WLAN

The Wireless Local Area Network Consortium

802.11 Base
AP MAC Layer Test Suite
Version 3.5

Technical Document

Last Updated: February 18, 2012

Wireless LAN Consortium
InterOperability Laboratory
University of New Hampshire

121 Technology Drive, Suite 2
Durham, NH 03824
Phone: +1-603- 862-2263
Fax: +1-603- 862-4181
http://www.iol.unh.edu/consortiums/wireless/

MODIFICATION RECORD

- February 18, 2012 – Version 3.5
  Jackson Corson: Updated references to 2012 standard
- September 15, 2009 – Version 3.4.1
  Anthony Murabito: Updated CTS-to-Self recognition to contain a proper value for the duration field included within the frame.
- November 25, 2008 – Version 3.4
  Daniel Reynolds: 1.1.2 – Added MSDU12 to part b. 1.1.8 – Updated MSDU9-42 to the new selection of MSDU9-16. 1.1.9 – Added commas to the observable results to make clearer that we mean the ACK times. 1.1.13 – Changed MPDU1, 2s, 1r to MSDUs. 1.2.2 – Fixed part a. with respect to the numbering. 1.2.3 – Added reference of 7.1.3.1.7 and in part c. the listen interval. 1.2.5 – Changed the DUT to TS in parts c and f.
- August 2007 – Version 3.3
  Anthony Murabito: Minor editorial changes. Moved Duplicate Detection and Recovery to Group 1. Also made modifications to tests 1.1.11 and 1.1.12
- June 2007 – Version 3.2
  Jonathan Zink: Changed Std references to IEEE Std 802.11™-2007
- August 22, 2006 – Version 3.1
  Anthony Murabito/Jonathan Zink: Added Test#1.1.11 ERP Protection Mechanism Validation and Test#1.1.12 Information Element Formatting
- July 16, 2006 – Version 3.0
  Anthony Murabito/Jonathan Zink: Test Suite Expansion. Separated out all test cases and renamed appropriately. Moved all state machine testing to new Test #1.1.8. State Variables and Services. Modified MAC Level Acknowledgement to include duration field validation. Combined RTS/CTS procedure and Directed MPDU Transfer. Added Test # 1.2.3 Broadcast and Multicast MPDU Transfer. Clarified observable results for Test #1.2.4 Duplicate Detection and Recovery. Added Test #1.2.5 Directed MSDU Fragmentation. Added Test #1.2.7 Defragmentation using RTS/CTS. Removed Pad Bits test from Test #1.3.1 WEP Decryption Procedure. Redesigned and enhanced Test #1.3.2 Aging Function to base all aging off of listen intervals. Added Test #1.3.3 PS-Poll Processing. Added Test #1.3.4 Defragmentation Using WEP.
- June 1, 2006 – Version 2.5
  Jonathan Zink: Minor script and procedural updates.
- November 22, 2005 – Version 2.4
  Chris Kane: Made default key #1 in Test #1.3.1 to work better with STAs that support only 1 WEP Key.
- August 29, 2005 – Version 2.3
  Chris Kane: Minor script and procedural updates.
- May 9, 2005 – Version 2.2
  Matt Newcomb: Procedural corrections
- April 20, 2005 – Version 2.1
  Procedures and observable results were updated to reflect changes in the IEEE 802.11 standard, along with editorial and technical modifications where appropriate.
- February 2005 - Version 2.0 Released
  Matt Newcomb: Renumbered tests, updated procedures and observable results.
- January 2003- Version 1.1 Released
- January 2001- Version 1.0 Released

ACKNOWLEDGMENTS

The University of New Hampshire would like to acknowledge the efforts of the following individuals in the development of this test suite.

Jackson Corson	University of New Hampshire
Ajay Dassu	University of New Hampshire
Chris Kane	University of New Hampshire
Kevin Karcz	University of New Hampshire
Matt Newcomb	University of New Hampshire
Chris Polanec	University of New Hampshire
Justin Rebe	University of New Hampshire
Jonathan Zink	University of New Hampshire
Anthony Murabito	University of New Hampshire
Daniel Reynolds	University of New Hampshire

INTRODUCTION

Overview
The University of New Hampshire's InterOperability Laboratory (UNH-IOL) is an institution designed to improve the interoperability of standards based products by providing an environment where a product can be tested against other implementations of a standard. This particular suite of tests has been developed to help implementers evaluate the functionality of the MAC layer of their 802.11 Wireless LAN APs.

These tests are designed to determine if a product conforms to specifications defined in the IEEE Std 802.11™-2012 Edition. Successful completion of all tests contained in this suite does not guarantee that the tested device will operate with other devices. However, combined with satisfactory operation in the IOL's interoperability test bed, these tests provide a reasonable level of confidence that the device under test (DUT) will function properly with the MAC layer of other devices.

Organization of Tests
The tests contained in this document are organized to simplify the identification of information related to a test and to facilitate in the actual testing process. Each test contains an identification section that describes the test and provides cross-reference information. The discussion section covers background information and specifies why the test is to be performed. Tests are grouped in order to reduce setup time in the lab environment. Each test contains the following information:

Test Number
The Test Number associated with each test follows a simple grouping structure. Listed first is the Test Group Number followed by the test's number within the group. This allows for the addition of future tests to the appropriate groups of the test suite without requiring the renumbering of the subsequent tests.

Purpose
The purpose is a brief statement outlining what the test attempts to achieve. The test is written at the functional level.

References
The references section lists cross-references to the IEEE 802.11 standards and other documentation that might be helpful in understanding and evaluating the test results.

Resource Requirements
The requirements section specifies the test hardware and/or software needed to perform the test. This is generally expressed in terms of minimum requirements, however in some cases specific equipment manufacturer/model information may be provided.

Last Modification
This specifies the date of the last modification to this test.

Discussion
The discussion covers the assumptions made in the design or implementation of the test, as well as known limitations. Other items specific to the test are covered here.

Test Setup
The setup section describes the initial configuration of the test environment. Small changes in the configuration should be included in the test procedure.

Procedure
The procedure section of the test description contains the systematic instructions for carrying out the test. It provides a cookbook approach to testing, and may be interspersed with observable results.

Observable Results
This section lists the specific observables that can be examined by the tester in order to verify that the DUT is operating properly. When multiple values for an observable are possible, this section provides a short discussion on how to interpret them. The determination of a pass or fail outcome for a particular test is often based on the successful (or unsuccessful) detection of a certain observable.

Possible Problems
This section contains a description of known issues with the test procedure, which may affect test results in certain situations. It may also refer the reader to test suite appendices and/or whitepapers that may provide more detail regarding these issues.

TABLE OF CONTENTS

GROUP 1: DEFAULT CONFIGURATION

Scope:
This group of tests pertains to the operation of the MAC layer authentication and association state machine, MPDU formats, and processing of received MPDUs.

Overview:
The following tests cover MAC layer operation specific to the configuration of the DUT where the beacon interval is 100 ms, the DTIM interval is 3 beacons, fragmentation and RTS are disabled, and without encryption. Also, there is to be an Ethernet STA with a static IP address on the same DS as the AP, which is capable of receiving and responding to ICMP Echo Requests as well as ARP Requests.

Test #1.1.1: Frame Processing

Purpose: To verify that the DUT processes the reception of MAC frames properly.

References:

[1] IEEE Std 802.11™-2012 Edition, Clause 8, Subclause 10.3.5.3, Annex J.5

Resource Requirements:

- A testing STA (TS) that is capable of transmitting user defined MAC frames and does not participate in the MAC protocol
- A monitor configured for capturing and analyzing MAC frames
- An Ethernet STA (STA-E) on the DS that is capable of receiving and responding to ICMP Echo Requests

Last Updated: June 2007

Discussion: This test verifies that the DUT properly handles MAC layer frames that it receives, while properly processing the received frame by continuing the frame exchange sequence. It also verifies that the DUT can operate upon reception of an unexpected or incorrectly formatted frame, testing the robustness of the DUT. It is assumed the data rate that frames are transmitted at is not a factor in this test other than in the calculation of the duration field.

Test Setup: Place the DUT, TS, and sniffer in a RF isolated environment and in range of each other. Place STA-E on the same DS as the DUT.

Table 1 - Test Frame(s)

Frame Label	Description
MSDU1	A valid ICMP Echo Request to STA-E with a Frame Control field Protocol Version greater than 0
MSDU2a-b	Control frames of reserved subtypes = [0000, 1001], and length = 20-bytes
MSDU3	Data frame with a zero-byte payload. This is not a null data frame
MSDU4	Data frame with WEP bit set, correct ICV and FCS with a 1-byte payload
MSDU5	A 500-byte ICMP Echo Request to STA-E with the ToDS bit unset, address 1 field value of the DUT's MAC address, and address 3 field value of a MAC address for a STA that is not in the BSS
MSDU6	Data frame with a length that is less than 64-bytes and ToDS bit set
MSDU7	ICMP Echo Request with both ToDS and FromDS bits set
MSDU8a-j	Management frames of reserved subtypes = [0110, 0111, 1101, 1110, 1111], and length = 28-bytes. One set with a zero-byte payload and another set with a random data payload
MSDU9a-b	Data frames of reserved subtypes=[1000, 1100], with a frame body of 2-bytes
MSDU10	Unfragmented ICMP Echo Request with payload of 2000-bytes to STA-E
MSDU11	A probe request with an SSID element with a length that is greater than 32-bytes
MSDU12a-l	Frames of Type=Reserved, subtypes=[0000, 0001, 0010, 0100, 1000, 1111], and length = 30-bytes. One set with a zero-byte payload and another set with a random data payload

Procedure:

Parts a: Non-acknowledged frames

1. Instruct the TS to authenticate and associate with the DUT.
2. Instruct the TS to transmit MSDU1-MSDU2b to the DUT.
3. After the test frame is transmitted, instruct the TS to transmit a valid ICMP Echo Request to the STA-E to ensure the DUT is operational.
4. For all cases, observe transmissions from the DUT.

Parts b: Acknowledged frames

1. Instruct the TS to authenticate and associate with the DUT.
2. Instruct the TS to transmit MSDU3-MSDU11 to the DUT.
3. After the test frame is transmitted, instruct the TS to transmit a valid ICMP Echo Request to the STA-E to ensure the DUT is operational.
4. For all cases, observe transmissions from the DUT.

Parts c: Reserved frames

1. Instruct the TS to authenticate and associate with the DUT.
2. Instruct the TS to transmit MSDU12a-l to the DUT.
3. After the test frame is transmitted, instruct the TS to transmit a valid ICMP Echo Request to the STA-E to ensure the DUT is operational.
4. For all cases, observe transmissions from the DUT.

Observable Results:

The DUT should:

a. not transmit an ACK for MSDU1-MSDU2b, but it should receive the frame without any system failures.
b. transmit an ACK for MSDU3-MSDU11 and receive the frame without any system failures.
c. receive MSDU12a-l without any system failures. The DUT may or may not transmit an ACK upon reception.

Possible Problems: None.

Test #1.1.2: Null Data Processing

Purpose: To verify that the DUT operates properly upon reception of Null Data frames.

