Network Working Group
Request for Comments: 3410
Obsoletes: 2570
Category: Informational

J. Case
SNMP Research, Inc.
R. Mundy
Network Associates Laboratories
D. Partain
Ericsson
B. Stewart
Retired

December 2002

Introduction and Applicability Statements for Internet Standard Management Framework

Status of this Memo

Copyright Notice

Abstract

The purpose of this document is to provide an overview of the third version of the Internet-Standard Management Framework, termed the SNMP version 3 Framework (SNMPv3). This Framework is derived from and builds upon both the original Internet-Standard Management Framework (SNMPv1) and the second Internet-Standard Management Framework (SNMPv2).

The architecture is designed to be modular to allow the evolution of the Framework over time.

The document explains why using SNMPv3 instead of SNMPv1 or SNMPv2 is strongly recommended. The document also recommends that RFCs 1157, 1441, 1901, 1909 and 1910 be retired by moving them to Historic status. This document obsoletes RFC 2570.

Table of Contents

1. Introduction

This document is an introduction to the third version of the Internet-Standard Management Framework, termed the SNMP version 3 Management Framework (SNMPv3) and has multiple purposes.

First, it describes the relationship between the SNMP version 3 (SNMPv3) specifications and the specifications of the SNMP version 1 (SNMPv1) Management Framework, the SNMP version 2 (SNMPv2) Management Framework, and the Community-based Administrative Framework for SNMPv2.

Second, it provides a roadmap to the multiple documents which contain the relevant specifications.

Third, this document provides a brief easy-to-read summary of the contents of each of the relevant specification documents.

This document is intentionally tutorial in nature and, as such, may occasionally be "guilty" of oversimplification. In the event of a conflict or contradiction between this document and the more detailed documents for which this document is a roadmap, the specifications in the more detailed documents shall prevail.

Further, the detailed documents attempt to maintain separation between the various component modules in order to specify well-defined interfaces between them. This roadmap document, however, takes a different approach and attempts to provide an integrated view of the various component modules in the interest of readability.

This document is a work product of the SNMPv3 Working Group of the Internet Engineering Task Force (IETF).

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14, RFC 2119 [1].

2. The Internet Standard Management Framework

The third version of the Internet Standard Management Framework (the SNMPv3 Framework) is derived from and builds upon both the original Internet-Standard Management Framework (SNMPv1) and the second Internet-Standard Management Framework (SNMPv2).

All versions (SNMPv1, SNMPv2, and SNMPv3) of the Internet Standard Management SNMP Framework share the same basic structure and components. Furthermore, all versions of the specifications of the Internet Standard Management Framework follow the same architecture.

2.1. Basic Structure and Components

An enterprise deploying the Internet Standard Management Framework contains four basic components:

* several (typically many) managed nodes, each with an SNMP entity which provides remote access to management instrumentation (traditionally called an agent);

* at least one SNMP entity with management applications (typically called a manager),

* a management protocol used to convey management information between the SNMP entities, and

* management information.

The management protocol is used to convey management information between SNMP entities such as managers and agents.

This basic structure is common to all versions of the Internet Standard Management Framework; i.e., SNMPv1, SNMPv2, and SNMPv3.

2.2. Architecture of the Internet Standard Management Framework

The specifications of the Internet Standard Management Framework are based on a modular architecture. This framework is more than just a protocol for moving data. It consists of:

* a data definition language,

* definitions of management information (the Management Information Base, or MIB),

* a protocol definition, and

* security and administration.

Over time, as the Framework has evolved from SNMPv1, through SNMPv2, to SNMPv3, the definitions of each of these architectural components have become richer and more clearly defined, but the fundamental architecture has remained consistent.

One prime motivator for this modularity was to enable the ongoing evolution of the Framework, as is documented in RFC 1052 [2]. When originally envisioned, this capability was to be used to ease the transition from SNMP-based management of internets to management based on OSI protocols. To this end, the framework was architected

with a protocol-independent data definition language and Management Information Base along with a MIB-independent protocol. This separation was designed to allow the SNMP-based protocol to be replaced without requiring the management information to be redefined or reinstrumented. History has shown that the selection of this architecture was the right decision for the wrong reason -- it turned out that this architecture has eased the transition from SNMPv1 to SNMPv2 and from SNMPv2 to SNMPv3 rather than easing the transition away from management based on the Simple Network Management Protocol.

The SNMPv3 Framework builds and extends these architectural principles by:

* building on these four basic architectural components, in some cases incorporating them from the SNMPv2 Framework by reference, and

* by using these same layering principles in the definition of new capabilities in the security and administration portion of the architecture.

Those who are familiar with the architecture of the SNMPv1 Management Framework and the SNMPv2 Management Framework will find many familiar concepts in the architecture of the SNMPv3 Management Framework. However, in some cases, the terminology may be somewhat different.

