

# SNMPv3 White Paper

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

First, it describes the relationship between the SNMPv3 specifications and the specifications of the SNMPv1 Management Framework, the 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.

## 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, SNMPv2c, and SNMPv3) of the Internet-Standard Management Framework share the same basic structure and components. Furthermore, all versions of the specifications of the Internet-Standard Management Framework follow the same architecture.

## Basic Structure and Components

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

- Several (typically many) managed nodes, each with an SNMP entity that provides remote access to management instrumentation (traditionally called an agent)
- At least one SNMP entity with management applications (traditionally called a manager)
- A management protocol used to convey management information between the SNMP entities
- Management information

This basic structure is common to all versions of the Internet-Standard Management Framework (i.e., SNMPv1, SNMPv2c, and SNMPv3).

## 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 SNMPv2c, 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. 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 structured with a protocol-independent data definition language and Management Information Base along with a MIB-independent protocol. This separation was designed

## SNMPv3 White Paper

to allow the SNMP-based protocol to be replaced without requiring the management information to be redefined or re-instrumented. 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.

### **The SNMPv1 Management Framework**

The original Internet-Standard Network Management Framework (SNMPv1) consists of three documents:

- RFC 1155 defines the Structure of Management Information (SMI)--the mechanisms used for describing and naming objects for the purpose of management.
- RFC 1212 defines a more concise description mechanism, but is wholly consistent with the SMI.
- RFC 1157 defines the Simple Network Management Protocol (SNMP), the protocol used for network access to managed objects.

The first two of these documents describe the SNMPv1 data definition language. The third document describes the SNMPv1 protocol operations performed by protocol data units (PDUs) on lists of variable bindings. 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.

Many of the concepts found in the SNMPv3 security and administration are found in the SNMPv1 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 SNMPv3, the concept of an authentication service is expanded to include other services, such as privacy.

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.

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. However, at that time, it was thought 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

# SNMPv3 White Paper

end, and because some users do not require strong authentication, the SNMPv1 structured an authentication service as a separate block to be defined "later." The SNMPv3 Framework provides an architecture for use within that block, as well as a definition for its subsystems.

## The SNMPv2 Management Framework

The SNMPv2 Management Framework is fully described in RFCs 1902, 1903, 1904, 1905, 1906, and 1907. Coexistence and transition issues relating to SNMPv1 and SNMPv2 are discussed in RFC 1908.

SNMPv2 provides several advantages over SNMPv1:

- Expanded data types: 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 tuned data definition language

However, the SNMPv2 Framework, as described in RFCs 1902-1907, is incomplete in that it does not meet the original design goals of the SNMPv2 project. The unmet goals include 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

The SNMPv3 Management Framework, as described in RFCs 3410, 3411, 3412, 3413, 3414, and 3415, addresses the deficiencies in SNMPv2 relating to security and administration. Coexistence issues relating to SNMPv1, SNMPv2c, and SNMPv3 can be found in RFC 3416.

The SNMPv3 RFCs were produced by the SNMPv3 Working Group of the Internet Engineering Task Force (IETF). The SNMPv3 Working Group did not "reinvent the wheel," but reused the SNMPv2 Draft Standard documents (i.e., RFCs 1902 through 1908). As a result, SNMPv3 is SNMPv2 plus security and administration. The new features of SNMPv3 (in addition to those of SNMPv2 listed above) include:

- Security
  - authentication and privacy
  - authorization and access control
- Administrative Framework
  - naming of entities
  - people and policies
  - usernames and key management
  - notification destinations
  - proxy relationships
  - remotely configurable via SNMP operations

## 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.

# SNMPv3 White Paper

Whenever feasible, the document set that 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
- Security and administration.

