The continuation of a success story

SNMP Version 3:

The Continuation of a Success Story

With the new Version 3 of SNMP, the Simple Network Management Protocol from the Internet Engineering Task Force (IETF), many wishes from the user's side have been fulfilled. Especially with regard to the lack in security SNMP Version 1 has neither means to guarantee a secure transmission of management commands nor a secure implementation of management applications without potential threats. SNMP Version 3 will cover all these needs and more: it comes with a well structured network management architecture which will meet the requirements of the growing SNMP users community much better than the previous two versions. This article describes the major parts of the new SNMP architecture with a strong focus on the new features which many SNMP users have been waiting for since years.

RÜDIGER SELLIN, BERN

The SNMP History

SNMP Version 1 (SNMPv1) has been very successful over the past decade. After the standard was launched in May 1990, SNMP gained more and more success especially on the LAN market (Local Area Network). Only after a few years more than 50 LAN equipment suppliers supported SNMP by putting SNMP Agents on their routers, bridges, servers and hosts (figure 1). It was the first time where systems management with one single management protocol became possible. Coupling this major advantage with SNMP's simplicity there were almost no doubts that SNMP is the industry standard management protocol for almost every multivendor LAN environment. Being that successful in the LAN market segment, SNMP increasingly got a foot into the WAN markets door (Wide Area Network). Many major data communications suppliers (like Cisco or Ascend) who offer or computer manufacturers (like IBM) who use data communications equipment, deliver global solutions for broadband communications e.g. for ATM networks in both segments, LANs and WANs. Therefore it was only a question of time as to when SNMPv1 would become a simple and easy-to-implement option for telecommunication networks as well.

But it appeared that the telecommunication market followed its own rules. On the one hand WANs normally are of a bigger size than LANs which requires much more powerful network management tools for the WAN. SNMPv1 did not always meet these requirements, especially with regard to its lack of performance and security. On the other hand the popularity of SNMP increased at the management interface towards the Telco's customers, better known as "Customer Network Management (CNM)". Because business customers predominantly use SNMP to manage their LANs, it was obvious to use SNMP to monitor the resources rented from the Telcos (e.g. leased lines).

Another important point where SNMP is increasingly used is on the element management level of the TMN's logical layered architecture (TMN: Telecommunications Management Network, an architecture developed by ITU-T for the management of public telecom networks). At

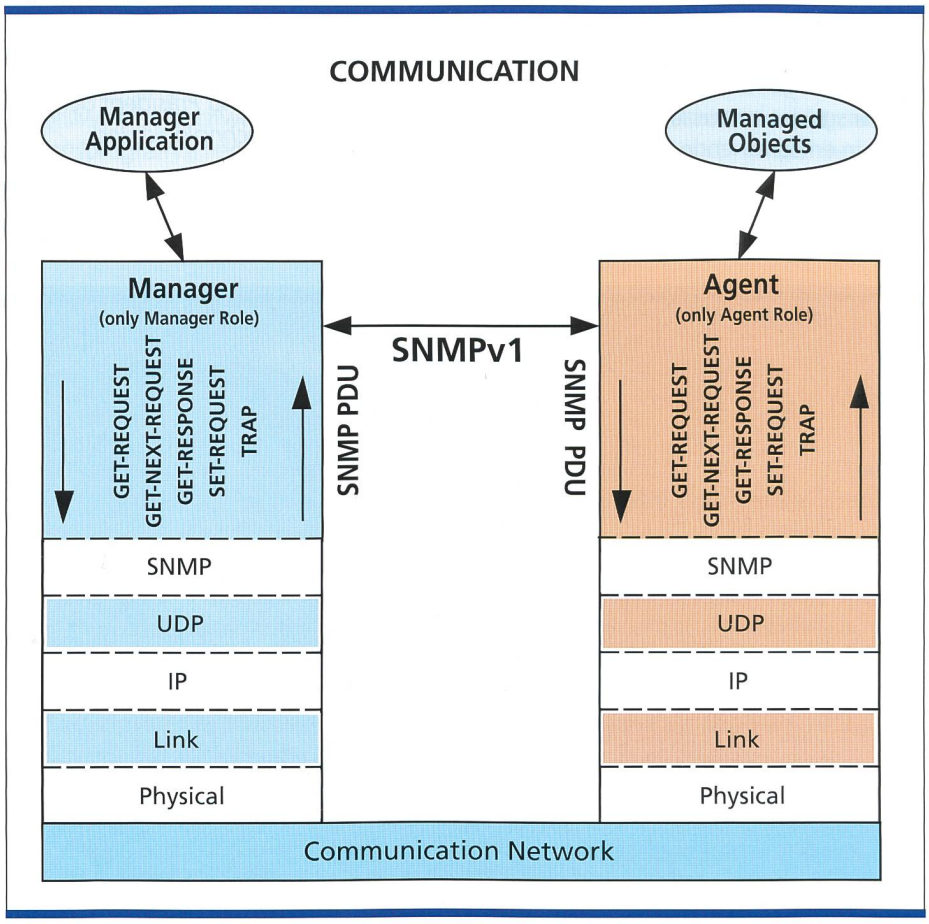

Fig. 1. Communication between manager and agent via SNPMv1. Abbreviations: SNMP: Simple Network Management Protocol; UDP: User Datagram Protocol; IP: Internet Protocol; PDU: Protocol Data Unit.

the beginning of its development, TMN was inadequate when it came to the detailed management of network elements. Quite often the appropriate information models needed for the use of CMIP (Common Management Information Protocol) where not available at all or not implemented in time. Thus in today's telecom's management environment both protocols, SNMP and CMIP are in use for different purposes, SNMP for the element management and CMIP for the overall network management. CORBA (Common Object Request Broker Architecture) may provide the bridge between CMIP and SNMP.

