CWS-101 Objectives

The Certified Wireless Specialist (CWS) is an individual who can explain basic features and capabilities of wireless solutions including APs, controllers, coordinators, gateways, wireless management solutions and networks. The individual can assist in selecting the best equipment for a deployment or communicate well with those who are responsible for such decisions. The individual is not responsible for the configuration and management of the wireless connections but must have the ability to gather information to determine requirements and match technologies to those requirements for a deployment.

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

Understand Basic RF Characteristics (15%)

1.1 Identify RF characteristics
- 1.1.1 RF waves
- 1.1.2 Amplitude
- 1.1.3 Frequency
- 1.1.4 Wavelength

1.2 Explain basic RF behaviors
- 1.2.1 Reflection
- 1.2.2 Absorption
- 1.2.3 Signal strength

1.3 Understand antenna types
- 1.3.1 Omnidirectional
- 1.3.2 Semi-directional
- 1.3.3 Highly directional
- 1.3.4 Internal vs. external

Identify 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 Identify Physical Layer (PHY) characteristics
  - 2.2.1 Data rates
  - 2.2.2 Channel widths and center frequencies
- 2.3 Select appropriate channels
  - 2.3.1 Channel selection best practices
  - 2.3.2 Common channel selection mistakes
- 2.4 Identify 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

Identify Wireless Hardware and Software (30%)

- 3.1 Identify APs, coordinators, gateways, 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 Cloud
  - 3.2.4 Custom or third-party management systems
- 3.3 Determine capabilities of network client or IoT 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 Identify when Power over Ethernet (PoE) should be used
- 3.5 Understand the basic requirements for voice over wireless networks
  - 3.5.1 Latency

- 3.5.2 Jitter
- 3.5.3 Signal strength

3.6 Determine the best solution for BYOD and guest access in wireless LANs

- 3.6.1 User provisioning
- 3.6.2 Captive portals
- 3.6.3 Device and software control solutions

Understand Organizational Goals (25%)

4.1 Understand issues in common vertical markets

- 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 IoT network implementations
- 4.2.4 Neighbor networks
- 4.2.5 Available network services
- 4.2.6 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, IoT 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 IoT sensors
- 4.4.6 IoT actuators

4.5 Determine the need for outdoor coverage networks, outdoor IoT connections, 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
- 4.5.4 Outdoor IoT connectivity options

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
- 4.7.4 Monitoring and control (IoT devices)

4.8 Match organizational goals to wireless network features and functions