CWT-100 Objectives

The Certified Wireless Technician (CWT) is an individual who can install APs based on a design document, configure the AP for initial operations and ensure connectivity. The individual can troubleshoot basic problems and assist users in-person or through remote communications in problem resolution. The ability to configure a WLAN client for connectivity is paramount with an understanding of the configuration process for SSIDs, security settings and other client adapter settings. This individual is not responsible for WLAN design, analysis or security design; however, the CWT should be able to gather information from a design specification document to properly configure an AP and troubleshoot individual connection issues. The CWT may not be aware of the actual WLAN architectural design, the RF design or the full feature set in use to implement the WLAN.

Knowledge Domain	Percentage
Basic RF Characteristics	15%
WLAN Client Features and Capabilities	25%
WLAN AP Features and Capabilities	25%
Configuration of 802.11 Security Parameters	15%
Troubleshooting Common WLAN Connection Issues	20%

1.0 Basic RF Characteristics (15%)

1.1 Describe RF signal characteristics
- 1.1.1 Frequency
- 1.1.2 Amplitude
- 1.1.3 Phase
- 1.1.4 Wavelength

1.2 Explain RF behaviors and signal propagation
- 1.2.1 Gain and loss
- 1.2.2 Reflection
- 1.2.3 Refraction
- 1.2.4 Scattering
- 1.2.5 Diffraction
- 1.2.6 Absorption
- 1.2.7 Free space path loss

1.3 Understand how to detect RF signal factors
- 1.3.1 Wi-FI scanner tools
- 1.3.2 Client signal strength reports

1.3.3 RSSI vs. dBm
1.3.4 Output power vs. received signal strength

1.4 Create basic RF channel plans
1.4.1 Available 2.4 GHz channels
1.4.2 Available 5 GHz channels
1.4.3 Regulatory constraints on channel selection
1.4.4 Best practices for channel selection
1.4.5 Co-Channel Interference (CCI)

1.5 Describe the basic differences among antenna types
1.5.1 Omnidirectional
1.5.2 Semi-directional
1.5.3 Highly directional
1.5.4 Antenna mounting kits

1.6 Select the appropriate external antenna when required
1.6.1 Antenna pattern charts
1.6.2 Antenna cables and connectors
1.6.3 Passive antenna gain

2.0 WLAN Client Features and Capabilities (25%)

2.1 Describe client types and varying capabilities
2.1.1 Laptops
2.1.2 Tablets
2.1.3 Mobile phones
2.1.4 Desktops
2.1.5 Specialty devices (video cameras, Wi-Fi peripheral connections, printers, IoT, etc.)

2.2 Explain the basic WLAN location processes
2.2.1 Passive scanning
2.2.2 Active scanning

2.3 Describe the basic steps required in the WLAN connection process
2.3.1 Authentication
2.3.2 Association
2.3.3 802.1X/EAP authentication

2.3.4 4-way handshake

2.4 Determine the channels and streams supported by client devices
- 2.4.1 2.4 GHz channels
- 2.4.2 5 GHz channels
- 2.4.3 Channel widths
- 2.4.4 Number of spatial streams (1x1, 2x2, 3x3, etc.)

2.5 Configure client devices
- 2.5.1 Configure client drivers for optimum performance (band preference, roaming threshold, regulatory domain, etc.)
- 2.5.2 Configure various client operating systems for wireless connectivity
  - 2.5.2.1 Windows
  - 2.5.2.2 Mac OS
  - 2.5.2.3 Chrome OS
  - 2.5.2.4 Linux
  - 2.5.2.5 Tablets and mobile phones (iOS and Android)

3.0 WLAN AP Features and Capabilities (25%)

3.1 Identify AP features and capabilities and understand configuration options related to them
- 3.1.1 PHY support
- 3.1.2 Single-band vs. dual-band
- 3.1.3 Output power control
- 3.1.4 Operational modes
- 3.1.5 Multiple-SSID support
- 3.1.6 Guest access
- 3.1.7 Security features
- 3.1.8 Management interfaces (web-based, CLI, remote CLI)
- 3.1.9 Internal and external antennas
- 3.1.10 PoE support

3.2 Select appropriate mounting kits for a specified installation location
- 3.2.1 Wall mount
- 3.2.2 Pole/mast mount
- 3.2.3 Ceiling mount

3.3 Ensure proper PoE provisioning when required
- 3.3.1 Power levels required
- 3.3.2 PoE switches
- 3.3.3 PoE injectors
- 3.3.4 Testing power availability

3.4 Configure APs as standalone devices
- 3.4.1 Admin account credentials
- 3.4.2 Administration interfaces
- 3.4.3 Wireless network profiles
- 3.4.4 Security parameters, including authentication, authorization and encryption

3.5 Validate AP wired interface connectivity
- 3.5.1 IP configuration
- 3.5.2 Internet access
- 3.5.3 Infrastructure service access
- 3.5.4 Appropriate Ethernet switch port settings

3.6 Validate proper AP WLAN configuration
- 3.6.1 Client connectivity
- 3.6.2 Accurate security settings
- 3.6.3 Client throughput performance

4.0 Configuration of 802.11 Security Parameters (15%)

4.1 Understand the basics of 802.11 standard security solutions
- 4.1.1 WPA vs. WPA2
- 4.1.2 Personal vs. Enterprise
- 4.1.3 Pre-Shared Key
- 4.1.4 802.1X/EAP
- 4.1.5 Common EAP methods

4.2 Identify legacy security technologies that should not be used
- 4.2.1 WEP
- 4.2.2 Shared Key Authentication
- 4.2.3 Hidden SSIDs
- 4.2.4 MAC filtering

4.3 Configure security parameters in an AP
- 4.3.1 Pre-Shared Key
- 4.3.2 RADIUS server
- 4.3.3 802.1X/EAP
- 4.3.4 WPA-WPA2

4.4 Configure security parameters in a client device
- 4.4.1 Pre-Shared Key
- 4.4.2 802.1X/EAP
- 4.4.3 WPA/WPA2

5.0 Troubleshooting Common WLAN Connection Issues (20%)

5.1 Troubleshoot connectivity problems
- 5.1.1 Configuration errors
- 5.1.2 Interference
- 5.1.3 Poor signal strength
- 5.1.4 Driver issues
- 5.1.5 Supplicant issues
- 5.1.6 Feature incompatibility

5.2 Troubleshoot performance problems
- 5.2.1 Configuration errors
- 5.2.2 Interference
- 5.2.3 Low data rates
- 5.2.4 Co-channel interference (CCI)

5.3 Troubleshoot security problems
- 5.3.1 Configuration errors
- 5.3.2 Incorrect passphrases
- 5.3.3 Incompatible EAP methods

5.4 Troubleshoot mobility problems
- 5.4.1 Configuration errors
- 5.4.2 Improper network settings
- 5.4.3 Unsupported fast roaming methods
- 5.4.4 Non-implemented roaming features