3. The SNMPv1 Management Framework

The original Internet-Standard Network Management Framework (SNMPv1) is defined in the following documents:

* STD 16, RFC 1155 [3] which defines the Structure of Management Information (SMI), the mechanisms used for describing and naming objects for the purpose of management.

* STD 16, RFC 1212 [4] which defines a more concise description mechanism for describing and naming management information objects, but which is wholly consistent with the SMI.

* STD 15, RFC 1157 [5] which defines the Simple Network Management Protocol (SNMP), the protocol used for network access to managed objects and event notification. Note this document also defines an initial set of event notifications.

Additionally, two documents are generally considered companions to these three:

* STD 17, RFC 1213 [6] which contains definitions for the base set of management information

* RFC 1215 [7] defines a concise description mechanism for defining event notifications, which are called traps in the SNMPv1 protocol. It also specifies the generic traps from RFC 1157 in the concise notation.

These documents describe the four parts of the first version of the SNMP Framework.

3.1. The SNMPv1 Data Definition Language

The first two and the last document, i.e., RFCs 1155, 1212, and 1215, describe the SNMPv1 data definition language and are often collectively referred to as "SMIv1". Note that due to the initial requirement that the SMI be protocol-independent, the first two SMI documents do not provide a means for defining event notifications (traps). Instead, the SNMP protocol document defines a few standardized event notifications (generic traps) and provides a means for additional event notifications to be defined. The last document specifies a straight-forward approach towards defining event notifications used with the SNMPv1 protocol. At the time that it was written, use of traps in the Internet-Standard network management framework was controversial. As such, RFC 1215 was put forward with the status of "Informational", which was never updated because it was believed that the second version of the SNMP Framework would replace the first version.

3.2. Management Information

The data definition language described in the first two documents was first used to define the now-historic MIB-I as specified in RFC 1066 [8], and was subsequently used to define MIB-II as specified in RFC 1213 [6].

Later, after the publication of MIB-II, a different approach to the management information definition was taken from the earlier approach of having a single committee staffed by generalists work on a single document to define the Internet-Standard MIB. Rather, many mini-MIB documents were produced in a parallel and distributed fashion by groups chartered to produce a specification for a focused portion of the Internet-Standard MIB and staffed by personnel with expertise in those particular areas ranging from various aspects of network management, to system management, and application management.

3.3. Protocol Operations

The third document, STD 15 [5], describes the SNMPv1 protocol operations performed by protocol data units (PDUs) on lists of variable bindings and describes the format of SNMPv1 messages. The operators defined by SNMPv1 are: get, get-next, get-response, set-request, and trap. Typical layering of SNMP on a connectionless transport service is also defined.

3.4. SNMPv1 Security and Administration

STD 15 [5] also describes an approach to security and administration. Many of these concepts are carried forward and some, particularly security, are extended by the SNMPv3 Framework.

The SNMPv1 Framework describes the encapsulation of SNMPv1 PDUs in SNMP messages between SNMP entities and distinguishes between application entities and protocol entities. In SNMPv3, these are renamed applications and engines, respectively.

The SNMPv1 Framework also introduces the concept of an authentication service supporting one or more authentication schemes. In addition to authentication, SNMPv3 defines the additional security capability referred to as privacy. (Note: some literature from the security community would describe SNMPv3 security capabilities as providing data integrity, source authenticity, and confidentiality.) The modular nature of the SNMPv3 Framework permits both changes and additions to the security capabilities.

Finally, the SNMPv1 Framework introduces access control based on a concept called an SNMP MIB view. The SNMPv3 Framework specifies a fundamentally similar concept called view-based access control. With this capability, SNMPv3 provides the means for controlling access to information on managed devices.

However, while the SNMPv1 Framework anticipated the definition of multiple authentication schemes, it did not define any such schemes other than a trivial authentication scheme based on community strings. This was a known fundamental weakness in the SNMPv1 Framework but it was thought at that time that the definition of commercial grade security might be contentious in its design and difficult to get approved because "security" means many different things to different people. To that end, and because some users do not require strong authentication, the SNMPv1 architected an authentication service as a separate block to be defined "later" and the SNMPv3 Framework provides an architecture for use within that block as well as a definition for its subsystems.

4. The SNMPv2 Management Framework

The SNMPv2 Management Framework is described in [8-13] and coexistence and transition issues relating to SNMPv1 and SNMPv2 are discussed in [15].

SNMPv2 provides several advantages over SNMPv1, including:

* expanded data types (e.g., 64 bit counter)

* improved efficiency and performance (get-bulk operator)

* confirmed event notification (inform operator)

* richer error handling (errors and exceptions)

* improved sets, especially row creation and deletion

* fine tuning of the data definition language

However, the SNMPv2 Framework, as described in these documents, is incomplete in that it does not meet the original design goals of the SNMPv2 project. The unmet goals included provision of security and administration delivering so-called "commercial grade" security with:

* authentication: origin identification, message integrity, and some aspects of replay protection;

* privacy: confidentiality;

* authorization and access control; and

* suitable remote configuration and administration capabilities for these features.

