400-101.examcollection.premium.exam.936q

Number: 400-101
Passing Score: 800
Time Limit: 120 min
File Version: 22.0

400-101

CCIE Routing and Switching (v5.0)

Version 22.0

Sections

1. Network Principles
2. Layer 2 Technologies
3. Layer 3 Technologies
4. VPN Technologies
5. Infrastructure Security
6. Infrastructure Services
7. Mix Questions

Exam A

QUESTION 1
Which two options are causes of out-of-order packets? (Choose two.)

A. a routing loop
B. a router in the packet flow path that is intermittently dropping packets
C. high latency
D. packets in a flow traversing multiple paths through the network
E. some packets in a flow being process-switched and others being interrupt-switched on a transit router

Correct Answer: DE
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
In traditional packet forwarding systems, using different paths have varying latencies that cause out of order packets, eventually resulting in far lower performance for the network application. Also, if some packets are process switched quickly by the routing engine of the router while others are interrupt switched (which takes more time) then it could result in out of order packets. The other options would cause packet drops or latency, but not out of order packets.

QUESTION 2
A TCP/IP host is able to transmit small amounts of data (typically less than 1500 bytes), but attempts to transmit larger amounts of data hang and then time out. What is the cause of this problem?

A. A link is flapping between two intermediate devices.
B. The processor of an intermediate router is averaging 90 percent utilization.
C. A port on the switch that is connected to the TCP/IP host is duplicating traffic and sending it to a port that has a sniffer attached.
D. There is a PMTUD failure in the network path.

Correct Answer: D
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
Sometimes, over some IP paths, a TCP/IP node can send small amounts of data (typically less than 1500 bytes) with no difficulty, but transmission attempts with larger amounts of data hang, then time out. Often this is observed as a unidirectional problem in that large data transfers succeed in one direction but fail in the other direction. This problem is likely caused by the TCP MSS value, PMTUD failure, different LAN media types, or defective links.

Reference: http://www.cisco.com/c/en/us/support/docs/additional-legacy-protocols/ms-windows-networking/13709-38.html

QUESTION 3
Refer to the exhibit.

```
Internet Protocol Version 4, Src: 10.149.4.110 (10.149.4.110), Dst: 192.168.3.1 (192.168.3.1)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 60
    Identification: 0x64ac (25772)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x8269 [correct]
    Source: 10.149.4.110 (10.149.4.110)
    Destination: 192.168.3.1 (192.168.3.1)
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d3d [correct]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 30 (0x001e)
    Sequence number (LE): 7680 (0x1e00)
    Data (32 bytes)

0000  61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70   abcdefghijklmnop
0010  71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69   qrstuvwabcdefghi
        Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
        [Length: 32]
```

ICMP Echo requests from host A are not reaching the intended destination on host B. What is the problem?

A. The ICMP payload is malformed.
B. The ICMP Identifier (BE) is invalid.
C. The negotiation of the connection failed.

D. The packet is dropped at the next hop.
E. The link is congested.

Correct Answer: D
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
Here we see that the Time to Live (TTL) value of the packet is one, so it will be forwarded to the next hop router, but then dropped because the TTL value will be 0 at the next hop.

QUESTION 4
Refer to the exhibit.

```
R101#show ip cache flow
[...]
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         10.0.0.1        Et0/0         15.0.0.2        01 0000 0800  2603
```

Which statement is true?

A. It is impossible for the destination interface to equal the source interface.
B. NAT on a stick is performed on interface Et0/0.
C. There is a potential routing loop.
D. This output represents a UDP flow or a TCP flow.

Correct Answer: C
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
In this example we see that the source interface and destination interface are the same (Et0/0). Typically this is seen when there is a routing loop for the destination IP address.

QUESTION 5
Which three conditions can cause excessive unicast flooding? (Choose three.)

A. Asymmetric routing

B. Repeated TCNs
C. The use of HSRP
D. Frames sent to FFFF.FFFF.FFFF
E. MAC forwarding table overflow
F. The use of Unicast Reverse Path Forwarding

Correct Answer: ABE
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
Causes of Flooding
The very cause of flooding is that destination MAC address of the packet is not in the L2 forwarding table of the switch. In this case the packet will be flooded out of all forwarding ports in its VLAN (except the port it was received on). Below case studies display most common reasons for destination MAC address not being known to the switch.
Cause 1: Asymmetric Routing
Large amounts of flooded traffic might saturate low-bandwidth links causing network performance issues or complete connectivity outage to devices connected across such low-bandwidth links.
Cause 2: Spanning-Tree Protocol Topology Changes
Another common issue caused by flooding is Spanning-Tree Protocol (STP) Topology Change Notification (TCN). TCN is designed to correct forwarding tables after the forwarding topology has changed. This is necessary to avoid a connectivity outage, as after a topology change some destinations previously accessible via particular ports might become accessible via different ports. TCN operates by shortening the forwarding table aging time, such that if the address is not relearned, it will age out and flooding will occur.
TCNs are triggered by a port that is transitioning to or from the forwarding state. After the TCN, even if the particular destination MAC address has aged out, flooding should not happen for long in most cases since the address will be relearned. The issue might arise when TCNs are occurring repeatedly with short intervals. The switches will constantly be fast-aging their forwarding tables so flooding will be nearly constant.
Normally, a TCN is rare in a well-configured network. When the port on a switch goes up or down, there is eventually a TCN once the STP state of the port is changing to or from forwarding. When the port is flapping, repetitive TCNs and flooding occurs.
Cause 3: Forwarding Table Overflow
Another possible cause of flooding can be overflow of the switch forwarding table. In this case, new addresses cannot be learned and packets destined to such addresses are flooded until some space becomes available in the forwarding table. New addresses will then be learned. This is possible but rare, since most modern switches have large enough forwarding tables to accommodate MAC addresses for most designs.
Forwarding table exhaustion can also be caused by an attack on the network where one host starts generating frames each sourced with different MAC address. This will tie up all the forwarding table resources. Once the forwarding tables become saturated, other traffic will be flooded because new learning cannot occur. This kind of attack can be detected by examining the switch forwarding table. Most of the MAC addresses will point to the same port or group of ports. Such attacks can be prevented by limiting the number of MAC addresses learned on untrusted ports by using the port security feature.

Reference: http://www.cisco.com/c/en/us/support/docs/switches/catalyst-6000-series-switches/23563-143.html#causes

QUESTION 6

Which congestion-avoidance or congestion-management technique can cause global synchronization?

A. Tail drop
B. Random early detection
C. Weighted random early detection
D. Weighted fair queuing

Correct Answer: A
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
Tail Drop
Tail drop treats all traffic equally and does not differentiate between classes of service. Queues fill during periods of congestion. When the output queue is full and tail drop is in effect, packets are dropped until the congestion is eliminated and the queue is no longer full.
Weighted Random Early Detection
WRED avoids the globalization problems that occur when tail drop is used as the congestion avoidance mechanism on the router. Global synchronization occurs as waves of congestion crest only to be followed by troughs during which the transmission link is not fully utilized. Global synchronization of TCP hosts, for example, can occur because packets are dropped all at once. Global synchronization manifests when multiple TCP hosts reduce their transmission rates in response to packet dropping, then increase their transmission rates once again when the congestion is reduced.

Reference: http://www.cisco.com/c/en/us/td/docs/ios/12_2/qos/configuration/guide/fqos_c/qcfconav.html#wp1002048

QUESTION 7
Which two options are reasons for TCP starvation? (Choose two.)

A. The use of tail drop
B. The use of WRED
C. Mixing TCP and UDP traffic in the same traffic class
D. The use of TCP congestion control

Correct Answer: CD
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
It is a general best practice to not mix TCP-based traffic with UDP-based traffic (especially Streaming-Video) within a single service-provider class because of the behaviors of these protocols during periods of congestion. Specifically, TCP transmitters throttle back flows when drops are detected. Although some UDP applications have application-level windowing, flow control, and retransmission capabilities, most UDP transmitters are completely

oblivious to drops and, thus, never lower transmission rates because of dropping.
When TCP flows are combined with UDP flows within a single service-provider class and the class experiences congestion, TCP flows continually lower their transmission rates, potentially giving up their bandwidth to UDP flows that are oblivious to drops. This effect is called TCP starvation/UDP dominance.
TCP starvation/UDP dominance likely occurs if (TCP-based) Mission-Critical Data is assigned to the same service-provider class as (UDP-based) Streaming-Video and the class experiences sustained congestion. Even if WRED or other TCP congestion control mechanisms are enabled on the service-provider class, the same behavior would be observed because WRED (for the most part) manages congestion only on TCP-based flows.

Reference: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book/VPNQoS.html

QUESTION 8
Refer to the exhibit.

```
%C4K_L3HWFORWARDING-2-FWDCAMFULL: L3 routing table is full. Switching to software forwarding
```

While troubleshooting high CPU utilization of a Cisco Catalyst 4500 Series Switch, you notice the error message that is shown in the exhibit in the log file.

What can be the cause of this issue, and how can it be prevented?

A. The hardware routing table is full. Redistribute from BGP into IGP.
B. The software routing table is full. Redistribute from BGP into IGP.
C. The hardware routing table is full. Reduce the number of routes in the routing table.
D. The software routing table is full. Reduce the number of routes in the routing table.

Correct Answer: C
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
L3HWFORWADING-2
Error MessageC4K_L3HWFORWARDING-2-FWDCAMFULL:L3 routing table is full. Switching to software forwarding.

Explanation: The hardware routing table is full; forwarding takes place in the software instead. The switch performance might be degraded.
Recommended Action: Reduce the size of the routing table. Enter the **ip cef** command to return to hardware forwarding.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/31sg/system/message/message/emsg.html

QUESTION 9
Refer to the exhibit.

```
#show interface FastEthernet0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is PQII_PRO_UEC, address is 0024.14ac.0d3c (bia 001f.9e3c.a5c2)
  Internet address is 1.1.1.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 100Mbps, media type is RJ45
  output flow-control is XON, input flow-control is XON
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/1000/0/0 (size/max/drops/flushes); Total output drops: 10000
  Queueing strategy: Class-based queueing
  Output queue: 100/1000/10000 (size/max total/drops)
  30 second input rate 361000 bits/sec, 204 packets/sec
  30 second output rate 711000000 bits/sec, 223000 packets/sec
     1221583901 packets input, 3044421428 bytes, 0 no buffer
     Received 91124750 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     1090847722 packets output, 796667418 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

Which two are causes of output queue drops on FastEthernet0/0? (Choose two.)

A. an oversubscribed input service policy on FastEthernet0/0
B. a duplex mismatch on FastEthernet0/0
C. a bad cable connected to FastEthernet0/0
D. an oversubscribed output service policy on FastEthernet0/0

E. The router trying to send more than 100 Mb/s out of FastEthernet0/0

Correct Answer: DE
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
Output drops are caused by a congested interface. For example, the traffic rate on the outgoing interface cannot accept all packets that should be sent out, or a service policy is applied that is oversubscribed. The ultimate solution to resolve the problem is to increase the line speed. However, there are ways to prevent, decrease, or control output drops when you do not want to increase the line speed. You can prevent output drops only if output drops are a consequence of short bursts of data. If output drops are caused by a constant high-rate flow, you cannot prevent the drops. However, you can control them.

Reference: http://www.cisco.com/c/en/us/support/docs/routers/10000-series-routers/6343-queue-drops.html

QUESTION 10
Refer to the exhibit.

```
Router#show ip cache flow
[...]
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Vl1           144.254.10.206  Local         10.48.77.208    06 C363 01BB     2
```

Which statement about the output is true?

A. The flow is an HTTPS connection to the router, which is initiated by 144.254.10.206.
B. The flow is an HTTP connection to the router, which is initiated by 144.254.10.206.
C. The flow is an HTTPS connection that is initiated by the router and that goes to 144.254.10.206.
D. The flow is an HTTP connection that is initiated by the router and that goes to 144.254.10.206.

Correct Answer: A
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
We can see that the connection is initiated by the Source IP address shown as 144.254.10.206. We also see that the destination protocol (DstP) shows 01BB, which is in hex and translates to 443 in decimal. SSL/HTTPS uses port 443.

QUESTION 11
What is the cause of ignores and overruns on an interface, when the overall traffic rate of the interface is low?

A. a hardware failure of the interface
B. a software bug
C. a bad cable
D. microbursts of traffic

Correct Answer: D
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
Micro-bursting is a phenomenon where rapid bursts of data packets are sent in quick succession, leading to periods of full line-rate transmission that can overflow packet buffers of the network stack, both in network endpoints and routers and switches inside the network.
Symptoms of micro bursts will manifest in the form of ignores and/ or overruns (also shown as accumulated in “input error” counter within show interface output). This is indicative of receive ring and corresponding packet buffer being overwhelmed due to data bursts coming in over extremely short period of time (microseconds). You will never see a sustained data traffic within show interface’s “input rate” counter as they are averaging bits per second (bps) over 5 minutes by default (way too long to account for microbursts). You can understand microbursts from a scenario where a 3-lane highway merging into a single lane at rush hour – the capacity burst cannot exceed the total available bandwidth (i.e. single lane), but it can saturate it for a period of time.

Reference: http://ccieordie.com/?tag=micro-burst

QUESTION 12
Refer to the exhibit.

```
San_Jose#show debug
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:10:59.124 PST Thu Aug 22 2013
Condition 1: ip 172.16.129.4 (0 flags triggered)
```

Which statement about the debug behavior of the device is true?

A. The device debugs all IP events for 172.16.129.4.
B. The device sends all debugging information for 172.16.129.4.
C. The device sends only NTP debugging information to 172.16.129.4.

D. The device sends debugging information every five seconds.

Correct Answer: A
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
This is an example of a conditional debug, where there is a single condition specified of IP address 172.16.129.4. So, all IP events for that address will be output in the debug.

QUESTION 13
Which statement about MSS is true?

A. It is negotiated between sender and receiver.
B. It is sent in all TCP packets.
C. It is 20 bytes lower than MTU by default.
D. It is sent in SYN packets.
E. It is 28 bytes lower than MTU by default.

Correct Answer: D
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
The maximum segment size (MSS) is a parameter of the Options field of the TCP header that specifies the largest amount of data, specified in octets, that a computer or communications device can receive in a single TCP segment. It does not count the TCP header or the IP header. The IP datagram containing a TCP segment may be self-contained within a single packet, or it may be reconstructed from several fragmented pieces; either way, the MSS limit applies to the total amount of data contained in the final, reconstructed TCP segment.
The default TCP Maximum Segment Size is 536. Where a host wishes to set the maximum segment size to a value other than the default, the maximum segment size is specified as a TCP option, initially in the TCP SYN packet during the TCP handshake. The value cannot be changed after the connection is established.

Reference: http://en.wikipedia.org/wiki/Maximum_segment_size

QUESTION 14
Which two methods change the IP MTU value for an interface? (Choose two.)

A. Configure the default MTU.
B. Configure the IP system MTU.

C. Configure the interface MTU.
D. Configure the interface IP MTU.

Correct Answer: CD
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
An IOS device configured for IP+MPLS routing uses three different Maximum Transmission Unit (MTU) values: The hardware MTU configured with the mtu interface configuration command

- The IP MTU configured with the ip mtu interface configuration command
- The MPLS MTU configured with the mpls mtu interface configuration command

The hardware MTU specifies the maximum packet length the interface can support … or at least that's the theory behind it. In reality, longer packets can be sent (assuming the hardware interface chipset doesn't complain); therefore you can configure MPLS MTU to be larger than the interface MTU and still have a working network. Oversized packets might not be received correctly if the interface uses fixed-length buffers; platforms with scatter/gather architecture (also called particle buffers) usually survive incoming oversized packets.
IP MTU is used to determine whether am IP packet forwarded through an interface has to be fragmented. It has to be lower or equal to hardware MTU (and this limitation is enforced). If it equals the HW MTU, its value does not appear in the running configuration and it tracks the changes in HW MTU. For example, if you configure ip mtu 1300 on a Serial interface, it will appear in the running configuration as long as the hardware MTU is not equal to 1300 (and will not change as the HW MTU changes). However, as soon as the mtu 1300 is configured, the ip mtu 1300 command disappears from the configuration and the IP MTU yet again tracks the HW MTU.

Reference: http://blog.ipspace.net/2007/10/tale-of-three-mtus.html

QUESTION 15
Which implementation can cause packet loss when the network includes asymmetric routing paths?

A. the use of ECMP routing
B. the use of penultimate hop popping
C. the use of Unicast RPF
D. disabling Cisco Express Forwarding

Correct Answer: C
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
When administrators use Unicast RPF in strict mode, the packet must be received on the interface that the router would use to forward the return packet. Unicast RPF configured in strict mode may drop legitimate traffic that is received on an interface that was not the router's choice for sending

return traffic. Dropping this legitimate traffic could occur when asymmetric routing paths are present in the network.

Reference: http://www.cisco.com/web/about/security/intelligence/unicast-rpf.html

QUESTION 16
Which two mechanisms can be used to eliminate Cisco Express Forwarding polarization? (Choose two.)

A. alternating cost links
B. the unique-ID/universal-ID algorithm
C. Cisco Express Forwarding antipolarization
D. different hashing inputs at each layer of the network

Correct Answer: BD
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
This document describes how Cisco Express Forwarding (CEF) polarization can cause suboptimal use of redundant paths to a destination network. CEF polarization is the effect when a hash algorithm chooses a particular path and the redundant paths remain completely unused.
How to Avoid CEF Polarization
1. Alternate between default (SIP and DIP) and full (SIP + DIP + Layer4 ports) hashing inputs configuration at each layer of the network.
2. Alternate between an even and odd number of ECMP links at each layer of the network.
   The CEF load-balancing does not depend on how the protocol routes are inserted in the routing table. Therefore, the OSPF routes exhibit the same behavior as EIGRP. In a hierarchical network where there are several routers that perform load-sharing in a row, they all use same algorithm to load-share.

The hash algorithm load-balances this way by default:

1: 1
2: 7-8
3: 1-1-1
4: 1-1-1-2
5: 1-1-1-1-1
6: 1-2-2-2-2-2
7: 1-1-1-1-1-1-1
8: 1-1-1-2-2-2-2-2

The number before the colon represents the number of equal-cost paths. The number after the colon represents the proportion of traffic which is forwarded per path.

This means that:

- For two equal cost paths, load-sharing is 46.666%-53.333%, not 50%-50%.
- For three equal cost paths, load-sharing is 33.33%-33.33%-33.33% (as expected).
- For four equal cost paths, load-sharing is 20%-20%-20%-40% and not 25%-25%-25%-25%.

This illustrates that, when there is even number of ECMP links, the traffic is not load-balanced.

1. Cisco IOS introduced a concept called unique-ID/universal-ID which helps avoid CEF polarization. This algorithm, called the universal algorithm (the default in current Cisco IOS versions), adds a 32-bit router-specific value to the hash function (called the universal ID - this is a randomly generated value at the time of the switch boot up that can can be manually controlled). This seeds the hash function on each router with a unique ID, which ensures that the same source/destination pair hash into a different value on different routers along the path. This process provides a better network-wide load-sharing and circumvents the polarization issue. This unique -ID concept does not work for an even number of equal-cost paths due to a hardware limitation, but it works perfectly for an odd number of equal-cost paths. In order to overcome this problem, Cisco IOS adds one link to the hardware adjacency table when there is an even number of equal-cost paths in order to make the system believe that there is an odd number of equal-cost links.

Reference: http://www.cisco.com/c/en/us/support/docs/ip/express-forwarding-cef/116376-technote-cef-00.html

QUESTION 17
Which two mechanisms provide Cisco IOS XE Software with control plane and data plane separation? (Choose two.)

A. Forwarding and Feature Manager
B. Forwarding Engine Driver
C. Forwarding Performance Management
D. Forwarding Information Base

Correct Answer: AB
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
Control Plane and Data Plane Separation
IOS XE introduces an opportunity to enable teams to now build drivers for new Data Plane ASICs outside the IOS instance and have them program to a set of standard APIs which in turn enforces Control Plane and Data Plane processing separation.
IOS XE accomplishes Control Plane / Data Plane separation through the introduction of the Forwarding and Feature Manager (FFM) and its standard interface to the Forwarding Engine Driver (FED). FFM provides a set of APIs to Control Plane processes. In turn, the FFM programs the Data Plane via the FED and maintains forwarding state for the system. The FED is the instantiation of the hardware driver for the Data Plane and is provided by the platform.

Reference: http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-xe-3sg/QA_C67-622903.html

QUESTION 18
Refer to the exhibit.

