

CWNA Wireless Network Administrator

Duration: 5 Days Course Code: CWNA

Overview:

This five-day course is a practical Wireless LAN course covering IEEE 802.11 WLAN technologies, site survey, installation, configuration, support, troubleshooting and security. The course gives experience with equipment from several leading vendors and teaches delegates how to install configure and support equipment from Cisco Systems, Symbol Technologies, Proxim, Orinoco, Colubris Networks, Netgear, Linksys, AirMagnet, WildPackets, Funk Software, Microsoft and more. The site survey labs now provide delegates hands-on experience using AirMagnet's latest site survey tools. Information is also provided on the latest innovations and developments across the complete range of wireless LAN industry vendors. This is a Planet3 Wireless INC course delivered in partnership with a Planet3 Authorised Partner.

Target Audience:

IT professionals and network engineers responsible for installing or supporting 802.11 Wireless networks. IT professionals wanting to progress into the wireless network industry. Network planners, designers and support staff. IT Security staff, managers and auditors.

Objectives:

- Understand and apply the essential concepts of Radio Frequency (RF) technology, including RF planning, RF-related calculations and spread spectrum technologies.
- Understand the fundamental operation of wireless LANs, for effective WLAN problem analysis and troubleshooting.
- Describe the rules governing wireless LANs, to comply with local radio regulations for setup and maintenance of WLANs.
- Correctly install, configure and support wireless NICs, access points, wireless bridges, workgroup bridges, wireless gateways and WLAN antennas from Cisco Systems, Proxim Inc, Orinoco, Colubris Networks and more.
- Secure the transmission of data over a wireless LAN using WEP and Wi-Fi Protected Access (WPA)Secure wireless LANs using VPN tunnelling and encryption techniques including PPTP and IPSec.
- Analyse and troubleshoot WLAN problems in-depth, including RF coverage, multipath, hidden nodes and interference problems
- Work with sophisticated WLAN diagnostic tools such as AirMagnet and WildPackets AiroPeek NX.
- Perform a site survey for the installation of WLANs.
- Understand the insecurities in IEEE 802.11 WLANs.
- Identify the attacks that can occur from network hackers.
- Secure the transmission of data over a wireless LAN using WEP and Wi-Fi Protected Access (WPA)
- Secure wireless LANs using generic 802.1x/EAP on access points from a range of manufacturers. Conduct essential security surveys to assess the presence and vulnerabilities of WLANs.

Prerequisites:

Delegates are required to meet the following prerequisites:

- Good understanding of Ethernet LANs, TCP/IP protocols, IP addressing and practical experience configuring and supporting Microsoft Windows 2000 or Windows XP. Net+, CCNA or MCP qualifications are recommended

Testing and Certification:

Recommended as preparation for exam(s):

- CWNA – PW0-100

Follow-on-Courses:

The following courses are recommended for further study:

- CWSP – Certified Wireless Security Professional
 - CWAP – Certified Wireless Analysis Professional
-

Content:

