UNH-IOL TEST SUITE

OFDM .11a Interoperability Tests

Technical Document

Version 2.0

InterOperability Laboratory
Research Computing Center
University of New Hampshire
http://www.iol.unh.edu

Chase OE bldg, room 201
Durham, NH 03824
Phone: (603) 862-0189
Fax: (603) 862-0898

Version 1.1	KJK	802.11a included	11/01/2001
Version 1.0		802.11b version	7/2001
Version 2.0	EMF	Edits and PER changes	6/2002

The following table contains possible results and their meanings.

Result	Interpretation
PASS	The DUT was observed to exhibit conformant behavior.
FAIL	The DUT was observed to exhibit non-compliant behavior.
PASS With Comments	The DUT was observed to exhibit conformant behavior, however this behavior deviated from previous compliant results. An additional explanation of the situation is included.
Warning	The DUT was observed to exhibit behavior that is not recommended.
Refer to Comments	From the observations, a valid pass or fail could not be determined. An additional explanation of the situation is included.
Not Applicable	The DUT does not support the technology required to perform these tests.
Not Available	Due to testing station or time limitations, the tests could not be performed, or were performed in a limited capacity.
Not Tested	Not tested due to time constraint of the test period.
Not Implemented	The corresponding section of the test is presently unimplemented, but will be implemented in the future.
Informative	Results are for informative purposes only and are not judged on a pass or fail basis.

Test Label: **Basic Point to Point Interoperability Test**

Purpose:
To observe and monitor authentication, association and data transfer for point-to-point operation between each unique pair of stations and access points using IEEE 802.11a physical layers.

References: IEEE Standards 802.11-1999, 802.11a-1999

Last Modification: January 29, 2002

Resources Requirements:

- Two OFDM PHY stations capable of participating in an infrastructure BSS
- An OFDM PHY access point
- An Ethernet station on the distribution system connected to the AP
- An Wireless station on the distribution system connected to the AP
- Wireless OFDM PHY sniffer to promiscuously capture traffic
- Software implementation capable of generating traffic (ICMP echo requests) of varying sizes

Discussion:
Point to point interoperability testing between stations and access points will have two stations and a single access point powered up. ICMP echo requests will be sent from the stations to both the other wireless station and a station on the Ethernet backbone. This process should be monitored with a wireless sniffer. To ensure basic interoperability, we identify simple problems that might be hard to find in more complex testing. Every unique station and AP pair will be tested.

After completion of the basic interoperability with all settings turned off, we will change the RTS and fragmentation threshold settings to test each operation independently.

The OFDM PHY also uses different block sizes for different frame rates and will need to fill in a frame with dummy bytes to fill out the remaining symbol of any frame that is not a multiple integer of the block size used. As a frame of any data rate will consist of symbols containing multiples of 6, 12, 24, or 36 bytes, a fragmentation threshold of 288 is a multiple of all of these. A frame of 289 will therefore have the last fragment containing only one byte of data and between 5 to 35 filler bytes to complete the symbol.

Test Setup:
The DUT and the sniffer shall be positioned so they can receive each other.

- ICMP payload sizes = 0, 101, 288, 289, 1468 (IP and MAC headers will increase total packet size by 64 bytes) 64, 165, 352, 353, 1532
- Beacon Interval = 128 Kus
- Fragmentation Threshold = 2300 or no fragmentation
- RTS threshold =2300 or no RTS/CTS
- Short and Long retry limit = 8
- Basic rates 6, 12, 24 Mbps
- Authentication is open system

Procedure:
For each unique set of stations and access point group:

A. **Basic test** - Power up the AP followed by the stations. Issue ping requests from each station with various sized data payloads to both a station on the wired network and to the other wireless station.

B. **RTS/CTS and Fragmentation test** – Use the largest and smallest ping sizes from the basic test. Set RTS threshold to 256 on STA and AP. Also set fragmentation threshold to 288 on STA and AP. Only ping the Ethernet station.

C. **Rate test** – the AP is configured to allow for one basic rate and no extended rates. This test will be repeated for each rate supported. Proprietary 72Mbps and 108 Mbps modes may be used if supported by multiple vendors. A consecutive range of ICMP payload sizes will be used as follows with the following rates:

Rate (Mbps)	Payload range (Bytes)		Frame size (Bytes)
6 or 9	224-229		288-293
12 or 18	224-235		288-299
24 or 36	224-247		288-311
48 or 54	224-260		288-323

Possible Problems:

- ICMP echo requests only generated by the wireless station not a wired station
- Input power levels are not measured
- Traffic between an AP and Station should be either translation or encapsulation. Translation (IEEE 802.1h or RFC1042) is preferred.

Observable results:
The wireless stations should stay synchronized and pass ICMP echo requests and responses without error.

Procedure A Basic Test:

	Verify proper association
	The wireless stations should stay synchronized and pass ICMP echo requests and responses without error.
	Verify proper association
	The wireless stations should stay synchronized and pass ICMP echo requests and responses without error.
	Verify proper association
	The wireless stations should stay synchronized and pass ICMP echo requests and responses without error.
	Verify proper association
	The wireless stations should stay synchronized and pass ICMP echo requests and responses without error.

