

200-355.349q

Number: 200-355
Passing Score: 925
Time Limit: 120 min
File Version: 1



VCE to PDF Converter : <https://vceplus.com/vce-to-pdf/>

Facebook: <https://www.facebook.com/VCE.For.All.VN/>

Twitter : https://twitter.com/VCE_Plus

Google+ : <https://plus.google.com/+Vcepluscom>

LinkedIn : <https://www.linkedin.com/company/vceplus>

Vendor: Cisco

Exam Code: 200-355

Exam Name: Implementing Cisco Wireless Network Fundamentals

Exam A**QUESTION 1**

When deploying a Cisco Cloud Wireless Infrastructure, what two destination ports must be open? (Choose two.)

- A. TCP/5246
- B. UDP/5246
- C. TCP/5247
- D. UDP/5247
- E. TCP/7351
- F. UDP/7351
- G. TCP/7734
- H. UDP/7734

Correct Answer: FG

Section: (none)

Explanation

Explanation/Reference:

**QUESTION 2**

A customer has ordered a Cisco 5760 Wireless Controller. What speed and quantity of ports are needed for full-speed operation?

- A. 6 x 1 Gb
- B. 6 x 10 Gb
- C. 2 x 10 Gb
- D. 2 x 1 Gb
- E. 8 x 1 Gb
- F. 8 x 10 Gb

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

Refer to the exhibit. A network administrator is attempting to connect to the GUI of a WLC with interfaces as shown. Which IP address should the network administrator use?

Interface Name	VLAN Identifier	IP Address	Interface Type
ap-manager	4	192.168.4.2	Dynamic
clients	2	192.168.2.2	Dynamic
guests	3	192.168.3.2	Dynamic
management	untagged	192.168.1.2	Static
mgmt	1	192.168.0.2	Dynamic
virtual	N/A	1.1.1.1	Static

- A. 192.168.0.2
- B. 192.168.1.2
- C. 192.168.2.2
- D. 192.168.3.2
- E. 192.168.4.2

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 4

A network engineer is connected via wireless to a Cisco AireOS WLC and wants to download the configuration but is unable to do so. Which change will correct the issue?

- A. enable management via wireless
- B. connect via wired network

- C. enable Telnet
- D. enable WebAuth SecureWeb
- E. connect on 5-GHz SSID

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 5

An engineer is trying to convert the IP Address of the wireless controller to amend DHCP Option 43 configuration on the DHCP server. What mathematical format must the IP address of the Wireless controller be converted to in order to function correctly?

- A. Hexadecimal
- B. Binary
- C. Decimal
- D. ASCII

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 6

Refer to the exhibit. WLC1 becomes unresponsive due to a power failure at a customer site. How does the access point that is shown in the WLC controller GUI behave now that WLC1 is disabled?

General
Credentials
Interfaces
High Availability
Inventory
Advanced

	Name	Management IP Address
Primary Controller	WLC1	10.201.204.8
Secondary Controller	WLC2	10.201.204.11
Tertiary Controller	WLC3	10.201.204.6

AP Failover Priority Low

High Availability

AP Heartbeat Timeout(1-30) 30

Local Mode AP Fast Heartbeat Timer State Disable

H-REAP Mode AP Fast Heartbeat Timer State Disable

AP Primary Discovery Timeout(30 to 3600) 120

Back-up Primary Controller IP Address 10.201.204.19

Back-up Primary Controller name Back-UP-WLC

Back-up Secondary Controller IP Address

Back-up Secondary Controller name

TCP MSS

Global TCP Adjust MSS ☐

AP Retransmit Config Parameters

AP Retransmit Count 5 ☐

AP Retransmit Interval 3 ☐

- A. associates to controller 10.201.204.6
- B. associates to controller 10.201.204.11
- C. associates to controller 10.201.204.8
- D. associates to controller 10.201.204.19

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 7

A customer wants to deploy a mesh network with 2 root access points and 10 mesh access points. The root access points should be configured as which mode on the WLC?

- A. mesh
- B. FlexConnect
- C. bridge
- D. rouge detection
- E. sniffer



Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 8

A customer has completed the installation of an 802.11ac greenfield deployment at their corporate headquarters. They would like to leverage 802.11ac enhanced speeds on the trusted employee WLAN. In order to configure the employee WLAN, what Layer 2 security policies are valid?

- A. WPA2 (TKIP)
- B. WPA(AES)
- C. OPEN
- D. WEP

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 9

Refer to the exhibit. A customer is using central web authentication with a Cisco 5508 Wireless Controller and Cisco Identity Services Engine. An error occurs when wireless clients are redirected to the hosted splash page. What is causing the client error?



```
(Cisco Controller) >show network summary
RF-Network Name..... Cisco
Web Mode..... Disable
Secure Web Mode..... Disable
Secure Web Mode Cipher-Option High..... Disable
Secure Web Mode Cipher-Option SSLv2..... Disable
Secure Web Mode RC4 Cipher Preference..... Disable
OCSP..... Disabled
OCSP responder URL.....
Secure Shell (ssh)..... Enable
Telnet..... Disable
Ethernet Multicast Forwarding..... Disable
Ethernet Broadcast Forwarding..... Disable
IPv4 AP Multicast/Broadcast Mode..... Multicast Address : 239.0.1.1
IGMP snooping..... Disabled
IGMP timeout..... 60 seconds
IGMP Query Interval..... 20 seconds
MLD snooping..... Disabled
MLD timeout..... 60 seconds
MLD query interval..... 20 seconds
User Idle Timeout..... 300 seconds
ARP Idle Timeout..... 300 seconds
```

- A. Secure Web Mode is disabled on the WLC.
- B. OCSP is disabled on the WLC.
- C. Management Via Dynamic Interface is disabled on the WLC.
- D. Ethernet Multicast Forwarding is enabled on the WLC.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 10

A customer cannot access the GUI on the Cisco 5508 Wireless Controller from the management interface due to network failure. Which interface can the customer use to access the WLC GUI until the network issues are resolved?

- A. virtual
- B. dynamic
- C. console port
- D. service port

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:



QUESTION 11

Which interface is used to connect the foreign and anchor controllers?

- A. management
- B. service
- C. virtual
- D. dynamic

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 12

Refer to the exhibit. An engineer is configuring a SSID to utilize the management interface on the WLC. The management interface is configured with an untagged VLAN in the wireless controller interface settings. The controller is connected to a neighboring switch via the interface shown in the diagram.

```
interface GigabitEthernet2/1
  no ip address
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1,5,15,20,25,30,35,40,45,50,55,100
  switchport trunk native vlan 44
  switchport mode trunk
end
```

Which VLAN will traffic coming from the newly created SSID use to traverse the wired network?

- A. 1
- B. 20
- C. 44
- D. 50

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 13

A customer has a corporate SSID that is configured to authenticate against an ACS server to validate client credentials on the corporate SSID. The customer has a firewall logically positioned on the network between the WLC and the ACS server in the network architecture. Which port must the firewall allow to ensure that authentication can occur?

- A. 43

- B. 1812
- C. 5146
- D. 8143

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 14

During an upgrade, the wireless infrastructure has seen a few access points join and then drop off the network. After further investigation, it appears the access points may have an IOS code version that is causing issues. Where in the controller is this information found?

- A. GUI > Wireless > Access Point > General
- B. CLI > show ap image all
- C. GUI > Monitor > Software Version
- D. CLI > show sysinfo

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 15

Microsoft Active Directory integrated machines are not authenticating to the internal WLAN. The WLAN settings are WPA2-AES-802.1x and are authenticating to a Cisco Identity Services Engine server. You investigate and note that non-domain authenticated machines are properly authenticating to the WLAN using their Active Directory credentials.

Why would this problem occur?

- A. The WLAN is configured improperly in group policy.
- B. The ACS server is not joined to the domain, causing authentications to fail.
- C. The domain machines are configured to disable the wireless adapter.
- D. The non-domain machines are using local accounts that are not authenticated through the domain.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 16

Mac OS X machines are having issues accessing the wireless network. While working with TAC, the administrator is asked to find the Mac laptop's wireless adapter model and driver. Where should the administrator look to find this information?

- A. About This Mac > System Report
- B. Control Panel > System
- C. System Preferences > Network > Wi-Fi Adapter > Advanced
- D. Control Panel > Networking > Adapters > Properties

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 17

An engineer is trying to determine from the controller CLI whether or not Telnet is enabled on the wireless controller. Which command can be entered to display this information?

- A. show network summary
- B. show aaa auth
- C. show radius summary
- D. show ldap statistics

Correct Answer: A

Section: (none)

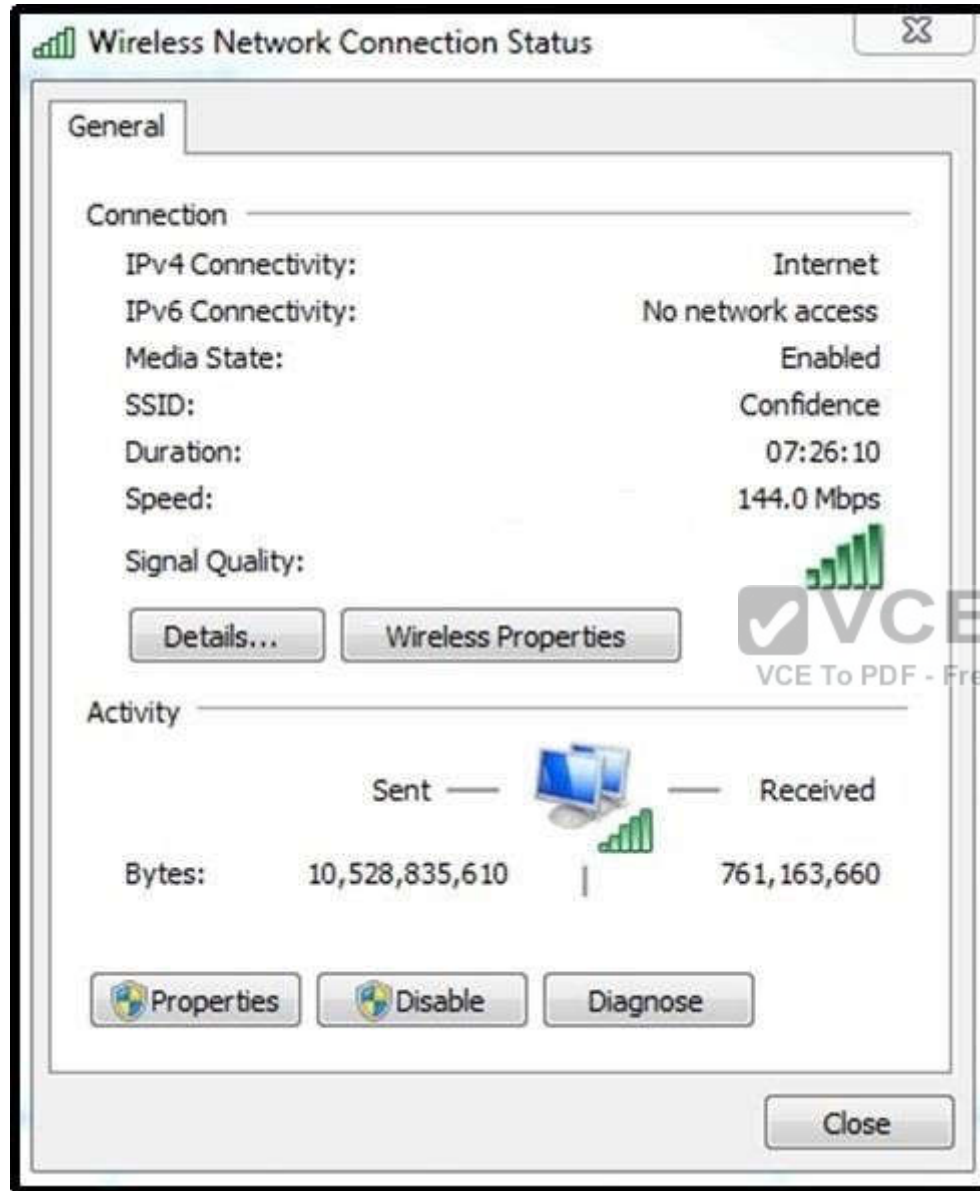
Explanation

Explanation/Reference:

QUESTION 18

Refer to the exhibit. A customer is determining whether a Windows 7 laptop is operating on the correct IEEE 802.11 standard. Which standard is being used by the laptop in the exhibit?





A. 802.11b

- B. 802.11g
- C. 802.11n
- D. 802.11p

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 19

An engineer is trying to identify if radar has impacted the wireless network at a customer site. When using the controller GUI, which dashboard in the Monitor section presents this information?

- A. 802.11a/n - Air Quality Reports
- B. Clean Air - Worst Air Quality Report
- C. 802.11b/g/n - Interfering Devices
- D. Statistics - Mobility Statistics

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 20

An engineer is using a predictive survey tool to estimate placement of APs in a carpeted office space. Most interior walls should be assigned which attenuation value?

- A. 2 dB
- B. 3 dB
- C. 4 dB
- D. 5 dB

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:**QUESTION 21**

An engineer is conducting an active survey for indoor coverage in a warehouse. The warehouse has long aisles with racks that extend to the ceiling. Which antenna type has a radiation pattern that is suited to provide coverage in each aisle?

- A. Yagi
- B. patch
- C. omnidirectional
- D. dipole

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:**QUESTION 22**

Following the deployment of a wireless network for data and voice services, an engineer is to validate the coverage. Which type of survey is required to ensure coverage?

- A. passive
- B. active
- C. fingerprinting
- D. calibrating

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:**QUESTION 23**

During the deployment of a wireless network for data and location services, an engineer is to fine- tune the location services. What is this type of survey called?

- A. passive fingerprinting
- B. passive calibrating
- C. active fingerprinting
- D. active calibrating

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 24

Refer to the exhibit. In an effort to identify RF characteristics at a customer location, an RF engineer uses the Spectrum Analyzer tool that is shown. Which feature that is native to the Spectrum Analyzer is identified by the exhibit?



A. Real-Time FFT

- B. Duty Cycle
- C. Max Hold
- D. Time Domain

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 25

Refer to the exhibit. The site in this AirMagnet Survey heat map is ready for which level of service?



A. data

- B. voice
- C. location
- D. RFID

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 26

Which two services require an RToWLAN design? (Choose two.)

- A. WVoIP
- B. video conferencing
- C. multicast video
- D. Telnet
- E. SSH

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 27

In the current RF environment, the noise floor is -95 dBm. A tablet needs an SNR of 25 dB to transmit at the required speed. What must the RSSI cell edge be to meet the required SNR?

- A. -120 dBm
- B. -90 dBm
- C. -70 dBm
- D. -60 dBm
- E. -50 dBm

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 28

An access point is currently transmitting at 4 mW. The customer needs to increase its signal strength by 6 dB to create a larger wireless cell. What should the new transmit power be?

- A. 8 mW
- B. 10 mW
- C. 12 mW
- D. 16 mW
- E. 24 mW

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:



QUESTION 29

A wireless engineer is designing the wireless networking for a company with offices in two different locations. Which two regulatory bodies should they check to find the maximum EIRP allowed? (Choose two.)

- A. IEEE
- B. FCC
- C. ITU-R
- D. ETSI
- E. Wi-Fi Alliance

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 30

After installing a Cisco 5508 Wireless Controller using the default settings, how often will the RRM update occur?

- A. 30 seconds
- B. 60 seconds
- C. 300 seconds
- D. 600 seconds
- E. 3600 seconds
- F. 7200 seconds

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 31

A customer has requested a single point of policy enforcement for LAN and WLAN. Which deployment model should be used?

- A. converged
- B. autonomous
- C. FlexConnect
- D. centralized

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 32

Which CLI command is used on a Cisco WLC to troubleshoot mobility, rogue detection, and load- balancing events?

- A. debug dot11
- B. debug capwap all

- C. show dot11 details
- D. show capwap details

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 33

Which three WLC debug commands are appropriate to troubleshoot a wireless client that is associated to an AP? (Choose three.)

- A. debug capwap
- B. debug mac addr
- C. debug dot11
- D. debug dhcp
- E. debug ap
- F. debug dtls

Correct Answer: BCD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 34

An engineer wants to have users who connect to a WLAN be redirected to a terms-of-service page with the company logo and a login. What should be configured on the WLAN to enable this capability?

- A. Layer 2 IEEE 802.1x
- B. Web Policy Slash Page Web Redirect
- C. Web Policy Authentication
- D. AAA Servers
- E. Web Policy Passthrough

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 35

Which two principles must be considered when deploying a wireless network through a wooded area? (Choose two.)

- A. absorption
- B. reflection
- C. diffraction
- D. scattering
- E. refraction

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:



QUESTION 36

What is an interferer that an engineer may see in Cisco CleanAir?

- A. microwave ovens
- B. rogue APs
- C. malicious clients
- D. co-channel interference

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 37

A network engineer notices that two mesh APs are having problems communicating. After reviewing the current radio configurations, it is noted that one AP is

transmitting at 3 mW while the other is transmitting at 60 mW. How many decibels would the 3-mW AP need its power increased to match the 60-mW AP?

- A. 8
- B. 12
- C. 13
- D. 20
- E. 57

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 38

A network engineer requires an antenna for a point-to-point bridge with at least 20 dBi of gain. Which antenna is appropriate for the task?

- A. Yagi
- B. patch
- C. parabolic dish
- D. dipole
- E. internal omnidirectional

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 39

An engineer needs to find out the maximum EIRP allowed for their office in Asia. What regulatory body should be contacted?

- A. CRTC
- B. ETSI
- C. IEEE

D. NTT

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 40

A wireless engineer has an access point using the 5.725-GHz channel in the United States. In which band is the AP operating?

- A. UNII-1
- B. UNII-2
- C. UNII-2 Extended
- D. UNII-3

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



QUESTION 41

Which RRM feature allows an access point to avoid non-IEEE 802.11 interference?

- A. DCA
- B. TPC
- C. RF groups
- D. coverage hole detection

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 42

Which IEEE 802.11n client feature can combine the signal from multiple antennas and radio chains to improve SNR?

- A. channel aggregation
- B. spatial multiplexing
- C. MAC layer efficiency
- D. TxBF
- E. MRC
- F. MCS

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

QUESTION 43

An engineer needs an AP with at least two spatial streams, four receivers, and three transmitters. Which device meets these requirements?

- A. 2x4:3
- B. 2x3:4
- C. 4x3:2
- D. 3x4:2

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 44

Which option is used to form the BSSID in a BSS?

- A. AP radio MAC address
- B. AP wired MAC address

- C. AP serial number
- D. client radio MAC address
- E. client wired MAC address
- F. client serial number

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 45

A network engineer at a retail store needs a wireless deployment that can be easily maintained and verified for PCI compliance. What solution will meet this need with the least work?

- A. Cloud
- B. Autonomous
- C. FlexConnect
- D. Centralized



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 46

When using a Split MAC architecture, how many CAPWAP data tunnels will be built to an AP with four SSIDs across two VLANs?

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

Correct Answer: A

Section: (none)

Explanation**Explanation/Reference:****QUESTION 47**

A customer is using the access point GUI to upgrade the software on an autonomous access point to convert it to a lightweight access point. Which two transfer protocols are valid for conducting this transfer from the WLC? (Choose two.)

- A. FTP
- B. RCP
- C. SFTP
- D. HTTP
- E. SCP
- F. TFTP

Correct Answer: DF

Section: (none)

Explanation**Explanation/Reference:****QUESTION 48**

An engineer wants to set up guest wireless that requires users to log in via a splash page prior to accessing the network. Which authentication method should be configured?

- A. LDAP
- B. RADIUS
- C. local authentication
- D. WebAuth
- E. PSK

Correct Answer: D

Section: (none)

Explanation**Explanation/Reference:**

QUESTION 49

An engineer would like to setup secure authentication for a wireless network that will utilize single sign-on. Which two authentication methods can be used to accomplish this? (Choose two.)

- A. LDAP
- B. RADIUS
- C. Local authentication
- D. WEP
- E. PSK

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 50

What suite of algorithms results in slower connection rates when using 802.11N technology?

- A. WPA2
- B. CCMP
- C. TKIP
- D. AES

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 51

An engineer assists a user in configuring an Android device for authentication to an IEEE 802.1x EAP WLAN with PEAPv1. The Phase 2 authentication should be configured as which option?

- A. LEAP
- B. MSCHAPv2

- C. TLS
- D. TTLS

Correct Answer: B

Section: (none)

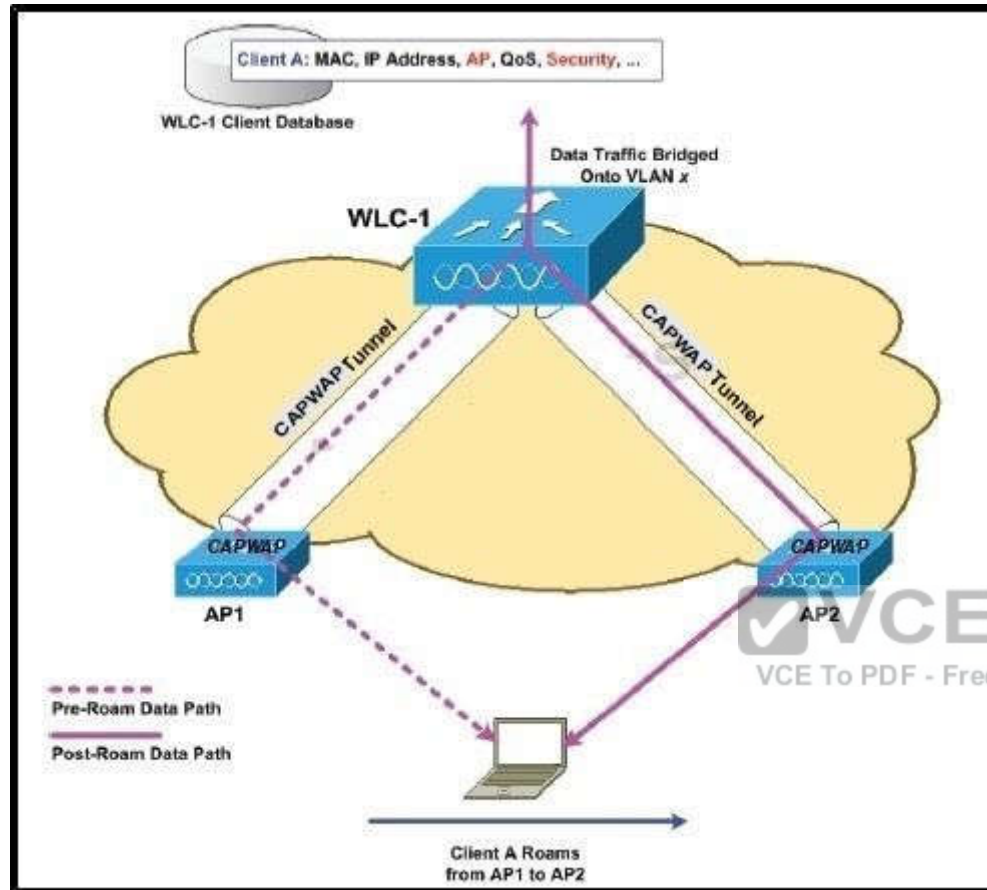
Explanation

Explanation/Reference:

QUESTION 52

Refer to the exhibit. Which two wireless functions is the client experiencing? (Choose two.)





- A. Inter-controller Roaming
- B. Intra-controller Roaming
- C. Layer 2 Roaming
- D. Layer 3 Roaming
- E. Inter-subnet roaming
- F. Re-authentication

Correct Answer: BC
Section: (none)

Explanation**Explanation/Reference:****QUESTION 53**

What is the approximate time difference for a client to perform an intracontroller roam compared to an intercontroller roam?

- A. 1 ms
- B. 10 ms
- C. 20 ms
- D. 30 ms

Correct Answer: B

Section: (none)

Explanation**Explanation/Reference:****QUESTION 54**

Which two attributes must be configured to match in order for WLCs to operate in the same mobility group? (Choose two.)

- A. mobility domain name
- B. virtual IP address
- C. service interface address
- D. hardware model
- E. software version

Correct Answer: AB

Section: (none)

Explanation**Explanation/Reference:****QUESTION 55**

Which operating mode is valid for controllers in a converged access architecture?

- A. switch peer groups
- B. mobility controller
- C. auto-anchor
- D. foreign anchor

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 56

An engineer wants to deploy a 2504 controller as the anchor controller for a guest WLAN that resides on a 5508 controller in a different mobility group. What configuration change must be applied to support this deployment strategy?

- A. UDP 16666 and IP Protocol 97 must be enabled on the 2504 controller
- B. UDP 5246 and TCP Protocol 97 must be enabled on the router
- C. The 2504 controller must be added to the same mobility group as the 5508.
- D. DHCP Option 43 must be added to the neighboring switchport

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 57

A help desk engineer is attempting to perform a remote packet capture on the wireless network. Which access point mode is necessary to perform this function?

- A. sniffer
- B. SE-Connect
- C. monitor
- D. rogue detector
- E. FlexConnect

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 58

Refer to the exhibit. A help desk ticket has been entered for the wireless infrastructure. A wireless client is not able to connect at IEEE 802.11n rates. Which option allows for connectivity?



General	Security	QoS	Policy-Mapping
Quality of Service (QoS) Gold (video) ▾			
Application Visibility <input checked="" type="checkbox"/> Enabled			
AVC Profile none ▾			
Netflow Monitor none ▾			
WMM			
WMM Policy Disabled ▾			
7920 AP CAC <input type="checkbox"/> Enabled			
7920 Client CAC <input type="checkbox"/> Enabled			
Media Stream			
Multicast Direct <input checked="" type="checkbox"/> Enabled			

- A. Set WMM mode to Optional or Required.
- B. Set Quality of Service (QoS) to Silver.
- C. Set Quality of Service (QoS) to Platinum.
- D. Set 7920 AP CAC to Enabled.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 59

An engineer has been asked to upgrade the FUS on the Wireless LAN controller. How can they monitor the status of the upgrade?

- A. WLC GUI
- B. WLC CLI
- C. WLC Console
- D. WLC Management in Prime Infrastructure

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



QUESTION 60

During a wireless site survey, the signal strength drops significantly when outside of the room containing the access point. The building is made of wood and drywall.

This is an example of which wireless anomaly?

- A. absorption
- B. refraction
- C. fading
- D. multipath
- E. reflection

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 61

Refer to the exhibit. The wireless engineer has deployed the Cisco 5508 Wireless Controller. The controller is responding on the service port; however, it will not respond on the management interface. Which configuration revision will fix the management interface?



WLC Management Interface Configuration

Interface Address

VLAN Identifier	<input type="text" value="10"/>
IP Address	<input type="text" value="172.30.1.30"/>
Netmask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="172.30.1.2"/>
IPv6 Address	<input type="text" value="::"/>
Prefix Length	<input type="text" value="128"/>
IPv6 Gateway	<input type="text" value="::"/>
Link Local IPv6 Address	<input type="text" value="fe80::d68c:b5ff:fec3:ee/64"/>

Physical Information

The interface is attached to a LAG. ☐

Enable Dynamic AP Management ☒

DHCP Information

Primary DHCP Server	<input type="text" value="172.30.1.20"/>
Secondary DHCP Server	<input type="text" value="172.30.1.21"/>
DHCP Proxy Mode	<input type="text" value="Global"/>
Enable DHCP Option 82	<input type="checkbox"/>

Switchport Configuration

```
Current configuration : 235 bytes
!
interface GigabitEthernet0/9
description 5508 Port 1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,20,30,40
switchport mode trunk
priority-queue out
mls qos trust dscp
spanning-tree portfast trunk
end
```

A. On the switch interface, configure switch(config-if)#switchport trunk allowed vlan add 10.

- B. On the WLC management interface, disable LAG on the management network.
- C. On the switch interface, configure switch(config-if)#switchport trunk allowed vlan 10.
- D. On the WLC management interface, change the VLAN ID to 20.
- E. On the switch interface, configure no spanning-tree portfast trunk.
- F. On WLC Controller > General, disable LAG and reboot.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 62

A wireless engineer has been asked to plan a deployment covering the aisles of a warehouse with optimal coverage while bleeding RF across aisles. Which antenna type provides the necessary coverage?

