Certified Wireless Network Expert (CWNE) Bootcamp Objectives and Sub-Objectives (curriculum details)

WORLD WIDE WIFI EXPERTS

Introduction:

This bootcamp is unique because it is an **40** hours program and covers the entire curriculum CWNP Certified Wireless Network Expert (CWNE), is fully didactic and consists of in person or online Live Expert Sessions, where you interact with a CWNE also senior instructor (CWNT). Online possible in your own familiar home (or work) environment.

After this CWNE bootcamp it will demonstrate that you have mastered all relevant skills to administer, install, configure, troubleshoot, and design wireless network systems. In addition, aspiring CWNE candidates will need to demonstrate deep understanding of protocol analysis, intrusion detection and prevention, performance and QoS analysis, spectrum analysis and management and advanced design.

The CWNE Bootcamp is a one week course of in total **5** days.

Each training module of the CWNP CWNE track will be covered out of their highlights so the list is as follows:

Training Modules	*Course Length*
2.0 Certified Wireless Network Administrator (CWNA) - Foundational Level	1 Day
3.0 Certified Wireless Security Professional (CWSP) - Secure Level	1 Day
4.0 Certified Wireless Analysis Professional (CWAP) - Troubleshoot Level	1 Day
5.0 Certified Wireless Design Professional (CWDP) - Design Level	1 Day
6.0 Certified Wireless IoT Solutions Administrator (CWISA) - Broaden Level	1 Day

Course Outline

2.0 Certified Wireless Network Administrator (CWNA) - Foundational Level

2.1 Radio Frequency (RF) Technologies

- 2.1.1 Wavelength, frequency, amplitude, phase, sine waves
- 2.1.2 RF propagation and coverage
- 2.1.3 Reflection, refraction, diffraction and scattering
- 2.1.4 Multipath and RF interference
- 2.1.5 Gain and loss
- 2.1.6 Amplification
- 2.1.7 Attenuation
- 2.1.8 Absorption
- 2.1.9 Voltage Standing Wave Ratio (VSWR)
- 2.1.10 Return Loss
- 2.1.11 Free Space Path Loss (FSPL)

- 2.1.12 Watt and milliwatt
- 2.1.13 Decibel (dB)
- 2.1.14 dBm and dBi
- 2.1.15 Noise floor
- 2.1.16 SNR
- 2.1.17 RSSI
- 2.1.18 dBm to mW conversion rules of 10 and 3
- 2.1.19 Equivalent Isotropically Radiated Power (EIRP)

- 2.1.20 RF and physical line of sight and Fresnel zone clearance
- 2.1.21 Beamwidths
- 2.1.22 Passive gain
- 2.1.23 Polarization
- 2.1.24 Antenna diversity types
- 2.1.25 Radio chains
- 2.1.26 Spatial multiplexing (SM)
- 2.1.27 Transmit Beamforming (TxBF)
- 2.1.28 Maximal Ratio Combining (MRC)
- 2.1.29 MIMO

2.1.30 Omni-directional antennas
2.1.31 Semi-directional antennas
2.1.32 Highly directional antennas
2.1.33 Reading Azimuth and Elevation charts for different antenna types
2.1.34 Antenna orientation
2.1.35 RF cables and connectors
2.1.36 Lightning arrestors and grounding rods/wires

2.2 Radio Frequency (RF) Validation

2.2.1 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
2.2.2 Identify sources of RF interference from non-802.11 wireless devices based on the investigation of airtime and frequency utilization
2.2.3 Understand interference mitigation options including removal of interference source or change of wireless channel usage
2.2.4 Network and service availability
2.2.5 VoIP testing
2.2.6 Real-time application testing
2.2.7 Throughput testing
2.2.8 Use of throughput testers for validation tasks
2.2.9 Use of wireless validation software (specifically survey software and wireless scanners)
2.2.10 Use of protocol analyzers for validation tasks
2.2.11 Use of spectrum analyzers for validation tasks