References:

[1] IEEE Std 802.11™-2012 Edition, Subclauses 8.2.4.1, 8.3.2, 9.3.2.2

Resource Requirements:

- A testing STA (TS) that is capable of transmitting user defined MAC frames and does not participate in the MAC protocol
- A monitor configured for capturing and analyzing MAC frames
- An Ethernet STA (STA-E) on the DS that is capable of receiving and responding to ICMP Echo Requests

Last Updated: November 2008

Discussion: APs and STAs must have the ability to operate properly upon reception of null frames with specific bits set in the Frame Control field, which consists of the following subfields: Protocol Version, Type, Subtype, To DS, From DS, More Fragments, Retry, Power Management, More Data, WEP, and Order.

Test Setup: Place the DUT, TS, and sniffer in a RF isolated environment and in range of each other. Place STA-E on the same DS as the DUT.

Table 2 - Test Frame(s)

Frame Label	Description
MSDU1	Null data frame with all Frame Control field bits set, except the FromDS bit
MSDU2	Null data frame with the Protocol Version field set to 1
MSDU3	Null data frame with invalid FCS
MSDU4	Null data frame with no Frame Control field bits set
MSDU5	Null data frame with the More Fragment field bit set
MSDU6	Null data frame with the Retry field bit set
MSDU7	Null data frame with the Power Management field bit set
MSDU8	Null data frame with the More Data field bit set
MSDU9	Null data frame with the WEP field bit set, without an IV and ICV expanded WEP frame body
MSDU10	Null data frame with the WEP field bit set and an 8-byte payload
MSDU11	Null data frame with the WEP field bit set and a 9-byte payload
MSDU12	Null data frame with the Order field bit set

Procedure:

Part a: Non-Acknowledged Frames

1. Instruct the TS to authenticate and associate with the DUT.
2. Instruct the TS to transmit MSDU1-MSDU3 to the DUT.
3. After each test frame is transmitted, instruct the TS to transmit a valid ICMP Echo Request to STA-E with a unique ICMP sequence number to the DUT to ensure the DUT is operational.
4. If the DUT deauthenticates or disassociates the TS during any part of the test, instruct the TS to authenticate and associate with the DUT again.
5. Observe transmissions from the DUT.

Part b: Acknowledged Frames

1. Instruct the TS to authenticate and associate with the DUT.
2. Instruct the TS to transmit MSDU4-11 to the DUT.
3. After each test frame is transmitted, instruct the TS to transmit a valid ICMP Echo Request to STA-E with a unique ICMP sequence number to the DUT to ensure the DUT is operational.
4. If the DUT deauthenticates or disassociates the TS during any part of the test, instruct the TS to authenticate and associate with the DUT again.
5. Observe transmissions from the DUT.

Observable Results:

The DUT should:

a. not transmit an ACK in response to MSDU1-MSDU3, but should transmit an ACK followed by an ICMP Echo Response following every valid ICMP Echo Request.

b. transmit an ACK in response to MSDU4-MSDU12, and also should transmit an ACK followed by an ICMP Echo Response following every valid ICMP Echo Request.

Possible Problems: None.

Test #1.1.3: Deauthentication Processing

Purpose: To verify that the DUT processes deauthentication frames properly.

References:

[1] IEEE Std 802.11™-2012 Edition, Subclauses 10.3, 4.5, 8.4.1.7, 9.3.2.2, Annex J [auth_rsp2b(2)]

Resource Requirements:

- A testing STA (TS) that is capable of transmitting user defined MAC frames and does not participate in the MAC protocol
- A monitor configured for capturing and analyzing MAC frames
- An Ethernet STA (STA-E) on the DS that is capable of receiving and responding to ICMP Echo Requests

Last Updated: June 2007

Discussion: Deauthentication is a class 1 management service that invalidates an authentication relationship with a peer MAC entity. This service may be invoked by any authenticated party (STA or AP), and is a notification rather than a request; therefore deauthentication can not be refused by either party. It is possible for a STA to transmit a deauthentication notification to a group address, terminating authentication to all APs at once. Within a BSS, the reception of a deauthentication frame also invalidates an association relationship.

Test Setup: Place the DUT, TS, and sniffer in a RF isolated environment and in range of each other. Place STA-E on the same DS as the DUT.

Table 3 - Test Frame(s)

Frame Label	Description
MSDU1	Deauthentication frame from the TS to the DUT
MSDU2	Broadcast Deauthentication frame from the TS
MSDU3	Deauthentication frame with invalid FCS

Procedure:

Part a: Deauthentication Reason Codes

1. Instruct the TS to authenticate and associate with the DUT.
2. Instruct the STA-E to transmit multiple ICMP Echo Requests to the TS.
3. Instruct the TS transmit MSDU1.
4. Instruct the TS to transmit an ICMP Echo Request to the DUT.
5. Repeat steps 1-4 for each non-reserved reason code, and each reserved reason code.
6. Observe transmissions from the DUT.

Part b: Broadcast Deauthentication

1. Instruct the TS to authenticate and associate with the DUT.
2. Instruct the STA-E to transmit a continuous stream of ICMP Echo Requests to the TS.
3. Instruct the TS to transmit MSDU2.
4. Instruct the TS to transmit an ICMP Echo Request to the DUT.
5. Instruct the TS to transmit MSDU1.
6. Repeat steps 1-5 5 times.
7. Observe transmissions from the DUT.

Part c: Deauthentication with invalid FCS

1. Instruct the TS to authenticate and associate with the DUT.
2. Instruct the STA-E to transmit a continuous stream of ICMP Echo Requests to the TS.
3. Instruct the TS to transmit MSDU3.
4. Instruct the TS to transmit an ICMP Echo Request to the DUT.
5. Instruct the TS to transmit MSDU1.
6. Repeat steps 1-5 5 times.
7. Observe transmissions from the DUT.

Observable Results:

a. The DUT should not transmit any class 2 or 3 traffic to the TS upon reception of MSDU1.
b. INFORMATIVE: Upon reception of MSDU2, [1] is unclear whether or not the frame should be processed. If the DUT processes the frame, then all traffic from the DUT to the TS should cease.
c. The DUT should not transmit an ACK upon reception of MSDU3, nor process the frame.

Possible Problems: None.

Test #1.1.4: Open System Authentication Processing

Purpose: To verify that the DUT properly handles received authentication request frames and generates authentication response frames properly.

References:

[1] IEEE Std 802.11™-2012 Edition, Subclauses 10.3, 4.5, 9.3.2.2, Annex J [auth_rsp2b(2)]

Resource Requirements:

- A testing STA (TS) that is capable of transmitting user defined MAC frames and does not participate in the MAC protocol
- A monitor configured for capturing and analyzing MAC frames
- An Ethernet STA (STA-E) on the DS that is capable of receiving and responding to ICMP Echo Requests

Last Updated: June 2007

Discussion: Open System Authentication is a mandatory algorithm for 802.11 networks. The authentication service allows class 2 traffic to be transferred from one peer MAC entity to another; it is also the first step in becoming part of a BSS network. If and only if a STA has successfully authenticated may it request association, the second step required to join a BSS network. This test is designed to ensure that an AP can properly process received authentication requests, and respond with appropriate authentication responses.

Test Setup: Place the DUT, TS, and sniffer in a RF isolated environment and in range of each other. Place STA-E on the same DS as the DUT.

Table 4 - Test Frame(s)

Frame Label	Description
MSDU1	Deauthentication frame from the TS to the DUT
MSDU2	Authentication Request with invalid transaction sequence number
MSDU3	Authentication Request with invalid authentication algorithm number
MSDU4	Valid Authentication Request from the TS to the DUT
MSDU5	Valid Authentication Request from the TS to the DUT with invalid FCS
MSDU6	Valid Association Request from the TS to the DUT

Procedure:

Part a: Invalid Transaction Sequence Number

1. Instruct the TS to transmit MSDU1.
2. Instruct the TS to transmit MSDU2.
3. Instruct the TS to transmit MSDU6.
4. Observe transmissions from the DUT.

Part b: Invalid Authentication algorithm number

1. Instruct the TS to transmit MSDU1.
2. Instruct the TS to transmit MSDU3.
3. Instruct the TS to transmit MSDU6.
4. Observe transmissions from the DUT.

Part c: Proper Authentication

1. Instruct the TS to transmit MSDU1.
2. Instruct the TS to transmit MSDU4.
3. Instruct the TS to transmit MSDU6.
4. Observe transmissions from the DUT.

Part d: Invalid FCS

1. Instruct the TS to transmit MSDU1.
2. Instruct the TS to transmit MSDU5.
3. Instruct the TS to transmit MSDU6.
4. Observe transmissions from the DUT.

Observable Results:

The DUT should:

a. respond to MSDU2 with an Authentication Response containing an unsuccessful status code, and not associate successfully.
b. respond to MSDU3 with an Authentication Response containing an unsuccessful status code, and not associate successfully.
c. respond to MSDU4 with an Authentication Response containing a successful status code, and also successfully associate.
d. not respond to MSDU5 with an ACK nor process the frame.

Possible Problems: None

Test #1.1.5: Association Processing

Purpose: To verify that the DUT properly handles received association request frames and generates association response frames properly.

References:

[1] IEEE Std 802.11™-2012 Edition, Subclauses 10.3, 4.5, 9.3.2.2

Resource Requirements:

- A testing STA (TS) that is capable of transmitting user defined MAC frames and does not participate in the MAC protocol
- A monitor configured for capturing and analyzing MAC frames
- An Ethernet STA (STA-E) on the DS that is capable of receiving and responding to ICMP Echo Requests

Last Updated: June 2007

Discussion: Association is a service that allows class 3 traffic to be transferred from one peer MAC entity to another. Transmitting an association request is the second and final step in becoming part of a non-secure BSS network. There are many fields within an association request, an AP must be able to properly interpret the contents of these fields, and react appropriately upon reception of such a frame. This test is designed to ensure that an AP can properly process received association requests, and respond with appropriate association responses.

Test Setup: Place the DUT, TS, and sniffer in a RF isolated environment and in range of each other. Place STA-E on the same DS as the DUT. Instruct the STA-E to transmit multiple ICMP Echo Requests to the TS.

Table 5 - Test Frame(s)

Frame Label	Description
MSDU1	Deauthentication from TS to DUT
MSDU2	Valid Authentication Request from TS to DUT
MSDU3-6	Association requests with Listen Intervals 2 through 5
MSDU7	An association request containing two reserved element IDs of length 255-bytes
MSDU8	An association request with more than 8 supported rates (Rates = [1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54])
MSDU9	Valid Association Request from TS to DUT
MSDU10	Association Request from TS to DUT with an invalid FCS
MSDU11	Association Request from TS to DUT with no supported rates

Procedure:

Part a: Listen Intervals 2 through 5

1. Instruct the TS to transmit MSDU1 followed by MSDU2.
2. Instruct STA-E to transmit multiple ICMP Echo Requests to the TS.
3. Instruct the TS transmit MSDU3.
4. Observe transmissions from the DUT.
5. Repeat 2-3 for MSDU4-6.

Part b: Duplicate Reserved Elements

1. Instruct the TS to transmit MSDU1 followed by MSDU2.
2. Instruct the TS to transmit MSDU7.
3. Observe transmissions from the DUT.

Part c: Greater than 8 Supported Rates

1. Instruct the TS to transmit MSDU1 followed by MSDU2.
2. Instruct the TS to transmit MSDU8.
3. Observe transmissions from the DUT.

Part d: Proper Association

1. Instruct the TS to transmit MSDU1 followed by MSDU2.
2. Instruct the TS to transmit MSDU9.
3. Observe transmissions from the DUT.

Part e: Invalid FCS

1. Instruct the TS to transmit MSDU1 followed by MSDU2.
2. Instruct the TS to transmit MSDU10.
3. Observe transmissions from the DUT.

