Diplomarbeit

Status des sicheren Netzwerkmanagement-Protokolls SNMPv3

Ausgeführt zum Zweck der Erlangung des akademischen Grades eines
Dipl.-Ing. (FH) für Telekommunikation und Medien
am Fachhochschul-Diplomstudiengang Telekommunikation und Medien St. Pölten

unter der Leitung von

Dipl.-HTL-Ing. Andreas Schaupp MSc MAS

Zweitbegutachtung von

FH Prof. Dipl. Ing. Johann Haag

ausgeführt von

Martin Schwaiger
tm0210038107

St. Pölten, im September 2006

Ehrenwörtliche Erklärung

Ich versichere, dass

- ich diese Diplomarbeit selbstständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich auch sonst keiner unerlaubten Hilfe bedient habe.

- ich dieses Diplomarbeitsthema bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.

Diese Arbeit stimmt mit der vom Begutachter beurteilten Arbeit überein.

……. ……..……

Ort, Datum Unterschrift

Kurzfassung

Die heutige Komplexität von Computernetzwerken macht es unmöglich, sie mit menschlichem Einsatz allein zu überwachen. Die Verwendung von Netzwerkmanagementtools ist gerade für größere Unternehmen unabdingbar.

Um das breite Spektrum an verschiedenen eingesetzten Netzwerkkomponenten mit einem System kontrollieren und steuern zu können, war es in der Vergangenheit notwendig, ein entsprechendes Netzwerkprotokoll zu entwickeln. Dieses im Jahr 1990 entstandene Protokoll nennt sich SNMP und wird in der Urversion (SNMP Version 1, kurz SNMPv1) von sehr vielen Geräten unterstützt. Bei der Entwicklung von SNMPv1 stand Funktionalität im Vordergrund und somit wurden praktisch keine Sicherheitsmechanismen integriert.
Neuere Versionen von SNMP (Version zwei und drei, letztere stammt aus dem Jahr 2002) bringen etliche Abhilfen und Verbesserungen mit sich. Ab Version drei ist ein verschlüsselter und authentifizierter Datenaustausch möglich, außerdem existieren ab dieser Version komplexere Möglichkeiten für die Vergabe von Zugriffsberechtigungen. Für den Einsatz von neueren SNMP Versionen ist es aber erforderlich, dass das Managementsystem und die Netzwerkkomponenten die entsprechende Version unterstützen. Ob dies bei aktuellen Komponenten bekannter Hersteller der Fall ist, wird in dieser Diplomarbeit untersucht.
Zusätzlich wird darauf eingegangen, ob die im Standard spezifizierten Sicherheitsmaßnahmen von den Herstellern vollständig umgesetzt wurden, oder ob nur Teile davon zur Anwendung kommen.

Im letzten Teil dieser Diplomarbeit wird ein Leitfaden für die Migration von SNMPv1 auf SNMPv3 für Unternehmen erstellt. Im Zuge dessen wird eine Teststellung mit Standardkomponenten inklusive Musterkonfiguration kreiert.

Schlussendlich soll der aktuelle Status der Verbreitung von SNMPv3 aufgezeigt werden. Dazu werden mögliche Gründe für die weniger rasante Verbreitung von SNMPv3 gegenüber seinen Vorgängern analysiert.

Abstract

The complexity of contemporary computer networks makes it impossible to keep them under surveillance with human employment only. Especially for larger companies, the usage of network management tools is indispensable.

To control and operate the broad spectrum of different network components with one system, it was necessary to develop an appropriate network protocol in the past. This protocol, generated in the year 1990, is named SNMP and is supported by many devices in the basic version (SNMP version 1, in short SNMPv1). During the development of SNMPv1, functionality had priority, for which reason virtually no safety mechanisms were integrated.
Newer versions of SNMP (version 2 and 3, latter originated in the year 2002) implicate several correctives and improvements. From version 3 on, an encrypted and authenticated data exchange is possible. In addition more complex possibilities exist for the award of access authorisations.
For the use of newer SNMP versions it is necessary that the management system and the network components support the appropriate version.
If this is the case with current components of the producers, is determined in this diploma thesis.

Furthermore the question is discussed, whether the safety measures, specified in the standard, were completely realised by the producers, or only parts of it.

In the last part of this work, a guideline for the migration from SNMPv1 to SNMPv3 is developed and a test with a sample configuration is created.

Finally, the current status of the distribution of SNMPv3 shall be shown. In addition this, possible reasons for the less rapid spread of SNMPv3 in comparison to its predecessors will be analysed.

Inhaltsverzeichnis

1. Einleitung

In der heutigen Zeit ist es wohl für die wenigsten Unternehmen denkbar, auf Computersysteme und des Weiteren auf deren Vernetzung zu verzichten. Auch kurze Ausfälle sind meist schon mit hohen Kosten verbunden. Genau aus diesem Grund ist es für moderne Unternehmen wichtig, das Netzwerk und alle wichtigen Komponenten zu überwachen und über deren genauen Status jederzeit Bescheid zu wissen. Im Ernstfall können so Stillstandszeiten wesentlich minimiert werden, da defekte Komponenten nicht erst langwierig gesucht werden müssen.

Die meisten Netzwerkkomponenten besitzen die Möglichkeit, über ihren Status Informationen preis zu geben. Da diese aber wiederum über das Netzwerk übertragen werden, sind spezielle Maßnahmen erforderlich, damit diese Informationen geschützt und nicht einfach mitgelesen und missbräuchlich verwendet werden können.

Des Weiteren bieten viele Netzwerkkomponenten bei entsprechender Konfiguration die Möglichkeit, nicht nur Informationen über ihren Status bekannt zu geben, sondern mit den gleichen Mechanismen auch aktiv gesteuert werden zu können. Gerade für diesen Fall ist es unerlässlich, mit geeigneten Schutzmaßnahmen Missbrauch zu unterbinden. Man bedenke, dass damit „remote“ (aus der Ferne) komplette Netzwerke lahm gelegt werden könnten.

Es existieren mehrere Möglichkeiten zur „remote“-Administration von Komponenten. Eine davon ist mittels des speziellen Netzwerkprotokolls SNMP[1]. Dieses Protokoll wird in der Urversion (SNMP Version 1, kurz SNMPv1) von sehr vielen Geräten unterstützt.
SNMPv1 sieht aber nur ansatzweise Möglichkeiten vor, die Informationen nur autorisierten Personen zugänglich zu machen. Ein Mechanismus zur sicheren Übertragung fehlt gänzlich. Auf diese und andere Risiken und Gefährdungen soll eingegangen werden.

[1] simple network management protocol

Neuere Versionen von SNMP (Version zwei und drei) bringen etliche Abhilfen und Verbesserungen mit sich.
Für den Einsatz von neueren SNMP Versionen ist es erforderlich, dass das Managementsystem und die Netzwerkkomponenten die entsprechende Version unterstützen.

Da SNMP in der Urversion ein hohes Risiko darstellt, ist es Unternehmen zu empfehlen, auf höhere Versionen umzusteigen. In der Praxis muss man dafür aber einige Dinge wie Hardware, Software und nötige Konfigurationsanpassungen berücksichtigen.

Das Ziel dieser Diplomarbeit ist es, den aktuellen Status der Verbreitung von SNMPv3 aufzuzeigen und einen Leitfaden für die Migration von SNMPv1 auf SNMPv3 für Unternehmen zu erstellen.
Dazu werden zuerst grundsätzliche Ziele und Problematiken beim „remote“ (Netzwerk) Management von Systemen analysiert. Es soll dabei auf mögliche Gefährdungen eingegangen werden. Anschließend werden der Einsatz, die Verbreitung und die Gefahren, die SNMPv1 mit sich bringt, behandelt. Durch Untersuchung der Mechanismen von SNMPv3 sollen Verbesserungen und Abhilfen zu früheren Versionen aufgezeigt werden.

Nach Abklärung dieser Punkte gilt es die eigentlichen Fragestellungen der Diplomarbeit zu beantworten: Um die spezifische Frage nach Unterstützung in aktuellen Managementsystemen und Netzwerkkomponenten klären zu können, wird mit Hard- und Software Herstellern Kontakt aufgenommen. Im Zuge dessen wird eine Teststellung implementiert.
Schlussendlich soll ein Leitfaden für die Migration von SNMPv1 auf SNMPv3 für mittlere Unternehmen entstehen.

2. Netzwerkmanagement Allgemein

2.1 Einführung

Durch das enorme Wachstum von Computernetzwerken, werden sie immer wichtiger und spielen eine immer größere Rolle für Unternehmen. Der Trend geht zu komplexeren Netzwerken, die mehr Anwendungen und mehr Benutzer unterstützen.
Genau aus diesem Grund ist es schon lange nicht mehr möglich, Computernetzwerke mit menschlichem Einsatz alleine zu überwachen. Die Verwendung von Netzwerkmanagementtools ist gerade für größere Unternehmen unabdingbar.

Die Anforderungen an solche Software sind oft sehr hoch, da Unternehmen meist sehr viele unterschiedliche Netzwerkkomponenten im Einsatz haben. Moderne Netzwerke bestehen schon längst nicht mehr nur aus Modems, Router, Switches und Server. Viele andere Komponenten wie zum Beispiel WLAN[2] Accesspoints, Printserver, Netzwerkfähige Drucker, Kopierer und Scanner, Firewalls, Klimaanlagen, unterbrechungsfreie Stromversorgungen aber auch proprietäre Lösungen für die unterschiedlichsten Aufgaben sind mit modernen Netzwerken verbunden und steigern dessen Komplexität. Zu diesen ganzen Hardwarekomponenten kommt noch eine Fülle von Softwareapplikationen, wie zum Beispiel Windows, Unix, Linux, Datenbanksysteme, Netzwerkdienste (DNS[3], DHCP[4]…), Applikationsserver und Cluster die ebenfalls enorme Anforderungen an das Netzwerkmanagement stellen, dazu.

Zu dem Zeitpunkt, als die Netzwerke immer größer, komplexer und heterogener wurden, explodierten gleichzeitig die Kosten für das Management, da für jede Produktgruppe ein eigenes Managementsystem notwendig war. Um diese Kosten in den Griff zu bekommen, waren standardisierte Tools, die ein großes Spektrum dieser Produkte abdecken,

[2] Wireless local area network

[3] Domain name system

[4] Dynamic host configuration protocol

notwendig. Erschwerend kommt dazu, dass praktisch alle Produkte von mehreren Herstellern angeboten und auch verwendet wurden.

Gesucht war also eine Möglichkeit, sehr heterogene Netzwerke mit möglichst geringem Aufwand überwachen und steuern zu können. Zusätzlich sollte ein solches System sehr flexibel ausgelegt sein, um einfach und kostengünstig an individuelle Lösungen angepasst werden zu können.

Aus diesem Bedürfnis heraus, wurde SNMP entwickelt. Dazu aber später.

Im Allgemeinen wird mit Netzwerkmanagement das Steuern und Überwachen von Hard- und Software bezeichnet. Die ISO[5] definiert Netzwerkmanagement wie folgt:

„Die Aktivität zur Steuerung, Koordination und Überwachung aller Ressourcen, welche eine Kommunikation ermöglichen“. [ISO 7498-4]

2.2 ISO-Anforderungen

2.2.1 Überblick

Da die Anforderungen, die an ein Netzwerkmanagementsystem gestellt werden, sehr komplex sind, wurden sie von der ISO genau definiert.
Diese Einteilung wurde für das OSI[6] Modell entwickelt und hat bei Herstellern von standardisierter aber auch proprietärer Hardware Anklang gefunden. Das OSI-Management kennt 5 Funktionsbereiche. Diese Bereiche werden „specific management functional areas“ (SMFA) oder FCAPS (Abkürzung der 5 Bereiche) genannt.

[5] International organization for standardization

[6] Open systems interconnection reference model

Die SMFA besteht aus folgenden Bereichen:

- **F** ault Management
- **C** onfiguration Management
- **A** ccounting Management
- **P** erformance Management
- **S** ecurity Management

Die folgenden Punkte stellen eine Zusammenfassung und Umschreibung der Bereiche wie sie die ISO definiert hat, dar. [vgl. ISO 7498-4 und Douglas, 2005]

2.2.2 Fault Management

Fault Management befasst sich mit der Fehlererkennung, Fehlerbehebung und Überwachung des Netzwerkes inkl. seiner Komponenten.

Tritt ein Fehler oder ein Problem auf, gilt es zuerst festzustellen, wo genau das Problem liegt. Danach soll der Rest des Netzwerks von dem Fehler isoliert werden, um den weiteren Betrieb nicht zu stören.
Anschließend sollte das Netzwerk so umkonfiguriert werden, dass der Fehler (z.B. Ausfall einer Komponente) nur minimale Auswirkungen auf das gesamte Netzwerk hat. Zuletzt muss der eigentliche Fehler durch Reparieren oder Austausch der fehlerhaften Komponente behoben werden.

2.2.3 Configuration Management

Configuration Management oder Konfigurationsmanagement wird dazu verwendet, um physische und logische Informationen zu beschreiben. Diese bestehen zum Beispiel aus Ressourcennamen, Adressen, Kontakten usw. Durch eine Sammlung solcher Informationen kann ein Verzeichnis von Netzwerkressourcen anlegt werden.

Zusätzlich ist das Konfigurationsmanagement für die Identifikation, die Überwachung und Kontrolle von Komponenten zuständig. Für diese Aufgaben werden alle Funktionen die im Zusammenhang mit den Konfigurationsdaten stehen, verwendet. Dazu zählen das Sammeln, Darstellen und Kontrollieren von Konfigurationsparametern.

Ein weiterer wichtiger Aufgabenbereich des Configuration Management ist die Bestandsführung durch Erfassung der bestehenden Software-Konfigurationen und die Softwareverteilung. Dazu gehört auch das Änderungsmanagement, bei dem ermittelt wird, welche Veränderungen durch die Software-Verteilung entstehen.

2.2.4 Accounting Management

Unter Accounting Management versteht man in der OSI Umgebung die Abrechnung über die Verwendung von Netzwerkdiensten und deren Zuordnung zu den verursachenden Personen oder Gruppen. Durch Accounting Management kann eventuell auch eine ineffiziente Benutzung des Netzwerks aufgespürt werden. Außerdem ist es für den Netzwerkverantwortlichen leichter, ein Netzwerk zu planen, wenn man bis zu einem gewissen Grad weiß, was der oder die Endbenutzer im Netzwerk machen und welche Auslastung sie im Netz verursachen.
Dieser Teil der OSI SMFA wird meist nicht direkt von heute verfügbarer Software abgedeckt, vielmehr kümmern sich Administratoren darum, das Netzwerk an die Benutzer anzupassen.

2.2.5 Performance Management

Moderne Netzwerke bestehen aus vielen verschiedenen Komponenten, die miteinander kommunizieren. Sie teilen Daten und Ressourcen. Für viele Anwendungen ist aber genau dieser Umstand ein kritischer Punkt.
Bei Performance Management geht es darum, durch Aufzeichnung, Messung und Analyse von Performancedaten so genannte „bottlenecks“ (Flaschenhälse) aufzuspüren. Es sollen Statistiken und Reports über die Auslastung von Netzwerkkomponenten generiert werden

können. Damit ist es möglich, Aussagen über die Auslastung und die Leistungsfähigkeit eines Netzwerks zu treffen.

2.2.6 Security Management

Das Sicherheitsmanagement soll das Netzwerk gegen Gefahren von außen aber auch gegen interne Sicherheitsgefahren schützen. Gefahren von außen können durch Firewalls abgeblockt werden. Innere Sicherheit kann durch Verschlüsselung der zu übertragenden Daten und durch Vergabe von Kennwörtern und Zugangsberechtigungen gewährleistet werden.

Außerdem muss sich das Managementsystem um die Erzeugung, Verteilung und Archivierung von Passwörtern kümmern. Autorisierungsinformationen und andere Zugriffsinformationen müssen verwaltet werden.

2.3 Sicherheit in Netzwerken

2.3.1 Allgemein

Durch die Größe von heutigen Netzwerken, ist man zwangsläufig mit anderen Nutzerkreisen verbunden, die nicht unbedingt vertrauenswürdig sein müssen.
Einige Beispiele dafür sind:

- große Firmen, wo hunderte oder tausende Mitarbeiter vernetzt sind
- das Internet
- Netzwerke, wo unbekannte Personen Zugriff haben

Bei jedem Austausch von Nachrichten über ein Netzwerk, sind viele Komponenten beteiligt. Nachrichten könnten durch fehlende Sicherheitsmaßnahmen eines solchen Gerätes mitgehört und verändert werden.

Speziell im Netzwerkmanagement stellt dies ein großes Problem dar, da veränderte Steuerungsbefehle für das Netzwerk katastrophale Folgen haben könnten. Aber auch das Mitlauschen von Statusinformationen stellt ein erhebliches Sicherheitsrisiko dar.

2.3.2 Definition

Viele Hersteller haben sich auf das Standardsicherheitsmodell CIA (Confidentiality, Integrity und Availability = Vertraulichkeit, Integrität und Verfügbarkeit) geeinigt.

Im Folgenden wird das CIA-Modell näher beschrieben:

- Confidentiality (Vertraulichkeit): Sicherheit gegen Angriffe durch unerlaubtes Abhören. Vertrauliche Informationen dürfen nur für autorisierte Personen verfügbar sein. Unautorisierte Übertragung und Verwendung von Informationen muss eingeschränkt werden.

- Integrity (Integrität): Schutz gegen die Änderung von Informationen. Sie dürfen nicht dahingehend verändert werden, so dass sie unvollständig oder falsch werden. Unbefugte dürfen nicht in der Lage sein, vertrauliche Informationen ändern oder zerstören zu können.

- Availability (Verfügbarkeit): Informationen müssen bei Bedarf für befugte Personen zugänglich sein. Verfügbarkeit ist die Garantie dafür, dass Informationen mit einer vereinbarten Häufigkeit und rechtzeitig abgerufen werden können.

Zusätzlich zum CIA Modell kann man Sicherheit in Zugriffssicherheit und Übertragungssicherheit unterscheiden:
(Literaturempfehlung: [Tanenbaum, 2003, Kapitel 4])

Zugriffssicherheit

- Authentifizierung: Bei der Authentifizierung gilt es festzustellen, ob ein Benutzer der ist, für den er sich ausgibt. Kurz: die Identität des Benutzers wird überprüft.

- Autorisierung: Zuordnung der Rechte für einen Benutzer

- Überwachung: Verhaltensweise eines Benutzers Überwachen

Übertragungssicherheit

- Vertraulichkeit: bedeutet hier, dass übertragene Daten garantiert nur von Sender und Empfänger gelesen werden können.

- Integrität: Unter Integrität versteht man die Sicherheit, dass übertragene Daten nicht verändert wurden. Weiters muss eine eventuelle Veränderung der Daten feststellbar sein.

- Nichtabstreitbarkeit: Der Sender kann nicht abstreiten, eine von ihm „unterschriebene“ Nachricht gesendet zu haben

2.3.3 Bedrohungen

Im Folgenden werden die Arten von Bedrohungen für Computernetzwerke behandelt. Weiters wird auf die Bedrohungen für die einzelnen Teile von Netzwerkmanagementsystemen eingegangen.
[vgl. Stallings, 1999, S. 60]

2.3.3.1 Arten von Bedrohungen

Es gibt naturgemäß mehrere Arten von Bedrohungen für Computer bzw. Netzwerksysteme.

Der normale Informationsfluss geht von der Quelle zum Ziel.

