WLAN Roaming Performance Testing

IxChariot

Contents

This Test Plan Primer contains a general outline for testing a particular technology. Not all the capabilities of Ixia technology have been exposed in this document. Please feel free to contact us if additional capabilities are required.

Overview

The expansion of single cell WLAN solutions that are deployed in small office/home office (SOHO) and most public HotSpot environments has driven the need to measure the performance of roaming between these WLAN cells. Today, these HotSpot environments include larger multi-cell WLAN networks typically found in enterprise and carrier-class networks. The objective of this test primer is to outline how Ixia's popular IxChariot test application can be used effectively to determine and measure WLAN roaming performance, both in lab environments and in the field as part of open air site surveys and pre-deployment tests.

A Brief Introduction to WLAN Roaming

In multi-cell WLAN networks that comprise a number of Access Points (AP), wireless LAN users or WLAN Stations (STA) can roam freely once they have been authenticated and associated to the wireless network. This means that STAs can pass in and out of range of the various WLAN cells, searching and associating with the strongest RF signal as they move across the multi-cell network. From an 802.11 perspective, WLAN roaming consists of four distinct steps:

- Disassociation

- Search

- Re-association

- Authentication

Measuring the performance of roaming across a multi-cell WLAN network is critical since slow or interrupted network connections can cause enterprise application access to either terminate or become too slow to be usable. This situation is exacerbated for connectionless protocols such as UDP and RTP since the quality of applications, such as VoWLAN and streaming media, decreases substantially with, for example, many consecutive lost datagrams.

Using IxChariot will help the network administrator to determine WLAN roaming performance in the context of popular business applications running over TCP, UDP or RTP, whether or not the underlying network is based on IPv4, IPv6, or both. 802.11 specific measurements, such as the Received Signal Strength Index (RSSI) and Basic Service Set Identifier (BSSID), can be combined effectively with proven IxChariot performance results to create a precise representation of the user experience.

Principal Test Cases for WLAN Roaming

Depending on the System under Test, there are four basic topologies for testing WLAN roaming. Although, open-air testing has been assumed in the test networks below (most network administrators are unlikely to have access to a controlled, cabled RF test bed), IxChariot can also be used effectively as a stateful traffic generator in cabled RF lab test beds. IxChariot can be used in both switched (same subnet) and routed networks. For the sake of simplicity, the topologies below assume that all test devices are part of the same subnet.

Test Objective

The objective of the following four test scenarios can be summarized as follows:

- Measure the Total Roaming Time for a Station, i.e., the time it takes a Station to disassociate, search, re-associate, and authenticate to a new Access Point

- Measure the impact of roaming on the performance of stateful traffic, such as Response Time, Maximum Lost Consecutive Datagrams, and Mean Opinion Score (MOS) estimates

These objectives are applied to each of the following four test topologies and the results are outlined in the second half of this document. The topologies used represent some of the most commonly used test scenarios and DUTs in WLAN industry today.

Topology 1 Setup — Distributed APs Using the Same 802.11 Standard

This topology is based on a number of APs operating on non-overlapping channels within the same 802.11 standard (e.g., 802.11b, 802.11a or 802.11g). Performance Endpoint 1 is located on the wired side of the network. Performance Endpoint 2 runs on a wireless Station setup with a WLAN interface adapter for the same 802.11 standard. IxChariot works with a library of Performance Endpoints to support a wide range of popular operating systems.
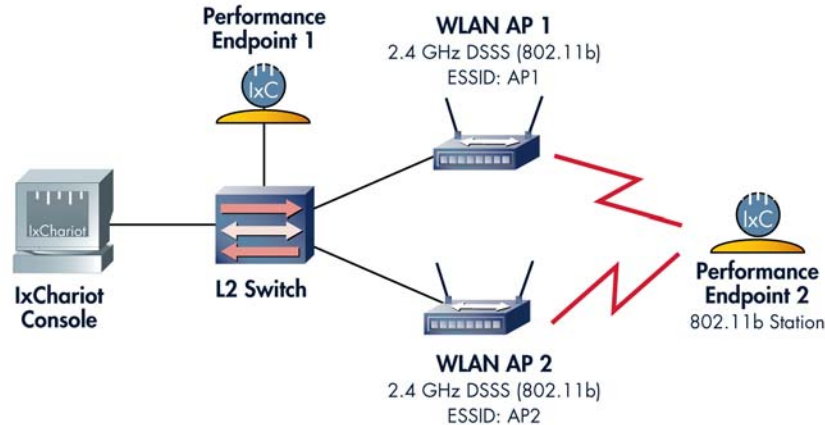

