Formalization and Verification of the SHIM6 Protocol

Matthijs Mekking

May 2007

Abstract

The Internet is a loosely-organized international collaboration of autonomous, interconnected networks. Host-to-host communication is supported by protocols and procedures defined by Internet Standards. An Internet Standard is stable, well-understood, technically competent and must have multiple, independent, and interoperable implementations with substantial operational experience. However, many specifications are written in an informal language that allows ambiguities, omissions and inconsistencies that are difficult to detect and which will possibly be adopted by implementations. By describing critical parts with the use of formal languages, such problems could be avoided.

This thesis shows how a formal derivation of a standard in development can improve the quality of the specification. I have partly modeled a protocol named Shim6, which will act between the transport layer and network layer of the network stack. Shim6 provides host-based multihoming to increase the reliability of your network connection. Two critical phases can be identified: the establishment communication exchange and the reachability protocol. The first phase enables multihoming for two communicating hosts. The second phase detects link failures during the communication.

The two algorithms have been modeled with UPPAAL , a model checking tool which allows us to specify, validate and verify models of real-time systems. The UPPAAL syntax is sufficiently expressive for the description of network protocol specifications, and has been used in many other case studies. My work revealed several errors that were not spotted before, and that were difficult to derive from the protocol specification.