Procedure B RTS/CTS -Fragmentation test:

	Verify proper association
	The wireless stations should stay synchronized and pass ICMP echo requests and responses without error.
	An RTS frame should proceed any directed MPDUs that exceed RTS threshold
	Upon receiving a RTS frame the station should send a CTS frame within a SIFS if the medium is not busy
	Directed MPDUs that exceed the fragmentation threshold should be fragmented.
	The more fragments bit should be set if applicable
	Verify proper association
	The wireless stations should stay synchronized and pass ICMP echo requests and responses without error.
	An RTS frame should proceed any directed MPDUs that exceed RTS threshold
	Upon receiving a RTS frame the station should send a CTS frame within a SIFS if the medium is not busy
	Directed MPDUs that exceed the fragmentation threshold should be fragmented.
	The more fragments bit should be set if applicable
	Verify proper association
	The wireless stations should stay synchronized and pass ICMP echo requests and responses without error.
	An RTS frame should proceed any directed MPDUs that exceed RTS threshold
	Upon receiving a RTS frame the station should send a CTS frame within a SIFS if the medium is not busy
	Directed MPDUs that exceed the fragmentation threshold should be fragmented.
	The more fragments bit should be set if applicable

Procedure B RTS/CTS –Fragmentation:

	Verify proper association
	The wireless stations should stay synchronized and pass ICMP echo requests and responses without error.
	An RTS frame should proceed any directed MPDUs that exceed RTS threshold
	Upon receiving a RTS frame the station should send a CTS frame within a SIFS if the medium is not busy
	Directed MPDUs that exceed the fragmentation threshold should be fragmented.
	The more fragments bit should be set if applicable

Procedure C Rate test:

	Verify proper association
DID WE DO A RATE TEST??????	The wireless stations should stay synchronized and pass ICMP echo requests and responses without error.

Test Label: **PSP Point to Point Interoperability Test**

Purpose:
To determine that:

- The STA is setting the Power Management bit to the appropriate value in the Frame Control field
- The STA uses correct frames (PS-Poll or Null Frame) to indicate it wants to retrieve queued data from its corresponding AP.
- The AP correctly indicates queued data to corresponding stations and forwards the data upon the receipt of either a PS-Poll frame or frame with a Frame Control field indicating the station is in CAM mode (e.g. Null frame).

References: IEEE 802.11-1999, Clause 11.2.1

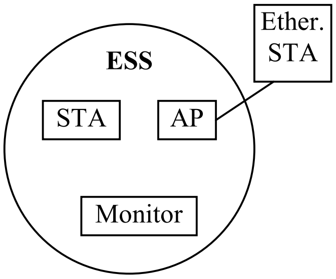
Last Modification: October 29, 2001

Resource Requirements:

- A monitor configured for capturing and analyzing MAC frames.
- An Ethernet station on the AP distribution system.

Discussion:
Power Management is used to allow stations to conserve power by running in a "Doze" mode, wherein a STA is not able to transmit or receive and consumes very low power. Stations inform the AP of its Power Management status through a successful frame exchange initiated by the STA, setting the Power Management bit to the appropriate value in the Frame Control field. A STA in Power Save mode will power down if it is not transmitting any data and has no data buffered for it by the AP. Stations learn of data queued at the AP for it through the Traffic Indication Map (TIM), which is transmitted in the Beacon frame by the AP. A STA wakes up every defined listen interval to check for queued data. If there is buffered data, it transmits PS-POLL frames for the received data until the AP no longer has any buffered data for the STA. The STA then powers down, waking up at listen intervals and DTIMs to check the beacons for queued data.

There is also a vendor implemented "Fast Power Save" in addition to the Power Management outlined in the IEEE 802.11 Standard, in which a STA switches into "Awake" mode (i.e. Fully powered) and acts normally for a period of time before returning to "Doze" mode. This increases efficiency in data transfer but reduces efficiency in power savings. The tests outlined do not utilize "Fast Power Save" unless the Product only implements "Fast Power Save" and the results will be noted as such.



Test Setup: See diagram. Setup the ESS as shown.

- Set DTIM Interval on AP to 3
- Power Save on STA enabled
- Beacon Interval = 100 Kus
- Authentication is open system

Procedure:
A. Power on AP and then STA. Use a Monitor to observe and record Probe Requests, Beacons, the Authentication and Association between AP and STA.

B. Using a station located on the distribution system, begin sending directed ping packets to the DUT. You should observe that the AP is queuing the data and upon a PS-Poll or Null data frame forwarding out the packets to the station. Next, send UDP directed packets to the STA. You should observe that the AP sends out the queued multicast traffic only after its DTIM beacons, but before it sends out queued directed frames.