```
R101#show ip cache verbose flow
[...]
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
Et0/0          10.0.0.1        Et1/0*         14.0.0.2        01 80  10       1
0000 /0  0                     0800 /0  0     0.0.0.0               100     0.0
```

What is the PHB class on this flow?

A. EF
B. none
C. AF21
D. CS4

Correct Answer: D
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
This command shows the TOS value in hex, which is 80 in this case. The following chart shows some common DSCP/PHB Class values:

Service	DSCP value	TOS value	Juniper Alias	TOS hexadecimal	DSCP - TOS Binary
Premium IP	46	184	ef	B8	101110 - 101110xx
LBE	8	32	cs1	20	001000 - 001000xx
DWS	**32**	**128**	**cs4**	**80**	**100000 - 100000xx**
Network control	48	192	cs6	c0	110000 - 110000xx
Network control 2	56	224	cs7	e0	111000 - 111000xx

Reference: http://www.tucny.com/Home/dscp-tos

QUESTION 19
Refer to the exhibit.

```
R101#show ip cache flow
[...]
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         10.0.0.1        Et1/0*        14.0.0.2        01 0000 0800    34
Et0/0         10.0.0.1        Et1/0         14.0.0.2        01 0000 0800   100
Et0/0         10.0.0.1        Se3/0*        14.0.0.2        01 0000 0800    33
Et0/0         10.0.0.1        Se2/0*        14.0.0.2        01 0000 0800    33
Et0/0         10.0.0.1        Null          224.0.0.5       59 0000 0000    26
```

What kind of load balancing is done on this router?

A. per-packet load balancing
B. per-flow load balancing
C. per-label load balancing
D. star round-robin load balancing

Correct Answer: A
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
Here we can see that for the same traffic source/destination pair of 10.0.0.1 to 14.0.0.2 there were a total of 100 packets (shown by second entry without the *) and that the packets were distributed evenly across the three different outgoing interfaces (34, 33, 33 packets, respectively.

QUESTION 20
What is the most efficient way to confirm whether microbursts of traffic are occurring?

A. Monitor the output traffic rate using the show interface command.
B. Monitor the output traffic rate using the show controllers command.
C. Check the CPU utilization of the router.
D. Sniff the traffic and plot the packet rate over time.

Correct Answer: D
Section: Network Principles
Explanation

Explanation/Reference:

Explanation:
Micro-bursting is a phenomenon where rapid bursts of data packets are sent in quick succession, leading to periods of full line-rate transmission that can overflow packet buffers of the network stack, both in network endpoints and routers and switches inside the network.
In order to troubleshoot microbursts, you need a packet sniffer that can capture traffic over a long period of time and allow you to analyze it in the form of a graph which displays the saturation points (packet rate during microbursts versus total available bandwidth). You can eventually trace it to the source causing the bursts (e.g. stock trading applications).

Reference: Adam, Paul (2014-07-12). All-in-One CCIE V5 Written Exam Guide (Kindle Locations 989-994). Kindle Edition.

QUESTION 21
What is a cause for unicast flooding?

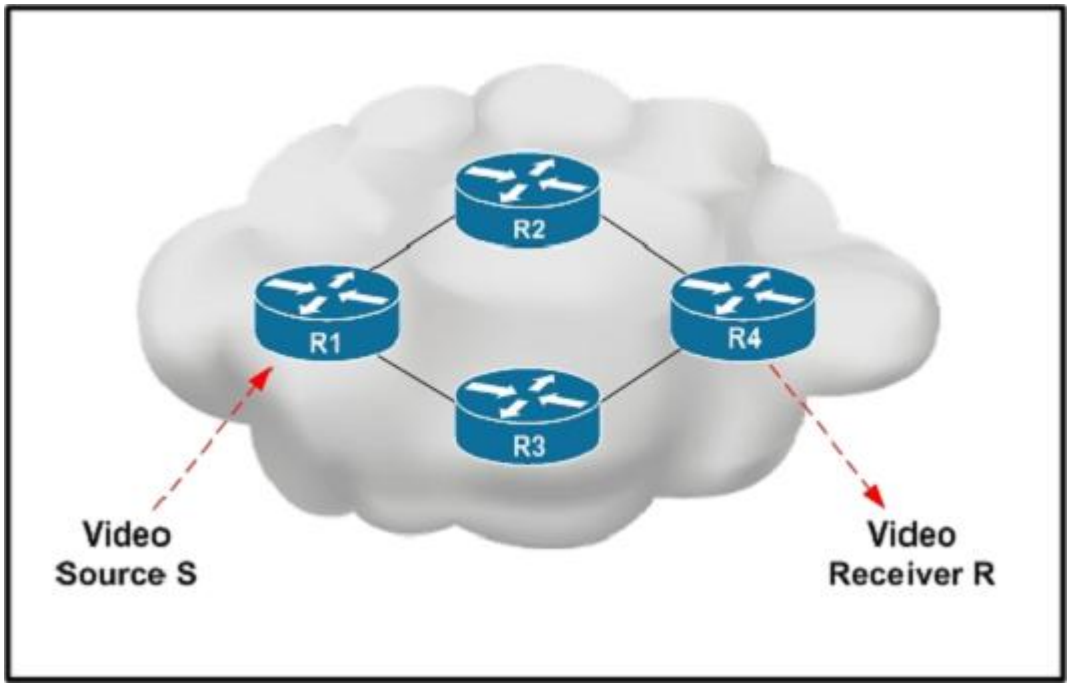
A. Unicast flooding occurs when multicast traffic arrives on a Layer 2 switch that has directly connected multicast receivers.
B. When PIM snooping is not enabled, unicast flooding occurs on the switch that interconnects the PIM-enabled routers.
C. A man-in-the-middle attack can cause the ARP cache of an end host to have the wrong MAC address. Instead of having the MAC address of the default gateway, it has a MAC address of the man-in-the-middle. This causes all traffic to be unicast flooded through the man-in-the-middle, which can then sniff all packets.
D. Forwarding table overflow prevents new MAC addresses from being learned, and packets destined to those MAC addresses are flooded until space becomes available in the forwarding table.

Correct Answer: D
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
Causes of Flooding
The very cause of flooding is that destination MAC address of the packet is not in the L2 forwarding table of the switch. In this case the packet will be flooded out of all forwarding ports in its VLAN (except the port it was received on). Below case studies display most common reasons for destination MAC address not being known to the switch.
Cause 1: Asymmetric Routing
Large amounts of flooded traffic might saturate low-bandwidth links causing network performance issues or complete connectivity outage to devices connected across such low-bandwidth links
Cause 2: Spanning-Tree Protocol Topology Changes
Another common issue caused by flooding is Spanning-Tree Protocol (STP) Topology Change Notification (TCN). TCN is designed to correct forwarding tables after the forwarding topology has changed. This is necessary to avoid a connectivity outage, as after a topology change some destinations previously accessible via particular ports might become accessible via different ports. TCN operates by shortening the forwarding table aging time, such that if the address is not relearned, it will age out and flooding will occur
Cause 3: Forwarding Table Overflow
Another possible cause of flooding can be overflow of the switch forwarding table. In this case, new addresses cannot be learned and packets destined to such addresses are flooded until some space becomes available in the forwarding table. New addresses will then be learned. This is possible but rare, since most modern switches have large enough forwarding tables to accommodate MAC addresses for most designs.

Reference:
http://www.cisco.com/c/en/us/support/docs/switches/catalyst-6000-series-switches/23563-143.html

QUESTION 22
Refer to the exhibit.



Video Source S is sending interactive video traffic to Video Receiver R. Router R1 has multiple routing table entries for destination R. Which load-balancing mechanism on R1 can cause out-of-order video traffic to be received by destination R?

A. per-flow load balancing on R1 for destination R
B. per-source-destination pair load balancing on R1 for destination R
C. CEF load balancing on R1 for destination R
D. per-packet load balancing on R1 for destination R

Correct Answer: D
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
Per-packet load balancing guarantees equal load across all links, however potentially the packets may arrive out-of-order at the destination as differential delay may exist within the network.

Reference: http://www.cisco.com/en/US/products/hw/modules/ps2033/prod_technical_reference09186a00800afeb7.html

QUESTION 23
What is Nagle's algorithm used for?

A. To increase the latency
B. To calculate the best path in distance vector routing protocols
C. To calculate the best path in link state routing protocols
D. To resolve issues caused by poorly implemented TCP flow control.

Correct Answer: D
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
Silly window syndrome is a problem in computer networking caused by poorly implemented TCP flow control. A serious problem can arise in the sliding window operation when the sending application program creates data slowly, the receiving application program consumes data slowly, or both. If a server with this problem is unable to process all incoming data, it requests that its clients reduce the amount of data they send at a time (the window setting on a TCP packet). If the server continues to be unable to process all incoming data, the window becomes smaller and smaller, sometimes to the point that the data transmitted is smaller than the packet header, making data transmission extremely inefficient. The name of this problem is due to the window size shrinking to a "silly" value. When there is no synchronization between the sender and receiver regarding capacity of the flow of data or the size of the packet, the window syndrome problem is created. When the silly window syndrome is created by the sender, Nagle's algorithm is used. Nagle's solution requires that the sender sends the first segment even if it is a small one, then that it waits until an ACK is received or a maximum sized segment (MSS) is accumulated.

Reference: http://en.wikipedia.org/wiki/Silly_window_syndrome

QUESTION 24
Which statement is true regarding the UDP checksum?

A. It is used for congestion control.
B. It cannot be all zeros.
C. It is used by some Internet worms to hide their propagation.
D. It is computed based on the IP pseudo-header.

Correct Answer: D
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
The method used to compute the checksum is defined in RFC 768:
"Checksum is the 16-bit one's complement of the one's complement sum of a pseudo header of information from the IP header, the UDP header, and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets."
In other words, all 16-bit words are summed using one's complement arithmetic. Add the 16-bit values up. Each time a carry-out (17th bit) is produced, swing that bit around and add it back into the least significant bit. The sum is then one's complemented to yield the value of the UDP checksum field.
If the checksum calculation results in the value zero (all 16 bits 0) it should be sent as the one's complement (all 1s).

Reference: http://en.wikipedia.org/wiki/User_Datagram_Protocol

QUESTION 25
Which statement describes the purpose of the Payload Type field in the RTP header?

A. It identifies the signaling protocol.
B. It identifies the codec.
C. It identifies the port numbers for RTP.
D. It identifies the port numbers for RTCP.

Correct Answer: B
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
PT, Payload Type. 7 bits: Identifies the format of the RTP payload and determines its interpretation by the application. A profile specifies a default static mapping of payload type codes to payload formats. Additional payload type codes may be defined dynamically through non-RTP means. An RTP sender emits a single RTP payload type at any given time; this field is not intended for multiplexing separate media streams. A full list of codecs and their payload type values can be found at the link below:

Reference: http://www.networksorcery.com/enp/protocol/rtp.htm

QUESTION 26
Which Cisco IOS XE process administers routing and forwarding?

A. Forwarding manager
B. Interface manager

C. Cisco IOS
D. Host manager

Correct Answer: C
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
Some of the processes are listed in the table below:

Process	Purpose	Affected FRUs	SubPackage Mapping
Host Manager	Provides an interface between the IOS process and many of the information-gathering functions of the underlying platform kernel and operating system.	RP (one instance per RP) SIP (one instance per SIP) ESP (one instance per ESP)	RPControl SIPBase ESPBase
Interface Manager	Provides an interface between the IOS process and the per-SPA interface processes on the SIP.	RP (one instance per RP) SIP (one instance per SIP)	RPControl SIPBase
IOS	The IOS process implements all forwarding and routing features for the router.	RP (one per software redundancy instance per RP). Maximum of two instances per RP.	RPIOS
Forwarding Manager	Manages the downloading of configuration to each of the ESPs and the communication of forwarding plane information, such as statistics, to the IOS process.	RP (one per software redundancy instance per RP). Maximum of two instances per RP. ESP (one per ESP)	RPControl ESPBase

Reference: http://www.cisco.com/c/en/us/td/docs/routers/asr1000/configuration/guide/chassis/asrswcfg/Software_Packaging_Architecture.html

QUESTION 27
Which circumstance can cause packet loss due to a microburst?

A. slow convergence
B. a blocked spanning-tree port
C. process switching

D. insufficient buffers

Correct Answer: D
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
Micro-bursting is a phenomenon where rapid bursts of data packets are sent in quick succession, leading to periods of full line-rate transmission that can overflow packet buffers of the network stack, both in network endpoints and routers and switches inside the network.
Symptoms of micro bursts will manifest in the form of ignores and/ or overruns (also shown as accumulated in “input error” counter within show interface output). This is indicative of receive ring and corresponding packet buffer being overwhelmed due to data bursts coming in over extremely short period of time (microseconds).

Reference: http://ccieordie.com/?tag=micro-burst

QUESTION 28
Which two statements about proxy ARP are true? (Choose two.)

A. It is supported on networks without ARP.
B. It allows machines to spoof packets.
C. It must be used on a network with the host on a different subnet.
D. It requires larger ARP tables.
E. It reduces the amount of ARP traffic.

Correct Answer: BD
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
Disadvantages of Proxy ARP
Hosts have no idea of the physical details of their network and assume it to be a flat network in which they can reach any destination simply by sending an ARP request. But using ARP for everything has disadvantages. These are some of the disadvantages:
- It increases the amount of ARP traffic on your segment.
- Hosts need larger ARP tables in order to handle IP-to-MAC address mappings.
- Security can be undermined. A machine can claim to be another in order to intercept packets, an act called "spoofing."
- It does not work for networks that do not use ARP for address resolution.
- It does not generalize to all network topologies. For example, more than one router that connects two physical networks.

Reference: http://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocation-resolution/13718-5.html

QUESTION 29
Refer to the exhibit.


```
R1
!
interface GigabitEthernet0/0
ip address 10.1.1.1 255.255.255.252
!
router ospf 1
router-id 10.1.1.1
network 10.1.1.1 0.0.0.0 area 0
!

