SNMP - Simple Network Management Protocol

Rene Brogatzki
Betreuer: Marc-Oliver Pahl
Seminar Innovative Internettechnologien und Mobilkommunikation SS2009
Lehrstuhl für Netzarchitekturen und Netzdienste
Fakultät für Informatik
Technische Universität München
Email: brogatzk@in.tum.de

***Abstract*— Today's networks grow in size and complexity. This includes physical devices like switches, routers or hosts and different types of protocols that deploy a networking environment. Considering many thousands of these components rises the problem of maintaining network performance. This document gives an introduction and solutions to the task of network management.**

***Index Terms*— Network Management, Structure of Management Information, SMI, Management Information Base, MIB, Simple Network Managemet Protocol, SNMP**

I. Introduction

Networks grow in size and complexity. In addition to this growth the number and variety of different components of modern networks (e.g. the Internet or corporate networks) increases as does the number of vendors. Every vendor developes its own network concepts and configuration tools. The increasing size of networks being administered demands more effort and money, to a point where a network might not be maintainable with affordable efforts concerning availability, security, manageability and quality of service. The Simple Network Management Protocol (SNMP) is intended to automate the task of network management.

This document is intended to give an introduction to problems, concepts and solutions of network management and an overview of the Simple Network Managment Protocol. The first section discusses the basics of network managment. The second section shows the development history of SNMP. Section three talks about the SNMP framework and takes closer look at its components. Section four gives information about practical apspects of network management with SNMP.

II. Basics of Network Managment

The importance of network management will be examplified by three real world scenarios:

A network administrator is assigned with the responsibility of a network. When a device or service fails an employee or customer might call in order to inform the IT department. The administrator will look for the problem and its solution. In this case the administrator acts *reactively*. Service unavailability causes high costs depening on duration and severity. If tools or services are available to the network administrator to discover malfunctions before they happen, precautionary measures can be taken before devices/services fail. This is called *proactive* action.

In order to be able to act proactively technology that is capable of indicating problems (monitoring) is required. Another example: An administrator observes traffic flows between network segments and discovers that moving a server from one segment to another could reduce overall network traffic. In this scenario information is gathered with e.g. a network sniffer. Observing a network with a network sniffer consisting of thousands of devices/services is not feasible.

A last example: A network administrator wants to be informed about suspicious traffic to specific hosts or ports. This could originate from an introuder, an attack or a port scan. *Prevention* of network security breaches is generally preferable to damage recovery.

The International Organization of Standardization (ISO) defined a model that describes different areas of network management in a structured way shown below. (The description is not intended to be exhaustive)

A. Performance Managment

The goal of performance management is measurement and analysis of link quality, network throughput and overall quality of service of network devices. Performance Management implements information gathering and storage. This is a central aspect of SNMP as will be shown later.

B. Fault Management

The goal of fault management is recognition, logging and elimination of error situations. Fault management can be understood as immediate response to faulty network conditions. The basis for appropriate fault management is well planned performance management. Gathering and storing is a key part of fault management so the border between fault management and performance management is smooth. SNMP facilitates fault management.

C. Configuration Managment

Configuration management enables network managers to monitor existing hard-/software and their configuration and to alter the configuration of devices on demand. This is a capability of SNMP.

D. Security Management

The goal of security management is controlling access to resources according to previously defined rules or policies (e.g. Common Creteria). Parts of security management are key infrastructures for cryptographic services and firewalls. Observation of services and devices can be implemented by SNMP.

E. Accounting Management

The goal of accounting management is to collect device and service access statistics for billing purposes. SNMP is rarely used for accounting management but monitoring information can be used for accounting purposes.

III. History of the Simple Network Management Protocol

This section shows the evolution of SNMP from version 1 over mutliple instances of version 2 to version 3, the latter being the current version of the Simple Network Management Protocol

In the late 1980s the internetworking community realized the demand of a coherent network management framework implementing the network management model described in the previous section.

