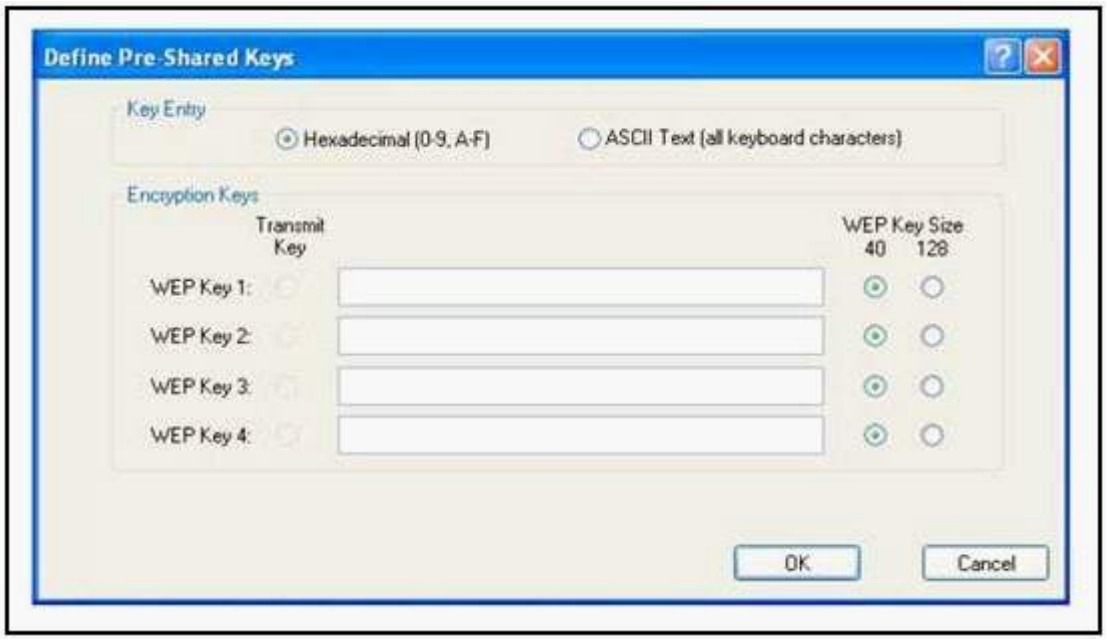
Exam: 642-812

Title: Building Converged Cisco Multilayer Switched Networks (BCMSN)

Version: Demo

QUESTION NO: 1
Refer to the exhibit. What should be taken into consideration when using the Cisco Aironet Desktop Utility (ADU) to configure the static WEP keys on the wireless client adapter?

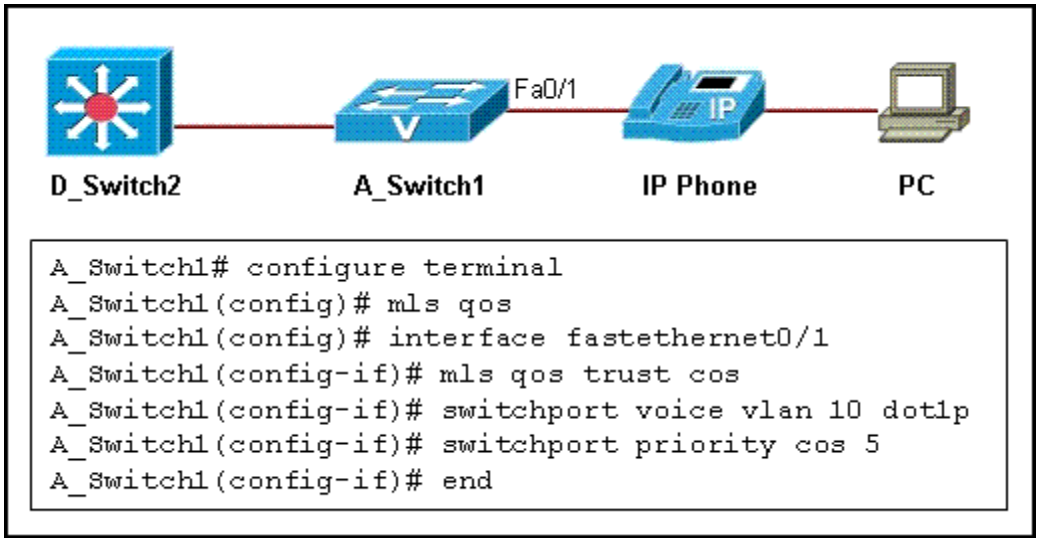


A. The client adapter WEP key should be generated by the authentication server and forwarded to the client adapter before the client adapter can establish communication with the wireless network.
B. The client adapter WEP key should be generated by the AP and forwarded to the client adapter before the client adapter can establish communication with the wireless network.
C. In infrastructure mode the client adapter WEP key must match the WEP key used by the access point. In ad hoc mode all client WEP keys within the wireless network must match each other.
D. Before the client adapter WEP key is generated, all wireless infrastructure devices (such as access points, servers, etc.) must be properly configured for LEAP authentication.

Answer: C

Explanation:
Your client adapter's WEP key must match the WEP key used by the access point (in infrastructure mode) or clients (in ad hoc mode) with which you are planning to communicate.
Reference:
http://www.cisco.com/en/US/docs/wireless/wlan_adapter/cb21ag/user/3.5/configuration/guide/winapekh.html

QUESTION NO: 2
Refer to the exhibit. On basis of the configuration that is provided, where will the trust boundary be established in this network?




```
A_Switch1# configure terminal
A_Switch1(config)# mls qos
A_Switch1(config)# interface fastethernet0/1
A_Switch1(config-if)# mls qos trust cos
A_Switch1(config-if)# switchport voice vlan 10 dot1p
A_Switch1(config-if)# switchport priority cos 5
A_Switch1(config-if)# end
```

A. at the PC
B. at the access switch
C. at the IP phone
D. at the distribution switch

Answer: B

QUESTION NO: 3
Which statement is true about the data traffic between the access point and controller?

A. The data traffic between the access point and controller is not encrypted.
B. The data traffic is encrypted with AES.
C. The data traffic is encapsulated with LWAPP.
D. The data traffic is switched at the access point before being sent to the WLAN controller where VLAN tagging and QoS are applied.