With the development of SNMP's version 2 (SNMPv2), the IETF tried to extend the capabilities of SNMPv1 by adding

- new PDUs (Protocol Data Units) for the transfer of bulk data (GET_BULK PDU) and for the manager-to-manager communication (INFORM PDU), see figure 2, and
- a new security concept.

Especially the new security concept which was developed between 1991 and 1992 (see [RFC 1351 to RFC 1353]) drew the attention of the SNMP users because SNMPv1's recognised lack of security. But SNMPv2's misfortune was that the U.S. DoD (Department of Defence) which still has its hands on the Internet did not agree to publish the security part of SNMPv2 due to export rules within the USA. After a longer period of debating the ongoing negotiations between the participating parties did not lead to an acceptable compromise, so SNMPv2 was published without the security part. Therefore, the needs of the growing SNMP user's community still were not met. In addition, many dialects of SNMPv2 appeared on the market which more or less led to an incompatibility. (For further details, see below under the chapter "SNMP Protocol Versions".)

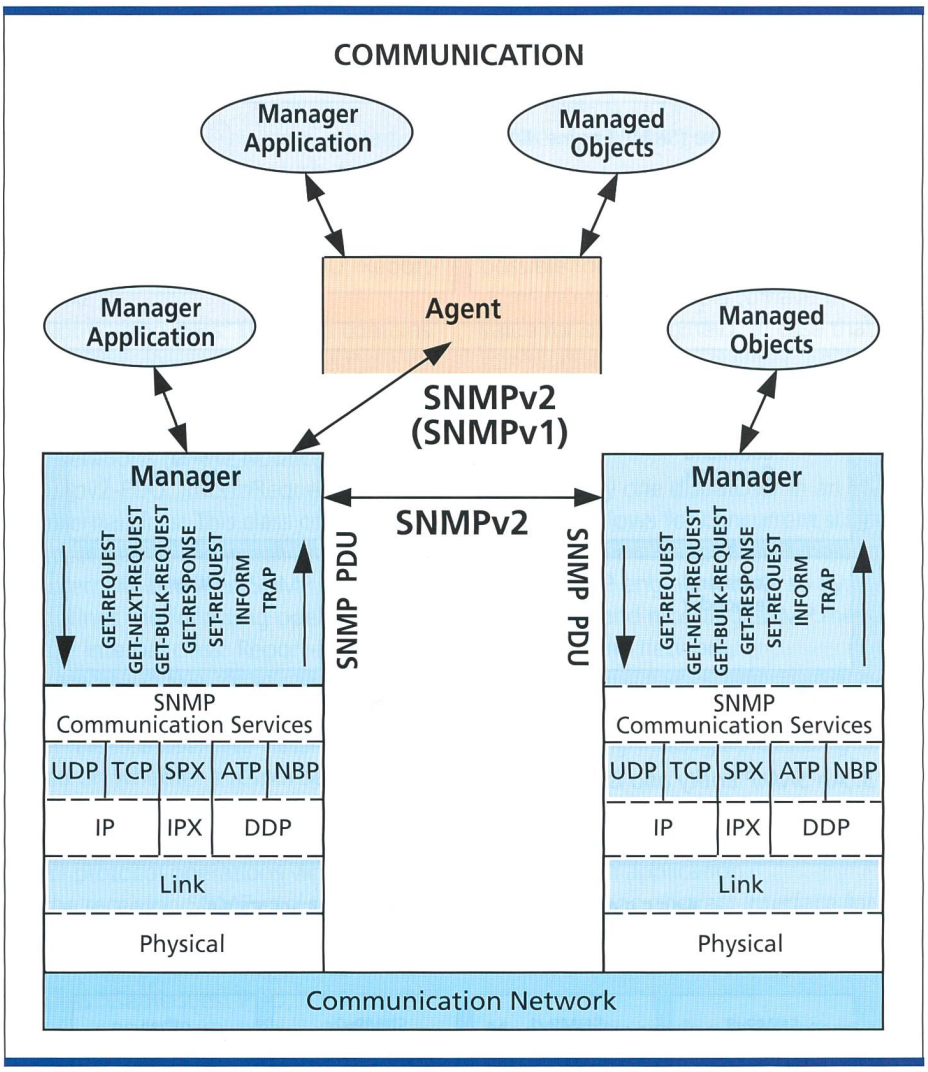

Fig. 2. Communication between Manager and agent via SNMPv2. Abbreviations: UDP: User Datagram Protocol; TCP: Transport Control Protocol; IP: Internet Protocol; PDU: Protocol Data Unit; SPX: Internet Packet Exchange; NBP: Name Binding Protocol; DDP: Datagram Delivery Protocol (SDX and IPX are Novell, NBP, ATP and DDP are Apple).

