

Nucleus SNMP

A White Paper

Network Management

Networking has become an essential part of our lives. Networks of all types and sizes are in existence today. There are home networks that connect as few as two people and then there are networks of multinational organizations, which span the globe. Desktops, cell phones, automobiles and the equipment in our kitchen form a part of the diverse networked community. There is only one common thing about all networks: their operation is critical to its users.

Networks need to be monitored for inefficient resource utilization and signs of pending failures. They also require reconfiguration based on changing and expanding needs of its users without affecting performance, services provided and most importantly, the users themselves. Additionally, making the problem more interesting is an increasing proportion of networked devices that come without a console and can only be managed through a remote interface.

Without a single management tool, the benefits and reliability of such a complex and varied infrastructure cannot be realized.

Introduction to SNMP

The Simple Network Management Protocol (SNMP) is a standards-based protocol that provides a single interface for remotely managing all types of devices. SNMP uses the User Datagram Protocol (UDP) for its communication mechanism. There are three basic parts to the SNMP; the SNMP Agent, the SNMP Manager and the SNMP MIB.

An SNMP Agent is a module, which resides on the managed device and has access to a database on that device with management information, such as TCP/IP traffic statistics. This database is called the Management Information Base (MIB).

Using an SNMP Manager, users can monitor and manipulate management information on an SNMP agent in effect altering behavior of the device. Network managers can update routing tables, bring up or take down network interfaces and even perform application-specific operations such as adjusting the temperature settings in an office building. All of this is accomplished remotely by way of the SNMP manager to SNMP Agent to SNMP MIB communication mechanism. SNMP can virtually be used to manage any device as is illustrated in figure 1.

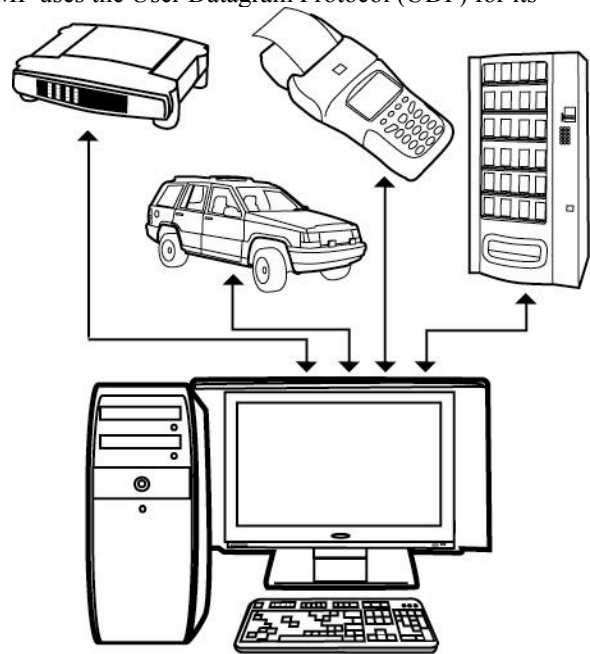


Figure 1

SNMPv1

The first version of SNMP came out in 1988 and defined operations to Get and Set entries in the Management Information Base. This allowed, for instance, the ability to retrieve the amount of time a device has been powered-up, or change security keys being used by the device's wireless interface. Also included was the ability to get the next element from the database. A "walk" or discovery of the MIBs on a SNMP Agent could be performed by executing repeated SNMP requests of Get-Next. Without knowing all

the entries in the database, an SNMP manager could sequentially walk the database, retrieving line after line of information, thus learning the available data.

Also part of the specification was a mechanism for an Agent to notify its Manager(s) about the occurrence of a certain event. In SNMP lingo, this action is called a trap. The trap could be one of the standard ones, for example, the linkUp trap which occurs when an interface is brought up, or it could be an enterprise specific trap defined for a particular application. For example, when the compressor fails on a remote refrigeration unit.

SNMPv2c

SNMPv2c was introduced in 1996 and provided quite a few operational enhancements to version 1. It expanded on the data types and included a 64-bit counter for recording rapidly increasing statistics. For example, to count the number of octets sent on a Giga-bit interface. The Get-Bulk operation was added, which enabled getting a “bulk” of next entries, as opposed to just one, as is the case with Get-Next. This reduced network traffic as well as increased throughput when large amounts of information had to be retrieved from the agent, during a walk for instance. Furthermore, the Set operation was enhanced to allow for addition and deletion of information in to the database. Error handling was also made richer providing more specific reasons for failure of a request.

SNMPv3

SNMPv3, which is the current IETF standard, was released in 2002, and has made obsolete both SNMPv1 and SNMPv2c. This improved version contains all the features present in the previous two versions of the protocol, plus it solves concerns about security. This is accomplished by incorporating authentication (origin identification, message integrity and some aspects of replay protection), privacy, authorization and access control. Remote configuration and administration of SNMP agents have also been added. Moreover, SNMPv3 defines a RFC for coexistence with SNMPv1 and SNMPv2c for situations in which a combination of versions is required.

