200-355 Q&As

Implementing Cisco Wireless Network Fundamentals

Pass Cisco 200-355 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/200-355.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

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

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_qas09186a00802030dc.html

QUESTION 2

Which three operations does the lightweight access point manage in a split-MAC design? (Choose three.)

A. association and re-association

B. frame exchange and client handshake

C. RF and mobility management

D. beacons and probe responses

E. MAC layer data encryption and decryption

F. authentication and key management

Correct Answer: BDE

QUESTION 3

Refer to the exhibit.

Which option must be chosen if only the WPA is needed?

A. WPA+WPA2

B. Static-WEP + 802.1X

C. 802.1X

D. CKIP

Correct Answer: A

Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks.
http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

QUESTION 4

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

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 5

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

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 6

You must resolve an issue in which an access point is not joining a controller. Which command can help you to troubleshoot the issue?

A. debug enable ap-name from the AP

B. debug capwap events enable from the AP

C. debug enable ap-name from the controller

D. debug capwap events enable from the controller

Correct Answer: D

QUESTION 7

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 ISE 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

QUESTION 8

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

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 9

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

QUESTION 10

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

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 11

Instructions:

THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION

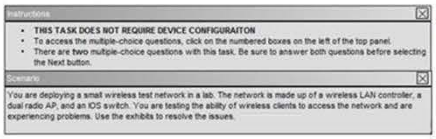
To access the multiple-choice questions, click on the numbered boxes on the left of the top panel.

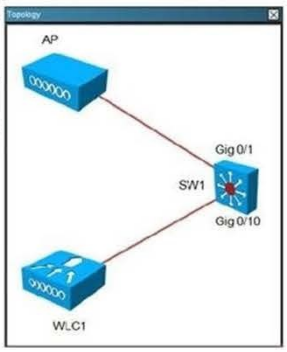
There is two multiple-choice question with this task. Be sure to answer the question before selecting the Next button

Scenario:

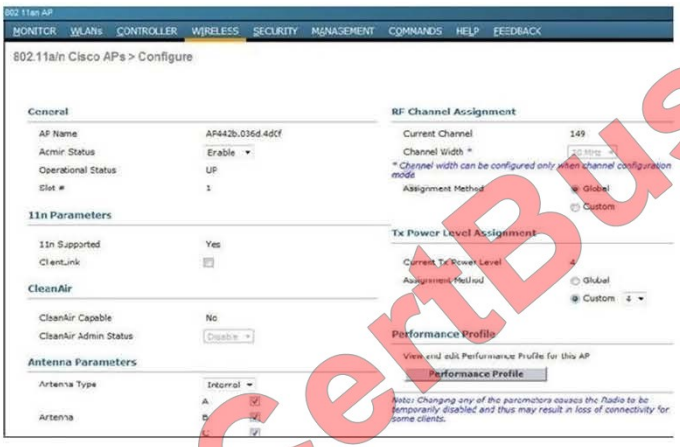
You are deploying a small wireless test network in a lab. The network is made up of a wireless LAN controller, a dual radio AP, and an iOS switch. You are testing the ability of wireless clients to access the network and are experiencing

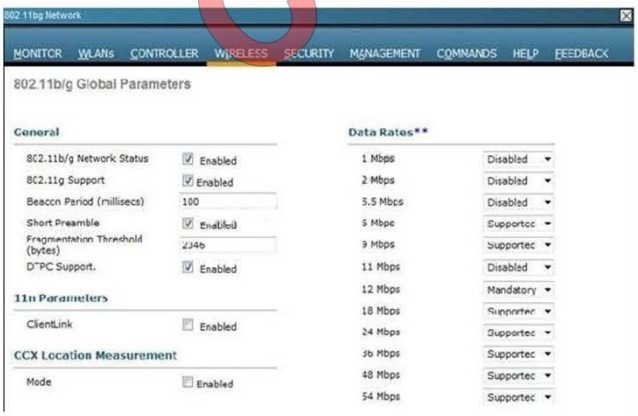
problems. Use the exhibits to resolve the issue.