- A. patch
- B. omnidirectional
- C. Yagi
- D. parabolic dish



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 63

A help desk ticket states that a wireless access point has not joined its controller and is flashing rapidly. How can the help desk administer the access point with the default settings?

- A. console
- B. SSH
- C. Telnet
- D. HTTP
- E. HTTPS

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 64

After you configure the Cisco 5508 Wireless Controller v7.6, a customer requests an SSID that allows for client web authentication with email input. Which authentication method should be used?

- A. pass-through
- B. authentication
- C. splash page web redirect
- D. conditional web redirect
- E. on MAC filter failure

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 65

A customer has asked for the proper port configuration to allow for LAG on a Cisco 2504 Wireless Controller to a Cisco IOS switch. Which EtherChannel mode should be used on the switch to allow for the WLC to connect?

- A. on
- B. auto
- C. desirable
- D. passive
- E. active

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:**QUESTION 66**

A customer has asked for its wireless equipment to be managed as securely as possible. Which three management protocols will provide encrypted access to the equipment? (Choose three.)

- A. Secure Shell
- B. HTTPS
- C. SNMPv3
- D. Telnet
- E. SNMPv2c
- F. HTTP

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:**QUESTION 67**

Which method of encryption does the 802.11i standard use?

- A. AES/CCMP
- B. AES/ECB
- C. AES/OCB
- D. TKIP
- E. both AES/ECB and AES/CCMP

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Counter Mode Cipher Block Chaining Message Authentication Code Protocol, Counter Mode CBC-MAC Protocol or simply CCMP (CCM mode Protocol) is an encryption protocol designed for Wireless LAN products that implement the standards of the IEEE 802.11i amendment to the original IEEE 802.11 standard. CCMP is an enhanced data cryptographic encapsulation mechanism designed for data confidentiality and based upon the Counter Mode with CBC-MAC (CCM) of the AES

standard. It was created to address the vulnerabilities presented by WEP, a dated, insecure protocol.
<http://en.wikipedia.org/wiki/CCMP>

QUESTION 68

Which type of authentication is used initially by a controller-based AP so that a guest client can get an IP address?

- A. 802.1x
- B. EAP
- C. LEAP
- D. open authentication
- E. TLS
- F. SSL

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Open authentication allows any device to authenticate and then attempt to communicate with the access point. Using open authentication, any wireless device can authenticate with the access point, but the device can communicate only if its Wired Equivalent Privacy (WEP) keys match the access point's WEP keys. Devices that are not using WEP do not attempt to authenticate with an access point that is using WEP. Open authentication does not rely on a RADIUS server on your network.

<http://www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/SecurityAuthenticationTypes.html#wp1035025>

QUESTION 69

What is the maximum number of lightweight APs that can be supported from a single Cisco WCS Navigator management console with Cisco WCS and Cisco WLC running version 7.0 code?

- A. 10,000
- B. 20,000
- C. 25,000
- D. 30,000
- E. 60,000

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:**Explanation:**

The Cisco WCS Navigator supports partitioning of the unified wireless network at the management level. It supports up to 20 Cisco WCS management platforms with manageability of up to 30,000 Cisco Aironet lightweight access points from a single management console. It runs on a server platform with an embedded database.

QUESTION 70

Which two tasks does RRM routinely perform? (Choose two.)

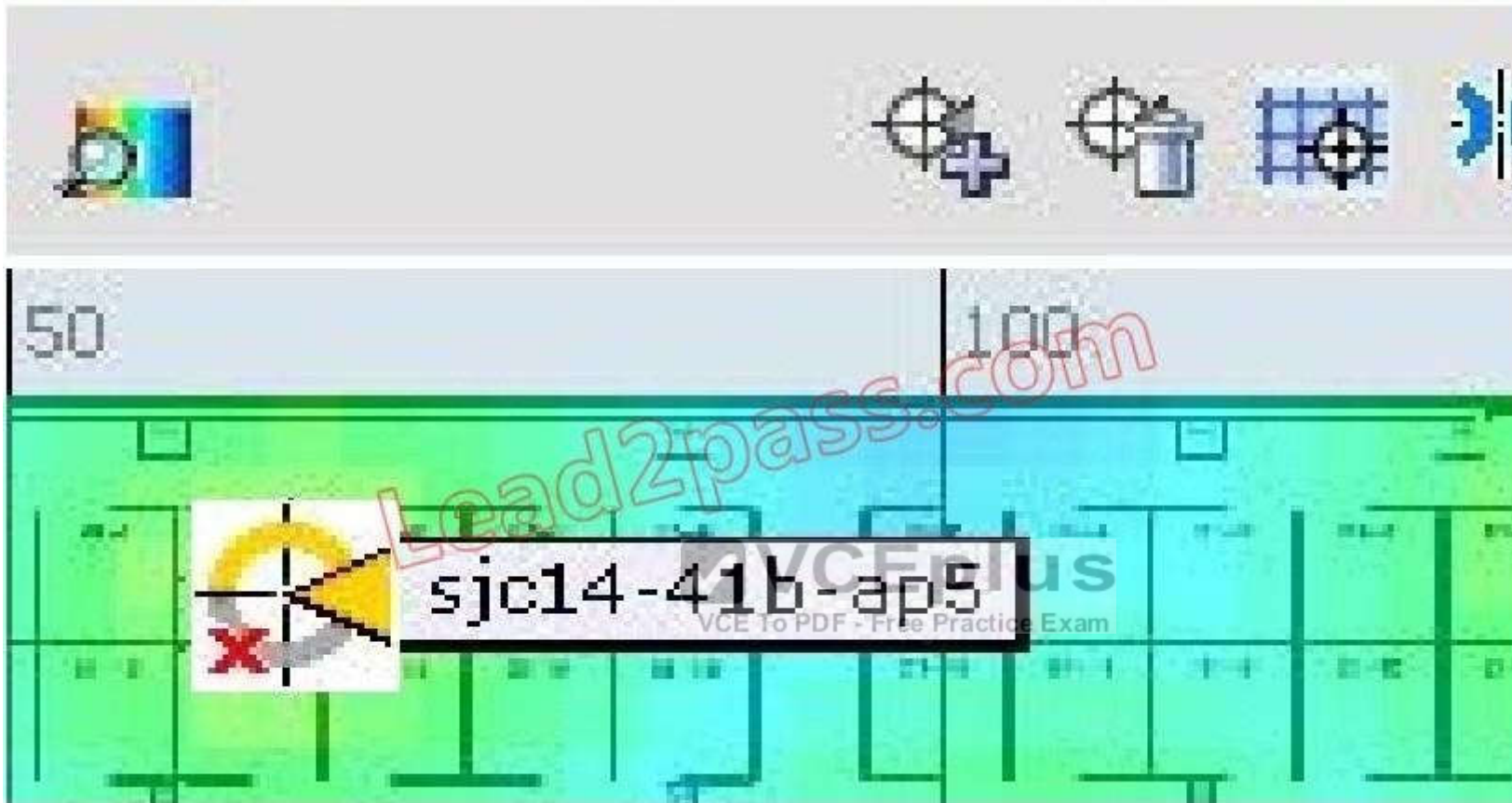
- A. antenna selection
- B. AP address assignment
- C. channel assignment
- D. encryption method assignment
- E. transmit power control

Correct Answer: CE

Section: (none)

Explanation**Explanation/Reference:****QUESTION 71**

Refer to the exhibit. Which two options does this icon represent about the status of the respective AP on a Cisco WCS version 7.0 map? (Choose two.)



- A. The 802.11a/n radio is administratively disabled.
- B. The 802.11a/n radio has a minor fault.
- C. The 802.11a/n radio has a major fault.
- D. The 802.11b/g/n radio is administratively disabled.
- E. The 802.11b/g/n radio has a minor fault.
- F. The 802.11b/g/n radio has a major fault.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

When Cisco WCS receives alarm messages from a controller, the Cisco WCS user interface displays an alarm indicator in the lower left corner in an alarm summary panel known as the alarm dashboard. The alarm dashboard only appears when the Macromedia flash is installed. Alarms indicate the current fault or state of an element that needs attention. These are usually generated by one or more events. The alarm can be cleared, but the event remains. An example of an alarm is AP down, which means that the current status of the access point is down.

QUESTION 72

In general, what is the difference in transmit power between an AP operating at Tx Power Level 1 and the same AP operating at Tx Power Level 3?

- A. 2 dB
- B. 3 dB
- C. 6 dB
- D. 11 dB
- E. 17 dB

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 73

Which two statements are true about WiMAX technology? (Choose two.)

- A. WiMAX is defined by 802.11i.
- B. Typically, fixed WiMAX networks have a higher gain direction antenna installed near the client.
- C. WiMAX is capable of working as a long-range system over several miles.
- D. WiMAX works only for licensed frequencies.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 74

Refer to the exhibit. Which menu gives you access to manage background tasks in Cisco WCS?

The screenshot shows the Cisco Wireless Control System (WCS) interface. The top navigation bar includes 'Monitor', 'Reports', 'Configure', 'Services', 'Administration', 'Tools', and 'Help'. The 'Monitor' tab is selected, showing 'WCS Home' with sub-tabs for 'General', 'Client', 'Security', 'Mesh', 'CleanAir', and 'ContextAware'. The 'General' sub-tab is active, displaying 'Inventory Detail Status' with pie charts for Controllers (1), Radios (4), and MSEs (0). It also shows 'Coverage Areas' with a table listing 'System Campus' and 'Recent Coverage Holes (0)'. A large 'VCEplus.com' watermark is overlaid on the interface.

- A. None, because the General tab provides access to the management of background tasks
- B. Monitor

- C. Configure
- D. Services
- E. Administration
- F. Tools

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The Administration menu enables you to schedule tasks like making a backup, checking a device status, auditing your network, synchronizing the MSE, and so on. It also contains Logging to enable various logging modules and specify restart requirements. For user administration such as changing passwords, establishing groups, setting application security settings, and so on, choose AAA. From the Administration Menu, you can also access the licensing information, set user preferences, and establish high availability (a secondary backup device running WCS).

http://www.cisco.com/c/en/us/td/docs/wireless/wcs/7-0/configuration/guide/WCS70cg/7_0wst.html#wp1060607

QUESTION 75

What is the difference between the IEEE, the WiFi Alliance, and the FCC, ETSI, and TELEC?

- A. The IEEE and FCC are responsible for the standards that apply to wireless networks. The WiFi Alliance, ETSI, and TELEC are the governmental agencies that regulate compliance with local standards.
- B. The IEEE is responsible for Layer 1 and Layer 2 protocols. The WiFi Alliance is responsible for interoperability testing. The FCC, ETSI, and TELEC are responsible for radio frequency and transmission power-level regulations and standards in the U.S., Europe, and Japan.
- C. The IEEE is responsible for Layer 1 and Layer 2 protocols. The FCC, ETSI, and TELEC are responsible for interoperability testing and compliance. The WiFi Alliance is responsible for radio frequency and transmission power-level regulations and standards on a global basis.
- D. The IEEE and FCC are responsible for the Layer 3 protocol support and frequency and power-level regulations in the United States. ETSI and TELEC are responsible for frequency and power-level regulations in Europe and Japan. The WiFi Alliance is responsible to interoperability testing.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The FCC is the local regulatory authority responsible for frequency regulation in the United States. ETSI is a European standards organization responsible for producing standards for information and communications technologies. The Wi-Fi Alliance is an interoperability testing organization. The IEEE creates standards, and WPA is a pre-802.11 certification by the Wi-Fi Alliance.

QUESTION 76

You are testing a new autonomous Cisco Aironet 1260 AP that has booted for the first time on the existing corporate network, which includes voice, data, and location services.

How do you reach the GUI of the AP?

- A. HTTP to 10.0.0.1.
- B. HTTP to 192.168.1.1.
- C. HTTP to the DHCP address.
- D. HTTPS to 10.0.0.1.
- E. HTTPS to the 192.168.1.1.
- F. HTTPS to the DHCP address.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Make sure DHCP is enabled on the network or DNS resolution is available. The access point must receive its IP address through DHCP or DNS resolution, and the GUI can be accessed by using HTTP to this address.

http://www.cisco.com/c/en/us/td/docs/wireless/access_point/1260/quick/guide/ap1260getstart.html

QUESTION 77

A WLAN deployment uses a combination of Cisco Aironet 1260 APs and multiple Cisco 5500 Wireless LAN Controllers to provide wireless LAN access to end-users. The network administrator has decided to use DHCP Option 43 to enable the APs to discover the wireless LAN controllers. When configuring the DHCP scope, which format should be used for the Cisco WLC addresses?

- A. a comma-separated ASCII string of Cisco WLC AP-manager addresses
- B. a comma-separated ASCII string of Cisco WLC management addresses
- C. a comma-separated ASCII string of Cisco WLC virtual IP addresses
- D. a hexadecimal string of Cisco WLC AP-manager addresses
- E. a hexadecimal string of Cisco WLC management addresses
- F. a hexadecimal string of Cisco WLC virtual IP addresses

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Complete these steps in order to configure DHCP Option 43, in the embedded Cisco IOS DHCP server, for all Cisco Aironet APs that run Cisco IOS. This includes all APs except for the VxWorks 1000 Series (see the next section) and the 600 Series OEAP which does not use Option 43.

```
ip dhcp pool <pool name>
network <ip network> <netmask>
default-router <default-router IP address>
dns-server <dns server IP address>
option 43 hex <hexadecimal string>
```

The hexadecimal string in step 3 is assembled as a sequence of the TLV values for the Option 43 suboption: Type + Length + Value. Type is always the suboption code 0xf1. Length is the number of controller management IP addresses times 4 in hex. Value is the IP address of the controller listed sequentially in hex.

<http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/97066-dhcp-option-43-00.html>

QUESTION 78

Which interface is considered a dynamic interface?

- A. the virtual interface
- B. the AP manager interface
- C. the LAG interface
- D. the management interface
- E. the service port interface
- F. a WLAN client data interface

Correct Answer: F

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Dynamic interfaces, also known as VLAN interfaces, are created by users and designed to be analogous to VLANs for wireless LAN clients. A controller can support up to 512 dynamic interfaces (VLANs). Each dynamic interface is individually configured and allows separate communication streams to exist on any or all of a controller's distribution system ports. Each dynamic interface controls VLANs and other communications between controllers and all other network devices, and each acts as a DHCP relay for wireless clients associated to WLANs mapped to the interface.

QUESTION 79

Which three items do you need to establish a wireless connection to an enterprise wireless network? (Choose three.)

- A. SSID name
- B. RF channel
- C. RF signal
- D. 802.1X/EAP credentials

- E. pre-shared key
- F. web page
- G. WPA/WPA2 settings

Correct Answer: ACD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Most clients enable you to associate to a detected network (broadcasted SSID) or configure a specific profile. In all cases, you must configure the network name (SSID), the operating mode (ad-hoc or infrastructure), and some security settings (that will be different depending on whether the SSID uses Pre-Shared Key Security or Enterprise [EAP/802.1x] security).

QUESTION 80

You have brought your MacBook Pro running OS 10.6 to work and intend use the enterprise wireless network. This network is using EAP-FAST and 2.4 GHz for data and 5 GHz for VoWLAN. Which statement about the laptop configuration and wireless connection is true?

- A. Install a USB wireless adapter and configure
- B. Install AppleEAP-Fast plug-in and configure
- C. Install Cisco AnyConnect v2.4 and configure
- D. Configure Apple network preferences for EAP-FAST
- E. The laptop does not support EAP-FAST and will be unable to connect
- F. The laptop only supports 5 GHz and will be unable to connect



Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

MacBook Pro using 10.6 supports 2.4Ghz only, so the EAP-FAST should be used. 5Ghz support was added to MacBook later.

QUESTION 81

Which Cisco AnyConnect module allows troubleshooting for core Cisco AnyConnect problems?

- A. telemetry
- B. web security
- C. VPN

- D. NAM
- E. DART
- F. posture
- G. CSSC

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation:

AnyConnect offers the DART module that can be used to analyze and troubleshoot connections. The information collected by DART can be examined locally or exported and sent to a network support desk for analysis.

QUESTION 82

Which Cisco AnyConnect module provides wireless connectivity?

- A. telemetry
- B. web security
- C. VPN
- D. NAM
- E. DART
- F. posture
- G. CSSC



Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The Cisco AnyConnect Secure Mobility Client is a multifunctional and modular security client. It was built to enable you to use the same interface across various hardware and software platforms (operating systems) to manage and secure your connections to the network. It contains several modules:

QUESTION 83

Which option is needed to earn the Cisco Compatible credential for Cisco Compatible Extensions Lite?

- A. Foundation and Management are required.

- B. Location and Management are required.
- C. Foundation and Location are required.
- D. Foundation and Voice are required.
- E. Voice is required.
- F. Foundation is required.
- G. Location is required.
- H. Management is required.

Correct Answer: F

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Historically, there have been five versions of the Cisco Compatible Extension (CCX) specification labeled Version 1(V1) to Version 5(V5). Each version built upon its predecessors. For example, CCXv5 added MFP, real-time reporting between client and AP, a diagnostic channel to help troubleshooting clients and optional location services, and improved several CCXv4 features. Each version contains a list of features. In summer 2011, Cisco separated the CCX features into four subfamilies to help vendors integrate only those features that are needed for their specific wireless clients (called application-specific devices, which are devices built for a specific function [for example, barcode scanners or VoWLAN phones] and therefore do not need all the CCX features that a data laptop would need).

QUESTION 84

In a typical wireless network using WPA, WPA2 or VPN, why is it still possible for a rogue client to launch a DOS attack?

- A. WPA and WPA2 are not considered strong encryption algorithms and are easily cracked.
- B. 802.11 management frames are easily compromised.
- C. Cisco Compatible Extensions v5 are required with WPA, WPA2, or VPN to keep rogues from launching attacks in the wireless network.
- D. The message integrity check frames are never encrypted or authenticated, which allows rogues to spoof clients.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A different receiver is needed for each 802.11a, b, g, and n radios, so using all simultaneously would severely impact the overall battery life of a mobile device.

QUESTION 85

Strong security is required, but a centralized RADIUS authenticator has not been implemented. Which two steps must you take to provide maximum security when using a pre-shared key? (Choose two.)

- A. Change the TKIP on a weekly basis.
- B. Use a key that includes mixed-case letters, numbers, and symbols with a length greater than 10 characters.
- C. Use only with WPA and WPA2, following proper strong key guidelines.
- D. Use the longest possible WEP key in your security policy.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Another form of basic security now available is WPA or WPA2 Pre-Shared Key (PSK). The PSK verifies users via a password, or identifying code, (also called a passphrase) on both the client station and the access point. A client may only gain access to the network if the client's password matches the access point's password. The PSK also provides keying material that TKIP or AES use to generate an encryption key for each packet of transmitted data. While more secure than static WEP, PSK is similar to static WEP in that the PSK is stored on the client station and can be compromised if the client station is lost or stolen. A strong PSK passphrase that uses a mixture of letters, numbers, and non-alphanumeric characters is recommended.

http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1200-access-point/prod_brochure09186a00801f7d0b.html

QUESTION 86

What is the impact of configuring a single SSID to support TKIP and AES encryption simultaneously?

- A. The overhead associated with supporting both encryption methods degrades client throughput significantly.
- B. Some wireless client drivers might not handle complex SSID settings and may be unable to associate to the WLAN.
- C. This configuration is unsupported and the Cisco Wireless Control System generates alarms continuously until the configuration is corrected.
- D. This configuration is common for migrating from WPA to WPA2. No problem is associated with using this configuration.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

AES encryption uses hardware so there is almost no overhead when using it. TKIP is based on software. So when we support both TKIP and AES the client throughput will not significantly degrade -> A is not correct.

When choosing both AES and TKIP, the router will support both encryption algorithms. Because not all wireless NICs support AES, some only support TKIP, so this option is probably the best

choice -> B is not correct.

As the picture below, Cisco Wireless Control System does support both simultaneously -> C is not correct.

QUESTION 87

Which key is established using the four-way handshake during the WPA authentication process?

- A. Pairwise Master Key
- B. Pairwise Multiple Key
- C. Pairwise Session Key
- D. Pairwise Transient Key
- E. Pairwise Transverse Key

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The authentication process leaves two considerations: the access point (AP) still needs to authenticate itself to the client station (STA), and keys to encrypt the traffic need to be derived. The earlier EAP exchange or WPA2-PSK configuration has provided the shared secret key PMK (Pairwise Master Key). To derive the PMK from the WPA-PSK, the PSK is put through PBKDF2-SHA1 as the cryptographic hash function. This key is, however, designed to last the entire session and should be exposed as little as possible. Therefore the four-way handshake is used to establish another key called the PTK (Pairwise Transient Key). The PTK is generated by concatenating the following attributes: PMK, AP nonce (ANonce), STA nonce (SNonce), AP MAC address, and STA MAC address. The product is then put through a pseudo random function.

http://en.wikipedia.org/wiki/IEEE_802.11i-2004

QUESTION 88

What are four features of WPA? (Choose four.)

- A. a larger initialization vector, increased to 48 bits
- B. a message integrity check protocol to prevent forgeries
- C. authenticated key management using 802.1X
- D. support for a key caching mechanism
- E. unicast and broadcast key management
- F. requires AES-CCMP

Correct Answer: ABCE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

TKIP and the related WPA standard implement three new security features to address security problems encountered in WEP protected networks. First, TKIP implements a key mixing function that combines the secret root key with the initialization vector before passing it to the RC4 initialization. WEP, in comparison, merely concatenated the initialization vector to the root key, and passed this value to the RC4 routine. This permitted the vast majority of the RC4 based WEP related key attacks. Second, WPA implements a sequence counter to protect against replay attacks. Packets received out of order will be rejected by the access point. Finally, TKIP implements a 64-bit Message Integrity Check (MIC).

To be able to run on legacy WEP hardware with minor upgrades, TKIP uses RC4 as its cipher. TKIP also provides a rekeying mechanism. TKIP ensures that every data packet is sent with a unique encryption key.

Key mixing increases the complexity of decoding the keys by giving an attacker substantially less data that has been encrypted using any one key. WPA2 also implements a new message integrity code, MIC. The message integrity check prevents forged packets from being accepted. Under WEP it was possible to alter a packet whose content was known even if it had not been decrypted.

http://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol

<http://documentation.netgear.com/reference/fra/wireless/WirelessNetworkingBasics-3-14.html>

QUESTION 89

When the enterprise-based authentication method is used for WPA2, a bidirectional handshake exchange occurs between the client and the authenticator. Which five options are results of that exchange being used on a controller-based network? (Choose five.)

- A. a bidirectional exchange of a nonce used for key generation
- B. binding of a Pairwise Master Key at the client and the controller
- C. creation of the Pairwise Transient Key
- D. distribution of the Group Transient Key
- E. distribution of the Pairwise Master key for caching at the access point
- F. proof that each side is alive

Correct Answer: ABCDF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Regardless of whether WPA or WPA2 is used during the initial connection between the station and the AP, the two agree on common security requirements. Following that agreement, a series of important key related activities occur in this specific order:

QUESTION 90

When a guest client is authenticated, which type of connection is created between the controller- based AP and the client?

- A. as SSL connection
- B. a TLS encrypted tunnel
- C. an unsecured connection

- D. a 802.1x/EAP tunnel
- E. an IPsec tunnel

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The wireless network at UNCG allows visitors to establish an unsecured connection. The unsecured network is available as a self-service wireless profile.
http://its.uncg.edu/Network_Services/Wireless/Connect/Guest/

QUESTION 91

When adding a controller to manage through Cisco WCS, which address type is used and which SNMP function does the Cisco WCS perform?

- A. The controller is managed through its MAC address and the Cisco WCS acts as a SNMP TRAP authenticator.
- B. The IP address of the controller is used and the Cisco WCS acts as a SNMP TRAP receiver.
- C. The controller is managed through its MAC address and the Cisco WCS acts as a SNMP agent.
- D. The controller connects through its MAC address to the Cisco WCS and the Cisco WCS uses the SNMP to manage the controller for all configured SNMP parameters.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 92

Which three severity levels are in the Cisco WCS alarm dashboard? (Choose three.)

- A. Critical
- B. Flash
- C. Major
- D. Minor
- E. Trivial
- F. Urgent

Correct Answer: ACD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Alarms are color coded as follows:

Red --Critical Alarm

Orange --Major Alarm

Yellow --Minor Alarm

The Alarm Summary displays the number of current critical, major, and minor alarms.

http://www.cisco.com/c/en/us/td/docs/wireless/wcs/6-0/configuration/guide/WCS60cg/6_0event.html

QUESTION 93

The existing Cisco Unified Wireless Controller is running version 7.0 code for both the controllers and the Cisco WCS. A controller has been configured with an appropriate rogue rule condition to report discovered APs to the Cisco WCS.

Which default alarm level is used to display all rogue APs in the Alarm Summary?

- A. Critical
- B. Flash
- C. Urgent
- D. Major
- E. Minor



Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Yellow-Minor alarm is used to display all rogue Aps in alarm summary.

QUESTION 94

Which Cisco WCS tool allows you to view current reports, open specific types of reports, create and save new reports, and manage scheduled runs?

- A. Reports menu
- B. Reports launch page
- C. Scheduled Run results
- D. saved reports

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The report launch pad provides access to all NCS reports from a single page. From this page, you can view current reports, open specific types of reports, create and save new reports, and manage scheduled runs.

<http://www.cisco.com/c/en/us/td/docs/wireless/ncs/1-0/configuration/guide/NCS10cg/rep.html#wp1089982>

QUESTION 95

Which path do you take to manage the results of a report that had been run on network utilization?

- A. Reports > Report Launch Pad > Device > Utilization
- B. Reports > Report Launch Pad > Scheduled Run Results
- C. Reports > Saved Reports > Scheduled Run Results
- D. Reports > Scheduled Run Results

Correct Answer: D

Section: (none)

Explanation



Explanation/Reference:

Explanation:

There are five menus on each window: Monitor, Reports, Configure, Location, Administration , and Help. When you move the mouse over any of the menus, a drop-down menu appears.

QUESTION 96

Which CLI command is used on a Cisco WLC to troubleshoot mobility, rogue detection, and load- balancing events?

- A. debug dot11
- B. debug capwap all
- C. show dot11 details
- D. show capwap details

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:**Explanation:**

http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-3/command/reference/cr73/b_cr_7-3_chapter_010.html#wp3619872221

QUESTION 97

Which three WLC debug commands are appropriate to troubleshoot a wireless client that is associated to an AP? (Choose three.)

- A. debug capwap
- B. debug mac addr
- C. debug dot11
- D. debug dhcp
- E. debug ap
- F. debug dtls

Correct Answer: BCD

Section: (none)

Explanation

Explanation/Reference:**Explanation:**

See reference link for associated WLC debug commands.

"WLC Debug and Show Commands"

<http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/112064-wlc-commands.html>

**QUESTION 98**

Which command path correctly describes how to access and troubleshoot clients with Cisco WCS version 7.0?

- A. Tools > Clients > select displayed client's MAC address
- B. Tools > Clients > enter client's MAC address
- C. Monitor > Clients > click displayed client's MAC address
- D. Monitor > Clients > enter client's MAC address

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:**Explanation:**

http://www.cisco.com/c/en/us/td/docs/wireless/prime_infrastructure/1-2/configuration/guide/pi_12_cg/clientmgmt.html

QUESTION 99

Which single tool helps to troubleshoot client-related issues in a WLAN?

- A. The show and debug commands on the controller.
- B. The show commands on the AP.
- C. Client templates on the Cisco WCS.
- D. Client troubleshooting on the Cisco WCS.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

<http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/107585-client-con.html>

QUESTION 100

Which option best describes the limitation of a client that is attempting to manage a WLC while using the client wireless adapter connection to the wireless infrastructure?