2.3 WLAN Regulations, Standards, Protocols, Devices, Networks Architecture and Design Concepts

2.3.1 IEEE
2.3.2 Wi-Fi Alliance
2.3.3 IETF
2.3.4 Regulatory domains and agencies

2.3.5 DSSS – 802.11
2.3.6 HR-DSSS – 802.11b
2.3.7 OFDM – 802.11a

2.3.8 ERP – 802.11g

2.3.9 Wi-Fi 4 - HT – 802.11n

2.3.10 Wi-Fi 5 - VHT – 802.11ac

2.3.11 Wi-Fi 6 - HE - 802.11ax

2.3.12 DSSS

2.3.13 OFDM

2.3.14 OFDMA and Resource Units

2.3.15 BPSK

2.3.16 QPSK

2.3.17 QAM (16, 64, 256,1024)

2.3.18 Primary channels

2.3.19 Adjacent overlapping and non-overlapping channels

2.3.20 Throughput vs. data rate

2.3.21 Bandwidth

2.3.22 Guard Interval

2.3.23 Frequency bands used by the 802.11 PHYs

2.3.24 Available channels

2.3.25 Regulatory power constraints

2.3.26 Dynamic Frequency Selection (DFS)

2.3.27 Transmit Power Control (TPC)

2.3.28 Wireless LAN (WLAN) – BSS and ESS

2.3.29 Wireless bridging

2.3.30 Wireless Ad-Hoc (IBSS)

2.3.31 Wireless Mesh

2.3.32 Stations (STAs)

2.3.33 Basic Service Set (BSS) (Infrastructure mode)

2.3.34 SSID

2.3.35 BSSID

2.3.36 Extended Service Set (ESS)

2.3.37 IBSS (Ad-Hoc)

2.3.38 Distribution System (DS)

2.3.39 Distribution System Media (DSM)

2.3.40 MSDU, MPDU, PSDU, and PPDU
2.3.41 A-MSDU and A-MPDU
2.3.42 PHY preamble and header

2.3.43 MAC frame format
2.3.44 MAC addressing

2.3.45 Management
2.3.46 Control
2.3.47 Data

2.3.48 Scanning (active and passive)
2.3.49 Authentication
2.3.50 Association
2.3.51 Open System Authentication and Shared Key authentication
2.3.52 Connecting to 802.1X/EAP and Pre-Shared Key authentication networks
2.3.53 BSS selection
2.3.54 Connecting to hidden SSIDs

2.3.55 DCF
2.3.56 EDCA
2.3.57 RTS/CTS
2.3.58 CTS-to-Self
2.3.59 NAV
2.3.60 Interframe spaces (SIFS, DIFS, EIFS, AIFS)
2.3.61 Physical carrier sense and virtual carrier sense
2.3.62 Hidden node

2.3.63 Roaming
2.3.64 Power save modes and frame buffering
2.3.65 Protection mechanisms

2.3.66 Access Points (APs)
2.3.67 WLAN controllers
2.3.68 Wireless network management systems
2.3.69 Wireless bridge and mesh APs

2.3.70 Client devices

2.3.71 Power Source Equipment
2.3.72 Powered Device
2.3.73 Midspan and endpoint PSEs
2.3.74 Power classes to include power differences between PSE and PD
2.3.75 Power budgets and powered port density

2.3.76 Centralized data forwarding
2.3.77 Distributed data forwarding
2.3.78 Control, Management and Data planes
2.3.79 Scalability and availability solutions
2.3.80 Tunneling, QoS and VLANs

2.3.81 Design considerations for data
2.3.82 Design considerations for voice
2.3.83 Design considerations for video
2.3.84 Design considerations for location services including Real-Time Location Services (RTLS)
2.3.85 Design considerations for highly mobile devices (e.g. tablets and smartphones)
2.3.86 Capacity planning for high and very high-density environments
2.3.87 Design considerations for guest access/BYOD
2.3.88 Design considerations for supporting legacy 802.11 devices

2.3.89 AirTime Fairness
2.3.90 Band steering
2.3.91 Dynamic power and channel management features

2.3.92 DHCP for client addressing, AP addressing and/or controller discovery
2.3.93 DNS for address resolution for clients and APs
2.3.94 Time synchronization protocols (e.g. NTP, SNTP)
2.3.95 VLANs for segmentation
2.3.96 Authentication services (e.g. RADIUS, LDAP)
2.3.97 Access Control Lists for segmentation
2.3.98 Wired network capacity requirements

3.0 Certified Wireless Security Professional (CWSP) - Secure Level

3.1 Security Policy, Lifecycle Management, Design and Architecture

3.1.1 Evaluate and incorporate business, technical, and applicable regulatory policies (for example, PCI-DSS, HIPAA, GDPR, etc.)
3.1.2 Involve appropriate stakeholders
3.1.3 Review client devices and applications
3.1.4 Review WLAN infrastructure devices

