1001 Aviation Parkway, Suite 400 • Morrisville, NC 27560 • 919-380-2800 • Fax 919-380-2899
320 B Lakeside Drive • Foster City, CA 94404 • 650-513-8000• Fax 650-513-8099
www.etestinglabs.com • info@etestinglabs.com • 877-619-9259 (toll free)

IEEE 802.11a Interoperability Testing Program

May 2002

Table of Contents

Summary of Testing Costs

Standard Interoperability Testing

Test with report and Web posting:	**$5,000**

Optional Testing (details in Appendix A)

Range Testing	**$1,000**
Throughput Testing	**$1,000**

Network Testbed Configuration

This 802.11a testing program will use four vendor solutions in the test bed in addition to the contracted client's solution in each section.

For all of the tests, we will set up a Basic Service Set (BSS) using the client's solution as the Access Point (AP), replacing it with the other vendors' products in the same environment in separate tests. If the client has only a wireless Station (STA) available for testing, we will still test that device against certified APs as well as the BSS or Ad-Hoc network connection to the other STAs.

We will install wireless hardware from the various vendors (as indicated above), including the client's solution, on each station (STA). The BSS will be part of a Distribution System (DS) that will also include a Public Domain Controller (PDC), which will also be used as Controller for use with NetIQ's Chariot and a network sniffing tool to verify packet activity. All systems will have Windows 2000, Service Pack 2 installed. Figure 1 below shows a graphic representation of this testbed.

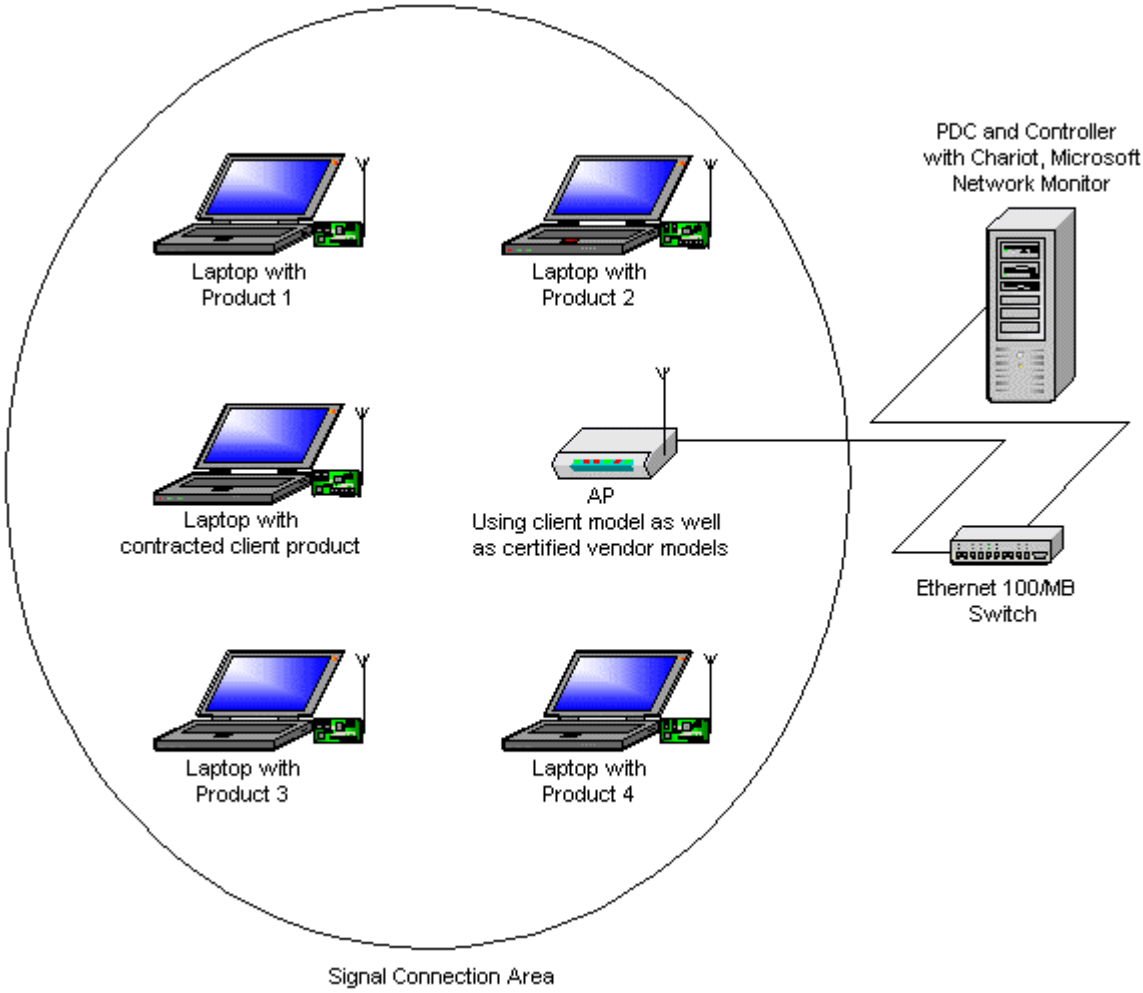

Figure 1: Proposed network testbed illustration for 802.11a compliance testing

Here are the reasons we chose this configuration:

- It includes the contracted client's wireless hardware along with the other four vendors in the same environment.
- It allows the ability to test between the various wireless STAs as well as between those STAs and the client's AP.
- Its ease of setup allows for minimal related costs. We use the same setup for the packet send and ACK transactions as well as the bandwidth capability and comparison tests.

Tools used for Certification Testing

eTesting Labs will use Chariot from NetIQ, Inc., and use the following scripts that come with the package:

- 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.

We will manage the script definition, test configuration, test execution, and results reporting through the Chariot "console," which we will install on a separate system within the BSS and ESS. We will use a network sniffing tool to verify network traffic. We will monitor sleep intervals and association activity using the Atheros LinkMon.exe tool. However, if the LinkMon tool does not support a vendor's device, the vendor must provide a means to monitor each of these activities to help facilitate execution of these tests.

Test Failures

It is possible that any device under test (DUT) could fail any part of this test for one reason or another. To allow for all possible variables during the testing process, eTesting Labs will contact the client immediately upon receiving a failing result for verification of proper setup and configuration. If we, or the client, can make the necessary changes or arrive at a solution to the problem within eight (8) business hours, we will retest the devices once more under the new environment immediately afterwards, before proceeding to the next phase. The time we require to complete the test will increase by the amount of time necessary to resolve the problem.

If the client cannot come up with a way to obtain a passing grade within the specified time, we will cease testing; the client will be liable for the full testing fee. The client has the option to contract eTesting Labs to conduct ad hoc investigations at a price of $250/hour to determine a resolution to this problem. In the event that the ad hoc investigation determines that eTesting Labs user error caused the problem, we will not bill the client for either the investigation time or the time it takes us to repeat the test.

In the event that the ad hoc investigation determines that a bug or anomaly in the client hardware caused the problem, eTesting Labs will have to repeat the entire test and charge the client for the new complete test (the client will already have paid for the original test).

Part 1: SSID Configuration Test

STA SSID Test

The STAs and APs communicate through beacon and probe requests using Service Set Identifiers (SSIDs). The SSID attaches to packets that a device sends over the wireless LAN when that device asks to join a particular Basic Service Set (BSS). The SSID is case sensitive and must be between 0 and 32 characters in length. A SSID set to null on the STA sends the SSID with the broadcast probe.

For this test, we will verify that the STA allows for configuration of the SSID and that it matches the above criteria. For example, the STA must allow for case sensitive configuration, special characters, limitation of the 32-character length, etc.

STA Test Configuration	
SSIDs	ETESTINGLABS ABCDEFG1234567890 1234567890qrstuvwxyz 1234567890ABCDEF ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890 (This entry should cause a failure because the SSID cannot be longer than 32 characters)
ASCII feature test SSIDs	<SPACE>!"#$%&'()*+,./0123456789 ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz :;<=>?@ [\]^_‘{|}~
TCP/IP Addressing	Static

Table 1: STA test configuration

Specific Requirements

The DUT will need the following capabilities and features to pass SSID testing:

- Service Set Identifier (SSID) Element
  The SSID is an identifier attached to packets that a device sends over the wireless LAN when that device asks to join a particular wireless network (BSS). All STAs and AP's within the same BSS must use the same SSID, or the devices will ignore their packets.
  - ✓ The DUT must support printable characters at a minimum
  - ✓ SSID character strings must not terminate with an ASCII null character
  - ✓ The ASCII SSID AP feature test includes special characters that may be problematic for some devices. We will test and report our results using four SSIDs that contain some of these known problematic characters.
    - A failure using any of these four unique SSIDs does not constitute a failing DUT for this particular SSID test. This test is for informational purposes.

STA SSID Test

1) Install and set up AP and STAs.
2) Set static TCP/IP addressing in all systems.
3) Test using each of the required SSIDs on each of the STAs to ensure compliance.

SSID to assign to DUT STA	D-Link AP	Netgear AP	Zcom AP	Sony AP	DUT AP
ETESTINGLABS					
ABCDEFG1234567890					
1234567890qrstuvwxyz					

1234567890ABCDEF					
ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890 (This entry should cause a failure since the SSID cannot be longer than 32 characters)					
ASCII SSID STA feature test	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
<SPACE>!"#$%&'()*+,./0123456789					
ABCDEFGHIJKLMNOPQRSTUVWXYZ					
abcdefghijklmnopqrstuvwxyz					
:;<=>?@ [\]^_‘{|}~					

Table 2: STA SSID Test checklist

AP SSID Test

We will apply the same test described above to the AP if one is available (configuration specs given below in Table 2). In addition to the SSID and WEP, we will also verify Channel and Data Rate configuration abilities. An SSID set to zero or null length sends the SSID with the broadcast probe.

AP Test Configuration	
SSIDs	ETESTINGLABS ABCDEFG1234567890 1234567890qrstuvwxyz 1234567890ABCDEF Null or zero length (the STA is set as a broadcast entity under this setting)
ASCII feature test SSIDs	<SPACE>!"#$%&'()*+,./0123456789 ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz :;<=>?@ [\]^_`{|}~
TCP/IP Addressing	Static

Table 3: AP test configuration

Specific Requirements
The DUT will need the following capabilities and features to pass SSID testing:

- Service Set Identifier (SSID) Element
  The SSID is an identifier attached to packets that a device sends over the wireless LAN when that device asks to join a particular wireless network (BSS). All STAs and access points within the same BSS must use the same SSID, or the devices will ignore their packets.
  - ✓ The DUT must support printable characters at a minimum
  - ✓ SSID character strings must not terminate with an ASCII null character
  - ✓ AP must respond to broadcast SSID probe requests
    - Confirm SSID response is enabled
  - ✓ The ASCII SSID AP feature test includes special characters that may be problematic for some devices. We will test and report our results using four SSIDs that contain some of these known problematic characters.
    - A failure using any of these four unique SSIDs does not constitute a failing DUT for this particular SSID test. This test is for informational purposes.

AP SSID Test
1) Install and set up APs.
2) Set static TCP/IP addressing in all systems.
3) Test using each of the required SSIDs on the APs to ensure compliance.

SSID to assign to DUT AP	D-Link STA	Netgear STA	Zcom STA	Sony STA	DUT STA
ETESTINGLABS					
ABCDEFG1234567890					
1234567890qrstuvwxyz					
1234567890ABCDEF					
ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890 (This entry should cause a failure since the SSID cannot be longer than 32 characters)					
0 or null (for the AP with the STA set to scan)					

ASCII SSID AP feature test	D-Link STA	Netgear STA	Zcom STA	Sony STA	DUT STA
<SPACE>!"#$%&'()*+,./0123456789					
ABCDEFGHIJKLMNOPQRSTUVWXYZ					
abcdefghijklmnopqrstuvwxyz					
:;<=>?@ [\]^_‘{|}~					

Table 4: AP SSID Test checklist

Part 2: Ad Hoc Tests

STA Ad Hoc Interoperability

Ad Hoc mode involves connecting two STAs without an AP. Testing will monitor and evaluate the authentication and packet transfer between two STAs in the signal control area. We will monitor the activity on the source STA as well as using a network sniffing tool on the controlling server.

