Internet Management Standards

Quo Vadis?

Jürgen Schönwälder
TU Braunschweig
Bültenweg 74/75
38106 Braunschweig

Kurzfassung

Dieser Beitrag gibt einen Überblick über die aktuellen Entwicklungen im Bereich der Internet Management Standards. Es werden die in den letzten zwei Jahren erarbeiteten Neuerungen kurz skizziert und der aktuelle Stand der Implementierungen beschrieben. Daran anschließend werden weiterhin bestehende Probleme erläutert und einige Lösungsmöglichkeiten aufgezeigt.

1. Einleitung

Vor 10 Jahren wurde das Simple Network Management Protocol (SNMP) innerhalb der Internet Engineering Task Force (IETF) entwickelt und standardisiert. SNMP in der Version 1 (SNMPv1) [RFC 1157] war sehr erfolgreich, da es eine zu der Zeit angemessene und von den Kosten her vertretbare und schnell umzusetzende Lösung war. Zum Zeitpunkt der Einführung von SNMP war die Sprache zur Beschreibung von sogenannten Management Information Bases (MIBs) noch nicht voll ausgereift, so daß die Standardisierung der Structure of Management Information (SMI) in der Version 1 (SMIv1) erst etwas später abgeschlossen wurde [RFC 1155, RFC 1212, RFC 1215].

SNMPv1 beinhaltet keine Sicherungsmechanismen, weshalb SNMPv1 vorwiegend zum Monitoring eingesetzt wird. Mit großen Bemühungen versuchte man viele Jahre lang dieses Problem zu beheben, ohne jedoch das Ziel mit SNMP Version 2 (SNMPv2) jemals zu erreichen [PIK 95]. Nebenprodukt dieser Bemühungen war jedoch auch eine Überarbeitung der Protokolloperationen und der SMI. Die überarbeitete SMI Version 2 (SMIv2) wurde fortan die Grundlage für alle neu entwickelten MIB Definitionen innerhalb der IETF. Dadurch bekam sie relativ große Bedeutung, während sichere Varianten von SNMPv2 niemals praktisch relevant wurden.

Ein Prozeß, der sich relativ unspektakulär vollzogen hat, ist die Standardisierung einer große Mengen von MIB Modulen, die im Laufe der Jahre erarbeitet wurden. Allein die IETF hat derzeit ca. 90 MIB Module standardisiert und es sind viele weitere Module in Arbeit. Einige Hersteller haben ähnlich große Mengen von herstellereigenen MIB Definitionen. Neben den standardisierten MIB Modulen, die auch zu einer Vereinheitlichung der verfügbaren Management-Information geführt haben, stellen insbesondere die vielen realisierten Instrumentierungen einen beachtlichen Wert dar.

Dieser Beitrag beschreibt zunächst im Abschnitt 2 die wichtigsten Neuerungen, die an den Internet Management Standards in den letzten zwei Jahren vorgenommen wurden. Daran schließt sich in Abschnitt 3 eine Diskussion weiterhin bestehender Probleme an, wobei auch einige Lösungsmöglichkeiten angerissen werden. Eine Zusammenfassung und Bewertung schließt diesen Beitrag im Abschnitt 4 ab.

2. Aktuelle Entwicklungen

Dieser Abschnitt gibt einen Überblick über die aktuelle Entwicklung der Internet Management Standards innerhalb der IETF. Es werden die wesentlichen Ergebnisse der Arbeiten der letzten zwei Jahre skizziert, um sie später in einen Kontext einordnen zu können. Da eine detaillierte Beschreibung der Neuerungen den Rahmen dieses Beitrags sprengen würde, sei an dieser Stelle auf die zitierte Originalliteratur verwiesen.