- A. Controllers must be managed using only secure protocols (that is, SSH and HTTPS), not nonsecure protocols (that is, HTTP and Telnet).
- B. Read-write access is not available; only read-only access is supported.
- C. Uploads and downloads from the controller are not allowed.
- D. Wireless clients can manage other controllers, but not the same controller and the AP to which the client is associated.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The Cisco WLAN Solution Management over Wireless feature allows Cisco WLAN Solution operators to monitor and configure local WLCs using a wireless client. This feature is supported for all management tasks, except uploads to and downloads from (transfers to and from) the WLC.

<http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/69561-wlc-faq.html>

QUESTION 101

Refer to the exhibit. With the current Cisco WLC version 7.0 syslog level settings set the way they are, which log levels are captured by the Syslog server?

Management

- Summary
- ▼ **SNMP**
 - General
 - SNMP V3 Users
 - Communities
 - Trap Receivers
 - Trap Controls
 - Trap Logs
- HTTP-HTTPS**
- Telnet-SSH**
- Serial Port**
- Local Management Users**
- User Sessions**
- ▼ **Logs**
 - Config
 - Message logs

Syslog Configuration

Syslog Server IP Address

Syslog Server

Syslog Level

Syslog Facility

Msg Log Configuration

Buffered Log Level

Console Log Level

File Info ☒

Trace Info ☒

- A. syslog level errors only
- B. all syslog levels
- C. only the syslog severity level number of error and greater
- D. only the syslog severity level number of error and less

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Here the syslog level is set to errors, so it will send all logs with a severity level of errors, as well as all other messages with a greater severity level.

QUESTION 102

Which two statements about beacon frames used by access points are true? (Choose two.)

- A. They contain SSIDs if this feature is enabled.
- B. They provide vendor proprietary information.

- C. They are another name for an associated request.
- D. They are sent in response to a probe frame.
- E. They include ATIM window information for power save operations.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Probably the most common 802.11 management frame is the beacon frame.

Beacon frame from a Cisco WLAN

Here we can easily make out some of the capabilities of the WLAN, for example the SSID is probably going to be the first thing you notice TestSSID in this case, this is what provides the name of the WLAN. As you know SSID broadcasting can be disabled (Also called Closed System) at which point the SSID field will be blank.

Now, at the end of the beacon frame you will notice all this Unknown information, as you have probably guessed (or read) this information is vendor specific, which is common for every vendor to have put their own proprietary information within the Beacon frames.

<http://ccie-or-null.net/2011/06/22/802-11-beacon-frames/>

QUESTION 103

Which two actions are best for deploying VoWLAN on a wireless network? (Choose two.)

- A. Minimize the use of Class 3 Bluetooth devices.
- B. Minimize the use of analog cameras.
- C. Minimize the use of IP cameras.
- D. Maximize client access by enabling all data rates used by clients.
- E. Maximize client access by enabling only a few high data rates used by clients.

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Analog cameras can operate in the same frequency of the wireless network, causing interference. The goal in setting the data rates for the VoWLAN network is to match the data rates of VoWLAN handsets as closely as possible, enabling a few high data rates used by the clients.

http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper/ch9_Voic.html

QUESTION 104

What is the equivalent of 26 dBm in milliwatts?

- A. 4 mW
- B. 40 mW
- C. 100 mW
- D. 400 mW
- E. 1000 mW

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

$\text{dBm} = \log_{10}(\text{mW}) \times 10$

$\text{mW} = 10^{(\text{dBm}/10)}$

Samples:

40 dBm=10.00 watts

36 dBm=4.00 watts

30 dBm=1.00 watts

27 dBm=500 milliwatts

26 dBm=400 milliwatts

<http://www.h-peters.com/dbmtomw.html>



QUESTION 105

What is the EIRP value for a transmitter that has a transmitter capable of 15 dBm, an antenna that has a gain of 12 dBi, and a cable that connects the transmitter to the antenna that has 1 db loss?

- A. 26 dBm
- B. 100 mW
- C. .86 dBm
- D. 165 dBm
- E. 1000 mW

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

To determine EIRP follow this equation:

<Transmit Power> -Cable Loss + Antenna Gain = EIRP

So in this case $15 - 1 + 12 = 26$

QUESTION 106

What are three primary components that describe TKIP? (Choose three.)

- A. broadcast key rotation
- B. dynamic WEP
- C. message integrity check
- D. per-packet key hashing
- E. symmetric key cipher
- F. WPA2 enterprise mode

Correct Answer: ACD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

TKIP uses the same underlying mechanism as WEP, and consequently is vulnerable to a number of similar attacks. The message integrity check, per-packet key hashing, broadcast key rotation, and a sequence counter discourage many attacks. The key mixing function also eliminates the WEP key recovery attacks.

http://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol

QUESTION 107

When an AP, in its default configuration mode, connects to a Cisco WLC, which methods are available for remote management access to an AP?

- A. SSL and SSH are available only after configuration by a Cisco WLC version 7.0.
- B. SSH only
- C. HTTPS, and SSH
- D. SSH and Telnet
- E. SSH and Telnet are available only after configuration by a Cisco WLC version 7.0.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

In Wireless LAN Controller release 5.0 and later, the controller supports the use of Telnet or Secure Shell (SSH) protocols to troubleshoot lightweight access points. You can use these protocols in order to make debugging easier, especially when the access point is unable to connect to the controller. You can configure Telnet and SSH support only through the controller CLI.
<http://www.cisco.com/c/en/us/support/docs/wireless/aironet-1200-series/70278-lap-faq.html>

QUESTION 108

Which three options are limitations when configuring basic security on an autonomous AP when using the express security page setup? (Choose three.)

- A. You need multiple SSIDs.
- B. Delete all the SSIDs.
- C. Edit the SSIDs.
- D. Use multiple authentication servers.
- E. Use the same SSID on both radios.
- F. Use a single SSID on a single radio.

Correct Answer: CDE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The security settings in the Easy Setup Radio Configuration section are designed for simple configuration of basic security. The options available are a subset of the wireless device security capabilities. Keep these limitations in mind when using the Express Security page:

http://www.cisco.com/c/en/us/td/docs/wireless/access_point/15_2_4_JB/configuration/guide/scg15-2-4-Book/scg15-2-4-chap4-first.html

QUESTION 109

Which two items are used to help convert a lightweight AP into an autonomous AP? (Choose two.)

- A. HTTP express setup on the AP
- B. Cisco WCS template
- C. Cisco WLC CLI
- D. Windows Cisco Conversion Tool
- E. image with naming convention of platform_name-k9w7-tar.default
- F. image with naming convention of platform_name-rcvk9w8-tar

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:**Explanation:**

See video tutorial in this process at the reference link below:

<https://supportforums.cisco.com/video/11928901/lwapp-lightweight-mode-autonomous-conversion-and-vice-versa>

QUESTION 110

Which three AP modes of operation allow for the wIPS sub mode? (Choose three.)

- A. local mode
- B. bridge mode
- C. monitor mode
- D. H-REAP mode
- E. rogue detector mode
- F. SE-Connect mode
- G. sniffer mode

Correct Answer: ACD

Section: (none)

Explanation**Explanation/Reference:****Explanation:**

Only Cisco Aironet 1130, 1140, 1240, 1250, 3502E and 3502I Series Access Points support wIPS monitor mode.

The wIPS sub mode is supported only when access point mode is Monitor, Local or HREAP. But for 1130 and 1240 access points, wIPS is supported only in Monitor Mode.

http://www.cisco.com/c/en/us/td/docs/wireless/mse/3350/7-0MR1/wIPS/configuration/guide/wIPS_70MR1/msecg7x_ch6_wIPS.html

QUESTION 111

A lightweight AP has been deployed in local mode in a network that consists of 10 wireless LAN controllers in a single mobility group. The AP has been configured to use primary, secondary, and tertiary Cisco WLCs. Due to a major power failure, all those Cisco WLCs are unavailable.

Which step does the AP take next?

- A. The AP reboots and repeatedly attempts to join the configured primary, secondary, and tertiary Cisco WLCs in that order. The process continues until one of the configured Cisco WLCs is available.
- B. The AP attempts to join a Cisco WLC configured as a master controller.
- C. The AP attempts to join the Cisco WLC that has the greatest capacity available.
- D. The AP state transitions to AP Fallback Mode and continues to provide limited WLAN services (that is, no new client authentications) until a Cisco WLC is available.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

If a WLC is configured as a Master Controller, the LAP selects that WLC and sends it an LWAPP join request.

<http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/70333-lap-registration.html>

QUESTION 112

An AP using version 7.0 MR1 broadcasts a Layer 3 CAPWAP discovery message on the local IP subnet. Which step does the AP take next?

- A. Determine if the controller responses include the primary controller.
- B. Determine if the controller responses include the master controller.
- C. Send a discovery request using DHCP option 43.
- D. Send a discovery request using DNS.
- E. Send a discovery request using locally stored information on the AP.
- F. Send a discovery request using OTAP.

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation:

If the LAP was registered to a WLC in a previous deployment, the LAP maintains the list of WLC

IP addresses locally in NVRAM. The stored WLC IP addresses include all of the WLCs that are in previously joined WLC "mobility groups". This is the discovery process:

<http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/70333-lap-registration.html#topic2>

QUESTION 113

Which three Cisco Unified Wireless Network capabilities use information that is provided by Radio Resource Management neighbor messages? (Choose three.)

- A. aggressive load balancing
- B. dynamic channel assignment
- C. hybrid remote edge access point
- D. intercontroller mobility (that is, mobility groups)
- E. over-the-air provisioning

F. rogue AP classification

Correct Answer: BEF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

First we should learn how the RRM works:

1) Controllers (whose APs need to have RF configuration computed as a single group) are provisioned with the same RF Group Name. An RF Group Name is an ASCII string each AP will use to determine if the other APs they hear are a part of the same system. (RF groups are groups of controllers that share the same RF group name and whose APs can hear the neighbor messages of each other)

2) APs periodically send out Neighbor Messages, sharing information about themselves, their controllers, and their RF Group Name. These neighbor messages can then be authenticated by other APs sharing the same RF Group Name.

3) APs that can hear these Neighbor Messages and authenticate them based on the shared RF Group Name, pass this information (consisting primarily of controller IP address and information on the AP transmitting the neighbor message) up to the controllers to which they are connected.

4) The controllers, now understanding which other controllers are to be a part of the RF Group, then form a logical group to share this RF information and subsequently elect a group leader.

5) Equipped with information detailing the RF environment for every AP in the RF Group, a series of RRM algorithms are used to optimize AP configurations. Information from Radio Resource Management (RRM) monitors the radio resources, performs dynamic channel assignments, provides detection and avoidance of interference, and provides the dynamic transmit power control (TPC).

The RRM neighbor message contains the following information:

* Radio Identifier: If the AP had multiple radios, this field identifies the radio used to transmit the message.

* Group ID: The 16-bit value and controller MAC address. This information is used to detect rogue access points. The access points will then check the beacon/probe-response frames in neighboring access point messages to see if they contain an authentication information element (IE) that matches that of the RF group. If the check is successful, the frames are authenticated. Otherwise, the authorized access point reports the neighboring access point as a rogue, records its BSSID in a rogue table, and sends the table to the controller.

* WLC IP Address: RF group leader's management IP address. This address is discovered through Over-the-Air Provisioning (OTAP)

* AP Channel: The native channel that the AP uses to service clients.

* Neighbor Message Channel: The channel the message is sent on.

* Power: The power level at which the message is transmitted.

* Antenna Pattern: The antenna pattern currently in use

Note:

Dynamic channel assignment is used to dynamically allocate access point channel assignments to avoid conflict and to increase capacity and performance. For example, two overlapping channels in the 802.11g band, such as 1 and 2, cannot both simultaneously use 54 Mbps. By effectively reassigning channels, the controller keeps adjacent channels separated, thereby avoiding this problem.

Over-the-Air Provisioning (OTAP) is a method for APs to discover the management IP of a controller over the air.

A rogue AP is an AP that is unknown to the controller.

http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a008072c759.shtml <http://www.cisco.com/en/US/docs/wireless/controller/5.2/configuration/guide/c52rrm.html>

QUESTION 114

A controller is connected to a Cisco Catalyst switch. The switch port configuration looks like this:

```
interface GigabitEthernet 1/0/10
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,20,30,50
switchport trunk native vlan 20
switchport mode trunk
```

Which controller CLI command assigns its management interface to the native VLAN interface of the Cisco Catalyst switch?

- A. config interface vlan management 0
- B. config interface vlan management 1
- C. config interface vlan management 20
- D. config interface vlan management 30
- E. config interface vlan management 50

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 115

Which three options relate to event-driven RRM? (Choose three.)

- A. any 802.11n AP models
- B. specific AP models
- C. minimum of AP and WLC
- D. minimum of AP, WLC, and WCS
- E. minimum of AP, WLC, WCS, and MSE
- F. configurable in WLC at 802.11b/g/n > RRM > TPC
- G. configurable in WLC at 802.11b/g/n > RRM > DCA

Correct Answer: BCG

Section: (none)

Explanation

Explanation/Reference:**Explanation:**

<http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-0/configuration/guide/c70/c70cleanair.html>

QUESTION 116

In the AP Layer 3 controller discovery process, after the LWAPP Discovery Request is broadcast on a local subnet, what is the next step that the AP takes?

- A. Determine whether the controller responses are the primary controller.
- B. Send an LWAPP discovery request to controllers learned via OTAP if operational.
- C. Send an LWAPP response to the master controller if known.
- D. Wait 5 seconds and resend a Discovery Request to the local subnet.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:**QUESTION 117**

Why are wireless analog video signals that are operating in the 2.4-GHz band particularly harmful to Wi-Fi service?

- A. Analog video is a strong signal and increases the SNR.
- B. Analog video is a constant signal with 100% duty cycle.
- C. Analog video signals are slow frequency hopping and tend to affect the entire band.
- D. Analog Video modulation is the same as Wi-Fi and causes interference.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:**QUESTION 118**

What security benefit is enabled by using Management Frame Protection?

- A. Provides encryption of administrator sessions between a wireless client and a wireless LAN controller.
- B. Protects the network infrastructure from denial-of-service attacks that attempt to flood the network with associations and probes.

- C. Prevents the formation of client ad hoc networks within the RF coverage domain.
- D. Detects network reconnaissance probes, like those used by tools like NetStumbler, that attempt to discover the wireless network topology.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 119

The corporate network locates all RADIUS servers at the centralized data center for authentication. The remote offices use access points operating in H-REAP mode using v5.0 code with various local and central switch WLANs. When a remote office has lost connectivity to the main corporate network due to a WAN outage, which two statements correctly describe the status of that remote office when H-REAP access points are operating in standalone mode? (Choose two.)

- A. All Cisco APs with 16 MB of RAM or more can operate as standalone H-REAP.
- B. All clients will continue association until the respective authentication timers expire.
- C. If configured, clients using WPA or WPA2 with PSK and locally switched WLANs will continue to operate.
- D. If configured, locally switched WLANs will continue operation using the backup RADIUS server feature.
- E. If configured, locally switched WLANs will continue operation using Local-EAP for EAP-LEAP and EAP-FAST for up to twenty users.
- F. If configured, locally switched WLANs will continue operation using Local-EAP for EAP-LEAP, EAP-FAST, EAP-TLS, and EAP-PEAP for up to twenty users.

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 120

An AP has been configured for personal wireless access to the Internet using appropriate security and cloaking. Which two items should be configured on the wireless client? (Choose two.)

- A. RF channel
- B. BSS
- C. PSK
- D. 802.1X/EAP
- E. broadcast SSID

- F. manual SSID
- G. IBSS

Correct Answer: CF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Neighboring APs offering the same connection type and parameters use the same name, or service set identifier (SSID, which is a simple ASCII string providing a name to the connection). Neighboring APs offering the same connection use the same SSID, but each AP identifies itself by associating its radio MAC address to the SSID string. This associated MAC address is called the basic service set identifier (BSSID), and it enables stations to know which AP offers which SSID

QUESTION 121

The introduction of consumer phones and tablets into enterprise WLANs can have an impact on 802.11a/b/g/n deployments. The Apple iPhone 4 and iPad 2 are very common examples. Which statement best describes the abilities of these devices?

- A. The Apple iPhone 4 and the iPad 2 use 2.4 GHz and 5 GHz. The Apple iPhone 4 uses only one spatial stream and the iPad 2 uses two spatial streams.
- B. The Apple iPhone 4 uses only 2.4 GHz and the iPad 2 only uses 5 GHz. The Apple iPhone 4 uses only one spatial stream and the iPad 2 uses two spatial streams.
- C. The Apple iPhone 4 uses 2.4 GHz and the iPad 2 uses 2.4 GHz or 5 GHz. The Apple iPhone 4 only uses one spatial stream and the iPad 2 uses two spatial streams.
- D. The Apple iPhone 4 uses 2.4 GHz and the iPad 2 uses 2.4 GHz or 5 GHz. The Apple iPhone 4 and the iPad 2 use only one spatial stream.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The apple iPhone 4 and iPad2 supports only 2.4 Ghz (no 5 Ghz) wireless networks. Support for 5Ghz networks was introduced with the Apple iPhone5 and the iPad 3.

QUESTION 122

Which key combination provides a detailed wireless connection status for an Apple MacBook running 10.6?

- A. Command + Click the SSID of the network
- B. Alt + Click the SSID of the network
- C. Command + the Airport icon

- D. Option + the Airport icon
- E. Ctrl + the Airport Icon
- F. Option + Click the SSID of the network

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You can hold the Option Key while clicking the Airport icon in the menu bar. This will provide you with more information about your connection status such as: data rate, signal strength, channel, etc.

<http://www.swilliamsgroup.com/3-ways-to-display-your-ssid-on-your-macbook/>

QUESTION 123

You are in a coffee shop and you have connected to their wireless hot-spot. Your Windows 7 wireless client shows five green bars with a yellow shield. Which statement about the level of signal strength and the WLAN security that is present is true?

- A. You have excellent signal strength and a secure network connection.
- B. Your wireless client needs a username and password before it can connect to the WLAN.
- C. You have excellent signal strength and the client is waiting for you to enter a username and password.
- D. Your laptop is not receiving a signal.
- E. Your laptop is receiving an excellent signal and the network security is open.

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Five green bars means that the signal you are receiving is excellent (there are up to 5 bars) and the yellow shield is a warning indication signal that the security settings have been set to open, meaning no authentication is needed.

QUESTION 124

You are sitting in an airport preparing to use a free WLAN. When you look at the connections in your Windows 7 wireless client, you see a network name and three boxes with a yellow shield.

What does this mean?

- A. You cannot connect to this WLAN.

- B. An open ad hoc network is nearby.
- C. The WLAN in the airport is open.
- D. A secure ad hoc network is nearby.
- E. A secure WLAN is in the airport.
- F. You must provide a username and password to access the WLAN in the airport.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You can connect to a detected network by clicking the wireless connection icon in the status bar, clicking an SSID name (the signal strength of the associated AP is represented by green bars, five bars representing the best signal; an exclamation mark inside a yellow shield is displayed if the SSID has no security [Open authentication, no encryption]), clicking Connect and completing the security parameters when applicable.

<http://www.ciscopress.com/articles/article.asp?p=2131139>

QUESTION 125

How are application-specific devices differentiated from laptop computers in the way they support Cisco Compatible Extensions?

- A. ASDs are required to support only Cisco Compatible Extensions v1 and v2 features. Laptops must support all Cisco Compatible Extensions features.
- B. ASDs are required to support only Cisco Compatible Extensions v5 management features, while laptops are required to support optional features.
- C. Several features that are required for laptops are not required for ASDs.
- D. There is no differentiation. ASDs and laptops must both support the same Cisco Compatible Extensions features.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

In each version of CCX some features are classified as optional for ASDs. Examples of ASDs are medical devices, mobile computers, smartphones, and printers. The CCX specification for ASDs is a subset of the CCX specification for laptops. Some CCX features are not required for ASDs because many ASDs lack the computing power or operating system foundation required to support the features.

<http://incenter.medical.philips.com/doclib/enc/fetch/2000/4504/577242/577243/577246/581601/711562/>

The_Value_of_CCX_for_Philips_PageWriter_Cardiographs.pdf%3fnodeid%3d5784998%26vernum%3d1

QUESTION 126

Which Cisco AnyConnect module allows troubleshooting for core AnyConnect problems?

- A. telemetry
- B. web security
- C. VPN
- D. NAM
- E. DART
- F. posture
- G. CSSC

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation:

AnyConnect offers the DART module that can be used to analyze and troubleshoot connections. The information collected by DART can be examined locally or exported and sent to a network support desk for analysis.

QUESTION 127

Which Cisco AnyConnect module provides wireless connectivity?

- A. telemetry
- B. web security
- C. VPN
- D. NAM
- E. DART
- F. posture
- G. CSSC

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The main components used in IUWNE are the Cisco AnyConnect Mobility Client itself, associated with the Network Access Module (NAM) used to manage existing profiles and provide the wireless connectivity.

QUESTION 128

Cisco Client Management Frame Protection is running on a mobility group with two controllers. Which two MFP requirements protect the network? (Choose two.)

- A. forces clients to authenticate, using a secure EAP method only
- B. implements the validation of wireless management frames
- C. requires Cisco Compatible Extensions v5
- D. requires the use of a nonbroadcast SSID
- E. requires Cisco Compatible Extensions v4

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Client MFP encrypts class 3 management frames sent between APs and Cisco Compatible Extension version 5 (CCXv5) --capable client stations, so that both AP and client can take preventive action by dropping spoofed class 3 management frames (management frames) that are passed between an AP and a client station that is authenticated and associated). Client MFP leverages the security mechanisms defined by IEEE 802.11i to protect class 3 unicast management frames. The unicast cipher suite that is negotiated by the STA in the reassociation request's Robust Security Network Information Element (RSNIE) is used to protect both unicast data and class 3 management frames. An AP in workgroup bridge mode, repeater mode, or no-root bridge mode must negotiate either Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard-Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP) to use Client MFP. Management Frame Protection operation requires a wireless domain service (WDS). MFP is configured at the wireless LAN solution engine (WLSE), but you can manually configure MFP on an AP and WDS.

http://www.cisco.com/c/en/us/td/docs/routers/access/3200/software/wireless/3200WirelessConfig_Guide/ManageFrameProt.html

QUESTION 129

Which open standard defines the combination of Extensible Authentication Protocol with Advanced Encryption Standard for providing strong wireless LAN client security?

- A. IEEE 802.1X
- B. IEEE 802.11i
- C. WEP
- D. WPA
- E. WPA2

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:**Explanation:**

802.11i supersedes the previous security specification, Wired Equivalent Privacy (WEP), which was shown to have security vulnerabilities. Wi-Fi Protected Access (WPA) had previously been introduced by the Wi-Fi Alliance as an intermediate solution to WEP insecurities. WPA implemented a subset of a draft of 802.11i. The Wi-Fi Alliance refers to their approved, interoperable implementation of the full 802.11i as WPA2, also called RSN (Robust Security Network). 802.11i makes use of the Advanced Encryption Standard (AES) block cipher, whereas WEP and WPA use the RC4 stream cipher.
http://en.wikipedia.org/wiki/IEEE_802.11i-2004

QUESTION 130

When a wireless client is authenticated in a controller-based wireless network, which three pieces of source identification information can be used by the controller for an Access-Request message that is sent to an external RADIUS server? (Choose three.)

- A. wireless client IP address
- B. controller IP address
- C. AP IP address
- D. wireless client MAC address
- E. controller MAC address
- F. AP MAC address

Correct Answer: BEF

Section: (none)

Explanation**Explanation/Reference:****Explanation:**

From the Call Station ID Type drop-down list, choose IP Address, System MAC Address, or AP MAC Address to specify whether the IP address, system MAC address, or AP MAC address of the originator will be sent to the RADIUS server in the Access-Request message.
<http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-0/configuration/guide/c70/c70sol.html#wp1389032> (Step 3)

QUESTION 131

Which official port should be used when configuring external RADIUS authentication on a Cisco WLC version 7.0?

- A. 49
- B. 1645
- C. 1646
- D. 1812
- E. 1813

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

RADIUS authentication uses UDP port 1812, while accounting uses UDP port 1813. Early implementations of RADIUS used ports 1645 and 1646, but that usage is obsolete.

http://docstore.mik.ua/oreilly/networking_2ndEd/fire/ch21_07.htm

QUESTION 132

How many RADIUS servers can be configured globally and per WLAN on a Cisco WLC version 7.0?

- A. 7 global; additional 1 per WLAN
- B. 7 global; additional 3 per WLAN
- C. 17 global; additional 1 per WLAN
- D. 17 global; additional 3 per WLAN
- E. 7 global; reuse of up to 1 maximum per WLAN
- F. 17 global; reuse of up to 1 maximum per WLAN
- G. 17 global; reuse of up to 3 maximum per WLAN

Correct Answer: G

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You can configure up to 17 RADIUS authentication and accounting servers each.

For example, you may want to have one central RADIUS authentication server but several RADIUS accounting servers in different regions. If you configure multiple servers of the same type and the first one fails or becomes unreachable, the controller automatically tries the second one, then the third one if necessary, and so on.

<http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-0/configuration/guide/c70/c70sol.html>

QUESTION 133

Which statement about the impact of configuring a single SSID to support TKIP and AES encryption simultaneously is true?

- A. The overhead associated with supporting both encryption methods significantly degrades client throughput.
- B. Some wireless client drivers might not handle complex SSID settings and may be unable to associate to the WLAN.
- C. This configuration is unsupported and the Cisco Wireless Control System generates alarms continuously until the configuration is corrected.
- D. This configuration is common for migrating from WPA to WPA2. No problem is associated with using this configuration.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

AES encryption uses hardware so there is almost no overhead when using it. TKIP is based on software. So when we support both TKIP and AES the client throughput will not significantly degrade -> A is not correct.

When choosing both AES and TKIP, the router will support both encryption algorithms. Because not all wireless NICs support AES, some only support TKIP, so this option is probably the best choice -> B is not correct.

As the picture below, Cisco Wireless Control System does support both simultaneously -> C is not correct.

QUESTION 134

When the pre-shared key authentication method is used for WPA or WPA2, for which two functions is the pre-shared key used? (Choose two.)

- A. to act as the Group Transient Key during the bidirectional handshake
- B. to act as the Pairwise Master Key during the bidirectional handshake
- C. to derive the nonce at each side of the exchange
- D. to derive the Pairwise Transient Key

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Pre-shared key (PSK) is computed based on a shared secret (pass-phrase) which was previously shared between the two parties using some secure channel before it needs to be used. It is used to identify both peers to each other.

The strength of the PSK depends on the strength of the pass-phrase. The strength of the PSK is important, because WPA-Personal (and WPA2-Personal) use the PSK as the Pairwise Master Key (PMK). The PMK, when combined with two random numbers (nonces) and the MAC addresses of the access point and the client, produces a unique Pairwise Transient Key (PTK) that secures the unicast traffic between the access point and the client. A new PTK is produced each time a client connects to the access point.

QUESTION 135

When using the CLI command `eping`, configured for auto-anchor mobility wireless guest access, which type of packet is tested?

- A. data packets
- B. mobility unencrypted packets
- C. mobility encrypted packets

- D. SNMP control packets
- E. NTP control packets

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Make sure that foreign to anchor communication is possible for mobility traffic. You can test this communication with the eping command (which tests data packets sent to the mobility port UDP 16666) and the mping command (which tests Ethernet over IP encapsulation over the tunnel).

QUESTION 136

When a wireless guest network is implemented using auto-anchor mobility in a controller-based wireless network, which controller is responsible for a guest client's IP address and their security configuration?

- A. any controller that supports the same VLAN
- B. foreign controller
- C. anchor controller
- D. master controller
- E. RF group master controller



Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The anchor controller is responsible for termination of guest WLAN traffic and subsequent access to the Internet. Guest traffic egress occurs at the anchor controller, and the anchor controller is responsible for the client IP address via DHCP and their security configuration.