Abbildung 1: Normaler Informationsfluss

Unterbrechung

Aus irgendeinem Grund, ist die Verbindung von Quelle zum Ziel nicht mehr vorhanden. Dies kann z.B. durch physikalisches Zerstören einer Leitung geschehen.
Betrifft: *Verfügbarkeit*

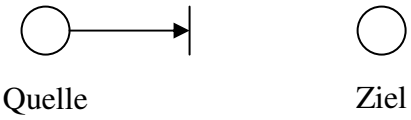

Abbildung 2: Bedrohung - Unterbrechung

Abfangen

Ein unautorisierter Benutzer/System/PC erhält Zugang zu vertraulichen Daten.
z.B. illegales Kopieren von Daten.
Betrifft: *Vertraulichkeit*

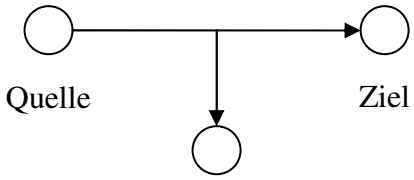

Abbildung 3: Bedrohung - Abfangen

Ändern

Ein unautorisierter Benutzer/System/PC erhält Zugriff auf Daten und verändert diese.
z.B. Änderung eines Logfiles
Betrifft: *Integrität*

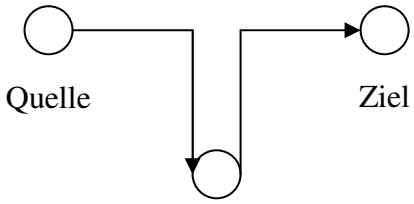

Abbildung 4: Bedrohung - Ändern

Erfinden

Ein unautorisierter Benutzer/System/PC schickt gefälschte Daten an das Ziel.
z.B. Hinzufügen von Daten in ein Logfile
Betrifft: *Integrität*

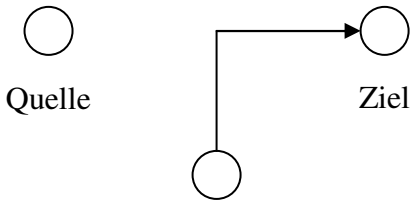

Abbildung 5: Bedrohung - Erfinden

2.3.3.2 Netzwerke

Da über Netzwerke Nutzinformationen aber auch Netzwerkmanagementinformationen übertragen werden, ist für Datenintegrität und Ausfallssicherheit zu sorgen.

Man kann prinzipiell zwischen aktiven und passiven Gefährdungen unterscheiden:

- Unter passive Gefährdungen fallen z.B. das Mitlauschen („sniffen“) von Nachrichten, die über ein Netzwerk gesendet werden. Passive Gefährdungen sind sehr schwer festzustellen, da sie das Netzwerk in deren Funktion nicht beeinträchtigen.

- Aktive Gefährdungen bezeichnen Änderungen oder die Erschaffung von Nachrichten. Sie sind meist einfacher zu finden als passive Gefährdungen.

2.3.3.3 Hardware

Hardware bringt das große Problem der Verfügbarkeit mit sich. Sie ist sehr leicht anfällig auf physische Angriffe. Zudem sind automatisierte Reparaturen praktisch nicht möglich. Gefährdungen liegen hier bei Defekten, Diebstahl und mutwilliger Beschädigung.
Um die Gefahren zu verringen, die durch den Hardwareeinsatz entstehen können, sind in erste Linie physische Maßnahmen notwendig. (z.B. sensible Hardware in eigens abgesicherten Räumen aufbewahren), aber auch administrative Sicherheitsmaßnahmen sind unabdingbar.

2.3.3.4 Software

Die Software ist es, die das Benutzen von Computern und anderen Geräten möglich macht. Die Hauptanforderung an Software ist die Verfügbarkeit. Programme abseits des Betriebssystems, können oft leicht verändert, gelöscht oder kopiert werden. Genau aus diesem Grund ist es absolut notwendig, regelmäßig Backups zu erstellen, um die Verfügbarkeit auf Softwareebene hoch zu halten.
Ein anderes Problem im Softwarebereich sind Programme, die die Funktionsweise der Software beeinträchtigen (beispielsweise Viren, Trojaner usw.).

2.3.3.5 Daten

Das Wertvollste an Netzwerkmanagementsystemen sind die gesammelten Daten. Werden diese Daten gelöscht, unautorisiert verändert oder gelangen sie in falsche Hände, kann dies möglicherweise katastrophale Auswirkungen haben.

2.4 Funktionen des Netzwerkmanagement

Parallel zu dem in Kapitel 2.2 erklärten ISO Anforderungen kann Netzwerkmanagement lt. [Stallings, 1999], in zwei Teilbereiche gegliedert werden.

- Network Monitoring – entspricht im OSI Modell den Aufgabenbereichen „Fault Management“ und „Performance Management“

- Network Control – ist im OSI Modell den Bereichen „Configuration Management“, „Accounting Management“ und „Security Management“ zuzuordnen.

2.4.1 Network Monitoring

Unter Network Monitoring versteht man das ständige Überwachen eines Computernetzwerkes auf Fehler und Engpässe. Gefundene Probleme sollen veranschaulicht werden und falls konfiguriert, soll eine entsprechende Aktion ausgelöst werden, beispielsweise einen zuständigen Administrator per SMS, Email usw. verständigen.

2.4.1.1 Performance Monitoring

Eines der wichtigsten Ziele eines Netwerkmanagementsystems ist die Messung der Performance. Ein Netzwerk kann nur dann kontrolliert werden, wenn die Performance ständig überwacht wird. Dies geschieht durch die Kontrolle geeigneter Parameter.
Nachfolgend sind einige wichtige Parameter für das Performance Monitoring angeführt:
[vgl. Stallings, 1999, S. 29]

Availability

Wird meist in Prozent angegeben. Es gibt an, zu wie viel Prozent ein Netzwerksystem, eine Komponente oder eine Anwendung verfügbar ist. Abhängig von der Komponente, sind sehr hohe Verfügbarkeiten üblich (eine Verfügbarkeit von 99% und mehr stellt keine Seltenheit dar).
Schon kurze Ausfälle sind häufig mit sehr hohen Kosten verbunden.

Response Time

Die Zeit, welche ein System benötig, um auf eine bestimmte Aktion zu reagieren. Wird meist in ms (Millisekunden) gemessen. Generell ist eine niedrige Antwortzeit besser.

Accuracy

„Fehlerfreie" Kommunikation zwischen Systemen ist absolut notwendig für jedes Netzwerk. „Accuracy" sollte dank der eingebauten Fehlerkorrekturmechanismen in den OSI-Schichten DataLink und Transport kein Problem darstellen. Wichtig ist allerdings, die Anzahl der Fehler, die korrigiert werden mussten, mitzuloggen.

Throughput

Der „Durchsatz" ist ein anwendungsorientierter Parameter. Er kann zum Beispiel Anzahl von definierten Transaktionen pro Zeiteinheit sein.

Utilization

Die Auslastung eines Systems ist meist aufschlussreicher, als die Information wie viel Durchsatz ein System schafft. Oft wird die Auslastung dazu verwendet, um Flaschenhälse eines Systems aufzuspüren. Dies ist wichtig, da bei Flaschenhälsen die Antwortzeiten rasch steigen.

2.4.1.2 Fault Monitoring

Die Aufgabe des Fault- oder Fehlermonitorings ist es, Fehler nach Auftreten so schnell als möglich zu finden und ihre Ursache zu bestimmen. Dies kann zum Beispiel durch Aufzeichnung (logging) von wichtigen Ereignissen und Fehlern geschehen. Weiters sollte ein Fehlermonitoringsystem in der Lage sein, gewisse Fehler voraussagen zu können. Dies kann mit Hilfe von definierten Grenzwerten geschehen. Wird ein gewisser Grenzwert überschritten, kann das System einen vielleicht bald auftretenden Fehler vorhersagen.

2.4.2 Network Control

Network-Control behandelt die aktive Steuerung von Computernetzwerken. Es ermöglicht, Einstellungen für die Optimierung von Netzwerken vorzunehmen.

Ein wichtiger Punkt des Network Control ist das Konfigurationsmanagement.
Dieses soll dazu dienen, Daten von Geräten im Netzwerk nicht nur zu sammeln, sondern auch deren Konfiguration verändern bzw. beeinflussen zu können. Weiters ist das Konfigurationsmanagement auch für die Initialisierung, Wartung und Abschaltung von Geräten im Netzwerk zuständig.
Konfigurationsmanagement beinhaltet folgende Funktionen [vgl. Stallings 1999, S. 55]:

Definition der Konfigurationsinformationen

Die Konfigurationsinformation beinhaltet die Art und den Status einer Ressource. Die Strukturierung solch einer Konfigurationsinformation kann auf mehrere Arten erfolgen, der einfachste Fall ist eine einfache Liste von Datenfeldern. Jedes Feld hat genau einen Wert.

Setzen und Verändern der Werte von Eigenschaften

Werte von Eigenschaften sollen natürlich verändert werden können. Dies darf aber nur möglich sein, wenn das Managementsystem autorisiert ist, die entsprechende Information

zu verändern. Weiters gibt es auch Werte, die die Eigenschaften von Netzwerkgeräten angeben (z.B. Anzahl der Ports eines Switches). Diese Werte dürften nicht veränderbar sein.

Man unterscheidet also in Werte, die einen Status wiedergeben und verändert werden dürfen und in Werte, die physische oder logische Zustände repräsentieren und somit softwaremäßig nicht veränderbar sein dürfen.

Initialisieren und Beenden von Netzwerkoperationen

Konfigurationsmanagement soll Benutzern die Möglichkeit geben, Netzwerkoperationen zu initialisieren oder zu beenden.
Beim Initialisieren muss sichergestellt sein, dass alle notwendigen Ressourcen und Beziehungen gesetzt bzw. vorhanden sind. Sollte eine wichtige Information fehlen, muss das Managementsystem entsprechend Bescheid geben.

Software verteilen

Mit Konfigurationsmanagement soll es außerdem möglich sein, Software/ Konfigurationen an diverse Netzwerkkomponenten (z.B. Server, Arbeitsstationen, aber auch Router usw.) zu verteilen. Dazu sind Funktionen wie Feststellen der aktuellen Version, Updaten und generell Managen von mehreren Versionen notwendig.

2.5 Typische NM Systeme

2.5.1 Aufbau

Im Folgenden soll der prinzipielle Aufbau und die Komponenten von typischen Netzwerkmanagementsystemen, die auf TCP/IP[7] basieren, gezeigt und erklärt werden. (siehe Abbildung 6: Aufbau typischer NM Systeme), [vgl. Ghetie, 1997]

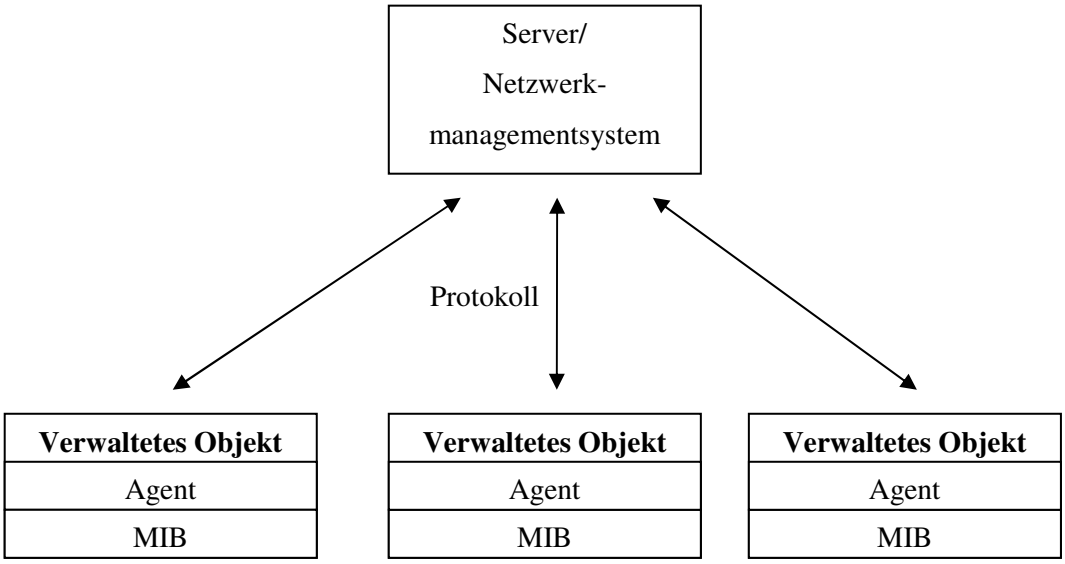

Abbildung 6: Aufbau typischer NM Systeme

Server/Netzwerkmanagementsystem

Hierbei handelt es sich typischerweise um einen PC mit entsprechender Netzwerkmanagementsoftware. Weiters bietet dieses Netzwerkmanagementsystem meist eine Benutzeroberfläche zur Verwaltung der Objekte.

[7] Transmission Control Protocol/Internet Protocol

Das Verwaltete Objekt / Agent / MIB

Die Aufgabe des NMS[8] ist, mehrere Objekte zu Verwalten. Solche Objekte können prinzipiell alle Netzwerkkomponenten sein (Switches, Router, Server, Applicationserver uvm.). Vorraussetzung dafür ist, das ein entsprechender Agent auf den Objekten läuft. Dieser Agent kommuniziert mit dem NMS. Weiters müssen die verwalteten Objekte/Systeme über eine so genannte MIB[9] verfügen. Diese MIBs enthalten die Zuordnung von Systemressourcen zur Position, wo diese Information zu finden ist.

Protokoll

Das Netzwerkmanagementsystem und der Agent kommunizieren über ein definiertes Protokoll.

2.5.2 Polling / Event Reporting

Es werden zwei prinzipielle Arten unterschieden, wie die Information vom Agent zum Managementsystem gelangt [vgl. Douglas, 2005, Kapitel 8 u. 9].
Diese beiden Möglichkeiten sind nach ISO Aufteilung der Managementfunktionalitäten in „Fault Management“ und „Performance Management“ einzuordnen.

Polling

Hierbei handelt es sich um ein Verfahren, wo das Managementsystem in regelmäßigen Zeitintervallen, die zu überwachenden Parameter vom Agent abruft. Das Managementsystem kann jeden Agent, für den es autorisiert ist, abfragen. Der Agent antwortet mit der entsprechenden Information.

[8] Network management system

[9] Management information base

Vorteil dieses Verfahrens ist der zentrale Ausgangspunkt der Abfragen. Der Nachteil dieser Methode ist aber, dass Fehler vom Managementsystem erst erkannt werden, nachdem die Information abgefragt wurde.

Event Reporting - Traps

Beim Event Reporting übernimmt der Agent die aktive Rolle. Tritt ein Ereignis auf, welches laut Konfiguration gemeldet werden soll, wird dieses an das Managementsystem auch gemeldet. Das Managementsystem übernimmt hier also die passive Rolle. Es wartet auf Nachrichten der Agents.
Auch hier ist es möglich, dass der Agent in periodischen Zeitintervallen seinen Status bzw. einzelne Informationen an das Managementsystem überträgt.

2.6 Herausforderungen

2.6.1 Prinzipbedingte Probleme und Herausforderungen

Das ganze Thema Netzwerkmanagement bringt viele Herausforderungen und Probleme mit sich.
Eine große Herausforderung an die Hersteller von Netzwerkmanagementsoftware sind die kurzen Entwicklungszeiten von Netzwerktechnologien. Es ist schwierig, ein Netzwerkmanagementsystem immer auf den laufenden Stand zu halten und alle aktuellen Technologien zu unterstützen.

Ein wesentliches Problem bringt der Umstand mit sich, dass die Managementinformationen über das Netzwerk selbst übertragen werden. Dies spart zwar Kosten, hat aber bei einem Leitungsausfall zur Folge, dass Geräte ggf. nicht mehr erreichbar sind.

Networkmonitoring ist der wichtigste Teil von Netzwerkmanagementsystemen. Viele Systeme beschränken sich auf das Monitoring und vernachlässigen Sicherheitsmechanismen wie Verschlüsselung oder Authentifizierung. Dies stellt ein enorm großes Sicherheitsproblem dar.

Die Tatsache, dass fast alle Netzwerke heterogen sind, d.h. sie bestehen aus Komponenten von unterschiedlichen Herstellern, stellt die nächste Problematik dar. Viele verschiedene Versionen von Hard- und Software, etliche Technologien und viele gänzlich verschiedene Produkte die zusammen ein Netzwerk ergeben.
Dies hat zur Folge, dass auftretende Fehler eines Gerätes zu unvorhersehbaren Problemen bei anderen Geräten führen. Aus diesem Grund ist es umso wichtiger dass eine einheitliche Managementplattform gefunden wird, um alle Geräte gemeinsam verwalten zu können.

Die Komplexität von Netzwerken führt meist auch dazu, dass nicht alle Komponenten vor Ort, sondern lediglich remote überprüft werden können.

Überdies ist das NMS von der Richtigkeit der Daten, die die Agents sammeln und senden, abhängig. Tritt ein lokaler Fehler bei einem Agent auf, der das Sammeln der Statusinformationen betrifft, kann dieser sehr spezifische Fehler mit hoher Wahrscheinlichkeit vom NMS nicht direkt festgestellt werden. Da dies ein grundsätzliches Problem darstellt, wird darauf in dieser Arbeit nicht weiter eingegangen.

2.6.2 Sicherheitsprobleme bei Netzwerkmanagement

Die Möglichkeit der Remotesteuerung eines Netzwerks bringt einige Sicherheitsrisiken mit sich. Wie in Kapitel 2.3 näher beschrieben, verwenden viele Hersteller das so genannte CIA Sicherheitsmodell. Wird nur einer dieser drei Sicherheitsaspekte vernachlässigt, ist die Sicherheit in Netzwerken massiv gefährdet.

Eine große Gefahr besteht, wenn eine unautorisierte Person oder ein unautorisiertes System Zugriff auf das Managementsystem erhält. In diesem Fall stehen dem Eindringling praktisch alle Türen offen. (siehe 2.3.2)

Unwissenheit über das Vorhandensein eines aktiven Agents auf einem System kann ebenfalls ein großes Sicherheitsproblem darstellen. Oft sind bei Geräten im Auslieferungszustand die Netzwerkmanagementfunktionalitäten aktiv. Wird vergessen diese zu deaktivieren oder entsprechend abzusichern, ist es für Angreifer leicht, die Steuerung eines solchen Gerätes zu übernehmen.
Weiters fehlen oft entsprechende Kontrollmechanismen wie Verschlüsselung oder Authentifizierung, um den Zugriff auf Informationen benutzerbezogen steuern zu können.

Nicht zuletzt bringen Netzwerkmanagementsysteme durch mangelnde Absicherung von transportierten Nachrichten oder Steuerbefehlen ein großes Sicherheitsproblem mit sich. In so einem Fall kann es für einen Angreifer genügen, am Netzwerk mitzulauschen, um genügend Informationen für einen Angriff oder eine Manipulation zu sammeln. (siehe 2.3.2)

Weiterführende Literaturempfehlung: [Tanenbaum, 2003, Kapitel 4]

2.6.3 Probleme verursacht durch Systemfehler

Probleme beim Netzwerkmanagement können auch durch Fehler des Managementsystems entstehen bzw. übersehen sehen.

Um einen mögliche Ausfall eines Überwachungssystems zu überbrücken, ist es ratsam, dieses redundant auszulegen oder verschiedene Systeme untereinander abzusichern.

NMS sind auch auf Falschinformationen von Agents, bedingt durch Systemfehler, anfällig.

Die Verwendung von Netzwerkprotokollen (z.B. UDP[10]), die keine oder nur mangelnde Fehlerabsicherung mitbringen, stellen ein zusätzliches Problem dar. Wichtige Nachrichten können im Netzwerk verloren gehen. Durch das nicht Erkennen solch verloren gegangener Nachrichten können Probleme unentdeckt bleiben und so großen Schaden anrichten.

