Certified Wireless Design Professional (CWDP-304) Objectives

Introduction

When you pass the CWDP exam and hold a valid CWNA certification, you earn the CWDP certification and credit towards the CWNE certification should you choose to pursue it.

The Certified Wireless Design Professional (CWDP) has the knowledge and skill set required to manage the entire WLAN design life cycle: defining, designing, deploying, and diagnosing. Tasks within these stages include gathering necessary information and requirements and creating a design. These professional implements, validates, and optimizes the solution to ensure objectives are met. A CWDP contributes to, or takes responsibility for, any or all stages within this process.

The skills and knowledge measured by this examination are derived from a Job Task Analysis (JTA) involving wireless networking experts (CWNEs) and professionals. The results of this JTA were used in weighing the subject areas and ensuring that the weighting is representative of the relative importance of the content.

The following table provides the breakdown of the exam as to the distribution of questions within each knowledge domain.

Knowledge Domain	**Percentage**
Define Specifications for the WLAN	25%
Design the WLAN	40%
Deploy the WLAN	10%
Validate and Optimize the WLAN	25%

CWNP Authorized Materials Use Policy

CWNP does not condone the use of unauthorized 'training materials' such as 'brain dumps'. Individuals who utilize such materials to pass CWNP exams will have their certifications revoked. In an effort to more clearly communicate CWNP's policy on use of unauthorized study materials, CWNP directs all certification candidates to the CWNP Candidate Conduct Policy at:

http://www.cwnp.com/wp-content/uploads/pdf/CWNPCandidateConductPolicy.pdf

Please review this policy before beginning the study process for any CWNP exam. Candidates will be required to state that they understand and have abided by this policy at the time of exam delivery. If a candidate has a question as to whether study materials are considered "brain dumps", he/she should perform a search using CertGuard's engine, found here: http://www.certguard.com/search.asp

1.0 Define Specifications for the WLAN – 25%

1.1 Collect business requirements and constraints

1.1.1 Business use cases and justification
1.1.2 User requirements
1.1.3 Regulatory compliance
1.1.4 Industry compliance
1.1.5 Budget
1.1.6 Aesthetics
1.1.7 Architectural constraints
1.1.8 Mounting restrictions
1.1.9 Access restrictions
1.1.10 Time constraints
1.1.11 Building codes and safety codes

1.2 Collect and define technical requirements

1.2.1 Vendor selection
1.2.2 Location services such as RTLS
1.2.3 Latency requirements
1.2.4 Signal strength requirements
1.2.5 Capacity requirements
1.2.6 Security requirements

- BYOD and guest access
- Roaming
- Monitoring
- Authentication and encryption

1.2.7 Applications and their specific requirements
1.2.8 WLAN upgrade requirements, when applicable
1.2.9 Bridge link requirements, when applicable
1.2.10 Voice over WLAN (VoWLAN), when applicable
1.2.11 Client devices including most important and least capable device
1.2.12 Requirement areas

1.3 Collect project documentation

1.3.1 Validated floor plans
1.3.2 Network infrastructure

- Network diagrams
- AP locations

- Existing network services including DNS, DHCP, NTP, and authentication servers
- Switch capabilities and capacity

1.3.3 Cabling infrastructure

- Cabling maps and plans
- Wiring closet locations

1.3.4 Power availability and PoE capabilities
1.3.5 Existing wireless systems
1.3.6 Previous design/survey documentation

1.4 Define requirement areas including essential metrics for each requirement

1.4.1 Client device types and capabilities
1.4.2 Applications and their requirements
1.4.3 User and device density
1.4.4 SSIDs
1.4.5 Security settings
1.4.6 Understand common vertical markets

1.5 Gather information on environmental factors

1.5.1 Building materials
1.5.2 Attenuation values
1.5.3 Ceiling heights
1.5.4 Site annotations (photos, notes, plans)
1.5.5 Wireless environment scan