Part f: No Supported Rates

1. Instruct the TS to transmit MSDU1 followed by MSDU2.
2. Instruct the TS to transmit MSDU11.
3. Observe transmissions from the DUT.

Observable Results:

The DUT should:

a. respond to MSDU3-6 with an association response. If successful, the DUT should forward the ICMP Echo Requests from STA-E to the TS. If unsuccessful, the DUT should not forward any class 3 traffic to the TS.
b. respond to MSDU7 with an association response. If successful, the DUT should forward the ICMP Echo Requests from STA-E to the TS. If unsuccessful, the DUT should not forward any class 3 traffic to the TS.
c. respond to MSDU8 with an association response. If successful, the DUT should forward the ICMP Echo Requests from STA-E to the TS. If unsuccessful, the DUT should not forward any class 3 traffic to the TS.
d. respond to MSDU9 with an association response containing a successful status code. Furthermore, the DUT should forward the ICMP Echo Requests from STA-E to the TS.
e. not respond to MSDU10 with an ACK nor process the frame.
f. respond to MSDU11 with an association response containing an unsuccessful status code.

Possible Problems: None.

Test #1.1.6: Disassociation Processing

Purpose: To verify that the DUT properly handles received disassociation frames.

References:

[1] IEEE Std 802.11™-2012 Edition, Subclause 10.3, 8.4.1.7, 9.3.2.2

Resource Requirements:

- A testing STA (TS) that is capable of transmitting user defined MAC frames and does not participate in the MAC protocol
- A monitor configured for capturing and analyzing MAC frames
- An Ethernet STA (STA-E) on the DS that is capable of receiving and responding to ICMP Echo Requests

Last Updated: June 2007

Discussion: Disassociation is a class 2 management service that invalidates strictly an association relationship with a peer MAC entity. This service may be invoked by any authenticated party (STA or AP), and is a notification rather than a request, therefore disassociation can not be refused by either party. It is possible for a STA to transmit a disassociation notice to a group address, terminating association to all APs at once. Reception of a disassociation frame invalidates specifically an association relationship and does not affect the underlying authentication relationship.

Test Setup: Place the DUT, TS, and sniffer in a RF isolated environment and in range of each other. Place STA-E on the same DS as the DUT.

Table 6 - Test Frame(s)

Frame Label	Description
MSDU1	Disassociation frame from the TS to the DUT
MSDU2	Broadcast Disassociation frame from the TS
MSDU3	Disassociation frame from the TS to the DUT with an invalid FCS

Procedure:

Part a: Disassociation Reason Codes

1. Instruct the TS to authenticate and associate with the DUT.
2. Instruct STA-E to transmit multiple ICMP Echo Requests to the TS.
3. Instruct the TS transmit MSDU1.
4. Instruct the TS to transmit an ICMP Echo Request to the DUT.
5. Repeat steps 1-4 for each non-reserved reason code, and once for reason code 0.
6. Observe transmissions from the DUT.

Part b: Broadcast Disassociation

1. Instruct the TS to authenticate and associate with the DUT.
2. Instruct STA-E to transmit multiple ICMP Echo Requests to the TS..
3. Instruct the TS to transmit MSDU2.
4. Instruct the TS to transmit an ICMP Echo Request to the DUT.
5. Instruct the TS to transmit MSDU1.
6. Repeat steps 1-5 5 times.
7. Observe transmissions from the DUT.

Part c: Invalid FCS

1. Instruct the TS to authenticate and associate with the DUT.
2. Instruct STA-E to transmit multiple ICMP Echo Requests to the TS.
3. Instruct the TS transmit MSDU3.
4. Instruct the TS to transmit an ICMP Echo Request to the DUT.
5. Observe transmissions from the DUT.

Observable Results:

a. The DUT should not transmit any class 3 traffic to the TS upon reception of MSDU1.
b. INFORMATIVE: Upon reception of MSDU2, [1] is unclear whether or not the frame should be processed. If the DUT processes the frame, then all class 3 traffic from the DUT to the TS should cease.
c. The DUT should not respond to MSDU3 with an ACK nor process the frame.

Possible Problems: None.

Test #1.1.7: Reassociation Processing

Purpose: To verify that the DUT properly handles received reassociation request frames, and generates reassociation response frames properly.

References:

[1] IEEE Std 802.11™-2012 Edition, Subclause 10.3, 9.3.2.2, 10.3.5.5

Resource Requirements:

- A testing STA (TS) that is capable of transmitting user defined MAC frames and does not participate in the MAC protocol
- A monitor configured for capturing and analyzing MAC frames
- An Ethernet STA (STA-E) on the DS that is capable of receiving and responding to ICMP Echo Requests

Last Updated: June 2007

Discussion: Reassociation is a class 2 management service within a BSS that allows a STA to become associated with an AP, typically an AP that it has previously held a valid association. There are many fields within a reassociation request. An AP must be able to properly interpret the contents of these fields, and react appropriately upon reception of such a frame. This test is designed to ensure that an AP can properly process received reassociation request frames, and respond with appropriate reassociation responses.

Test Setup: Place the DUT, TS, and sniffer in a RF isolated environment and in range of each other. Place STA-E on the same DS as the DUT.

Table 6 - Test Frame(s)

Frame Label	Description
MSDU1	Deauthentication with reason code 1
MSDU2	Valid Authentication Request with transaction sequence number 1
MSDU3	Association Request with rates reflecting those of the DUT
MSDU4	Disassociation with reason code 8
MSDU5	ICMP Echo Request to STA-E
MSDU6	Reassociation Request with rates reflecting those of the DUT
MSDU7	Reassociation Request with a rate set of only 1 or 6 Mbps.
MSDU8	Reassociation Request with a rate set of only 11 or 18 Mbps.
MSDU9	Reassociation Request with an SSID of “incorrect SSID”
MSDU10	Reassociation Request with the Current AP field containing the DUT’s MAC Address
MSDU11	Reassociation Request with the Current AP field containing the TS’s MAC Address
MSDU12	Reassociation Request with an invalid FCS

Procedure:

Part a: Proper Reassociation

1. Instruct the TS to transmit MSDU1.
2. Instruct the TS to transmit MSDU2, and wait for successful authentication response.
3. Instruct the TS to transmit MSDU3, and wait for successful association response.
4. Instruct the TS to transmit MSDU4.
5. Instruct the TS to transmit MSDU6, and wait for a reassociation response.
6. Instruct the TS to transmit MSDU5.

7. Observe transmissions from the DUT.

Part b: Reassociation with Only 1 Mbps or 6 Mbps Supported As Basic

1. Instruct the TS to transmit MSDU1.
2. Instruct the TS to transmit MSDU2, and wait for successful authentication response.
3. Instruct the TS to transmit MSDU3, and wait for successful association response.
4. Instruct the TS to transmit MSDU4.
5. Instruct the TS to transmit MSDU7, and wait for a reassociation response.
6. Instruct the TS to transmit MSDU5.
7. Observe transmissions from the DUT.

Part c: Reassociation with Only 11 Mbps or 54 Mbps Supported As Extended

1. Instruct the TS to transmit MSDU1.
2. Instruct the TS to transmit MSDU2, and wait for successful authentication response.
3. Instruct the TS to transmit MSDU3, and wait for successful association response.
4. Instruct the TS to transmit MSDU4.
5. Instruct the TS to transmit MSDU8, and wait for a reassociation response.
6. Instruct the TS to transmit MSDU5.
7. Observe transmissions from the DUT.

Part d: Reassociation with an Incorrect SSID

1. Instruct the TS to transmit MSDU1.
2. Instruct the TS to transmit MSDU2, and wait for successful authentication response.
3. Instruct the TS to transmit MSDU3, and wait for successful association response.
4. Instruct the TS to transmit MSDU4.
5. Instruct the TS to transmit MSDU9, and wait for a reassociation response.
6. Instruct the TS to transmit MSDU5.
7. Observe transmissions from the DUT.

Part e: Invalid FCS

1. Instruct the TS to transmit MSDU1.
2. Instruct the TS to transmit MSDU2, and wait for successful authentication response.
3. Instruct the TS to transmit MSDU3, and wait for successful association response.
4. Instruct the TS to transmit MSDU4.
5. Instruct the TS to transmit MSDU12.
6. Observe transmissions from the DUT.

Part f: Current AP Field Processing

1. Instruct the TS to transmit MSDU1.
2. Instruct the TS to transmit MSDU2, and wait for successful authentication response.
3. Instruct the TS to transmit MSDU3, and wait for successful association response.
4. Instruct the TS to transmit MSDU4.
5. Instruct the TS to transmit MSDU10.
6. Repeat steps 1-5 using MSDU11.
7. Observe transmissions from the DUT.

Observable Results:

a. The DUT should
   - respond to MSDU6 with a reassociation response with a successful status code.
   - include the non-zero AID assigned to the TS in the reassociation response.
   - set the two MSB of the AID field in the reassociation response.
   - forward the response from STA-E of MSDU5 to the TS.

b. The DUT should
   - respond to MSDU7 with a reassociation response with an unsuccessful status code.

- not transmit any class 3 frames to the TS after receiving MSDU4.

c. The DUT should
   - respond to MSDU8 with a reassociation response with an unsuccessful status code.
   - not transmit any class 3 frames to the TS after receiving MSDU4.

d. The DUT should
   - respond to MSDU9 with a reassociation response with an unsuccessful status code.
   - not transmit any class 3 frames to the TS after receiving MSDU4.

e. The DUT should not transmit an ACK upon reception of MSDU12 nor process the frame.

f. The DUT should respond to MSDU10 and MSDU11 with a reassociation response with a successful status code.

Possible Problems: Since 802.11a devices do not support operation at 1 and 11 Mbps data rates, MSDU7 will advertise 6 Mbps and MSDU8 will advertise 18 Mbps support.

Test #1.1.8: State Variables and Services

Purpose: To verify that

- the DUT maintains which STAs are authenticated and which STAs are associated.
- the DUT does not process class 2 frames from unauthenticated STAs, and responds appropriately.
- the DUT does not process class 3 frames from unassociated STAs, and responds appropriately.
- the DUT is able to respond to Probe Requests in all states.

References:

[1] IEEE Std 802.11™-2012 Edition, Subclause 10.3

Resource Requirements:

- A testing STA (TS) that is capable of transmitting user defined MAC frames and does not participate in the MAC protocol
- A monitor configured for capturing and analyzing MAC frames
- An Ethernet STA (STA-E) on the DS that is capable of receiving and responding to ICMP Echo Requests

Last Updated: November 2008

Discussion: For devices to engage in higher-level communication they must be part of the same BSS. The first part of becoming part of a BSS is authenticating with the AP. After a device has been successfully authenticated the next step to join the BSS is association. In order for the AP to keep track of what class frames it may transmit to a particular STA, each STA is given a state variable. The values for this variable are unauthenticated, authenticated but unassociated, and authenticated and associated. Each value of this variable determines a different state that the STA is currently in for communication with the AP. These three different states determine which class of frames the AP and STA may exchange. If an AP receives a frame that is not allowed by the state relationship, the AP must respond appropriately. This test is designed to ensure that an AP responds appropriately upon reception of such frames.

Test Setup: Place the DUT, TS, and sniffer in a RF isolated environment and in range of each other. Place STA-E on the same DS as the DUT.