Architecture of SNMP Version 3 (SNMPv3)

Considering the above mentioned background it is no surprise that the specifications for SNMPv3 were developed under high expectations. Therefore, the architecture for SNMPv3 has to meet all the requirements which already were stated for SNMPv2, and it has to be in a way flexible to be backwards compatible at least with SNMPv1 and the "official" IETF specification of SNMPv2.

In general, an SNMP management system contains:

- several (potentially many) nodes, each with an SNMP entity containing command responder and notification originator applications, which have access to management information (traditionally called Agents);
- at least one SNMP entity containing command generator and/or notification receiver applications (traditionally called a Manager),
- a management protocol (here SNMP), used to convey management information between the SNMP entities, and
- the management information itself which is stored in a MIB (Management Information Base).

Note that 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.

Thinking in object-oriented terms, an SNMP "MIB" is organised as a table where the entries in this table are considered as the "Managed Objects". It should be noted that in this context "MIB" and "Managed Objects" have different meanings compared to a CMIP environment. Where with SNMP the entries in the table (values) are set or changed, CMIP in fact manages Managed Objects which are abstract representations of real managed resources. Thus, SNMP is closer linked to the reality, the managed element. SNMP entities execute command generators, and notification receiver applications monitor and

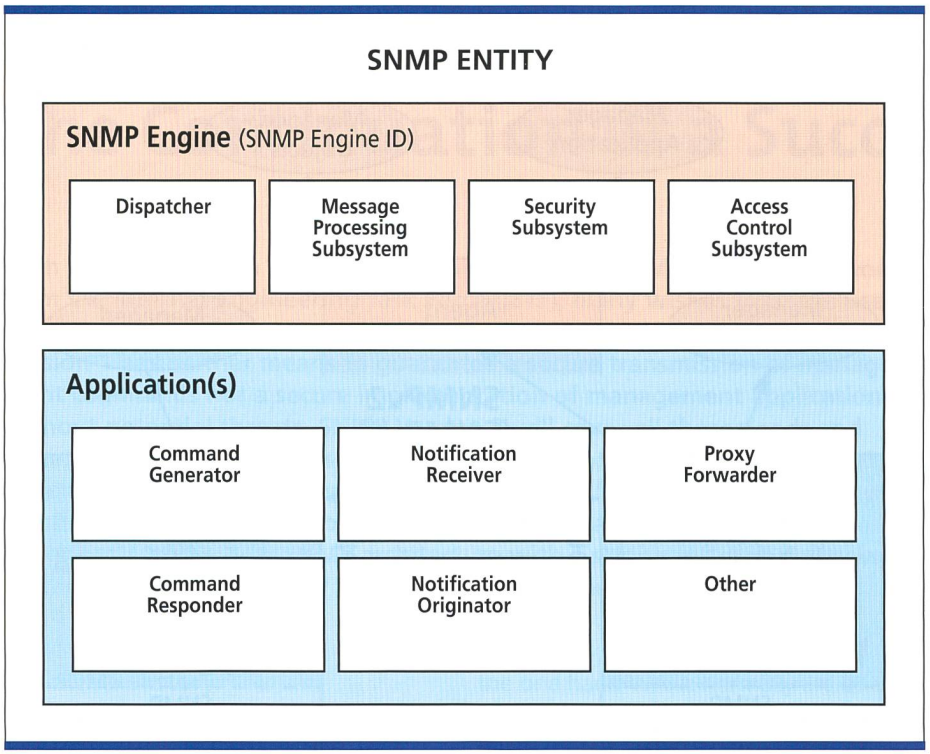

Fig. 3. An SNMP Entity and ist compenents.

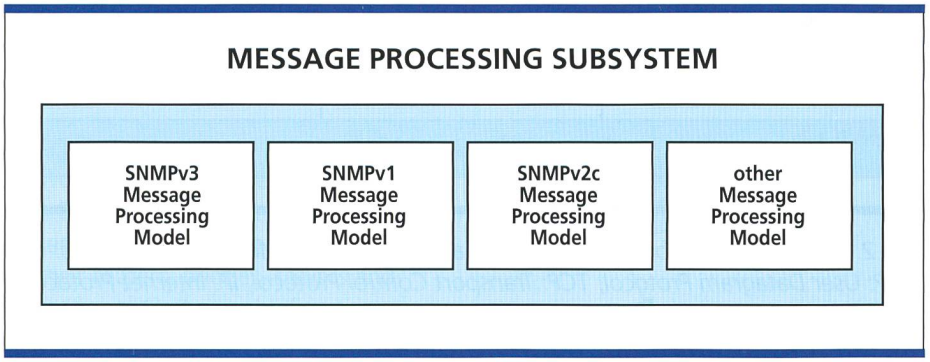

Fig. 4. Message Processing Subsystem.

control managed elements. Managed elements are devices such as hosts, routers, terminal servers, etc., which are monitored and controlled via access to their management information.

It was the purpose of the development of the specifications for SNMPv3 to realise effective management in a variety of configurations and environments. The architecture has been designed to meet the needs of implementations of:

- command responder and/or notification originator applications (traditionally called SNMP agents),
- SNMP entities with proxy forwarder applications (traditionally called SNMP proxy agents),
- command line driven SNMP entities with command generator and/or notification receiver applications (traditionally called SNMP command line managers),
- SNMP entities with command generator and/or notification receiver, plus command responder and/or notification originator applications (traditionally called SNMP mid-level managers or dual-role entities),
- SNMP entities with command generator and/or notification receiver and possibly other types of applications for managing a potentially very large number of managed nodes (traditionally called (network) management stations).