<http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper/ch10GuAc.html#wp1064207>

QUESTION 137

You have a small organization with multiple Cisco WCS servers. Management has become cumbersome and you are planning to deploy Cisco WCS Navigator. When the Cisco WCS Navigator has been deployed, how are the existing Cisco WCS servers added to the Cisco WCS Navigator, which software versions are supported, and which protocol(s) do they use to communicate with Navigator?

- A. Cisco WCS Navigator searches the enterprise intranet to locate the existing Cisco WCS servers and adds them automatically using SOAP as long as there is only a difference of one version or less between Cisco WCS and WCS Navigator.

- B. Each existing Cisco WCS server must be added manually and use SOAP/HTTP to communicate with the Cisco WCS Navigator platform as long as the software versions of Cisco WCS and Cisco WCS Navigator are the same.
- C. Cisco WCS must be on the same software version as Cisco WCS Navigator and each Cisco WCS server is added automatically using XML over HTTP.
- D. When Cisco WCS Navigator is added, all the Cisco WCS servers must be added manually, each system must use the same software release as Navigator, and the Cisco WCS communicates with Cisco WCS Navigator by using SOAP/XML over HTTPS.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Please refer to the link to understand this part.

http://www.cisco.com/c/en/us/products/collateral/wireless/wireless-control-system-navigator/product_data_sheet0900aecd80633649.html

QUESTION 138

Which two features are available in the Cisco WCS Plus license over the base license? (Choose two.)

- A. ad hoc rogue detection
- B. high availability between two Cisco WCS stations
- C. mobility service engine management
- D. auto discovery and containment or notification of rogue APs
- E. client location to the nearest AP



Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Cisco WCS PLUS license supports Cisco WCS base license features and the following capabilities: mobility services enablement and high availability. An older Cisco WCS Location license is forward compatible and equivalent to a PLUS license. When upgrading to this release, older Location licenses will appear as PLUS licenses. Older Enterprise licenses are also forward compatible and become PLUS licenses when loaded. The process to provision a Cisco WCS PLUS license is the same as provisioning a current Cisco WCS license.

http://www.cisco.com/c/en/us/td/docs/wireless/wcs/7-0/configuration/guide/WCS70cg/7_0warr.html

QUESTION 139

Refer to the exhibit. Cisco WCS version 7.0 has a configuration mismatch with what is actually running in the controller. Which menu leads to the Audit Status Report?

Config Audit

Cisco Prime
Network Control System

Audit Summary

Controller Name	Audit Status	Audit Time	Controller IP Address	Message
Cisco_07:21:43	Identical	2011-May-18, 04:00:03 UTC	10.33.126.2	
Cisco_20:5b:03	Identical	2011-May-18, 04:00:03 UTC	10.32.188.164	
Cisco_32:1b:23	Identical	2011-May-18, 04:00:03 UTC	10.32.37.4	
Cisco_63:c3:03	Mismatch	2011-May-18, 04:00:03 UTC	10.32.52.5	
Cisco_69:51:e0	Mismatch	2011-May-18, 04:00:03 UTC	10.32.36.10	
Cisco_72:16:c3	Mismatch	2011-May-18, 04:00:03 UTC	10.32.53.5	
Cisco_7d:88:00	Mismatch	2011-May-18, 04:00:03 UTC	171.70.35.131	
Cisco_7d:e2:43	Identical	2011-May-18, 04:00:03 UTC	10.194.145.10	
Cisco_7e:fc:23	Identical	2011-May-18, 04:00:03 UTC	10.32.188.162	
Cisco_91:26:03	Identical	2011-May-18, 04:00:03 UTC	10.34.145.84	
Cisco_91:29:83	Identical	2011-May-18, 04:00:03 UTC	10.34.145.86	

- A. Security
- B. Monitor
- C. Configure
- D. Services
- E. Administration
- F. Tools

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The Configure menu enables you to configure templates, controllers, access points, Ethernet switches, chokepoints, Wi-Fi TDOA receivers, config groups, auto provisioning, scheduled configuration tasks, profiles, ACS view servers, and TFTP servers on your network.

http://www.cisco.com/c/en/us/td/docs/wireless/wcs/7-0/configuration/guide/WCS70cg/7_0wst.html#wp1068994

QUESTION 140

What does the current European Telecommunications Standards Institute rule state is the 2.4-GHz maximum transmitter output power for point-to-point installations?

- A. 16 dBm
- B. 17 dBm
- C. 20 dBm
- D. 30 dBm
- E. 36 dBm

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 141

What are two attributes used to characterize antenna performance? (Choose two.)

- A. attenuation
- B. beamwidth
- C. gain
- D. harmony
- E. interference

Correct Answer: BC

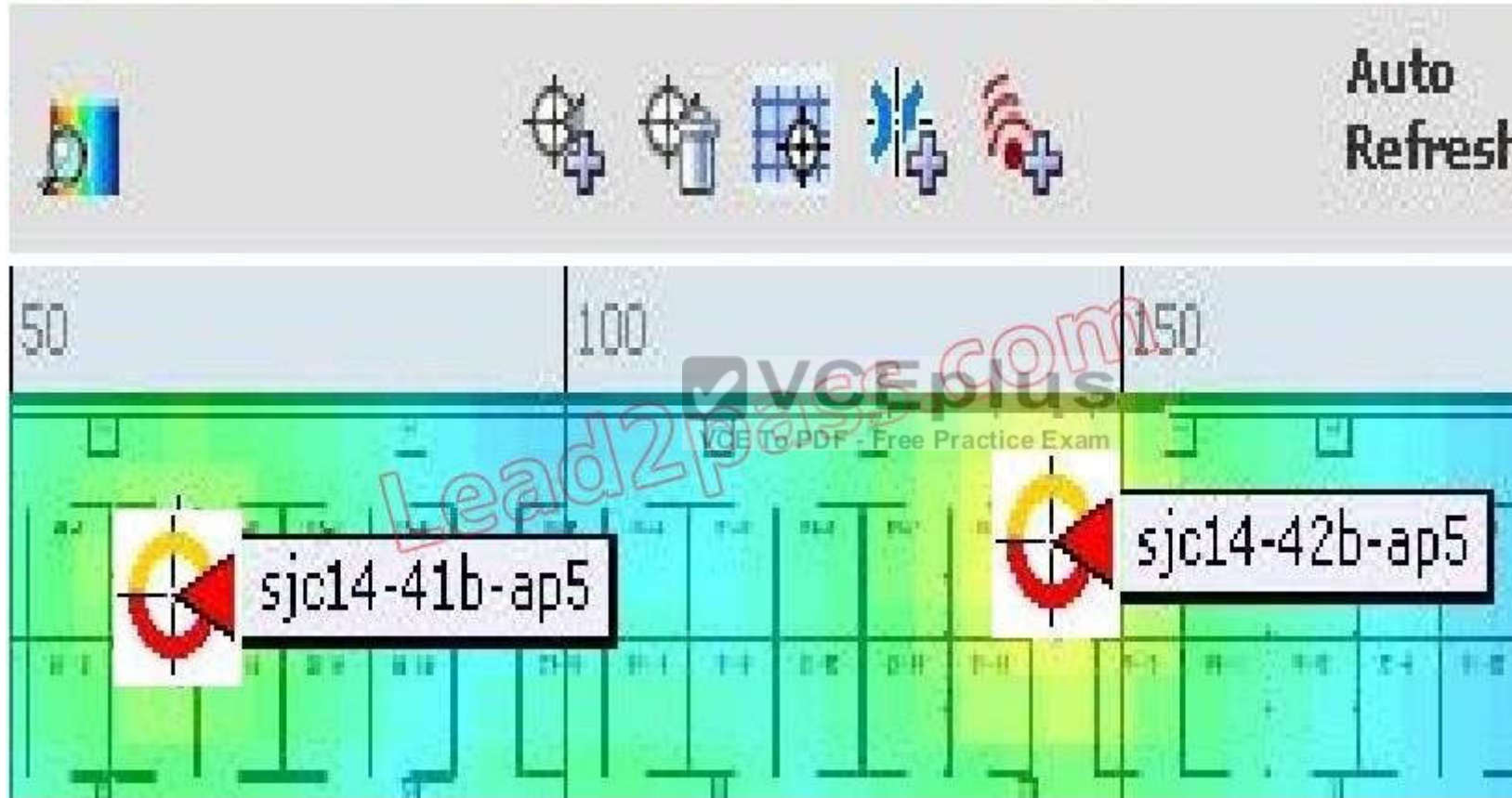
Section: (none)

Explanation

Explanation/Reference:

QUESTION 142

Refer to the exhibit. Which two statements about the status of the respective AP on a Cisco WCS version 7.0 map does this icon represent? (Choose two.)



- A. The 802.11a/n radio is administratively disabled.
- B. The 802.11a/n radio has a minor fault.
- C. The 802.11a/n radio has a major fault.

- D. The 802.11b/g/n radio is administratively disabled.
- E. The 802.11b/g/n radio has a minor fault.
- F. The 802.11b/g/n radio has a major fault.

Correct Answer: BF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The icon with the top half yellow and the lower half red indicates that the optional 802.11a Cisco Radio (top) has a minor fault, and the 802.11b/g Cisco Radio (bottom) has a major or critical fault. The worst of the two Cisco Radio colors determines the color of the large triangular pointer.

<http://www.cisco.com/c/en/us/td/docs/wireless/wcs/7-0MR1/configuration/guide/WCS70MR1/maps.html#wp1090761>

QUESTION 143

How do the features that are available on the Cisco WCS for Linux version differ from those of the Cisco WCS for Windows version?

- A. Assuming that there are no differences in hardware, a Cisco WCS for Linux can support up to 750 wireless LAN controllers. A Cisco WCS for Windows can support up to 250 wireless LAN controllers.
- B. Cisco WCS for Windows includes support for Cisco Spectrum Expert clients. Cisco WCS for Linux does not support Cisco Spectrum Expert clients.
- C. Cisco WCS for Linux is required for deployments.
- D. There are no differences in features between the Linux and Windows versions of Cisco WCS.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 144

Refer to the exhibit. If Cisco WCS version 7.0 needs to have APs added, relocated, or removed on a respective map, which menu leads to the correct location to make that adjustment?

Monitor > Maps > floor 01 > Position access points on Floor Area

Select each AP by clicking on it. Update its position, antenna information, height and when done with all APs click on Save.

Access Points	Horiz	Vert	AP Height	Zoom	Save	Cancel
-- Select an AP --			(feet)	100 %		



- A. Security
- B. Monitor
- C. Configure
- D. Services
- E. Administration
- F. Tools

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 145

Which two statements about the results of the Cisco WCS version 7.0 client troubleshooting tool are true? (Choose two.)

- A. Results of Layers 1 - 3 are provided.
- B. Results of only Layers 2 and 3 are provided.
- C. Results of Layers 4 - 7 are provided.
- D. The tabulated results vary depending on the client type.
- E. Results are provided in a fixed four-part tabulation.
- F. Results are provided in a fixed six-part tabulation.

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:



QUESTION 146

When using Cisco WCS version 7.0, which two features are available for the client troubleshooting tool when a Cisco Compatible Extensions v5 wireless client gets connected? (Choose two.)

- A. Request CleanAir reports from the client
- B. Send text messages to the client
- C. Aggregated Cisco ACS authentication client information
- D. Request the client to ping the DHCP-supplied IP gateway
- E. Display a summary of client event history

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 147

Which modulation technique allows you to achieve a data rate of 54Mb/s in the 2.4GHz-band?

- A. Complimentary Code Keying
- B. Differential Binary Phase Shift Keying
- C. Differential Quadrature Phase Shift Keying
- D. Quadrature Amplitude Modulation

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 148

Which limitation applies to the use of the Cisco WLAN Solution Management over Wireless feature?

- A. Controllers must be managed using only secure protocols (that is, SSH and HTTPS), not nonsecure protocols (that is, HTTP and Telnet).
- B. Read-write access is not available; only read-only access is supported.
- C. Uploads and downloads from the controller are not allowed.
- D. Wireless clients can manage other controllers however not the same controller and AP to which the client is associated.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 149

The results of a Cisco WCS client troubleshooting tool are summarized into a simple visual representation of a four-part progression of the connection status for a wireless client.

What are the four parts? (Choose four.)

- A. client MAC address
- B. 802.11 authentication
- C. IP address assignment

- D. 802.11 association
- E. successful association
- F. authentication method
- G. SSID
- H. client radio type

Correct Answer: BCDE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Please refer to this link for more information about the topic.

<http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/107585-client-con.html>

QUESTION 150

Refer to the exhibit. Which action allows you to view a summary count by alarm types for the displayed total of 11 alarms?

WCS Home

General | **Client** | **Security** | **Mesh** | **CleanAir** | **ContextAware**

Inventory Detail Status

Controllers: 1 | Radios: 4 | MSEs: 0

Client Count

6h | 1d | 1w | 2w | 4w | 3m | 6m | 1y | Custom | View History

Client Count
Time: Wed May 4 2011 08:30:49 AM | Time: Wed May 4 2011 08:30:49 AM
Authenticated Client Count: 0 | Associated Client Count: 0

Coverage Areas

Name	Total APs	a/n Radios	b/g/n Radios	Critical Radio Alarms	Clients
System Campus	2	2	2	0	0

[View All Maps](#)

Recent Coverage Holes (0)

Access Point	Interface	Failed Clients	Total Clients	Percent
None detected				

- A. Choose Monitor > Alarms
- B. Click the Security tab
- C. Click a respective number in the Alarm Summary
- D. Click the Alarm Summary blue arrow
- E. Choose Home (house icon) > Alarm Summary

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 151

Which two statements about the Cisco WLC and AP code upgrade when 7.0 is running are true? (Choose two.)

- A. The AP can download and run new code only after a Cisco WLC reboot causes the AP discovery and join.
- B. The AP can download new code before the Cisco WLC reboot, but only if the AP is configured the CLI via SSH.
- C. The AP can download new code before Cisco WLC reboot if it is configuring the Cisco WLC directly using the GUI via HTTP or HTTPS.
- D. The Cisco WLC defaults to booting newer code, but it can boot older backup code only from the CLI configuration.
- E. The Cisco WLC can boot either primary or back code configured from the GUI.
- F. The Cisco WLC can download only a single code at a time for reboot.

Correct Answer: CE

Section: (none)

Explanation



Explanation/Reference:

Explanation:

Each Cisco WLC can boot off the primary, last-loaded OS image or boot off the backup, earlier-loaded OS image. In order to change a Cisco WLC boot option, issue the config boot command. By default, the primary image on the controller will be chosen as the active image.

Examples

> config boot primary

> config boot backup

In order to configure the boot order using the WLC GUI, complete these steps:

When the WLC reboots and comes back up, it will boot with the backup image.

<http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/107530-backup-image-wlc.html>

QUESTION 152

You are on the phone working with a colleague that is console connected to a lightweight AP that has lost its configuration.

Which three actions are necessary to allow the AP to connect to a controller? (Choose three.)

- A. Configure the AP IP address.
- B. Configure the controller name.
- C. Configure the controller IP address.
- D. Configure the AP hostname.

- E. Configure the AP IP default-gateway.
- F. Configure the AP username and password.

Correct Answer: ACE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

In order to manually configure static information on a LAP using the AP CLI interface, you can use these EXEC mode CLI commands:

AP#capwap ap ip address <IP address> <subnet mask>

AP#capwap ap ip default-gateway <IP-address>

AP#capwap ap controller ip address <IP-address>

AP#capwap ap hostname <name>

(optional)

Notice the first 3 are needed for the AP to connect to the controller; the last step is optional and not needed for basic connectivity to the controller.

<http://www.cisco.com/c/en/us/support/docs/wireless/aironet-1200-series/99763-reset-lwappconfig-lap.html>

QUESTION 153

You have a lightweight AP that has been moved to a new subnet and has become stranded because DNS and DHCP servers are unavailable. The AP cannot connect to the controller. When connected to the console port, which three minimum parameters must you configure? (Choose three.)

- A. AP IP address
- B. controller name
- C. AP hostname
- D. default gateway IP address
- E. controller IP address
- F. username and password

Correct Answer: ADE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

In order to manually configure static information on a LAP using the AP CLI interface, you can use these EXEC mode CLI commands:

AP#capwap ap ip address <IP address> <subnet mask>

AP#capwap ap ip default-gateway <IP-address>

AP#capwap ap controller ip address <IP-address>

AP#capwap ap hostname <name>

(optional)

Notice the first 3 are needed for the AP to connect to the controller; the last step is optional and not needed for basic connectivity to the controller.
<http://www.cisco.com/c/en/us/support/docs/wireless/aironet-1200-series/99763-reset-lwappconfig-lap.html>

QUESTION 154

The IEEE 802.11n standard provides 40-MHz channels, improved MAC efficiency, and MIMO.
Which three elements define the 802.11n implementation of MIMO? (Choose three.)

- A. channel bonding
- B. dynamic frequency selection
- C. maximal ratio combining
- D. packet aggregation
- E. spatial multiplexing
- F. transmit beam forming

Correct Answer: CEF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Maximal ratio combining (MRC) is typically used on all 802.11n access points. Transmit beam forming is used to increase the gain towards the client. For 802.11n clients, spatial multiplexing is used to deliver enhanced high throughput data rates upwards of 300 Mbps
http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1130-ag-series/white_paper_c11-516389.html

QUESTION 155

Which two statements about WiMAX technology are true? (Choose two.)

- A. WiMAX is defined by 802.11i.
- B. Typically, fixed WiMAX networks have a higher-gain directional antenna installed near the client.
- C. WiMAX is capable of working as a long-range system over several miles.
- D. WiMAX works only for licensed frequencies.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

WiMAX is defined by 802.16, that is intended for wireless "metropolitan area networks". WiMAX can provide broadband wireless access (BWA) up to 30 miles (50 km) for fixed stations, and 3 - 10 miles (5 - 15 km) for mobile stations. In contrast, the WiFi/802.11 wireless local area network standard is limited in most cases to only 100 - 300 feet (30 - 100 m). Fixed WiMAX networks typically have a higher-gain directional antenna installed near the client (customer) which results in greatly increased range and throughput. Using 802.11 with high-gain antenna can bridge last-mile gaps, but they require more power. WiMAX operates on both licensed and non-licensed frequencies, providing a regulated environment and viable economic model for wireless carriers. In particular, WiMax operates on the 10-to 66-GHz frequency band, so it doesn't interfere with 802.11 LANs.

QUESTION 156

Which governing body analyzes the applications and environments in which wireless networks are used?

- A. EIRP
- B. ETSI
- C. FCC
- D. IEEE
- E. WiFi Alliance

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Hence the various wireless standards prefixed with IEEE. Wireless LANs are described in IEEE 802.11 standard that contains 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac and so forth.

QUESTION 157

Which description best describes upfade in a multipath environment?

- A. In this situation, multiple signal paths are not sent at exactly the same time. The receiver receives a positive crest on the primary signal and a negative crest on the secondary signal.
- B. In this situation, the multiple signal paths are distorted and difficult to understand.
- C. In this situation, the multiple signal paths are weaker than they should be because the signals are out of phase with each other.
- D. In this situation, the signal is stronger than it should be because multiple signal paths are received twice at exactly the same time, which results in the multiple signals being in-phase.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:**Explanation:**

If a signal is received twice at exactly the same time, the secondary wave adds its power to the primary wave, so the receiver gets twice the positive energy (positive crest) at the same instant, then twice the negative energy (negative crest) at the same instant. The result is that both waves add up to twice the amplitude (energy) of a single wave, and both signals are said to be in phase (both signals are said to have an angle of 0 degrees). This rare condition is called upfade. If the second signal negative energy (negative crest) reaches the receiver just when the first signal positive energy (positive crest) also reaches the receiver, both signals can cancel each other, resulting in no signal at all (this is the principle used in noise cancellation headsets).

QUESTION 158

A controller is connected to a Cisco Catalyst switch. The switch port configuration looks like this:

```
interface GigabitEthernet 1/0/10
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,20,30,50
switchport trunk native vlan 20
switchport mode trunk
```

Which controller CLI command assigns its management interface to the native VLAN interface of the Cisco Catalyst switch?

- A. config interface vlan management 0
- B. config interface vlan management 1
- C. config interface vlan management 20
- D. config interface vlan management 30
- E. config interface vlan management 50



Correct Answer: A

Section: (none)

Explanation**Explanation/Reference:****Explanation:**

Since the controller management interface is connected to the native vlan interface of the Cisco Catalyst switch, the correct command is: config interface vlan management vlan-id 0

<http://www.cisco.com/en/US/docs/wireless/controller/5.0/configuration/guide/c5mint.html#wp11828>

QUESTION 159

Which statement about an infrastructure basic service set is true according to IEEE 802.11 specifications?

- A. The set also is called an ad hoc network.

- B. The BSSID is generated from the first wireless client that starts up in the IBSS.
- C. The set enables the use of ESS.
- D. No signals are relayed from one client to another client.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The set-up formed by the access point and the stations located within its coverage area are called the basic service set (or infrastructure basic service set, or BSS for short).

Each BSS forms one cell.

We can link several BSS's together (it means we link access points) using a connection called a distribution system in order to form an extended service set or ESS. The distribution system can also be a wired network, a cable between two access points or even a wireless network.

Note: When a station moves from one access point to another in an ESS, it is called roaming.

QUESTION 160

Which two factors must be considered when evaluating an RF interferer for severity? (Choose two.)

- A. distance from the AP
- B. dBm
- C. the type of security crack being used
- D. duty cycle
- E. number of interfering IP stations in the cell
- F. duplicate SSID

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

On controller code 7.0 and later, you can configure Event Driven RRM (EDRRM) from the Wireless > 802.11a/n [802.11b/g/n] > RRM > DCA page. Enabling EDRRM allows the controller to bypass the 600-second default interval for DCA and change an AP channel immediately if a disturbing non-802.11 interference is detected on the AP channel. You can set the sensitivity threshold to High (60), Medium (50), or Low (35). This threshold refers to the Air Quality index. CleanAir-capable APs (3500 and 3600 Series APs, with their CleanAir capable chipset) can detect and identify non-802.11 interferences and report them to the controller. These APs can report interferers when in local mode and monitor mode. Notice that the AP cannot report to the controller when in Spectrum Only Monitor Mode (SOMM). The controller uses the reported information to list non-802.11 interferers along with their zone of impact and severity and establish an Air Quality Index

(AQI) from 100 (perfect) to 0 (network unusable). Notice that the logic of the global AQ index (higher is better) is exactly the opposite of the logic of the individual interferer severity index (higher is more severe, and therefore worse). The severity index is calculated individually by each detecting AP based on the power (signal strength), duty cycle (how often the device uses the air per second), and detected type of interferer. The louder an interferer device, the higher the duty cycle will mean a higher severity index for the reporting AP. The severity index is calculated for a specific device, without regard to what channels are being affected.

QUESTION 161

Which two items are needed to discover the IP address of a new Cisco Aironet 1260 autonomous AP that just finished booting? (Choose two.)

- A. username = "cisco" and password = "cisco"
- B. username = "Admin" and password = "Cisco"
- C. username = none and password = "Cisco"
- D. show int vlan1
- E. show int bvi1
- F. show int gigabitethernet0
- G. show int radio0-802.11n
- H. show int radio1-802.11n

Correct Answer: CE

Section: (none)

Explanation



Explanation/Reference:

Explanation:

Enter your username in the User Name field. The default username is Cisco. Enter the wireless device password in the Password field and press Enter. The default password is Cisco. The Summary Status page appears.

The access point is configured with the factory default values including the IP address (set to receive an IP address using DHCP). To obtain the new IP address for an access point/bridge, you can use the show interface bvi1 CLI command.

http://www.cisco.com/c/en/us/td/docs/wireless/access_point/12-4-25d-JA/Configuration/guide/cg_12_4_25d_JA/scg12-4-25d-JA-chap4-first.html

QUESTION 162

Which statement correctly describes the procedure for a lightweight AP to successfully establish a connection to a controller?

- A. The AP authenticates the received Cisco WLC certificate as valid. The AP then sends its certificate to the controller.
- B. The AP sends its certificate to the controller. The AP then authenticates the received Cisco WLC certificate as valid.
- C. The AP sends its certificate to the RADIUS server. The AP then authenticates the controller certificate as valid.
- D. The AP sends its certificate to the RADIUS server. The AP then authenticates the RADIUS certificate as valid.
- E. The AP authenticates the received RADIUS server certificate as valid. The AP then sends its certificate to the RADIUS server.
- F. The AP authenticates the received RADIUS server certificate as valid. The AP then sends its certificate to the controller.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The controller will respond to all discovery requests without checking certificates or AP credentials. However, join requests must have a valid certificate in order to get a join response from the controller. If the LAP does not receive a join response from its choice, the LAP will try the next controller in the list unless the controller is a configured controller (Primary/Secondary/Tertiary).

<http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/99948-lap-notjoin-wlc-tshoot.html#backinfo>

QUESTION 163

Which two statements about the requirements to configure inter-controller roaming are true? (Choose two.)

- A. The same mobility domain names are configured across controllers.
- B. The same RF group names are configured across controllers.
- C. The same controller hardware version is configured across controllers.
- D. The same AP manager interface is configured across controllers.
- E. The same virtual interface is configured across controllers.
- F. The same controller software version is configured across controllers.

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

All controllers must be configured with the same mobility group name. All controllers must be configured with the same virtual interface IP address. If necessary, you can change the virtual interface IP address by editing the virtual interface name on the Controller > Interfaces page.

If all the controllers within a mobility group are not using the same virtual interface, inter-controller roaming may appear to work, but the handoff does not complete, and the client loses connectivity for a period of time.

<http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-0/configuration/guide/c70/c70mobil.html>

QUESTION 164

Which two statements best describe the LAG configuration between a Cisco WLC and a Cisco Catalyst switch? (Choose two.)

- A. The Catalyst switch should be configured for PAgP.
- B. The Catalyst switch should be configured only for Layer 2 load balancing.

- C. The Catalyst switch should be configured for "on" mode.
- D. The Cisco WLC relies on the connected switch to perform the load-balance of traffic.
- E. The Cisco WLC aggregates multiple management interfaces into a single virtual interface.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Restrictions for Link Aggregation

You can bundle all eight ports on a Cisco 5508 Controller into a single link.

Terminating on two different modules within a single Catalyst 6500 series switch provides redundancy and ensures that connectivity between the switch and the controller is maintained when one module fails. The controller's port 1 is connected to Gigabit interface 3/1, and the controller's port 2 is connected to Gigabit interface 2/1 on the Catalyst 6500 series switch. Both switch ports are assigned to the same channel group.

LAG requires the EtherChannel to be configured for 'mode on' on both the controller and the Catalyst switch.

Once the EtherChannel is configured as on at both ends of the link, the Catalyst switch should not be configured for either Link Aggregation Control Protocol (LACP) or Cisco proprietary Port Aggregation Protocol (PAgP) but be set unconditionally to LAG. Because Cisco WLC relies on the connected switch to perform the load-balance of traffic, the controller does not answer to negotiation frames and the LAG is not formed if a dynamic form of LAG is set on the switch.

Additionally, LACP and PAgP are not supported on the controller.

http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_0100011.html

QUESTION 165

What is the result when client exclusion is enabled with a timeout value of zero?

- A. Clients are excluded indefinitely.
- B. Clients are never excluded.
- C. Client exclusion is disabled.
- D. Clients must be explicitly included by specifying the MAC address.
- E. Exclusion and inclusion is determined by access list.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 166

An indoor 1240 AP is booting and has obtained an IP address using DHCP. The AP has confirmed prior controller IP addresses from a previously joined mobility group stored in NVRAM. What is the next step the AP performs?

- A. DHCP option 43.
- B. DNS resolution of CISCO-LWAPP-CONTROLLER.localdomain.
- C. Layer 2 LWAPP discovery broadcast.
- D. Layer 3 LWAPP discovery broadcast.
- E. Ping each Cisco WLC to verify its current status.
- F. Select a Cisco WLC based on its position in the configured join selection sequence.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 167

Which AP to Wireless LAN Controller discovery process requires a previous association of the AP with a Cisco WLC?

