642-812

Building Converged Cisco Multilayer Switched Networks (BCMSN)

Version 3.2

642-812

Contents

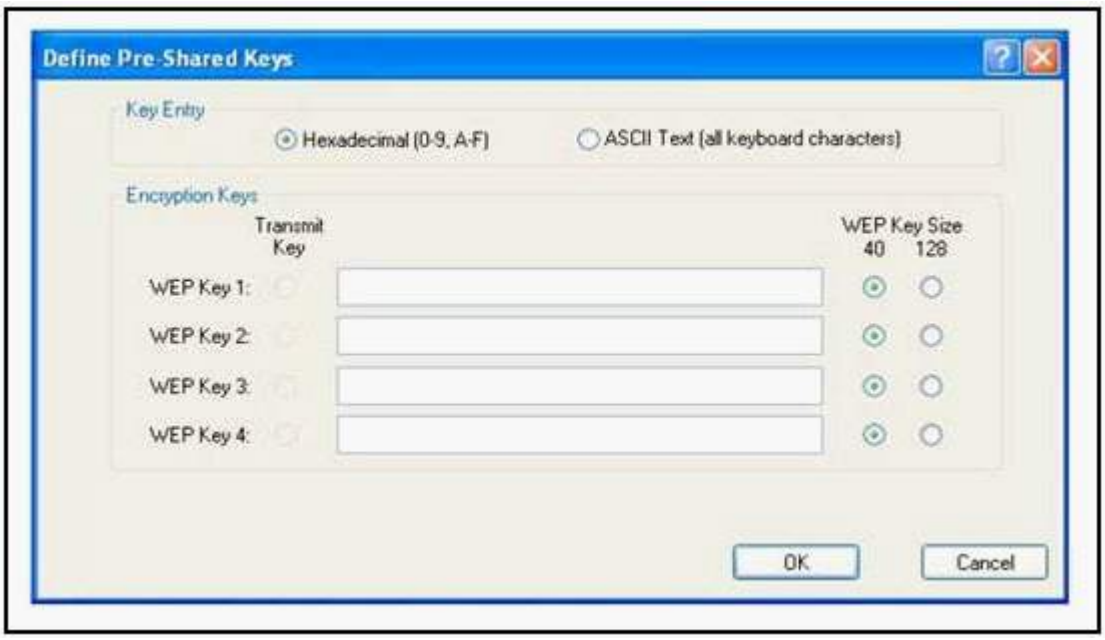
Total number of questions = 465

642-812

Topic 1, Main Questions, (340 Questions)

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.

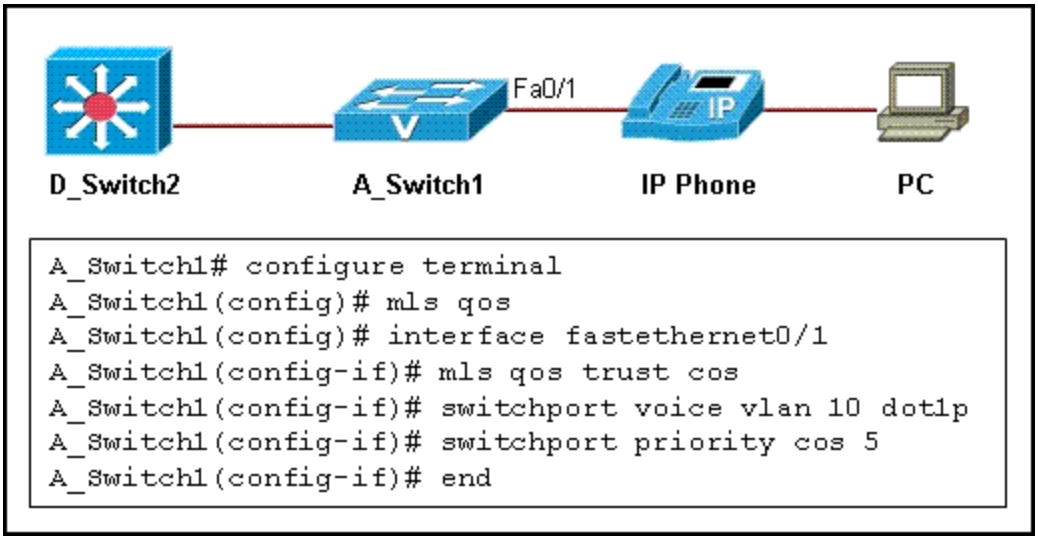
Answer: C

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

642-812

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

QUESTION NO: 4

642-812

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?


```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet0/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# switchport voice vlan dot1p
Switch(config-if)# end
```

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: