Software Wrappers to Support Nonstop Computing

Franklin Webber
Key Software, Inc.
840 Hanshaw Road, Suite 1
Ithaca, NY 14850
webber@keysoft.com

In the future, an increasing number of systems will require nonstop computing. A *nonstop computing system* is one that must continue processing in spite of subsystem failures, while adapting to a changing environment, and while permitting software and hardware upgrades. Nonstop computer systems continue to operate over long periods of time and must not be rebooted during those periods, either because reboot is impractical or because a reboot would result in failure to satisfy real time constraints. Over a long period of time, change is inevitable; to cope with that change, a nonstop computer system must be flexible enough to adapt and to be modified while it is in use.

The largest nonstop computer system in use today is the Internet. Although the Internet is not a real time system, rebooting it would still be costly. So the currently planned upgrade of the Internet, to replace the Internet Protocol (IP), will be a gradual replacement of IP version 4 with IP version 6[1]. The two versions of IP will coexist in the Internet for a long time, and at no time will the Internet be rebooted to make the upgrade.

Nonstop computing systems will become more common as the embedded systems now used for real time control of many processes become increasingly linked into larger distributed systems. Currently, most embedded systems are isolated: in cars, VCRs, machine tools, etc. Soon, however, many of these embedded controllers will be part of the Internet and will be interconnected into systems of systems. The larger such a system of systems grows, the harder it will be to decide when rebooting it is acceptable. Eventually reboot will be unacceptable and a new nonstop computing system will be born.

We will eventually need better technology to support nonstop computing. The upgrade of the Internet Protocol will be an expensive change and so is not ideal as an example of how to upgrade a nonstop system. Better would be support for incremental changes that could be applied as routinely and as inexpensively as single-host operating systems are now upgraded and patched. This support should allow:

- incorporation of new code into running systems and diffusion of new code throughout distributed subsystems;
- automatic analysis of new code to identify its worst-case behavior and identify interference with previously running code;
- fine-grained control over privilege given to new code;
- protocols to coordinate the diffusion of new code;
- replacement of protocol layers without disruption to processing in other protocol layers;
- protocols to tolerate and adapt to subsytem failures.

Much of the technology needed for nonstop computing can be localized in software wrappers. A *wrapper* is a software layer used to change the interface of a component or to give new properties, such as fault tolerance or security, to the interaction between components. Software wrappers are often used to glue existing subsystems into a larger system with new properties and functions. The wrappers know the protocols needed to make the subsystems work together, even if they were not originally designed for a common purpose. When a system is reconfigured, either to replace a subsystem or to change the quality of service offered on a communication link between subsystems, it is the software wrappers that enable the reconfiguration by replacing or augmenting the protocols they use.

The Adaptable Dependable Wrappers Project underway at Key Software is concentrating on developing better wrapper technology to support nonstop computing[2]. We are designing software wrappers that can adapt by changing the set of protocols they use. Our wrappers feature:

- protocols that can be replaced without disrupting communication channels they implement;
- metaprotocols for coordinating the upgrade and replacement of other protocols;
- protocols that share data securely and efficiently through the use of capabilities enforced by compile-time checking;
- the use of group coordination protocols to support fault tolerance and the use of encryption protocols to support security in a distributed system.

Our project is sponsored by DARPA and USAF Rome Laboratory.

References

[1] S. Bradner and A. Mankin. The recommendation for the IP next generation protocol. Technical Report RFC 1752, Internet Engineering Task Force, http://ietf.org/rfc/, Jan. 1995.

[2] F. Webber, J. R. M. Enerney, and D. McCullough. The adaptable dependable wrappers project. In *Dual-Use Applications Conference*, 1997.