With these possibilities, the architecture for SNMPv3 can be scaled much better than Version 1 ever could, so an application using SNMPv3 can grow together with the target managed network. Thus SNMPv3 is much more appropriate even for medium-sized WANs than the commonly used Version 1. This leads to another important aspect of SNMPv3. To protect the massive investment in SNMPv1 environment, it was obvious that SNMPv3 had to be backwards compatible to its previous version – even to SNMPv2 which was not very successful neither in technical nor in commercial terms.

Overall, the development of the new architecture for SNMPv3 had the following goals:

- Use existing materials as much as possible. It is heavily based on previous work, informally known as SNMPv2u (published in [RFC 1909 and RFC1910]) and SNMPv2 (published in [6] [7] [8] [9] [10] [11] [12]), based in turn on SNMPv2p (the "Party-based SNMPv2", developed between 1993 and 1995, published in [RFC 1441 to RFC 1452]).
- Address the need for secure SET support, which is considered the most important deficiency in SNMPv1 and SNMPv2c.
- Make it possible to move portions of the architecture forward in the standards track, even if consensus has not been reached on all pieces.
- Define an architecture that allows to integrate existing and new functions which will be defined in the future.
- Keep SNMP as simple as possible.
- Make it relatively inexpensive to deploy a minimal conforming implementation.
- Make it possible to upgrade portions of SNMP as new approaches become available, without disrupting an entire SNMP framework.
- Make it possible to support features required in large networks, but make the expense of supporting a feature directly related to the support of the feature.

Protocol Versions

SNMP version 1 (SNMPv1), is the original Internet-standard network management framework, as described in [1] to [5]. This standard is still heavily used and supported by a majority of the SNMP vendors.

SNMP version 2 (SNMPv2), is the SNMPv2 framework as derived from the SNMPv1 framework. It is described in [6] to [12] and has no message definition. – The Community-based SNMP version 2

(SNMPv2c), is an experimental SNMP framework which supplements the SNMPv2 framework, as described in RFC 1901. It adds the SNMPv2c message format, which is similar to the SNMPv1 message format. As mentioned above, these protocol versions are slightly different and not 100% compatible to each other.

SNMP version 3 (SNMPv3, see [13] to [17]) is an extendable SNMP framework which supplements the SNMPv2 framework, by supporting the following:

- a new SNMP message format,
- Security for messages,
- Access control, and
- Remote configuration of SNMP parameters.

Other SNMP framework, i.e., other configurations of implemented subsystems, are expected to also be consistent with this architecture.

Protocol Operations

SNMP messages encapsulate an SNMP Protocol Data Unit (PDU). SNMP PDUs define the operations performed by the receiving SNMP engine (similar to the protocol entities in SNMPv1). Every PDU belongs to one or more of the PDU classes defined below:

1. Read Class: This class contains protocol operations that retrieve management information. [9] defines the following protocol operations for the Read Class: GetRequest-PDU, GetNextRequest-PDU, and GetBulkRequest-PDU.
2. Write Class: This class contains protocol operations which attempt to modify management information. [9] defines the following protocol operation for the Write Class: SetRequest-PDU.
3. Response class: This class contains protocol operations which are sent in response to a previous request. [9] defines the following for the response class: Response-PDU, Report-PDU.
4. Notification class: This class contains protocol operations which send a notification to a notification receiver application. [9] defines the following operations for the Notification class: Trapv2-PDU, InformRequest-PDU.
5. Internal class: This class contains protocol operations which are exchanged internally between SNMP engines. [9] defines the following operation for the internal class: Report-PDU.

The preceding five classifications are based on the functional properties of a PDU. It is also useful to classify PDUs based on whether a response is expected:

6. Confirmed class: This class contains all protocol operations which cause the receiving SNMP engine to send back a response. [9] defines the following operations for the confirmed class: GetRequest-PDU, GetNextRequest-PDU, GetBulkRequest-PDU, SetRequest-PDU, and InformRequest-PDU.
7. Unconfirmed class: This class contains all protocol operations which are not acknowledged. [9] defines the following operations for the unconfirmed class: Report-PDU, Trapv2-PDU, and GetResponse-PDU.

When an application makes use of SNMP, it has to be defined which protocol operations are supported by the application.

SNMP Engine

An SNMP engine (in SNMPv1 called a protocol entity) as one part of the SNMP entity provides services for sending and receiving messages, authenticating and encrypting messages, and controlling access to managed objects. There is a one-to-one association between an SNMP engine and the SNMP entity which contains it (figure 3).

The engine contains:

1. a dispatcher,
2. a message processing subsystem,
3. a security subsystem, and
4. an access control subsystem.

Within an administrative domain, an snmpEngineID is the unique and unambiguous identifier of an SNMP engine. Since there is a one-to-one association between SNMP engines and SNMP entities, it also uniquely and unambiguously identifies the SNMP entity within that administrative domain. Note that it is possible for SNMP entities in different administrative domains to have the same value for snmpEngineID. In case that administrative domains are merged, it may be necessary to assign new values.

Dispatcher

There is only one dispatcher in an SNMP engine. It allows for concurrent support of multiple versions of SNMP messages in the SNMP engine. It does so by:

- sending and receiving SNMP messages to/from the network,
- determining the version of an SNMP message and interacting with the corresponding message processing model,
- providing an abstract interface to SNMP applications for delivery of a PDU to an application,
- providing an abstract interface for SNMP applications that allows them to send a PDU to a remote SNMP entity.