How Nucleus SNMP Works

Nucleus SNMP is an optimized implementation of an SNMP Agent. It is easy to configure, while at the same time providing extensive options for customizing to a devices’ particular needs. For example, Nucleus SNMP can be built with support for only SNMPv3 or it can be built with support for SNMPv1, SNMPv2c and SNMPv3. Developers can opt to completely configure Nucleus SNMP’s administrative parameters at compile time or they can use the rich set of available APIs to administer the Agent at run-time--or a combination of the two. And last but not least, the SNMPv3 MIB can be used to remotely manage the SNMP engine itself.

Nucleus SNMP has been rigorously tested with third-party test suites to ensure complete conformance to IETF standards.

Management Information Base (MIB)

Structure of Management Information (SMI) is a specification for writing a Management Information Base (MIB). Each MIB document defines information that is stored on the SNMP Agent. Many standards based MIBs have been defined to manage various protocols (L2TP, Mobile IP, etc) and devices (Ethernet, WiFi, PPP, etc). Equipment manufacturer associations, like the North American Association of Food Equipment Manufacturers (NAFEM), have also released MIBs related to their industries. Furthermore, organizations can create their own enterprise-specific MIBs to describe information that is relevant to their hardware or application.

Supported MIBs

At the time of this writing, the following Nucleus products are provided with support for the listed MIBs:

- Nucleus NET (MIB-II, IP Tunnels MIB)
- Nucleus NETv6 (IPv6 MIB)
- Nucleus SNMP (SNMPv3 MIB)
- Nucleus RMON (RMON MIB)
- Nucleus PPP (PPP MIB)
- Nucleus L2TP (L2TP MIB)
- Nucleus 802.11 STA (802.11 MIB)
- Nucleus NAFEM (NAFEM MIB)

The list of supported MIBs is rapidly expanding and additional MIBs may have been added since this paper was published.

Developing a new MIB

Nucleus SNMP is shipped with a kit for rapid integration of MIBs. Using any off the shelf MIB compilers, developers can convert their MIBs into the popular MOSY format. A MOSY Compiler is shipped with Nucleus SNMP and is used to generate code for the Agent. With minor customizations to the generated code, the enterprise-specific MIB becomes accessible through Nucleus SNMP. Figure 2 demonstrates the flow for integrating new MIBs in to the SNMP Agent.

New MIBs are registered with the Agent using a run-time API, avoiding the need for re-compiling the SNMP library every time a new MIB is added or when modifications to an existing MIB are made.

Non-volatile storage

Using Nucleus FILE, or some type of off-line storage system, developers can save MIB information into non-volatile memory. SMI defines a storage-type object that is part of MIB entries and it indicates whether a particular entry should be saved to non-volatile storage. At initialization, the SNMP Agent reloads previously saved management information effectively maintaining its state from the last power down.

SNMP Operations

Nucleus SNMP has support for all three retrieval operations: Get, Get-Next and Get-Bulk. Get-Bulk has been defined in the SNMPv2c and SNMPv3 specifications, it is not available with SNMPv1. Set and Create requests have been completely implemented for all versions of SNMP.

Multiple variable bindings are also supported i.e., an SNMP Manager can send multiple objects in the same request. A Set or Create request with multiple variable bindings is treated as an atomic transaction; either all the instances specified are set or none are set. This avoids inconsistencies in data that may arise if some but not all values are successfully set.

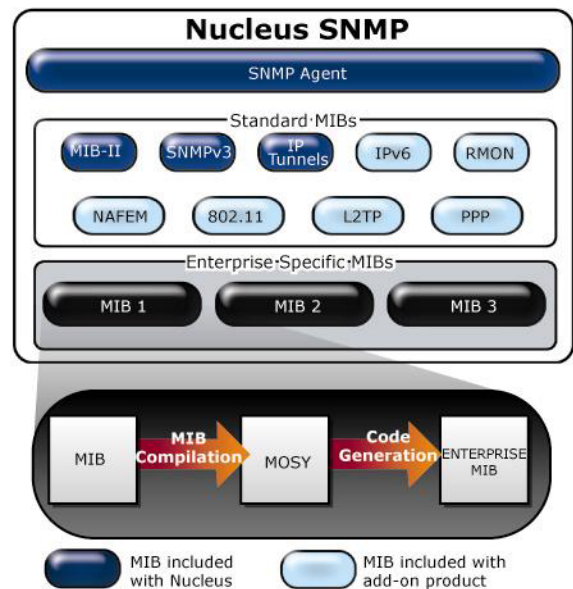


Figure 2

An API to send traps is provided. Administrative parameters determine receiving hosts and format of the trap message to be sent, including if any type of security should be used.

