Wireless LAN Consortium

802.11abgn

Infrastructure Interoperability Test Suite

Version 4.5

Technical Document

Last Updated: May 27, 2014

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/

Table of Contents

Modification Record

- February 26, 2009 – Version 1.0 Release
    - Daniel Reynolds: Original Document creation.
- January 20, 2011 – Version 2.0 Release
    - Craig Chabot: Revision
- March 9, 2012 – Version 3.0 Release
    - Craig Chabot: Revision
- March 27, 2012 – Version 4.0 Release
    - Craig Chabot: Revision
- April 20, 2012 – Version 4.1 Release
    - Craig Chabot: Revision
- May 17, 2012 – Version 4.2 Release
    - Craig Chabot: Revision
- July 24, 2012 – Version 4.3 Release
    - Craig Chabot: Revision
- September 18, 2012 – Version 4.4 Release
    - Craig Chabot: Addition of test case 1.11, and Revisions
- May 27, 2014 – Version 4.5 Release
    - Mike Bogochow: Fixed formatting and minor errata

Acknowledgments

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

Craig Chabot	University of New Hampshire
Mike Bogochow	University of New Hampshire
Chris McGown	University of New Hampshire
Daniel Reynolds	University of New Hampshire
Jeremy deVries	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.

Note: Successful completion of all tests contained in this suite does not guarantee that the tested device will operate with other compliant 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 well in most environments.

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.

Legend
For Reasons of brevity, the following abbreviations have been used in this test suite:

DUT	Device under test
STA	Test bed Station
AP	Test bed Access Point
LSTA	Legacy Station not capable of using 802.11n
ETH	Ethernet endpoint on the wired side of the network
11n	IEEE 802.11n
OOB	Out of Box Settings
ESS	Extended Service Set

Group 1: 802.11abgn Interoperability

Overview: This group tests various 802.11n features specific to 11n STAs operating in an infrastructure network environment as well as basic interoperability with Legacy Devices. The 801.11n tests are designed to identify problems that IEEE 802.11n compliant devices may have in establishing a link and exchanging packets with each other. It also tests the ability of 11n devices to communicate with both 11n and non-11n devices while 11n and non-11n traffic is being transmitted. The following tables are the default settings for the chosen testbed APs or STAs during testing. These configurations are to be used unless noted otherwise within a test case. The DUT should remain in its OOB settings unless noted otherwise within a test case.

Table - STA Setup

Parameter	Value	Parameter	Value
Security	Open	Number of Spatial Streams	Maximum Supported
Band	2.4 GHz	Channel Width	OOB

Table - AP Setup

Parameter	Value	Parameter	Value
Security	Open	Number of Spatial Streams	Maximum Supported
Band	2.4 GHz	Channel Width	OOB
SSID	Interop	Hidden SSID	Off

Test #1.1: Initial OOB

Purpose: To test for proper scanning, authentication, association and data exchanges between a wireless station and an access point with Open, and varying other Security mechanisms.

References:
- IEEE 802.11n - 2009

Resource Requirements:
- An 802.11n STA and a set of 802.11n APs that can be used as link partners or an 802.11n AP and a set of 802.11n STAs that can be used as link partners.
- An Ethernet station on the distribution system (ETH) capable of transmitting unicast traffic of various sizes
- A monitor configured for capturing and analyzing WLAN MAC frames.

Last Updated: May 17, 2012

Discussion: This will verify the very basics of authentication, association and data exchanges between a STA and an AP. This test verifies the ability of the AP and STA to communicate by transmitting an ICMP Echo Request from the ETH through the AP to the STA. Various size frames are transmitted including the minimum and maximum ETH frame payload.

Test Setup: Place the STA, AP, and sniffer in an RF isolated environment and in range of each other. Attach the ETH to the AP.

