15

SNMP and TL-1: Simply integrating management of legacy systems?

A. Clemm
Ericsson Fiber Access
1525 O'Brien Drive, Menlo Park, CA 94025-1451
Tel. (415) 463-6722, fax (415) 463-6755
E-mail: aclemm@eur.ericsson.se

Abstract

One of the challenges associated with open telecommunications network management is the integration of legacy systems. SNMP is as open management paradigm of growing importance in telecommunications. This raises the question whether it could also form an appropriate basis for an integrated management of TL-1 based devices. This paper takes a closer look at this possibility. TL-1 and SNMP are compared. Technical issues involved in managing TL-1 based systems using SNMP are investigated. Because of the differences in power and intended operating paradigms, it is argued that the suitability of an according management integration depends very much on the application.

Keywords

SNMP, TL-1, TMN, legacy systems, management protocols, management gateways, integrated network management, telecommunications network management

1 MOTIVATION

Open management architectures and standard management protocols have reached maturity and gained widespread acceptance. This is no longer true only for data but increasingly also for telecommunications. The main driving force for this is the desire to achieve an integrated network management, both in terms of components to be managed and of functionality. With the Telecommunications Management Network (TMN) framework in place and commercial tools available, an increasing number of Q3 interface implementations can be expected in the near future. SNMP (Simple Network Management Protocol) management, although not originally designed for use in the telecommunications arena, plays an important role as well.

However, for any of the new standard compliant management systems, it must be taken into consideration that they do not exist in a vacuum but that they belong to a history of network management which cannot be ignored. Two main challenges are associated with this:

A. A. Lazar et al. (eds.), *Integrated Network Management V*
© Springer Science+Business Media Dordrecht 1997

- The new, integrated management systems must offer at least the same level of functionality that users were provided by legacy management systems. Reducing the functionality that they previously had is simply not acceptable from the users' point of view. Such legacy management systems tend to be highly specialized and very well geared for a particular management function or for the management of a particular product or technology. Extracting this functionality in an integrated, generic way that allows reuse of the existing code base rather than having to recreate it from scratch is in general far from trivial.
- The need for integration does not pertain only to new systems. Rather, the value of an integrated management depends just as much on the ability to include legacy systems that coexist with systems based on open standards. Otherwise, in the users' perception a new, "integrated" management system means just another system in addition to those that they already have to operate and maintain, adding to the complexity of their network operations instead of doing just the opposite.

In this paper, we deal with the second challenge. In particular, we explore what an integration of (legacy) TL-1 based systems into (open) SNMP management environments entails.

Despite (or rather, because of) its primitive capabilities, SNMP (Simple Network Management Protocol) has started playing an important role also in the telecommunications area. This is underlined by work of industry consortia, such as the ATM Forum and its SNMP MIB definitions for management of ATM devices, and by industry projects [2]. TL-1 (Transaction Language 1), on the other hand, is a Man Machine Language (MML) introduced by Bellcore. These systems have very high commercial relevance in the telecommunications area as they are widely deployed throughout telecommunications networks especially in North America.

SNMP is praised for its simplicity, ease of agent implementation, and flexibility. Most importantly, rich and relatively inexpensive off-the-shelf management tools and implementation environments are available. As a consequence, there is a growing trend to consider SNMP as a pragmatic solution to achieve management integration also of systems until now managed using TL-1. In this paper, we take a closer look at this conception and point out what technical challenges are involved. It is shown that such an integration, while possible, does not come without tradeoffs. Depending on the application, it may not be as simple as it may perhaps initially appear. Consequently, "open" does not in every case mean "preferable". We focus on the original SNMP as opposed to SNMPv2 [7-9], as it is currently the much wider accepted of the two. Most of our results apply however also to SNMPv2, as can be inferred by the reader.