- A. AP priming
- B. defining a master controller
- C. DHCP Option 6
- D. DHCP Option 43
- E. over-the-air provisioning

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 168

What two statements are true about AES-CCMP? (Choose two.)

- A. It is an encryption algorithm used in the 802.11i security protocol.
- B. It is defined in 802.1X.

- C. It is the encryption algorithm used in TKIP implementations.
- D. It is required in WPA.
- E. It is required in WPA2.

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 169

Which two Cisco Unified Wireless Network capabilities use information that is provided by Radio Resource Management neighbor messages in version 7.0 MR1? (Choose two.)

- A. aggressive load balancing
- B. dynamic channel assignment
- C. hybrid remote edge access point
- D. inter-controller mobility (that is, mobility groups)
- E. rogue AP classification



Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

<http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/71113-rrm-new.html>

QUESTION 170

Which option lists the key features of Cisco Compatible Extensions v5?

- A. Roaming and real-time diagnostics, MFP, a diagnostic channel that allows troubleshooting of the client, client reporting, optional location service, and expedited bandwidth
- B. AP assisted roam, Cisco Centralized Key Management, radio measurements, and transmit power control
- C. CAC, UPSD, voice metrics, MBSSIDs, location, link tests, and NAC
- D. WME, proxy ARP, EAP-FAST, and WPA2, and single sign-on
- E. LEAP, WPA, 802.1x and VLANs per AP, TKIP, and WiFi

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

http://www.cisco.com/web/partners/downloads/765/ccx/Comp_Ext_Cust_Preso.pdf

QUESTION 171

A client is attached to the Cisco Unified Wireless Network using controllers. When the client is using WPA2 and EAP authentication, where are the wireless encryption keys located during the active user session? (Choose two.)

- A. on the access point
- B. on the RADIUS server
- C. on the Cisco WCS
- D. on the client
- E. on the Cisco WLC

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

During the Active user session, WEP keys can be located on the access point as well as on the client. Network managers need to provide end users with freedom and mobility without offering intruder's access to the WLAN or the information sent and received on the wireless network. With a WLAN, transmitted data is broadcast over the air using radio waves that travel between client devices, or stations, and access points-the WLAN endpoints on the Ethernet network that link stations to the network. This means that any WLAN client device within an access point service area can receive data transmitted to or from the access point.

QUESTION 172

Which Extensible Authentication Protocol types are supported by the Cisco Unified Wireless Network?

- A. EAP-TLS, PEAP-MSCHAPv2, and PEAP-GTC only
- B. LEAP and EAP-FAST only
- C. EAP-TLS, PEAP-MSCHAPv2, PEAP-GTC, LEAP, and EAP-FAST only
- D. any EAP supported by the RADIUS authentication server

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Extensible Authentication Protocol, or EAP, is an authentication framework frequently used in wireless networks and point-to-point connections. EAP is an authentication framework providing for the transport and usage of keying material and parameters generated by EAP methods. There are many methods defined by RFCs and a number of vendor specific methods and new proposals exist. EAP is not a wire protocol; instead it only defines message formats. Each protocol that uses EAP defines a way to encapsulate EAP messages within that protocol's messages.

http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol

QUESTION 173

What unit of measurement is used to represent the strength of an antenna's radiation pattern?

- A. dBi
- B. dBm
- C. mW
- D. GHz

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 174

Which four parameters must be configured for local EAP-FAST on the controller? (Choose four.)

- A. authority ID
- B. authority ID Information
- C. client key
- D. PAC
- E. server key
- F. TTL for PAC
- G. monitor key
- H. NTP source

Correct Answer: ABEF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

EAP-FAST is designed to speed re-authentication when a station roams from one AP to another.

Here are the parameters that can be configured:

* Server Key (in hexadecimal): The key (in hexadecimal characters) used to encrypt and decrypt PACs.

* Time to Live for the PAC: Enter the number of days for the PAC to remain viable. The valid range is 1 to 1000 days, and the default setting is 10 days.

* Authority ID (in hexadecimal): Enter the authority identifier of the local EAP-FAST server in hexadecimal characters. It is possible to enter up to 32 hexadecimal characters, but an even number of characters must be entered. This will identify the controller as the emitter of the PAC.

* Authority ID Information: Enter the authority identifier of the local EAP-FAST server in text format.

* Anonymous Provision: Enable this setting to allow anonymous provisioning. This feature allows PACs to be sent automatically to clients that do not have one during PAC provisioning. If this feature is disabled, PACS must be manually provisioned. Disable this feature when using EAP-FAST with certificates. The default setting is enabled.

QUESTION 175

Which type of management tasks can be completed on a Cisco WLC remotely from a wireless client?

- A. All management and configuration tasks can be performed from a wireless client except for using debug commands.
- B. In the default configuration, no management or configuration is possible through the GUI or CLI on the Cisco WLC.
- C. The default configuration of the Cisco WLC allows only CLI access and then only the use of show commands, so no configuration is possible.
- D. All management and configuration tasks, except uploads from and downloads to the Cisco WLC, are permitted.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

<http://www.cisco.com/c/en/us/td/docs/wireless/controller/6-0/configuration/guide/Controller60CG/c60intf.html>

QUESTION 176

When using a Cisco WLC version 7.0 with a default configuration, how is a remote management HTTPS access connection secured?

- A. The Cisco WLC uses a pre-shared key to authenticate the user, which limits the number of potential users that can access the controller.
- B. The Cisco WLC generates its own local web administration SSL certificate and automatically applies it to the GUI.
- C. The Cisco WLC uses a CA certificate for SSL access.
- D. The Cisco WLC uses HTTPS to secure the HTTP session via a preconfigured password that generates a certificate for each session.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You can protect communication with the GUI by enabling HTTPS. HTTPS protects HTTP browser sessions by using the Secure Socket Layer (SSL) protocol. When you enable HTTPS, the controller generates its own local web administration SSL certificate and automatically applies it to the GUI. You also have the option of downloading an externally generated certificate.

<http://www.cisco.com/c/en/us/td/docs/wireless/controller/6-0/configuration/guide/Controller60CG/c60intf.html>

QUESTION 177

Which physical layer encoding technology is common to both the IEEE 802.11g and the IEEE 802.11a standards?

- A. BPSK
- B. CCK
- C. DSSS
- D. OFDM

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Exam B**QUESTION 1**

Which set of commands assigns a standalone access point an IP address of 10.0.0.24 with a 27-bit subnet mask and a gateway of 10.0.0.1?

- A.

```
config t
interface BVI1
ip address 10.0.0.24 255.255.255.192
exit
ip default-gateway 10.0.0.1
```
- B.

```
config t
interface BVI1
ip address 10.0.0.24 255.255.255.224
exit
ip default-gateway 10.0.0.1
```
- C.

```
config t
interface FastEthernet1
ip address 10.0.0.24 255.255.255.224
exit
ip default-gateway 10.0.0.1
```
- D.

```
config t
interface Dot11Radio0
ip address 10.0.0.24 255.255.255.224
exit
ip default-gateway 10.0.0.1
```
- E.

```
config t
interface FastEthernet1
ip address 10.0.0.24 255.255.255.192
exit
ip default-gateway 10.0.0.1
```
- F.

```
config t
interface Dot11Radio0
ip address 10.0.0.24 255.255.255.192
exit
ip default-gateway 10.0.0.1
```



Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

A controller-based wireless solution can avoid interference by dynamically adjusting what two access point transmission characteristics? (Choose two.)

- A. operating RF channel
- B. SSID names
- C. transmit power levels
- D. switch port parameters
- E. antenna gain

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

The network administrator receives complaints of slow wireless network performance and performs a sniffer trace of the wireless network in preparation for migration to 802.11n. The sample capture shows frames that contains AP beacons with NonERP_Present bit set to 1 and frames with RTS/CTS. Which two conclusions can be interpreted from these frames? (Choose two.)

- A. The network is performing slowly because 802.11n clients are already mixed with 802.11g clients.
- B. The network is performing slowly because 802.11b clients still exist in the network.
- C. The network is performing slowly because a wireless client is incorrectly configured, which results in RF interference.
- D. Possible 802.11b wireless clients are located only in the AP cell radius where the sniffer capture was performed.
- E. Possible 802.11b wireless clients could be located anywhere in the wireless network.

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

If an ERP AP hears a beacon from an AP where the supported data rates contain only 802.11b or 802.11 DSSS rates, it will enable the NonERP_Present bit in its own beacons, enabling protection mechanisms in its BSS. In simpler terms, if an 802.11g AP hears a beacon frame from an 802.11 or 802.11b access point or ad hoc client, the protection mechanism will be triggered.

<http://mrnciew.com/2014/11/02/cwap-802-11-protection-mechanism/>

QUESTION 4

How many dBm is 40 mW?

- A. 10 dBm
- B. 16 dBm
- C. 20 dBm
- D. 22 dBm
- E. 40 dBm

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The dB measures the power of a signal as a function of its ratio to another standardized value. The abbreviation dB is often combined with other abbreviations in order to represent the values that are compared. Here are two examples:

You can calculate the power in dBs from this formula:

Power (in dB) = $10 * \log_{10} (\text{Signal/Reference})$

This list defines the terms in the formula:

Here is an example. If you want to calculate the power in dB of 50 mW, apply the formula in order to get:

Power (in dB) = $10 * \log_{10} (50/1) = 10 * \log_{10} (50) = 10 * 1.7 = 17 \text{ dBm}$

Because decibels are ratios that compare two power levels, you can use simple math in order to manipulate the ratios for the design and assembly of networks. For example, you can apply this basic rule in order to calculate logarithms of large numbers:

$\log_{10} (A*B) = \log_{10}(A) + \log_{10}(B)$

If you use the formula above, you can calculate the power of 50 mW in dBs in this way:

Power (in dB) = $10 * \log_{10} (50) = 10 * \log_{10} (5 * 10) = (10 * \log_{10} (5)) + (10 * \log_{10}(10)) = 7 + 10 = 17 \text{ dBm}$

<http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/23231-powervalues-23231.html>

QUESTION 5

If an antenna has a dBd of 8.6, what is the dBi value?

- A. 6.2
- B. 6.46
- C. 8.6
- D. 10.74
- E. 12.88

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Antenna performance is measured in dBi (the antennas gain/loss over a theoretical isotropic antenna) dBd (the antennas gain/loss over a dipole antenna)

$\text{dBi} = \text{dBd} + 2.15$

$\text{dBd} = \text{dBi} - 2.15$

QUESTION 6

Which calculation computes the EIRP of an antenna?

- A. $\text{EIRP} = \text{Tx power (dBm)} + \text{Antenna Gain (dBi)} - \text{Cable Loss (dB)}$
- B. $\text{EIRP} = \text{Cable Loss (dB)} + \text{Antenna Gain (dBi)} - \text{Tx power (dBm)}$
- C. $\text{EIRP} = \text{Cable Loss (dB)} + \text{Antenna Gain (dBi)} / \text{Tx power (dBm)}$
- D. $\text{EIRP} = \text{Tx power (dBm)} + \text{Antenna Gain (dBi)} / \text{Cable Loss (dB)}$
- E. $\text{EIRP} = \text{Antenna Gain (dBi)} - \text{Cable Loss (dB)} * \text{Tx power (dBm)}$
- F. $\text{EIRP} = \text{Tx power (dBm)} * \text{Antenna Gain (dBi)} / \text{Cable Loss (dB)}$

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

EIRP (Effective Isotropic Radiated Power)

EIRP (Effective Isotropic Radiated Power) is the actual amount of signal leaving the antenna and is a value measured in db and is based on 3 values:

- a) Transmit Power (dBm)
- b) Cable Loss (dB)
- c) Antenna Gain (dBi)

The dB measures the power of a signal as a function of its ratio to another standardized value. The abbreviation dB is often combined with other abbreviations in order to represent the values that are compared. Here are two examples:

dBm --The dB value is compared to 1 mW.

dBw --The dB value is compared to 1 W.

You can calculate the power in dBs from this formula:

$\text{Power (in dB)} = 10 * \log_{10} (\text{Signal/Reference})$

This list defines the terms in the formula:

\log_{10} is logarithm base 10.

Signal is the power of the signal (for example, 50 mW). Reference is the reference power (for example, 1 mW).

How to find EIRP

To determine EIRP follow this equation:

$\text{<Transmit Power> - Cable Loss + Antenna Gain = EIRP}$

<https://supportforums.cisco.com/document/49506/snr-rssi-eirp-and-free-space-path-loss>

QUESTION 7

Which three items are allowed on an Ethernet trunk port? (Choose three.)

- A. autonomous AP
- B. FlexConnect AP
- C. local AP
- D. monitor AP
- E. rogue detector AP
- F. sniffer AP
- G. SE-Connect AP
- H. Cisco WLC

Correct Answer: ABE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A: The basic reason as to why autonomous AP's need trunk ports and lightweight AP's don't does indeed have to do with the capwap tunnel that is used between the AP and the controller.

B: you can attach the access point that is enabled for FlexConnect to a trunk or access port on the switch.

E: APs can also be placed in rogue detector mode. In this mode, the rogue detector AP is placed on a trunk port so it can monitor all wired-side connected VLANs, and the AP radios are turned off.

QUESTION 8

Which option describes computer-to-computer wireless communication?

- A. BSS and BSA
- B. IBSS and ad hoc network
- C. ad hoc network and BSA
- D. IBSS and ESS
- E. ESS and BSA
- F. BSS and ad hoc network

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Ad-hoc mode is an 802.11 networking framework in which devices or stations communicate directly with each other, without the use of an access point (AP). Ad-hoc mode is also referred to as peer-to-peer mode or an Independent Basic Service Set (IBSS). Ad-hoc mode is useful for establishing a network where wireless infrastructure does not exist or where services are not required.

http://www.webopedia.com/TERM/A/ad_hoc_mode.html

QUESTION 9

Which two statements about AES-CCMP are true? (Choose two.)

- A. It is an encryption algorithm used in the 802.11i security protocol.
- B. It is defined in 802.1X.
- C. It is the encryption algorithm used in TKIP implementations.
- D. It is required in WPA.
- E. It is required in WPA2.

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

WPA2 has replaced WPA. WPA2, which requires testing and certification by the Wi-Fi Alliance, implements the mandatory elements of IEEE 802.11i. In particular, it includes mandatory support for CCMP, an AES-based encryption mode with strong security.

http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

QUESTION 10

Effective Isotropic Radiated Power is calculated by using which three values? (Choose three.)

- A. antenna bandwidth
- B. antenna gain
- C. cable loss
- D. receiver sensitivity
- E. SSID

F. transmission power

Correct Answer: BCF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 11

Which statement best represents the authorization aspect of AAA?

- A. Authorization takes place after a successful authentication and provides the Cisco WLC the information needed to allow client access to network resources.
- B. Authorization is the validation of successful DHCP address delivery to the wireless client.
- C. Authorization must be successfully completed in order to proceed with the authentication phase.
- D. Successful authorization will provide encryption keys that will be used to secure the wireless communications between client and AP.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 12

What increases bandwidth and resists multipath problems by carrying data in subcarriers?

- A. Direct Sequence Spread Spectrum
- B. Frequency Hopping Spread Spectrum
- C. Narrow Band Frequency
- D. Orthogonal Frequency Division Multiplexing

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 13

Which two statements best describe LWAPP? (Choose two.)

- A. Cisco proprietary
- B. communication between the AP and client
- C. communication between the AP and the WLC
- D. Lightweight Access Point provisioning
- E. used to encrypt control and data packets

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 14

What is fading?

- A. Another signal source is producing energy on the channel in which you are trying to operate.
- B. The desired signal reaches the receiving antenna via multiple paths, each of which has a different propagation delay and path loss.
- C. A time-varying change in the path loss of a link with the time variance governed by the movement of objects in the environment, including the transmitter and receiver themselves.
- D. A function of the frequency and should be provided in the cable specification by the vendor.
- E. The minimum signal level for the receiver to be able to acceptably decode the information.
- F. The time delay from the reception of the first instance of the signal until the last instance.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 15

What three roles are defined by 802.1X? (Choose three.)

- A. AAA Server

- B. Authenticatee
- C. Authenticator
- D. Authentication Server
- E. Supplicant

Correct Answer: CDE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 16

What is an MBSSID?

- A. a virtual AP configured on a physical AP that share a single physical device, which is one half-duplex radio
- B. a set of physical APs configured in a BSA to form cells that are controlled by a single controller
- C. the group of clients that are allowed to gain access to one or more SSIDs configured in an AP
- D. the identified overlap area between two cells, which identifies the clients that are operating in that area at any given time

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Some APs can offer only one SSID per radio. Other APs have a slot of MAC addresses available and can support several SSIDs per radio, using Multiple BSSIDs (MBSSID). MBSSIDs basically are virtual APs that still share the same physical device, which has a half-duplex radio. MBSSIDs are a way to differentiate the traffic reaching the AP, not a way to increase the capacity of the AP.

QUESTION 17

A Cisco Aironet 1260 AP is unable to join a Cisco 2500 Series WLC that is connected through a Layer 2 switch. Which three options help to verify the wireless network operation and locate a possible issue? (Choose three.)

- A. Verify status of GUI Wireless > Country
- B. Verifystatus of GUI Wireless > Timers
- C. Verify status of GUI WLANs > ID > Advanced
- D. CLI debug of dot11

- E. CLI debug of DHCP
- F. Verify Cisco WLC license
- G. Verify Cisco WLC model

Correct Answer: AEF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

See reference link below for troubleshooting.

"Troubleshoot a Lightweight Access Point Not Joining a Wireless LAN Controller"

<http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/99948-lap-notjoin-wlc-tshoot.html#topic1>

QUESTION 18

An AP has been configured for personal wireless access to the Internet.

Which item should be configured on the wireless client?

- A. RF channel
- B. BSS
- C. PSK
- D. 802.1X/EAP
- E. broadcast SSID
- F. IBSS



Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Using Pre-shared keys (PSK) is the easiest and best method for allowing Internet access to a wireless client using an access point.

QUESTION 19

You need to set up an ad hoc connection to another client in a conference room to exchange files using Windows 7.

Which two items do you need to create this connection? (Choose two.)

- A. SSID name
- B. RF channel

- C. 802.1X/EAP credentials
- D. pre-shared key
- E. Telnet
- F. IBSS name
- G. SSH

Correct Answer: DF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A wireless ad-hoc network is when two or more wireless nodes communicate directly on a peer-to-peer basis with no wireless network infrastructure. This is also referred to as an independent basic service set (IBSS). Wireless ad-hoc networks are typically formed on a temporary basis to rapidly enable communication between hosts, such as to exchange files during a spontaneous meeting or between hosts at home. The pre-shared key and the IBSS name need to be configured to allow for this.

http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/secwlandg20/sw2dg/ch7_2_SPMb.html

QUESTION 20

Which option describes why most wireless phones and tablets do not use 802.11a/n and 40 MHz channels?

- A. a lack of radio range when using these radios
- B. a lack of device battery capacity to operate concurrent a/b/g/n radios
- C. a lack of cooling in the device necessary to operate these radios
- D. These radios would require the devices to be larger.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 21

An AP was reset while working on the correct association to a Cisco WCS version 7.0.
Which item was cleared during the reset?

- A. static IP address
- B. the location ID of the AP

- C. WLC primary, secondary, tertiary
- D. AP name
- E. certificate
- F. Nothing was cleared.

Correct Answer: F

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Reset --Sets the table to the default display so nothing will be cleared.

QUESTION 22

Which two actions would you use to begin to troubleshoot an access point that fails to join a wireless LAN controller successfully? (Choose two.)

- A. SSH to the AP.
- B. SSH to the Cisco WCS.
- C. SSH to the Cisco WLC.
- D. Issue the Cisco WLC command debug capwap events enable
- E. Issue the Cisco WLC command show capwap events

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The controller supports the use of the Telnet and Secure Shell (SSH) protocols to troubleshoot lightweight access points. Using these protocols makes debugging easier, especially when the access point is unable to connect to the controller. You can monitor the APs dialog with the controller using the debug capwap family of commands.

QUESTION 23

Which portion of a WLAN deployment can WLC message logs help to troubleshoot?

- A. RF issues
- B. encryption issues between APs and clients
- C. configuration verification issues

- D. infrastructure and client Issues
- E. AP placement issues

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The message logs include information related to the network infrastructure, client issues, authentication issues, and AP association issues

QUESTION 24

Configurations are commonly uploaded and downloaded to a WLC. Which options are other examples of a file that can be uploaded from a Cisco 2500 Series WLC?

- A. packet capture
- B. crash file
- C. code
- D. login banner
- E. PAC

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

From Management > Tech Support, you can access useful information, such as controller crash files or AP crash logs (which logs the reasons for the crash). These files are usually transmitted to advanced tech support or TAC but usually not managed directly by Wireless CCNAs. Then, from the Command > Upload page in the web interface, you can upload the configuration file or other system files (event logs, message logs, trap logs, crash file, debug file, wireless attack signatures file, etc).

QUESTION 25

The wireless network is using controller-based APs and version 7.0 MR1. The APs appear to be connected properly to the controllers. A wireless user near one of the APs reports that they are unable to connect to the network with their pre-shared key. Which option shows the GUI path where you can check the connection status of that client?

- A. WLANs > WLAN_ID > Advanced
- B. Security > Clients

- C. Security > Advanced > Clients
- D. Monitor > Clients
- E. Wireless > 802.11b/g/n > clients

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Choose Monitor > Clients to open the Clients page.

This page lists all of the clients that are associated to the controller's access points. It provides the following information for each client:

http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_010000000.html

QUESTION 26

You are about to use a hotel's guest wireless services using a wireless laptop. Which three items do you need to establish a wireless connection? (Choose three.)

- A. SSID name
- B. RF channel
- C. RF signal
- D. 802.1X/EAP credentials
- E. pre-shared key
- F. web page
- G. WPA/WPA2 settings



Correct Answer: ACF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Another common authentication method, especially for guest networks (for example, in hotels, where Internet access must be simple, requiring only an SSID with decent RF signal in each room and a web page to authenticate the user, regardless of the underlying operating system), is Web authentication.

QUESTION 27

You have an Apple IOS iPhone4 that is used on your home Wi-Fi network and a personal laptop that is used on your work's enterprise wireless network. At your office, you are unable to see the enterprise wireless network on your iPhone4.

What is the most likely cause of this issue?

- A. WPA2 CPU intensive encryption is not supported on the client.
- B. WPA2 must be enabled on the client.
- C. A new profile must be created on the client.
- D. Wi-Fi must be enabled on the client.
- E. The enterprise is 2.4 GHz only.
- F. The enterprise is 5 GHz only.
- G. The RF channel must be adjusted on the client.

Correct Answer: F

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The iPhone4 only supports 2.4 Ghz wireless. 5 Ghz wireless support was added with the iPhone5.

QUESTION 28

When Cisco AnyConnect modules are installed on a PC, which module must be installed first?

- A. telemetry
- B. web security
- C. VPN
- D. NAM
- E. DART
- F. posture
- G. CSSC

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The VPN module is mandatory for all other modules to function correctly and must be installed first. Even if the VPN module is not selected for installation, it will be pushed and installed on the client.

<http://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/118714-configure-ise-00.html>

QUESTION 29

You have an organization that has a growing number of standalone APs. You would like to migrate to lightweight APs and manage them through Cisco WCS. Which software platform allows you to make this migration?

- A. The enterprise version of Cisco WCS allows this migration and provides the most flexibility in the number of APs supported.
- B. CiscoWorks WLSE is the only management platform that allows this migration, but it is limited to 500 APs.
- C. You can migrate your network to Cisco WCS single server with the CiscoWorks WLSE upgrade software upgrade.
- D. You can migrate the network by using either the single server or enterprise software platforms, both using the CiscoWorks WLSE upgrade software upgrade.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

<http://www.cisco.com/c/en/us/td/docs/wireless/wcs/4-1/configuration/guide/wcscfg41/wcswarr.html>

QUESTION 30

Which statement best describes the ability of a wireless client to access and transmit a data frame to an AP?

- A. The client listens to the media until polled by the AP using PCF to send its data.
- B. The client listens to the media until a data frame is finished, at which time it transmits, unless a collision of data frames has occurred.
- C. The client uses random countdown timers to start the transmission of a data frame.
- D. The client listens to the media and countdown timers to start the transmission of a data frame.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

<http://www.ciscopress.com/articles/article.asp?p=1271797&seqNum=2>

QUESTION 31

Which statement about ZigBee technology is true?

- A. It has low power consumption.
- B. It is designed only for point-to-point communications.
- C. It ranges up to 250 meters.

D. It supports data rates up to 1 and 2 Mb/s.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

ZigBee is based on the IEEE 802.15.4 protocol for WPAN, and aims at developing hardware and applications with a low data rate but also low power consumption and low complexity --for example, to control sensors. ZigBee-based products can access up to 16 separate 5 MHz channels in the 2.4 GHz band and are not compatible with 802.11 devices. The maximum power of ZigBee is 60 mW. Devices use low.

QUESTION 32

Which four options are the characteristics of the original 802.11 protocol? (Choose four.)

- A. Defined DSSS and FHSS as possible methods for modulation
- B. Designed to operate in the 5 GHz ISM frequency spectrum
- C. The most common deployment is three non-overlapping channels that are 20 MHz wide
- D. The protocol sets the maximum throughput at 1 Mb/s or 2 Mb/s
- E. Defined FHSS and OFDM as possible methods for modulation
- F. The most common deployment is three non-overlapping channels that are 22 MHz wide
- G. Designed to operate in the 2.4 GHz ISM frequency spectrum
- H. The protocol sets the maximum throughput at 1 Mb/s

Correct Answer: ACDG

Section: (none)

Explanation

Explanation/Reference:

Explanation:

FHSS is still described in the original 802.11 protocol, but another technique was preferred and adopted by all 802.11 networks: Direct Sequence Spread Spectrum. Instead of small channels and a jumping sequence, the information is sent over a wider channel. This channel is 22 MHz wide (if the center frequency is 2.412, this channel spans from 2.401 GHz to 2.423 GHz) and does not move (no hopping, which is why the sequence is said to be direct instead of hopping). Then, over this 22 MHz channel, several bits of information are sent in parallel. If a source of interference affects part of the channel, it will prevent only the bits sent in that frequency from reaching the receiver.

QUESTION 33

Which two attacks does Management Frame Protection help to mitigate? (Choose two.)

- A. Eavesdropping
- B. Denial of Service
- C. War Driving
- D. Man-in-the-Middle

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 34

Which statement about customization of a web page that is used on a WLC to authorize guest users is true?

- A. The administrator can use either a modified internal login page or the customized web page.
- B. The administrator can use only the internal login page, and only the organization logo can be changed.
- C. The administrator can use only the internal login page with a customized logo, headline, and message.
- D. The administrator can use only the customized web page that is uploaded to a WLC.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

<http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-0/configuration/guide/c70/c70users.html#wp1049273>

QUESTION 35

What is Cisco WCS Navigator?

- A. a single point of management for multiple Cisco WCS servers
- B. a server for storing and reviewing Cisco Spectrum Expert station data
- C. a server for storing the location data of wireless clients
- D. a GUI for displaying the data of Cisco CleanAir APs, aligned with an uploaded map
- E. a single point of management for multiple Cisco WLC systems

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The Cisco WCS Navigator centralizes the operational control and management of multiple Cisco WCS management platforms. This easy-to-use platform delivers the following cross-system capabilities:

<http://www.cisco.com/c/en/us/products/wireless/wireless-control-system-navigator/index.html>

QUESTION 36

What is the maximum number of access points supported on Cisco WCS with an enterprise license?

- A. 5,000
- B. 10,000
- C. 50,000
- D. 100,000

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

http://www.cisco.com/c/en/us/products/collateral/wireless/wireless-control-system/product_data_sheet0900aecd804b4646.html

QUESTION 37

Which user group has the ability to configure all features of the Cisco WCS except the user accounts and passwords?

- A. Admin
- B. SuperUser
- C. Root
- D. Supervisor

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

System Monitoring --Allows users to monitor WCS operations.

ConfigManagers --Allows users to monitor and configure WCS operations.