The SNMPv3 Management Framework, as described in this document and the companion documents, addresses these significant deficiencies.

5. The SNMPv3 Working Group

This document, and its companion documents, were produced by the SNMPv3 Working Group of the Internet Engineering Task Force (IETF). The SNMPv3 Working Group was chartered to prepare recommendations for the next generation of SNMP. The goal of the Working Group was to produce the necessary set of documents that provide a single standard for the next generation of core SNMP functions. The single, most critical need in the next generation is a definition of security and administration that makes SNMP-based management transactions secure

in a way which is useful for users who wish to use SNMPv3 to manage networks, the systems that make up those networks, and the applications which reside on those systems, including manager-to-agent, agent-to-manager, and manager-to-manager transactions.

In the several years prior to the chartering of the Working Group, there were a number of activities aimed at incorporating security and other improvements to SNMP. These efforts included:

* "SNMP Security" circa 1991-1992 (RFC 1351 - RFC 1353),

* "SMP" circa 1992-1993, and

* "The Party-based SNMPv2" (sometimes called "SNMPv2p") circa 1993-1995 (RFC 1441 - RFC 1452).

Each of these efforts incorporated commercial grade, industrial strength security including authentication, privacy, authorization, view-based access control, and administration, including remote configuration.

These efforts fed the development of the SNMPv2 Management Framework as described in RFCs 1902 - 1908. However, the Framework described in those RFCs had no standards-based security and administrative framework of its own; rather, it was associated with multiple security and administrative frameworks, including:

* "The Community-based SNMPv2" (SNMPv2c) as described in RFC 1901 [16],

* "SNMPv2u" as described in RFCs 1909 and 1910, and

* "SNMPv2*."

SNMPv2c had the most support within the IETF but had no security and administration whereas both SNMPv2u and SNMPv2* had security but lacked a consensus of support within the IETF.

The SNMPv3 Working Group was chartered to produce a single set of specifications for the next generation of SNMP, based upon a convergence of the concepts and technical elements of SNMPv2u and SNMPv2*, as was suggested by an advisory team which was formed to provide a single recommended approach for SNMP evolution.

In so doing, the Working Group charter defined the following objectives:

* accommodate the wide range of operational environments with differing management demands;

* facilitate the need to transition from previous, multiple protocols to SNMPv3;

* facilitate the ease of setup and maintenance activities.

In the initial work of the SNMPv3 Working Group, the group focused on security and administration, including:

* authentication and privacy,

* authorization and view-based access control, and

* standards-based remote configuration of the above.

The SNMPv3 Working Group did not "reinvent the wheel", but reused the SNMPv2 Draft Standard documents, i.e., RFCs 1902 through 1908 for those portions of the design that were outside the focused scope.

Rather, the primary contributors to the SNMPv3 Working Group, and the Working Group in general, devoted their considerable efforts to addressing the missing link -- security and administration -- and in the process made invaluable contributions to the state-of-the-art of management.

They produced a design based on a modular architecture with evolutionary capabilities with emphasis on layering. As a result, SNMPv3 can be thought of as SNMPv2 with additional security and administration capabilities.

In doing so, the Working Group achieved the goal of producing a single specification which has not only the endorsement of the IETF but also has security and administration.

6. SNMPv3 Framework Module Specifications

The specification of the SNMPv3 Management Framework is partitioned in a modular fashion among several documents. It is the intention of the SNMPv3 Working Group that, with proper care, any or all of the individual documents can be revised, upgraded, or replaced as requirements change, new understandings are obtained, and new technologies become available.

Whenever feasible, the initial document set which defines the SNMPv3 Management Framework leverages prior investments defining and implementing the SNMPv2 Management Framework by incorporating by reference each of the specifications of the SNMPv2 Management Framework.

The SNMPv3 Framework augments those specifications with specifications for security and administration for SNMPv3.

The documents which specify the SNMPv3 Management Framework follow the same architecture as those of the prior versions and can be organized for expository purposes into four main categories as follows:

* the data definition language,

* Management Information Base (MIB) modules,

* protocol operations, and

* security and administration.

The first three sets of documents are incorporated from SNMPv2. The documents in the fourth set are new to SNMPv3, but, as described previously, build on significant prior related works.

6.1. Data Definition Language

The specifications of the data definition language include STD 58, RFC 2578, "Structure of Management Information Version 2 (SMIv2)" [17], and related specifications. These documents are updates of RFCs 1902 - 1904 [9-11] which have evolved independently from the other parts of the framework and were republished with minor editorial changes as STD 58, RFCs 2578 - 2580 [17-19] when promoted from Draft Standard to full Standard.

