CWNP CWNA-109

CWNP Wi-Fi Admin Certification Questions & Answers

Exam Summary – Syllabus – Questions

CWNA-109

CWNP Certified Wireless Network Administrator

60 Questions Exam – 70 Cut Score – Duration of 90 minutes

Table of Contents:

Know Your CWNA-109 Certification Well:

The CWNA-109 is best suitable for candidates who want to gain knowledge in the CWNP Wireless Network. Before you start your CWNA-109 preparation you may struggle to get all the crucial Wi-Fi Admin materials like CWNA-109 syllabus, sample questions, study guide.

But don't worry the CWNA-109 PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all **your queries like**-

- What is in the CWNA-109 syllabus?
- How many questions are there in the CWNA-109 exam?
- Which Practice test would help me to pass the CWNA-109 exam at the first attempt?

Passing the CWNA-109 exam makes you CWNP Certified Wireless Network Administrator. Having the Wi-Fi Admin certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

CWNP CWNA-109 Wi-Fi Admin Certification Details:

Exam Name	Wireless Network Administrator
Exam Code	CWNA-109
Exam Price	$275 USD
Duration	90 minutes
Number of Questions	60
Passing Score	70
Recommended Training	**CWNA Certification Self Study Kit** **Live Training Wireless Network Certification Class**
Exam Registration	**PEARSON VUE**
Sample Questions	**CWNP CWNA-109 Sample Questions**
Practice Exam	**CWNP Certified Wireless Network Administrator Practice Test**

CWNA-109 Syllabus:

Section	Objectives
Radio Frequency (RF) Technologies - 15%	
Define and explain the basic characteristics and behavior of RF	- Wavelength, frequency, amplitude, phase, sine waves - RF propagation and coverage - Reflection, refraction, diffraction, and scattering - Multipath and RF interference - Gain and loss - Amplification - Attenuation - Absorption - Voltage Standing Wave Ratio (VSWR) - Return Loss - Free Space Path Loss (FSPL)
Apply the basic concepts of RF mathematics and measurement	- Watt and milliWatt - Decibel (dB) - dBm and dBi - Noise floor - SNR - RSSI - dBm to mW conversion rules of 10 and 3 - Equivalent Isotropically Radiated Power (EIRP)
Identify RF signal characteristics as they relate to antennas	- RF and physical line of sight and Fresnel zone clearance - Beamwidths - Passive gain - Polarization - Antenna diversity types - Radio chains - MIMO
Explain and apply the functionality of RF antennas, antenna systems, and accessories available	- Omni-directional antennas - Semi-directional antennas - Highly directional antennas - Reading Azimuth and Elevation charts for different antenna types - Antenna orientation - RF cables and connectors - Lightning arrestors and grounding rods/wires - Enclosures, mounting and aesthetic concerns
WLAN Regulations and Standards - 20%	
Explain the roles of WLAN and networking industry organizations	- IEEE - Wi-Fi Alliance

Section	Objectives
	- IETF - Regulatory domains and agencies
Explain and apply the various Physical Layer (PHY) solutions of the IEEE 802.11-2020 standard and amendments including supported channel widths, spatial streams, and data rates	- DSSS – 802.11 - HR-DSSS – 802.11b - OFDM – 802.11a - ERP – 802.11g - Wi-Fi 4 - HT – 802.11n - Wi-Fi 5 - VHT – 802.11ac - Wi-Fi 6 - HE - 802.11ax (2.4 and 5 GHz) - Wi-Fi 6E - HE - 802.11ax (6 GHz)
Understanding spread spectrum technologies, Modulation and Coding Schemes (MCS)	- DSSS - OFDM - OFDMA and Resource Units - BPSK - QPSK - QAM (16, 64, 256,1024)
Identify and apply 802.11 WLAN functional concepts	- Primary channels - OBSS - Adjacent overlapping and non-overlapping channels - Throughput vs. data rate - Bandwidth - Guard Interval
Describe the OSI and TCP/IP model layers affected by the 802.11-2020 standard and amendments	
Identify and comply with regulatory domain requirements and constraints	- Frequency bands used by the 802.11 PHYs - Available channels - Regulatory power constraints - Indoor, outdoor deployments and implementation variants - Dynamic Frequency Selection (DFS) - Transmit Power Control (TPC)
Explain basic use case scenarios for 802.11 wireless networks	- Wireless LAN (WLAN) – BSS and ESS - Wireless bridging - Wireless Peer to peer solutions - Wireless Mesh
WLAN Protocols and Devices - 20%	
Describe the components and functions that make up an 802.11 wireless service set	- Stations (STAs) - Basic Service Set (BSS) (Infrastructure mode) - SSID - BSSID - Extended Service Set (ESS)