Figure 1. Topology 1: Distributed 802.11b APs and STAs

Topology 2 Setup — Distributed APs Using Different 802.11 Standards

This topology is based on a number of APs operating on different 802.11 standards with a STA capable of switching between them (e.g., AP1 supports 802.11a, AP2 supports 802.11g and the STA contains a Dual-Band A+G Network Interface Adapter). As detailed in Topology 1, Performance Endpoint 1 is located on the wired side of the network and Performance Endpoint 2 runs on a wireless Station on the RF side.
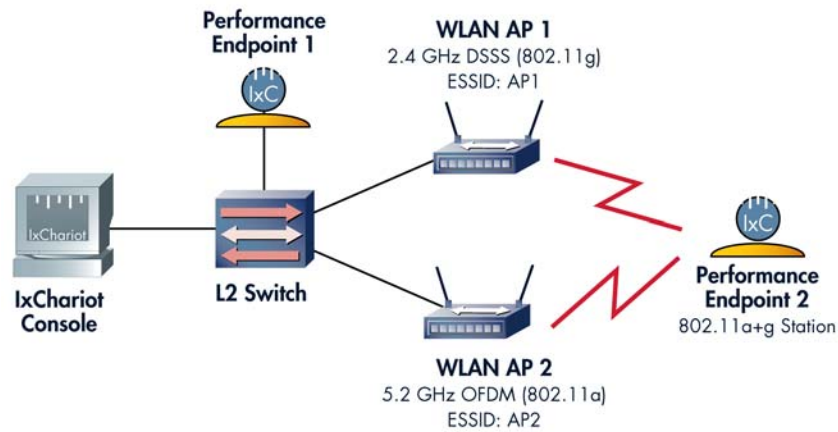

Figure 2. Topology 2: Distributed 802.11 APs and STAs operating at different 802.11 standards

Topology 3 Setup — WLAN Switches Managing a Set of "Thin" APs Operating on Either the Same or Different 802.11 Standard

This topology tests the performance of WLAN switches to support roaming between their APs. In contrast to traditional WLANs that are based on a network of essentially independent memory and processing power intensive APs with complex local firmware, WLAN switches centralize specific functions in a dedicated appliance. In most cases, addressing, management, firmware upgrades, roaming, and security functionality are centralized in the WLAN switch, with "thin" APs functioning as radios and bridges. With regard to roaming, a number of WLAN switch vendors have also developed features such as "pre-emptive roaming," which ensures that Stations roam prior to signal degradation to support continuous operation of critical applications.

The diagram below shows a suggested network topology for testing the roaming performance of WLAN switches. This topology is based on a number of "thin" APs operating on either the same or different 802.11 standard with a STA capable of switching between them. Depending on the system vendor, the "thin" APs are either directly connected to the WLAN switch or aggregated into a PoE and/or 802.1Q switch. Some vendors also unify WLAN, PoE, and standard wired 802.1Q switching functionality into one device.
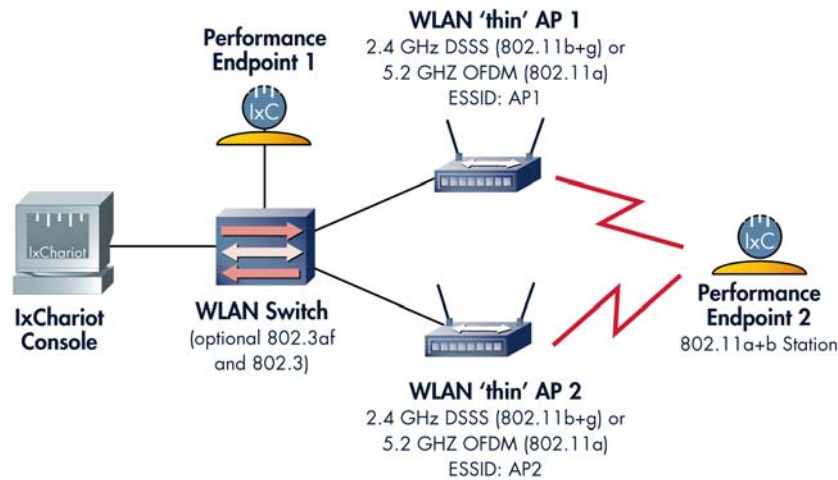