[10] User datagram protocol

3. SNMPv3 Vorgänger

3.1 SNMPv1

3.1.1 Ursprung von SNMP

Bei der Entwicklung von TCP/IP wurde wenig an Netzwerkmanagement gedacht. Der Grund dafür lag an den relativ wenigen Rechner, die es gab. Die ganze Problematik kam erst später durch die explosionsartige Vergrößerung des Internets am Ende der 80er Jahre auf. Netzwerke wurden immer komplexer und heterogener. Dies hatte zur Folge, dass das Management immer aufwendiger wurde und mit den bisherigen Mitteln praktisch unmöglich zu bewerkstelligen war.
Gesucht war ein einfaches Protokoll, das aber eine große Funktionalität bietet. Als erstes wurde das „Simple Gateway Monitoring Protocol“ (SGMP) im November 1982 vorgestellt. Sein Funktionsumfang beschränkte sich auf das Monitoring von Gateways.
Der Bedarf nach einem universellen Netzwerkmanagementtool wurde aber größer und so entstanden drei Projekte:

- High-Level Entity Management System (HEMS)
- Simple Network Management Protocol (SNMP)
- CMIP over TCP/IP

Dank seiner Einfachheit und des dadurch relativ geringen Aufwandes fremde Systeme einzubinden, hat sich SNMP als „Standard“ für Netzwerkmanagement etabliert.
Dies hat zur Folge, dass heute praktisch jedes Netzwerkfähige Gerät über SNMP steuerbar ist.
Weiterführende Literatur: [Stallings, 1999, S. 71]

3.1.2 Allgemein

SNMP wird landläufig oft benutzt, um das Protokoll selbst zu bezeichnen. Es handelt sich dabei aber vielmehr um eine Definition des Protokolls und eine genaue Content-Spezifikation:

> „The term Simple Network Management Protocol (SNMP) is actually user to refer to a collection of specifications for network management that include the protocol itself, the definition of data structures, and associated concepts.“ [Stallings, 1999, S.71]

SNMPv1 bezeichnet die erste Version von SNMP. Es stellt den Internetstandard für das Netzwerkmanagement auf TCP/IP basierten Netzwerken dar.

3.1.3 Ziele von SNMP

SNMP wurde erschaffen, um Netzwerkmanagement zu vereinfachen. Es sollte eine Verringerung der Komplexität mit sich bringen. Außerdem sollte es leicht erweiterbar und unabhängig von irgendwelchen Netzwerkkomponenten sein. Jede Komponente soll ihre Aufgabe ausführen und Kapazitäten nicht durch Abwicklung von Managementprotokollen vergeuden.
Das Netzwerkmanagement basierend auf SNMP unter Zuhilfenahme von SMI[11] und MIB[12] hat das Ziel, den Netzwerkmanagern einen zentralen Punkt zur Beobachtung, Kontrolle und Verwaltung ihres Netzwerkes zu geben.

[11] Structure of Management Information

[12] Management Information Base

3.1.4 SNMP Standards

SNMP basiert auf einer Menge von RFCs. Die wichtigsten sind:
[vgl. URL1]

- Structure and Identification of Management Information for TCP/IP based networks (RFC 1155)

- Management Information Base for Network Management of TCP/IP based Internets: MIBII (RFC1213)

- Simple Network Management Protocol (RFC1157)

3.1.5 SNMP Protokoll Architektur

Grundsätzlich muss jede Station und jeder Agent SNMP, UDP und IP implementiert haben. SNMP wurde als Applikation Level Protokoll entworfen. Version eins von SNMP verwendet entsprechend RFC 1157 (Mai 1990) UDP auf Basis von IP. UDP deshalb, weil TCP zu langsam wäre, da es sich dabei um ein verbindungsorientiertes Protokoll handelt und hier jedes Paket bestätigt wird. UDP ist einfacher und schneller.
Da SNMP über das verbindungslose UDP funktioniert, ist auch eine SNMP Nachricht allein für sich verbindungslos, auf SNMP Ebene allerdings werden manche Anforderungen (Requests, siehe 3.1.9.1) laut Spezifikation mit einer Antwort bestätigt. Dieser Vorgang Anforderung - Antwort entspricht einer verbindungsorientierten Übertragung.
Verwendet wird prinzipiell Port 161 und für TRAP Meldungen Port 162.
Bei Bedarf können laut RFC 1418 bis 1420 auch andere Trägerprotokolle (OSI, IPX, Appletalk) verwendet werden.

3.1.6 Architektur von SNMP

Die Architektur von SNMP sieht folgendermaßen aus:

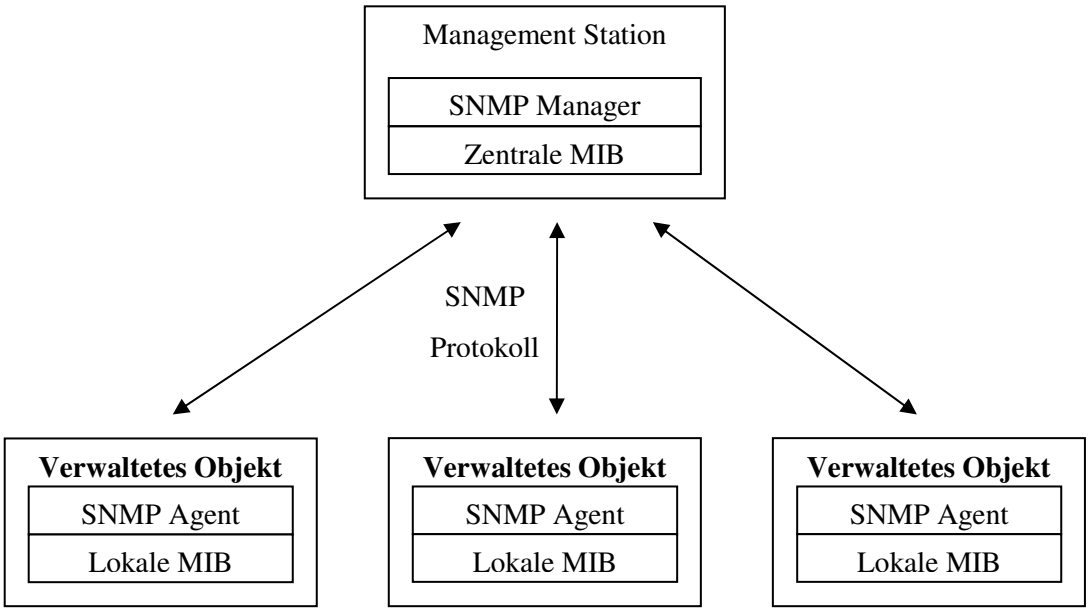

Abbildung 7: Architektur von SNMP

3.1.6.1 Management Station

Hierbei handelt es sich meist um einen (oder mehrere) PC, ausgestattet mit der entsprechenden Managementsoftware. Diese stellt die Schnittstelle zum Menschen dar, über diese das Netzwerk im Endeffekt überwacht und gesteuert wird. Weiters muss die Managementstation Funktionen bereitstellen, um die gewünschten Anforderungen des Netzwerkmanager umsetzen zu können und in die Netzwerküberwachung aufnehmen zu können.

Außerdem muss die Managementstation über eine Datenbank aller MIBs der zu verwaltenden Station verfügen.

3.1.6.2 Management Agent

Der Managementagent ist die zweite aktive Komponente bei Netzwerkmanagementsystemen. Er ist in den Clients (Server, Router, Switches usw.) implementiert und ermöglicht die Kommunikation zur Managementstation. Der Agent antwortet auf Anfragen der Managementstation bzw. leitet, wenn so konfiguriert, Nachrichten an die Station weiter.

3.1.6.3 Management Information Base

Jede Netzwerkressource entspricht im Netzwerkmanagementsystem einem Objekt. Ein Objekt repräsentiert im Wesentlichen genau eine Eigenschaft eines Clients und wird in Form einer Datenvariable gespeichert. Eine Zusammenfassung von mehreren (vielen) Objekten nennt man Management Information Base (MIB).
Diese Objekte sind geräteübergreifend definiert, d.h. mit einer gemeinsamen MIB können beispielsweise unterschiedliche Router verwaltet werden.

3.1.6.4 Network Management Protocol

Die Managementstation und die Managementagents kommunizieren über das Network Management Protocol. Im Falle von TCP/IP Netzwerken ist dies das Simple Network Management Protocol.

3.1.7 Proxy-Systeme

Wenn SNMP in einem Netzwerk eingesetzt werden soll, ist es erforderlich, dass alle beteiligten Komponenten einen SNMP Agent haben, UDP und IP sprechen. Um trotzdem Komponenten verwalten zu können, die eine dieser Anforderungen nicht erfüllen, kann

man einen SNMP-Proxy[13] einsetzen (siehe Abbildung 8: SNMP Proxies). Dieser kommuniziert mit dem Gerät der die SNMP Anforderungen nicht erfüllt über ein beliebiges Protokoll, dass sowohl er als auch der SNMP-Proxy beherrschen. Der Proxy wiederum „übersetzt“ diese Nachrichten und stellt sie somit dem SNMP Manager zur Verfügung.

Die Vermittlung erfolgt zwischen Computern oder Programmen in so genannten Rechnernetzen. Aus Sicht des Servers verhält sich der Proxy wie ein Client, dem Client gegenüber wie ein Server.

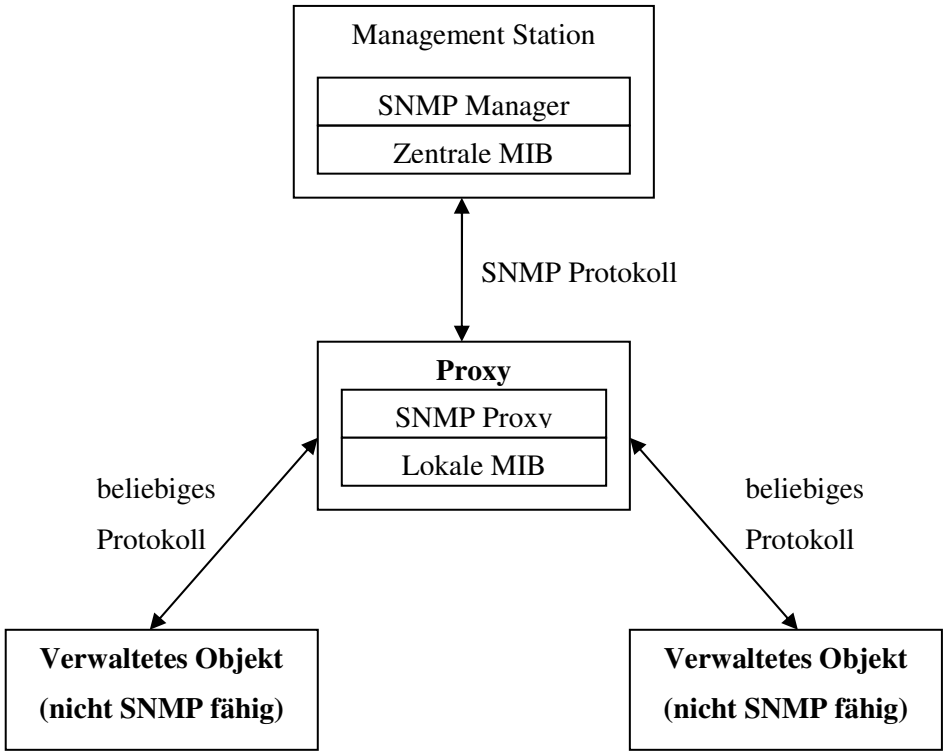

Abbildung 8: SNMP Proxies

[13] Proxy: „Stellvertreter“, steigert die Effizienz von Datentransfer und erhöht die Sicherheit [vgl. URL2]

3.1.8 Sicherheitsmaßnahmen

Die Struktur von SNMP sieht es vor, dass eine Managementstation mehrere Agents verwaltet. Diese Form ist zwar gängig, aber nicht vorgeschrieben. Es ist auch möglich, dass mehrere Managementstationen einen Agent verwalten, bzw. das ein gesamtes Netzwerk mit vielen Agents von mehr als einer Station verwaltet werden.
Da jeder Agent eine eigene MIB zu verwalten hat, muss er den Zugriff auf diese durch Managementstationen kontrollieren und beeinflussen können.

In der RFC 1157 ist eine nur sehr einfache Sicherheitsmaßnahme vorgesehen, die Community.

Dabei handelt es sich um ein lokales Konzept. Jeder Client definiert seine eigenen Communities. Jede Community beinhaltet eine eigene Kombination aus Authentication, Zugriffskontrolle und Proxyeigenschaften. Weiters benötigt jede Community innerhalb eines Clients einen eindeutigen Namen. Dieser Name kann von Client zu Client für die gleichen Zugriffsrechte unterschiedlich sein bzw. bedeutet ein gleicher Name nicht zwangsläufig die gleichen Rechte auf verschiedenen Clients.
Eine Managementstation muss bei jeder Lese- oder Schreiboperation den Communitynamen angeben, weshalb jede Managementstation über die Communities ihres Clients Bescheid wissen muss. [vgl. Stallings, 1999, S.164]

Authentication Service mittels Communties

Das Ziel eines Authentication Services ist es, sicherzustellen, dass eine Kommunikation authentisch ist. Im Falle von SNMP bedeutet das, festzustellen, dass eine SNMP Nachricht wirklich von der Quelle stammt, als die sie sich ausgibt.
In der RFC 1157 ist dafür nur ein sehr einfaches Schema vorgesehen: Jede Operation (set oder get) muss einen Communityname beinhalten, dieser dient als Passwort.
Dies stellt ein wesentliches Sicherheitsproblem dar und ist auch der Grund dafür, dass oft nur reine get Communities definiert werden und auf Schreiboperationen gänzlich verzichtet wird. (siehe 3.1.12)

Access Policy mit Communties

Durch das Definieren von Communities, kann der Client den Zugriff auf Managementstations einschränken, die im Besitz der Namen der Communities sind.
Durch die Verwendung mehrerer unterschiedlicher Communities kann der Client zwischen mehreren Zugriffsarten unterscheiden.

Durch eine so genannte „SNMP MIB view“ kann der Zugriff auf die MIB weiters eingeschränkt werden. Es wird dabei nur Zugriff auf einen Teil des MIB-Baums gestattet.

Zusätzlich kann pro Community ein SNMP Access Mode (Read only/Write only) angegeben werden. Dieser Access Mode gilt für alle Objekte in einer MIB view.

Die Kombination aus MIB View und Access mode nennt man „SNMP community profile“.
Ein „community profile“ wird am Client mit einer Community verknüpft. Diese Kombination nennt man SNMP access policy.

3.1.9 Protocol Specification

Bei SNMP werden Informationen von der Managementstation zum Client oder umgekehrt in Form vom SNMP Messages übertragen. Jede dieser Messages enthält die entsprechende SNMP Versionsnummer, einen Communitynamen und einen von fünf Arten von PDUs[14]. (siehe Abbildung 9: SNMPv1 PDU)

Version	Community	SNMP PDU		
		PDU Type	…	…

Abbildung 9: SNMPv1 PDU

[14] Protocol data unit

Die fünf verschiedenen Arten der PDUs werden folgender Tabelle entnommen (siehe Tabelle 1: PDU Typen):

Tabelle 1: PDU Typen

PDU type	Bezeichnung
0	Get Request
1	Get Next Request
2	Get Response
3	Set Request
4	Trap

3.1.9.1 Transferablauf

In Abbildung 10: SNMP Transferablauf werden die verschiedenen Arten von Transferabläufen bei SNMPv1 gezeigt. Prinzipiell gilt, dass auf eine Request PDU immer eine Response PDU folgt. Eine Trap PDU hingegen bleibt unbestätigt.

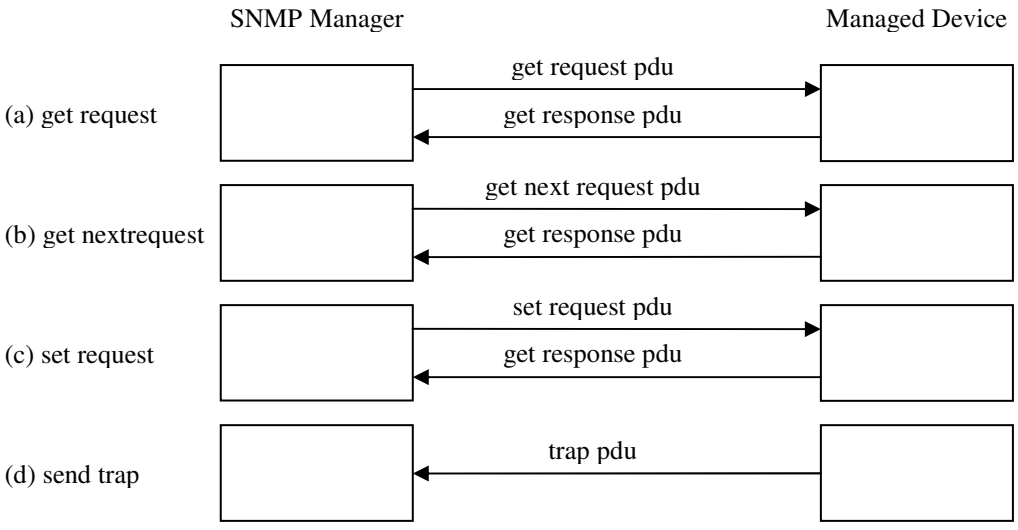

Abbildung 10: SNMP Transferablauf

3.1.9.2 GetRequest PDU

Die GetRequest Funktion wird von der Netzwerkmanagementstation verwendet. Sie enthält folgende Felder:

PDU type=0	request id	0	0	variablebindings

Abbildung 11: GetRequest PDU

PDU type Gibt an, dass es sich um ein GetRequest handelt

Request-id Eine eindeutige Nummer, die diese Anforderung pro Client eindeutig identifiziert. Somit können Antworten auf diese Anforderung eindeutig zugewiesen werden. Außerdem können damit zum Beispiel doppelt gesendete UDP Pakete identifiziert werden.

Variablebindings Gibt an, welche Werte angefordert werden.
(name1 – wert1, name2 – wert2, usw.)

Die Antwort von einem Client auf eine GetRequest PDU ist eine GetResponse PDU (siehe Abbildung 10: SNMP Transferablauf (a)).
Diese besitzt die gleiche Request-id um Anfrage und Antwort eindeutig zuordnen zu können.
Es handelt sich hierbei um eine nicht aufsplittbare (atomare) Funktion: kann einer der angeforderten Werte nicht geliefert werden, wird gar kein Wert zurückgegeben.

3.1.9.3 GetNextRequest PDU

PDU type=1	request id	0	0	variablebindings

Abbildung 12: GetNextRequest PDU

Gleicher Aufbau wie bei GetRequest PDU.

Einziger Unterschied: beim GetNextRequest wird der Wert der nächstliegenden Variable angefordert. Diese Funktion wird für Tabellenabarbeitung verwendet.
(siehe Abbildung 10: SNMP Transferablauf (b)).

3.1.9.4 SetRequest PDU

PDU type=3	request id	0	0	variablebindings

Abbildung 13: SetRequest PDU

Gleicher Aufbau wie bei GetRequest PDU.
Allerdings soll hier eine Variable geschrieben statt gelesen werden. Variablebindings listet hier alle Objekte inkl. der einzutragenden Werte auf. Bestätigt wird ein SetRequestPDU mit einer GetResponse PDU wieder mit gleicher Request-id.
Hier handelt es sich wieder um eine nicht aufsplittbare Funktion.
(siehe Abbildung 10: SNMP Transferablauf (c)).

3.1.9.5 GetResponse PDU

PDU type=2	Request id	errorstatus	errorindex	Variablebindings

Abbildung 14: GetResponse PDU

GetResponse ist die Antwort des Managers auf GetRequest, GetNextRequest und SetRequest. Dementsprechend ist die „Request id“ bei einer GetResponse PDU gleich der „Request id“ der entsprechenden Anforderung.

errorstatus Gibt an, ob und welcher Fehler beim Bearbeiten des entsprechenden Requests aufgetreten ist.

errorindex Gibt für den Fall eines Fehlers den Index des Objektes an, an dem der Fehler aufgetreten ist. [vgl. Stallings, 1999, S. 175]

3.1.9.6 TrapPDU

Wird von einem Netzwerkmanagement-Agent verwendet. Eine TrapPDU ist die einzige Möglichkeit des Agents, der Station etwas aktiv mitzuteilen. Traps werden von der Station nicht bestätigt!