- Packet captures
- Spectrum captures
- Wi-Fi scanners

2.0 Design the WLAN – 40%

2.1 Define WLAN architectures and select the appropriate architecture for a design

2.1.1 Controller-based (physical and virtual) architectures
2.1.2 Distributed (cloud-based and local WNMS)
2.1.3 Standalone/Autonomous APs
2.1.4 Dynamic vs. static channel assignment
2.1.5 Dynamic radio management
2.1.6 Software defined radios
2.1.7 RF profiles
2.1.8 Select and/or recommend the appropriate equipment for the design and selected architecture (APs, antennas, controllers, managed services)

2.2 Produce a design to meet requirements

2.2.1 Select and use the appropriate design tools

- Design and survey software and hardware
- Spectrum analysis software and hardware
- Access points and antennas
- Portable power source
- Tripods
- Measuring tools
- Cameras
- Personal Protective Equipment (PPE)

2.2.2 Select and use the appropriate design methodologies

- WLAN predictive design (new builds/site or area not accessible)
- Validated RF modeling
- AP-on-a-Stick (APoS) measurements
- Bridge and mesh planning

2.2.3 Understand and use the common features of wireless design software

- Import and scale floor plans
- Model attenuation of the site (including calibration)
- Select and place APs and antennas
- Adjust AP and antenna settings
- Define requirement areas and parameters
- Define channel and power settings

2.2.4 Select and use common vendor features and make configuration recommendations

- Band steering
- Automatic/static channel selection
- Load balancing
- RF/AP templates

2.2.5 Design for different client and application types

- VoIP handsets
- Laptops
- Handheld scanners
- Smartphones and tablets
- IoT and smart devices
- Location tracking systems
- Voice and video systems

2.2.6 Ensure end-to-end QoS is properly implemented

- WMM
- Wired and wireless QoS mappings

- QoS markings, classifications, and queues

2.2.7 Define and recommend security solutions
- Monitoring (detection and prevention)
- Authentication servers
- EAP methods
- Authentication types
- Encryption types

2.2.8 Design for secure roaming
- Secure BSS transition (roaming)
- Vendor roaming solutions
- Client support issues

2.3 Create, distributed, and communicate design documentation

2.3.1 Bill of Materials (BoM)
2.3.2 Design reports
2.3.3 Physical installation guide

3.0 Deploy the WLAN – 10%

3.1 Ensure proper understanding and implementation of the design

3.1.1 Implementation meeting
- Explain design decisions to implementers
- Ensure understanding of design deployment

3.1.2 Distribute required documentation

3.2 Recommend or perform essential deployment tasks

3.2.1 Understand and perform installation procedures for different WLAN architectures (cloud-based, controller-based, WNMS, autonomous)

3.2.2 Infrastructure configuration supporting the WLAN (DHCP, DNS, NTP, switches, and routers)

3.2.3 Channel assignment, automatic radio management, and transmit power configuration

3.2.4 Installation procedures for cloud-based APs, controller-based APs, WNMS APs, and autonomous APs

3.3 Perform an installation audit for quality assurance

3.3.1 Verify proper AP and antenna location and orientation
3.3.2 Verify aesthetic requirements are met
3.3.3 Verify physical security of the installation

4.0 Validate and Optimize the WLAN – 25%

4.1 Confirm the WLAN system is operational

4.1.1 AP Status
4.1.2 Verify PoE provisioning of power requirements are met

4.2 Perform an RF validation survey

4.2.1 Ensure coverage requirements
4.2.2 Evaluate impacts of contention and interference

4.3 Perform client performance testing

4.3.1 Connectivity testing
4.3.2 Application testing
4.3.3 Roaming testing
4.3.4 Capacity testing
4.3.5 Security testing

4.4 Recommend appropriate physical adjustments

4.4.1 AP
4.4.2 Antenna and connectors

4.5 Recommend appropriate RF adjustments

4.5.1 RF channel assignment
4.5.2 RF channel bandwidth
4.5.3 RF coverage (transmit power, radio count, antennas)
4.5.4 RF interference issues

4.6 Recommend remediation for application issues

4.6.1 Connectivity issues
4.6.2 Application issues
4.6.3 Roaming issues
4.6.4 Capacity issues
4.6.5 Security issues

4.7 Implement knowledge transfer and hand-off

4.7.1 System training

4.7.2 Solution documentation and assets

- Validation documentation
- Digital or physical assets
- Guides
- Floorplans
- Configuration documents

4.7.3 Final meeting (Q&A and hand-off)

CWDP-304 Exam Acronyms

For the CWDP-304 exam, you should be able to understand clearly define the following acronyms in relation to 802.11 WLAN operations and analysis. Such acronyms may be used on the CWDP-304 exam without definition.