2.1 SMI Version 2

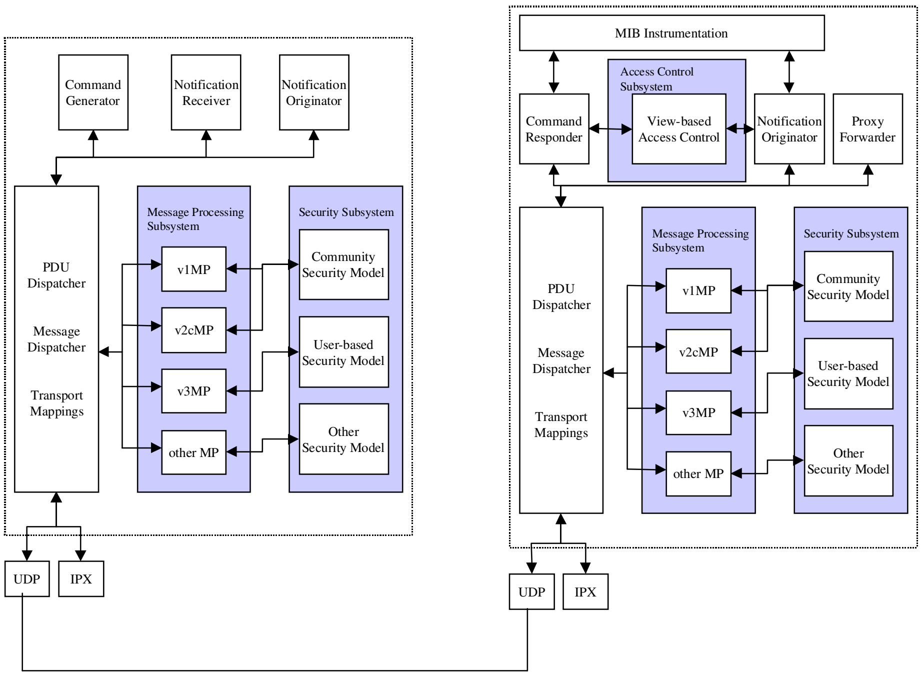
Die SMIv2 bildet derzeit die Grundlage zur Beschreibung von Management-Informationen innerhalb der IETF. Der Standardisierungsprozeß der IETF verlangt, daß Spezifikationen nur von anderen Spezifikationen abhängen dürfen, die mindestens denselben Status haben. Da einige MIB Spezifikationen den vollen Internet-Standard Status anstreben, war es notwendig, die SMIv2 ebenfalls zu einem vollen Internet-Standard zu erheben.

Im Sommer 1998 wurde ein kleines Entwurfsteam zusammengestellt, um die SMIv2 zu überarbeiten und vorhandene Fehler und Ungenauigkeiten zu beheben. Änderungen der SMIv2, die eventuell Interoperabilitätsprobleme verursachen können, sind beim Übergang vom Draft-Standard Status zum Internet-Standard Status nicht erlaubt. Es wurden insgesamt 75 Probleme eingereicht, von denen 25 abgelehnt wurden, da ihre Lösung Inkompatibilitäten erzeugt hätten. Die restlichen Fragen wurden in mehreren Runden diskutiert und die SMIv2 Dokumente anschließend überarbeitet. Die überarbeiteten Dokumente wurden im August 1998 auf einem IETF-Treffen diskutiert, nochmals überarbeitet und schließlich Anfang 1999 von der IESG verabschiedet [RFC SMI, RFC TC, RFC CONF].

Die eingebrachten Änderungen beseitigen eine Reihe von Fehlern wie z.B. Widersprüche zwischen der formalen Definition in ASN.1 Makros und den textuellen Beschreibungen oder Fehler in den ASN.1 Makros selbst. Außerdem wurden Regeln festgeschrieben, die erlaubte und unerlaubte Änderungen am MIB Modulen beschreiben und die Konsequenzen von Statusänderungen einzelner Definitionen regeln. Mit der Publikation der neuen SMIv2 Dokumente als Internet-Standards ist die SMIv2 quasi festgeschrieben und es kann mit einer schrittweisen Ablösung der SMIv1 begonnen werden. Der Internet-Standard Status bedeutet auch eine große Stabilität für MIB Module und Werkzeuge, die auf der SMIv2 beruhen.

2.2 SNMP Version 3

Die Arbeiten an SNMP Version 3 (SNMPv3) wurden Ende 1996 aufgenommen und resultierten in der Publikation von SNMPv3 als Proposed-Standard im Januar 1998 [RFC 2271, RFC 2272, RFC 2273, RFC 2274, RFC 2275]. SNMPv3 bietet neben der Lösung der Sicherheitsproblematik ein lang überfälliges Architekturmodell und eine Modularisierung von SNMP. Die Unterstützung der SNMP Toolkit Hersteller ist sehr gut. Zum Zeitpunkt der Erstellung dieses Beitrags sind auf der SNMPv3 Web-Seite (http://www.ibr.cs.tu-bs.de/projects/snmpv3/) 14 unabhängige Implementationen aufgelistet.



Die Arbeiten an SNMPv3 haben, als Nebeneffekt der Modularisierung, auch einige bisher ungelöste Fragen im Rahmen von SNMPv1 beantwortet. So ist z.B. das View-Based Access Control Model (VACM), mit dem der Zugriff auf MIB Objekte kontrolliert werden kann, nicht an eine spezielle SNMP Version gebunden. Derzeit finden Arbeiten zur Koexistenz von SNMPv1 und SNMPv3 und zum Übergang von SNMPv1 zu SNMPv3 statt, in denen beispielsweise Fragen geklärt werden, wie man in SNMPv3 analog zu SNMPv1 die Erzeuger von Ereignismeldungen identifizieren kann bzw. wie mit nicht vorhandenen Datentypen umgegangen werden soll. Diese Arbeiten sollen im Frühjahr des Jahres 1999 abgeschlossen werden. Die Definition von SNMPv3 selbst wird derzeit aufgrund der Erfahrungen mit mehreren Implementationen überarbeitet und wahrscheinlich beim Erscheinen dieses Artikels bereits als Draft-Standard von der IETF publiziert worden sein.

