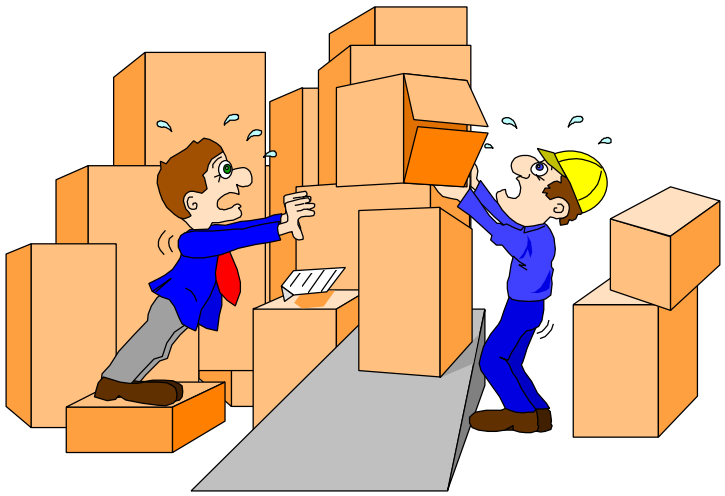
r u h r - u n i v e r s i t ä t b o c h u m

*Lehrstuhl für Datenverarbeitung*
Prof. Dr.-Ing. Dr.E.h. Wolfgang Weber

# Verteilte Systeme

## SNMP: Aufbau, Funktion, Sicherheit

Seminar Datenverarbeitung WS 1999/2000



Referent: cand.-Ing. Marko Vogel
Betreuer: Dipl.-Ing. Thomas Droste

# Inhalt

# 1 Netzwerkmanagement

## 1.1 Motivation

Mittlerweile gewinnt die strategische Ressource „Information“ für Unternehmen eine immer größere Bedeutung. Dies führt dazu, daß Rechnernetze nicht mehr nur ein unterstützendes Element in einem Unternehmen sind, sondern immer häufiger eine Schlüsselstellung einnehmen.
Weiterhin läßt sich feststellen, daß die Anzahl der vernetzten Rechner in den letzten Jahren sprunghaft angestiegen ist und dieser Trend sich weiter fortsetzt. Zusätzlich wächst die Komplexität und Funktionalität der einzelnen Komponenten entsprechend der Leistungssteigerung der zugrundeliegenden Hardware.
Ebenso müssen die Anforderungen, die an ein Netzwerk gestellt werden, mit Hilfe geeigneter Managementsysteme erfüllt werden.
Zu diesen Anforderungen gehören:

- Sicherstellung der Funktionsbereitschaft des Netzwerkes
  - Die Serviceleistung (Verfügbarkeit, Antwortzeit, etc.) soll trotz technologischer Änderungen und hohen Wachstumsraten aufrechterhalten werden.
  - Die Dienstgüte (z.B. Antwortzeit) ist durch Überwachung der Komponenten sicherzustellen.
  - Fehler und Engpässe sollen vorbeugend erkannt und behoben werden.
- automatische oder halbautomatische Reaktion auf Betriebsstörungen
  - Konfigurationsänderung erfolgen im Fehlerfall in Echtzeit.
  - Redundante Komponenten werden im Fehlerfall aktiviert.
- Dynamische Reaktion auf Änderungen im Netz und der Umgebung
  - Auf Änderungen bezüglich Anwendungen, Teilnehmern, Komponenten, Diensten oder Gebühren wird geeignet reagiert.
  - Es erfolgt eine dynamische Anpassung der Übertragungsbandbreiten.
- Beherrschbarkeit des Netzes
  - Netzrelevante Informationen werden geordnet und komprimiert dargestellt.
  - Es erfolgt der Aufbau und die Pflege einer Datenbasis für Konfigurations-, Leistungs- und Abrechnungsdaten.
  - Die Steuerung erfolgt zentralisiert mit möglichst dezentraler Realisierung der Funktionen.
- Verbesserung der Arbeitsbedingungen der Administratoren
  - Die Benutzungsoberflächen von Werkzeugen werden verbessert und vereinheitlicht.

