

Introduction

When you pass the CWNA exam, you earn credit towards the CWNA, CWSP, and CWNE certifications.

This exam measures the candidate's ability to understand the fundamentals of RF behavior and to describe the features and functions of WLAN components. Also tested are the skills needed to install, configure, and troubleshoot WLAN hardware peripherals and protocols.

The skills and knowledge measured by this examination are derived from a survey of wireless networking experts and professionals. The results of this survey were used in weighing the subject areas and ensuring that the weighting is representative of the relative importance of the content.

The following chart provides the breakdown of the exam as to the weight of each section of the exam.

Subject Area	% of Exam
Radio Frequency (RF) Technologies	21%
IEEE 802.11 Regulations and Standards	12%
IEEE 802.11 Protocols and Devices	14%
IEEE 802.11 Network Implementation	21%
IEEE 802.11 Network Security	16%
IEEE 802.11 RF Site Surveying	16%
Total	100%

Radio Frequency (RF) Technologies – 21%

1.1. RF Fundamentals

1.1.1. Define and explain the basic concepts of RF behavior

- Gain
- Loss
- Reflection
- Refraction
- Diffraction
- Scattering
- VSWR
- Return Loss
- Amplification
- Attenuation
- Absorption
- Wave propagation
- Free Space Path Loss
- Delay Spread

1.2. RF Mathematics

1.2.1. Understand and apply the basic components of RF mathematics

- Watt
- Milliwatt
- Decibel (dB)
- dBm
- dBi
- dBd
- SNR
- RSSI
- System Operating Margin (SOM)
- Fade Margin
- Link Budget
- Intentional Radiator
- Equivalent Isotropically Radiated Power (EIRP)

1.3. RF Signal and Antenna Concepts

1.3.1. Identify RF signal characteristics, the applications of basic RF antenna concepts, and the implementation of solutions that require RF antennas

- Visual LOS
- RF LOS
- The Fresnel Zone
- Beamwidths
- Azimuth & Elevation
- Passive Gain
- Isotropic Radiator
- Polarization
- Antenna Diversity
- Wavelength
- Frequency

- Amplitude
- Phase

1.3.2. Explain the applications of basic RF antenna and antenna system types and identify their basic attributes, purpose, and function

- Omni-directional / Dipole antennas
- Semi-directional antennas
- Highly-direction antennas
- Sectorized antennas
- Multiple Input, Multiple Output (MIMO)

1.3.3. Describe the proper locations and methods for installing RF antennas

- Pole/mast mount
- Ceiling mount
- Wall mount

1.4. RF Antenna Accessories

1.4.1. Identify the use of the following WLAN accessories and explain how to select and install them for optimal performance and regulatory domain compliance.

- Amplifiers
- Attenuators
- Lightning Arrestors
- Mounting Systems
- Grounding Rods/Wires
- Towers, Safety Equipment, and Concerns
- RF Cables
- RF Connectors
- RF Signal Splitters

IEEE 802.11 Regulations and Standards – 12%

2.1. Spread Spectrum Technologies

2.1.1. Identify some of the uses for spread spectrum technologies

- Wireless LANs
- Wireless PANs
- Wireless MANs
- Wireless WANs

2.1.2. Comprehend the differences between, and explain the different types of spread spectrum technologies and how they relate to the IEEE 802.11 standard's PHY clauses

- FHSS
- DSSS
- HR-DSSS
- ERP
- OFDM

2.1.3. Identify the underlying concepts of how spread spectrum technology works

- Modulation
- Coding

2.1.4. Identify and apply the concepts which make up the functionality of spread spectrum technology

- Co-location
- Channel Centers and Widths
- Carrier Frequencies
- Dwell time & Hop time
- Throughput vs. Data Rate
- Bandwidth
- Communication Resilience

2.2. IEEE 802.11 Standard (as amended)

2.2.1. Identify, explain, and apply the frame and frame exchange sequences covered by the IEEE 802.11 standard (as amended).