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

## Data Definition Language

The specifications of the data definition language includes

- RFC 2578, "The Structure of Management Information Version 2 (SMIv2)" and related specifications. The Structure of Management Information (SMI) defines fundamental data types, an object model, and the rules for writing and revising MIB modules. Related specifications include RFC 2579 and RFC 2580.
- RFC 2579, "Textual Conventions for SMIv2," defines an initial set of shorthand abbreviations, which are available for use within all MIB modules for the convenience of human readers and writers.
- RFC 2580, "Conformance Statements for SMIv2," defines the format for compliance statements, which are used for describing requirements for agent implementations and capability statements that can be used to document the characteristics of particular implementations.

## MIB Modules

MIB modules usually contain object definitions, may contain definitions of notifications, and sometimes include compliance statements specified in terms of appropriate object groups. As such, MIB modules define the management information 1) maintained by the instrumentation in managed nodes, 2) made remotely accessible by management agents, 3) conveyed by the management protocol, and 4) manipulated by management applications.

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

There is a large and growing number of standards-based MIB modules as defined in the periodically updated list of standard protocols (RFC 2400). As of this writing, there are about 100 standards-based MIB modules with a total number of defined objects of approximately 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 are compatible with the SNMPv3 Management Framework and

## SNMPv3 White Paper

can be conveyed by the protocols specified therein. Conversely, with one notable exception, MIB modules defined using the SNMPv2 SMI are compatible with the SNMPv1 protocol operations. The exception is the new Counter64 datatype introduced in the SNMPv2 SMI: an SNMPv1 protocol engine is unable to convey data of this type.

### Protocol Operations and Transport Mappings

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

- The specification for protocol operations is found in RFC 1905, "Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)."
- The specification of transport mappings is found in RFC 1906, "Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)."

### SNMPv3 Security and Administration

The SNMPv3 document series defined by the Network Working Group consists of the following documents:

- RFC 3410, "Introduction and Applicability Statements for Internet Standard," provides an overview of SNMPv3.
- RFC 3411, "An Architecture for Describing SNMP Management Frameworks," describes the overall architecture with special emphasis on the architecture for security and administration.
- RFC 3412, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)," describes the possibly multiple message processing models and the dispatcher portion that can be a part of an SNMP protocol engine.
- RFC 3413, "Simple Network Management Protocol (SNMP) Applications," describes the five types of applications that can be associated with an SNMPv3 engine and their elements of procedure.
- RFC 3414, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)," describes the threats, mechanisms, protocols, and supporting data used to provide SNMP message-level security.
- RFC 3415, "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)," describes the VACM for use in the SNMP architecture.

### Architecture / Security and Administration

It is the purpose of the SNMPv3 Architecture document, RFC 3411, to define an architecture for defining SNMP 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 that is implemented by all authoritative SNMPv3 protocol engines. An authoritative engine is the receiver of a message if the message requires a response (such as a get or set) or the sender if the message does not require a response.

# SNMPv3 White Paper

## Message Processing and Dispatch (MPD)

RFC 3412, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)," 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. It also defines the procedures for dispatching PDUs to SNMP applications. This document 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, a multilingual system may provide simultaneous support of SNMPv3 and SNMPv1 and/or SNMPv2c.

## SNMPv3 Applications

It is the purpose of RFC 3413, "SNMPv3 Applications" to describe the five types of applications that can be associated with an SNMP engine. The applications 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.

## User-based Security Model (USM)

RFC 3414, the "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)," 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 that are defended against by the User-based Security Model. These threats are: modification of information, masquerade, message stream modification, and [optionally] disclosure.

- The USM utilizes MD5 and the Secure Hash Algorithm as keyed hashing algorithms 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) in the cipher block chaining mode (CBC) [optionally] to protect against disclosure.

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

A single protocol 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 symmetric cryptography (i.e., private key mechanisms). The SNMPv3 architecture admits the use of public key cryptography, but as of this writing, no SNMPv3 security models utilizing public key cryptography have been published.

## View-based Access Control (VACM)

The purpose of RFC 3415, the "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)," is to describe the View-based Access Control Model for use in the SNMP architecture. It defines the Elements of Procedure for controlling access to management

## SNMPv3 White Paper

information. This document also includes a MIB for remotely managing the configuration parameters for the View-based Access Control Model.

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, 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.