  - Die Möglichkeiten zur schrittweisen Automatisierung von Managementaufgaben wird eingerichtet.
  - Es erfolgt eine Integration der Werkzeuge in die Arbeitsabläufe.
- Reduktion der Kosten für den Betrieb der Netzinfrastruktur

Aus diesen Problemen und Anforderungen ergibt sich die Notwendigkeit eines rechnergestützten Managements der meist heterogenen Netze in den Organisationen.
Das Netzwerkmanagement kann als ein organisatorisches Problem angesehen werden, welches durch Menschen (Netzwerkadministratoren) mit Hilfe von speziellen Werkzeugen (Hardware- und Softwarekomponenten) gelöst werden soll. Die Werkzeuge und deren technologische Grundlagen sind jedoch lediglich Hilfsmittel zum erfolgreichen Netzwerkmanagement.

## 1.2 Teilbereiche

Das Netzwerkmanagement läßt sich in 5 Teilbereiche, bzw. Funktionsbereiche, eingruppieren:

- Fehlermanagement (fault management)
  Zum Fehlermanagement gehören Probleme wie Fehlererkennung, Fehlerisolation und Fehlerbehebung.
- Konfigurationsmanagement (configuration management)
  Die Erzeugung und Verwaltung von Konfigurationsinformationen sowie die Namensverwaltung fallen beispielsweise unter das Konfigurationsmanagement.
- Abrechnungsmanagement (account management)
  Das Erfassen von Verbrauchsdaten und Führen von Verbrauchsstatistiken sind Beispiele für das Abrechnungsmanagement.
- Leistungsmanagement (performance management)
  Die Ermittlung der Systemleistung und die Sammlung von statistischen Daten werden dem Leistungsmanagement zugeordnet.
- Sicherheitsmanagement (security management)
  Die Erzeugung und Kontrolle von Sicherheitsdiensten oder das Melden und die Analyse von sicherheitsrelevanten Ereignissen fallen unter das Sicherheitsmanagement.

Alle Bereiche sind nicht unabhängig voneinander, wodurch bei z.B. Maßnahmen zur Leistungssteigerung oft auch Änderungen der Konfiguration notwendig sind.
Weiterhin lassen sich oftmals Grundfunktionen, wie z.B. die Überwachung eines Zählers auf Grenzwerte, in verschiedenen Funktionsbereichen anwenden.
Das Simple Network Management Protocol (SNMP) ist allerdings nicht für alle obigen Teilbereiche geeignet. So ist insbesondere im Bereich Fehlermanagement SNMP

wenig hilfreich. Fehlerhafte Steckverbindungen oder Fehler aufgrund falscher Kabelführung können nicht mit Hilfe von SNMP erkannt werden.

# 2 Netzwerkmanagement-Systeme

## 2.1 Prinzip

Die Abbildung 2-1 zeigt den prinzipiellen Aufbau von Netzwerkmanagement-Systemen.

