[Feb-2016 Update Free Share 375q 200-355 Exam Questions From PassLeader (101-120)

Pass 200-355 exam with premium 200-355 exam dumps! PassLeader are offering the newest 375q 200-355 vce dumps and 200-355 pdf dumps including all the new added 200-355 exam questions, which are 100% valid for passing the 200-355 exam. PassLeader provide PDF and VCE format exam 200-355 briandumps with free version VCE player! Visit passleader.com now and download the 100% passing guarantee 375q 200-355 vce and pdf dumps to achieve 200-355 certification today! keywords: 200-355 exam,375q 200-355 exam dumps,375q 200-355 exam questions,200-355 pdf dumps,200-355 practice test,200-355 vce dumps,200-355 study guide,200-355 braindumps,Implementing Cisco Wireless Network Fundamentals Exam

QUESTION 101   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. Answer: CD   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 102   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. Answer: A   QUESTION 103   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. Answer: A   QUESTION 104   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   Answer: A   QUESTION 105   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.   Answer: AE   QUESTION 106   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 Answer: BE Explanation: http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/71113-rrm-new.html QUESTION 107 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 Answer: A   Explanation: http://www.cisco.com/web/partners/downloads/765/ccx/Comp_Ext_Cust_Preso.pdf QUESTION 108 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 Answer: AD   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 109 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 Answer: D   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 110 What unit of measurement is used to represent the strength of an antenna's radiation pattern? A.   dBi   B.   dBm C.   mW   D.   GHz Answer: A

 http://www.passleader.com/200-355.html QUESTION 111 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 Answer: ABEF   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

112   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. Answer: B   Explanation:
http://www.cisco.com/c/en/us/td/docs/wireless/controller/6-0/configuration/guide/Controller60CG/c60intf.html   QUESTION 113   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. Answer: B   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 114   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 Answer: D   QUESTION 115   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 Answer: B   QUESTION 116   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 Answer: AC   QUESTION 117   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. Answer: BE   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://mrncciew.com/2014/11/02/cwap-802-11-protection-mechanism/   QUESTION 118   How many dBm is 40 mW? A.   10 dBm   B.   16 dBm   C.   20 dBm   D.   22 dBm   E.   40 dBm Answer: B   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 * log10 (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 * log10 (50/1) = 10 * log10 (50) = 10 * 1.7 = 17 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: log10 (A*B) = log10(A) + log10(B)   If you use the formula above, you can calculate the power of 50 mW in dBs in this way: Power (in dB) = 10 * log10 (50) = 10 * log10 (5 * 10) = (10 * log10 (5)) + (10 * log10(10)) = 7 + 10 = 17 dBm   http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/23231-powervalues-23231.html
QUESTION 119   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 Answer: D   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)   dBi = dBd + 2.15   dBd = dBi - 2.15 QUESTION 120   Which calculation computes the EIRP of an antenna? A.   EIRP = Tx power (dBm) + Antenna Gain (dBi) - Cable Loss (dB)   B.   EIRP= Cable Loss (dB)+ Antenna Gain (dBi) - Tx power (dBm)   C.   EIRP = Cable Loss (dB)+ Antenna Gain (dBi) / Tx power (dBm)   D.   EIRP = Tx power (dBm) + Antenna Gain (dBi) / Cable Loss (dB)   E.   EIRP = Antenna Gain (dBi) - Cable Loss (dB) * Tx power (dBm)   F.   EIRP = Tx power (dBm) * Antenna Gain (dBi) / Cable Loss (dB) Answer: A   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: Power (in dB) = 10 * log10 (Signal/Reference)   This list defines the terms in the formula: log10 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: <Transmit Power> -Cable Loss + Antenna Gain = EIRP
https://supportforums.cisco.com/document/49506/snr-rssi-eirp-and-free-space-path-loss