Figure 3. Topology 3: WLAN switch roaming testing

Topology 4 Setup — Virtual AP Tests

The Virtual AP concept is driven by the need to present multiple ESSIDs and VLANs to different user groups. For example, on a single AP, ESSID "Marketing" would be linked to the "Marketing" VLAN; whereas ESSID "Development" would be linked to the "Development" VLAN. Initial implementations of the Virtual AP concept were limited by using a single BSSID on the AP, thus creating the potential for ARP and broadcast issues. However, there are now a number of vendors that offer true Virtual AP implementations with differentiated BSSIDs per ESSIDs on both "thin" and fully-featured APs.

The diagram below shows a suggested network topology for testing the roaming performance of Virtual APs. The test case is based on a single AP and switching the ESSID/VLAN/BSSID on PE2 (RF side).
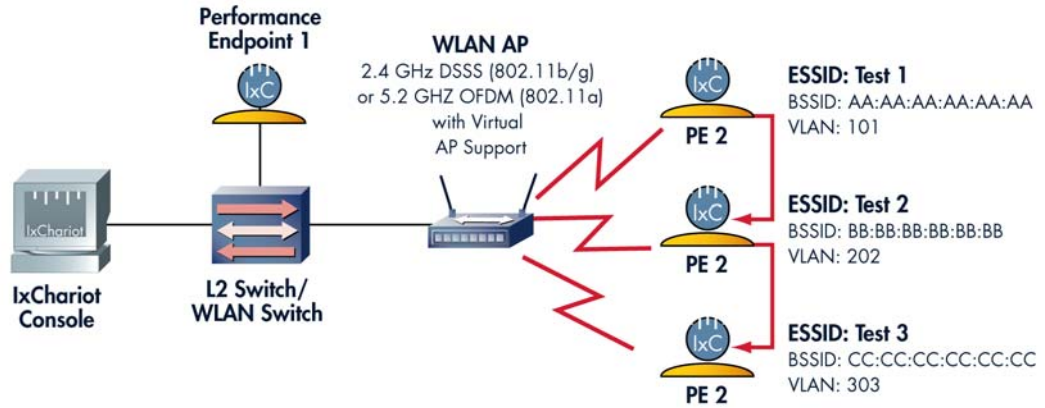