Section	Objectives
	- IBSS - Distribution System (DS) - Distribution System Media (DSM)
Define terminology related to the 802.11 MAC and PHY	- MSDU, MPDU, PSDU, and PPDU - A-MSDU and A-MPDU - PHY preamble and header
Identify and explain the MAC frame format	- MAC frame format - MAC addressing
Identify and explain the purpose of the three main 802.11 frame types	- Management - Control - Data
Explain the process used to locate and connect to a WLAN	- Scanning (active and passive) - 802.11 Authentication - 802.11 Open System Authentication - 802.11 Association - BSS selection - Connecting to hidden SSIDs
Explain 802.11 channel access methods	- DCF - EDCA - RTS/CTS - CTS-to-Self - NAV - Interframe spaces (SIFS, DIFS, EIFS, AIFS) - Physical carrier sense and virtual carrier sense
Explain 802.11 MAC operations	- Roaming - Power save modes and frame buffering - Protection mechanisms
Describe features of, select, and install WLAN devices, control, and management systems	- Access Points (APs) - WLAN controllers - Wireless network management systems - Wireless bridge and mesh APs Client devices
WLAN Network Architecture and Design Concepts - 15%	
Describe and implement Power over Ethernet (PoE)	- Power Source Equipment - Powered Device - Midspan and endpoint PSEs - Power classes to include power differences between PSE and PD - Power budgets and powered port density
Define and describe differences, advantages and constraints of the different wireless LAN architectures	- Centralized data forwarding - Distributed data forwarding - Control, Management and Data planes - Scalability and availability solutions - Tunneling, QoS and VLANs

Section	Objectives
Describe basic design considerations for common deployment scenarios in wireless such as coverage requirements, roaming considerations and throughput.	- Design considerations for data, voice and video - Design considerations for specific applications such as location services, high density and guest access/BYOD - Design considerations for supporting legacy 802.11 devices
Demonstrate awareness of common proprietary features in wireless networks.	- AirTime Fairness - Band steering - Dynamic power and channel management features - Internal Wireless architecture communication
Determine and configure required network services supporting the wireless network	- DHCP for client addressing, AP addressing and/or controller discovery - DNS for address resolution for clients and APs - Time synchronization protocols (e.g. NTP, SNTP) - VLANs for segmentation - Authentication services (e.g. RADIUS, LDAP) - Access Control Lists for segmentation - Wired network capacity requirements
WLAN Network Security - 10%	
Identify weak security options that should not be used in enterprise WLANs	- WEP - 802.11 Shared Key authentication - SSID hiding as a security mechanism - MAC filtering - Use of deprecated security methods (e.g. WPA and/or WPA2 with TKIP)
Identify and configure effective security mechanisms for enterprise WLANs	- Application of AES for encryption and integrity - WPA2-Personal including limitations and best practices for pre-shared (PSK) use - WPA2-Enterprise -configuring wireless networks to use 802.1X including connecting to RADIUS servers and appropriate EAP methods
Understand basic concepts of WPA3 and Opportunistic Wireless Encryption (OWE) and enhancements over WPA2	- Understand basic security enhancements in WPA3 vs. WPA2 - Understand basic security enhancements of encryption and integrity in WPA3 - Simultaneous Authentication of Equals (SAE) in WPA3 as an enhancement for legacy pre-shared key technology - Opportunistic Wireless Encryption (OWE) for public and guest networks
Describe common security options and tools used in wireless networks	- Access control solutions - Protected management frames - Fast Secure Roaming methods