Message Processing Subsystem

The Message Processing Subsystem is responsible for preparing messages for sending, and extracting data from received messages. It potentially contains multiple message processing models as shown in the figure 4.

Each message processing model defines the format of a particular version of an SNMP message and co-ordinates the preparation and extraction of each such version-specific message format.

Security Subsystem

The security subsystem provides security services such as the authentication and privacy of messages and potentially contains multiple security models as shown in figure 5. One or more security models may be present.

A security model specifies

- the threats against which it protects,
- the goals of its services,
- the security protocols used to provide security services such as authentication and privacy, and
- the mechanisms, procedures, and MIB objects used to provide a security service such as authentication or privacy.

Seminar- und Beratungsangebot

Wenn Sie Interesse an Seminaren über SNMP und dessen Umfeld im Netzmanagement haben, so können Sie den Autor unter dessen Mailadresse ruediger.sellin@swisscom.com oder unter seiner Telefonnummer 031 386 74 52 kontaktieren. Er wird Ihnen gerne weitere Informationen zu seinem Seminar- und Beratungsangebot in den Gebieten ATM, Netzmanagement und CORBA geben. Auch individuelle Themen nach Absprache sind möglich.

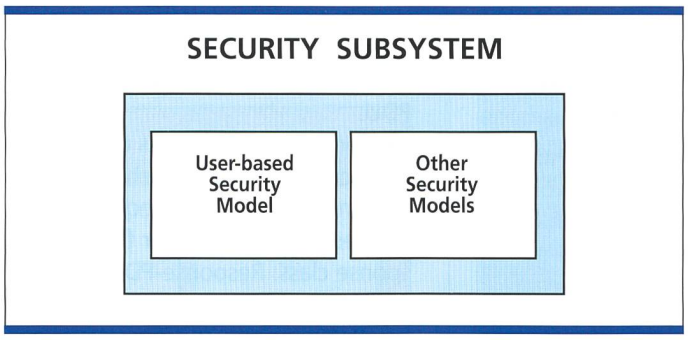

Fig. 5. Security Subsystem.

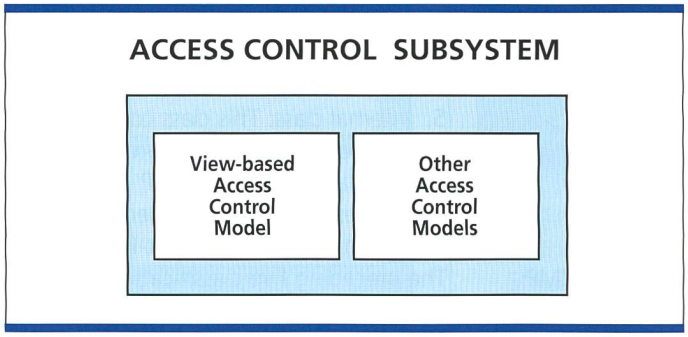

Fig. 6. Access Control Subsystem.

Access Control Subsystem

The access control subsystem provides authorisation services by means of one or more access control models. An access control model defines a particular access decision function in order to support decisions regarding access rights (figure 6).

Applications

The applications (in SNMPv1 called an application entity) form the other part of an SNMP entity. There are several types of applications, including:

- command generators, which monitor and manipulate management data,
- command responders, which provide access to management data,
- notification originators, which initiate asynchronous messages,
- notification receivers, which process asynchronous messages, and
- proxy forwarders, which forward messages between entities.

These applications make use of the services provided by the SNMP engine.

Command Generator Applications

A command generator application initiates SNMP Read-Class and/or Write-Class requests, as well as processing the response to a request which it generated.

Command Responder Applications

A command responder application receives SNMP Read-Class and/or Write-Class requests destined for the local system as indicated by the fact that the contextEngineID in the received request is equal to that of the local engine through which the request was received. The command responder application will perform the appropriate protocol operation, using access control, and will generate a response message to be sent to the request's originator.

Notification Originator Applications

A notification originator application conceptually monitors a system for particular events or conditions, and generates Notification-Class messages based on these events or conditions. A notification originator must have a mechanism for determining where to send messages, and what SNMP version and security parameters to use when sending messages. Note that Notification-Class PDUs generated by a notification originator may be either Confirmed-Class or Unconfirmed-Class PDU types.

Notification Receiver Applications

A notification receiver application listens for notification messages, and generates response messages when a message containing a Confirmed-Class PDU is received.

Proxy Forwarder Applications

A proxy forwarder application forwards SNMP messages. The term "proxy" has historically been used with multiple different meanings, e.g.

- to translate SNMP requests of one version into SNMP requests of another version, or
- to translate SNMP requests into operations of some non-SNMP management protocol.

In this context, "proxy" refers to a proxy forwarder application which forwards either SNMP messages without regard for what managed objects are contained within those messages.

Quite often a traditional SNMP agent and a proxy forwarder application were hard to distinguish from the outside because both contain a kind of agent functionality and a Management Information Base (MIB). However, an SNMP proxy does not access the target MIB directly but rather translates the incoming SNMP requests to appropriate (e.g. proprietary) protocol operations outside the SNMP environment. In comparison to an SNMP proxy, the classical SNMP agent resides within the managed network element, so the SNMP manager accesses the target MIB directly without protocol or MIB conversion.

