

Introduction

When you pass the Wireless LAN Analysis Exam, you earn credit towards the CWAP certification.

This exam measures your ability to understand the frame structures and exchange processes for each of the 802.11 series of standards and how to use the tools that are available for analyzing and troubleshooting today's wireless LANs.

The skills and knowledge measured by this examination are derived from a survey of wireless networking professionals and analyzer product manufacturers from around the world. The results of this survey were used in weighing the subject areas and ensuring that the weighting is representative of the relative importance of the content.

The following chart provides the breakdown of the exam as to the weight of each section of the exam.

Wireless LAN Analysis Subject Area	% Of Exam
802.11 MAC Frames and Exchange Processes	42%
802.11 Physical Layer Technologies	20%
802.11 Wireless LAN Protocol Analyzer Use and Trace Interpretation	38%
Total	100%

802.11 MAC Frames and Exchange Processes – 42%

- 1.1. Distinguish the intended purpose of each 802.11 MAC layer frame type
 - 1.1.1. Control frames
 - 1.1.2. Management frames
 - 1.1.3. Data Frames
- 1.2. Explain the structure of each 802.11 MAC layer frame type
 - 1.2.1. MAC Layer terminology used in the 802.11 series of standards
 - 1.2.2. Header fields and subfields
 - 1.2.3. Control, Management, and Data frame payload contents and sizes
 - Fixed fields
 - Information elements
 - 1.2.4. Frames sizes
 - 1.2.5. MAC layer addressing
 - 1.2.6. Modifications for 802.11e
- 1.3. Explain and describe the frame exchange processes involved in:
 - 1.3.1. Authentication and Association
 - 1.3.2. Disassociation, Reassociation, and Deauthentication
 - 1.3.3. Active and Passive Scanning
 - 1.3.4. Roaming within an ESS
 - 1.3.5. Power Management mode operation
 - 1.3.6. Fragmentation
 - 1.3.7. 802.11b/g mixed mode environments and protection mechanisms
 - 1.3.8. Security mechanisms
 - WEP
 - WPA / WPA2 / 802.11i
 - 802.1x/EAP
- 1.4. Contrast the differences between the frame exchange processes in:
 - 1.4.1. Infrastructure vs. Independent Service Sets
 - 1.4.2. PCF vs. DCF access methods

802.11 Physical Layer Technologies – 20%

- 2.1. Explain PHY Layer terminology used in the 802.11 series of standards
- 2.2. Explain Interframe Spacing
 - 2.2.1. SIFS
 - 2.2.2. PIFS
 - 2.2.3. DIFS
 - 2.2.4. EIFS
- 2.3. Explain Slot Times
 - 2.3.1. 802.11a
 - 2.3.2. 802.11b
 - 2.3.3. 802.11g
 - 2.3.4. Special operation in 802.11b/g mixed mode environments
- 2.4. Explain 802.11 Contention (DCF Mode)
 - 2.4.1. CSMA/CA (half duplex)
 - 2.4.2. Backoff timer operation
 - 2.4.3. Virtual Carrier Sense (NAV)
 - 2.4.4. Physical Carrier Sense (CCA)
 - 2.4.5. Contention Window operation
- 2.5. Describe the PLCP Sublayer (802.11a/b/g)
 - 2.5.1. Purpose
 - 2.5.2. Preambles and Headers for each PHY
 - 2.5.3. Payloads
- 2.6. Describe the PMD Layer

802.11 Wireless LAN Protocol Analyzer Use and Trace Interpretation – 38%

- 3.1. Demonstrate appropriate application of an 802.11a/b/g protocol analyzer for:
 - 3.1.1. Troubleshooting
 - 3.1.2. Performance testing
 - 3.1.3. Security analysis
 - 3.1.4. Intrusion analysis
 - 3.1.5. Distributed analysis

- 3.2. Interpret 802.11a/b/g protocol traces when performing:
 - 3.2.1. Troubleshooting
 - 3.2.2. Performance testing
 - 3.2.3. Security analysis
 - 3.2.4. Intrusion analysis

- 3.3. Apply generic features common to most 802.11a/b/g protocol analyzers (not limited to those listed)
 - 3.3.1. Protocol decodes
 - 3.3.2. Peer map functions
 - 3.3.3. Conversation analysis
 - 3.3.4. Expert functions