PROGRAMMA CWNP Certified Wireless Network Administrator (CWNA-109)

40 ore

Parts I: Radio Frequency (RF) Technologies

- Define and explain the basic characteristics and behavior of RF
- Apply the basic concepts of RF mathematics and measurement
- Identify RF signal characteristics as they relate to antennas
- Explain and apply the functionality of RF antennas, antenna systems, and accessories available

Parts II: WLAN Regulations and Standards

- Explain the roles of WLAN and networking industry organizations
- Explain and apply the various Physical Layer (PHY) solutions of the IEEE 802.11-2020 standard and amendments including supported channel widths, spatial streams, and data rates
- Understanding spread spectrum technologies, Modulation and Coding Schemes (MCS)
- Identify and apply 802.11 WLAN functional concepts
- Describe the OSI and TCP/IP model layers affected by the 802.11-2020 standard and amendments
- Identify and comply with regulatory domain requirements and constraints
- Explain basic use case scenarios for 802.11 wireless networks

Parts III: WLAN Protocols and Devices

- Describe the components and functions that make up an 802.11 wireless service set
- Define terminology related to the 802.11 MAC and PHY
- Identify and explain the MAC frame format

- Identify and explain the purpose of the three main 802.11 frame types
- Explain the process used to locate and connect to a WLAN
- Explain 802.11 channel access methods
- Explain 802.11 MAC operations
- Describe features of, select, and install WLAN devices, control, and management systems

Parts IV: WLAN Network Architecture and Design Concepts

- Describe and implement Power over Ethernet (PoE)
- Define and describe differences, advantages and constraints of the different wireless LAN architectures
- Describe basic design considerations for common deployment scenarios in wireless such as coverage requirements, roaming considerations and throughput
- Demonstrate awareness of common proprietary features in wireless networks
- Determine and configure required network services supporting the wireless network

Parts V: WLAN Network Security

- Identify weak security options that should not be used in enterprise WLANs
- Identify and configure effective security mechanisms for enterprise WLANs
- Understand basic concepts of WPA3 and Opportunistic Wireless Encryption (OWE) and enhancements over WPA2
- Describe common security options and tools used in wireless networks

Parts VI: RF Validation and WLAN remediation

- Verify and document that design requirements are met including coverage, throughput, roaming, and connectivity with a post-implementation validation survey
- Locate and identify sources of RF interference

- Perform application testing to validate WLAN performance
- Understand and use the basic features of validation tools
- Describe and apply common troubleshooting tools used in WLANs
- Identify and troubleshoot common wireless issues