

System Interoperability Test Plan
for IEEE 802.11a Devices
and IEEE 802.11a + b Devices

Wi-Fi Alliance

Version 1.0

December 4, 2002



1 OVERVIEW 5

2 IMPLEMENTATION REQUIREMENTS FOR WI-FI ALLIANCE
CERTIFICATION 6

 2.1 GENERAL HANDLING FOR RESERVED BITS 6

 2.2 SSID ELEMENT:..... 6

 2.3 BEACON INTERVAL:..... 6

 2.4 TIM ELEMENT 6

 2.5 DATA PAYLOAD..... 6

 2.6 POWER SAVE..... 6

 2.7 WEP 7

 2.8 RTS/CTS 7

 2.9 FRAGMENTATION..... 7

 2.10 PCF..... 7

 2.11 PACKET RESPONSE TIMES 7

 2.12 DATA RATES 7

 2.13 HANDLING UNEXPECTED FRAMES 7

 2.14 ABILITY TO HANDLE NULL FRAMES 8

 2.15 ABILITY TO HANDLE PROPRIETARY MESSAGES 8

 2.16 ABILITY TO HANDLE UNSOLICITED PS-POLL 8

 2.17 AP NOTIFICATION OF BRIDGES UPON STATION ROAMING 8

 2.18 AD HOC SUPPORT (IBSS) REQUIREMENTS 8

3 TEST TOOLS 10

 3.1 TEST SOFTWARE 10

 3.2 TEST SCRIPTS..... 10

 3.3 BASIC SYSTEM TEST CONFIGURATION..... 10

4 AP TESTING..... 12

 4.1 AP CONFIGURABILITY TEST 12

 4.2 INITIAL AP/STATION INTEROPERABILITY TESTS 12

 4.2.1 Description of Initial Tests..... 12

 4.2.2 Configurations for AP Testing..... 13

 4.2.3 AP Special Tests 18

5 STATION TESTING - INFRASTRUCTURE 22

 5.1 STATION CONFIGURABILITY TEST..... 22

 5.2 STATION/AP INTEROPERABILITY TESTS..... 23

 5.2.1 Description of Tests 23

 5.2.2 AP Configurations 24

 5.3 SPECIAL TESTS FOR STATIONS 27

 5.3.1 Roaming 27

 5.3.2 Data Payload (Encapsulation) 28

 5.3.3 Broadcast/Multicast reception..... 28

 5.3.4 Negative Tests..... 30

- 6 STATION TESTING - IBSS 30
 - 6.1 ACTIVE SCAN TESTS 31
 - 6.1.1 Configuration SI1 31
 - 6.1.2 Test Sequence 32
 - 6.2 PASSIVE SCAN TESTS 33
 - 6.3 CONFIGURATION SI2..... 33
 - 6.3.1 Test Sequence 34
 - 6.4 IBSS WEP ON TESTS 34
 - 6.4.1 Configuration SI3..... 34
 - 6.4.2 Test Sequence 35
 - 6.5 IBSS WEP OFF TESTS 36
 - 6.5.1 Configuration SI4..... 36
 - 6.5.2 Test Sequence 37
 - 6.6 RE-JOIN TESTS 38
 - 6.6.1 Configuration SI5..... 39
 - 6.6.2 Test Sequence 40
- 7 DUAL BAND TESTS 41
 - 7.1 BRIDGING THROUGHPUT TEST FOR DUAL BAND APs 41
 - 7.2 CROSS-BAND STATION ROAMING TEST FOR DUAL BAND STATIONS..... 42
 - 7.3 ESSID..... 43
- 8 APPENDIX A: THROUGHPUT VALUES 44
- 9 APPENDIX B: CHANNEL NUMBERS..... 47
- 10 APPENDIX C: VENDOR EQUIPMENT LIST 48
 - 10.1 STATIONS..... 48
 - 10.2 ACCESS POINTS..... 50
- 11 APPENDIX D..... 52
 - 11.1 Atheros WIRELESS NETWORK ADAPTER 52
 - 11.1.1 Parameter Configurable 52
 - 11.1.2 Channel Frequency 52
 - 11.1.3 RTS Threshold 54
 - 11.1.4 Fragmentation Threshold 54
 - 11.1.5 Beacon Interval 54
 - 11.1.6 The Changes to Take Effect..... 54
 - 11.2 INTEL PROWIRELESS 5000..... 54

Document History

Version 1.0 issued December 4th, 2002
original document.

1 Overview

The goal of the Wi-Fi Alliance is to ensure interoperability among IEEE 802.11b High Rate and IEEE 802.11a products from multiple manufacturers, and to promote this technology within both the business and consumer markets. To this end, we have developed the following interoperability test suite for IEEE 802.11a products. Working in conjunction with Agilent ICL we will execute these tests on vendor products so as to grant products a “seal of interoperability” upon successful completion of the tests.

Products which pass the following tests are granted the Wi-Fi Alliance logo to be used on both product materials and marketing materials. In this fashion, customers may look to the WI-FI ALLIANCE logo as a mark of multi-vendor interoperability. Two documents have been written to define tests for both technologies. Document 1.0a addresses IEEE 802.11b High Rate (Wi-Fi Alliance) tests, and this document addresses IEEE 802.11a tests.

2 Implementation Requirements for Wi-Fi Alliance Certification

The following items describe the necessary features that will be required for an implementation to pass Wi-Fi Alliance interoperability testing. This is intended to provide vendors with guidance as they prepare their product for Wi-Fi Alliance certification testing.

2.1 General handling for reserved bits

- Ignore on receive.
- Set to zero on transmit.

2.2 SSID Element:

- Support for ASCII printable characters as a minimum.
- SSID character strings are not terminated by ASCII null.
- AP must respond to broadcast SSID probe requests.

2.3 Beacon Interval:

- Stations must be able to support any beacon interval within the range 20 ms - 1000 ms.
- AP must support at least one beacon/DTIM interval of within the range 20 ms - 1000 ms.

2.4 TIM Element

- AP must be capable of generating correct TIM for PSP nodes.
- Stations in PSP must interpret TIM correctly.

2.5 Data Payload

- Encrypted and unencrypted support is required.
- Data payload size is limited to Ethernet payload size.
- Payload formats will conform to 802.1H, which specifies the use of RFC1042.
- General rule: if a specific Ethertype in the table, then 802.1H bridge tunnel encapsulation format shall be used, otherwise RFC1042 applies.
- Ethernets 80F3 and 8137 shall be in the table.

2.6 Power Save

- Station power save mode not mandatory.
- AP support of power save stations is mandatory.
- APs must be capable of generating DTIMs at a DTIM interval between 1 and 5.
- APs must support the dynamic switching of a station between power save and CAM states as indicated by the power save bit in frames generated by the station.
- APs should ignore the power save bit in any received broadcast/multicast Probe Request.

- APs should ignore the power save bit in any received Authenticate and (Re)Associate, and should assume the station is awake for the response.

2.7 WEP

- Support of a single 40-bit WEP key is required.
- A minimum support requires reception and transmission using default key 0 (IV:KeyID=00).
- APs must support a totally unencrypted cell and a totally encrypted cell
- Open system authentication is mandatory.
- A station with WEP off should never attempt to associate with an AP that has WEP on.
- An AP or a station with WEP on should discard all received data frames that have the WEP bit off in the MAC header.

2.8 RTS/CTS

- Must correctly support reception of RTS and generation of CTS.
- Generation of RTS is not mandatory.

2.9 Fragmentation

- Must support reception of fragmented packets.
- Fragmented transmission is not mandatory.

2.10 PCF

- PCF support is not mandatory

2.11 Packet Response Times

- Probe response must occur within 5 ms (assuming clear channel).
- Stations must wait for a minimum of 5 ms for a probe response.
- Authenticate response in case of open system authentication must occur within 100 ms when AP is idle .
- (Re)Associate response must occur with 100 ms when AP is idle.
- Stations must be capable of associating to APs that respond at the maximum times allowed.

2.12 Data Rates

- APs and stations must be capable of operating at each data rate (6, 12, 24, and 54 Mbps).
- APs and stations must be capable of operating within a BSS with 6, 12, and 24 Mbps considered the basic rates, and 54 Mbps which is a supported rate.

2.13 Handling Unexpected Frames

- Ability to ignore unknown information elements.

- APs and stations must be capable of operating properly upon receipt of unknown information elements (i.e. they must ignore them).
- Any AP or station that generates an information element not specified by 802.11 must include the vendor's OUI as the first three bytes of the information field within the element.

2.14 Ability to handle null frames

- APs and stations must be capable of operating properly upon receipt of null frames.
- Control bits within null frames are to be acted upon (e.g. power save bits).
- Null frames received from a non-authenticated or non-associated station should elicit a De-authenticate/Disassociate response from the AP.

2.15 Ability to handle proprietary messages

- Stations and APs must be able to operate properly upon receipt of any proprietary message that is formatted in accordance with SNAP with the manufacturer OUI.

2.16 Ability to handle unsolicited PS-Poll

- if poller is not associated, response is ACK followed by De-authenticate or Disassociate.
- if poller is associated, allowable responses include: 1) ACK 2) data 3) null data or empty data, or 3) ACK followed by data or null data or empty data.

2.17 AP notification of bridges upon station roaming

- When a station roams from an old AP to a new AP, the new AP is responsible for ensuring that any bridges between the two APs are properly notified of the station's new location.
- The manner in which this is accomplished is not specified. The only requirement is that some method is implemented which ensures that packets will flow properly to the station's new AP.

2.18 Ad Hoc Support (IBSS) Requirements

- Station must be able to create an IBSS network
 - Must be able to create an IBSS network with a specified SSID.
 - SSIDs can be up to 32 characters, and are not null terminated
 - Must be able to select the channel to be used
 - Must be able to create both an encrypted IBSS (with 40 bit WEP key) and an unencrypted IBSS
 - BSSID must be randomly selected
 - Must allow stations doing active scanning and passive scanning to join
 - Basic Rate Set see 2.12 above.