1.1.1: Initial OOB – No Security

Procedure: For each AP/STA

1) Allow the STA to Authenticate and Associate to the AP
2) Instruct ETH to transmit ICMP Echo Requests of payload sizes 0, 512, 1468 to the STA

1.1.2: Initial OOB – Open Authentication WEP

Table - STA Setup

Parameter	Value	Parameter	Value
Security	WEP	WEP Key	6162636465 (Hex)

Table - AP Setup

Parameter	Value	Parameter	Value
Security	WEP	WEP Key	6162636465 (Hex)

Procedure: For each AP/STA

1) Allow the STA to Authenticate and Associate to the AP
2) Instruct ETH to transmit ICMP Echo Requests of payload sizes 0, 512, 1468 to the STA

1.1.3: Initial OOB – WPA-PSK TKIP

Table - STA Setup

Parameter	Value	Parameter	Value
Security	WPA-PSK TKIP	PSK	wireless

Table - AP Setup

Parameter	Value	Parameter	Value
Security	WPA-PSK TKIP	PSK	wireless

Procedure: For each AP/STA

1) Allow the STA to Authenticate, Associate and complete the 4-way handshake with the AP
2) Instruct ETH to transmit ICMP Echo Requests of payload sizes 0, 512, 1468 to the STA

1.1.4: Initial OOB – WPA2-PSK AES

Table - STA Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	PSK	wireless

Table - AP Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	PSK	wireless

Procedure: For each AP/STA

1) Allow the STA to Authenticate, Associate and complete the 4-way handshake with the AP
2) Instruct ETH to transmit ICMP Echo Requests of payload sizes 0, 512, 1468 to the STA

1.1.5: Initial OOB – WPA2-TLS AES

Table - STA Setup

Parameter	Value	Parameter	Value
Security	WPA2-TLS AES		

Table - AP Setup

Parameter	Value	Parameter	Value
Security	WPA2-TLS AES		

Procedure: For each AP/STA

1) Allow the STA to Authenticate, Associate and complete the 4-way handshake with the AP
2) Instruct ETH to transmit ICMP Echo Requests of payload sizes 0, 512, 1468 to the STA

1.1.6: Initial OOB – WPA2-PSK AES With Hidden SSID

Table - STA Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	PSK	wireless

Table - AP Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	PSK	wireless
Hidden SSID	On		

Procedure: For each AP/STA

1) Allow the STA to Authenticate, Associate and complete the 4-way handshake with the AP
2) Instruct ETH to transmit ICMP Echo Requests of payload sizes 0, 512, 1468 to the STA

Observable Results:

The DUT should:

- In all cases, verify that the STA and AP connect properly and the STA responds with ICMP responses and the AP passes ICMP echo requests and responses without error and with a ping loss percentage no greater than 5%.

Possible Problems: None

Test #1.2: Spatial Streams

Purpose: To test for proper data exchanges between a wireless station and an access point while using various MCS Rates within each supported Spatial Stream.

References:
- IEEE 802.11n - 2009

Resource Requirements:
- An 802.11n STA and a set of 802.11n APs that can be used as link partners or an 802.11n AP and a set of 802.11n STAs that can be used as link partners.
- An Ethernet station on the distribution system (ETH) capable of transmitting unicast traffic of various sizes
- A monitor configured for capturing and analyzing WLAN MAC frames.

Last Updated: March 9, 2012

Discussion: This will verify the operations of the various MCS Rates for both STAs and APs. Since most real-world devices will be operated with security, AES CCMP will be enabled for this test.

Test Setup: Place the STA, AP and sniffer in an RF isolated environment and in range of each other. Attach the ETH to the AP.

1.2.1: One Spatial Stream

Table - STA Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	Number of Spatial Streams	1
PSK	wireless		

Table - AP Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	Number of Spatial Streams	1
PSK	wireless		

Procedure: For each AP/STA

1) Allow the STA to Authenticate, Associate and complete the 4-way handshake with the AP
2) Instruct ETH to transmit ICMP Echo Requests of payload sizes 0, 512, 1468 to the STA

1.2.2: Two Spatial Streams

Table - STA Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	Number of Spatial Streams	2
PSK	wireless		

Table - AP Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	Number of Spatial Streams	2
PSK	wireless		

Procedure: For each AP/STA

1) Allow the STA to Authenticate, Associate and complete the 4-way handshake with the AP
2) Instruct ETH to transmit ICMP Echo Requests of payload sizes 0, 512, 1468 to the STA