Security

Nucleus SNMP is shipped with the following security models:

- Community-Based Security Model for SNMPv1 (CBSMv1)
- Community-Based Security Model for SNMPv2 (CBSMv2)
- User-Based Security Model for SNMPv3 (USM)

The Community-Based Security Models use a SNMP Manager's IP address along with an unencrypted string to grant access to MIBs. They provide neither authentication nor privacy, i.e all data is transmitted in the clear. Also, since the SNMP Manager's IP address is the only item restricting who can access the SNMP agent from remote, this method is not very secure. Entire networks could be given access to the remote device if, for example, the network is behind a NAT router. Intruders could also easily spoof the SNMP Manager's IP address, thus gaining access to the remote device.

On the other hand, when using the USM, user-specific security keys can be used to sign and encrypt SNMP messages, keeping unwanted eyes from viewing possible sensitive information. Authentication is enforced, per SNMP manager, through a secured name and password mechanism. The following authentication and privacy algorithms are supported:

Authentication

- HMAC-MD5-96
- HMAC-SHA-96

Privacy

- CBC-DES encryption

Nucleus SNMP Agents can also benefit from hardware offloading of encryption and hashing algorithms, support for which is provided by the Nucleus Cipher Accelerator. Hardware offloading increases system and network performance by moving CPU-intensive software calculations to specialized hardware. Details on this subject are beyond the scope of this document but information is available from Accelerated Technology upon request.

Access Control

All versions of SNMP use the View-Based Access Control Model to determine privileges for different groups of users on the management information. Nucleus SNMP allows access rights to be defined right down to the level of an individual instance. It is therefore possible to allow a user to have read rights on all entries in a routing table, but permit write access on only a few of the entries.

Portability

Nucleus SNMP is tuned for applications where memory and CPU resources are limited. It is extremely portable, written in ANSI C and all that is required is a re-compile with the required tool set to port it to a new target platform.

RFC Support

The Nucleus SNMP supports following RFCs:

1. RFC 1157 - Simple Network Management Protocol (SNMP).

2. RFC 1901 - Introduction to Community-based SNMPv2.
3. RFC 1213 - Management Information Base for Network Management of TCP/IP-based Internets.
4. RFC 2011 - SNMPv2 Management Information Base for the Internet Protocol using SMIPv2.
5. RFC 2012 - SNMPv2 Management Information Base for the Transmission Control Protocol using SMIPv2.
6. RFC 2013 - SNMPv2 Management Information Base for the User Datagram Protocol using SMIPv2.
7. RFC 2863 - The Interfaces Group MIB.
8. RFC 2576 - Coexistence between Version 1, Version 2 and Version 3 of the Internet-standard Network Management Framework.
9. RFC 3410 - Introduction and Applicability Statements for Internet-Standard Management Framework.
10. RFC 3411 – An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks.
11. RFC 3412 - Message Processing and Dispatching for the Simple Network Management Protocol (SNMP).
12. RFC 3413 - Simple Network Management Protocol (SNMP) Applications - Partial Support:
 - i. Complete implementation of the Command Responder Application
 - ii. Partial (but compliant) implementation of the Notification Originator Application. Confirmed class PDUs not supported
 - iii. SNMP TARGET MIB and SNMP NOTIFICATION MIB only support reads
13. RFC 3414 - User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3).
14. RFC 3415 - View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP).
15. RFC 3416 - Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP).
16. RFC 3417 - Transport Mappings for the Simple Network Management Protocol (SNMP) – Partial Support:
 - i. Section 3: SNMP over UDP over IPv4
17. RFC 3418 - Management Information Base (MIB) for the Simple Network Management Protocol (SNMP).
18. RFC 3584 - Coexistence between Version 1, Version 2 and Version 3 of the Internet-standard Network Management Framework

Working with Nucleus Products

Nucleus SNMP is dependent on Nucleus PLUS and Nucleus NET. Nucleus FILE is required for non-volatile storage of MIBs. And if IPv6 connectivity is needed, Nucleus IPv6 is available as a plug-in to the networking stack.

Requirements

This section specifies the software, hardware and memory requirements of Nucleus SNMP.

Software Requirements

- Nucleus PLUS v1.14 or greater.
- Nucleus NET v5.1 or greater.
- Nucleus Cipher Suite v1.1 or greater (Full or Lite version – lite version included with Nucleus SNMPv3).
- Nucleus FILE v2.1 (or greater) is required for non-volatile storage support.

Hardware Requirements

There are no specific hardware requirements. Only that a network interface is present.

Memory Requirements

The memory requirements of Nucleus SNMP can vary considerably depending on the build configuration used. The RAM-ROM requirements sizes for Nucleus SNMP are available from Accelerated Technology. Please feel free to contact us at 800-468-6853 or info@acceleratedtechnology.com to receive this information.

Export Restraints

Nucleus SNMPv3 contains security algorithms; therefore export restraints apply. Please consult your local export laws for more information concerning the importation and/or exportation of encryption technology.