R2
!
interface GigabitEthernet0/0
ip address 10.1.1.2 255.255.255.252
!
router ospf 1
router-id 10.1.1.2
network 10.1.1.2 0.0.0.0 area 0
default-information originate
!
interface GigabitEthernet0/1
description INTERNET
ip address 209.165.202.129 255.255.255.224
!
ip route 209.165.201.254 255.255.255.255 GigabitEthernet0/1
!
```

Routers R1 and R2 are configured as shown, and traffic from R1 fails to reach host 209.165.201.254.

Which action can you take to correct the problem?

A. Ensure that R2 has a default route in its routing table.
B. Change the OSPF area type on R1 and R2.
C. Edit the router configurations so that address 209.165.201.254 is a routable address.
D. Remove the default-information originate command from the OSPF configuration of R2.

Correct Answer: A
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
Not sure that any of these answers are correct, it appears that this configuration is valid for reaching that one specific host IP. Answer A does have a route to that host so it would not need a default route to get to it. Choice B is incorrect as the area types have nothing to do with this. C is incorrect as that IP address is routable, and D is needed so that R1 will have a default route advertised to it from R2 so that it can reach this destination.

QUESTION 30
Which service is disabled by the no service tcp-small-servers command?

A. the finger service
B. the Telnet service
C. the Maintenance Operation Protocol service
D. the chargen service

Correct Answer: D
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
The TCP small servers are:
- **Echo:** Echoes back whatever you type through the **telnet x.x.x.x echo** command.
- **Chargen:** Generates a stream of ASCII data. Use the **telnet x.x.x.x chargen** command.
- **DiscarD.** Throws away whatever you type. Use the **telnet x.x.x.x discard** command.
- **DaytimE.** Returns system date and time, if it is correct. It is correct if you run Network Time Protocol (NTP), or have set the date and time manually from the exec level. Use the **telnet x.x.x.x daytime** command.

Reference: http://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-110/12815-23.html

QUESTION 31
DRAG DROP
Drag and drop the extended ping command field on the left to its usage on the right.

Select and Place:

Drag and drop the extended ping command field on the left to its usage on the right.

type of service	discovering framing issues on serial lines
sweep range of sizes	adjusting delay, throughput, and reliability preferences for the ping
data pattern	configuring the IP header options of the ping
loose, strict, record, timestamp, verbose	determining the minimum MTU in a path

Correct Answer:

Drag and drop the extended ping command field on the left to its usage on the right.

	data pattern
	type of service
	loose, strict, record, timestamp, verbose
	sweep range of sizes

Section: Network Principles
Explanation

Explanation/Reference:

QUESTION 32
DRAG DROP
Drag and drop the argument of the mls ip cef load-sharing command on the left to the function it performs on the right.

Select and Place:

Drag and drop the argument of the **mls ip cef load-sharing** command on the left to the function it performs on the right.

simple	configures CEF load balancing to use Layer 3 and Layer 4 information, excluding m adjacencies
full	configures CEF load balancing to use only destination Layer 4 ports
full simple	configures CEF load balancing to use only Layer 3 information, excluding multip adjacencies
exclude-port source	configures CEF load balancing to use only source Layer 4 ports
exclude-port destination	configures CEF load balancing to use source and destination Layer 3 and Layer 4 information, including multiple adjacencies

Correct Answer:

Drag and drop the argument of the **mls ip cef load-sharing** command on the left to the function it performs on the right.

	full simple
	exclude-port source
	simple
	exclude-port destination
	full

Section: Network Principles
Explanation

Explanation/Reference:

QUESTION 33
Which two Cisco Express Forwarding tables are located in the data plane? (Choose two.)

A. the forwarding information base
B. the label forwarding information base
C. the IP routing table
D. the label information table
E. the adjacency table

Correct Answer: AB
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
The control plane runs protocols such as OSPF, BGP, STP, LDP. These protocols are needed so that routers and switches know how to forward packets and frames.
The data plane is where the actual forwarding takes place. The data plane is populated based on the protocols running in the control plane. The Forwarding Information Base (FIB) is used for IP traffic and the Label FIB is used for MPLS.

QUESTION 34
Which option is the most effective action to avoid packet loss due to microbursts?

A. Implement larger buffers.
B. Install a faster CPU.
C. Install a faster network interface.
D. Configure a larger tx-ring size.

Correct Answer: A
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
You can't avoid or prevent them as such without modifying the sending host's application/network stack so it smoothes out the bursts. However, you can manage microbursts by tuning the size of receive buffers / rings to absorb occasional microbursts.

QUESTION 35
Which two statements about packet fragmentation on an IPv6 network are true? (Choose two.)

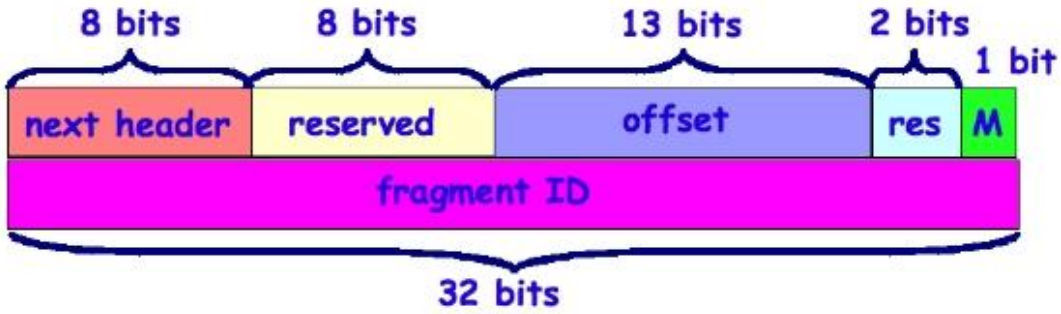
A. The fragment header is 64 bits long.
B. The identification field is 32 bits long.
C. The fragment header is 32 bits long.
D. The identification field is 64 bits long.
E. The MTU must be a minimum of 1280 bytes.
F. The fragment header is 48 bits long.

Correct Answer: AB
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
The fragment header is shown below, being 64 bits total with a 32 bit identification field:

Fragment Header

- **Offset**: the offset, in 8-octet units, of the data following this header, relative to the start of the Fragmentable Part of the packet
- **M flag**: 1 – more fragments, 0 – last fragment



Reference: http://www.openwall.com/presentations/IPv6/img24.html

QUESTION 36
You are backing up a server with a 1 Gbps link and a latency of 2 ms. Which two statements about the backup are true? (Choose two.)

A. The bandwidth delay product is 2 Mb.
B. The default TCP send window size is the limiting factor.
C. The default TCP receive window size is the limiting factor.
D. The bandwidth delay product is 500 Mb.
E. The bandwidth delay product is 50 Mb.

Correct Answer: AC
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
1 Gbps is the same as 1000 Mbps, and 1000Mb x .0002 = 2 Mbps. With TCP based data transfers, the receive window is always the limiting factor, as the sender is generally able to send traffic at line rate, but then must wait for the acknowledgements to send more data.

QUESTION 37
Which two pieces of information does RTCP use to inform endpoint devices about the RTP flow? (Choose two.)

A. the transmitted octet
B. the lost packet count
C. session control function provisioning information
D. the CNAME for session participants
E. the authentication method
F. MTU size changes in the path of the flow

Correct Answer: AB
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
RTCP transports statistics for a media connection and information such as transmitted octet and packet counts, packet loss, packet delay variation, and round-trip delay time. An application may use this information to control quality of service parameters, perhaps by limiting flow, or using a different codec.

Reference: http://en.wikipedia.org/wiki/RTP_Control_Protocol

QUESTION 38
DRAG DROP
Drag and drop the argument of the ip cef load-sharing algorithm command on the left to the function it performs on the right.

Select and Place:

Drag and drop the argument of the **ip cef load-sharing algorithm** command on the left to the function it performs on the right.

original	sets the load-balancing algorithm to use a source, a destination, and an ID hash
universal	sets the load-balancing algorithm for environments with a small number of sourc destination IP address pairs
tunnel	sets the load-balancing algorithm to use Layer 4 information
include-ports source destination	sets the load-balancing algorithm to use a source and destination hash

Correct Answer:

Drag and drop the argument of the **ip cef load-sharing algorithm** command on the left to the function it performs on the right.

	universal
	tunnel
	include-ports source destination
	original

Section: Network Principles
Explanation

Explanation/Reference:

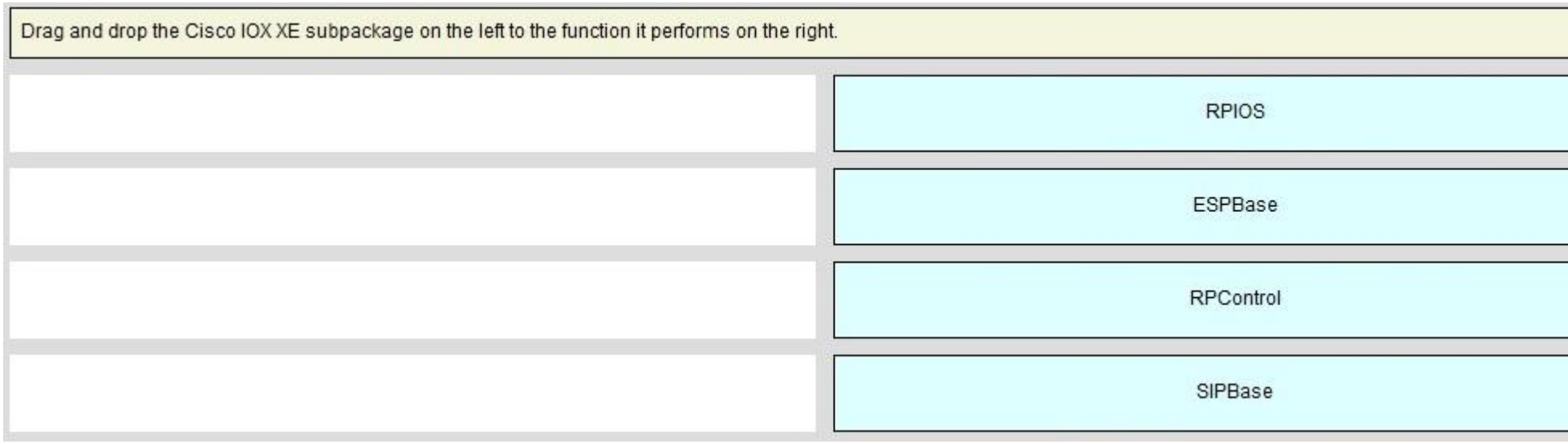
QUESTION 39
DRAG DROP
Drag and drop the Cisco IOX XE subpackage on the left to the function it performs on the right.

Select and Place:

Drag and drop the Cisco IOX XE subpackage on the left to the function it performs on the right.

RPIOS	provisions the Cisco IOS Software kernel from which the IOS software features are housed and run
ESPBase	produces the ESP software, ESP operating system, and control processes
SIPBase	manages the Cisco IOS Software and the rest of the platform via the control plane
RPControl	manages the Session Initiation Protocol carrier card operating system and control processes

Correct Answer:



Section: Network Principles
Explanation

Explanation/Reference:

QUESTION 40
DRAG DROP
Drag and drop each description of IPv6 transition technology on the left to the matching IPv6 transition technology category on the right.

Select and Place:

Drag and drop each description of IPv6 transition technology on the left to the matching IPv6 transition technology category on the right.

- encapsulates IPv6 packets within IPv4 packets
- supports translation between IPv4 and IPv6 by using algorithms to map addresses
- supports stateful translation between IPv4 and IPv6 with static and manual mappings
- requires IPv6-capable infrastructure
- uses routing protocols to maintain IPv4 and IPv6 routing adjacencies
- encapsulates IPv4 packets within IPv6 packets

Dual-Stack Network

Tunneling

NAT64

Correct Answer:

Drag and drop each description of IPv6 transition technology on the left to the matching IPv6 transition technology category on the right.

Dual-Stack Network
- requires IPv6-capable infrastructure
- uses routing protocols to maintain IPv4 and IPv6 routing adjacencies

Tunneling
- encapsulates IPv6 packets within IPv4 packets
- encapsulates IPv4 packets within IPv6 packets

NAT64
- supports translation between IPv4 and IPv6 by using algorithms to map addresses
- supports stateful translation between IPv4 and IPv6 with static and manual mappings

Section: Network Principles
Explanation

Explanation/Reference:

QUESTION 41

How many hash buckets does Cisco Express Forwarding use for load balancing?

A. 8
B. 16
C. 24
D. 32

Correct Answer: B
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
In order to understand how the load balance takes place, you must first see how the tables relate. The Cisco Express Forwarding table points to 16 hash buckets (load share table), which point to the adjacency table for parallel paths. Each packet to be switched is broken up into the source and destination address pair and checked against the loadshare table.

Reference: http://www.cisco.com/c/en/us/support/docs/ip/express-forwarding-cef/18285-loadbal-cef.html

QUESTION 42
Which three features require Cisco Express Forwarding? (Choose three.)

A. NBAR
B. AutoQoS
C. fragmentation
D. MPLS
E. UplinkFast
F. BackboneFast

Correct Answer: ABD
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
QoS Features That Require CEF

These class-based QoS features are supported only on routers that run CEF.

- Network Based Application Recognition (NBAR) provides intelligent network classification. For more information, refer to Network Based Application Recognition.

- The AutoQoS -VoIP feature simplifies and speeds up the implementation and provisioning of QoS for VoIP traffic. This feature is enabled with the help of the auto qos voip command. CEF must be enabled at the interface or ATM PVC before the auto qos command can be used. For more information about this feature and its prerequisites, refer to AutoQoS - VoIP.

From MPLS Fundamentals - Luc De Ghein
Why Is CEF Needed in MPLS Networks?
Concerning MPLS, CEF is special for a certain reason; otherwise, this book would not explicitly cover it. Labeled packets that enter the router are switched according to the label forwarding information base (LFIB) on the router. IP packets that enter the router are switched according to the CEF table on the router. Regardless of whether the packet is switched according to the LFIB or the CEF table, the outgoing packet can be a labeled packet or an IP packet

Reference: http://www.cisco.com/c/en/us/support/docs/asynchronous-transfer-mode-atm/ip-to-atm-class-of-service/4800-cefreq.html

QUESTION 43
Which two options are interface requirements for turbo flooding? (Choose two.)

A. The interface is Ethernet.
B. The interface is configured for ARPA encapsulation.
C. The interface is PPP.
D. The interface is configured for GRE encapsulation.
E. The interface is configured for 802.1Q encapsulation.

Correct Answer: AB
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
In the switch, the majority of packets are forwarded in hardware; most packets do not go through the switch CPU. For those packets that do go to the CPU, you can speed up spanning tree-based UDP flooding by a factor of about four to five times by using turbo-flooding. This feature is supported over Ethernet interfaces configured for ARPA encapsulation.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/metro/me3400/software/release/12-2_50_se/configuration/guide/scg/swiprout.html

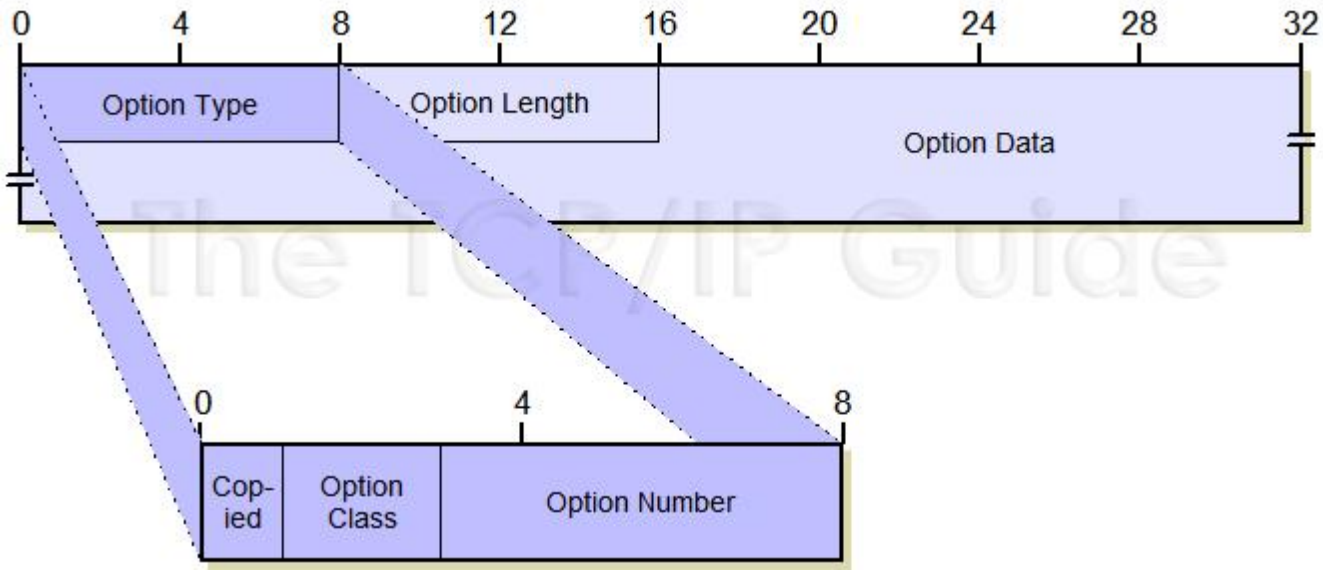
QUESTION 44
Which three options are sub-subfields of the IPv4 Option Type subfield? (Choose three.)

A. Option Class
B. GET
C. Copied

D. PUSH
E. Option Number
F. TTL

Correct Answer: ACE
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
Each IP option has its own subfield format, generally structured as shown below. For most options, all three subfields are used. Option Type, Option Length and Option Data.



Reference: http://www.tcpipguide.com/free/t_IPDatagramOptionsandOptionFormat.htm

QUESTION 45
Which TCP mechanism prevents the sender from sending data too quickly for the receiver to process?

A. Congestion control
B. Error detection
C. Selective acknowledgement

D. Flow control

Correct Answer: D
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
In data communications, flow control is the process of managing the rate of data transmission between two nodes to prevent a fast sender from overwhelming a slow receiver. It provides a mechanism for the receiver to control the transmission speed, so that the receiving node is not overwhelmed with data from transmitting node.

Reference: http://en.wikipedia.org/wiki/Flow_control_(data)

QUESTION 46
Which two packet types does an RTP session consist of? (Choose two.)

A. TCP
B. RTCP
C. RTP
D. ICMP
E. BOOTP
F. ARP

Correct Answer: BC
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
An RTP session is established for each multimedia stream. A session consists of an IP address with a pair of ports for RTP and RTCP. For example, audio and video streams use separate RTP sessions, enabling a receiver to deselect a particular stream. The ports which form a session are negotiated using other protocols such as RTSP (using SDP in the setup method) and SIP. According to the specification, an RTP port should be even and the RTCP port is the next higher odd port number.

Reference: http://en.wikipedia.org/wiki/Real-time_Transport_Protocol

QUESTION 47
Which technology can create a filter for an embedded packet capture?

A. Control plane policing

B. Access lists
C. NBAR
D. Traffic shaping

Correct Answer: B
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
A filter can be applied to limit the capture to desired traffic. Define an Access Control List (ACL) within config mode and apply the filter to the buffer:

```
ip access-list extended BUF-FILTER
    permit ip host 192.168.1.1 host 172.16.1.1
    permit ip host 172.16.1.1 host 192.168.1.1
monitor capture buffer BUF filter access-list BUF-FILTER
```

Reference: http://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-embedded-packet-capture/116045-productconfig-epc-00.html

QUESTION 48
Which option describes a limitation of Embedded Packet Capture?

A. It can capture data only on physical interfaces and subinterfaces.
B. It can store only packet data.
C. It can capture multicast packets only on ingress.
D. It can capture multicast packets only on egress.

Correct Answer: C
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
Restrictions for Embedded Packet Capture
- In Cisco IOS Release 12.2(33)SRE, EPC is supported only on 7200 platform.
- **EPC only captures multicast packets on ingress and does not capture the replicated packets on egress.**
- Currently, the capture file can only be exported off the device; for example, TFTP or FTP servers and local disk.

Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/epc/configuration/15-mt/epc-15-mt-book/nm-packet-capture.html

QUESTION 49

Refer to the exhibit.