Section	Objectives
	- Wireless Intrusion Prevention System (WIPS) and/or rogue AP detection - Protocol and spectrum analyzers - Best practices in secure management protocols
RF Validation and WLAN remediation - 10%	
Verify and document that design requirements are met including coverage, throughput, roaming, and connectivity with a post-implementation validation survey.	
Locate and identify sources of RF interference	- Identify RF disruption from 802.11 wireless devices including contention vs. interference and causes/sources of both including co-channel contention (CCC), overlapping channels, and 802.11 wireless device proximity. - Identify sources of RF interference from non-802.11 wireless devices based on the investigation of airtime and frequency utilization - Understand interference mitigation options including removal of interference source or change of wireless channel usage
Perform application testing to validate WLAN performance	- Network and service availability - VoIP testing - Real-time application testing - Throughput testing
Understand and use the basic features of validation tools	- Use of throughput testers for validation tasks - Use of wireless validation software (survey software and wireless scanners) - Use of protocol analyzers for validation tasks - Use of spectrum analyzers for validation tasks
Describe and apply common troubleshooting tools used in WLANs	- Use of protocol analyzers for troubleshooting tasks - Use of spectrum analyzers for identifying sources of interference - Use of management, monitoring, and logging systems for troubleshooting task - Use of wireless LAN scanners for troubleshooting tasks
Identify and troubleshoot common wireless issues	- Identify causes of insufficient throughput in the wireless distribution system including LAN port speed/duplex misconfigurations, insufficient PoE budget, and insufficient Internet or WAN bandwidth - Identify and solve RF interference using spectrum analyzers

Section	Objectives
	- Identify wireless performance issues using SNR, retransmissions, and airtime utilization statistics - Identify causes of wireless issues related to network services including DHCP, DNS, and time protocols including using native interface and IP configuration tools - Identify wireless issues related to security configuration mismatches - Identify hidden node issues

CWNP CWNA-109 Sample Questions:

Question: 1

What wireless security solutions are defined by Wi-Fi Protected Access?

a) Passphrase authentication
b) LEAP
c) TKIP/RC4
d) Dynamic WEP

Answer: a, c

Question: 2

Semidirectional antennas are often used for which of the following purposes?

a) Providing short-distance point-to-point communications
b) Providing long-distance point-to-point communications
c) Providing unidirectional coverage from an access point to clients in an indoor environment
d) Reducing reflections and the negative effects of multipath

Answer: a, c, d

Question: 3

Which of the following are examples of mobile office networking?

a) Construction-site offices
b) Temporary disaster-assistance office
c) Remote sales office
d) Temporary classrooms

Answer: a, b, d

Question: 4

Which of the following statements are true?

a) When upfade occurs, the final received signal will be stronger than the original transmitted signal.
b) When downfade occurs, the final received signal will never be stronger than the original transmitted signal.
c) When upfade occurs, the final received signal will never be stronger than the original transmitted signal.
d) When downfade occurs, the final received signal will be stronger than the original transmitted signal.

Answer: b, c

Question: 5

In the U-NII-1 band, what is the center frequency of channel 40?

a) 5.2 GHz
b) 5.4 GHz
c) 5.8 GHz
d) 5.140 GHz

Answer: a

Question: 6

What is the maximum power used by a PD Class 0 device?

a) 3.84 W
b) 6.49 W
c) 12.95 W
d) 15.4 W

Answer: c

Question: 7

The ratio between the maximum peak voltage and minimum voltage on a line is known as what?

a) Signal flux
b) Return loss
c) VSWR
d) Signal incidents

Answer: c

Question: 8

What organization ensures interoperability of WLAN products?

a) IEEE
b) ITU-R
c) ISO
d) Wi-Fi Alliance
e) FCC

Answer: d

Question: 9

What are some of the negative effects of layer 2 retransmissions?

a) Decreased range
b) Excessive MAC sublayer overhead
c) Decreased latency
d) Increased latency
e) Jitter

Answer: b, d, e

Question: 10

Which of these encryption technologies have been cracked?

a) 64-bit WEP
b) TKIP/RC4
c) CCMP/AES
d) 128-bit WEP
e) Wired Equivalent Privacy

Answer: a, d, e

Study Guide to Crack CWNP Wi-Fi Admin CWNA-109 Exam:

- Getting details of the CWNA-109 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the CWNA-109 exam.

- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the CWNP provided training for CWNA-109 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the CWNA-109 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on CWNA-109 practice tests is must. Continuous practice will make you an expert in all syllabus areas.