Answer: C

NO EXPANATION.

QUESTION NO: 4
Which two statements are true about a switched virtual interface (SVI)? (Choose two.)

A. An SVI is created by entering the no switchport command in interface configuration mode.
B. SVI is another name for a routed port.
C. Multiple SVIs can be associated with a VLAN.

D. An SVI is created for the default VLAN (VLAN1) to permit remote switch administration by default.
E. An SVI provides a default gateway for a VLAN.

Answer: D,E

Explanation:
On a multilayer switch, you can also enable Layer 3 functionality for an entire VLAN on the switch. This allows a network address to be assigned to a logical interface—that of the VLAN itself. This is useful when the switch has many ports assigned to a common VLAN, and routing is needed in and out of that VLAN.
The logical Layer 3 interface is known as an *SVI*. However, when it is configured, it uses the much more intuitive interface name **vlan** *vlan-id*, as if the VLAN itself is a physical interface. First, define or identify the VLAN interface, and then assign any Layer 3 functionality to it with the following configuration commands:

Switch(config)# interface vlan vlan-id
Switch(config-if)# ip address ip-address mask [secondary]
The VLAN must be defined and active on the switch before the SVI can be used. Make sure the new VLAN interface is also enabled with the **no shutdown** interface configuration command.

QUESTION NO: 5
Refer to the exhibit. What is the configuration an example of?

```
track 1 interface POS 5/0 ip routing
track 2 interface POS 6/0 ip routing
interface fastethernet 0/0
glpb 10 weighting 110 lower 95 upper 105
glbp 10 weighting track 1 decrement 10
glbp 10 weighting track 2 decrement 10
glbp 10 forwarder preempt delay minimum 60
```

A. GLBP weighting
B. default AVF and AVG configuration
C. GLBP MD5 authentication
D. GLBP text authentication
E. GLBP timer manipulation

Answer: A

Explanation:
Configuring GLBP Weighting: Example
In the following example, Router A, shown in Figure 1, is configured to track the IP routing state of the POS interface 5/0 and 6/0, an initial GLBP weighting with upper and lower thresholds is

set, and a weighting decrement value of 10 is set. If POS interface 5/0 and 6/0 goes down, the weighting value of the router is reduced.
track 1 interface POS 5/0 ip routing
track 2 interface POS 6/0 ip routing
interface fastethernet 0/0
 glbp 10 weighting 110 lower 95 upper 105
 glbp 10 weighting track 1 decrement 10
 glbp 10 weighting track 2 decrement 10
 glbp 10 forwarder preempt delay minimum 60
Reference:
http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_glbp_ps6922_TSD_Products_Configuration_Guide_Chapter.html#wp1055542

QUESTION NO: 6
Which issue or set of issues does the Lightweight Access Point Protocol (LWAPP) address?

A. distributed approach to authentication, encryption, and policy enforcement
B. reduction of processing in wireless controllers
C. access point discovery, information exchange, and configuration
D. provides security by blocking communication between access points and wireless clients

Answer: C

Explanation:
The control traffic between the access point and the controller is encapsulated with the LWAPP.
The control traffic is encrypted via the Advanced Encryption Standard (AES).
The data traffic between the access point and controller is also encapsulated with LWAPP. The data traffic is not encrypted. It is switched at the WLAN controller, where VLAN tagging and quality of service (QoS) are also applied.
Lightweight access points first search for a WLAN controller using LWAPP in Layer 2 mode. Then the access point searches for a WLAN in Layer 3 mode.
The access point requests an IP address via DHCP. The access point then sends a LWAPP discovery request to the management IP address of the WLAN controller via a broadcast.
The WLAN controller responds with a discovery response from the manager IP address. This response includes the number of access points that are currently associated to that access point manager interface and the access point manager IP address.
The access point chooses the access point manager with the least number of associated access points and sends the join request.
All subsequent LWAPP communication is done to the access point manager IP address of the WLAN controller.
•Real-timeframe exchange and certain real-time portions of MAC management are accomplished within the access point.
•Authentication, security management, and mobility are handled by WLAN controllers.
•Data and control messages are exchanged between the access point and the WLAN controller using LWAPP.

•Control messages are encrypted.
•All client data traffic is sent via the WLAN controller.

QUESTION NO: 7
Which three WLAN statements are true? (Choose three.)

A. Another term for infrastructure mode is independent service set (IBSS).
B. Ad hoc mode allows mobile clients to connect directly without an intermediate AP.
C. The Aironet 1230 access point is an example of an access point that operates solely as a lightweight access point.
D. A lightweight AP receives control and configuration from a WLAN controller to which it is associated.
E. WLANs are designed to share the medium and can easily handle an increased demand of channel contention.
F. A WLAN client that is operating in half-duplex mode will delay all clients in that WLAN.

Answer: B,D,F

Explanation:
The 802.11 standard specifies a Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) transmit-recieve environment. Therefore, all 802.11 are half-duplex/simplex in nature.
Lightweight access points first search for a WLAN controller using LWAPP in Layer 2 mode. Then the access point searches for a WLAN in Layer 3 mode. The control traffic between the access point and the controller is encapsulated with the LWAPP. The control traffic is encrypted via the Advanced Encryption Standard (AES). Lightweight APs need configuration and control information from a WLAN controller
Incorrect Answers:
A: Ad hoc mode: This mode is called Independent Basic Service Set (IBSS). Mobile clients connect directly without an intermediate access point.

QUESTION NO: 8
Which two WLAN client utility statements are true? (Choose two.)