At that time no unified standard existed. Protocols in use were the High Level Entity Management System (RFC 1021), the Simple Gateway Monitoring Protocol (RFC 1028) and the Common Management Information Protocol (CMIP ITU-T X.700). The mentioned protocols were either complex or designed for special purposes.

The Internet Architecture Board (IAB) released RFC 1052 "IAB Recommendations for the Development of Internet Network Management Standards". In this document the IAB set the general requirements for an Internet Standard Management Framework and assigned the Internet Engeneering Task Force (IETF) to work on an Internet Standard Management Framework. The assigned workgroup was to create a draft within 90 days. An easy framework was demanded that could be implemented and adopted by everyone who needed to address network management tasks. This means that no special requirements should be needed in order to use the framework. The design should be based on CMIP of the ISO to keep the design process short.

The next three sections describe the design process from version 1 to the current version 3 and briefly introduce key concepts of the framework

A. SNMPv1

Basic design decisions of the IETF for the Internet Standard Management Framework were based on the following four principles. The first principle is the separation of information and communication, which means that the protocol operations should be independent from the information transmitted avoiding complexity of the protocol itself (e.g the protocol operation should not change whether an integer or an IP address is submitted).

The second principle is to abstract and describe managed information in a consistent way not dependent on the information type.

The third principle is keeping the architecture as a whole modular to be able to developing or changing parts of the architecture without changing the whole framework.

The fourth goal was the demand of ease of implementation.In 1988 the definition of SNMPv1 was released in three RFCs.These RFCs document the basic components of the SNMPv1 framework. The first document describes the Structure of Management Information (SMI) [1] which is an abstract description language based on a subset of the Abstract Syntax Notation One (ASN.1). ASN.1 is a description language used for defining data and transmission of data. The SMI is used to describe the format of information transmitted and stored by SNMP. To represent, store and transmit information the second document defines the Management Information Base (MIB) [2]. The MIB in SNMPv1 consists of objects. An object is the smallest entity of information defined by the SMI. The third document describes actual protocol operations [3]. These three documents are the basic components of the architecture. They are independent from each other, as a consequence of the goal of a modular design. The three core parts will be further discussed in Section IV

B. SNMPv2

SNMPv1 was accepted by network administrators, as it solved the problems with network management. The functionality and mechanisms of SNMPv1 were revised and security weaknesses were discovered. Plain text transmission of passwords (Community Strings), a lack of authorisation, a lack of integrity checks and missing replay protection were points criticised by the community. These security flaws did not arise from a lack of knowledge rather than assumptions made during the design: The working group of the IETF assumed that information read and transmitted would not reveal information relevant to a possible attacker. Writable information was not considered to control fundamental devices/services of the network. The second assumption was that the aforementioned Community Strings would serve the need for security as they take the role of passwords for the managed network.

In consequence three aditional RFCs(1351,1352,1353) were released. These documents describe methods for authentication, integrity, privacy, authorisation. These extensions are known as SNMPsec. The focus on security made it more secure than its predecessor but did not achieve acceptance and was superseded by SNMPv2 [4]. SNMPv2 updated the Management Information Base(MIB-2) [5], which introduced the capability of grouping single MIB objects to represent devices as a whole. This enables network managers to define MIB entries for a kind of device/service and to reuse them for similar devices/services. The Structure of Management Information was revised to version 2 (SMIv2) to address the definition of MIB groups.

The development community was not able to achieve consensus concerning the security model to be used with version

2. Consequently it divided into different groups. One group implement a security model based on Community Strings. A Comunity String is a password which grants either read only or read-write acces permisson. Community String names are transmitted in clear text. Any attacker auditing the network traffic can read the name from passing traffic enabling him to view or alter SNMP information. Another group implemented the User-based Security Model (USM). This model makes use of a username with two associated cryptographic keys and protocols (e.g. DES,MD5). Both an agent and a NMS need to know the same username and its associated security context in order to exchange information. This lead to the following different instances of SNMPv2: SNMPv2, SNMPv2c, SNMPv2u and SNMPv2*. The different versions of SNMPv2 did not get adopted. [6] The disunity of the developers is considered to be the cause of this rejection. [6]