Admin --Allows users to monitor and configure WCS operations and perform all system administration tasks except administering WCS user accounts and passwords.

SuperUsers --Allows users to monitor and configure WCS operations and perform all system administration tasks including administering WCS user accounts and passwords. Superusers tasks can be changed.

North bound API --A user group used only with WCS Navigator.

Users Assistant --Allows only local net user administration. User assistants cannot configure or monitor controllers. They must access the Configure > Controller path to configure these local net features.

QUESTION 38

What must be done for Cisco WLC and Cisco WCS to communicate?

- A. The IP address and subnet mask of the Cisco WLC must be configured in the Cisco WCS.
- B. The IP address and subnet mask of the Cisco WCS must be configured in the Cisco WLC.
- C. The identity certificate of the Cisco WLC must be added to the Cisco WCS.
- D. The Cisco WLC and Cisco WCS must exchange identity certificates.

Correct Answer: A

Section: (none)

Explanation



Explanation/Reference:

Explanation:

In Cisco WCS, you need to add the ip address and subnet of the WLC. Autodiscovery is a feature that is used to search for a single controller by IP Address however this feature is restricted to Cisco WLAN Solution mobility group subnets defined by the operator.

QUESTION 39

Which protocol is used for Cisco WCS to communicate with Cisco WLC?

- A. SNMP
- B. CAPWAP
- C. HTTPS
- D. SSH

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

WCS simplifies controller configuration and monitoring and reduces data entry errors. WCS uses the industry-standard SNMP protocol to communicate with the controllers. WCS also includes the Floor Plan editor which allows you to do the following:

Vectorize bitmapped campus, floor plan, and outdoor area maps.

Add and change wall types.

Import the vector wall format maps into the database.

QUESTION 40

The administrator has noticed that the configuration on a controller is different than in Cisco WCS.

How can the administrator fix this issue?

- A. The configuration can be copied from the controller to the Cisco WCS or from the WCS to the controller.
- B. The configuration can be copied only from the Cisco WCS to the controller.
- C. The configuration can be copied only from the controller to the Cisco WCS.
- D. The controller must be removed from the Cisco WCS and then added again.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The Copy and Replace AP feature is useful if you need to remove an access point from the network and replace it with a new access point. All of the access point information, such as AP mode, name, and map location needs to be copied from the old access point to the new access point.

<http://www.cisco.com/c/en/us/td/docs/wireless/wcs/7-0MR1/configuration/guide/WCS70MR1/ctrlcfg.html#wp1097509>

QUESTION 41

The Cisco WCS administrator wants to create an accurate RF heat map based on RF prediction data. Which statement about map creation in Cisco WCS is true?

- A. The administrator must manually add walls, doors, and windows to the map.
- B. Cisco WCS automatically detects walls, doors, and windows and adds them to the map, but only when Cisco WCS Navigator is available.
- C. Cisco WCS automatically detects walls, doors, and windows and adds them to the map, but only when a Cisco 3300 Series MSE is available.
- D. All walls, doors, and windows must be included in the file that is uploaded as a background map.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

General Notes and Guidelines for Using the Map Editor Consider the following when modifying a building or floor map using the map editor. Cisco recommends that you use the map editor to draw walls and other obstacles rather than importing an .FPE file from the legacy floor plan editor. If necessary, you can still import .FPE files. To do so, navigate to the desired floor area, choose box, and browse to and choose the .FPE file. You can add any number of walls to a floor plan with the map editor; however, the processing power and memory of a client workstation may limit the refresh and rendering aspects of WCS. Cisco recommends a practical limit of 400 walls per floor for machines with 1-GB RAM or less. All walls are used by WCS when generating RF coverage heatmaps. However, the MSEs use no more than 50 heavy walls in its calculations, and the MSE does not use light walls in its calculations because those attenuations are already accounted for during the calibration process. If you have a high resolution image (near 12 megapixels), you may need to scale down the image resolution with an image editing software prior to using map editor.
http://www.cisco.com/c/en/us/td/docs/wireless/wcs/7-0/configuration/guide/WCS70cg/7_0maps.html

QUESTION 42

A Cisco WCS administrator has marked an alarm as acknowledged. For how many days does Cisco WCS prevent the alarm from reappearing, even if the source of the alarm reoccurs?

- A. 1
- B. 7
- C. 10
- D. 30



Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

WCS automatically deletes cleared alerts that are more than seven days old; therefore, your results can show activity only for the last seven days. Until an existing alarm is deleted, a new alarm cannot be generated for any managed entity for which WCS has already generated an alarm.

http://www.cisco.com/c/en/us/td/docs/wireless/wcs/7-0/configuration/guide/WCS70cg/7_0event.pdf

QUESTION 43

The administrator needs to create a report that shows all controllers, APs, and Cisco 3300 Series MSEs in the WLAN, including hardware and software information. Which report includes this information?

- A. Device > Inventory
- B. Mesh > Nodes
- C. Network Summary > Executive Summary
- D. Network Summary > 802.11 Summary

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

In the left sidebar menu, all of the inventory report options are listed. These reports are generated based on the data already stored in the WCS database. Because inventory reports are not on-demand reports, some configuration changes may have occurred since the storage and may not duplicate the attributes of the controller that are reflected in the stored data. The choices are as follows:

Access Point Inventory Report --Provides data on deployed access points. The data that is returned includes but is not limited to the following: the access points' MAC address, model, location, and radio status.
location appliances.

Controller Inventory Report --Provides data on deployed controllers. The data that is returned includes but is not limited to the following: the model, IP address, and serial number of the controller, what software version it is running, and where it is located.

Location Server Inventory Report --Provides data on deployed location appliances. The data that is returned includes but is not limited to the following: the IP address and version of the location appliance, which port is being used, and the time the appliance starts up.

<http://www.cisco.com/c/en/us/td/docs/wireless/wcs/4-1/configuration/guide/wcscfg41/wcsreps.html#wp1080212>

QUESTION 44

Which Cisco WLC command family can help to troubleshoot communication between an AP and the WLC?

- A. (Cisco Controller) >debug capwap
- B. (Cisco Controller) >debug ap
- C. (Cisco Controller) >debug cac
- D. (Cisco Controller) >debug dot11

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Example debugs available for this shown below:

WLC side debug commands:

(Cisco Controller) >debug capwap?

<https://mrncciew.files.wordpress.com/2013/03/brkewn-3011-troubleshooting-wireless-lans.pdf>

QUESTION 45

Which action secures the SNMPv2C protocol in a Cisco WLC?

- A. configure new communities and disable default communities
- B. use digital certificates to authenticate and encrypt transmissions
- C. enable password or transfer encryption
- D. set a username and difficult-to-guess password

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

See the SNMP configuration for Cisco WLC page shown in reference link below:

http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_0111.html

QUESTION 46

What is the purpose of the Log Analysis tab on the Client Troubleshooting page in Cisco WCS?

- A. After you click start, the tab shows debug information for the client that is trying to re-associate.
- B. The tab searches the logs for similar problems of other clients and generates a report.
- C. The tab generates a report from historical logs for the client that is having problems.
- D. The tab shows logs from the past hour for the client that is having problems.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 47

How can you protect the configuration file from eavesdropping, when uploading from a Cisco WLC?

- A. Use the Configuration File Encryption option.
- B. Choose an SCP as the transfer method.
- C. Connect to the Cisco WLC by using HTTPS.
- D. Connect to the Cisco WLC by using SSH.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Uploading the Configuration Files (GUI)

Step 1

Choose Commands > Upload File to open the Upload File from Controller page.

Step 2

From the File Type drop-down list, choose Configuration.

Step 3

Encrypt the configuration file by selecting the Configuration File Encryption check box and entering the encryption key in the Encryption Key text box.

Step 4

From the Transfer Mode drop-down list, choose from the following options:

Step 5

In the IP Address text box, enter the IP address of the server.

Step 6

In the File Path text box, enter the directory path of the configuration file.

Step 7

In the File Name text box, enter the name of the configuration file.

Step 8

If you are using an FTP server, follow these steps:

Step 9

Click Upload to upload the configuration file to the server. A message appears indicating the status of the upload. If the upload fails, repeat this procedure and try again.

http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-3/configuration/guide/b_cg73/b_wlc-cg_chapter_01010.html

QUESTION 48

Which CAPWAP AP management-access method is available as the default setting?

- A. only the console port
- B. the console port and SSH
- C. the console port, SSH, and HTTPS
- D. SSH only

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

After an access point joins the controller, the access point enables console port security only, and you are prompted for your username and password whenever you log into the access point's console port. When you log in, you are in non-privileged mode, and you must enter the enable password in order to use the privileged mode.

<http://www.cisco.com/c/en/us/td/docs/wireless/controller/5-2/configuration/guide/Controller52CG/c52lwap.pdf>

QUESTION 49

What tab contains access point configuration in the WCS?

- A. Controller > Access Points
- B. Configure > Access Points
- C. General > Configure > Access Points
- D. System > Configure > Access Points

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 50

What path displays the current maps within the WCS version 7 GUI?

- A. Monitor > Maps
- B. Reports > Maps
- C. Services > Maps
- D. Administration > Maps
- E. Configure > Maps
- F. Tools > Maps

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The physical location of the client (such as building, floor, and so on). Clicking the map location displays information in the Monitor > Maps page.

http://www.cisco.com/c/en/us/td/docs/wireless/wcs/7-0/configuration/guide/WCS70cg/7_0clientmgmt.html

QUESTION 51

A network engineer in the GUI of WCS version 7 wants to add an access point to a map. Where can this command be found within the drop-down menu?

- A. Monitor > Maps
- B. Reports > Maps
- C. Monitor > Network Summary
- D. Configure > Maps

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The physical location of the client (such as building, floor, and so on). Clicking the map location displays information in the Monitor > Maps page.

http://www.cisco.com/c/en/us/td/docs/wireless/wcs/7-0/configuration/guide/WCS70cg/7_0clientmgmt.html

QUESTION 52

A network engineer in the GUI of WCS version 7 wants to add an autonomous access point.

Where can this command be found in the drop-down menu?

- A. Configure > Access Point > Add Autonomous APs
- B. Manage > Access Points > Add Autonomous APs
- C. Administration > Access Point > Add Autonomous APs
- D. Location > Access Point > Add Autonomous APs

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

From WCS, the following methods are available for adding autonomous access points:

Add autonomous access points by Device information (IP addresses and credentials).

Add autonomous access points by CSV file

http://www.cisco.com/c/en/us/td/docs/wireless/wcs/7-0/configuration/guide/WCS70cg/7_0apcfg.html#wp1054452

QUESTION 53

What technology consists of small, low-power digital radios?

- A. LTE
- B. WiFi
- C. ZigBee
- D. Bluetooth

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

ZigBee is based on the IEEE 802.15.4 protocol for WPAN, and aims at developing hardware and applications with a low data rate but also low power consumption and low complexity --for example, to control sensors. ZigBee-based products can access up to 16 separate 5 MHz channels in the 2.4 GHz band and are not compatible with 802.11 devices. The maximum power of ZigBee is 60 mW. Devices use low consumption most of the time but can spike when needed: The impact on wireless networks can then be significant.

QUESTION 54

What protocol is used to determine the best pathway back to a root access point?

- A. CCKM
- B. WNMP
- C. AWPP
- D. LWAP

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

AWPP enables a remote access point to dynamically find the best path back to a RAP for each MAP that is part of the RAP's bridge group (BGN). Unlike traditional routing protocols, AWPP takes RF details into account. To optimize the route, a MAP actively solicits neighbor MAP. During the solicitation, the MAP learns all of the available neighbors back to a RAP (Root Access Point), determines which neighbor offers the best path, and then synchronizes with that neighbor. The path decisions of AWPP are based on link quality and the number of hops.

http://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/7-0/design/guide/MeshAP_70.html#wp1351984

QUESTION 55

How does an LWAP receive a configuration file?

- A. It is configured manually.
- B. It receives a configuration from the controller.
- C. It automatically ships with a configuration.
- D. It receives a configuration from a TFTP server.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You can use an upgrade conversion tool to convert autonomous Cisco Aironet 1100, 1130AG, 1200, 1240AG, and 1300 Series Access Points to lightweight mode. When you upgrade one of these access points to lightweight mode, the access point communicates with a controller and receives a configuration and software image from the controller.

<http://www.cisco.com/c/en/us/td/docs/wireless/controller/5-2/configuration/guide/Controller52CG/c52lwap.html>

QUESTION 56

A network engineer is troubleshooting a LAP that is unable to join the controller and receives the message below:

LWAPP_CLIENT_ERROR_DEBUG. No more AP manager IP addresses remain

What does the log indicate?

- A. Two or more LAPs have the same IP address.
- B. An AP manager has the same IP address as another AP manager.
- C. A LAP has the same IP address as the AP manager.
- D. Two or more controllers have the same IP address.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

This is another common issue that is seen when the AP tries to join the WLC. You might see this error message when the AP tries to join the controller.

No more AP manager IP addresses remain

One of the reasons for this error message is when there is a duplicate IP address on the network that matches the AP manager IP address. In such a case, the LAP keeps power cycling and cannot join the controller.

The debugs will show that the WLC receives LWAPP discovery requests from the APs and transmits a LWAPP discovery response to the APs. However, WLCs do not receive LWAPP join requests from the APs.

In order to troubleshoot this issue, ping the AP manager from a wired host on the same IP subnet as the AP manager. Then, check the ARP cache. If a duplicate IP address is found, remove the device with the duplicate IP address or change the IP address on the device so that it has a unique IP address on the network. The AP can then join the WLC.

<http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/99948-lap-notjoin-wlc-tshoot.html>

QUESTION 57

Which two of the following authentication methods used for WiFi security require the use of certificates? (Choose two.)

- A. PEAP
- B. EAP-FAST
- C. WPA2
- D. WPA1
- E. EAP-TLS
- F. EAP-MD5

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

When you use EAP with a strong EAP type, such as TLS with smart cards or TLS with certificates, both the client and the server use certificates to verify their identities to each other. Certificates must meet specific requirements both on the server and on the client for successful authentication.

<https://support.microsoft.com/en-us/kb/814394>

QUESTION 58

You are designing a wireless network in a medical facility. Which three areas are bad locations in which to install a wireless access point? (Choose three.)

- A. in front of the elevators doors
- B. in the hallways
- C. next to the electrical room
- D. inside offices
- E. near medical imaging devices
- F. in the lobby

Correct Answer: ACE

Section: (none)

Explanation

Explanation/Reference:**Explanation:**

You should not install access points in areas where interference from outside devices can occur. A great deal of electrical interference can occur near the electrical room and near medical imaging devices. Also, because elevators often have metal doors and the shafts are often concrete or contain other materials that degrade Wi-Fi coverage, it is best to avoid them.

QUESTION 59

What are the three primary functions of the Cisco Unified Wireless LWAPP architecture? (Choose three.)

- A. control and management of the CAPWAP
- B. tunneling of VPN clients over the WAN
- C. tunneling of WLAN client traffic to the WLC
- D. collection of 802.1Q trunks
- E. collection of 802.11 data for management
- F. control and management of VTP

Correct Answer: ACE

Section: (none)

Explanation**Explanation/Reference:****Explanation:**

Figure below illustrates one of the primary features of the architecture -- how Lightweight Access Point Protocol (LWAPP) access points (LAPs) use the LWAPP protocol to communicate with and tunnel traffic to a WLC.

http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/secwlandg20/sw2dg/ch4_2_SPMb.html

QUESTION 60

During Layer 2 intercontroller roaming, which two items change? (Choose two.)

- A. SSID
- B. VLAN
- C. IP address
- D. AP
- E. controller

Correct Answer: DE

Section: (none)

Explanation

Explanation/Reference:**Explanation:**

When the client associates to an access point joined to a new controller, the new controller exchanges mobility messages with the original controller, and the client database entry is moved to the new controller. New security context and associations are established if necessary, and the client database entry is updated for the new access point. This process remains transparent to the user.

<http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-0/configuration/guide/c70/c70mobil.html>

QUESTION 61

Which of the following are three functions of Cisco RRM? (Choose three.)

- A. TPC
- B. intercontroller roaming
- C. dynamic channel assignment
- D. intracontroller roaming
- E. coverage hole detection

Correct Answer: ACE

Section: (none)

Explanation**Explanation/Reference:****Explanation:**

RRM can periodically reconfigure the 802.11 RF network for best efficiency.

To do this, RRM performs these functions:

Radio resource monitoring

Transmit power control

Dynamic channel assignment

Coverage hole detection and correction

http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-0MR1/configuration/guide/wlc_cg70MR1/cg_rrm.pdf

QUESTION 62

You are setting up a laptop to connect to the wireless network of your organization. The protocols that are used for the corporate network are WPA2 Enterprise, PEAP, and AES. Which three parameters do you need to configure in the Windows 7 wireless network properties for this connection? (Choose three.)

- A. VLAN
- B. encryption type
- C. authentication method
- D. VRF
- E. security type

F. IP address

Correct Answer: BCE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

On the Security tab, you can specify the following security types:

Based on the selected security type, you can configure either a network security key or specify and configure a network authentication method. If you specify WPA-Enterprise, WPA2-Enterprise, or 802.1x as your security type, you must configure the following (as shown in the previous figure):

If you specify the use of WPA-Personal or WPA2-Personal as your security type or No authentication (Open) or Shared as your security type with WEP as your encryption type, you must configure a network security key, as shown in Figure 10.

<https://technet.microsoft.com/en-us/magazine/ff847520.aspx>

QUESTION 63

What are three characteristics of the 802.11g standard? (Choose three.)

- A. speed of as much as 11 Mb/s
- B. speed of as much as 54 Mb/s
- C. backward-compatibility with 802.11a
- D. backward-compatibility with 802.11b
- E. OFDM as an additional modulation technique
- F. OFDM and CCK as additional modulation techniques



Correct Answer: BDE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

802.11g is the third modulation standard for wireless LANs. It works in the 2.4 GHz band (like 802.11b) but operates at a maximum raw data rate of 54 Mbit/s. Using the CSMA/CA transmission scheme, 31.4 Mbit/s [1] is the maximum net throughput possible for packets of 1500 bytes in size and a 54 Mbit/s wireless rate (identical to 802.11a core, except for some additional legacy overhead for backward compatibility). In practice, access points may not have an ideal implementation and may therefore not be able to achieve even 31.4 Mbit/s throughput with 1500 byte packets. 1500 bytes is the usual limit for packets on the Internet and therefore a relevant size to benchmark against. Smaller packets give even lower theoretical throughput, down to 3 Mbit/s using 54 Mbit/s rate and 64 byte packets. Also, the available throughput is shared between all stations transmitting, including the AP so both downstream and upstream traffic is limited to a shared total of 31.4 Mbit/s using 1500 byte packets and 54 Mbit/s rate. 802.11g hardware is fully backwards compatible with 802.11b hardware. Details of making b and g work well together occupied much of the lingering technical process. In an 802.11g network, however, the presence of a legacy 802.11b participant will significantly reduce the speed of the overall 802.11g network. Some 802.11g routers employ a back-compatible mode for 802.11b clients called 54g LRS (Limited Rate Support). [2]

The modulation scheme used in 802.11g is orthogonal frequency-division multiplexing (OFDM) copied from 802.11a with data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbit/s, and reverts to CCK (like the 802.11b standard) for 5.5 and 11 Mbit/s and DBPSK/DQPSK+DSSS for 1 and 2 Mbit/s. Even though 802.11g operates in the same frequency band as 802.11b, it can achieve higher data rates because of its heritage to 802.11a.
http://en.wikipedia.org/wiki/IEEE_802.11g-2003

QUESTION 64

Which two types of encryption does Windows support for WPA2 security for wireless connections? (Choose two.)

- A. AES
- B. DES
- C. PGP
- D. TKIP
- E. WEP

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

TKIP and AES are two different types of encryption that can be used by a Wi-Fi network. TKIP stands for "Temporal Key Integrity Protocol." It was a stopgap encryption protocol introduced with WPA to replace the very-insecure WEP encryption at the time. TKIP is actually quite similar to WEP encryption. TKIP is no longer considered secure, and is now deprecated. In other words, you shouldn't be using it.

AES stands for "Advanced Encryption Standard." This was a more secure encryption protocol introduced with WPA2, which replaced the interim WPA standard. AES isn't some creaky standard developed specifically for Wi-Fi networks; it's a serious worldwide encryption standard that's even been adopted by the US government. For example, when you encrypt a hard drive with TrueCrypt, it can use AES encryption for that. AES is generally considered quite secure, and the main weaknesses would be brute-force attacks (prevented by using a strong passphrase) and security weaknesses in other aspects of WPA2.

<http://www.howtogeek.com/204697/wi-fi-security-should-you-use-wpa2-aes-wpa2-tkip-or-both/>

QUESTION 65

Which two wireless technologies can interfere with 802.11 networks? (Choose two.)

- A. DECT
- B. ZigBee
- C. WiMax
- D. GSM

Correct Answer: AB

Section: (none)

Explanation**Explanation/Reference:****Explanation:**

Here is how Cisco RRM works from a high level:

What are the algorithms that the RF Group Leader will be busy with?

<http://blog.ine.com/2010/10/08/cisco-radio-resource-management-rrm/>

QUESTION 66

Which two algorithms are available in RRM? (Choose two.)

- A. coverage-hole detection
- B. dynamic channel assignment
- C. RSSI normalizer
- D. transmitting channel expander
- E. rogue detection

Correct Answer: AB

Section: (none)

Explanation**Explanation/Reference:****Explanation:**

Most clients enable you to associate to a detected network (broadcasted SSID) or configure a specific profile. In all cases, you must configure the network name (SSID), the operating mode (ad-hoc or infrastructure), and some security settings (that will be different depending on whether the SSID uses Pre-Shared Key Security or Enterprise [EAP/802.1x] security).

QUESTION 67

Which two pieces of information are needed for the wireless client to connect to the wireless network? (Choose two.)

- A. SSID
- B. security settings
- C. channel number
- D. AP name

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:**QUESTION 68**

What are two wireless configuration utilities for Apple Mac computers? (Choose two.)

- A. AirPort
- B. AirPort Extreme
- C. AirManager
- D. AirManager Supreme
- E. AirAssistant Ultimate

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:**Explanation:**

AirPort (for 802.11b) and AirPort Extreme (for 802.11b/g/n or 802.11a/b/g/n) are WLAN configuration utilities from Apple. The utility allows the creation of network profiles, association to detected networks, and advanced configuration and troubleshooting. The wireless card can be disabled or enabled from the utility main window.

QUESTION 69

What are two modules of the CCX Lite program? (Choose two.)

- A. foundation
- B. voice
- C. RF power
- D. roaming

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:**Explanation:**

In summer 2011, Cisco separated the CCX features into four subfamilies to help vendors integrate only those features that are needed for their specific wireless clients (called application-specific devices, which are devices built for a specific function [for example, barcode scanners or VoWLAN phones] and therefore do not need all the CCX features that a data laptop would need). This is called the CCX Lite program, with four components:

QUESTION 70

What are two security threats to wireless networks? (Choose two.)

- A. ad-hoc networks
- B. client misassociation
- C. port redirection
- D. cross-site scripting

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

An ad hoc network is a collection of wireless clients that form a network amongst themselves without the use of an AP. As far as network administrators are concerned, ad hoc wireless networks are uncontrolled. If they do not use encryption, they may expose sensitive data to outside eavesdroppers. If a device is connected to a wired network and has bridging enabled, an ad-hoc network may also function like a rogue AP. Additionally, ad-hoc networks can expose client devices to viruses and other security vulnerabilities. For these reasons, many administrators choose to prohibit ad-hoc networks.

Valid Client Misassociation:

This feature does not detect attacks, but rather it monitors authorized (valid) wireless clients and their association within the network. Valid client misassociation is potentially dangerous to network security. The four types of misassociation that we monitor are:

http://www.arubanetworks.com/techdocs/ArubaOS_61/ArubaOS_61_UG/New_WIP.php

QUESTION 71

In a network with a deployed Cisco WLC, which two entities must be configured with the shared secret key for 802.1X authentication? (Choose two.)

- A. WLC
- B. RADIUS server
- C. AP
- D. supplicant
- E. wireless client

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The WLC needs to be configured in order to forward the user credentials to an external RADIUS server. The external RADIUS server then validates the user credentials and provides access to the wireless clients.

<http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/69730-eap-auth-wlc.html>

QUESTION 72

Which two formats are supported for uploading background graphics to create a network map in Cisco WCS? (Choose two.)

- A. PNG
- B. JPEG
- C. DWG
- D. TIFF

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 73

Which two destinations can Cisco WCS administrators specify for a scheduled report? (Choose two.)

- A. a file on the Cisco WCS
- B. a specified email address
- C. a specified World Wide Web server
- D. a TFTP server

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

http://www.cisco.com/c/en/us/td/docs/wireless/wcs/7-0/configuration/guide/WCS70cg/7_0reps.html

QUESTION 74

Which two formats are available for Cisco WCS reports? (Choose two.)

- A. PDF

- B. CSV
- C. HTML
- D. TXT

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Reports are saved in either CSV or PDF format and are either saved to a file on WCS for later download or e-mailed to a specific e-mail address.
http://www.cisco.com/c/en/us/td/docs/wireless/wcs/7-0/configuration/guide/WCS70cg/7_0reps.html.

QUESTION 75

Which two protocols are available to download or upload files to or from Cisco WLC? (Choose two.)

- A. FTP
- B. TFTP
- C. SCP
- D. HTTP
- E. HTTPS



Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Uploading the Configuration Files (GUI)

Step 1

Choose Commands > Upload File to open the Upload File from Controller page.

Step 2

From the File Type drop-down list, choose Configuration.

Step 3

Encrypt the configuration file by selecting the Configuration File Encryption check box and entering the encryption key in the Encryption Key text box.

Step 4

From the Transfer Mode drop-down list, choose from the following options:

Step 5

In the IP Address text box, enter the IP address of the server.

Step 6

In the File Path text box, enter the directory path of the configuration file.

Step 7

In the File Name text box, enter the name of the configuration file.

Step 8

If you are using an FTP server, follow these steps:

Step 9

Click Upload to upload the configuration file to the server. A message appears indicating the status of the upload. If the upload fails, repeat this procedure and try again.

http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-3/configuration/guide/b_cg73/b_wlc-cg_chapter_01010.html

QUESTION 76

Which two Cisco WLC management-access methods are available as the default setting? (Choose two.)

- A. SSH
- B. HTTPS
- C. Telnet
- D. HTTP

Correct Answer: AB

Section: (none)

Explanation



Explanation/Reference:

Explanation:

The less secure methods of telnet and SSH are disabled by default and need to be manually configured. Only SSH and HTTPS are enabled by default.

QUESTION 77

Which statement describes spread spectrum technology in wireless communications?

- A. Signal is spread across optical pulses.
- B. Signal is spread across variations of amplitudes.
- C. Signal is spread across one frequency.
- D. Signal is spread across a whole band of frequencies.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

spread-spectrum techniques are methods by which a signal with a particular bandwidth is deliberately spread in the frequency domain, resulting in a signal with a wider bandwidth. Spread spectrum generally makes use of a sequential noise-like signal structure to spread the normally narrowband information signal over a relatively wideband (radio) band of frequencies.
http://en.wikipedia.org/wiki/Spread_spectrum

QUESTION 78

Which type of basic radiation pattern does a Yagi antenna have?

- A. circular
- B. semicircular
- C. straight line
- D. cone

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

High gain directional antennas: A point to point high gain antenna is a directional antenna that has a focused radiation pattern. The radiation pattern is typically a cone 10 to 30 degrees wide.

A yagi and a parabolic dish are examples of high gain directional antennas.

http://www.hp.com/rnd/pdfs/antenna_tech_brief.pdf

QUESTION 79

Which wireless topology supports roaming?

- A. IBSS
- B. BSS
- C. ESS
- D. bridging

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 80

You are configuring an IP address on an autonomous access point. Which interface do you use to configure the IP address?