```
switch#show mls cef exception status
Current IPv4 FIB exception state = TRUE
Current IPv6 FIB exception state = FALSE
Current MPLS FIB exception state = FALSE
```

A Cisco Catalyst 6500 Series Switch experiences high CPU utilization. What can be the cause of this issue, and how can it be prevented?

A. The hardware routing table is full. Redistribute from BGP into IGP.
B. The software routing table is full. Redistribute from BGP into IGP.
C. The hardware routing table is full. Reduce the number of routes in the routing table.
D. The software routing table is full. Reduce the number of routes in the routing table.

Correct Answer: C
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
FIB TCAM Exception - If you try to install more routes than are possible into the FIB TCAM you will see the following error message in the logs:

CFIB-SP-STBY-7-CFIB_EXCEPTION : FIB TCAM exception, Some entries will be software switched

%CFIB-SP-7-CFIB_EXCEPTION : FIB TCAM exception, Some entries will be software switched.
%CFIB-SP-STBY-7-CFIB_EXCEPTION : FIB TCAM exception, Some entries will be software switched.

This error message is received when the amount of available space in the TCAM is exceeded. This results in high CPU. This is a FIB TCAM limitation. Once TCAM is full, a flag will be set and FIB TCAM exception is received. This stops from adding new routes to the TCAM. Therefore, everything will be software switched. The removal of routes does not help resume hardware switching. Once the TCAM enters the exception state, the system must be reloaded to get out of that state. You can view if you have hit a FIB TCAM exception with the following command:

6500-2#sh mls cef exception status
Current IPv4 FIB exception state = TRUE
Current IPv6 FIB exception state = FALSE
Current MPLS FIB exception state = FALSE

When the exception state is TRUE, the FIB TCAM has hit an exception.
The maximum routes that can be installed in TCAM is increased by the mls cef maximum-**routes** command.

Reference: https://supportforums.cisco.com/document/59926/troubleshooting-high-cpu-6500-sup720

QUESTION 50
Refer to the exhibit.

```
access-switch-1#show interface fastethernet0/9
FastEthernet0/9 is up, line protocol is up (connected)
   Hardware is Fast Ethernet, address is 04da.d237.9f09 (bia 04da.d237.9f09)
   Auto-duplex, Auto-speed, media type is 10/100BaseTX
   Last clearing of "show interface" counters never
   Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 59137853

access-switch-1#show mls qos interface fastethernet0/9 statistics
Queueset: 1
output queues dropped:
   queue:    threshold1   threshold2   threshold3
   -----------------------------------------------
   queue 0:           0            0        48252
   queue 1:    23164955     35924645            1
   queue 2:           0            0            0
   queue 3:           0            0            0
```

Your network is suffering excessive output drops. Which two actions can you take to resolve the problem? (Choose two.)

A. Install a switch with larger buffers.
B. Configure a different queue set.
C. Reconfigure the switch buffers.
D. Configure the server application to use TCP.
E. Update the server operating system.

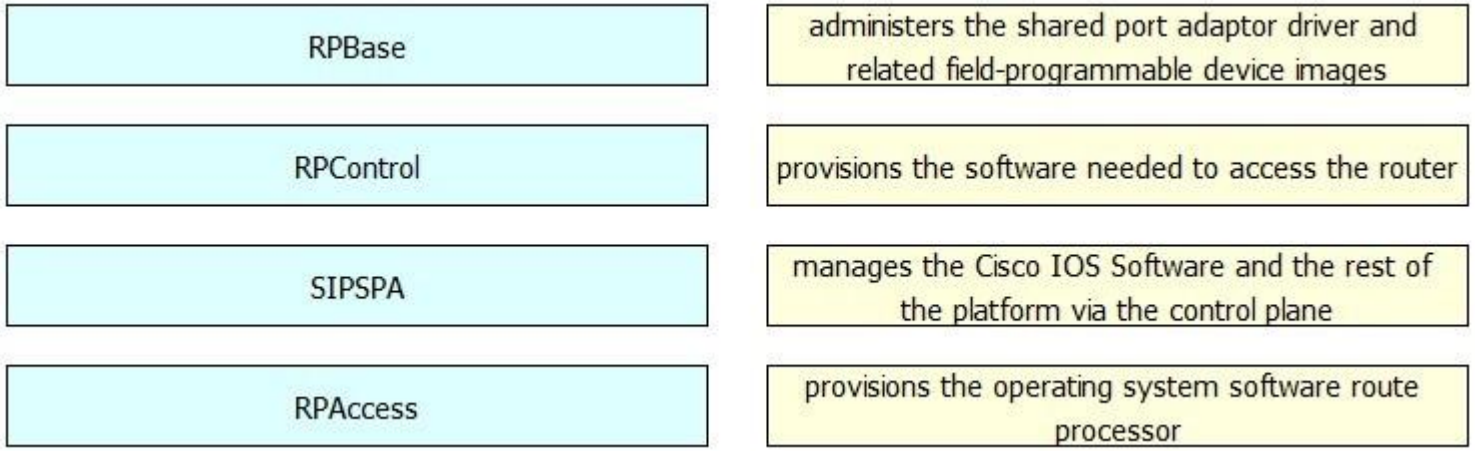
Correct Answer: AB
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
Installing a switch with larger buffers and correctly configuring the buffers can solve output queue problems.
For each queue we need to configure the assigned buffers. The buffer is like the ‘storage’ space for the interface and we have to divide it among the different queues. This is how to do it:
mls qos queue-set output <queue set> buffers Q1 Q2 Q3 Q4

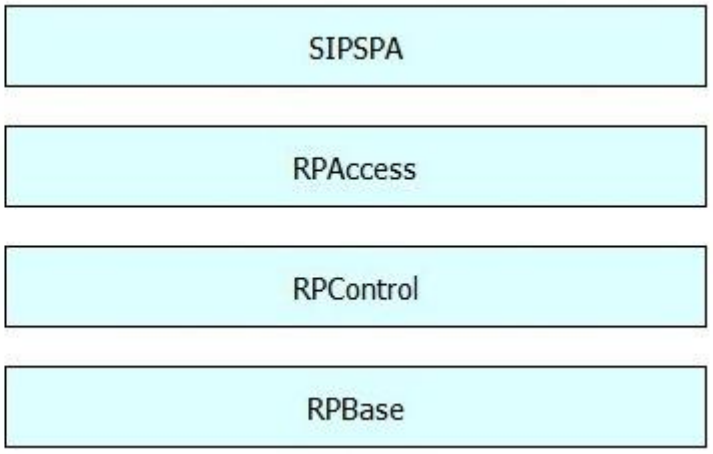
In this example, there is nothing hitting queue 2 or queue 3 so they are not being utilized.

QUESTION 51
DRAG DROP
Drag and drop the Cisco IOS XE subpackage on the left to the function it performs on the right.

Select and Place:



Correct Answer:



Section: Network Principles

Explanation

Explanation/Reference:

QUESTION 52
Which two Cisco IOS XE commands can install a subpackage onto a router? (Choose two.)

A. request platform software package install rp rpSlotNumber file fileURL
B. boot system flash bootflash:filename
C. copy sourceUrl destinationUrl
D. license install file storedLocationUrl
E. issu loadversion rp identifier file diskType imageFilename
F. config-register value

Correct Answer: AC
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
Managing and Configuring a Consolidated Package Using the request platform software package install Command
In the following example, the **request platform software package install** command is used to upgrade a consolidated package running on RP 0. The **force** option, which forces the upgrade past any prompt (such as already having the same consolidated package installed), is used in this example.
Router# **request platform software package install rp 0 file bootflash:asr1000rp1-adventerprisek9.02.01.00.122-33.XNA.bin force**
To upgrade a consolidated package on the Cisco ASR 1000 Series Routers using the **copy** command, copy the consolidated package into the bootflash: directory on the router using the **copy** command as you would on most other Cisco routers. After making this copy, configure the router to boot using the consolidated package file.
In the following example, the consolidated package file is copied onto the bootflash: file system from TFTP. The config-register is then set to boot using **boot system** commands, and the **boot system** commands instruct the router to boot using the consolidated package stored in the bootflash: file system. The new configuration is then saved using the **copy running-config startup-config** command, and the system is then reloaded to complete the process.
Router# **dir bootflash:**
Directory of bootflash:/

11 drwx 16384 Dec 4 2007 04:32:46 -08:00 lost+found
86401 drwx 4096 Dec 4 2007 06:06:24 -08:00.ssh
14401 drwx 4096 Dec 4 2007 06:06:36 -08:00.rollback_timer
28801 drwx 4096 Mar 18 2008 17:31:17 -07:00.prst_sync
43201 drwx 4096 Dec 4 2007 04:34:45 -08:00.installer
13 -rw- 45977 Apr 9 2008 16:48:46 -07:00 target_support_output.tgz.tgz

928862208 bytes total (712273920 bytes free)
Router# **copy tftp bootflash:**
Address or name of remote host []? **172.17.16.81**
Source filename []? **/auto/tftp-users/user/asr1000rp1-adventerprisek9.02.01.00.122-33.XNA.bin**
Destination filename [asr1000rp1-adventerprisek9.02.01.00.122-33.XNA.bin]?

Reference: http://www.cisco.com/c/en/us/td/docs/routers/asr1000/configuration/guide/chassis/asrswcfg/Package_Management.html#78189

QUESTION 53
Which two statements about Cisco Express Forwarding are true? (Choose two.)

A. Cisco Express Forwarding tables contain reachability information and adjacency tables contain forwarding information.
B. Cisco Express Forwarding tables contain forwarding information and adjacency tables contain reachability information.
C. Changing MAC header rewrite strings requires cache validation.
D. Adjacency tables and Cisco Express Forwarding tables can be built separately.
E. Adjacency tables and Cisco Express Forwarding tables require packet process-switching.

Correct Answer: AD
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
Main Components of CEF
Information conventionally stored in a route cache is stored in several data structures for Cisco Express Forwarding switching. The data structures provide optimized lookup for efficient packet forwarding. The two main components of Cisco Express Forwarding operation are the forwarding information base (FIB) and the adjacency tables.
The FIB is conceptually similar to a routing table or information base. A router uses this lookup table to make destination-based switching decisions during Cisco Express Forwarding operation. The FIB is updated when changes occur in the network and contains all routes known at the time.
Adjacency tables maintain Layer 2 next-hop addresses for all FIB entries.
This separation of the reachability information (in the Cisco Express Forwarding table) and the forwarding information (in the adjacency table), provides a number of benefits:

- The adjacency table can be built separately from the Cisco Express Forwarding table, allowing both to be built without any packets being process-switched.
- The MAC header rewrite used to forward a packet is not stored in cache entries, so changes in a MAC header rewrite string do not require validation of cache entries.

Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipswitch_cef/configuration/15-mt/isw-cef-15-mt-book/isw-cef-overview.html

QUESTION 54
Which TCP feature allows a client to request a specific packet that was lost?

A. flow control
B. sliding window
C. fast recovery
D. selective acknowledgment

Correct Answer: D
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
TCP Selective Acknowledgment
The TCP Selective Acknowledgment feature improves performance if multiple packets are lost from one TCP window of data.
Prior to this feature, because of limited information available from cumulative acknowledgments, a TCP sender could learn about only one lost packet per-round-trip time. An aggressive sender could choose to resend packets early, but such re-sent segments might have already been successfully received.
The TCP selective acknowledgment mechanism helps improve performance. The receiving TCP host returns selective acknowledgment packets to the sender, informing the sender of data that has been received. In other words, the receiver can acknowledge packets received out of order. The sender can then resend only missing data segments (instead of everything since the first missing packet).
Prior to selective acknowledgment, if TCP lost packets 4 and 7 out of an 8-packet window, TCP would receive acknowledgment of only packets 1, 2, and 3. Packets 4 through 8 would need to be re-sent. With selective acknowledgment, TCP receives acknowledgment of packets 1, 2, 3, 5, 6, and 8. Only packets 4 and 7 must be re-sent.
TCP selective acknowledgment is used only when multiple packets are dropped within one TCP window. There is no performance impact when the feature is enabled but not used. Use the **ip tcp selective-ack** command in global configuration mode to enable TCP selective acknowledgment.

Refer to RFC 2018 for more details about TCP selective acknowledgment.

QUESTION 55
Which two solutions can reduce UDP latency? (Choose two.)

A. fast retransmission
B. fast recovery
C. fast start
D. low-latency queuing
E. IP service level agreements
F. congestion-avoidance algorithm

Correct Answer: DE
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
IP SLA uses active traffic monitoring, which generates traffic in a continuous, reliable, and predictable manner to measure network performance. IP SLA sends data across the network to measure performance between multiple network locations or across multiple network paths. It simulates network data and IP services, and collects network performance information in real time. This information is collected:

- Response times
- One-way latency, jitter (interpacket delay variance)
- Packet loss
- Network resource availability

LLQ uses the priority command. The priority command allows you to set up classes based on a variety of criteria (not just User Datagram Ports (UDP) ports) and assign priority to them, and is available for use on serial interfaces and ATM permanent virtual circuits (PVCs). A similar command, the ip rtp priority command, allows you to stipulate priority flows based only on UDP port numbers.
Note: All the other answer choices can be used to improve TCP performance, but not UDP.

References:
http://www.cisco.com/c/en/us/td/docs/routers/xr12000/software/xr12k_r4-2/system_monitoring/configuration/guide/b_sysmon_cg42xr12k/b_sysmon_cg42xr12k_chapter_011.html
http://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/fsllq26.html

QUESTION 56
DRAG DROP
Drag and drop the argument of the mpls ip cef load-sharing command on the left to the function it performs on the right.

Select and Place:

simple	configures cef load balancing to use Layer 3 and Layer 4
full	configures CEF load balancing to use only destination Layer 4 ports
full simple	configures CEF load balancing to use only Layer 3 information,
exclude-port source	configures CEF load balancing to use only source Layer 4 ports
exclude-port destination	configures CEF load balancing to use source and destination

Correct Answer:

	full simple
	exclude-port source
	simple
	exclude-port destination
	full

Section: Network Principles
Explanation

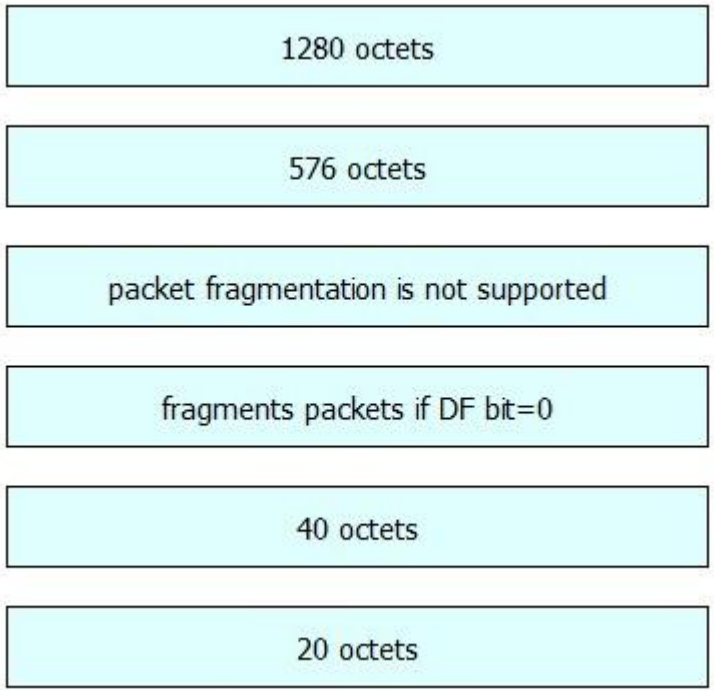
Explanation/Reference:

QUESTION 57
DRAG DROP
Drag and drop the fragmentation characteristics on the left to the corresponding protocol on the right.

Select and Place:

40 octets	IPv6 minimum MTU
fragments packets if DF bit=0	IPv4 minimum MTU
1280 octets	IPv6 routers
20 octets	IPv4 routers
packet fragmentation is not supported	IPv6 header length
576 octets	IPv4 header length

Correct Answer:



Section: Network Principles
Explanation

Explanation/Reference:

QUESTION 58
Refer to the exhibit.

```
Switch#show spanning-tree

VLAN0001

   Spanning tree enabled protocol ieee

   Root ID    Priority    32769
      Address     001a.6d4b.c500
      This bridge is the root
      Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

   Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
      Address     001a.6d4b.c500
      Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
      Aging Time 15

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------
Fa0/1            Desg FWD 19        128.1    P2p
```

If you change the Spanning Tree Protocol from pvst to rapid-pvst, what is the effect on the interface Fa0/1 port state?

A. It transitions to the listening state, and then the forwarding state.
B. It transitions to the learning state and then the forwarding state.
C. It transitions to the blocking state, then the learning state, and then the forwarding state.
D. It transitions to the blocking state and then the forwarding state.

Correct Answer: C
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
First, the port will transition to the blocking state, immediately upon the change, then it will transition to the new RSTP states of learning and forwarding.
Port States
There are only three port states left in RSTP that correspond to the three possible operational states. The 802.1D disabled, blocking, and listening states are merged into a unique 802.1w discarding state.

STP (802.1D) Port State	RSTP (802.1w) Port State	Is Port Included in Active Topology?	Is Port Learning MAC Addresses?
Disabled	Discarding	No	No
Blocking	Discarding	No	No
Listening	Discarding	Yes	No
Learning	Learning	Yes	Yes
Forwarding	Forwarding	Yes	Yes

QUESTION 59
Which type of port would have root guard enabled on it?

A. A root port
B. An alternate port
C. A blocked port
D. A designated port

Correct Answer: D
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
The root guard feature provides a way to enforce the root bridge placement in the network.
The root guard ensures that the port on which root guard is enabled is the designated port. Normally, root bridge ports are all designated ports, unless two or more ports of the root bridge are connected together. If the bridge receives superior STP Bridge Protocol Data Units (BPDUs) on a root guard-enabled port, root guard moves this port to a root-inconsistent STP state. This root-inconsistent state is effectively equal to a listening state. No traffic is forwarded across this port. In this way, the root guard enforces the position of the root bridge.

Reference: http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10588-74.html

QUESTION 60
Refer to the exhibit.

