Arguably the largest, most rigorous and comprehensive set of competitive tests ever performed on wireless LAN equipment, Microsoft Corporation created a test plan that required three different labs to complete: Iometrix Labs in South San Francisco, the University of New Hampshire’s Interoperability Laboratory and Microsoft’s own labs in Redmond, Washington.

The goal of this competitive testing was to find the next generation of wireless LAN platform upon which Microsoft would build its worldwide wireless infrastructure.

In 2004, Microsoft Corporation decided to upgrade its massive WLAN infrastructure with next generation technology. Considered one of the largest enterprise WLANs in operation, Microsoft’s wireless network consists of approximately 5,000 wireless access points (APs) supporting 25,000 concurrent users daily across some 277 buildings spanning 17 million square feet in more than 60 countries around the world.

Consequently, testing and verification of vendor products and claims played a crucial role in Microsoft’s decision-making process.

Testing next generation WLAN solutions presents many new challenges as mobile computing is moving quickly to play a prominent role in the networks of the very large enterprise.

To meet Microsoft’s requirements, the ideal wireless LAN platform needed to scale to large numbers of users, provide multi-faceted security, perform solidly with a minimal deployment of hardware; be cost effective in its deployment and be able to support real-time applications such as voice as well as data. These criteria translate into a list of requirements which, once they are well understood, must be fully tested and verified.

In this paper, we characterize and summarize the tests performed, discuss their relevance and highlight the results of Aruba Networks, the vendor chosen by Microsoft for its next generation WLAN infrastructure. Detailed results are available in the Iometrix Test Report.

Microsoft’s test plan called out 35 discrete test cases that measured both the qualitative and quantitative aspects of the WLAN devices under test (DUT) in the following areas: performance, security, quality of service, standards conformance, roaming and interoperability.

Each of the four vendors received a score for each test which was then multiplied by a weighting factor provided by Microsoft. For the combined tests, Aruba received the highest weighted score.
Network Test Bed and Wireless Test Equipment Utilized

Achieving repeatable results in the wireless space is a challenge because air, the medium interconnecting stations and APs, is inherently unstable. RF interference generated from a wide variety of sources (2.4 GHz phones and microwave ovens, radars, adjacent channels, people and objects in motion) make the acquisition of repeatable results near impossible.

To remedy this, Microsoft executed all performance tests with Iometrix in a controlled RF environment using the W800 wireless test platform from Azimuth Systems equipped with multiple TMM, STM, RFM and WLA modules. Iometrix also used the ESG series signal generator from Agilent Technologies to run the RF impairment tests and Agilent’s N2X Multi-service Tester to generate and analyze data traffic for the performance tests.

Finally, Iometrix relied on Ixia’s ANVIL tools to test 802.1X and 802.1D conformance. Ixia supplied on-site engineering support to adapt the 802.1X conformance test suite to the 802.11 wireless environment.

For the integration testing at Microsoft, Microsoft’s warehouse was used. There were approximately 12 APs positioned in the two warehouses covering 250K square feet. APs were spread out ranging from 30 to 100 feet from each other throughout the building and were indirectly connected to Cisco 3750 switches for PoE and L2 connectivity to the core Cisco 6509 switch which performed all the routing for the entered network.

Each AP was configured with five separate SSIDs with different encryption types, such as static WEP, WPA, and WPA2 along with different authentication methods. The APs were also logically divided into five groups with five separate IP subnets and three physical areas.

There were two backend Microsoft Windows 2003 servers. One server was configured for SNMP, Syslog, and Ixia Chariot Server capability. The other was configured to be the Primary Domain Controller with Active Directory, Certificate Authority, DHCP, DNS, and IIS server capability. The wireless devices used were 15 Compaq HP PP3000 Tablet PCs with multiple internal and external NICs.
Cognio ISM sensors were also used to monitor the RF spectrum during all the testing. This complex topology allowed Microsoft to test inter-subnet and multi-switch roaming capabilities for each vendor.

**Lab Performance and Conformance Testing Results (Iometrix)**

The Iometrix testing for Microsoft evaluated the WLAN vendors using very specific and repeatable tests to help answer the basic questions asked by any IT administrator when evaluating a WLAN solution. This testing provided quantitative results that are easy to analyze and compare.

Among other things, the Iometrix testing for Microsoft measured the rate and range of an AP (for different bands – 802.11a, b and g) and to observe the traffic pattern as the client was moved away from the AP. This includes finding the “distance” at which the forwarding rate from the AP to the client drops and becomes sub-optimal. Also observed was the rate-adaptation algorithm used by each AP as the client moves away.

In these tests, Aruba WLAN system provided outstanding performance at an optimal forwarding rate for a “distance” of more than 80dB path loss and the rate adaptation is smooth as well.

This testing also included other important and basic performance tests such as testing the throughput of the AP for different packet sizes as well as for different mixes of packet sizes. To emulate different kinds of packet distributions, the testing was conducted with a standard packet distribution (containing an equal ratio of packets of different sizes ranging from 64 bytes to 1500 bytes) as well as a customized packet distribution (as obtained by collecting real-life data from the current Microsoft network).