C. SNMPv3

The SNMP work group learned from the mistakes made when revising SNMPv1 and adapted to the demand for different security mechanisms. The SMIv2 and MIB2 got adopted. Further improvements were applied to the actual communication protocol. The security model may be USM or any older security model either with or without implementing the View-based Access Control Model (VACAM). VACAM handles access depending on the following factors: The username and group for general access control, where permission is bound to the group, the security protocol used for communication and permissions of the MIB. [7]. The second version of the communication protocol was adopted from SNMPv2 as was the MIB-2 and SMIv2. [6] Additional tools were added to assist the administration of SNMP. The standardisation process was finished in 2002 with RFC 3410-3418.

D. Remarks on versioning of SNMP

Usually a newer version of a RFC obsoletes older versions. This was not the case with further improvements of the SNMP framework, e.g. SNMPsec did not obsolete SNMPv1. This was addressed later, but did not change the fact that SNMPv1 is the most widely used version of the SNMP framework. This holds true for today. Though SNMPv3 is considered to be the technically most mature version.

IV. Simple Network Management Protocol Framework

The following sections describe the infrastructure of network management with SNMP. This describes the layout of a managed network and the different roles the single participants assume. The subsequent sections show the specific elements of the SNMP framework in detail. These are the SMI, the MIB and the protocol operations. The closing subsection will introduce basic security features SNMP is capable of.

Network management in context of SNMP is the ability to gather, store and alter information when needed. To acomplish this task the three aforementioned modules of SNMP work together, while using the infrastructure of the managed network itself, raising two problems: Dispatching too many network management tasks might affect network throughput and dispatching too less might lead to loss of important information. This decision depends on the network administrator [8]

The following four sections describe the core parts of SNMP beginning with an overview of different roles of participants of a SNMP network.

A. Infrastructure of network managment

A managed network consists of three basic parts. A host taking the role of the management station, a number of managed devices/services, called managed nodes, and the actual protocol operations enabling communication between stations (discussed later in this section). Fig. 1. gives an overview of this concept:

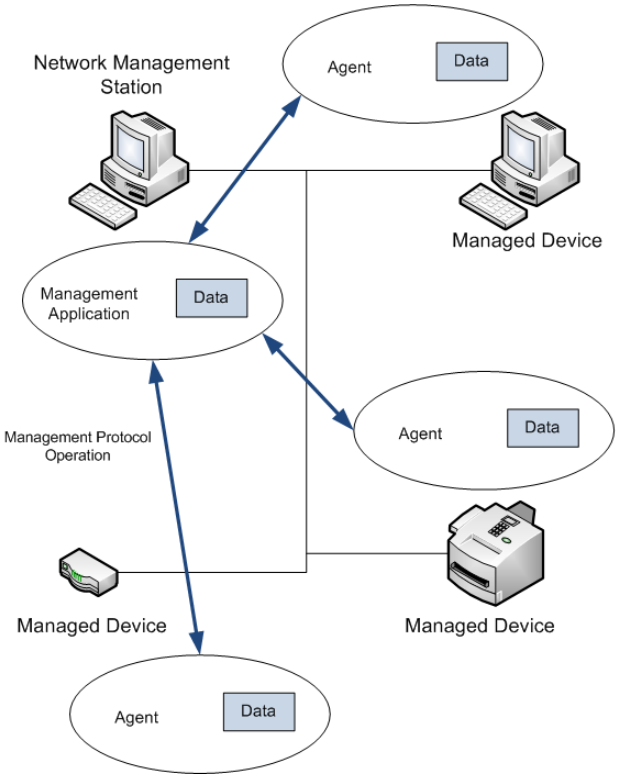

Fig. 1. Infrastructure of Network Management

The Network Management Station (NMS) consists of two software components: The management application - the interface between the managed network and the administration staff - and the database holding the managed information. This station collects, analyzes, processes and displays information from managed nodes as needed. The NMS reacts to the information collected either automatically or requested by the administrator in order to control the managed nodes of the network. The database of the NMS is a collection of MIB objects of managed nodes. This collection does not need to be exhaustive. If information is needed the NMS polls managed

nodes for it. All information centers at the NMS so the NMS is the place where network management takes place. [8]