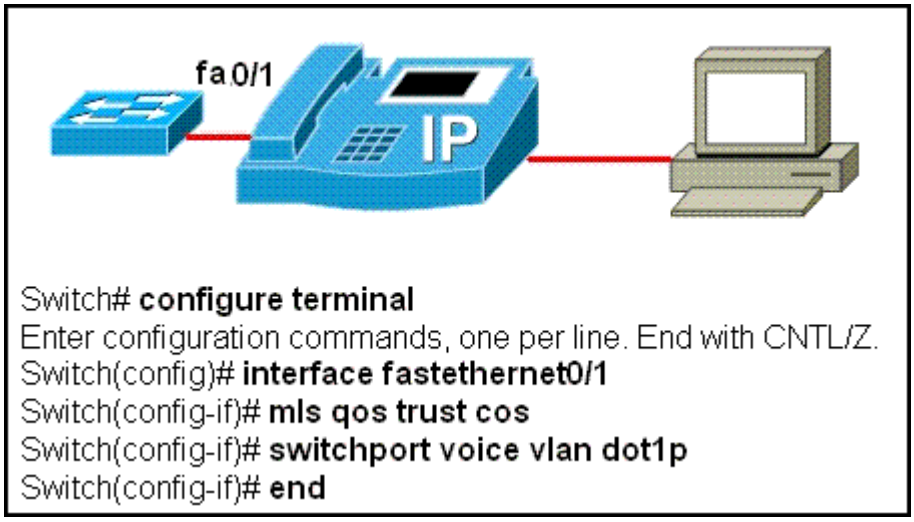
A. The Cisco Aironet Desktop Utility (ADU) and the Microsoft Wireless Configuration Manager can both be enabled at the same time to setup WLAN client cards.
B. In a Windows XP environment, a client adapter can only be configured and managed with the Microsoft Wireless Configuration Manager.
C. The Aironet Desktop Utility (ADU) can be used to enable or disable the adapter radio and to configure LEAP authentication with dynamic WEP.
D. The Microsoft Wireless Configuration Manager can be configured to display the Aironet System Tray Utility (ASTU) icon in the Windows system tray.

Answer: C,D

Explanation:

Enable/Disable Radio:
On the ADU, this option enables you to disable or enable the client adapter's radio. Disabling the radio prevents the adapter from transmitting RF energy. You might want to disable the client adapter's radio in the following situations:
• You are not transmitting data and want to conserve battery power.
• You are using a laptop on an airplane and want to prevent the adapter's transmissions from potentially interfering with the operation of certain devices.
ASTU is an optional application that provides a small subset of the features available through ADU. Specifically, it enables you to access status information about your client adapter and perform basic tasks. ASTU is accessible from an icon in the Windows system tray, making it easily accessible and convenient to use. The ASTU icon appears only if a client adapter is installed in your computer and you did not disable ASTU during installation.
Reference:
http://www.cisco.com/en/US/docs/wireless/wlan_adapter/cb21ag/user/1.0/configuration/guide/khicg1.pdf

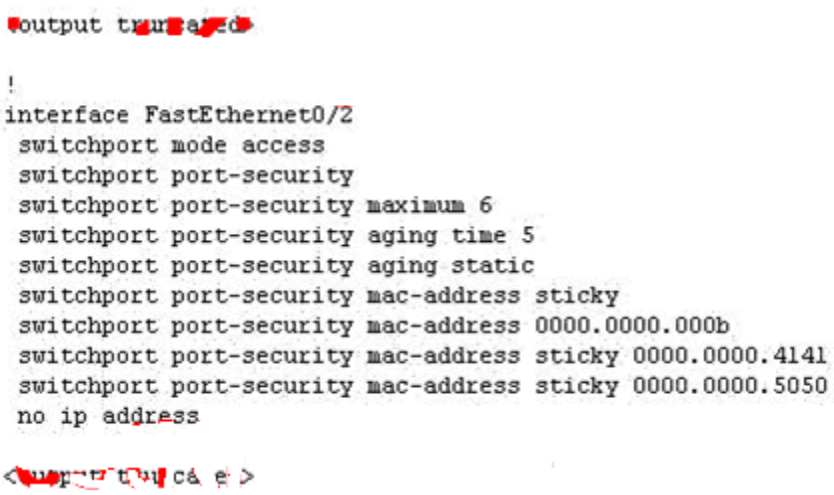
QUESTION NO: 9
Refer to the exhibit. Which statement is true about the configuration that is shown?



A. Untagged ingress traffic will be dropped.
B. Ingress traffic from the host will be tagged with the CoS value of 5.
C. Tagged and untagged ingress traffic will be carried on VLAN 1.
D. Untagged ingress traffic will be marked with the default CoS value of the port.

Answer: D

QUESTION NO: 10
Refer to the exhibit. Based on the running configuration that is shown for interface FastEthernet0/2, what two conclusions can be deduced? (Choose two.)



```
output truncated

!
interface FastEthernet0/2
 switchport mode access
 switchport port-security
 switchport port-security maximum 6
 switchport port-security aging time 5
 switchport port-security aging static
 switchport port-security mac-address sticky
 switchport port-security mac-address 0000.0000.000b
 switchport port-security mac-address sticky 0000.0000.4141
 switchport port-security mac-address sticky 0000.0000.5050
 no ip address

<output truncated>
```

A. Connecting a host with MAC address 0000.0000.4147 will move interface FastEthernet0/2 into error disabled state.
B. The host with address 0000.0000.4141 is removed from the secure address list after 5 seconds of inactivity.
C. The sticky secure MAC addresses are treated as static secure MAC addresses after the running configuration is saved to the startup configuration and the switch is restarted.
D. Interface FastEthernet0/2 is a voice VLAN port.
E. The host with address 0000.0000.000b is removed from the secure address list after 300 seconds.

Answer: C,E

Explanation:
The time *aging_time* keyword specifies the aging time for this port. Valid range for aging_time is from 0 to 1440 minutes. If the time is equal to 0, aging is disabled for this port. In this case, the aging time is set for 5 minutes, or 300 seconds.
You can configure an interface to convert the dynamic MAC addresses to sticky secure MAC addresses and to add them to the running configuration by enabling *sticky* port security. To enable sticky port security, enter the **switchport port-security mac-address sticky** command. When you enter this command, the interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses.
The sticky secure MAC addresses do not automatically become part of the configuration file, which is the startup configuration used each time the switch restarts. If you save the running config file to the configuration file, the interface does not need to relearn these addresses when the switch restarts.
Reference:
http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/25sg/configuration/guide/port_sec.html

QUESTION NO: 11
Which two statements are true about an 802.11g access point? (Choose two.)

