CWTS-102 Objectives

The Certified Wireless Technology Specialist (CWTS) is an individual who installs and configures Wi-Fi hardware based on the IEEE 802.11 standard and amendments. The individual understands the fundamental concepts related to Wi-Fi networks and can install, mount, configure, and validate equipment for effective network operations. The CWTS may work in organizations as an installation technician, a support professional, an administrator, or a configuration specialist, among other roles.

To acquire the CWTS certification, candidates must pass the CWTS exam offered through the CWNP learning management system. Exam vouchers may be purchased in the CWNP store at www.CWNP.com. The CWTS-102 exam tests your knowledge against five knowledge domains as documented in Table 1.1 and requires a passing score of 70 percent with 60 total questions offered in 90 minutes. The CWTS candidate should understand the knowledge domains before taking the exam. The CWTS-102 objectives follow.

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

Table 1.1: CWTS-102 Exam Knowledge Domains

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 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 Understand basic RF channel plans

- 1.4.1 Available channels by protocol
- 1.4.2 Regulatory constraints on channel selection
- 1.4.3 Best practices for channel selection
- 1.4.4 Co-Channel Interference (CCI) and Co-Channel Contention (CCC)

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 Use 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 Wireless Client Features and Capabilities (25%)

2.1 Describe device 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 for 802.11 wireless networks

- 2.2.1 Passive scanning
- 2.2.2 Active scanning

2.3 Describe the basic steps required in the WLAN connection process for 802.11 wireless networks

- 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 RF features supported by client and Wi-Fi-based IoT devices

- 2.4.1 Supported channels
- 2.4.2 Channel widths
- 2.4.3 Transmit power
- 2.4.4 Receive sensitivity

2.5 Configure client and Wi-Fi-based IoT devices

- 2.5.1 Configure client drivers for optimum performance (band preference, roaming threshold, regulatory domain, etc.) for 802.11 devices
    - ▪ Configure various client operating systems for wireless connectivity
        - ▪ Windows
        - ▪ Mac OS
        - ▪ Chrome OS
        - ▪ Linux
        - ▪ Tablets and mobile phones (iOS and Android)
- 2.5.2 Configure various Wi-Fi-based IoT devices based on the supported protocol
    - ▪ Provisioning
    - ▪ Network join
    - ▪ Security

3.0 Wireless AP Features and Capabilities (25%)

3.1 Identify 802.11 AP features and capabilities and understand configuration options related to them

- 3.1.1 PHY and frequency band 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 Use 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 for 802.11 APs and other wireless devices, when required

- 3.3.1 Power levels required
- 3.3.2 PoE switches
- 3.3.3 PoE injectors
- 3.3.4 Testing power availability

4.0 Configuration of Security Parameters (15%)

4.1 Understand the basics of 802.11 standard security solutions

- 4.1.1 WPA vs. WPA2 vs. WPA3
- 4.1.2 Personal vs. Enterprise
- 4.1.3 6 GHz security requirements
- 4.1.4 Pre-Shared Key

- 4.1.5 802.1X/EAP
- 4.1.6 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 Understand the basic security options available for common Wi-Fi-based IoT devices

5.0 Troubleshooting Common Wireless 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
- 5.3.4 Incorrect network keys
- 5.3.5 Incorrect join keys

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