Observable Results:

STA –
Procedure A:

	Association is performed properly
	Association is performed properly
	Association is performed properly
	Association is performed properly

Procedure B:

	STA should wake up to receive DTIM beacons
	Verify receipt of multicast/broadcast data frames
	Verify STA sleeps after receipt of DTIM
	Verify STA uses PS-Polls or changes PS state to receive queued unicast traffic (verify AID is set in beacon)
	Verify STA uses frame exchanges to notify AP of PS state change
	STA should wake up to receive DTIM beacons
	Verify receipt of multicast/broadcast data frames
	Verify STA sleeps after receipt of DTIM
	Verify STA uses PS-Polls or changes PS state to receive queued unicast traffic (verify AID is set in beacon)
	Verify STA uses frame exchanges to notify AP of PS state change
	STA should wake up to receive DTIM beacons
	Verify receipt of multicast/broadcast data frames
	Verify STA sleeps after receipt of DTIM
	Verify STA uses PS-Polls or changes PS state to receive queued unicast traffic (verify AID is set in beacon)
	Verify STA uses frame exchanges to notify AP of PS state change
	STA should wake up to receive DTIM beacons
	Verify receipt of multicast/broadcast data frames
	Verify STA sleeps after receipt of DTIM
	Verify STA uses PS-Polls or changes PS state to receive queued unicast traffic (verify AID is set in beacon)
	Verify STA uses frame exchanges to notify AP of PS state change

AP –
Procedure A:

	Association is performed properly
	Association is performed properly
	Association is performed properly
	Association is performed properly
	Association is performed properly
	Association is performed properly

Procedure B:

	AP should be queuing all data for stations in Power Save state.
	Verify the TIM indicates in beacons whether the AP 1) has broadcast/multicast traffic queued 2) has the AIDs set for STAs that have data queued (if any).
	Verify AP is sending all queued broadcast/multicast traffic during DTIM period.
	Verify AP is sending all directed data frames as STAs change states
	Verify AP sends all queued broadcast/multicast first, and directed frames second.
	Verify AP is setting the More Data bit if it has more broadcast/multicast or unicast frames queued.
	Verify AP is not setting the More Data bit on the last broadcast/multicast or unicast frame queued.

Procedure B (cont'd):

	AP should be queuing all data for stations in Power Save state.
	Verify the TIM indicates in beacons whether the AP 1) has broadcast/multicast traffic queued 2) has the AIDs set for STAs that have data queued (if any).
	Verify AP is sending all queued broadcast/multicast traffic during DTIM period.
	Verify AP is sending all directed data frames as STAs change states
	Verify AP sends all queued broadcast/multicast first, and directed frames second.
	Verify AP is setting the More Data bit if it has more broadcast/multicast or unicast frames queued.
	Verify AP is not setting the More Data bit on the last broadcast/multicast or unicast frame queued.
	AP should be queuing all data for stations in Power Save state.
	Verify the TIM indicates in beacons whether the AP 1) has broadcast/multicast traffic queued 2) has the AIDs set for STAs that have data queued (if any).
	Verify AP is sending all queued broadcast/multicast traffic during DTIM period.
	Verify AP is sending all directed data frames as STAs change states
	Verify AP sends all queued broadcast/multicast first, and directed frames second.
	Verify AP is setting the More Data bit if it has more broadcast/multicast or unicast frames queued.
	Verify AP is not setting the More Data bit on the last broadcast/multicast or unicast frame queued.
	AP should be queuing all data for stations in Power Save state.
	Verify the TIM indicates in beacons whether the AP 1) has broadcast/multicast traffic queued 2) has the AIDs set for STAs that have data queued (if any).
	Verify AP is sending all queued broadcast/multicast traffic during DTIM period.
	Verify AP is sending all directed data frames as STAs change states
	Verify AP sends all queued broadcast/multicast first, and directed frames second.
	Verify AP is setting the More Data bit if it has more broadcast/multicast or unicast frames queued.
	Verify AP is not setting the More Data bit on the last broadcast/multicast or unicast frame queued.
	AP should be queuing all data for stations in Power Save state.
	Verify the TIM indicates in beacons whether the AP 1) has broadcast/multicast traffic queued 2) has the AIDs set for STAs that have data queued (if any).
	Verify AP is sending all queued broadcast/multicast traffic during DTIM period.
	Verify AP is sending all directed data frames as STAs change states
	Verify AP sends all queued broadcast/multicast first, and directed frames second.
	Verify AP is setting the More Data bit if it has more broadcast/multicast or unicast frames queued.
	Verify AP is not setting the More Data bit on the last broadcast/multicast or unicast frame queued.

Test Label: **WEP Point to Point Interoperability Test**

Purpose:
To observe and monitor authentication, association and data transfer for point-to-point WEP operation between each unique pair of stations and access points using an OFDM PHY.

References: IEEE Standards 802.11-1999, IEEE 802.11a-1999

Last Modification: October 29, 2001

Resources Requirements:

- OFDM PHY STAs capable of participating in an infrastructure BSS using WEP
- An OFDM PHY access point capable of participating in an infrastructure BSS using WEP
- A wireless sniffer to promiscuously capture traffic
- Software implementation capable of generating traffic (ICMP echo requests) of varying size

Discussion:
In a wired LAN, only those stations physically connected to the wire may hear LAN traffic. With a wireless shared medium, this is not the case. Any IEEE 802.11-compliant STA may hear all like-PHY IEEE 802.11 traffic that is within range. Thus, the connection of a single wireless link (without privacy) to an existing wired LAN may seriously compromise the security of the wired LAN.

To bring the functionality of the wireless LAN up to the level implicit in wired LAN design, IEEE 802.11 provides the ability to encrypt the contents of messages. IEEE 802.11 specifies an optional privacy algorithm [WEP] that is designed to satisfy the goal of wired LAN “equivalent” privacy. The algorithm is not designed for ultimate security but rather to be “at least as security as a wire”.