Table 7 - Test Frame(s)

Frame Label	Description
MSDU1	Deauthentication frame
MSDU2	Disassociation frame
MSDU3	Valid Authentication request
MSDU4	Valid Association request
MSDU5	Valid Reassociation request
MSDU6	Valid ICMP Echo Request from the TS to STA-E
MSDU7	ARP Request from the TS to STA-E
MSDU8	Probe Request directed to the DUT
MSDU9-16	PS-Poll w/ AID 1-5, 0, 2007, 257

Procedure:

Part a: Class 2 traffic in State 1

1. Instruct the TS to transmit MSDU1 followed by MSDU4.
2. Instruct the TS to transmit MSDU1 followed by MSDU5.
3. Observe transmissions from the DUT.

Part b: Class 3 traffic in State 1

1. Instruct the TS to transmit MSDU1 followed by MSDU6.
2. Instruct the TS to transmit MSDU1 followed by MSDU7.
3. Instruct the TS to transmit MSDU1 followed by MSDU9.
4. Repeat step 3 for MSDU10-16.
5. Observe transmissions from the DUT.

Part c: Class 3 traffic in State 2

1. Instruct the TS to transmit MSDU1.
2. Instruct the TS to transmit MSDU3 and wait for a response.
3. Instruct the TS to transmit MSDU6.
4. Repeat steps 1-2.
5. Instruct the TS to transmit MSDU7.
6. Repeat steps 1-2.
7. Instruct the TS to transmit MSDU1 followed by MSDU9.
8. Repeat steps 6-7 for MSDU10-16.
9. Repeat steps 1-8 after transmitting MSDU1, MSDU3, MSDU4, then MSDU2.
10. Observe transmissions from the DUT.

Part d: Probe Requests in States 1-3

1. Instruct the TS to transmit MSDU1.
2. Instruct the TS to transmit MSDU8.
3. Instruct the TS to transmit MSDU3 and wait for a response.
4. Instruct the TS to transmit MSDU8.
5. Instruct the TS to transmit MSDU4 and wait for a response.
6. Instruct the TS to transmit MSDU8.
7. Observe transmissions from the DUT.

Observable Results:

The DUT should:

a. respond to MSDU4 and MSDU5 with a deauthentication.
b. respond to MSDU6-7, and MSDU9-16 with a deauthentication.
c. respond to MSDU6-7, and MSDU9-16 with a deauthentication or disassociation.
d. respond to MSDU8 with a Probe Response for all transmissions of MSDU8.

Possible Problems: None.

Test #1.1.9: Acknowledgement and Duration Field Validation

Purpose: To verify that the DUT can properly calculate the duration field, and does not transmit an ACK upon reception of frames which do not contain a valid FCS field.

References:

[1] IEEE Std 802.11™-2012 Edition, Subclauses 7.2.1.3, 9.3.2.2, 9.3.2.8, 9.7

Resource Requirements:

- A testing STA (TS) that is capable of transmitting user defined MAC frames and does not participate in the MAC protocol
- A monitor configured for capturing and analyzing MAC frames
- An Ethernet STA (STA-E) on the DS that is capable of receiving and responding to ICMP Echo Requests

Last Updated: November 2008

Discussion: When a directed frame is successfully transmitted from one MAC entity to another, a CRC value is calculated by the receiving station to verify the integrity of the frame, and an acknowledgement frame is transmitted to indicate successful reception to the source station. In the event that the acknowledgement frame is lost (i.e. the ACK is not successfully received), the transmitter should attempt to re-transmit the frame. If a directed frame is successfully received but contains an invalid CRC value, the frame should be discarded. When a directed frame is fragmented each fragment should have a calculated duration field, with the exception of the last fragment (i.e. More Fragments bit is *not* set) which should have a duration field of 0.

Test Setup: Place the DUT, TS, and sniffer in a RF isolated environment and in range of each other.

Table 8 - Test Frame(s)

Frame Label	Description
MSDU1	ICMP Echo Request with a length of 96-bytes to DUT
MSDU2	ICMP Echo Request with a length of 400-bytes to DUT
MSDU3	Data frame with a valid FCS
MSDU4	Data frame with an invalid FCS
MSDU5	CTS frame with a duration of 32767 μs
MSDU6	Data frame with a length of 1500-bytes
MSDU7	ICMP Echo Request with a length of 96-bytes and a SA of a non-authenticated STA to DUT
MPDU8	Data frame with a length of 320-bytes, the More Fragments bit set, a fragment number of 0, and a duration field based off of MSDU5

Procedure:

Part a: Duration Field 0 μs

1. Configure the TS for a fragmentation threshold of 256 bytes.
2. Allow the DUT to authenticate and associate.
3. Instruct the TS to transmit MSDU1.
4. Observe transmissions from the DUT.

Part b: Calculated Duration Field

1. Configure the TS for a fragmentation threshold of 256 bytes.
2. Allow the DUT to authenticate and associate.
3. Instruct the TS to transmit the first fragment of MSDU2.
4. Instruct the TS to transmit the second fragment of MSDU2.
5. Observe transmissions from the DUT.

Part c: Frame Check Sequence Validation

1. Repeat step 1 from Part a.
2. Instruct the TS to transmit MSDU3.
3. Instruct the TS to transmit MSDU4.
4. Repeat steps 2 and 3 a total of 3 times.
5. Observe transmissions from the DUT.

Part d: Large Duration Field Value

1. Repeat step 1 from Part a.
2. Instruct the TS to transmit MSDU5.
3. Instruct the TS to transmit MPDU8.
4. Observe transmissions from the DUT.

Part e: New STA

1. Repeat step 1 from Part a.
2. Instruct the TS to transmit MSDU7.
3. Observe transmissions from the DUT.

Observable Results:
The DUT should:

a. transmit an ACK, for MSDU1, with a duration field of 0 μs.
b. transmit an ACK, for the first fragment of MSDU2, with an appropriate duration field; transmit an ACK, for the second fragment, of MSDU2 with a duration field of 0 μs.
c. transmit ACKs for all transmissions by the TS of MSDU3, not transmit ACKs for all transmissions by the TS of MSDU4.
d. transmit an ACK, for the first fragment of MPDU8, with an appropriate duration field.
e. transmit an ACK for MSDU7.
f. transmit all data frames with appropriate duration fields.

Possible Problems: None.

Test #1.1.10: Defragmentation

Purpose: To verify that the DUT is capable of receiving fragments of an arbitrary length, and is able to reassemble them.

References:

[1] IEEE Std 802.11™-2012 Edition, Subclause 9.2.7, 9.6

Resource Requirements:

- A testing STA (TS) that is capable of transmitting user defined MAC frames and does not participate in the MAC protocol
- A monitor configured for capturing and analyzing MAC frames
- An Ethernet STA (STA-E) on the DS that is capable of receiving and responding to ICMP Echo Requests

Last Updated: June 2007

Discussion: Defragmentation is the process of assembling successfully received fragments back into the original MSDU or MMPDU. Since it is possible for source STAs to transmit fragments of an arbitrary length, destination STAs must be capable of defragmenting fragments of arbitrary length. This test is designed to ensure that an AP can properly reassemble arbitrarily fragmented MSDUs.

Test Setup: Place the DUT, TS, and sniffer in a RF isolated environment and in range of each other. Place STA-E on the same DS as the DUT.

Table 9 - Test Frame(s)

Frame Label	Description
MPDU1	ICMP Echo Request with payload size of 1514-bytes to STA-E

Procedure:

Part a: Various Threshold Defragmentation

1. Instruct the TS to authenticate and associate with the DUT.
2. Instruct the TS to transmit MPDU1, fragmented at varying sizes from 256-bytes to 1456-bytes. After MPDU1 has been transmitted at a fragment size twice, increment the fragment size by 60 and repeat until the fragment size is equal to 1456-bytes.
3. Observe transmissions from the DUT.

Observable Results:

a. The DUT should defragment MPDU1 for all the fragmentation thresholds, forward MPDU1 to STA-E, and forward the ICMP Echo Response to the TS.

Possible Problems: None.

Test #1.1.11: Information Element Formatting

Purpose: To verify that the DUT includes and properly formats Information Elements within beacons, probes and association frames.

References:

[1] IEEE Std 802.11™-2012 Edition, Subclauses 8.3.3.2, 8.3.3.10, 8.4.2.14

Resource Requirements:

- A testing station (TS) that is capable of transmitting user defined MAC frames and does not participate in the MAC protocol.
- A monitor configured for capturing and analyzing MAC frames.

Last Modification: June 2007

Discussion: Information Elements (IEs) are subfields contained within beacons, probe requests, probe responses, association requests and association responses. Each IE is assigned a unique Element Identifier (EID) to distinguish it from the others. Also each IE must follow the format specified within the standard for which it is defined. This test is designed to ensure that a device properly formats IEs defined within [1].

Test Setup: Place the DUT, TS, and sniffer in a RF isolated environment and in range of each other. Place STA-E on the same DS as the DUT. Configure to the DUT to default settings, no encryption, and Domain Capability set to true.

Frame Label	Description
MSDU1	Probe request without the request information element.
MSDU2	Probe request requesting element id 255.
MSDU3	Probe request requesting element ids 0, 1, 2, 4, 7, 3, and 255.
MSDU4	Probe request requesting element ids 0-16, 42, 43, 46, 48,and 50.
MSDU5	Probe request requesting element ids 0-179.
MSDU6	Probe request requesting element ids 180-255.

Procedure:

Part a: Request Information Element Processing

1. Instruct the TS to send MSDU1 to the DUT and wait for a response.
2. Instruct the TS to send MSDU2 to the DUT and wait for a response.
3. Instruct the TS to send MSDU3 to the DUT and wait for a response.
4. Observe transmissions from the DUT.

Part b: Unreserved Element IDs

1. Instruct the TS to send MSDU4 to the DUT and wait for a response.
2. Observe transmissions from the DUT.

Part c: All Element IDs

1. Instruct the TS to send MSDU5 to the DUT and wait for a response.
2. Instruct the TS to send MSDU6 to the DUT and wait for a response.
3. Observe transmissions from the DUT.

Part d: Beacon Information Elements

1. Observe transmissions from the DUT.

Observable Results:

The DUT should:

a-d. properly format any and all supported Information Elements within beacons and Probe Response frames .

Notes:

The DUT should return the supported information elements in ascending order sorted by element id. Section 7.2.3.9 states that request information elements should be returned in the same order as they were requested; also Section 7.3.2.12 states that information elements requested out of order may be ignored as well as subsequent requested information elements.

Possible Problems: None.

Test #1.1.12: CTS-to-self Recognition

Purpose: To verify that the DUT will delay transmission of any non-ACK frame for the time period specified in a CTS-to-self frame.

References:

[1] IEEE Std. 802.11-2012, Clauses 8.3.1.3, 9.3.2.11, 9.8

Resource Requirements:

- A testing station (TS) that is capable of transmitting user defined MAC frames and does not participate in the MAC protocol.
- A monitor configured for capturing and analyzing MAC frames.
- An Ethernet STA (STA-E) on the DS that is capable of receiving and responding to ICMP Echo Requests

Last Modification: August 2006

Discussion: With the addition of the 802.11g specifications to the base standard, ERP STAs are allowed to transmit CTS frames with a RA matching its own MAC address as a protection mechanism for legacy stations. Legacy stations and ERP stations must update their NAV counters with the duration field specified in the CTS frame. Since CTS frames are class 1 frames, a STA does not need to be authenticated or associated in order for the STA to update it's NAV with the duration field.