Die Sicherheitsmechanismen in SNMPv3 sind von verschiedenen Vorläuferversionen übernommen worden. Durch die Modularisierung ist allerdings ein schrittweiser Umstieg auf SNMPv3 möglich. Es können sogar einzelne kryptographische Verfahren ausgetauscht werden, ohne eine neue SNMP Version zu benötigen. Hier bietet sich entsprechend auch Potential für eine zukünftige geordnete Evolution von SNMP.

2.3 SNMP Infrastruktur

Im Rahmen der Entwicklung von SNMPv3 wurde auch die SNMP Infrastruktur erweitert. So wurde eine Reihe von MIB Modulen definiert, mit denen Parameter von SNMP Agenten eingestellt werden können. Dies erlaubt z.B. die einheitliche Konfiguration von Empfängern für Ereignismeldungen, was derzeit nur durch proprietäre MIBs möglich ist. Durch die Modularisierung von SNMP und die Arbeiten zur Koexistenz von SNMPv1 und SNMPv3 ist es möglich, diese MIB Module auch im Zusammenhang mit SNMPv1 zu verwenden.

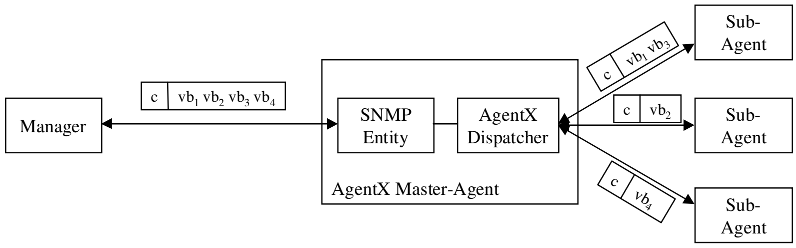
Weitere Erweiterungen der Infrastruktur betreffen die Behandlung von Ereignismeldungen. Durch die Benutzung der SNMPv2 Protokolloperationen ist es möglich, Ereignismeldungen unbestätigt (Traps) oder bestätigt (Informs) zu übermitteln. Die gewünschte Art der Übertragung wird durch eine MIB Variable kontrolliert. Außerdem ist es möglich, die Übertragung einer Ereignismeldung abhängig vom Ereignistyp und den Variablen, die das Ereignis beschreiben, zu unterdrücken. Damit existiert ein Mechanismus, die Weiterleitung von „störenden“ Ereignismeldungen bereits an der Quelle zu unterbinden.

Desweiteren existiert ein Vorschlag für ein MIB Modul, mit dem Ereignismeldungen in einem lokalen Log abgelegt werden können. Dadurch kann gewährleistet werden, daß bei zeitlich begrenzten Partitionierungen eines Netzes oder bei Überlastsituationen keine Ereignismeldungen verloren gehen. Die Menge der im Log zu speichernden Ereignisse wird ebenfalls durch einen Filtermechanismus eingeschränkt und kann so geeignet kontrolliert werden.

Die soeben beschriebenen Erweiterungen der Infrastruktur sorgen dafür, daß Ereignismeldungen in der Zukunft wesentlich mehr Gewicht zugesprochen werden kann, da eine zuverlässige Weiterleitung von gefilterten Ereignismeldungen möglich ist.

2.4 Erweiterbare Agenten

Erweiterbare SNMP Agenten erlauben es, MIB-Module separat zu implementieren. Ein erweiterbarer Agent bietet im Gegensatz zu einem Proxy-Agenten einen für den Manager transparenten Zugriff [EMVA 95]. Erweiterbare Agentensysteme sind von hoher praktischer Bedeutung für alle Hersteller, die Produkte auf mehreren Plattformen anbieten. Ein Standard-Protokoll zur Realisierung von erweiterbaren Agenten senkt deutlich die Kosten für die Unterstützung verschiedener Betriebssysteme und Plattformen.



Lange hat sich die IETF gegen eine Standardisierung von Protokollen für erweiterbare Agenten gesperrt. Es gab mehrere proprietäre Ansätze wie z.B.

SMUX, DPI oder EMANATE, die aber wiederum Hard- und Softwarehersteller an die Lieferanten dieser proprietären Ansätze gebunden haben.

Im Januar 1998 wurde das Agent Extensibility Protokoll (AgentX) in der Version 1 als Proposed-Standard veröffentlicht [RFC 2257]. Dieses Protokoll schafft den lang vermißten Standard für erweiterbare Agenten. AgentX beschränkt sich in der Version 1 bewußt auf die elementaren Funktionen, um so die Kosten für den Einstieg in diese Technologie gering zu halten. Dadurch lassen sich allerdings mit AgentX auch nicht alle MIB-Module als erweiterbare Agenten realisieren. Insbesondere erlaubt AgentX derzeit einem sogenannten Subagent nicht, Zugriffskontrollrechte auf beliebige MIB Objekten zu prüfen oder gar die Werte beliebiger MIB-Objekte unter Beachtung der Zugriffskontrolle zu lesen. Dies hat zur Folge, daß Realisierungen von MIBs, die die Überprüfung von Zugriffsrechten auf andere MIB Objekte erfordern, derzeit nicht möglich ist. Dies ist sicherlich auch eine Folge der Tatsache, daß AgentX parallel zu den SNMPv3 Spezifikationen entwickelt worden ist.