Figure 4. Topology 4: Virtual AP roaming testing

IxChariot Setup and Test Methodology

IxChariot Test and Script Setup

All pre-programmed IxChariot test scripts (e.g., Business, Internet, Benchmark, Streaming, etc.) and protocols can be used without edits in the above test topologies; however, it is recommended to review the options in the script editor to achieve the required granularity of timing records. As shown in the screen below, setting the "transactions_per_record" option to equal the "number_of_timing_records" (in this case, setting both them to 1) will yield a very granular capture of data points. Please note, however, that care must be taken when setting the IxChariot test run options to avoid the creation of too many timing records (i.e., more than 10,000 per test).
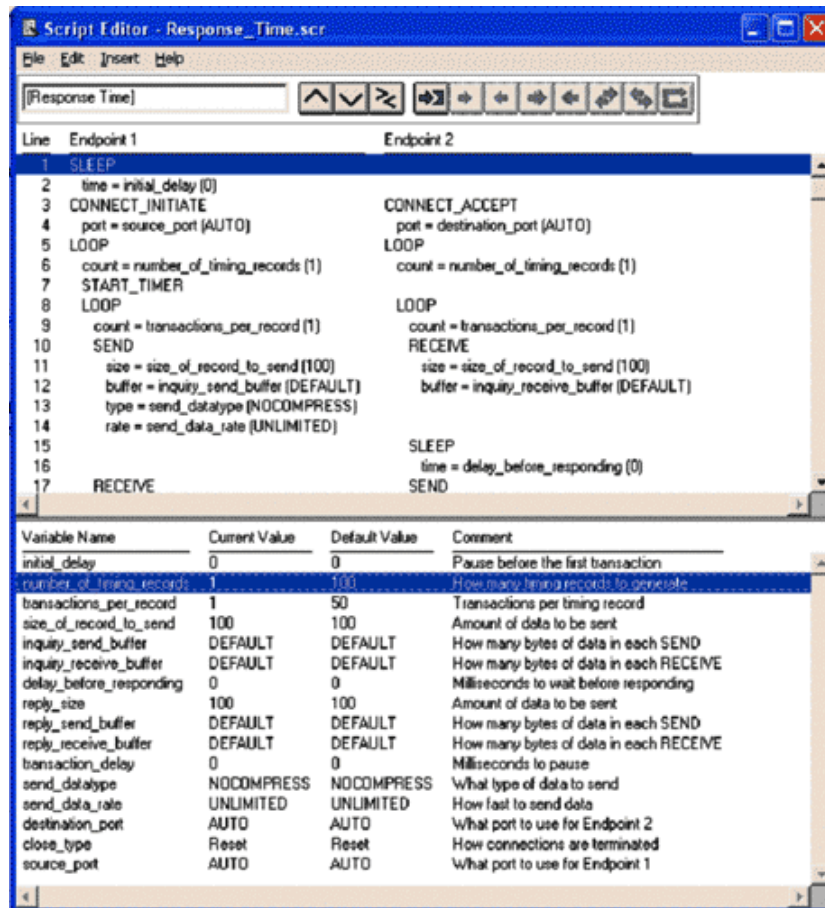
Figure 5. Script Editor setting for testing WLAN roaming.

Test Methodology

The suggested test methodology is:

1. Set up a test network as shown in any of the four topologies above (Topology 1 was used in the tests below).

2. Choose Performance Endpoints appropriate to the operating system of the devices and install one Performance Endpoint (E1) on the wired side of the network and another Performance Endpoint (E2) on the wireless side of the network. The designation of E1 and E2 can be reversed. However, please note that if the real-time reporting mode is used, E2 may add additional stress to the RF network by sending back results while executing the tests. Also, test results may be lost because of the roaming process between APs.

3. Install the IxChariot console on a separate Win32 device.

4. Set up a baseline TCP "Response Time" test between E1 and E2. Edit the script as shown in Figure 5.

5. Set the Run options to 10 seconds and select batch reporting.

6. After 2–4 seconds, initiate roaming process of E2 (e.g., by forcing E2 to change its ESSID association)

7. Review test results.

Execute steps 4–7 to perform a connectionless protocol test using either a streaming script (e.g., Realaud) or a VoIP script (as shown in Figure 7 below).

IxChariot Test Results

Depending on the underlying transport protocol, IxChariot allows you to view and analyze the impact of the WLAN roaming process by focusing on a chosen parameter.

Measuring the Impact of WLAN Roaming on Application Response Times

The time it takes to complete the roaming process of E2 can be determined by looking at the timing records of the test. By changing the script variables in the editor as shown above, it is generally possible to receive timing records every 3ms or less (depending on the link quality). You will then need to look for the timing record where a change in the BSSID has occurred.

IxChariot defines a response time as the time it takes to complete one transaction. By completing a WLAN roaming process during the test run, the IxChariot test application essentially introduces a short-lived network impairment. This impairment can be seen in the sharp spike in the response time. From a measurement perspective, the Response Time Maximum data point can also be used to determine the time it took to complete the roaming process. It should be pointed out that in the case of a forced ESSID change, the initial spike in the Response Time graph is a straight line since the connection was "cut" at a specific time. Once the maximum point has been reached and E2 has successfully associated with the new ESSID, then the graph will gradually go down to the levels recorded prior to the completion of the roaming process (i.e., reporting the interim timing records as the new association process completes).

As shown in Figure 6, the Response Time for timing record 400 is 33ms, which means that it took 33ms to complete the individual timing record. Since the standard timing record completion time was 4ms, the cause of the change was the completion of the roaming process.