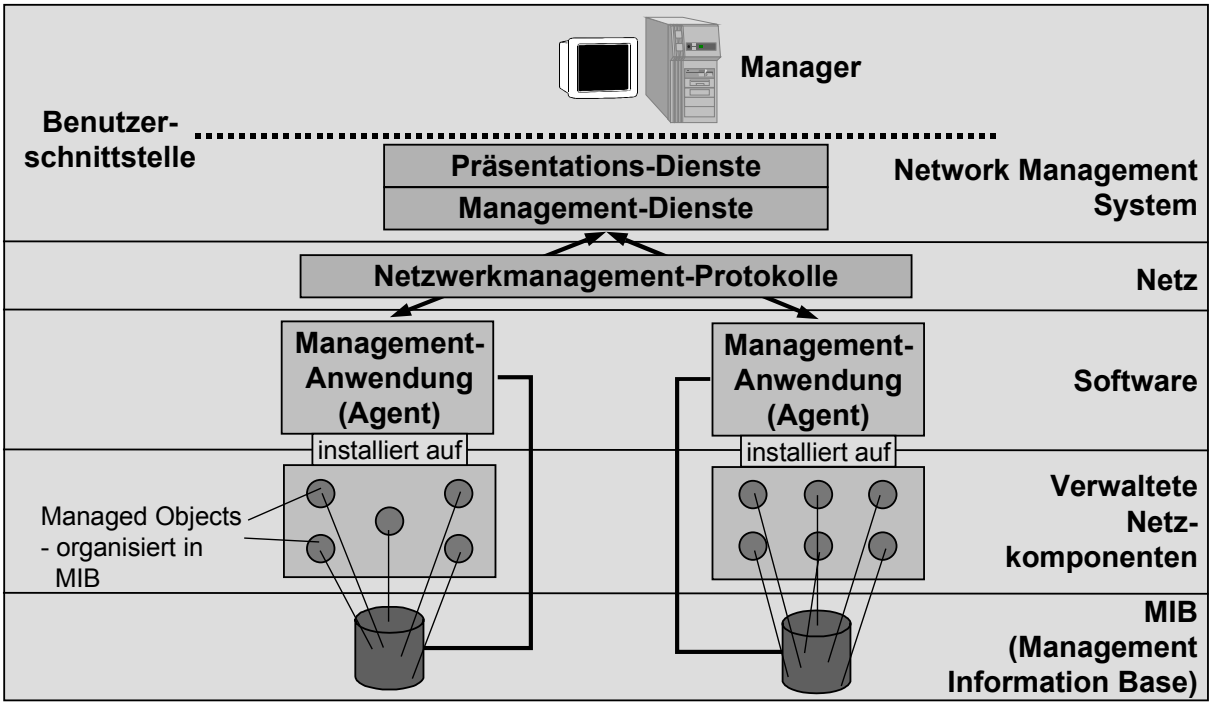



***Abbildung 2-1: Prinzipieller Aufbau eines Netzwerkmanagement-Systems***

Die wesentlichen Komponenten sind das Network Management System (NMS), der Agent und die Management Information Base (MIB).
Der Administrator verwaltet mit Hilfe des Network Management Systems das Netzwerk. Um die Informationen von den verwalteten Ressourcen zu bekommen und sie aufbereitet dem Administrator zur Verfügung zu stellen, benötigt das Network Management System ein Netzwerkprotokoll mit dessen Hilfe es auf die Agenten zugreift, die auf den verwalteten Ressourcen installiert sind. Eines dieser Netzwerkprotokolle ist das Simple Network Management Protocol (SNMP). Darüber hinaus existieren weitere Netzwerkmanagementprotokolle, die ebenfalls genutzt werden könnten. Diese besitzen allerdings eigene Manager und Agenten.
Der Agent ist eine für die jeweilige Ressource entwickelte Anwendung, die auf der Ressource installiert ist. Er verwaltet die Informationen und greift konfigurierend auf die Ressource zu.

Die Informationen der Ressource (Managed Objects) werden in der Management Information Base (MIB) verwaltet.
Die drei wesentlichen Komponeneten, das Network Management System, der Agent und die Management Information Base werden im folgenden Kapitel genauer betrachtet.
Es ist wichtig zwischen dem Systemadministrator, oft als Manager bezeichnet und dem Network Management System, das ebenfalls oftmals als Manager bezeichnet wird, zu unterscheiden und die Namensbezeichnung eindeutig zu halten.