```
switch#show spanning-tree detail

 MST0 is executing the mstp compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, sysid 0, address f4ac.c1c4.2b80
  Configured hello time 2, max age 20, forward delay 15, transmit hold-count 6
  Current root has priority 24576, address 0019.07aa.9ac0
  Root port is 56 (Port-channel1), cost of root path is 0
  Topology change flag not set, detected flag not set
  Number of topology changes 296 last change occurred 00:01:17 ago
          from GigabitEthernet0/15
```

While troubleshooting high CPU utilization on one of your Cisco Catalyst switches, you find that the issue is due to excessive flooding that is caused by STP. What can you do to prevent this issue from happening again?

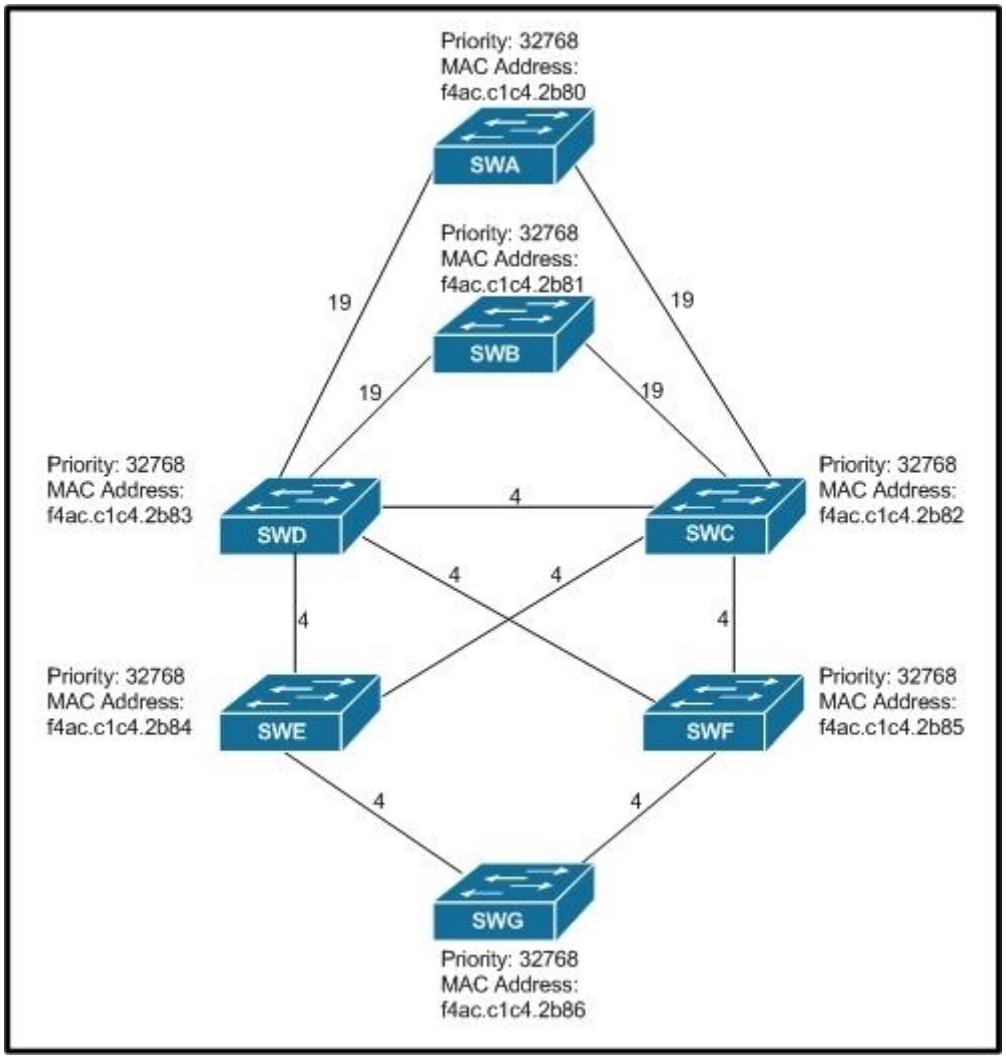
A. Disable STP completely on the switch.
B. Change the STP version to RSTP.
C. Configure PortFast on port-channel 1.
D. Configure UplinkFast on the switch.
E. Configure PortFast on interface Gi0/15.

Correct Answer: E
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
Topology Changes (TC) should be a rare event in a well-configured network. When a link on a switch port goes up or down, there is eventually a TC, once the STP state of the port is changing to or from forwarding. When the port is flapping, this would cause repetitive TCs and flooding.
Ports with the STP portfast feature enabled will not cause TCs when going to or from the forwarding state. The configuration of portfast on all end-device ports (such as printers, PCs, and servers) should limit TCs to a low amount and is highly recommended.

Reference: http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/28943-170.html

QUESTION 61
Refer to the exhibit.



All switches have default bridge priorities, and originate BPDUs with MAC addresses as indicated. The numbers shown are STP link metrics. Which two ports are forwarding traffic after STP converges? (Choose two.)

A. The port connecting switch SWD with switch SWE
B. The port connecting switch SWG with switch SWF
C. The port connecting switch SWC with switch SWE

D. The port connecting switch SWB with switch SWC

Correct Answer: CD
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
Here, we know SWB to SWC are forwarding because we already identified the blocking port. So for the last correct answer let's consider what must be done to prevent a switch loop between SWC/SWD/SWE. SWE to SWD will be blocked because SWC has a lower MAC address so it wins the forwarding port. And to look at it further, you could try to further understand what would happen with ports on SWG. Would the ports on SWG try to go through SWE or SWF? SWE has the lower MAC address so the port from SWG to SWE would win the forwarding election. Therefore, answer B could never be correct.

QUESTION 62
Refer to the exhibit.

```
Switch# show ip igmp snooping mrouter
Vlan    ports
----    -----
  10    Gi2/0/1(dynamic), Router
  20    Gi2/0/1(dynamic), Router
```

Which three statements about the output are true? (Choose three.)

A. An mrouter port can be learned by receiving a PIM hello packet from a multicast router.
B. This switch is configured as a multicast router.
C. Gi2/0/1 is a trunk link that connects to a multicast router.
D. An mrouter port is learned when a multicast data stream is received on that port from a multicast router.
E. This switch is not configured as a multicast router. It is configured only for IGMP snooping.
F. IGMP reports are received only on Gi2/0/1 and are never transmitted out Gi2/0/1 for VLANs 10 and 20.

Correct Answer: ABC
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
In this example, the switch has been configured as a multicast router since IGMP snooping has been enabled. All mrouters can learn about other

mrouters by receiving a PIM hello packet from another multicast router. Also, since two different VLANs are being used by the same port of gi 2/0/1, it must be a trunk link that connects to another multicast router.

QUESTION 63
Refer to the exhibit.

```
Switch#show int fastEthernet0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dotlq
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 2 (VLAN0002)
Trunking Native Mode VLAN: 3 (VLAN0003)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dotlq
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

If a port is configured as shown and receives an untagged frame, of which VLAN will the untagged frame be a member?

A. VLAN 1
B. VLAN 2
C. VLAN 3
D. VLAN 4

Correct Answer: B
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
When typing:
Switch(config-if)#**switchport mode?**
access Set trunking mode to ACCESS unconditionally
dynamic Set trunking mode to dynamically negotiate access or trunk mode
trunk Set trunking mode to TRUNK unconditionally
and
Switch(config-if)#**switchport mode dynamic?**
auto Set trunking mode dynamic negotiation parameter to AUTO
desirable Set trunking mode dynamic negotiation parameter to DESIRABLE
So if we configure Fa0/1 as **dynamic auto** mode, it will not initiate any negotitation but waiting for the other end negotiate to be a trunk with DTP. If the other end does not ask it to become a trunk then it will become an access port. Therefore when using the "show interface fastEthernet0/1 switchport" command we will see two output lines "**Administrative Mode. dynamic auto**" and "**Operational Mode. static access**"
Note. To set this port to VLAN 2 as the output above just use one additional command. "switchport access vlan 2".
Now back to our question, from the output we see that Fa0/1 is operating as an access port on VLAN 2 so if it receive untagged frame it will suppose that frame is coming from VLAN 2.

QUESTION 64
Refer to the exhibit.

```
Switch#show interfaces switchport backup detail

Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
FastEthernet0/1         FastEthernet0/2         Active Up/Backup Standby

Interface Pair   : Fa0/1, Fa0/2
Preemption Mode  : off
Bandwidth : 100000 Kbit (Fa0/1), 10000 Kbit (Fa0/2)
Mac Address Move Update Vlan : auto
```

Which statement describes the effect on the network if FastEthernet0/1 goes down temporarily?

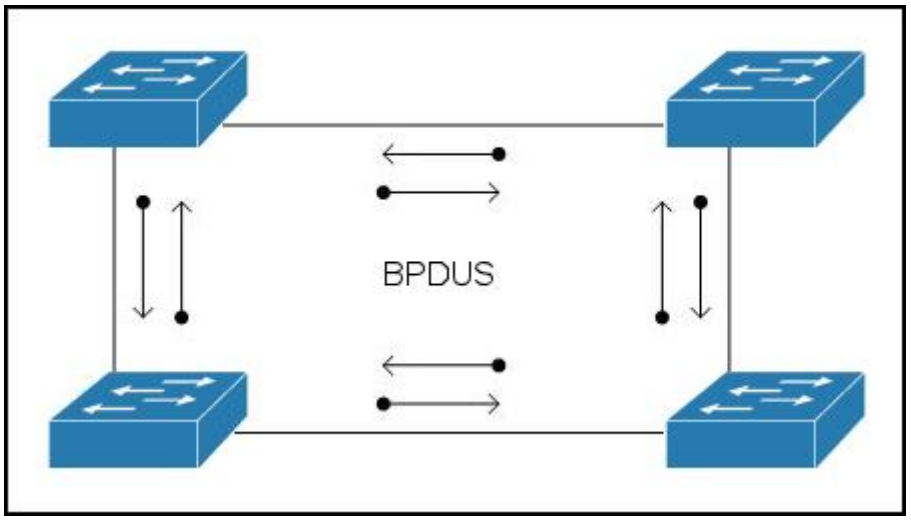
A. FastEthernet0/2 forwards traffic only until FastEthernet0/1 comes back up.
B. FastEthernet0/2 stops forwarding traffic until FastEthernet0/1 comes back up.
C. FastEthernet0/2 forwards traffic indefinitely.
D. FastEthernet0/1 goes into standby.

Correct Answer: C
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
Use the switchport backup interface interface configuration command on a Layer 2 interface to configure Flex Links, a pair of interfaces that provide backup to each other. Use the no form of this command to remove the Flex Links configuration.
With Flex Links configured, one link acts as the primary interface and forwards traffic, while the other interface is in standby mode, ready to begin forwarding traffic if the primary link shuts down. The interface being configured is referred to as the active link; the specified interface is identified as the backup link. The feature provides an alternative to the Spanning Tree Protocol (STP), allowing users to turn off STP and still retain basic link redundancy.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_53_se/command/reference/2960ComRef/cli3.html#wp3269214

QUESTION 65
Refer to the exhibit.

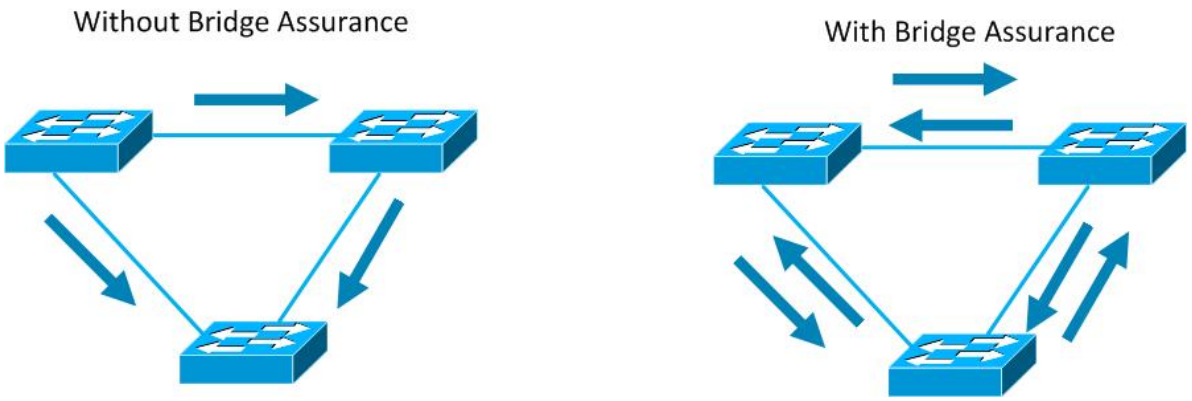


Which technology does the use of bi-directional BPDUs on all ports in the topology support?

A. RSTP
B. MST
C. Bridge Assurance
D. Loop Guard
E. Root Guard
F. UDLD

Correct Answer: C
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
Spanning Tree Bridge Assurance
- Turns STP into a bidirectional protocol
- Ensures spanning tree fails “closed” rather than “open”
- If port type is “network” send BPDU regardless of state
- If network port stops receiving BPDU it’s put in BA-inconsistent state



Bridge Assurance (BA) can help protect against bridging loops where a port becomes designated because it has stopped receiving BPDUs. This is similar to the function of loop guard.

Reference: http://lostintransit.se/tag/convergence/

QUESTION 66
Which three statements are true about PPP CHAP authentication? (Choose three.)

A. PPP encapsulation must be enabled globally.
B. The LCP phase must be complete and in closed state.
C. The hostname used by a router for CHAP authentication cannot be changed.
D. PPP encapsulation must be enabled on the interface.
E. The LCP phase must be complete and in open state.
F. By default, the router uses its hostname to identify itself to the peer.

Correct Answer: DEF
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
Point-to-Point Protocol (PPP) authentication issues are one of the most common causes for dialup link failures. This document provides some troubleshooting procedures for PPP authentication issues.
Prerequisites
- Enable **PPP encapsulation**
- The PPP authentication phase does not begin until the Link Control Protocol (LCP) phase is complete and is in the open state. If **debug ppp negotiation** does not indicate that LCP is open, troubleshoot this issue before proceeding.

Note. By default, the router uses its hostname to identify itself to the peer. However, this CHAP username can be changed through the ppp chap hostname command.

Reference: http://www.cisco.com/c/en/us/support/docs/wan/point-to-point-protocol-ppp/25647-understanding-ppp-chap.html

QUESTION 67
Which two statements are true about an EPL? (Choose two.)

A. It is a point-to-point Ethernet connection between a pair of NNIs.
B. It allows for service multiplexing.
C. It has a high degree of transparency.
D. The EPL service is also referred to as E-line.

Correct Answer: CD
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
Ethernet private line (EPL) and Ethernet virtual private line (EVPL) are carrier Ethernet data services defined by the Metro Ethernet Forum. EPL provides a point-to-point Ethernet virtual connection (EVC) between a pair of dedicated user–network interfaces (UNIs), with a high degree of transparency. EVPL provides a point-to-point or point-to-multipoint connection between a pair of UNIs.
The services are categorized as an E-Line service type, with an expectation of low frame delay, frame delay variation and frame loss ratio. EPL is implemented using a point-to-point (EVC) with no Service Multiplexing at each UNI (physical interface), i.e., all service frames at the UNI are mapped to a single EVC (a.k.a. all-to-one bundling).

Reference: http://en.wikipedia.org/wiki/Ethernet_Private_Line

QUESTION 68
Which two statements describe characteristics of HDLC on Cisco routers? (Choose two.)

A. It supports multiple Layer 3 protocols.
B. It supports multiplexing.
C. It supports only synchronous interfaces.
D. It supports authentication.

Correct Answer: AC
Section: Layer 2 Technologies
Explanation

Explanation/Reference:

Explanation:
Cisco High-Level Data Link Controller (HDLC) is the Cisco proprietary protocol for sending data over synchronous serial links using HDLC. Cisco HDLC also provides a simple control protocol called Serial Line Address Resolution Protocol (SLARP) to maintain serial link keepalives. Cisco HDLC is the default for data encapsulation at Layer 2 (data link) of the Open System Interconnection (OSI) stack for efficient packet delineation and error control. The absence of a protocol type field in the HDLC header posed a problem for links that carried traffic from more than one Layer 3 protocol. Cisco, therefore, added an extra Type field to the HDLC header, creating a Cisco-specific version of HDLC. Cisco routers can support multiple network layer protocols on the same HDLC link. For example an HDLC link between two Cisco routers can forward both IPv4 and IPv6 packets because the Type field can identify which type of packet is carried inside each HDLC frame.

Reference: http://www.cisco.com/c/en/us/td/docs/routers/access/800/819/software/configuration/Guide/819_SCG/6ser_conf.html#pgfId-1073734

QUESTION 69
Which mechanism can be used on Layer 2 switches so that only multicast packets with downstream receivers are sent on the multicast router-connected ports?

A. IGMP snooping
B. Router Guard
C. PIM snooping
D. multicast filtering

Correct Answer: C
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
Ideally, the Layer 2 device should forward the multicast transmission only out ports to which receivers are connected and also out any ports that are connected to downstream multicast routers. This configuration requires a Layer 2 device to be able to determine the ports on which multicast routers and receivers for each separate (S,G) or (*,G) multicast group are located. To facilitate intelligent forwarding of multicast traffic on the LAN, Cisco Catalyst switches support two mechanisms:

- **IGMP snooping** — The switch listens in or "snoops" IGMP communications between receivers and multicast routers. This snooping enables the switch to determine which ports are connected to receivers for each multicast group and which ports are connected to multicast routers.
- **Cisco Group Management Protocol (CGMP)** — The switch communicates with multicasts routers, with multicast routers relaying group membership information to switches.

Reference: https://www.informit.com/library/content.aspx?b=CCNP_Studies_Switching&seqNum=59

QUESTION 70
Which technology can be used to prevent flooding of IPv6 multicast traffic on a switch?

