

General Project Description

Project title: Verification of an IPv6 implementation for Windows CE 4.1
Project kind: Industrial project
Contractor: Nickolay Pakoulin and Gregory Kluchnikov (ISP RAS)
Customer: Microsoft Research Cambridge
Project start date: 15 May 2002
Project end date: 15 March 2003 г.

Project Goals

The goals of the project were: (1) to test conformance of IPv6 implementation in Windows CE 4.1; (2) to develop a test suite for conformance testing of Mobile IPv6; (3) to demonstrate portability and reuse test suite components developed using UniTesK; (4) to demonstrate applicability of formal methods to specification and verification of internals of embedded OSes, such as Windows CE.

Project Input

The implementation under test is an implementation of IPv6 for Windows CE and Windows XP from Microsoft, based on the IPv6 implementation from Microsoft Research. The IUT is distributed in binary form, source code is not available. For more details about IPv6 support in Microsoft operating systems please visit company's web site, <http://www.microsoft.com/ipv6/>.

The project includes two stages – MSR IPv6 test suite porting to Windows CE and extension of the test suite with specification and tests for Mobile IPv6 features.

We tested how implementation of certain host-related features of Mobile IPv6 and Multicast Listener Discovery protocol (MLD) conform to the protocols' specification.

IUT size is unknown as the sources are not available.

Requirements for features of Mobile IPv6 and that were added to the test suite were elicited from plain text Mobile IPv6 and MLD specifications (domain standards). Requirements to Mobile IPv6 implementation were elicited from Mobile IPv6 Specification draft 13 because the implementation claims to support this particular draft of the standard. Requirement to MLD were elicited from MLD specification version one, RFC 2710, because the IUT supports MLDv1 only. Other RFC were used as well: RFC 2462, RFC 2473. Total size of documentation used is about 195 pages, plain text.

Process Used

Method: CTesK super-lite toolkit. The project features that distinguish it from other UniTesK applications are presence of non-procedural stimuli in IUT interface and deferred reactions. Another distinguishing feature is distributed scheme of the test harness.

Development: Development was done on Windows 2000 using CTesK super-lite and Microsoft Visual Studio 6.0. Test suite components that run on Windows CE were developed using Microsoft Platform Builder 4.1.

We developed a toolkit for distributed testing that controls test agents and other remote test suite components.

Test harness and tools: The test harness is spatially distributed. Test system core components run on Windows 2000 box, test agents run on Windows CE CEPC, and some auxiliary components.

Project Effort:

Project duration: 10 months

Effort estimate: about 3 men-years

Project Results

Size of tested subsystems is unknown.

Estimation of changes to MSR IPv6 test suite during porting to Windows CE:

Test suite component	Changes, %
Specification	7%
Test Scenarios	5%
Mediators	35%

Estimation of extensions to the test suite:

Test suite component	Additions, lines
Specification	5000
Test Scenarios	2000
Mediators	5000

The total size of the manually developed components of the test suite is about 25, 000 lines.

Project goals were achieved.

The test suite for IPv6 conformance testing was ported from MSR IPv6 / Windows 2000 to IPv6 on Windows CE 4.1. Porting demonstrated high portability and reusability of the test suite components -- most changes are localized in system-specific mediator layer. Specifications and test descriptions were left almost unchanged.

The test suite was extended with specifications and tests for Mobile IPv6 and MLD. It showed that UniTesK-based test suites are easily extensible.

Applicability of UniTesK to specifying and testing Windows CE internals was demonstrated.