The Structure of Management Information (SMIv2) defines fundamental data types, an object model, and the rules for writing and revising MIB modules. Related specifications include STD 58, RFCs 2579, 2580.

STD 58, RFC 2579, "Textual Conventions for SMIv2" [18], defines an initial set of shorthand abbreviations which are available for use within all MIB modules for the convenience of human readers and writers.

STD 58, RFC 2580, "Conformance Statements for SMIv2" [19], defines the format for compliance statements which are used for describing requirements for agent implementations and capability statements which can be used to document the characteristics of particular implementations.

The term "SMIv2" is somewhat ambiguous because users of the term intend it to have at least two different meanings. Sometimes the term is used to refer the entire data definition language of STD 58, defined collectively in RFCs 2578 - 2580 whereas at other times it is used to refer to only the portion of the data definition language defined in RFC 2578. This ambiguity is unfortunate but is rarely a significant problem in practice.

6.2. MIB Modules

MIB modules usually contain object definitions, may contain definitions of event notifications, and sometimes include compliance statements specified in terms of appropriate object and event notification groups. As such, MIB modules define the management information maintained by the instrumentation in managed nodes, made remotely accessible by management agents, conveyed by the management protocol, and manipulated by management applications.

MIB modules are defined according to the rules defined in the documents which specify the data definition language, principally the SMI as supplemented by the related specifications.

There is a large and growing number of standards-track MIB modules, as defined in the periodically updated "Internet Official Protocol Standards" list [20]. As of this writing, there are more than 100 standards-track MIB modules with a total number of defined objects exceeding 10,000. In addition, there is an even larger and growing number of enterprise-specific MIB modules defined unilaterally by various vendors, research groups, consortia, and the like resulting in an unknown and virtually uncountable number of defined objects.

In general, management information defined in any MIB module, regardless of the version of the data definition language used, can be used with any version of the protocol. For example, MIB modules defined in terms of the SNMPv1 SMI (SMIv1) are compatible with the SNMPv3 Management Framework and can be conveyed by the protocols specified therein. Furthermore, MIB modules defined in terms of the SNMPv2 SMI (SMIv2) are compatible with SNMPv1 protocol operations and can be conveyed by it. However, there is one noteworthy exception: the Counter64 datatype which can be defined in a MIB module defined

in SMIv2 format but which cannot be conveyed by an SNMPv1 protocol engine. It can be conveyed by an SNMPv2 or an SNMPv3 engine, but cannot be conveyed by an engine which exclusively supports SNMPv1.

6.3. Protocol Operations and Transport Mappings

The specifications for the protocol operations and transport mappings of the SNMPv3 Framework are incorporated by reference to the two SNMPv2 Framework documents which have subsequently been updated.

The specification for protocol operations is found in STD 62, RFC 3416, "Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)" [21].

The SNMPv3 Framework is designed to allow various portions of the architecture to evolve independently. For example, it might be possible for a new specification of protocol operations to be defined within the Framework to allow for additional protocol operations.

The specification of transport mappings is found in STD 62, RFC 3417, "Transport Mappings for the Simple Network Management Protocol (SNMP)" [22].

6.4. SNMPv3 Security and Administration

The document series pertaining to SNMPv3 Security and Administration defined by the SNMPv3 Working Group consists of seven documents at this time:

RFC 3410, "Introduction and Applicability Statements for the Internet-Standard Management Framework", which is this document.

STD 62, RFC 3411, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks" [23], describes the overall architecture with special emphasis on the architecture for security and administration.

STD 62, RFC 3412, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)" [24], describes the possibility of multiple message processing models and the dispatcher portion that can be a part of an SNMP protocol engine.

STD 62, RFC 3413, "Simple Network Management Protocol (SNMP) Applications" [25], describes the five initial types of applications that can be associated with an SNMPv3 engine and their elements of procedure.

STD 62, RFC 3414, "User-Based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)" [26], describes the threats against which protection is provided, as well as the mechanisms, protocols, and supporting data used to provide SNMP message-level security with the user-based security model.

STD 62, RFC 3415, "View-based Access Control Model (VCAM) for the Simple Network Management Protocol (SNMP)" [27], describes how view-based access control can be applied within command responder and notification originator applications.

RFC 2576, "SNMPv3 Coexistence and Transition" [28], describes coexistence between the SNMPv3 Management Framework, the SNMPv2 Management Framework, and the original SNMPv1 Management Framework, and is in the process of being updated by a Work in Progress.

7. Document Summaries

The following sections provide brief summaries of each document with slightly more detail than is provided in the overviews above.