A. IGMP snooping
B. IGMP filtering

C. MLD snooping
D. MLD filtering

Correct Answer: C
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
MLD snooping allows the switch to examine MLD packets and make forwarding decisions based on their content.
You can configure the switch to use MLD snooping in subnets that receive MLD queries from either MLD or the MLD snooping querier. MLD snooping constrains IPv6 multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward IPv6 multicast traffic only to those ports that want to receive it.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/snoopmld.html

QUESTION 71
Refer to the exhibit.

```
Switch#show interfaces fastEthernet0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dotlq
Operational Trunking Encapsulation: dotlq
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 3 (VLAN0003)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dotlq
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: 4-100
Pruning VLANs Enabled: 100-200
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Which VLANs are permitted to send frames out port FastEthernet0/1?

A. 100 - 200
B. 4 - 100
C. 1 and 4 - 100
D. 3 and 4 - 100

Correct Answer: D
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
Traffic on the native vlan does not get tagged as it crosses a trunk, so there is no dot1q tag in the first place to be filtered. And you don't need to allow the native vlan. But if we force to tag the native vlan (with the "switchport trunk native vlan tag" command) then if the native vlan is not in the "allowed vlan" list it will be dropped.

QUESTION 72
Which option is the default maximum age of the MAC address table?

A. 300 seconds
B. 500 seconds
C. 1200 seconds
D. 3600 seconds

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
To configure the maximum aging time for entries in the Layer 2 table, use the mac-address-table aging-time command in global configuration mode.

Syntax Description

seconds	MAC address table entry maximum age. Valid values are 0, and from 5 to 1000000 seconds. Aging time is counted from the last time that the switch detected the MAC address. The default value is 300 seconds.

Reference: http://www.cisco.com/c/en/us/td/docs/ios/lanswitch/command/reference/lsw_book/lsw_m1.html

QUESTION 73
Refer to the exhibit.

```
Switch# show spanning-tree vlan 1 detail

VLAN0001 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, sysid 1, address 0007.0e8f.04c0
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 8192, address 0007.4f1c.e847
  Root port is 65 (GigabitEthernet2/1), cost of root path is 119
  Topology change flag not set, detected flag not set
  Number of topology changes 1 last change occurred 00:00:35 ago
          from GigabitEthernet1/1
  Times:  hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0, aging 300
```

Which two statements about the output are true? (Choose two.)

A. 802.1D spanning tree is being used.
B. Setting the priority of this switch to 0 for VLAN 1 would cause it to become the new root.
C. The hello, max-age, and forward delay timers are not set to their default values.
D. Spanning-tree PortFast is enabled on GigabitEthernet1/1.

Correct Answer: AB
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
802.1D is the standard for Spanning tree, which is being used here. For priority, The priority order starts from 0 (yes, 0 is valid) and then increases in 4096.
0, 4096, 8192, 12288, …. Etc.
The lower the number is, the higher is the priority. Here we see that the current root has a priority of 8192, so configuring this with a priority of 0 will make it the new root.

QUESTION 74
Which statement is true about Fast Link Pulses in Ethernet?

A. They are used during collision detection.
B. They are used only if the media type is optical.
C. They are part of UniDirectional Link Detection.
D. They are used during autonegotiation.

Correct Answer: D
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
To make sure that your connection is operating properly, IEEE 802.3 Ethernet employs normal link pulses (NLPs), which are used for verifying link integrity in a 10BaseT system. This signaling gives you the link indication when you attach to the hub and is performed between two directly connected link interfaces (hub-to-station or station-to-station). NLPs are helpful in determining that a link has been established between devices, but they are not a good indicator that your cabling is free of problems.
An extension of NLPs is fast link pulses. These do not perform link tests, but instead are employed in the autonegotiation process to advertise a device's capabilities.

Reference: http://www.cisco.com/en/US/docs/internetworking/troubleshooting/guide/tr1904.html

QUESTION 75
Which statement is true regarding UDLD and STP timers?

A. The UDLD message timer should be two times the STP forward delay to prevent loops.
B. UDLD and STP are unrelated features, and there is no relation between the timers.
C. The timers need to be synced by using the spanning-tree udld-sync command.
D. The timers should be set in such a way that UDLD is detected before the STP forward delay expires.

Correct Answer: D

Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
UDLD is designed to be a helper for STP. Therefore, UDLD should be able to detect an unidirectional link before STP would unblock the port due to missed BPDUs. Thus, when you configure UDLD timers, make sure your values are set so that unidirectional link is detected before "STP MaxAge + 2xForwardDelay" expires.

Reference: http://blog.ine.com/tag/stp/

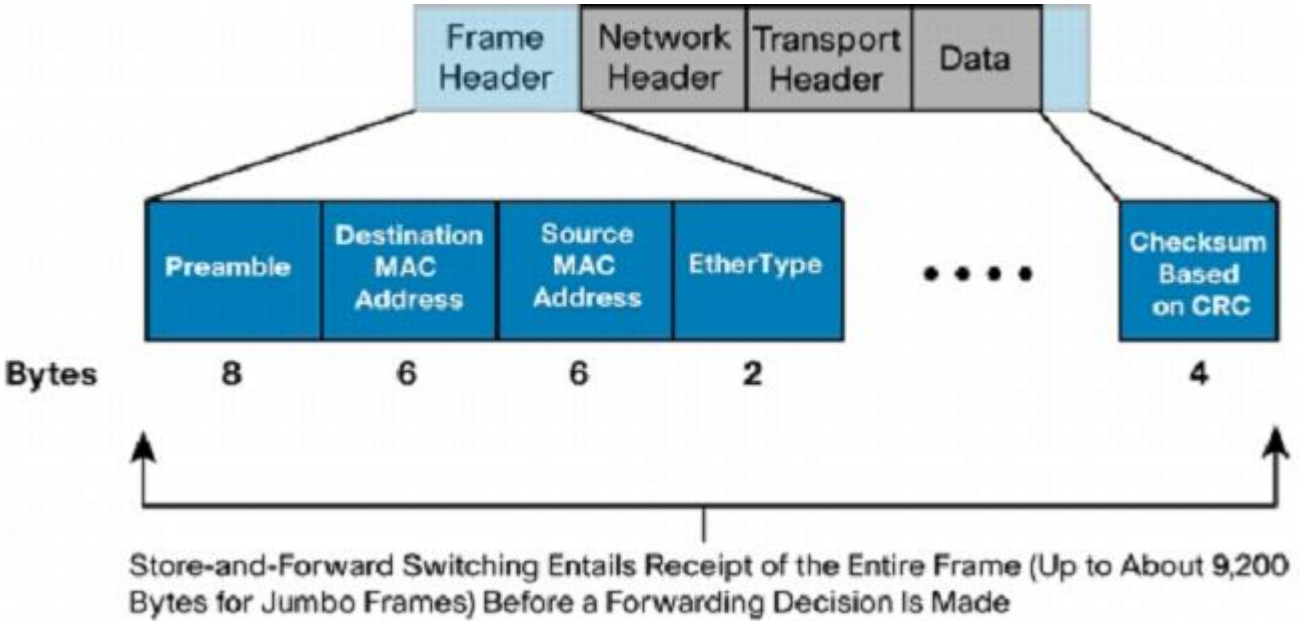
QUESTION 76
Which switching technology can be used to solve reliability problems in a switched network?

A. fragment-free mode
B. cut-through mode
C. check mode
D. store-and-forward mode

Correct Answer: D
Section: Layer 2 Technologies
Explanation

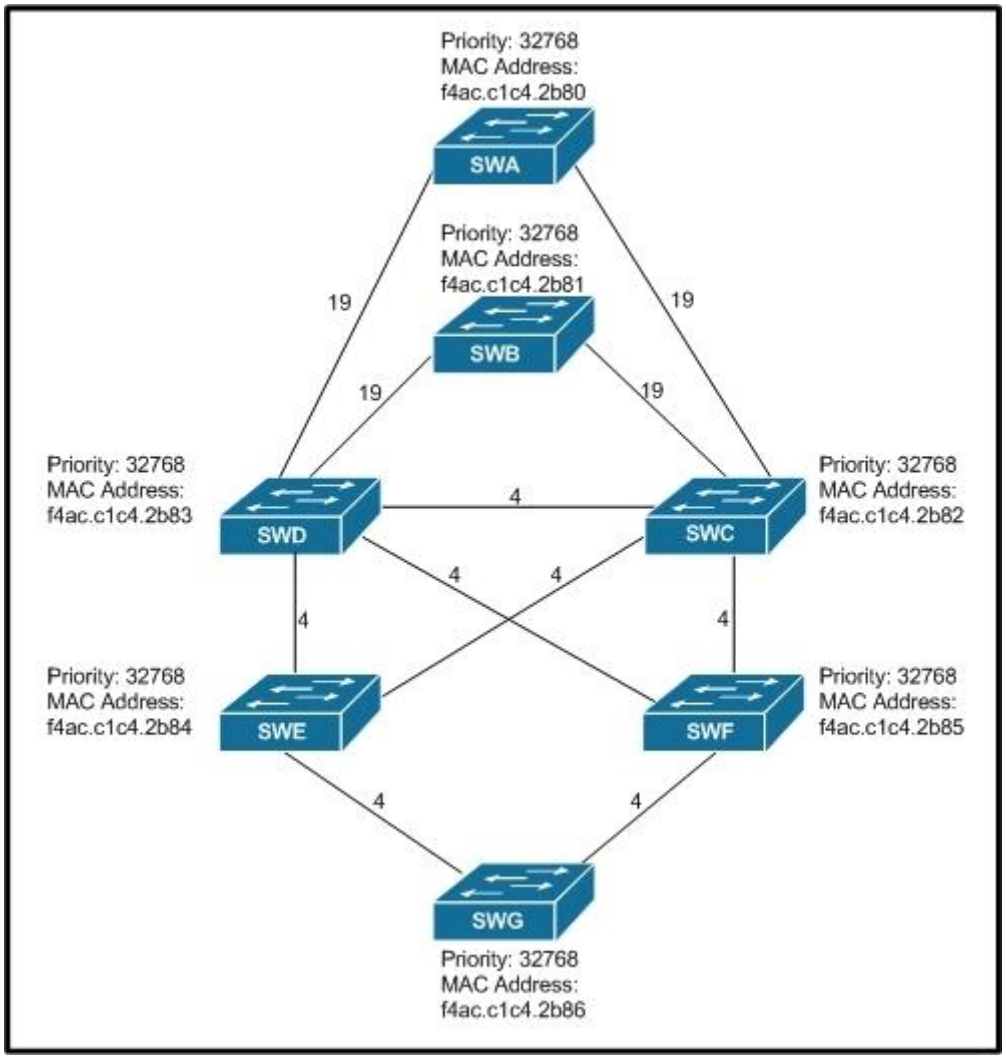
Explanation/Reference:
Explanation:
Characteristics of Store-and-Forward Ethernet Switching
This section provides an overview of the functions and features of store-and-forward Ethernet switches.
Error Checking
Figure 1 shows a store-and-forward switch receiving an Ethernet frame in its entirety. At the end of that frame, the switch will compare the last field of the datagram against its own frame-check-sequence (FCS) calculations, to help ensure that the packet is free of physical and data-link errors. The switch then performs the forwarding process.
Whereas a store-and-forward switch solves reliability issues by dropping invalid packets, cut-through devices forward them because they do not get a chance to evaluate the FCS before transmitting the packet.

Figure 1. Ethernet Frame Entering a Store-and-Forward Bridge or Switch (from Left to Right)



Reference: http://www.cisco.com/c/en/us/products/collateral/switches/nexus-5020-switch/white_paper_c11-465436.html

QUESTION 77
Refer to the exhibit.



All switches have default bridge priorities, and originate BPDUs with MAC addresses as indicated. The numbers shown are STP link metrics. Which two ports are in blocking state after STP converges? (Choose two.)

A. the port on switch SWD that connects to switch SWE
B. the port on switch SWF that connects to switch SWG
C. the port on switch SWD that connects to switch SWC

D. the port on switch SWB that connects to switch SWD

Correct Answer: CD
Section: Layer 2 Technologies
Explanation

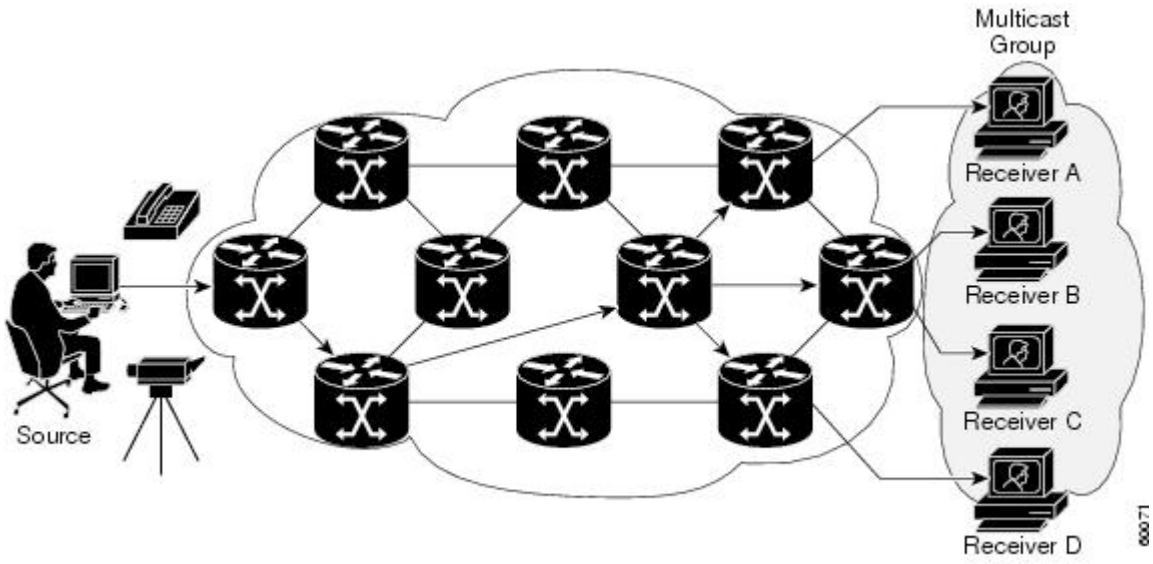
Explanation/Reference:
Explanation:
This is a scenario that wants you to demonstrate understanding of the Root switch and Root port election process. So, it's best to start with where the root switch will be and work down from there. It's setup nicely because the lowest MAC address switch starts at the top and then the lower priority/higher mac addresses move down the architecture. SWA wins the root election and of course all ports in SWA are forwarding. SWB introduces the possibility for a switching loop so it's important to understand which ports will be put into the blocking state. Since SWD is a higher MAC address it will end up with a blocked port connected to SWB to prevent a loop: and this is one of the correct answers. To prevent the possibility of another potential switching loop, SWD again ends up with the higher MAC address so blocking the link between D and C prevents a B/C/D switching loop.

QUESTION 78
Which statement is true about IGMP?

A. Multicast sources send IGMP messages to their first-hop router, which then generates a PIM join message that is then sent to the RP.
B. Multicast receivers send IGMP messages to their first-hop router, which then forwards the IGMP messages to the RP.
C. IGMP messages are encapsulated in PIM register messages and sent to the RP.
D. Multicast receivers send IGMP messages to signal their interest to receive traffic for specific multicast groups.

Correct Answer: D
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:



In the example shown above, the receivers (the designated multicast group) are interested in receiving the video data stream from the source. The receivers indicate their interest by sending an Internet Group Management Protocol (IGMP) host report to the routers in the network. The routers are then responsible for delivering the data from the source to the receivers.

Reference:
http://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/mcst_ovr.html

QUESTION 79
Which two statements are true about RSTP? (Choose two.)

A. By default, RTSP uses a separate TCN BPDU when interoperating with 802.1D switches.
B. By default, RTSP does not use a separate TCN BPDU when interoperating with 802.1D switches.
C. If a designated port receives an inferior BPDU, it immediately triggers a reconfiguration.
D. By default, RTSP uses the topology change TC flag.
E. If a port receives a superior BPDU, it immediately replies with its own information, and no reconfiguration is triggered.

Correct Answer: BD
Section: Layer 2 Technologies
Explanation

Explanation/Reference:

Explanation:
The RSTP does not have a separate topology change notification (TCN) BPDU. It uses the topology change (TC) flag to show the topology changes.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2950/software/release/12-1_9_ea1/configuration/guide/scg/swmstp.html

QUESTION 80
Refer to the exhibit.