STA Test Configuration	
SSID	ETESTINGLABS
TCP/IP Addressing	Static
Packet Sizes in bytes	32, 101, 961, 962, 1468

Table 5: STA test configuration

STA Ad Hoc Interoperability Test

1) Configure all the STAs with the same SSID ("ETESTINGLABS"), and set them for Ad Hoc mode.
2) From the STA, use a network sniffing tool to capture packet activity.
3) Issue ping requests from each STA to the other STA using the required packet sizes, and confirm ICMP activity and validation.
   (Example: ping 10.0.0.1 –L 32) PASS: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Ping from STA to STA	D-Link STA	Netgear STA	Zcom STA	Sony STA	DUT STA
D-Link STA ping with 32 bytes	N/a				
D-Link STA ping with 101 bytes	N/a				
D-Link STA ping with 961 bytes	N/a				
D-Link STA ping with 962 bytes	N/a				
D-Link STA ping with 1468 bytes	N/a				
Netgear STA ping with 32 bytes		N/a			
Netgear STA ping with 101 bytes		N/a			
Netgear STA ping with 961 bytes		N/a			
Netgear STA ping with 962 bytes		N/a			
Netgear STA ping with 1468 bytes		N/a			
Zcom STA ping with 32 bytes			N/a		
Zcom STA ping with 101 bytes			N/a		
Zcom STA ping with 961 bytes			N/a		
Zcom STA ping with 962 bytes			N/a		
Zcom STA ping with 1468 bytes			N/a		
Sony STA ping with 32 bytes				N/a	
Sony STA ping with 101 bytes				N/a	
Sony STA ping with 961 bytes				N/a	
Sony STA ping with 962 bytes				N/a	
Sony STA ping with 1468 bytes				N/a	
DUT STA ping with 32 bytes					N/a
DUT STA ping with 101 bytes					N/a
DUT STA ping with 961 bytes					N/a
DUT STA ping with 962 bytes					N/a

DUT STA ping with 1468 bytes					N/a

Table 6: Ad Hoc Interoperability Test checklist

STA Ad Hoc SSID Negative Interoperability Test

We will also create mismatched configurations between the DUT and other STAs and use this to verify that association and data transfers will not be possible between the DUT and other STAs.

Configuration mismatches between the STAs will consist of incorrect SSIDs, including case-sensitive errors.

STA Ad Hoc SSID Negative Interoperability Test

1) Configure each of the STAs with the different SSIDs in Table 5 and set each for Ad Hoc mode.

STA	D-Link STA	Netgear STA	Zcom STA	Sony STA	DUT STA
SSID	DLINK	NETGEAR	ZCOM	SONY	DUT

Table 7: STA configuration

2) From the source STA, use a network sniffing tool to capture packet activity.
3) Issue ping requests from each STA to the other STA using the required packet sizes, and confirm association and data transfers will not be possible during ICMP activity.
(Example: ping 10.0.0.1 –L 32) PASS: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)

Ping From STA to STA	D-Link STA	Netgear STA	Zcom STA	Sony STA	DUT STA
D-Link STA ping with 32 bytes	N/a				
D-Link STA ping with 101 bytes	N/a				
D-Link STA ping with 961 bytes	N/a				
D-Link STA ping with 962 bytes	N/a				
D-Link STA ping with 1468 bytes	N/a				
Netgear STA ping with 32 bytes		N/a			
Netgear STA ping with 101 bytes		N/a			
Netgear STA ping with 961 bytes		N/a			
Netgear STA ping with 962 bytes		N/a			
Netgear STA ping with 1468 bytes		N/a			
Zcom STA ping with 32 bytes			N/a		
Zcom STA ping with 101 bytes			N/a		
Zcom STA ping with 961 bytes			N/a		
Zcom STA ping with 962 bytes			N/a		
Zcom STA ping with 1468 bytes			N/a		
Sony STA ping with 32 bytes				N/a	
Sony STA ping with 101 bytes				N/a	
Sony STA ping with 961 bytes				N/a	
Sony STA ping with 962 bytes				N/a	
Sony STA ping with 1468 bytes				N/a	
DUT STA ping with 32 bytes					N/a
DUT STA ping with 101 bytes					N/a
DUT STA ping with 961 bytes					N/a
DUT STA ping with 962 bytes					N/a
DUT STA ping with 1468 bytes					N/a

Table 8: Ad Hoc Negative Interoperability Test checklist

STA Ad Hoc Interoperability WEP Test

Perform the same Ad-Hoc interoperability test as described above between the DUT and STAs that have the ability to communicate on this level.

We will also test the STA's ability to configure Wired Equivalent Privacy (WEP). WEP is an optional function ratified by the IEEE that offers frame transmission privacy similar to a wired network. It generates a secret shared algorithmic encryption key that both source and destination stations can use to alter frame bits to avoid disclosure to eavesdroppers. WEP thus denies access to anyone who does not have an assigned key.

To increase security on wireless systems by wired standards, IEEE 802.11 allows for encryption in its communication by using an optional privacy algorithm. The test will report the ability of each vendor's solution to include this standard and measure the performance levels when the standard is in use.

Configuration mismatches between the STAs and the DUT STA will include:

- Incorrect WEP keys
- One device using WEP while the other is not

Specific Requirements

As well as satisfying previous Ad Hoc testing requirements, the DUT will need the following capabilities and features to pass this test:

- Wired Equivalent Privacy
  - ✓ The STA with WEP off must never attempt to associate with an AP that has WEP on
  - ✓ An AP or STA with WEP on must discard all received data frames that have the WEP bit off in the MAC header
  - ✓ The DUT must support a single 128-bit WEP key (length includes the 24-bit IV Key)
  - ✓ The DUT must support ASCII or hex key inputs for WEP keys
  - ✓ 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 (WEP is not active, allowing any STA to authenticate by default)
  - ✓ WEP keys must not be not case-sensitive

STA Ad Hoc Interoperability WEP Test

1) Configure the STAs and DUT STA with SSID "ETESTINGLABS".
2) Activate WEP encryption on the STAs and DUT STA.
3) Set the shared keys to 128-bit encryption.
4) Enter the following share key for authentication for ASCII (13 Characters): 1234567890ABC.
   a.
5) Enter the following share key for authentication for hex (26 Characters): 12345678901234567890ABCDEF.
6) From each STA, use a network sniffing tool to capture packet activity.
7) Set the STAs and DUT STA to use the first shared key (ASCII or hex) and verify authentication.
8) Issue ping requests from each STA using the required packet sizes, and confirm ICMP activity and validation.
   (Example: ping 10.0.0.1 –L 32) PASS: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)),

Ping From STA to STA: (ASCII or hex)	D-Link STA	Netgear STA	Zcom STA	Sony STA	DUT STA
D-Link STA ping with 32 bytes	N/a				
D-Link STA ping with 101 bytes	N/a				
D-Link STA ping with 961 bytes	N/a				
D-Link STA ping with 962 bytes	N/a				

Ping From STA to STA: (ASCII or hex)	D-Link STA	Netgear STA	Zcom STA	Sony STA	DUT STA
D-Link STA ping with 1468 bytes	N/a				
Ping from STA to STA: (ASCII or hex)	**D-Link STA**	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
Netgear STA ping with 32 bytes		N/a			
Netgear STA ping with 101 bytes		N/a			
Netgear STA ping with 961 bytes		N/a			
Netgear STA ping with 962 bytes		N/a			
Netgear STA ping with 1468 bytes		N/a			
Ping From STA to STA Key: (ASCII or hex)	**D-Link STA**	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
Zcom STA ping with 32 bytes			N/a		
Zcom STA ping with 101 bytes			N/a		
Zcom STA ping with 961 bytes			N/a		
Zcom STA ping with 962 bytes			N/a		
Zcom STA ping with 1468 bytes			N/a		
Ping From STA to STA Key: (ASCII or hex)	**D-Link STA**	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
Sony STA ping with 32 bytes				N/a	
Sony STA ping with 101 bytes				N/a	
Sony STA ping with 961 bytes				N/a	
Sony STA ping with 962 bytes				N/a	
Sony STA ping with 1468 bytes				N/a	
Ping From STA to STA Key: (ASCII or hex)	**D-Link STA**	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
DUT STA ping with 32 bytes					N/a
DUT STA ping with 101 bytes					N/a
DUT STA ping with 961 bytes					N/a
DUT STA ping with 962 bytes					N/a
DUT STA ping with 1468 bytes					N/a

Table 9: Ad Hoc WEP Test checklist

STA Ad Hoc WEP Mode Negative Test

We will also create mismatched WEP configurations between the STAs and the DUT STA and use these to verify that association and data transfers will not be possible between the STAs and the DUT STA.

STA Ad Hoc WEP Interoperability Negative Test

1) Configure the STAs with the same SSID ("ETESTINGLABS") but with a different WEP key (ASCII or hex) on each station.
2) Enter the following share keys for authentication if ASCII (13 Characters):
    a. STA 1: 1234567890ABC
    b. STA 2: DEFGHIJKLMNOP
    c. STA 3: QRSTUXWXYZ123
    d. STA 4: abcdefghijklm
    e. DTU STA: X234567890ABC
3) Enter the following share keys for authentication if HEX (26 Characters):
    a. STA 1: 12345678901234567890ABCDEF
    b. STA 2: 21345678901234567890ABCDEF
    c. STA 3: 32145678901234567890ABCDEF
    a. STA 4: 43215678901234567890ABCDEF
    b. DUT STA: FFFF5678901234567890ABCDEF
4) From the Controller, use a network sniffing tool to capture packet activity.
5) Issue ping requests from each STA to confirm no association.
    (Example: ping 10.0.0.1) PASS: 4- Request timed out.
    Ping statistics for 10.0.0.1 Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)

Ping From STA to STA	D-Link STA	Netgear STA	Zcom STA	Sony STA	DUT STA
D-Link STA (ASCII or hex)	N/a				
Netgear STA (ASCII or hex)		N/a			
Zcom STA (ASCII or hex)			N/a		
Sony STA (ASCII or hex)				N/a	
DUT STA (ASCII or hex)					N/a

Table 10: STA Ad Hoc WEP Negative Interoperability Test checklist

Part 3: STA/AP Infrastructure Tests

STA/AP Infrastructure Interoperability

STA/AP Infrastructure Interoperability involves connecting the STAs through the AP. This section tests this communication between the STAs and the AP. We will send probe requests from the STAs in the test group using the same SSID and monitoring the STAs response, verifying response and case-sensitive recognition.

STA/AP Infrastructure Test Configuration	
SSID	ETESTINGLABS
TCP/IP Addressing	Static
Channel	1 (odd), 4 (even)
Frequency	5.2 GHz
Frame Sizes	32, 101, 961, 962, 1468

Table 11: AP test configuration

Specific Requirements
As well as satisfying previous Ad Hoc testing requirements, the DUT will need the following capabilities and features to pass this test:

- Service Set Identifier (SSID) Element
  - ✓ AP must be able to respond to broadcast SSID probe requests

DUT STA/AP Infrastructure Test

1) Configure the STAs and AP for Infrastructure mode.
2) Set the SSID for all participating APs to the appropriate SSID.
3) Configure the AP for Open System authentication.
   a. Open System: the default authentication service that simply announces the desire to associate with another station or access point. The STA can authenticate with any other STA or AP using open system authentication if the receiving STA designates open system authentication.
   b. Shared Key: the optional authentication that involves a more rigorous exchange of frames, ensuring that the requesting STA is authentic. For the STA to use shared key authentication, it must implement WEP.
4) From the source STA probe for an AP that is using OSA, then use a network sniffing tool to capture packet activity.
5) Issue ping requests from another DUT to the first STA using the required packet sizes, and confirm ICMP activity and validation.
   (Example: ping 10.0.0.1 –L 32) PASS: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

DUT STA to AP Infrastructure Test

Ping from DUT STA to AP AP SSID= ETESTINGLABS	D-Link AP	Netgear AP	Zcom AP	Sony AP	DUT AP
DUT STA ping with 32 bytes					
DUT STA ping with 101 bytes					
DUT STA ping with 961 bytes					
DUT STA ping with 962 bytes					
DUT STA ping with 1468 bytes					
Ping from DUT STA to AP AP SSID = ABCDEFG1234567890	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
DUT STA ping with 32 bytes					

DUT STA ping with 101 bytes					
DUT STA ping with 961 bytes					
DUT STA ping with 962 bytes					
DUT STA ping with 1468 bytes					
Ping from DUT STA to AP AP SSID = 1234567890qrstuvwxyz	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
DUT STA ping with 32 bytes					
DUT STA ping with 101 bytes					
DUT STA ping with 961 bytes					
DUT STA ping with 962 bytes					
DUT STA ping with 1468 bytes					
Ping from DUT STA to AP AP SSID = 1234567890ABCDEF	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
DUT STA ping with 32 bytes					
DUT STA ping with 101 bytes					
DUT STA ping with 961 bytes					
DUT STA ping with 962 bytes					
DUT STA ping with 1468 bytes					

STA to AP Infrastructure Test

Ping from DLINK STA to AP AP SSID = ETESTINGLABS	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
D-Link STA ping with 32 bytes					
D-Link STA ping with 101 bytes					
D-Link STA ping with 961 bytes					
D-Link STA ping with 962 bytes					
D-Link STA ping with 1468 bytes					
Ping from Netgear STA to AP AP SSID = ABCDEFG1234567890	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
Netgear STA ping with 32 bytes					
Netgear STA ping with 101 bytes					
Netgear STA ping with 961 bytes					
Netgear STA ping with 962 bytes					
Netgear STA ping with 1468 bytes					
Ping from Zcom STA to AP AP SSID = 1234567890qrstuvwxyz	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
Zcom STA ping with 32 bytes					
Zcom STA ping with 101 bytes					
Zcom STA ping with 961 bytes					
Zcom STA ping with 962 bytes					
Zcom STA ping with 1468 bytes					
Ping from Sony to AP AP SSID = 1234567890ABCDEF	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
Sony STA ping with 32 bytes					
Sony STA ping with 101 bytes					
Sony STA ping with 961 bytes					
Sony STA ping with 962 bytes					
Sony STA ping with 1468 bytes					

STA to STA via AP Infrastructure

Ping from the STA listed below to each STA using DLINK AP SSID= ETESTINGLABS	D-Link STA	Netgear STA	Zcom STA	Sony STA	DUT STA
D-Link STA	N/A				
Netgear STA		N/A			
Zcom STA			N/A		
Sony STA				N/A	
DUT STA					N/A
Ping from the STA listed below to each STA using Netgear AP SSID= ETESTINGLABS	**D-Link STA**	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
D-Link STA	N/A				
Netgear STA		N/A			
Zcom STA			N/A		
Sony STA				N/A	
DUT STA					N/A
Ping from the STA listed below to each STA using Zcom AP SSID= ETESTINGLABS	**D-Link STA**	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
D-Link STA	N/A				
Netgear STA		N/A			
Zcom STA			N/A		
Sony STA				N/A	
DUT STA					N/A
Ping from the STA listed below to each STA using Sony AP SSID= ETESTINGLABS	**D-Link STA**	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
D-Link STA	N/A				
Netgear STA		N/A			
Zcom STA			N/A		
Sony STA				N/A	
DUT STA					N/A
Ping from the STA listed below to each STA using DUT AP SSID= ETESTINGLABS	**D-Link STA**	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
D-Link STA	N/A				
Netgear STA		N/A			
Zcom STA			N/A		
Sony STA				N/A	
DUT STA					N/A

Table 12: STA Interoperability Test checklist

STA/AP Infrastructure Negative Interoperability

We will also create mismatched configurations between the STAs their respective APs. We will use this to verify that association and data transfers will not be possible between STAs and APs.

