Internet Network Management Using The Simple Network Management Protocol

Jeffrey D. Case	James R. Davin	Mark S. Fedor	Martin L. Schoffstall
The University of Tennessee, Knoxville Knoxville, Tennessee	MIT Laboratory for Computer Science Boston, Massachusetts	NYSERNet Incorporated Albany, New York	NYSERNet Incorporated Albany, New York

Abstract

The Simple Network Management Protocol, or SNMP, is an application protocol that that allows logically remote users to inspect or alter management variables. The SNMP is typically used for the management of networks of networks, or internets, which utilize the TCP/IP protocol suite.

This paper provides a brief introduction to the SNMP and describes its architectural principles. The transport paradigm and SNMP applications are discussed. The status of the SNMP standard is described. Important lessons learned from the SNMP experience and a brief look at the future are included.

1 Introduction

The Simple Network Management Protocol (SNMP) [1] is an application protocol by which network management variables may be inspected or altered. The SNMP is typically used to convey network management information between network management systems and agents in managed network elements such as hosts, terminal servers, network attached printers, bridges, routers, and gateways.

Networks of networks, or internets, pose significant network management challenges. The SNMP was designed for the management of TCP/IP-based internets and is often applied in that context. Increasingly, the SNMP is being applied to the management of internets based on other protocol suites.

1.1 Heritage

The SNMP evolved from the Simple Gateway Monitoring Protocol (SGMP) [2]. That protocol was designed for the monitoring of gateways in TCP/IP-based internets and became widely deployed in that environment. However, the growing success of the protocol led to increasing demands for changes.

Some of these changes, based on operational experience, enhanced the service. One major set of changes included extensions to strengthen management capabilities, beyond just monitoring. The language was generalized beyond gateways to include end systems and other network elements. These changes were made in order to meet existing needs.

Other changes, based on future expectations, altered the protocol. These changes were made in order to ease the transition to OSI-style network management. These changes included the definition and adoption of an OSI-style Structure of Management Information (SMI) [3] and Management Information Base (MIB) [4].

1.2 Design Process

The SNMP was built via the correct design process. First, SNMP was shaped by the collaborative effort of university researchers, users and managers of networks, and communications vendors. The principle designers were individuals actively involved in the management and research of internets who had a practical focus. This practical focus was grounded by applicable experience. The short time in which the SNMP was designed, implemented, and deployed was possible because of this shared focus.

Second, design ideas were gleaned from the research results of parallel efforts by other researchers. The operational experience of the SGMP was used to refine many design ideas.

Finally, all design proposals were prototyped and tested by the implementation experiences of multiple independent implementations. These independent implementations were tested for interoperability.

2 Architectural Principles

The SNMP design is based on correct architectural principles. There are three basic principles characterize the architectural selections which shaped the design of the SNMP: designed for ubiquity, engineered economy, and planned extensibility.

2.1 Designed for Ubiquity

Today's network management requirements demand end-to-end monitoring and control. The use of a single management scheme, including a singe management protocol, facilitates end-to-end management. This implies that the management system must be implemented on a wide range of platforms. SNMP-based network management is implementable and has been implemented on a wide range of platforms, from PCs to supercomputers.

2.2 Engineered Economy

The SNMP was engineered for economy. In particular, it is conservative in the memory and computational requirements placed on the management agents in the managed network elements (nodes). Conscious design decisions were made to place the greater demands on the systems in the network operations centers (NOCs) rather than on the agents. This was done for two important reasons. First, there are many more agents than NOCs. Second, this allows the network elements to focus their resources on their principle efforts rather than on network management overhead.

A concrete example of engineering for economy may be found in the selection of the presentation protocol. The SNMP utilizes a well-engineered subset of the Abstract Syntax Notation One (ASN.1) [5] and encoding rules [6] to concisely and unambiguously define the protocol and to convey the network management information in a widely understood and machine independent form. While the ASN.1 defines a several built-in data types and provides rich mechanisms for defining more data types, encodings of data types such as booleans and bit strings are unnecessary if data types such as integers and octet strings are supported. The SNMP makes obvious mappings in these cases. In addition, restrictions such as limiting the encoding of octet strings to the primitive form were made in the interest of minimizing code size and maximizing execution speed. The authors' and designers' experience is that large programs run slowly. These design decisions were examined carefully during the process and have not led to any practical limitations on the utility of the resulting design.