Note: Roaming time is generally split into Decision Time and Switch-over time. Decision time is the time it takes an STA to stop attempting to transmit packets to the AP1 after the degradation of the signal. Switch-over time is the time it takes a STA to complete its association/authentication with AP2. Since this test setup was simplified by forcing the STA to change its association, only the Switch-over time is shown in Table 1.
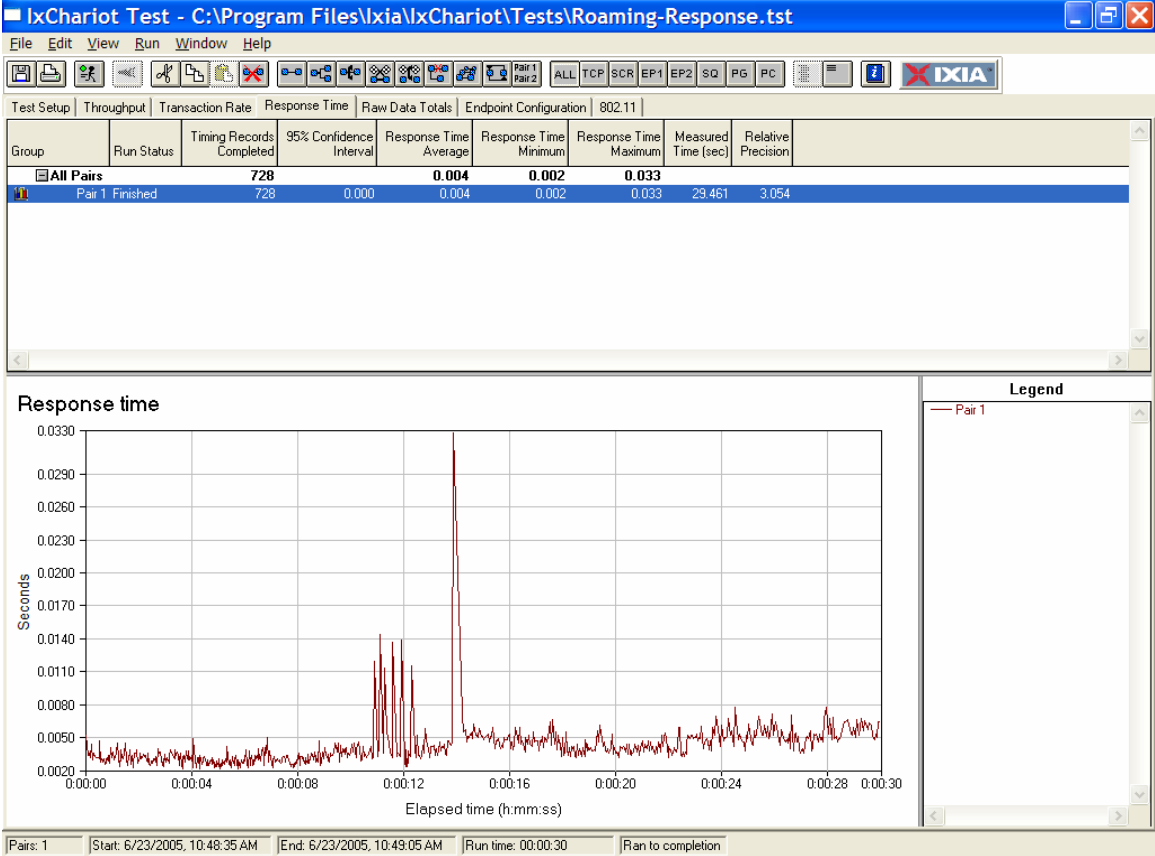

Figure 6. WLAN roaming response time measurements

Timing Records - C:\Program Files\Ixia\IxChariot\Tests\Roaming-Response.tst Pair number 1