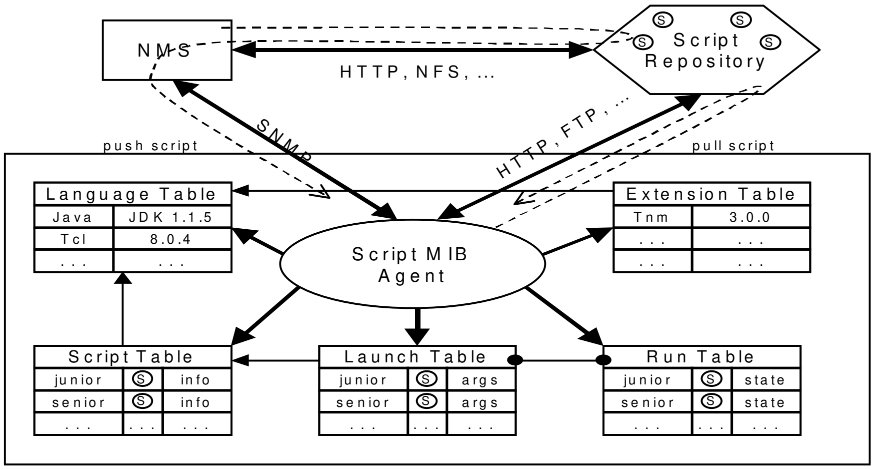
Derzeit existieren mehrere kommerzielle Implementationen von AgentX. An der Carnegie Mellon Universität wird an einer frei verfügbaren Implementation von AgentX gearbeitet.

2.5 Verteiltes Management

Die Skalierbarkeit von Managementsystemen kann im allgemeinen nur durch die Dezentralisierung von Managementfunktionen verbessert werden. Eine spezielle Arbeitsgruppe der IETF hat sich diesem wichtigen Thema angenommen und MIBs entwickelt, mit denen wichtige und häufig benutzte Teilfunktionen dezentral realisiert werden können. Dabei war eine der wichtigsten Randbedingungen die Integration in die Sicherheitsfunktionen von SNMPv3.

Innerhalb der Arbeitsgruppe werden zwei Wege parallel verfolgt. Zum einen wird an der Definition von MIBs gearbeitet, die häufig benötigte Teilfunktionen in MIB Modulen festschreiben. Beispiele hierfür sind die Expression MIB [RFC EX] und die Event MIB [RFC EV], mit denen Ausdrücke über MIB Objekte definiert werden können und beim Über- oder Unterschreiten von Grenzwerten Ereignismeldungen generiert werden. (Die Expression MIB und die Event MIB sind logisch gesehen Weiterentwicklungen der Alarm-Gruppen in RMON.) Außerdem gibt es einen Vorschlag für eine MIB, mit der sich Ping- und Traceroute-Funktionen auf entfernten Agenten ausführen lassen.

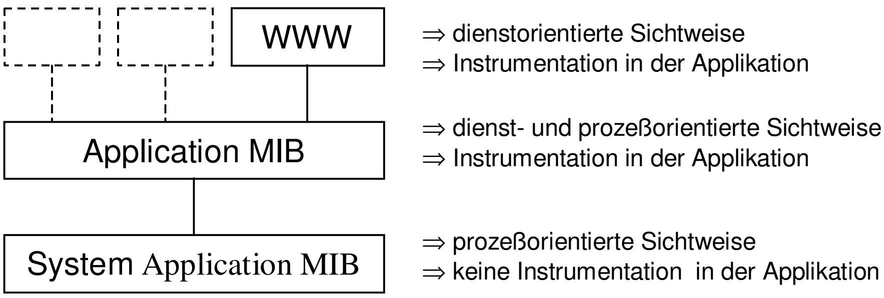
Ein anderer Teil der Arbeitsgruppe beschäftigte sich mit der Frage, wie beliebige Managementfunktionen dynamisch verteilt und aktiviert werden können (management by delegation). Das Ergebnis ist die Script MIB, mit der ausführbare Managementfunktionen auf Netzelementen installiert und aktiviert werden können [RFC SM, CN97]. Mit Hilfe der Scheduling MIB können Managementfunktionen periodisch oder zu einem festem Datum aktiviert bzw. deaktiviert werden [RFC SD].



Für die Script MIB liegen mittlerweile zwei unabhängige Implementationen vor. Beide Implementationen benutzen eine virtuelle Java Maschine als Laufzeitumgebung. Eine Implementation, die an der TU Braunschweig in Kooperation mit NEC C&C Research in Berlin realisiert wurde, erlaubt die Unterstützung von beliebigen Laufzeitumgebungen und Sprachen durch ein entsprechendes Protokoll zwischen der Script MIB Implementation und den Laufzeitumgebungen [IM 99].

