Training: CWNP
CWNA Certified Wireless Network Administrator

AUTHORIZED LEARNING CENTER cwnp

TRANING TERMS

2026-12-07 | 4 days | Virtual Classroom
2026-12-28 | 4 days | Virtual Classroom

TRAINING GOALS:

The Enterprise Wi-Fi Administration course, provides the networking professional a complete foundation of knowledge for entering into or advancing in the wireless networking industry. The Certified Wireless Network Administrator (CWNA) understands standards and operations of 802.11 wireless networks. Responsibilities include deploying, managing, monitoring, and basic troubleshooting of these networks. The CWNA can describe devices and operations of current WLAN technologies.

Main Areas Covered by CWNA:

- Radio Frequency (RF) Technologies
- Antenna Concepts
- Wireless LAN Hardware and Software
- Network Design, Installation, and Management
- Wireless Standards and Organizations
- 802.11 Network Architecture
- Wireless LAN Security
- Troubleshooting
- How to Perform Site Surveys

Each participant in an authorized CWNP CWNA training held in Compendium CE will receive a free CWNA-109 Certified Wireless Network Administrator Exam voucher.

CONSPECT:

- Radio Frequency (RF) Technologies
  - Define and explain the basic characteristics and behavior of RF
    - Wavelength, frequency, amplitude, phase, sine waves
    - RF propagation and coverage

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- 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

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- WLAN Regulations and Standards
  - Explain the roles of WLAN and networking industry organizations
    - IEEE
    - Wi-Fi Alliance
    - 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

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

        - 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
    - 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)
        - 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)
        - 11 Authentication
        - 11 Open System Authentication
        - 11 Association
        - BSS selection
        - Connecting to hidden SSIDs

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- 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
  - 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
  - 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

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- 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
  - Identify weak security options that should not be used in enterprise WLANs
    - WEP
    - 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

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- 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
  - 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 tasks
    - 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
    - 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

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Identify wireless issues related to security configuration mismatches
- Identify hidden node issues

REQUIREMENTS:

The CWNA has no prerequisites; however, the following are recommended knowledge and experience before attempting the CWNA training and exam:

- Basic knowledge of networking (routers, switches, cabling, etc.)
- Basic knowledge of TCP/IP
- At least 1 year of work experience with wireless LAN technologies

Difficulty level



CERTIFICATE:

The participants will obtain certificates signed by Compendium CE (course completion).

The CWNA certification is a foundational level wireless LAN certification for the CWNP Program. To earn a CWNA certification, you must take the CWNA exam at a Pearson Vue Testing Center and pass with a 70% or higher. Instructors must pass with a 80% or higher. However you choose to prepare for the CWNA exam, you should start with the exam objectives, which cover the full list of skills tested on the exam. The CWNA certification is valid for three (3) years. To recertify, pass one of the professional level certifications exams (CWSP,CWDP, CWAP) BEFORE your CWNA expires. By doing so, the CWNA will be renewed for another three (3) years. Or retake the current version of the CWNA exam.

While the Certified Wireless Specialist (CWS) and Certified Wireless Technician (CWT) certifications are not a required prerequisite to the CWNA certification, it is highly recommended. It will provide a solid learning foundation before continuing to pursue the CWNA.

CWNA exam is available through the Pearson VUE test centers.

Each participant in an authorized CWNP CWNA training held in Compendium CE will receive a free CWNA-109 Certified Wireless Network Administrator Exam voucher.

TRAINER:

Authorized CWNP Trainer.

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007