Timing record count: 728

Raw Data

Record Number	Elapsed Time (sec)	Measured Time (sec)	Inactive Time (sec)	Throughput (Mbps)	Transaction Rate (#/sec)	Response Time (sec)	Transaction Count	Bytes Sent by E1	Bytes Received by E1	RSSI E1 (dBm)	BSSID E1	RSSI E2 (dBm)	BSSID E2
392	13.575	0.044		0.364	227.273	0.004	10	1,000	1,000	-35	00:09:5b:66:39:c4	n/a	n/a
393	13.611	0.036		0.444	277.778	0.004	10	1,000	1,000	-35	00:09:5b:66:39:c4	n/a	n/a
394	13.646	0.034		0.471	294.118	0.003	10	1,000	1,000	-35	00:09:5b:66:39:c4	n/a	n/a
395	13.693	0.047		0.340	212.766	0.005	10	1,000	1,000	-35	00:09:5b:66:39:c4	n/a	n/a
396	13.741	0.047		0.340	212.766	0.005	10	1,000	1,000	-35	00:09:5b:66:39:c4	n/a	n/a
397	13.786	0.044		0.364	227.273	0.004	10	1,000	1,000	-35	00:09:5b:66:39:c4	n/a	n/a
398	13.829	0.043		0.372	232.558	0.004	10	1,000	1,000	-35	00:09:5b:66:39:c4	n/a	n/a
399	13.876	0.046		0.348	217.391	0.005	10	1,000	1,000	-35	00:09:5b:66:39:c4	n/a	n/a
400	14.203	0.327		0.049	30.581	0.033	10	1,000	1,000	-39	00:40:96:a2:b7:39	n/a	n/a
401	14.276	0.072		0.222	138.889	0.007	10	1,000	1,000	-39	00:40:96:a2:b7:39	n/a	n/a
402	14.332	0.055		0.291	181.818	0.006	10	1,000	1,000	-39	00:40:96:a2:b7:39	n/a	n/a
403	14.390	0.057		0.281	175.439	0.006	10	1,000	1,000	-39	00:40:96:a2:b7:39	n/a	n/a
404	14.436	0.046		0.348	217.391	0.005	10	1,000	1,000	-39	00:40:96:a2:b7:39	n/a	n/a
405	14.488	0.051		0.314	196.078	0.005	10	1,000	1,000	-39	00:40:96:a2:b7:39	n/a	n/a
406	14.539	0.050		0.320	200.000	0.005	10	1,000	1,000	-39	00:40:96:a2:b7:39	n/a	n/a

Switch over results

[OK]   [Refresh]   [Show Latest]   [Help]

Table 1. WLAN roaming response time measurements

Measuring the Impact of WLAN Roaming on VoIP Tests

As Figure 7a shows, the impact during the time of the roaming process was severe (i.e., MOS estimate drops to 2.53) even though the overall MOS score impact caused by WLAN roaming was minimal (i.e., the average MOS score stayed above 4 at 4.03).
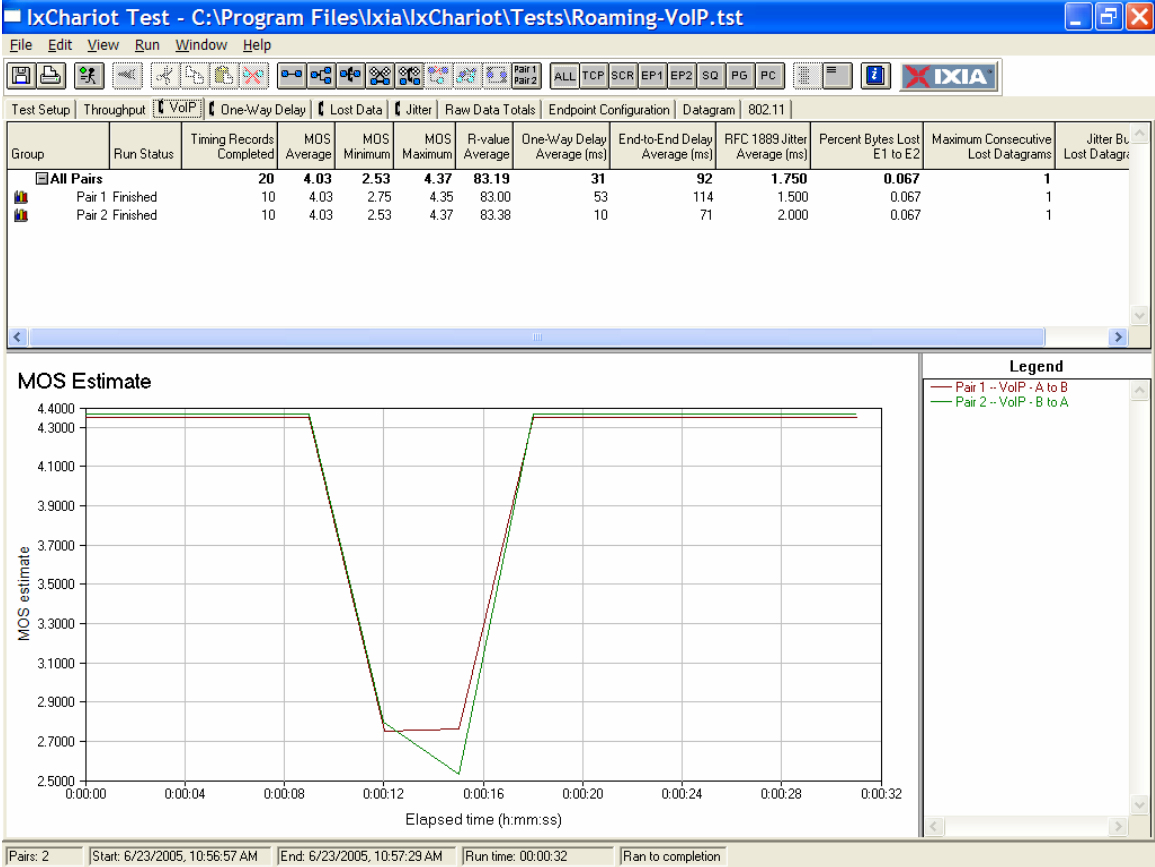

