# WLAN

The Wireless Local Area Network Consortium

## 802.11 Base
## Station MAC Layer Test Suite

*Version 3.2*

*Technical Document*

*Last Updated: November 25, 2008*

***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/](http://www.iol.unh.edu/consortiums/wireless/)

## MODIFICATION RECORD

- November 2008 – Version 3.2 Released

  Daniel Reynolds: Removed RCC reference, 1.1.1 – added in MSDU1-4 and MSDU5-12 instead of "the frame". 1.1.4 – added the 0 to MSDU1 and reworded part a. observable results. 1.1.5 – Removed "repeat for…" in cases c-f, changed from responding to transmitting class 3. 1.1.6 – Added in the continue class 3 traffic to part c. 1.1.7 – changed part a. in the observable results, changed to transmit class 3 traffic. 1.1.8 – updated part a. to include MSDU4. 1.1.9 – Moved frag. threshold to test setup, added commas to observables to make clearer. 1.2.1 – Changed MSDU1 in part a&b to MSDU2, added DUT should not transmit other fragments to part d. 1.2.2 – MSDU6 changed from bytea to bytes. 1.2.3 – added in "except last one" to part a. also the "(MSDU1)" comment. 1.2.4 – part c and f changed from DUT to TS. 1.3.1 – Changed MSDU1 from all zeros to "invalid ICV".
- June 2007

  Anthony Murabito & Jonathan Zink: Changed Std references to IEEE Std 802.11™-2007, and minor editorial modifications. Also moved Duplicate Detection and Recovery to Group 1.
- August 25, 2006 – Version 3.0 Released

  Anthony Murabito & Jonathan Zink: Test Suite Expansion and Redundancy Removal. Separated 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. Clarified Duplicate Direction and Recovery observable results. Added Test#1.3.3 Defragmentation using WEP.
- April 19, 2006 – Version 2.1.1 Released

  Anthony Murabito: Minor editorial and renumbering of tests 1.1.8 and 1.1.9 to 1.1.5 and 1.1.6.
- August 2005 - Version 2.1 Released

  Jon Zink: Minor script and procedural updates
- May 2005 - Version 2.0 Released

  Matt Newcomb: Renumbered tests, updated procedures and observable results.
  MAC team: Revisions
- 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.**

| | |
|---|---|
| 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 stations.

These tests are designed to determine if a product conforms to specifications defined in IEEE Std 802.11™-2007 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, MSDU formats, and processing of received MSDUs.

**Overview:**
The following tests cover MAC layer operation specific to the configuration of the DUT where fragmentation, RTS, and encryption are disabled and uses a static IP address. Also, the DUT must be 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 handles the reception of MAC frames correctly.

**References:**

[1] IEEE Std 802.11™-2007 Edition, Clause 7, Subclause 9.7, and A.4.4.2 FR1-FR25 (PICS)

**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 Updated:** November 2008

**Discussion:** This test verifies that the DUT correctly formats MAC layer frames that it receives. This test checks that the DUT properly processes the received frame by continuing the frame exchange sequence. It also verifies that the DUT can handle the reception of an unexpected or incorrectly formatted frame without error. This is to test the robustness of the DUT. It is assumed that the data rate that frames are sent 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.

| Frame Label | Description |
|---|---|
| MSDU1 | A valid ICMP Echo Request to the DUT containing a Frame Control field Protocol Version greater than 0. |
| MSDU2a-b | Control frames of reserved subtype. One with and one without an address 3 field. |
| MSDU3 | Beacons containing bits 5-15 in the capability information field set to 1. |
| MSDU4 | Beacon containing no supported rates. |
| MSDU5 | Data Frame containing frame control = 0x08, 0-byte payload. This is not a null data frame. |
| MSDU6 | Same as MSDU3 but also containing WEP bit set, and 8 extra associated bytes for encryption. |
| MSDU7 | 500-byte ICMP Echo Request to the DUT containing FromDS bit unset, address 1 field value of the DUT's MAC address, address 2 field of the TS's MAC address, and address 3 field value of a MAC address for a station that is not within the BSS. |
| MSDU8 | A frame containing the Order bit set. |
| MSDU9 | Data frame containing a length that is less than 64-bytes and ToDS bit set. |
| MSDU10a-b | Management frames of reserved subtypes = [0111, 1111] (binary). One set with a zero byte payload and another set with a random data payload. |
| MSDU11a | Data frames of reserved subtypes = [1101] (binary) containing a frame body of 2-bytes, both set to 0. |
| MSDU12 | Unfragmented ICMP Echo Request containing payload of 2000-bytes to the DUT. |
| MSDU13a-j | Frames of Type = Reserved, subtypes = [0000, 0001, 0010, 0100, 1000, 1111] (binary). One set with a 0-byte payload and another set with a random data payload. |

**Procedure:**

*Part a: Non-Acknowledged Frames:*

1. Instruct the TS to transmit MSDU1-MSDU4 to the DUT.
2. Send a valid ICMP Echo Request between each test case to validate that the DUT is responding with an ACK.
3. Observe transmissions from the DUT.

*Part b: Acknowledged Frames:*

1. Instruct the TS to transmit MSDU5-MSDU12 to the DUT.
2. Send a valid ICMP Echo Request between each test case to validate that the DUT is responding with an ACK.
3. Observe transmissions from the DUT.

*Part c: Reserved Frames:*

1. Instruct the TS to transmit MSDU13a-j to the DUT.
2. Send a valid ICMP Echo Request between each test case to validate that the DUT is responding with an ACK.
3. Observe transmissions from the DUT.

**Observable Results:**

The DUT should:

a. not transmit an ACK upon reception of MSDU1-4, but should receive the frames without system failure.
b. transmit an ACK upon reception of MSDU5-12, and should receive the frames without system failure.
c. receive the frame without system failure. The DUT may or may not transmit an ACK upon reception of these frames.