A. It provides the same network throughput whether operating with 802.11b clients, 802.11g clients, or a mixed environment where both clients are present.
B. It is fully backward compatible with 802.11b.
C. It supports eight different data rates.
D. It is only compatible with the 11 Mbps 802.11b transfer rate.
E. It has three non-overlapping channels in its channel options.

Answer: B,E

Explanation:
The 802.11g standard is currently the most popular Wi-Fi standard. 802.11g is the successor to 802.11b, **but it is backward-compatible with 802.11b as well**. The two standards operate at the same frequency (2.4GHz). With a throughput of about 22Mbps, 802.11g delivers four times the throughput of 802.11b. 802.11g has been the de facto home network standard for a few years and now dominates in retail markets. As it's been widely adopted, the price of 802.11g products has fallen significantly, making it a cost-effective choice. The only downside to 802.11g is the fact that **it uses a crowded slice of the spectrum, with room for only three nonoverlapping channels.** This will make 802.11a a better choice for some environments, especially those populated with devices that share the 2.4GHz spectrum, such as cordless phones, baby monitors, microwave ovens, and Bluetooth radios.
Reference: http://reviews.cnet.com/4520-7605_7-1023478-2.html

QUESTION NO: 12
With route processor redundancy (RPR+), the redundant supervisor engine is fully initialized and configured, which shortens the switchover time if the active supervisor engine fails. Which three statements are true about the RPR + operations when the redundant supervisor engine switched over the failed primary supervisor engine? (Choose three.)

A. Static IP routes are maintained across a switchover because they are configured from entries in the configuration file.
B. Information about dynamic routing states, maintained on the active supervisor engine, is synchronized to the redundant supervisor engine and is transferred during the switchover.
C. Information about dynamic routing states, maintained on the active supervisor engine, is not synchronized to the redundant supervisor engine and is lost on switchover.
D. The Forwarding Information Base (FIB) tables are cleared on a switchover. As a result, routed traffic is interrupted until route tables reconverge.
E. Static IP routes are cleared across a switchover and recreated from entries in the configuration file on the redundant supervisor engine.
F. The Forwarding Information Base (FIB) tables are maintained during the switchover. As a result, routed traffic continues without any interruption when the failover occurs.

Answer: A,C,D

QUESTION NO: 13
Refer to the exhibit. What command was issued on the Layer 3 switch Sw1 between Exhibit #1 and Exhibit #2?

EXHIBIT #1

```
Sw1# show ip interface vlan 10
Vlan10 is up, line protocol is up
  Internet address is 10.1.1.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
```

EXHIBIT #2

```
Sw1# show ip interface vlan 10
Vlan10 is up, line protocol is up
  Internet address is 10.1.1.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Null turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are None
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
```

A. router eigrp 1

B. no mls qos
C. no router eigrp 1
D. ip routing
E. no ip routing
F. mls qos

Answer: E

Explanation:
IP routing is Enabled, so to disabled IP routing use:
#no ip routing

QUESTION NO: 14
Refer to the exhibit. What will happen when one more user is connected to interface FastEthernet 5/1?

```
Switch# show port-security interface fastethernet 5/1

Port Security:  EnabledPort
Status: SecureUp
Violation mode:  Shutdown
Maximum MAC Addresses:  11
Total MAC Addresses:  11
Configured MAC Addresses:  3
Aging time:  20 mins
Aging type:  Inactivity
SecureStatic address aging:  Enabled
Security Violation count:  0
```

A. The first address learned on the port will be removed from the secure address list and be replaced with the new address.
B. All secure addresses will age out and be removed from the secure address list. This will cause the security violation counter to increment.
C. The packets with the new source addresses will be dropped until a sufficient number of secure MAC addresses are removed from the secure address list.
D. The interface will be placed into the error-disabled state immediately, and an SNMP trap notification will be sent.

Answer: D

Explanation:

Port security is a feature supported on Cisco Catalyst switches that restricts a switch port to a specific set or number of MAC addresses. Those addresses can be learned dynamically or configured statically. The port will then provide access to frames from only those addresses. If, however, the number of addresses is limited to four but no specific MAC addresses are

configured, the port will allow any four MAC addresses to be learned dynamically, and port access will be limited to those four dynamically learned addresses.

Port Security Implementation:

Step	Description
1.	Enables port security. Switch(config-if)#**switchport port-security**
2.	Sets a maximum number of MAC addresses that will be allowed on this port. Default is one. Switch(config-if)#**switchport port-security maximum** value
3.	Specifies which MAC addresses will be allowed on this port (optional). Switch(config-if)#**switchport port-security mac-** **address** mac-address Switch(config-if)#**switchport port-security mac-address** mac-address
4.	Defines what action an interface will take if a nonallowed MAC address attempts access. Switch(config-if)#**switchport port-security violation** {shutdown | restrict | protect}

When Switch port security rules violate different action can be applied:

1. Protect: Frames from the nonallowed address are dropped, but there is no log of the violation.

2. Restrict: Frames from the nonallowed address are dropped, a log message is created, and a Simple Network Management Protocol (SNMP) trap is sent.

3. Shutdown: If any frames are seen from a nonallowed address, the interface is errdisabled, a log entry is made, an SNMP trap is sent, and manual intervention or errdisable recovery must be used to make the interface usable.

QUESTION NO: 15
Which three statements are correct with regard to the IEEE 802.1Q standard? (Choose three.)