- Station must be able to join an existing IBSS network
 - Must be able to join an IBSS network with specified SSID
 - Must be able to join an IBSS that has been started on an arbitrary channel
 - either active or passive scanning is allowed
 - authentication is not required
 - must be able to join an encrypted IBSS (40 bit WEP key) and unencrypted IBSS
 - WEP keys are not adopted like other parameters
 - Basic Rate Sets see 2.12 above.
- Communication test between multiple IBSS stations
 - Support of clear text operation is required.
 - Support of a totally encrypted cell using a single 40-bit WEP key is required
 - Stations must be capable of operating at 54 Mbps
 - Station must receive data packets sent using RTS/CTS
 - Station must receive fragmented data packets
- Multicast traffic must be supported
 - Station must support transmission of multicast traffic
 - Station must support reception of multicast traffic
- Station Coalescing ability to merge two IBSS cells.
 - The station must change to a new BSSID if it encounters an existing cell with the same SSID and a greater TSF on the same channel
- IBSS distributed beaconing.
 - Station must continue beaconing when the station that created the IBSS is turned off.
 - Station must implement distributed the beaconing algorithm.
- IBSS Power management support is not required
- IBSS network isolation testing
 - The station, while a member of on IBSS, shall not receive packets from another IBSS (with different SSID) on the same channel

3 Test Tools

3.1 Test Software

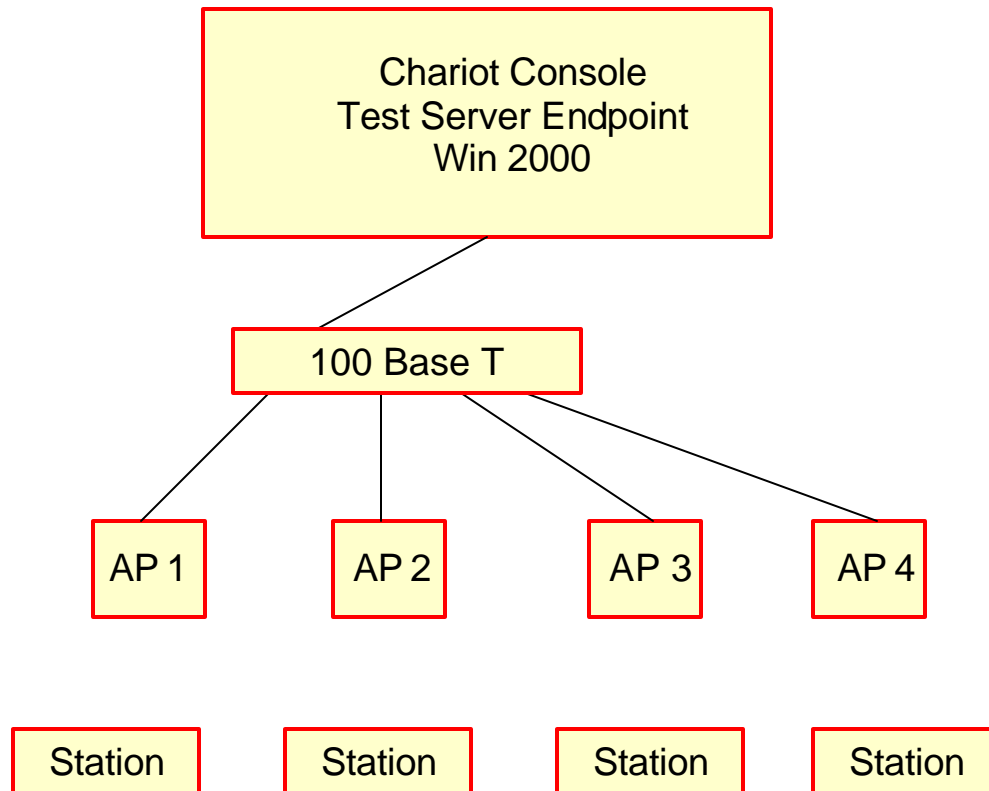
Chariot version 4.1 software from NetIQ Corporation. will be used. Chariot includes a large set of standard, editable scripts, which can be used to define a particular traffic flow between two “endpoints”. The script definition, test configuration, test execution, and results reporting are managed through the Chariot “console”, which in our case will be separate machine from the units under test.

3.2 Test Scripts

The scripts which are to be used in the testing are the following:

- FILESNDL (“File Send Long”)
 - This emulates a large file transfer between endpoints.
- INQUIRYL (“Inquiry Long”)
 - This emulates a series of client/server transactions.
- REALAUD
 - This emulates a multicast Real Audio stream.

3.3 Basic System Test Configuration

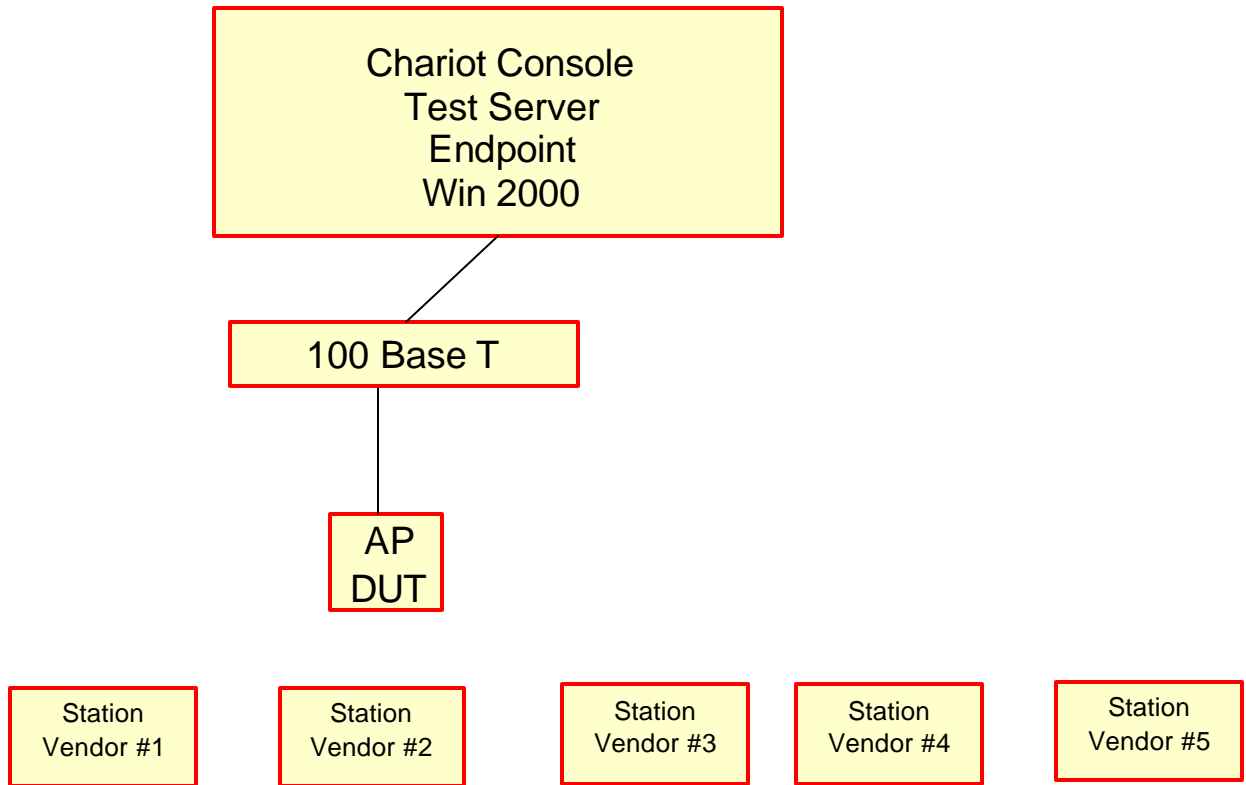


Basic System Test Configuration

The stations and the Test Server operate as Chariot endpoints, with the tests configured and controlled from the Chariot Console.

When a station is being tested, only one station is typically present, namely the station-under-test. When an AP is being tested, only one AP is typically present, namely the AP-under-test. The specific products used in these testing configurations are listed in Appendix C.

4 AP Testing



AP Test Set-Up

4.1 AP Configurability Test

APs must be capable of being configured in the following ways:

- ESSID
- WEP Key
- Channel
- Basic Rate Set

4.2 Initial AP/Station Interoperability Tests

We want to make sure that the AP can operate with a variety of ESSIDs, can handle RTS, fragmentation, WEP, Power Save, and different channels. The approach is similar to the approach for Initial Station/AP Interoperability Tests.

4.2.1 Description of Initial Tests

The basic idea is as follows: to test an AP, we want to test its ability to work with stations from a variety of manufacturers, with and without RTS, with and without fragmentation,

with and without WEP, and with and without power save. In addition, the AP must operate on various channels.

There are four tests which are executed for each configuration. Prior to the execution of these tests, the AP is configured so as to match the ESSID and WEP parameters of the station. The AP is also configured with specific settings for Basic Rate and Channel, as identified in the tables below. Once the AP is configured, the following four tests are executed:

4.2.1.1 Association

The AP is powered on in its defined configuration. The station is powered on in its (complementary) configuration. The station and the AP are both examined to determine whether or not the station properly associates with the AP.

4.2.1.2 Data Transfer 1

With the station associated with the AP, the Chariot script FILESENDL is executed, with the station running as Endpoint 2 and the Test Server running as Endpoint 1. The Chariot console is examined to determine whether or not the station was able to pass data successfully. The definition of success or failure is specific to the configuration, as described below.

4.2.1.3 Data Transfer 2

With the station associated with the AP, the Chariot script FILESENDL is executed with the station running as Endpoint 1 and the Test Server running as Endpoint 2. The Chariot console is examined to determine whether or not the station was able to pass data successfully. The definition of success or failure is specific to the configuration, as described below.

4.2.1.4 Data Transfer 3

With the station associated with the AP, the Chariot script INQUIRYL is executed with the station running as Endpoint 2 and the Test Server running as Endpoint 1. The Chariot console is examined to determine whether or not the station was able to pass data successfully. The definition of success or failure is specific to the configuration, as described below.

4.2.2 Configurations for AP Testing

All configurations use the ESSID “aicl”.