Configuration mismatches between the STAs and AP will include:

- Incorrect SSIDs, including case-sensitive errors
- Incorrect WEP keys, where case sensitivity is not an issue
- One device using WEP while the other is not

Specific Requirements

The DUT will need to have satisfied previous Infrastructure Interoperability testing requirements.

DUT STA/AP Infrastructure Negative Interoperability Test

1) Configure each device in the test group for Infrastructure mode and use the following SSIDs:

DUT STA	D-Link AP	Netgear AP	Zcom AP	Sony AP	DUT AP
DUTSTA	DLINKAP	NETGEARAP	ZCOMAP	SONYAP	DUTAP

Table 13: Infrastructure mode configuration

2) From each source STA, use a network sniffing tool to capture packet activity.
3) Issue ping requests from the DUT STA to confirm ICMP activity and no association with each AP. (Example: ping 10.0.0.1) PASS: 4- Request timed out. Ping statistics for 10.0.0.1. Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)

Ping from DUT STA to each AP	D-Link AP	Netgear AP	Zcom AP	Sony AP	DUT AP
DUT STA ping with 32 bytes					

Table 14: DUT STA/AP Infrastructure Negative Interoperability Test checklist

STA/AP Infrastructure Negative Test

1) Configure each device in the test group for Infrastructure mode and use the following SSIDs:

D-Link AP	Netgear AP	Zcom AP	Sony AP	DUT AP
DLINK	NETGEAR	ZCOM	SONY	DUTAP
D-Link STA	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
DLINKSTA	NETGEARSTA	ZCOMSTA	SONYSTA	DUTSTA

Table 15: Infrastructure mode configuration

2) From each source STA, use a network sniffing tool to capture packet activity.
3) Issue ping requests from the STA to DUT STA and confirm ICMP activity and no association with each AP.
(Example: ping 10.0.0.1) PASS: 4- Request timed out. Ping statistics for 10.0.0.1. Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)

Ping from each STA to each AP	D-Link AP	Netgear AP	Zcom AP	Sony AP	DUT AP
D-Link STA ping with 32 bytes					
Netgear STA ping with 32 bytes					
Zcom STA ping with 32 bytes					

Sony STA ping with 32 bytes					

Table 16: STA/AP Infrastructure Negative Test checklist

STA to STA via AP Infrastructure Negative Test

1) Configure each device in the test group for Infrastructure mode and use the following SSIDs:

D-Link AP	Netgear AP	Zcom AP	Sony AP	DUT AP
DLINK	NETGEAR	ZCOM	SONY	DUTAP
D-Link STA	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
DLINKSTA	NETGEARSTA	ZCOMSTA	SONYSTA	DUTSTA

Table 17: Infrastructure mode configuration

2) From each source STA, use a network sniffing tool to capture packet activity.
3) Issue ping requests from each STA to confirm ICMP activity and no association with AP. (Example: ping 10.0.0.1) PASS: 4- Request timed out. Ping statistics for 10.0.0.1. Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)

Ping from STA to STA using DLINK AP	D-Link STA	Netgear STA	Zcom STA	Sony STA	DUT STA
D-Link STA ping	N/a				
Netgear STA ping		N/a			
Zcom STA ping			N/a		
Sony STA ping				N/a	
DUT STA ping					N/a
Ping from STA to STA using Netgear AP	**D-Link STA**	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
D-Link STA ping	N/a				
Netgear STA ping		N/a			
Zcom STA ping			N/a		
Sony STA ping				N/a	
DUT STA ping					N/a
Ping from STA to STA using Zcom AP	**D-Link STA**	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
D-Link STA ping	N/a				
Netgear STA ping		N/a			
Zcom STA ping			N/a		
Sony STA ping				N/a	
DUT STA ping					N/a
Ping from STA to STA using Sony AP	**D-Link STA**	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
D-Link STA ping	N/a				
Netgear STA ping		N/a			
Zcom STA ping			N/a		
Sony STA ping				N/a	
DUT STA ping					N/a
Ping from STA to STA using DUT AP	**D-Link STA**	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
D-Link STA ping	N/a				

Netgear STA ping		N/a			
Zcom STA ping			N/a		
Sony STA ping				N/a	
DUT STA ping					N/a

Table 18: STA Infrastructure Negative Interoperability Test checklist

STA/AP Infrastructure PSP Mode Interoperability

This only applies to Infrastructure mode. We will perform the same interoperability tests we described above, using Power Management on each STA that has that function. The STA will generate further packet activity when, in a powered-down state, it reports its Power Management status to the AP, queuing packets for delivery when the STA is awake. Test will include both low power and high power states.

We will compare the constantly awake status in the previous section to the status in power management mode. We will monitor sleep intervals and association activity using the Atheros LinkMon.exe tool. However, if the LinkMon tool does not support a vendor's device, the vendor must provide a means to monitor each of these activities to help facilitate execution of these tests.

Specific Requirements

As well as satisfying previous Infrastructure Interoperability testing requirements, the DUT will need the following capabilities and features to pass this test:

- Traffic Indicator Map (TIM) Element
  TIM alerts stations in sleep state to stay awake long enough to receive their data frames.
  - ✓ AP must be capable of generating correct TIM for PSP (Power Saving Polls) nodes
  - ✓ Stations in PSP must interpret TIM correctly

- Power Save Mode
  - ✓ STA power save mode is not mandatory
  - ✓ AP support of power save stations is mandatory

STA/AP Infrastructure PSP Mode Test

1) Confirm the following settings on the AP:
   a. Enable support for Power Save functionality for the STAs.
   b. Configure both AP and STAs with SSID "ETESTINGLABS".
   c. Set BSS for OSA.
   d. Activate Power Save mode on the STAs, and verify packet STA is in power saving mode.
2) From the Controller, use a network sniffing tool to capture network ICMP activity between the AP and the STAs.
3) From a participating STA, send continuous ICMP ping requests to the DUT STA.
   a. To execute this test, use the following command; ping ip_address –t
   b. To stop the continuous ping command, use Control-C
   c. For the STA, verify Wakeup.
   d. For the STA, verify sleep after receipt of the ping

From a participating STA, ping the DUT STA	D-Link AP	Netgear AP	Zcom AP	Sony AP	DUT AP
D-Link STA ping with 32 bytes					
D-Link STA ping with 101 bytes					
D-Link STA ping with 961 bytes					
D-Link STA ping with 962 bytes					
D-Link STA ping with 1468 bytes					
From a participating STA, ping the DUT STA	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
Netgear STA ping with 32 bytes					
Netgear STA ping with 101 bytes					
Netgear STA ping with 961 bytes					
Netgear STA ping with 962 bytes					
Netgear STA ping with 1468 bytes					

From a participating STA, ping the DUT STA	D-Link AP	Netgear AP	Zcom AP	Sony AP	DUT AP
Zcom STA ping with 32 bytes					
Zcom STA ping with 101 bytes					
Zcom STA ping with 961 bytes					
Zcom STA ping with 962 bytes					
Zcom STA ping with 1468 bytes					
From a participating STA, ping the DUT STA	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
Sony STA ping with 32 bytes					
Sony STA ping with 101 bytes					
Sony STA ping with 961 bytes					
Sony STA ping with 962 bytes					
Sony STA ping with 1468 bytes					
From a participating STA, ping the DUT STA	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
DUT STA ping with 32 bytes					
DUT STA ping with 101 bytes					
DUT STA ping with 961 bytes					
DUT STA ping with 962 bytes					
DUT STA ping with 1468 bytes					

Table 19: STA/AP Infrastructure PSP Mode Test checklist

STA/AP Infrastructure WEP Mode Interoperability

Perform the same Infrastructure Interoperability test as described above between the DUT and the STAs that have the ability to communicate on this level.

We will also test the DUT's ability to configure Wired Equivalent Privacy (WEP). WEP is an optional function ratified by the IEEE that offers frame transmission privacy similar to a wired network. It generates a secret shared algorithmic encryption key that both source and destination stations can use to alter frame bits to avoid disclosure to eavesdroppers. WEP thus denies access to anyone who does not have an assigned key.

To increase security on wireless systems by wired standards, IEEE 802.11 allows for encryption in its communication by using an optional privacy algorithm. The test will report the ability of each vendor's solution to include this standard and measure the performance levels when the standard is in use.

Specific Requirements

As well as satisfying previous Infrastructure Interoperability testing requirements, the DUT will need the following capabilities and features to pass this test:

- Wired Equivalent Privacy
  - ✓ The STA with WEP off must never attempt to associate with an AP that has WEP on.
  - ✓ An AP or STA with WEP on must discard all received data frames that have the WEP bit off in the MAC header.
  - ✓ The DUT must support a single 128-bit WEP key (length includes the 24-bit IV Key).
    - ASCII or hex
  - ✓ 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 (WEP is not active, allowing any STA to authenticate by default).
  - ✓ Case sensitivity must be non-specific

STA/AP Interoperability WEP Test

1) Configure the STAs and APs with SSID "ETESTINGLABS".
2) Activate WEP encryption on the STAs and APs.
3) Set the shared keys to 128-bit encryption.
4) Enter the following share key for authentication for ASCII (13 Characters): 1234567890ABC.
5) Enter the following share key for authentication for hex (26 Characters): 12345678901234567890ABCDEF.
6) From each source STA, use a network sniffing tool to capture packet activity.
7) Set the STAs and AP to use the first shared key (ASCII or hex) and verify authentication.
8) Issue ping requests from each STA using the following packet sizes and confirm ICMP activity and validation:
   (Example: ping 10.0.0.1 –L 32) PASS: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)),

Ping from STA to AP Key: (ASCII or hex)	D-Link AP	Netgear AP	Zcom AP	Sony AP	DUT AP
D-Link STA ping with 32 bytes					
D-Link STA ping with 101 bytes					
D-Link STA ping with 961 bytes					
D-Link STA ping with 962 bytes					
D-Link STA ping with 1468 bytes					
Ping from STA to AP Key: (ASCII or hex)	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
Netgear STA ping with 32 bytes					
Netgear STA ping with 101 bytes					

Ping from STA to AP Key: (ASCII or hex)	D-Link AP	Netgear AP	Zcom AP	Sony AP	DUT AP
Netgear STA ping with 961 bytes					
Netgear STA ping with 962 bytes					
Netgear STA ping with 1468 bytes					
Ping From STA to AP Key: (ASCII or hex)	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
Zcom STA ping with 32 bytes					
Zcom STA ping with 101 bytes					
Zcom STA ping with 961 bytes					
Zcom STA ping with 962 bytes					
Zcom STA ping with 1468 bytes					
Ping from STA to AP Key: (ASCII or hex)	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
Sony STA ping with 32 bytes					
Sony STA ping with 101 bytes					
Sony STA ping with 961 bytes					
Sony STA ping with 962 bytes					
Sony STA ping with 1468 bytes					
Ping from STA to AP Key: (ASCII or hex)	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
DUT STA ping with 32 bytes					
DUT STA ping with 101 bytes					
DUT STA ping with 961 bytes					
DUT STA ping with 962 bytes					
DUT STA ping with 1468 bytes					

Table 20: STA/AP Infrastructure WEP Mode Test checklist

STA/AP Infrastructure WEP Mode Negative Interoperability Test

We will also create mismatched WEP configurations between the STAs and APs. We will use this test to verify that association and data transfers will not be possible between the STAs and APs.

Configuration mismatches between the STAs and APs will include:

- Incorrect WEP keys
- One device using WEP while the other is not

Specific Requirements

The DUT will need to have satisfied previous Infrastructure Interoperability testing requirements.

