QUESTION 61
Which TCP setting is tuned to minimize the risk of fragmentation on a GRE/IP tunnel?

A. MTU
B. Window size
C. MRU
D. MSS

Answer: D
Explanation:
The TCP Maximum Segment Size (TCP MSS) defines the maximum amount of data that a host is willing to accept in a single TCP/IP datagram. This TCP/IP datagram might be fragmented at the IP layer. The MSS value is sent as a TCP header option only in TCP SYN segments. Each side of a TCP connection reports its MSS value to the other side. Contrary to popular belief, the MSS value is not negotiated between hosts. The sending host is required to limit the size of data in a single TCP segment to a value less than or equal to the MSS reported by the receiving host.
TCP MSS takes care of fragmentation at the two endpoints of a TCP connection, but it does not handle the case where there is a smaller MTU link in the middle between these two endpoints. PMTUD was developed in order to avoid fragmentation in the path between the endpoints. It is used to dynamically determine the lowest MTU along the path from a packet's source to its destination.
Reference: http://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/25885-pmtud-ipfrag.html (there is some examples of how TCP MSS avoids IP Fragmentation in this link but it is too long so if you want to read please visit this link)
Note: IP fragmentation involves breaking a datagram into a number of pieces that can be reassembled later.

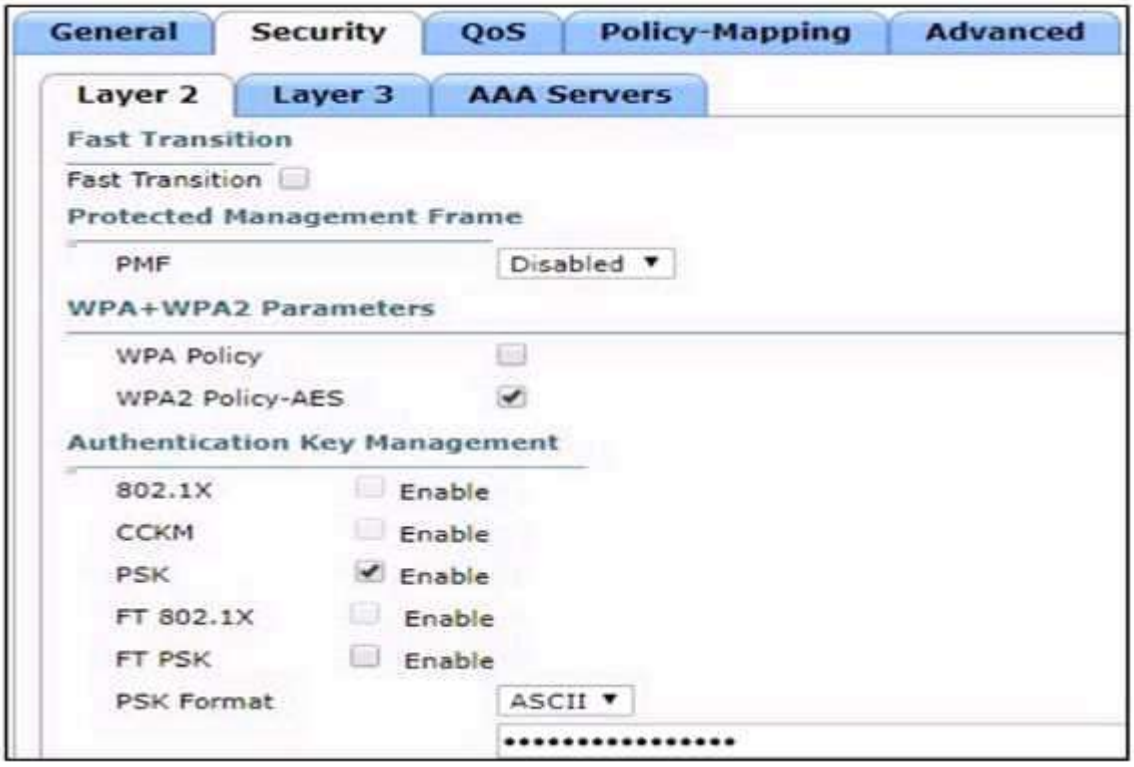
QUESTION 62
Which statement about an RSPAN session configuration is true?