AAA	Authentication, Authorization, and Accounting
ACI	Adjacent Channel Interference
AD DS	Active Directory Domain Services
AES	Advanced Encryption Standard
AP	Access Point
ARM	Adaptive Radio Management
ASK	Amplitude Shift Keying
BPSK	Binary Phase Shift Keying
BSA	Basic Service Area
BSS	Infrastructure Basic Service Set
BSSID	Basic Service Set Identifier
BYOD	Bring Your Own Device
CCI	Co-Channel Interference
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Protocol
CIA	Confidentiality, Integrity, and Availability
CRC	Cyclic Redundancy Check
CTS	Clear to Send
dB	Decibel
dBi	Decibel to Isotropic
dBm	Decibel to Milliwatt
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol

DMG	Directional Multi-Gigabit
DMZ	Demilitarized Zone
DNS	Domain Name System
DRS	Dynamic Rate Switching
DS	Distribution System
DSM	Distribution System Medium
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EIRP	Equivalent Isotropically Radiated Power
ERP	Extended Rate PHY
ESS	Extended Service Set
FCC	Federal Communications Commission
FHSS	Frequency Hopping Spread Spectrum
FSK	Frequency Shift Keying
FSR	Fast Secure Roaming
FT	Fast BSS Transition
FTP	File Transfer Protocol
Gbps	Gigabits Per Second
GBps	Gigabytes Per Second
GHz	Gigahertz
GI	Guard Interval
GTK	Group Temporal Key
HE	High Efficiency
HR/DSSS	High Rate DSSS
HT	High Throughput

HTTP	Hypertext Transfer Protocol
Hz	Hertz
IBSS	Independent Basic Service Set
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IR	Intentional Radiator
ISP	Internet Service Provider
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
MAC	Medium Access Control
Mbps	Megabits Per Second
MBps	Megabytes Per Second
MBSS	Mesh Basic Service Set
MCA	Multiple Channel Architecture
MCS	Modulation and Coding Scheme
MDM	Mobile Device Management
MHz	Megahertz
MIMO	Multiple-Input/Multiple-Output
MOS	Mean Opinion Score
MSK	Master Session Key
MU-MIMO	Multi-User MIMO
mW	Milliwatt

NAC	Network Access Control
NIC	Network Interface Card
NTP	Network Time Protocol
OFDM	Orthogonal Frequency Division Multiplexing
OKC	Opportunistic Key Caching
OTA	Over-the-Air
OWE	Opportunistic Wireless Encryption
PCI-DSS	Payment Card Industry Data Security Standard
PD	Powered Device
PHY	Physical Layer
PIN	Personal identification Number
PKI	Public Key Infrastructure
PoE	Power over Ethernet
PSE	Power Source Equipment
PSK	Pre-Shared Key or Phase Shift Keying
PTK	Pairwise Transient Key
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
RADIUS	Remote Authentication Dial-In User Service
RBAC	Role-Based Access Control
RC4	Rivest Cipher 4
RF	Radio Frequency
RFC	Request for Comments
RRM	Radio Resource Management
RSNA	Robust Security Network Association

RSN	Robust Security Network
RSSI	Received Signal Strength Indicator
RTS	Request to Send
Rx	Receive or Receiver
S1G	Sub-1 GHz
SCA	Single Channel Architecture
SINR	Signal-to-Interference plus Noise Ratio
SISO	Single-Input/Single-Output
SNR	Signal-to-Noise Ratio
SOHO	Small Office Home Office
SS	Spatial Streams
SSH	Secure Shell
SSID	Service Set Identifier
STA	Station
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TVHT	TV (Television) High Throughput
Tx	Transmit or Transmitter
UDP	User Datagram Protocol
VHT	Very High Throughput
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice over Internet Protocol
VoWLAN	Voice over WLAN
VPN	Virtual Private Network

W	Watt
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area network
WNMS	Wireless Network Management System
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access version 2
WPA3	Wi-Fi Protected Access version 3