

## **Certified Wireless Network Administrator (CWNA)**

- **Course Number:** PW0-100
- **Length:** 5 Day(s)

### **Certification Exam**

This course will help you prepare for the following exam:

- **Exam PW0-100:** Certified Wireless Network Administrator

### **Course Overview**

CWNA (Certified Wireless Network Administrator) is the foundation level wireless LAN certification for the industry standard CWNP Program. CWNA covers a broad range of wireless LAN topics focused on 802.11 wireless technology rather than products of specific vendors.

### **Prerequisites**

No specific prerequisite is required for this course.

### **Audience**

The CWNA course is a starting point for IT professionals who require wireless training and certification.

### **Course Outline**

- Level 1
- Certification Information
- Intro To Wireless
- 2.1 Wireless Lab Standards
- 2.2 Extending Wired Lans
- 2.3 Mobility
- 2.4 Small and Home Offices
- 2.5 Summary
- Radio Frequency
- 3.1 Gain and Reflection
- 3.2 Absorption and VWSR
- 3.3 Antenna Line of Sight
- 3.4 Antenna Gain and EIRP
- 3.5 Radio Frequency Math
- 3.6 Watts and Decibels
- 3.7 Gain and Loss Measurements
- 3.8 Convention Examples
- 3.9 Summary
- Spread Spectrum
- 4.1 RF Bands
- 4.2 Unlicensed Bands
- 4.3 Spread Spectrum
- 4.4 Direct Sequence and Spectrum
- 4.5 DS VS FH

- 4.6 Channel Sets
- 4.7 Summary
- Level 2
- Access Points
  - 1.1 Access Point Modes
  - 1.2 Modular Radio Cards
  - 1.3 Management and Configuration
  - 1.4 Wireless Bridge Modes
  - 1.5 Client Devices
  - 1.6 Configure Client Devices
  - 1.7 Wireless Residential Gateways
  - 1.8 Setup a Client
  - 1.9 Aironet Client Utility
  - 1.10 Summary
- Antennas
  - 2.1 Omni and Semi Directional
  - 2.2 Highly Directional
  - 2.3 Polarization and Gain
  - 2.4 Free Space Path Loss
  - 2.5 Placement and Mounting
  - 2.6 Alignment and Safety
  - 2.7 POE Devices and WLAN Accessories
  - 2.8 Cables, Adapters and Testing
  - 2.9 Summary
- Standards
  - 3.1 Industrial, Scientific and Medical
  - 3.2 P2P and P2MP
  - 3.3 IEEE Standards
  - 3.4 WI-FI 802.11
  - 3.5 Other WLAN Organizations
  - 3.6 Summary
- Level 3
- Network Architecture Overview
  - 1.1 SSID
  - 1.2 Beacons
  - 1.3 Authentication and Association
  - 1.4 802.1X and EAP
  - 1.5 VPN
  - 1.6 Service Sets
  - 1.7 Roaming
  - 1.8 VLANs
  - 1.9 Power Management
  - 1.10 Lab- Ad Hoc Mode
- MAC and Physical Layer
  - 2.1 WLAN and Ethernet Frames
  - 2.2 Control
  - 2.3 Collisions
  - 2.4 Fragmentation
  - 2.5 DRS/NAV
  - 2.6 DCF/PCF
  - 2.7 IFS/SIFS/PIFS
  - 2.8 DIFS/Slot Times

- 2.9 RTS/CTS
- 2.10 Modulation
- Level 4
- Security Overview
- 1.1 WEP
- 1.2 Actual Threats
- 1.3 Encryption Suites
- 1.4 TKIP VS CKIP
- 1.5 WPA
- 1.6 MIC (Michael)
- 1.7 Keys and Key Management
- 1.8 Authentication Methods
- 1.9 802.11 WPA2
- 1.10 WLAN Security Hierarchy
- 1.11 War Driving
- 1.12 War Checking
- 1.13 Inherent Problems with Wireless Networks
- 1.14 New Security Enhancements
- 1.15 Security Policy
- 1.16 Cell Sizing
- 1.17 SSID Wireless DMZ
- 1.18 Lab- Net Slumbler
- 1.19 Lab HOT Spot Def Kit
- 1.20 EAP FAST
- 1.21 RADIUS?TACACS+
- 1.22 AAA/ACS
- 1.23 Summary
- Level 5
- Troubleshooting
- 1.1 Multipath
- 1.2 Hidden Node
- 1.3 Near/Far and Throughout
- 1.4 Throughput Solutions
- 1.5 Interference
- 1.6 Channel and Co/Channel
- 1.7 Summary
- Site Survey
- 2.1 Preparation
- 2.2 Facility
- 2.3 Existing Network
- 2.4 Business requirements
- 2.5 Throughput and Roaming
- 2.6 Site Survey Equipment
- 2.7 Coverage
- 2.8 Documentation
- 2.9 Summary
- 2.10 Course Conclusion