In the SNMPv3 architecture both applications are defined as follows:

- a proxy forwarder application forwards SNMP messages to other SNMP engines according to the context, and irrespective of the specific managed object types being accessed, and forwards the response to such previously forwarded messages back to the SNMP engine from which the original message was received;
- a command responder application (that is part of what is traditionally

thought of as an SNMP agent) processes SNMP requests according to the (names of the) individual managed object types and instances being accessed. Within this context, it is not viewed as part of a proxy forwarder application.

Since the proxy forwarder application forwards the request irrespective of the managed object types and does not access the target MIB, the proxy forwarder application has no need of a detailed definition of a MIB view. On the contrary, a command responder application must have the detailed definition of the MIB view, and even if it needs to issue requests to other entities, via SNMP or otherwise, that need is dependent on the individual managed object instances being accessed. Therefore, one design goal of a proxy forwarder application is to act as an intermediary between the endpoints of a transaction. In the TMN context, a proxy forwarder is called a Q-Adapter which is located at the edge of the TMN.

SNMP Manager-Agent Communication

A typical SNMP environment consists of one SNMP manager and at least one SNMP agent. Both, manager and agent can be viewed as an SNMP entity containing an SNMP engine and the (management) applications. The SNMP engine and the SNMP applications contain the subsystems which were introduced above. It should be noted that not every SNMP engine must contain all subsystems because an SNMP manager requires partly different subsystems than an SNMP agent.

For example, the management application within an SNMP manager contains a command generator, for which the command responder as part of the management application running on the SNMP Agent is the appropriate partner (figure 7).

Or the Access Control subsystem is present in an SNMP Agent only because it is the SNMP Manager which wants to obtain management information from his SNMP Agents by reading MIB entries. – In addition, a proxy forwarder which allows support to other management protocols than SNMP (e.g. proprietary management protocols) by converting SNMP commands to appropriate commands in the other management protocol, is present in the SNMP Agent only. This has the advantage that the management environment from the SNMP Manager's perspective provides an homogenous view of the managed resources (e.g. a whole network or a collection of network elements).

SNMP Security

From the SNMP user's perspective, the extension of the former SNMP framework by adding useful security mechanisms is the major new feature of SNMPv3. The access control subsystem and the security subsystem guarantee this step forward in the evolution of SNMP. For this purpose, a security model was developed for the architecture of SNMPv3 where a number of classical threats to any network protocols are applicable, too. Within the SNMP management framework, principal threats, secondary threats, and less important threats are considered.

1. The principal threats against which any security model should provide protection are:

- *Modification of information:* The modification threat is the danger that some unauthorised entity may alter in-transit SNMP messages generated on behalf of an authorised principal in such a way as to effect unauthorised management operations, including falsifying the value of an object.
- *Masquerade:* The masquerade threat is the danger that management operations not authorised for some principal may be attempted by assuming the identity of another principal that has the appropriate authorisations.