- A. BVI1
- B. FastEthernet 0
- C. Dot11Radio0
- D. VLAN 1

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Assigning the IP Address to the BVI

When you assign an IP address to the access point by using the CLI, you must assign the address to the bridge-group virtual interface (BVI). Beginning in a privileged EXEC mode, follow these steps to assign an IP address to the access point BVI using the access point console port.

Command

Purpose

Step 1

configure terminal

Enter global configuration mode.

Step 2

interface bvi1

Enters interface configuration mode for the BVI.

Step 3

ip address ip_address net_mask

Assigns an IP address and subnet mask address to the BVI.

http://www.cisco.com/c/en/us/td/docs/wireless/access_point/1140/autonomous/getting_started/gui_de/ap1140aut_getstart.html



QUESTION 81

You run minimum PEAP-GTC authentication in your wireless environment. Which version of Cisco Compatible Extensions supports PEAP-GTC?

- A. Cisco Compatible Extensions v1
- B. Cisco Compatible Extensions v2
- C. Cisco Compatible Extensions v3
- D. Cisco Compatible Extensions v4
- E. Cisco Compatible Extensions v5

Correct Answer: B

Section: (none)

Explanation**Explanation/Reference:****Explanation:**

* PEAP/GTC is supported on Cisco Compatible Version 2 clients and above.

http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1300-series/prod_gas09186a00802030dc.html

QUESTION 82

Which device divides a signal between two antennas?

- A. splitter
- B. lightening arrestor
- C. attenuator
- D. amplifier

Correct Answer: A

Section: (none)

Explanation**Explanation/Reference:****Explanation:**

A splitter causes insertion loss and divides available power between two antennas.

QUESTION 83

What does RF determine?

- A. cycle pattern size
- B. how often a wave occurs
- C. signal size
- D. quantity of energy injected in a signal

Correct Answer: B

Section: (none)

Explanation**Explanation/Reference:****Explanation:**

RF communication works by creating electromagnetic waves at a source and being able to pick up those electromagnetic waves at a particular destination. These electromagnetic waves travel through the air at near the speed of light. The wavelength of an electromagnetic signal is inversely proportional to the frequency; the

higher the frequency, the shorter the wavelength.
<http://www.digi.com/technology/rf-articles/rf-basic>

QUESTION 84

Which module does the Cisco AnyConnect Secure Mobility client integrate into the AnyConnect client package for access to both wired and wireless networks?

- A. Network Access Manager
- B. Telemetry
- C. Web Security
- D. DART

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The main components used in IUWNE are the Cisco AnyConnect Mobility Client itself, associated with the Network Access Module (NAM) used to manage existing profiles and provide the wireless connectivity.

QUESTION 85

Access points must discover a wireless LAN controller before they can become an active part of the network.
In which order does an access point try to discover a controller?

- A. Layer 3 CAPWAP or LWAPP broadcast discovery
DHCP option 43
Locally stored controller IP address discovery
DNS controller name resolution
- B. Layer 3 CAPWAP or LWAPP broadcast discovery
Locally stored controller IP address discovery
DNS controller name resolution
DHCP option 43
- C. Layer 3 CAPWAP or LWAPP broadcast discovery
Locally stored controller IP address discovery
DHCP option 43
DNS controller name resolution
- D. DNS controller name resolution
DHCP option 43
Layer 3 CAPWAP or LWAPP broadcast discovery
Locally stored controller IP address discovery

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 86

You are configuring SNMPv1/v2c on a WLC. What should you do for improved security?

- A. Remove the default SNMPv1 community.
- B. Remove the default SNMPv1 and SNMPv2 communities.
- C. Remove the default SNMPv2 community.
- D. Remove the default SNMPv3 users.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The controller has commonly known default values of "public" and "private" for the read-only and read-write SNMP community strings. Using these standard values presents a security risk. If you use the default community names, and since these are known, the community names could be used to communicate to the controller using SNMP. Therefore, we strongly advise that you change these values.

Step 1

Choose Management and then Communities under SNMP. The SNMP v1 / v2c Community page appears.

Step 2

If "public" or "private" appears in the Community Name column, hover your cursor over the blue drop-down arrow for the desired community and choose Remove to delete this community.

Step 3

Click New to create a new community. The SNMP v1 / v2c Community > New page appears.

Step 4

In the Community Name text box, enter a unique name containing up to 16 alphanumeric characters. Do not enter "public" or "private."

Step 5

In the next two text boxes, enter the IPv4/IPv6 address and IP Mask/Prefix Length from which this device accepts SNMP packets with the associated community and the IP mask.

Step 6

Choose Read Only or Read/Write from the Access Mode drop-down list to specify the access level for this community.

Step 7

Choose Enable or Disable from the Status drop-down list to specify the status of this community.

Step 8

Click Apply to commit your changes.

Step 9

Click Save Configuration to save your settings.

Step 10

Repeat this procedure if a "public" or "private" community still appears on the SNMP v1 / v2c Community page.

QUESTION 87

Which spread spectrum technique uses 11-bit chips to transmit 1 bit of data over a 22-MHz channel?

- A. DSSS
- B. FHSS
- C. OFDM
- D. MIMO
- E. CCK

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

For every 0 or 1 you want to send, DSSS generates a code representing that 0 or that 1. This code, also called symbol or chip, can be a sequence of up to 11 bits (this is called the Barker 11 code), and these 11 bits are sent in parallel over the 22 MHz channel. You can lose up to nine of these 11 bits due to interferences and still understand whether the code sent was supposed to represent a 0 or a 1.

QUESTION 88

The network administrator has used VLANs to separate VoIP frames from data frames in the wired network. What must the administrator use to separate those frames in the wireless network?

- A. multiple SSIDs
- B. multiple authentications
- C. multiple WEP or WPA keys
- D. multiple channels
- E. multiple 802.11 radios (a, b, g, n)

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:**Explanation:**

Multiple IEEE 802.11 service set identifiers (SSIDs) allow you to create different levels of network access and to access virtual LANs (VLANs). You can configure up to 16 separate SSIDs to support up to 16 VLANs. Each VLAN can have a different wireless security configuration so that the devices that support the latest Cisco security enhancements can exist alongside legacy devices. This additional access point functionality enables a variety of users having different security levels to access different parts of the network.

http://www.cisco.com/en/US/docs/wireless/access_point/350/configuration/guide/ap350ch1_ps458_TSD_Products_Configuration_Guide_Chapter.html

QUESTION 89

What is the IEEE name for a group of access points that are connected by using the Ethernet?

- A. ESS
- B. BSS
- C. IBSS
- D. ISS

Correct Answer: A

Section: (none)

Explanation

**Explanation/Reference:****Explanation:**

The wired section of the network that can be reached through the AP is called, from the perspective of the wireless side, the Distribution System (DS). When the distribution system links two APs, or two cells, via Ethernet, the group is called an Extended Service Set (ESS).

QUESTION 90

Which type of frames are ACK and CF-ACK?

- A. control
- B. management
- C. RTS/CTS
- D. association

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Wireless LANs come in three frame types:

Frame Types Table

Management

Control

Data

Beacon

Request to Send (RTS)

Simple data

Probe Request

Clear to Send (CTS)

Null function

Probe Response

Acknowledgment

Data+CF-ACK

Association Request

Power-Save-Poll (PS-Poll)

Data+CF-Poll

Association Response

Contention Free End (CF-End)

Data+CF-Ack

Authentication Request

Contention Free End + Acknowledgment (CF-End +ACK)

ACK+CF-Poll

Authentication Response

CF-ACK

Deauthentication

CF-ACK+CF-Poll

Reassociation request

Reassociation response

Announcement traffic indication message (ATIM)

<http://www.ciscopress.com/articles/article.asp?p=1271797&seqNum=2>

**QUESTION 91**

The network administrator wants an access point to be able to find rogue APs and to support location-based services. Which AP mode meets this requirement while having the radios up and preventing client connections?

- A. monitor
- B. sniffer
- C. rogue-detection
- D. H-REAP

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

If you have enough access points, you can even dedicate an AP to making it's only job picking up other networks, this a mode that the AP can be in and is called "Monitor Mode" to change an AP to monitor mode, navigate to the following on the WLC:

This will place the AP into a dedicated monitor mode, it will not service clients but will sit and scan for you.

QUESTION 92

What are the interface statuses of a lightweight AP working in rogue-detection mode?

- A. radios turned off, Ethernet interface up
- B. radios and Ethernet interfaces up
- C. radios turned on, Ethernet interface shut down
- D. radios turned on, Ethernet interface status controlled by Cisco WLC

Correct Answer: A

Section: (none)

Explanation



Explanation/Reference:

Explanation:

In this mode, the AP radio is turned off, and the AP listens to wired traffic only. The controller passes the APs configured as rogue detectors as well as lists of suspected rogue clients and AP MAC addresses. The rogue detector listens for ARP packets only, and can be connected to all broadcast domains through a trunk link if desired.

<http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/70987-rogue-detect.html>

QUESTION 93

Which Cisco AnyConnect module allows you to set the parameters that are needed to connect to the wireless network?

- A. NAM
- B. DART
- C. posture
- D. telemetry

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The main components used in IUWNE are the Cisco AnyConnect Mobility Client itself, associated with the Network Access Module (NAM) used to manage existing profiles and provide the wireless connectivity. You also can click Advanced to open the NAM front end. You can then manage profiles (create, delete, reorder). The network administrator can restrict the types of networks that the end user can manipulate on the NAM.

QUESTION 94

What is the function of the Cisco AnyConnect DART tool?

- A. creates a compressed bundle of client logs and information
- B. visualizes a WLAN environment, showing the possible locations of problems
- C. gathers statistics from neighboring clients for comparison to the baseline
- D. helps to troubleshoot a WLAN connection by using easy-to-use wizards and statistic viewers

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

AnyConnect offers the DART module that can be used to analyze and troubleshoot connections.

The information collected by DART can be examined locally or exported and sent to a network support desk for analysis. The DART tool is able to create a bundle to log information for all the wireless clients.

QUESTION 95

Which Cisco program for WLAN client vendors helps to ensure that their devices are interoperable with Cisco WLAN infrastructure?

- A. CCX
- B. CCMP
- C. ASDM
- D. WLSE

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:**Explanation:**

IEEE and industry standards define how a Wi-Fi radio interoperates with a wireless LAN infrastructure, and the Wi-Fi CERTIFIED™ seal ensures interoperability. For many organizations that rely on mobile computers, however, Wi-Fi CERTIFIED is not enough. These organizations need assurance that their mobile computers will interoperate with a Cisco wireless LAN infrastructure and support Cisco wireless LAN innovations for enhanced security, mobility, quality of service, and network management. The Cisco Compatible seal gives organizations the assurance that they seek.

A mobile computer earns the Cisco Compatible seal through a program called Cisco Compatible Extensions, or CCX. Like the Wi-Fi certification program, CCX: The CCX specification is a superset of that used for Wi-Fi certification. In fact, a device cannot be certified for CCX unless it, or the Wi-Fi radio inside it, is Wi-Fi CERTIFIED.

http://www.digikey.com/Web%20Export/Supplier%20Content/Laird_776/PDF/laire-wireless-value-cisco-compatible-extension.pdf?redirected=1

QUESTION 96

Which information on the Monitoring page of a Cisco WLC verifies that the wireless network is operational?

- A. In the Access Point Summary section, the All APs number in the Up column is the same as in the Total column.
- B. In the Client Summary section, the Current Clients number is positive.
- C. In the Controller Summary section, the 802.11b/g Network State is shown as Enabled.
- D. In the Controller Summary section, the CPU Usage number is positive.

Correct Answer: A

Section: (none)

Explanation

**Explanation/Reference:****Explanation:**

The output from the access point summary section of the Cisco WLC can be seen at the reference link below:

http://www.cisco.com/c/en/us/td/docs/wireless/wcs/6-0/configuration/guide/WCS60cg/6_0mon.html

QUESTION 97

What is a risk when initiating the containment of a rogue AP?

- A. disassociating clients of valid access points that are operated by a neighboring organization
- B. disrupting transmission of neighboring AP clients
- C. breaking the radio of the containing AP
- D. breaking the rogue client radio or its firmware

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:**Explanation:**

Rogue Containment Caveats

<http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/112045-handling-rogue-cuwn-00.html>

QUESTION 98

Which method is used to shield the client from class 3 management attacks?

- A. client MFP
- B. WEP
- C. WPA
- D. client protection suite
- E. 802.1X

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:**Explanation:**

With MFP, all management frames are cryptographically hashed to create a Message Integrity Check (MIC). The MIC is added to the end of the frame (before the Frame Check Sequence (FCS)).

When MFP is enabled on one or more WLANs configured in the WLC, the WLC sends a unique key to each radio on each registered AP. Management frames are sent by the AP over the MFP-enabled WLANs. These APs are labeled with a frame protection MIC IE. Any attempt to alter the frame invalidates the message, which causes the receiving AP that is configured to detect MFP frames to report the discrepancy to the WLAN controller.

<http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/82196-mfp.html>

QUESTION 99

Which protocol helps the administrator to determine whether a detected rogue AP is in the network of the organization?

- A. RLDP
- B. RCP
- C. RDP
- D. RAPP

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:**Explanation:**

RLDP is an active approach, which is used when rogue AP has no authentication (Open Authentication) configured. This mode, which is disabled by default, instructs an active AP to move to the rogue channel and connect to the rogue as a client. During this time, the active AP sends deauthentication messages to all connected clients and then shuts down the radio interface. Then, it will associate to the rogue AP as a client.

The AP then tries to obtain an IP address from the rogue AP and forwards a User Datagram Protocol (UDP) packet (port 6352) that contains the local AP and rogue connection information to the controller through the rogue AP. If the controller receives this packet, the alarm is set to notify the network administrator that a rogue AP was discovered on the wired network with the RLDP feature.

<https://supportforums.cisco.com/discussion/10941011/rd-rogue-detector-or-rldp-rogue-location-discovery-protocol>

QUESTION 100

Which wireless client attempts to authenticate by using 802.1X?

- A. supplicant
- B. authenticator
- C. EAP
- D. RADIUS

Correct Answer: A

Section: (none)

Explanation**Explanation/Reference:****Explanation:**

802.1x is an Institute of Electrical and Electronics Engineers (IEEE) standard that provides an authentication framework for WLANs. 802.1x uses the Extensible Authentication Protocol (EAP) to exchange messages during the authentication process. The authentication protocols that operate inside the 802.1x framework that are suitable for wireless networks include EAP-Transport Layer Security (EAP-TLS), Protected EAP (PEAP), and EAP-Tunneled TLS (EAP-TTLS). These protocols allow the network to authenticate the client while also allowing the client to authenticate the network.

802.1x authentication consists of three components:

http://www.arubanetworks.com/techdocs/ArubaOS_60/UserGuide/802.1x.php

QUESTION 101

Which EAP protocol requires a certificate only on the server side?

- A. EAP-PEAP
- B. EAP-FAST
- C. EAP-TLS
- D. EAP-SSL

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

PEAP is not an encryption protocol; as with other EAP types it only authenticates a client into a network.

PEAP uses only server-side public key certificates to authenticate clients by creating an encrypted SSL/TLS tunnel between the client and the authentication server, which protects the ensuing exchange of authentication information from casual inspection.

<http://wiki.freeradius.org/protocol/EAP-PEAP>

QUESTION 102

Which encryption algorithm does WPA use?

- A. RC4
- B. DES
- C. AES
- D. DH5

Correct Answer: A

Section: (none)

Explanation



Explanation/Reference:

Explanation:

The RC4 Encryption Algorithm, developed by Ronald Rivest of RSA, is a shared key stream cipher algorithm requiring a secure exchange of a shared key. The symmetric key algorithm is used identically for encryption and decryption such that the data stream is simply XORed with the generated key sequence. The algorithm is serial as it requires successive exchanges of state entries based on the key sequence. Hence implementations can be very computationally intensive.

The RC4 encryption algorithm is used by standards such as IEEE 802.11 within WEP (Wireless Encryption Protocol) using 40 and 128-bit keys. Published procedures exist for cracking the security measures as implemented in WEP.

<http://www.vocal.com/cryptography/rc4-encryption-algorithm/>

QUESTION 103

Which statement about configuration of Layer 2 wireless user authentication on a Cisco WLC is true?

- A. Local EAP is used only if an external RADIUS is not configured or is unreachable.
- B. The external RADIUS is used only if local EAP is not configured.
- C. The administrator chooses whether local EAP or an external RADIUS is used first.
- D. The external RADIUS is used only if local EAP is explicitly disabled.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

If any RADIUS servers are configured on the controller, the controller tries to authenticate the wireless clients using the RADIUS servers first. Local EAP is attempted only if no RADIUS servers are found, either because the RADIUS servers timed out or no RADIUS servers were configured. If four RADIUS servers are configured, the controller attempts to authenticate the client with the first RADIUS server, then the second RADIUS server, and then local EAP. If the client attempts to then reauthenticate manually, the controller tries the third RADIUS server, then the fourth RADIUS server, and then local EAP.

http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_0110010.html

QUESTION 104

Which statement describes a security weakness of a WPA2 with a PSK?

- A. The compromised key can be used for another connection.
- B. The key can be eavesdropped from the wireless medium.
- C. The key can be recreated from a few eavesdropped frames.
- D. The key is not case-sensitive and is vulnerable to compromise by brute-force methods.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

WPA2-Enterprise is (in my opinion) considerably more secure than PSK.

QUESTION 105

To implement a more secure means of communication for voice and data, what technology successfully resists interference by utilizing a wider bandwidth than needed for the transmitting signal?

- A. Spread Spectrum
- B. Microwave
- C. Extended U-NII2
- D. ISM Bands

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:**QUESTION 106**

An 802.11g network is experiencing intermittent signal degradation and Spectrum Analyzer is being used to try and locate the problem. What two interferers would likely be identified? (Choose two.)

- A. multiple cell phones
- B. microwave oven
- C. FM Radio
- D. cordless phone
- E. document scanner

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:**QUESTION 107**

A wireless bridge is being installed near an airport. An organization informs the city council about complying with max power levels that could be used and settings on any 5GHz channels used that might interfere with the airport radar. What organization is this?

- A. Institute of Electrical and Electronics Engineers
- B. Internet Engineering Task Force
- C. Federal Communications Commission
- D. Wireless Fidelity Alliance

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:**QUESTION 108**

An installation uses a 21dBi parabolic dish. It is connected to the 802.11n radio via low loss antenna coax rated at 4dB loss/100 feet. After testing, it has been

determined that 2mW of power will be lost in the cable. An EIRP producing 200mW is desired. What should the transmit power be set to?

- A. 8mW
- B. 3dBm
- C. 3.16mW
- D. 5mW

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 109

An engineer is seeing a pattern closest to that of an Isotropic Radiator. What other antenna will produce a similar pattern?

- A. 5 dBi patch
- B. 13.5 dBi Yagi
- C. 2.2 dBi omni
- D. 21 dBi parabolic



Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 110

When using multiple SSIDs on a lightweight AP, how does the traffic of each SSID reach the 802.3 network?

- A. provide routing between them at the core so that the SSIDs can reach the internet
- B. configure 802.11q trunking on the Ethernet switch port that is connected to the AP
- C. configure ACLs at the switch port that will allow all desired SSIDs to pass traffic
- D. configure the SSIDs on the WLC and it will regulate the traffic based on traffic type

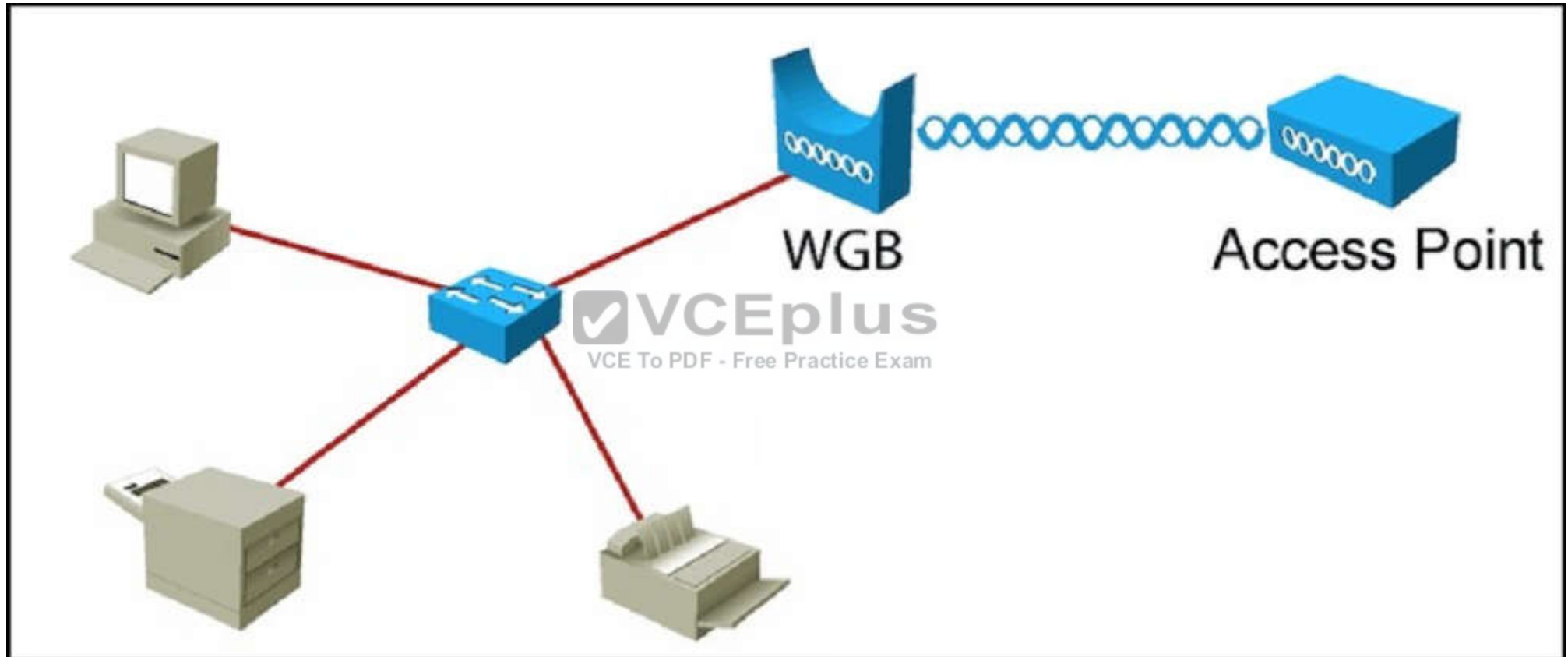
Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 111



Refer to the exhibit. Based on the diagram, what two design requirements must be met? (Choose two.)

- A. WGB is Autonomous
- B. WGB is Universal
- C. WGB can be Autonomous or Universal

- D. Upstream AP is Aironet
- E. Upstream AP is not Aironet
- F. Upstream AP can be any make/model

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 112

What 802.1x role is responsible for moving a port to the authorized state?

- A. Supplicant
- B. Authenticator
- C. Authentication Server
- D. RADIUS Server

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 113

How many types of control frames are only used in PCF mode?

- A. 0
- B. 1
- C. 2
- D. 3
- E. 4
- F. 5

Correct Answer: D

Section: (none)

Explanation**Explanation/Reference:****QUESTION 114**

An engineer is gathering information for a wireless survey of a hospital. What three pieces of information must be collected for an active survey to assess the outcome best suited for the facility? (Choose three.)

- A. presence of microwave ovens
- B. number of patients that are at the facility
- C. utilization of Location Services or voice applications
- D. floor plans of adjacent facilities
- E. use of wireless for secure records
- F. spectrum analysis to locate all the computer work stations
- G. existing Network Switch types and model numbers
- H. type of devices present on the new wireless network

Correct Answer: ACH

Section: (none)

Explanation

**Explanation/Reference:****QUESTION 115**

A company wants to implement wireless in all 20 remote office locations and wants centralized management of these remote sites. What application would meet the requirements?

- A. Control And Provisioning of Wireless Access Points
- B. Cisco point- to multi-point wireless bridging
- C. Cisco autonomous access points in FlexConnect mode
- D. Split MAC architecture utilizing LWAPP and WLC

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 116

A customer mounted three new APs in a small business. After configuring the IP address, users still could not access the web through the new access points. What two configurations are needed to fix this? (Choose two.)

- A. Security parameters
- B. Gateway address
- C. Service Set ID
- D. Antenna option
- E. EAP Authentication
- F. Unique AP Name

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

**QUESTION 117**

A client is deploying lightweight APs. Those with LAN connections to the controller would be considered what mode of deployment, while access points deployed across a higher latency connection are deployed in what mode?

- A. HREAP; Bridge
- B. Local; Bridge
- C. HREAP; Flex Connect
- D. Local; Flex Connect

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 118

When using DHCP option 43, the discovery option supports vendor specific identifiers in order to obtain what IP address?

- A. core router's gateway
- B. closest distribution switch
- C. local WLAN controller
- D. local Radius Server

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 119

Wireless clients are experiencing loss of connectivity while roaming between controllers. To fix this, what configuration should be the same on all controllers within the mobility group?

- A. management interface IP address
- B. IP address of the virtual interface
- C. AP Manager interface IP address
- D. IP address of the Service Port



Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 120

What is a function of the service port on a WLC?

- A. controls mobility manager communications on all physical ports
- B. controls out-of-band management for system recovery and maintenance
- C. controls communication with Cisco Aps
- D. controls communications for all physical ports

Correct Answer: B

Section: (none)

Explanation**Explanation/Reference:****QUESTION 121**

What are three functions of RRM? (Choose three.)

- A. dynamic channel assignment
- B. detection and avoidance of interference
- C. dynamic antenna polarization
- D. dynamic transmit power control
- E. dynamic controller selection
- F. detection and avoidance of AP client load

Correct Answer: ABD

Section: (none)

Explanation**Explanation/Reference:****QUESTION 122**

What three components are required to configure Mobility Group Members between Wireless LAN Controllers? (Choose three.)

- A. Controller Management IP Address
- B. Controller Virtual IP Address
- C. Controller Multicast IP Address
- D. Controller MAC Address
- E. Controller Mobility Group Name
- F. Controller AP Management IP Address
- G. Controller RF Group Name

Correct Answer: ADE

Section: (none)

Explanation**Explanation/Reference:**

QUESTION 123

What authentication method requires a certificate on both the client and authentication server?

- A. PEAP
- B. EAP-TLS
- C. EAP-FAST
- D. WPA-PSK
- E. WEP
- F. EAP-TTLS

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 124

An enterprise needs their iPhones to connect to the EAP-TLS network. How should the devices be configured?

- A. push profile and certificate through Configuration Utility
- B. configure directly through Settings application
- C. email certificate to device then configure through Settings application
- D. download certificate from web page then configure through Settings application
- E. push profile and certificate through iTunes

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 125

What AnyConnect module can be used to provide a detailed scan list of the Wi-Fi environment?

- A. DART

- B. Telemetry
- C. Web Security
- D. NAM
- E. Posture

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 126

What two capabilities would be present on a wireless client device that supports CCXv3? (Choose two.)

- A. WPA2
- B. 802.1x
- C. PEAP-MSCHAP
- D. NAC
- E. MFP
- F. EAP-TLS



Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 127

To mitigate DoS attacks on a network, what security method should be implemented?

- A. WEP
- B. 802.1x
- C. Non-broadcast SSID
- D. Client MFP

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 128

What protocol overcomes the weaknesses of LEAP?

- A. EAP-TLS
- B. PEAP
- C. EAP-FAST
- D. EAP-TTLS

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



QUESTION 129

What encryption standards describe WPA and WPA2?

- A. WPA mandates AES with TKIP optional, WPA2 mandates TKIP
- B. WPA mandates TKIP with AES optional, WPA2 mandates AES
- C. WPA mandates CKIP, WPA2 mandates AES
- D. WPA mandates CKIP with AES optimal, WPA2 mandates AES

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 130

What two methods of authentication are available for Local EAP?

- A. LDAP and RADIUS
- B. Local and RADIUS
- C. Local Only
- D. LDAP and Local

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 131

What three components must be the same on a controller and the RADIUS server when adding a RADIUS server to a WLC? (Choose three.)