A. the packet is encapsulated with a 26 byte header and a 4 byte FCS
B. the IEEE 802.1Q frame retains the original MAC destination address
C. protocol uses point-to-point connectivity
D. the IEEE 802.1Q frame format adds a 4 byte field to a Ethernet frame
E. protocol uses point-to-multipoint connectivity
F. the IEEE 802.1Q frame uses multicast destination of 0x01-00-0c-00-00

Answer: B,C,D

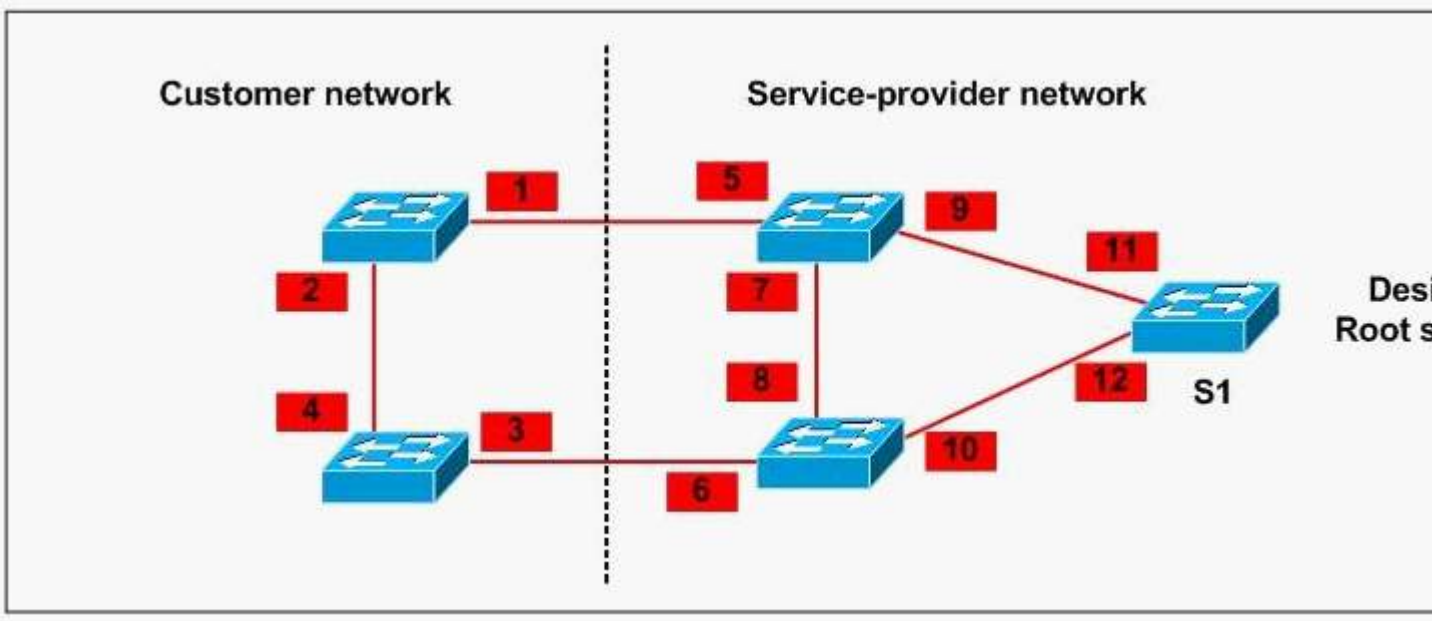
Explanation:
The IEEE 802.1Q protocol can also carry VLAN associations over trunk links. However, this frame identification method is standardized, allowing VLAN trunks to exist and operate between equipment from multiple vendors.
In particular, the IEEE 802.1Q standard defines an architecture for VLAN use, services provided with VLANs, and protocols and algorithms used to provide VLAN services. Like Cisco ISL, IEEE 802.1Q can be used for VLAN identification with Ethernet trunks. Instead of encapsulating each frame with a VLAN ID header and trailer, 802.1Q embeds its tagging information within the Layer 2 frame. This method is referred to as *single-tagging* or *internal tagging*.
802.1Q also introduces the concept of a *native VLAN* on a trunk. Frames belonging to this VLAN are *not* encapsulated with any tagging information. In the event that an end station is connected to an 802.1Q trunk link, the end station can receive and understand only the native VLAN frames. This provides a simple way to offer full trunk encapsulation to the devices that can understand it, while giving normal access stations some inherent connectivity over the trunk.

QUESTION NO: 16
What does the auto qos voip cisco-phone command do?

A. If a Cisco IP phone is attached and removed, the switch continues to trust the CoS values as long as the switch is not rebooted.
B. If a Cisco IP phone is attached, the switch trusts the CoS.
C. It turns on STP to see if a Cisco IP phone is attached.
D. The switch assigns a CoS value of 5 to incoming packets.
E. It disables the trust boundary feature because the switch knows a Cisco IP phone is attached.

Answer: B

QUESTION NO: 17
Refer to the exhibit. The service provider wants to ensure that switch S1 is the root switch for its own network and the network of the customer. On which interfaces should root guard be configured to ensure that this happens?



A. interfaces 5 and 6
B. interfaces 1, 3, 5, and 6
C. interfaces 5, 6, 7, and 8
D. interfaces 11 and 12
E. interfaces 1, 2, 3, and 4
F. interfaces 1 and 2

Answer: A

Explanation:
The traditional STP does not provide any means for the network administrator to securely enforce the topology of the switched Layer 2 network. This may become especially important in networks with shared administrative control. For example, one switched network controlled by different administrative entities or companies.

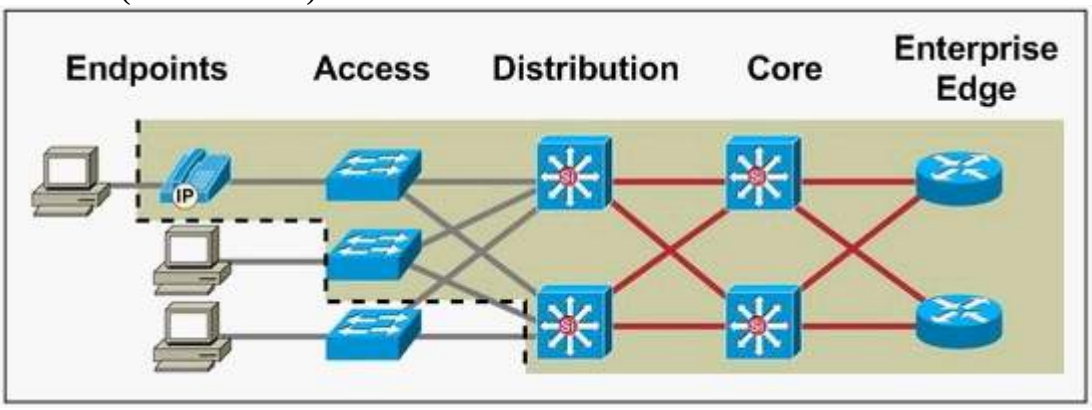
Forwarding topology of the switched network is calculated, based among other parameters, on the root bridge position. Although any switch can be Root Bridge in the network, it is better to place the root bridge manually, (somewhere in the core layer) so the forwarding topology will be optimal. The standard STP does not allow the administrator to enforce the position of the root bridge. If a bridge is introduced into the network with lower bridge priority, it will take the role of the root bridge.

