

Introduction

The highlighted areas in this document are the differences between the CWNA exam PW0100 v3 and the new PW0104 (to be released on November 3rd, 2008)

When you pass the CWNA exam, you earn credit towards the 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	17%
IEEE 802.11 Protocols and Devices	17%
IEEE 802.11 Network Implementation	17%
IEEE 802.11 Network Security	10%
IEEE 802.11 RF Site Surveying	18%
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
- Simple Antenna Diversity
- MIMO Diversity
- Radio Chains

- Spatial Multiplexing (SM)
- Transmit Beam Forming (TxBF)
- Maximal Ratio Combining (MRC)
- Wavelength
- Frequency
- Amplitude
- Phase

1.3.2. Explain the applications of physical 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

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 – 17%

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 802.11-2007 standard's (as amended and including 802.11n-draft2.0) PHY clauses

- DSSS
- HR-DSSS
- ERP

- OFDM
- HT (MIMO)

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 (all PHYs)
- Primary and Secondary Channels
- Overlapping and Non-Overlapping Channels
- Carrier Frequencies
- Throughput vs. Data Rate
- Bandwidth
- Communication Resilience
- Physical Carrier Sense (CSMA/CA)
- Virtual Carrier Sense (NAV)

2.2. IEEE 802.11-2007 Standard (as amended and including 802.11n-draft2.0)

2.2.1. Identify, explain, and apply the frame types and frame exchange sequences covered by the IEEE 802.11-2007 standard

2.2.2. Identify and apply regulatory domain requirements

- Dynamic Frequency Selection (DFS)
- Transmit Power Control (TPC)
- Available Channels
- Output Power

2.2.3. OSI model layers affected by the 802.11-2007 standard and amendments

2.2.4. Use of ISM and UNII bands in Wi-Fi networks

2.2.5. Supported data rates for each IEEE 802.11-2007 PHY

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 – 17%

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
- Unscheduled Automatic Power Save Delivery (U-APSD)
- WMM Power-Save (WMM-PS)
- Power Save Multi-Poll (PSMP)
- Spatial Multiplexing Power Save (SMPS)
- 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
 - Guard Interval (GI)
 - PSDU
 - PPDU
 - PPDU Formats
 - MSDU
 - MPDU
 - A-MPDU
 - A-MSDU
 - 802.11 Frame Format
 - 802.11 Frame Types
 - Interframe Spaces (RIFS, SIFS, PIFS, DIFS, AIFS, EIFS)
 - Block Acknowledgements
- Jumbo frame support (Layer 2)
- MTU discovery and functionality (Layer 3)

3.2.2. Identify methods described in the IEEE 802.11-2007 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
- HT Dual-CTS Protection
- HT L-SIG Protection
- HT Channel Width Operation (20 MHz, 20/40 MHz, PCO)
- HT Operation Modes (0, 1, 2, 3)
- 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
- Mesh Access Points / Routers
- Enterprise WLAN Controllers
- Remote Office WLAN Controllers
- PoE Injectors (single and multi-port) and PoE-enabled Ethernet Switches
- WLAN Bridges
- Residential WLAN Gateways
- Enterprise Encryption Gateways

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)
- USB2, CF, and SD Devices
- PCI, Mini-PCI, and Mini-PCIe Cards
- Workgroup Bridges

IEEE 802.11 Network Implementation – 17%

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
- Municipal Networks
- Transportation Networks (trains, planes, automobiles)
- Law Enforcement Networks

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 (in SISO and MIMO environments)
- Hidden nodes
- Near/Far
- Weather

4.3. Power over Ethernet (PoE)

4.3.1. IEEE 802.3-2005, Clause 33 (formerly IEEE 802.3af)

4.3.2. Powering HT (802.11n) devices

- Proprietary midspan & endpoint PSEs
- IEEE 802.3at draft midspan & endpoint PSEs

4.4. WLAN Architectures

4.4.1. Define, describe, and implement autonomous APs

- Network connectivity
- Common feature sets
- Configuration, installation, and management
- Advantages and limitations
- QoS and VLANs

4.4.2. Define, describe, and implement WLAN controllers that use centralized and/or distributed forwarding

- Network connectivity
- Core, Distribution, and Access layer forwarding
- Lightweight, mesh, and portal APs
- WLAN profiles
- Multiple BSSIDs per radio
- Scalability
- Intra- and Inter-controller station handoffs
- Configuration, installation, and management
- Advantages and limitations
- Tunneling, QoS, and VLANs

4.4.3. Define, describe, and implement a WNMS that manages autonomous APs, WLAN controllers, and mesh nodes

- Network connectivity
- Common feature sets
- Configuration, installation, and management
- Advantages and limitations