2.3 Planned Extensibility

Several extensibility "hooks" were designed into the SNMP system for network management. Among the most important is the mechanism for extending the management information base. A rigorous process is defined which allows the generation of new versions of the Internet standard MIB. New versions may declare old objects obsolete (but not delete their names to avoid possible naming conflicts), augment the definition of existing objects, or define entirely new objects. Mechanisms for vendor or enterprise specific extensions to the MIB are also defined.

3 Transport Paradigm

The SNMP uses a correct transport paradigm which is characterized by conservative expectations of the services provided by the underlying protocols. Most implementations of the SNMP are layered with the presentation layer stacked atop the User Datagram Protocol (UDP) [7] and Internet Protocol (IP) [8]. However, the SNMP can also utilize other transport protocols such as the Transmission Control Protocol (TCP) [9], the OSI Connectionless Transport Service (CLTS) [10], the OSI Transport Protocol Class 4 (TP4) or Class 0 (TP0) [11], and link layer or MAC layer protocols [12]. Experimentation has occured with several of these transport options. Of course, only those systems which share common protocol stacks will yield interoperable network management implementations.

The SNMP, like its predecessor the SGMP, works best with connectionless transport layers such as the UDP, CLTS, and MAC. Implementations based on these stacks are more robust in networks which are lossy and error prone. While connection oriented protocols may (but may not) be superior for system management functions, the robustness and survivability resulting from the use of a connectionless transport are key for network management protocols used for diagnosing and repairing problems in operating internets. In addition, the NOC remains in control of the retransmission strategy because there is not gratuitous retransmissions by the lower layers. As a result, the NOC controls the amount of network bandwidth to be allocated to the network management function.

4 SNMP Applications

The SNMP presently supports a wide range of applications. Some applications are used in network operations centers; others are agent applications.

4.1 NOC Applications

Many powerful, yet friendly SNMP-based tools for monitoring and controlling networks are available. Some of these tools utilize the powerful X-Windows system [13] on modern workstations. Some execute on entry level MSDOS systems. Finally, many others provide a command line interface and are available on a wide range of platforms. Several of these applications are quite mature, having been ported from the SGMP environment [14].

These applications have proven effective for the management of today's networks. Most of these tools address one or more of the five OSI functional management facilities [15]:

- fault management,
- performance management,
- configuration management,
- accounting management, and
- security management.

Most of the work to date has been in the areas of fault and performance management.

Production of new NOC applications based on the SNMP continues. For example, research is underway which investigates the use of dynamic SQL as a network management meta-language to provide powerful and portable user interfaces.

4.2 Agent Applications

The SNMP supports agent applications on a wide range of platforms. The SNMP is being used with many types of end systems. These end systems include hosts, workstations, terminal servers, and network connected printers.

In addition, the SNMP is being used to communicate network management information for many types of intermediate systems. These include physical layer devices such as fiber optic hubs, MAC layer devices such as bridges, gateways and routers, and other communications gear.

Proxy agents may be used for the monitoring and control of network elements which do not directly support the SNMP.

5 Standardization Status

The SNMP is both a declared standard and a *de facto* standard.

5.1 IAB Activities

The SNMP was declared a draft standard by the Internet Activities Board, the governing standards body for TCP/IP networking in March, 1988. After a period of successful deployment, the specification was elevated to recommended status in April, 1989.

5.2 Adoption of the Protocol

The SNMP is also a *de facto* standard as measured by the number of vendors producing products based on the protocol and the number of fielded systems. The growth continues. In the absence of interoperating and fielded competitive implementations, the SNMP is the only practical choice for the management of multivendor heterogeneous networks based on TCP/IP.

6 The Future

While the SNMP has a rich past and an expanding present, it is forward looking as well by implementing the common basis for network management of TCP/IP-based networks. The Internet standard SMI defines the rules for describing objects and the Internet standard MIB describes the syntax and semantics of the managed information. These rules should be independent of the management protocol used and will ease the long-term transition to OSI-based network management strategies once they are fully defined and implemented.