Configuration #A1

PARAMETER	STATION Values	AP Values
Vendor	Cisco	APUT
<i>RTS Threshold</i>	Off	default for AP
<i>Fragmentation</i>	Off	default for AP
<i>WEP</i>	on, key = 0x9876543210	on, key = 0x9876543210
<i>Power Save</i>	No	-
<i>AP Channel</i>	-	36

<i>Association Test</i>	if association occurs, pass
<i>Data Transfer #1</i>	throughput > A1DT1
<i>Data Transfer #2</i>	throughput > A1DT2
<i>Data Transfer #3</i>	throughput > A1DT3

Configuration #A2

PARAMETER	STATION Values	AP Values
Vendor	Cisco	APUT
<i>RTS Threshold</i>	300 bytes	default for AP
<i>Fragmentation</i>	500 bytes	default for AP
<i>WEP</i>	Off	Off
<i>Power Save</i>	No	-
<i>AP Channel</i>	-	40

<i>Association Test</i>	if association occurs, pass
<i>Data Transfer #1</i>	throughput > A2DT1
<i>Data Transfer #2</i>	throughput > A2DT2
<i>Data Transfer #3</i>	throughput > A2DT3

Configuration #A3

PARAMETER	STATION Values	AP Values
Vendor	Intel	APUT
<i>RTS Threshold</i>	Off	default for AP
<i>Fragmentation</i>	500 bytes	default for AP
<i>WEP</i>	Off	Off
<i>Power Save</i>	On (Lowest Power / Performance)	-
<i>AP Channel</i>	-	44

<i>Association Test</i>	if association occurs, pass
<i>Data Transfer #1</i>	throughput > A3DT1
<i>Data Transfer #2</i>	throughput > A3DT2
<i>Data Transfer #3</i>	throughput > A3DT3

Configuration #A4

PARAMETER	STATION Values	AP Values
Vendor	Atheros	APUT
<i>RTS Threshold</i>	400 bytes	default for AP
<i>Fragmentation</i>	Off	default for AP
<i>WEP</i>	On, key = 0x0123456789	On, key = 0x0123456789
<i>Power Save</i>	On	-
<i>AP Channel</i>	-	48

Association Test	if association occurs, pass
<i>Data Transfer #1</i>	throughput > A4DT1
<i>Data Transfer #2</i>	throughput > A4DT2
<i>Data Transfer #3</i>	throughput > A4DT3

Configuration #A5

In this configuration, the AP is set to channel 52 with WEP on (key = 0xABCDEABCDE), and all four stations are brought up using the parameters for RTS, Fragmentation, and Power Save identified in tests A1 - A4.

A1	Cisco
A2	Intersil
A3	Intel
A4	Atheros

This test passes when all stations have completed the three data transfers (no throughput measurement is required – Chariot script complete without Chariot errors).

Configuration #A6

PARAMETER	STATION Values	AP Values
Vendor	Atheros	APUT
<i>RTS Threshold</i>	300 bytes	default for AP
<i>Fragmentation</i>	400 bytes	default for AP
<i>WEP</i>	on, key = 0x9876543210	on, key = 0x9876543210
<i>Power Save</i>	No	-
<i>AP Channel</i>	-	56

Association Test	if association occurs, pass
<i>Data Transfer #1</i>	throughput > A6DT1
<i>Data Transfer #2</i>	throughput > A6DT2
<i>Data Transfer #3</i>	throughput > A6DT3

Configuration #A7

PARAMETER	STATION Values	AP Values
Vendor	Intersil	APUT
<i>RTS Threshold</i>	300 bytes	default for AP
<i>Fragmentation</i>	Off	default for AP
<i>WEP</i>	Off	Off
<i>Power Save</i>	On – PSP (max.)	-
<i>AP Channel</i>	-	60

<i>Association Test</i>	if association occurs, pass
<i>Data Transfer #1</i>	throughput > A7DT1
<i>Data Transfer #2</i>	throughput > A7DT2
<i>Data Transfer #3</i>	throughput > A7DT3

Configuration #A8

PARAMETER	STATION Values	AP Values
Vendor	Cisco	APUT
<i>RTS Threshold</i>	300 bytes	default for AP
<i>Fragmentation</i>	500 bytes	default for AP
<i>WEP</i>	Off	Off
<i>Power Save</i>	On - Dynamic	-
<i>AP Channel</i>	-	64

<i>Association Test</i>	if association occurs, pass
<i>Data Transfer #1</i>	throughput > A8DT1
<i>Data Transfer #2</i>	throughput > A8DT2
<i>Data Transfer #3</i>	throughput > A8DT3

Configuration #A9

PARAMETER	STATION Values	AP Values
Vendor	Intel	APUT
<i>RTS Threshold</i>	Off	default for AP
<i>Fragmentation</i>	400 bytes	default for AP
<i>WEP</i>	On, key = 0x0123456789	On, key = 0x0123456789
<i>Power Save</i>	Off	-
<i>AP Channel</i>	-	36

<i>Association Test</i>	if association occurs, pass
<i>Data Transfer #1</i>	throughput > A9DT1
<i>Data Transfer #2</i>	throughput > A9DT2
<i>Data Transfer #3</i>	throughput > A9DT3

Configuration #A10

PARAMETER	STATION Values	AP Values
Vendor	Atheros	APUT
<i>RTS Threshold</i>	256 bytes	default for AP
<i>Fragmentation</i>	Off	default for AP
<i>WEP</i>	on, key = 0x9876543210	on, key = 0x9876543210
<i>Power Save</i>	No	-
<i>AP Channel</i>	-	40

Association Test	if association occurs, pass
<i>Data Transfer #1</i>	throughput > A10DT1
<i>Data Transfer #2</i>	throughput > A10DT2
<i>Data Transfer #3</i>	throughput > A10DT3

Configuration #A11

PARAMETER	STATION Values	AP Values
Vendor	Atheros	APUT
<i>RTS Threshold</i>	off	default for AP
<i>Fragmentation</i>	500 bytes	default for AP
<i>WEP</i>	Off	Off
<i>Power Save</i>	No	-
<i>AP Channel</i>	-	44

Association Test	if association occurs, pass
<i>Data Transfer #1</i>	throughput > A11DT1
<i>Data Transfer #2</i>	throughput > A11DT2
<i>Data Transfer #3</i>	throughput > A11DT3

Configuration #A12

PARAMETER	STATION Values	AP Values
Vendor	Intersil	APUT
<i>RTS Threshold</i>	Off	default for AP
<i>Fragmentation</i>	Off	default for AP
<i>WEP</i>	Off	Off
<i>Power Save</i>	On - PSP (max.)	-
<i>AP Channel</i>	-	48

Association Test	if association occurs, pass
<i>Data Transfer #1</i>	throughput > A12DT1
<i>Data Transfer #2</i>	throughput > A12DT2
<i>Data Transfer #3</i>	throughput > A12DT3

Configuration #A13

<i>PARAMETER</i>	STATION Values	AP Values
Vendor	Intersil	APUT
<i>RTS Threshold</i>	Off	default for AP
<i>Fragmentation</i>	Off	default for AP
<i>WEP</i>	On, key = 0x0123456789	On, key = 0x0123456789
<i>Power Save</i>	On - Dynamic	-
<i>AP Channel</i>	-	52

Association Test	if association occurs, pass
<i>Data Transfer #1</i>	throughput > A13DT1
<i>Data Transfer #2</i>	throughput > A13DT2
<i>Data Transfer #3</i>	throughput > A13DT3

4.2.3 AP Special Tests**4.2.3.1 Re-Association/Roaming**

Requirement: An AP must handle the re-association properly. This includes the notification of any intervening bridges that a station has roamed to the AP.

Test: Set-up the APUT and another AP, with the same ESSID, and with an intervening bridge between the APs. The APUT is initially off, and the other AP is on. Set-up a Test STA to associate with the other AP. From the Test Server, ping the station once. Then power up the APUT and power down the other AP, forcing the Test STA to roam to the APUT. Ping the station again from the Test Server. The ping should succeed.

4.2.3.2 Data Payload

We will verify the AP's ability to correctly encapsulate packets. This involves verifying that various packets from the Ethernet are correctly received at the station, and that packets generated on the station host are correctly transferred to the Ethernet.

- Test for various payload types
- DIX Ethertypes (assorted)
- LLC (802.2) packets
- Verify RFC1042 and basic Ethertype transfer for 8137 and 80F3.

The test configuration is as follows: a station is selected for the test, and the test server and the station are configured to use IPX with the same frame type selected including

Ethernet 802.2, Ethernet 802.3, and Ethernet II. The Chariot script INQUIRYL is then used to verify that packet transfer can occur through the AP under test.

4.2.3.3 *Multicast*

In each of the configurations described below, the Test Server is set up to support multicasts as Chariot Endpoint 1. Two stations are set up to be Endpoint 2, called Multicast Test Station 1 and Multicast Test Station 2. The streaming Chariot script REALAUD is used to generate a multicast stream of data.

Using the Chariot Console, the two Multicast Test Stations are set up with IP Multicast Address 225.0.0.1. Each station's unique IP address must also be configured into the test in order for Chariot to be able to configure the IP Multicast Address on those stations.

“Validate Data upon Receipt” is selected on the Chariot Run Options tab of the Run Options dialog.

UDP is selected as the underlying protocol.

REALAUD is selected as the Chariot script.