PDU type=4	enterprise	agent-addr	generic-trap	specific-trap	time-stamp	variablebindings

Abbildung 15: Trap PDU

Sie enthält folgende Felder [Stallings, 1999, Seite 189]:

PDU type Gibt an, das es sich um eine TrapPDU handelt

Enterprise Identifiziert das Network Management Subsystem.

Agent-addr IP Adresse des Agent, an dem der Trap generiert wurde.

Generic-trap Gibt einen der folgenden vordefinierten Trap Typen an:

- coldStart
- warmStart
- LinkDown
- LinkUp
- ifIndex
- authenticationFailure
- egpNeighborLoss
- enterpriseSpecific

Specific-trap Gibt die Trap-Ursache genauer an.

Time-Stamp Zeit zwischen letzter Initialisierung des „Trap-Verursachers“ und der Erzeugung des Traps.

variableBindings Zusätzliche Informationen zu dem Trap

3.1.10 SNMP Management Information

Die Grundlage für ein Netzwerkmanagementsystem ist eine Datenbank, die alle Objekte beinhaltet, die überwacht bzw. gesteuert werden sollen. Jede Netzwerkressource entspricht im Netzwerkmanagementsystem einem Objekt. Die strukturierte Zusammenfassung dieser Objekte nennt man Management Information Base. Bei SNMP sind die MIBs baumförmig (siehe Abbildung 16: MIB Tree Struktur) aufgebaut.
Jeder Client (Server, Workstation usw.) im Netzwerk besitzt eine MIB, die den Status des Gerätes widerspiegelt. Überwacht bzw. gesteuert kann eine Ressource werden, indem Werte aus der MIB ausgelesen bzw. verändert werden.

Damit dies funktioniert, ist es aber notwendig, dass dieselben Informationen in verschiedenen Systemen an derselben Stelle in der MIB stehen.
Weiters ist es erforderlich, die Struktur der Management Information (SMI) zu definieren. [vgl. Stallings, 1999, S. 85]

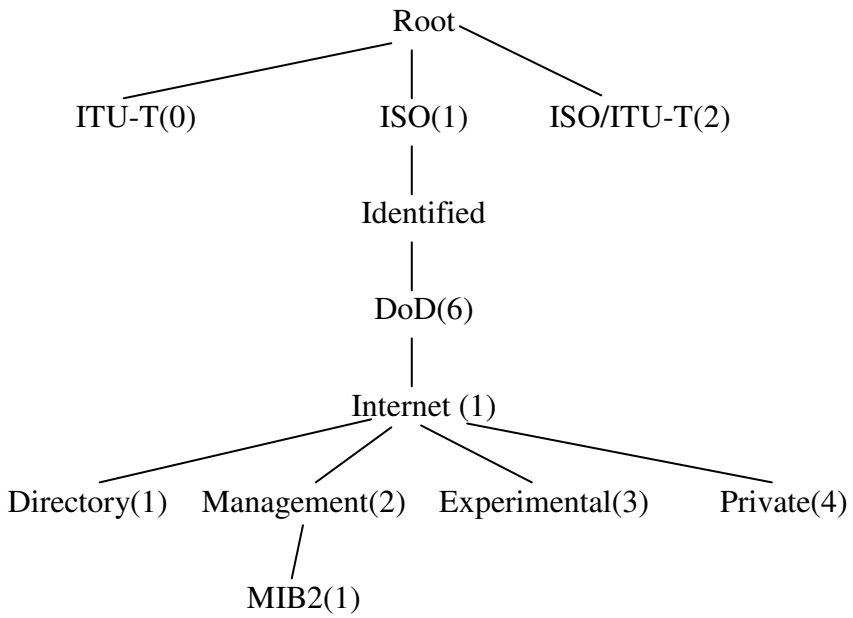

Abbildung 16: MIB Tree Struktur

3.1.10.1 Structure of Management Information

Die Structure of Management Information (SMI) ist in der RFC 1155 spezifiziert. Dort wird festgelegt, welche Datentypen verwendet werden können und wie Ressourcen in einer MIB dargestellt und genannt werden. Ziel der SMI ist es, MIBs so einfach wie möglich zu halten. Aus diesem Grund kann eine MIB nur einfache Skalare und zweidimensionale Skalarfelder speichern. Auf komplexere Strukturen wurde verzichtet.
Der Vorteil dieser einfachen Strukturen liegt in der einfachen Implementierbarkeit.
Die Beschreibung erfolgt in ASN.1[15]

„Abstract Syntax Notation number One is a standard that defines a formalism for the specification of abstract data types." [URL3]

Näheres zum Thema ASN.1 kann auf [URL3] nachgelesen werden.

3.1.10.2 Standard MIBs

Einer der Hauptgründe für die weite Verbreitung von SNMPv1 liegt in der großen Anzahl verfügbarer MIBs. Eine, wenn nicht die wichtigste MIB, ist die MIB-2. Sie wird in der RFC 1213 spezifiziert und stellt die zweite Version der Management Information Base dar (siehe Tabelle 2: MIB 2 Gruppen [Stallings, 1999, S. 122])

Beispiele für andere Standard MIBs (genaue Liste: [URL4]):

- RFC 1215: Traps
- RFC 1214: OSI Internet Management
- RFC 1284: Ethernet-like Interface
- RFC 1285: FDDI
- RFC 1286: Bridges
- RFC 1628: UPS

[15] Abstract Syntax Notation number One

Tabelle 2: MIB 2 Gruppen [Stallings, 1999, S. 122]

system(1)	overall information about the system
interfaces(2)	information about each of the interfaces from the system to a subnetwork
at(3)	description of address translation table for internet-to-subnet address mapping
ip(4)	information related to the implementation and execution experience of IP on this system
icmp(5)	information related to the implementation and execution experience of ICMP on this system
tcp(6)	information related to the implementation and execution experience of TCP on this system
udp(7)	information related to the implementation and execution experience of UDP on this system
egp(8)	information related to the implementation and execution experience of EGP on this system
dot(10)	information about the transmission schemas and access protocols at each system interface
snmp(11)	information related to the implementation and execution experience of SNMP on this system

3.1.10.3 MIB Variablen

Jeder MIB Variable ist ein eindeutiger Objektname + Objektidentifier (OID) zugewiesen.

Beispiel – Variable sysName aus MIB2:
Objektname: iso.org.dod.internet.mgmt.mib.system.sysName
Objektidentifier: 1.3.6.1.2.1.1.5

3.1.11 Einsatz und Verbreitung von SNMPv1

Die Notwendigkeit für Unternehmen, irgendeine Form der Netzwerküberwachung anzuwenden wurde bereits am Beginn dieser Arbeit erläutert.
Ausfälle müssen möglichst schnell erkannt und entsprechende Maßnahmen getroffen werden.
Stillstandszeiten sollen möglichst kurz gehalten werden, Engpässe sind zu erkennen und beseitigen. Die Netzwerkkomponenten vieler unterschiedlicher Hersteller müssen überwacht und gesteuert werden.
Mit SNMP können Netzwerke proaktiv überwacht werden, d.h. Abweichungen von Parametern können vorzeitig festgestellt werden. Auf diese Änderungen kann reagiert werden, noch bevor es zu einem teuren Ausfall kommt.

Der Grund warum sich SNMPv1 zum Standard im Netzwerkmanagement entwickelt hat, liegt sicherlich in der einfachen Erweiterbarkeit von MIBs und der somit verbundenen einfachen Integration von unterschiedlichster Hardware. Es existiert praktisch für alle netzwerkfähigen Geräte eine Vielzahl von MIBs. Bei Bedarf kann zudem ohne großen Aufwand eine neue MIB erstellt und in das NMS eingebunden werden.
Durch diese große Verbreitung von SNMPv1 bei netzwerkfähigen Geräten, gibt es praktisch auch keine Netzwerkmanagementsoftware, die SNMPv1 nicht unterstützt.

Die Mehrkosten SNMPv1-fähiger Geräte sind für Firmen zudem unerheblich und amortisieren sich spätestens nach einem frühzeitigen Erkennen von Defekten und den dadurch verhinderten Stillstandszeiten.

Eingesetzt wird SNMPv1 in Unternehmen aller Größen zur Überwachung und Steuerung des Netzwerkes und zur Alarmierung im Fehlerfall.

3.1.12 Schwachpunkte

3.1.12.1 Sicherheit

Trotz der großen Verbreitung von SNMPv1, bringt es auch einige Sicherheitsrisiken mit sich, diese Version des Netzwerkmanagementprotokolls einzusetzen.

Der größte Schwachpunkt von SNMPv1 liegt wohl im praktisch nicht vorhandenen Sicherheitskonzept:
Das tiefgreifendste Problem dabei stellt die Tatsache dar, dass Nachrichten im Klartext übermittelt werden. Dies bedeutet, sie können ohne weiteres mit Hilfe eines Packetsniffers aufgefangen und mitgelesen werden. Dies ermöglicht es einem potentiellen Angreifer, die für die Authentifizierung vorgesehen Communitynames auszulesen. Da diese wiederum die einzige Form der Authentifizierung darstellen, stehen dem Angreifer somit alle Türen offen.

Eine geringfügige Verbesserung stellt ein SNMP Client dar, der die Möglichkeit bietet, den Zugriff auf die SNMP Datenbank zusätzlich zum Communitynamen nur von definierten IP Adressen zu erlauben. Da IP Adressen aber gefälscht werden können, stellt auch diese keine große Hürde für mögliche Angreifer dar.

Ein nicht zu unterschätzendes Problem bringt der Umstand mit sich, dass viele netzwerkfähige Geräte mit einem werkseitig aktiven SNMP-Agent ausgeliefert werden. Read und Write Communitynamen sind leichtsinnigerweise oft auf „public“ für Lesezugriff und „private“ für Lese- und Schreizugriff voreingestellt. Wird bei der Konfiguration des Gerätes vergessen, diese Standardcommunities zu ändern oder zu entfernen, stellt dies ein enorm hohes Sicherheitsrisiko dar.

SNMP Nachrichten sind leicht veränderbar, d.h. Nachrichten können durch Manipulation geändert werden. Solche Veränderungen können nicht aufgespürt werden, da jegliche Form von Prüfsummen oder andere Sicherheitsmaßnahmen, die die Authentizität sicherstellen, fehlen.

Ein weiteres Problem liegt in der Verwendung des verbindungslosen Protokolls UDP. Nachrichten können unbemerkt verloren gehen. Dies stellt insbesondere bei Traps eine Gefahr dar, da das Protokoll keine Bestätigung eines empfangenen Traps vorsieht und somit potentielle Fehler unbemerkt bleiben können.

All diese sicherheitskritischen Aspekte haben dazu geführt, dass SNMPv1 hauptsächlich zum Netzwerkmonitoring, nicht aber zur Steuerung von Geräten verwendet wird. Einen wirksameren Schutz als bei SNMPv1 auf Write-Community gänzlich zu verzichten, gibt es auch nicht.

3.1.12.2 Effizienz

Durch den wenig komplexen Aufbau von SNMP MIBs, bleibt zwar die Anzahl der SNMP Funktionen gering, jedoch wird dieses System bei der Übertragung von großen Datenmengen sehr ineffizient. Für jede angeforderte Information muss ein Paket gesendet und ein Paket empfangen werden. Dadurch entsteht sehr viel Overhead, da es sich immer wieder um „Standardnachrichten“ handelt. Dies hat insbesondere beim Auslesen komplexerer Strukturen wie z.B. Routingtabellen enorm viel Netzwerklast zur Folge. Viele einzelne Nachrichten erhöhen außerdem die Antwortzeiten der beteiligten Geräte.

3.1.12.3 Kommunikation mehrerer NM-Systeme

Ein weiterer Schwachpunkt von SNMP ist die Tatsache, dass es keine Möglichkeit zur Kommunikation von mehreren Managementstations untereinander gibt. Mehrere Stationen müssen einzeln verwaltet und manuell synchron gehalten werden.

Einige dieser Mängel wurden in höheren SNMP Versionen berücksichtigt.

3.2 SNMPv2

3.2.1 Entwicklung von SNMPv2

Durch die Schwachpunkte von SNMPv1 bezüglich Sicherheit (Übertragung von Communities im Klartext) und der geringeren Effizienz wurde klar, dass eine neue Version von SNMP entwickelt werden musste.
Der 1993 von der IETF[16] vorgeschlagene Standard für SNMPv2, wurde jedoch von den Herstellern nicht angenommen, da er einige Mängel beinhaltete.
Eine überarbeitete Version davon wurde 1996 vorgestellt. Diese Version war zwar funktional erweitert gegenüber SNMPv1, aber die Sicherheitsmaßnahmen wurden aus Version 1 (Communities) übernommen. Diese Version wurde SNMPv2c genannt.
Um die Sicherheitsprobleme dieser Version zu beheben, wurde an SNMPv2 weitergearbeitet.
Daraus resultierten wiederum zwei Versionen: SNMPv2u und SNMPv2*.
[vgl. URL5], [vgl. Stallings, 1999, S. 477]
Schlussendlich gibt es also vier verschiedene Varianten von SNMPv2:

SNMPv2p	mit Party Based Sicherheitsmodell
SNMPv2c	mit Community-Based Sicherheitsmodell
SNMPv2u	mit User-Based Sicherheitsmodell
SNMPv2*	mit Sicherheits- und Administrationsmodell

Im Folgenden werden die wesentlichen funktionellen Verbesserungen von SNMPv2 gegenüber Version 1 erläutert. [vgl. Stallings, 1999, S334]

[16] Internet engineering task force

3.2.2 SNMPv2 Protokolloperationen

Bei SNMPv2 werden drei Arten von Protokolloperationen unterschieden:

Manager-agent request-response

Ein SNMPv2 Manager schickt eine Nachricht an einen SNMPv2 Agent und erhält von diesem eine Antwort.

Manager-manager request-response

Ein SNMPv2 Manager schickt eine Nachricht an einen anderen SNMPv2 Manager und erhält von diesem eine Antwort. Dieser Typ wird verwendet um Informationen zwischen mehreren SNMPv2 Managern auszutauschen.

Agent-manager unconfirmed

Ein SNMPv2 Agent schickt eine Nachricht an einen SNMPv2 Manager. Diese Nachricht bleibt unbestätigt. (entspricht Trap aus SNMPv1).

3.2.3 Protocol Specification

Wie bei SNMPv1 werden bei SNMPv2 Informationen in Form von Messages übertragen. Jede dieser Messages enthält die entsprechende SNMP Versionsnummer, einen Communitynamen und einen von 8 Arten von protocol data units (siehe Abbildung 17: SNMPv2 PDU).

<table>
<tr><td rowspan="2">Version</td><td rowspan="2">Community</td><td colspan="3">SNMP PDU</td></tr>
<tr><td>PDU Type</td><td>…</td><td>…</td></tr>
</table>

Abbildung 17: SNMPv2 PDU

Die acht verschiedenen Arten der PDUs sind aus folgender Tabelle ersichtlich (siehe Tabelle 3: SNMPv2 PDU Typen).

Tabelle 3: SNMPv2 PDU Typen

PDU type	Bezeichnung
0	Get Request
1	Get Next Request
2	Response
3	Set Request
5	Get Bulk Request
6	Inform Request
7	SNMPv2 Trap
8	Report

3.2.3.1 Transferablauf

In Abbildung 18: SNMPv2 Transferablauf werden die verschiedenen Arten von Transferabläufen bei SNMPv2 gezeigt. Prinzipiell gilt auch hier wieder wie bei SNMPv1, dass auf eine Request PDU immer eine Responce PDU folgt. Eine Trap PDU bleibt hingegen unbestätigt.

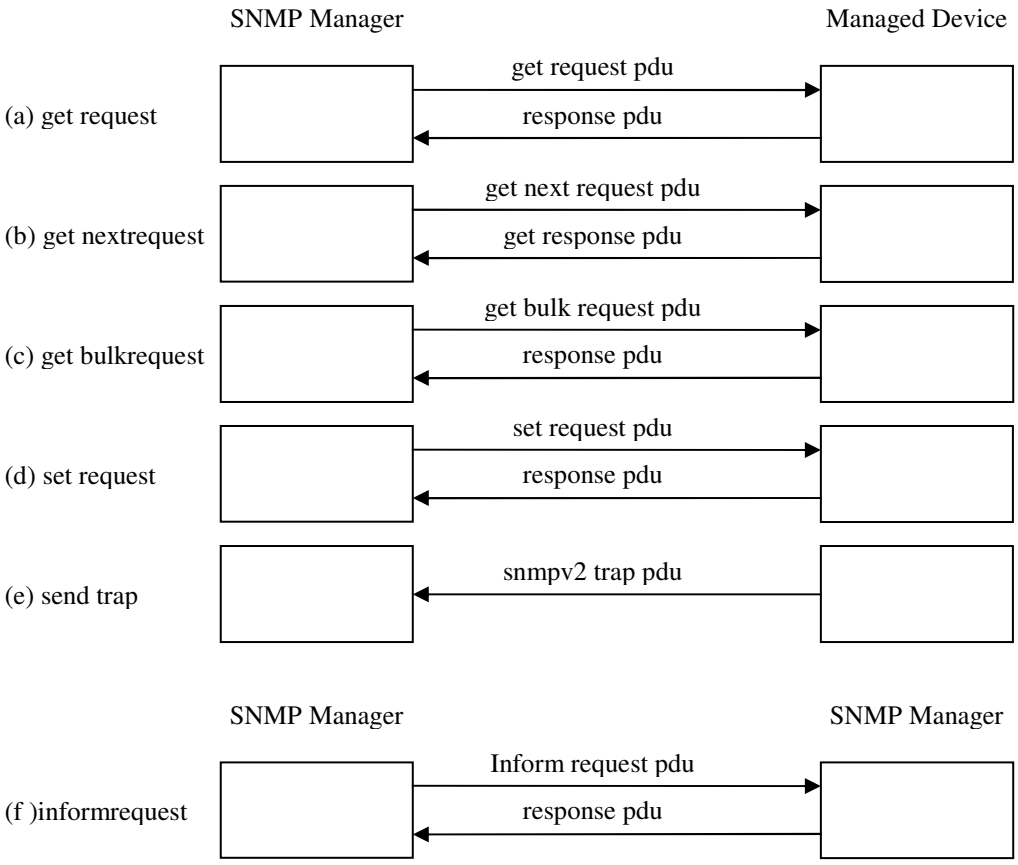

Abbildung 18: SNMPv2 Transferablauf

3.2.3.2 GetRequest, GetNextRequest, SetRequest

Weitgehend identisch mit den entsprechenden Funktionen aus SNMPv1.

3.2.3.3 GetBulkRequest

Diese Funktion stellt eine der wesentlichen Verbesserungen von SNMPv2 dar: Ziel ist eine Minimierung des Protokollaufwandes für den Versand von größeren Informationsblöcken. [vgl. Stallings, 1999, 378]

3.2.3.4 SNMPv2 Trap

Wird bei SNMPv2 im gleichen PDU Format wie GetRequest gesendet.
Das variablebindings-Feld enthält die entsprechenden Trapinformationen.

3.2.3.5 InformRequest

Wird verwendet, um Informationen zwischen zwei SNMPv2 Managern auszutauschen.
Gleicher Aufbau wie bei GetRequest.

3.2.3.6 Report

Die SNMPv2 Spezifikation enthält eine Report PDU, die jedoch nicht näher definiert ist!

3.2.4 SMIv2

Die Structure of management information (SMI) der Version zwei basiert auf der SMI von Version eins. Die SMIv2 enthält genauere Spezifikationen und Dokumentationen der Managed Objects und der MIBs.