**Possible Problems:** None.

**Test #1.1.2:Null Data Processing**

**Purpose:** To verify that the DUT operates properly upon reception of Null Data frames, and interprets the frame control field properly.

**References:**

[1] IEEE Std 802.11™-2007 Edition, Subclauses 7.1.3.1, 7.2.2

**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 Updated:** June 2007

**Discussion:** All 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.

Table 1 - Test Frame(s)

| Frame Label | Description |
|---|---|
| MSDU1 | Null data frame containing the Protocol Version Bits set to 1 |
| MSDU2 | Null data frame containing all Frame Control Bits set, except the ToDS Bit |
| MSDU3 | Null data frame containing no Frame Control Bits set |
| MSDU4 | Null data frame containing the More Fragment Bit set |
| MSDU5 | Null data frame containing the Retry Bit set |
| MSDU6 | Null data frame containing the Power Management Bit set |
| MSDU7 | Null data frame containing the More Data Bit set |
| MSDU8 | Null data frame containing the WEP Bit set, without an IV and ICV expanded WEP frame body |
| MSDU9 | Null data frame containing the WEP Bit set and an 8-byte payload |
| MSDU10 | Null data frame containing the WEP Bit set and a 9-byte payload |
| MSDU11 | Null data frame containing the Order Bit set |

**Procedure:**

*Part a: Non-Acknowledged Frames*

1. Wait for the DUT to authenticate and associate with the TS.
2. Instruct the TS to transmit MSDU1-2.
3. After each test frame is sent, instruct the TS to send an ICMP Echo Request to the DUT to ensure the DUT is operational.
4. Observe transmissions from the DUT.

*Part b: Acknowledged Frames*

1. Wait for the DUT to authenticate and associate with the TS.
2. Instruct the TS to transmit MSDU3-11.
3. After each test frame is sent, instruct the TS to send an ICMP Echo Request to the DUT to ensure the DUT is operational.
4. Observe transmissions from the DUT.

**Observable Results:**

The DUT should:

a. not send an ACK in response to MSDU1 and MSDU2.
b. send an ACK in response to MSDU3-MSDU11.

**Possible Problems:** None.

**Test #1.1.3: Deauthentication Processing**

**Purpose:** To verify that the DUT properly handles received deauthentication frames and generates deauthentication frames properly.

**References:**

[1] IEEE Std 802.11™-2007 Edition, Subclauses 11.3, 5.4, Annex C [auth_rsp2b(2)], and A.4.4.1 FR11 (PICS)

**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 Updated:** June 2007

**Discussion:** Deauthentication nullifies authentication and is a notification rather than a request. It is important that a station properly handle a deauthentication notice as it should terminates network connectivity. Deauthentication frames can also be sent to a group address to deauthenticate from all APs at once or it can also be used in an IBSS using authentication.

**Test Setup:** Place the DUT, TS, and sniffer in a RF isolated environment and in range of each other. Instruct the DUT to transmit a continuous stream of ICMP Echo Requests to the TS.

Table 2 - Test Frame(s)

| Frame Label | Description |
|---|---|
| MSDU1 | Deauthentication from the TS to the DUT. |
| MSDU2 | Deauthentication from the TS to the broadcast address |
| MSDU3 | Deauthentication from the TS to the DUT with invalid FCS. |

**Procedure:**

*Part a: Reason Codes*

1. Wait for the DUT to authenticate and associate with the TS.
2. Instruct the TS send MSDU1.
3. Repeat steps 1-3 for each non-reserved reason code, and each reserved.
4. Observe transmissions from the DUT.

*Part b: Broadcast Deauthentication*

1. Wait for the DUT to authenticate and associate with the TS.
2. Instruct the TS to send MSDU2.
3. Observe transmissions from the DUT.

*Part c: Invalid FCS*

1. Wait for the DUT to authenticate and associate with the TS.
2. Instruct the TS to send MSDU3 to the DUT.
3. Observe transmissions from the DUT.

**Observable Results:**

The DUT should:

a. 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. not transmit an ACK upon reception of MSDU3, nor process the frame.

**Possible Problems:** None.

**Test #1.1.4: Authentication Processing**

**Purpose:** To verify that

- The DUT can transmit an Authentication Request frame.
- The DUT can handle Authentication Responses with status codes other than “successful”.

**References:**

[1] IEEE Std 802.11™-2007 Edition, Subclauses 7.3.1.9, 11.3

**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 Updated:** November 2008

**Discussion:** Authentication is a distribution system (DS) service that allows an authenticated STA to transmit class 2 frames. Only after a STA has successfully authenticated with an AP, may it associate with that AP. The Authentication response that is transmitted by an AP will have a status code indicating either success or failure. If the Authentication is successful, the status code should be zero. The STA must be able to handle Authentication responses transmitted by the AP that include any Authentication related status code. If the Authentication response indicates a status code other than successful, the STA is not authenticated with the AP.

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

Table 3 - Test Frame(s)

| Frame Label | Description |
|---|---|
| MSDU1a-e | Authentication Responses containing status codes = [0, 1,8,12,256] |
| MSDU2 | Authentication Response containing invalid transaction sequence number. |
| MSDU3 | Authentication Response containing invalid authentication algorithm number. |
| MSDU4 | Authentication Response containing invalid FCS. |
| MSDU5 | Deauthentication from the TS to the DUT. |

**Procedure:**

*Part a: Authentication Status Codes*

1. Instruct the TS to transmit MSDU5.
2. Wait for the DUT to authenticate normally with the TS.
3. Instruct the TS to transmit MSDU1a.
4. Observe transmissions from the DUT.
5. Repeat steps 1-4 using MSDU1b-MSDU1e.

*Part b: Invalid Authentication Transaction Sequence Number*

1. Instruct the TS to transmit MSDU5.
2. Wait for the DUT to authenticate with the TS.
3. Instruct the TS to transmit MSDU2.
4. Observe transmissions from the DUT.

