Certified Wireless Design Professional (CWDP-303) Objectives

Introduction

When you pass the CWDP exam and hold a valid CWNA certification, you earn the CWDP certification and credits 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, creating a design, implementing the network, and validating and optimizing to ensure objectives are met. A CWDP can contribute to any stage of the life cycle and is able to take responsibility for any or all the 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 weighting the subject areas and ensuring that the weighting is representative of the relative importance of the content.

Subject matter experts (SMEs) involved in the development of these objectives and/or the JTA included:

Ryan Adzima, Robert Bartz, Tom Carpenter, Rowell Dionicio, Dawn Douglass, Manon Lessard, Peter Mackenzie, and George Stefanick

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	45%
Deploy the WLAN	10%
Validate and Optimize the WLAN	20%

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 and use business requirements

1.1.1 Business use cases and justification
1.1.2 User requirements
1.1.3 Regulatory compliance
1.1.4 Industry compliance

1.2 Collect, define, and use technical requirements

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

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

1.2.6 Discover applications and their specific requirements
1.2.7 Discover WLAN upgrade requirements when applicable
1.2.8 Define bridge link requirements when applicable
1.2.9 Voice over WLAN (VoWLAN) Requirements
1.2.10 Identify client devices including most Important and least capable device
1.2.11 Requirement Areas

1.3 Identify design constraints

1.3.1 Regulatory compliance
1.3.2 Aesthetics
1.3.3 Budget
1.3.4 Architectural constraints
1.3.5 Mounting restrictions
1.3.6 Access restrictions
1.3.7 Vendor selection
1.3.8 Time constraints
1.3.9 Building codes and safety codes

1.4 Collect, use, and deliver essential documents where applicable

1.4.1 Validated floorplans
1.4.2 Network diagrams
1.4.3 Existing AP locations
1.4.4 Network closet locations
1.4.5 Existing cabling standards
1.4.6 Existing cable drop locations
1.4.7 Switch capabilities and capacity
1.4.8 Existing network services including DNS, DHCP, NTP and authentication servers
1.4.9 PoE capabilities and power budget
1.4.10 Existing wireless system data
1.4.11 Previous design/survey documentation
1.4.12 Site survey deliverables

1.5 Define requirement areas including essential metrics for each requirement

1.5.1 Capacity
1.5.2 Client device types
1.5.3 Applications and their requirements
1.5.4 SSIDs and WLAN profiles
1.5.5 Security settings
1.5.6 Understand the various issues introduced by common vertical markets such as healthcare, education, retail, hospitality, high-density scenarios, public hotspots and outdoor networks

1.6 Implement effective project management

1.6.1 Statement of Work (SoW)
1.6.2 Non-Disclosure Agreements (NDAs)
1.6.3 Project plans
1.6.4 Resource management
1.6.5 Role definition

2.0 Design the WLAN – 45%

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

2.1.1 Controller-based (physical and virtual controllers)
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 radio
2.1.7 RF profiles
2.1.8 Select and/or recommend the appropriate equipment for the design (APs, antennas, controllers, managed services)

2.2 Produce a design and communicate with appropriate individuals related to the design

2.2.1 Use WLAN design software including the common features found in the solutions provided by various vendors
- Import and calibrate floor plans
- Set project parameters
- Select and place APs and antennas manually or using automated placement tools and define configuration parameters
- Adjust AP settings to accommodate design requirements
- Define appropriate requirements areas using software features
- Define channel plans (MCA or SCA, channel widths, frequency bands, output power levels, DFS and TPC requirements) including solutions for CCI, adjacent channel interference (ACI), non-overlapping ACI, and non-802.11 interferers within regulatory constraints
- Document cabling requirements

2.2.2 Select and use appropriate tools for a design project
- Site survey hardware (camera, marking tools, spare batteries, survey trays, 2-way radios, USB adapters, USB hubs, external antennas)
- Distance measuring tools (laser measure, tape measure, measuring wheel, angle finder, mapping software)
- Personal Protective Equipment (PPE) (hardhat, steel-toe shoes, glasses, gloves, clean suits, masks, high visibility clothing)
- Use WLAN analysis tools for appropriate use cases in WLAN design (spectrum analyzer, protocol analyzer, scanner/discovery tools, cable testers)
- Use performance measurement tools to assist in WLAN design (throughput testers, QoS assessment, network functionality)
- Perform client measurements and analysis to determine client capabilities (received signal measurements, roaming behavior, QoS capabilities)
- Gather attenuation measurements for building materials and objects
- Understand the differences between AP-on-a-Stick surveys and predictive modeling software and select the appropriate solution between them for a design project