The results of the tests clearly demonstrated Aruba's performance in terms of high and consistent throughput for all types of packet sizes and distributions.

One of the important challenges introduced in enterprise WLANs is the concept of roaming and its effect on the performance of the wireless network as well as the end-user experience. The Iometrix testing also delved deep into this issue, evaluating the roaming times between two APs. The testing broke up these results into the times required for different stages of the roam including the scanning by the client, probe request/response process and the 802.11 association process.
The roam times in the case of Aruba averages approximately 29ms. In all the cases it was clearly illustrated that the time taken by the access point was extremely low and thus in the presence of well-implemented clients, the roaming times would be within acceptable limits for enterprise usage.

Since most enterprise WLANs now contain multiple BSSs on the same AP to accommodate multiple services such as employee access, guest access and VoWLAN, the testing also evaluated the abilities of the WLAN system to support different security mechanisms for different BSSID’s on the same AP as well as the ability to perform traffic shaping to ensure required bandwidth for each type of application.

Special tests were conducted to evaluate each WLAN solution for its capabilities to provide sufficient QoS capabilities to support sensitive applications such as VoWLAN in the presence of other (competing) data applications such as employee access. Since the roaming between APs can potentially affect voice applications more than data applications, special tests were also conducted to ensure that the roaming times of voice devices were lower than the human threshold for detecting any erosion in voice quality. The results of these tests indicate that the prioritization mechanism used by Aruba ensures that voice quality does not suffer in the presence of background data traffic. Also, the roam times for the voice devices ranged from about 22ms to 35ms, which is low enough to be not noticeable to the human ear.

Microsoft Onsite Integration Testing and Results

The WLAN testing performed at Microsoft’s own labs in Redmond focused on eight areas of integration:

- Usability
- RF management
- Network management
- Network security
- Intrusion detection
- Location awareness
- Mobility
- Voice

As enterprise networks or universities, there are several cases where many users will congregate in an area and use Wi-Fi (eg. lecture halls and conference rooms). Most legacy wireless systems would be heavily burdened due to the large number of 802.11 associations and a high amount of throughput require for a single AP.

For Microsoft, it was critical to test each DUT’s ability to handle a highly concentrated amount of wireless stations in the same physical area. Also examined was the ability for the DUT provide seamless roaming and the best performance between APs without being affected by the amount of wireless devices regardless of the security method deployed in the network.

Fifteen Compaq HP PP3000 wireless tablet PCs in a single room were used to associate with three different APs. The first test required the tablets’ Wi-Fi interface to be configured to associate to an SSID without encryption (i.e. an open system). The second required the tablet’s Wi-Fi interface to utilize WPA2. Testers then monitored association times and how each DUT balanced users among available APs. The results of this test suite indicate that the Aruba WLAN system was able to quickly and smoothly balance the 15+ tablet PCs amongst the three APs (approximately five per AP) without affecting user traffic even while roaming. The tablets were also monitored over time and it was verified that they had no problems in staying associated to the APs in this model.

RF Management

The first critical step in deploying a high performance WLAN is to choose the best 802.11 channel and power setting plan for each AP in every part of the building while providing the best redundancy design in case of an AP failure.

Most IT administrators take hours, even days worth of planning and site-surveying to get the correct channel/power plan per AP per floor per building - making sure that any of there manual choices will not cause interference to any part of there network.

To this end, Microsoft set out to scrutinize each WLAN vendor’s RF capabilities to ascertain which platform was the easiest, most intelligent, and provided the best methods in
dynamically choosing the highest performing 802.11 setting regardless of what other interference is within its environment.

For these tests, Microsoft required each vendor to set up at least 13 APs (that were reset to factory defaults) throughout the building. Once the APs were placed in position they were all powered on at the same time. Meanwhile engineers measured the effectiveness of the vendor’s APs in dynamically learning its environment, in reporting statistics in its environment and the time (in seconds) to find the best setting. This included measuring the accuracy of how the APs minimized their co-channel interference with each other and how efficient they were to avoid any 3rd party AP or non-802.11 interference that was placed in the network.

To test resilience around failures, an AP was physically disconnected (simulating complete failure) from the network and an AP’s radio was failed (simulating partial failure) while its Ethernet link remained operable. DUTs were measured on their ability to quickly adapt and/or mitigate the loss in the environment and in a transparent fashion to client devices.

Microsoft’s RF management tests indicate that the 12 Aruba APs were able to pick the best 802.11a/b/g channel and power settings within several seconds.

When an AP was removed from the network (simulating a complete failure) the Aruba APs in that area converged within several seconds to increase their power and coverage to dynamically heal for the loss in Wi-Fi while making it transparent for all the wireless tablets in that area.

When a simulated radio failure occurred in the network the Aruba APs took two or three seconds to detect the loss and then dynamically fill the coverage hole. To test the advanced RF intelligence of the Aruba WLAN System, an interference generator for non-802.11 noise was used at a certain RF frequency range within which the AP was operating. In a matter of seconds, Aruba’s system determined that its channel had greatly degraded and automatically moved to a more optimal channel that would provide higher performance to users.