7.1. Structure of Management Information

Management information is viewed as a collection of managed objects, residing in a virtual information store, termed the Management Information Base (MIB). Collections of related objects are defined in MIB modules. These modules are written in the SNMP data definition language, which evolved from an adapted subset of OSI's Abstract Syntax Notation One (ASN.1) [29] language. STD 58, RFCs 2578, 2579, 2580, collectively define the data definition language, specify the base data types for objects, specify a core set of short-hand specifications for data types called textual conventions, and specify a few administrative assignments of object identifier (OID) values.

The SMI is divided into three parts: module definitions, object definitions, and notification definitions.

(1) Module definitions are used when describing information modules. An ASN.1 macro, MODULE-IDENTITY, is used to convey concisely the semantics of an information module.

(2) Object definitions are used when describing managed objects. An ASN.1 macro, OBJECT-TYPE, is used to convey concisely the syntax and semantics of a managed object.

(3) Notification definitions are used when describing unsolicited transmissions of management information. An ASN.1 macro, NOTIFICATION-TYPE, is used to convey concisely the syntax and semantics of a notification.

As noted earlier, the term "SMIv2" is somewhat ambiguous because users of the term intend it to have at least two different meanings. Sometimes the term is used to refer to the entire data definition language of STD 58, defined collectively in RFCs 2578 - 2580 whereas at other times it is used to refer to only the portion of the data definition language defined in RFC 2578. This ambiguity is unfortunate but is rarely a significant problem in practice.

7.1.1. Base SMI Specification

STD 58, RFC 2578 specifies the base data types for the data definition language, which include: Integer32, enumerated integers, Unsigned32, Gauge32, Counter32, Counter64, TimeTicks, INTEGER, OCTET STRING, OBJECT IDENTIFIER, IpAddress, Opaque, and BITS. It also assigns values to several object identifiers. STD 58, RFC 2578 further defines the following constructs of the data definition language:

* IMPORTS to allow the specification of items that are used in a MIB module, but defined in another MIB module.

* MODULE-IDENTITY to specify for a MIB module a description and administrative information such as contact and revision history.

* OBJECT-IDENTITY and OID value assignments to specify an OID value.

* OBJECT-TYPE to specify the data type, status, and the semantics of managed objects.

* SEQUENCE type assignment to list the columnar objects in a table.

* NOTIFICATION-TYPE construct to specify an event notification.

7.1.2. Textual Conventions

When designing a MIB module, it is often useful to specify, in a short-hand way, the semantics for a set of objects with similar behavior. This is done by defining a new data type using a base data type specified in the SMI. Each new type has a different name, and specifies a base type with more restrictive semantics. These newly defined types are termed textual conventions, and are used for the convenience of humans reading a MIB module and potentially by "intelligent" management applications. It is the purpose of STD 58,

RFC 2579, Textual Conventions for SMIv2 [18], to define the construct, TEXTUAL-CONVENTION, of the data definition language used to define such new types and to specify an initial set of textual conventions available to all MIB modules.

7.1.3. Conformance Statements

It may be useful to define the acceptable lower-bounds of implementation, along with the actual level of implementation achieved. It is the purpose of STD 58, RFC 2580, Conformance Statements for SMIv2 [19], to define the constructs of the data definition language used for these purposes. There are two kinds of constructs:

(1) Compliance statements are used when describing requirements for agents with respect to object and event notification definitions. The MODULE-COMPLIANCE construct is used to convey concisely such requirements.

(2) Capability statements are used when describing capabilities of agents with respect to object and event notification definitions. The AGENT-CAPABILITIES construct is used to convey concisely such capabilities.

Finally, collections of related objects and collections of related event notifications are grouped together to form a unit of conformance. The OBJECT-GROUP construct is used to convey concisely the objects in and the semantics of an object group. The NOTIFICATION-GROUP construct is used to convey concisely the event notifications in and the semantics of an event notification group.

7.2. Protocol Operations

The management protocol provides for the exchange of messages which convey management information between the agents and the management stations. The form of these messages is a message "wrapper" which encapsulates a Protocol Data Unit (PDU).

It is the purpose of STD 62, RFC 3416, "Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)" [21], to define the operations of the protocol with respect to the sending and receiving of the PDUs.

7.3. Transport Mappings

SNMP messages may be used over a variety of protocol suites. It is the purpose of STD 62, RFC 3417, "Transport Mappings for the Simple Network Management Protocol (SNMP)" [22], to define how SNMP messages

map onto an initial set of transport domains. Other mappings may be defined in the future.

Although several mappings are defined, the mapping onto UDP is the preferred mapping. As such, to provide for the greatest level of interoperability, systems which choose to deploy other mappings should also provide for proxy service to the UDP mapping.

7.4. Protocol Instrumentation

It is the purpose of STD 62, RFC 3418, "Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)" [30], to define managed objects which describe the behavior of portions of an SNMP entity.