```
switch#show spanning-tree detail

 MST0 is executing the mstp compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, sysid 0, address f4ac.c1c4.2b80
  Configured hello time 2, max age 20, forward delay 15, transmit hold-count 6
  Current root has priority 24576, address 0019.07aa.9ac0
  Root port is 56 (Port-channel1), cost of root path is 0
  Topology change flag not set, detected flag not set
  Number of topology changes 296 last change occurred 00:01:17 ago
          from GigabitEthernet0/15
```

Which two statements are true about the displayed STP state? (Choose two.)

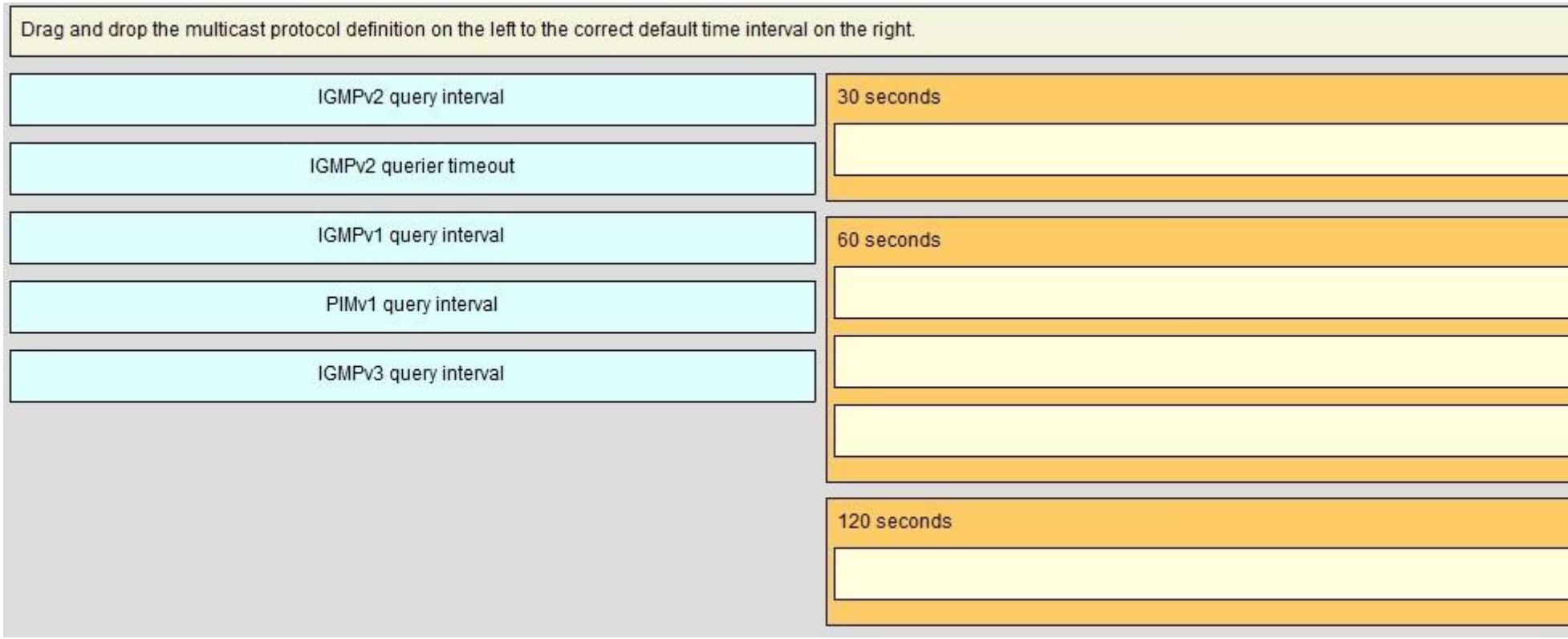
A. The STP version configured on the switch is IEEE 802.1w.
B. Port-channel 1 is flapping and the last flap occurred 1 minute and 17 seconds ago.
C. The switch does not have PortFast configured on Gi0/15.
D. BPDUs with the TCN bit set are transmitted over port channel 1.

Correct Answer: CD
Section: Layer 2 Technologies
Explanation

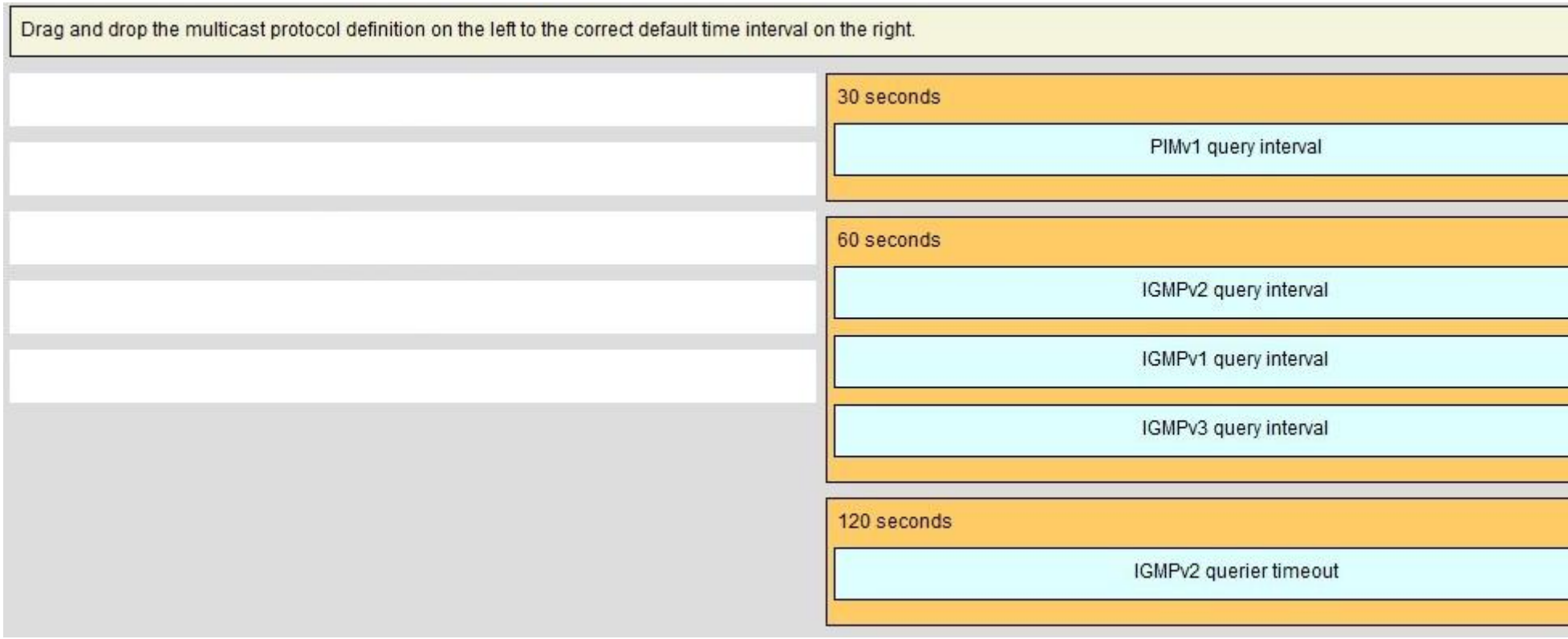
Explanation/Reference:
Explanation:
A port enabled with portfast will not send topology changes when a port goes up or down, but here we see that 296 TCN's were sent so we know that Gi 0/15 does not have portfast enabled.
TCN's are sent using BPDU's over the root port, which we see is port channel 1.

QUESTION 81
DRAG DROP
Drag and drop the multicast protocol definition on the left to the correct default time interval on the right.

Select and Place:



Correct Answer:



Section: Layer 2 Technologies
Explanation

Explanation/Reference:

QUESTION 82
When you migrate a network from PVST+ to rapid-PVST+, which two features become inactive? (Choose two.)

A. Root guard
B. Loop guard
C. UplinkFast
D. UDLD
E. BackboneFast

F. Bridge Assurance

Correct Answer: CE
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
It is good to know the UplinkFast and BackboneFast behavior before you start the migration process.
Here, the Access1 switch runs Cisco IOS. This output is taken before migration to the rapid-PVST+ mode:

```
Access1#show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    24586
             Address     0015.63f6.b700
             Cost        3019
             Port        107 (FastEthernet3/0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    49162  (priority 49152 sys-id-ext 10)
             Address     000f.f794.3d00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300
  Uplinkfast enabled

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa3/0/1          Root FWD 3019      128.107  P2p
Fa3/0/2          Altn BLK 3019      128.108  P2p


Access1#show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is enabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is enabled
UplinkFast                   is enabled
BackboneFast                 is enabled
Configured Pathcost method used is short
```

```
Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------

VLAN0010                      1         0        0          1          2
VLAN0020                      1         0        0          1          2
---------------------- -------- --------- -------- ---------- ----------
2 vlans                       2         0        0          2          4
This output is taken after the mode is changed to rapid-PVST+:

Access1#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    24586
             Address     0015.63f6.b700
             Cost        3019
             Port        107 (FastEthernet3/0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    49162  (priority 49152 sys-id-ext 10)
             Address     000f.f794.3d00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300
  UplinkFast enabled but inactive in rapid-pvst mode

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa3/0/1          Root FWD 3019      128.107  P2p
Fa3/0/2          Altn BLK 3019      128.108  P2p

Access1#show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: none
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is enabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is enabled
UplinkFast          is enabled but inactive in rapid-pvst mode
BackboneFast        is enabled but inactive in rapid-pvst mode
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
```

```
VLAN0010                         1         0         0          1          2
VLAN0020                         1         0         0          1          2
---------------------- -------- --------- -------- ---------- ----------
2 vlans                          2         0         0          2          4
```

You can see in the show spanning-tree summary command output that UplinkFast and BackboneFast are enabled, but are inactive in rapid-PVST mode.

Reference: http://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/72836-rapidpvst-mig-config.html#upback1

QUESTION 83
Which statement is true about MLD?

A. MLD v1 gives hosts the ability to receive multicast packets from specific source addresses.
B. All MLD messages are sent with a link-local IPv6 source address of FF02::D.
C. The multicast address field is cleared to zero when sending an MLD report message.
D. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link.

Correct Answer: D
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
IPv6 Multicast Listener Discovery (MLD) is used by IPv6 devices to discover multicast listeners (nodes that want to receive multicast packets destined for specific multicast addresses) on directly attached links. There are two versions of MLD. MLD version 1 is based on version 2 of the IGMP for IPv4, and MLD version 2 is based on version 3 of the IGMP for IPv4. IPv6 multicast for Cisco software uses both MLD version 2 and MLD version 1.

Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_lsm/configuration/xe-3s/imc-lsm-xe-3s-book/ipv6-mcast-mld-xe.html

QUESTION 84
Which statement is true about LLDP?

A. LLDP provides VTP support.
B. LLDP does not use a multicast address to communicate.
C. LLDP can indicate only the duplex setting of a link, and not the speed capabilities.
D. LLDP does not support native VLAN indication.

Correct Answer: D
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
Cisco Discovery Protocol Versus LLDP-MED TLV Comparison

TLV Function	LLDP TLV	Cisco Discovery Protocol TLV
Native VLAN support-Indicates the native VLAN	No	*Native VLAN TLV*

Reference: http://www.cisco.com/en/US/technologies/tk652/tk701/technologies_white_paper0900aecd804cd46d.html

QUESTION 85
Which statement is true when using a VLAN ID from the extended VLAN range (1006–4094)?

A. VLANs in the extended VLAN range can be used with VTPv2 in either client or server mode.
B. VLANs in the extended VLAN range can only be used as private VLANs.
C. STP is disabled by default on extended-range VLANs.
D. VLANs in the extended VLAN range cannot be pruned.

Correct Answer: D
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
Enabling VTP pruning on a VTP server enables pruning for the entire management domain. Making VLANs pruning-eligible or pruning-ineligible affects pruning eligibility for those VLANs on that device only (not on all switches in the VTP domain). VTP pruning takes effect several seconds after you enable it. VTP pruning does not prune traffic from VLANs that are pruning-ineligible. VLAN 1 and VLANs 1002 to 1005 are always pruning-ineligible; traffic from these VLANs cannot be pruned. Extended-range VLANs (VLAN IDs higher than 1005) are also pruning-ineligible.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3550/software/release/12-1_13_ea1/configuration/guide/3550scg/swvtp.html#wpxref48156

QUESTION 86
Which statement is true about trunking?

A. Cisco switches that run PVST+ do not transmit BPDUs on nonnative VLANs when using a dot1q trunk.
B. When removing VLAN 1 from a trunk, management traffic such as CDP is no longer passed in that VLAN.
C. DTP only supports autonegotiation on 802.1q and does not support autonegotiation for ISL.
D. DTP is a point-to-point protocol.

Correct Answer: D
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
Ethernet trunk interfaces support different trunking modes. You can set an interface as trunking or nontrunking or to negotiate trunking with the neighboring interface. To autonegotiate trunking, the interfaces must be in the same VTP domain.
Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP), which is a Point-to-Point Protocol. However, some internetworking devices might forward DTP frames improperly, which could cause misconfigurations.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2_55_se/configuration/guide/scg3750/swvlan.html

QUESTION 87
Which three statements are true about an EtherChannel? (Choose three.)

A. PAGP and LACP can be configured on the same switch if the switch is not in the same EtherChannel.
B. EtherChannel ports in suspended state can receive BPDUs but cannot send them.
C. An EtherChannel forms between trunks that are using different native VLANs.
D. LACP can operate in both half duplex and full duplex, if the duplex setting is the same on both ends.
E. Ports with different spanning-tree path costs can form an EtherChannel.

Correct Answer: ABE
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
Answer A. EtherChannel groups running PAgP and LACP can coexist on the same switch or on different switches in the stack. Individual EtherChannel groups can run either PAgP or LACP, but they cannot interoperate.

Answer B:

EtherChannel Member Port States

Port States	Description
bundled	The port is part of an EtherChannel and can send and receive BPDUs and data traffic.
suspended	The port is not part of an EtherChannel. The port can receive BPDUs but cannot send them. Data traffic is blocked.
standalone	The port is not bundled in an EtherChannel. The port functions as a standalone data port. The port can send and receive BPDUs and data traffic.

Answer E. Ports with different spanning-tree path costs can form an EtherChannel if they are otherwise compatibly configured. Setting different spanning-tree path costs does not, by itself, make ports incompatible for the formation of an EtherChannel.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0_2_EX/layer2/configuration_guide/b_lay2_152ex_2960-x_cg/b_lay2_152ex_2960-x_cg_chapter_010.html

QUESTION 88
Which technology can be affected when switches are used that do not support jumbo frames?

A. 802.1x
B. BFD
C. OSPFv3
D. 802.1q

Correct Answer: D
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
The 802.1Q tag is 4 bytes. Therefore, the resulting Ethernet frame can be as large as 1522 bytes. If jumbo frames are not supported, then typically the MTU on an Ethernet link needs to be lowered to 1496 to support this extra 802.1Q tag.

QUESTION 89
Which statement describes the native VLAN concept in an ISL trunk?

A. It is the VLAN ID that is assigned to untagged packets.
B. It is the VLAN with highest priority.
C. It is the default VLAN for a trunk.
D. There is no native VLAN concept in an ISL trunk.

Correct Answer: D
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
ISL has no native VLAN concept because it places the entire Ethernet frame in the payload of an ISL frame. Native VLANs is an 802.1Q specific concept

QUESTION 90
Which protocol is the encapsulating protocol for mtrace packets?

A. ICMP
B. IGMP
C. PIM
D. GRE

Correct Answer: B
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
“mtrace” is a diagnostic tool to trace the multicast path from a specified source to a destination for a multicast group. It runs over IGMP protocol. Mtrace uses any information available to it to determine a previous hop to forward the trace towards the source.

Reference: http://www.brocade.com/downloads/documents/html_product_manuals/NI_05500c_MULTICAST/wwhelp/wwhimpl/common/html/wwhelp.htm#context=NI_MCAST&file=IP_Multicast.3.04.html

QUESTION 91
Assume that the following MAC addresses are used for the bridge ID MAC address by four different switches in a network. Which switch will be elected as the spanning-tree root bridge?

A. SwitchA uses MAC 1000.AA-AA-AA-AA-AA-AA.
B. SwitchB uses MAC 2000.BB-BB-BB-BB-BB-BB.
C. SwitchC uses MAC 3000.CC-CC-CC-CC-CC-CC.
D. SwitchD uses MAC 4000.DD-DD-DD-DD-DD-DD.

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
The switch with the highest switch priority (the lowest numerical priority value) is elected as the root switch. If all switches are configured with the default priority (32768), the switch with the lowest MAC address in the VLAN becomes the root switch.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_53_se/configuration/guide/2960scg/swstp.html

QUESTION 92
What is the destination MAC address of a BPDU frame?

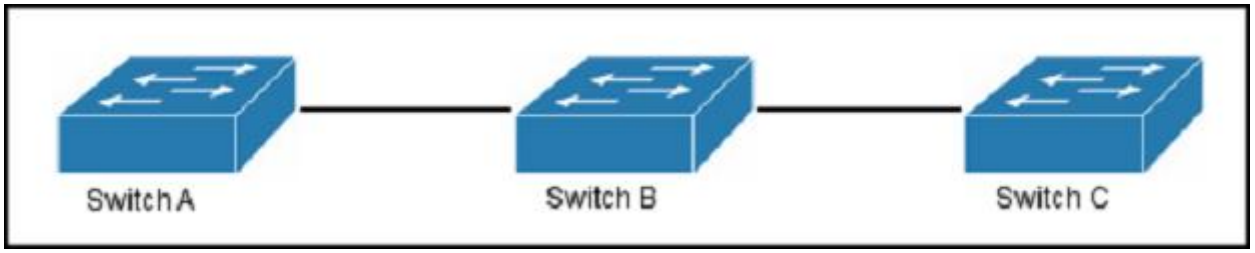
A. 01-80-C2-00-00-00
B. 01-00-5E-00-00-00
C. FF-FF-FF-FF-FF-FF
D. 01-80-C6-00-00-01

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
The root-bridge election process begins by having every switch in the domain believe it is the root and claiming it throughout the network by means of Bridge Protocol Data Units (BPDU). BPDUs are Layer 2 frames multicast to a well-known MAC address in case of IEEE STP (01-80-C2-00-00-00) or vendor-assigned addresses, in other cases.

Reference: http://www.ciscopress.com/articles/article.asp?p=1016582

QUESTION 93
Refer to the exhibit.



All switches are Cisco switches. Assume that Cisco Discovery Protocol is enabled only on switches A and C.

Which information is returned when you issue the command show cdp neighbors on switch C?

A. a limited amount of information about switch B
B. no neighbor details will be returned
C. neighbor details for switch B
D. neighbor details for switch A
E. neighbor details for switch C

Correct Answer: B
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
CDP is used to discover information on directly connected neighbors only, so in this case SwitchC would only be able to obtain CDP information from SwitchB. However, since SwitchB is not running CDP then no neighbor information will be seen on SwitchC. Same goes for Switch A also in this topology.

QUESTION 94
Which two features are supported when Cisco HDLC is implemented? (Choose two.)

A. error recovery
B. error detection
C. asynchronous links
D. multiple protocols

Correct Answer: BD

Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
HDLC's frame check sequence (FCS) is a 16-bit CRC-CCITT or a 32-bit CRC-32 computed over the Address, Control, and Information fields. It provides a means by which the receiver can detect errors that may have been induced during the transmission of the frame, such as lost bits, flipped bits, and extraneous bits.
Cisco's HDLC contains a proprietary field that is used to support multiple protocols.

Reference: http://en.wikipedia.org/wiki/High-Level_Data_Link_Control

QUESTION 95
Refer to the exhibit.