STA/AP WEP Interoperability Negative Test (Incorrect WEP Keys)

1) Configure the STAs with the same SSID ("ETESTINGLABS") but with a different WEP key (ASCII or hex) on each station.
2) Enter the following share keys for authentication if ASCII (13 Characters).
    a. STA 1: 1234567890ABC
    b. STA 2: DEFGHIJKLMNOP
    c. STA 3: QRSTUXWXYZ123
    d. STA 4: abcdefghijklm
    e. DUT STA: X234567890ABC
    f. ALL AP's: 1234567890CCC
3) Enter the following share keys for authentication if hex (26 Characters).
    a. STA 1: 12345678901234567890ABCDEF
    b. STA 2: 21345678901234567890ABCDEF
    c. STA 3: 32145678901234567890ABCDEF
    d. STA 4: 43215678901234567890ABCDEF
    e. DUT STA: FFFF5678901234567890ABCDEF
    f. ALL AP's: 123456789012345678 90FFFFFF
4) From the source STA, use a network sniffing tool to capture packet activity.
5) Issue ping requests from each STA to confirm no association.
    (Example: ping 10.0.0.1) PASS: 4- Request timed out.
    Ping statistics for 10.0.0.1 Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)

Note: The STA should not associate with an AP without the correct WEP key. This response constitutes a pass for this negative test.

Ping from STA to AP	D-Link AP	Netgear AP	Zcom AP	Sony AP	DUT AP
D-Link STA (ASCII or hex)					
Netgear STA (ASCII or hex)					
Zcom STA (ASCII or hex)					
Sony STA (ASCII or hex)					
DUT STA (ASCII or hex)					

Table 21: STA/AP WEP Interoperability Negative Test (Incorrect WEP Keys) checklist

STA/AP WEP Interoperability Negative Test (AP WEP, STA no WEP key)

1) Configure the STAs with the same SSID ("ETESTINGLABS") but where the AP has WEP keys and each STA does not (ASCII or hex).
2) Enter the following share key for authentication if ASCII (13 Characters):
    a. All APs: 1234567890CCC
3) Enter the following share key for authentication if hex (26 Characters):
    a. All APs: 123456789012345678 90FFFFFF
4) From the source STA, use a network sniffing tool to capture packet activity.

5) Issue ping requests from each STA to confirm no association.
(Example: ping 10.0.0.1) PASS: 4- Request timed out.
Ping statistics for 10.0.0.1 Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)

Note: The STA should not associate with an AP without the correct WEP key. This response constitutes a pass for this negative test.

Ping From STA to AP	D-Link AP	Netgear AP	Zcom AP	Sony AP	DUT AP
D-Link STA (ASCII or hex)					
Netgear STA (ASCII or hex)					
Zcom STA (ASCII or hex)					
Sony STA (ASCII or hex)					
DUT STA (ASCII or hex)					

Table 22: STA/AP Infrastructure WEP Negative Test (AP WEP, STA no WEP key) checklist

STA/AP Infrastructure Wired and Wireless Test

Testing will monitor and evaluate the authentication and packet transfer between a station in the signal control area and the PDC/Controller. We will monitor the activity on the source STA and on the network-sniffing tool on the controlling server.

Specific Requirements

The DUT will need to have satisfied previous Infrastructure Interoperability testing requirements.

STA/AP Infrastructure Wired and Wireless Test

1) Configure the STAs for Infrastructure mode.
2) Configure the AP for Open System authentication.
3) From the Controller, use a network sniffing tool to capture packet activity.
4) Issue ping requests from the Controller to each of the STAs using the required packet sizes, and confirm ICMP activity and validation.
   (Example: ping 10.0.0.1 –L 32) PASS: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)

From the Controller, Ping STA via AP	D-Link AP	Netgear AP	Zcom AP	Sony AP	DUT AP
Ping from Controller to Dlink STA with 32 bytes					
Ping from Controller to Dlink STA with 101 bytes					
Ping from Controller to Dlink STA with 961 bytes					
Ping from Controller to Dlink STA with 962 bytes					
Ping from Controller to Dlink STA with 1468 bytes					
From the Controller, Ping STA via AP	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
Ping from Controller to Netgear STA with 32 bytes					
Ping from Controller to Netgear STA with 101 bytes					
Ping from Controller to Netgear STA with 961 bytes					
Ping from Controller to Netgear STA with 962 bytes					
Ping from Controller to Netgear STA with 1468 bytes					
From the Controller, Ping STA via AP	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
Ping from Controller to Zcom STA with 32 bytes					
Ping from Controller to Zcom STA with 101 bytes					
Ping from Controller to Zcom STA with 961 bytes					
Ping from Controller to Zcom STA with 962 bytes					
Ping from Controller to Zcom STA with 1468 bytes					
From the Controller, Ping STA via AP	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
Ping from Controller to Sony STA with 32 bytes					
Ping from Controller to Sony STA with 101 bytes					
Ping from Controller to Sony STA with 961 bytes					
Ping from Controller to Sony STA with 962 bytes					
Ping from Controller to Sony STA with 1468 bytes					
From the Controller, Ping STA via AP	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
Ping from Controller to DUT STA with 32 bytes					
Ping from Controller to DUT STA with 101 bytes					
Ping from Controller to DUT STA with 961 bytes					
Ping from Controller to DUT STA with 962 bytes					

Ping from Controller to DUT STA with 1468 bytes					

Table 23: STA Infrastructure Wired and Wireless Interoperability Test checklist

STA/AP Infrastructure Wired and Wireless PSP Mode Test

Perform the same interoperability tests described above using Power Management on each STA if the function is available.

We will compare the STA's constantly awake status in the previous section to the same status in power management mode. We will monitor sleep intervals and association activity using the Atheros LinkMon.exe tool. However, if the LinkMon tool does not support a vendor's device, the vendor must provide a means to monitor each of these activities to help facilitate execution of these tests.

Specific Requirements
The DUT STA and AP will need to have satisfied previous Infrastructure Interoperability testing requirements.

STA Infrastructure Wired and Wireless PSP Mode Test

1) Confirm the following features on the AP:
    a. Support for Power Save functionality for the STAs.
    b. Configure both AP and STAs with SSID "ETESTINGLABS".
    c. Set BSS for OSA.
    d. Activate Power Save mode on the STAs, verify packet STA is in power saving mode.
2) From the Controller, use a network sniffing tool to capture network ICMP activity between the AP and the STAs.
3) From the Controller, send continuous ICMP ping requests to the DUT STA:
    e. To execute this test, use the following command; ping ip_address –t
    a. To stop the continuous ping command, use Control-C
    b. For the STA, verify Wakeup.
    c. For the STA, verify sleep after receipt of the ping.

From the Controller, Ping STA via AP	D-Link AP	Netgear AP	Zcom AP	Sony AP	DUT AP
Ping from Controller to Dlink STA ping with 32 bytes					
Ping from Controller to DLink STA with 101 bytes					
Ping from Controller to Dlink STA with 961 bytes					
Ping from Controller to Dlink STA with 962 bytes					
Ping from Controller to Dlink STA with 1468 bytes					
From the Controller, Ping STA via AP	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
Ping from Controller to Netgear STA with 32 bytes					
Ping from Controller to Netgear STA with 101 bytes					
Ping from Controller to Netgear STA with 961 bytes					
Ping from Controller to Netgear STA with 962 bytes					
Ping from Controller to Netgear STA with 1468 bytes					
From the Controller, Ping STA via AP	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
Ping from Controller to Zcom STA with 32 bytes					
Ping from Controller to Zcom STA with 101 bytes					
Ping from Controller to Zcom STA with 961 bytes					
Ping from Controller to Zcom STA with 962 bytes					
Ping from Controller to Zcom STA with 1468 bytes					
From the Controller, Ping STA via AP	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
Ping from Controller to Sony STA with 32 bytes					

Ping from Controller to Sony STA ping with 101 bytes					
Ping from Controller to Sony STA ping with 961 bytes					
Ping from Controller to Sony STA ping with 962 bytes					
Ping from Controller to Sony STA ping with 1468 bytes					
From the Controller, Ping STA via AP	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
Ping from Controller to DUT STA with 32 bytes					
Ping from Controller to DUT STA with 101 bytes					
Ping from Controller to DUTSTA with 961 bytes					
Ping from Controller to DUT STA with 962 bytes					
Ping from Controller to DUT STA with 1468 bytes					

Table 24: STA/AP Infrastructure Wired and Wireless PSP Mode Test checklist

STA/AP Infrastructure Wired and Wireless WEP Mode Test

Perform the same interoperability test as described above between the controlling server and the STAs in the test group that have the ability to communicate on this level.

Specific Requirements

The DUT STA and AP will need to have satisfied previous Infrastructure Interoperability testing requirements.

STA/AP Infrastructure Wired and Wireless WEP Mode Test

1) Configure both APs and STAs with SSID "ETESTINGLABS".
2) Activate WEP encryption on both the APs and the STAs.
3) Set the shared keys to 128-bit encryption.
4) Enter the following share keys for authentication for ASCII (13 Characters): 1234567890ABC.
    a.
5) Enter the following share keys for authentication for hex (26 Characters): 12345678901234567890ABCDEF.
    a.
6) Set the STAs to use the first shared key and verify authentication.

7) From the Controller, use a network sniffing tool to capture packet activity.
8) Issue ping requests from the Controller to each of the STAs using the required packet sizes, and confirm ICMP activity and validation.
   (Example: ping 10.0.0.1 –L 32) PASS: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)

From the Controller, Ping STA via AP WEP KEY: (ASCII or hex)	D-Link AP	Netgear AP	Zcom AP	Sony AP	DUT AP
Ping from Controller to Dlink STA with 32 bytes					
Ping from Controller to Dlink STA with 101 bytes					
Ping from Controller to Dlink STA with 961 bytes					
Ping from Controller to Dlink STA with 962 bytes					
Ping from Controller to Dlink STA with 1468 bytes					
From the Controller, Ping STA via AP WEP KEY: (ASCII or hex)	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
Ping from Controller to Netgear STA with 32 bytes					
Ping from Controller to Netgear STA with 101 bytes					
Ping from Controller to Netgear STA with 961 bytes					
Ping from Controller to Netgear STA with 962 bytes					
Ping from Controller to Netgear STA with 1468 bytes					
From the Controller, Ping STA via AP WEP KEY: (ASCII or hex)	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
Ping from Controller to Zcom STA with 32 bytes					
Ping from Controller to Zcom STA with 101 bytes					
Ping from Controller to Zcom STA with 961 bytes					
Ping from Controller to Zcom STA with 962 bytes					
Ping from Controller to Zcom STA with 1468 bytes					
From the Controller, Ping STA via AP WEP KEY: (ASCII or hex)	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
Ping from Controller to Sony STA with 32 bytes					
Ping from Controller to Sony STA with 101 bytes					
Ping from Controller to Sony STA with 961 bytes					

Ping from Controller to Sony STA with 962 bytes					
Ping from Controller to Sony STA with 1468 bytes					
From the Controller, Ping each STA via AP WEP KEY: (ASCII or hex)	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
Ping from Controller to DUT STA with 32 bytes					
Ping from Controller to DUT STA with 101 bytes					
Ping from Controller to DUT STA with 961 bytes					
Ping from Controller to DUT STA with 962 bytes					
Ping from Controller to DUT STA with 1468 bytes					

Table 25: STA/AP Infrastructure Wired and Wireless WEP Mode Test checklist

Part 4: Extended Interoperability Tests

STA/AP Infrastructure Interoperability with Data Encapsulation Test

Using the INQUIRYL script in Chariot, we will test the STAs' and APs' ability to encapsulate packets and to send and receive them accurately through the DS. The servers and STAs will use the IPX protocol including Ethernet, 802.2, 802.3 and Ethernet II.

Specific Requirements
As well as satisfying previous Infrastructure Interoperability testing requirements, the DUT will need the following capabilities and features to pass this test:

- Data Payload
  - ✓ STAs and APs must support encrypted and unencrypted data payloads
  - ✓ Data payload size must be limited to Ethernet payload size
  - ✓ Payload formats must conform to 802.1H, which specifies the use of RFC1O42
  - ✓ Ethertypes 80F3 and 8137 must be in the table
  - ✓ General rule: If the Ethertype table contains a specific Ethertype, then the APs and STAs must use 802.1H bridge tunnel encapsulation format; otherwise RFC1042 applies

Note for two auto-negotiated devices: If a DUT does not support a fixed data rate, then attempt to limit its throughput by adjusting its complementary device under test. If neither user interface permits adjustments to limit the data rate, then use at least one auto-negotiated link speed between the STA and the AP and confirm that both successfully handle the packet exchange for this test. In addition, for a device that supports fixed link speeds, test and report the optional rates of 6, 12, 24, and 54 Mbit per second.