Managed nodes are either physical devices or software services e.g. a webserver that is managed by the NMS. In order to facilitate network management functionality managed nodes include a sofware service called the agent and a set of MIB objects that describe the manageable information. The agent is the interface between the NMS and the remote physical device or software service. It receives incoming messages, processes them and dispatches answer messages, e.g. the NMS wants to know the uptime of the host therefore sending a message to the node to get the required data. The node receives the message, looks in its database for the appropriate value and generats a response message with the desired data and sending it to the NMS. [9]

Each node of a managed network holds managed information in the MIB in the form of single objects. The format of each object is defined by the SMI. The next two subsections will therefore introduce both concepts of SNMP in more detail.

B. SMIv2 and MIB2

The Structure of Management Information (SMI) is a language that is used to describe the format of managed information. It ensures that syntax and semantics of managed data are well defined and unambiguous. The SMI itself does not define management data of a managed system, it rather defines the format. As with object oriented programming the concept of a class relates to the abstract definition of a data type which is not usable until instantiated. The SMI is the syntax to define the format of managed information, whereas the instantiation of a class resulting in an usable object corresponds to the previously defined information as a MIB Object. To be able to describe a broad variety of manageable devices the SMI contains the necessary syntactical elements and data types (e.g. IpAddress, Counter, NetworkAddress, Integer, Octet String). The syntax below shows the exact definition of a MIB object that counts the successfully delivered datagrams to IP user protocols. Each MIB Object follows this scheme.

```
ipSystemStatsInDelivers OBJECT-TYPE
SYNTAX          Counter32
MAX-ACCESS      read-only
STATUS          current
DESCRIPTION
"The total number of datagrams successfully
    delivered to IP user-protocols"
::= { ipSystemStatsEntry 18 }
```

The individual syntactical elements of the example above will be explained briefly. Object identifier (OBJECT-TYPE) defines the name of the object. SYNTAX defines the data type of this object. In this case it is a 32-bit counter. MAX-ACCESS describes access control. It is either read-only or read-write. The STATUS element is used to indicate whether the object is up to date, obsoleted, mandatory or optional. Individual objects are revised over time and eventually obsolete so that they should not be implemented. The DESCRIPTION element contains human readable description text. The sample above is representative for the design of all basic MIB objects.

MIB objects are arranged in a hierarchical tree structure where a single object can be thought of as a variable of managed information. Fig. 2 shows a part of a tree to visualize its layout. Single objects are referenced via the number or the name separated by a dot. The IP module is addressed by the Objec identifier (OID) 1(ISO).3(org).6(dod).1(internet).2(mgmt).1(MIB-2).4(IP). The OID of the example object above is 1.3.6.1.2.1.4.18. The addressing is relevant when looking in more detail at the protocol operations, since a read-message would address managed information via the combination of the OID and the corresponding value of the object.

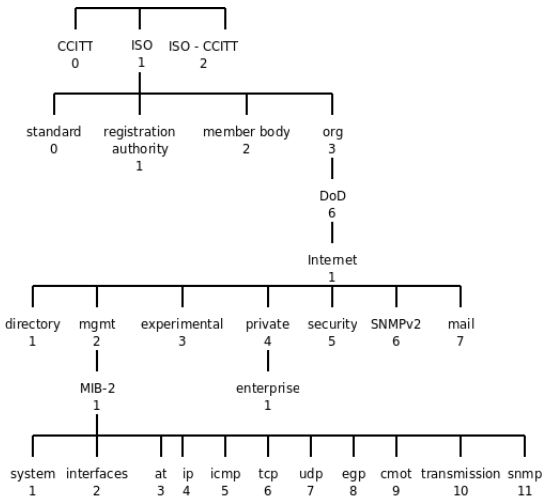

Fig. 2. Example view of the MIB Tree

With the next section the protocol operations shall be discussed to illustrate how network management with SNMP works in regards to communication between the NMS and managed nodes.