Sie basiert auf vier Konzepten:

Object definitions Wie bei SNMPv1 SMI. Wird verwendet um Managed Objects zu beschreiben

Conceptual tables Komplexere Strukturen durch Tabellen

Notification definitions Wird verwendet, um Informationen zu definieren, die im Falle von „nichtnormalen“ Ereignissen gesendet werden.

Information modules Spezifiziert eine Gruppe von zugehörigen Definitionen.

An dieser Stelle soll auf SMIv2 nicht näher eingegangen werden.
Weiterführende Literatur [Stallings, 1999, Chapter 11]

3.2.5 Einsatz und Verbreitung von SNMPv2

Wie in Kapitel 3.2.1 erwähnt, existieren mehrere unterschiedliche Versionen von SNMPv2. Genau aus diesem Grund und angesichts dieser Verwirrungen um diese unterschiedlichen Versionen, wurde SNMPv2 nur von wenigen Herstellern implementiert und blieb somit auch relativ wenig benutzt.
Die größte Verbreitung fand noch Version SNMPv2c, da diese die altbekannten Sicherheitsmechanismen von Version eins verwendet.
Die beiden wesentlichen Vorteile von SNMPv2, nämlich die Funktionen GetBulkRequest und InformRequest, waren zuwenig Anreiz für viele Hersteller und Firmen, um die neuere Version einzusetzen.

4. SNMPv3

4.1 Entwicklung von SNMPv3

Da SNMPv2 zwar funktionelle Erweiterungen brachte, aber aus sicherheitstechnischer Sicht kein Fortschritt war, sollte eine neue Version, SNMP Version 3, kurz SNMPv3, diese Probleme beseitigen.
1998 wurden von der IETF einige RFC's veröffentlicht. Diese RFC's beschreiben die grundsätzliche Architektur inkl. der spezifischen Nachrichtenstrukturen und der Sicherheitsmaßnahmen. Sie definieren aber kein neues PDU Format. Es handelt sich also bei SNMPv3 um eine Architektur, die auf bewährte Funktionalität von SNMPv1/SNMPv2 aufbaut und diese mit neuen Sicherheitsmerkmalen erweitert.

„SNMPv3 is SNMPv2 plus administration and security" [Stallings, 1999, S. 450]

2002 wurde SNMPv3 von der IETF zum „full standard" erklärt. Die Dokumente von 1998 wurden überarbeitet (vgl. Tabelle 4: SNMPv3 Dokumente [URL6]).
Hauptaugenmerk lag bei der Entwicklung bei Modularität und Erweiterbarkeit der Architektur. Zu den wichtigsten Features von SNMPv3 zählen Verschlüsselungs- und Authentifizierungsmechanismen sowie die Möglichkeit zur Zugriffskontrolle.

Tabelle 4: SNMPv3 Dokumente [URL6]

RFC 3410	Introduction and Applicability Statements for Internet-Standard Management Framework
RFC 3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC 3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413	Simple Network Management Protocol (SNMP) Applications
RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3415	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC 3416	Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
RFC 3417	Transport Mappings for the Simple Network Management Protocol (SNMP)
RFC 3418	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)

4.2 Architektur

Wie in RFC 3411 beschrieben, besteht die SNMP Architektur aus verteilten, sich gegenseitig beeinflussenden SNMP entities (Entitäten). Jede dieser Entitäten kann als Agent, Manager oder als beides fungieren. Sie bestehen aus einer Sammlung von Modulen, wodurch entsprechende Services bereitgestellt werden (siehe Abbildung 19: SNMP entity [RFC 3411]).

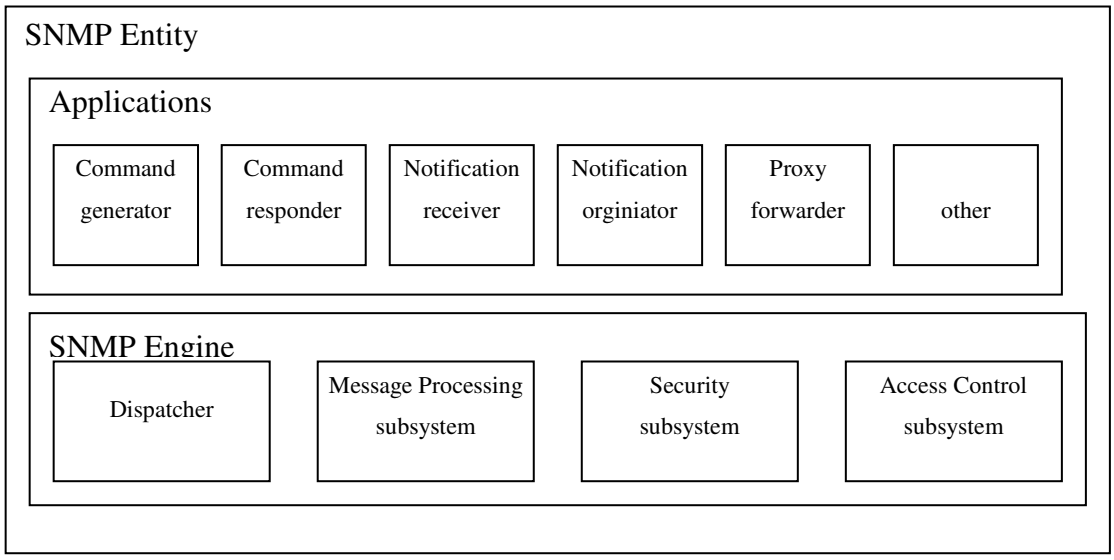

Abbildung 19: SNMP entity [RFC 3411]

4.2.1 SNMP Applications

Wie in Abbildung 19: SNMP entity [RFC 3411] zu sehen ist, beinhaltet eine SNMP entity mehrere Applikationen [vgl. RFC 3411]:

Command Generator

Zuständig für SNMP Get, GetNext, GetBulk und SetRequest PDUs und Zuordnung der Antworten auf die erzeugten Anfragen.

Command Responder

Führt die Anfragen, die an das lokale System gestellt wurden, unter Berücksichtigung der Zugriffskontrolle durch (Get, GetNext, GetBulk, SetRequest) und antwortet entsprechend.

Notification Receiver

Lauscht und antwortet auf Inform PDU Nachrichten.

Notification Originator

Zuständig für die Überwachung auf bestimmte Ereignisse oder Zustände. Erzeugt Traps und oder Inform Nachrichten, basierend auf den aufgetretenen Ereignissen. Der Notification Originator muss Information über das System, an die er die Nachrichten schicken soll (SNMP Version, Sicherheitseinstellungen), besitzen.

Proxy Forwarder

Leitet SNMP Nachrichten zu anderen SNMP Entitäten weiter. Die Implementierung des ProxyForwarders ist optional.

4.2.2 SNMP Engine

Wie in Abbildung 19: SNMP entity [RFC 3411]zu sehen ist, besteht eine SNMPv3 Engine aus folgenden Teilen [vgl. RFC 3411]:

Dispatcher

Erlaubt gleichzeitige Verwendung mehrere SNMP Versionen.
Schickt PDUs von Applikationen über das Netzwerk und stellt empfangene PDUs an die entsprechenden Applikationen zu (mit Hilfe des Message Processing Subsystems).

Message Processing Subsystem

Erzeugt Nachrichten die gesendet werden sollen und extrahiert die Daten von empfangenen Nachrichten. Unterstützt Message Processing Modelle für SNMPv1, SNMPv2c, SNMPv3.

Security Subsystem

Zuständig für die Authentifizierung der Nachrichten. Beinhaltet mehrere Security Models (Sicherheitsmodelle).

Access Control Subsystem

Stellt einige Authorizationservices zur Verfügung, mit deren Hilfe Applikationen Rechte überprüfen können.

Um die Aufgaben der einzelnen Systeme besser zu verstehen, sollen nachfolgend Agent und Manager mit SNMPv3 Modulen erklärt werden.

4.2.3 SNMPv3 Manager

Umgelegt auf SNMPv3, enthält ein klassischer SNMP Manager drei Arten von Applikationen:
(siehe Abbildung 20: SNMPv3 Manager [Stallings, 1999, Figure 15.4])

- Command generator Applikation – verwendet Get, GetNext, GetBulk und Set von v1/v2, um Informationen auf Agents zu sammeln oder zu ändern.
- Notification Originator Application – zuständig für das Senden von InformRequest
- Notification Receiver Application – zuständig für das Empfangen von InformRequest, SNMP Traps (v1 und v2) und deren Bestätigung mit ResponsePDU.

Die SNMP Engine selbst stellt prinzipiell folgende beiden Funktionen zur Verfügung:
(siehe Abbildung 20: SNMPv3 Manager [Stallings, 1999, Figure 15.4])

- Eingehende PDU von SNMP Applikationen akzeptieren und weiterverarbeiten (Authentifizierung und Verschlüsselung hinzufügen, „Verpacken“ der PDUs in Nachrichten, die verschickt werden können).
- Eingehende Nachrichten vom Transport Layer[17] annehmen, authentifizieren, entschlüsseln und an die entsprechende SNMP Applikation weiterreichen.

Der Dispatcher übernimmt PDUs von den SNMP Applikationen und reicht es an das entsprechende Message Processing Subsystem weiter (unterschieden wird SNMPv1, SNMPv2c, SNMPv3). Das Message Processing Subsystem gibt eine SNMP Message zurück, die die PDU und entsprechende Header enthält. Diese SNMP Message wird vom Dispatcher dann an die Transportschicht weitergegeben und versendet. Nachrichten vom Transport layer werden vom Dispatcher an das entsprechende Message Processing Subsystem geliefert. Dieses gibt die PDU an den Dispatcher zurück, der diese an die entsprechende SNMP Applikation weitergibt.

Das Message Processing Subsystem übernimmt Nachrichten vom Dispatcher und ergänzt sie mit entsprechenden Headerinformationen, damit der Dispatcher sie anschließend verschicken kann. Umgekehrt entfernt das Message Processing Subsystem Headerinformationen von eingehenden Nachrichten und gibt diese an den Dispatcher zurück. Das Message Processing Subsystem kann aus einem oder mehreren Modulen (jeweils für SNMPv1, SNMPv2c, SNMPv3) bestehen.

Das Security Subsystem ist für die Authentifizierung und Verschlüsselung zuständig. Jede ausgehende Nachricht wird vom Message Processing Subsystem an das Security Subsystem weitergeleitet. Dieses ent- oder verschlüsselt die Nachricht, generiert Authentifizierungs-informationen bzw. überprüft diese. Anschließend wird die Nachricht an das Message Processing Subsystem zurückgegeben.

[17] Siehe OSI Modell

Das Security Subsystem kann ein oder mehrere Sicherheitsmodelle unterstützen (das einzig Definierte, ist das User-Based security-model (USM) für SNMPv3).

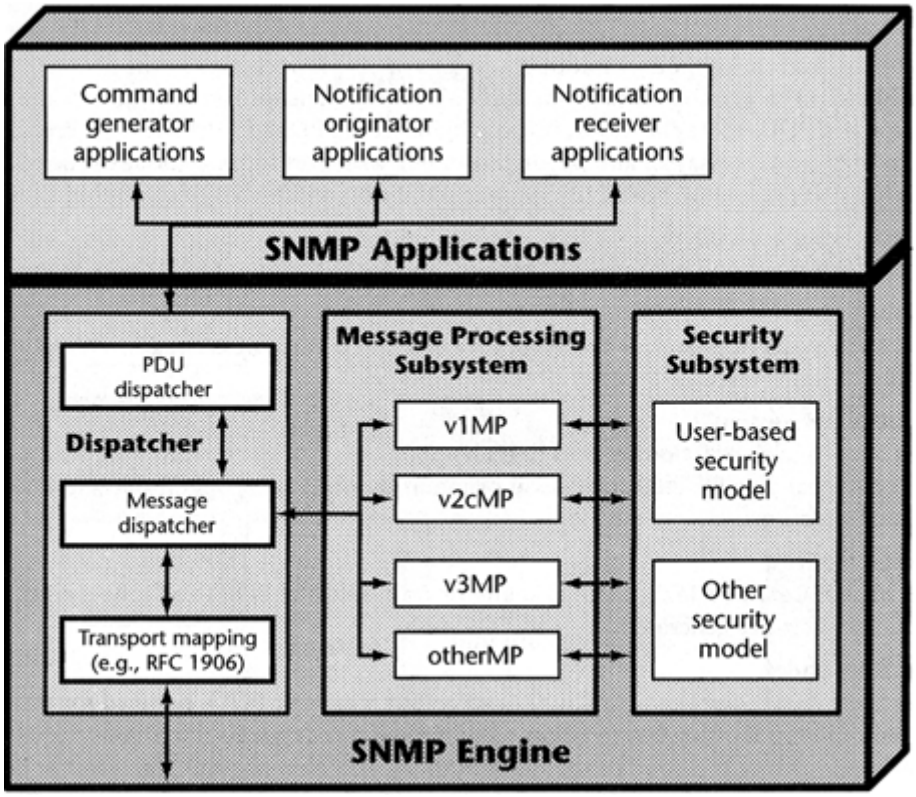

Abbildung 20: SNMPv3 Manager [Stallings, 1999, Figure 15.4]

4.2.4 SNMPv3 Agent

Bezogen auf SNMPv3, enthält ein klassischer SNMP Agent folgende Applikationen: (siehe Abbildung 21: SNMPv3 Agent [Stallings, 1999, Figure 15.5])

- Command Responder Application – für Zugriff auf Management Daten.
- Notification Originator Application – löst Trap (v1/v2) aus.
- Proxy Forwarder Application – gibt Nachrichten an andere Entitäten weiter

Die SNMP Engine eines SNMPv3 Agent enthält alle Teile, die auch ein SNMPv3 Manager beinhaltet. Zusätzlich besitzt es ein Access Control Subsystem, welches für Zugriffskontrolle auf die MIBs zuständig ist. Das Access Control Subsystem kann eines

oder mehrere Sicherheitsmodelle unterstützen. (das einzig-definierte security model ist das View-Based Access Control Model (VACM) für SNMPv3).

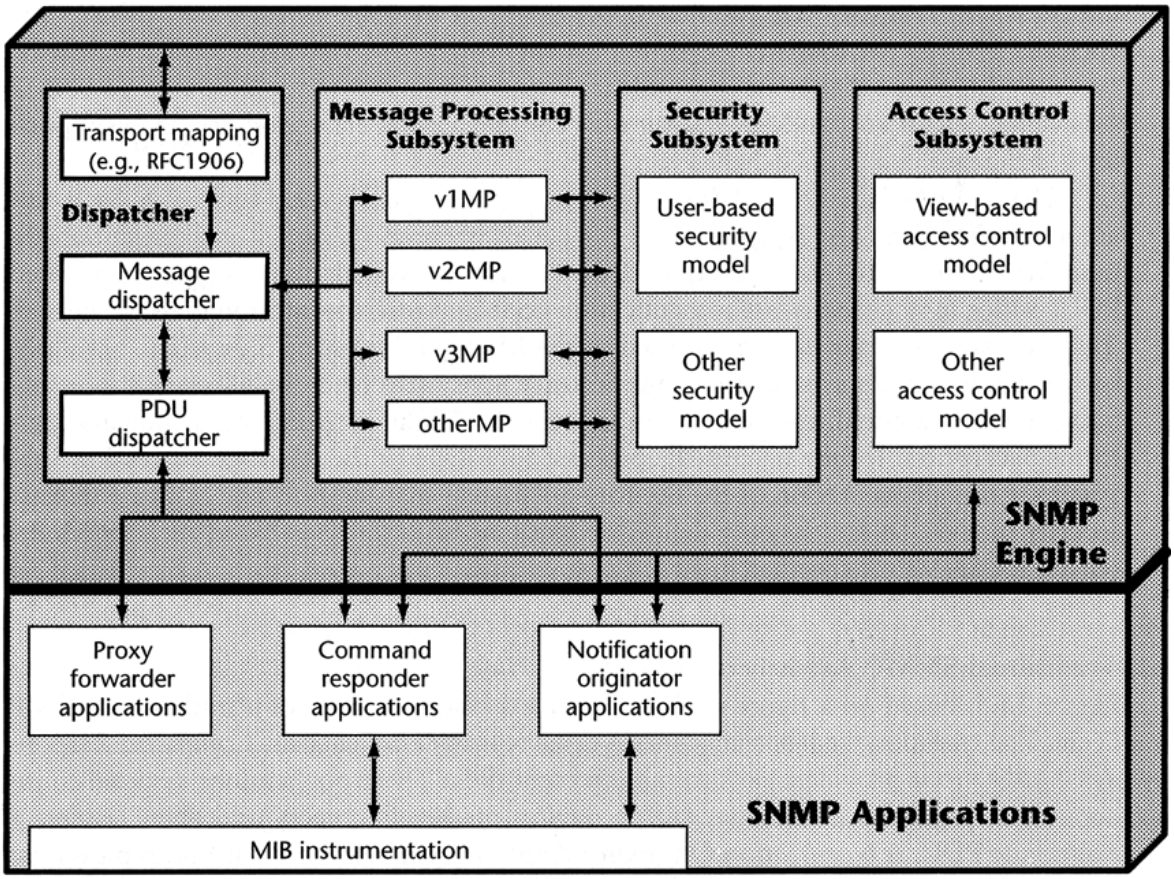

Abbildung 21: SNMPv3 Agent [Stallings, 1999, Figure 15.5]

4.3 SNMPv3 Nachrichtenformat

Genauso wie in früheren SNMP Versionen (SNMPv1, SNMPv2), werden bei SNMPv3 Informationen zwischen SNMP Entitäten in Form von Nachrichten ausgetauscht. Jede dieser Nachrichten enthält einen Nachrichtenkopf (Message header) und eine PDU.
Der Aufbau von SNMPv3 Nachrichten sieht folgendermaßen aus: [vgl. RFC 3412]

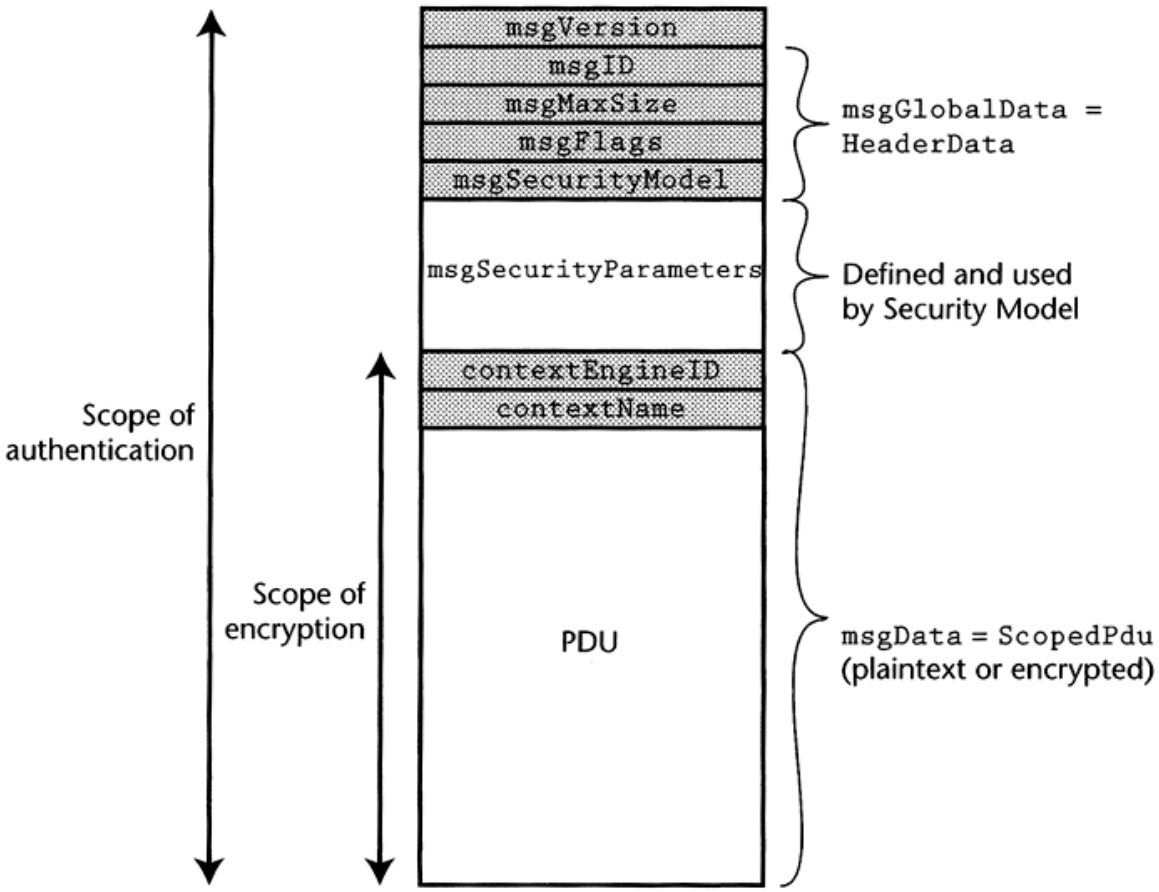

Abbildung 22: SNMPv3 Nachrichtenformat [Stallings, 1999, Figure 16.1]

msgVersion

hat bei SNMPv3 den Wert 3.

msgID

Die msgID wird zwischen zwei SNMP Entitäten verwendet, um Anfragen und Antworten einander zuordnen zu können. Wertebereich: $0 – 2^{31}-1$.

msgMaxSize

Gibt die Maximalgröße einer Nachricht an, die die Quelle der Nachricht unterstützt.

msgFlags

Beinhaltet einige Bits, welche die Verarbeitung der Nachricht steuern.