3.1.5 Translate security requirements to high-level policy statements
3.1.6 Write policies conforming to common practices including definitions of enforcement and constraint specifications
3.1.7 Ensure appropriate approval and support for all policies
3.1.8 Implement security policy lifecycle management

3.1.9 Identify technologies being introduced to the WLAN
3.1.10 Assess security requirements for new technologies
3.1.11 Implement appropriate protective measures for new technologies and validate the security of the measures
3.1.12 Monitor and audit the new technologies for security compliance (Security Information Event Management (SIEM), portable audits, infrastructure-based audits, WIPS/WIDS)

3.1.13 User interviews
3.1.14 Vulnerability scans
3.1.15 Reviewing access controls
3.1.16 Penetration testing
3.1.17 System log analysis
3.1.18 Report findings to management and support professionals as appropriate

3.1.19 WPA/WPA2-Personal (Pre-Shared Key)
3.1.20 WPA/WPA2-Enterprise
3.1.21 WPA3-SAE and 192-Bit enterprise security
3.1.22 Opportunistic Wireless Encryption (OWE)
3.1.23 Fast Initial Link Setup (FILS)
3.1.24 802.1X/EAP

3.1.25 Understand the capabilities of EAP methods including EAP-TLS, EAP-TTLS, PEAP, EAP-FAST, EAP-SIM, and EAP-GTC
3.1.26 Guest access authentication

3.1.27 Encryption methods and concepts
3.1.28 Deprecated solutions TKIP/RC4
3.1.29 CCMP/AES
3.1.30 SAE and 192-bit security
3.1.31 OWE
3.1.32 Virtual Private Network (VPN)

3.1.33 Wireless Intrusion Prevention System (WIPS) - overlay and integrated
3.1.34 Laptop-based monitoring with protocol and spectrum analyzers

3.1.35 Encryption keys and key hierarchies
3.1.36 Handshakes and exchanges (4-way, SAE, OWE)
3.1.37 Pre-shared keys
3.1.38 Pre-RSNA security (WEP and 802.11 Shared Key authentication)
3.1.39 TSN security
3.1.40 RSN security
3.1.41 WPA, WPA2, and WPA3

3.1.42 Physical port security in Ethernet switches
3.1.43 Network segmentation, VLANs, and layered security solutions
3.1.44 Tunneling protocols and connections
3.1.45 Access Control Lists (ACLs)
3.1.46 Firewalls

3.1.47 Role-Based Access Control (RBAC)
3.1.48 Certificate Authorities (CAs) and Public Key Infrastructure (PKI)
3.1.49 AAA Servers
3.1.50 Client onboarding
3.1.51 Network Access Control (NAC)
3.1.52 BYOD and MDM

3.1.53 802.11r Fast BSS Transition (FT)
3.1.54 Opportunistic Key Caching (OKC)

3.1.55 Pre-Shared Key (PSK) - standard and per-user

3.1.56 Guest access
3.1.57 Peer-to-peer connectivity
3.1.58 Captive portals
3.1.59 Hotspot 2.0/Wi-Fi Certified Passpoint
3.1.60 OWE

3.1.61 Weak/default passwords
3.1.62 Misconfiguration
3.1.63 Firmware/software updates
3.1.64 HTTP-based administration interface access
3.1.65 Telnet-based administration interface access
3.1.66 Older SNMP protocols such as SNMPv1 and SNMPv2

3.2 Vulnerabilities, Threats, and Attacks

3.2.1 Use information sources to identify the latest vulnerabilities related to a WLAN including online repositories containing CVEs
3.2.2 Determine the risk and impact of identified vulnerabilities
3.2.3 Select appropriate actions to mitigate threats exposed by vulnerabilities
3.2.4 Describe and detect possible, common WLAN attacks including eavesdropping, man-in-the-middle, cracking, phishing, and other social engineering attacks
3.2.5 Implement penetration testing procedures to identify weaknesses in the WLAN
3.2.6 Implement network monitoring to identify attacks and potential vulnerabilities

3.2.7 Asset management
3.2.8 Risk ratings
3.2.9 Loss expectancy calculations
3.2.10 Develop risk management plans for WLANs

4.0 Certified Wireless Analysis Professional (CWAP) - Troubleshoot Level

4.1 Protocol and Spectrum Analysis

4.1.1 Laptop protocol analyzers
4.1.2 APs, controllers, and other management solutions
4.1.3 Specialty devices (hand-held analyzers and custom-built devices)
4.1.4 Install monitor mode drivers
4.1.5 Select capture location(s)
4.1.6 Capture sufficient data for analysis
4.1.7 Capture all channels or capture on a single channel as needed
4.1.8 Capture roaming events