STA Infrastructure Interoperability with Data Encapsulation Test

1) Configure both AP and DUT STA with SSID "ETESTINGLABS".
2) Disable WEP and Power Save modes on the STAs.
3) Configure Controller and STAs with IPX protocol. Use "00000001" as the Internal Network Address and use the 802.2 protocol.
4) For IPX Chariot test, insert a valid IPX network address in the following format:
   00000001:xxxxxxxxxxxx
   where 00000001 is the internal network address, and xxxxxxxxxxxx is the machine's MAC address.
5) Change the value of the variable "transactions_per_record" to 200 in the "INQUIRYL.SCR" script.
6) Note: Remove the TCP protocol from the stack on the Controller system running the Chariot console. Use Network Monitor to verify that the Controller system sends the packets via IPX protocol frame.
7) Configure the AP for any successfully negotiated data rate.
8) From the Controller, use Chariot to run the script, "INQUIRYL.SCR". Designate the STAs as Endpoint 1 and the Controller as Endpoint 2.
9) At the end of the test, verify that all bytes were sent and received between the Endpoints without error.
10) Swap the Endpoints (Source and Destination addresses) in Chariot and repeat Steps 6 and 7.
11) Configure Controller and STAs to use the 802.3 protocol.
12) Repeat Steps 6 and 7.
13) Swap the Endpoints (Source and Destination addresses) in Chariot.
14) Repeat Steps 6 and 7.
15) Configure Controller and STAs to use the Ethernet II protocol.
16) Repeat Steps 6 and 7.
17) Swap the Endpoints (Source and Destination addresses) in Chariot.

From the Controller, test DUT STA via each AP IPX/802.2	D-Link AP	Netgear AP	Zcom AP	Sony AP	DUT AP
INQUIRYL.SCR (Controller End pt1 STA End pt2)					
INQUIRYL.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT STA via each AP IPX/802.3	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
INQUIRYL.SCR (Controller End pt1 STA End pt2)					
INQUIRYL.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT STA via each AP IPX/Ethernet II	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
INQUIRYL.SCR (Controller End pt1 STA End pt2)					
INQUIRYL.SCR (Controller End pt2 STA End pt1)					

Table 26: STA Infrastructure Interoperability with Data Encapsulation Test checklist

AP Infrastructure Interoperability with Data Encapsulation Test

1) Configure both AP and DUT STA with SSID “ETESTINGLABS”.
2) Disable WEP and Power Save modes on the STAs.
3) Configure Controller and STAs with IPX protocol. Use “00000001” as the Internal Network Address and use the 802.2 protocol.
   Note: Remove the TCP protocol from the stack on the Controller system running the Chariot console. Use Network Monitor to verify that the Controller system sends the packets via IPX protocol frame.
4) Configure the AP for any negotiated data rate.
5) From the Controller, use Chariot to run the script, “INQUIRY.SCR”. Designate the STAs as Endpoint 1 and the Controller as Endpoint 2.
6) At the end of the test, verify that all bytes were sent and received between the Endpoints without error.
7) Swap the Endpoints (Source and Destination addresses) in Chariot and repeat Steps 6 and 7.
8) Configure Controller and STAs to use the 802.3 protocol.
9) Repeat Steps 6 and 7.
10) Swap the Endpoints (Source and Destination addresses) in Chariot.
11) Repeat Steps 6 and 7.
12) Configure Controller and STAs to use the Ethernet II protocol.
13) Repeat Steps 6 and 7.
14) Swap the Endpoints (Source and Destination addresses) in Chariot.
15) Repeat Steps 6 and 7.

From the Controller, test DUT AP with each STA IPX/802.2	D-Link STA	Netgear STA	Zcom STA	Sony STA	DUT STA
INQUIRYL.SCR (Controller End pt1 STA End pt2)					
INQUIRYL.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT AP with each STA IPX/802.3	**D-Link STA**	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
INQUIRYL.SCR (Controller End pt1 STA End pt2)					
INQUIRYL.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT AP with each STA IPX/Ethernet II	**D-Link STA**	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
INQUIRYL.SCR (Controller End pt1 STA End pt2)					
INQUIRYL.SCR (Controller End pt2 STA End pt1)					

Table 27: AP Interoperability with Data Encapsulation checklist

STA/AP Infrastructure Interoperability with Broadcast/Multicast Reception Test

Using the REALAUD script available with Chariot, we will test the STAs' and APs' ability to receive and send broadcast and multicast packets. The originating source will use the multicast address 225.0.0.1.

For the purposes of this test, we will select "Validate Data upon Receipt" on the Chariot Run Options tab of the Run Options dialog and select UDP as the underlying protocol.

Specific Requirements
The DUT (AP or STA) will need to have satisfied previous Infrastructure Interoperability testing requirements.

Note for two auto-negotiated devices: If a DUT does not support a fixed data rate, then attempt to limit its throughput by adjusting its complementary device under test. If neither user interface permits adjustments to limit the data rate, then use at least one auto-negotiated link speed between the STA and the AP and confirm that both successfully handle the packet exchange for this test. In addition, for a device that supports fixed link speeds, test and report the optional rates of 6, 12, 24, and 54 Mbit per second.

DUT STA Infrastructure Interoperability with Broadcast/Multicast Reception Test

1) Configure both AP and STAs with SSID "ETESTINGLABS".
2) Configure the AP for Data Rate 6 Mbps.
    a. See note above for auto-negotiated devices.
3) Disable WEP and Power Save modes on the STAs.
4) From the Controller, use a network sniffing tool to capture packet activity. Configure Chariot to use the Multicast address 225.0.0.1 and include all of the STAs within the Multicast group. Use any available open port for the "Multicast port" setting. Each STA'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.
5) Select "Validate Data upon Receipt" on the Chariot Run Options tab of the Run Options dialog and select UDP as the underlying protocol.
6) Select REALAUD.scr as the Chariot script.
7) Use Chariot to run the "REALAUD.SCR" script. Designate the STAs as Endpoint 2 and the Controller as Endpoint 1.
8) At the end of the test, verify that all bytes were sent and received between the Endpoints without error.
9) Configure the AP for Data Rate 12 Mbps.
    a. See note above for auto-negotiated devices.
10) Repeat Steps 6 and 7.
11) Configure the AP for Data Rate 24 Mbps.
    a. See note above for auto-negotiated devices.
12) Repeat Steps 6 and 7.
13) Configure the AP for Data Rate 54 Mbps.
    a. See note above for auto-negotiated devices.
14) Repeat Steps 6 and 7.

From the Controller, test DUT STA with each AP Data Rate= 6 Mbps	D-Link AP	Netgear AP	Zcom AP	Sony AP	DUT AP
REALAUD.SCR (Controller End pt1 STA End pt2)					
REALAUD.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT STA with each AP Data Rate= 12 Mbps	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
REALAUD.SCR (Controller End pt1 STA End pt2)					
REALAUD.SCR (Controller End pt2 STA End pt1)					

From the Controller, test DUT STA with each AP Data Rate= 24 Mbps	D-Link AP	Netgear AP	Zcom AP	Sony AP	DUT AP
REALAUD.SCR (Controller End pt1 STA End pt2)					
REALAUD.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT STA with each AP Data Rate= 54 Mbps	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
REALAUD.SCR (Controller End pt1 STA End pt2)					
REALAUD.SCR (Controller End pt2 STA End pt1)					

Table 28: STA Infrastructure Interoperability Broadcast/Multicast Reception Test checklist

DUT AP Infrastructure Interoperability with Broadcast/Multicast Reception Test

1) Configure both AP and STAs with SSID "ETESTINGLABS".
2) Configure the AP for Data Rate 6 Mbps.
    a. See note above for auto-negotiated devices.
3) Disable WEP and Power Save modes on the STAs.
4) From the Controller, use a network sniffing tool to capture packet activity.
5) Configure Chariot to use the Multicast address 225.0.0.1 and include all of the STAs within the Multicast group. 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.
6) "Validate Data upon Receipt" is selected on the Chariot Run Options tab of the Run Options dialog and select UDP as the underlying protocol.
7) Select the REALAUD.scr as the Chariot script.
8) Use Chariot to run the script, "REALAUD.SCR". Designate STAs as Endpoint 2 and the Controller as Endpoint 1.
9) At the end of the test, verify that all bytes were sent and received between the Endpoints without error.
10) Configure the AP for Data Rate 12 Mbps.
    a. See note above for auto-negotiated devices.
11) Repeat Steps 6 and 7.
12) Configure the AP for Data Rate 24 Mbps.
    a. See note above for auto-negotiated devices.
13) Repeat Steps 6 and 7.
14) Configure the AP for Data Rate 54 Mbps.
    a. See note above for auto-negotiated devices.
15) Repeat Steps 6 and 7.

From the Controller, test DUT AP with each STA Data Rate= 6 Mbps	D-Link STA	Netgear STA	Zcom STA	Sony STA	DUT STA
REALAUD.SCR (Controller End pt1 STA End pt2)					
REALAUD.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT AP with each STA Data Rate= 12 Mbps	**D-Link STA**	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
REALAUD.SCR (Controller End pt1 STA End pt2)					
REALAUD.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT AP with each STA Data Rate= 24 Mbps	**D-Link STA**	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
REALAUD.SCR (Controller End pt1 STA End pt2)					
REALAUD.SCR (Controller End pt2 STA End pt1)					

From the Controller, test DUT AP with each STA Data Rate= 54 Mbps	D-Link STA	Netgear STA	Zcom STA	Sony STA	DUT STA
REALAUD.SCR (Controller End pt1 STA End pt2)					
REALAUD.SCR (Controller End pt2 STA End pt1)					

Table 29: AP Infrastructure Interoperability Broadcast/Multicast Reception Test checklist

STA/AP Infrastructure Interoperability with Broadcast/Multicast Reception Test with PSP enabled

We will test the STAs' and APs' ability to receive and send broadcast and multicast packets, using Power Management on each STA that has that function. We will monitor sleep intervals and association activity using the Atheros LinkMon.exe tool. However, if the LinkMon tool does not support a vendor's device, the vendor must provide a means to monitor each of these activities to help facilitate execution of these tests.

Specific Requirements
The DUT (AP or STA) will need to have satisfied previous Infrastructure Interoperability testing requirements.

Note for two auto-negotiated devices: If a DUT does not support a fixed data rate, then attempt to limit its throughput by adjusting its complementary device under test. If neither user interface permits adjustments to limit the data rate, then use at least one auto-negotiated link speed between the STA and the AP and confirm that both successfully handle the packet exchange for this test. In addition, for a device that supports fixed link speeds, test and report the optional rates of 6, 12, 24, and 54 Mbit per second.

DUT STA Infrastructure Interoperability with Broadcast/Multicast Reception Test with PSP

1) Configure both AP and STAs with SSID "ETESTINGLABS".
2) Configure the AP for Data Rate 6 Mbps.
    a. See note above for auto-negotiated devices.
3) Disable WEP and enable Power Save modes on the STAs.
4) From the Controller, use a network sniffing tool to capture packet activity.
5) Configure Chariot to use the Multicast address 225.0.0.1 and include all of the STAs within the Multicast group. Use any available open port for the "Multicast port" setting. 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.
6) Select "Validate Data upon Receipt" on the Chariot Run Options tab of the Run Options dialog and select UDP as the underlying protocol.
7) Select the REALAUD.scr as the Chariot script.
8) Use Chariot to run the script, "REALAUD.SCR". Designate the STAs as Endpoint 2 and the Controller as Endpoint 1.
9) At the end of the test, verify that all bytes were sent and received between the Endpoints without error.
10) Configure the AP for Data Rate 12 Mbps.
    a. See note above for auto-negotiated devices.
11) Repeat Steps 6 and 7.
12) Configure the AP for Data Rate 24 Mbps.
    a. See note above for auto-negotiated devices.
13) Repeat Steps 6 and 7.
14) Configure the AP for Data Rate 54 Mbps.
    a. See note above for auto-negotiated devices.
15) Repeat Steps 6 and 7.

From the Controller, test DUT STA with each AP Data Rate= 6 Mbps	D-Link AP	Netgear AP	Zcom AP	Sony AP	DUT AP
REALAUD.SCR (Controller End pt1 STA End pt2)					
REALAUD.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT STA with each AP Data Rate= 12 Mbps	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
REALAUD.SCR (Controller End pt1 STA End pt2)					
REALAUD.SCR (Controller End pt2 STA End pt1)					

From the Controller, test DUT STA with each AP Data Rate= 24 Mbps	D-Link AP	Netgear AP	Zcom AP	Sony AP	DUT AP
REALAUD.SCR (Controller End pt1 STA End pt2)					
REALAUD.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT STA with each AP Data Rate= 54 Mbps	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
REALAUD.SCR (Controller End pt1 STA End pt2)					
REALAUD.SCR (Controller End pt2 STA End pt1)					

Table 30: STA Infrastructure Interoperability Broadcast/Multicast Reception Test with PSP checklist

DUT AP Infrastructure Interoperability with Broadcast/Multicast Reception Test with PSP

1) Configure both AP and STAs with SSID "ETESTINGLABS".
2) Configure the AP for Data Rate 6 Mbps.
    a. See note above for auto-negotiated devices.
3) Disable WEP and enable Power Save modes on the STAs.
4) From the Controller, use a network sniffing tool to capture packet activity.
5) Configure Chariot to use the Multicast address 225.0.0.1 and include all of the STAs within the Multicast group. 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.
6) Select "Validate Data upon Receipt" on the Chariot Run Options tab of the Run Options dialog and select UDP as the underlying protocol.
7) Select the REALAUD.scr as the Chariot script.
8) Use Chariot to run the script, "REALAUD.SCR". Designate STAs as Endpoint 2 and the Controller as Endpoint 1.
9) At the end of the test, verify that all bytes were sent and received between the Endpoints without error.
10) Configure the AP for Data Rate 12 Mbps.
    a. See note above for auto-negotiated devices.
11) Repeat Steps 6 and 7.
12) Configure the AP for Data Rate 24 Mbps.
    a. See note above for auto-negotiated devices.
13) Repeat Steps 6 and 7.
14) Configure the AP for Data Rate 54 Mbps.
    a. See note above for auto-negotiated devices.
15) Repeat Steps 6 and 7.