# 3 SNMPv1

## 3.1 Historischer Überblick

Das Simple Network Management Protocol ist in seiner ersten Version (SNMPv1) im Jahre 1988 aus dem Simple Gateway Monitoring Protocol (SGMP) und dem High-Level Entity Management System (HEMS) entstanden (vgl. Abbildung 3-1). Dieser Vorschlag (RFC 1157) bekam 1990 den Status eines Standards und war somit festgeschrieben. 1991 folgte die Management Information Base II als Standard (RFC 1213), welche die wichtigsten Informationen verbindlich festschreibt. Beide zusammen entwickelten sich schnell zum Quasi-Standard auf dem Markt der Managementanwendungen für Computernetzwerke.
In den Jahren 1993 und 1996 erfolgten zwei Versuche eine neue Version des SNMP-Protokolls herauszubringen. Da die neuen Versionen (SNMPv2p und SNMPv2c) jedoch partiell inkompatibel zu SNMPv1 waren und die erste Version weit verbreitet war, fanden die neueren Versionen keinen Zuspruch auf dem Markt. Es sind nur wenige Implementationen entwickelt worden. Aus heutiger Sicht kann SNMPv2 daher als gescheitert betrachtet werden.
Im Jahre 1998 wurde der erste Vorschlag zu SNMPv3 herausgebracht. Der Vorschlag umfaßte u.a. ein neues Architekturmodell, ein Modell zur Zugriffskontrolle und ein Sicherheitsmodell. Dieser Vorschlag findet bei den Herstellern eine gute Unterstützung.

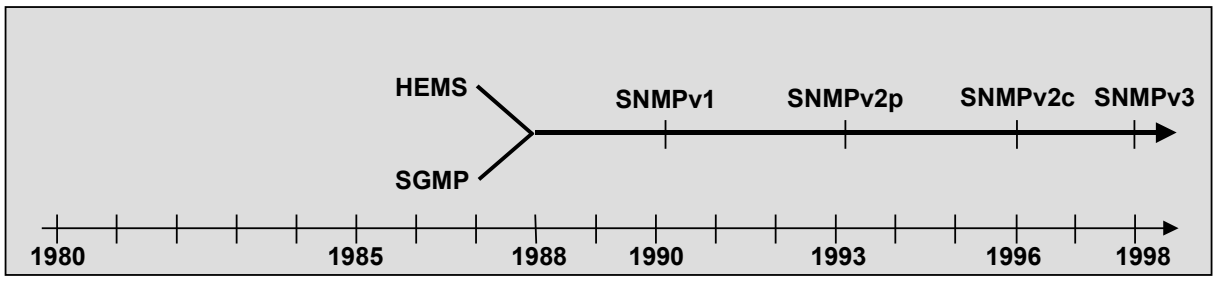



*Abbildung 3-1: Historische Entwicklung*

## 3.2 Protokollübersicht

Das Simple Network Management Protocol ist auf Schicht sieben des ISO[1]/OSI[2]-Modells zu finden (vgl. Abbildung 3-2). Es setzt im Regelfall auf dem User Datagram Protocol (UDP) auf (vgl. RFC 1157). Diese Struktur ist nicht zwingend vorgeschrieben, genauso gut kann das SNMP auch auf z.B. dem Transmission Control Protocol (TCP) oder auf dem IPX (Internet Packet Exchange) von Novell aufsetzen.