The root guard ensures that the port on which it is enabled is the designated port (normally, root bridge ports are all designated, unless two or more ports of the root bridge are connected together). If the bridge receives superior STP Bridge Port Data Units (BPDUs) on a root guard enabled port, this port will be moved to a root-inconsistent STP state (effectively equal to listening state), and no traffic will be forwarded across this port. The position of the root bridge will be enforced.

Configuring Root Guard

	Command	Purpose
Step 1	`configure terminal`	Enter global configuration mode.
Step 2	`interface` *interface-id*	Enter interface configuration mode, and specify the interface to configure.
Step 3	`spanning-tree guard root`	Enable root guard on the interface. By default, root guard is disabled on all interfaces.
Step 4	`end`	Return to privileged EXEC mode.
Step 5	`show running-config`	Verify your entries.
Step 6	`copy running-config startup-config`	(Optional) Save your entries in the configuration file.

QUESTION NO: 18
Refer to the exhibit. Which three statements are true about trust boundaries in the campus network? (Choose three.)



A. Classification and marking occur using 802.1ab QoS bits before reaching the trust boundary.
B. A device is trusted if it correctly declassifies packets.
C. A device is trusted if it correctly classifies packets.
D. Network trust boundaries are automatically configured in IOS version 12.3 and later.
E. The outermost trusted devices represent the trust boundary.
F. For scalability, classification should be done as close to the edge as possible.

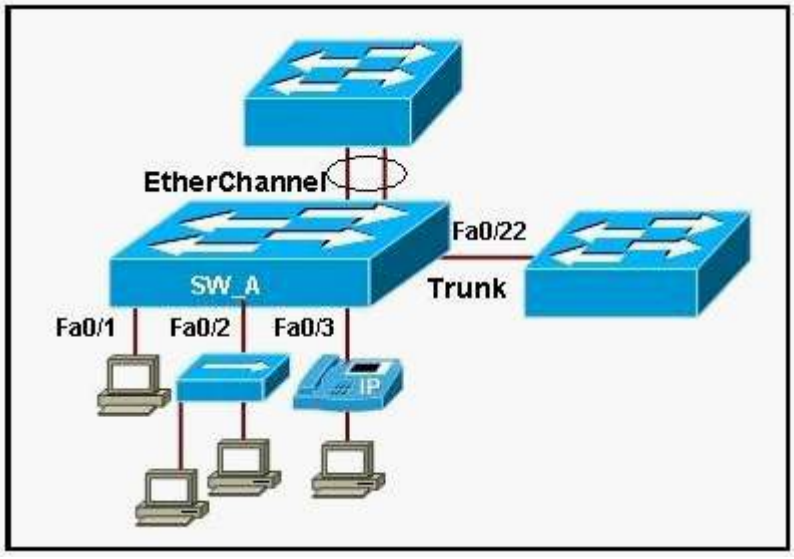
Answer: C,E,F

QUESTION NO: 19
Which set of statements describes the correct order and process of a wireless client associating with a wireless access point?

A. 1. Access point sends probe request .2. Client sends probe response.3. Client initiates association.4. Access point accepts association.5. Client adds access point MAC address to association table.
B. 1. Client sends probe request.2. Access point sends probe response.3. Client initiates association.4. Access point accepts association.5. Access point adds client MAC address to association table.
C. 1. Client sends probe request.2. Access point sends probe response.3. Access point initiates association.4. Client accepts association.5. Access point adds client MAC address to association table.
D. 1. Access point sends probe request .2. Client sends probe response.3. Client initiates association.4. Access point accepts association.5. Access point adds client MAC address to association table.
E. 1. Client sends probe request.2. Access point sends probe response.3. Client initiates association.4. Access point accepts association.5. Client adds access point MAC address to association table.

Answer: B

QUESTION NO: 20
Refer to the exhibit. Which interface or interfaces on switch SW_A can have the port security feature enabled?



A. Ports 0/1 and 0/2
B. The trunk port 0/22 and the EtherChannel ports
C. Ports 0/1, 0/2 and 0/3
D. Ports 0/1, 0/2, 0/3, the trunk port 0/22 and the EtherChannel ports
E. Port 0/1
F. Ports 0/1, 0/2, 0/3 and the trunk port 0/22

