Wireless LAN Consortium

802.11ac

Infrastructure Interoperability Test Suite

Version1.0

Technical Document

Last Updated: April 12, 2013

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

- March 4, 2013 – Version 1.0 Release
    - Craig Chabot

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

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
ETH	Ethernet endpoint on the wired side of the network
11ac	IEEE 802.11ac
OOB	Out of Box Settings
ESS	Extended Service Set
VHT	Very High Throughput (Term used for 802.11ac specific devices)
SGI	Short Guard Interval

Group 1: 802.11ac Interoperability

Overview: This group tests various VHT features specific to 11ac devices operating in an infrastructure network environment. The 801.11ac tests are designed to identify problems that IEEE 802.11ac compliant devices may have in establishing a link and exchanging packets with each other. 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
Channel Width	OOB		

Table - AP Setup

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

Test #1.1: OOB Basic Ping Interoperability

Purpose: To test for proper scanning, authentication, association and data exchanges between a wireless station and an access point with Open, and WPA2-PSK Security.

References:

- IEEE 802.11ac - Draft3.0

Resource Requirements:

- An 802.11ac STA and a set of 802.11ac APs that can be used as link partners or an 802.11ac AP and a set of 802.11ac 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: April 4, 2013

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. In addition, through observing the physical layer rates of the ICMP data packets, this test confirms the use of the supported number of spatial streams as well as the use of optional VHT supported features such as short guard interval and 256QAM.

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: OOB Basic Ping Interoperability – No Security

Procedure: For each AP/STA

1) Allow the STA to Authenticate and Associate to the AP
2) Observe the Association Response of the AP to discern the number of spatial streams to be used as well as the support of SGI and 256QAM
3) Instruct ETH to transmit ICMP Echo Requests of payload sizes 0, 512, 1468 to the STA

1.1.2: OOB Basic Ping Interoperability – 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) Observe the Association Response of the AP to discern the number of spatial streams to be used as well as the support of SGI and 256QAM
3) Instruct ETH to transmit ICMP Echo Requests of payload sizes 0, 512, 1468 to the STA

1.1.3 : OOB Basic Ping Interoperability – 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) Observe the Association Response of the AP to discern the number of spatial streams to be used as well as the support of SGI and 256QAM
3) 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 Echo Replies and the AP transmits ICMP Echo Requests without error and with a ping loss percentage no greater than 5%. The physical layer rates of the DUT should reflect the supported number of spatial streams, as well as the use of 256QAM and Short Guard Interval if supported.

Possible Problems: None

Test #1.2: Channel Width

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

References:

- IEEE 802.11ac - Draft3.0

Resource Requirements:

- An 802.11ac STA and a set of 802.11ac APs that can be used as link partners or an 802.11ac AP and a set of 802.11ac 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: April 4, 2013

Discussion: This will verify the operation of various channel widths between a STA and an AP. Note that per the IEEE 802.11ac Standard Section 4.3.10a, every VHT device must have support for 20MHz, 40MHz, and 80MHz Channel Width operation, therefore test cases 1.2.1-3 are mandatory. 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: 20 MHz

Table - STA Setup

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

Table - AP Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	Channel Width	20 Mhz
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: 40 MHz

Table - STA Setup

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

Table - AP Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	Channel Width	40 Mhz
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: 80 MHz

Table - STA Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	Channel Width	80 MHz
PSK	wireless		

Table - AP Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	Channel Width	80 MHz
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: 80+80 MHz

Table - STA Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	Channel Width	80+80 MHz
PSK	wireless		

Table - AP Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	Channel Width	80+80 MHz
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

1.2.5: 160 MHz

Table - STA Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	Channel Width	160 MHz
PSK	wireless		

Table - AP Setup

Parameter	Value	Parameter	Value
Security	WPA2-PSK AES	Channel Width	160 MHz
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 Echo Replies and the AP transmits ICMP Echo Requests without error and with a ping loss percentage no greater than 5%. The physical layer rates of the DUT should reflect the specified channel width of each performed test case.

Possible Problems: None

Test #1.3: MPDU Aggregation

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

References:

- IEEE 802.11ac - Draft3.0

Resource Requirements:

- An 802.11ac STA and a set of 802.11ac APs that can be used as link partners or an 802.11ac AP and a set of 802.11ac 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: April 4, 2013

Discussion: This will verify the operations of A-MPDU and Block Acknowledgment (BA) of 11ac devices. Reception of these BA frames are required by HT and VHT devices after all A-MPDUs are transmitted. Note that per the IEEE 802.11ac Standard Section 4.3.10a, every VHT device must have support for A-MPDU, therefore this test case is mandatory. 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	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) 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:

- In all cases, verify that the STA and AP connect properly and the STA responds with ICMP Echo Replies and the AP transmits ICMP Echo Requests without error and 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 #1.4: MSDU Aggregation

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

References:

- IEEE 802.11ac - Draft3.0

Resource Requirements:

- An 802.11ac STA and a set of 802.11ac APs that can be used as link partners or an 802.11ac AP and a set of 802.11ac 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: April 4, 2013

Discussion: This will verify the operation of A-MSDU for 11ac devices. 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:

- In all cases, verify that the STA and AP connect properly and the STA responds with ICMP Echo Replies and the AP transmits ICMP Echo Requests without error and 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 #1.5: 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 802.11ac - Draft3.0

Resource Requirements:

- An 802.11ac STA and a set of 802.11ac 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: April 4, 2013
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.

1.5.1: 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)

1.5.2 : 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 #1.6: 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 802.11ac - Draft3.0

Resource Requirements:

- An 802.11ac STA and a set of 802.11ac APs that can be used as link partners or an 802.11ac AP and a set of 802.11ac 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: April 4, 2013

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.

1.6.1: 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, 12,000, 12,000, 14,000, 16,000, 18,000, 20,000 bytes to the STA
3) Record the Ping Loss Percentage for each payload size

1.6.2 : 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 #1.7: 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 802.11ac - Draft3.0

Resource Requirements:

- An 802.11ac STA and a set of 802.11ac APs that can be used as link partners or an 802.11ac AP and a set of 802.11ac 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: April 4, 2013

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.

1.7.1: 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

1.7.2 : 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