Optionally running the test with multiple features such as fragmentation and power save enabled allows an opportunity for a more complicated operating environment. Interdependent problems that do not appear when each feature is tested independently will become apparent more easily if present. If a device is previously found to not implement one of the features correctly in the independent configuration testing then that feature will be disabled for this part of the test and noted as such in the results.

Test Setup:
The DUT and the sniffer shall be positioned so they can receive each other.

- ICMP payload sizes = 0, 101, 288, 289, 1468 (IP and MAC headers will increase total packet size by 64 bytes to total frame lengths of 64, 165, 352, 353, 1532 bytes)
- Beacon Interval = 100 Kus
- Fragmentation Threshold = 2300 or no fragmentation
- RTS threshold =2300 or no RTS/CTS
- Short and Long retry limit = 8
- Shared Key Authentication – if configurable
- Key 1: 0x: 6162636465 (or ASCII value of “abcde”)
- Key 2: 0x: 6263646566 *is specified as the TX default key
- Key 3: 0x: 6364656667
- Key 4: 0x: 6465666768

Procedure:
For each unique set of stations and access point group:

A. Power up the AP followed by the stations. Issue ping requests from each station with various sized data payloads to both a station on the wired network and to another wireless station. Repeat for each AP.
B. **WEP128** - Optional may be tested with key lengths of 13 bytes instead of 5 bytes. Key1 would be ASCII “abcdefghijklm” and the remaining keys would be incremented as in the original 40-bit WEP case.
C. **All On test** - Optional rerun the test with the fragmentation threshold set at 288, the RTS threshold set at 0 and power save on with a DTIM of 5.

Possible Problems:
Traffic between an AP and Station should be either translation or encapsulation. Translation is preferred.

If the DUT does not allow the direct entry of a hex key then it may be required to enter a hash phrase and set the other devices to the resultant hex values.

Observable results:

Procedure A:

	Verify proper association.
	The wireless stations should stay synchronized and pass ICMP echo requests and responses without error.
	Observe that the DUT encrypts and decrypts properly.
	Verify proper association.
	The wireless stations should stay synchronized and pass ICMP echo requests and responses without error.
	Observe that the DUT encrypts and decrypts properly.
	Verify proper association.
	The wireless stations should stay synchronized and pass ICMP echo requests and responses without error.
	Observe that the DUT encrypts and decrypts properly.
	Verify proper association.
	The wireless stations should stay synchronized and pass ICMP echo requests and responses without error.
	Observe that the DUT encrypts and decrypts properly.

Procedure B:

	Verify proper association
	The wireless stations should stay synchronized and pass ICMP echo requests and responses without error.
	Observe that the DUT encrypts and decrypts properly.
	Verify proper association
	The wireless stations should stay synchronized and pass ICMP echo requests and responses without error.
	Observe that the DUT encrypts and decrypts properly.
	Verify proper association
	The wireless stations should stay synchronized and pass ICMP echo requests and responses without error.
	Observe that the DUT encrypts and decrypts properly.
	Verify proper association
	The wireless stations should stay synchronized and pass ICMP echo requests and responses without error.
	Observe that the DUT encrypts and decrypts properly.

Procedure C:

	Verify proper association
	The wireless stations should stay synchronized and pass ICMP echo requests and responses without error.
	Observe that the DUT encrypts and decrypts properly.
	The DUT is in accordance with observable results from the fragmentation section of Observable Results in Basic Point to Point Interoperability Test procedure C.
	The DUT is in accordance with observable results from the RTS section of Observable Results in Basic Point to Point Interoperability Test procedure B.
	The DUT is in accordance with observable results from the PSP Point to Point Interoperability Test

Procedure C(cont'd):

	Verify proper association
	The wireless stations should stay synchronized and pass ICMP echo requests and responses without error.
	Observe that the DUT encrypts and decrypts properly.
	The DUT is in accordance with observable results from the fragmentation section of Observable Results in Basic Point to Point Interoperability Test procedure C.
	The DUT is in accordance with observable results from the RTS section of Observable Results in Basic Point to Point Interoperability Test procedure B.
	The DUT is in accordance with observable results from the PSP Point to Point Interoperability Test
	Verify proper association
	The wireless stations should stay synchronized and pass ICMP echo requests and responses without error.
	Observe that the DUT encrypts and decrypts properly.
	The DUT is in accordance with observable results from the fragmentation section of Observable Results in Basic Point to Point Interoperability Test procedure C.
	The DUT is in accordance with observable results from the RTS section of Observable Results in Basic Point to Point Interoperability Test procedure B.
	The DUT is in accordance with observable results from the PSP Point to Point Interoperability Test
	Verify proper association
	The wireless stations should stay synchronized and pass ICMP echo requests and responses without error.
	Observe that the DUT encrypts and decrypts properly.
	The DUT is in accordance with observable results from the fragmentation section of Observable Results in Basic Point to Point Interoperability Test procedure C.
	The DUT is in accordance with observable results from the RTS section of Observable Results in Basic Point to Point Interoperability Test procedure B.
	The DUT is in accordance with observable results from the PSP Point to Point Interoperability Test

Test Label: **Packet Error Rate Test (with Range measurements)**

Purpose:

- To observe, monitor and calculate a packet error rate for multicast traffic between an access point and multiple stations using OFDM modulation.
- To also observe how distance (from AP to STA) and date rate impact packet error rate.