In section 2, TL-1 and SNMP based management are compared and contrasted on the basis of their communication, information, organisation, and function models. This forms the basis for understanding what commonalities can be exploited and what differences have to be overcome to integrate TL-1 and SNMP based management. Section 3 discusses different possibilities for integration of TL-1 and SNMP based management. Section 4 explores technical issues involved in the realization of one of the alternatives, namely the introduction of a management gateway between SNMP managers and TL-1 agents which holds the promise of using off-the-shelf SNMP management platforms for managing TL-1 systems. Drawbacks of trading off the relative openness of SNMP against the legacy management framework of TL-1 are pointed out, as TL-1 is the more powerful of the two. From this, it is inferred which kinds of applications are good candidates for SNMP based management integration, and for which kinds drawbacks may offset the potential advantages. Conclusions are offered in section 5.

2 TL-1 AND SNMP: A COMPARISON

TL-1 and SNMP differ entirely in their communication, information, function, and to some extent even in their organisation models. They are compared in the following section. Because more readers will be familiar with SNMP than with TL-1, TL-1 is treated in a little more detail than SNMP.

2.1 TL-1

TL-1 is a MML which was standardized by Bellcore [11-13]. Communication between managers and network elements (i.e. agents) takes place by exchange of operations application messages, essentially simple text strings that follow a particular (TL-1) format. The management services are defined by contracts which specify the messages to be exchanged. A contract may specify an (input) command and an (output) response constituting a management operation, or an autonomous message.

A large number of different contracts exists, in particular for management operations. They can roughly be classified with respect to the kind of function they provide, and with respect to what aspect of the network element respectively what Managed Object (MO) they refer to. As they are rather closely related to the particular function and often the type of MO they refer to, a clear separation of information, communication, and function models is difficult. Whenever there is a requirement for a new operation, it is simple and legal to add a new (proprietary) transaction. This has resulted in many proprietary TL-1 dialects. Essentially, they all have in common services to enter, edit, delete, and retrieve various kinds of management information as well as to invoke special functions such as the execution of tests.

Contracts refer to object entities which are addressed using hierarchical "access identifiers", or AIDs. An AID reflects at the same time the type of object, e.g. a linecard, and the instance itself. The hierarchies are based on containment, closely reflecting physical reality, and are addressed that way. The following is an example for an AID in an Ericsson LOC (Loop Optical Carrier) system realizing FITL (Fiber In The Loop) technology: DFM-2-ONU-15-LC-5. It denotes the linecard in slot 5 of Optical Network Unit 15 on the Passive Optical Network (PON) off Distribution Fiber Module 2 of a particular Host Digital Terminal. An AID can be used to refer not only to one particular but also to groups of entities, subject to the individual contract definitions, which makes scoping of management operations across several MOs possible (e.g. DFM-2-ONU-15-LC would refer to all linecards in that particular ONU). Also associated with object entities is usually a service state, indicating their ability to perform their functions. A state machine ensures that no operations are enacted when it is illegal to do so.

The following examples of an input command and an output response illustrate what typical TL-1 messages look like.

```
RTRV-EQPT:SYS001:HDT:20;
```

This is a typical command to retrieve parameters from a particular device. RTRV-EQPT ("retrieve equipment") constitutes the command code, with RTRV being the command verb which specifies the action to be performed, and EQPT being a command modifier expressing the constraint that the action is performed against a piece of equipment (versus for instance a line). SYS001:HDT:20 constitute the staging parameters. SYS001 is the target identifier. It identifies the network element to receive and process the command and can be thought of as the agent identifier. HDT is the AID. It identifies the entity within the network element against which the retrieve is to be performed, in this case the "host digital terminal", a piece of equipment used in FITL systems. 20 is the correlation tag ("ctag"); it is sent back in the response so that the manager can correlate responses it receives against the respective commands. TL-1 commands may in addition (not shown here) contain a general block following the correlation tag with data parameters. The data parameters allowed differ for different command codes and AIDs.