Multicast Configuration #MCA1

<i>Vendor</i>	Intel
<i>ESSID</i>	Multicast
<i>Beacon Interval</i>	default for AP
<i>Channel</i>	56
<i>RTS Threshold</i>	default for AP
<i>Fragmentation</i>	default for AP
<i>WEP</i>	on, key = 0x0123456789
<i>MC Test Station 1</i>	CAM
<i>MC Test Station 2</i>	CAM

<i>MC Data Transfer</i>	throughput > MCA1DT
-------------------------	---------------------

Multicast Configuration #MCA2

<i>Vendor</i>	Atheros
<i>ESSID</i>	Multicast
<i>Beacon Interval</i>	default for AP
<i>Channel</i>	60
<i>RTS Threshold</i>	default for AP
<i>Fragmentation</i>	default for AP
<i>WEP</i>	on, key = 0x0123456789
<i>Station-Under-Test</i>	CAM
<i>MC Test Station 1</i>	CAM
<i>MC Test Station 2</i>	CAM

<i>MC Data Transfer</i>	throughput > MCA2DT
-------------------------	---------------------

Multicast Configuration #MCA3

<i>Vendor</i>	Atheros
<i>ESSID</i>	Multicast
<i>Beacon Interval</i>	default for AP
<i>Channel</i>	64
<i>RTS Threshold</i>	default for AP
<i>Fragmentation</i>	default for AP
<i>WEP</i>	on, key = 0x0123456789
<i>Station-Under-Test</i>	CAM
<i>MC Test Station 1</i>	PS
<i>MC Test Station 2</i>	PS

<i>MC Data Transfer</i>	throughput > MCA3DT
-------------------------	---------------------

Configuration #MCA4Multicast

<i>Vendor</i>	Cisco
<i>ESSID</i>	default for AP
<i>Beacon Interval</i>	150 ms
<i>Channel</i>	36
<i>RTS Threshold</i>	default for AP
<i>Fragmentation</i>	default for AP
<i>WEP</i>	on, key = 0x0123456789
<i>Station-Under-Test</i>	CAM
<i>MC Test Station 1</i>	PS
<i>MC Test Station 2</i>	PS

<i>MC Data Transfer</i>	throughput > MCA4DT
-------------------------	---------------------

4.2.3.4 Intra-BSS Transfer

Requirement: Two STAs associated to the same AP must be able to communicate intra-BSS via the relay in the AP.

Test Suggestions: The APUT is configured in its default mode and started. Two Test STAs are configured to associate with the APUT and started up nearby the APUT. FILESENDL is run with the two stations operating as Endpoints 1 and 2.

4.2.3.5 Negative Tests

The AP under test is checked with stations in a mismatched configuration to ensure that association and/or data transfer does not occur.

The configuration mismatches to be tested include:

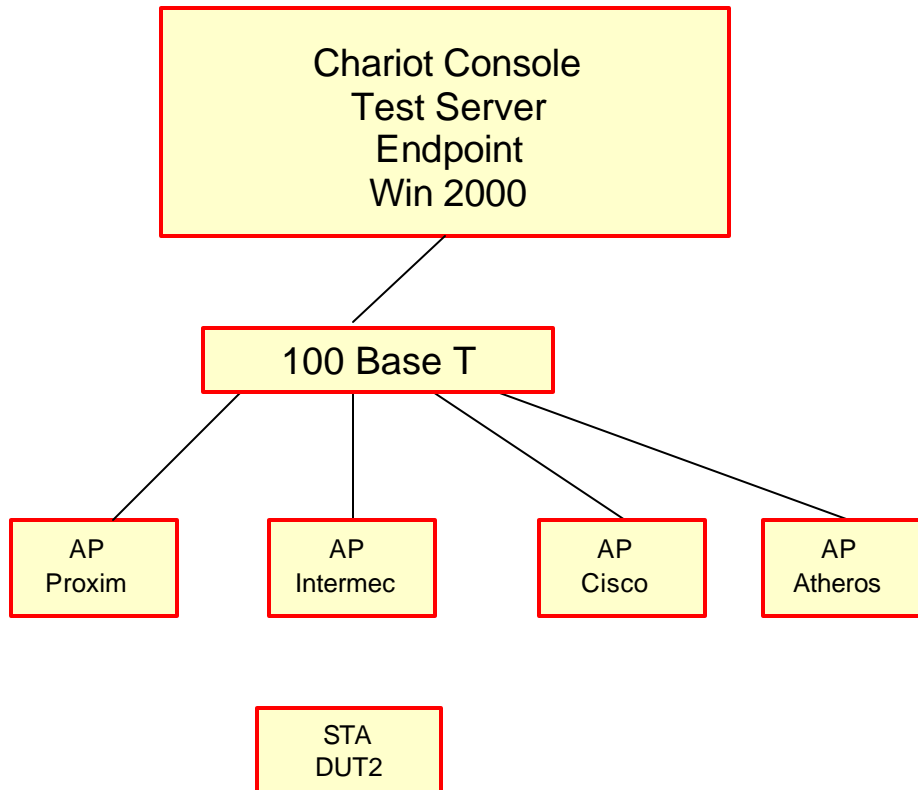
- wrong ESSID: the AP is configured with ESSID abc and the station is configured with ESSID def. The station should not associate.
- wrong case in ESSID characters: the AP is configured with ABC and the station is configured with abc, and vice versa. The station should not associate in either case.
- ESSID substring: the AP is configured with abc and the station is configured with abcde, and vice versa. The station should not associate in either case.
- WEP key mismatch: the station is configured with WEP key 0x0123456789 and the AP is configured with WEP key 0x9876543210. The script FILESENDL is run, and it should fail.
- Station configured for WEP with key 0x0123456789, AP configured for non-WEP. The station should not associate.
- AP configured for WEP with key 0x0123456789, station configured for non-WEP. The station should not associate.

5 Station Testing - Infrastructure

There are two categories of tests which will be executed:

- Station Configurability
- Station/AP Interoperability Tests
-

These three tests are run in the order listed above. If a station does not pass a test within one of the categories, testing will not proceed into the next category.



Station Test Set-Up

5.1 Station Configurability Test

The station-under-test will be examined to verify that certain parameters can be configured. These parameters include the following:

ESSID
WEP Key

A station passes this test if these parameters can be configured as required by Section 2. It fails if one or more of these parameters cannot be configured.

5.2 Station/AP Interoperability Tests

The purpose of these initial tests is to verify that the station is able to associate and exchange data with a variety of AP configurations. These various configurations consist of APs from several different vendors, with various different values for AP (and consequently BSS) parameters. This collection of APs can be viewed as forming a fixed test bed against which the station-under-test will be exercised.

5.2.1 Description of Tests

The basic idea is as follows: to test a station, we want to test its ability to work with APs from a variety of manufacturers, with a variety of ESSIDs, with a variety of beacon intervals, with and without RTS, with and without fragmentation, with and without WEP, and on a variety of channels.

There are four tests which are executed for each configuration. Prior to the execution of these tests, the station is configured so as to match the ESSID and WEP parameters of the AP. Once the station is configured, the following four tests are executed:

5.2.1.1 Association

The AP is powered on in its defined configuration. The station is powered on in its (complementary) configuration. The station and the AP are both examined to determine whether or not the station properly associates with the AP.

5.2.1.2 Data Transfer 1

With the station associated with the AP, the Chariot script FILESENDL is executed, with the Test Server playing the role of Endpoint 1 and the station-under-test acting as Endpoint 2. The Chariot console is examined to determine whether or not the station was able to pass data successfully. The definition of success or failure is specific to the configuration, as described below.

5.2.1.3 Data Transfer 2

With the station associated with the AP, the Chariot script FILESENDL is executed, with the Test Server playing the role of Endpoint 2 and the station-under-test acting as Endpoint 1. The Chariot console is examined to determine whether or not the station was able to pass data successfully. The definition of success or failure is specific to the configuration, as described below.

5.2.1.4 Data Transfer 3

With the station associated with the AP, the Chariot script INQUIRYL is executed. The Chariot console is examined to determine whether or not the station was able to pass data successfully. The definition of success or failure is specific to the configuration, as described below.

5.2.2 AP Configurations

A number of AP’s will be pre-configured in the following configurations. The throughput values for pass/fail are specific to both the test script and the AP configuration and are identified below using the convention “CxDTy” for “Configuration x, Data Transfer Test y”.

AP Configuration #S1

<i>Vendor</i>	Proxim
<i>ESSID</i>	short
<i>Beacon Interval</i>	100 ms
<i>Channel</i>	36
<i>RTS Threshold</i>	off
<i>Fragmentation</i>	off
<i>WEP</i>	on, key = 0x1234567890

<i>Association Test</i>	if association occurs, pass
<i>Data Transfer #1</i>	throughput > S1DT1
<i>Data Transfer #2</i>	throughput > S1DT2
<i>Data Transfer #3</i>	throughput > S1DT3

Pass/Fail Criteria for Tests

AP Configuration #S2

<i>Vendor</i>	Intermec
<i>ESSID</i>	01234567890123456789012345678901 5678901
<i>Beacon Interval</i>	70 ms
<i>Channel</i>	40
<i>RTS Threshold</i>	500 bytes
<i>Fragmentation</i>	600 bytes
<i>WEP</i>	off

<i>Association Test</i>	if association occurs, pass
<i>Data Transfer #1</i>	throughput > S2DT1
<i>Data Transfer #2</i>	throughput > S2DT2
<i>Data Transfer #3</i>	throughput > S2DT3

Pass/Fail Criteria for Tests

AP Configuration #S3

Vendor	Cisco
ESSID	a
Beacon Interval	50 ms
Channel	44
RTS Threshold	off
Fragmentation	400 bytes
WEP	on, key = 0x1234567890

Association Test	if association occurs, pass
Data Transfer #1	throughput > S3DT1
Data Transfer #2	throughput > S3DT2
Data Transfer #3	throughput > S3DT3

Pass/Fail Criteria for Tests

AP Configuration #S4

Vendor	Atheros
ESSID	0123456789
Beacon Interval	120 ms
Channel	48
RTS Threshold	300 bytes
Fragmentation	off
WEP	on, key = 0x0987654321

Association Test	if association occurs, pass
Data Transfer #1	throughput > S4DT1
Data Transfer #2	throughput > S4DT2
Data Transfer #3	throughput > S4DT3

Pass/Fail Criteria for Tests

AP Configuration #S5

Vendor	Proxim
ESSID	shortESS
Beacon Interval	100 ms
Channel	52
RTS Threshold	300 bytes
Fragmentation	off
WEP	off

Association Test	if association occurs, pass
Data Transfer #1	throughput > S5DT1
Data Transfer #2	throughput > S5DT2
Data Transfer #3	throughput > S5DT3

Pass/Fail Criteria for Tests

Additional verification checks for Configuration ES1: using a wireless sniffer, verify that the station is generating ACKs and CTSs at the proper rates.