Test Setup: Place the DUT, TS, and sniffer in a RF isolated environment and in range of each other. Place STA-E on the same DS as the DUT.

Frame Label	Description
MSDU1	CTS-to-self with a duration of 32767µs.

Procedure:

Part a: Duration Processing

1. Instruct the TS to authenticate and associate with the DUT.
2. Instruct STA-E to transmit multiple ICMP Echo Requests to the TS.
3. Instruct the TS to transmit MPDU1 in 100 frame floods, 10 times.

Observable Results:

a. The DUT should not transmit any frames during the CTS flood.

Possible Problems: None.

Test #1.1.13: Duplicate Detection and Recovery

Purpose: To verify that the DUT properly detects and filters duplicate frames.

References:

[1] IEEE Std 802.11™-2012 Edition, Subclause 9.3.2.10

Resource Requirements:

- A testing STA (TS) that is capable of transmitting user defined MAC frames and does not participate in the MAC protocol
- A monitor configured for capturing and analyzing MAC frames
- An Ethernet STA (STA-E) on the DS that is capable of receiving and responding to ICMP Echo Requests

Last Updated: November 2008

Discussion: Due to the design of the MAC layer protocol, it is possible for a STA to successfully receive the same frame or fragment of a frame more than once. Accordingly, duplicate detection and recovery is built into the MAC layer. The primary mechanism to detect duplicates is the sequence and fragment numbers contained in each frame. STAs generate sequence numbers as an incrementing sequence of integers. All STAs should maintain a cache of recently received sequence and fragment numbers from each STA. Whenever a STA receives a frame with a matching source address, sequence number, and fragment number, with the retry bit set, it should discard the frame as a duplicate (but still transmit an ACK). Due to the sequence number field being a modulo 4096 counter, it is possible for a frame to be improperly discarded as a duplicate, although it is highly unlikely.

Test Setup: Place the DUT, TS, and sniffer in a RF isolated environment and in range of each other. Place STA-E on the same DS as the DUT.

Table 10 - Test Frame(s)

Frame Label	Description
MSDU1	ICMP Echo Request with a 1000-byte payload.
MSDU1r	MSDU1 with the retry bit set and same Sequence Number as MSDU1.
MSDU2s	MSDU1r with a different Source Address.
MSDU2ss	MSDU1r with a different Source Address than MSDU2s and MSDU1r.
MSDU2sq	MSDU1r with a different Source Address and Sequence Number.
MSDU2sr	MSDU1r with a different Source Address and the retry bit unset.
MSDU2sqr	MSDU1r with a different Source Address, Sequence Number and retry bit unset.
MSDU2q	MSDU1r with a different Sequence Number.
MSDU2qr	MSDU1r with a different Sequence Number and retry bit unset.
MSDU2r	MSDU1r with the retry bit unset.
MSDU3	ICMP Echo Request with a 1000-byte payload.
MPDU3a	Fragment 0 of MSDU3.
MPDU3b	Fragment 1 of MSDU3.
MPDU3br	Fragment 1 of MSDU3 with the retry bit set.
MPDU3c	Fragment 1 of MSDU3 with the retry bit set and different frame body (of same length) than MPDU3b.
MSDU4	ICMP Echo Request with a 1000-byte payload.

Procedure:

Part a: Positive Duplicate Detection

1. Instruct the TS to authenticate and associate with the DUT.
2. Instruct the TS to transmit MSDU1 followed by MSDU1r.
3. Instruct the TS to transmit MPDU3a, MPDU3b, and MPDU3c with a 2 * SIFS + ACK time in between each MPDU.
4. Observe transmissions from the DUT.

Part b: Negative Duplicate Detection

1. Repeat steps 1 from Part a.
2. Instruct the TS to transmit MSDU1 followed by MSDU2s.
3. Instruct the TS to transmit MSDU1 followed by MSDU2sq.
4. Instruct the TS to transmit MSDU1 followed by MSDU2sr.
5. Instruct the TS to transmit MSDU1 followed by MSDU2sqr.
6. Instruct the TS to transmit MSDU1 followed by MSDU2q.
7. Instruct the TS to transmit MSDU1 followed by MSDU2qr.
8. Instruct the TS to transmit MSDU1 followed by MSDU2r.
9. Instruct the TS to transmit MPDU3a followed by MPDU3br with a 2 * SIFS + ACK time in between each MPDU.
10. Instruct the TS to transmit MSDU1 followed by MSDU2s, and MSDU2ss.

Observable Results:

a. The DUT should
   - use the same sequence number in the sequence control for all MPDUs that make up the same MSDU.
   - use an incrementing sequence number for all transmitted frames.
   - acknowledge and forward MSDU1 to STA-E and forward the ICMP Echo Response to the TS.
   - acknowledge but not forward MSDU1r to STA-E nor forward an ICMP Echo Response to the TS.
   - acknowledge MPDU3a, MPDU3b, MPDU3c and forward the frame composed of MPDU3a and MPDU3b to STA-E and the ICMP Echo Response to the TS.

b. The DUT should
   - use the same sequence number in the sequence control for all MPDUs that make up the same MSDU.
   - use an incrementing sequence number for all transmitted frames.
   - acknowledge and forward each MSDU to STA-E and forward the ICMP Echo Response to the TS.

Possible Problems: None

GROUP 2: RTS AND FRAGMENTATION

Scope:
This group of tests pertains to the operation of the MAC layer transmission and usage of RTS/CTS exchanges as well as fragmentation of MSDUs.

Overview:
The following tests cover MAC layer operation specific to the configuration of the DUT with various combinations of RTS thresholds and fragmentation thresholds. In addition to the RTS and fragmentation thresholds, other configuration values for the DUT are the beacon interval is 100 ms, the DTIM interval is 3 beacons, and without encryption. Also, there is to be an Ethernet STA with a static IP address on the same DS as the AP, which is capable of receiving and responding to ICMP Echo Requests as well as ARP Requests.

Test #1.2.1: Recovery Procedure and Retransmit Limits

Purpose: To verify that the DUT properly increments and resets the appropriate retry counters, and sets the Retry Bit in all retransmitted MSDUs.

References:

[1] IEEE Std 802.11™-2012 Edition, Subclause 9.3.4.4

Resource Requirements:

- A testing STA (TS) that is capable of transmitting user defined MAC frames and does not participate in the MAC protocol
- A monitor configured for capturing and analyzing MAC frames
- An Ethernet STA (STA-E) on the DS that is capable of receiving and responding to ICMP Echo Requests

Last Updated: June 2007

Discussion: Each MSDU should have its own short retry counter (SRC) and long retry counter (LRC), and the STA must also keep a separate STA short retry counter (SSRC) and STA long retry counter (SLRC). When the DUT does not successfully transmit a frame (i.e. receives no CTS in response to RTS, or ACK in response to data frame), it should increment the SSRC or SLRC and the SRC or LRC for the MSDU. The counter used is dependent on whether the frame exceeds dot11RTSThreshold. Whenever a directed frame is successfully transmitted, the SSRC or SLRC and either the SRC or LRC is reset to 0. A STA should stop retrying a frame once the MPDU's SRC has reached dot11ShortRetryLimit, or the MSDU's LRC has reached dot11LongRetryLimit. [1] recommends that 7 and 4 be used for dot11ShortRetryLimit and aLongRetryLimit respectively.

Test Setup: Place the DUT, TS, and sniffer in a RF isolated environment and in range of each other. Place STA-E on the same DS as the DUT.

Table 11 - Test Frame(s)

Frame Label	Description
MSDU1	ICMP Echo Request with a frame length of 512-bytes to STA-E
MSDU2	ICMP Echo Request with a frame length of 1500-bytes to STA-E

Procedure:

Part a: RTS Retries (SRC)

1. Disable encryption on the DUT. If possible set the fragmentation threshold to 2346-bytes and set the RTS threshold to 512-bytes.
2. Instruct the TS to authenticate and associate with the DUT.
3. Instruct the TS to transmit MSDU2 to the DUT.
4. When the DUT responds with an RTS, do not allow the TS to transmit a CTS in response.
5. Observe transmissions from the DUT.

Part b: Data Frame Retries (LRC)

1. Repeat steps 1 - 3 from Part a.
2. Observe transmissions from the DUT.

Part c: Data Frame Retries (SRC)

1. Repeat steps 1 - 2 from Part a.
2. Instruct the TS to transmit MSDU1 to the DUT.
3. When the DUT transmits an ICMP Echo Response, do not allow the TS to transmit an ACK in response.
4. Observe transmissions from the DUT.

Part d: Powersave Retries (SRC)

1. Instruct TS1 and TS2 to authenticate and associate with the DUT.
2. Instruct TS1 to go into Power Save mode.
3. Instruct TS2 to transmit MSDU2 to TS1.
4. Once the DUT sets TS1's AID in the TIM, instruct TS1 to transmit a PS-Poll to the DUT.
5. When the DUT transmits the ICMP Echo Response, do not allow TS1 to transmit an ACK in response.
6. Observe transmissions from the DUT.

Part e: Fragmented Retries (SRC)

1. Disable encryption on the DUT. If possible set the fragmentation threshold to 512-bytes and set the RTS threshold to 512-bytes.
2. Instruct the TS to authenticate and associate with the DUT.
3. Instruct the TS to transmit MSDU2 to the DUT.
4. When the DUT transmits an ICMP Echo Response, do not allow the TS to transmit an ACK in response to the first fragment.
5. Observe transmissions from the DUT.

Observable Results:

The DUT should:

a. transmit a RTS in response to MSDU1 exactly dot11ShortRetryLimit times, each RTS with the retry bit set to 0.
b. transmit the ICMP Echo Response in response to MSDU1 exactly dot11LongRetryLimit times.
c. transmit the ICMP Echo Response to MSDU1 exactly dot11ShortRetryLimit times.
d. transmit the ICMP Echo Response to MSDU2 exactly dot11ShortRetryLimit times.
e. transmit the first fragment of the ICMP Echo Response dot11ShortRetryLimit times.

Possible Problems: The value of the dot11ShortRetryLimit and aLongRetryLimit may not be known, in which case consistency of the number of retries is checked.

Test #1.2.2: RTS/CTS and Directed MPDU Transfer

Purpose: To verify that

- the DUT properly receives frames from devices with a different RTS threshold than its own.
- the DUT initiates an RTS/CTS exchange for directed frames when the length of the MSDU is greater than the dot11RTSThreshold.
- the DUT does not initiate an RTS/CTS exchange for all MPDUs if the value of the dot11RTSThreshold is larger than the maximum MSDU length.

References:

[1] IEEE Std 802.11™-2012 Edition, Subclauses 9.3.2.5, 9.3.2.6, 9.3.5, 8.3.1

Resource Requirements:

- A testing STA (TS) that is capable of transmitting user defined MAC frames and does not participate in the MAC protocol
- A monitor configured for capturing and analyzing MAC frames
- An Ethernet STA (STA-E) on the DS that is capable of receiving and responding to ICMP Echo Requests

Last Updated: June 2007

Discussion: When a directed MPDU has a length that exceeds the transmitting STA's dot11RTSThreshold, an RTS/CTS exchange is performed prior to the directed MPDU transfer. Since dot11RTSThreshold can be set on a per-STA basis, STAs must also be capable of receiving frames larger than their dot11RTSThreshold that are not preceded by an RTS/CTS exchange. This test is designed to ensure that a STA uses an RTS/CTS exchange only when appropriate.