The following is a possible response for the above TL-1 command:

```
SYS001 96-4-15 11:30:45
M  20 COMPLD
   "HDT::GENERIC=rel2.0,TMG=SLV1&SLV5&INT,DIAGINTVL=4,
DIAGALARM=2,STATINTVL=48,SAMCHAN=LOCAL,LBO=266:IS-NR,SX"
```

The first line contains the identifier of the system issuing the response, followed by a date and time stamp. The M in the following line indicates the mcode which specifies the type of output message. In this case, it is the response to an input command. The value of the ctag of the input command follows, 20 in this case. COMPLD indicates the command has successfully completed. The following lines contain the response data block, i.e. parameter values of the HDT that were requested. IS-NR refers to the HDT's service state: in service, normal. An error response would have contained e.g. a DENY instead of a COMPLD, followed by an error code and error text.

Autonomous messages look similar to response messages, indicating the type of autonomous message and level of severity. Instead of a ctag, they contain an automatic message tag (atag) which is automatically incremented for each new autonomous message, except for messages indicating the clearance of an alarm condition which contain the atag of the message in which the alarm was first reported.

2.2 SNMP

SNMP is a management protocol originally designed for the management of TCP/IP capable data communications network devices. The guiding principle for its design was simplicity, to ensure agent implementations could easily be made available. The management information base consists of objects (not in the object oriented sense) representing variables. Both object types and object instances ("SNMP variables") are viewed as parts of the Internet registration tree, with instances forming the leaves. Columnar and non-columnar objects are distinguished, depending on whether or not they are conceptually considered part of a table entry. The management protocol itself offers a set of operations to retrieve and set values of particular object instances, to traverse tables, and to send simple traps, i.e unsolicited events from the manager to the agent. The SNMP management framework is in general considered polling based, trap directed. The reader unfamiliar with SNMP concepts is asked to refer to the literature [5,6].

Similar to TL-1, new SNMP object types are easy to define and add, leading to a wide variety of proprietary MIBs (Management Information Bases), i.e. collections of object type definitions. However, two aspects make the dealing with proprietary aspects in SNMP easier than in TL-1: the clear separation of the management information from the other aspects of the management framework which are commonly shared, and the availability of standardized MIBs for many purposes.

2.3 Differences between TL-1 and SNMP

The following tables summarize the most important differences between TL-1 and SNMP.

Table 1 Communication model

SNMP	*TL-1*
Small set of general, basic communication services (get, set, get-next, trap), parametrized as to to which SNMP object (i.e. variable) to apply	Large set of specialized communication services, parametrized to a lesser extent (different services for semantically analogous operations on different types of objects)
Unreliable as based on UDP	Unreliable, however, message sequencing aids in detecting lost messages
No scoping	Scoping to some extent
Target for read operations not necessarily required ("Get-next" for MIB-discovery)	Target required
ASN.1 encoding	ASCII strings
Minimal security (community name as unencrypted password)	Very basic security (log on and off)
Connectionless, datagram oriented	Session oriented
Polling based, trap directed	Polling and event based

Table 2 Information model

SNMP	*TL-1*
Simple information model using tables and variables plus grouping mechanism Clear separation of information from communication model	No explicit information model, implicit information model underlying addressing scheme (AIDs), operations and parameters but no clean separation of information, communication, and function models
No state model	Inherent state model
Objects abstracted away from physical world	Objects reflect physical world directly

Table 3 Function model

SNMP	*TL-1*
Design for monitoring of devices in TCP/IP based data networks	Design for operations, administration, maintenance, and provisioning in telecommunication networks
No dedicated function model	Extensive function model, e.g. testing, protection switching, alarm status retrieval, etc.
No dedicated state and lifecycle management	Extensive state and lifecycle management (e.g. inventory of equipment before it is installed)

Table 4 Organisation model

SNMP	*TL-1*
Manager-agent paradigm	Manager-agent paradigm; variation possible with a mediation device involved in certain management functions

To summarize, TL-1 is actually the richer and more powerful of the two, while SNMP is better structured and typically the easier to understand. The differences in the goals of their design clearly show: SNMP for the monitoring of devices in TCP/IP based networks, TL-1 for the OAM&P (Operations, Administration, Maintenance, and Provisioning) of very specialized telecommunications systems. Provisioning for instance is a concept virtually unknown in the management of data networks. In the following sections, the issues involved in applying SNMP on this unusual terrain are inspected more closely.