AP Configuration #S6

Vendor	Cisco
ESSID	abc
Beacon Interval	200 ms
Channel	56
RTS Threshold	500 bytes
Fragmentation	off
WEP	on, key = 0xA1B2C3D4E5

Association Test	if association occurs, pass
Data Transfer #1	throughput > S6DT1
Data Transfer #2	throughput > S6DT2
Data Transfer #3	throughput > S6DT3

Pass/Fail Criteria for Tests

AP Configuration #S7

Vendor	Atheros
ESSID	MnKz
Beacon Interval	200 ms
Channel	60
RTS Threshold	500 bytes
Fragmentation	600 bytes
WEP	off

Association Test	if association occurs, pass
Data Transfer #1	throughput > S7DT1
Data Transfer #2	throughput > S7DT2
Data Transfer #3	throughput > S7DT3

Pass/Fail Criteria for Tests

AP Configuration #S8

Vendor	Intermec
ESSID	abcDEFghi
Beacon Interval	200 ms
Channel	64
RTS Threshold	300 bytes
Fragmentation	off
WEP	on, key = 0x0123456789

Association Test	if association occurs, pass
Data Transfer #1	throughput > S8DT1
Data Transfer #2	throughput > S8DT2
Data Transfer #3	throughput > S8DT3

Pass/Fail Criteria for Tests

5.3 Special Tests for Stations

The following Special Tests will be executed. Some of these require examination of sniffer traces to determine success or failure of the station-under-test under the given test.

5.3.1 Roaming

We will test a station's ability to roam across access points from multiple vendors. This will involve setting up a configuration in which the APs are within the same ESS, starting up a Chariot test between a station and the Test Server through a first AP, and then artificially taking that AP down so as to force the station to re-associate with a second AP. This cycle continues through a set of four APs from different vendors.

The station passes this test if it re-associates with each AP.

5.3.2 Data Payload (Encapsulation)

We will verify the station's ability to correctly encapsulate packets. This involves verifying that various packets from the Ethernet are correctly received at the station, and that packets generated on the station host are correctly transferred to the Ethernet.

- Test for various payload types
- DIX Ethertypes (assorted)
- LLC (802.2) packets
- Verify RFC1042 and basic ethertype transfer for 8137 and 80F3.

The test configuration is as follows: the test server and the station under test are configured to use IPX with the same frame type selected including Ethernet 802.2, Ethernet 802.3, and Ethernet II. The Chariot script INQUIRYL is then used to verify that packet transfer can occur.

5.3.3 Broadcast/Multicast reception

We will verify the station's ability to receive broadcast and multicast packets.

In each of the AP configurations described below, the Test Server is set up to support multicasts as Chariot Endpoint 1, with the station-under-test set up as Endpoint 2. An additional station is also configured as Endpoint 2 (called the "multicast test station"). The streaming Chariot script REALAUD is used to generate a multicast stream of data.

Multicast Test Configuration

Using the Chariot Console, the station-under-test and the multicast test station are set up with IP Multicast Address 225.0.0.1. Each station's unique IP address must also be configured into the test in order for Chariot to be able to configure the IP Multicast Address on those stations.

"Validate Data upon Receipt" is selected on the Chariot Run Options tab of the Run Options dialog.

UDP is selected as the underlying protocol.

REALAUD is selected as the Chariot script.

Multicast Configuration #MCS1

Vendor	Proxim
ESSID	Multicast
Beacon Interval	100 ms
Channel	36
RTS Threshold	off
Fragmentation	off
WEP	on, key = 0x0123456789
Station-Under-Test	CAM
MC Test Station 1	CAM
MC Test Station 2	CAM

MC Data Transfer	throughput > MCS1DT
------------------	---------------------

Multicast Configuration #MCS2

Vendor	Intermec
ESSID	Multicast
Beacon Interval	80 ms
Channel	40
RTS Threshold	off
Fragmentation	off
WEP	on, key = 0x0123456789
Station-Under-Test	CAM
MC Test Station 1	CAM
MC Test Station 2	CAM

MC Data Transfer	throughput > MCS2DT
------------------	---------------------

Multicast Configuration #MCS3

Vendor	Cisco
ESSID	Multicast
Beacon Interval	100 ms
Channel	44
RTS Threshold	off
Fragmentation	off
WEP	on, key = 0x0123456789
Station-Under-Test	CAM
MC Test Station 1	PS
MC Test Station 2	PS

MC Data Transfer	throughput > MCS3DT
------------------	---------------------

Multicast Configuration #MCS4

Vendor	Atheros
ESSID	Multicast
Beacon Interval	150 ms
Channel	48
RTS Threshold	off
Fragmentation	off
WEP	on, key = 0x0123456789
Station-Under-Test	CAM
MC Test Station 1	PS
MC Test Station 2	PS

MC Data Transfer	throughput > MCS4DT
------------------	---------------------

5.3.4 Negative Tests

The station under test is checked with APs in a mismatched configuration to ensure that association and/or data transfer does not occur.

The configuration mismatches to be tested include:

- wrong ESSID: the AP is configured with ESSID abc and the station is configured with ESSID def. The station should not associate.
- wrong case in ESSID characters: the AP is configured with ABC and the station is configured with abc, and vice versa. The station should not associate in either case.
- ESSID substring: the AP is configured with abc and the station is configured with abcde, and vice versa. The station should not associate in either case.
- WEP key mismatch: the station is configured with WEP key 0x0123456789 and the AP is configured with WEP key 0x9876543210. The script FILESENDL is run, and it should fail.
- Station configured for WEP with key 0x0123456789, AP configured for non-WEP. The station should not associate.
- AP configured for WEP with key 0x0123456789, station configured for non-WEP. The station should not associate.

6 Station Testing - IBSS

If 802.11a stations under test support IBSS then these tests are required. IBSS Interoperability testing is divided into a five test campaign that covers all of the requirements enumerated in section 2. Each test has a separate test bed configuration which utilizes different options such that all meaningful combinations are verified.

The network performance in each test configuration is measured using the Chariot file send capability. The Chariot console is included as an implied member of the IBSS. In

practice the console and the test server (EP1) are run on separate PCs for 802.11a testing. However, for ad-hoc testing the tests server and the console are run on the same PC.

6.1 Active Scan Tests

Active scan tests verify that the SUT can create an IBSS, respond to active scans, and pass data.

6.1.1 Configuration S11

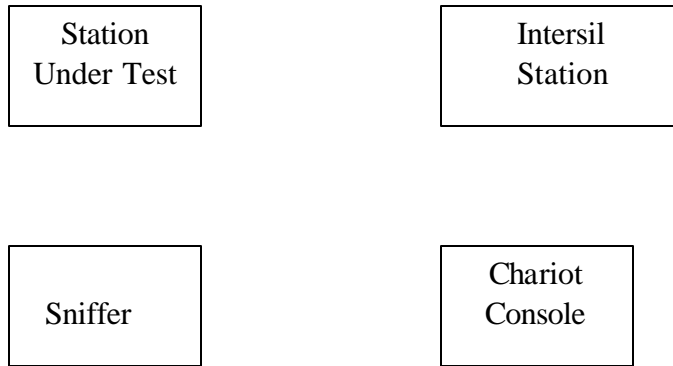


Figure 1: Active Scan Test, Configuration S11

S11 Configuration Station Under Test - Creator

<i>Vendor</i>	Station under test
<i>ESSID</i>	active scan
<i>Channel</i>	48
<i>WEP</i>	Off
<i>Fragmentation</i>	Default
<i>RTS</i>	Default
<i>Scanning</i>	Default

SI1 Configuration Vendor #1 - Joiner

Vendor	Intersil
<i>ESSID</i>	active scan
<i>Channel</i>	-
<i>WEP</i>	Off
<i>Fragmentation</i>	384
<i>RTS</i>	Off
<i>Scanning</i>	Active

6.1.2 Test Sequence

Configure SUT and Intersil as defined above.

Start SUT first so that it is the IBSS creator.

Start Intersil while monitoring with Sniffer.

Verify that when Symbol sends an active probe, that the SUT responds with a valid response. Check that

- the basic rate enumerated in the beacon message is as per the default
- The channel is correct
- Record the BSSID for later comparison to assure that it is a random value

Run the Chariot file send test from Intersil to the SUT and from SUT to Intersil. The test must complete within 1.5 minutes.

6.2 Passive Scan Tests

6.3 Configuration SI2

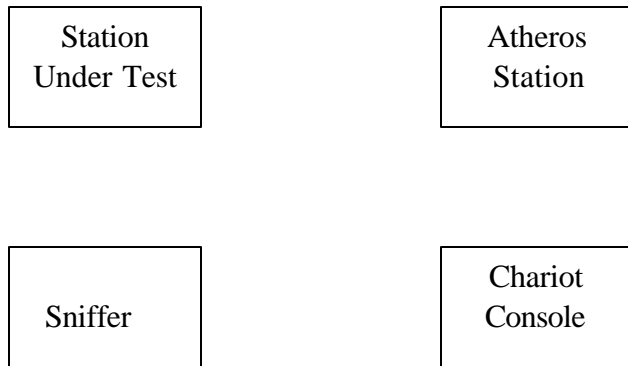


Figure 2: Passive Scan Test, Configuration SI2

SI2 Configuration Station Under Test - Creator

Vendor	Station under test
ESSID	passive scan
Channel	52
WEP	0x1122334455
Fragmentation	Default
RTS	Default
Scanning	-

SI2 Configuration Vendor #2 - Joiner

Vendor	Atheros
ESSID	passive scan
Channel	-
WEP	0x1122334455
Fragmentation	Off
RTS	300
Scanning	Passive

6.3.1 Test Sequence

Configure SUT and Atheros as defined above.

Start SUT first so that it is the IBSS creator.

Start Atheros while monitoring with Sniffer.

Verify that Atheros joins SUT IBSS. Check that

- The basic rate enumerated in the beacon message is as per the default
- The channel is correct
- Record the BSSID for later comparison to assure that it is a random value

Run the Chariot file send test from Atheros to the SUT and from SUT to Atheros. Verify that the test completes within 1.5 minutes.