2.6 Management von Applikationen und Diensten

Die andere Arbeitsgruppe innerhalb der IETF hat in den letzten Jahren an einem Satz von MIBs zum Management von Applikationen gearbeitet. Die grundlegende MIB hat eine systemweite Sicht auf Applikationen und läßt sich ohne eine Instrumentierung der Applikationen implementieren [RFC 2287].



Darauf aufbauend definiert die Application Management MIB Objekte, die für viele Applikationen angewendet werden können, aber im allgemeinen eine Instrumentation der Applikation erfordern [RFC APP]. Hier findet man insbesondere Information über geöffnete Dateien und bestehende Netzverbindungen. Auf diesen geöffneten Kanälen können Transaktionsströme existieren, über die Statistiken bereitstellt werden. Bei der Definition der MIB wurde außerdem darauf geachtet, daß eine Realisierung der Instrumentierung mit Hilfe der Application Response Time Monitoring (ARM) API möglich ist.

Die dritte Ebene besteht aus MIBs, die für spezielle Arten von Applikationen MIB Objekte definieren. Derzeit gibt es auf dieser Ebene nur die WWW Services MIB, die zum Management von WWW Diensten definiert wurde [RFC W3, DSOM 97]. Es ist zu erwarten, daß auf der dritten Ebene weitere MIBs für spezielle Arten von Applikationen entstehen werden.

Es bleibt zu erwähnen, daß die Bereitstellung von Instrumentierungen in Applikationen nur durch ein allgemein akzeptiertes Protokoll für erweiterbare Agenten möglich ist. In diesem Sinn schafft der AgentX Standard die Basis für eine erfolgreiche Umsetzung der MIBs zum Management von Applikationen und Diensten.

3. Ungelöste Probleme

Dieser Abschnitt gibt einen Überblick über weiterhin ungelöste Probleme im Zusammenhang mit den Internet Management Standards.

3.1 Fehlende Basis-Datentypen

Die SMIv2 und die SNMPv2 Protokolloperationen unterstützen nur einen unvollständigen Satz von Basis-Datentypen. Bei der Einführung von 64-Bit Zählern (Counter64) während der Entwicklung von SNMPv2 hat man die Unterstützung von anderen 64-Bit Datentypen (Unsigned64 und Integer64) für nicht notwendig erachtet. Mittlerweile ist in verschiedenen Arbeitsgruppen der Bedarf an einem kompletten Satz von 64-Bit Datentypen deutlich geworden.

Es gibt derzeit auch keine Basis-Datentypen für Gleitpunktzahlen (Float, Double), da in den meisten Fällen durch geeignete Skalierungen Gleitpunktzahlen vermieden werden können. Andererseits wäre es sicherlich naheliegend, einen kompletten Satz von Basis-Datentypen bereitzustellen, wie er auch in den meisten gebräuchlichen Programmiersprachen existiert.

Die Einführung neuer Datentypen ist eng verzahnt mit der Art und Weise, wie die SNMP Protokolloperationen definiert sind. Da SNMPv3 die Protokolloperationen von SNMPv2 verwendet, wurden an dieser Stelle auch keine Änderungen vorgenommen. Insbesondere fehlt derzeit ein Erweiterungsmechanismus, der die kontrollierte Einführung von neuen Basis-Datentypen erlaubt, ohne etwa die Versionsnummer des Protokolls inkrementieren zu müssen. Es existiert ein Vorschlag zur Benutzung des Datentyps Opaque, um die Kompatibilität zwischen SNMP Implementationen zu gewährleisten, die verschiedene Mengen von Basis-Datentypen unterstützen. Dieser Vorschlag ist jedoch umstritten, da ein Teil der SNMPv3 Arbeitsgruppe durch die Benutzung des Opaque Datentyps Interoperabilitätsprobleme befürchtet.

Da das Fehlen eines vollständigen Satzes von 64-Bit Datentypen ein drängendes Problem in mehreren IETF Arbeitsgruppen darstellt, ist damit zu rechnen, daß eine Arbeitsgruppe bzw. ein Entwurfsteam im Laufe des Jahres 1999 mit der Lösung dieses Problems beauftragt wird.

3.2 Unterstützung neuer Protokolloperationen

Die Modularisierung von SNMPv3 beschränkt sich auf das Nachrichtenformat und die Sicherheitsprotokolle. Es war während der Entwicklung von SNMPv3 nicht vorgesehen, etwa über die Unterstützung neuer Protokolloperationen nachzudenken. Als Folge ist SNMPv3 sehr eng an die SNMPv2 Protokolloperationen gebunden. Es existiert derzeit kein Erweiterungsmechanismus, mit dem neue Protokolloperationen mit vertretbarem Aufwand eingeführt werden können.