1.2.3: Three Spatial Streams

Table - STA Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	Number of Spatial Streams	3
PSK	wireless		

Table - AP Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	Number of Spatial Streams	3
PSK	wireless		

Procedure: For each AP/STA

1) Allow the STA to Authenticate, Associate and complete the 4-way handshake with the AP
2) Instruct ETH to transmit ICMP Echo Requests of payload sizes 0, 512, 1468 to the STA

1.2.4: Four Spatial Streams

Table - STA Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	Short Guard Interval	Off, On
PSK	wireless	Number of Spatial Streams	4

Table - AP Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	Short Guard Interval	Off, On
PSK	wireless		

Procedure: For each AP/STA

1) Allow the STA to Authenticate, Associate and complete the 4-way handshake with the AP
2) Instruct ETH to transmit ICMP Echo Requests of payload sizes 0, 512, 1468 to the STA

Observable Results:

The DUT should:

- In all cases, verify that the STA and AP connect properly and the STA responds with ICMP responses and the AP passes ICMP echo requests and responses without error and with a ping loss percentage no greater than 5%. The physical layer rates should reflect the utilized number of spatial streams.

Possible Problems: None.

Test #1.3: Short Guard Interval

Purpose: To test for proper data exchanges between a wireless station and an access point while using Short Guard Interval

References:
- IEEE 802.11n - 2009

Resource Requirements:
- An 802.11n STA and a set of 802.11n APs that can be used as link partners or an 802.11n AP and a set of 802.11n STAs that can be used as link partners.
- An Ethernet station on the distribution system (ETH) capable of transmitting unicast traffic of various sizes
- A monitor configured for capturing and analyzing WLAN MAC frames.

Last Updated: March 9, 2012

Discussion: This will verify the operations of the use of the Short Guard Interval for STAs and APs. Since most real-world devices will be operated with security, AES CCMP will be enabled for this test.

Test Setup: Place the STA, AP, and sniffer in an RF isolated environment and in range of each other. Attach the ETH to the AP.

Table - STA Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	Short Guard Interval	On
PSK	wireless		

Table - AP Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	Short Guard Interval	On
PSK	wireless		

Procedure: For each AP/STA

1) Allow the STA to Authenticate, Associate and complete the 4-way handshake with the AP
2) Instruct ETH to transmit ICMP Echo Requests of payload sizes 0, 512, 1468 to the STA

Observable Results:

The DUT should:
- In all cases, verify that the STA and AP connect properly and the STA responds with ICMP responses and the AP passes ICMP echo requests and responses without error and with a ping loss percentage no greater than 5%. The physical layer rates should reflect that Short Guard Interval is in fact being used.

Possible Problems: None

Test #1.4: Channel Width

Purpose: To test for proper data exchanges between a wireless station and an access point while using various channel widths.

References:
- IEEE 802.11n - 2009

Resource Requirements:
- An 802.11n STA and a set of 802.11n APs that can be used as link partners or an 802.11n AP and a set of 802.11n STAs that can be used as link partners.
- An Ethernet station on the distribution system (ETH) capable of transmitting unicast traffic of various sizes
- A monitor configured for capturing and analyzing WLAN MAC frames.

Last Updated: March 9, 2012

Discussion: This will verify the operation of various channel widths between a STA and an AP. 2.4GHz, and 5GHz are defined. All other tests are performed with a single STA and AP. Since most real-world devices will be operated with security, AES CCMP will be enabled for this test.

Test Setup: Place the STA, AP, and sniffer in an RF isolated environment and in range of each other. Attach the ETH to the AP.