Disable Atheros and restart SUT with SSID Passive Scan. Use Sniffer to record the BSSID in a beacon message. Verify that this and the two previously recorded BSSID are different.

6.4 IBSS WEP On Tests

This tests that beacons are distributed fairly among participating IBSS, validates that the SUT can join an established, WEP *enabled* IBSS and communicate with stations having RTS off or on.

Multicast operation is also tested.

6.4.1 Configuration SI3

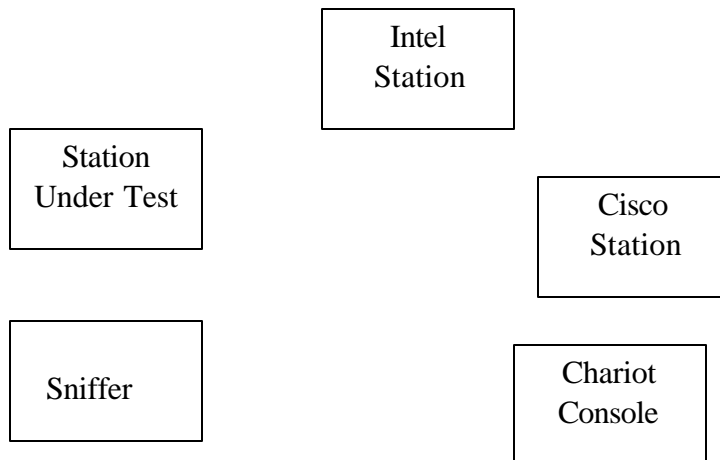


Figure 3: IBSS WEP On Test, Configuration SI3

1.

SI3 Configuration Vendor #3 - Creator

Vendor	Intel
ESSID	IBSS wep on
Channel	56
WEP	0xdeadbeef12
Fragmentation	Off
RTS	Off
Scanning	Passive

SI3 Configuration Vendor #4 - Joiner

Vendor	Cisco
ESSID	IBSS wep on
Channel	-
WEP	0xdeadbeef12
Fragmentation	Off
RTS	300
Scanning	Default

SI3 Configuration Station Under Test

Vendor	Station under test
ESSID	IBSS wep on
Channel	-
WEP	0xdeadbeef12
Fragmentation	Default
RTS	Default
Scanning	Default

6.4.2 Test Sequence

Configure SUT, Intel and Cisco as defined above.

Start Intel first so that it is the IBSS creator, then start Cisco.

Start SUT while monitoring with Sniffer.

Verify that SUT joins the IBSS. Check that the basic rate enumerated in the beacon message is as per the default.

Using the Sniffer, verify that beacons are distributed fairly between participating stations.

After the network is up, capture a trace for 2 minutes and look at the results.

Hint: Set up the Sniffer to show only beacon messages. Use pie chart distribution to show distribution of traffic by node, including source and destination MAC addresses. Approximately 50% of packets should be the destination broadcast address (0xfffff), the other 50% should be the source MAC addresses of the participating IBSS members.

There should be four stations sending beacons (including the Chariot console). Consequently, each station should be approximately 12% of the total (25% of 50%).

A range between 4.5% (9% of packets) and 20% (40% of packets) is acceptable.

Run the Chariot file send test from Cisco to the SUT
 Verify that throughput is greater than SI3DT1.

Run the Chariot file send test from SUT to Cisco.
 Verify that throughput is greater than SI3DT2.

Run the Chariot multicast Real-Audio test with Intel as the broadcaster, and verify the SUT receives the multicast.

Verify that multicast throughput is greater than SI3DT3.

Run the Chariot multicast Real-Audio test with SUT as the broadcaster, and verify that Intel and Cisco receive the multicast.

Verify that multicast throughput is greater than SI3DT4 in both cases.

6.5 IBSS WEP Off Tests

This tests that beacons are distributed fairly among participating IBSS, validates that the SUT can join an established, WEP *disabled* IBSS and communicate with stations having RTS off or on. Multicast operation is also tested.

6.5.1 Configuration SI4

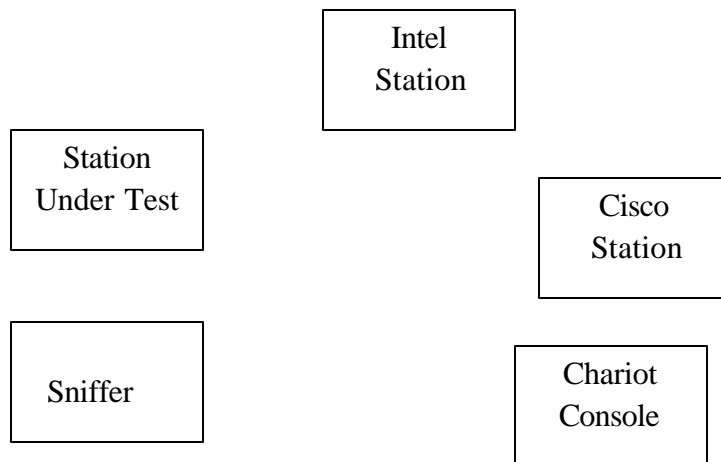


Figure 4: IBSS WEP Off Test, Configuration SI4

SI4 Configuration Vendor #3- Creator

<i>Vendor</i>	Intel
<i>ESSID</i>	IBSS wep off
<i>Channel</i>	60
<i>WEP</i>	Off
<i>Fragmentation</i>	Off
<i>RTS</i>	Off
<i>Scanning</i>	Passive

SI4 Configuration Vendor #4 - Joiner

<i>Vendor</i>	Cisco
<i>ESSID</i>	IBSS wep off
<i>Channel</i>	-
<i>WEP</i>	Off
<i>Fragmentation</i>	400
<i>RTS</i>	300
<i>Scanning</i>	-

SI4 Configuration Station Under Test - Joiner

<i>Vendor</i>	Station under test
<i>ESSID</i>	IBSS wep off
<i>Channel</i>	-
<i>WEP</i>	Off
<i>Basic Rates</i>	Default
<i>Fragmentation</i>	Default
<i>RTS</i>	Default
<i>Scanning</i>	Default

6.5.2 Test Sequence

Configure SUT, Intel and Cisco as defined above.

Start Intel first so that it is the IBSS creator, then start Cisco.4

Start SUT while monitoring with Sniffer.

Verify that SUT joins the IBSS. Check that the basic rate enumerated in the beacon message is as per the default

Using the Sniffer, verify that beacons are distributed fairly between participating stations as described in the previous section.

Run the Chariot file send test from Intel to the SUT.

Verify that throughput is greater than SI4DT1.

Run the Chariot file send test from SUT to Intel.

Verify that throughput is greater than SI4DT2.

Run the Chariot file send test from Cisco to the SUT
Verify that throughput is greater than SI4DT3.

Run the Chariot file send test from SUT to Cisco.
Verify that throughput is greater than SI4DT4.

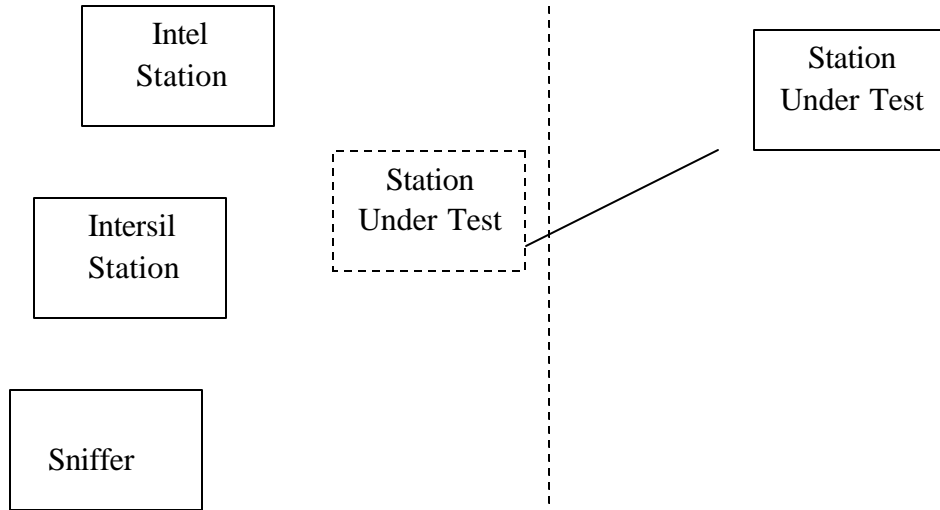
6.6 Re-Join Tests

Tests the ability of the SUT to leave an IBSS and later re-join it.

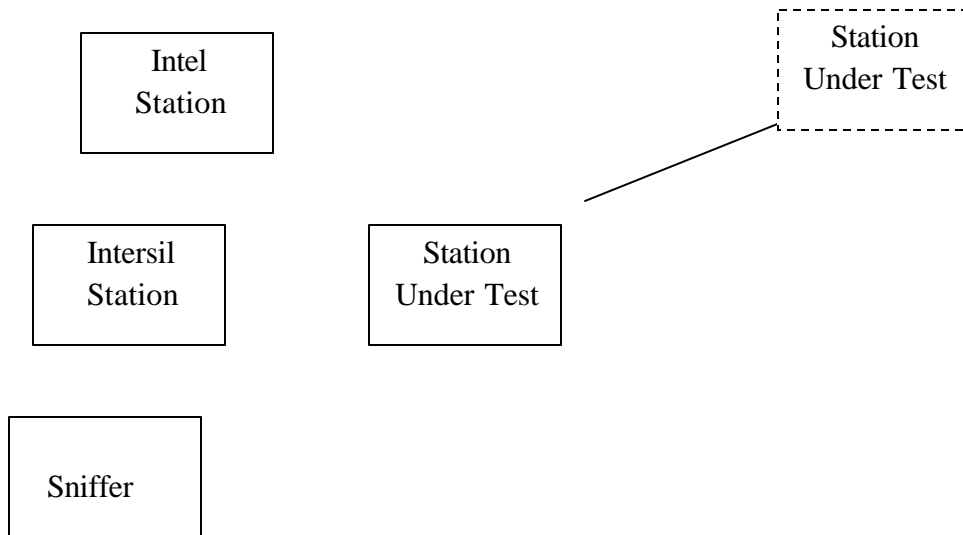
The SUT is initially a member of an IBSS. It is then isolated from the IBSS, without restarting it. This isolation may be achieved either by physically moving the stations or by isolating in a suitable RF cage. Once isolated, the SUT is then brought back within range of the original IBSS.