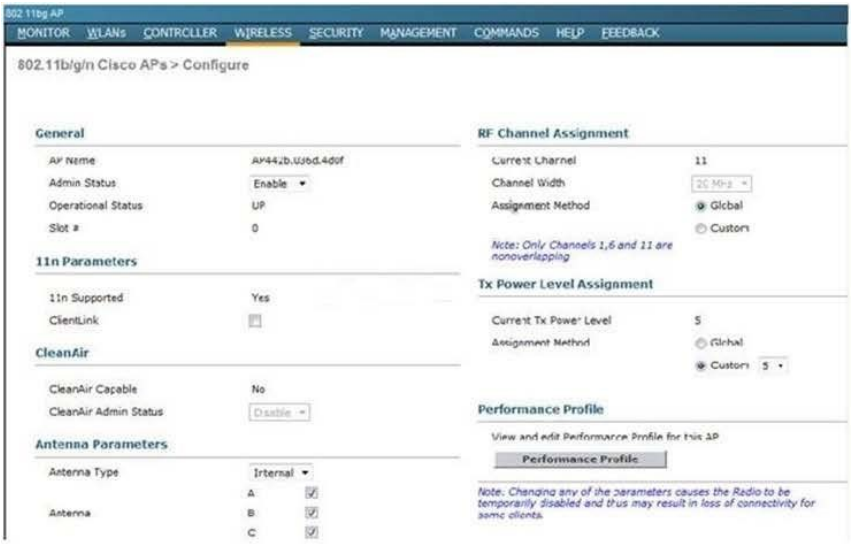

Instructions
THIS TASK DOES NOT REQUIRE DEVICE CONFIGURAITON
To access the multiple-choice questions, click on the numbered boxes on the left of the top panel.
There are two multiple-choice questions with this task. Be sure to answer both questions before selecting the Next button.
Scenario
You are deploying a small wireless test network in a lab. The network is made up of a wireless LAN controller, a dual radio AP, and an IOS switch. You are testing the ability of wireless clients to access the network and are experiencing problems. Use the exhibits to resolve the issues.


Topology
AP
Gig 0/1
SW1
Gig 0/10
WLC1

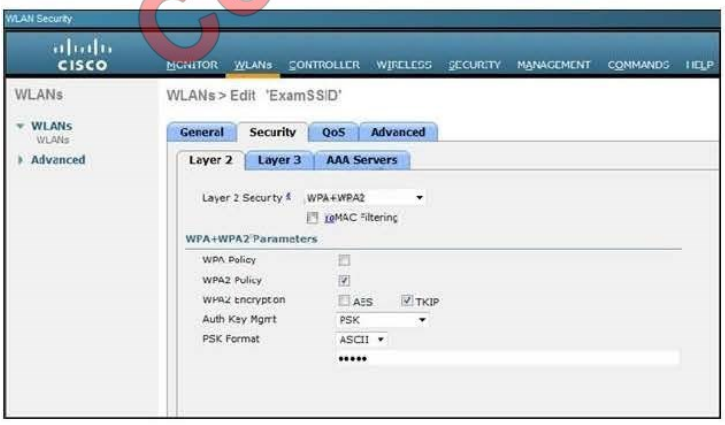

802.11an Network
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
802.11a Global Parameters
General
802.11a Network Status Enabled
Beacon Period (millisecs) 100
Fragmentation Threshold (bytes) 2346
DTPC Support. Enabled
802.11a Band Status
Low Band Enabled
Mid Band Enabled
High Band Enabled
11n Parameters
ClientLink Enabled
Data Rates**
6 Mbps Mandatory
9 Mbps Supported
12 Mbps Mandatory
18 Mbps Supported
24 Mbps Mandatory
36 Mbps Supported
48 Mbps Supported
54 Mbps Supported
CCX Location Measurement
Mode Enabled