**Network Management**

IT administrators’ biggest struggle with wireless today is in figuring out a mechanism for measuring their WLANs overall health with the controllers, the APs, and the wireless devices within the company. Too many operations personnel are blind to their wireless network and often find it difficult to be proactive in finding problems before users complain.

For Microsoft it was imperative to have each DUT demonstrate its ability to alert the operations personnel whenever any local or third-party interference was detected on any of their APs in their network – providing timestamps, duration of interference, and in-depth 802.11 display of statistics. Each DUT was also required to identify the stations affected and what percentage of each stations’ traffic was affected by this interference in verbose 802.11 output.

In the event of any failure in the processes of the AP, or the radio of the AP, or even in its Ethernet connection to the network, the IT staff must be immediately notified with SNMP and Syslog traps. Each DUT was also required to demonstrate how it could provide full 802.11 and above protocol level analysis of frames from any wireless device or AP in the network remotely without having to use any wireless LAN card in their PDA or laptop.

The results of Microsoft’s network management test showed that the Aruba WLAN System was able to proactively alert through SNMP, Syslog, and graphically display where interference was detected in the network.

The radio failure testing showed that Aruba WLAN controller could detect and alert (SNMP / Syslog / Aruba NMS trap) within seconds of any AP failure. For the troubleshooting and remote analyzing test the Aruba WLAN System was deemed to be the easiest and most flexible in providing full 802.11 and above protocol level packet tracing regardless where the Aruba AP and monitoring station were located within the L3 network.

**Network Security**

A rogue AP is an AP not sanctioned or authorized by network administrators. Typically, rogue APs are connected to a network by well intentioned employees unaware of the security risks they cause. Enhanced security monitoring enables faster response to these
security breaches by performing the following functions: detection, classification, and containment.

It’s important that WLAN security solutions must not have any false positives about declaring which devices are connected to its internal network (a security hole) and which devices are just neighboring Wi-Fi networks (not a security risk).

For Microsoft testing, each DUT had to demonstrate the ability to detect a rogue AP whether it is unencrypted, heavily encrypted, enabled with NAT, or even configured as a bridge. Once the rogue AP is classified and detected, the WLAN vendor must contain the device so that no wireless device may use it to access the internal network more than a seconds worth of time until the device is located and removed.

At a minimum, DUTs needed to demonstrate the ability to detect the common 802.11 attacks such as de-authentication floods, Airjack driver use, AP spoofing, client spoofing, client-to-client attacks, RF jamming, and any enterprise policy violations. For the Microsoft testing, each DUT was also required to demonstrate the capability of interception, monitoring, reporting, and trending of such attacks.

This security test suite showed that the Aruba WLAN System was able to quickly classify, report, and contain any type of rogue AP whether it was unencrypted, heavily encrypted, enabled with NAT, or even configured as a bridge. The Aruba WLAN switch successfully pass the 802.11 DoS attack testing by quickly intercepting, trending, and reporting in detail of all the attacks that were launched.

**Voice over Wireless**

Despite improved maintenance and administration tools, switched WLAN networks are vulnerable to issues arising from the heterogeneous network environment, especially the integration of services such as voice over IP (VoIP).

Because VoIP services are in demand in professional settings, it is imperative to enterprise adoption that wireless data and sensitive VoIP streams coexist in a WLAN switch system.

Running voice over a WLAN, packets have limited lifetime, traffic bandwidth is deterministic, latency and jitter must be kept at a minimum, and the phone’s IP session must never drop.

Microsoft’s test procedure was designed to ensure that at least 12 wireless tablet PCs were able to roam across five groups of APs, configured with the same SSID. These wireless devices were forced to cross different VLANs in the process of roaming.

The first test used no encryption on 802.11a, then 802.11b, and then 802.11g. Subsequent tests utilized WPA2 on all bands. The 12 wireless tablet PC leveraged Ixia voice software that was managed by an Ixia server sending bi-directional traffic throughout each test procedure.

As the wireless tablet PCs roamed together, testers monitored voice monitored for authentications per minute, data transfer rate, jitter, delay, R-value, roaming time, and the dropping of any voice calls.

The mobility and voice test suite showed that the 12 wireless tablet PCs could seamlessly roam together across the Aruba WLAN System in 802.11a, b, or g mode using the strongest encryption (WPA2) at a high data rate and quality with minimal jitter and delay regardless of the amount of VLANs or WLAN switches they crossed - and without dropping any calls.

**Location Awareness**

At the time of troubleshooting Wi-Fi connectivity problems or hunting down Wi-Fi security breaches, an administrator needs a tool to be able to accurately locate a specific AP, wireless laptop, or any 802.11 device within the building or campus. Each WLAN DUT was required to graphically demonstrate quick and accurate location tracking of any 802.11 device within one to nine feet.

In this location testing, Aruba’s WLAN system was able to pinpoint a single rogue AP within less than four feet.