Test Setup: Place the DUT, TS, and sniffer in a RF isolated environment and in range of each other. Place STA-E on the same DS as the DUT.

Table 12 - Test Frame(s)

Frame Label	Description
MSDU1	ICMP Echo Request with a frame length of 255-bytes to STA-E
MSDU2	ICMP Echo Request with a frame length of 256-bytes to STA-E
MSDU3	ICMP Echo Request with a frame length of 257-bytes to STA-E
MSDU4	ICMP Echo Request with a frame length of 750-bytes to STA-E
MSDU5	ICMP Echo Request with a frame length of 1023-bytes to STA-E
MSDU6	ICMP Echo Request with a frame length of 1024-bytea to STA-E
MSDU7	ICMP Echo Request with a frame length of 1025-bytes to STA-E
MSDU8	ICMP Echo Request with a frame length of 1400-bytes to STA-E

Procedure:

Part a: RTS Threshold at 256

1. Disable encryption on the DUT. If possible set the fragmentation threshold to 512-bytes and the RTS threshold to 256-bytes. Ensure no other STAs associate to the DUT.
2. Instruct the TS to authenticate and associate with the DUT.
3. Instruct the TS to transmit MSDU1 to the DUT.
4. Instruct the TS to transmit MSDU2 to the DUT.
5. Instruct the TS to transmit MSDU3 to the DUT.
6. Observe transmissions from the DUT.
7. Repeat steps 3 - 6 two more times.

Part b: RTS with Fragmentation

1. Repeat steps 1 - 2 from Part a.
2. Instruct the TS to transmit MSDU4 to the DUT.
3. Observe transmissions from the DUT.
4. Repeat steps 1 - 3 two more times.

Part c: Receiving RTS

1. Repeat steps 1 - 2 from Part a.
2. Instruct the TS to transmit MSDU8 with an RTS/CTS exchange and fragmented at 356 bytes to the DUT.
3. Observe transmissions from the DUT.

Part d: RTS Threshold at 1024

1. Disable encryption on the DUT. If possible set the fragmentation threshold to 2346-bytes and the RTS threshold to 1024-bytes. Ensure no other STAs associate to the DUT.
2. Instruct the TS to authenticate and associate with the DUT.
3. Instruct the TS to transmit MSDU5 to the DUT.
4. Instruct the TS to transmit MSDU6 to the DUT.
5. Instruct the TS to transmit MSDU7 to the DUT.
6. Observe transmissions from the DUT.
7. Repeat steps 3 - 6 two more times.

Observable Results:

a. The DUT should :
   - not use RTS/CTS preceding the ICMP Echo Response to MSDU1.
   - not use RTS/CTS preceding the ICMP Echo Response to MSDU2.
   - use RTS/CTS preceding the ICMP Echo Response to MSDU3.

b. The DUT should:
   - use RTS/CTS preceding the first fragment of the ICMP Echo Response to MSDU4.
   - use RTS/CTS only preceding the first fragment.

c. The DUT should:
   - use RTS/CTS preceding the first fragment of the ICMP Echo Response to MSDU8.
   - use RTS/CTS only preceding the first fragment.

d. The DUT should:
   - not use RTS/CTS preceding the ICMP Echo Response to MSDU5.
   - not use RTS/CTS preceding the ICMP Echo Response to MSDU6.
   - use RTS/CTS preceding the ICMP Echo Response to MSDU7.

Possible Problems: None.

Test #1.2.3: Broadcast and Multicast MPDU Transfer

Purpose: To verify that the DUT properly transfers broadcast and multicast traffic.

References:

[1] IEEE Std 802.11™-2012 Edition, Subclause 9.3.6

Resource Requirements:

- A testing STA (TS) that is capable of transmitting user defined MAC frames and does not participate in the MAC protocol
- A monitor configured for capturing and analyzing MAC frames
- An Ethernet STA (STA-E) on the DS that is capable of receiving and responding to ICMP Echo Requests

Last Updated: November 2008

Discussion: Broadcast and Multicast traffic is intended for multiple STAs and must be handled differently than directed unicast traffic. When traffic is sent to a broadcast or multicast address it is never fragmented, and consequently never contains a duration field value other than 0. Furthermore broadcast and multicast traffic should never be preceded by an RTS/CTS exchange. This test is designed to ensure that the DUT properly handles broadcast and multicast traffic.

Test Setup: Place the DUT, TS, and sniffer in a RF isolated environment and in range of each other. Place STA-E on the same DS as the DUT.

Table 13 - Test Frame(s)

Frame Label	Description
MSDU1	Broadcast frame with length of 356-bytes
MSDU2	Multicast frame with length of 356-bytes
MSDU3	Broadcast frame with length of 512-bytes
MSDU4	Multicast frame with length of 512-bytes
MSDU5	Broadcast frame with length of 513-bytes
MSDU6	Multicast frame with length of 513-bytes
MSDU7	Broadcast frame with length of 1300-bytes
MSDU8	Multicast frame with length of 1300-bytes
MSDU9	Multicast frame with the ToDS and FromDS bits set

Procedure:

Part a: No RTS/CTS and No Fragmentation

1. Disable encryption on the DUT, set the fragmentation, and RTS thresholds to 512-bytes.
2. Instruct the TS to authenticate and associate with the DUT.
3. Instruct the TS to transmit MSDU1 - 9 at an extended rate to the DUT.
4. Observe transmissions from the DUT.

Part b: Using RTS/CTS and Fragmentation

1. Disable encryption on the DUT, set the fragmentation, and RTS thresholds to 512-bytes.
2. Instruct the TS to authenticate and associate with the DUT.
3. Instruct the TS to transmit MSDU1 - 9 at an extended rate to the DUT preceded by an RTS/CTS exchange.
4. Observe transmissions from the DUT.

Part c: Power Save

1. Repeat steps 1 - 2 from Part b.
2. Instruct the TS to go into PS mode.
3. Instruct TS2 to authenticate and associate with the DUT.
4. Following a DTIM, instruct TS2 to transmit MSDU1, MSDU2, MSDU3, MSDU4, and MSDU9 at an extended rate to the DUT.
5. Observe transmissions from the DUT.

Observable Results:

a. For all MSDUs transmitted without using RTS/CTS or Fragmentation, the DUT should:
   - not use fragmentation when forwarding the frames to the BSS.
   - not use RTS/CTS when forwarding the frames to the BSS.

b. For all MSDUs transmitted using RTS/CTS and Fragmentation, the DUT should:
   - not use fragmentation when forwarding the frames to the BSS.
   - not use RTS/CTS when forwarding the frames to the BSS.

c. The DUT should
   - buffer broadcast and multicast frames when there are PS-STAs present (at least the Listen Interval of the TS).
   - set the More Data bit when transmitting all buffered broadcast and multicast frames except for the last one.
   - be able to properly handle receiving data frames with the ToDS and FromDS bits both set to 1.

Possible Problems: The DUT may not respond to all multicast addresses, so the MSDUs that are to have a multicast destination address are actually multiple MSDUs. These MSDUs cycle through the following MAC addresses: 0180:c18c:145f, 3333:0000:0001, 3333:ffff:ffff, 0100:0ccc:cccc, 0100:5e00:0000, 0100:5e7f:ffff, 0100:5e80:0000, and 0100:5eff:ffff. Also, the broadcast and multicast frames use a SNAP header of AA AA 03 00 00 00 08 06.

Test #1.2.4: Directed MSDU Fragmentation

Purpose: To verify that the DUT properly fragments directed MSDUs and MMPDUs when the frame length exceeds the DUT's fragmentation threshold.

References:
[1] IEEE Std 802.11™-2012 Edition, Subclauses 9.2.7, 9.3.2.6, 9.5

Resource Requirements:
- A testing STA (TS) that is capable of transmitting user defined MAC frames and does not participate in the MAC protocol
- A monitor configured for capturing and analyzing MAC frames
- An Ethernet STA (STA-E) on the DS that is capable of receiving and responding to ICMP Echo Requests

Last Updated: June 2007

Discussion: A STA's fragmentation threshold is the maximum transmission length that a directed MSDU or MMPDU can be before fragmentation will occur. To determine whether or not a MSDU or MMPDU should be fragmented, a transmitting STA must account for the length and type of frame (unicast, broadcast, or multicast). If the MSDU or MMPDU is unicast and is larger than the transmitting STA's fragmentation threshold, it should be fragmented before transmission.

Each fragment contains specific information included by the transmitting STA that includes the frame type, more fragments indicator bit, destination address, retry bit, sequence number, and fragment number. All of these values should be correctly set by the source STA before the fragment is transmitted. If they are not correctly set before transmission, they will not be received or assembled correctly by the receiving station. This test is designed to ensure that the DUT is capable of properly fragmenting directed MSDUs and MMPDUs when necessary.

Test Setup: Place the DUT, TS, and sniffer in a RF isolated environment and in range of each other. Place STA-E on the same DS as the DUT.

Table 14 - Test Frame(s)

Frame Label	Description
MSDU1	ICMP Echo Request with a frame length of 1500-bytes to STA-E
MSDU2	ICMP Echo Request with a frame length of 512-bytes to STA-E
MSDU3	ICMP Echo Request with a frame length of 256-bytes to STA-E
MSDU4	ICMP Echo Request with a frame length of (3*[fragmentation threshold - 1])-bytes to STA-E
MSDU5	ICMP Echo Request with a frame length of (4*[fragmentation threshold + 1])-bytes to STA-E

Procedure:
Part a: Even Fragmentation Threshold
1. Disable encryption on the DUT, set the fragmentation threshold equal to 512-bytes and the RTS threshold to 600-bytes. Ensure no other STAs are associated to the DUT.
2. Instruct the TS to authenticate and associate with the DUT.
3. Instruct the TS to transmit MSDU1.
4. Instruct the TS to transmit MSDU2.
5. Instruct the TS to transmit MSDU3.
6. Repeat steps 3-5.

7. Observe transmissions from the DUT.

Part b: Odd Fragmentation Threshold (illegal)

1. Disable encryption on the DUT, set the fragmentation threshold equal to 301-bytes (if possible), and disable RTS/CTS exchanges. Ensure no other STAs are associated to the DUT.
2. Instruct the TS to authenticate and associate with the DUT.
3. Instruct the TS to transmit MSDU4 to the DUT
4. Instruct the TS to transmit MSDU5 to the DUT.
5. Repeat steps 3-4.
6. Observe transmissions from the DUT.

Observable Results:

a. The DUT should:
- transmit the response to MSDU1 fragmented at 512-bytes.
- correctly set the More Fragments Bit in all fragments.
- correctly set the Destination Address in all fragments.
- correctly maintain the same Sequence Number for all fragments belonging to the response to MSDU1.
- begin the Fragment Number at 0 and increments it by 1 for each successive fragment belonging to the response to MSDU1.

b. The DUT should:
- transmit the response to MSDU4 and MSDU5 fragmented at 300-bytes.
- correctly set the More Fragments Bit in all fragments.
- correctly set the Destination Address in all fragments.
- correctly maintain the same Sequence Number for all fragments belonging to the response to MSDU4 and MSDU5.
- begin the Fragment Number at 0 and increments it by 1 for each successive fragment belonging to the response to MSDU4 and MSDU5.

Possible Problems: None.

Test #1.2.5: Multirate Support

Purpose: To verify that the DUT's dynamic rate-switching algorithm will properly interoperate and coexist with all supported physical layer data transmission rates.