4.1.9 Save to disk
4.1.10 Packet slicing
4.1.11 Event triggers
4.1.12 Buffer options
4.1.13 Channels and channel widths
4.1.14 Capture filters
4.1.15 Channel scanning and dwell time

4.1.16 Use appropriate display filters to view relevant frames and packets
4.1.17 Use colorization to highlight important frames and packets
4.1.18 Configure and display columns for analysis purposes
4.1.19 View frame and packet decodes while understanding the information shown and applying it to the analysis process
4.1.20 Use multiple adapters and channel aggregation to view captures from multiple channels
4.1.21 Implement protocol analyzer decryption procedures
4.1.22 View and use a capture's statistical information for analysis
4.1.23 Use expert mode for analysis
4.1.24 View and understand peer maps as they relate to communications analysis

4.1.25 WLAN scanners and discovery tools
4.1.26 Protocol capture visualization and analysis tools

4.1.27 Centralized monitoring, alerting, and forensic tools

4.1.28 Define the problem
4.1.29 Determine the scale of the problem
4.1.30 Identify probable causes
4.1.31 Capture and analyze the data
4.1.32 Observe the problem
4.1.33 Choose appropriate remediation steps
4.1.34 Document the problem and resolution

4.1.35 Install, configure, and use spectrum analysis software and hardware
4.1.36 Capture RF spectrum data using handheld, laptop-based, and infrastructure spectrum capture solutions
4.1.37 Understand and use spectrum analyzer views

4.1.38 RF noise floor in an environment
4.1.39 Signal-to-Noise Ratio (SNR) for a given signal
4.1.40 Sources of RF interference and their locations
4.1.41 RF channel utilization
4.1.42 Non-Wi-Fi transmitters and their impact on WLAN communications
4.1.43 Overlapping and non-overlapping adjacent channel interference
4.1.44 Poor performing or faulty radios

4.1.45 Identify various 802.11 PHYs
4.1.46 Identify non-802.11 devices based on RF behaviors and signatures
4.1.47 Use centralized spectrum analysis solutions

4.2 802.11 Frame Exchanges

4.2.1 BSS discovery
4.2.2 802.11 Authentication and Association
4.2.3 802.1X/EAP exchanges
4.4.4 Pre-Shared Key authentication
4.4.5 Four-way handshake
4.4.6 Group key exchange
4.4.7 Simultaneous Authentication of Equals (SAE)

4.4.8 Opportunistic Wireless Encryption (OWE)
4.4.9 WPA2 and WPA3

4.4.10 Fast secure roaming mechanisms
4.4.11 Neighbor discovery (802.11k/v)
4.4.12 Hotspot 2.0 protocols and operations from the client access perspective

4.4.13 Sticky clients
4.4.14 Excessive roaming
4.4.15 Channel aggregation for roaming analysis

4.4.16 Data frames and acknowledgement frames
4.4.17 RTS/CTS data frame exchanges
4.4.18 QoS Data frame exchanges
4.4.19 Block Acknowledgement exchanges

4.4.20 MIMO
4.4.21 OFDMA

4.4.22 Power Save operations
4.4.23 Protection mechanisms
4.4.24 Load balancing
4.4.25 Band Steering

5.0 Certified Wireless Design Professional (CWDP) - Design Level

5.1 Define Specifications for the WLAN

5.1.1 Business use cases and justification
5.1.2 User requirements
5.1.3 Regulatory compliance
5.1.4 Industry compliance
5.1.5 Budget
5.1.6 Aesthetics
5.1.7 Architectural constraints
5.1.8 Mounting restrictions
5.1.9 Access restrictions
5.1.10 Time constraints
5.1.11 Building codes and safety codes

5.1.12 Vendor selection
5.1.13 Location services such as RTLS
5.1.14 Latency requirements
5.1.15 Signal strength requirements
5.1.16 Capacity requirements
5.1.17 Security requirements
5.1.18 Applications and their specific requirements
5.1.19 WLAN upgrade requirements, when applicable
5.1.20 Bridge link requirements, when applicable
5.1.21 Voice over WLAN (VoWLAN), when applicable
5.1.22 Client devices including most important and least capable device
5.1.23 Requirement areas