- A. Username
- B. Shared Secret
- C. Index Priority
- D. Port Number
- E. IP Address
- F. Network Mask



Correct Answer: BDE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 132

An engineer wants to setup WPA2 Enterprise using EAP-TLS and a remote RADIUS server. What device(s) would the engineer specify the EAP type on?

- A. the supplicant and authentication server
- B. the supplicant and authenticator
- C. the authenticator and authentication server
- D. the supplicant only
- E. the authentication server only

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 133

What three characteristics are components of mobility anchoring? (Choose three.)

- A. enabled as a global setting
- B. enabled on a per WLAN basis
- C. restricts clients to a specific subnet
- D. client traffic is tunneled to predefined WLC(s)
- E. only one mobility anchor is allowed per WLAN
- F. acts as master controller for a mobility group

Correct Answer: BCD

Section: (none)

Explanation

Explanation/Reference:



QUESTION 134

Mobility Anchors

WLAN SSID	Cisco	
Switch IP Address (Anchor)	Data Path	Control Path
<div>Mobility Anchor Create</div>		
Switch IP Address (Anchor)	<div>✓ local</div>	

Refer to the exhibit. An engineer wants to setup a mobility anchor for the Guest WLAN, but does not see the Anchor IP address listed in the drop-down. What is the most likely cause of this problem?

- A. The mobility anchor is currently unreachable.
- B. The mobility anchor must also be included in the mobility group of the WLC.
- C. Layer 3 Security must be configured for Web Policy Authentication.
- D. The mobility anchor is attached to another WLAN.
- E. Layer 3 Security must be configured for Web Policy Passthrough.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 135

What are three characteristics of WCS? (Choose three.)

- A. based on a single server licensing system
- B. used for wireless planning
- C. used for real-time tracking of multiple clients

- D. used for wireless management
- E. used for RF fingerprinting
- F. based on a per server licensing system

Correct Answer: ABD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 136

In what WCS menu would an engineer locate the WCS software version?

- A. Administration > Settings
- B. Help > About Cisco WCS
- C. Help > Online Help
- D. Administration > License Center

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 137

What three configuration options can be executed by navigating to the WCS Administration > AAA menu? (Choose three.)

- A. Add a Lobby Ambassador guest
- B. Add a LDAP server
- C. Add an administrative user
- D. Add a MAC address list filter
- E. Add a RADIUS server
- F. Add a TACAS+ server

Correct Answer: CEF

Section: (none)

Explanation**Explanation/Reference:****QUESTION 138**

An engineer is adding a controller to a WCS. What three categories of parameters are needed? (Choose three.)

- A. IP parameters
- B. SNMP Parameters
- C. Mobility Parameters
- D. Telnet/SSH Parameters
- E. TFTP Parameters
- F. RADIUS Parameters

Correct Answer: ABD

Section: (none)

Explanation**Explanation/Reference:****QUESTION 139**

An engineer recently removed a WLC from a WCS, but the APs associated to the WLC are still showing on the WCS. What is a reason for this?

- A. The associated APs must be removed manually.
- B. The APs must be removed from the WCS map.
- C. The hold-down timer must expire before the APs will be removed.
- D. The APs must be audited.

Correct Answer: A

Section: (none)

Explanation**Explanation/Reference:****QUESTION 140**

What two AP configurations will show RF prediction on maps in WCS? (Choose two.)

- A. Lightweight APs with internal antennas
- B. Lightweight APs with external Cisco antennas
- C. Lightweight APs with external 3rd Party antennas
- D. Autonomous APs with internal antennas
- E. Autonomous APs with external Cisco antennas
- F. Autonomous APs with external 3rd Party antennas

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 141

What tool can be used to increase accuracy of WCS heat maps?

- A. Map Editor
- B. Planning Tool
- C. CleanAir
- D. Cisco Spectrum Expert

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 142

Top 5 APs

AP Name	Map Location	a/n Clients	b/g/n Clients	Total
1252-1	Campus1 > Building1 > Floor1	2	0	2
1252-2	Campus1 > Building1 > Floor1	0	0	0
1250-3	Unassigned	0	0	0
1250-4	Unassigned	0	0	0

Refer to the exhibit. In WCS, what Monitor submenu would provide the table shown?

- A. Clients
- B. Access Points
- C. Controllers
- D. Security
- E. Alarms

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 143

An engineer is troubleshooting why wireless clients have not been able to connect to the network. Where would an engineer verify the total number of excluded clients in the last day?

- A. Security > Miscellaneous

- B. Security > Rogues
- C. Alarms
- D. Events
- E. Clients > Troubleshoot
- F. Access Points

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 144

What WCS report displays hardware type, software distribution, and CDP information?

- A. Device > AP Profile Status
- B. Device > AP Summary
- C. Network Summary > Executive Summary
- D. Device > Inventory
- E. Network Summary > 802.11n Summary



Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 145

An engineer has been noticing the power settings on several of the office APs change from day to day ever since two more APs were installed. After logging into the WLC, the engineer verifies that the power levels on 4 of the 802.11n radios are fluctuating up and down. What is the reason for this?

- A. The controller has the APs in H-REAP mode and are on a Layer 2 connection instead of Layer 3.
- B. The RRM has revealed a bad survey and is attempting to power down some of the radios to make up for it.
- C. The WLC has created temporary coverage holes while stepping through power levels for some of the APs.
- D. Several APs have high levels of overlapping coverage in the same area and the WLC is using RRM to correct the cell sizes AP coverage.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 146

An engineer is using WCS' client troubleshooting tool to investigate issues with a client device. What is the longest log capture they will be able to take?

- A. 2 minutes
- B. 5 minutes
- C. 10 minutes
- D. 30 minutes

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



QUESTION 147

A network engineer is upgrading the WLC image through the GUI for maintenance. What three transfer methods are available? (Choose three.)

- A. FTP
- B. SNMP
- C. TFTP
- D. SFTP
- E. HTTP
- F. SMB
- G. HTTPS
- H. SCP

Correct Answer: ACD

Section: (none)

Explanation

Explanation/Reference:**QUESTION 148**

On the Cisco Wireless LAN Controller GUI, what sub-menu option under the Command menu will transfer code and configuration files to the controller?

- A. Download File
- B. Upload File
- C. Download Configuration
- D. Upload Configuration

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:**QUESTION 149**

What two access methods are enabled by default on a Cisco WLC? (Choose two.)

- A. HTTP
- B. HTTPS
- C. Telnet
- D. SSH
- E. VPN
- F. SFTP

Correct Answer: BD

Section: (none)

Explanation


Explanation/Reference:**QUESTION 150**

Drag and Drop Questions

Select and Place:

Drag the 802.11 functional responsibility in the Cisco "Split MAC" design from the left and drop it on a platform on the right:

	Access Point	Controller
802.11 association and re-association		
beacons		
client authentication		
encryption / decryption		
RF management		
transmission and buffering of frames		

 **VCEplus**
VCE To PDF - Free Practice Exam

Correct Answer:

Drag the 802.11 functional responsibility in the Cisco "Split MAC" design from the left and drop it on a platform on the right:

	Access Point	Controller
	beacons	802.11 association and re-association
	encryption / decryption	client authentication
	transmission and buffering of frames	RF management

Section: (none)

Explanation

Explanation/Reference:

QUESTION 151

Drag and Drop Questions

Select and Place:

Drag the feature descriptions from the left and drop them onto the corresponding AP operational mode names on the right.

Layer 2 forwarding for remote analysis	local mode
wIPS, MSE	monitor mode
AWPP, local bridging	rogue detector mode
Layer 1 forwarding for remote analysis	bridge mode
VLAN trunk access, wired IDS	H-REAP mode
local bridging, wIPS, OEAP, VLAN trunk access	SE-Connect mode
site survey, wIPS, MSE	sniffer mode

Correct Answer:

Drag the feature descriptions from the left and drop them onto the corresponding AP operational mode names on the right.

	site survey, wIPS, MSE
	wIPS, MSE
	VLAN trunk access, wired IDS
	AWPP, local bridging
	local bridging, wIPS, OEAP, VLAN trunk access
	Layer 1 forwarding for remote analysis
	Layer 2 forwarding for remote analysis

Section: (none)

Explanation

Explanation/Reference:

QUESTION 152

Drag and Drop Questions

Select and Place:

When working with alarms in Cisco WCS version 7.0, several actions can be performed on respective alarms. Common actions include "Assign to me," "Unassign," or "Email Notification." However, three other action types provide similar, but important differences. Drag the alarm action names from the left and drop them on the correct corresponding definitions on the right.

Acknowledge

Remove from Alarm Summary.
Allow alarm to show again.
Remove alarm from database

Delete

Remove from Alarm Summary.
Allow alarm to show again.
Keep alarm in database for up to 30 days.

Clear

Remove from Alarm Summary.
Prevent alarm from showing again.
Keep alarm in database.

Correct Answer:

When working with alarms in Cisco WCS version 7.0, several actions can be performed on respective alarms. Common actions include "Assign to me," "Unassign," or "Email Notification." However, three other action types provide similar, but important differences. Drag the alarm action names from the left and drop them on the correct corresponding definitions on the right.

	Delete
	Clear
	Acknowledge

Section: (none)

Explanation

Explanation/Reference:

QUESTION 153

Drag and Drop Questions

Select and Place:

Drag the Cisco WCS report from the left and drop it on the category it reports on to the right.

Executive Summary	CleanAir
Configuration Audit	Devices
Inventory	Compliance
Security Risk Interferers	Network Summary

Correct Answer:

Drag the Cisco WCS report from the left and drop it on the category it reports on to the right.

	Security Risk Interferers
	Inventory
	Configuration Audit
	Executive Summary

Section: (none)

Explanation

Explanation/Reference:

QUESTION 154

Drag and Drop Questions

Select and Place:

Drag the Cisco WCS report from the left and drop it on the category it reports on to the right.

Worst Interferers	Performance
Network Utilization	CleanAir
PCI DSS Summary	Network Summary
802.11n Summary	Compliance

Correct Answer:

Drag the Cisco WCS report from the left and drop it on the category it reports on to the right.

	Network Utilization
	Worst Interferers
	802.11n Summary
	PCIDSS Summary

Section: (none)

Explanation

Explanation/Reference:

QUESTION 155

Drag and Drop Questions

Select and Place:

Drag the description from the left and drop it on the name of the wireless LAN controller interface that it describes on the right.

Always available. Controls intercontroller communications.	AP manager interface
Not always required for configuration. IP source address of CAPWAP tunnels.	management interface
Always available. Used for DHCP relay.	virtual
Not always required for configuration. Require static routes.	dynamic interface
Not always required for configuration. Known as the VLAN interface.	service interface

Correct Answer:

Drag the description from the left and drop it on the name of the wireless LAN controller interface that it describes on the right.

	Not always required for configuratoin. IP source address of CAPWAP tunnels.
	Always available. Controls intercontroller communications.
	Always available. Used for DHCP relay.
	Not always required for configuration. Known as the VLAN interface.
	Not always required for configuration. Require static routes.

Section: (none)
Explanation

Explanation/Reference:

QUESTION 156

Drag and Drop Questions

Select and Place:

Drag the authentication types from the left and drop them on the correct descriptions on the right.

EAP-FAST		Not used much anymore.
EAP-MD5		Requires a certificate on the server but not on the client.
EAP-TLS		Requires a client-side certificate.
LEAP		Strong password policies recommended.
PEAP		Uses a Protected Access Credential.

Correct Answer:

Drag the authentication types from the left and drop them on the correct descriptions on the right.

		EAP-MD5
		PEAP
		EAP-TLS
		LEAP
		EAP-FAST

Section: (none)

Explanation

Explanation/Reference:

QUESTION 157

Drag and Drop Questions

Select and Place:

Drag from the left the characteristics that are associated with the specific controller-based AP deployment mode and drop them in the appropriate category on the right.

can be used for site surveys	AP Sniffer Mode
no client connectivity	Target
seeks rouge APs and clients	Target
requires external server to capture data	AP Monitor Mode
works with third-party products	Target
data services	Target
	AP Local Mode
	Target
	Target

Correct Answer:

Drag from the left the characteristics that are associated with the specific controller-based AP deployment mode and drop them in the appropriate category on the right.

	AP Sniffer Mode	AP Monitor Mode	AP Local Mode
	requires external server to capture data		
	works with third-party products		
		no client connectivity	
		seeks rouge APs and clients	
			can be used for site surveys
			data services

Section: (none)

Explanation

Explanation/Reference:

QUESTION 158

Drag and Drop Questions

Select and Place:

Drag the correct visual description from left to the matching Windows 7 wireless client description on the right.

three boxes with gold shield

three boxes without gold shield

three boxes with gold star

three boxes without gold star

five bars with shield

five bars without shield

five bars with gold star

five bars without gold star

Open BSS

Secure BSS

Open IBSS

Secure IBSS

Correct Answer:

Drag the correct visual description from left to the matching Windows 7 wireless client description on the right.

	five bars with shield
	five bars without shield
three boxes with gold star	three boxes with gold shield
three boxes without gold star	three boxes without gold shield
five bars with gold star	
five bars without gold star	

Section: (none)

Explanation

Explanation/Reference:

QUESTION 159

Drag and Drop Questions

Select and Place:

Cisco WLCs running version 7.0 can be enabled for CleanAir functionality by using an AQI rating from 1 to 100. Event-driven RRM can take immediate action on AQI levels based on three sensitivity thresholds (Low, Medium, High), which are configurable in the web-based GUI. The network administrator must understand what AQI value is set using these sensitivity thresholds in version 7.0. Drag the AQI values on the left and drop them on the threshold name they belong to on the right.

20	Low
35	Medium
40	High
45	
50	
60	
70	

Correct Answer:

Cisco WLCs running version 7.0 can be enabled for CleanAir functionality by using an AQI rating from 1 to 100. Event-driven RRM can take immediate action on AQI levels based on three sensitivity thresholds (Low, Medium, High), which are configurable in the web-based GUI. The network administrator must understand what AQI value is set using these sensitivity thresholds in version 7.0. Drag the AQI values on the left and drop them on the threshold name they belong to on the right.

20	35
	50
40	60
45	
70	

Section: (none)

Explanation

Explanation/Reference:

QUESTION 160

Drag and Drop Questions

Select and Place:

Drag the features that are associated with Cisco Compatible Extensions Lite from the left and drop them in the appropriate category on the right.

Features	Categories
Wi-Fi Multimedia	Foundation
link test	Target
management frame protection	Target
expedited bandwidth request	Target
PEAP-GTC	Voice
WPA2	Target
	Target
	Management
	Target

Correct Answer:

Drag the features that are associated with Cisco Compatible Extensions Lite from the left and drop them in the appropriate category on the right.

	Foundation
	management frame protection
	PEAP-GTC
	WPA2
	Voice
	Wi-Fi Multimedia
	expedited bandwidth request
	Management
	link test

Section: (none)

Explanation

Explanation/Reference:

QUESTION 161

Drag and Drop Questions

Select and Place:

Drag the appropriate EAP descriptions on the left and drop them in the correct sequence of events for PEAP or the right.

Client sends fictitious identity.	Event 1
Client sends its certificate.	Event 2
Client sends its real identity.	Event 3
RADIUS server sends a fictitious username.	
RADIUS server sends its certificate.	
RADIUS server sends a real username.	

Correct Answer:

Drag the appropriate EAP descriptions on the left and drop them in the correct sequence of events for PEAP or the right.

	Client sends fictitious identity.
Client sends its certificate.	RADIUS server sends its certificate.
	Client sends its real identity.
RADIUS server sends a fictitious username.	
RADIUS server sends a real username.	

Section: (none)

Explanation

Explanation/Reference:

QUESTION 162

Drag and Drop Questions

Select and Place:

Drag the commands on the left that are enabled during a SSH or Telnet session with a lightweight AP and drop them on the right.

config terminal	Target
debug	Target
show	Target
enable	
clear	
delete	
reload	
upgrade	

Correct Answer:

Drag the commands on the left that are enabled during a SSH or Telnet session with a lightweight AP and drop them on the right.

config terminal	debug
	show
	enable
clear	
delete	
reload	
upgrade	

Section: (none)

Explanation

Explanation/Reference:

QUESTION 163

Drag and Drop Questions

Select and Place:

Drag the features on the left that use the "split MAC" model and drop them on the appropriate device on the right.

Features	Controller	AP
802.11 frame translation and bridging	Target	Target
mobility management	Target	Target
encryption downstream	Target	Target
providing real-time signal-quality information	Target	Target
QoS policies		Target
decryption upstream		Target

Correct Answer:

Drag the features on the left that use the "split MAC" model and drop them on the appropriate device on the right.

	Controller	AP
	802.11 frame translation and bridging	
	mobility management	
	QoS policies	
		encryption downstream
		providing real-time signal-quality information
		decryption upstream

Section: (none)

Explanation

Explanation/Reference:

QUESTION 164

Drag and Drop Questions

Select and Place:

Refer to the exhibit. Drag the steps for Open Authentication from the left and drop them in the correct order on the right.

Client sends probe request.	Target
Either Access Point A or Access Point B sends probe response. Client evaluates access point response. Selects best access point.	Target
Client sends association request to selected Access Point A.	Target
Client sends authentication request to selected access point A.	Target
Access point confirms authentication and registers client.	Target
Access point A confirms association and registers client.	Target

Correct Answer:

Refer to the exhibit. Drag the steps for Open Authentication from the left and drop them in the correct order on the right.

	Client sends probe request.
	Either Access Point A or Access Point B sends probe response. Client evaluates access point response. Selects best access point.
	Client sends association request to selected Access Point A
	Access point confirms authentication and registers client.
	Client sends authentication request to selected access point A.
	Access point A confirms association and registers client.

Section: (none)

Explanation

Explanation/Reference:

QUESTION 165

Drag and Drop Questions

Select and Place:

Drag the characteristics on the left that are associated with the specific controller-based AP deployment mode and drop them in the appropriate category on the right.

available on Cisco 3500 Series APs	AP SE-Connect Mode
A minimum of a 500-byte MTU is supported between the AP and the controller.	Target
allows APs to act as a network-connected sensor	Target
may operate in connected or standalone modes	AP Bridging Mode
mode used to set up a mesh network, either indoor or outdoor	Target
APs can switch client data traffic locally and perform client authentication locally when their connection to a centralized controller is lost.	H-REAP
	Target
	Target
	Target

Correct Answer:

Drag the characteristics on the left that are associated with the specific controller-based AP deployment mode and drop them in the appropriate category on the right.

Empty boxes for dragging characteristics.

AP SE-Connect Mode

available on Cisco 3500 Series APs

allows APs to act as a network-connected sensor

AP Bridging Mode

mode used to set up a mesh network, either indoor or outdoor

H-REAP

A minimum of a 500-byte MTU is supported between the AP and the controller.

may operate in connected or standalone modes

APs can switch client data traffic locally and perform client authentication locally when their connection to a centralized controller is lost.

Section: (none)

Explanation

Explanation/Reference:

QUESTION 166

Drag and Drop Questions

Select and Place:

Refer to the exhibit. Drag the MAC addresses on the left that will allow the wireless station Host A to send a frame through a controller based AP to the wired station Host B and drop them in the correct order on the right. Not all options are used.

controller	Target
Host A	Target
AP	Target
Empty	Target
Host B	

Correct Answer:

Refer to the exhibit. Drag the MAC addresses on the left that will allow the wireless station Host A to send a frame through a controller based AP to the wired station Host B and drop them in the correct order on the right. Not all options are used.

controller	AP
	Host A
	Host B
	Empty

Section: (none)

Explanation

Explanation/Reference:

QUESTION 167

Drag and Drop Questions

Drag each description on the left to the appropriate term on the right.

PEAP

Need Certificate on both Server and Client

LEAP

Need Certificate on Authentication Server only

EAP-MD5

Out of date

EAP-TLS

Need strong password

EAP-FAST

Need client credential

Select and Place:

Drag each description on the left to the appropriate term on the right.

PEAP

Need Certificate on both Server and Client

LEAP

Need Certificate on Authentication Server only

EAP-MD5

Out of date

EAP-TLS

Need strong password

EAP-FAST

Need client credential

Correct Answer:

Drag each description on the left to the appropriate term on the right.

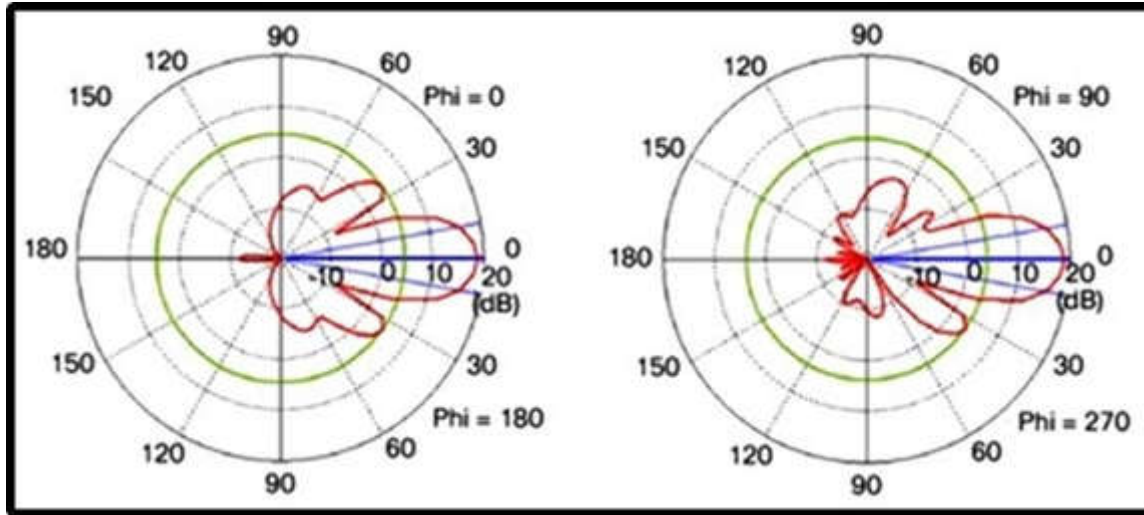
	EAP-TLS	Client
	PEAP	Server only
	LEAP	
	EAP-MD5	
	EAP-FAST	

Section: (none)
Explanation

Explanation/Reference:

QUESTION 168

Refer to the exhibit. Which antenna would produce the given radiation pattern?



- A. patch
- B. Yagi
- C. parabolic dish
- D. dipole
- E. omni-directional

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 169

An engineer has been asked to disable all OFDM rates in the wireless environment. What three rates should be disabled to fulfill this requirement? (Choose three.)

- A. 2
- B. 5.5
- C. 6
- D. 9
- E. 11

- F. 12
- G. 18

Correct Answer: ABE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 170

A customer wants to deploy Cisco Cloud Wireless architecture with 802.11ac capabilities. Which access points would meet the customers' requirements? (Choose two.)

- A. Cisco 3700 Access Points
- B. Cisco MR34 Access Points
- C. Cisco MR18 Access Points
- D. Cisco 3600 Access Points
- E. Cisco MR72 Access Points
- F. Cisco 1570 Access Points
- G. Cisco MR26 Access Points



Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 171

A customer is deploying the Cisco 5508 Wireless Controller in a unified wireless solution. Which command must be configured on the neighboring switch port if the management interface on the WLC is configured to send untagged traffic to ensure that management traffic utilizes VLAN 10?

- A. switchport trunk native vlan 10
- B. spanning-tree portfast
- C. switchport trunk allowed vlan 10
- D. channel-group 10

Correct Answer: A

Section: (none)

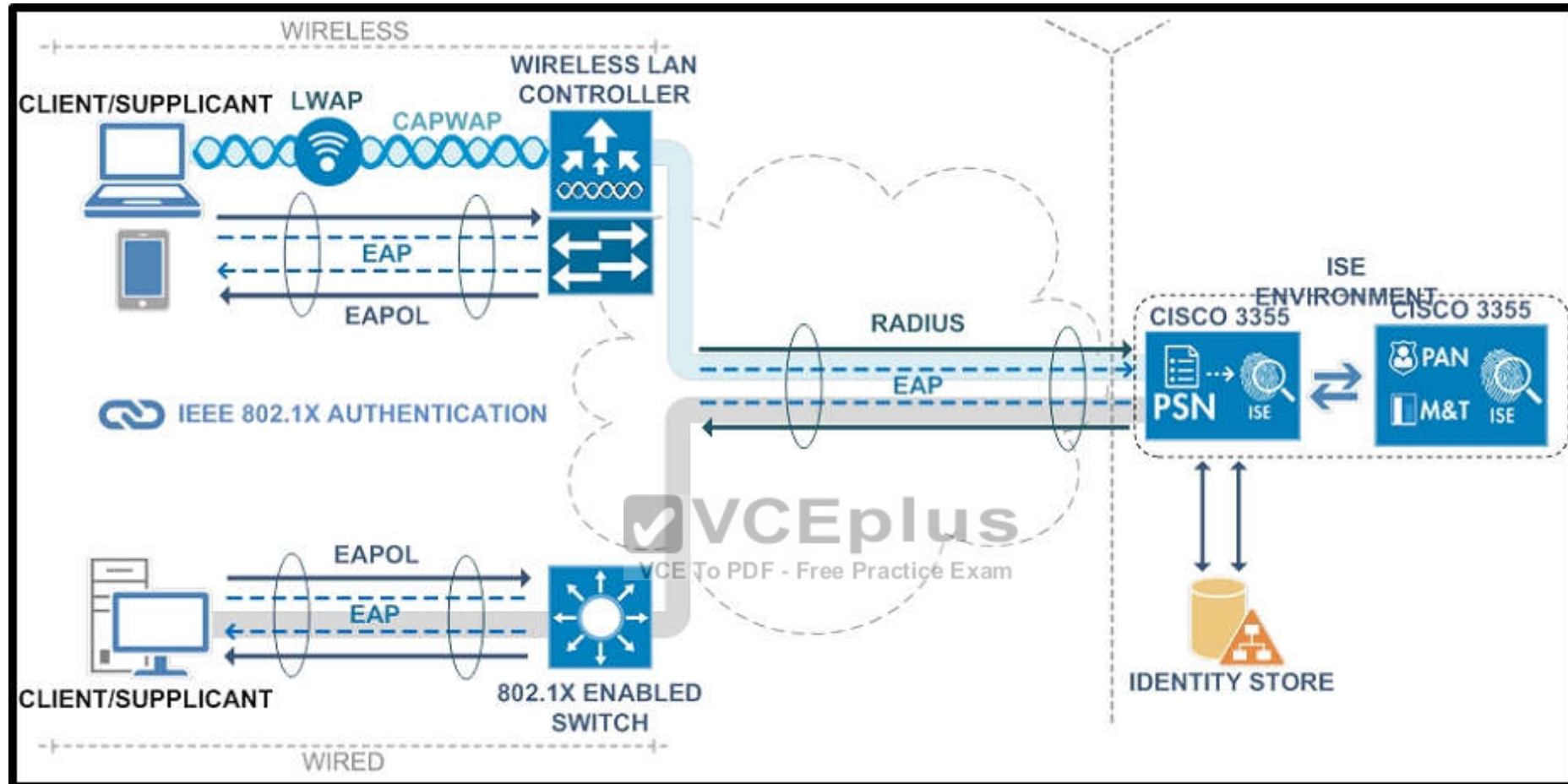
Explanation

Explanation/Reference:

QUESTION 172

Refer to the exhibit. A customer has enabled the primary DNS server to return the correct controller IP address in response to a CISCO-CAPWAP-CONTROLLER.localdomain request coming from new access points associating to the wireless network. The access points seem to still be receiving the wrong IP address and cannot associate to the primary controller. Why are the access points receiving the wrong IP information?





- A. The DHCP option 43 has an incorrect controller IP address configured.
- B. The DNS server must be configured to respond to CISCO-LWAPP-CONTROLLER.localdomain request.
- C. The controller and wireless action point need to be Layer 2 adjacent.
- D. The controller must be configured for DHCP option 15 request.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

