

A Simple Network Management Protocol

Table of Contents

1. Status of this Memo .....	2
2. Introduction .....	2
3. The SNMP Architecture .....	4
3.1 Goals of the Architecture .....	4
3.2 Elements of the Architecture .....	4
3.2.1 Scope of Management Information .....	5
3.2.2 Representation of Management Information .....	5
3.2.3 Operations Supported on Management Information .....	6
3.2.4 Form and Meaning of Protocol Exchanges .....	7
3.2.5 Definition of Administrative Relationships .....	7
3.2.6 Form and Meaning of References to Managed Objects ..	11
3.2.6.1 Resolution of Ambiguous MIB References .....	11
3.2.6.2 Resolution of References across MIB Versions.....	11
3.2.6.3 Identification of Object Instances .....	11
3.2.6.3.1 ifTable Object Type Names .....	12
3.2.6.3.2 atTable Object Type Names .....	12
3.2.6.3.3 ipAddrTable Object Type Names .....	13
3.2.6.3.4 ipRoutingTable Object Type Names .....	13
3.2.6.3.5 tcpConnTable Object Type Names .....	13
3.2.6.3.6 egpNeighTable Object Type Names .....	14
4. Protocol Specification .....	15
4.1 Elements of Procedure .....	16
4.1.1 Common Constructs .....	18
4.1.2 The GetRequest-PDU .....	19
4.1.3 The GetNextRequest-PDU .....	20
4.1.3.1 Example of Table Traversal .....	22
4.1.4 The GetResponse-PDU .....	23
4.1.5 The SetRequest-PDU .....	24
4.1.6 The Trap-PDU .....	26
4.1.6.1 The coldStart Trap .....	27
4.1.6.2 The warmStart Trap .....	27
4.1.6.3 The linkDown Trap .....	27
4.1.6.4 The linkUp Trap .....	27

4.1.6.5 The authenticationFailure Trap .....	27
4.1.6.6 The egpNeighborLoss Trap .....	27
4.1.6.7 The enterpriseSpecific Trap .....	28
5. Definitions .....	29
6. Acknowledgements .....	32
7. References .....	33

## 1. Status of this Memo

This memo defines a simple protocol by which management information for a network element may be inspected or altered by logically remote users. In particular, together with its companion memos which describe the structure of management information along with the initial management information base, these documents provide a simple, workable architecture and system for managing TCP/IP-based internets and in particular the Internet.

This memo specifies a draft standard for the Internet community. TCP/IP implementations in the Internet which are network manageable are expected to adopt and implement this specification.

Distribution of this memo is unlimited.

## 2. Introduction

As reported in [RFC 1052](#), IAB Recommendations for the Development of Internet Network Management Standards [1], the Internet Activities Board has directed the Internet Engineering Task Force (IETF) to create two new working groups in the area of network management. One group is charged with the further specification and definition of elements to be included in the Management Information Base (MIB). The other is charged with defining the modifications to the Simple Network Management Protocol (SNMP) to accommodate the short-term needs of the network vendor and operations communities, and to align with the output of the MIB working group.

The MIB working group has produced two memos, one which defines a Structure for Management Information (SMI) [2] for use by the managed objects contained in the MIB. A second memo [3] defines the list of managed objects.

The output of the SNMP Extensions working group is this memo, which incorporates changes to the initial SNMP definition [4] required to attain alignment with the output of the MIB working group. The changes should be minimal in order to be consistent with the IAB's directive that the working groups be "extremely sensitive to the need to keep the SNMP simple." Although considerable care and debate has gone into the changes to the SNMP which are reflected in this memo,

the resulting protocol is not backwardly-compatible with its predecessor, the Simple Gateway Monitoring Protocol (SGMP) [5]. Although the syntax of the protocol has been altered, the original philosophy, design decisions, and architecture remain intact. In order to avoid confusion, new UDP ports have been allocated for use by the protocol described in this memo.

### 3. The SNMP Architecture

Implicit in the SNMP architectural model is a collection of network management stations and network elements. Network management stations execute management applications which monitor and control network elements. Network elements are devices such as hosts, gateways, terminal servers, and the like, which have management agents responsible for performing the network management functions requested by the network management stations. The Simple Network Management Protocol (SNMP) is used to communicate management information between the network management stations and the agents in the network elements.

#### 3.1. Goals of the Architecture

The SNMP explicitly minimizes the number and complexity of management functions realized by the management agent itself. This goal is attractive in at least four respects:

- (1) The development cost for management agent software necessary to support the protocol is accordingly reduced.
- (2) The degree of management function that is remotely supported is accordingly increased, thereby admitting fullest use of internet resources in the management task.
- (3) The degree of management function that is remotely supported is accordingly increased, thereby imposing the fewest possible restrictions on the form and sophistication of management tools.
- (4) Simplified sets of management functions are easily understood and used by developers of network management tools.

A second goal of the protocol is that the functional paradigm for monitoring and control be sufficiently extensible to accommodate additional, possibly unanticipated aspects of network operation and management.

A third goal is that the architecture be, as much as possible, independent of the architecture and mechanisms of particular hosts or particular gateways.

#### 3.2. Elements of the Architecture

The SNMP architecture articulates a solution to the network management problem in terms of:

- (1) the scope of the management information communicated by the protocol,
- (2) the representation of the management information communicated by the protocol,
- (3) operations on management information supported by the protocol,
- (4) the form and meaning of exchanges among management entities,
- (5) the definition of administrative relationships among management entities, and
- (6) the form and meaning of references to management information.

### 3.2.1. Scope of Management Information

The scope of the management information communicated by operation of the SNMP is exactly that represented by instances of all non-aggregate object types either defined in Internet-standard MIB or defined elsewhere according to the conventions set forth in Internet-standard SMI [2].

Support for aggregate object types in the MIB is neither required for conformance with the SMI nor realized by the SNMP.

### 3.2.2. Representation of Management Information

Management information communicated by operation of the SNMP is represented according to the subset of the ASN.1 language [6] that is specified for the definition of non-aggregate types in the SMI.

The SGMP adopted the convention of using a well-defined subset of the ASN.1 language [6]. The SNMP continues and extends this tradition by utilizing a moderately more complex subset of ASN.1 for describing managed objects and for describing the protocol data units used for managing those objects. In addition, the desire to ease eventual transition to OSI-based network management protocols led to the definition in the ASN.1 language of an Internet-standard Structure of Management Information (SMI) [2] and Management Information Base (MIB) [3]. The use of the ASN.1 language, was, in part, encouraged by the successful use of ASN.1 in earlier efforts, in particular, the SGMP. The restrictions on the use of ASN.1 that are part of the SMI contribute to the simplicity espoused and validated by experience with the SGMP.

# 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.