Figure 7a. WLAM roaming MOS measurement

Figure 7b provides the corresponding RSSI values for this bi-directional VoIP test. Notice that pair 1 was associated with 2 Access Points and therefore represents the STA that roamed. Pair 2 represents the second STA that was stationary.
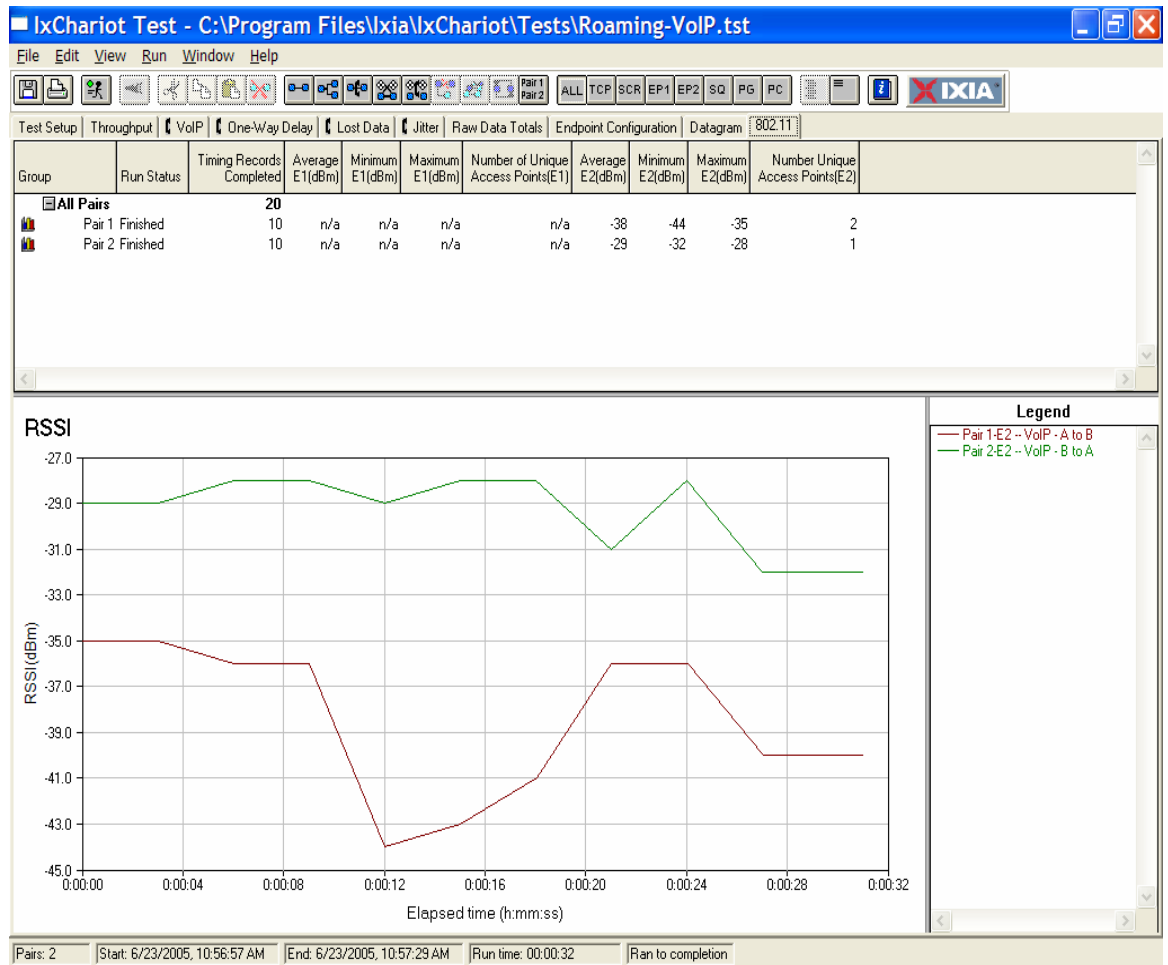
Figure 7b. WLAN roaming RSSI measurements