*Part c: Invalid Authentication Algorithm Number*

1. Instruct the DUT to transmit MSDU5.
2. Wait for the DUT to authenticate with the TS.
3. Instruct the TS to send MPDU3.

4. Observe transmissions from the DUT.

*Part d: Invalid FCS*

1. Instruct the DUT to transmit MSDU5.
2. Wait for the DUT to authenticate with the TS.
3. Instruct the TS to transmit MSDU4.
4. Observe transmissions from the DUT.

**Observable Results:**
The DUT should:

a. authenticate successfully and attempt association for status code 0. The DUT should not attempt association upon reception of MSDU1b-e.
b. authenticate unsuccessfully and not attempt to associate.
c. authenticate unsuccessfully and not attempt to associate.
d. not transmit an ACK upon reception of MSDU4, nor process the frame.

**Possible Problems:** The results of part d are only valid if the value of Authentication Failure Timeout is known or configurable on the DUT.

**Test #1.1.5: Association Processing**

**Purpose:** To verify that

- The DUT can transmit an Association Request frame.
- The DUT can handle Association Responses with a status value other than "successful".

**References:**

[1] IEEE Std 802.11™-2007 Edition, Clause 11.3, and A.4.4.1 PC14.2 (PICS)

**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 Updated:** November 2008

**Discussion:** Association is a distribution system (DS) state which allows an associated STA to transmit class 3 frames. Only after a STA has successfully authenticated with an AP, may it associate with that AP. To become associated with an AP that it is currently authenticated with, the STA must transmit an association request to the AP. The association response that is transmitted by an AP will have a status code indicating either success or failure. If the association is successful, the response should include the unique association identifier (AID). The STA must be able to handle association responses transmitted by the AP that include any association related status code. If the association response indicates a status code other than successful, the STA is not associated with the AP and should not attempt to transmit class 3 traffic to the AP.

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

Table 4 - Test Frame(s)

| Frame Label | Description |
|---|---|
| MSDU1 | Association Responses containing status codes = [1, 8, 12, 256] |
| MSDU2 | Association Response containing two reserved element IDs of length 255-bytes. |
| MSDU3 | Association Response containing duplicate valid element IDs. |
| MSDU4 | Association Response containing no supported rates. |
| MSDU5 | Association Response containing more than 8 supported rates. |
| MSDU6 | Deauthentication from the TS to the DUT. |

**Procedure:**

*Part a: Successful Association*

1. Instruct the TS to transmit MSDU6.
2. Wait for the DUT to authenticate and associate with the TS.
3. Instruct the DUT to transmit a valid association request with status code 0.
4. Observe transmissions from the DUT.

*Part b: Invalid Status Codes*

1. Instruct the TS to transmit MSDU6.
2. Wait for the DUT to authenticate and associate with the TS.
3. Instruct the DUT to transmit MSDU1 to the DUT.
4. Observe transmissions from the DUT.
5. Repeat for each invalid status code.

*Part c: Two Reserved Elements IDs*

1. Instruct the TS to transmit MSDU6.
2. Wait for the DUT to authenticate and associate with the TS.
3. Instruct the DUT to transmit MSDU2 to the DUT.
4. Observe transmissions from the DUT.

*Part d: Duplicate Valid Element IDs*

1. Instruct the TS to transmit MSDU6.
2. Wait for the DUT to authenticate and associate with the TS.
3. Instruct the DUT to transmit MSDU3 to the DUT.
4. Observe transmissions from the DUT.

*Part e: No Supported Rates*

1. Instruct the TS to transmit MSDU6.
2. Wait for the DUT to authenticate and associate with the TS.
3. Instruct the DUT to transmit MSDU4 to the DUT.
4. Observe transmissions from the DUT.

*Part f: Greater than 8 Supported Rates*

1. Instruct the TS to transmit MSDU6.
2. Wait for the DUT to authenticate and associate with the TS.
3. Instruct the DUT to transmit MSDU5 to the DUT.
4. Observe transmissions from the DUT.

**Observable Results:**

The DUT should:

a. successfully associate and transmit Class 3 traffic.
b. not associate successfully, nor transmit Class 3 traffic. The DUT should send an ACK for the test frames without any system failure.
c-f. successfully associate and transmit Class 3 traffic without any system failure.

**Possible Problems:** None.

**Test #1.1.6: Disassociation Processing**

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

**References:**

[1] IEEE Std 802.11™-2007 Edition, Clause 11.3

**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 Updated:** November 2008

**Discussion:** Disassociation nullifies association and is a notification rather than a request. It is important that a station properly handle a disassociation notice as it partially terminates network connectivity. Disassociation frames can also be sent to a group address to disassociate from all APs at once.

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

Table 5 - Test Frame(s)

| Frame Label | Description |
|---|---|
| MSDU1 | Disassociation from the TS to the DUT containing various reason codes. |
| MSDU2 | Disassociation from the TS to the broadcast address |
| MSDU3 | Disassociation from the TS to the DUT containing invalid FCS. |

**Procedure:**

*Part a: Disassociation Reason Codes*

1. Wait for the DUT to authenticate and associate with the TS.
2. Instruct the TS send MSDU1.
3. Observe transmissions from the DUT.
4. Repeat steps 1-3 for each non-reserved reason code, and once for each reserved.

*Part b: Broadcast Disassociation*

1. Wait for the DUT to authenticate and associate with the TS.
2. Instruct the TS to send MSDU2.
3. Observe transmissions from the DUT.

*Part c: Invalid FCS*

4. Wait for the DUT to authenticate and associate with the TS.
5. Instruct the TS to send MSDU3.
6. Observe transmissions from the DUT.

**Observable Results:**

The DUT should:

a. not transmit class 3 traffic upon reception of MSDU1 for each test frame.
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. not transmit an ACK upon reception of MSDU3, nor process the frame. The DUT should continue transmitting Class 3 traffic.