References:

[1] IEEE Std 802.11™-2012 Edition, Subclause 9.7

Resource Requirements:

- A testing STA (TS) that is capable of transmitting user defined MAC frames and does not participate in the MAC protocol
- A monitor configured for capturing and analyzing MAC frames
- An Ethernet STA (STA-E) on the DS that is capable of receiving and responding to ICMP Echo Requests

Last Updated: November 2008

Discussion: One performance enhancer of the 802.11 specification is the dynamic rate-switching mechanism. Rate-switching allows a STA to determine a transmit rate that gives it the optimal throughput based on the number of retries per rate and the throughput per rate. Since dynamic rate-switching may be supported, a STA must also support successful reception and acknowledgement of frames at different transmit rate values. An example of successful reception and acknowledgement is having all frames with multicast and broadcast RA transmitted at one of the rates included in the BSSBasicRateSet, regardless of the underlying physical layer.

The intention for the stringent requirements for rate selection is to allow for multiple STAs in a network to use different rate configurations. In this scenario, it guarantees that an optimal amount of traffic be heard by every STA in the BSS. It also allows for a STA to properly set its NAV value to include any necessary control response frames needed to complete the frame exchange.

Test Setup: Place the DUT, TS, and sniffer in a RF isolated environment and in range of each other. Place STA-E on the same DS as the DUT.

Table 15 - Test Frame(s)

Frame Label	Description
MPDU1	ICMP Echo Request with a payload size of 1028-bytes to STA-E

Procedure:

Part a: CCK, RTS at a Basic Rate

1. Disable encryption and fragmentation on the DUT and set the RTS threshold to 256-bytes. Also, have the DUT transmit frames at CCK rates using long preamble. The default rate set advertised by the DUT should be:

   CCK: Basic Rates = 1, 2
   Extended Rates = 5.5, 11

2. Instruct the TS to authenticate and associate to the DUT.
3. Instruct the TS to transmit MPDU1 using all available CCK rates. Also instruct the TS to precede the frame exchange with an RTS transmitted at 1 Mbps.
4. Repeat step 3; however, instruct the TS to transmit the RTS frame at 2 Mbps.
5. Observe transmissions from the DUT.

Part b: CCK, RTS at an Extended Rate

1. Repeat steps 1 - 2 from Part a.
2. Instruct the TS to transmit MPDU1 using all available CCK rates. Also, instruct the TS to precede the frame exchange with an RTS transmitted at 5.5 Mbps.
3. Repeat step 2; however, instruct the TS to transmit the RTS frame at 11 Mbps.
4. Observe transmissions from the DUT.

Part c: CCK, no RTS

1. Repeat steps 1 - 2 from Part a.
2. Instruct the TS to transmit MPDU1 at 1 Mbps.
3. Instruct the TS to transmit MPDU1 at 2 Mbps.
4. Instruct the TS to transmit MPDU1 at 5.5 Mbps.
5. Instruct the TS to transmit MPDU1 at 11 Mbps.
6. Observe transmissions from the DUT.

Part d: OFDM and ERP-OFDM, RTS at a Basic Rate

1. Repeat steps 1 - 2 from Part a using OFDM/ERP-OFDM rates. The default rate set advertised by the DUT should be:
   (ERP-) OFDM: Basic Rates = 6, 12, 24
   Extended Rates = 9, 18, 36, 48, 54
2. Instruct the TS to transmit MPDU1 using all available OFDM/ERP-OFDM rates. Also, instruct the TS to precede the frame exchange with an RTS transmitted at 6 Mbps.
3. Repeat step 2; however, instruct the TS to transmit the RTS frame at 12 and 24 Mbps.
4. Observe transmissions from the DUT.

Part e: OFDM and ERP-OFDM, RTS at an Extended Rate

1. Repeat steps 1 - 2 from Part a using OFDM/ERP-OFDM rates.
2. Instruct the TS transmit MPDU1 using all available OFDM/ERP-OFDM rates. Also have the TS precede the frame exchange with an RTS transmitted at 9 Mbps.
3. Repeat step 2, however, instruct the TS transmit the RTS frame at 18, 36, 48, and 54 Mbps.
4. Observe transmissions from the DUT.

Part f: OFDM and ERP-OFDM, no RTS

1. Repeat steps 1 - 2 from Part a using OFDM/ERP-OFDM rates.
2. Instruct the TS to transmit MPDU1 at 9 Mbps.
3. Instruct the TS to transmit MPDU1 at 18 Mbps.
4. Instruct the TS to transmit MPDU1 at 36 Mbps.
5. Instruct the TS to transmit MPDU1 at 48 Mbps.
6. Instruct the TS to transmit MPDU1 at 54 Mbps.
7. Observe transmissions from the DUT.

Observable Results:

a-f. The DUT should

- transmit all control response (CTS and ACK) frames at one of the basic rates in the BSSBasicRateSet that is not only of the same modulation, but at a rate less than or equal to the rate that the previous frame was transmitted at.
- transmit all other control frames at one of the rates in the BSSBasicRateSet.
- transmit directed data and management frames at a rate that is known to be supported by the receiving STA.

- transmit all frames with multicast and broadcast address 1 field are transmitted at one of the rates included in the BSSBasicRateSet, regardless of their PHY type.
- Not initiate transmission of a data or management frame at a data rate higher than the greatest rate in the OperationalRateSet.

Possible Problems: An 802.11g device may transmit control response (CTS and ACK) frames at PHY mandatory rates provided that the duration of the control response frame at the alternative rate is the same as the duration of the control response frame at the originally chosen rate.

Test #1.2.6: Defragmentation using RTS/CTS

Purpose: To verify that the DUT is capable of receiving fragments of an arbitrary length, and is able to reassemble them properly while using RTS/CTS.

References:

[1] IEEE Std 802.11™-2012 Edition, Subclause 9.2.7, 9.6

Resource Requirements:

- A testing STA (TS) that is capable of transmitting user defined MAC frames and does not participate in the MAC protocol
- A monitor configured for capturing and analyzing MAC frames
- An Ethernet STA (STA-E) on the DS that is capable of receiving and responding to ICMP Echo Requests

Last Updated: June 2007

Discussion: Defragmentation is the process of assembling successfully received fragments back into the original MSDU or MMPDU. Since it is possible for source STAs to transmit fragments of an arbitrary length, destination STAs must be capable of defragmenting fragments of arbitrary length. It is also possible for a STA to precede the transmission of a fragmented MSDU with an RTS/CTS exchange. This test is designed to ensure that an AP can properly reassemble arbitrarily fragmented MSDUs while simultaneously using the RTS/CTS procedure.

Test Setup: Place the DUT, TS, and sniffer in a RF isolated environment and in range of each other. Place STA-E on the same DS as the DUT.

Table 16 - Test Frame(s)

Frame Label	Description
MSDU1	ICMP Echo Request with payload size of 1514-bytes to STA-E

Procedure:

Part a: Various Threshold Defragmentation

1. Configure the DUT to use an RTS threshold of 512
2. Instruct the TS to authenticate and associate with the DUT.
3. Instruct the TS to transmit MSDU1, fragmented at varying sizes from 256-bytes to 1456-bytes. After MSDU1 has been transmitted at a fragment size twice, increment the fragment size by 60 and repeat until the fragment size is equal to 1456-bytes.
4. Observe transmissions from the DUT.

Observable Results:

a. The DUT should defragment MSDU1 for all the fragmentation thresholds used to fragment it, use the RTS/CTS procedure, forward MSDU1 to STA-E, and forward the ICMP Echo Response to the TS.

Possible Problems: None.

GROUP 3: WEP AND POWERSAVE

Scope:
This group of tests pertains to the operation of the MAC layer when using WEP or when a STA in the BSS is using powersave.

Overview:
The following tests cover MAC layer operation specific to the configuration of the DUT when using WEP or a STA in the BSS is in powersave. In addition to the test specific settings, other configuration values for the DUT unless otherwise specified are the beacon interval is 100ms, the DTIM interval is 3 beacons, and without encryption. Also, there is to be an Ethernet STA with a static IP address on the same DS as the AP, which is capable of receiving and responding to ICMP Echo Requests as well as ARP Requests.

Test #1.3.1: WEP Decryption Procedure

Purpose: To verify that
- the DUT properly decrypts data as specified by the 802.11 standard.
- the DUT does not process encrypted frames with an invalid ICV.

References:
[1] IEEE Std 802.11™-2012 Edition, Clause 11.2.2

Resource Requirements:
- A testing STA (TS) that is capable of transmitting user defined MAC frames and does not participate in the MAC protocol
- A monitor configured for capturing and analyzing MAC frames
- An Ethernet STA (STA-E) on the DS that is capable of receiving and responding to ICMP Echo Requests

Last Updated: June 2007

Discussion: Due to the inherent nature of the WLAN environment, the opportunity for eavesdropping is greatly increased. Therefore, the Wired Equivalent Privacy (WEP) algorithm was developed. WEP attempts to give 802.11 networks the same amount of security that would be provided on a regular wired network using no extra security functions. There are four parts that are essential to the performance of the WEP algorithm:
- The secret key: is the key that is entered into the "WEP key" value.
- The initialization vector (IV): extends the useful lifetime of a secret key and provides the self-synchronous property of the WEP algorithm.
- The pseudorandom number generator (PRNG): transforms a relatively short secret key into an arbitrary length key sequence.
- The integrity check value (ICV): protects against unauthorized data modification.

Given these components, it is imperative that a device have the ability to correctly decrypt received frames.

Test Setup: Place the DUT, TS, and sniffer in a RF isolated environment and in range of each other. Place STA-E on the same DS as the DUT.

Table 17 - Test Frames

Frame Label	Description
MSDU1	ICMP Echo Request to STA-E encrypted with WEP key id 1 with WEP bit set and that includes an ICV field of all zeroes
MSDU2	ICMP Echo Request to STA-E encrypted with WEP key id 1 with WEP bit set, but does not include the IV or ICV fields
MSDU3	ICMP Echo Request to STA-E encrypted with WEP key id 1 with WEP bit not set, but includes the IV, ICV, and a FCS of all zeroes
MSDU4	ICMP Echo Request to STA-E encrypted with WEP key id 1 with WEP bit set and valid IV and ICV fields

Procedure:

Part a: Invalid ICV

1. Configure the DUT and TS with four WEP keys:
   - Key 1: 0x6162636465 or abcde (use as the TX default key)
   - Key 2: 0x6263646566 or bcdef
   - Key 3: 0x6364656667 or cdefg
   - Key 4: 0x6465666768 or defgh
2. Instruct the TS to authenticate and associate to the DUT.
3. Instruct the TS to transmit MSDU1 to the DUT.
4. Observe transmissions from the DUT.

Part b: No IV or ICV

1. Repeat steps 1 - 3 from Part a, however, in step 3 transmit MSDU2.
2. Observe transmissions from the DUT.

Part c: Invalid IV, ICV, and FCS

1. Repeat steps 1 - 3 from Part a, however, in step 3 transmit MSDU3.
2. Observe transmissions from the DUT.

Part d: Proper Encryption, All Keys

1. Repeat step 1 from Part a.
2. Instruct the TS to transmit MSDU4 encrypted with WEP key id 1 to the DUT.
3. Repeat step 2 using each WEP key only once.
4. Observe transmissions from the DUT.