6.6.1 Configuration SI5

The test configuration consists a three node IBSS.



SUT Moving Out of Range



SUT Moving Back Into Range

Figure 5: Rejoin Test – Configuration SI5

SI5 Configuration Vendor #3 – Creator 1

Vendor	Intel
ESSID	rbejoin
Channel	36
WEP	Off
Fragmentation	Off
RTS	Off
Scanning	-

SI5 Configuration Vendor #1 - Joiner

Vendor	Intersil
ESSID	rejoin
Channel	-
WEP	Off
Fragmentation	Off
RTS	Off
Scanning	-

SI5 Configuration Station Under Test - Joiner

Vendor	Station under test
ESSID	rejoin
Channel	-
WEP	Default
Fragmentation	Default
RTS	Default
Scanning	Default

6.6.2 Test Sequence

Configure the stations as described above.

Co-locate all stations within range of each other, and join all three stations into one IBSS.

Sniff the beacon messages and record contents of a beacon used for this IBSS.

Move the SUT out of range. Verify that it is out of range using the Sniffer to validate that beacon messages from SUT are no longer received. (The original IBSS survives without the SUT). Move the SUT back within range of the original IBSS. Verify that all 3 stations have rejoined into one IBSS by sniffing beacon messages. Each station must use the BSS parameters of the original IBSS, including Basic Rate Set. Further verify operation by pinging from the SUT to all other stations.

7 Dual Band Tests

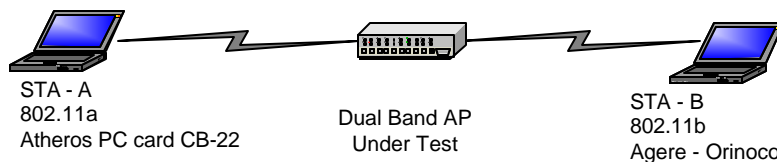
When a station or an access point supports both 802.11a and 802.11b then each must be tested sequentially.

When an AP support both modes simultaneously, the Bridging Throughput Test is required

When a station automatically supports either band, then the Cross-Band Roaming test is required.

7.1 Bridging Throughput Test for Dual Band APs

When an AP supports both 802.11a and 802.11b simultaneously, it must be possible to pass data between stations operating on 802.11a and 802.11b. This is an addition to the Intra-BSS Transfer test specified elsewhere¹.



The Chariot FILESENDL is used to send data between the two stations operating as Endpoints 1 and 2.

This test is used to measure throughput when data is sent from STA-A to STA-B, then the throughput is measured when sending data in the opposite direction (EP1 and EP2 reversed).

The configuration specified in Configuration A1 in the 802.11b test specification (Section 4.2.2) is used for the 802.11b portion of the AP.

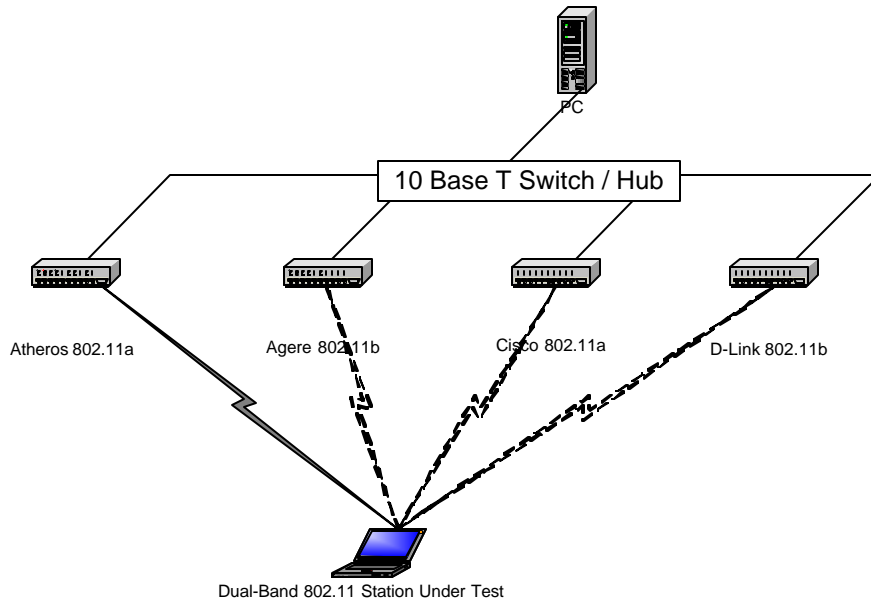
The configuration A1 in the 802.11a test specification (Section 4.2.2) is used for the 802.11a portion of the AP.

The throughput must be equal to or greater than value S1DT1 specified in the 802.11b test specification.

¹ 802.11b products – System Interoperability Test Plan for IEEE 802.11b Devices Version 1.1
802.11a products – System Interoperability Test Plan for IEEE 802.11a Devices Version 1.0 (this document)

7.2 Cross-Band Station Roaming Test for Dual Band Stations

This tests the ability of the station to roam between 802.11a and 802.11b access points.



The Station Under Test (SUT) is forced to roam from AP #1 to AP #2 to AP #3 to AP #4 and back to AP #1. One second pings are used to validate connectivity with the PC. Pings must not be lost for more than 11 seconds (11 lost pings) during a roam from one AP to the next. (Note: the roaming requirement is 10 seconds, one additional second is allowed for ping accuracy purposes.)

1. The station is associated with AP#1, pings OK, (all other APs are disabled.)
2. AP#2 is enabled and AP#1 is disabled. If the SUT roams within 10 seconds, PASS
3. AP#3 is enabled and AP#2 is disabled. If the SUT roams within 10 seconds, PASS.
4. AP#4 is enabled and AP#3 is disabled. If the SUT roams within 10 seconds, PASS.
5. AP#1 is enabled and AP#4 is disabled. If the SUT roams within 10 seconds, PASS.

Access Points

AP #1	802.11a	Cisco Aironet 1200 Series AP
AP #2	802.11b	Agere AP-1000
AP #3	802.11a	Atheros AR5001 AP Reference Design AP
AP #4	802.11b	D-Link DWL-900AP

AP Configuration

7.3 ESSID	“012345678901232456789012345678901”
<i>Beacon Interval</i>	100Kus
<i>Channel #</i>	60 (802.11a) 10 (802.11b)
<i>RTS Threshold</i>	Off
<i>Fragmentation</i>	Off
<i>WEP</i>	Off
<i>Basic Rates</i>	All (802.11b)

8 Appendix A: Throughput Values

This appendix defines the required throughput values for the specific test configurations and data transfer tests.

The following values are identified by codes of the form XXnDTm, where the XX prefix describes the basic type of test configuration, n is the number of the specific configuration within that type, and DTm identifies the data transfer test and script used.

Test Configuration Types

S	Initial Station Testing Configurations
IBSSC	IBSS Create
IBSSJ	IBSS Join
A	Initial AP Testing Configurations
EA	Extended AP Testing Configurations
MCS	Multicast Station Testing Configurations
MCA	Multicast AP Testing Configurations

Throughput Values

A1DT1	7 Mbps - Cisco
A1DT2	8 Mbps - Cisco
A1DT3	0.5 Mbps - Cisco
A2DT1	6 Mbps - Cisco
A2DT2	8 Mbps - Cisco
A2DT3	1 Mbps - Cisco
A3DT1	10 Mbps - Intel
A3DT2	5 Mbps - Intel
A3DT3	0.5 Mbps - Intel
A4DT1	13 Mbps - Atheros
A4DT2	11 Mbps - Atheros
A4DT3	1 Mbps - Atheros
A6DT1	13 Mbps - Atheros
A6DT2	8 Mbps - Atheros
A6DT3	0.9 Mbps - Atheros
A7DT1	5 Mbps - Intersil
A7DT2	0.4 Mbps - Intersil
A7DT3	0.01 Mbps - Intersil
A8DT1	8 Mbps - Cisco
A8DT2	9 Mbps - Cisco
A8DT3	0.7 Mbps - Cisco
A9DT1	10 Mbps - Intel
A9DT2	7 Mbps - Intel
A9DT3	1.1 Mbps - Intel

Wi-Fi Alliance CONFIDENTIAL

A10DT1	11 Mbps - Atheros
A10DT2	11 Mbps - Atheros
A10DT3	1 Mbps - Atheros
A11DT1	11 Mbps - Atheros
A11DT2	11 Mbps - Atheros
A11DT3	1.1 Mbps - Atheros
A12DT1	5 Mbps - Intersil
A12DT2	2 Mbps - Intersil
A12DT3	0.1 Mbps - Intersil
A13DT1	15 Mbps - Intersil
A13DT2	10 Mbps - Intersil
A13DT3	0.8 Mbps - Intersil
MCA	Multicast AP Test Configurations
MCA1DT	0.05 Mbps
MCA2DT	0.05 Mbps
MCA3DT	0.05 Mbps
MCA4DT	0.05 Mbps
S1DT1	10 Mbps - Proxim
S1DT2	13 Mbps - Proxim
S1DT3	1 Mbps - Proxim
S2DT1	9 Mbps - Intermec
S2DT2	9 Mbps - Intermec
S2DT3	1.1 Mbps - Intermec
S3DT1	6 Mbps - Cisco
S3DT2	6 Mbps - Cisco
S3DT3	0.9 Mbps - Cisco
S4DT1	15 Mbps - Atheros
S4DT2	9 Mbps - Atheros
S4DT3	1.0 Mbps - Atheros
S5DT1	9 Mbps - Proxim
S5DT2	11 Mbps - Proxim
S5DT5	1 Mbps - Proxim
S6DT1	8 Mbps - Cisco
S6DT2	14 Mbps - Cisco
S6DT3	0.9 Mbps - Cisco
S7DT1	7 Mbps - Atheros
S7DT2	15 Mbps - Atheros
S7DT3	1.1 Mbps - Atheros
S8DT1	8 Mbps - Intermec
S8DT2	13 Mbps - Intermec
S8DT3	1.2 Mbps - Intermec
MCS	Multicast Station Test Configurations
MCS1DT	0.05 Mbps
MCS2DT	0.05 Mbps

