Network Working Group
Internet-Draft

April 1991
SNMP Working Group

IETF SNMP Working Group
Internet Draft
SNMP Communications Services

April 1991

Frank J. Kastenholz

1. Status of This Memo

This Internet Draft document will be submitted to the RFC editor for publication as an Informational RFC. The following is proposed as the status paragraph of the published RFC:

> This RFC is being distributed to members of the Internet community as an Informational RFC. The intent is to present a discussion on the issues relating to the communications services for SNMP. While the issues discussed may not be directly relevant to the research problems of the Internet, they may be interesting to a number of researchers and implementors.

Distribution of this memo is unlimited.

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

2. Introduction

This document discusses various issues to be considered when determining the underlying communications services to be used by an SNMP implementation.

As reported in RFC 1052, IAB Recommendations for the Development of Internet Network Management Standards [8], a two-prong strategy for network management of TCP/IP-based internets was undertaken. In the short-term, the Simple Network Management Protocol (SNMP), defined in RFC 1067, was to be used to manage nodes in the Internet community. In the long-term, the use of the OSI network management framework was to be examined. Two documents were produced to define the management information: RFC 1065, which defined the Structure of Management Information (SMI), and RFC 1066, which defined the Management Information Base (MIB). Both of these documents were designed so as to be compatible with both the SNMP and the OSI network management framework.

This strategy was quite successful in the short-term: Internet-based network management technology was fielded, by both the research and commercial communities, within a few months. As a result of this, portions of the Internet community became network manageable in a timely fashion.

In May of 1990, the core documents were elevated to "Standard Protocols" with "Recommended" status. As such, the Internet-standard network management framework consists of: Structure and Identification of Management Information for TCP/IP-based internets, RFC 1155 [9], which describes how managed objects contained in the MIB are defined; Management Information Base for Network Management of TCP/IP-based internets, which describes the managed objects contained in the MIB, RFC 1156 [10]; and, the Simple Network Management Protocol, RFC 1157 [1], which defines the protocol used to manage these objects.

In parallel with this activity, documents specifying how to transport SNMP messages over protocols other than UDP/IP have been developed and published: SNMP Over Ethernet [3], SNMP Over OSI [2], and SNMP Over IPX [6] and it would be suprising if more were not developed. These memos have caused a degree of confusion in the community. This document is intended to disperse that confusion by discussing the issues of relevance to an implementor when choosing how to encapsulate SNMP

packets.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

Experimental protocols. SNMP Over IPX [6] is an Internet Draft. Only the SNMP Specification [1] is an Internet Standard.

No single transport scheme can be considered the absolute best solution for all circumstances. This note will argue that, except for a very small set of special circumstances, operating SNMP over UDP/IP is the optimal scheme.

This document does not present a standard or a protocol for the Internet Community. For production use in the Internet the SNMP and its required communication services are specified in [1].

3. Standardization

Currently, the SNMP Specification [1] only specifies that the UDP protocol be used to exchange SNMP messages. While the IAB may standardize other protocols for use in exchanging SNMP messages in the future, only UDP is currently standardized for this purpose.

In order to claim full compliance with the SNMP Specification, an implementation would have to use UDP for SNMP message exchange.

4. Interoperability

Interoperability is the degree to which the equipment produced by one vendor can can operate with equipment produced by another vendor.

Related to Interoperability is compliance with a standard. Everything else being equal, a device that complies with some standard is more likely to be interoperable than a device that does not.

For commercial product development, the pros and cons of developing an interoperable product must be weighed and a choice made. Both engineering and marketing organizations participate in this process.

The Internet is the single largest market for SNMP systems. A large portion of SNMP systems will be developed with the Internet as a target environment. Therefore, it may be

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

the "Internet Standard" protocol. Therefore, in order to operate in the Internet and be managed in that environment on a production basis, a device must support SNMP over UDP/IP. This situation will lead to SNMP over UDP/IP being the most common method of operating SNMP. Therefore, the widest degree of interoperability and widest acceptance of a commercial product will be attained by operating SNMP over UDP/IP.

The preponderance of UDP/IP based network management stations also strongly suggests that an agent should operate SNMP over UDP/IP.

The results of the interoperability decision drive a number of technical decisions. If interoperability is desired, then SNMP must be operated over UDP/IP.

5. To Transport or Not To Transport

A major issue is whether SNMP should run on top of a transport-layer protocol (such as UDP) or not. Typically, the choice is to run over a transport/network/data link protocol or just run over the datalink. In fact, several protocols have been published for operating SNMP over several different datalink and transport protocols.

Operation of SNMP over a Transport and Network protocol stack is preferred. These protocols provide at least five functions that are of vital importance to the movement of SNMP packets through a network:

o Routing
  The network layer provides routing functions, which improves the overall utility of network management. The

  network has the ability to re-route packets around failed areas. This allows network management to continue operating during localized losses of service (It should be noted that these losses of service occur not only because of failures, but also for non-failure reasons such as preventive maintenance).

o Media Independence
  The network layer provides a high degree of media independence. By using this capability, many different types of network elements may be managed. Tying SNMP to a particular data link protocol limits the management scope of those SNMP entities to just those devices that use that datalink protocol.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

The end-to-end checksum provided by transport protocols improves the reliability of the data transfer.

o Multiplexing/Demultiplexing
Transport protocols provide multiplexing and demultiplexing services. These services facilitate the many-to-many management relationships possible with SNMP.

o Fragmentation and Reassembly
This is related to media independence. IP allows SNMP packets to transit media with differing MTU sizes. This capability is not available for datalink specific transmission schemes.

Fragmentation and Reassembly does reduce the overall robustness of network management since, if any single fragment is lost along the way, the operation will fail. The worse the network operates, the higher the probability that a fragment will get lost or delayed. For monitoring and data gathering while the network is operating normally, Fragmentation and Reassembly is not a problem. When the network is operating poorly (and the network operators are typically trying to diagnose and repair a failure), small packets should to be used, preventing the packet from being fragmented.

There are other services and functions that are provided by a connection oriented transport. These services and functions are not desired for SNMP. A later section will explore this

issue in more detail.

The main drawbacks that are cited with respect to using Transport and Network layers in the managed object are: a) Increased development time and b) Increased resource requirements. These arguments are less than compelling.

There are several excellent public domain or freely redistributable UDP/IP stacks that provide enough support for SNMP. The effort required to port the essential components of one of these stacks is small compared to the overall effort of installing the SNMP software.

The additional resources required in the managed object to support UDP/IP are minimal. CPU resources are required only when actually transmitting or receiving a packet. The largest single resource requirement of a UDP/IP is calculating the UDP checksum, which is very small compared to the cost of doing the ASN.1 encoding/decoding, Object Identifier lookup, and so on.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.