2.2.2. Identify and apply regulatory domain requirements

2.2.3. IEEE 802.11 CSMA/CA

2.3. IEEE 802.11 Industry Organizations and Their Roles

2.3.1. Define the roles of the following organizations in providing direction, cohesion, and accountability within the WLAN industry

- Regulatory Domain Governing Bodies
- IEEE
- Wi-Fi Alliance

IEEE 802.11 Protocols and Devices – 14%

3.1. IEEE 802.11 Protocol Architecture

3.1.1. Summarize the processes involved in authentication and association

- The IEEE 802.11 State Machine
- Open System Authentication, Shared Key Authentication, and Deauthentication
- Association, Reassociation, and Disassociation

3.1.2. Define, describe, and apply the following concepts associated with WLAN service sets

- Stations and BSSs
- Starting and Joining a BSS
- BSSID and SSID
- Ad Hoc Mode and IBSS
- Infrastructure Mode and ESS
- Distribution System (DS)
- Distribution System Media
- Layer 2 and Layer 3 Roaming

3.1.3. Explain and apply the following power management features of WLANs

- Active Mode

- Power Save Mode
- WMM Power Save (U-APSD)
- TIM/DTIM/ATIM

3.2. IEEE 802.11 MAC & PHY Layer Technologies

3.2.1. Describe and apply the following concepts surrounding WLAN frames

- IEEE 802.11 Frame Format vs. IEEE 802.3 Frame Format
- Layer 3 Protocol Support by IEEE 802.11 Frames
- Terminology Review: Frames, Packets, and Datagrams
- Terminology Review: Bits, Bytes, and Octets
- Terminology: MAC & PHY
 - MSDU
 - MPDU
 - PSDU
 - PPDU
- Jumbo frame support (Layer 2)
- MTU discovery and functionality (Layer 3)

3.2.2. Identify methods described in the IEEE 802.11 standard for locating, joining, and maintaining connectivity with an IEEE 802.11 WLAN

- Active Scanning (Probes)
- Passive Scanning (Beacons)
- Dynamic Rate Switching

3.2.3. Define, describe, and apply IEEE 802.11 coordination functions and channel access methods and features available for optimizing data flow across the RF medium

- DCF and HCF coordination functions
- EDCA channel access method
- RTS/CTS and CTS-to-Self protocols
- Fragmentation

3.3. WLAN Infrastructure and Client Devices

3.3.1. Identify the purpose of the following WLAN infrastructure devices and describe how to install, configure, secure, and manage them

- Autonomous Access Points
- Lightweight Access Points
- Enterprise WLAN Switches/Controllers
- Remote Office WLAN Switches/Controllers
- PoE Injectors and PoE-enabled Ethernet Switches
- WLAN Bridges
- Residential WLAN Gateways
- Enterprise Encryption Gateways
- WLAN Mesh Routers

3.3.2. Describe the purpose of the following WLAN client devices and explain how to install, configure, secure, and manage them

- PC Cards (ExpressCard, CardBus, and PCMCIA)
- USB, CF, and SD Devices

- PCI and Mini-PCI Cards

IEEE 802.11 Network Implementation – 21%

4.1. IEEE 802.11 Network Design, Implementation, and Management

4.1.1. Identify technology roles for which WLAN technology is appropriate and describe implementation of WLAN technology in those roles

- Corporate data access and end-user mobility
- Network extension to remote areas
- Building-to-building connectivity - Bridging
- Last-mile data delivery – Wireless ISP
- Small Office / Home Office (SOHO) use
- Mobile office networking
- Educational / Classroom use
- Industrial – Warehousing and Manufacturing
- Healthcare – Hospitals and Offices
- Hotspots – Public Network Access
- Power-over Ethernet (PoE) (IEEE 802.3-2005, Clause 33)
 - Formerly known as IEEE 802.3af

4.2. IEEE 802.11 Network Troubleshooting

4.2.1. Identify and explain how to solve the following WLAN implementation challenges using features available in enterprise class WLAN equipment.