References: IEEE Standards 802.11-1999, IEEE 802.11a-1999 clause 17.3.10.1

Last Modification: June 7, 2002

Resources Requirements:

- An OFDM PHY access point for participation in an infrastructure BSS
- OFDM PHY stations capable of participating in an infrastructure BSS
- Wireless OFDM PHY sniffer to promiscuously capture traffic
- An Ethernet multicast traffic generator (e.g. UNH-IOL mc3.exe program)

Discussion:

A single vendor's Access Point will be powered up and the other vendors' stations should associate with it. The AP 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 OFDM PHY, all multicast frames should be sent at a basic rate. The AP will also be moved to test varying distances and the basic rates will also be changed to measure the impact both variables have on packet error rate.

Test Setup: The AP, stations and the sniffer shall be positioned so they can receive each other.

- frame size = 1000 (966 bytes payload + 34 bytes MAC header and FCS)
- frame rate = 50 frames/sec* (may want to increase this rate)
- 10,000 frames of pseudorandom data per test
- Use different channels for each test (i.e. OFDM channels 36, 64, and 161)
- AP power level at maximum for the particular band (i.e. 40mW, 200mW, and 800mW)
- Beacon interval set at 128 Kus
- Fragmentation and RTS off
- PSP setup – DTIM= 4
- Basic Rates = **Test 1:** 6, 12, 24 Mbps, **Test 2:** 54 Mbps
- Distances measured for each test: 10 meters, 50 meters, 100 meters

Procedure:

A single Access Point will be powered up and multiple stations will associate with it. It is best to have the AP centered in a circle between all stations to keep received signal strength as equal as possible among all stations. An Ethernet station will generate multicast traffic that is distributed to the wireless media through the AP. Each station will join the multicast pool and the packet error rate calculated. Values shall be recorded and the test repeated at each distance. The test should then be re-run using the basic rate set defined for test 2 at each distance. This test may also be repeated with PSP enabled.

Possible Problems:

- No attempt is made to measure the transmit power levels.
- Traffic between an AP and Station should be either translation or encapsulation. Translation is preferred.
- PC performance can affect the UDP packet reception.
- Performance of the AP receiver and Station transmitter pair is not tested. The station transmitter could be tested in an ad hoc mode.
- Distances may not be great enough to impact packet error rate.

Observable results:

Test 1 (Atheros AP):

Station:	The OFDM station should stay synchronized and record the multicast traffic received. .
10: 50: 100:	A Packet Error Rate (PER) will be calculated for each individual station. The PER should be no more than 10% of the total packets sent.
Station:	The OFDM station should stay synchronized and record the multicast traffic received. .
10: 50: 100:	A Packet Error Rate (PER) will be calculated for each individual station. The PER should be no more than 10% of the total packets sent.
Station:	The OFDM station should stay synchronized and record the multicast traffic received. .
10: 50: 100:	A Packet Error Rate (PER) will be calculated for each individual station. The PER should be no more than 10% of the total packets sent.
Station:	The OFDM station should stay synchronized and record the multicast traffic received. .
10: 50: 100:	A Packet Error Rate (PER) will be calculated for each individual station. The PER should be no more than 10% of the total packets sent.
Station:	The OFDM station should stay synchronized and record the multicast traffic received. .
10: 50: 100:	A Packet Error Rate (PER) will be calculated for each individual station. The PER should be no more than 10% of the total packets sent.

Test 1: (Atheros STA):

AP:	The OFDM station should stay synchronized and record the multicast traffic received. .
10: 50: 100:	A Packet Error Rate (PER) will be calculated for each individual station. The PER should be no more than 10% of the total packets sent.
AP:	The OFDM station should stay synchronized and record the multicast traffic received. .
10: 50: 100:	A Packet Error Rate (PER) will be calculated for each individual station. The PER should be no more than 10% of the total packets sent.
AP:	The OFDM station should stay synchronized and record the multicast traffic received. .
10: 50: 100:	A Packet Error Rate (PER) will be calculated for each individual station. The PER should be no more than 10% of the total packets sent.
AP:	The OFDM station should stay synchronized and record the multicast traffic received. .
10: 50: 100:	A Packet Error Rate (PER) will be calculated for each individual station. The PER should be no more than 10% of the total packets sent.
AP:	The OFDM station should stay synchronized and record the multicast traffic received. .
10: 50: 100:	A Packet Error Rate (PER) will be calculated for each individual station. The PER should be no more than 10% of the total packets sent.

Test 2 (Atheros AP):

Station:	The OFDM station should stay synchronized and record the multicast traffic received. .
10:	A Packet Error Rate (PER) will be calculated for each individual station. The PER should be no more than 10% of the total packets sent.
50:	
100:	
Station:	The OFDM station should stay synchronized and record the multicast traffic received. .
10:	A Packet Error Rate (PER) will be calculated for each individual station. The PER should be no more than 10% of the total packets sent.
50:	
100:	
Station:	The OFDM station should stay synchronized and record the multicast traffic received. .
10:	A Packet Error Rate (PER) will be calculated for each individual station. The PER should be no more than 10% of the total packets sent.
50:	
100:	
Station:	The OFDM station should stay synchronized and record the multicast traffic received. .
10:	A Packet Error Rate (PER) will be calculated for each individual station. The PER should be no more than 10% of the total packets sent.
50:	
100:	
Station:	The OFDM station should stay synchronized and record the multicast traffic received. .
10:	A Packet Error Rate (PER) will be calculated for each individual station. The PER should be no more than 10% of the total packets sent.
50:	
100:	

