

## [Sep-2019Valid 200-355 VCE and 200-355 PDF Free Download in Braindump2go(New Questions)

Sep/2019 Braindump2go 200-355 Exam Dumps with PDF and VCE New Updated Today! Following are some new 200-355 Real Exam Questions!1.|2019 Latest Braindump2go 200-355 Exam Dumps (VCE & PDF) Instant

Download:<https://www.braindump2go.com/200-355.html>2.|2019 Latest Braindump2go 200-355 Exam Questions & Answers Instant Download:<https://drive.google.com/drive/folders/0B75b5xYLjSSNRmRpZmZRdkotbUk?usp=sharing>New QuestionsWhat authentication method requires a certificate on both the client and authentication server?A. PEAPB. EAP-TLSC. EAP-FASTD.

WPA-PSKE. WEPF. EAP-TTLSEAnswer: BNew QuestionsAn enterprise needs their iPhones to connect to the EAP-TLS network. How should the devices be configured?A. push profile and certificate through Configuration UtilityB. configure directly through Settings applicationC. email certificate to device then configure through Settings applicationD. download certificate from web page then configure through Settings applicationE. push profile and certificate through iTunesAnswer: ANew QuestionsWhat AnyConnect module can be used to provide a detailed scan list of the Wi-Fi environment?A. DARTB. Telemetry C. Web SecurityD. NAME. PostureAnswer: ANew QuestionsWhat two capabilities would be present on a wireless client device that supports CCXv3? (Choose two.)A. WPA2B. 802.1xC. PEAP-MSCHAPD. NACE. MFPF. EAP-TLSEAnswer: AB

New QuestionsTo mitigate DoS attacks on a network, what security method should be implemented?A. WEPB. 802.1xC. Non-broadcast SSIDD. Client MFPAnswer: DNew QuestionsWhat protocol overcomes the weaknesses of LEAP?A. EAP-TLS B. PEAPC. EAP-FASTD. EAP-TTLSEAnswer: CNew QuestionsWhat encryption standards describe WPA and WPA2?A. WPA mandates AES with TKIP optional, WPA2 mandates TKIPB. WPA mandates TKIP with AES optional, WPA2 mandates AESC. WPA mandates CKIP, WPA2 mandates AESD. WPA mandates CKIP with AES optimal, WPA2 mandates AESAnswer: B

New QuestionsWhat two methods of authentication are available for Local EAP?A. LDAP and RADIUSB. Local and RADIUSC. Local OnlyD. LDAP and LocalAnswer: DNew QuestionsWhat three components must be the same on a controller and the RADIUS server when adding a RADIUS server to a WLC? (Choose three.)A. UsernameB. Shared SecretC. Index PriorityD. Port NumberE. IP AddressF. Network MaskAnswer: BDENew QuestionsAn 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 serverB. the supplicant and authenticatorC. the authenticator and authentication serverD. the supplicant onlyE. the authentication server onlyAnswer: ANew QuestionsWhat three characteristics are components of mobility anchoring? (Choose three.)A. enabled as a global settingB. enabled on a per WLAN basisC. restricts clients to a specific subnet D. client traffic is tunneled to predefined WLC(s)E. only one mobility anchor is allowed per WLANF. acts as master controller for a mobility groupAnswer: BCDNew QuestionsWhich of the following are three functions of Cisco RRM? (Choose three.)A. TPCB. intercontroller roamingC. dynamic channel assignmentD. intracontroller roamingE. coverage hole detectionAnswer: ACE

Explanation:RRM can periodically reconfigure the 802.11 RF network for best efficiency. To do this, RRM performs these functions:Radio resource monitoringTransmit power controlDynamic channel assignmentCoverage hole detection and correction[http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-0MR1/configuration/guide/wlc\\_cg70MR1/cg\\_rrm.pdf](http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-0MR1/configuration/guide/wlc_cg70MR1/cg_rrm.pdf)New QuestionsYou 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. VLANB. encryption typeC. authentication methodD. VRFE. security typeF. IP addressAnswer: BCEExplanation: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>New QuestionsWhat are three characteristics of the 802.11g standard? (Choose three.)A. speed of as much as 11 Mb/sB. speed of as much as 54 Mb/sC. backward-compatibility with 802.11aD. backward-compatibility with 802.11bE. OFDM as an additional modulation techniqueF.

OFDM and CCK as additional modulation techniquesAnswer: BDEExplanation: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

OFDM and CCK as additional modulation techniquesAnswer: BDEExplanation: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

OFDM and CCK as additional modulation techniquesAnswer: BDEExplanation: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](http://en.wikipedia.org/wiki/IEEE_802.11g-2003)New QuestionsWhich two types of encryption does Windows support for WPA2 security for wireless connections? (Choose two.)A. AESB. DESB. PGPD. TKIPB. WEPAnswer: ADExplanation: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/>New QuestionsRefer to the exhibit. Which three switch port types are valid for these connections? (Choose three.)A. accessB. port-channelC. port-channel trunkD. trunkE. port-channel accessF. routed portAnswer: ACDEExplanation:The switch must be configured for access or trunks to the WLC, and using trunks over port channel interfaces is supported.New QuestionsWhich two wireless technologies can interfere with 802.11 networks? (Choose two.)A. DECTB. ZigBeeC. WiMaxD. GSMAnswer: ABExplanation:Digital Enhanced Cordless Telecommunication (DECT), also known as cordless telephones, and Zigbee are both well-known sources of interferences within an 802.11 network.New QuestionsWhich two algorithms are available in RRM? (Choose two.)A. coverage-hole detectionB. dynamic channel assignmentC. RSSI normalizerD. transmitting channel expanderE. rogue detectionAnswer: ABExplanation: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/>New QuestionsWhich two pieces of information are needed for the wireless client to connect to the wireless network? (Choose two.)A. SSIDB. security settingsC. channel numberD. AP nameAnswer: ABExplanation: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).New QuestionsWhat are two wireless configuration utilities for Apple Mac computers? (Choose two.)A. AirPortB. AirPort ExtremeC. AirManagerD. AirManager SupremeE. AirAssistant UltimateAnswer: ABExplanation: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.New QuestionsWhat are two modules of the CCX Lite program? (Choose two.)A. foundationB. voiceC. RF powerD. roamingAnswer: ABExplanation: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:New QuestionsWhat are two security threats to wireless networks? (Choose two.)A. ad-hoc networksB. client misassociationC. port redirectionD. cross-site scriptingAnswer: ABExplanation: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](http://www.arubanetworks.com/techdocs/ArubaOS_61/ArubaOS_61_UG/New_WIP.php) **!!!RECOMMEND!!!**

1. | 2019 Latest Braindump2go 200-355 Exam Dumps (VCE & PDF) Instant

Download: <https://www.braindump2go.com/200-355.html> 2. | 2019 Latest Braindump2go 200-355 Study Guide Video Instant

Download: YouTube Video: [YouTube.com/watch?v=2oAx48AzKPo](https://www.youtube.com/watch?v=2oAx48AzKPo)