The Simple Times is an openly-available publication devoted to the promotion of the Simple Network Management Protocol. In each issue, The Simple Times presents technical articles and featured columns, along with a standards summary and a list of Internet resources. In addition, some issues contain summaries of recent publications and upcoming events.

In this Issue:

Applications, Tools, and Operations

- Editorial .................................. 1
- IAB Network Management Workshop .......... 2
- GetBulk Worth Fixing .......................... 3
- Net-SNMP: Old Wine in a New Wineskin? ....... 6
- Evaluating MIB II (RFC1213) Implementations 8
- The Story Behind the SNMP Vulnerabilities .... 15

Miscellany

- Book Reviews ............................. 17
- Standards Summary .......................... 19
- Recent Publications .......................... 22
- Calendar and Announcements .................. 23

Publication Information 23

The Simple Times is openly-available. You are free to copy, distribute, or cite its contents; however, any use must credit both the contributor and The Simple Times. (Note that any trademarks appearing herein are the property of their respective owners.) Further, this publication is distributed on an “as is” basis, without warranty. Neither the publisher nor any contributor shall have any liability to any person or entity with respect to any liability, loss, or damage caused or alleged to be caused, directly or indirectly, by the information contained in The Simple Times.

The Simple Times is available as an online journal in HTML, PDF and PostScript. New issues are announced via an electronic mailing list. For information on subscriptions, see page 23.

Editorial

Aiko Pras, University of Twente
Jürgen Schönwälder, University of Osnabrück

This issue of The Simple Times is published at a historic moment: SNMPv3 has just been published as an Internet Standard (STD 62). As a consequence, the original SNMPv1 protocol has been removed from the official list of Internet standards by declaring it Historic. Despite that status change, we may expect that SNMPv1 will stay with us for many more years. Therefore it remains important to maintain SNMPv1 implementations and correct bugs. As demonstrated earlier this year, more than a decade of SNMP implementation experience could not prevent that there are still many bugs in existing implementations. In February, CERT published an advisory (CA-2002-03) that received a lot of attention within the Internet management community. This issue of The Simple Times includes an article from the Oulu University Secure Programming Group; the group that performed the tests that resulted in the CERT advisory mentioned above. In addition to that article, this issue of The Simple Times also includes an article discussing the correctness of MIB implementations.

The process of standardizing a successor for SNMPv1 has not always been easy. In fact, work already started in the earlier nineties with two activities to improve SNMP: one activity focused on adding security and the other on enhancing functionality. In 1992, it was decided to join these activities and produce a new standard called SNMPv2. The first set of SNMPv2 RFCs appeared in April 1993; these RFCs were based on the so-called “party based security model.” Since SNMPv1 has been very successful, many groups started to experiment with SNMPv2 prototypes. After some time, it turned out that the party based model was difficult to understand and use. One reason for confusion was the fact that the administrative model was general enough to accommodate single (shared) key approaches, as well as two (public and private) key approaches. The actual protocols, however, realised only the second approach. After many heated discussions the climax was in June 1995, when two of the SNMPv2 editors ceased support for their party-based model. Only two months later, there was general agreement that the party based model...
was too complex; unfortunately, there was no agreement on how the alternative should look like. Consequently, many competing alternatives appeared; the best known ones were SNMPv2u, SNMPv2+ and SNMPv2c. At that time, it seemed no longer obvious that discussions should be based on technical arguments; as a result this period turned out to be quite bad for SNMP’s reputation. Fortunately, it was decided to form an SNMP Advisory Team, which recommended in 1996 to further progress a simplified version of SNMPv2. In March 1997, a new IETF working group was formed with the task to develop SNMPv3; this group published in January 1998 the first SNMPv3 RFCs as Proposed Standards. In April 1999, the status of SNMPv3 was raised to Draft Standard, and now SNMPv3 has become Internet Standard. This milestone should be important for software developers; an article that discusses the best known open source implementation that supports SNMPv3 is included in this issue of The Simple Times.

Despite the fact that SNMPv3 is now an Internet Standard, improvements are still possible. This issue includes an article that discusses possible improvements of the GetBulkRequest. Recently, the IETF has chartered a new working group that should work on the Evolution of SNMP (EOS). As the name of this working group already suggests, this group should take an evolutionary approach and propose relatively small improvements. Many possible improvements have already been proposed by the IRTF Network Management Research Group (NMRG). Since SNMP is primarily being used for monitoring purposes and has not been widely accepted for configuration purposes, several groups are currently discussing more revolutionary approaches. In June this year, the Internet Architecture Board (IAB) organised a special workshop to discuss the future of Internet management; an article about this workshop is included in this issue of The Simple Times. Various people within the IETF and IRTF-NMRG are now investigating revolutionary approaches for Internet management. Work in this area has just started and we hope to report on these activities in a future issue of The Simple Times.

IAB Network Management Workshop

Ran Atkinson, Extreme Networks

At the Spring IETF meeting, the Internet Architecture Board (IAB) announced that it planned to hold an IAB Network Management Architecture Workshop, in coordination with the IESG. The workshop was held in early June at the IETF Secretariat offices in Reston, VA.

IAB Workshops are normally invitation-only because of limited space for attendance and to keep the group small enough that focused architectural discussions are possible. Roughly 30 people were invited and about 25 people actually attended. There was a deliberate effort to get a broad mixture of people with experience in different technologies and different kinds of networks. This was largely successful, though enterprise network operators were probably under-represented. Invitations went out to people in North America, Europe, and Asia/Pacific. Most attendees were from Europe or North America.

Goals for the workshop were to discuss the various alternative approaches to various aspects of network management and to continue the effort to obtain more operator input on significant unresolved problem areas relating to network management.

Several people wrote white papers before the workshop that were distributed to the workshop invitees. This was very helpful in getting a wide range of perspectives out for discussion prior to the meeting. It is expected that several of these white papers will be made available either on the web or as Informational RFCs, as their authors prefer.

The workshop met for two and a half days, discussing a wide range of topics. The discussions were productive, but there were more potential topics than could fit into that time period. On the first morning, the group split into two. One sub-group consisted mostly of network operators and focused on enumerating unresolved network management problems they are facing. The other sub-group consisted mostly of protocol developers and developed a taxonomy of the several network management technologies that exist today. For the remainder of the workshop, the whole group met together. One of the several topics raised by the network operators was the challenge of managing configurations for the many devices inside the network – particularly remote devices in unstaffed locations. Throughout the workshop, there was also extensive discussion about the roles and opportunities for SNMP, COPS, COPS-PR, XML-oriented configuration, and other technologies. On the second day there was a significant discussion about perceived IETF process issues as those relate to network management technologies. A wide range of views emerged throughout the workshop. While unanimity was rare, consensus emerged on several topics after significant discussion.

The workshop report, which will be published as an Informational RFC once it is ready, will discuss the details of these consensus areas in detail. The attendees also agreed not to individually comment in public about what any conclusions of the workshop might have been, in order to prevent misunderstandings from emerging. IAB Workshops do not have any formal standing to force