Test 2: (Atheros STA):

AP:	The OFDM station should stay synchronized and record the multicast traffic received. .
10:	A Packet Error Rate (PER) will be calculated for each individual station. The PER should be no more than 10% of the total packets sent.
50:	
100:	
AP:	The OFDM station should stay synchronized and record the multicast traffic received. .
10:	A Packet Error Rate (PER) will be calculated for each individual station. The PER should be no more than 10% of the total packets sent.
50:	
100:	
AP:	The OFDM station should stay synchronized and record the multicast traffic received. .
10:	A Packet Error Rate (PER) will be calculated for each individual station. The PER should be no more than 10% of the total packets sent.
50:	
100:	
AP:	The OFDM station should stay synchronized and record the multicast traffic received. .
10:	A Packet Error Rate (PER) will be calculated for each individual station. The PER should be no more than 10% of the total packets sent.
50:	
100:	
AP:	The OFDM station should stay synchronized and record the multicast traffic received. .
10:	A Packet Error Rate (PER) will be calculated for each individual station. The PER should be no more than 10% of the total packets sent.
50:	
100:	

Test Label: **Fail-over Re-association and Operating Channel Test**

Purpose:
To observe the behavior of stations when an AP within an ESS fails and the stations are forced to re-associate with a different AP within the same ESS. It also verifies that the DUTs can communicate on all supported OFDM channels.

Last Modification: October 29, 2001

References: IEEE Standards 802.11-1999, IEEE 802.11a-1999

Resources Requirements:

- OFDM PHY stations capable of participating in an infrastructure BSS
- OFDM PHY Access points with portal capabilities and Distribution system (Ethernet network)
- Wireless OFDM PHY sniffer to promiscuously capture traffic

Discussion:
All stations and one AP in the group will be turned on. Each station shall continuously ping a station connected to the Ethernet backbone. Once all the stations are successfully pinging, the second AP in the ESS shall be powered on and then the first AP powered off. Each station should re-associate with the new AP and continue to ping the Ethernet station with minimal loss of service. Transitions to and from each AP will be tested. Selecting channels within different U-NII bands is desired when setting up transitions.

Optionally repeat the procedures with the equipment configured to support PSP.

Channel test:	U-NII lower	36, 40, 44, 48 – 40 mW
	U-NII middle	52, 56, 60, 64 – 200 mW
	U-NII upper	149, 153, 157, 161 – 800 mW

Test Setup:

- Beacon interval = 128Kus
- Short and Long retry = 6
- DTIM = 3
- Fragmentation threshold = or 2300 i.e.disabled
- RTS threshold = 2300 i.e. disabled
- Ping payload size = 32 bytes

Procedures:

- Connect the APs to the network and verify that the Ethernet STA can communicate with each AP.
- Turn off the secondary APs.
- Sequentially power up each station and verify proper association with the first AP.
- Send continuous ICMP Echoes from each wireless station to the station located on the Ethernet backbone.
- Power on the second AP and Power off the first AP for each ESS.
- Wait for all stations to re-associate with the new AP in the ESS.
- Repeat this process until each AP was used as the AP that the station re-associated to.
- Optionally, repeat the procedures 1-7 above but with the equipment configured to support power save.

Channel	Freq GHz	AP1	AP2	AP3	AP4	AP5	AP6	AP7
36	5.18							
40	5.2							
44	5.22							
48	5.24							
52	5.26							
56	5.28							
60	5.3							
64	5.32							
149	5.745							
153	5.765							
157	5.785							
161	5.805							

Observable results:

	When the AP within a BSS fails (powers off), the stations should re-associate with the new AP without noticeable failure of services.

Test Label: **DCF Functionality Test**

Purpose:
To observe connectivity through an Ethernet distribution system and to verify that each STA is utilizing proper DCF functionality according to 802.11 for access to the medium.

References: IEEE Standard 802.11-1999, IEEE 802.11a-1999

Last Modification: October 29, 2001

Resources Requirements:

- OFDM PHY stations capable of participating in an infrastructure BSS
- OFDM PHY Access points with Portal capabilities
- Wireless OFDM PHY sniffer to promiscuously capture traffic
- Distribution system (10bt/100bt Ethernet network)
- An Ethernet UDP directed packet traffic generator (UNH Hive/Swarm program)

Discussion:
The goal of this testing is to create a small somewhat realistic network that is still uncomplicated enough to identify and isolate problems. The configuration includes multiple STAs sending simultaneous UDP packets (using Swarm) directed to a station located on the Ethernet backbone (using Hive to collect data). The Ethernet station will collect the total number of packets sent and received. By comparing these percentages we will be able to ascertain whether or not a STA is observing proper DCF functionality in terms of gaining access to the media.

Test Setup:

- Beacon Interval = 128 Kus
- Fragmentation Threshold = 2300 or disabled
- RTS threshold = 2300 or disabled
- Short and Long retry limit = 6
- Power save is disabled
- Packets/second =

Procedure:

- Connect an AP to the network and verify that the Ethernet Station can ping the AP.
- Power up all stations and verify that each STA can ping the Ethernet Station.
- Run Hive.exe on the Ethernet station and Swarm.exe on each wireless STA simultaneously.
- Replace the AP and repeat at step one until all access points have been tested

Observable results:

	Should see that each station has equitable access to the shared distribution system during the contention period.
	Should see that each station has equitable access to the shared distribution system during the contention period.
	Should see that each station has equitable access to the shared distribution system during the contention period.
	Should see that each station has equitable access to the shared distribution system during the contention period.
	Should see that each station has equitable access to the shared distribution system during the contention period.