2.2.3 Perform a pre-design site survey when required
- Select and perform the appropriate type of site survey (manual active, manual passive, AP-on-a-Stick)

- Use the appropriate site survey tools during the survey
- Gain appropriate access and clearance to perform the survey
- Document metrics and other information collected during the survey (RSSI, SNR, noise floor, interference, cell coverage, application and connectivity data such as data rates, latency, loss, and retries)
- Perform survey procedures for bridge links when required

2.2.4 Design special WLAN deployments, including branch and remote offices, mesh networks, and bridge links
2.2.5 Select among common vendor features and make configuration recommendations in a design scenario (band steering, automatic channel selection, load balancing, VLAN configuration)
2.2.6 Design for different client and application types and the constraints they introduce (tablets, barcode scanners, VoIP handsets, laptops, ID badges, location tracking systems, voice and video)
2.2.7 Ensure proper end-to-end QoS is understood and implemented including WMM, wired QoS, QoS markings and queues
2.2.8 Define and recommend proper security solutions in the design including monitoring, authentication servers, EAP methods, authentication, and encryption
2.2.9 Design for secure roaming including 802.11-2016 FT roaming, SCA roaming, vendor roaming solutions, and client support issues

2.3 Create, distribute, and communicate design documentation

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

3.0 Deploy the WLAN – 10%

3.1 Ensure proper understanding and implementation of design documentation
3.1.1 Implementation meeting (explain design decisions to implementers and ensure understanding of design deployment)
3.1.2 Distribute documents to appropriate individuals
3.1.3 Select qualified implementation technicians when required

3.2 Perform validation and optimization tasks during deployment

3.2.1 Verify proper AP installation location
3.2.2 Verify PoE provisioning requirements are met
3.2.3 Verify channel selections and output power
3.2.4 Verify aesthetic requirements are met

3.2.5 Verify proper security configuration

3.3 Recommend or perform essential deployment tasks

3.3.1 Understand and perform installation procedures for different WLAN architectures (cloud-based, controller-based, WNMS, autonomous)
3.3.2 Infrastructure configuration supporting the WLAN (DHCP, DNS, NTP, switches and routers)
3.3.3 Channel assignment, automatic radio management, and output power configuration
3.3.4 Installation procedures for cloud-based APs, controller-based APs, WNMS APs, and autonomous APs

4.0 Validate and Optimize the WLAN – 20%

4.1 Perform an RF validation survey

4.1.1 Ensure coverage requirements
4.1.2 Ensure capacity requirements
4.1.3 Evaluate CCI impact

4.2 Perform client performance testing

4.2.1 Application testing
4.2.2 Roaming testing
4.2.3 Connectivity testing

4.3 Recommend and/or perform appropriate physical adjustments

4.3.1 AP locations
4.3.2 Antenna locations

4.4 Recommend and/or perform appropriate configuration adjustments

4.4.1 Transmitter RF output power
4.4.2 RF channel selection
4.4.3 RF channel bandwidth

4.5 Select remediation solutions for problems discovered during post-validation

4.5.1 RF coverage problems
4.5.2 Capacity problems

4.5.3 QoS problems
4.5.4 Security configuration errors
4.5.5 Client connectivity issues
4.5.6 Resolve interference issues

4.6 Implement knowledge transfer and hand-off

4.6.1 End user training
4.6.2 Support staff training
4.6.3 Solution documentation and assets (digital or physical assets, guides, floorplans, configuration documents)
4.6.4 Final meeting (Q&A and hand-off)

CWDP-303 Exam Acronyms

For the CWDP-303 exam, you should be able to understand clearly define the following acronyms in relation to 802.11 WLAN operations and analysis. Such acronyms shall be used on the CWDP-303 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
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
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
RSNA	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	Television Very 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