**Possible Problems:** None.

### Test #1.1.7: Reassociation Processing

**Purpose:** To verify that

- The DUT can transmit an Reassociation Request frame (if implemented).
- The DUT can handle Reassociation Responses with status codes other than “successful.”

**References:**

[1] IEEE Std 802.11™-2007 Edition, Clause 11.3

**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 Updated:** November 2008

**Discussion:** For devices to engage in higher-level communication, such as IP layer, 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. If a device becomes disassociated from a BSS it is possible to re-associate. If A STA attempts reassociation, it should be able to handle all types of reassociation responses, and behave with regards to the reason code within the reassociation response. This test is designed to ensure that a device properly processes re-association responses, and can handle unsuccessful status codes.

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

Table 6 - Test Frame(s)

| Frame Label | Description |
|---|---|
| MSDU1 | Reassociation Responses containing status codes = [1, 8, 12, 256] |
| MSDU2 | Reassociation Response containing two reserved element IDs of length 255-bytes. |
| MSDU3 | Reassociation Response containing duplicate valid element IDs. |
| MSDU4 | Reassociation Response containing no supported rates. |
| MSDU5 | Reassociation Response containing more than 8 supported rates. |
| MSDU6 | Deauthentication from the TS to the DUT. |
| MSDU7 | Disassociation from the TS to the DUT. |

**Procedure:**

*Part a: Successful Reassociation*

1. Instruct the TS to transmit MSDU6.
2. Wait for the DUT to authenticate and associate with the TS.
3. Instruct the TS to transmit MSDU7.
4. Wait for the DUT to re-associate with the TS ( if possible ).
5. Observe transmissions from the DUT.

*Part b: Invalid Status Codes*

1. Instruct the TS to transmit MSDU6.
2. Wait for the DUT to authenticate and associate with the TS.
3. Instruct the DUT to transmit MSDU7.
4. Observe transmissions from the DUT.
5. Repeat for each invalid status code.

*Part c: Two Reserved Elements IDs*

1. Instruct the TS to transmit MSDU6.
2. Wait for the DUT to authenticate and associate with the TS.
3. Instruct the DUT to transmit MSDU2 to the DUT.
4. Observe transmissions from the DUT.
5. Repeat for each invalid status code.

*Part d: Duplicate Valid Element IDs*

1. Instruct the TS to transmit MSDU6.
2. Wait for the DUT to authenticate and associate with the TS.
3. Instruct the DUT to transmit MSDU3 to the DUT.
4. Observe transmissions from the DUT.
5. Repeat for each invalid status code.

*Part e: No Supported Rates*

1. Instruct the TS to transmit MSDU6.
2. Wait for the DUT to authenticate and associate with the TS.
3. Instruct the DUT to transmit MSDU4 to the DUT.
4. Observe transmissions from the DUT.
5. Repeat for each invalid status code.

*Part f: Greater than 8 Supported Rates*

1. Instruct the TS to transmit MSDU6.
2. Wait for the DUT to authenticate and associate with the TS.
3. Instruct the DUT to transmit MSDU5 to the DUT.
4. Observe transmissions from the DUT.
5. Repeat for each invalid status code.

**Observable Results:**

The DUT should:

a. successfully associate and transmit Class 3 traffic.
b. send an ACK for the test frames without any system failure, but not associate successfully, and also not attempt to transmit Class 3 traffic.
c-f. successfully associate and transmit Class 3 traffic without any system failure.

**Possible Problems:** None.

### Test #1.1.8: State Variables and Services

**Purpose:** To verify that

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

**References:**

[1] IEEE Std 802.11™-2007 Edition, Clause 11.3, 11.1.3.2.1

**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 Updated:** November 2008

**Discussion:** For devices to engage in higher-level communication, such as IP layer, 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 station, each station is given a variable that determines that stations authentication and association state with the AP. 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 station is in for communication with the AP, which determines which classes of frames the AP and station may exchange.

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

Table 7 - Test Frame(s)

| Frame Label | Description |
|---|---|
| MSDU1 | Deauthentication from the TS to the DUT |
| MSDU2 | Disassociation from the TS to the DUT |
| MSDU3 | Valid Authentication response |
| MSDU4 | Valid Association response |
| MSDU5 | Valid Reassociation response |
| MSDU6 | Valid ICMP Echo Request from the TS to DUT |
| MSDU7 | ARP Request from the TS to DUT |
| MSDU8 | Probe Request directed to the DUT |
| MSDU9-16 | PS-Poll w/ AID 0-5, 256, 2007 |

**Procedure:**

*Part a: Class 2 traffic in State 1*

1. Instruct the TS to transmit MSDU1 followed by MSDU2.
2. Ensure MSDU2 is transmitted prior to successful authentication.
3. Instruct the TS to transmit MSDU1 followed by MSDU4.
4. Ensure MSDU4 is transmitted prior to successful authentication.
5. Instruct the TS to transmit MSDU1 followed by MSDU5.
6. Ensure MSDU5 is transmitted prior to successful authentication.
7. Observe transmissions from the DUT.

*Part b: Class 3 traffic in State 1*

1. Instruct the TS to transmit MSDU1.
2. Instruct the TS to transmit MSDU6.
3. Instruct the TS to transmit MSDU1.
4. Instruct the TS to transmit MSDU7.
5. Instruct the TS to transmit MSDU1.
6. Instruct the TS to transmit MSDU9.
7. Repeat step 5-6 for MSDU10-16.
8. Observe transmissions from the DUT.