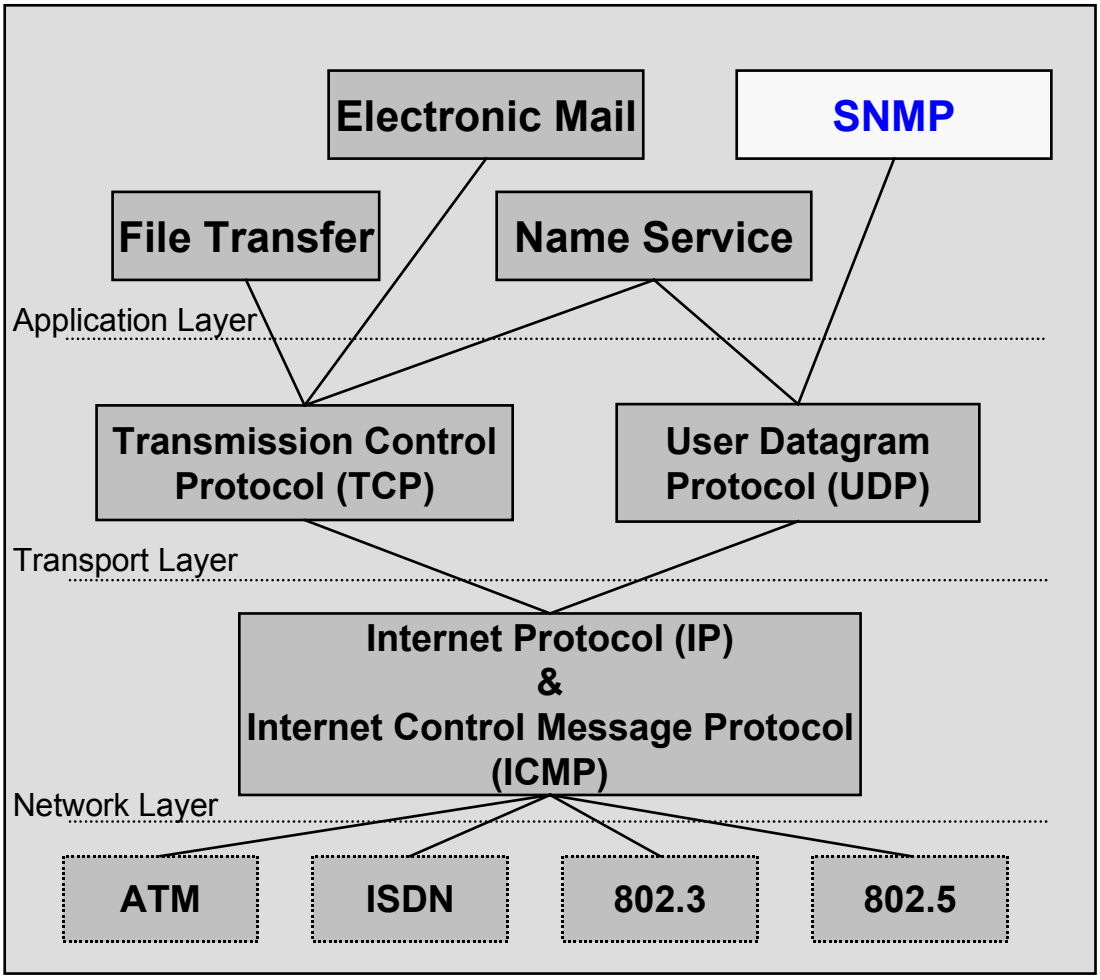



***Abbildung 3-2: vereinfachtes ISO/OSI-Modell***

Das Simple Network Management Protocol hat sich als Quasi-Standard durchgesetzt, ist aber nicht das einzige Managementprotokoll.
Ein weiteres Protokoll ist das Common Management Information Protocol (CMIP). Die Entwickler von CMIP versuchten, bekanntgewordene Probleme beim SNMP zu beheben und entwickelten dadurch ein ausgereifteres Protokoll. Es ist jedoch umfang-

[1] ISO – International Standard Organisation

[2] OSI – Open System Interconnection

reich und teilweise umständlich zu handhaben und stellt hohe Anforderungen an die Ausstattung des Netzwerkes. Das CMIP-Protokoll hat sich auf dem Markt nicht durchgesetzt.
Einfache Managementfunktionalitäten lassen sich auch mittels des Internet Control Message Protocol (ICMP) realisieren. So kann z.B. mit Hilfe des Befehls „ping“, der ICMP-Nachrichten nutzt, überprüft werden, ob ein Rechner über das Netz erreichbar ist.