A. A fitter mutt be configured for RSPAN Regions
B. Only one session can be configured at a time
C. A special VLAN type must be used as the RSPAN destination.
D. Only incoming traffic can be monitored

Answer: C
Explanation:
The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches -> This VLAN can be considered a special VLAN type -> Answer C is correct.
Reference: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swspan.html

We can configure multiple RSPAN sessions on a switch at a time, then continue configuring multiple RSPAN sessions on the other switch without any problem -> Answer B is not correct.
This is how to configure Remote SPAN (RSPAN) feature on two switches. Traffic on FastEthernet0/1 of Switch 1 will be sent to Fa0/10 of Switch2 via VLAN 40.
+ Configure on both switches
Switch1,2(config)#vlan 40
Switch1,2(config-vlan)#remote-span
+ Configure on Switch1
Switch1(config)# monitor session 1 source interface FastEthernet 0/1
Switch1(config)# monitor session 1 destination remote vlan 40
+ Configure on Switch2
Switch2(config)#monitor session 5 source remote vlan 40
Switch2(config)# monitor session 5 destination interface FastEthernet 0/10

QUESTION 63
Refer to the exhibit. Based on the configuration in this WLAN security setting.
Which method can a client use to authenticate to the network?



A. text string
B. username and password
C. certificate
D. RADIUS token

Answer: A

QUESTION 64
Which two pieces of information are necessary to compute SNR? (Choose two.)

A. EIRP
B. noise floor
C. antenna gain
D. RSSI

E. transmit power

Answer: BD
Explanation:
Signal to Noise Ratio (SNR) is defined as the ratio of the transmitted power from the AP to the ambient (noise floor) energy present. To calculate the SNR value, we add the Signal Value to the Noise Value to get the SNR ratio. A positive value of the SNR ratio is always better.
Here is an example to tie together this information to come up with a very simple RF plan calculator for a single AP and a single client.
+ Access Point Power = 20 dBm
+ 50 foot antenna cable = – 3.35 dB Loss
+ Signal attenuation due to glass wall with metal frame = -6 dB
+ External Access Point Antenna = + 5.5 dBi gain
+ RSSI at WLAN Client = -75 dBm at 100ft from the AP
+ Noise level detected by WLAN Client = -85 dBm at 100ft from the AP
Based on the above, we can calculate the following information.
+ EIRP of the AP at source = 20 – 3.35 + 5.5 = 22.15 dBm
+ Transmit power as signal passes through glass wall = 22.15 – 6 = 16.15 dBm
+ SNR at Client = -75 + -85 = 10 dBm (difference between Signal and Noise)
Reference:
https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/CMX/CMX_RFFund.html
Receive Signal Strength Indicator (RSSI) is a measurement of how well your device can hear a signal from an access point or router. It's a value that is useful for determining if you have enough signal to get a good wireless connection.
EIRP tells you what's the actual transmit power of the antenna in milliwatts.
dBm is an abbreviation for "decibels relative to one milliwatt," where one milliwatt (1 mW) equals 1/1000 of a watt. It follows the same scale as dB. Therefore 0 dBm = 1 mW, 30 dBm = 1 W, and -20 dBm = 0.01 mW

QUESTION 65
Refer to the exhibit. The WLC administrator sees that the controller to which a roaming client associates has Mobility Role Anchor configured under Clients > Detail.
Which type of roaming is supported?

A. Indirect
B. Layer 3 intercontroller
C. Layer 2 intercontroller
D. Intercontroller

Answer: B
Explanation:
If the clients roam between APs registered to different controllers and the client WLAN on the two controllers is on different subnet, then it is called inter-controller L3 roam.
In this situation as well controllers exchange mobility messages. Client database entry change is completely different that to L2 roam(instead of move, it will copy). In this situation the original controller marks the client entry as “Anchor” where as new controller marks the client entry as “Foreign“.The two controllers now referred to as “Anchor controller” & “Foreign Controller” respectively. Client will keep the original IP address & that is the real advantage.
Note: Inter-Controller (normally layer 2) roaming occurs when a client roam between two APs registered to two different controllers, where each controller has an interface in the client subnet.

QUESTION 66
What is the difference between the enable password and the enable secret password when password encryption is enable on an IOS device?

A. The enable password is encrypted with a stronger encryption method.
B. There is no difference and both passwords are encrypted identically.
C. The enable password cannot be decrypted.
D. The enable secret password is protected via stronger cryptography mechanisms.

Answer: D
Explanation:
The “enable secret” password is always encrypted (independent of the “service password-encryption” command) using MD5 hash algorithm. The “enable password” does not encrypt the password and can be view in clear text in the running-config. In order to encrypt the “enable password”, use the “service password-encryption” command. This command will encrypt the passwords by using the Vigenere encryption algorithm. Unfortunately, the Vigenere encryption method is cryptographically weak and trivial to reverse.
The MD5 hash is a stronger algorithm than Vigenere so answer D is correct.