1.4.1: 2.4GHz @ 20MHz

Table - STA Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	Band	2.4 GHz
PSK	wireless	Channel Width	20 Mhz

Table - AP Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	Band	2.4 GHz
PSK	wireless	Channel Width	20 Mhz

Procedure: For each AP/STA

1) Allow the STA to Authenticate, Associate and complete the 4-way handshake with the AP
2) Instruct ETH to transmit ICMP Echo Requests of payload sizes 0, 512, 1468 to the STA

1.4.2: 2.4GHz @ 40MHz

Table - STA Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	Band	2.4 GHz
PSK	wireless	Channel Width	40 Mhz

Table - AP Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	Band	2.4 GHz
PSK	wireless	Channel Width	40 Mhz

Procedure: For each AP/STA

1) Allow the STA to Authenticate, Associate and complete the 4-way handshake with the AP
2) Instruct ETH to transmit ICMP Echo Requests of payload sizes 0, 512, 1468 to the STA

1.4.3: 5GHz @ 20MHz

Table - STA Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	Band	5 GHz
PSK	wireless	Channel Width	20 MHz

Table - AP Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	Band	5 GHz
PSK	wireless	Channel Width	20 MHz

Procedure: For each AP/STA

1) Allow the STA to Authenticate, Associate and complete the 4-way handshake with the AP
2) Instruct ETH to transmit ICMP Echo Requests of payload sizes 0, 512, 1468 to the STA

1.4.4: 5GHz @ 40MHz

Table - STA Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	Band	5 GHz
PSK	wireless	Channel Width	40 Mhz

Table - AP Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	Band	5 GHz
PSK	wireless	Channel Width	40 Mhz

Procedure: For each AP/STA

1) Allow the STA to Authenticate, Associate and complete the 4-way handshake with the AP
2) Instruct ETH to transmit ICMP Echo Requests of payload sizes 0, 512, 1468 to the STA

Observable Results:

The DUT should:

- In all cases, verify that the STA and AP connect properly and the STA responds with ICMP responses and the AP passes ICMP echo requests and responses without error and with a ping loss percentage no greater than 5%. The physical layer rate should reflect that a 40MHz channel width is being used in 1.4.2 and 1.4.4.

Possible Problems: None

Test #1.5: Legacy Coexistence

Purpose: To test for proper scanning, authentication, association and data exchanges between a wireless station and an access point with simultaneous 11n and non-11n (Legacy) traffic.

References:

- IEEE 802.11n - 2009

Resource Requirements:

- An 802.11n STA and a set of 802.11n APs that can be used as link partners or an 802.11n AP and a set of 802.11n STAs that can be used as link partners.
- A station capable of 802.11 operations (LSTA)
- An Ethernet station on the distribution system (ETH) capable of transmitting unicast traffic of various sizes
- A monitor configured for capturing and analyzing WLAN MAC frames.

Last Updated: March 9, 2012

Discussion: This will verify the very basics of authentication, association and data exchanges between 11n and non-11n devices. This test verifies the ability of the AP, STA and LSTA to communicate by transmitting ICMP Echo Requests from the ETH through the AP to the STA and LSTA. Various size frames are transmitted including the minimum and maximum frame payload.

Test Setup: Place the STA, LSTA, and AP and sniffer in an RF isolated environment and in range of each other. Attach the ETH to the AP.

1.5.1: No Security

Procedure: For each AP/STA

1) Allow the STA and LSTA to Authenticate and Associate to the AP
2) Instruct ETH to transmit ICMP Echo Requests of payload sizes 0, 512, 1468 to the STA and LSTA

1.5.2: WPA2-PSK AES

Table - LSTA Setup

Parameter	Value	Parameter	Value
Security	WPA2-AES PSK	PSK	wireless

Table - STA Setup

Parameter	Value	Parameter	Value
Security	WPA2-AES PSK	PSK	wireless

Table - AP Setup

Parameter	Value	Parameter	Value
Security	WPA2-AES PSK	PSK	wireless

Procedure: For each AP/STA

1) Allow the STA and LSTA to Authenticate, Associate and complete the 4-way handshake with the AP
2) Instruct ETH to transmit ICMP Echo Requests of payload sizes 0, 512, 1468 to the STA and LSTA

Observable Results:

The DUT should:

- In all cases, verify that the STA and AP connect properly and the STA responds with ICMP responses and the AP passes ICMP echo requests and responses without error and with a ping loss percentage no greater than 5%.

Possible Problems: None.

Test #1.6: MPDU Aggregation and Block Acknowledgment

Purpose: To test for proper data exchanges between a wireless station and an access point while using MPDU aggregation and Block Acknowledgements.