From the Controller, test DUT AP with each STA Data Rate= 6 Mbps	D-Link STA	Netgear STA	Zcom STA	Sony STA	DUT STA
REALAUD.SCR (Controller End pt1 STA End pt2)					
REALAUD.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT AP with each STA Data Rate= 12 Mbps	**D-Link STA**	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
REALAUD.SCR (Controller End pt1 STA End pt2)					
REALAUD.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT AP with each STA Data Rate= 24 Mbps	**D-Link STA**	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
REALAUD.SCR (Controller End pt1 STA End pt2)					
REALAUD.SCR (Controller End pt2 STA End pt1)					

From the Controller, test DUT AP with each STA Data Rate= 54 Mbps	D-Link STA	Netgear STA	Zcom STA	Sony STA	DUT STA
REALAUD.SCR (Controller End pt1 STA End pt2)					
REALAUD.SCR (Controller End pt2 STA End pt1)					

Table 31: AP Infrastructure Interoperability Broadcast/Multicast Reception Test with PSP checklist

STA/AP Infrastructure Interoperability with Broadcast/Multicast Reception Test with WEP enabled

We will test the STAs' and APs' ability to receive and send broadcast and multicast packets with Wired Equivalency Privacy (WEP) enabled.

Specific Requirements
The DUT (AP or STA) will need to have satisfied previous Infrastructure Interoperability testing requirements.

Note for two auto-negotiated devices: If a DUT does not support a fixed data rate, then attempt to limit its throughput by adjusting its complementary device under test. If neither user interface permits adjustments to limit the data rate, then use at least one auto-negotiated link speed between the STA and the AP and confirm that both successfully handle the packet exchange for this test. In addition, for a device that supports fixed link speeds, test and report the optional rates of 6, 12, 24, and 54 Mbit per second.

DUT STA Infrastructure Interoperability with Broadcast/Multicast Reception Test with WEP enabled

1) Configure both AP and STAs with SSID "ETESTINGLABS".
2) Configure the AP for Data Rate 6 Mbps.
    a. See note above for auto-negotiated devices.
3) Enable WEP and disable Power Save modes on the STAs.
    a. Use any (ASCII or HEX) key
4) From the Controller, use a network sniffing tool to capture packet activity.
5) Configure Chariot to use the Multicast address 225.0.0.1 and include all of the STAs within the Multicast group. Use any available open port for the "Multicast port" setting. 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.
6) Select "Validate Data upon Receipt" on the Chariot Run Options tab of the Run Options dialog and select UDP as the underlying protocol.
7) Select the REALAUD.scr as the Chariot script.
8) Use Chariot to run the script, "REALAUD.SCR". Designate the STAs as Endpoint 2 and the Controller as Endpoint 1.
9) At the end of the test, verify that all bytes were sent and received between the Endpoints without error.
10) Configure the AP for Data Rate 12 Mbps.
    a. See note above for auto-negotiated devices.
11) Repeat Steps 6 and 7.
12) Configure the AP for Data Rate 24 Mbps.
    a. See note above for auto-negotiated devices.
13) Repeat Steps 6 and 7.
14) Configure the AP for Data Rate 54 Mbps.
    a. See note above for auto-negotiated devices.
15) Repeat Steps 6 and 7.

From the Controller, test DUT STA with each AP Data Rate= 6 Mbps	D-Link AP	Netgear AP	Zcom AP	Sony AP	DUT AP
REALAUD.SCR (Controller End pt1 STA End pt2)					
REALAUD.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT STA with each AP Data Rate= 12 Mbps	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
REALAUD.SCR (Controller End pt1 STA End pt2)					
REALAUD.SCR (Controller End pt2 STA End pt1)					

From the Controller, test DUT STA with each AP Data Rate= 24 Mbps	D-Link AP	Netgear AP	Zcom AP	Sony AP	DUT AP
REALAUD.SCR (Controller End pt1 STA End pt2)					
REALAUD.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT STA with each AP Data Rate= 54 Mbps	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
REALAUD.SCR (Controller End pt1 STA End pt2)					
REALAUD.SCR (Controller End pt2 STA End pt1)					

Table 32: STA Infrastructure Interoperability Broadcast/Multicast Reception Test with WEP checklist

DUT AP Infrastructure Interoperability with Broadcast/Multicast Reception Test with WEP enabled

1) Configure both AP and STAs with SSID "ETESTINGLABS".
2) Configure the AP for Data Rate 6 Mbps.
    a. See note above for auto-negotiated devices.
3) Enable WEP and disable Power Save modes on the STAs.
    a. Use any (ASCII or HEX) key
4) From the Controller, use a network sniffing tool to capture packet activity.
5) Configure Chariot to use the Multicast address 225.0.0.1 and include all of the STAs within the Multicast group. 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.
6) Select "Validate Data upon Receipt" on the Chariot Run Options tab of the Run Options dialog and select UDP as the underlying protocol.
7) Select the REALAUD.scr as the Chariot script.
8) Use Chariot to run the script, "REALAUD.SCR". Designate STAs as Endpoint 2 and the Controller as Endpoint 1.
9) At the end of the test, verify that all bytes were sent and received between the Endpoints without error.
10) Configure the AP for Data Rate 12 Mbps.
    a. See note above for auto-negotiated devices.
11) Repeat Steps 6 and 7.
12) Configure the AP for Data Rate 24 Mbps.
    a. See note above for auto-negotiated devices.
13) Repeat Steps 6 and 7.
14) Configure the AP for Data Rate 54 Mbps.
    a. See note above for auto-negotiated devices.
15) Repeat Steps 6 and 7.

From the Controller, test DUT AP with each STA Data Rate= 6 Mbps	D-Link STA	Netgear STA	Zcom STA	Sony STA	DUT STA
REALAUD.SCR (Controller End pt1 STA End pt2)					
REALAUD.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT AP with each STA Data Rate= 12 Mbps	**D-Link STA**	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
REALAUD.SCR (Controller End pt1 STA End pt2)					
REALAUD.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT AP with each STA Data Rate= 24 Mbps	**D-Link STA**	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
REALAUD.SCR (Controller End pt1 STA End pt2)					
REALAUD.SCR (Controller End pt2 STA End pt1)					

From the Controller, test DUT AP with each STA Data Rate= 54 Mbps	D-Link STA	Netgear STA	Zcom STA	Sony STA	DUT STA
REALAUD.SCR (Controller End pt1 STA End pt2)					
REALAUD.SCR (Controller End pt2 STA End pt1)					

Table 33: AP Infrastructure Interoperability Broadcast/Multicast Reception Test checklist with WEP

Part 5: Bandwidth and Data Rate Test

STA/AP Data Rate Test

In this test, we will push bandwidth from the STA to the controlling server using Chariot. We will use a custom script to evaluate the wireless solution's ability to meet the standard 802.11a data rates of 6, 12, 24, and 54 Mbps as well as to measure the higher data rates each device can attain. A network-sniffing tool on the controller will provide further verification of data rates and packet activity.

Specific Requirements
As well as satisfying previous Infrastructure Interoperability testing requirements, the DUT (Client AP or STA) will need the following capabilities and features to pass this test:

- Data Rates
  - ✓ APs and STAs must be capable of operating at each data rate (6, 12, 24, and 54 Mbps)
  - ✓ APs and STAs must be capable of operating within a BSS with all data rates (6, 12, 24, and 54 Mbps) considered as standard rates as defined in 802.11a

Note for two auto-negotiated devices: If a DUT does not support a fixed data rate, then attempt to limit its throughput by adjusting its complementary device under test. If neither user interface permits adjustments to limit the data rate, then use at least one auto-negotiated link speed between the STA and the AP and confirm that both successfully handle the packet exchange for this test. In addition, for a device that supports fixed link speeds, test and report the optional rates of 6, 12, 24, and 54 Mbit per second.

DUT STA Data Rate Test

1) Configure both AP and STAs with SSID "ETESTINGLABS".
2) Configure the AP or STA for 6 Mbps Data Rate
   a. See note above for auto-negotiated devices..
3) Disable WEP and Power Save modes on the STAs.
4) From the Controller, use Chariot to run the script, "FILESNDL.SCR". Designate the STA as Endpoint 1 and the Controller as Endpoint 2.
5) At the end of the test, verify that all bytes were sent and received between the Endpoints without error.
6) Configure for Data Rate 12 Mbps.
   a. See note above for auto-negotiated devices.
7) Repeat Steps 4 and 5.
8) Configure for Data Rate 24 Mbps.
   a. See note above for auto-negotiated devices.
9) Repeat Steps 4 and 5.
10) Configure for Data Rate 54 Mbps.
    a. See note above for auto-negotiated devices.
11) Repeat Steps 4 and 5.

From the Controller, test DUT STA via each AP Data Rate= 6 Mbps	D-Link AP	Netgear AP	Zcom AP	Sony AP	DUT AP
FILESNDL.SCR (Controller End pt1 STA End pt2)					
FILESNDL.SCR (Controller End pt2 STA End pt1)					
INQUIRYL.SCR (Controller End pt1 STA End pt2)					
INQUIRYL.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT STA via each AP Data Rate= 12 Mbps	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
FILESNDL.SCR (Controller End pt1 STA End pt2)					
FILESNDL.SCR (Controller End pt2 STA End pt1)					

INQUIRYL.SCR (Controller End pt1 STA End pt2)					
INQUIRYL.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT STA via each AP Data Rate= 24 Mbps	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
FILESNDL.SCR (Controller End pt1 STA End pt2)					
FILESNDL.SCR (Controller End pt2 STA End pt1)					
INQUIRYL.SCR (Controller End pt1 STA End pt2)					
INQUIRYL.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT STA via each AP Data Rate= 54 Mbps	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
FILESNDL.SCR (Controller End pt1 STA End pt2)					
FILESNDL.SCR (Controller End pt2 STA End pt1)					
INQUIRYL.SCR (Controller End pt1 STA End pt2)					
INQUIRYL.SCR (Controller End pt2 STA End pt1)					

Table 34: STA Data Rate Test checklist

DUT AP Data Rate Test

1) Configure both AP and STAs with SSID “ETESTINGLABS”.
2) Configure the AP or STA for a 6 Mbps Data Rate.
    a. See note above for auto-negotiated devices.
3) Disable WEP and Power Save modes on the STAs.
4) From the Controller, use Chariot to run the script, “FILESNDL.SCR”. Designate the STA as Endpoint 1 and the Controller as Endpoint 2.
5) At the end of the test, verify that all bytes were sent and received between the Endpoints without error.
6) Configure for Data Rate 12 Mbps.
    a. See note above for auto-negotiated devices.
7) Repeat Steps 4 and 5.
8) Configure for Data Rate 24 Mbps.
    a. See note above for auto-negotiated devices.
9) Repeat Steps 4 and 5.
10) Configure for Data Rate 54 Mbps.
    a. See note above for auto-negotiated devices.
11) Repeat Steps 4 and 5.

From the Controller, test DUT AP via each STA Data Rate= 6 Mbps	**D-Link STA**	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
FILESNDL.SCR (Controller End pt1 STA End pt2)					
FILESNDL.SCR (Controller End pt2 STA End pt1)					
INQUIRYL.SCR (Controller End pt1 STA End pt2)					
INQUIRYL.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT AP via each STA Data Rate= 12 Mbps	**D-Link STA**	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
FILESNDL.SCR (Controller End pt1 STA End pt2)					
FILESNDL.SCR (Controller End pt2 STA End pt1)					
INQUIRYL.SCR (Controller End pt1 STA End pt2)					
INQUIRYL.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT AP via each STA Data Rate= 24 Mbps	**D-Link STA**	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**

FILESNDL.SCR (Controller End pt1 STA End pt2)					
FILESNDL.SCR (Controller End pt2 STA End pt1)					
INQUIRYL.SCR (Controller End pt1 STA End pt2)					
INQUIRYL.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT AP via each STA Data Rate= 54 Mbps	**D-Link STA**	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
FILESNDL.SCR (Controller End pt1 STA End pt2)					
FILESNDL.SCR (Controller End pt2 STA End pt1)					
INQUIRYL.SCR (Controller End pt1 STA End pt2)					
INQUIRYL.SCR (Controller End pt2 STA End pt1)					

Table 35: AP Data Rate Test checklist

STA/AP PSP Mode Data Rate Test

Perform the same interoperability tests as described above using Power Management on each STA if the function is available. We will configure the STA into power-saving mode before Chariot initiates each subsequent client mix. We will monitor sleep intervals and association activity using the Atheros LinkMon.exe tool. However, if the LinkMon tool does not support a vendor's device, the vendor must provide a means to monitor each of these activities to help facilitate execution of these tests.