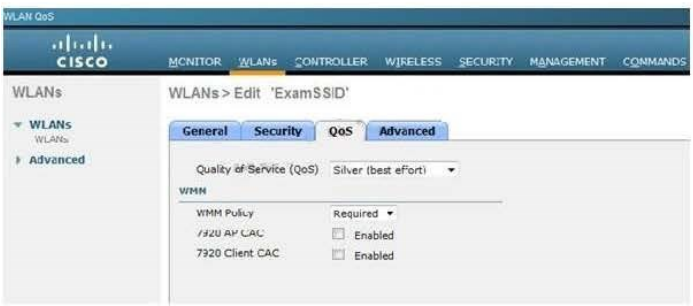

802.11an AP
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
802.11a/n Cisco APs > Configure
General
AP Name AP442b.036d.4dcf
Admin Status Enable
Operational Status UP
Slot # 1
11n Parameters
11n Supported Yes
ClientLink
CleanAir
CleanAir Capable No
CleanAir Admin Status Disable
Antenna Parameters
Antenna Type Internal
Antenna A B C
RF Channel Assignment
Current Channel 149
Channel Width * 20 MHz
* Channel width can be configured only when channel configuration mode
Assignment Method Global Custom
Tx Power Level Assignment
Current Tx Power Level 4
Assignment Method Global Custom 4
Performance Profile
View and edit Performance Profile for this AP
Performance Profile
Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity for some clients.


802.11bg Network
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
802.11b/g Global Parameters
General
802.11b/g Network Status Enabled
802.11g Support Enabled
Beacon Period (millisecs) 100
Short Preamble Enabled
Fragmentation Threshold (bytes) 2346
DTPC Support. Enabled
11n Parameters
ClientLink Enabled
CCX Location Measurement
Mode Enabled
Data Rates**
1 Mbps Disabled
2 Mbps Disabled
5.5 Mbps Disabled
6 Mbps Supported
9 Mbps Supported
11 Mbps Disabled
12 Mbps Mandatory
18 Mbps Supported
24 Mbps Supported
36 Mbps Supported
48 Mbps Supported
54 Mbps Supported


802.11bg AP
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
802.11b/g/n Cisco APs > Configure
General
AP Name
Admin Status
Enable
Operational Status
UP
Slot #
0
11n Parameters
11n Supported
Yes
CleanAir
CleanAir Capable
No
CleanAir Admin Status
Antenna Parameters
Antenna Type
Internal
Antenna
A
B
C
RF Channel Assignment
Current Channel
11
Channel Width
Assignment Method
Global
Custom
Note: Only Channels 1,6 and 11 are nonoverlapping
Tx Power Level Assignment
Current Tx Power Level
5
Assignment Method
Global
Custom
Performance Profile
View and edit Performance Profile for this AP
Performance Profile
Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity for some clients.


WLAN General
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs > Edit 'ExamSSID'
General Security QoS Advanced
Profile Name
ExamSSID
Type
WLAN
SSID
ExamSSID
Status
Enabled
Security Policies
[WPA2][Auth(PSK)]
(Modifications done under security tab will appear after applying the changes.)
Radio Policy
802.11b/g only
Interface/Interface Group(G)
management
Multicast Vlan Feature
Enabled
Broadcast SSID
Enabled


WLAN Security
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
WLANs > Edit 'ExamSSID'
General Security QoS Advanced
Layer 2 Layer 3 AAA Servers
Layer 2 Security
WPA+WPA2
MAC Filtering
WPA+WPA2 Parameters
WPA Policy
WPA2 Policy
WPA2 Encryption
AES
TKIP
Auth Key Mgmt
PSK
PSK Format
ASCII


WLAN QoS
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS
WLANs
WLANs
WLANs
Advanced
WLANs > Edit 'ExamSSID'
General Security QoS Advanced
Quality of Service (QoS)
Silver (best effort)
WMM
WMM Policy
Required
7920 AP CAC
Enabled
7920 Client CAC
Enabled

Old 2.4-GHz wireless laptops are unable to connect. What is the most likely cause of this problem?

A. WLAN > General properties are incorrectly configured.

B. WLAN > QoS properties are incorrectly configured.

C. WLAN > Security properties are incorrectly configured.

D. WLAN > Advanced properties are incorrectly configured.

E. Wireless > AP > 802.11 b/g/n AP is incorrectly configured.

F. Wireless > AP > 802.11 b/g/n > Network is incorrectly configured.

Correct Answer: F

Clientlink is not enabled and should be in a mixed client environment. Many networks still support a mix of 802.11a/g and 802.11n clients. Because 802.11a/g clients (legacy clients) operate at lower data rates, the older clients can reduce the capacity of the entire network. Cisco\\'s ClientLink technology can help solve problems related to adoption of 802.11n in mixed-client networks by ensuring that 802.11a/g clients operate at the best possible rates, especially when they are near cell boundaries.

QUESTION 12

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

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.certbus.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: