CWNA Wireless Network Administrator

Duration: 4 Days **Course Code: CWNA** **Version: 110** **Delivery Method: Company Event**

Overview:

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 CWNP Remote Proctored Exams and pass with a 70% or higher.

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

***The CWNA certification is valid for three (3) years.**

Updated November 2026

Company Events

These events can be delivered exclusively for your company at our locations or yours, specifically for your delegates and your needs. The Company Events can be tailored or standard course deliveries.

Target Audience:

This class is intended for the following participants:

- IT professionals and network engineers responsible for installing or supporting 802.11 (Wi-Fi) Wireless networks
- IT professionals wanting to progress within the wireless network industry
- Network planners, designers and support staff
- IT Security staff, managers and auditors

Objectives:

- After completing this course, you will be able to:
- Understand and apply the essential concepts of Radio Frequency (RF) technology, including RF planning, RF-related calculations and spread spectrum technologies.
- Perform RF Spectrum Analysis for the 2.4GHz and 6GHz bands.
- Describe the rules governing wireless LANs, to comply with local radio regulations for setup and maintenance of WLANs.
- Describe the fundamental operation of wireless LANs, for effective WLAN problem analysis and troubleshooting.
- Understand IEEE 802.11b, 802.11g, 802.11a, 802.11n, 802.11ac and 802.11ax (Wi-Fi 6) standards and amendments; and their practical relevance in depth.
- Understand 802.11 / Wi-Fi WLAN Physical and MAC -layer operation in depth.
- Describe and troubleshoot WLAN problems including RF coverage, multipath, hidden nodes and interference problems.
- Understand the essential tools and processes used in Wi-Fi Site Survey.
- Work with sophisticated WLAN diagnostic tools from Ekahau, AirMagnet, MetaGeek, Savvius, Tamosoft and more.
- Describe the insecurities inherent in IEEE 802.11 WLANs.
- Apply best security practices, including WPA2 and WPA3, to secure Wi-Fi networks for small, medium and large organisations.

- Correctly install, configure and support Wi-Fi adapters, access points, wireless bridges and WLAN antennas.

Prerequisites:

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

- Basic knowledge of networking (routers, switches, cabling, etc.)
- Basic knowledge of TCP/IP
- CNAE certification or equivalent knowledge
- At least 1 year of work experience with wireless LAN technologies
- GK3150 - Understanding Networking Fundamentals (Network+)

Testing and Certification

This course prepares for the CWNA (Certified Wireless Network Administrator) exam (CWNA-110). Self-study will be needed before taking the exam.

Exam Number: CWNA-110
Availability: CWNP Remote Proctored Exam
Duration: 90 minutes
Questions: 60 multiple choice / multiple answer
Language: English

The **CWNA** certification is valid for three (3) years. To recertify, pass one of the professional level certifications exams (CWAP, CWDP, or CWSP) before your CWNA expires. By doing so, the CWNA will be renewed for another three (3) years. Or just retake the current version of the CWNA exam. While the Certified Wireless Specialist (CWSS) and Certified Wireless Technician (CWTS) 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.

NOTE: *If your CWNA expires and you pass a professional level certification (CWAP, CWDP, or CWSP) within 30 days of expiration, it will renew your CWNA. When you pass the CWNA exam, you earn the required prerequisite for the CWSP, CWDP, CWAP, CWNE, and CWISE certifications and you earn the CWNA certification.*

Content:

1.Radio Frequency (RF) Technologies – 15%

1.1. Define and explain the basic characteristics and behavior of RF

1.1.1 Wavelength, frequency, amplitude, phase, sine waves

1.1.2 RF propagation and coverage

1.1.3 Reflection, refraction, diffraction, and scattering

1.1.4 Multipath and RF interference

1.1.5 Gain and loss

1.1.6 Amplification

1.1.7 Attenuation

1.1.8 Absorption

1.1.9 Voltage Standing Wave Ratio (VSWR)

1.1.10 Return Loss

1.1.11 Free Space Path Loss (FSPL)

1.2. Apply the basic concepts of RF mathematics and measurement

1.2.1. Watt and milliWatt

1.2.2. Decibel (dB)

1.2.3. dBm and dBi

1.2.4. Noise floor

1.2.5. SNR

1.2.6. RSSI

2.5 Describe the OSI and TCP/IP model layers affected by the 802.11-2024 standard and amendments

2.6 Identify and comply with regulatory domain requirements and constraints

2.6.1 Frequency bands used by the 802.11 PHYs

2.6.2 Available channels

2.6.3 Regulatory power constraints

2.6.4 Indoor, outdoor deployments and implementation variants

2.6.5 Dynamic Frequency Selection (DFS)

2.6.6 Transmit Power Control (TPC)

2.7 Explain basic use case scenarios for 802.11 wireless networks

2.7.1 Wireless LAN (WLAN) – BSS and ESS

2.7.2 Wireless bridging

2.7.3 Wireless Peer to peer solutions

2.7.4 Wireless Mesh

3.WLAN Protocols and Devices – 20%

3.1 Describe the components and functions that make up an 802.11 wireless service set

3.1.1 Stations (STAs)

3.1.2 Basic Service Set (BSS) (Infrastructure mode)

3.1.3 SSID

4.2.5 Tunneling, QoS and VLANs

4.3 Describe basic design considerations for common deployment scenarios in wireless such as coverage requirements, roaming considerations and throughput.

4.3.1 Design considerations for data, voice and video

4.3.2 Design considerations for specific applications such as location services, high density and guest access/BYOD

4.3.3 Design considerations for supporting legacy 802.11 devices

4.4 Demonstrate awareness of common proprietary features in wireless networks.

4.4.1 AirTime Fairness

4.4.2 Band steering

4.4.3 Dynamic power and channel management features

4.4.4 Internal Wireless architecture communication

4.4.5 AI monitoring, management, and reporting

4.5 Determine and configure required network services supporting the wireless network

4.5.1 DHCP for client addressing, AP addressing and/or controller discovery

4.5.2 DNS for address resolution for clients and APs

4.5.3 Time synchronization protocols (e.g. NTP, SNTP)

4.5.4 VLANs for segmentation

1.2.7. dBm to mW conversion rules of 10 and 3

1.2.8. Equivalent Isotropically Radiated Power (EIRP)

1.3. Identify RF signal characteristics as they relate to antennas

1.3.1. RF and physical line of sight and Fresnel zone clearance

1.3.2. Beamwidths

1.3.3. Passive gain

1.3.4. Polarization

1.3.5. Antenna diversity types

1.3.6. Radio chains

1.3.7. MIMO

1.4. Explain and apply the functionality of RF antennas, antenna systems, and accessories available

1.4.1. Omni-directional antennas

1.4.2. Semi-directional antennas

1.4.3. Highly directional antennas

1.4.4. Reading Azimuth and Elevation charts for different antenna types

1.4.5. Antenna orientation

1.4.6. RF cables and connectors

1.4.7. Lightning arrestors and grounding rods/wires

3.1.4 BSSID

3.1.5 Extended Service Set (ESS)

3.1.6 IBSS

3.1.7 Distribution System (DS)

3.1.8 Distribution System Media (DSM)

3.2 Define terminology related to the 802.11 MAC and PHY

3.2.1 MSDU, MPDU, PSDU, and PPDU

3.2.2 A-MSDU and A-MPDU

3.2.3 PHY preamble and header

3.3 Identify and explain the MAC frame format

3.3.1 MAC frame format

3.3.2 MAC addressing

3.4 Identify and explain the purpose of the three main 802.11 frame types

3.4.1 Management

3.4.2 Control

3.4.3 Data

3.5 Explain the process used to locate and connect to a WLAN

3.5.1 Scanning (active and passive, RNR)

3.5.2 802.11 Authentication

3.5.3 802.11 Open System Authentication

4.5.5 Authentication services (e.g. RADIUS, LDAP)

4.5.6 Access Control Lists for segmentation

4.5.7 Wired network capacity requirements

5.WLAN Network Security – 10%

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

5.1.1 WEP

5.1.2 802.11 Shared Key authentication

5.1.3 SSID hiding as a security mechanism

5.1.4 MAC filtering

5.1.5 Use of deprecated security methods (e.g. WPA and/or WPA2 with TKIP)

5.2 Identify and configure effective security mechanisms for enterprise WLANs

5.2.1 Application of AES for encryption and integrity

5.2.2 WPA2-Personal including limitations and best practices for pre-shared (PSK) use

5.2.3 WPA2-Enterprise -configuring wireless networks to use 802.1X including connecting to RADIUS servers and appropriate EAP methods

5.3 Understand basic concepts of WPA3 and Opportunistic Wireless Encryption (OWE) and enhancements over WPA2

5.3.1 Understand basic security enhancements in WPA3 vs. WPA2

5.3.2 Understand basic security

1.4.8. Enclosures, mounting and aesthetic concerns

2.WLAN Regulations and Standards – 20%

2.1 Explain the roles of WLAN and networking industry organizations

2.1.1 IEEE

2.1.2 Wi-Fi Alliance

2.1.3 IETF

2.1.4 Regulatory domains and agencies

2.2 Explain and apply the various Physical Layer (PHY) solutions of the IEEE 802.11-2024 standard and amendments including supported channel widths, spatial streams, and data rates