- reportable Flag - Gibt an, ob ein Report PDU an den Sender der Nachricht geschickt werden muss (Wert 1) oder nicht (Wert 0). (bei allen Get, Set Operationen = 1, bei Response, Trap = 0)
- privFlag – Gibt an, dass die Nachricht verschlüsselt ist.
- authFlag – Gibt an, dass Authentifizierung notwendig ist

privFlag und authFlag können beliebig kombiniert werden (bis auf die Kombination: Verschlüsselung = ein und Authentifizierung = aus)

msgSecurityModel

Gibt das Sicherheitsmodell an, dass der Sender beim Erzeugen der Nachricht verwendet hat. Das gleiche Modell, muss der Empfänger benutzen, um die Nachricht verarbeiten zu können.

msgSecurityParameters

Diese Parameter werden für die Kommunikation der SecurityModel Module in der Sender- und Empfänger SNMP Engine verwendet.
Der Inhalt wird ausschließlich vom SecurityModel benutzt. Der Inhalt und das Format dieser Daten wird vom SecurityModel definiert.

contextEngineID

Die contextEngineID ist für die eindeutige Identifizierung einer SNMP Entität zuständig.

contextName

contextName in Verbindung mit contextEngineID identifiziert den Kontext, der im PDU Teil der Nachricht enthalten ist.

data

Beinhaltet eine PDU. Das SNMPv3 Message Processing Model legt fest, dass es sich hierbei um eine SNMPv2 PDU handeln muss.

4.4 User-Based Security Model

4.4.1 Allgemein

Die Idee hinter USM[18] ist, dass verschiedene Benutzer (identifiziert durch Benutzername) inkl. zusätzlicher Sicherheitsinformationen (geheime Schlüssel – authKey, privKey) verwaltet werden.
Für dieses Sicherheitsmodell ist der Begriff der „authoritative SNMP Engine“ entscheidend. [vgl. Stallings, 1999, S. 499].
Bei jedem Nachrichtenaustausch, muss eine der beiden SNMP Engines authoritative, also bestimmend, fungieren. Welche der beiden das ist, wird mit folgenden Regeln festgelegt:

- Bei SNMP Nachrichten, wo eine Antwort erwartet wird (Get, GetNext, GetBulk, Set, Inform), ist der Empfänger dieser Nachricht bestimmend.
- Bei SNMP Nachrichten, wo keine Antwort erwartet wird (SNMPv2 Trap, Response, Report), ist der Sender dieser Nachricht bestimmend.

Das USM ist modular aufgebaut. Es wird in der RFC 3414 spezifiziert und umfasst im Wesentlichen folgende Punkte:

- Message format: Definiert msgSecurityParamters (siehe Abbildung 22: SNMPv3 Nachrichtenformat)

[18] User-Based Security Model

- Timeliness: Prüft auf Aktualität (Schutz gegen verzögerte (delay) oder wiederholte (Replay) Sendung von Nachrichten – message stream modification)
- Authentication: Bietet Datenintegrität (Überprüfung auf Veränderungen der Daten – modification of information) und Überprüfung der korrekten Identität des Benutzers (ein unbefugter Benutzer versucht sich als ein autorisierter User auszugeben – masquerade)
- Privacy: Schutz durch Verschlüsselung (unautorisierte Entitäten dürfen den Inhalt von einer SNMP Kommunikation nicht sehen – disclosure)

Im Folgenden werden die wichtigsten Funktionen des USM erklärt.
Für nähere Informationen: [RFC 3414]

4.4.2 USM Security Parameters

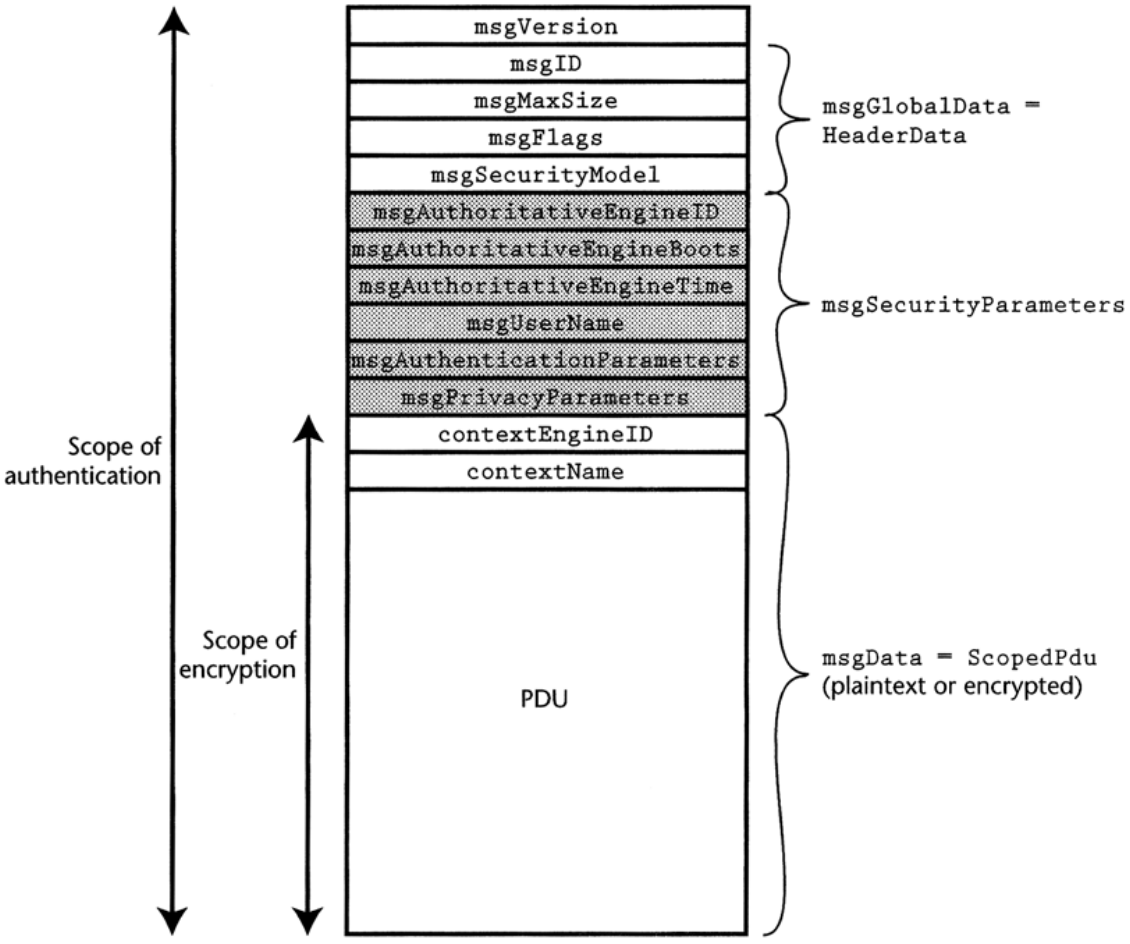

Abbildung 23: USM Security Parameters [Stallings, 1999, Figure 16.6]

Das USM verwendet folgende Sicherheitsparameter:

msgAuthoriatativeEngineID

Gibt snmpEngineID (eindeutige ID jeder SNMP Engine) der autoritativen SNMP Engine (siehe 4.4.1) für diese Nachricht an. Das bedeutet, dass dieses Feld bei Trap, Response oder Report auf die Quelle und bei Get, GetNext, GetBulk, Set oder Inform auf den Empfänger verweist.

msgAuthoritativeEngineBoots

Gibt an, wie oft die SNMP Engine, seit dem letzten Ändern der snmpEngineID, initialisiert wurde.

msgAuthoritativeEngineTime

EngineTime der authoritative SNMP Engine.

msgUserName

Spezifiziert den User, der für den Nachrichtenaustausch verantwortlich ist.

msgAuthenticationParamters

Wird durch das Authenticationprotocol definiert, dass für diese Nachricht verwendet wird.

msgPrivacyParameters

Gibt Information über die verwendete Verschlüsselung.

4.4.3 Aktualität

Das „Timeliness Module“ ist zuständig für Schutz vor mutwilliger Nachrichtenverspätung (Delay) und wiederholter Versendung identischer Nachrichten (Replay). Es stellt also die Aktualität der empfangenen Nachrichten sicher.
Prinzipiell werden für den Schutz gegen Delay und Replay die drei Parameter msgAuthoriatativeEngineID, msgAuthoritativeEngineBoots und msgAuthoritative-EngineTime verwendet. Außerdem werden diese drei Parameter für die zeitliche Synchronisation von „Non-Authoritative Engine“ und „Authoritative Engine“ verwendet. Auf dieses Modul soll hier nicht näher eingegangen werden).
[vgl. Stallings, 1999, S. 502]

4.4.4 Authentifizierung

Das „Authentication Module“ stellt Datenintegrität und Korrektheit der angegebenen Herkunft der Nachrichten sicher. Bisher erlaubt das „User-based Security Model“ für diesen Zweck die Verwendung zweier Authentifizierungsprotokolle (HMAC-MD5-96 und HMAC-SHA-96), weitere können allerdings definiert werden.
Zum Einsatz kommen innerhalb der Implementierungen die Hashfunktionen MD5 [RFC 1321] (mit einer Schlüssellänge von 128 bit) und SHA-1 [URL7] (160 bit), die im HMAC-Verfahren verwendet werden.
Auf diese Algorithmen wird hier nicht näher eingegangen.

4.4.5 Verschlüsselung

Das „User-based Security Model“ kann zur Verschlüsselung der Nutzdaten einer Nachricht verschiedene Implementierungen von Verschlüsselungsalgorithmen verwenden. Im Standard definiert ist allerdings nur ein konventionelles, symmetrisches Kryptosystem: bei CBC-DES handelt es sich um den Data Encryption Standard (DES), betrieben im Cipher Block Chaining Mode (CBC). Dieser Modus sorgt dafür, dass das Verschlüsseln eines

Klartextblocks immer zu unterschiedlichen Ergebnissen führt, indem dem Verschlüsselungsalgorithmus exklusiv verodert der aktuelle Klartextblock und der letzte Chiffreblock zugeführt werden. Besonders bei längerem, stark durchstrukturiertem Klartext erhöht dieses Verfahren deutlich die Sicherheit. [vgl. Stallings, 1999, S.430-432]

4.5 View-Based Access Control Model

Beim „View-Based Access Control Model“ (VACM) handelt es sich um ein Modul für die Zugriffskontrolle. Es wird in der RFC 3415 definiert. Die Aufgabe der Zugriffskontrolle fällt prinzipiell den „Authoritative SNMP Engines“ zu, die somit dieses Access Control Subsystem integriert haben müssen.
VACM ist rein für die Zugriffskontrolle zuständig. Deshalb ist vorhergehend ein Sicherheitsmodell (zum Beispiel USM) notwendig, dass Nachrichten auf Echtheit überprüft und Sicherheitsinformationen und Nutzdaten zur Verfügung stellt.
VACM trifft Entscheidungen, ob eine Aktion erlaubt oder nicht erlaubt ist, anhand von Security Model/Security Level (der eigentlichen Anfrage), Context, Zugriffstyp (lesen, schreiben, informieren) und des Objekts für welches Zugriff angefordert wird. (s. Abbildung 24: Beispiel VACM)

Elemente des VACM Models: [vgl. RFC 3415]:

- Groups
- Security Level
- Contexts
- MIB Views
- Access policy

Nachstehend werden diese Elemente erklärt.

4.5.1 Groups / Security Level

Im Gegensatz zum „User-based Security Model“, das auf Benutzern basiert, definiert das „Viewbased Access Control Model“ Rechte auf Basis von Gruppen, in denen verschiedene Benutzer mittels ihres Namens und des verwendeten Sicherheitsmodells zusammengefasst werden. Prinzipiell haben alle Mitglieder einer Gruppe identische Rechte, eine feinere Aufteilung wird allerdings über den Security Level der Nachricht vorgenommen. So wird es zum Beispiel möglich, sensible Daten nur bei Verwendung von sowohl Authentifizierung als auch Verschlüsselung freizugeben, oder für Nachrichten mit noAuthNoPriv den Zugriff auf nur Lesen zu beschränken.

4.5.2 Contexts / MIB Views

Informationen innerhalb einer SNMP Entität werden zunächst in Contexts organisiert. Dabei handelt es sich um eine Zusammenstellung von Managementinformation, die einem Kontext zugehörig ist. In [Stallings, 1999, S. 527] wird hierfür ein Beispiel angeführt, in dem eine SNMP entity Information zweier nicht-SNMP-fähiger Bridges verwaltet wird und somit außer dem eigenen default-Kontext zwei weitere, bridge1 und bridge2 benannte, enthält.
Innerhalb des Contexts wird das Rechtesystem noch feiner granuliert, indem MIB Views den Zugriff gemäß der viewTypes read (Lesezugriff), write (Lese- und Schreibzugriff) und notify (lokaler Zugriff zum Verschicken von Benachrichtigungen) unterteilen. Jede MIB View wird als Menge von Unterbäumen der Management Information Base strukturiert, die jeweils unter dem Object Identifier ihrer Wurzel abgelegt werden.

4.5.3 Access policy

VACM ermöglicht SNMP Engines Zugriffsunterscheidungen nach folgenden Kriterien zu treffen [Stallings, 1999, S. 528]:

- Nach Benutzer: VACM erlaubt SNMP Agents verschiedenen Usern verschiedene Zugriffsrechte zu geben.
- Nach Security Level: beispielsweise kann ein Agent Authentifizierung für SET-Requests voraussetzen.
- Nach Security Model: Wenn mehrere Security Models verwendet werden, kann ein Agent je nach verwendetem Security Model einer Nachricht unterschiedliche Rechte vergeben. Zum Beispiel kann ein Objekt lesbar sein, wenn das Security Model USM ist, nicht aber wenn es SNMPv1 ist.
- Nach MIB context
- Nach Art des Zugriffs (verschiedene Policies für Read, Write und Notify sind möglich)

MIB View	allowed operations	allowed managers	required level of security
Interface Table	GET / GETNEXT	ro_user1, wr_user1	authentication
Interface Table	SET	wr_user1	authentication, encryption
Systems Group	GET / GETNEXT	ro_user2, wr_user1	authentication, encryption
Systems Group	SET	wr_user1	authentication, encryption

Abbildung 24: Beispiel VACM

4.6 Verbesserungen gegenüber früheren Versionen

Die wohl wichtigste Verbesserung von SNMPv3 gegenüber den früheren Versionen liegt in der Integration der verbesserten Sicherheitsmechanismen. Bezogen auf das CIA Sicherheitsmodell sind damit die Vertraulichkeit und Integrität sichergestellt. Weiters schützen die SNMPv3 Mechanismen gegen Replay-Attacken (aufgezeichnete Pakete werden nochmals gesendet).

Damit sind die entscheidenden Schwächen von SNMPv1 und SNMPv2c behoben. Gleichzeitig wird mit SNMPv3 eine erweiterbare Architektur definiert, die so flexibel ist, dass sie einen abermaligen Sprung zu einer neuen Version aus heutiger Sicht unnötig macht. Durch die flexible Struktur können nicht nur alle verwenden Sicherheitsprotokolle wie MD5, SHA-1 oder DES ersetzt werden, sondern auch ganze Modelle für Sicherheit und Zugriffskontrolle definiert werden.
Die Verwendung des DES Kryptosystems ist aus heutiger Sicht nur mehr bedingt sicher – für den Einsatz innerhalb eines Netzwerkgerätes ist es aus Kosten sowie Designgründen anderen komplizierteren Mechanismen vorzuziehen. Durch Austausch des PrivacyModules könnte zudem leicht auf 3DES oder AES umgestellt werden.

Ein Problem, dass aber das SNMP Konzept mit sicht bringt, können auch die nunmehr vorhandenen Sicherheitsmechanismen nicht ändern: die Verwendung des verbindungslosen Protokolls UDP.

Aber auch die neueste Version von SNMP schützt nicht gegen „Denial of Service“ Attacken: Ein potentieller Angreifer kann den Nachrichtenaustausch von Manager und Agent verhindern, da zwischen einem solchen Angriff und dem tatsächlichen Ausfall des Netzwerks bzw. einer Komponente des Netzwerks nicht unterschieden werden kann.
Außerdem kann weiterhin von Angreifern eine prinzipielle „Traffic Analysis“ durchgeführt werden um den Nachrichtenaustausch von Manager und Agent zu beobachten, wenngleich die Nachrichten auch verschlüsselt und somit unlesbar für den Außenstehenden sind.

4.7 SNMPv3 in der Praxis

Im Folgenden werden die wichtigsten Parameter zusammengefasst, die bei der Konfiguration eines SNMPv3 Gerätes zu beachten sind. Wichtig ist, dass entsprechende Parameter immer paarweise auf dem SNMPv3 Gerät selbst und in der Managementsoftware konfiguriert werden müssen.
(s. weiterführend [Douglas, 2005, S. 91])

Benutzername / Username
Benutzername, der für den Zugriff verwendet werden soll.

Sicherheit / Securitylevel

Gibt an, welcher Sicherheitslevel beim Zugriff angewendet werden soll. (siehe 4.3)
Prinzipiell möglich ist: keine Authentifizierung, keine Verschlüsselung (noAuthNoPriv)
Authentifizierung, keine Verschlüsselung (authNoPriv)
Authentifizierung, Verschlüsselung (authPriv)

Authentifizierung / Authentication
Gibt an, welche Art der Authentifizierung verwendet werden soll (die RFCs definieren MD5 oder SHA-1)

Authentifizierungskennwort / Authentication passphrase
Wird in Verbindung mit dem Authentifizierungsprotokoll verwendet.

Verschlüsselung / Privacy
Gibt an, welche Verschlüsselung verwendet werden soll (die RFCs definieren DES)

Verschlüsselungskennwort / Privacy passphrase
Wird in Verbindung mit der Verschlüsselung verwendet.