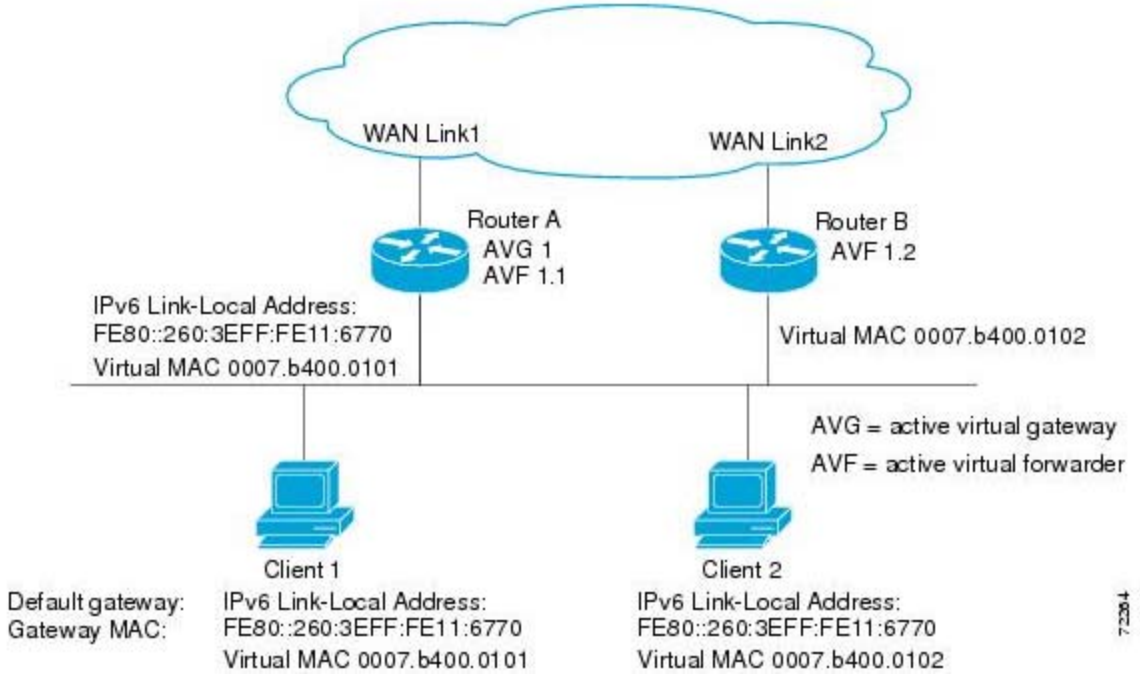
Answer: C

Explanation:

Port security is a feature supported on Cisco Catalyst switches that restricts a switch port to a specific set or number of MAC addresses. Those addresses can be learned dynamically or configured statically. The port will then provide access to frames from only those addresses. If, however, the number of addresses is limited to four but no specific MAC addresses are configured, the port will allow any four MAC addresses to be learned dynamically, and port access will be limited to those four dynamically learned addresses. A port security feature called "sticky learning," available on some switch platforms, combines the features of dynamically learned and statically configured addresses. When this feature is configured on an interface, the interface converts dynamically learned addresses to "sticky secure" addresses. This adds them to the running configuration as if they were configured using the **switchport port-security mac-address** command.

QUESTION NO: 21
Refer to the exhibit.

Which three statements accurately describe this GLBP topology? (Choose three.)



A. Router A is responsible for answering ARP requests sent to the virtual IP address.
B. If Router A becomes unavailable, Router B will forward packets sent to the virtual MAC address of Router A.

C. Router A alternately responds to ARP requests with different virtual MAC addresses.
D. Router B will transition from blocking state to forwarding state when it becomes the AVG.
E. If another router were added to this GLBP group, there would be two backup AVGs.
F. Router B is in GLBP listen state.

Answer: A,B,C

QUESTION NO: 22
Which three statements are true of the Link Aggregation Control Protocol (LACP)? (Choose three.)

A. LACP packets are sent with the command channel-group 1 mode active.
B. Standby interfaces should be configured with a higher priority.
C. Standby interfaces should be configured with a lower priority.
D. LACP packets are sent with the command channel-group 1 mode desirable.
E. LACP is used to connect to non-Cisco devices.

Answer: A,B,E

Explanation:
LACP is a standards-based alternative to PAgP, defined in IEEE 802.3ad (also known as IEEE 802.3 Clause 43, "Link Aggregation"). LACP packets are exchanged between switches over EtherChannelcapable ports. Like PAgP, the identification of neighbors and port group capabilities is learned and compared with local switch capabilities. However, LACP also assigns roles to the EtherChannel's endpoints.
The switch with the lowest *system priority* (a 2-byte priority value followed by a 6-byte switch MAC address) is allowed to make decisions about what ports are actively participating in the EtherChannel at a given time.
Ports are selected and become active according to their *port priority* value (a 2-byte priority followed by a 2-byte port number), where a low value indicates a higher priority. A set of up to 16 potential links can be defined for each EtherChannel. Through LACP, a switch selects up to eight of these having the lowest port priorities as active EtherChannel links at any given time. The other links are placed in a standby state and will be enabled in the EtherChannel if one of the active links goes down.
Like PAgP, LACP can be configured in active mode ("active"), where a switch actively asks a farend switch to negotiate an EtherChannel, or in passive mode ("passive"), where a switch negotiates an EtherChannel only if the far-end initiates it.

To configure switch ports for LACP negotiation, use the following commands:
Switch(config)# lacp system-priority priority
Switch(config)# interface type mod/num
Switch(config-if)# channel-protocol lacp
Switch(config-if)# channel-group number mode {on | passive | active}
Switch(config-if)# lacp port-priority priority

First, the switch should have its LACP system priority defined (1 to 65,535, default 32,768). If desired, one switch should be assigned a lower system priority than the other so that it can make decisions about the EtherChannel's makeup. Otherwise, both switches will have the same system priority (32,768), and the one with the lower MAC address will become the decision-maker.

QUESTION NO: 23
Which two Lightweight Access Point Protocol (LWAPP) statements are true? (Choose two.)

A. Data traffic is encapsulated in UDP packets with a source port of 1024 and a destination port of 12223.
B. LWAPP is a proprietary protocol, and because of its very high overhead it is not widely adopted .
C. Control traffic is encapsulated in TCP packets with a source port of 1024 and a destination port of 12223.
D. Layer 3 LWAPP is a UDP / IP frame that requires a Cisco Aironet AP to obtain an IP address using DHCP.
E. Data traffic is encapsulated in TCP packets with a source port of 1024 and destination port of 12223.
F. Control traffic is encapsulated in UDP packets with a source port of 1024 and a destination port of 12223.

Answer: D,F

Explanation:
For Layer 3, LWAPP uses packets in a UDP/IP frame. LWAPP control traffic uses source port 1024 or greater and destination port 12223, and LWAPP data traffic uses source port 1024 or greater and destination port 12222. The Cisco wireless LAN controller and access point can be connected to the same VLAN/subnet or to a different VLAN/subnet.
In Layer 3 operation, the access point and the controller can be on the same or different subnets. Layer 3 operation is scalable and is recommended by Cisco. A Layer 3 access point on a different subnet than the controller requires a DHCP server on the access point subnet and a route to the controller. The route to the controller must have destination UDP ports 12222 and 12223 open for LWAPP communications. The route to the primary, secondary, and tertiary controllers must allow IP packet fragments.
References:
http://www.cisco.com/en/US/docs/wireless/technology/7920/design/guide/7920DG.html
http://www.cisco.com/en/US/docs/wireless/access_point/1000/installation/guide/1000h_c3.html

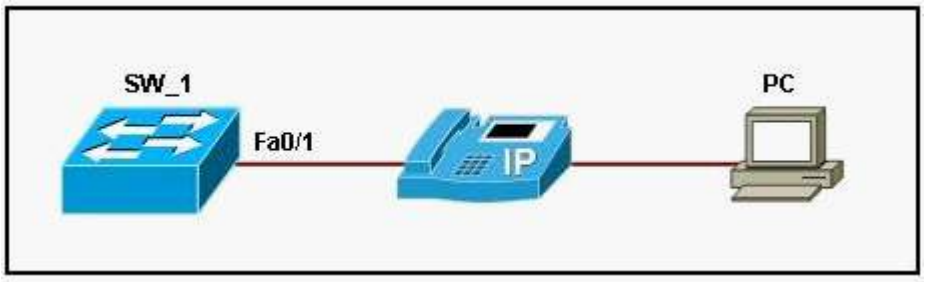
QUESTION NO: 24
Which set of statements describes the correct order and process of a wireless client associating with a wireless access point?