C. SNMP Protocol Operation

The role of SNMP is to grant access to management information requestable over the network. This includes read and write operations and an alert notification. This allows an administrator to look for or alter specific information. In order to automate the functionality of network management, SNMP uses two policies. The first policy constitutes polling for reading/writing access. Only NMSes can poll agents for values of objects and instruct them to alter one or more objects. The second policy enables an agent to inform the NMS autonomously of special events (alarms, interrupts). With the NMS polling an agent for read/write operations the communication model can be considered a server client model, where the agents act as servers since they respond to messages sent by a distant peer - the NMS.

The SNMP protocol operations reside on Layer 7 of the ISO/OSI referrence model. As transport service UDP is used on port 161 for read, write and response messages. Port 162 is used for trap messages. Only NMSes are supposed to listen

for traps. On the network layer the Internet Protocol is used. The payload of SNMP will be referred to as Protocol Data Units (PDU). [8]

When a NMS requests information it sends a GetRequest-PDU. The PDU consists of the address, an identifier of the message, which is an integer used to relate replys of managed nodes to requests sent previously by a NMS. This represents the header of the message. The payload of a Request-PDU contains the the OID of the requested object. The agent looks for the OID in its MIB on arrival of a message takes the value bound to the OID and sends a Response-PDU to the NMS. The NMS is now able to update the local MIB at the OID with the value sent. When a NMS needs more than one OID it can send an GetBulkRequest-PDU. The structure of the GetBulk-PDU is the same as with the GetRequest-PDU despite the fact that it contains more than one OID. The agent will respond the same way but the response contains more bindings of OID and value. If the agent could not locate a requested OID it is responding with a Response-PDU containing an error code describing the error condition.

For writing purposes the NMS sends SetRequest-PDUs. The structure is the same as with GetRequest-PDUs but it contains a value associated with an OID. The agent has to sent an response with either no error code indicating a successful change of the value or an error code describing the reason.

As mentioned before SNMP was designed to be flexible and usable on any kind of network therfore it is possible to use different transportation protocols, e.g. AppleTalk,TCP or IPX. [10]

D. Security

Considering a mechanism to monitor and control a network the mechanisms have to be protected agains possible attackers. Therefore SNMPv3 tries to achieve a set of security goals: Privacy is addressed with encryption of the SNMP-PDUs. The cyphersuite used is the Data Encryption Standard (DES) or Advanced Encryption Standard (AES)in Cipher-Block-Chaining-Mode (CBC). The administrator has to distribute the keys to all participating nodes.

Authentication is addressed with the utilization of a cryptographic hash function (e.g. MD5) and a secret but shared key. This mechnism is know as Hashed Message Authentication Code (HMAC). This mechanism concatenates the message with the secret key, which does not need to be the one used with DES, and then hashed. The hash value is concatenated to the message and sent. The receiver knows a key and is able to recalculate the hash. Do the results match with the transmitted HMAC the sender is authenticated. As a side effect this effect ensures the integrity a message, which means it can be decided if the message was altered during transfer.

Another security issue addressed by SNMP is the protection against reinjected old messages. This is called replay protection and might lead to inconsitent MIBs, which could lead to erroneous actions taken by the NMS. Therefor a value representing the uptime of the system is calculated and used as a timestamp. [8]

V. Conclusion

The Simple Network Management Protocol Framework is a tool for managing networks consisting of different devices and protocols. The modularity makes it extensible and flexible. The mistakes made with the design of version two are still visible as the insecure version 1 is still the most used one. An explanation might be the multiple, partially not standardised, revisions of version two. In comparision to other management tools and frameworks SNMP is the most widely deployed one of all available solutions, nevertheless newer technologies exist, e.g. Netconf, which focuses on managing configuration. A varity of tools implementing SNMP exist open source as commercial ones. Two examples of open source SNMP implementations are Net-SNMP and Nagios. Both implement the entire IETF framework specification.