Test Label: **AP SSID Test**

Purpose:
To determine that:

- An access point (AP) correctly forms beacons with SSIDs from 1 to 32 characters
- An AP correctly forms probe responses with SSIDs from 1 to 32 characters
- An AP only responds to probe requests and re-association requests whose SSID match its SSID exactly, or which contain broadcast SSIDs
- The DUT responds to probe requests that have broadcast/unicast SSIDs with a probe response
- The DUT performs the following comparison of the SSID:
- Case Sensitivity
- Compares the Length of the SSID
- Validates the entire SSID
- Observes special characters within the SSID

References: IEEE 802.11-1999, Clause7.3.2.1, PICS Proforma – FT6, FT7

Last Modification: October 29, 2001

Resource Requirements:

- A monitor configured for capturing and analyzing MAC layer frames.
- Six 802.11 compliant STAs which participate in the MAC protocol, one which performs active scanning with a broadcast SSID.

Discussion:
It is important to be able to separate networks into segments, and 802.11 uses SSIDs to accomplish this. APs must only respond to probe requests whose SSID match their SSID exactly. To facilitate passive scanning, it is also important that APs correctly form their beacons and probe responses no matter how large or small the SSID is (as long as the length of the SSID is less than or equal to 32 characters). The SSID is case sensitive and must have a length between 0 and 32 characters. An SSID field with zero length is considered a broadcast SSID, which is sometimes transmitted by a probing STA to determine which APs are collocated in the STA's area.

Test Setup:
Configure the STAs with the following SSIDs:
STA 1: 123456ABCDEFGHIJKLMNOPQRSTUVWXYZ
STA 2: 123456abcdefghijklmnopqrstuvwxyz
STA 3: 1
STA 4: 123456ABCDEFGHIJKLMNOPQRSTUVWXYA
STA 5: "~!@#$%^&*()_+=-`<>?/.,;':" {}|" total of 32 characters including a space
STA 6: Broadcast SSID: 0 characters. *Note:* STA should be set to active scan

Procedure:
Part a): Verify that you are unable to configure the DUT with either an SSID larger than 32 characters or a null SSID. Then configure the DUT with the following SSID: 123456ABCDEFGHIJKLMNOPQRSTUVWXYZ

Part b): Power up DUT and then power up STA 6. Verify that the DUT responds to the probe request containing the broadcast SSID with a Probe response containing its correct SSID. Power down STA 6.

Part c): Power up STA's 1-5. Verify that none of the STA with the incorrect SSID Associate with the DUT and only STA 1 associates with the DUT.

Part d): Configure the DUT with the following SSID: 123456ABCDEFGHIJKLMNOPQRSTUVWXY (shorten to first 31 characters) to invoke a Disassociation of STA 1. Then reconfigure the DUT with the following SSID: 123456ABCDEFGHIJKLMNOPQRSTUVWXYZ. Verify that STA 1 is able to reassociate with the DUT.

Part e): Configure the DUT with an SSID of "~!@#$%^&*()_+=-`<>?/.,;':" {}|" Power up DUT and verify that only STA 5 associates with the DUT.

Possible problems:

- Not being able to set the SSID in the STA
- Ensuring a re-association request from the STA after the disassociation from the DUT

Observable Results:

	Does the DUT disallow a SSID both Null and over 32 characters in length?
	Does the DUT respond to probe request containing broadcast SSID and probe response with correct SSID?
	Does the DUT disregard any probe requests containing the wrong SSID and respond to a request with a correct SSID? *Note: DUT should ACK a directed probe request but not send a probe response*
	Does the DUT respond to a re-association request with the correct SSID?
	Does the DUT allow non-alphanumeric characters from within the SSID?

Test Label: **STA SSID Test**

Purpose:
To determine that:

- The DUT correctly forms probe requests with SSIDs of length 0 to 32 characters
- The DUT disregards any probe responses containing the wrong SSID
- The DUT Authenticates, Associates and Reassociates with only the AP with the same SSID
- The DUT performs the following comparison of the SSID:
  - Case Sensitivity
  - Compares the Length of the SSID
  - Validates the entire SSID
  - Observes special characters within the SSID

References: IEEE 802.11-1999, Clause7.3.2.1, PICS Proforma – FT6, FT7

Last Modification: October 29, 2001

Resource Requirements:

- A monitor configured for capturing and analyzing MAC layer frames.
- Six 802.11 compliant APs which participate in the 802.11 MAC Protocol.

Discussion:
The Service Set Identifier (SSID) is used to allow many Basic Service Sets (BSS) to operate together as an Extended Service Set (ESS) or to simultaneously allow many independent collocated networks. Only STAs with an identical SSID as the AP should be allowed to associate with that AP. The STA includes an SSID field in all probe requests, association requests, and re-association requests. The frames that an AP transmits containing an SSID field are beacons and probe responses. The SSID is case sensitive and must have a length between 0 and 32 characters inclusive. The SSID field with zero length is considered a broadcast SSID which may transmitted by a probing STA to determine which APs are collocated in the STA's area.