MCS3DT	0.05 Mbps
MCS4DT	0.05 Mbps
SI3DT1	9 Mbps – Intel & Cisco
SI3DT2	9 Mbps – Intel & Cisco
SI3DT3	0.05 Mbps – Intel & Cisco
SI4DT1	11 Mbps – Intel & Cisco
SI4DT2	11 Mbps – Intel & Cisco
SI4DT3	10 Mbps – Intel & Cisco
SI4DT4	10 Mbps – Intel & Cisco

9 Appendix B: Channel Numbers

Frequency MHz	IEEE 802.11a Channel #	CEPT Channel #	Remarks
5180	36		40 mW
5200	40		40 mW
5220	44		40 mW
5240	48		40 mW
5260	52		100 mW
5280	56		100 mW
5300	60		100 mW
5320	64		100 mW
5745	149		100 mW
5765	153		100 mW
5785	157		100 mW
5805	161		100 mW

IEEE 802.11a channel number / frequency definition: $f \text{ (MHz)} = 5000 + 5 * \text{Channel \#}$

10 Appendix C: Vendor Equipment List

10.1 Stations

Vendor Name	Atheros ²
Product Name	AR 5001X Cardbus Reference Design Board - Station
Model #	AR5BCB-00022A
Driver Revision #	2.1.0.355
Firmware Revision #	N/A
Config Utility Revision #	2.1.0.355
Contact Info Name	Andy Davidson
Phone #	408-773-5248
Email address	adavidson@atheros.com
Address	529 Almanor Avenue, Sunnyvale, CA 94085
Comments	

Vendor Name	Cisco
Product Name	Cisco Aironet 5GHz WLAN Adaptor - Station
Model #	AIR-CB20A
Driver Revision #	3.4.19
Firmware Revision #	5.01.02
Config Utility Revision #	5.03.009
Contact Info Name	Dale Williams
Phone #	330-664-7908
Email address	dwill@cisco.com
Address	320 Springside Drive, Suite 350, Akron, OH 44333
Comments	

Vendor Name	Intel ³
Product Name	Pro Wireless 5000 LAN CardBus - Station
Model #	WCB 5000
Driver Revision #	1.0.1.31
Firmware Revision #	N/A
Config Utility Revision #	1.0.1.31
Contact Info Name	Elsa Zendejas
Phone #	805-376-6810
Email address	elsa.zendejas@intel.com
Address	2300 Corporate Center Dr., Thousand Oaks, CA 91320
Comments	

² Requires Registry manipulation for test settings – see Appendix D, section 11.1

³ Requires Registry manipulation test settings – see Appendix D, section 11.2

Vendor Name	Intersil
Product Name	Indigo - Station
Model #	ISL 37703C
Driver Revision #	1.0.2.0
Firmware Revision #	N/A
Config Utility Revision #	1.0.0
Contact Info Name	Bruce Kraemer
Phone #	321-729-5683
Email address	bkraemer@intersil.com
Address	2401 Palm Bay Road NE, Palm Bay, FL 32905
Comments	

10.2 Access Points

Vendor Name	Atheros
Product Name	AR5001AP Reference Design Access Point
Model #	AR5BAP-00021A
Driver Revision #	N/A
Firmware Revision #	2.1.0.355
Config Utility Revision #	N/A
Contact Info Name	Andy Davidson
Phone #	408-773-5248
Email address	adavidson@atheros.com
Address	529 Almanor Avenue, Sunnyvale, CA 94085
Comments	

Vendor Name	Cisco
Product Name	Cisco Aironet 1200 Series Access Point
Model #	AIR-AP1220A + AIR-RM20A
Driver Revision #	N/A
Firmware Revision #	11.56 + RF 5.01.02
Config Utility Revision #	HTML
Contact Info Name	Dale Williams
Phone #	330-664-7908
Email address	dwill@cisco.com
Address	320 Springside Drive, Suite 350, Akron, OH 44333
Comments	

Vendor Name	Intermec
Product Name	Mobilan Access Point
Model #	2106
Driver Revision #	N/A
Firmware Revision #	1.73-5.98
Config Utility Revision #	1.73-5.98
Contact Info Name	Tom Seedorff
Phone #	319-369-3500
Email address	tom.seedorff@intermec.com
Address	550 2 nd Street SE., Cedar Rapids, IA 52401
Comments	

Vendor Name	Proxim ⁴
Product Name	Orinoco AP 2000 Access Point
Model #	AP2000
Driver Revision #	N/A
Firmware Revision #	8.42 build 2.0.3 (303)
Config Utility Revision #	HTML
Contact Info Name	Douglas M. Cohen
Phone #	678-924-6583
Email address	dcohen@proxim.com
Address	3950 Shackleford Road, Suite 500, Duluth, GA 30096
Comments	

⁴ Requires a MIB Browser for test settings – e.g. NuDesign Visual MIB Browser

11 Appendix D

11.1 Atheros Wireless Network Adapter

Section 11.2 provides basic information for selecting channel frequency, fixed data rate, RTS threshold parameter, fragmentation parameter, and beacon interval in the NDIS driver. This becomes necessary if you want to implement the Atheros Wireless Network Adapter at a specific interoperability testing.

11.1.1 Parameter Configurable

11.1.2 Channel Frequency

To select channel frequency in the Windows environment with NDIS driver installed:

1. Click Start, Run, and type “regedit” to open Registry Editor.
2. For Windows 2000 and Windows XP, locate the following registry key, and select “Find” from the Edit menu:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
3. For Windows 98SE and Windows Me, locate the following registry key, and select “Find” from the Edit menu:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\
4. Type “clist” and click “Find Next” to find the registry key. Note that if you have multiple instances of the Atheros Wireless Network Adapter installed, for instance, the NDIS driver is installed more than once, then you will need to click “Find Next” to locate the current instance of the device that is in use.
5. Double-click on “clist” and enter the channel number in the “Value Data” field. Enter the channel frequency followed by an “a” for 802.11a, “b” for 802.11b Mode. For example, enter 5200a for channel 40. The channel numbers follow the IEEE format:

$$\text{Channel Frequency (in GHz)} = 5 + 0.005 * (\text{Channel Number})$$

Follow the tables below for 802.11a and 802.11b channel values.

802.11a Channel Number	Channel Frequency	Regulator Domain
26	5130 MHz	N/A
28	5140 MHz	N/A
30	5150 MHz	N/A
32	5160 MHz	N/A
34	5170 MHz	TELEC
36	5180 MHz	FCC/ ETSI
38	5190 MHz	TELEC
40	5200 MHz	FCC/ ETSI
42	5210 MHz	TELEC
44	5220 MHz	FCC/ ETSI
46	5230 MHz	TELEC
48	5240 MHz	FCC/ ETSI
50	5250 MHz	N/A
52	5260 MHz	FCC/ ETSI
54	5270 MHz	N/A
56	5280 MHz	FCC/ ETSI
58	5290 MHz	N/A
60	5300 MHz	FCC/ ETSI
62	5310 MHz	N/A
64	5320 MHz	FCC/ ETSI
66	5330 MHz	N/A
68	5340 MHz	N/A
70	5350 MHz	N/A
72	5360 MHz	N/A
74	5370 MHz	N/A
76	5380 MHz	N/A
78	5390 MHz	N/A
80	5400 MHz	N/A
82	5410 MHz	N/A
84	5420 MHz	N/A
86	5430 MHz	N/A
100	5500 MHz	ETSI
104	5520 MHz	ETSI
108	5540 MHz	ETSI
112	5560 MHz	ETSI
116	5580 MHz	ETSI
120	5600 MHz	ETSI
124	5620 MHz	ETSI
128	5640 MHz	ETSI
132	5660 MHz	ETSI
136	5680 MHz	ETSI
140	5700 MHz	ETSI
149	5745 MHz	FCC
153	5765 MHz	FCC
157	5785 MHz	FCC
161	5805 MHz	FCC

802.11b Channel Number	Channel Frequency	Regulator Domain
1	2412 MHz	FCC/ ETSI
2	2417 MHz	FCC/ ETSI
3	2422 MHz	FCC/ ETSI
4	2427 MHz	FCC/ ETSI
5	2432 MHz	FCC/ ETSI
6	2437 MHz	FCC/ ETSI
7	2442 MHz	FCC/ ETSI
8	2447 MHz	FCC/ ETSI
9	2452 MHz	FCC/ ETSI
10	2457 MHz	FCC/ ETSI
11	2462 MHz	FCC/ ETSI
12	2467 MHz	ETSI
13	2472 MHz	ETSI
14	2484 MHz	N/A

11.1.3 RTS Threshold

To select the RTS threshold parameter configurable, double-click on the “RTSThreshold” from the same registry key location where clist resides, and enter the value. For example, enter “2346” for RTS threshold off.

11.1.4 Fragmentation Threshold

To select the fragmentation parameter configurable, double-click on the “FragThreshold” from the same registry key location where clist resides, and enter the value. For example, enter “2346” for fragmentation threshold off.

11.1.5 Beacon Interval

To select the beacon interval parameter configurable, double-click on the “beaconInterval” from the same registry key location where clist resides, and enter the value. For example, enter “100” for 100ms.

11.1.6 The Changes to Take Effect

2. If you are running Windows 98SE or Windows ME, close Register Editor and restart the systems.
3. If you are running Windows 2000 or Windows XP, unload and load the driver from Linkmon (or via “Disable” and “Enable” functions via Right-click on the NIC Icon in the “Network & Dial-up Connections” window).

11.2 Intel ProWireless 5000

To change settings, use the following:

Start->Run->"regedit.exe"

Edit->Find->"pro/wireless 5000" (You may have to search multiple times, typically the 2nd or 3rd instance will contain the settings)

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\(Look for instance)

Here you can edit the following keys

beaconInterval : Same as name implies default 100

FragThreshold : Frag Threshold default 2346

RTSThreshold : RTS Threshold default 2346

- End -