*Part c: Class 3 traffic in State 2*

1. Wait for the DUT to authenticate with the TS.
2. Instruct the TS to transmit MSDU6.
3. Instruct the TS to transmit MSDU7.
4. Instruct the TS to transmit MSDU9.
5. Repeat step 4 for MSDU10-16.
6. Wait for the DUT to authenticate and association with the TS.
7. Instruct the TS to transmit MSDU2.
8. Repeat steps 6-7 prior to transmitting MSDU6, MSDU7, MSDU9-16.
9. 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. Wait for the DUT to authenticate with the TS.
4. Instruct the TS to transmit MSDU8.
5. Wait for the DUT to authenticate and associate with the TS.
6. Instruct the TS to transmit MSDU8.
7. Observe transmissions from the DUT.

**Observable Results:**

The DUT should:

a. respond to MSDU2, and MSDU4-5 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 will transmit an ACK with all zeros in its duration field in response to a data frame with the More Fragments bit set to zero.
- the DUT will transmit an ACK with a properly calculated duration field (duration of data frame minus time to transmit the ACK and a SIFS, with fractional microseconds rounded up) in response to a data frame with the more fragments bit set.
- the DUT will transmit an ACK in response to a directed frame
- the DUT will only transmit an ACK upon reception of frames with a valid FCS.

**References:**

[1] IEEE Std 802.11™-2007 Edition, Subclauses 7.2.1.3, 9.2.2, 9.2.8, 9.6

**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 Updated:** November 2008

**Discussion:** Whenever a directed frame is successfully transmitted from one MAC entity to another, an acknowledgement frame must be transmitted. In the event that the acknowledgement frame is lost (e.g. destination receives frame ok and transmit an ACK for it, but source does not receive the ACK), the transmitter should re-transmit the frame, and the receiver must transmit an ACK for the re-transmitted frame. When the last fragment of a MSDU is received, the ACK should have the duration field set to zero to indicate the medium is available. However, when there are more frames in the MSDU, the acknowledging station must take the duration field from the frame it is acknowledging, subtract two SIFS and the time it took to transmit the ACK, and include the result as its duration field.

**Test Setup:** Place the DUT, TS, and sniffer in a RF isolated environment and in range of each other. Configure the TS for a fragmentation threshold of 256 bytes.

Table 8 - Test Frame(s)

| Frame Label | Description |
|---|---|
| MSDU1 | ICMP Echo Request containing a length of 96-bytes to DUT. |
| MSDU2 | ICMP Echo Request containing a length of 400-bytes to DUT. |
| MSDU3 | Data frame containing a valid FCS |
| MSDU4 | Data frame containing an invalid FCS |
| MSDU5 | CTS frame containing a duration of 32767 μs |
| MSDU6 | Data frame containing a length of 1500-bytes |
| MSDU7 | ICMP Echo Request containing a length of 96-bytes and a SA of a non-authenticated STA to DUT |
| MSDU8 | Data frame containing 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. Instruct the TS to authenticate and associate to the DUT.
2. Instruct the TS to transmit MSDU1.
3. Observe transmissions from the DUT.

*Part b: Calculated Duration Field*

1. Instruct the TS to authenticate and associate to the DUT.
2. Instruct the TS to transmit the first fragment of MSDU2.
3. Instruct the TS to transmit the second fragment of MSDU2.
4. Observe transmissions from the DUT.

*Part c: Frame Check Sequence Validation*

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

*Part d: Large Duration Field Value*

1. Instruct the TS to transmit MSDU5.
2. Instruct the TS to transmit MSDU8.
3. Observe transmissions from the DUT.

*Part e: New Station*

1. Instruct the TS to transmit MSDU7.
2. Observe transmissions from the DUT.

**Observable Results:**

The DUT should:

a. transmit an ACK, for MSDU1, containing 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 containing 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 MSDU8, with an appropriate duration field.
e. transmit an ACK for MSDU7.

**Possible Problems:** None.

**Test #1.1.10: Defragmentation**

**Purpose:** To verify that the DUT is capable of receiving fragments of an arbitrary length, and can properly reassemble these fragments.

**References:**

[1] IEEE Std 802.11™-2007 Edition, Subclauses 9.1.5, 9.5, and A.4.4.1 PC7 (PICS)

**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 Updated:** June 2007

**Discussion:** Defragmentation is the process of assembling successfully received fragments back into the original MSDU or MMPDU. Each fragment contains information in the header that is used to put a sequence of fragments together after the entire sequence has been received. The information that the defragmenting STA must use includes; the frame type, address of sender, sequence control field, and the More Fragments indicator. All STAs must be capable of defragmentation. Since it is possible for source STAs to transmit fragments of an arbitrary length, destination STAs must also be capable of defragmenting fragments of arbitrary length.

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

Table 9 - Test Frame(s)

| Frame Label | Description |
|---|---|
| MSDU1 | ICMP Echo Request containing payload size of 1450 bytes to the DUT |

**Procedure:**

1. Instruct the TS to authenticate and associate with the DUT.
2. Instruct the TS to send MSDU1, fragmented at varying sizes from 256 bytes to 1486 bytes. After MSDU1 has been transmitted at a fragment size, increment the fragment size by 60 bytes and repeat until the fragment size is equal to 1486 bytes.
3. Observe transmissions from the DUT.

**Observable Results:**

The DUT should defragment MSDU1 for each of the fragmentation thresholds used by the TS, and send an ICMP Echo Response for each transmission of MSDU1.

**Possible Problems:** None.

**Test #1.1.11: Duplicate Detection and Recovery**

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

**References:**

[1] IEEE Std 802.11™-2007 Edition, Subclause 9.2.9

**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 Updated:** June 2007

**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. Stations 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 address 2, 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.