Test Setup:
Configure the AP's with the following SSIDs:
AP 1,6: 123456ABCDEFGHIJKLMNOPQRSTUVWXYZ
AP 2: 123456abcdefghijklmnopqrstuvwxyz
AP 3: 1
AP 4: 123456ABCDEFGHIJKLMNOPQRSTUVWXYA
AP 5: "~!@#$%^&*()_+=-`<>?/.,;':" {}|" total of 32 characters including a space

Procedure:
Part a): Verify that you are unable to configure the DUT with a SSID larger than 32 characters. Then configure the DUT with the following SSID: 123456ABCDEFGHIJKLMNOPQRSTUVWXYZ

Part b): Power up APs 2-5. Power up DUT and verify that it does not associate with the any of the APs.

Part c): Power up AP 1 and verify that the DUT associates with that AP. Power down AP 1 and verify that the DUT does not roam to any of the AP's 2-5. Power up AP 6 and observe that the DUT roams to AP 6.

Part d): Configure the DUT with an SSID of "~!@#$%^&*()_+=-`<>?/.,;':" {}|" Power up DUT and verify that the DUT associates with AP 5.

Possible problems:
Having to select an SSID from a list of scanned APs and not being able to enter the SSID directly in the DUT.

Observable Results:

	Does the DUT disallow a SSID both Null and over 32 characters in length?
	Does the DUT disregard any probe responses containing the wrong SSID and not attempt to associate with an AP with an incorrect SSID?
	Does the DUT associate to the AP with the correct SSID?
	Does the DUT reassociate to an AP with the correct SSID?
	Does the DUT allow non-alphanumeric characters to be defined in the SSID?

Test Label: **CFPDurRemaining NAV Test**

Purpose:
To verify a device updates its NAV from the CFPDurRemaining element (non-PCF devices) or the CFPMaxDuration element (PCF devices) of beacons.

References: IEEE Standard 802.11-1999 clause 9.3.2.2

Last Modification: June 28, 2000

Resources Requirements:

- An 802.11 access point, if the device is a station
- Wireless 802.11 sniffer to promiscuously capture traffic
- A device capable of generating user defined 802.11 frames (TX-STA)

Discussion:
One of the fundamental difficulties in the use of a wireless medium is the “hidden node” problem. This occurs when an access point is within range of two or more stations, which are not within range of each other. If STA1 begins transmitting a frame to the AP, and STA2 decides it wishes to transmit a frame to the AP as well, it will not hear STA1’s transmission, it will transmit its frame, and a collision will occur. To reduce the likelihood of this problem, the 802.11 protocol has devised a system of reserving the medium with what is known as a Network Allocation Vector (NAV). The NAV contains how much longer the medium will be in use, and can be updated from a variety of frames. One of the more notable cases is the CFPDurRemaining and CFPMaxDuration element used by Point Coordinators. PCF is optional method whereby medium use is delegated through the access point. This allows for some quality of service control and potentially bandwidth reservations. However, PCF is only effective if devices update their NAV from the CFPDurRemaining element if the device is non-PCF capable or the CFPMaxDuration element if the device is PCF capable. This grants the PCF access point exclusive control of the medium for the duration of the Contention Free Period (CFP), so it can properly carry out PCF functionality in environments with the hidden node problem. This test verifies that functionality by continuously transmitting beacons with CFPDurRemaining and CFPMaxDuration set to non-zero values, and observing if any devices violate the medium reservation.

Test Setup:
The DUT, sniffer, TX-STA, and access point (if present) shall be arranged such that they can communicate with each other. If the DUT is a station, it shall be configured to authenticate and associate with the access point. RTS/CTS, fragmentation, and WEP shall be disabled in all devices. Access point settings are as follows:

- Beacon Interval = 256 Kus
- Dwell Time = 128 Kus (N/A for DS)
- Short and Long retry limit = 8
- CFP disabled

Configure the TX-STA to generate properly formed beacon frames with the following properties:

- CFP Count = 0
- CFP Period = 1
- CFPMaxDuration = 256Kus
- CFPDurRemaining = 128Kus

Each new transmission should have an updated sequence number and timestamp.

Procedure:
Multiple DUTs may be simultaneously tested. Bring all the DUTs online, and have each transmit one 32-byte ICMP ping per second across the wireless medium. Each STA DUT should ping a host on the distribution system, and for each AP DUT, a host on the distribution system should generate pings to one of the STAs associated with that AP DUT. Do not proceed unless all of the DUT are receiving ping replies. Have the TX-STA begin transmitting the CFP beacons with an interval no greater than 128Kus. Optionally, CF-ACKs may be interspersed in between the beacons to simulate hidden nodes. This should completely reserve the medium. Capture a trace and observe if any stations attempt to transmit frames despite the medium being allocated. No ping replies should be received from this point on.

Observable results:

	The MAC addresses of stations that attempted transmission while the CFP beacons were being generated.
	No ping replies should be received by the DUT
	The MAC addresses of stations that attempted transmission while the CFP beacons were being generated.
	No ping replies should be received by the DUT
	The MAC addresses of stations that attempted transmission while the CFP beacons were being generated.
	No ping replies should be received by the DUT