3 ALTERNATIVES FOR INTEGRATION OF SNMP AND TL-1 BASED MANAGEMENT

There are different possiblities for the integration of SNMP and TL-1 based management:

- Multi-protocol (or rather, multi management paradigm) management agents, i.e. addition of SNMP capabilities to TL-1. This alternative is not flexible enough as basis for management integration, as changing existing agent implementations in the field may be impossible.
- Multi-protocol (or rather, multi management paradigm) managers. The actual management protocol that is used is hidden inside a layer within the management system. This layer offers an internal unified model which is as homogeneous as possible to management applications which need not be aware of differences in management protocols. This alternative mandates extensions to existing management platforms, which arguably some are equipped to accomodate (e.g. PMI (Portable Management Interface) adapters in SunSoft's Solstice [10]).
- Management gateway between SNMP manager and TL-1 agent (figure 1). Different possibilities exist for where to place the system boundaries. The gateway could be realized in the network element itself (as indicated in the figure) or outside, e.g. in a mediation device or even in the management system itself, making this alternative similar to the previous one.

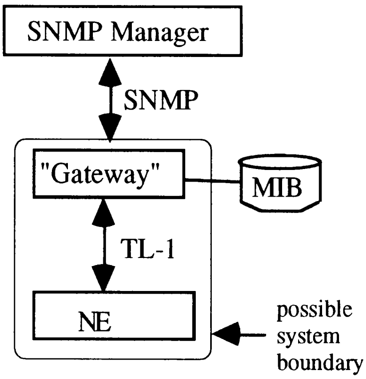


Figure 1 Management gateway as integration means.

Because the last alternative illustrates best the issues involved in the integration of SNMP and TL-1 management, it is the one which shall be investigated further. It also holds the promise to be able to use standard SNMP management platforms without further modifications as basis for integration and therefore deserves a closer look. Gateway approaches have been successful and are well accepted to achieve interoperability in the management arena, e.g. for interoperability between CMIP and SNMP [1, 3, 4]. On a broader note, the considerations in building a gateway contrast also the SNMP and TL-1 based management paradigms rather nicely. We focus on conceptual issues. The actual design of a gateway is beyond the scope of this paper.

From section 2 follows that a gateway means that TL-1 agents will be managed using a less powerful paradigm than the one used before. Since this may involve not being able to use the full power these agents offer, at first sight this may appear like something that should be avoided. However, there are several advantages to be gained which makes this alternative well worth exploring. Most importantly, management which is integrated and homogeneous is preferable in many scenarios over one which is not, even if a subset of the devices to be managed could be managed more efficiently differently. This is especially true for applications not taking advantage of the full capabilities TL-1 might offer. SNMP tools available today hold the promise for rapid development cycles if the devices to be managed can be managed using SNMP.

4 BUILDING AN SNMP-TL-1-MANAGEMENT GATEWAY

A management gateway introduces a management hierarchy. It fulfills management operation requests from the upper-level management system in terms of management operations enacted upon lower-level management systems. As SNMP is less powerful than TL-1, in general the mapping between them is fairly straightforward, as the gateway does not have to fill a gap in functional power between the two. This means that besides keeping track of the different addressing schemes, the gateway will not have to keep much state which keeps it relatively simple.