Table 10 - Test Frame(s)

| Frame Label | Description |
|---|---|
| MSDU1 | ICMP Echo Request containing a 1000-byte payload. |
| MSDU1r | MSDU1 containing the retry bit set and same Sequence Number as MPDU1. |
| MSDU2q | MSDU1r containing a different Sequence Number. |
| MSDU2qr | MSDU1r containing a different Sequence Number and retry bit unset. |
| MSDU2r | MSDU1r containing the retry bit unset. |
| MSDU3 | ICMP Echo Request containing a 1000-byte payload. |
| MPDU3a | Fragment 0 of MSDU3. |
| MPDU3b | Fragment 1 of MSDU3. |
| MPDU3br | Fragment 1 of MSDU3 containing the retry bit set. |
| MPDU3c | Fragment 1 of MSDU3 containing the retry bit set and different frame body (of same length) than MPDU3b. |
| MSDU4 | ICMP Echo Request containing a 1000-byte payload. |

**Procedure:**

*Part a: Positive Duplicate Detection*

1. Wait for the DUT to authenticate and associate with the TS.
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 MSDU2q.
3. Instruct the TS to transmit MSDU1 followed by MSDU2qr.
4. Instruct the TS to transmit MSDU1 followed by MSDU2r.
5. Instruct the TS to transmit MPDU3a followed by MPDU3br with a 2 * SIFS + ACK time in between each MPDU.

**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 the ICMP Echo Response to the TS.
   - acknowledge but not forward MSDU1r ICMP Echo Response to the TS.
   - acknowledge MPDU3a, MPDU3b, MPDU3c and forward the frame composed of MPDU3a and MPDU3b 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 each MPDU 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 encryption disabled, and a static IP address. Also, the DUT must be 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.
- the DUT sets the Retry Bit in all retransmitted MSDUs.

**References:**

[1] IEEE Std 802.11™-2007 Edition, Subclause 9.2.5.3, 7.1.3.5

**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 Updated:** November 2008

**Discussion:** Each MSDU within a frame exchange should have its own short retry counter (SRC) and long retry counter (LRC), and the station must also keep a separate station short retry counter (SSRC) and station long retry counter (SLRC). When the DUT does not successfully transmit a frame (e.g. 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. Whenever a group frame is successfully transmitted, both the SSRC and SLRC should be reset to 0. A DUT should stop retrying a frame once the MSDU's SRC has reached dot11ShortRetryLimit, or the MSDU's LRC has reached aLongRetryLimit. [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.

Table 11 - Test Frame(s)

| Frame Label | Description |
|---|---|
| MSDU1 | ICMP Echo Request containing a frame length of 512-bytes to STA-E |
| MSDU2 | ICMP Echo Request containing 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. Wait for the DUT to authenticate and associate with the TS.
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. Allow the TS to transmit a CTS in response.
3. 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: 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. Wait for the DUT to authenticate and associate with the TS.
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 MSDU2 exactly dot11ShortRetryLimit times, each RTS with the retry bit set to 0.
b. transmit the ICMP Echo Response in response to MSDU2 exactly dot11LongRetryLimit times.
c. transmit the ICMP Echo Response to MSDU1 exactly dot11ShortRetryLimit times.
d. transmit the first fragment of the ICMP Echo Response dot11ShortRetryLimit times. The DUT should not attempt to transmit any other fragments of the ICMP Echo Response.

**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 MPDU 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 MPDU length.
- An asynchronous data frame is transmitted using the basic access procedure when a RTS/CTS exchange is not used.

**References:**

[1] IEEE Std 802.11™-2007 Edition, Subclauses 9.2.5.4, 9.2.5.6, 9.2.5.7, 9.6, 7.2.1

**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 Updated:** June 2007

**Discussion:** For virtual carrier sense to work properly, RTS and CTS frames must include a properly calculated duration field to indicate to other stations how long the medium will be occupied. The device transmitting an RTS should reserve the medium up until the first ACK of the frame exchange. A CTS frame should be calculated by subtracting (aSIFSTime + aCTSTime) from the RTS frame's duration field. Additionally, both RTS and CTS frames must be transmitted at one of the basic rates so that all stations are aware that the medium will be busy. Consequently, stations must support receiving data frames at a different rate than the rate of the RTS/CTS frames. In order to allow the transmitting station to calculate the duration field for the RTS frame, a receiving station must respond with a CTS at the same rate as the RTS. Since dot11RTSThreshold can be set on a per-station basis, STAs must also be capable of receiving frames larger than their dot11RTSThreshold without a RTS/CTS exchange. A device should process received frames that are longer than its RTS threshold that are not preceded by a RTS/CTS exchange.

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

Table 12 - Test Frame(s)

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

**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.
2. Allow the DUT to authenticate and associate with the TS.
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 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.
2. Allow the DUT to authenticate and associate with the TS.
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.

*Part c: 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 d: 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.

**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:
   - 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.

c. 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.

d. 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.

**Possible Problems:** None.

### Test #1.2.3: 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™-2007 Edition, Subclauses 9.1.5, 9.2.5.6, 9.4, and A.4.4.1 PC6 (PICS)

**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 Updated:** November 2008

**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) as well as the type of network that the frame is to be transmitted in (Ad-hoc or Infrastructure).

For either type of network, if the MSDU or MMPDU is unicast and is larger than the transmitting STA's fragmentation threshold, it should be fragmented before transmission. RTS/CTS may be used immediately preceding the first fragment of the sequence dependingon the RTS thresholdof the transmitting STA. An ACK from the receiving STA immediately following every successfully received fragment is required in this case. The receiving STA will reassemble the fragments after receiving the last fragment.

Each fragment has specific information included by the transmitting STA. This includes the frame type, more fragments indicator bit, destination address, retry bit, sequence number, and fragment number. All of these values should be correctly setup by the source STA before the fragment is transmitted. If they are not correctly setup before transmission, they will not be received or assembled correctly.

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

Table 13 - Test Frame(s)

| Frame Label | Description |
|---|---|
| MSDU1 | ICMP Echo Request containing a frame length of 1500 bytes to the DUT |
| MSDU2 | ICMP Echo Request containing a frame length of 512 bytes to the DUT |
| MSDU3 | ICMP Echo Request containing a frame length of 256 bytes to the DUT |
| MSDU4 | ICMP Echo Request containing a frame length of (3*[fragmentation threshold - 1]) bytes to the DUT |
| MSDU5 | ICMP Echo Request containing a frame length of (3*[fragmentation threshold + 1]) bytes to the DUT |

**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.
2. Wait for the DUT to authenticate and associate to the TS.
3. Instruct the TS to send MSDU1.
4. Instruct the TS to send MSDU2.
5. Instruct the TS to send MSDU3.
6. Observe transmissions from the DUT.