7.5. Architecture / Security and Administration

It is the purpose of STD 62, RFC 3411, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks" [23], to define an architecture for specifying Management Frameworks. While addressing general architectural issues, it focuses on aspects related to security and administration. It defines a number of terms used throughout the SNMPv3 Management Framework and, in so doing, clarifies and extends the naming of:

* engines and applications,

* entities (service providers such as the engines in agents and managers),

* identities (service users), and

* management information, including support for multiple logical contexts.

The document contains a small MIB module which is implemented by all authoritative SNMPv3 protocol engines.

7.6. Message Processing and Dispatch (MPD)

STD 62, RFC 3412, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)" [24], describes the Message Processing and Dispatching for SNMP messages within the SNMP architecture. It defines the procedures for dispatching potentially multiple versions of SNMP messages to the proper SNMP Message Processing Models, and for dispatching PDUs to SNMP applications. This document also describes one Message Processing Model - the SNMPv3 Message Processing Model.

An SNMPv3 protocol engine MUST support at least one Message Processing Model. An SNMPv3 protocol engine MAY support more than one, for example in a multi-lingual system which provides simultaneous support of SNMPv3 and SNMPv1 and/or SNMPv2c. For example, such a tri-lingual system which provides simultaneous support for SNMPv1, SNMPv2c, and SNMPv3 supports three message processing models.

7.7. SNMP Applications

It is the purpose of STD 62, RFC 3413, "Simple Network Management Protocol (SNMP) Applications" [25] to describe the five types of applications which can be associated with an SNMP engine. They are: Command Generators, Command Responders, Notification Originators, Notification Receivers, and Proxy Forwarders.

The document also defines MIB modules for specifying targets of management operations (including notifications), for notification filtering, and for proxy forwarding.

7.8. User-based Security Model (USM)

STD 62, RFC 3414, the "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)" [26] describes the User-based Security Model for SNMPv3. It defines the Elements of Procedure for providing SNMP message-level security.

The document describes the two primary and two secondary threats which are defended against by the User-based Security Model. They are: modification of information, masquerade, message stream modification, and disclosure.

The USM utilizes MD5 [31] and the Secure Hash Algorithm [32] as keyed hashing algorithms [33] for digest computation to provide data integrity:

* to directly protect against data modification attacks,

* to indirectly provide data origin authentication, and

* to defend against masquerade attacks.

The USM uses loosely synchronized monotonically increasing time indicators to defend against certain message stream modification attacks. Automatic clock synchronization mechanisms based on the protocol are specified without dependence on third-party time sources and concomitant security considerations.

The USM uses the Data Encryption Standard (DES) [34] in the cipher block chaining mode (CBC) if disclosure protection is desired. Support for DES in the USM is optional, primarily because export and usage restrictions in many countries make it difficult to export and use products which include cryptographic technology.

The document also includes a MIB suitable for remotely monitoring and managing the configuration parameters for the USM, including key distribution and key management.

An entity may provide simultaneous support for multiple security models as well as multiple authentication and privacy protocols. All of the protocols used by the USM are based on pre-placed keys, i.e., private key mechanisms. The SNMPv3 architecture permits the use of symmetric and asymmetric mechanisms and protocols (asymmetric mechanisms are commonly called public key cryptography) but, as of this writing, there are no SNMPv3 security models on the IETF standards track that use public key cryptography.

Work is underway to specify how AES is to be used within the User-based Security Model (USM). This will be a separate document.

7.9. View-based Access Control (VACM)

The purpose of STD 62, RFC 3415, the "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)" [27], is to describe the View-based Access Control Model for use in the SNMP architecture. The VACM can simultaneously be associated in a single engine implementation with multiple Message Processing Models and multiple Security Models.

It is architecturally possible to have multiple, different, Access Control Models active and present simultaneously in a single engine implementation, but this is expected to be *_very_* rare in practice and *_far_* less common than simultaneous support for multiple Message Processing Models and/or multiple Security Models.

7.10. SNMPv3 Coexistence and Transition

The purpose of RFC 2576, "Coexistence between Version 1, Version 2, and Version 3 of the Internet-Standard Network Management Framework" [28], is to describe coexistence between the SNMPv3 Management Framework, the SNMPv2 Management Framework, and the original SNMPv1 Management Framework. In particular, this document describes four aspects of coexistence:

* Conversion of MIB documents from SMIv1 to SMIv2 format

* Mapping of notification parameters

* Approaches to coexistence between entities which support the various versions of SNMP in a multi-lingual network, in particular the processing of protocol operations in multi-lingual implementations, as well as behavior of proxy implementations

* The SNMPv1 Message Processing Model and Community-Based Security Model, which provides mechanisms for adapting SNMPv1 and SNMPv2c into the View-Based Access Control Model (VACM) [27]

8. Standardization Status

Readers should consult the latest version of the "Internet Official Protocol Standards" list [20] to determine the standardization status of any document.