Zur Lösung dieses Problem sind ebenfalls zwei Ansätze denkbar. Einerseits kann man die existierenden SNMPv3 Spezifikationen so interpretieren, daß eine kontrollierte Erweiterung der Protokolloperationen ohne Einführung einer neuen Version möglich ist. Andererseits kann durch die Einführung einer neuen Version das Problem eleganter und unter Vermeidung eventueller Interoperabilitätsprobleme gelöst werden.

Da mit der Einführung einer neuen Version sowohl das Problem fehlender Basis-Datentypen als auch das Problem der Unterstützung neuer Protokolloperationen gelöst werden kann, gewinnt diese Lösung an Attraktivität. Andererseits sind die Kosten einer weiteren Version von SNMP sehr hoch, da dies auch als ein Zeichen für fehlende Stabilität der SNMPv3 Spezifikationen interpretiert werden kann.

3.3 Erweiterung der SMI

Mit der Überarbeitung der SMIv2 zu einem Internet-Standard sind natürlich nicht alle Probleme der SMIv2 behoben. Insbesondere besteht Bedarf, zusätzliche Informationen maschinenlesbar in MIB Modulen abzulegen. Dadurch könnten Werkzeuge zur Generierung von MIB Implementationen einen höheren Automatisierungsgrad erreichen und leistungsfähigere generische Management-Applikationen realisiert werden. Beispiele sind etwa die maschinenlesbare Beschreibung der Zeitbasis und des Diskontinuitätsindikators für Zählvariablen (Counter32 und Counter64) oder die Festlegung von Beziehungen zwischen MIB Objekten (beispielsweise ist eine Interpretation eines TAddress Werts nur unter Kenntnis des entsprechenden TDomain Werts möglich).

Ein weiteres Problem der SMIv2 ist deren Abhängigkeit von ASN.1 [ASN1]. Die verwendete Version von ASN.1 stammt aus dem Jahre 1988 und ist zum einen schwer zugänglich und zum anderen auch schwer verständlich. Es wäre daher sinnvoll, bei der Definition einer neuen SMI die Abhängigkeit von ASN.1 aufzulösen und die Sprache mit allen lexikalischen und grammatikalischen Regeln in einem eigenständigen Dokument zu spezifizieren.

Derzeit hat ein solches Projekt innerhalb der IETF eine relativ geringe Priorität. Es laufen aber zur Zeit Arbeiten an der TU Braunschweig, in denen verschiedene Möglichkeiten zur Erweiterung der SMI untersucht und prototypisch implementiert werden. Ein wichtiger Aspekt ist dabei die Gewährleistung einer automatisierten Umsetzung zwischen einer neuen SMI und der derzeit gültigen SMIv2. Dies schränkt natürlich den Lösungsraum stark ein. Ohne eine automatisierten Umsetzung von MIB Modulen ist jedoch eine neue SMI nicht praktisch anwendbar.

3.4 Effiziente Übertragung von großen Datenmengen

Die effiziente Übertragung großer Datenmengen mit SNMP ist weiterhin ein ungelöstes Problem. Die Einführung der get-bulk Operation in SNMPv2 liefert zwar eine Beschleunigung, die aber nicht ausreicht, um große Tabellen effizient übertragen zu können. Dies liegt nicht zuletzt daran, daß die Kodierung der Information extrem ineffizient ist und durch die Begrenzung der Nachrichtengrößen und fehlende Flußkontroll- und Fehlerbehebungsmechanismen in dem normalerweise verwendeten Transport über UDP Probleme auftreten können. Außerdem verlangt die Benutzung der get-bulk Operation, daß der Manager eine Vorstellung über den Umfang der erfragten MIB Objekte besitzt, da er sonst riskiert, über das Ende einer Tabelle hinauszuschießen.

Alle diese Probleme lassen sich mit drei relativ kleinen Erweiterungen befriedigend lösen:

1. Die offizielle Anerkennung von TCP als möglichen Transport von SNMP Nachrichten löst die Flußkontroll- und Fehlerbehandlungsproblematik. Mittlerweile verfügen fast alle Geräte über eingebettete TCP Protokollmaschinen, so daß die Kosten vertretbar sind. Natürlich sollte SNMP über UDP weiterhin zum regelmäßigen Überwachen von Geräten (polling) verwendet werden. Es sollte die freie Entscheidung des Entwicklers einer Management-Applikation sein, welcher Transport für eine gegebene Aufgabe die effektivste Lösung ist.

2. Das Sicherheitsmodell von SNMPv3 erlaubt die Definition weiterer Authentifizierungs- und Verschlüsselungsverfahren. Dies kann man benutzen, um neue Verschlüsselungsverfahren zu definieren, die eine Komprimierung der Nutzlast durchführen. Experimente haben gezeigt, daß Kompressionsraten von 80-90% sehr einfach zu erreichen sind.

3. Durch die Einführung einer neuen Protokolloperation, mit der ganze MIB-Teilbäume (und damit eben auch Tabellen) gelesen werden können, lassen sich die Probleme der get-bulk Operation lösen. Da viele SNMP Agenten nur begrenzte Datenpuffer zur Verfügung haben, muß dafür gesorgt werden, daß die Übertragung der Antwort auch mit begrenzten Puffern möglich ist. Die Lösung dieses Problems besteht in der Aufteilung der Antwort in eine Sequenz von Antwortnachrichten. All dies ist ohne Änderung des Nachrichtenformats der SNMPv2 Protokolloperationen möglich.

