

Training: CWNP
CWTS Enterprise Wi-Fi Fundamentals

FORM OF TRAINING	MATERIALS	PRICE	DURATION
Traditional	Hardcopy	785 EUR	2 days
Traditional	CTAB Tablet	885 EUR	2 days
Distance learning	Hardcopy	785 EUR	2 days
Distance learning	CTAB Tablet	785 EUR	2 days

LOCATIONS

Krakow - 5 Tatarska Street, II floor, hours: 9:00 am - 4:00 pm
Warsaw - 17 Bielska Street, hours: 9:00 am - 4:00 pm

TRAINING TERMS

2019-10-28 | 2 days | Warszawa

TRAINING GOALS:

The **Enterprise Wi-Fi Fundamentals** course provides the networking professional a foundation of knowledge for entering into or advancing within the wireless networking industry.

From basic RF theory and regulatory requirements to implementation of WLAN devices, this course focuses on bringing Wi-Fi sales and support professionals up-to-speed on the latest in 802.11 technologies in a practical way.

The expected audience includes Wi-Fi sales professionals, project managers and networkers new to Wi-Fi.

CONSPECT:

- Introduction to Networking
 - Understanding Network Models
 - Understanding Protocols
 - SDUv
 - PDU
 - OSI - The de facto reference model
 - The seven layer model

- Equipment per layer
- Mapping other protocols into the OSI model
- TCP/IP – four layer model
- Wi-Fi Organizations and Standards
 - Regulatory Bodies
 - IEEE
 - Wi-Fi Alliance
 - WLAN Connectivity
 - WLAN Security
 - WLAN QoS & Power-Save
 - IEEE 802.11 Standards
 - Amendments and Drafts
 - 802.11-2007
 - 802.11a/b/g
 - 802.11e/h/i
 - 802.11n Draft
- Wi-Fi Hardware & Software
 - Access Points
 - Lightweight
 - Autonomous
 - WLAN Routers
 - WLAN Bridges
 - WLAN Repeaters
 - WLAN Controllers/Switches
 - Direct-connect APs
 - Distributed-connect APs
 - PoE Infrastructure
 - Midspan
 - Endpoint
 - Client hardware and software
 - Antenna types and uses
- Wi-Fi Security & Compliance
 - 802.11 Legacy Security Methods
 - Encryption – TKIP/CCMP
 - Authentication Passphrases & 802.1X/EAP
 - WPA/WPA2-Personal

- WPA/WPA2-Enterprise
- WPS Pushbutton/ PIN
- Role-Based Access Control (RBAC)
- VPN Security
- Wireless Intrusion
- Protection Systems (WIPS)
- PCI Compliance
- HIPAA Compliance
- Enforcing Compliance
- Wi-Fi Site Surveying
 - Information gathering and reporting
 - Multiple Channel Architecture (MCA) cell planning basics
 - Single Channel Architecture (SCA) cell planning basics
 - Predictive Site Survey
 - Manual Site Survey
 - Passive Survey
 - Active Survey
 - Mesh Access Layers
 - Use of Analyzers
 - Protocol
 - Survey
 - Spectrum
 - Identifying and locating RF interference sources
 - Wi-Fi vs. Non-Wi-Fi
 - Hardware placement limitations
 - Best practices for antenna use
- Wi-Fi Operational Concepts
 - Range, coverage, and capacity
 - Frequencies/channels used
 - Channel reuse and co-location
 - Active and passive scanning
 - Power saving operation
 - Data rates and throughput
 - Dynamic rate selection
 - Authentication and association
 - The distribution system and roaming

- Infrastructure and ad hoc modes
- BSSID and ESSID
- Protection mechanisms
- Applications, Support, and Troubleshooting
 - Installation/configuration of common network typesv
 - Small Office / Home Office (SOHO)
 - Extension of existing networks into remote locations
 - Building-to-building connectivity
 - Public wireless hotspots
 - Mobile office, classroom, industrial, and healthcare
 - Municipal and law-enforcement connectivity
 - Corporate data access and end-user mobility
 - Last-mile data delivery (WISP)
 - Transportation networks
 - Recognize and troubleshoot wireless network problems
 - Decreased throughput
 - Intermittent or no connectivity
 - Weak signal strength
 - Device upgrades
 - Wi-Fi Network Optimization Procedures
 - Infrastructure hardware selection and placement
 - Identifying, locating, and removing sources of interference
 - Client load-balancing
 - Analyzing infrastructure capacity and utilization
 - Multipath and hidden nodes
- Radio Frequency (RF) Fundamentals
 - Units of RF measurements
 - Factors affecting network range and speed
 - Environment
 - Line-of-sight
 - Interference
 - Defining differences between physical layers
 - OFDM
 - HR/DSSS
 - MIMO
- Spread Spectrum Concepts

- OFDM & HR/DSSS channels
- Co-location of HR/DSSS and OFDM systems
- Adjacent-channel and co-channel interference
- WLAN / WPAN co-existence
- CSMA/CA operation half duplex
- RF Antenna Concepts
 - Passive gain
 - Beam widths
 - Simple diversity
 - Polarization
 - Antenna Mounting
 - Pole/mast mount
 - Ceiling mount
 - Wall mount
 - WLAN Accessories
 - RF cables
 - RF connectors
 - Lightning arrestors and grounding rods

Workshop

- AP/Client Connectivity with WPA2-Personal Security and PoE Power
- Spectrum Analysis of RF Environment
- Protocol Analysis of RF Environment
- Configuration Parameter Modification in an Enterprise-Class Autonomous AP

REQUIREMENTS:

This is a foundation course - no initial knowledge is required, however it is much better for students to know at least basic concepts of networking and radio communications.

Difficulty level



CERTIFICATE:

This course helps prepare for **CWTS exam** PW0-070 available at VUE test centers (www.vue.com/cwnp).

The **CWTS certification** validates the knowledge of enterprise WLAN sales and support professionals who must be familiar and confident with the terminology and basic functionality of enterprise 802.11

wireless networks.

The exam contains 60 multiple/single choice questions. Passing score is 70%.

TRAINER:

Authorized CWNP Trainer.

ADDITIONAL INFORMATION:

Course language depends on participants choice while original materials are in English.