



Wireless Validation

Superior wireless product performance in the market is dependent upon the driver's ability to perform in a variety of real world functional circumstances. Wireless driver validation and testing is separate from the interoperability compliance that the Wi-Fi Alliance Certification [<http://www.wi-fi.org/>] will provide. Wi-Fi driver validation at nResult consists of two core components. These components are Functional Testing and Localization Testing.

Functionality Testing

The following selections can be utilized as iterations in wireless driver functionality testing. This provides you with dynamically scalable coverage for your testing needs.

802.11x Standards

- A Only
- B Only
- G Only
- BG Only
- ABG Only
- Pre-N

Networking Protocols

- IPv4
- IPv6

Security

Authentication	Encryption	Options
Open	None	
Open Shared	WEP 64bit	Passphrase Hex Key Index : 1,2,3,4
Open Shared	WEP 128bit	Passphrase Hex Key Index : 1,2,3,4
WPA – Personal Pre Shared Key WPA – Enterprise 802.1x	TKIP AES	Passphrase Hex 802.1x – TLS (PC Certificate, User Certificate)
WPA2 – Personal Pre Shared Key WPA2 – Enterprise 802.1x	TKIP AES	Passphrase Hex 802.1x – TLS (PC Certificate, User Certificate)

Basic Connectivity

These tests are designed to validate the most basic elements of Wi-Fi networking. They can be executed in any array of security, wireless standards (A/B/G/Pre-N) and Operating System (OS) iterations as requested. Validating the basic connectivity of wireless device drivers is essential to a Wi-Fi device.

- Basic Association
 - Basic association with the Access Point (AP) connects the Device Under Test (DUT) to the AP with the same settings (SSID, 802.11x, Security) as the AP using both proprietary device application and the Windows Zero Configuration (WZC) for Microsoft Windows XP (WinXP). The DUT's ability to execute a basic association with the AP is fundamental to networking.
- Connectivity Stress Testing
 - Connecting the DUT to the AP with the same settings (SSID, security settings) as the AP using both proprietary application and WZC (WinXP) and sustaining the connection through a large transfer is verified.
 - In order for the DUT to have a standard level of QOS it must be able to sustain connection amidst a large file transfer and transmit data accurately. The integrity of the data will be verified at the raw data level after the data transfer stress test.
- Basic AdHoc Network

- The DUT's ability to create and sustain an AdHoc network is tested using WZC or a proprietary device application and an additional third party DUT.
- AdHoc network is then created by configuring the DUT and the third party DUT with static IP addressing and dynamic addressing.
- An AdHoc profile is created on the DUT and the third party DUT is connected to the network. Data integrity is verified after file transfers and stress testing on the AdHoc network.
- These tests are usually repeated with various security settings (WEP, WPA).
- Validating Radio HW/SW Switch (on/off)
 - The hardware switch is tested thoroughly to verify its functionality with the wireless drivers. If the hardware is turned off and the drivers do not recognize how to turn it back on, this would be a failure in wireless validation.
 - HW Switch validation include tests that turn HW switch on/off and the SW switch on/off and validating that every combination of these switch operations is functioning as designed.
- Verification of Tray-Set Icon
 - The tray set icon is the quickest way (and generally the primary means) to check the status of the WiFi connection to the AP. Verifying that the visual icon is representative of the status of the device is necessary. The mouse over tool tips should provide a standard amount of connection data, such as the network connected to, IP address and Link Quality.
 - The tray set icon right click context menu will generally have a radio switch for easy connectivity access. The functionality of this option and the appearance of the appropriate icon for connection status will be verified.
- Verification of Main GUI
 - The application main GUI is the primary interface for changing settings of the WiFi device and troubleshooting any connectivity issues. Validation of the GUI is integral to product performance in the market.
 - The connection status, connection details, AP listing, AP details, adapter settings and wireless preference configuration are all validated.

Localization Testing

Localization testing of wireless drivers and software is a fundamental step to achieving success in the global market. Wireless devices can be difficult to troubleshoot and manage in the original domestic release. Imagine the frustration and disappointment you would have trying to manage and troubleshoot a wireless network in a version that has missing words, sentences that make little or no sense, menus and settings that make no sense, network and connection details reported inaccurately and not to mention if the functionality simply failed after the localization development cycle. Localization testing works to identify and evaluate these all too common failures. To make sure there are no cultural or other native issues in a translated text, all our localization editors are native speakers of the languages they are editing. Our localization testing services are a key step in the development cycle to ensure the global market readiness of your product.

About nResult

Mail

nResult
2811 E Evergreen Blvd
Vancouver, WA 98661

Voice

503-257-8000

Fax

503-257-8835

Online

<http://www.nresult.com>

E-Mail

info@nresult.com