References:

- IEEE 802.11n - 2009

Resource Requirements:

- An 802.11n STA and a set of 802.11n APs that can be used as link partners or an 802.11n AP and a set of 802.11n STAs that can be used as link partners.
- An Ethernet station on the distribution system (ETH) capable of transmitting unicast traffic of various sizes
- A monitor configured for capturing and analyzing WLAN MAC frames.

Last Updated: March 9, 2012

Discussion: This will verify the operations of A-MPDU and Block Acknowledgment (BA) of 11n devices. Reception of these BA frames are required by 11n devices after all A-MPDUs are transmitted. Since most real-world devices will be operated with security, AES CCMP will be enabled for this test.

Test Setup: Place the STA, AP, and sniffer in an RF isolated environment and in range of each other. Attach the ETH to the AP.

Table - STA Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	Aggregate MPDU	On
PSK	wireless	Block Acknowledgement	On

Table - AP Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	Aggregate MPDU	On
PSK	wireless	Block Acknowledgement	On

Procedure: For each AP/STA

1) Allow the STA to Authenticate, Associate and complete the 4-way handshake with the AP
2) The AP and STA should set up a Block Ack and MPDU Aggregation Policy
3) Instruct ETH to transmit 1000 continuous ICMP Echo Requests of payload size 10,000 to the STA

Observable Results:

The DUT should:

- Verify that the STA and AP connect properly and the STA responds with ICMP Responses and the AP passes ICMP echo requests and responses without error with a ping loss percentage no greater than 5%. Either the STA and AP should setup the BA using an ADDBA Request, ADDBA Response followed by the transmission of the ICMP packets, or the STA and AP should setup the BA using an ADDBA Request, ADDBA Response followed by the transmission of ICMP packets and a BAR and BA.

Possible Problems: None

Test #1.7: MSDU Aggregation

Purpose: To test for proper data exchanges between a wireless station and an access point while using A-MSDUs.

References:
- IEEE 802.11n - 2009

Resource Requirements:
- An 802.11n STA and a set of 802.11n APs that can be used as link partners or an 802.11n AP and a set of 802.11n STAs that can be used as link partners.
- An Ethernet station on the distribution system (ETH) capable of transmitting unicast traffic of various sizes
- A monitor configured for capturing and analyzing WLAN MAC frames.

Last Updated: March 9, 2012

Discussion: This will verify the operation of A-MSDU for 11n devices. A-MSDU is only required upon reception. Transmission will be tested only on devices that support this feature. ICMP Echo Request frames will be transmitted from the ETH to the STA through the AP and aggregated by either the STA, AP or both. At least one device, that is not the DUT, must be able to transmit A-MSDUs to complete this test. Since most real-world devices will be operated with security, AES CCMP will be enabled for this test.

Test Setup: Place the STA, AP, and sniffer in an RF isolated environment and in range of each other. Attach the ETH to the AP.

Table - STA Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	Aggregate MSDU	On
PSK	wireless		

Table - AP Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	Aggregate MSDU	On
PSK	wireless		

Procedure: For each AP/STA

1) Allow the STA to Authenticate, Associate and complete the 4-way handshake with the AP
2) The AP and STA should set up an MSDU Aggregation Policy
3) Instruct ETH to transmit 1000 continuous ICMP Echo Requests of payload size 10,000 to the STA

Observable Results:

The DUT should:
- Verify that the STA and AP connect properly and the STA responds with ICMP Responses and the AP passes ICMP echo requests and responses without error with a ping loss percentage no greater than 5%. The STA or AP should aggregate frames into one A-MSDU before transmission.

Possible Problems: None

Test #1.8: Packet Error Rate

Purpose: To determine if the DUT can exchange packets with a link partner such that the exchange of packets must produce a packet error rate that is low enough to meet a desired rate.

References:
- IEEE 802.11n – 2009

Resource Requirements:
- An 802.11n STA and a set of 802.11n APs that can be used as link partners or an 802.11n AP and a set of 802.11n STAs that can be used as link partners.
- An Ethernet station on the distribution system (ETH) capable of transmitting unicast traffic of various sizes
- A monitor configured for capturing and analyzing WLAN MAC frames.