However, the SNMPv3 Working Group explicitly requested that text be included in this document to amplify on the status of SMIv1, SNMPv1, and SNMPv2c.

8.1. SMIv1 Status

SMIv1, as described in STD 16, RFCs 1155 and 1212, was promoted to full Standard status in 1990 and has remained a Standard even after SMIv2 reached full Standard (see RFC 2026 [35] for more information about the Internet Standards Process). In many cases, a Standard is declared "Historic" when its replacement reaches full Standard. For example, MIB-1 [8] was declared "Historic" when MIB-2 [6] reached full Standard. Similarly, when SMIv2 reached full Standard, it might have been reasonable at that time to retire SMIv1 and declare it to be "Historic" but as the result of a conscious decision, STD 16, RFCs 1155 and 1212 continue to have the standardization status of full "Standard" but are not recommended. These documents were not declared "Historic" and remain on the standards track because they provide normative references for other documents on the standards track and cannot be declared "Historic" without rendering the documents which rely on them to also become "Historic". Consequently, STD 16 retains its standardization status but is not recommended because it has been superseded by the newer SMIv2 specifications which are identified somewhat later in this document.

On a pragmatic level, since about 1993 it has been wise for users of the data definition language to use SMIv2 for all new work because the realities of the marketplace have occasionally required the support of data definitions in both the SMIv1 and SMIv2 formats. While there are tools widely available at low cost or no cost to translate SMIv2 definitions to SMIv1 definitions, it is impractical

to build automatic tools that automatically translate SMIv1 definitions to SMIv2 definitions. Consequently, if one works in primarily SMIv2, the cost of providing data definitions in both SMIv1 and SMIv2 formats is trivial. In contrast, if one works primarily in SMIv1 format, providing data definitions in both SMIv1 and SMIv2 is significantly more expensive. The market requirements today for providing data definitions in SMIv1 format are greatly diminished when compared to those of 1993, and SMIv2 continues to be the strongly preferred format even though SMIv1 has not been declared "Historic". Indeed, the IETF currently requires that new MIB modules be written using SMIv2.

8.2. SNMPv1 and SNMPv2 Standardization Status

Protocol operations via SNMPv1 and SNMPv2c message wrappers support only trivial authentication based on plain-text community strings and, as a result, are fundamentally insecure. When the SNMPv3 specifications for security and administration, which include strong security, reached full Standard status, the full Standard SNMPv1, formerly STD 15 [5], and the experimental SNMPv2c specifications described in RFC 1901 [16] were declared Historic due to their weaknesses with respect to security and to send a clear message that the third version of the Internet Standard Management Framework is the framework of choice. The Party-based SNMPv2 (SNMPv2p), SNMPv2u, and SNMPv2* were either declared Historic circa 1995 or were never on the standards track.

On a pragmatic level, it is expected that a number of vendors will continue to produce and users will continue to deploy and use multi-lingual implementations that support SNMPv1 and/or SNMPv2c as well as SNMPv3. It should be noted that the IETF standards process does not control actions of vendors or users who may choose to promote or deploy historic protocols, such as SNMPv1 and SNMPv2c, in spite of known short-comings. However, it is not expected that vendors will produce nor that users will deploy multi-lingual implementations that support the Party-based SNMPv2p (SNMPv2p), SNMPv2u, or SNMPv2*.

Indeed, as described above, one of the SNMPv3 specifications for security and administration, RFC 2576, Coexistence between Version 1, Version 2, and Version 3 of the Internet-Standard Management Framework [28], addresses these issues.

Of course, it is important that users deploying multi-lingual systems with insecure protocols exercise sufficient due diligence to insure that configurations limit access via SNMPv1 and SNMPv2c appropriately, in keeping with the organization’s security policy, just as they should carefully limit access granted via SNMPv3 with a security level of no authentication and no privacy which is roughly

equivalent from a security point of view. For example, it is probably unwise to allow SNMPv1 or SNMPv2c a greater level of access than is provided to unauthenticated SNMPv3 users, e.g., it does not make sense to guard the front door with armed guards, trained attack dogs, moats and drawbridges while providing unfettered access through an open back door.

The SNMPv1 framework, SNMPv2 framework, and SNMPv2c had limited capabilities for administering the SNMPv1 and SNMPv2c protocols. For example, there are no objects defined to view and configure communities or destinations for notifications (traps and informs). The result has been vendor defined mechanisms for administration that range from proprietary format configuration files that cannot be viewed or configured via SNMP to enterprise specific object definitions. The SNMPv3 framework provides a rich standards-based approach to administration which, by design, can be used for the SNMPv1 and SNMPv2c protocols. Thus, to foster interoperability of administration of SNMPv1 and SNMPv2c protocols in multi-lingual systems, the mechanisms and objects specified in [25], [27], and [28] should be used to supplement or replace the equivalent proprietary mechanisms.