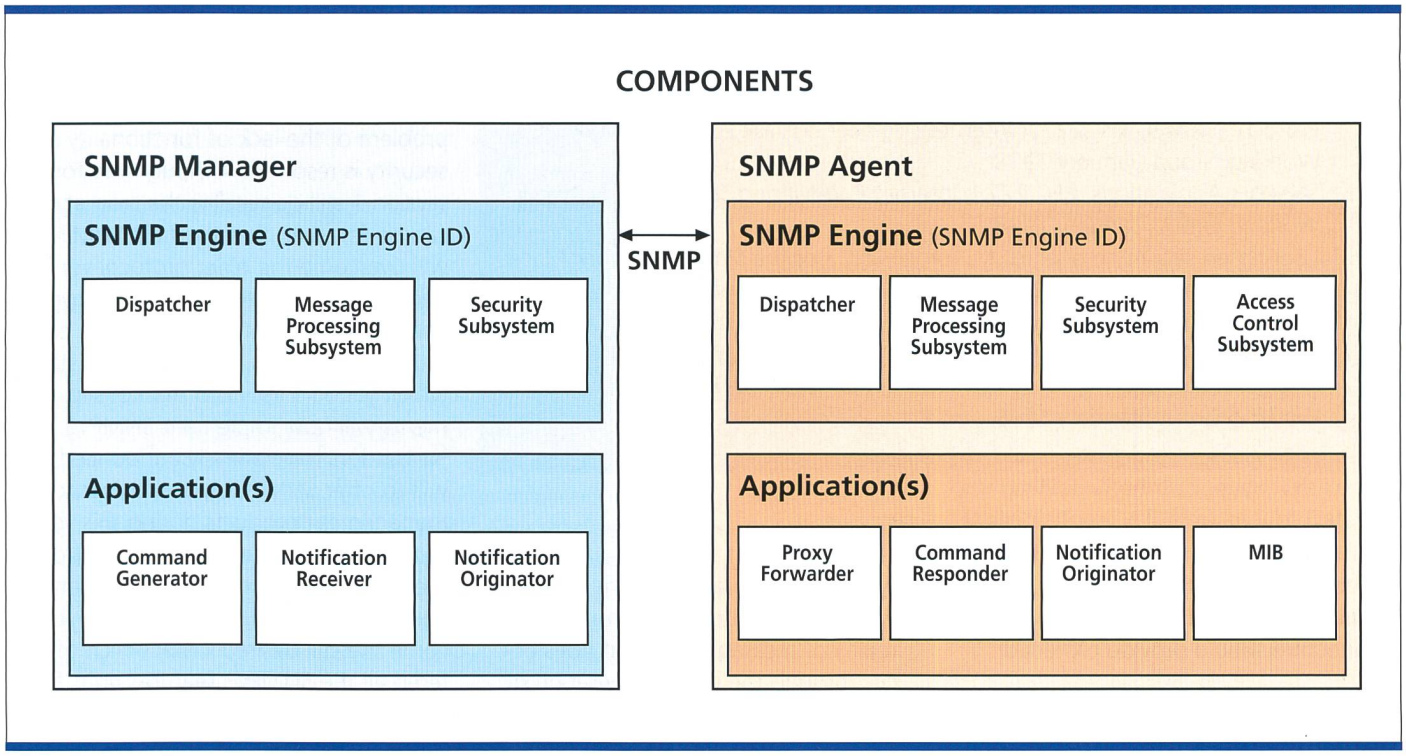

Fig. 7. Components of an SNMP manager and an SNMP agent.

References: Related IETF Requests for Comments (RFC)
(can be downloaded from www.ietf.org free of charge)

SNMP Version 1

[1] Management Information Base for Network Management of TCP/IPbased Internets, RFC 1066, Internet Engineering Task Force, August 1988.
[2] Structure and Identification of Management Information for TCP/IP-based internets, RFC 1155, Internet Engineering Task Force, May 1990.
[3] Concise MIB Definitions, RFC 1212, Internet Engineering Task Force, March 1991.
[4] Simple Network Management Protocol, RFC 1157, SNMP Research, Performance Systems International, MIT Laboratory for Computer Science, May 1990.
[5] Management Information Base for Network Management of TCP/IP-based internets: MIB-II, RFC 1213, Internet Engineering Task Force, March 1991.

SNMP Version 2

[6] Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2), RFC 1902, Internet Engineering Task Force, January 1996.
[7] Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2), RFC 1903, Internet Engineering Task Force, January 1996.
[8] Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2), RFC 1904, Internet Engineering Task Force, January 1996.
[9] Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2), RFC 1905, Internet Engineering Task Force, January 1996.
[10] Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2), RFC 1906, Internet Engineering Task Force, January 1996.
[11] Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2), RFC 1907, Internet Engineering Task Force, January 1996.
[12] Coexistence between Version 1 and Version 2 of the Internet-standard Network Management framework, RFC 1908, Internet Engineering Task Force, January 1996.

SNMP Version 3

[13] An Architecture for Describing SNMP Management frameworks, RFC 2271, Internet Engineering Task Force, Network Working Group, January 1998
[14] Message Processing and Dispatching for the Simple Network Management Protocol (SNMP), RFC 2272, Internet Engineering Task Force, Network Working Group, January 1998
[15] SNMPv3 Applications, RFC 2273, Internet Engineering Task Force, Network Working Group, January 1998
[16] User-based security model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), RFC 2274, Internet Engineering Task Force, Network Working Group, January 1998
[17] View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP), RFC 2275, Internet Engineering Task Force, Network Working Group, January 1998

2. Secondary threats against which any security model used within the SNMPv3 architecture should provide protection are:
- *Message stream modification:* The SNMP protocol is typically based upon a connectionless transport service which may operate over any subnetwork service. The re-ordering, delay or replay of messages can and does occur through the natural operation of many such subnetwork services. The message stream modification threat is the danger that messages may be maliciously re-ordered, delayed or replayed to an extent which is greater than can occur through the natural operation of a subnetwork service, in order to effect unauthorised management operations.
- *Disclosure:* The disclosure threat is the danger of eavesdropping on the exchanges between SNMP engines. Protecting against this threat may be required as a matter of local policy.

3. There are at least two threats against which an SNMP security model does not require any protection:
- *Denial of service:* A security model need not attempt to address the broad range of attacks by which service on behalf of authorised users is denied. Indeed, such denial-of-service attacks are in many cases indistinguishable from the type of network failures with which any viable management protocol must cope as a matter of course.
- *Traffic analysis:* A security model need not attempt to address traffic analysis attacks. Many traffic patterns are predictable – entities may be managed on a regular basis by a relatively small number of management stations – and therefore there is no significant advantage afforded by protecting against traffic analysis.

Author's comment: Another article about the detailed security functions and mechanisms of SNMPv3 was already published in ComTec 7-8/99.

Outlook

With SNMP Version 3 (SNMPv3) the problem of the lack of functionality and security is resolved. Although the former version 1 still dominates the market, it can be foreseen that the new SNMPv3 will overcome the older protocol versions because it offers features which have been expected by the SNMP user's community since years. It will be interesting which vendors in which market segments will now implement SNMPv3. Major vendors have already announced their will to offer SNMPv3-based network management products during this year. But the most interesting question from the users of WAN network management equipment is: Will SNMPv3 even overcome the still desired CMIP which offered all the SNMPv3 features right from the beginning? There is a simple answer to that: the future will show, because the race is now open. 9.4

SNMP-Related Articles and Books from the Author in German

TMN – die Basis für das Telekom-Management der Zukunft, R. Sellin, dpunkt-Verlag Heidelberg, 1995, ISBN 3-7685-4294-7