As TL-1 does not really separate communication, information, and function models, it has to be investigated what transactions are provided by TL-1 and determined how the same information and operations can be conveyed using SNMP. We do this by drawing on examples from the set of TL-1 transactions used for the management of Ericsson's LOC systems. In subsection 4.1, we describe how communication and function model can be mapped. In 4.2, we look more closely at the mapping of the information model. This provides the basis for understanding the following discussion in 4.3 as to where applications are likely to benefit from the integration of TL-1 based systems in SNMP environments and where its practical limitations are.

Not discussed are aspects dealing with the use of a gateway to also implement a management information hierarchy in which the most recent information is collected at the leaves and propagated to some degree into the higher levels. Implementing caching strategies to keep static information in the gateway is desirable from a performance standpoint but adds complexity because state and replicated management information have to be maintained. In the context of this paper, we consider this a design issue which is beyond its scope.

4.1 Mapping TL-1 contracts and SNMP operations

As explained in section 2, TL-1 messages start with a command code, followed by lists of various parameters. The command code consists of an (action) verb and one or two modifiers that state the kind and instance of "MO" the operation is to be applied to. Accordingly, TL-1 transactions can be grouped along the type of actions (that are being applied to different entities). Different modifiers will be reflected in what parts of the MIB the respective SNMP operation(s) refer to.

Memory administration contracts

Memory administration contracts allow the configuration, i.e. the changing, deleting, adding and querying of network element parameters.

- *Enter*: Corresponding to a "create", these contracts are not directly mappable. However, they can be simulated if the "MO type" being entered is modeled as an SNMP table, using set operation(s) to implicitly create a new table entry (compare with [8]).
- *Retrieve*: Correspond and can be mapped to SNMP get operations. Scoping is not available in SNMP. To imitate scoped retrieves à la TL-1, multiple gets or sequential get-next operations have to be issued. The use of SNMP here is less efficient.
- *Edit*: In general, the changing of parameters can be mapped to set operation(s).
- *Delete*: Analogous to the case of *Enter*, these contracts are not directly mappable to SNMP. However, they can be simulated if the type of the MO to be deleted is modeled as an SNMP table, using a set operation to delete the table entry (compare with [8]).

Network maintenance contracts

Network maintenance contracts provide the means for surveillance, alarming, recovery, and state control. They are fairly hard to imitate in SNMP as it is they which define to a large extent the function model for which SNMP has no counterpart. Where TL-1 contracts define "actions", these have to be simulated by means of SNMP variables whose setting to certain values implies the side effect that a certain operation is executed. The SNMP get response returns the success indication. If the action has failed, an error is reported. In cases where more detailed information has to be provided, a dedicated SNMP variable can be introduced whose value is to be retrieved separately. Some examples for network maintenance contracts follow.

- *Message reporting control*: The contracts allow for the enabling and inhibiting of message reporting. This constitutes "actions" for which there are no corresponding SNMP counterpart operations. They can be simulated by introduction of an SNMP variable whose value implies whether message reporting is enabled or inhibited. To differentiate between different logged on users, message reporting control requires the use of an actual table instead of a simple variable.
- *Alarm and event status retrieval*: TL-1-based systems typically maintain status information of any outstanding alarms and events, which can be retrieved through these contracts. In SNMP, this has to be simulated by introducing a table to maintain alarm information. The table can be retrieved using get and get-next operations. TL-1 parameters identifying the entity an alarm or event pertains to have to be translated into SNMP MIB counterparts. The table needs to include the alarmed entity as part of the index, otherwise random access to alarm information pertaining to a particular piece of equipment is not possible. Complete table traversal may still occasionally be necessary as random access across several dimensions is not possible in SNMP tables.
- *Performance monitoring*: TL-1 allows retrieval of certain performance related parameters. This translates in a straightforward manner, mapping to SNMP get operations on MIB variables introduced for that purpose.
- *Testing*: These contracts allow the remote execution of a wide variety of tests on equipment, e.g. on leakage, capacitance, or the presence of dial tone. Notice that the execution of some tests may span longer time intervals during which service supported by the system may be affected, which requires also the means for aborting tests in progress. There is no counterpart for any of this in SNMP, as this resembles actions. The corresponding actions can be simulated by introducing dedicated SNMP variables whose setting to a certain value implies that a test is to be executed. Action parameters

will have to be placed into additional SNMP variables. The response to the test result can be placed into yet additional MIB variables which will have to be retrieved separately. A special value can be used to indicate that a test has not been finished. The variable(s) will have to be reset after a test result has been retrieved, or have to be reset as a side effect of the setting of the variable resembling the action. Again, SNMP concepts are being stretched a bit.