4.4.4. Define, describe, and implement a multiple channel architecture (MCA) network model

- BSSID / ESSID configuration
- Site surveying methodology
- Network throughput capacity
- Co-channel and adjacent channel interference
- Cell sizing (including micro-cell)

4.4.5. Define, describe, and implement a single channel architecture (SCA) network model

- BSSID / ESSID configuration (including Virtual BSSIDs)
- Site surveying methodology
- Network throughput capacity
- Co-channel and adjacent channel interference
- Cell sizing
- Transmission coordination
- Channel stacking

4.4.6. Define and describe alternative WLAN architectures

- WLAN Arrays
- Cooperative Control
- Mesh Networks

IEEE 802.11 Network Security – 10%

5.1. IEEE 802.11 Network Security Architecture

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

- Legacy Security Mechanisms
 - WEP Cipher Suite
 - Open System Authentication
 - Shared Key Authentication
 - MAC Filtering
 - SSID Hiding
- Modern Security Mechanisms
 - WPA- / WPA2-Enterprise
 - WPA- / WPA2-Personal
 - Wi-Fi Protected Setup (WPS)
 - TKIP and CCMP Cipher Suites
 - 802.1X / EAP Framework
 - Preshared Key (PSK) / Passphrase Authentication
- Additional Mechanisms
 - Secure Device Management Protocols (HTTPS, SNMPv3, SSH2)
 - Role Based Access Control (RBAC)

5.2. IEEE 802.11 Network Security Analysis, Performance Analysis, and Troubleshooting

5.2.1. Describe, explain, and illustrate the appropriate applications for the following wireless security solutions

- Wireless Intrusion Protection System (WIPS)
 - Security Monitoring, Containment, and Reporting
 - Performance Monitoring and Reporting

- Troubleshooting and Analysis
- Protocol Analyzers
 - Security and Performance Monitoring
 - Troubleshooting and Analysis

5.3. IEEE 802.11 Network Security Policy Basics

5.3.1. Describe the following General Security Policy elements

- Applicable Audience
- Risk Assessment
- Impact Analysis
- Security Auditing
- Policy Enforcement
- Monitoring, Response, and Reporting
- Asset Management

5.3.2. Describe the following Functional Security Policy elements

- Design and Implementation Best Practices
 - Small Office / Home Office (SOHO)
 - Small & Medium Business (SMB)
 - Enterprise
- Password Policy
- Acceptable Use & Abuse Policy
- Training Requirements
- Physical Security
- Social Engineering

IEEE 802.11 RF Site Surveying – 18%

6.1. IEEE 802.11 Network Site Survey Fundamentals

6.1.1. Explain the importance of and the processes involved in information collection for manual and predictive RF site surveys. (These happen in preparation for an RF site survey)

- Gathering business requirements
- Interviewing managers and users
- Defining physical and data security requirements
- Gathering site-specific documentation
- Documenting existing network characteristics
- Gathering permits and zoning requirements
- Indoor- or Outdoor-specific information
- Identifying infrastructure connectivity and power requirements
- Understanding RF coverage requirements
- Understanding data capacity and client density requirements
- VoWiFi considerations for delay and jitter
- Client connectivity requirements
- Antenna use considerations
- Aesthetics requirements
- Tracking system considerations
- WIPS sensor considerations

6.1.2. Explain the technical aspects involved in performing manual and predictive RF site surveys. (These happen as part of the RF site survey)

- Locating and identifying RF interference sources
- Defining AP and antenna types to be used
- Defining AP and antenna placement locations
- Defining AP output power and channel assignments
- Defining co-channel and adjacent-channel interference
- Testing applications for proper operation

6.1.3. Describe site survey reporting and follow-up procedures for manual and predictive RF site surveys. (These happen after the RF site survey)

- Reporting methodology
- Customer reporting requirements
- Hardware recommendations and bills of material
- Application analysis for capacity and coverage verification

6.2. IEEE 802.11 Network Site Survey Systems and Devices

6.2.1. Identify the equipment, applications, and system features involved in performing predictive site surveys

- Predictive analysis / simulation applications (also called RF planning and management tools)
- Integrated predictive site survey features of WLAN controllers
- Site survey verification tools and/or applications
- Indoor site surveys versus outdoor site surveys

6.2.2. Identify the equipment, applications, and methodologies involved in performing manual site surveys

- Site survey hardware kits
- Spectrum analyzers
- Protocol analyzers
- Active site survey tools and/or applications
- Passive site survey tools and/or applications
- VoWiFi site survey best practices (dB boundaries, antenna use, balanced links)
- Manufacturer's client utilities

6.2.3. Identify the equipment, applications, and methodologies involved in self-managing RF technologies

- Automated RF resource management