## 3.3 Arbeitsmodell

Das Arbeitsmodell des Simple Network Management Protocol folgt dem bereits vorgestellten Prinzip von Netzwerkmanagement-Systemen (vgl. Kapitel 2).
Das Modell besteht aus drei wichtigen Konstrukten (vgl. Abbildung 3-3):

- einem Host, der als Manager auftritt (Network Management System)
- einem oder mehreren Agenten, die auf der verwalteten Ressource Informationen bereitstellen und konfigurierend eingreifen
- der Management Information Base (MIB), einer Datenbank mit Angaben zu den verwalteten Objekten (Managed Objects)

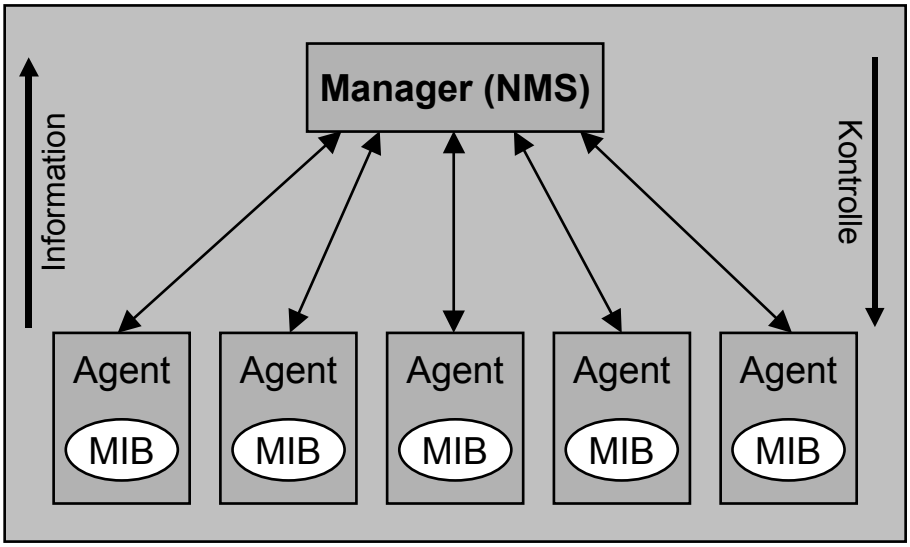



***Abbildung 3-3: Das Arbeitsmodell von SNMP***

Es handelt sich um ein streng zentralisiertes Modell, in dem der Manager (NMS) die ganze Funktionalität und Verantwortung trägt. Er übt die Kontrolle über alle Agenten aus und holt sich die Informationen die er benötigt, von den Agenten der jeweiligen Ressource.

### 3.3.1 Das Network Management System

Das Network Management System (NMS) ist in der Regel auf einem gut ausgestatteten Hostrechner installiert. Dieser stellt genügend Arbeitsspeicher, Plattenkapazität und Grafikaustattung zur Verfügung, um die umfangreichen Daten auszuwerten bzw. zu visualisieren. So erhält der Administrator z.B. statistische Ergebnisse, wie Datendurchsatz, Fehlerhäufigkeit oder Antwortzeiten in adäquater Form präsentiert.
Das Network Management System führt also die von den Agenten gesammelten Informationen zusammen und wertet diese aus.
Es fragt in regelmäßigen Intervallen die Informationen der Agenten ab. Dieser Vorgang wird Polling genannt. Wird durch einen Agenten eine Ausnahmesituation angezeigt, kann die Pollingstrategie angepaßt werden (trap-directed polling).
Weiterhin initiiert das Network Management System Managementoperationen zur Manipulation der verwalteten Objekte (Managed Objects).

### 3.3.2 Der Agent

Der Agent ist die auf der verwalteten Ressource laufende Anwendung. Verwaltete Ressourcen können z.B. Hosts, Kommunikations- und Druckserver, Drucker, Router, Bridges oder Hubs sein.
Er nimmt die Anfragen des Managers (NMS) entgegen, bearbeitet sie und sendet entsprechende Antworten an den Manager zurück. Der Agent realisiert die Managed Objects durch Zugriff auf das reale Betriebsmittel.
Weil sie die Betriebscharakteristik der jeweiligen Ressource nicht nachteilig beeinflussen sollen, werden sie meist auf geringen Speicher- und Rechenleistungsverbrauch hin optimiert. Dies ist ein Grund für das Wort „Simple“ im Begriff Simple Network Management Protocol.
Eine weitere Form der Agenten stellen die sogenannten Proxy-Agenten dar. Sie ermöglichen das Verwalten von Ressourcen, die nicht das Simple Network Management Protocol unterstützen.