Last Updated: March 9, 2012

Discussion: The standard does not specify PER with respect to security. Therefore security will NOT be enabled in this case. Packet Error Rate Interoperability testing ensures that stations and access points can correctly pass large volumes of traffic over the network with minimal errors. A single vendor's access point will be powered up and the other stations should associate with it. The access point will broadcast the multicast traffic generated by an Ethernet station onto the wireless media. Multicast traffic does not use RTS/CTS, ACK frames, retries, or fragmentation, which simplifies the Packet Error Rate calculation; however, in an infrastructure network this will only be the case for traffic coming from the distribution system. For the DSSS PHY, all multicast frames should be sent at a basic rate. The stations and access point should stay connected and pass traffic with at least 90% efficiency.

The underlying issues, which cause bit errors in the transmission of packets in this testing process, have the tendency to vary due to the statistical nature of such events. In past testing, the UNH-IOL has observed a significant variation in the number of packets in error for a given set up after running the test multiple times. **The results obtained from this testing process should therefore not be seen as a true measure of the bit error rate, but as information that may suggest the need for further analysis.**

Test Setup: Place the STA, AP, and sniffer in an RF isolated environment and in range of each other. Attach the ETH to the AP.

Table - STA Setup

Parameter	Value	Parameter	Value
Security	Open	Power Save	Off

Table - AP Setup

Parameter	Value	Parameter	Value
Security	Open		

Procedure: For each AP/STA

1) Allow the STA to Authenticate and Associate to the AP
2) Instruct the ETH to transmit a continuous stream of 10000 128 byte frames at a rate of 50 frames per second to the STA using the multicast traffic generator

Observable Results:

The DUT should:
- The PER should be no more than 10% of the total packets sent. This value should be examined with other information gathered during the testing process to ensure that the failure is due to bit errors and not resource errors on the testing stations or the distribution system.

Possible Problems: None.

Test #1.9: Failover / Reassociation

Purpose: To observe the behavior of the DUT when an AP within an ESS fails and is forced to Reassociate with another AP within the ESS. Note that this test is only for STAs.

References:
- IEEE 802.11n - 2009

Resource Requirements:
- An 802.11n STA and a set of 802.11n APs that can be used as link partners.
- An Ethernet station on the distribution system (ETH) capable of transmitting unicast traffic of various sizes
- A monitor configured for capturing and analyzing WLAN MAC frames.

Last Updated: March 9, 2012

Discussion: Failover / Reassociation Interoperability testing tests to ensure that a station will scan, assess, and reconnect to other APs if the one it previously was connected to becomes unavailable. If a station loses connection to an AP, it should scan the other available channels until it finds another AP that is an acceptable replacement. After probing and gathering information, a station may associate to this new AP by Authenticating and then using either Reassociation or Association to connect.

Test Setup: Place the STA, APs, and sniffer in an RF isolated environment and in range of each other. Attach the ETH to the AP.

1.9.1: No Security

Procedure:

1) Allow the STA to Authenticate and Associate to the first AP
2) Instruct the ETH to transmit a continuous stream of ICMP Echo Requests to the STA
3) Power on the second AP and verify that it is beaconing
4) Power off the first AP and wait for the STA to Reassociate and continue replying to ICMP Echo Requests.
5) Repeat this process until each AP has acted as the AP to which the STA Reassociated (This includes the first AP)

1.9.2: WPA2-PSK AES

Table - STA Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	PSK	wireless

Table - AP Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	PSK	wireless

Procedure:

1) Allow the STA to Authenticate and Associate to the first AP
2) Instruct the ETH to transmit a continuous stream of ICMP Echo Requests to the STA
3) Power on the second AP and verify that it is beaconing
4) Power off the first AP and wait for the STA to Reassociate and continue replying to ICMP Echo Requests.
5) Repeat this process until each AP has acted as the AP to which the STA Reassociated (This includes the first AP)

Observable Results:

The DUT should:

- When the AP within the ESS fails, the STA previously Associated with the AP should Reassociate with the new AP without appreciable packet loss occurring.