Specific Requirements
The DUT will need to have satisfied previous Infrastructure Interoperability testing requirements.

Note: If a DUT does not support fixed data rate, then attempt to limit its throughput by adjusting its complementary device under test. If neither user interface permits adjustments to limit the data rate, then induce a signal strength change by using physical distance to achieve the desired data rate.

DUT STA PSP Mode Data Rate Test

1) Configure both AP and STAs with SSID "ETESTINGLABS".
2) Configure the AP or STA for each Data Rate. Disable WEP and enable Power Save modes on the STAs.
3) From the Controller, use Chariot to run the script "FILESNDL.SCR". Designate the STA as Endpoint 1 with the Controller as Endpoint 2.
4) At the end of the test, verify that all bytes were sent and received between the Endpoints without error.

From the Controller, test DUT STA via each AP Data Rate= 6 Mbps	D-Link AP	Netgear AP	Zcom AP	Sony AP	DUT AP
FILESNDL.SCR (Controller End pt1 STA End pt2)					
FILESNDL.SCR (Controller End pt2 STA End pt1)					
INQUIRYL.SCR (Controller End pt1 STA End pt2)					
INQUIRYL.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT STA via each AP Data Rate= 12 Mbps	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
FILESNDL.SCR (Controller End pt1 STA End pt2)					
FILESNDL.SCR (Controller End pt2 STA End pt1)					
INQUIRYL.SCR (Controller End pt1 STA End pt2)					
INQUIRYL.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT STA via each AP Data Rate= 24 Mbps	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
FILESNDL.SCR (Controller End pt1 STA End pt2)					
FILESNDL.SCR (Controller End pt2 STA End pt1)					
INQUIRYL.SCR (Controller End pt1 STA End pt2)					
INQUIRYL.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT STA via each AP Data Rate= 54 Mbps	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
FILESNDL.SCR (Controller End pt1 STA End pt2)					
FILESNDL.SCR (Controller End pt2 STA End pt1)					
INQUIRYL.SCR (Controller End pt1 STA End pt2)					
INQUIRYL.SCR (Controller End pt2 STA End pt1)					

Table 36: STA Data Rate PSP Mode Test checklist

DUT AP PSP Mode Data Rate Test

1) Configure both AP and STAs with SSID "ETESTINGLABS".

2) Configure the AP or STA for each Data Rate. Disable WEP and enable Power Save modes on the STAs.
3) From the Controller, use Chariot to run the script “FILESNDL.SCR”. Designate the STA as Endpoint 1 with the Controller as Endpoint 2.
4) At the end of the test, verify that all bytes were sent and received between the Endpoints without error.

From the Controller, test DUT AP via each STA Data Rate= 6 Mbps	D-Link STA	Netgear STA	Zcom STA	Sony STA	DUT STA
FILESNDL.SCR (Controller End pt1 STA End pt2)					
FILESNDL.SCR (Controller End pt2 STA End pt1)					
INQUIRYL.SCR (Controller End pt1 STA End pt2)					
INQUIRYL.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT AP via each STA Data Rate= 12 Mbps	**D-Link STA**	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
FILESNDL.SCR (Controller End pt1 STA End pt2)					
FILESNDL.SCR (Controller End pt2 STA End pt1)					
INQUIRYL.SCR (Controller End pt1 STA End pt2)					
INQUIRYL.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT AP via each STA Data Rate= 24 Mbps	**D-Link STA**	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
FILESNDL.SCR (Controller End pt1 STA End pt2)					
FILESNDL.SCR (Controller End pt2 STA End pt1)					
INQUIRYL.SCR (Controller End pt1 STA End pt2)					
INQUIRYL.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT AP via each STA Data Rate= 54 Mbps	**D-Link STA**	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
FILESNDL.SCR (Controller End pt1 STA End pt2)					
FILESNDL.SCR (Controller End pt2 STA End pt1)					
INQUIRYL.SCR (Controller End pt1 STA End pt2)					
INQUIRYL.SCR (Controller End pt2 STA End pt1)					

Table 37: AP Data Rate PSP Mode Test checklist

STA/AP WEP Mode Data Rate Test

Perform the same interoperability test as described above between the controlling server and the STAs that have the ability to communicate on this level.

Specific Requirements
The DUT will need to have satisfied previous Infrastructure Interoperability testing requirements.

Note: If a DUT does not support fixed data rate, then attempt to limit its throughput by adjusting its complementary device under test. If neither user interface permits adjustments to limit the data rate, then induce a signal strength change by using physical distance to achieve the desired data rate.

DUT STA WEP Mode Data Rate Test

1) Configure both AP and STAs with SSID "ETESTINGLABS".
2) Configure the AP or STA for each Data Rate.
3) Enable WEP (ASCII or HEX) key and disable Power Save modes on the STAs.
4) From the Controller, use Chariot to run the script, "FILESNDL.SCR". Designate the STA as Endpoint 1 with the Controller as Endpoint 2.
5) At the end of the test, verify that all bytes sent and received between the Endpoints completed without error.

From the Controller, test DUT STA via each AP Data Rate= 6 Mbps	D-Link AP	Netgear AP	Zcom AP	Sony AP	DUT AP
FILESNDL.SCR (Controller End pt1 STA End pt2)					
FILESNDL.SCR (Controller End pt2 STA End pt1)					
INQUIRYL.SCR (Controller End pt1 STA End pt2)					
INQUIRYL.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT STA via each AP Data Rate= 12 Mbps	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
FILESNDL.SCR (Controller End pt1 STA End pt2)					
FILESNDL.SCR (Controller End pt2 STA End pt1)					
INQUIRYL.SCR (Controller End pt1 STA End pt2)					
INQUIRYL.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT STA via each AP Data Rate= 24 Mbps	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
FILESNDL.SCR (Controller End pt1 STA End pt2)					
FILESNDL.SCR (Controller End pt2 STA End pt1)					
INQUIRYL.SCR (Controller End pt1 STA End pt2)					
INQUIRYL.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT STA via each AP Data Rate= 54 Mbps	**D-Link AP**	**Netgear AP**	**Zcom AP**	**Sony AP**	**DUT AP**
FILESNDL.SCR (Controller End pt1 STA End pt2)					
FILESNDL.SCR (Controller End pt2 STA End pt1)					
INQUIRYL.SCR (Controller End pt1 STA End pt2)					
INQUIRYL.SCR (Controller End pt2 STA End pt1)					

Table 38: STA WEP Mode Data Rate Test checklist

DUT AP WEP Mode Data Rate Test

1) Configure both AP and STAs with SSID "ETESTINGLABS".
2) Configure the AP or STA for each Data Rate.
3) Enable WEP (ASCII or HEX) key and disable Power Save modes on the STAs

4) From the Controller, use Chariot to run the script, “FILESNDL.SCR”. Designate the STA as Endpoint 1 with the Controller as Endpoint 2.
5) At the end of the test, verify that all bytes sent and received between the Endpoints completed without error.

From the Controller, test DUT AP via each STA Data Rate= 6 Mbps	D-Link STA	Netgear STA	Zcom STA	Sony STA	DUT STA
FILESNDL.SCR (Controller End pt1 STA End pt2)					
FILESNDL.SCR (Controller End pt2 STA End pt1)					
INQUIRYL.SCR (Controller End pt1 STA End pt2)					
INQUIRYL.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT AP via each STA Data Rate= 12 Mbps	**D-Link STA**	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
FILESNDL.SCR (Controller End pt1 STA End pt2)					
FILESNDL.SCR (Controller End pt2 STA End pt1)					
INQUIRYL.SCR (Controller End pt1 STA End pt2)					
INQUIRYL.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT AP via each STA Data Rate= 24 Mbps	**D-Link STA**	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
FILESNDL.SCR (Controller End pt1 STA End pt2)					
FILESNDL.SCR (Controller End pt2 STA End pt1)					
INQUIRYL.SCR (Controller End pt1 STA End pt2)					
INQUIRYL.SCR (Controller End pt2 STA End pt1)					
From the Controller, test DUT AP via each STA Data Rate= 54 Mbps	**D-Link STA**	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
FILESNDL.SCR (Controller End pt1 STA End pt2)					
FILESNDL.SCR (Controller End pt2 STA End pt1)					
INQUIRYL.SCR (Controller End pt1 STA End pt2)					
INQUIRYL.SCR (Controller End pt2 STA End pt1)					

Table 39: AP WEP Mode Data Rate Test checklist

Part 6: STA Roaming ESS Transfer Test

STA and AP Interoperability

For this test, we will use an Extended Service Set (ESS) that includes two Basic Service Sets, each with an AP from the contracted client tied back to the Controller through the DS. Figure 2 below provides a graphic illustration of this network testbed. Subsequent tests will utilize the other vendors' APs to ensure compatibility for all devices.

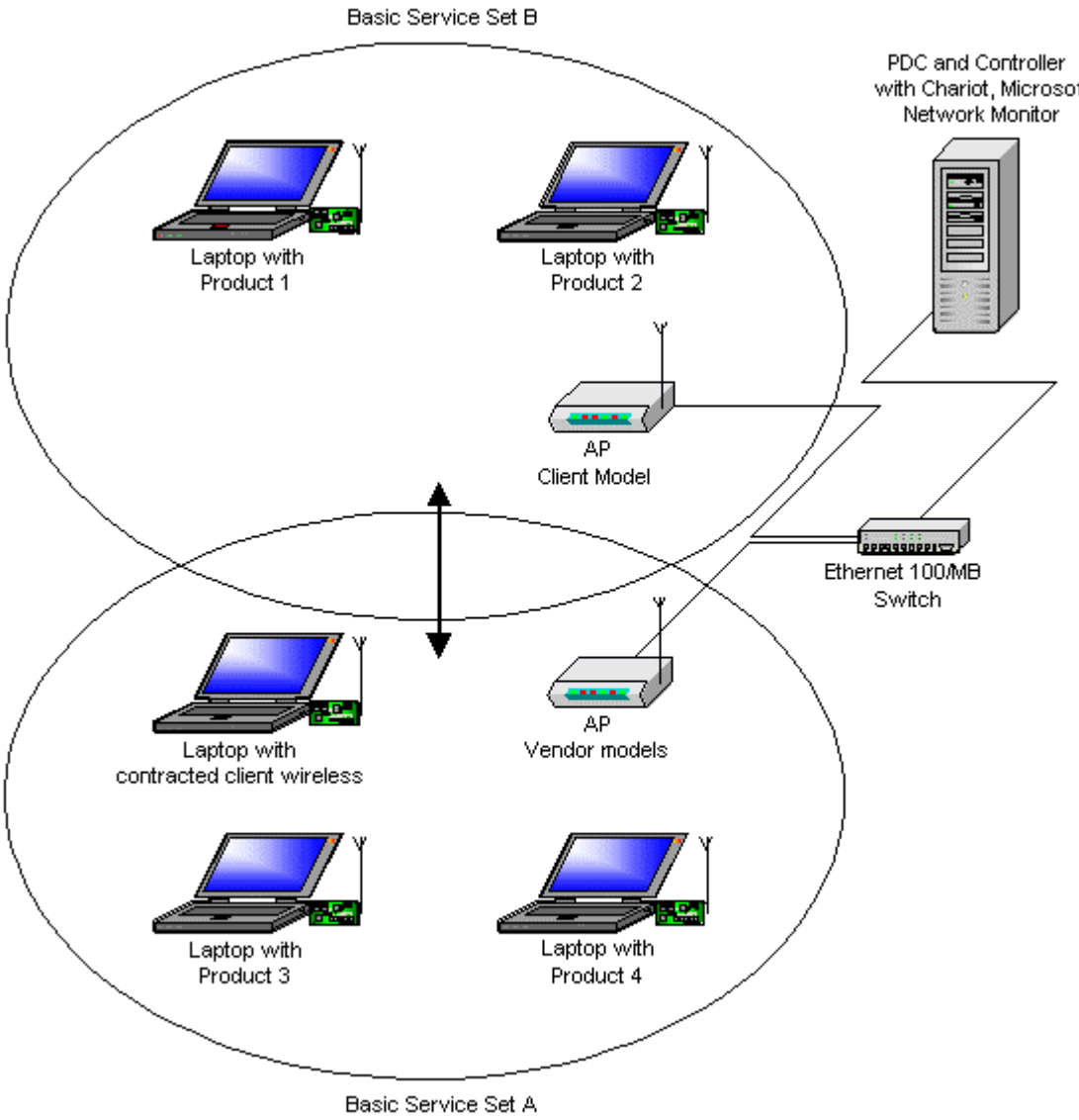

Figure 2: Illustration of the ESS for the STA Roaming Test

We will power up all nodes (STAs and APs) and connect them through the DS, and we will verify connectivity into the network through constant pinging and activity. Once established, we will power down one of the two APs causing that BSS (for this example, BSS A) to fail and migrate the connected STAs to the other BSS (BSS B), forcing reconnection through a separate AP.