2.2.1 DSSS – 802.11

2.2.2 HR-DSSS – 802.11b

2.2.3 OFDM – 802.11a

2.2.4 ERP – 802.11g

2.2.5 Wi-Fi 4 - HT – 802.11n

2.2.6 Wi-Fi 5 - VHT –802.11ac

2.2.7 Wi-Fi 6 - HE - 802.11ax (2.4 and 5 GHz)

2.2.8 Wi-Fi 6E - HE - 802.11ax (6 GHz)

2.2.9 Wi-Fi 7 - EHT - 802.11be

2.3 Understanding spread spectrum technologies, Modulation and Coding Schemes (MCS)

2.3.1 DSSS

3.5.4 802.11 Association

3.5.5 BSS selection

3.5.6 Connecting to hidden SSIDs

3.6 Explain 802.11 channel access methods

3.6.1 DCF

3.6.2 EDCA

3.6.3 RTS/CTS

3.6.4 CTS-to-Self

3.6.5 NAV

3.6.6 Interframe spaces (SIFS, DIFS, EIFS, AIFS)

3.6.7 Physical carrier sense and virtual carrier sense

3.7 Explain 802.11 MAC operations

3.7.1 Roaming

3.7.2 Power save modes and frame buffering

3.7.3 Protection mechanisms

3.8 Describe features of, select, and install WLAN devices, control, and management systems

3.8.1 Access Points (APs)

3.8.2 WLAN controllers

3.8.3 Wireless network management systems

3.8.4 Wireless bridge and mesh APs

enhancements of encryption and integrity in WPA3

5.3.3 Simultaneous Authentication of Equals (SAE) in WPA3 as an enhancement for legacy pre-shared key technology

5.3.4 Opportunistic Wireless Encryption (OWE) for public and guest networks

5.4 Describe common security options and tools used in wireless networks

5.4.1 Access control solutions

5.4.2 Protected management frames

5.4.3 Fast Secure Roaming methods

5.4.4 Wireless Intrusion Prevention System (WIPS) and/or rogue AP detection

5.4.5 AI monitoring and alert systems

5.4.6 Protocol and spectrum analyzers

5.4.7 Best practices in secure management protocols

6.RF Validation and WLAN remediation– 10%

6.1 Verify and document that design requirements are met including coverage, throughput, roaming, and connectivity with a post-implementation validation survey.

6.2 Locate and identify sources of RF interference

6.2.1 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.

6.2.2 Identify sources of RF interference from non-802.11 wireless devices based on the investigation of airtime and frequency utilization

2.3.2 OFDM

2.3.3 OFDMA and Resource Units

2.3.4 BPSK

2.3.5 QPSK

2.3.6 QAM (16, 64, 256, 1024, 4096)

2.4 Identify and apply 802.11 WLAN functional concepts

2.4.1 Primary channels

2.4.2 OBSS

2.4.3 Adjacent overlapping and non-overlapping channels

2.4.4 Multi-Link Operation (MLO)

2.4.5 Throughput vs. data rate

2.4.6 Bandwidth

2.4.7 Guard Interval

3.8.5 Client devices

4.WLAN Network Architecture and Design Concepts– 15%

4.1 Describe and implement Power over Ethernet (PoE)

4.1.1 Power Source Equipment

4.1.2 Powered Device

4.1.3 Midspan and endpoint PSEs

4.1.4 Power-classes to include power differences between PSE and PD

4.1.5 Power budgets and powered port density

4.2 Define and describe differences, advantages and constraints of the different wireless LAN architectures

4.2.1 Centralized data forwarding

4.2.2 Distributed data forwarding

4.2.3 Control, Management and Data planes

4.2.4 Scalability and availability solutions

6.2.3 Understand interference mitigation options including removal of interference source or change of wireless channel usage

6.3 Perform application testing to validate WLAN performance

6.3.1 Network and service availability

6.3.2 VoIP testing

6.3.3 Real-time application testing

6.3.4 Throughput testing

6.4 Understand and use the basic features of validation tools

6.4.1 Use of throughput testers for validation tasks

6.4.2 Use of wireless validation software (survey software and wireless scanners)

6.4.3 Use of protocol analyzers for validation tasks

6.4.4 Use of spectrum analyzers for validation tasks

6.5 Describe and apply common troubleshooting tools used in WLANs

6.5.1 Use of protocol analyzers for troubleshooting tasks

6.5.2 Use of spectrum analyzers for identifying sources of interference

6.5.3 Use of management, monitoring, and logging systems for troubleshooting tasks

6.5.4 Use of wireless LAN scanners for troubleshooting tasks

6.6 Identify and troubleshoot common wireless issues

		6.6.1 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 6.6.2 Identify and solve RF interference using spectrum analyzers 6.6.3 Identify wireless performance issues using SNR, retransmissions, and airtime utilization statistics 6.6.4 Identify causes of wireless issues related to network services including DHCP, DNS, and time protocols including using native interface and IP configuration tools 6.6.5 Identify wireless issues related to security configuration mismatches 6.6.6 Identify hidden node issues

Additional Information:

Global Knowledge is a CWNP Authorized Learning Center.

The official CWNA courseware will be used during the course. This course is based on the current CWNA-109 release and will prepare you for the belonging certification.

Further Information:

For More information, or to book your course, please call us on +1 (800) 268 7737

ilt.customerservice@globalknowledge.com

www.globalknowledge.com/en-ca/

Global Knowledge Network (Canada) Inc., 150 Knowledge Park Drive, Suite 130, Fredericton, NB, E3C 0N9