Possible Problems: None

Test #1.10: Varying ICMP Payload Ping Loss Threshold

Purpose: To give an informative set of data relating to the ping loss percentage at varying ICMP payload sizes with a constant ICMP timeout value.

References:

- IEEE 802.11n - 2009

Resource Requirements:

- An 802.11n STA and a set of 802.11n APs that can be used as link partners or an 802.11n AP and a set of 802.11n STAs that can be used as link partners.
- An Ethernet station on the distribution system (ETH) capable of transmitting unicast traffic of various sizes
- A monitor configured for capturing and analyzing WLAN MAC frames.

Last Updated: September 18, 2012

Discussion: This test is informative and as such will not be based on Pass/Fail criteria. This test will show the theoretical limits of interoperability between different AP/STA pairs with a fixed ICMP timeout and increasing payload sizes. Poor results will not necessarily reflect poor operation on the DUT, but could show poor operation between the DUT and a specific device in the testbed.

Test Setup: Place the STA, AP, and sniffer in an RF isolated environment and in range of each other. Attach the ETH to the AP.

1.10.1: No Security

Procedure: For each AP/STA

1) Allow the STA to Authenticate and Associate to the AP
2) Instruct the ETH to transmit ICMP Echo Requests of payload sizes 2,000, 4,000, 6,000, 8,000, 10,000, 12,000, 14,000, 16,000, 18,000, 20,000 bytes to the STA
3) Record the Ping Loss Percentage for each payload size

1.10.2: WPA2-PSK AES

Table - STA Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	PSK	wireless

Table - AP Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	PSK	wireless

Procedure: For each AP/STA

1) Allow the STA to Authenticate and Associate to the AP
2) Instruct the ETH to transmit ICMP Echo Requests of payload sizes 2,000, 4,000, 6,000, 8,000, 10,000, 12,000, 14,000, 16,000, 18,000, 20,000 bytes to the STA
3) Record the Ping Loss Percentage for each payload size

Observable Results:

The DUT should:

- Respond to ICMP Echo Requests of varying sizes as efficiently as possible. As this test case is informative, there are no strict Pass/Fail criteria.

Possible Problems: None

Test #1.11: Varying ICMP Timeout Ping Loss Threshold

Purpose: To give an informative set of data relating to the ping loss percentage at varying ICMP timeout values with a constant ICMP payload size.

References:
- IEEE 802.11n - 2009

Resource Requirements:
- An 802.11n STA and a set of 802.11n APs that can be used as link partners or an 802.11n AP and a set of 802.11n STAs that can be used as link partners.
- An Ethernet station on the distribution system (ETH) capable of transmitting unicast traffic of various sizes
- A monitor configured for capturing and analyzing WLAN MAC frames.

Last Updated: September 18, 2012

Discussion: This test is informative and as such will not be based on Pass/Fail criteria. This test will show the theoretical limits of interoperability between different AP/STA pairs with a fixed ICMP payload size and decreasing ICMP timeout values. Poor results will not necessarily reflect poor operation on the DUT, but could show poor operation between the DUT and a specific device in the testbed.

Test Setup: Place the STA, AP, and sniffer in an RF isolated environment and in range of each other. Attach the ETH to the AP.

1.11.1: No Security

Procedure: For each AP/STA

1) Allow the STA to Authenticate and Associate to the AP
2) Instruct the ETH to transmit ICMP Echo Requests of payload size 10000 to the STA at ICMP timeout values 50, 40, 30, 20, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1
3) Record the Ping Loss Percentage for each timeout value

1.11.2: WPA2-PSK AES

Table - STA Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	PSK	wireless

Table - AP Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	PSK	wireless

Procedure: For each AP/STA

1) Allow the STA to Authenticate and Associate to the AP
2) Instruct the ETH to transmit ICMP Echo Requests of payload size 10000 to the STA at ICMP timeout values 50, 40, 30, 20, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1
3) Record the Ping Loss Percentage for each timeout value

Observable Results:

The DUT should:

- Respond to ICMP Echo Requests at varying timeouts as efficiently as possible. As this test case is informative, there are no strict Pass/Fail criteria.

Possible Problems: None