8.3. Working Group Recommendation

Based on the explanations above, the SNMPv3 Working Group recommends that RFCs 1157, 1441, 1901, 1909 and 1910 be reclassified as Historical documents.

9. Security Considerations

As this document is primarily a roadmap document, it introduces no new security considerations. The reader is referred to the relevant sections of each of the referenced documents for information about security considerations.

10. References

10.1. Normative References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March, 1997.

10.2. Informative References

[2] Cerf, V., "IAB Recommendations for the Development of Internet Network Management Standards", RFC 1052, April 1988.

[3] Rose, M. and K. McCloghrie, "Structure and Identification of Management Information for TCP/IP-based internets", STD 16, RFC 1155, May 1990.

[4] Rose, M. and K. McCloghrie, "Concise MIB Definitions", STD 16, RFC 1212, March 1991.

[5] Case, J., Fedor, M., Schoffstall, M. and Davin, J., "Simple Network Management Protocol", STD 15, RFC 1157, May 1990.

[6] McCloghrie, K. and M. Rose, "Management Information Base for Network Management of TCP/IP-based internets: MIB-II", STD 17, RFC 1213, March 1991.

[7] Rose, M., "A Convention for Defining Traps for use with the SNMP", RFC 1215, March 1991.

[8] McCloghrie, K. and M. Rose, "Management Information Base for Network Management of TCP/IP-based Internets", RFC 1156, March 1990.

[9] Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)", RFC 1902, January 1996.

[10] Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)", RFC 1903, January 1996.

[11] Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)", RFC 1904, January 1996.

[12] Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)", RFC 1905, January 1996.

[13] Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)", RFC 1906, January 1996.

[14] Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)", RFC 1907, January 1996.

[15] Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Coexistence between Version 1 and Version 2 of the Internet-Standard Network Management Framework", RFC 2576, January 1996.

[16] Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Introduction to Community-based SNMPv2", RFC 1901, January 1996.

[17] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M. and S. Waldbusser, "Structure of Management Information Version 2 (SMIv2)", STD 58, RFC 2578, April 1999.

[18] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M. and S. Waldbusser, "Textual Conventions for SMIv2", STD 58, RFC 2579, April 1999.

[19] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M. and S. Waldbusser, "Conformance Statements for SMIv2", STD 58, RFC 2580, April 1999.

[20] "Official Internet Protocol Standards", http://www.rfc-editor.org/rfcxx00.html also STD0001.

[21] Presuhn, R., Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3416, December 2002.

[22] Presuhn, R., Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Transport Mappings for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3417, December 2002.

[23] Harrington, D., Presuhn, R. and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", STD 62, RFC 3411, December 2002.

[24] Case, J., Harrington, D., Presuhn, R. and B. Wijnen, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3412, December 2002.

[25] Levi, D., Meyer, P. and B. Stewart, "Simple Network Management Protocol (SNMP) Applications", STD 62, RFC 3413, December 2002.

[26] Blumenthal, U. and B. Wijnen, "User-Based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)", STD 62, RFC 3414, December 2002.

[27] Wijnen, B., Presuhn, R. and K. McCloghrie, "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3415, December 2002.

[28] Frye, R., Levi, D., Routhier, S. and B. Wijnen, "Coexistence between Version 1, Version 2, and Version 3 of the Internet-Standard Network Management Framework", RFC 2576, March 2000.

[29] Information processing systems - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1), International Organization for Standardization. International Standard 8824, (December, 1987).

[30] Presuhn, R., Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3418, December 2002.

[31] Rivest, R., "Message Digest Algorithm MD5", RFC 1321, April 1992.

[32] Secure Hash Algorithm. NIST FIPS 180-1, (April, 1995) http://csrc.nist.gov/fips/fip180-1.txt (ASCII) http://csrc.nist.gov/fips/fip180-1.ps (Postscript)

[33] Krawczyk, H., Bellare, M. and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[34] Data Encryption Standard, National Institute of Standards and Technology. Federal Information Processing Standard (FIPS) Publication 46-1. Supersedes FIPS Publication 46, (January, 1977; reaffirmed January, 1988).

[35] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October, 1996.

11. Editors' Addresses

Jeffrey Case
SNMP Research, Inc.
3001 Kimberlin Heights Road
Knoxville, TN 37920-9716
USA

Phone: +1 865 573 1434
EMail: case@snmp.com

Russ Mundy
Network Associates Laboratories
15204 Omega Drive, Suite 300
Rockville, MD 20850-4601
USA

Phone: +1 301 947 7107
EMail: mundy@tislabs.com

David Partain
Ericsson
P.O. Box 1248
SE-581 12 Linkoping
Sweden

Phone: +46 13 28 41 44
EMail: David.Partain@ericsson.com

Bob Stewart
Retired

12. Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.