Many other network maintenance contracts exist that each require their own mapping, for instance for protection switching control, loopback control, alarm error tracing, or the backing up of network element state information.

Security management
Unlike TL-1, SNMP does not require logging on and off managed devices. A management gateway can just log on as a registered user before the first SNMP command is issued.

Autonomous messages
Facilities for transmitting autonomous messages are much richer in TL-1 than in SNMP. In general, for autonomous messages to be reported, an SNMP enterprise specific trap will have to be used, with some information to be retrieved manually from the SNMP agent. For this purpose, an "alarm MIB" with variables to keep information on all standing alarms has to be introduced. Events which are reported only once and are not subject to clearing have to be investigated separately.

4.2 Management information

TL-1 messages refer to an implied model of the network, as stated in the modifiers of the command code and the AID used to address the particular "MO instance" that the TL-1 message refers to. The AID is not just an address but along with the command code indicates the type of MO that is being referred to. The underlying TL-1 model has to be translated into an explicit SNMP model. Figure 2 depicts an excerpt of the model which is implied by the AIDs used in the TL-1 transactions for the management of Ericsson's LOC system. Indentation depicts hierarchical dependency.

- *HDT Host Digital Terminal*
  - *TGM Timing Generator Module*
  - *DFM Distribution Fiber Module*
    - *ONU Optical Network Unit*
      - *PAD Packet Assembler Disassembler*
      - *PM Power Module*
      - *LC Line Card*
      - *BP Binding Post*
      - *CPT Contact Point*
  - *OFT Office Feeder Termination*
    - *DG Digroup*
    - *CH Channel*

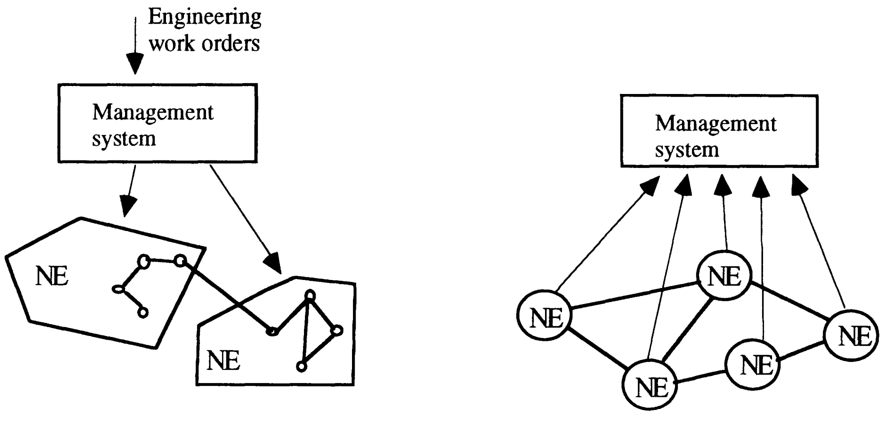
Figure 2 Excerpts of LOC object model as implied by TL-1 transactions.

A specification of a methodology to be used to derive the SNMP model from the TL-1 transactions is beyond the scope of this paper. Here, only a few aspects are mentioned: different types of objects have to be translated into different SNMP groups. The individual parameters of transactions indicate which variables have to be provided as part of the objects. Objects that may occur more than once in a LOC system have to be translated into tables - in this example anything at a lower hierarchy level. TL-1 does not really make use of complex data types so the mapping of data types is straighforward. One restriction exists in the case of enumerated types of which there are several, the most prominent example being the system state. Here, values can be transferred as graphic strings which will have to be interpreted in the management system.