Derzeit arbeitet eine Gruppe von Mitarbeitern verschiedener europäischer Universitäten (EPFL Lausanne, Universität Twente, Universität Pisa, TU Braunschweig) an der Spezifikation und Implementation des oben skizzierten Lösungsansatzes. Alternative Ansätze sehen die Verwendung von Dateitransferprotokollen wie FTP zum Austausch großer Datenmengen vor. Der große Nachteil dieser Ansätze ist jedoch, daß sich dadurch neue Sicherheitsproblematiken ergeben.

3.4 Beschreibung von Operationen auf MIB Objekten

Die SMI modelliert Operationen als Seiteneffekte von Schreiboperationen auf MIB Objekten. Aufgrund der fehlenden Sicherheit in SNMPv1 gibt es derzeit relativ wenige schreibbare MIB Objekte. Durch die Einführung von SNMPv3 wird sich dies aber ändern. Die SNMPv3 Spezifikationen enthalten selbst etliche MIB Module, die die Konfiguration von SNMP Agenten durch schreibbare MIB Objekte ermöglichen.

Zur effizienten Benutzung dieser Operationen ist es erforderlich, Bibliotheken zu erstellen, die Sequenzen von Schreiboperationen auf ausgewählten Objekten als Funktionen aufrufbar machen. Beispielsweise würde eine derartige Bibliothek für SNMPv3 Funktionen zum Einrichten eines Benutzers, zum Ändern der benutzten Schlüssel und zur Konfiguration der Zugriffskontrolle umfassen. Bei der Realisierung dieser Funktionen ist es oftmals notwendig, mehrere MIB Objekte in einer sinnvollen Reihenfolge zu manipulieren. Eine Beschreibung, wie solche Operationen zu kombinieren sind und wie Fehlerfälle behandelt werden sollen, fehlt jedoch in den meisten MIB Spezifikationen. Dies führt schließlich zu unterschiedlichen Strategien, die im Extremfall eine gleichzeitige Benutzung verschiedener Werkzeuge verhindern.

Es wäre daher sinnvoll, zu MIB Modulen weitere Spezifikationen zu veröffentlichen, die Hinweise zur Benutzung der MIB Module geben. Im Idealfall würde eine solche Beschreibung in maschinenlesbarer Form erfolgen, so daß daraus automatisch entsprechende Funktionsbibliotheken generiert werden können.

3.6 Standardisierte Programmierschnittstellen

Es gibt derzeit keine offiziell standardisierten Programmierschnittstellen für SNMP. Dies behindert die Portabilität von Managementapplikationen zwischen verschiedenen Betriebssystemen und Plattformen.

Die WinSNMP API (basierend auf C) besitzt sicherlich im Windows-Umfeld eine gute Verbreitung und breite Unterstützung der Hersteller. Die Verbreitung von WinSNMP unter anderen Betriebssystemen ist jedoch eher gering. Die SNMP++ API (basierend auf C++) ist dagegen eher über Betriebssystem- und Plattformgrenzen hinweg portabel. Allerdings liefern nur wenige Hersteller eine SNMP++ API aus. Für die Sprache Java gibt es eine ganze Reihe verschiedener APIs und es ist derzeit nicht abzusehen, ob sich eine der APIs als defacto Standard durchsetzen wird. Ähnlich sieht es auch im Bereich der Skript-Sprachen wie Perl oder Tcl aus. Auch hier gibt es viele verschiedene APIs, was die Portabilität von Skripten deutlich einschränkt und die Programmierer an die Hersteller der Spracherweiterungen bindet.

Traditionell versteht sich die IETF nicht als Standardisierungsgremium für Programmierschnittstellen. Andererseits sind brauchbare weit verbreitete APIs mit eine Voraussetzung, um Applikationen, die bestimmte Protokolle nutzen, weit verbreiten zu können. So findet beispielsweise die Erweiterung der BSD socket-Schnittstelle zur Unterstützung von IPv6 innerhalb der entsprechenden IETF Arbeitsgruppe statt. Vielleicht ist dies ein Modell, das auch für eine Vereinheitlichung von SNMP APIs genutzt werden kann. Ein entsprechender Vorschlag wurde bereits von den Entwicklern der WinSNMP API an die IETF herangetragen.