5. Unterstützung in aktuellen Systemen

5.1 Grundsätzliches zur Verbreitung von SNMPv3

Trotz der wesentlichen Verbesserungen, die SNMPv3 bezüglich Sicherheit mit sich bringt, hält sich seine Präsenz in der „Netzwerk-Community“ in Grenzen.
Ein Grund dafür dürfte im ungleich höheren Implementierungsaufwand für Hersteller von Netzwerkkomponenten liegen. Dieser höhere Aufwand, um SNMPv3 in Geräte zu integrieren, hat wiederum Auswirkungen auf den Preis von Geräten, da durch die komplexeren Mechanismen von SNMPv3 oft auch leistungsfähigere Hardware von Nöten ist. Dies könnte auch der Anlass sein, warum SNMPv3 bei Geräten eines Herstellers nicht durchgängig verfügbar ist.

Weiters ist auch der Verwaltungsaufwand für Netzwerkadministratoren, verglichen mit SNMPv1 Installationen, sehr viel größer.
Die Konfiguration von SNMPv1 ist dazu nahezu selbsterklärend und wird deshalb nach wie vor von sehr vielen Systemverantwortlichen eingesetzt. Die komplexere Konfiguration der Version 3 und der dadurch entstehende Mehraufwand schrecken sicher einige Netzwerkbetreiber ab.

Ein zusätzliches Problem, dass zur derzeit relativ geringen Verbreitung von SNMPv3 beiträgt, ist die Tatsache, dass viele Unternehmen reine Monitoringlösungen im Einsatz haben und per SNMP keine aktive Steuerung vornehmen. Somit erscheint diesen Betreibern die mangelhafte Sicherheit von SNMPv1 als ausreichend.

5.2 Managementsysteme

Im Folgenden sollen aktuelle Netzwerkmanagementsysteme (NMS) auf die SNMPv3 Unterstützung untersucht werden. Die Liste relevanter NMS wurde durch Internetrecherche und Vergleiche mit [Douglas, 2005, S. 378] und [Zechmeister, 2005, S. 70] ermittelt.
Alle angegebenen Daten beziehen sich auf den aktuellen Stand der Systeme (Juni 2006).

Folgende Managementsysteme werden auf SNMPv3 Unterstützung untersucht:

Kommerzielle Produkte:

- HP OpenView
- IBM Tivoli
- CastleRock SNMPc
- CiscoWorks
- IPSwitch WhatsUp Gold
- Solarwinds

OpenSource Produkt:

- OpenNMS

Andere bekannte OpenSource Produkte wie Nagios oder JFFNMS wurden nicht näher untersucht, da diese Produkte reine Monitoringlösungen sind und keine Steuerungsmöglichkeiten bieten.

5.2.1 HP OpenView Network Node Manager

Homepage: [INFOURL1]
Aktuelle Version: 7.5 (Juli 2004)
Betriebssysteme: Solaris, HP-UX, Windows NT/2000/2003, Linux

Das Basisprodukt unterstützt standardmäßig SNMPv1 und SNMPv2C (CommunityBased) (lt. HP Handbuch Network Note Manager vom Juli 2004). Mit dem Zusatz: „SNMP Security Pack“ von SNMP Research kann HP OpenView allerdings SNMPv3-fähig gemacht werden. Der „SNMP Security Pack“ unterstützt USM und VACM [vgl. INFOURL2]. Damit können mehrere Benutzer angelegt und verschiedene Sicherheitsgruppen mit unterschiedlichen Rechten auf Views erstellt werden.

5.2.2 IBM Tivoli NetView

Homepage: [INFOURL3]
Aktuelle Version: 7.1.4 (Dezember 2004)
Betriebssysteme: AIX, Linux, Solaris, WindowsNT/2000

Wie bei HP OpenView unterstützt auch das Basisprodukt kein SNMPv3. Diese Funktionalität kann abermals mit dem „SNMP Security Pack“ von SNMP Research nachgereicht werden. Der „SNMP Security Pack“ unterstützt USM und VACM. [vgl. INFOURL2]
Eine eigene SNMPv3 Unterstützung ist für das nächste Release von Tivoli NetView geplant, voraussichtlicher Termin 2. Hälfte 2006 [vgl. INFOURL4]. Ein Anruf beim zuständigen Serviceteam brachte leider keine näheren Informationen, da ohne gültigen Servicevertrag eine Weiterleitung an das technische Fachpersonal verwährt wurde.

5.2.3 CastleRock SNMPc

Homepage: [INFOURL5]
Aktuelle Version: 7.0 (Juni 2004)
Betriebssysteme: Windows 98/ME/NT/2000/XP/2003

CastleRock SNMPc bringt in seiner Netzwerkmanagementsuite eine hauseigene SNMPv3 Unterstützung mit:

„Safely manage devices with SNMPv3 Authentication and Encryption. Tailor views and capabilities to each management user“ [INFOURL6]

Diese Aussage auf dem Datenblatt von SNMPc lässt darauf schließen, das sowohl USM als auch VACM unterstützt werden.

5.2.4 CiscoView

Homepage: [INFOURL7]
Aktuelle Version: 6.1.2
Betriebssysteme: Windows

CiscoView ist Teil des Pakets CiscoWorks von Cisco. In diesem Paket ist eine ältere Version von Whats Up Gold für das Netzwerkmanagement enthalten. CiscoView selbst ist eine Weboberfläche mit der Möglichkeit Cisco Komponenten grafisch zu bedienen.

„CiscoView supports SNMPv3 communication with authentication but without privacy (AuthNoPriv support) for greater security“ [INFOURL8]

5.2.5 Whats Up Gold

Homepage: [INFOURL9]
Aktuelle Version: Professional 2006 (Dezember 2005)
Betriebssysteme: Windows XP/2000/2003

Die aktuelle Version von Whats Up Gold kann mit einer SNMPv3 Unterstützung aufwarten. Unterstützt wird Authentifizierung und Verschlüsselung. [vgl. INFOURL10]

5.2.6 Solarwinds

Homepage: [INFOURL11]
Aktuelle Version: 8.0 Professional (Juni 2005)
Betriebssysteme: Windows 95 – 2003 Server

Bei Solarwinds Professional handelt es sich um eine ganze Sammlung von nützlichen Netzwerkmanagementtools. Aus diesem Grund kann keine pauschale Aussage über die Unterstützung der höchsten SNMP Versionen von allen Tools getroffen werden. Der Homepage ist zu entnehmen, dass einige Tools SNMPv2C unterstützen, andere wiederum nur SNMPv1. Auf eine Anfrage bzgl. SNMPv3 Unterstützung an den Support kam folgende klärende Antwort per Mail:

„Thank you for contacting SolarWinds.Net. At this time none of our tools support SNMP v3. We are working on this for a future release; however I do not have a timeframe for when this will be available. Please let us know if we can provide any additional information or assistance.“

5.2.7 OpenNMS

Homepage: [INFOURL12]
Aktuelle Version: 1.2.8 (letzte „Stable“ Version, Juni 2006)
Betriebssysteme: Linux, Solaris

In der aktuellen stabilen Version gibt es keine Unterstützung für SNMPv3, lediglich SNMPv1 und SNMPvc2 werden unterstützt. Ab Version 1.3 soll es aber lt. [INFOURL13] möglich sein, alternative SNMP Libraries zu verwenden. Damit steht einer Unterstützung für SNMPv3 ab dieser Version nichts mehr im Wege. Eine Unstable-Version 1.3.1 für Linux ist bereits verfügbar, ein Termin für die fertige Version konnte nicht in Erfahrung gebracht werden.

6. Clients

In diesem Abschnitt sollen verschiedene Netzwerkclients auf ihre SNMP Fähigkeit untersucht werden. Dazu muss man prinzipiell zwei Kategorien von Clients unterscheiden:

- Clients, wo ein SNMP Agent fix integriert ist (Beispiel: Router, Switches, meist netzwerkfähige Geräte mit proprietärer Software bzw. Firmware)
- Clients, wo ein SNMP Software-Agent installiert werden kann/muss (Beispiel: Betriebssysteme wie Windows oder Linux). Durch die freie Auswahl des Software-Agents sind diese Clients bezüglich SNMPv3 Unterstützung meist flexibler.

Nachfolgend wird zunächst auf die SNMP Unterstützung von Netzwerkgeräten mit integriertem Agenten eingegangen. Anschließend sollen SNMP Software-Agents auf Kompatibilität überprüft werden. Zu erwähnen ist, dass lediglich Produktgruppen für Unternehmen und keine SOHO Geräte auf Kompatibilität überprüft wurden.

6.1 Clients mit integriertem Agent

Netzwerkprodukte wie Switches und Router haben praktisch immer einen Agent, der in die Firmware des Gerätes integriert ist. Dadurch ist es den Herstellern möglich, SNMPv3 Unterstützung für ältere Geräte nachzureichen. Vorraussetzung dafür ist natürlich die Bereitschaft des Herstellers eine entsprechende Firmware zu entwickeln und dass die Geräte entsprechend ausgerüstet sind. Beispielsweise könnte für eine Firmware mit mehr Features mehr Speicher notwendig sein.

6.1.1 Cisco

Cisco bietet für alle Clients ab IOS Version 12.0(3)T eine Unterstützung von SNMPv3, allerdings nur Authentifizierung. Ab IOS Version 12.4(T) bzw. CatOS Version 6.3.1 wird auch Verschlüsselung unterstützt. [URL8]
Cisco unterstützt in allen seinen Geräten mit entsprechend oben genannter IOS Version neben USM auch VACM.

6.1.2 HP

Nach Auskunft von HP und Begutachtung einiger Datenblätter wird SNMPv3 durchgängig von den aktuellen Netzwerkprodukten unterstützt.
Konkret wurde eine SNMPv3 Unterstützung in den Datenblättern von folgenden Produkten gefunden (die Datenblätter dieser Geräte wurden untersucht):

- ProCurve Switch 2600 Serie
- ProCurve Switch 4100 Serie
- ProCurve Switch 5300 Serie
- ProCurve AccessPoint 520WL

Eine genaue Auskunft, ob USM oder VACM unterstützt werden, konnte weder den Datenblättern, noch der Supporthotline entnommen werden. Folgende Information auf den Datenblättern lässt aber erahnen, dass lediglich Verschlüsselung unterstützt wird:

„Alle Zugriffsmethoden (CLI, GUI oder MIB) sind über SSHv2, SSL und/oder SNMPv3 verschlüsselt“

VACM wird demnach nicht unterstützt.

6.1.3 3COM

Nach Auskunft eines 3COM Support Mitarbeiters ist bei allen aktuellen Netzwerkprodukten eine SNMPv3 Unterstützung vorhanden bzw. per Softwareupgrade nachrüstbar. Nach stichprobenartiger Durchsicht der Datenblätter aktueller Netzwerkprodukte, scheint überall SNMPv3 Support vorhanden zu sein. Besichtigt wurden die Datenblätter folgender Produkte:

- 3COM Switch 4500 Serie
- 3COM Switch 5500 Serie
- 3COM Switch 7700 Serie
- 3COM Switch 8800 Serie

Eine klare Aussage darüber, welche Features von SNMPv3 wirklich unterstützt werden, war nicht zu finden. Wiederum lässt folgende Information auf den Datenblättern aber erahnen, dass Verschlüsselung und Authentifizierung unterstützt werden, VACM aber nicht:

„Secure Shell (SSHv2) and SNMPv3 support ensure secure management access to switches via authentication and encryption of management traffic.“

6.1.4 Nortel

Auch Nortel bietet bei seinen aktuellen Netzwerkprodukten eine unterschiedliche Unterstützung für SNMPv3. Folgende Datenblätter von Nortel-Produkten wurden überprüft:

- Nortel Business Ethernet Switch 100 Serie
  Unterstützt nur SNMPv1 und v2

- Nortel Ethernet Switch 425
  Es wird ausdrücklich erwähnt, dass dieses Produkt USM (Verschlüsselung + Authentifizierung) und VACM unterstützt.

- Nortel BayStack 470
  In diesem Datenblatt wird SNMPv3 nur in Verbindung mit Authentifizierung und Verschlüsselung erwähnt.

6.2 Software-Agents

Bei Software-Agents handelt es sich um Programme, die entsprechende SNMPv3 Funktionen für bestehende Betriebssysteme nachreichen.

6.2.1 MG-Soft SNMP Master Agent

Homepage: [INFOURL14]
Betriebssysteme: Windows 95/98/ME/NT/2000/XP/2003

MG-Soft SNMP Agent ist ein Ersatz für das Windows-interne SNMP Service. Dieser Agent unterstützt SNMPv1, SNMPv2c und SNMPv3 mit Verschlüsselung und Authentifizierung. VACM wird in der derzeitigen Version nicht unterstützt. Eine Unterstützung ist lt. Support für eine der nächsten Versionen geplant.

6.2.2 Net-SNMP Agent

Homepage: [INFOURL15]
Betriebssysteme: Windows, Linux, Unix

Bei Net-SNMP handelt es sich um einen Agent für Windows und Linux Systeme. Unterstützt werden SNMPv1, SNMPv2 und SNMPv3 mit Verschlüsselung und Authentifizierung.

7. Leitfaden für die Migration von SNMPv1 auf SNMPv3 für mittlere Unternehmen

7.1 Allgemein

Dieses Kapitel soll einen Leitfaden für die Migration von SNMPv1 auf SNMPv3 für mittlere Unternehmen darstellen. Es sollen dabei grundlegende Schritte für diesen Vorgang beschrieben werden. Für größere Netzwerke sind entsprechend gut durchdachte komplexere Sicherheitsmaßnahmen (Benutzerberechtigungen, Ansichten, Gruppen) empfehlenswert. Zwecks Überschaubarkeit werden in diesem Leitfaden lediglich einfache Sicherheitsstrukturen verwendet.

7.2 Generelle Vorgehensweise

Zunächst soll die generelle Vorgehensweise für eine Migration auf SNMPv3 behandelt werden.
Folgende Punkte sind dafür notwendig.

- Ist-Bestandsaufnahme
- Ziele definieren
- Realisierbarkeit
- Aktualisierung der Komponenten
- Konfiguration der Komponenten
- Konfiguration der Managementsoftware
- Test der Konfiguration

Alle diese Punkte werden nachstehend erläutert:

7.2.1 Ist-Bestandsaufnahme

Als ersten Schritt gilt es den Ist-Zustand des Netzwerks festzustellen. Darunter fallen folgende Punkte:

- Art und Anzahl der Netzwerkprodukte (Switches, Router, usw) feststellen.
- Welche Firmwareversionen sind auf den Netzwerkprodukten im Einsatz?
- Welche sonstigen Komponenten (Server, Applikationen) sind im Netzwerk vorhanden?
- Bestandaufnahme und Analyse der bisherigen SNMP Konfiguration (Communitynamen, Traps, ..)

7.2.2 Ziele definieren

Um weiter vorgehen zu können, ist es notwendig, Ziele zu definieren. Das generelle Ziel, beim Einsatz von SNMPv3, lautet mehr Sicherheit. Es gilt zu definieren, welche Funktionen von SNMPv3 unterstützt werden sollen. Ein Optimum stellt natürlich die Verwendung von sämtlichen Sicherheitsmechanismen dar, die SNMPv3 bietet.
Weiters soll hier definiert werden, welche Netzwerkgeräte in das Netzwerkmanagement aufgenommen werden sollen. Zusätzlich ist abzuklären, welche Personen welchen Zugriff auf welche Netzwerkressourcen bekommen.

7.2.3 Realisierbarkeit

An dieser Stelle ist zu überprüfen, ob die oben beschlossenen Ziele, mit realistischem Aufwand erreicht werden können. Mögliche Gründe für das nicht Erreichen von zuvor definierten Zielen können sein:

- Spezifische Geräte, die die geforderten Sicherheitsmaßnahmen erfüllen, existieren nicht am Markt.

- Die bestehende Infrastruktur beherrscht SNMPv3 nicht und eine Unterstützung kann zum Beispiel auch nicht per Firmwareupdate nachgerüstet werden. Ein Austausch dieser Komponenten könnte einen enormen finanziellen Aufwand bedeuten und somit das Ende eines möglichen Migrationsszenario bedeuten.

Weiters gilt es zu überprüfen, ob eine Managementsoftware existiert, die die geforderten Voraussetzungen erfüllt.
An diesem Punkt muss entschieden werden, ob eine Migration technisch, sowie finanziell durchführbar ist.

7.2.4 Aktualisierung der Komponenten

Die Aktualisierung der Komponenten um SNMPv3 Tauglichkeit zu erlangen, kann auf mehreren Wegen erfolgen: Im einfachsten Fall genügt ein simples Firmwareupdate. Eventuell ist auch ein Hardwareupgrade (z.B. Speicher) möglich/notwendig. Dies stellt die kostengünstigste Variante dar. Ist eine entsprechende Unterstützung für ein Produkt nicht vorhanden bzw. nicht nachrüstbar, muss ein entsprechendes Neugerät besorgt werden.

7.2.5 Konfiguration der Komponenten

An diesem Punkt sollten bereits alle Netzwerkkomponenten über eine SNMPv3 Unterstützung verfügen. Nun gilt es, die alte SNMP Konfiguration zu deaktivieren/löschen und SNMPv3 auf den einzelnen Geräten zu aktivieren plus die Benutzer, Gruppen und Ansichten anzulegen.

7.2.6 Konfiguration der Managementsoftware

Zunächst die Managementsoftware installieren. Anschließend müssen die nun konfigurierten Geräte in die Managementsoftware integriert werden.

7.2.7 Test der Konfiguration

Abschließend ist es notwendig, die neu durchgeführte Konfiguration schrittweise zu überprüfen.
Dabei ist zunächst eine reine Funktionsprüfung zu empfehlen. Anschließend gilt es, Sicherheitslöcher ausfindig zu machen und zu beseitigen. Durch eine zuvor wohldurchdachte Struktur der Zugriffsberechtigungen kann dieser Punkt unter Umständen vereinfacht werden.

7.3 Beispiel einer Migration

7.3.1 Allgemein

Im Folgenden soll eine Migration von SNMPv1 auf SNMPv3 eines kleinen Netzwerks durchgeführt werden. Ausgegangen wird von einer bestehenden SNMPv1 Konfiguration, wie sie in vielen Unternehmen vorhanden sein könnte.

7.3.2 Ist-Bestandsaufnahme

Von folgenden Komponenten wird in diesem Szenario ausgegangen:

- Cisco Router C2600, IP Adresse 192.168.100.1
- Cisco Switch C2950, IP Adresse 192.168.100.2

- Netzwerkmanagementsoftware SNMPc Version 7.0.14a unter Windows XP SP2, IP Adresse 192.168.100.10
- Windows 2003 Server mit ServicePack 1, IP Adresse 192.168.100.100

Bestehende Konfiguration:
Auf allen Geräten ist SNMPv1 mit einer read und einer write community („private“/„public“) eingerichtet. Bisherige Sicherheitsmaßnahme war Lese- und Schreiboperationen nur von einer definierten IP Adresse (die des Managementsystems) zu erlauben.

7.3.3 Ziele definieren

Ziel ist es, alle Komponenten mit SNMPv3 zu verwalten. Wie bei der bestehenden SNMPv1 Konfiguration sollen zwei Zugriffsvarianten möglich sein (Leserecht, Lese- und Schreibrecht)

Zu diesem Zweck sollen zwei Benutzer angelegt werden:

1. Benutzer: nur Authentifizierung, nur Leserechte

Benutzername:	**readuser**
Authentifizierung:	**MD5**
Authentifizierung – Passwort:	**wxyz9876**

2. Benutzer: Authentifizierung + Verschlüsselung, Lese- und Schreibrechte

Benutzername:	**writeuser**
Authentifizierung:	**MD5**
Authentifizierung – Passwort:	**a1b2c3d4**
Verschlüsselung:	**DES**
Verschlüsselung – Passwort:	**e5f6g7h8**

7.3.4 Realisierbarkeit

Folgende Tabelle soll eine Übersicht über die technische Realisierbarkeit der Migration geben:

Tabelle 5: Migrationsbeispiel - SNMP Unterstützung

Gerät	SNMP Unterstützung derzeit für	Update notwendig	Erfüllt Anforderungen	Anmerkung
Microsoft Windows 2003 Server	v1	JA	NEIN	Softwareagent notwendig
Cisco Router	v1, v2, v3	NEIN	JA	Ok
Cisco Switch	v1, v2	JA	NEIN	IOS Upgrade notwendig

Prinzipiell ist die Nachrüstung für SNMPv3 Unterstützung bei allen Geräten möglich, jedoch ist kein Client verfügbar, der dem Windows 2003 Server eine VACM Unterstützung liefert. Aus diesem Grund wird entschieden, lediglich „Benutzer Zwei“ anzulegen.
Bei einer realen Migration könnte dieser Punkt ein „Kill-Kriterium“ sein, da die ursprünglich definierten Ziele (zwei verschiedene Benutzer mit unterschiedlichen Zugriffsrechten) somit nicht erreicht werden können.