The many extensibility features which were included in the design in keeping with the evolving nature of network management technology afford other opportunities. While the SNMP was originally designed for the management of TCP/IP-based networks, it has successfully been used for the management of other networking technologies as well. This expansion beyond TCP/IP-based networks is likely to accelerate.

7 Lessons Learned

There are several important lessons which may be gleaned from the SNMP experience.

1. Implementation experience is essential. The implementation of the protocol **before** standardization gave opportunity to correct multiple flaws.
2. The powerful SNMP *get-next* operator provides functional requirements without the unnecessary overhead and drawbacks of a separate synchronization mechanism.
3. The request / response paradigm is sufficient. As a result, there is no need for imperative commands.
4. Trap directed polling is an effective network management technique.
5. Parsers and generators of a well engineered subset of ASN.1 may be implemented and executed with only modest impact on the network elements' memory and computational requirements.

8 Conclusion

Today's multivendor heterogeneous networks typically use TCP/IP as the protocol which provides interoperating networking implementations for the widest number of platforms. The SNMP is the protocol which makes those systems manageable. Consequently, systems produced and acquired for use in heterogeneous multivendor networks should implement TCP/IP and the SNMP.

References

[1] Jeffrey D. Case, Mark S. Fedor, Martin L. Schoffstall, and James R. Davin. A Simple Network Management Protocol. Request for Comments 1089, DDN Network Information Center, SRI International, April 1989.

[2] James R. Davin, Jeffrey D. Case, Mark S. Fedor, and Martin L. Schoffstall. A Simple Gateway Monitoring Protocol. Request for Comments 1028, DDN Network Information Center, SRI International, November 1987.

[3] Marshall T. Rose and Keith McCloghrie. Structure and Identification of Management Information for TCP/IP based internets. Request for Comments 1065, DDN Network Information Center, SRI International, August 1988.

[4] Keith McCloghrie and Marshall T. Rose. Management Information Base for Network Management of TCP/IP based internets. Request for Comments 1066, DDN Network Information Center, SRI International, August 1988.

[5] Information Processing — Open Systems Interconnection — Specification of Abstract Syntax Notation One (ASN.1). International Organization for Standardization, 1987. International Standard 8824.

[6] Information Processing — Open Systems Interconnection — Specification of basic encoding rules for Abstract Syntax Notation One (ASN.1). International Organization for Standardization, 1987. International Standard 8825.

[7] J. Postel. User Datagram Protocol. Request for Comments 768, DDN Network Information Center, SRI International, August 1980.

[8] Internet Protocol. DDN Protocol Handbook, Volume One: DoD Military Standard Protocols, DDN Network Information Center, SRI International, September 1981. MIL-STD 1777 (also available as ARPA Internet Request for Comments 791).

[9] Transmission Control Protocol. DDN Protocol Handbook, Volume One: DoD Military Standard Protocols, DDN Network Information Center, SRI International, September 1981. MIL-STD 1778 (also available as ARPA Internet Request for Comments 793).

[10] Information Processing Systems — Open Systems Interconnection — Connectionless Transport Service Definition. International Organization for Standardization, 1986. International Standard 8072/AD 1.

[11] Information Processing Systems — Open Systems Interconnection — Transport Service Definition. International Organization for Standardization, 1985. International Standard 8072.

[12] Martin L. Schoffstall, James R. Davin, Mark S. Fedor, and Jeffrey D. Case. SNMP over Ethernet. Request for Comments 1089, DDN Network Information Center, SRI International, February 1989.

[13] Robert W. Scheifler and Jim Gettys. The X Window System. *ACM Transactions on Graphics*, 5(2):79–109, April 1986. Special Issue on User Interface Software.

[14] Jeffrey D. Case, James R. Davin, Mark S. Fedor, and Martin L. Schoffstall. Introduction to the simple gateway monitoring protocol. *IEEE Network*, 2(2), March 1988.

[15] Information Processing Systems — Open Systems Interconnection: Basic Reference Model, 1984. International Standard 7498.