Observable Results:

The DUT should:

a. transmit an ACK upon reception of MSDU1, however, not transmit an ICMP Echo Response.
b. transmit an ACK upon reception of MSDU2, however, not transmit an ICMP Echo Response.
c. not transmit an ACK upon reception of MSDU3, nor process the frame.
d. transmit an ACK for each transmission of MSDU4, and transmit an ICMP Echo Response.

Possible Problems: None.

Test #1.3.2: Aging Function

Purpose: To verify that

- the DUT discards any buffered traffic that has been queued for an excessive period of time.
- the DUT does not discard any buffered traffic after any period less than the Listen Interval of the STA for which the traffic is buffered.

References:

[1] IEEE Std 802.11™-2012 Edition, subclause 10.2.1.12

Resource Requirements:

- Four testing STAs (TS1 through TS4) that are capable of transmitting user defined MAC frames and do not participate in the MAC protocol
- A monitor configured for capturing and analyzing MAC frames

Last Updated: June 2007

Discussion: As APs have a limited amount of memory reserved for buffering, and it is possible for STAs to fail or go out of range without properly disassociating, an aging function must be designed into APs to discard old frames. The exact point at which frames should be discarded is not defined in the standard, but the period must not be shorter than a Listen Interval, otherwise frames could be discarded before a STA has a chance to poll for them.

Test Setup: Place the DUT, TS, and sniffer in a RF isolated environment and in range of each other. Place STA-E on the same DS as the DUT.

Table 18 - Test Frames

Frame Label	Description
MSDU1	ICMP Echo Request to TS1 from TS2.
MSDU2	ICMP Echo Request to TS1 from TS4.
MSDU3	ICMP Echo Request to TS2 from TS4.
MSDU4	ICMP Echo Request to TS3 from TS4.
MSDU5	Association Request with a Listen Interval of 1.
MSDU6	Association Request with a Listen Interval of 16.
MSDU7	Association Request with a Listen Interval of 64.
MSDU8	Association Request with a Listen Interval of 256.
MSDU9	Association Request with a Listen Interval of 1024.

Procedure:

Part a: Beacon Interval of 50ms.

1. Configure the DUT to a Beacon Interval of 50ms and the DTIM Interval to 3. Disable fragmentation, RTS/CTS exchanges, and encryption.
2. Instruct TS2 to authenticate and associate with the DUT.
3. Instruct TS1 to authenticate with the DUT and associate using MSDU5.
4. Instruct TS1 to enter Doze mode.
5. Instruct TS2 to transmit MSDU1.
6. Monitor the TIM elements to observe when the DUT no longer indicates that it has any directed frames buffered for TS1.
7. Repeat steps 2 - 6 using the remaining association requests.
8. Observe transmissions from the DUT.

Part b: Beacon Interval of 100ms.

1. Configure the DUT to a Beacon Interval of 100ms and the DTIM Interval to 3. Disable fragmentation, RTS/CTS exchanges, and encryption.
2. Repeat steps 2 - 8 from Part a.

Part c: Beacon Interval of 500ms.

1. Configure the DUT to a Beacon Interval of 500ms and the DTIM Interval to 3. Disable fragmentation, RTS/CTS exchanges, and encryption.
2. Repeat steps 2 - 8 from Part a.

Part d: Maximum Listen Interval

1. Configure the DUT to a Beacon Interval of 50ms and the DTIM Interval to 3. Disable fragmentation, RTS/CTS exchanges, and encryption. Configure TS1 to have a Listen Interval of 65535.
2. Instruct TS2 to authenticate and associate with the DUT.
3. Instruct TS1 to authenticate and associate with the DUT.
4. Instruct TS1 to enter Doze mode.
5. Instruct TS2 to transmit MSDU1.
6. Monitor the TIM elements to observe when the DUT no longer indicates that it has any directed frames buffered for TS1.
7. Observe transmissions from the DUT.

Part e: Multi-STA Listen Intervals

1. Configure the DUT to a Beacon Interval of 100ms and the DTIM Interval to 3. Disable fragmentation, RTS/CTS exchanges, and encryption.
2. Instruct TS4 to authenticate and associate with the DUT.
3. Instruct TS1 to authenticate with the DUT and associate using MSDU5.
4. Instruct TS2 to authenticate with the DUT and associate using MSDU8.
5. Instruct TS3 to authenticate with the DUT and associate using MSDU9.
6. Instruct TS1, TS2, and TS3 enter Doze mode.
7. Instruct TS4 transmit MSDU2, MSDU3, and MSDU4.
8. Monitor the TIM elements to observe when the DUT no longer indicates that it has any directed frames buffered for TS1, TS2, and TS3.
9. Instruct TS1, TS2, TS3 and TS4 to deauthenticate from the DUT.
10. Do steps 2, 5, 4, 3, 6, and 7 in that order.
11. Monitor the TIM elements to observe when the DUT no longer indicates that it has any directed frames buffered for TS1, TS2, and TS3.
12. Observe transmissions from the DUT.

Observable Results:

The DUT should:

a-d. eventually discard traffic that has been buffered for a period of time longer than the listen interval of TS1. Additionally, the DUT should not discard traffic that has been buffered for TS1 for less than the listen interval of TS1.

e. eventually discard traffic that has been buffered for a period of time longer than the Listen Interval of each TS. Additionally, the DUT should not discard traffic that has been buffered for each TS for less than the Listen Interval of each TS.

Possible Problems: If the DUT deauthenticates or disassociates a STA it has buffered traffic for prior to reaching the STA's Listen Interval the test results will become invalid.

Test #1.3.3: PS-Poll Processing

Purpose: To verify that the DUT has the ability to operate properly upon reception of PS-Poll frames.

References:

[1] IEEE Std 802.11™-2012 Edition, Clause 10.2.1 and subclauses 10.3, 8.3.1.5

Resource Requirements:

- A testing STA (TS) that is capable of transmitting user defined MAC frames and does not participate in the MAC protocol
- A monitor configured for capturing and analyzing MAC frames
- An Ethernet STA (STA-E) on the DS that is capable of receiving and responding to ICMP Echo Requests

Last Updated: June 2007

Discussion: A STA may be in two different power states: awake and doze. The two ways a STA changes from these states, determined by the STA's power management mode, are active mode and power save mode (PS). A STA that changes from doze to awake for frame transmission shall perform a clear channel assessment in order to set its NAV appropriately, or until a ProbeDelay period has occurred. All MSDUs or management frames destined for STAs in PS mode will be buffered at the AP, and all broadcast/multicast frames, if destined to any STA in PS mode, will also be buffered at the AP before distribution. After a DTIM, the AP shall transmit any buffered broadcast/multicast frames, with the More Data field set for each MSDU except the last, indicating the presence of more buffered broadcast/multicast frames at the AP. All buffered MSDUs and management frames shall be transmitted in the same manner as buffered broadcast/multicast frames, upon reception of a PS-Poll from the STA by the AP. Retried PS-Polls will not be treated as new requests to deliver any traffic that is buffered. When a STA changes back to Active mode, the AP shall transmit buffered MSDUs and management frames, if they exist, without waiting for a PS-Poll.

Test Setup: Place the DUT, TS, and sniffer in a RF isolated environment and in range of each other. Place STA-E on the same DS as the DUT.

Table 19 - Test Frame(s)

Frame Label	Description
MPDU1-30	PS Poll with AID of 1 – 30 (in decimal)
MPDU31	PS Poll with AID 0 (in decimal)
MPDU32	PS Poll with AID 257 (in decimal)
MPDU33	PS Poll with AID 2000 (in decimal)

Procedure:

Part a: PS-Poll with AID 1-30

1. Instruct the TS to deauthenticate, then successfully authenticate and associate with the DUT.
2. Instruct the TS to transmit MPDU1-30 to the DUT.
3. Observe transmissions from the DUT.

Part b: PS-Poll with AID 0

1. Instruct the TS to deauthenticate, then successfully authenticate and associate with the DUT.
2. Instruct the TS to transmit MPDU31 to the DUT.
3. Observe transmissions from the DUT.

Part c: PS-Poll with AID 257

1. Instruct the TS to deauthenticate, then successfully authenticate and associate with the DUT.
2. Instruct the TS to transmit MPDU32 to the DUT.
3. Observe transmissions from the DUT.

Part d: PS-Poll with AID 2000

1. Instruct the TS to deauthenticate, then successfully authenticate and associate with the DUT.
2. Instruct the TS to transmit MPDU33 to the DUT.
3. Observe transmissions from the DUT.

Observable Results:

a-d. The DUT should either transmit a queued data frame, or transmit an ACK followed by a queued data frame or a null data frame, upon reception of each PS-Poll.

Possible Problems: None.

Test #1.3.4: Defragmentation using WEP

Purpose: To verify that the DUT is capable of receiving WEP encrypted fragments of an arbitrary length, is able to reassemble them, and properly encrypt the resulting MSDU.

References:

[1] IEEE Std 802.11™-2012 Edition, Clause 11.2.2 and subclause 9.2.7, 9.6

Resource Requirements:

- A testing STA (TS) that is capable of transmitting user defined MAC frames and does not participate in the MAC protocol
- A monitor configured for capturing and analyzing MAC frames
- An Ethernet STA (STA-E) on the DS that is capable of receiving and responding to ICMP Echo Requests

Last Updated: June 2007

Discussion: Defragmentation is the process of assembling successfully received fragments back into the original MSDU or MMPDU. Since it is possible for source STAs to transmit fragments of an arbitrary length, destination STAs must be capable of defragmenting fragments of arbitrary length. Defragmentation must also be properly handled when accounting for the extra overhead created by using WEP encryption. This test is designed to ensure that an AP can properly reassemble WEP encrypted arbitrarily fragmented MSDUs.

Test Setup: Place the DUT, TS, and sniffer in a RF isolated environment and in range of each other. Place STA-E on the same DS as the DUT.

Table 20 - Test Frame(s)

Frame Label	Description
MSDU1	ICMP Echo Request with payload size of 1514-bytes to STA-E

Procedure:

Part a: Various Threshold Defragmentation

1. Configure the DUT and TS with four WEP keys:
   - Key 1: 0x6162636465 or abcde (use as the TX default key)
   - Key 2: 0x6263646566 or bcdef
   - Key 3: 0x6364656667 or cdefg
   - Key 4: 0x6465666768 or defgh
2. Instruct the TS to authenticate and associate with the DUT.
3. Instruct the TS to transmit MSDU1, fragmented at varying sizes from 256-bytes to 1456-bytes. After MSDU1 has been transmitted at a fragment size twice, increment the fragment size by 60 and repeat until the fragment size is equal to 1456-bytes.
4. Observe transmissions from the DUT.

Observable Results:

a. The DUT should defragment MSDU1 for all the fragmentation thresholds used to fragment it, forward MSDU1 to STA-E, and forward the ICMP Echo Response to the TS.

Possible Problems: The DUT may not be capable of supporting more than one WEP key index. If so, the DUT should only be configured to use Key 1.

Appendix A: Abbreviations

Abbreviation	Description
AID	Association ID
AP	AP
ARP	Address Resolution Protocol
BSS	Basic Service Set
DS	Distribution System
DTIM	Delivery Traffic Indication Message
DUT	Device Under Test
FCS	Frame Check Sequence
ICMP	Internet Control Message Protocol
ICV	Integrity Check Value
IV	Initialization Vector
MAC	Media Access Control
MPDU	MAC Protocol Data Unit
MSDU	MAC Service Data Unit
STA	STA
TS	Testing STA