5.1.24 Validated floor plans
5.1.25 Network infrastructure
5.1.26 Cabling infrastructure
5.1.27 Power availability and PoE capabilities
5.1.28 Existing wireless systems
5.1.29 Previous design/survey documentation

5.1.30 Client device types and capabilities
5.1.31 Applications and their requirements
5.1.32 User and device density
5.1.33 SSIDs
5.1.34 Security settings
5.1.35 Understand common vertical markets

5.1.36 Building materials
5.1.37 Attenuation values
5.1.38 Ceiling heights
5.1.39 Site annotations (photos, notes, plans)
5.1.40 Wireless environment scan

5.2 Design the WLAN

5.2.1 Controller-based (physical and virtual) architectures
5.2.2 Distributed (cloud-based and local WNMS)
5.2.3 Standalone/Autonomous APs
5.2.4 Dynamic vs. static channel assignment
5.2.5 Dynamic radio management
5.2.6 Software defined radios
5.2.7 RF profiles
5.2.8 Select and/or recommend the appropriate equipment for the design and selected architecture (APs, antennas, controllers, managed services)
5.2.9 Select and use the appropriate design tools
5.2.10 Select and use the appropriate design methodologies
5.2.11 Understand and use the common features of wireless design software
5.2.12 Select and use common vendor features and make configuration recommendations
5.2.13 Design for different client and application types
5.2.14 Ensure end-to-end QoS is properly implemented
5.2.15 Define and recommend security solutions
5.2.16 Design for secure roaming
5.2.17 Create, distributed, and communicate design documentation

5.3 Deploy the WLAN

- 5.3.1 Ensure proper understanding and implementation of the design
- 5.3.2 Recommend or perform essential deployment tasks
- 5.3.3 Perform an installation audit for quality assurance

5.4. Validate and Optimize the WLAN

- 5.4.1 Confirm the WLAN system is operational
- 5.4.2 Perform an RF validation survey
- 5.4.3 Perform client performance testing
- 5.4.4 Recommend appropriate physical adjustments
- 5.4.5 Recommend appropriate RF adjustments
- 5.4.6 Recommend remediation for application issues
- 5.4.7 Implement knowledge transfer and hand-off

6.0 Certified Wireless IoT Solutions Administrator (CWISA) - Broaden Level

6.1 Wireless Technologies

- 6.1.1 Maintain continued awareness of wireless IoT technologies and applications of those technologies
- 6.1.2 Understand industry standard, certification and regulatory organizations and standards development processes
- 6.1.3 Define wireless network types (WLAN, WPAN, WBAN, WMAN, WWAN, WSN, IoT
- 6.1.4 Understand hardware and software components of IoT end devices and gateways (processors, memory, radios, storage, sensors, network connections, operating systems/firmware, application/service software, off-the-shelf devices, custom devices)

6.2 Radio Frequency Communications

- 6.2.1 Explain the basic RF wave characteristics, behaviors and measurements used for wireless communications
- 6.2.2 Describe the fundamentals of modulation techniques used in wireless communications (ASK, FSK, PSK, APSK, QAM, OFDM, OFDMA, Frequency Hopping, CSS, AM, FM, CW)
- 6.2.3 Explain the basic capabilities of components used in RF communications
- 6.2.4 Describe the basic use and capabilities of the RF bands

6.3 Planning, Implementing and Supporting Wireless Solutions

- 6.3.1 Identify and use the wireless IoT system requirements
- 6.3.2 Identify and comply with system constraints
- 6.3.3 Select appropriate wireless IoT solutions based on requirements and constraints
- 6.3.4 Plan for the technical requirements of the wireless IoT solution
- 6.3.5 Understand the basic features and capabilities of common wireless IoT solutions and plan for their implementation
- 6.3.6 Understand the wireless IoT solution and consider key issues related to automation, integration, monitoring, and management
- 6.3.7 Use best practices in wireless IoT solution implementations
- 6.3.8 Validate wireless solution implementations including RF communications and application functionality
- 6.3.9 Understand and implement basic installation procedures

6.3.10 Implement best practices in knowledge transfer and hand-off

6.3.11 Administer the wireless solution while considering the implications of various vertical markets

6.3.12 Troubleshoot common problems in wireless IoT solutions

6.3.13 Understand and determine the best use of scripting and programming solutions for wireless IoT implementations

6.3.14 Understand application architectures and their impact on wireless IoT solutions