4. Zusammenfassung und Bewertung

In diesem Beitrag wurden zunächst die wichtigsten der in den letzten zwei Jahren vorgenommenen Änderungen an den Internet Management Standards skizziert. Wesentliche Elemente sind die Verabschiedung von SNMPv3 (Modularisierung und Sicherheit), die Festschreibung der SMIv2 (Ablösung der SMIv1), die Schaffung eines Standards für erweiterbare SNMP Agenten (AgentX) sowie die Arbeiten zur Verteilung von Managementfunktionen und zum Management von Applikationen. Obwohl die erarbeiteten Lösungen sicher nicht in allen Aspekten optimal sind, zeigt doch schon allein der Umfang, daß die Arbeit an den Internet Management Standards in der IETF nach einer Phase der Spaltung und Zerrüttung wieder erfolgreich und produktiv fortgesetzt wird. Trotz anhaltender und oftmals sehr engagiert geführter Diskussionen um technische Details ist insgesamt eine positive Bewegung zur Lösung realer Probleme erkennbar.

Betrachtet man die weiterhin bestehenden Probleme, so lassen sich einige mit relativ einfachen Mitteln lösen. Sollte es möglich sein, in evolutionären Schritten Konsens über mögliche Lösungen zu schaffen und diese Lösungen in Implementationen und Produkte umzusetzen, dann hat das SNMP-basierte Management durchaus gute Zunkunftsaussichten.

Literatur

[RFC 1157] J. Case, M. Fedor, M. Schoffstall, J. Davin, A Simple Network Management Protocol (SNMP), RFC 1157, Mai 1990.

[RFC 1155] M. Rose, K. McCloghrie, Structure and Identification of Management Information for TCP/IP-based Internets, RFC 1155, Mai 1990.

[RFC 1212] M. Rose, K. McCloghrie, Concise MIB Definitions, RFC 1212, März 1991.

[RFC 1215] M. Rose, A Convention for Defining Traps for use with the SNMP, März 1991.

[PIK 95] J. Schönwälder, Zur aktuellen Entwicklung von SNMPv2, Praxis der Informationsverarbeitung und Kommunikation, 18(4), 1995.

[RFC SMI] K. McCloghrie, D. Perkins, J. Schönwälder, M. Rose, J. Case, S. Waldbusser, Structure of Management Information Version 2 (SMIv2), RFC (to appear), 1999.

[RFC TC] K. McCloghrie, D. Perkins, J. Schönwälder, M. Rose, J. Case, S. Waldbusser, Textual Conventions for SMIv2, RFC (to appear), 1999.

[RFC CONF] K. McCloghrie, D. Perkins, J. Schönwälder, M. Rose, J. Case, S. Waldbusser, Conformance Statements for SMIv2, RFC (to appear), 1999.

[RFC 2271] D. Harrington, R. Presuhn, B. Wijnen, An Architecture for Describing SNMP Management Frameworks, RFC 2271, Januar 1998.

[RFC 2272] J. Case, D. Harrington, R. Presuhn, B. Wijnen, Message Processing and Dispatching for the Simple Network Management Protocol, RFC 2272, Januar 1998.

[RFC 2273] D. Levi, B. Meyer, B. Stewart, SNMPv3 Applications, RFC 2273, Januar 1998.

[RFC 2274] U. Blumenthal, B. Wijnen, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol, RFC 2274, Januar 1998.

[RFC 2275] B. Wijnen, R. Presuhn, K. McCloghrie, View-based Access Control Model (VACM) for the Simple Network Management Protocol, RFC 2275, Januar 1998.

[EMVA 95] J. Schönwälder, Einbindung applikations-spezifischer Agenten in das SNMP Management, Proc. EMVA ´95, Dortmund, Oktober 1995.

[RFC 2257] M. Daniele, B. Wijnen, D. Francisco, Agent Extensibility (AgentX) Protocol Version 1, RFC 2257, Januar 1998.

[RFC EX] B. Stewart, Expression MIB, work in progress, November 1998.

[RFC EV] B. Stewart, Event MIB, work in progress, Oktober 1998.

[RFC SM] D. Levi, J. Schönwälder, Definitions of Managed Objects for the Delegation of Management Scripts, RFC (to appear), 1999.

[CN 97] J. Schönwälder, Network Management by Delegation - From Research Prototypes Towards Standards, Computer Networks and ISDN Systems, November 1997.

[RFC SD] D. Levi, J. Schönwälder, Definitions of Managed Objects for Scheduling Management Operations, RFC (to appear), 1999.

[DSOM 97] J. Schönwälder, M. Toet, Management of the World Wide Web, Proc. DSOM ´97, Oktober 1997.

[IM 99] J. Schönwälder, J. Quittek, Secure Management By Delegation within the Internet Management Framework, Proc. IM ´99, Boston 1999. (to appear)

[RFC 2287] C. Krupczak, J. Saperia, Definitions of System-Level Managed Objects for Applications, RFC 2287, Februar 1998.

[RFC APP] C. Kalbfleisch, C. Krupczak, R. Presuhn, J. Saperia, Application Management MIB, RFC (to appear), 1999.

[RFC W3] H. Hazewinkel, C. Kalbfleisch, J. Schönwälder, Definitions of Managed Objects for WWW Services, RFC (to appear), 1999.

[ASN1] D. Steedman, Abstract Syntax Notation One (ASN.1), Technology Appraisals, 1990.