------------------  ------------  ----  --------------------
        00b0.d056.fe4d       Dynamic        1    FastEthernet0/3
        00b0.d043.ac2e       Dynamic        1    FastEthernet0/4
        00b0.d0fe.ac32       Dynamic        1    FastEthernet0/5
        00b0.d0da.cb56       Dynamic        1    FastEthernet0/6

Frame received by SwitchA:
```

Source MAC	Destination MAC	Source IP	Destination IP
00b0.d056.fe4d	00b0.d0da.895a	192.168.40.5	192.168.40.6

SwitchA receives the frame with the addressing shown in the exhibit. According to the command output also shown in the exhibit, how will SwitchA handle this frame?

A. It will drop the frame.
B. It will forward the frame out port Fa0/6 only.
C. It will forward the frame out port Fa0/3 only.
D. It will flood the frame out all ports.
E. It will flood the frame out all ports except Fa0/3.

Answer: E

Explanation:
When frame receives the frame, it checks the source address on MAC table if MAC address found in MAC table it tries to forward if not in MAC table adds the Address on MAC table. After checking the source address, it checks the destination address on MAC table, if MAC address found on MAC table it forwards to proper ports otherwise floods on all ports except the source port.

Question: 26

Refer to the exhibit.
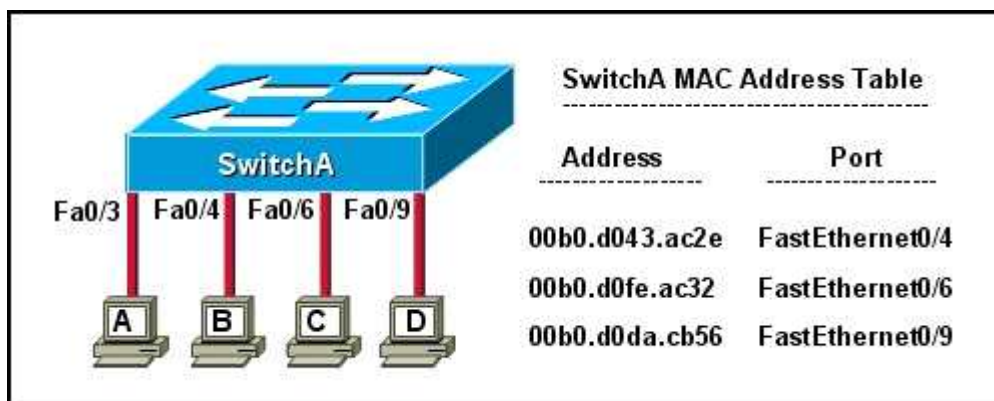
The exhibit is showing the topology and the MAC address table. Host A sends a data frame to host D. What will the switch do when it receives the frame from host A?

A. The switch will add the source address and port to the MAC address table and forward the frame to host D.
B. The switch will discard the frame and send an error message back to host A.
C. The switch will flood the frame out of all ports except for port Fa0/3.
D. The switch will add the destination address of the frame to the MAC address table and forward the frame to host D.

Answer: A

Explanation:
When switch receives the data frame from the host not having the MAC address already on the MAC table, it will add the MAC address to source port on MAC address table and sends the data frame.

Question: 27

Which two statements describe the operation of the CSMA/CD access method? (Choose two.)

A. In a CSMA/CD collision domain, multiple stations can successfully transmit data simultaneously.
B. In a CSMA/CD collision domain, stations must wait until the media is not in use before transmitting.
C. The use of hubs to enlarge the size of collision domains is one way to improve the operation of the CSMA/CD access method.
D. After a collision, the station that detected the collision has first priority to resend the lost data.
E. After a collision, all stations run a random backoff algorithm. When the backoff delay period has expired, all stations have equal priority to transmit data.
F. After a collision, all stations involved run an identical backoff algorithm and then synchronize with each other prior to transmitting data.

Answer: B, E

Explanation:
Ethernet networking uses Carrier Sense Multiple Access with Collision Detect (CSMA/CD), a protocol that helps devices share the bandwidth evenly without having two devices transmit at the same time

on the network medium. CSMA/CD was created to overcome the problem of those collisions that occur when packets are transmitted simultaneously from different nodes. And trust me, good collision management is crucial, because when a node transmits in a CSMA/CD network, all the other nodes on the network receive and examine that transmission. Only bridges and routers can effectively prevent a transmission from propagating throughout the entire network! So, how does the CSMA/CD protocol work? Like this: when a host wants to transmit over the network, it first checks for the presence of a digital signal on the wire. If all is clear (no other host is transmitting), the host will then proceed with its transmission. But it doesn't stop there. The transmitting host constantly monitors the wire to make sure no other hosts begin transmitting. If the host detects another signal on the wire, it sends out an extended jam signal that causes all nodes on the segment to stop sending data (think, busy signal). The nodes respond to that jam signal by waiting a while before attempting to transmit again. Backoff algorithms determine when the colliding stations can retransmit. If collisions keep occurring after 15 tries, the nodes attempting to transmit will then time out.

Question: 28

Refer to the exhibit.