- Introduction to Wireless LANs
- The Wireless Network industry
- The Wireless LAN market
- Wireless LAN applications
- Wireless terminology
- Radio Frequency (RF) fundamentals
- RF behaviour
- Reflection, Refraction, Diffraction, Scattering and Absorption.
- The Fresnel zone
- Principles of antennas
- Gain and loss
- Understanding dB,dBi,dBd,dBm,
- Understanding power output regulations
- Systems Operating Margin (SOM)
- RF maths calculations.
- Spread Spectrum technologies
- Uses of Spread Spectrum
- Frequency Hopping (FHSS)
- Direct Sequencing (DSSS)
- Barker Coding
- Packet Binary Convolutional Coding
- Orthogonal Frequency Division Modulation (OFDM)
- 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.
- Access Points, Service Sets, and the Distribution System.
- Access Points
- SSID, BSSID, ESS and ESSID.
- Wireless Distribution System (WDS)
- Wireless Domain System (WDS)
- Client devices and accessories
- SOHO networks
- Wireless Residential gateways
- Wireless repeaters
- Power over Ethernet (PoE)
- PoE Switches and patch panels
- Wireless LAN switches
- Wireless Routers
- Enterprise wireless gateways
- VoWiFi systems
- Wireless Bridges
- Point-to-Point bridging
- Point-to-Multipoint bridging
- Increasing bridge link distance
- Bridge link calculations
- Wireless workgroup bridges
- Wireless Ad Hoc Networks
- Ad Hoc WLAN concepts
- The IBSS
- IBSS Process
- IBSS Coalescence Antennas and Accessories
- Omni-directional
- Semi-directional
- Highly-directional
- Determining coverage areas
- Calculating 1FZ Size and Minimum Clearance
- Free Space Path loss (FSPL)
- Free Space Path Loss Calculation
- Co-location and throughput analysis
- Interference
- Common causes of RF Interference
- Fading
- Multipath
- Signal Range
- Delay Spread
- Reducing Reflections
- Site Monitoring tools Wireless network Organisations and Standards
- FCC and ETSi rules for RF.
- Worldwide frequency ranges and channels
- IEEE 802.11 family of standards
- Wireless LAN organizations
- Wi-Fi Alliance standardization
- HomeRF, Bluetooth and Infrared.
- 802.11 Network Architecture
- Joining a wireless LAN
- Authentication
- Open System Authentication
- Shared Key Authentication
- Association
- Beacons
- Passive Scanning
- Active Scanning
- Probe Frames
- Reassociation Process
- Roaming in a wireless LAN
- Inter-Access Point Protocol (IAPP)
- IEEE 802.11f
- Physical and Mac Layers
- Differences between 802.11 wireless and Ethernet frames
- Arbitration
- Carrier Sense
- Acknowledgement.
- Collision handling
- Using RTS/CTS
- Throughput and dynamic rate selection
- Interframe spacing
- Understanding DCF and PCF
- Effects of packet fragmentation
- Setting the Fragmentation Threshold
- 802.11 protocol analysis
- Bandwidth Control, Network Management and AAA
- Bandwidth Control Unit
- Enterprise Wireless Gateways with Bandwidth Management
- Wireless LAN Management Appliances and software
- Placing Wireless LAN Management Devices in the Network
- Authentication, Authorisation and Accounting.
- AAA Server Software and Appliances
- Placing AAA Servers in the Network
- Routers, Gateways, Switches and VoWi-Fi.
- Using Wireless LAN Antenna Switches and bridges
- Wireless LAN VoIP Phones (a.k.a VoWiFi Phones)
- Complete VoIP System with Secure 802.11b mobility
- Cisco Fast Securing Roaming
- Hand-free VoWiFi Communication System (Vocera)
- Troubleshooting Wireless LANs
- Understanding multipath effects.
- Identifying and resolving Hidden nodes
- Identifying and resolving Near/Far issues
- Identifying and resolving interference problems
- Maximizing system and co-location throughput
- Channel re-use for roaming
- Range considerations
- Wireless LAN Security
- Types of network attacks
- Analysis of 802.11 security
- Understanding Wired Equivalence Privacy (WEP)
- Configuring WEP
- The insecurity problems with WEP
- Cracking WEP security
- Understanding access point security
- Practical War Driving
- WLAN Security solutions
- Available Security solutions
- IEEE802.1x
- EAP
- TKIP
- Wi-Fi Protected Access (WPA) v1
- Configuring WPA v1
- Using Cisco LEAP,TKIP,MIC,
- Using RADIUS authentication 802.1x, EAPOL, EAP-TLS, EAP-TTLS, PEAP
- Secure wireless LANs using generic 802.1x/EAP
- Using 802.1x/EAP on Proxim, Symbol, D-Link and Buffalo access points.
- IEEE 802.11i security enhancements
- WLAN Security solutions
- Available Security solutions
- IEEE802.1x, EAP, TKIP
- Wi-Fi Protected Access (WPA) v1
- Configuring WPA v1
- Using Cisco LEAP,TKIP,MIC,
- Using RADIUS authentication 802.1x, EAPOL, EAP-TLS, EAP-TTLS, PEAP
- Secure wireless LANs using generic 802.1x/EAP
- Using 802.1x/EAP on Proxim, Symbol, D-Link and Buffalo access points.
- IEEE 802.11i security enhancements
- Employing Advanced Encryption Standard (AES)
- VPN-based security solutions
- Using VPNs over WLANs:
- Access point-based VPN solutions
- Security regulations
- Protecting the network from attacks

- Proper mounting and safety
- Performing outdoor and indoor installations
- Power over Ethernet (802.3af and proprietary implementations)
- Cables and connector usage requirements
- Amplifiers, attenuators, lightning arrestors and splitters. RF Propagation
- Fresnel Zones

- Describe the components of a simple VOIP system operating over a WLAN.
- Describe problems associated with VOIP over a WLAN
- Wireless Routers
- Using Wireless Routers
- Enterprise Wireless gateway (Vernier Networks)
- Using Enterprise Wireless Gateways
- Wireless LAN Switch System (Trapeze Networks)
- Placing Wireless LAN Switches in the Network
- Wireless Antenna Switch

- Security recommendations RF Site Surveys
- The Administrative perspective
- The Technical Perspective
- Defining business requirements
- Facility analysis
- Interviewing network management and users
- Supporting Voice over WLAN (VoWLAN)
- Identifying bandwidth requirements
- Determining contours of RF coverage
- Documenting installation problems
- Locating Interference
- Site Survey using AirMagnet

Further Information:

For More information, or to book your course, please call us on +971 4 366 4550

training@globalknowledge.ae

www.globalknowledge.ae

Global Knowledge, Dubai Knowledge Village, Block 2A,First Floor, Office F68, Dubai, UAE