CMIP (Common Management Information Protocol) – das OSI Network Management Protokoll, R. Sellin, Technische Mitteilungen Telecom PTT, Juli 1992, Hallwag Verlags AG Bern

SNMP (Simple Network Management Protocol) – das Internet Network Management Protokoll, R. Sellin, Technische Mitteilungen Telecom PTT, Januar 1994, Hallwag Verlags AG Bern

CORBA – die Lösung für das Netzmanagement? – R. Sellin, ComTec, November 1998, Hallwag Verlags AG Bern

ATM und ATM-Management – die Basis für das B-ISDN der Zukunft, R. Sellin, VDE-Verlag Offenbach/Berlin, 1997, ISBN

Note

All of the above mentioned RFCs will be succeeded or extended by follow-up documents which already exist as drafts dated end of January 1999. These documents (which are not official standards yet) comment on the original RFCs and will replace or complement them.

Rüdiger Sellin, *dipl. Ing., schloss das Studium der Nachrichtentechnik 1986 erfolgreich ab und ist seitdem in den Branchen Telekommunikation und angewandte Informatik tätig. Er bekleidete verschiedene Positionen bei Netzbetreibern und Systemhäusern in Deutschland und in der Schweiz, unter anderem als Systems Engineer in der OSI-Entwicklung und als Product Manager im Marketing von Network Support Systems. Rüdiger Sellin ist seit 1992 bei Swisscom AG beschäftigt und hier seit 1. Juli 1999 als Senior Consultant bei Marketing & Sales, Major Accounts, Consulting & Design für das Aufspüren und die Nutzung neuester Trends und Techniken zum Vorteil der grössten Geschäftskunden von Swisscom mitverantwortlich. Er ist zudem Autor von zwei Fachbüchern zu den Themen ATM und TMN sowie Verfasser von zahlreichen Fachbeiträgen für Kommunikationsmagazine im In- und Ausland. Er leitet darüber hinaus in Westeuropa Fachseminare auf dem Gebiet der Telekommunikation und tritt gelegentlich als Referent an internationalen Kongressen auf.*

Rüdiger Sellin ist unter der E-Mail-Adresse ruediger.sellin@swisscom.com erreichbar.

Zusammenfassung

Eine Erfolgsgeschichte setzt sich fort

Mit der Version 3 von SNMP, dem Simple Network Management Protocol der Internet Engineering Task Force (IETF), gehen zahlreiche Benutzerwünsche in Erfüllung. Das gilt insbesondere für die Anforderungen an die Sicherheit, denen die Version 1 nicht immer genügte, wenn es um die Übertragung von Steuerbefehlen oder die Implementierung von Managementanwendungen ging. Die Version 3 von SNMP leistet das und noch viel mehr: Sie schafft eine klar gegliederte Netzwerkmanagementarchitektur, welche die Erwartungen der wachsenden SNMP-Nutzergemeinde weit besser erfüllt als ihre Vorgängerinnen. Der vorliegende Artikel beschreibt die wichtigsten Komponenten der neuen SNMP-Architektur. Sein Hauptaugenmerk gilt den neuen Funktionen, auf die so viele SNMP-Nutzer seit Jahren gewartet haben.

Noch einmal: Jahr-2000-Problem

Die Gartner Group, Stamford (Connecticut), hat mehr als 15 000 Firmen und Regierungsdienststellen in über achtzig Ländern nach dem Stand ihrer Vorbereitungen für das «Y2K»-Problem befragt. Und daraufhin die Empfehlung gegeben, man solle sich zum fraglichen Zeitpunkt mit Bargeld für zwei Wochen und mit den Gegenständen des täglichen Bedarfs für fünf Tage versehen. Die Tatsache, dass selbst innerhalb der Europäischen Union Unterschiede in der Vorbereitung auf den Jahrtausendwechsel festgestellt werden, sollte hingegen zu denken geben. Andererseits herrscht in den USA so etwas wie Hysterie im Hinblick auf die möglichen Schwierigkeiten.

Japaner wollen häusliche Netze vereinheitlichen

Das japanische Postministerium hat unter Einbezug der Industrie ein Forum ins Leben gerufen, das innerhalb von drei Jahren Vorschläge für einen einheitlichen Verdrahtungsstandard im häuslichen Bereich unterbreiten soll. Firmen wie NTT, Sony, Microsoft, aber auch die japanische Rundfunkgesellschaft NHK wollen dabei Computer, AV-Systeme, Hörfunk- und Fernsehkabelanschlüsse, Antennenanlagen und Haushaltsgeräte (zum Zweck der Fernsteuerung) unter ein Dach bringen – einschliesslich der Steckanschlüsse. Die Initiative hat den vorläufigen Namen «Advanced Home Information Communications and Broadcast Systems» bekommen.

Japan will drahtlose 60-GHz-Systeme genehmigen

Das japanische Postministerium will im Februar 2000 die eigene Regulierungsbehörde beauftragen, bis zum Sommer des nächsten Jahres den 60-GHz-Bereich für die Nutzung freizugeben. Die kurze Wellenlänge (l = 5 mm) erlaubt Datenkommunikation mit 300 Mbit/s. Die Antennen sind entsprechend klein, die Transceiver werden leichter. Das Postministerium erwartet davon einen Impuls für drahtlose Breitband-LANs im Heimbereich.