CWSS-102 Objectives

The Certified Wireless Sales Specialist (CWSS) is an individual who recommends, selects, promotes, or justifies a wireless local area network (WLAN) solution. The CWSS understands the fundamental concepts related to Wi-Fi networks based on the IEEE 802.11 standard and amendments. This individual can determine the proper solution for an organization based on needs and requirements. The CWSS may work in sales, marketing, consulting, and management roles, among others.

To acquire the CWSS certification, candidates must pass the CWSS exam offered through the CWNP learning management system. Exam vouchers may be purchased in the CWNP store at www.CWNP.com. The CWSS-102 exam tests your knowledge against four 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 CWSS candidate should understand the knowledge domains before taking the exam. The CWSS-102 objectives follow.

Knowledge Domain	Percentage
Define Basic RF Characteristics	15%
Describe Wireless Networking Features and Functions	30%
Identify Wireless Hardware and Software	30%
Understand Organizational Goals	25%

Table 1.1: CWSS-102 Exam Knowledge Domains

1.0 Define Basic RF Characteristics (15%)

1.1 Define RF characteristics

1.1.1 RF waves
1.1.2 Amplitude
1.1.3 Frequency
1.1.4 Wavelength

1.2 Define basic RF behaviors

- 1.2.1 Reflection
- 1.2.2 Absorption
- 1.2.3 Signal strength

1.3 Define antenna types

- 1.3.1 Omnidirectional
- 1.3.2 Semi-directional
- 1.3.3 Highly directional
- 1.3.4 Internal vs. external

2.0 Define Wireless Networking Features and Functions (30%)

2.1 Know the frequency bands used by common wireless protocols

- 2.1.1 Sub-1 GHz
- 2.1.2 2.4 GHz
- 2.1.3 5 GHz
- 2.1.4 6 GHz
- 2.1.5 Above 7 GHz

2.2 Describe Physical Layer (PHY) characteristics

- 2.2.1 Data rates
- 2.2.2 Channel widths
- 2.2.3 Multiple Input/Multiple Output

2.3 Define channels

- 2.3.1 Channel widths
- 2.3.2 Channel designators (numbers)

2.4 Describe factors impacting wireless network performance

- 2.4.1 Coverage or link requirements
- 2.4.2 Capacity requirements
- 2.4.3 Required features
- 2.4.4 Poor configuration and implementation

2.5 Explain the basic security solutions used

- 2.5.1 Authentication and key management
- 2.5.2 Encryption

3.0 Identify Wireless Hardware and Software (30%)

3.1 Identify AP and controller features and capabilities
- 3.1.1 Routing
- 3.1.2 Security
- 3.1.3 Network management
- 3.1.4 Connection interfaces
- 3.1.5 Device management solutions
- 3.1.6 Internal and external antennas
- 3.1.7 PoE support

3.2 Describe wireless network management systems
- 3.2.1 Autonomous
- 3.2.2 Controller
- 3.2.3 Wireless Network Management System (WNMS)
- 3.2.4 Cloud
- 3.2.5 Custom or third-party management systems

3.3 Determine capabilities of client or IoT stations and devices
- 3.3.1 Protocol support
- 3.3.2 Power provisioning
- 3.3.3 Sensor support
- 3.3.4 Security options
- 3.3.5 Mobile vs. stationary

3.4 Describe when Power over Ethernet (PoE) should be used

3.5 Describe the basic requirements for voice over wireless networks
- 3.5.1 Latency
- 3.5.2 Jitter
- 3.5.3 Signal strength

4.0 Understand Organizational Goals (25%)

4.1 Understand issues in common vertical markets for Wi-Fi
- 4.1.1 Standard Enterprise Offices
- 4.1.2 Healthcare
- 4.1.3 Hospitality

- 4.1.4 Conference Centers
- 4.1.5 Education
- 4.1.6 Government
- 4.1.7 Retail
- 4.1.8 Industrial
- 4.1.9 Emergency Response
- 4.1.10 Temporary Deployments
- 4.1.11 Small Office/Home Office (SOHO)
- 4.1.12 Public Wi-Fi

4.2 Identify information sources related to existing networks

- 4.2.1 Network diagrams
- 4.2.2 Wi-Fi implementations
- 4.2.3 Neighbor networks
- 4.2.4 Available network services
- 4.2.5 PoE availability

4.3 Discover coverage/link and capacity needs from a functional perspective

- 4.3.1 Define coverage areas
- 4.3.2 Define capacity zones
- 4.3.3 Define link requirements

4.4 Discover client devices, spcialty devices, and applications in use

- 4.4.1 Laptops, tablets, mobile phones, desktops, and specialty devices
- 4.4.2 Real-time applications
- 4.4.3 Standard applications (e-mail, web browsing, database access, etc.)
- 4.4.4 Data-intensive applications (file downloads/uploads, cloud storage, cloud backup, etc.)
- 4.4.5 Additional specialty devices (door locks, cameras, healthcare devices, etc.)

4.5 Determine the need for outdoor coverage networks and bridge links

- 4.5.1 Bridge link distance and required throughput
- 4.5.2 Outdoor areas requiring coverage
- 4.5.3 Use cases for outdoor access

4.6 Define security constraints

- 4.6.1 Regulatory
- 4.6.2 Industry standards and guidelines
- 4.6.3 Organizational policies

4.7 Discover use cases and access types

- 4.7.1 Authorized users
- 4.7.2 Onboarded guest access
- 4.7.3 Public Wi-Fi

4.8 Match organizational goals to WLAN features and functions