QUESTION 67
When reason could cause an OSPF neighborship to be in the EXSTART/EXCHANGE state?

A. Mismatched OSPF network type
B. Mismatched areas
C. Mismatched MTU size
D. Mismatched OSPF link costs

Answer: C
Explanation:
When OSPF adjacency is formed, a router goes through several state changes before it becomes fully adjacent with its neighbor. The states are Down -> Attempt (optional) -> Init -> 2-Way -> Exstart -> Exchange -> Loading -> Full. Short descriptions about these states are listed below:
Down: no information (hellos) has been received from this neighbor.
Attempt: only valid for manually configured neighbors in an NBMA environment. In Attempt state, the router sends unicast hello packets every poll interval to the neighbor, from which hellos have not been received within the dead interval.
Init: specifies that the router has received a hello packet from its neighbor, but the receiving router’s ID was not included in the hello packet
2-Way: indicates bi-directional communication has been established between two routers.
Exstart: Once the DR and BDR are elected, the actual process of exchanging link state information can start between the routers and their DR and BDR.
Exchange: OSPF routers exchange database descriptor (DBD) packets
Loading: In this state, the actual exchange of link state information occurs
Full: routers are fully adjacent with each other
(Reference: http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080093f0e.shtml)
Neighbors Stuck in Exstart/Exchange State

The problem occurs most frequently when attempting to run OSPF between a Cisco router and another vendor's router. The problem occurs when the maximum transmission unit (MTU) settings for neighboring router interfaces don't match. If the router with the higher MTU sends a packet larger that the MTU set on the neighboring router, the neighboring router ignores the packet.

QUESTION 68
Which two statements about VRF-lite are true? (Choose two)

A. It can increase the packet switching rate.
B. It supports most routing protocols, including EIGRP, ISIS, and OSPF.
C. It supports MPLS-VRF label exchange and labeled packets.
D. It should be used when a customer's router is connected to an ISP over OSPF.
E. It can support multiple customers on a single switch.

Answer: BE
Explanation:
In VRF-Lite, Route distinguisher (RD) identifies the customer routing table and allows customers to be assigned overlapping addresses. Therefore it can support multiple customers with overlapping addresses -> Answer E is correct.
VRFs are commonly used for MPLS deployments, when we use VRFs without MPLS then we call it VRF lite -> Answer C is not correct.
VRF-Lite supports most populr routing protocols: BGP, OSPF, EIGRP, RIP, and static routing -> Answer B is correct.

QUESTION 69
Which statement about the default QoS configuration on a Cisco switch is true?

A. All traffic is sent through four egress queues.
B. Port trust is enabled.
C. The Port Cos value is 0.
D. The Cos value of each tagged packet is modified.

Answer: C

QUESTION 70
Which IPv6 migration method relies on dynamic tunnels that use the 2002::/16 reserved address space?

A. 6RD
B. 6to4
C. ISATAP
D. GRE

Answer: B
Explanation:
6to4 tunnel is a technique which relies on reserved address space 2002::/16 (you must remember this range). These tunnels determine the appropriate destination address by combining the IPv6 prefix with the globally unique destination 6to4 border router's IPv4 address, beginning with the 2002::/16 prefix, in this format:
2002:border-router-IPv4-address::/48
For example, if the border-router-IPv4-address is 64.101.64.1, the tunnel interface will have an IPv6 prefix of 2002:4065:4001:1::/64, where 4065:4001 is the hexadecimal equivalent of 64.101.64.1. This technique allows IPv6 sites to communicate with each other over the IPv4 network without explicit tunnel setup but we have to implement it on all routers on the path.

QUESTION 71
How are the Cisco Express Forwarding table and the FIB related to each other?

A. The FIB is used to populate the Cisco Express Forwarding table.
B. The Cisco Express Forwarding table allows route lookups to be forwarded to the route processor

for processing before they are

C. There can be only one FIB but multiple Cisco Express Forwarding tables on IOS devices.
D. Cisco Express Forwarding uses a FIB to make IP destination prefix-based switching decisions.

Answer: D
Explanation:
The Forwarding Information Base (FIB) table – CEF uses a FIB to make IP destination prefix-based switching decisions. The FIB is conceptually similar to a routing table or information base. It maintains a mirror image of the forwarding information contained in the IP routing table. When routing or topology changes occur in the network, the IP routing table is updated, and these changes are reflected in the FIB. The FIB maintains next-hop address information based on the information in the IP routing table.
Reference: https://www.cisco.com/c/en/us/support/docs/routers/12000-series-routers/47321-ciscoef.html