*Part b: Odd Fragmentation Threshold*

1. Disable encryption on the DUT, set the fragmentation threshold equal to 399 bytes, and disable RTS/CTS exchanges.
2. Wait for the DUT to authenticate and associate to the TS.
3. Instruct the TS to send MSDU4 to the DUT
4. Instruct the TS to send MSDU5 to the DUT.
5. Observe transmissions from the DUT.

**Observable Results:**

The DUT should:

a. only uses an RTS/CTS exchange when appropriate (MSDU1), correctly set the More Fragments Bit in all fragments (except the last one), correctly sets the Destination Address in all fragments, correctly maintains the same Sequence Number for all fragments belonging to one MSDU or MMPDU, begins the Fragment Number at 0 and increments it by 1 for each successive fragment belonging to one MSDU or MMPDU.
b. not attempt to break MSDU's down into odd sized fragments. The DUT should round down from the configured odd value if it attempts transmission of fragments.

**Possible Problems:** Software may prevent an odd-fragmentation threshold from being configured, in which case a device shall automatically pass *Part b: Odd Fragmentation Threshold.*

### Test #1.2.4: 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™-2007 Edition, Subclause 9.6

**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 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.

Table 14 - Test Frame(s)

| Frame Label | Description |
|---|---|
| MSDU1 | ICMP Echo Request containing a payload size of 1028-bytes to DUT. |

**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 DUT to authenticate and associate with the TS.
3. Instruct the TS to transmit MSDU1 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 MSDU1 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 MSDU1 at 1 Mbps.
3. Instruct the TS to transmit MSDU1 at 2 Mbps.
4. Instruct the TS to transmit MSDU1 at 5.5 Mbps.
5. Instruct the TS to transmit MSDU1 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 MSDU1 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 MSDU1 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 MSDU1 at 9 Mbps.
3. Instruct the TS to transmit MSDU1 at 18 Mbps.
4. Instruct the TS to transmit MSDU1 at 36 Mbps.
5. Instruct the TS to transmit MSDU1 at 48 Mbps.
6. Instruct the TS to transmit MSDU1 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 #1.2.5: 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™-2007 Edition, Subclause 9.1.5, 9.5

**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 Updated:** June 2007

**Discussion:** Defragmentation is the process of reassembling successfully received fragments back into the original MSDU or MMPDU. Each fragment contains information in the header that is used to put a sequence of fragments together again after the entire sequence has been received. This information that the defragmenting STA must use includes the frame type, address of transmitter, sequence control field, and the More Fragments indicator. All STAs must be capable of defragmentation. Because it is possible for source STAs to transmit fragments of an arbitrary length, destination STAs must be capable of defragmenting fragments of arbitrary length.

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

Table 15 - Test Frame(s)

| Frame Label | Description |
|---|---|
| MSDU1 | ICMP Echo Request containing payload size of 1514-bytes to DUT. |

**Procedure:**

*Part a: Various Threshold Defragmentation*

1. Configure the DUT to use an RTS threshold of 512
2. Wait for the DUT to authenticate and associate with the TS.
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 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 the DUT is using powersave.

**Overview:**
The following tests cover MAC layer operation specific to the configuration of the DUT when using WEP or powersave. In addition to the test specific settings, other configuration values for the DUT, unless otherwise specified, are fragmentation and RTS disabled, and a static IP address. Also, the DUT must be 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™-2007 Edition, Clause 8.2.1 and B.4.4.1 PC2.2 (PICS)

**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 Updated:** November 2008

**Discussion:** Due to the inherent nature of the WLAN environment, there is an opportunity for eavesdropping. Therefore, the Wired Equivalent Privacy (WEP) algorithm was developed. WEP gives 802.11 networks the same amount of security that would be provided on a regular wired network that was 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.

Table 16 - Test Frames

| Frame Label | Description |
|---|---|
| MSDU1 | ICMP Echo Request to the DUT encrypted containing WEP key id 1, with WEP bit set and that includes an invalid ICV field |
| MSDU2 | ICMP Echo Request to the DUT encrypted containing WEP key id 1, with WEP bit set, but does not include the IV or ICV fields |
| MSDU3 | ICMP Echo Request to the DUT encrypted containing 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 the DUT encrypted containing WEP key id 1, with WEP bit set and an IV field that sets all bits in the pad (6 LSB in the Key ID byte) to 1 |
| MSDU5 | ICMP Echo Request to the DUT encrypted containing WEP key id 1, with WEP bit set and valid IV and ICV fields (correctly encrypted ICMP Echo Request) |

**Procedure:**

*Part a: Invalid ICV*

1. Configure the DUT and TS with four WEP keys (if possible):
    - 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. Wait for the DUT to authenticate and associate to the TS.
3. Instruct the TS to send MSDU1 to the DUT.
4. Observe transmissions from the DUT.

*Part b: No IV or ICV*

1. Repeat steps 1 – 2 from Part a.
2. Instruct the TS to send MSDU2 to the DUT.
3. Observe transmissions from the DUT.

*Part c: Invalid IV, ICV, and FCS*

1. Repeat steps 1 – 2 from Part a.
2. Instruct the TS to send MSDU3 to the DUT.
3. Observe transmissions from the DUT.

*Part d: Pad Bits Set*

1. Repeat steps 1 – 2 from Part a.
2. Instruct the TS to send MSDU4 to the DUT.
3. Observe transmissions from the DUT.

*Part e: Proper Encryption, All Keys*

1. Repeat steps 1 – 2 from Part a.
2. Instruct the TS to send MSDU5 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-b. transmit an ACK upon reception of MSDU1, however, not send an ICMP Echo Response.
c. not transmit an ACK upon reception of MSDU3, nor send an ICMP Echo Response.
d. receive the frame without system failure.
e. transmit an ACK for each transmission of MSDU5, and send an ICMP Echo Response.