4.3 Benefits and limits of TL-1 management integration based on SNMP

Management applications communicating with TL-1 devices through the gateway may constrain themselves to the same applications which are typical for the management of TCP/IP based networks: occasional polling of devices to determine operational state, processing of traps for that same purpose, plotting of performance-related attributes over time, remote inspection of system configurations, etc. As was shown, the mappings for these communications exchanges are very straightforward. It is reasonable to expect the gateway approach to work very well here and achieve management integration with minimum effort, both development and computationwise.

However, in general the desire for management integration in a telecommunications environment does not stop here. Rather, in addition to these applications, all the other kinds of applications that previously TL-1 was applied to are expected to carry over into the SNMP environment. After all, the same level of functionality as before still has to be supported. In many cases, integration of SNMP and TL-1 based management does not only have to be concerned with the mere mapping of SNMP onto TL-1 at the protocol level. It also needs to be concerned at an application level with the paradigms according to which TL-1 is used. Where SNMP lacks the facilities to support these paradigms, the now SNMP-based applications need to make up for these deficiencies by adding something on top. It is here where the technical challenges come in and where the limits of this approach lie. They extend beyond the mapping of TL-1 network maintenance contracts and autonomous messages. The challenges include the following (see also figure 3):



(a) few complex NEs, flow of static information from top to bottom

(b) many simple NEs, flow of static information from bottom to top

Figure 3 Typical management scenarios: (a) TL-1, (b) SNMP.

- Control of management information. In SNMP, it is typically the agent who owns and controls all management information. The manager discovers new agents and new pieces of equipment as it polls the network. In TL-1 based management, it is common for the manager to be in control of the static management information and retrieve only dynamic state information and alarms from the network element. An operator inventories equipment of the network, the information of which is obtained for instance from engineering work orders. The associated management information is communicated to the agent. Only from this point in time is it possible to actually monitor the equipment. Differences between the management view and the real world can be resolved through discrepancy reports or sophisticated reconciliation procedures. This reflects that typically telecom operators have much more complete and central control over the network than their datacommunications counterparts. The case where network elements simply pop up or disappear, common in data communications networks where users simply plug, unplug, and move their machines, simply does not occur in a telecom environment.

- Complexity and distribution of managed systems. TL-1 based systems are typically more complex and may be more geographically distributed than their usual SNMP counterparts. This results in a higher number of tables as opposed to non-columnar objects, making management information more cumbersome to access and manipulate.
  Also, graphical topology display is no longer automatically obtained by using a management platform, as much of the topology of interest is defined not through the different SNMP agents that are out there but rather within the MIB tables of a single agent.

5 CONCLUSIONS

Will SNMP based systems form the next generation of legacy systems in the telecommunications industry, soon obsoleting efforts to integrate TL-1 legacy systems into SNMP management? Quite possible, especially considering the limitations inherent in SNMP and the advent of TMN. Why, then, should integration of SNMP and TL-1 based management be considered? The answer to this is manyfold. First, comparing the two provides insight about the strengths and weaknesses of each, so there is an educational benefit. Second, as of today, SNMP is undoubtedly the most prevalent approach to open management, with other more powerful open management technologies still to be proven. Third, because of its importance, mappings from other technologies to and from SNMP exist (e.g. OSI management / CMIP and CORBA). Accordingly, management of TL-1 devices through SNMP automatically opens them also up to management by other paradigms through use of multi-stage gateways - concerns about performance aside.

