

## CWNA™ – Wireless LAN Administration Course Outline

The Wireless LAN Administration course, whether in an academic format or a 5-day fast-track format, provides the networking professional a complete foundation of knowledge for entering into or advancing in the wireless networking industry. From basic RF theory to link budget math, including topics from troubleshooting to performing a site survey, this course delivers hands on training that will benefit the novice as well as the experienced network professional.

**Audience:** This course targets both novice and experienced networking professionals who wish to gain a solid understanding of wireless networking to complement their knowledge of traditional wired networking.

**Duration:** The Wireless LAN Administration course consists of 40 hours of material, incorporating both lecture and hands-on labs. The class may be taught in a 5-day period, over the course of a semester, or in other variations, depending on the training organization.

**Certification:** This course may be used - and is the ideal track - for preparing students for the CWNA exam (exam PW0-100).

**Prerequisites:** It is recommended that all students have at least a basic knowledge of networking (as exhibited in Net+, CCNA, CNA, or MCP) prior to enrolling in the course.

### Radio Frequency (RF) Fundamentals

- RF behavior and properties
- Principles of antennas
- RF math calculations
- Link budgets and system operating margins

### Spread Spectrum Technologies

- Uses of Spread Spectrum
- Frequency Hopping (FHSS)
- Direct Sequencing (DSSS)
- Orthogonal Frequency Division Multiplexing (OFDM)
- Packet Binary Convolutional Coding (PBCC)
- Comparing DSSS, FHSS, PBCC, and OFDM
- Co-location and throughput analysis
- Chipping code, processing gain, and spreading functions
- Channels, data rates, ranges, and comparisons
- Channel reuse in pure and mixed environments

### Antennas and Accessories

- Omni-directional
- Semi-directional
- Highly-directional
- Determining coverage areas
- Proper mounting and safety
- Performing outdoor/indoor installations
- Power over Ethernet (802.3af and proprietary implementations)
- Cables and connector usage requirements
- Amplifiers, attenuators, lightning arrestors, and splitters
- Fresnel Zones and Free Space Path Loss
- Interference, Fading, and Multipath

### Wireless Network Management

- Authentication, Authorization, and Accounting (AAA) functions
- Bandwidth control
- Wireless Network Management features and products

### Organizations and Standards

- FCC rules
- Frequency ranges and channels
- IEEE 802.11 family of standards
- Wireless LAN organizations
- Proper application of WLANs in distribution and access roles
- Interoperability standards

### 802.11 Network Architecture

- Joining a wireless LAN
- Authentication and association
- Basic Service Sets
- Extended Service Sets
- Independent Basic Service Sets
- Distribution systems
- Roaming in a wireless LAN
- Scanning modes using Beacons and Probe Frames
- Power management features

**Hardware Installation, Configuration, and Management**

- Access points
- Wireless bridges
- Wireless workgroup bridges
- Client devices and accessories
- Residential gateways
- Enterprise gateways
- Wireless LAN switches
- PoE Switches and patch panels
- VoWiFi systems
- Wireless Routers

**Troubleshooting Wireless LANs**

- Multipath
- Hidden node
- Near/Far
- Identifying and resolving interference problems
- Maximizing system throughput
- Maximizing co-location throughput
- Range considerations

**Physical and MAC Layers**

- Differences between wireless and Ethernet frames
- Collision handling and the use of RTS/CTS
- Throughput and dynamic rate selection
- Analysis of DCF mode and the CSMA/CA protocol
- How frame fragmentation works and its affects on throughput

**Wireless LAN Security**

- Analysis of 802.11 security including WEP, WPA, 802.1x/EAP types, and 802.11i
- Available security solutions at Layer2, 3, & 7
- Types of network attacks, and protecting the network from attacks
- Corporate security policies including baseline practices, and common security solutions
- Security recommendations