- System throughput
- Co-channel and adjacent-channel interference
- RF Noise and noise floor
- Narrowband and wideband RF interference
- Multipath
- Hidden nodes
- Near/Far
- Weather

IEEE 802.11 Network Security – 16%

5.1. IEEE 802.11 Network Security Architecture

5.1.1. Identify and describe the strengths, weaknesses, appropriate uses, and appropriate implementation of the following IEEE 802.11 security-related items:

- Pre-RSNA Security
 - WEP-40 and RC4
 - WEP-104 and RC4
 - Open System Authentication
 - Shared Key Authentication
- RSNA Security
 - IEEE 802.11, Clause 8
 - TKIP and RC4
 - CCMP and AES
 - IEEE 802.1X Authentication and Key Management (AKM)
 - Preshared Key (PSK) / Passphrase Authentication

- Certificates and PACs
- The 4-Way Handshake
- Key Hierarchies
- Transition Security Network (TSN)
- AAA Security Components
 - EAP types
 - RADIUS
 - LDAP Compliant/Compatible
 - Local Authentication Database

5.1.2. Describe the following types of WLAN security attacks, and explain how to identify and prevent them where possible

- Eavesdropping
- Denial of Service (physical and data link attacks)
- Man-in-the-middle
- Management Interface Exploits
- Encryption Cracking
- Authentication Cracking
- Hijacking

5.1.3. Describe, explain, and illustrate the appropriate applications for the following client-related wireless security solutions

- Role-based Access Control
- IPSec VPN
- Profile-based firewalls
- Captive Portals / Web Authentication
- Network Access Control (NAC)

5.1.4. Describe, explain, and illustrate the appropriate applications for the following WLAN system security and management features

- Rogue AP and client detection and/or containment
- SNMPv3 / HTTPS / SSH2

5.2. IEEE 802.11 Network Security Analysis and Troubleshooting

5.2.1. Identify the purpose and features of the following wireless analysis systems and explain how to install, configure, integrate, and manage them as applicable

- Handheld and Laptop protocol analyzers
- RF spectrum analyzers
- Distributed Wireless Intrusion Prevention Systems (WIPS)
- Distributed RF Spectrum Analyzers

5.3. IEEE 802.11 Network Security Policy Basics

5.3.1. Describe the following General Security Policy elements

- Risk Assessment
- Impact Analysis
- Security Auditing

5.3.2. Describe the following Functional Security Policy elements

- Baseline Practices
- Design and Implementation Practices
- Physical Security
- Social Engineering
- Monitoring, Response, and Reporting

IEEE 802.11 RF Site Surveying – 16%

6.1. IEEE 802.11 Network Site Survey Fundamentals

- 6.1.1. Explain the importance and processes involved in conducting a complete manual RF site survey
- 6.1.2. Explain the importance of and the processes involved in documenting manual RF site surveys
 - Gathering business requirements
 - Interviewing managers and users
 - Defining security requirements
 - Gathering site-specific documentation
 - Documenting existing network characteristics
 - Gathering permits and zoning requirements
 - Indoor- or Outdoor-specific information
 - Outdoor WLANs versus Mesh Networks
- 6.1.3. Explain the technical aspects and information collection procedures involved in manual and virtual RF site surveys
 - Interference sources
 - Infrastructure connectivity and power requirements
 - RF coverage requirements
 - Data capacity requirements
 - Voice Considerations
 - Client connectivity requirements
- 6.1.4. Describe site survey reporting procedures for manual and virtual RF site surveys
 - Customer reporting requirements
 - Reporting methodology
 - Graphical documentation
 - Hardware recommendations and bills of material

6.2. IEEE 802.11 Network Site Survey Systems and Devices

- 6.2.1. Identify the equipment, applications, and system features involved in performing virtual site surveys
 - Predictive analysis / simulation applications (also called RF planning tools)
 - Integrated virtual site survey features of WLAN switches/controllers
 - Site survey verification tools and/or applications
 - Indoor site surveys versus outdoor site surveys
- 6.2.2. Identify the equipment and applications involved in performing manual site surveys
 - Site survey hardware kits
 - Active site survey tools and/or applications
 - Passive site survey tools and/or applications
 - Manufacturer's client utilities