```
R1
interface Serial0/0
   encapsulation ppp
   ppp pap sent-username SITE2 password cisco

R2
username SITE2 password cisco
   interface Serial0/0
   encapsulation ppp
   ppp authentication pap
```

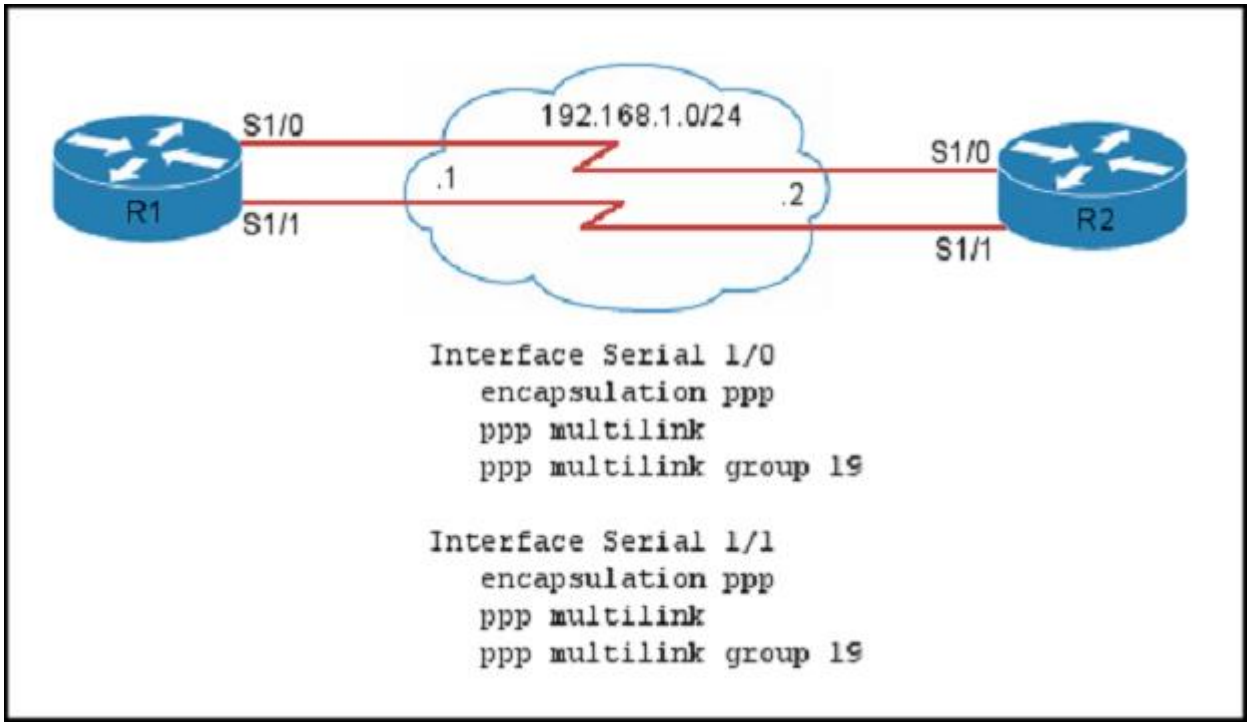
With these configurations for R1 and R2, which statement about PPP authentication is true?

A. Authentication fails because R1 is missing a username and password.
B. R2 responds with the correct authentication credentials.
C. R2 requires authentication from R1.
D. R1 requires authentication from R2.

Correct Answer: C
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
Only R2 is configured with the “PPP authentication PAP” command so it requires authentication from R1, but R1 does not require authentication from R2.

QUESTION 96
Refer to the exhibit.



You must complete the configuration on R1 so that a maximum of three links can be used and fragmentation is supported.

Which additional configuration accomplishes this task?

A. interface Multilink19
ip address 192.168.1.1 255.255.255.0
ppp multilink
ppp multilink group 19
ppp multilink links minimum 1
ppp multilink links maximum 3

ppp multilink interleave

B. interface Multilink19
ip address 192.168.1.1 255.255.255.0
ppp multilink
ppp multilink group 19
ppp multilink links maximum 3
ppp multilink fragment delay 20

C. interface Multilink19
ip address 192.168.1.1 255.255.255.0
ppp multilink
ppp multilink group 19
ppp multilink links maximum 3
ppp multilink fragment delay 20
ppp multilink interleave

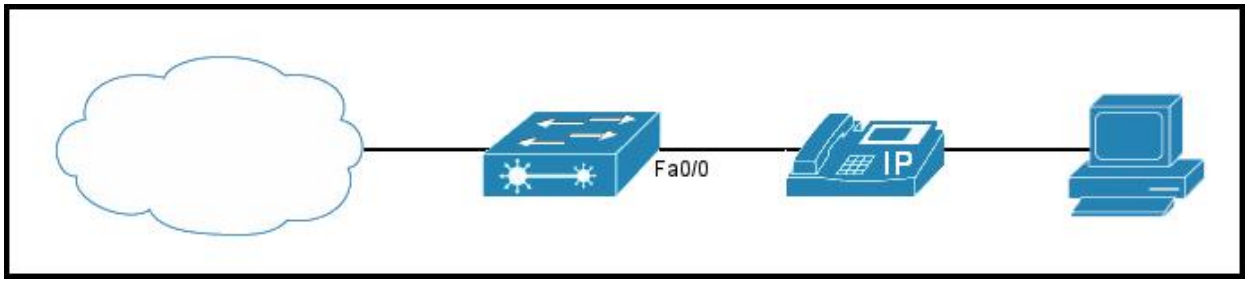
D. interface Multilink19
ip address 192.168.1.1 255.255.255.252
ppp multilink
ppp multilink group 19
ppp multilink links maximum 3
ppp multilink interleave

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
The “ppp multilink interleave” command is needed to enable link fragmentation and Interleaving (LFI). The Cisco IOS Link Fragmentation and Interleaving (LFI) feature uses Multilink PPP (MLP). MLP provides a method of splitting, recombining, and sequencing datagrams across multiple logical data links. MLP allows packets to be fragmented and the fragments to be sent at the same time over multiple point-to-point links to the same remote address.
ppp multilink links maximum
To limit the maximum number of links that Multilink PPP (MLP) can dial for dynamic allocation, use the **ppp multilink links maximum** command in interface configuration mode.

Reference: http://www.cisco.com/c/en/us/td/docs/ios/12_2/qos/configuration/guide/fqos_c/qcflfi.html

QUESTION 97
Refer to the exhibit.



Which statement about configuring the switch to manage traffic is true?

A. The switchport priority extend cos command on interface FastEthernet0/0 prevents traffic to and from the PC from taking advantage of the high-priority data queue that is assigned to the IP phone.
B. The switchport priority extend cos command on interface FastEthernet0/0 enables traffic to and from the PC to use the high priority data queue that is assigned to the IP phone.
C. When the switch is configured to trust the CoS label of incoming traffic, the trusted boundary feature is disabled automatically.
D. The mls qos cos override command on interface FastEthernet0/0 configures the port to trust the CoS label of traffic to and from the PC.

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
In some situations, you can prevent a PC connected to the Cisco IP Phone from taking advantage of a high-priority data queue. You can use the switchport priority extend cos interface configuration command to configure the telephone through the switch CLI to override the priority of the traffic received from the PC.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2950/software/release/12-1_22_ea2/configuration/guide/2950scg/swqos.html

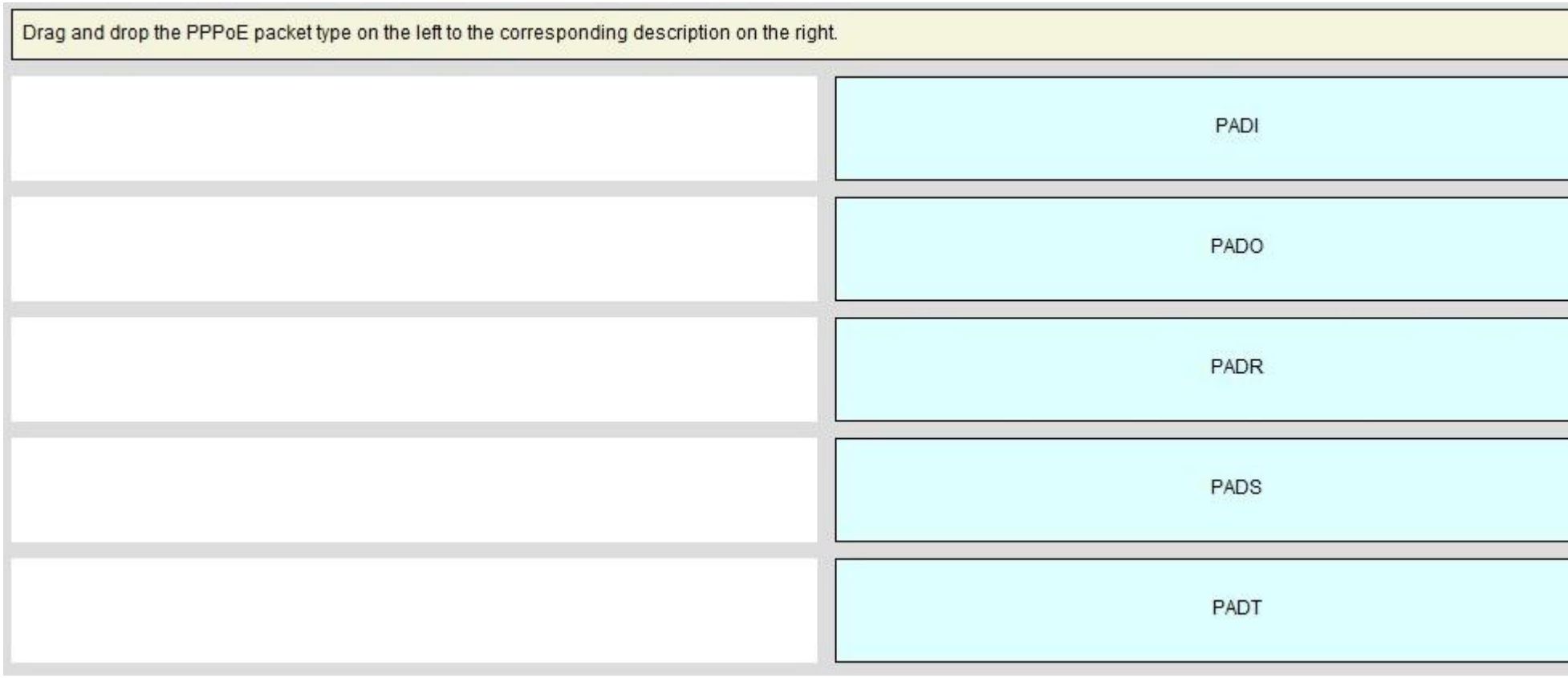
QUESTION 98
DRAG DROP
Drag and drop the PPPoE packet type on the left to the corresponding description on the right.

Select and Place:

Drag and drop the PPPoE packet type on the left to the corresponding description on the right.

PADR	A packet that is sent with the destination_addr set to the broadcast address. The p indicates the type of service requested.
PADT	A packet that is sent with the destination_addr set to the unicast address of the PF client. The packet contains an offer for the client.
PADO	A packet that is sent from the PPPoE client with the destination_addr set to the ch access concentrator. The packet contains a session request from the client.
PADI	A packet that is sent as confirmation to the client. The packet contains the unique PPPoE session ID.
PADS	A packet that is sent to terminate the PPPoE session.

Correct Answer:



Section: Layer 2 Technologies
Explanation

Explanation/Reference:

QUESTION 99
What is the destination multicast MAC address for BPDUs on the native VLAN, for a switch that is running 802.1D?

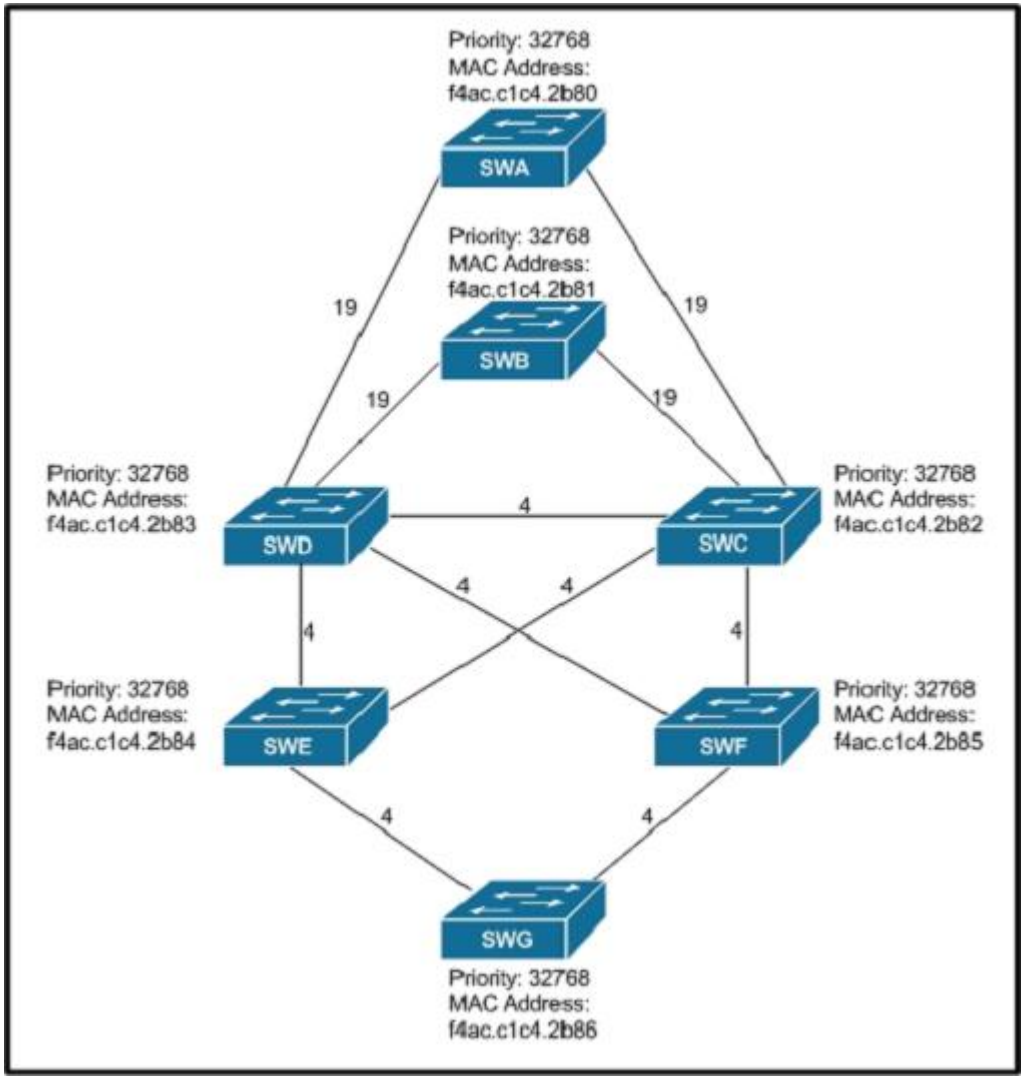
A. 0185. C400. 0000
B. 0100.0CCC.CCCC
C. 0100.0CCC.CCCD
D. 0180.C200.0000

Correct Answer: D
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
If the native vlan is 1:
A STP BPDU for VLAN 1 will be sent untagged to MAC 0180.c200.0000 (this is the common spanning tree)
A PVST+ BPDU for VLAN 1 will be sent untagged to MAC 0100.0ccc.cccd
A PVST+ BPDU for all other vlans will be sent with a 802.1Q tag to MAC 0100.0ccc.cccd (with a PVID = to the VLAN)

If the native vlan is not 1:
A STP BPDU for VLAN 1 will be sent untagged (on the native vlan) to MAC 0180.c200.0000 (this is the common spanning tree)
A PVST+ BPDU for VLAN1 will be sent with a 802.1Q tag to MAC 0100.0ccc.cccd (with a PVID=1)
A PVST+ BPDU for the native vlan will be sent untagged to MAC 0100.0ccc.cccd (with a PVID=native vlan)
A PVST+ BPDU for all other vlans will be sent with a 802.1Q tag to MAC 0100.0ccc.cccd (with a PVID = to the VLAN)

QUESTION 100
Refer to the exhibit.



All switches have default bridge priorities, and originate BPDUs with MAC addresses as indicated. The numbers shown are STP link metrics.

After STP converges, you discover that traffic from switch SWG toward switch SWD takes a less optimal path. What can you do to optimize the STP tree in this switched network?

A. Change the priority of switch SWA to a lower value than the default value.

B. Change the priority of switch SWB to a higher value than the default value.
C. Change the priority of switch SWG to a higher value than the default value.
D. Change the priority of switch SWD to a lower value than the default value.

Correct Answer: D
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
In this topology, we see that all port paths and priorities are the same, so the lowest MAC address will be used to determine the best STP path. From SWG, SWE will be chosen as the next switch in the path because it has a lower MAC address than SWF. From SWE, traffic will go to SWC because it has a lower MAC address, and then to SWD, instead of going from SWE directly to SWD. If we lower the priority of SWD (lower means better with STP) then traffic will be sent directly to SWD.

QUESTION 101
Which three statements are true about VSS? (Choose three.)

A. VSS separates the control planes of the active and the standby chassis.
B. Configuration changes can be made on both active and standby chassis.
C. When the VSS active chassis recovers after a failure, it initiates a switchover and takes on the active role again.
D. VSS unifies the control planes of the active and the standby chassis.
E. HSRP configuration is not required to run VSS.
F. The VSS standby chassis monitors the VSS active chassis using the VSL.

Correct Answer: DEF
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
VSS operates on a unified control plane with a distributed forwarding architecture in which the active supervisor (or switch) is responsible for actively participating with the rest of the network and for managing and maintaining control plane information.
VSS actually removes the need for a next-hop redundancy protocol like HSRP or VRRP. These first-hop redundancy protocols are usually heavily tied to a fast-converging routing protocol like EIGRP, and still require that each device maintain its own control plane.
The standby chassis monitors the active chassis using the VSL. If it detects failure, the standby chassis initiates a switchover and takes on the active role. When the failed chassis recovers, it takes on the standby role.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup2T/15_1_sy_swcg_2T/virtual_switching_systems.pdf