A. 1. Client sends probe request.
2. Access point sends probe response.
3. Client initiates association.
4. Access point accepts association.

5. Access point adds client MAC address to association table.
B. 1. Client sends probe request.
2. Access point sends probe response.
3. Access point initiates association.
4. Client accepts association.
5. Access point adds client MAC address to association table.
C. 1. Access point sends probe request .
2. Client sends probe response.
3. Client initiates association.
4. Access point accepts association.
5. Client adds access point MAC address to association table.
D. 1. Access point sends probe request .
2. Client sends probe response.
3. Client initiates association.
4. Access point accepts association.
5. Access point adds client MAC address to association table.
E. 1. Client sends probe request.
2. Access point sends probe response.
3. Client initiates association.
4. Access point accepts association.
5. Client adds access point MAC address to association table.

Answer: A

QUESTION NO: 25
Refer to the exhibit. Which statement is true when voice traffic is forwarded on the same VLAN used by the data traffic?



A. The voice traffic cannot be forwarded to the distribution layer.
B. The voice traffic cannot use 802.1p priority tagging.
C. Port security cannot be enabled on the switch that is attached to the IP phone.
D. Quality of service cannot be applied for the voice traffic.

Answer: B

Explanation:

You can configure a port connected to the Cisco IP Phone to send CDP packets to the phone to configure the way in which the phone sends voice traffic. The phone can carry voice traffic in 802.1Q frames for a specified voice VLAN with a Layer 2 CoS value. It can use 802.1P priority tagging to give voice traffic a higher priority and forward all voice traffic through the native (access) VLAN. The IP phone can also send untagged voice traffic or use its own configuration to send voice traffic in the access VLAN. In all configurations, the voice traffic carries a Layer 3 IP precedence value (the default is 5).
If the Cisco IP Phone and a device attached to the Cisco IP Phone are in the same VLAN, they must be in the same IP subnet. These conditions indicate that they are in the same VLAN:
– They both use 802.1p or untagged frames.
– The Cisco IP Phone uses 802.1p frames and the device uses untagged frames.
– The Cisco IP Phone uses untagged frames and the device uses 802.1p frames.
– The Cisco IP Phone uses 802.1Q frames and the voice VLAN is the same as the access VLAN.
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps5206/products_configuration_guide_chapter09186a00801a64ea.html

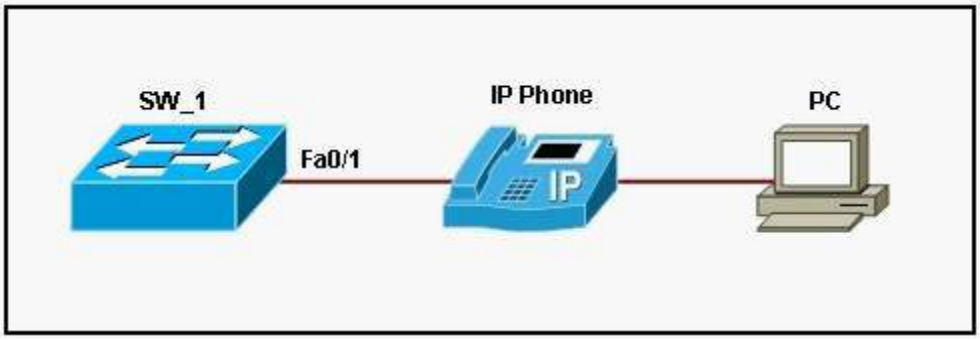
QUESTION NO: 26
On a multilayer Catalyst switch, which interface command is used to convert a Layer 3 interface to a Layer 2 interface?

A. switchport
B. no switchport
C. swithport access vlan vlan-id
D. switchport mode access

Answer: A

Explanation:
The **switchport** command puts the port in Layer 2 mode. Then, you can use other **switchport** command keywords to configure trunking, access VLANs, and so on.

QUESTION NO: 27
Refer to the exhibit. Which Catalyst switch interface command would be used to cause the switch to instruct the phone to override the incoming CoS from the PC before forwarding the packet to the switch?



A. mls qos cos 2 override
B. switchport priority extend cos 11
C. switchport priority extend trust
D. switchport priority extend none
E. mls qos cos 2
F. switchport priority extend cos 2

Answer: F

QUESTION NO: 28
Which three protocols have been developed for IP routing redundancy to protect against first-hop router failure? (Choose three.)

A. GLBP
B. ICMP
C. MSTP
D. HSRP
E. VRRP

Answer: A,D,E

QUESTION NO: 29
For what purpose is the command config network webmode enable used?

A. to allow HTTP access to the WLAN controller
B. to allow SSH access to the CLI of the WLAN controller
C. to allow SSL access to the CLI of the WLAN controller
D. to allow HTTPS access to the WLAN controller

Answer: D

QUESTION NO: 30
Which two statements about VLAN hopping are true? (Choose two.)

A. An end station attempts to gain access to all VLANs by transmitting Ethernet frames in the 802.1q encapsulation.
B. Configuring an interface with the switchport mode dynamic command will prevent VLAN hopping.
C. Attacks are prevented by utilizing the port-security feature.

D. Configuring an interface with the switchport mode access command will prevent VLAN hopping.
E. An end station attempts to redirect VLAN traffic by broadcasting multiple ARP requests.

Answer: A,D