**Possible Problems:** None.

**Test #1.3.2: TIM Transmission**

**Purpose:** To verify that

- The DUT processes the TIM element of beacons properly.
- The DUT receives broadcast frames properly when the TIM element indicates that there is broadcast traffic.
- The DUT receives directed frames properly when the TIM element indicates that there is directed traffic for the DUT.
- The DUT does not process directed frames when the TIM element indicates that there is no directed or broadcast traffic for the DUT.

**References:**

[1] IEEE Std 802.11™-2007 Edition, Clause 11.2 and A.4.4.1 PC12.2 (PICS)

**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 Updated:** June 2007

**Discussion:** Whenever a station enters power save, the AP is supposed to buffer frames for all stations in power save. In order to ensure the AP doesn't need an infinite amount of memory to buffer the frames, all stations are required to at least wake up on DTIMs when their AID is set in the TIM element of beacons. To keep the size of beacons at a reasonable size, part of the TIM element is the bitmap offset. The bitmap offset is the number of bytes that are not being included in the partial virtual bitmap. This allows for the beacons to be kept to a reasonable size and avoid clogging the medium too much.

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

Table 17 - Test Frames

| Frame Label | Description |
|---|---|
| MSDU1 | ARP Request for the DUT's IP address |
| MSDU2 | ICMP Echo Request to the DUT |

**Procedure:**

*Part a: Broadcast and Directed Without Offset*

1. Configure the DUT to default settings and maximum power save. Disable fragmentation, RTS/CTS exchanges, and encryption. Configure the TS to have a beacon interval of 128 ms and a DTIM period of 3. Also, configure the TS to give the DUT the following AIDs when the DUT associates: 1, 10, 19, 28, 37, 46, 55, 64, 255, 256, 257, 1000, 2000, 2007.
2. Wait for the DUT to authenticate and associate with the TS, with the AID for this iteration.
3. Wait for the DUT to enter power save.
4. Change the TIM of beacons to indicate a broadcast frame is waiting transmission.
5. Transmit MSDU1 after DTIM beacon is transmitted.
6. Change the TIM of beacons to indicate a directed frame for the DUT, with a bitmap offset of 0.
7. Wait for the DUT to transmit a PS Poll, then transmit MSDU2.
8. Observe transmissions from the DUT.
9. Repeat steps 2 – 8 once for each AID.

*Part b: Broadcast and Directed With Maximum Offset*

1. Repeat steps 1 – 5 of Part a.
2. Change the TIM of beacons to indicate a directed frame for the DUT, with the maximum bitmap offset that allows for the inclusion of the DUT’s AID.
3. Wait for the DUT to transmit a PS Poll, then transmit MSDU2.
4. Observe transmissions from the DUT.
5. Repeat steps 1 – 8 once for each AID.

*Part c: Broadcast and Directed Not to DUT Without Offset*

1. Repeat steps 1 – 5 of Part a.
2. Change the TIM of beacons to indicate a directed frame for all AIDs up to 8 greater than the DUT’s AID, other than the DUT’s AID, with a bitmap offset of 0.
3. Wait for the DUT to transmit a PS Poll, then transmit MPDU2.
4. Observe transmissions from the DUT.
5. Repeat steps 1 – 8 once for each AID.

*Part d: Broadcast and Directed Not to DUT With Maximum Offset*

1. Repeat steps 1 – 5 of Part a.
2. Change the TIM of beacons to indicate a directed frame for all AIDs up to 8 greater than the DUT’s AID, other than the DUT’s AID, with the maximum bitmap offset that allows for the inclusion of the DUT’s AID.
3. Wait for the DUT to transmit a PS Poll, then transmit MSDU2.
4. Observe transmissions from the DUT.
5. Repeat steps 1 – 8 once for each AID.

**Observable Results:**
The DUT should:

a. receive and respond to broadcast traffic sent after DTIMs.
b. request its buffered traffic when the Partial Virtual Bitmap indicates that there is directed buffered traffic for the DUT’s AID.
c-d. remain in power save when the Partial Virtual Bitmap indicates that there is no directed traffic being buffered for the DUT’s AID.

**Possible Problems:** The DUT might not remain in power save for a sufficient period of time for this test to complete.

### Test #1.3.3: 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™-2007 Edition, Clause 8.2.1, subclauses 9.1.5, 9.5 and A.4.4.1 PC2.2 (PICS)

**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 Updated:** June 2007

**Discussion:** Defragmentation is the process of reassembling successfully received fragments back into the original MSDU or MMPDU. Defragmentation can be a difficult process for the receiving STA, especially when receiving pieces of different MSDUs or MPDUs at a time. To aid the receiving STA in the assembly process, specific information is included in each fragment by the transmitting STA. Each fragment contains information in the header that is used to put a sequence of fragments together again after the entire sequence has been received. This information that the defragmenting STA must use includes the frame type, address of transmitter, sequence control field, and the More Fragments indicator. All STAs must be capable of defragmentation. Because it is possible for source STAs to transmit fragments of an arbitrary length, destination STAs must be capable of defragmenting fragments of arbitrary length.

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

Table 18 - Test Frame(s)

| Frame Label | Description |
|---|---|
| MSDU1 | ICMP Echo Request containing payload size of 1514-bytes to DUT. |

**Procedure:**

*Part a: Various Threshold Defragmentation*

1. Configure the DUT and TS with four WEP keys (if possible):
   - 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. Wait for the TS to authenticate and associate with the TS.
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 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 | Access Point |
| 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 | Station |
| TS | Testing Station |