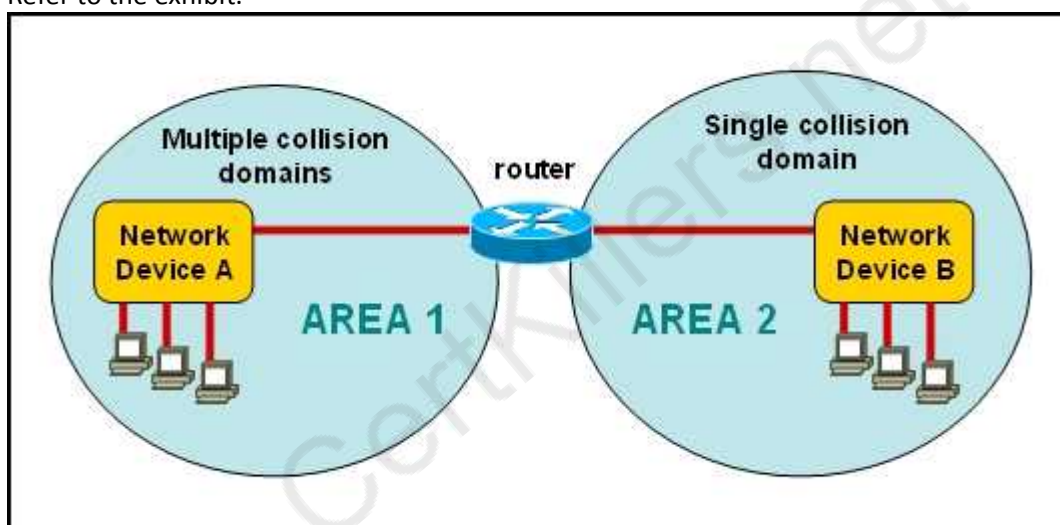
A network has been planned as shown. Which three statements accurately describe the areas and devices in the network plan? (Choose three.)

A. Network Device A is a switch.
B. Network Device B is a switch.
C. Network Device A is a hub.
D. Network Device B is a hub.
E. Area 1 contains a Layer 2 device.
F. Area 2 contains a Layer 2 device.

Answer: A, D, E

Explanation:
Switches use a separate collision domain for each port, so device A must be a switch. Hubs, however, place all ports in the same collision domain so device B is a hub. Switches reside in layer 2 while hubs

are layer 1 devices.

Question: 29

On a Cisco switch, which protocol determines if an attached VoIP phone is from Cisco or from another vendor?

A. RTP
B. TCP
C. CDP
D. UDP

Answer: C

Explanation:
The Cisco Unified IP Phone uses CDP to communicate information such as auxiliary VLAN ID, per port power management details, and Quality of Service (QoS) configuration information with the Cisco Catalyst switch.
Cisco Discovery Protocol (CDP) is a proprietary protocol designed by Cisco to help administrators collect information about both locally attached and remote devices. By using CDP, you can gather hardware and protocol information about neighbor devices, which is useful info for troubleshooting the network.
CDP messages are generated every 60 seconds as multicast messages on each of its active interfaces.
The information shared in a CDP packet about a Cisco device includes the following:
Name of the device configured with the hostname command
IOS software version
Hardware capabilities, such as routing, switching, and/or bridging
Hardware platform, such as 2600, 2950, or 1900
The layer-3 address(es) of the device
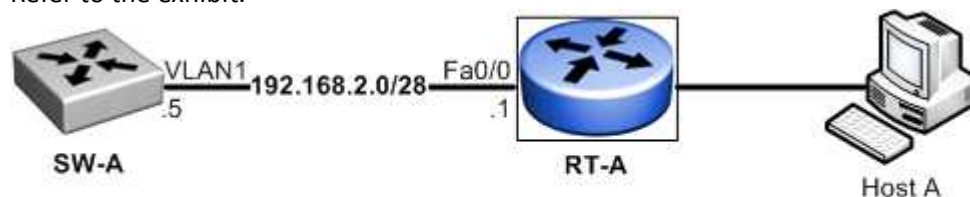The interface the CDP update was generated on
Reference: http://computernetworkingnotes.com/cisco-devices-administration-and-configuration/cisco-discoHYPERLINK "http://computernetworkingnotes.com/cisco-devices-administration-and-configuration/cisco-discoveryprotocol#_blank"veryprotocol

Question: 30

Refer to the exhibit.

What must be configured to establish a successful connection from Host A to switch SW-A through router RT-A?

A. VLAN 1 on RT-A
B. IP routing on SW-A
C. default gateway on SW-A
D. crossover cable connecting SW-A and RT-A

Answer: C

Explanation:
In order for the switch to reach networks that are not local, such as networks attached to different interfaces of the router, it will need to set its default gateway to be the IP address of the attached router.

Thank You for trying 100-105 PDF Demo

To Buy Latest 100-105 Full Version Download visit link below

https://www.certkillers.net/Exam/100-105

Start Your 100-105 Preparation

[Limited Time Offer] Use Coupon "CKNET" for Further discount on your purchase. Test your 100-105 preparation with actual exam questions.

https://www.certkillers.net