7.3.5 Aktualisierung der Komponenten

Windows 2003 Server

Da Windows 2003 Server keine eigene SNMPv3 Unterstützung bietet, ist die Installation eines Software-Agents notwendig. Die Auswahl fiel auf MG-Soft SNMP Master Agent. MG-Soft hat freundlicherweise eine Testversion des Agents zur Verfügung gestellt (offiziell ist keine Testversion zu diesem Programm verfügbar). Zu beachten ist, dass das

Microsoft Windows SNMP Service installiert sein muss, um den MG-Soft SNMP Master Agent installieren zu können.

Cisco Router

Der Cisco Router besitzt bereits ein aktuelles SNMPv3-fähiges IOS. Ein Upgrade ist nicht notwendig.

Cisco Switch

Verfügt über eine nicht SNMPv3-fähige IOS Version. Ein Upgrade ist deshalb notwendig. Die aktuellste verfügbare Firmware mit SNMPv3 Unterstützung wird auf [INFOURL16] gefunden und installiert.

7.3.6 Konfiguration der Komponenten

Windows 2003 Server

Nach der Installation des SNMP Master Agents werden zunächst die standardmäßig aktivierten „SNMPv1 Security“ und „SNMPv2 Security“ Punkte deaktiviert (deselektieren von „Enabled“).
Anschließend wird „SNMPv3 Security“ aktiviert, bei Bedarf kann auch hier wiederum eine Beschränkung der SNMP Pakete auf die IP Adresse des Servers erfolgen [s. Abbildung 25: SNMPv3 Konfiguration 1].

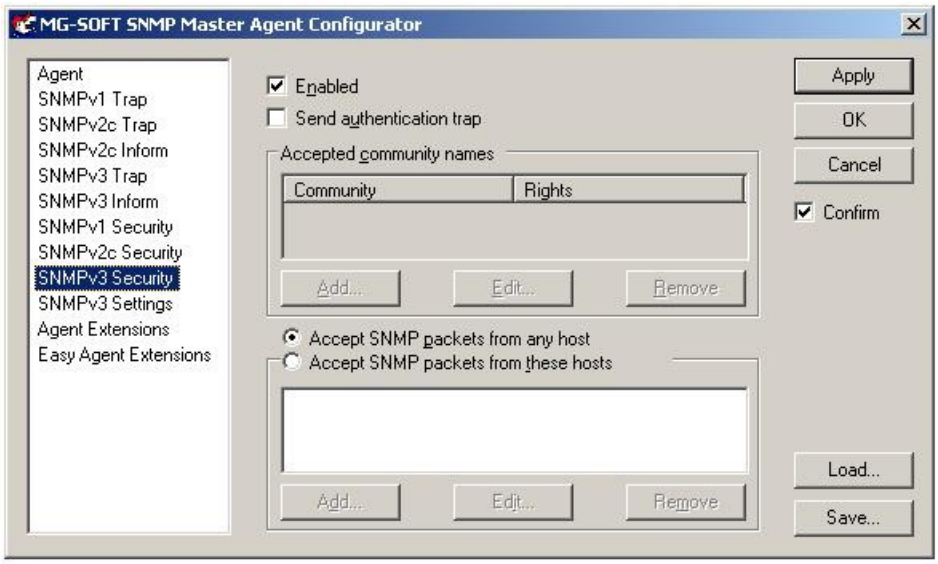

Abbildung 25: SNMPv3 Konfiguration 1

Danach werden die User angelegt. Da der MG-Soft SNMP Master Agent kein VACM unterstützt, können die Rechte bei einem erfolgreichen Zugriff über SNMPv3 nicht konfiguriert werden. Aus diesem Grund wird hier nur „Benutzer Zwei“ mit Lese- und Schreibrechten angelegt und die Authentifizierung und Verschlüsselung jeweils inklusive Passwörter konfiguriert.

[s. Abbildung 26: SNMPv3 Konfiguration 2]

Abbildung 26: SNMPv3 Konfiguration 2

Damit die Konfiguration übernommen wird, muss der „MG-SOFT SNMP Agent“ Dienst neu gestartet werden. Diese Konfiguration ist somit aktiv.

Cisco Router & Switch

Cisco bietet als einer der wenigen Hersteller die Möglichkeit, nicht nur Benutzername, Verschlüsselung und Authentifizierung für SNMPv3 zu verwenden (USM), sondern auch Lese- und Schreibzugriff mit Hilfe von Views und Gruppen einzuschränken (VACM).
D.h. die unterschiedlichen Rechte werden nicht wie bei SNMPv1 mit Communities sondern nun mit unterschiedlichen Gruppen definiert.
Für die Erstellung mehrere User mit unterschiedlichen Rechten auf ein Gerät sind folgende Schritte notwendig:

1. Eine Ansicht erstellen, gewünschte MIBs hinzufügen
2. Erste Gruppe erstellen und Lesezugriff auf eine View zu geben
3. Zweite Gruppe erstellen und Schreibzugriff auf eine View zu geben
4. User erstellen und je nach Bedarf in Gruppe eins oder zwei zuordnen

Bei Cisco gliedert sich die SNMPv3 Konfiguration in mehrere Schritte:

SNMPv3 für Polling aktivieren

1. Ansicht (View) erstellen, gewünschte MIBs hinzufügen
2. Gruppe erstellen und Rechte auf eine View vergeben
3. User anlegen, einer Gruppe zuordnen und Passwörter vergeben

SNMPv3 Traps aktivieren:

1. Ansicht und User müssen existieren
2. Traps aktivieren
3. Trap für entsprechendes Ziel anlegen, User angeben der für Authentifizierung verwendet wird

Die Konfiguration für dieses Beispiel sieht nun folgendermaßen aus:

```
#View anlegen, Mib2 hinzufügen
Router(config)#snmp-server view view1 mib-2 include

#Read-Only Gruppe anlegen
Router(config)#snmp-server group group-ro v3 priv read view1

#Gruppe mit Schreibzugriff anlegen
Router(config)#snmp-server group group-wr v3 priv write view1

#User 1 anlegen
Router(config)#snmp-server user readuser group-ro auth md5 wxyz9876

#User 2 anlegen
Router(config)#snmp-server user writeuser group-wr auth md5 a1b2c3d4 priv
des56 e5f6g7h8

#Traps aktivieren
Router(config)#snmp-server enable traps

#Trap einrichten
Router(config)#snmp-server host 192.168.0.x version 3 auth secureuser
```

Konfiguration der Managementsoftware

Nach Installation von CastleRock SNMPc, kann nun ein Autodiscovery durchgeführt werden. Dazu müssen die auf den Geräten konfigurierten UserProfiles der Managementsoftware bekannt gegeben werden. Optional können die Geräte auch manuell hinzugefügt werden.

Dabei lautet die Vorgehensweise:

- Geräte hinzufügen
- Benutzereinstellungen einrichten [s. Abbildung 27: SNMPv3 Konfiguration 3]
- Kommunikation überprüfen

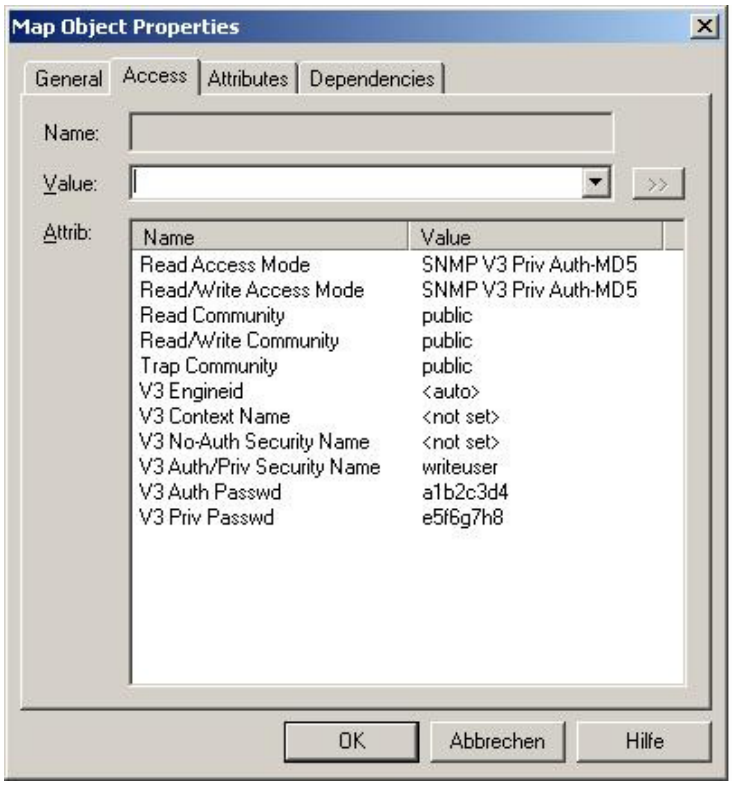

Abbildung 27: SNMPv3 Konfiguration 3

7.3.7 Test der Konfiguration

Nun gilt es, diese Konfiguration zu testen. Dabei ist zunächst eine prinzipielle Funktionsprüfung zu empfehlen. Diese umfasst folgende Punkte:

- Wurden alle konfigurierten Geräte im Managementsystem erfasst?
- Kann das Managementsystem auf die hinzugefügten Geräte zugreifen?
- Überprüfung, welche Operationen zulässig sind und welche nicht.

Dieser Punkt wird bei einer realen Migration sehr viel Zeit in Anspruch nehmen. Schlussendlich nützt aber die beste Verschlüsselung nichts, wenn sie durch Konfigurationsfehler umgangen werden kann.

8. Fazit

Die weite Verbreitung von SNMPv1 mit seinen praktisch nicht vorhandenen Sicherheitsmaßnahmen hat es notwendig gemacht, eine neue, sicherere Version zu spezifizieren. Der unmittelbare Nachfolger, SNMPv2, konnte sich aus Folgen der Instabilität des Standards aber nicht etablieren, zumal die gängigste SNMPv2-Subvariante wiederum keine Verbesserung der Sicherheit mit sich brachte.
Erst mit Version 3 ist SNMP „secure“ geworden. Aus sicherheitstechnischer Sicht, ist jedem Benutzer einer älteren Version ein Update auf SNMPv3 zu empfehlen, da die implementierten Sicherheitsmaßnahmen endlich dem Stand der Technik entsprechen. Zudem ist seine Architektur so flexibel, dass die bestehenden Sicherheitsprotokolle relativ leicht durch kommende, noch sicherere Verfahren ersetzt werden könnten.
Ein abermaliges Scheitern des Standards wie bei SNMPv2 dürfte zudem unwahrscheinlich sein, da die neueste Version technisch wesentlich ausgereifter scheint.
Aus all diesen Gründen darf das Protokoll SNMPv3 somit als zukunftssicher angesehen werden.

Trotz dieser technischen Ausgereiftheit, hält sich die Verbreitung von SNMPv3 in Grenzen: Nach eingehender Betrachtung der SNMPv3 Unterstützung von aktuellen Netzwerkgeräten diverser Hersteller, ist es für mittlere Unternehmen zwar durchaus möglich, auf die letzte Version von SNMP umzusteigen, einfach dürfte dies jedoch in den seltensten Fällen werden.

Ein großes Problem für Unternehmen, die mehr Sicherheit mit SNMPv3 erreichen wollen, könnte die Verwendung von Nicht-Standardhardware mit sich bringen. Obwohl bei der für diese Diplomarbeit durchgeführte Teststellung ausschließlich Standardkomponenten im Einsatz waren, war ein Firmwareupdate notwendig und auf definierte Ziele musste wegen mangelnder Verfügbarkeit eines SNMP-Agents für Windows mit VACM Unterstützung, verzichtet werden. Beim Einsatz von weniger weit verbreiteten Geräten bzw. von Geräten kleinerer Hersteller kann es deshalb durchaus möglich sein, dass eine SNMPv3 Unterstützung schlichtweg nicht vorhanden ist. In diesem Fall ist eine Koexistenz von SNMPv1 und SNMPv3 denkbar.

Während der Untersuchung von weit verbreiteten Netzwerkgeräten (z.B.: Router, Switches) auf SNMPv3 Unterstützung, wurde außerdem folgende Problematik festgestellt: Fast alle Geräte rühmen sich damit SNMPv3-fähig zu sein, aber nur wenige Fabrikanten machen in ihren Produktbeschreibungen genaue Angaben darüber, welche SNMPv3 Features von ihrer Hardware wirklich unterstützt werden. Oft ist von „SNMPv3 Verschlüsselung“ die Rede, dies lässt aber vermuten, dass lediglich das User Security Modell unterstützt wird, d.h. die Kommunikation kann zwar verschlüsselt und authentifiziert erfolgen, jedoch gibt es keine Möglichkeit der Zugriffskontrolle.

Das Pendant zu den Netzwerkgeräten, die Netzwerkmanagementsoftware, ist zwar prinzipiell ebenfalls mit SNMPv3 Unterstützung vorhanden, aber die erweiterten Funktionen werden oft per Modul von Fremdanbietern verwirklicht.

Ein weiterer Grund für die zurzeit geringe Verbreitung von SNMPv3, könnte zudem die komplexere Konfiguration die diese Version mit sich bringt, sein. Außerdem wird SNMP ohnehin in vielen Unternehmen zur reinen Überwachung eingesetzt, ohne Funktionen zur Steuerung des Netzwerkes. Die mangelnde Sicherheit der Urversion scheint den Betreibern solcher Netzwerke somit ausreichend zu sein.

Abschließend ist zu sagen, dass der SNMPv3 Standard technisch sehr ausgereift erscheint, ob dies allerdings genug ist, um sich jemals so stark wie sein Vorgänger SNMPv1 zu verbreiten, bleibt abzuwarten.

9. Abkürzungsverzeichnis

ASN.1	Abstract Syntax Notation Number One
CBC	Cipher Block Chaining
CIA	hier: Confidentiality, Integrity und Availability
CMIP	Common Management Information Protocol
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
HEMS	High-Level Entity Management System
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
MIB	Management Information Base
NMS	Netzwerkmanagementsystem
OID	Object Identifier
OSI	Open Systems Interconnection reference model
PDU	Protocol Data Unit
RFC	Request For Comments
SGMP	Simle Gateway Monitoring Protocol
SMFA	Specific Management Functional Areas
SMI	Structure of Management Information
SNMP	Simple Network Management Protocol
SOHO	Small Office Small Home
TCP/IP	Transmission Control Protocol/Internet Protocol
UDP	User Datagram Protocol
USM	User-Based Security Model
VACM	View-based Access Control Model
WLAN	Wireless Local Area Network

10. Quellenverzeichnis

10.1 Bücher

[Tanenbaum, 2003] Computer Networks, Fourth Edition, 2003
Andrew S. Tanenbaum
ISBN: 0130384887

[Stallings, 1999] SNMP, SNMPv2, SNMPv3, and RMON 1 and 2, Third Edition, 1999
William Stallings
ISBN: 0201485346

[Ghetie, 1997] Networks and Systems Management, 1997
Iosif G. Ghetie
ISBN: 0792398793

[Douglas, 2005] Essential SNMP, 2nd Edition, 2005
Douglas Mauro, Kevin Schmidt
ISBN: 0596008406

[Zechmeister, 2005] Diplomarbeit: Netzwerkmanagement über SNMP
Zechmeister Andreas, FH St. Pölten

10.2 Spezifikationen

[ISO 7498-4] ISO Norm 7498-4, Management Framework, 1989
http://standards.iso.org/ittf/PubliclyAvailableStandards/s014258_ISO_IEC_7498-4_1989(E).zip

[RFC 3411] An Architecture for Describing Simple Network Management Protocol
http://www.isi.edu/in-notes/rfc3411.txt

[RFC 3412] RFC 3412: Message Processing and Dispatching for the SNMP, 2002
D. Harrington
http://www.isi.edu/in-notes/rfc3412.txt

[RFC 3414] RFC 3414: User-based Security Model (USM) for SNMPv3, 2002
U. Blumenthal
http://www.isi.edu/in-notes/rfc3414.txt

[RFC 3415] RFC 3415: View-based Access Control Model (VACM), 2002
B. Wijnen
http://www.isi.edu/in-notes/rfc3415.txt

[RFC 1321] The MD5 Message Digest Algorithm, 1992
R. Rivest
http://www.ietf.org/rfc/rfc1321.txt

10.3 Artikel und Beitrage

[URL1] TCP/IP Internet Standard Management, 2005
http://www.tcpipguide.com/free/t_TCPIPInternetStandardManagementFrameworkandSNMPSta.htm

[URL2] Wikipedia, die freie Enzyklopädie
http://de.wikipedia.org/wiki/Proxy

[URL3] Introduction to ASN.1, 2005
http://asn1.elibel.tm.fr/en/introduction/index.htm

[URL4] On-Line MIBs
http://www.netdiscover.org/MibDoc/Standards(OnLineMIB)/index.html

[URL5] SNMPv3: A Security Enhancement for SNMP, 1998
William Stallings
http://www.comsoc.org/livepubs/surveys/public/4q98issue/stallings.html

[URL6] SNMPv3 Request For Comments (RFC)
http://www.snmplink.org/SNMPv3.html

[URL7] Secure Hash Standard, 1997
http://www.itl.nist.gov/fipspubs/fip180-1.htm

[URL8] SNMPv3 Implementations
http://www.ibr.cs.tu-bs.de/projects/snmpv3

10.4 Produktinformationen

[INFOURL1] HP OpenView Network Node Manager
http://www.openview.hp.com

[INFOURL2] SNMP Security Pack
http://www.snmp.com/products/snmpsecpack.html

[INFOURL3] IBM Tivoli NetView
http://www-306.ibm.com/software/tivoli/products/netview/

[INFOURL4] Fragen zu IBM Tivoli
http://www.tivoli-ug.org/docs/TECandNetviewWebcast%20_QandA_9-22-05.pdf

[INFOURL5] CastleRock SNMPc
http://www.castlerock.com

[INFOURL6] Castlerock SNMPc Datasheet
http://www.castlerock.com/pdf/SNMPc7-datasheet-hr.pdf

[INFOURL7] CiscoView
http://www.cisco.com/en/US/products/sw/cscowork/ps4565/index.html

[INFOURL8] CiscoView 6.1.2 UserGuide
http://www.cisco.com/application/pdf/en/us/guest/products/ps5948/c1629/ccmigration_09186a008056c020.pdf

[INFOURL9] Whats Up Gold
http://www.ipswitch.com/products/whatsup/professional/index.asp

[INFOURL10] Whats Up Gold Features
http://www.ipswitch.com/products/whatsup/professional/features.asp

[INFOURL11] Solarwinds
http://www.solarwinds.net/

[INFOURL12] OpenNMS
http://www.opennms.org

[INFOURL13] OpenNMS SNMPv3 Protocol Configuration
http://www.opennms.org/index.php/SNMPv3_protocol_configuration

[INFOURL14] MG-Soft SNMP Master Agent
http://www.mg-soft.si/agent.html

[INFOURL15] NET-SNMP Agent
http://net-snmp.sourceforge.net/

[INFOURL16] Cisco Feature Navigator
http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

11. Abbildungsverzeichnis

Appendix

CD-ROM

Inhalt:

- Diplomarbeit
- Literaturangaben

Hier sollte die CD kleben!