References

[1] M. Rose and K. McCloghrie, "Structure and identification of management information for TCP/IP-based internets," RFC 1155 (Standard), Internet Engineering Task Force, May 1990. [Online]. Available: http://www.ietf.org/rfc/rfc1155.txt

[2] K. McCloghrie and M. Rose, "Management Information Base for network management of TCP/IP-based internets," RFC 1156 (Historic), Internet Engineering Task Force, May 1990. [Online]. Available: http://www.ietf.org/rfc/rfc1156.txt

[3] J. Case, M. Fedor, M. Schoffstall, and J. Davin, "Simple Network Management Protocol (SNMP)," RFC 1157 (Historic), Internet Engineering Task Force, May 1990. [Online]. Available: http://www.ietf.org/rfc/rfc1157.txt

[4] J. Case, K. McCloghrie, M. Rose, and S. Waldbusser, "Introduction to version 2 of the Internet-standard Network Management Framework," RFC 1441 (Historic), Internet Engineering Task Force, Apr. 1993. [Online]. Available: http://www.ietf.org/rfc/rfc1441.txt

[5] K. McCloghrie and M. Rose, "Management Information Base for Network Management of TCP/IP-based internets:MIB-II," RFC 1213 (Standard), Internet Engineering Task Force, Mar. 1991, updated by RFCs 2011, 2012, 2013. [Online]. Available: http://www.ietf.org/rfc/rfc1213.txt

[6] C. M. Kozierok, "The TCP/IP Guide," Book, Oct. 2005.

[7] B. Wijnen, R. Presuhn, and K. McCloghrie, "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)," RFC 3415 (Standard), Internet Engineering Task Force, Dec. 2002. [Online]. Available: http://www.ietf.org/rfc/rfc3415.txt

[8] J. F. Kurose and K. W. Ross, "Computernetwerke," Book, 2008.

[9] J. Case, D. Harrington, R. Presuhn, and B. Wijnen, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)," RFC 3412 (Standard), Internet Engineering Task Force, Dec. 2002. [Online]. Available: http://www.ietf.org/rfc/rfc3412.txt

[10] R.Presuhn, "Transport Mappings for the Simple Network Management Protocol (SNMP)," RFC 3417 (Standard), Internet Engineering Task Force, Dec. 2002, updated by RFC 4789. [Online]. Available: http://www.ietf.org/rfc/rfc3417.txt

[11] J. Case, R. Mundy, D. Partain, and B. Stewart, "Introduction and Applicability Statements for Internet-Standard Management Framework," RFC 3410 (Informational), Internet Engineering Task Force, Dec. 2002. [Online]. Available: http://www.ietf.org/rfc/rfc3410.txt

[12] D. Harrington, R. Presuhn, and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks," RFC 3411 (Standard), Internet Engineering Task Force, Dec. 2002, updated by RFC 5343. [Online]. Available: http://www.ietf.org/rfc/rfc3411.txt

[13] D. Levi, P. Meyer, and B. Stewart, "Simple Network Management Protocol (SNMP) Applications," RFC 3413 (Standard), Internet Engineering Task Force, Dec. 2002. [Online]. Available: http://www.ietf.org/rfc/rfc3413.txt

[14] U. Blumenthal and B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)," RFC 3414 (Standard), Internet Engineering Task Force, Dec. 2002. [Online]. Available: http://www.ietf.org/rfc/rfc3414.txt

[15] R. Presuhn, “Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP),” RFC 3416 (Standard), Internet Engineering Task Force, Dec. 2002. [Online]. Available: http://www.ietf.org/rfc/rfc3416.txt
[16] R.Presuhne, “Management Information Base (MIB) for the Simple Network Management Protocol (SNMP),” RFC 3418 (Standard), Internet Engineering Task Force, Dec. 2002. [Online]. Available: http://www.ietf.org/rfc/rfc3418.txt
[17] R. Frye, D. Levi, S. Routhier, and B. Wijnen, “Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework,” RFC 3584 (Best Current Practice), Internet Engineering Task Force, Aug. 2003. [Online]. Available: http://www.ietf.org/rfc/rfc3584.txt