We will verify reestablishment of connectivity through network browsing on the STAs, through the network-sniffing tool on the controller, and through ICMP echo requests to evaluate any effect on performance with the new connection. We will monitor sleep intervals and association activity using the Atheros LinkMon.exe tool. However, if the LinkMon tool does not support a vendor's device, the vendor must provide a means to monitor each of these activities to help facilitate execution of these tests.

Specific Requirements
As well as satisfying previous Infrastructure Interoperability testing requirements, the DUT STA will need the following capabilities and features to pass this test:

- AP notification of bridges upon station roaming
  - ✓ When the STA roams from an old AP to a new AP, the new AP must ensure that any bridges between the two APs are properly notified of the station's new location.
  - ✓ The standard does not specify the manner in which the AP must accomplish this notification, only that the packets flow properly to the station's new AP

D-Link AP	Netgear AP	Zcom AP	Sony AP	DUT AP
BSSB	N/a	N/a	N/a	BSSA
D-Link STA	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
BSSB	BSSB	BSSA	BSSA	BSSA

Table 40: STA Roaming ESS Transfer Test 1

D-Link AP	Netgear AP	Zcom AP	Sony AP	DUT AP
N/a	BSSB	N/a	N/a	BSSA
D-Link STA	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
BSSB	BSSB	BSSA	BSSA	BSSA

Table 41: STA Roaming ESS Transfer Test 2

D-Link AP	Netgear AP	Zcom AP	Sony AP	DUT AP
N/a	N/a	BSSB	N/a	BSSA
D-Link STA	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
BSSB	BSSB	BSSA	BSSA	BSSA

Table 42: STA Roaming ESS Transfer Test 3

D-Link AP	Netgear AP	Zcom AP	Sony AP	DUT AP
N/a	N/a	N/a	BSSB	BSSA
D-Link STA	**Netgear STA**	**Zcom STA**	**Sony STA**	**DUT STA**
BSSB	BSSB	BSSA	BSSA	BSSA

Table 43: STA Roaming ESS Transfer Test 4

STA Roaming ESS Transfer Test with Open System authentication

1) Configure both of the APs and all the STAs with Open System authentication. Disable WEP and Power Save modes.
2) Confirm association of all STAs to their respective APs.
3) Once confirmed, power down the DUT AP in BSSA.
4) Confirm all of the STAs associated with DUT AP in BSSA and move their associations to the AP in BSSB.
5) After all STAs migrate to the AP in BSSB, power the DUT AP in BSSA.
6) After the DUT AP in BSSA completes the boot process, power down AP in BSSB.
7) Confirm all of the STAs associated with the AP in BSSB and move their associations back to the DUT AP in BSSA.

AP STATUS	D-Link STA	Netgear STA	Zcom STA	Sony STA	DUT STA
DLINK BSSB ON DUT AP BSSA ON	BSSB (Start)	BSSB (Start)	BSSA (Start)	BSSA (Start)	BSSA (Start)
DLINK BSSB ON DUT AP BSSA OFF	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)
DLINK BSSB OFF DUT AP BSSA ON	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)

Table 44: D-Link AP checklist

AP STATUS	D-Link STA	Netgear STA	Zcom STA	Sony STA	DUT STA
Netgear BSSB ON DUT AP BSSA ON	BSSB (Start)	BSSB (Start)	BSSA (Start)	BSSA (Start)	BSSA (Start)
Netgear BSSB ON DUT AP BSSA OFF	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)
Netgear BSSB OFF DUT AP BSSA ON	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)

Table 45: Netgear AP checklist

AP STATUS	D-Link STA	Netgear STA	Zcom STA	Sony STA	DUT STA
Zcom BSSB ON DUT AP BSSA ON	BSSB (Start)	BSSB (Start)	BSSA (Start)	BSSA (Start)	BSSA (Start)
Zcom BSSB ON DUT AP BSSA OFF	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)
Zcom BSSB OFF DUT AP BSSA ON	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)

Table 46: Zcom AP checklist

AP STATUS	D-Link STA	Netgear STA	Zcom STA	Sony STA	DUT STA
Sony BSSB ON DUT AP BSSA ON	BSSB (Start)	BSSB (Start)	BSSA (Start)	BSSA (Start)	BSSA (Start)
Sony BSSB ON DUT AP BSSA OFF	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)
Sony BSSB OFF DUT AP BSSA ON	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)

Table 47: Sony AP checklist

STA Roaming ESS Transfer Test with Power saving enabled

1) Enable Power Save mode on all of the STAs.
2) Confirm association of all STAs to their respective APs.
3) Once confirmed, power down DUT AP in BSSA.
4) Confirm all of the STAs associated with the DUT AP in BSSA and move their associations to the AP in BSSB.
5) After all STAs migrate to the AP in BSSB, power the DUT AP in BSSA.
6) After the DUT AP in BSSA completes the boot process, power down the AP in BSSB.

7) Confirm all of the STAs associated with the AP in BSSB, and move their associations back to the DUT AP in BSSA.

AP STATUS	D-Link STA	Netgear STA	Zcom STA	Sony STA	DUT STA
DLINK BSSB ON DUT AP BSSA ON	BSSB (Start)	BSSB (Start)	BSSA (Start)	BSSA (Start)	BSSA (Start)
DLINK BSSB ON DUT AP BSSA OFF	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)
DLINK BSSB OFF DUT AP BSSA ON	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)

Table 48: D-Link AP checklist

AP STATUS	D-Link STA	Netgear STA	Zcom STA	Sony STA	DUT STA
Netgear BSSB ON DUT AP BSSA ON	BSSB (Start)	BSSB (Start)	BSSA (Start)	BSSA (Start)	BSSA (Start)
Netgear BSSB ON DUT AP BSSA OFF	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)
Netgear BSSB OFF DUT AP BSSA ON	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)

Table 49: Netgear AP checklist

AP STATUS	D-Link STA	Netgear STA	Zcom STA	Sony STA	DUT STA
Zcom BSSB ON DUT AP BSSA ON	BSSB (Start)	BSSB (Start)	BSSA (Start)	BSSA (Start)	BSSA (Start)
Zcom BSSB ON DUT AP BSSA OFF	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)
Zcom BSSB OFF DUT AP BSSA ON	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)

Table 50: Zcom AP checklist

AP STATUS	D-Link STA	Netgear STA	Zcom STA	Sony STA	DUT STA
Sony BSSB ON DUT AP BSSA ON	BSSB (Start)	BSSB (Start)	BSSA (Start)	BSSA (Start)	BSSA (Start)
Sony BSSB ON DUT AP BSSA OFF	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)
Sony BSSB OFF DUT AP BSSA ON	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)

Table 51: Sony AP checklist

STA Roaming ESS Transfer Test

1) Disable Power Save mode and enable WEP mode on both APs and all the STAs.
2) Use shared key: “ABCDEFABCDEF1234567890ABCD”.
3) Confirm association of all STAs to their respective APs.
4) Once confirmed, power down the DUT AP in BSSA.

5) Confirm all of the STAs associated with the DUT AP in BSSA, and move their associations to the AP BSSB.
6) After all the STAs migrate to the AP in BSSB, power the DUT AP in BSSA.
7) After the DUT AP in BSSA completes the boot process, power down the AP in BSSB.
8) Confirm all of the STAs associated with the AP in BSSB, and move their associations back to the DUT AP in BSSA

AP STATUS	D-Link STA	Netgear STA	Zcom STA	Sony STA	DUT STA
DLINK BSSB ON DUT AP BSSA ON	BSSB (Start)	BSSB (Start)	BSSA (Start)	BSSA (Start)	BSSA (Start)
DLINK BSSB ON DUT AP BSSA OFF	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)
DLINK BSSB OFF DUT AP BSSA ON	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)

Table 52: D-Link AP checklist

AP STATUS	D-Link STA	Netgear STA	Zcom STA	Sony STA	DUT STA
Netgear BSSB ON DUT AP BSSA ON	BSSB (Start)	BSSB (Start)	BSSA (Start)	BSSA (Start)	BSSA (Start)
Netgear BSSB ON DUT AP BSSA OFF	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)
Netgear BSSB OFF DUT AP BSSA ON	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)

Table 53: Netgear AP checklist

AP STATUS	D-Link STA	Netgear STA	Zcom STA	Sony STA	DUT STA
Zcom BSSB ON DUT AP BSSA ON	BSSB (Start)	BSSB (Start)	BSSA (Start)	BSSA (Start)	BSSA (Start)
Zcom BSSB ON DUT AP BSSA OFF	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)
Zcom BSSB OFF DUT AP BSSA ON	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)

Table 54: Zcom AP checklist

AP STATUS	D-Link STA	Netgear STA	Zcom STA	Sony STA	DUT STA
Sony BSSB ON DUT AP BSSA ON	BSSB (Start)	BSSB (Start)	BSSA (Start)	BSSA (Start)	BSSA (Start)
Sony BSSB ON DUT AP BSSA OFF	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)	BSSB (Pass/Fail)
Sony BSSB OFF DUT AP BSSA ON	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)	BSSA (Pass/Fail)

Table 55: Sony AP checklist

Appendix A: Optional Testing

Range Testing

For an additional fee, eTesting Labs will essentially repeat the tests in Parts 4 and 5, setting the STAs at varying distances from the AP to determine the effects on ad hoc and Infrastructure Interoperability bandwidth capabilities. We will use a network-sniffer tool on the controller to verify bandwidth and packet activity.

Specific Requirements
For this phase of testing, we require all DUTs to have met all of the interoperability testing requirements as described in Parts 1-6 of this document.

Throughput Testing

Vendors developing devices under the 802.11a standard created the encoding scheme COFDM to break up the data carrier into 52 subchannels, allowing for multichannel encoding for the wider bandwidth. The vendor can then design a product to encode the data per channel as densely as possible, beyond the 6, 12, 24, and 54 Mbps standard.

For an additional fee, eTesting Labs can not only certify the devices for compliance with IEEE standards, but also fully test the ability of these devices beyond those standards. The throughput test will evaluate the basic throughput capabilities of each device as well as determine the abilities of proprietary enhancements and features built into each device. The objective would be to push as much data and as many file requests as possible between the AP and the STA to verify the top performance levels of those devices beyond the standard data rates.

The user must select Turbo mode manually. The STA or AP is either in 802.11a mode OR in turbo mode. In Turbo each of the data rates doubles, so 6, 12, 24 becomes 12, 24, 48. Some vendors may support up to 108, but 72 is the more likely peak value in turbo mode and therefore, 36 Mbps will be the top data rate in this section of testing. Testing Turbo mode is optional and we will test it only if the vendor implements it.

APs and stations that implement turbo mode must be capable of operating within a BSS with 12, 24, and 48 Mbps considered the standard data rates and 72 as a supported data rate.

For the purposes of this test, we will use custom scripts in Chariot to test total throughput capabilities for sustained periods.

Specific Requirements
For this phase of testing, we require all DUTs to have met all of the interoperability testing requirements as described in Parts 1-6 of this document.

eTesting Labs Inc. (www.etestinglabs.com), a Ziff Davis Media company, leads the industry in Internet and technology testing. In June 2000, ZD Labs changed its name to eTesting Labs to better reflect the breadth of its testing services. Building on Ziff Davis Media's history of leadership in product reviews and benchmark development, eTesting Labs brings independent testing, research, development, and analysis directly to publications, Web sites, vendors, and IT organizations everywhere.

For more information email us at etesting_labs_info@ziffdavis.com or call us toll free at 877-619-9259.

Disclaimer of Warranties; Limitation of Liability:

eTESTING LABS INC. HAS MADE REASONABLE EFFORTS TO ENSURE THE ACCURACY AND VALIDITY OF ITS TESTING, HOWEVER, eTESTING LABS SPECIFICALLY DISCLAIMS ANY WARRANTY, EXPRESSED OR IMPLIED, RELATING TO THE TEST RESULTS AND ANALYSIS, THEIR ACCURACY, COMPLETENESS OR QUALITY, INCLUDING ANY IMPLIED WARRANTY OF FITNESS FOR ANY PARTICULAR PURPOSE. ALL PERSONS OR ENTITIES RELYING ON THE RESULTS OF ANY TESTING DO SO AT THEIR OWN RISK, AND AGREE THAT eTESTING LABS, ITS EMPLOYEES AND ITS SUBCONTRACTORS SHALL HAVE NO LIABILITY WHATSOEVER FROM ANY CLAIM OF LOSS OR DAMAGE ON ACCOUNT OF ANY ALLEGED ERROR OR DEFECT IN ANY TESTING PROCEDURE OR RESULT.

IN NO EVENT SHALL eTESTING LABS BE LIABLE FOR INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH ITS TESTING, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL eTESTING LABS' LIABILITY, INCLUDING FOR DIRECT DAMAGES, EXCEED THE AMOUNTS PAID IN CONNECTION WITH eTESTING LABS' TESTING. CUSTOMER'S SOLE AND EXCLUSIVE REMEDIES ARE AS SET FORTH HEREIN.