The mapping of SNMP to TL-1 is straightforward in areas where the traditional strengths of SNMP lie. It is here where an integration of TL-1 based systems into SNMP environments is sound and well-suited. Beyond that, integration of TL-1 based systems into SNMP environments is not trivial. The attempt to carry over TL-1 concepts into SNMP reveals in many cases SNMP's limitations in this terrain. SNMP concepts have to be stretched to be able to achieve if the full management functionality provided by the richer TL-1. Certain features that TL-1 offers with respect to better management efficiency cannot be used, like scoping. Network maintenance contracts can often only be simulated through MIB extensions which make for very complex MIB semantics. Autonomous messages and alarming may require a two-phase concept. However, a mapping is certainly possible.

In general, the best use of SNMP is when it is constrained to those applications for which it was designed, namely polling based monitoring of network equipment. This is by comparison relatively simple to support. It is also where SNMP based integration of TL-1 based systems provides the most value. Use of SNMP for applications to manage TL-1 capable devices beyond that is certainly possible although it may at times be awkward in the described telecom environment and offset the desired benefits. Here, the SNMP management applications are no longer off-the-shelf and take more effort to develop than under the legacy paradigm. Therefore, an integration of TL-1 based systems into SNMP based management has to be carefully considered on an application by application basis. Nevertheless, management gateways, along with adaptation layers, are important and in general very suitable techniques to cope with the integrated management challenge posed by legacy systems.

ACKNOWLEDGEMENTS

For valuable discussions and comments on earlier versions of this paper which undoubtedly helped improve it, I want to thank my colleagues at Ericsson Fiber Access, in particular David Hood, Steve Cutcomb, Alice Bedoyan, and Ron Reedy.

REFERENCES

[1] S. Abeck, A. Clemm, U. Hollberg. Simply Open Network Management - An Approach for the Integration of SNMP into OSI Management. *3rd IFIP/IEEE Int. Symposium on Integrated Network Management*, San Francisco, CA, April 1993.
[2] M. Ho, A. Farrell, J. De Wiele. SNMP Management of Telecommunications Carrier Networks. *IFIP/IEEE Network Operations and Management Symposium*, Kyoto, Japan, April 1996.
[3] K. McCarthy, G. Pavlou, S. Bhatti, J. Neuman de Souza. Exploiting the power of OSI management for the control of SNMP-capable resources using generic application level gateways. *4th IFIP/IEEE Int. Symposium on Integrated Network Management*, Santa Barbara, CA, May 1995.
[4] Network Management Forum CS341. *CMIP/SNMP Interworking*. Includes Forum 026: Translation of Internet MIBs to ISO/CCITT GDMO MIBs, Issue 1.0, October 1993, and Forum 028: ISO/CCITT to Internet Management Proxy, Issue 1.0, October 1993.
[5] RFC 1155. *Structure and Identification of Management Information for TCP/IP-Based Internets*. Internet Engineering Task Force, May 1990.
[6] RFC 1157. *A Simple Network Management Protocol (SNMP)*. Internet Engineering Task Force, May 1990.
[7] RFC 1902. *Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)*. Internet Engineering Task Force, January 1996.
[8] RFC 1903. *Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)*. Internet Engineering Task Force, January 1996.
[9] RFC 1905. *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)*. Internet Engineering Task Force, January 1996.
[10] *Enterprise Manager 1.1.1 Video Workbook*. Order No. 802-3197-02, SunSoft, 1995.
[11] TR-TSY-000831. *Operations technology generic requirements (OTGR): Operations application messages - Language for operations application messages*. Issue 2, Bellcore, February 1988.
[12] TR-TSY-000833. *Operations technology generic requirements (OTGR): Operations application messages - Network maintenance: Network element and transport surveillance messages*. Bellcore, Issue 5 Revision 1, April 1993.
[13] TR-1093. *Generic State Requirements for Network Elements*. Issue1, Bellcore, September 1993.

BIOGRAPHY

Alexander Clemm has been actively involved in network management research and development since 1990. Currently he is responsible for the systems engineering of Network Management Systems at Ericsson Fiber Access in Menlo Park, California. He has published about a dozen papers and holds a Ph.D. in computer science from the University of Munich and an M.S. from Stanford University.