The Lost Datagram tab is of particular importance to VoIP and streaming media application tests. To calculate lost data, Endpoint 1 tells Endpoint 2 how much data was sent in each timing record. E2 compares the amount sent to the amount it actually received.

Using the Maximum Consecutive Lost Datagram tab in IxChariot, the total number of datagrams lost consecutively can be determined. As shown in Figure 8 below, WLAN roaming causes a spike in the number of consecutive datagrams lost, identifying both their time and severity.

As shown in Figure 8, when using the same 802.11 standard and the same AP and NIC manufacturer, the number of consecutive lost data grams caused by roaming is generally going to be minimal. However, this number can go up significantly when executing test scenarios with equipment from different manufacturers and when switching between 802.11 standards.
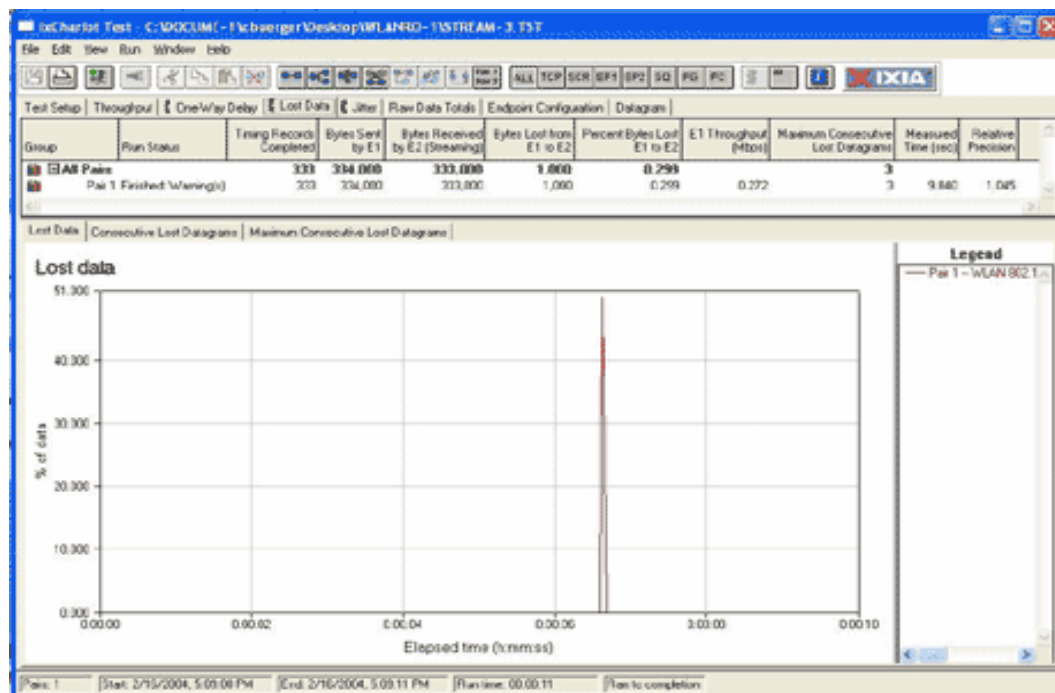

Figure 8.