**Site Surveying**

- Understanding the need for a site survey
- Defining business requirements and justification
- Facility analysis
- Interviewing network management and users
- Identifying bandwidth requirements
- Determining contours of RF coverage
- Documenting installation problems
- Locating interference
- Reporting methodology and procedures
- Understanding specifics of each vertical market
- Understanding the customer's network topology
- Creating appropriate documentation during and after the site survey
- Understanding FCC/FAA rules regarding towers
- Understanding safety hazards
- Using appropriate hardware and software to perform the survey

---

**Hands-on Lab Exercises****Lab 1 - Infrastructure Mode Connectivity**

This exercise demonstrates wireless client devices connecting to an access point. Students configure the access point, wireless stations, and view the association table in the access point in order to understand the process a client goes through to become connected to the network. RF output power is explained and client utilities are viewed to show RF signal quality and strength. Access point features, authentication, association, and encryption are all discussed and demonstrated. 802.11a/b/g technologies are each shown independently to demonstrate channel usage and spread spectrum technologies.

**Lab 2: Infrastructure Mode Throughput Analysis**

This exercise demonstrates the expected throughput achievable from a wireless station to a wired station and a wireless station to a wireless station using FTP and throughput measuring software. The point of this lab is for the student to understand the half-duplex nature of wireless LANs and how the data rate relates to actual throughput in a real-world scenario. Access point frame relay is proven and explained.

---

**Lab 3: Ad Hoc Connectivity & Throughput Analysis**

In this exercise, wireless clients will connect to each other without use of an access point. Beacons and channel configuration in an Ad Hoc environment will be explained and throughput will be analyzed and compared against an infrastructure environment. Use of SSIDs, WEP/WPA, channels, and other connectivity factors will be discussed and demonstrated.

**Lab 4: Cell Sizing and Automatic Rate Selection (ARS) in an Infrastructure Environment**

In this exercise, RF cell sizing and ARS will be demonstrated. Cell sizing is important for seamless connectivity while roaming and for security purposes. ARS is the wireless LAN client's ability to increase or decrease the data rate of the wireless connection in order to maintain optimum connectivity with the access point. Environmental factors will be analyzed. A basic site survey will be performed during this lab exercise using 802.11a/b/g technologies.

**Lab 5: Co-Channel and Adjacent Channel Interference**

In this exercise, the effects of co-channel and adjacent channel interference are demonstrated and explained. Throughput tests using FTP and throughput measurement software are performed using fully-overlapping, partially-overlapping, and non-overlapping channels. Effects are analyzed and compared for DSSS and OFDM environments.

**Lab 6: Rudimentary Security Features**

In this exercise, the security features that are specified in the IEEE 802.11 standard and the new WPA 1.0 interoperability standard are demonstrated in a mobile environment. Wireless clients attempt roaming between access points while using like and different Service Set Identifiers (SSIDs), MAC filters, Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) using Pre-shared Keys (WPA-PSK). Configuration, use, and security issues are discussed, explained, and demonstrated in 802.11a/b/g environments.

**Lab 7: Dynamic WEP Keys and Mutual Authentication using 802.1x/EAP and RADIUS**

The need for wireless security stronger than that which is available in static WEP or WPA-PSK is explained. Port-based access control with EAP authentication is also demonstrated and explained. Cisco's proprietary Lightweight EAP is used with RADIUS for scalability of authentication. The 802.1x/LEAP association process is analyzed and rotating unicast and broadcast keys are explained. User-based authentication is demonstrated and compared to MAC-based authentication used in the 802.11 standard.

**Lab 8: Wireless VPNs using PPTP tunnels and RADIUS**

In this exercise, the access point is the VPN tunnel server and the PPTP VPN client software built into Microsoft Windows is used to establish an encrypted VPN tunnel from the wireless client to the access point. The access point then sends the authentication request to a RADIUS server and a tunnel is established. Use of the PPTP protocol with encryption in a wireless environment is discussed and explained.