### 3.3.3 Die Management Information Base

Die Kontrolle, Koordination und Überwachung der Betriebsmittel erfolgt durch die Manipulation der Managed Objects (MO). Sie bilden die abstrakte Repräsentation der realen Ressource. Durch Attribute wird der Zustand der Managed Objects beschrieben. Der Zugriff auf die Managed Objects wird durch definierte Operationen ermöglicht, z.B. durch Get oder Set-Operationen analog zu bekannten Programmiersprachen. Das festgelegte Verhalten der Managed Objects bestimmt die Interaktion mit dem Betriebsmittel. Im Regelfall handelt es sich um einfache Variablen im Gegensatz zu Objekten aus der objektorientierten Programmierung.

Weiterhin können Managed Objects Meldungen generieren (Traps), die beim Eintreten vordefinierter Situationen an den Manager geschickt werden.
Um die Managed Objects eindeutig identifizieren zu können, besitzt jedes Managed Object einen eindeutigen Namen, den Object Identifier (OID). Konkrete Ausprägungen eines Objekttypes werden durch einen Instance Identifier eindeutig benannt. Durch das Anhängen des Instance Identifiers an den Object Identifier ergibt sich eine eindeutige Bezeichnung einer Instanz eines Objektes. Einfache Variablen haben grundsätzlich nur eine Instanz, wobei der Instance Identifier den Wert Null erhält. Für nicht-skalare Objekte, wie z.B. Tabellen, werden die Instance Identifier aus dem „Schlüssel" der Tabelle abgeleitet. So kann beispielweise der erste Eintrag in der ersten Spalte den Instance Identifier 1.1 erhalten, der zweite Eintrag in der ersten Spalte den Instance Identifier 1.2 usw. Der Zusammenhang zwischen den Managed Objects und der Management Information Base kann durch die folgende Definition beschrieben werden:

> Die Menge aller Managed Objects eines Systems bildet die Management Information Base des Systems. (ISO 7498-4).

Bei der Management Information Base (MIB) handelt es sich um eine Datenbank mit baumartiger Struktur (vgl. Abbildung 3-4). Sämtliche Knoten einer Ebene werden durch eine Nummer eindeutig identifiziert. Der Object Identifier (OID) besteht aus einer Nummernfolge, die sich durch den Pfad von der Wurzel der MIB zu einem Knoten ergibt.
Die wichtigsten Object Identifier sind in der MIB-II festgelegt und dürfen nicht selbständig verändert werden.
Als Beispiel ist in Abbildung 3-4 im Zweig IP (*ip*) innerhalb der MIB-II (*mib-2*) die Variable *IPDefaultTTL* herausgegriffen worden. Ihr Object Identifier ergibt sich gemäß der obigen Regel zu „1.3.6.1.2.1.4.2". Da es sich um eine einfache Variable handelt, folgt noch ein Instance Identifier „Null", so daß sich der eindeutige Gesamtname zu „1.3.6.1.2.1.4.2.0" ergibt. Die angegebenen Klartextnamen helfen nur dem Nutzer sich zurechtzufinden und haben für das Managementsystem keine Bedeutung, da es nur auf den Object Identifiern operiert.
Firmeneigene MIBs, die z.B. zusätzliche Variablen oder Funktionen anbieten die nicht innerhalb der MIB-II zu finden sind, können in einem eigenen Knoten *enterprises* untergebracht werden. Jede Firma muß einen eigenen Knoten beantragen, innerhalb dessen dann die eigenen MIBs untergebracht werden können.

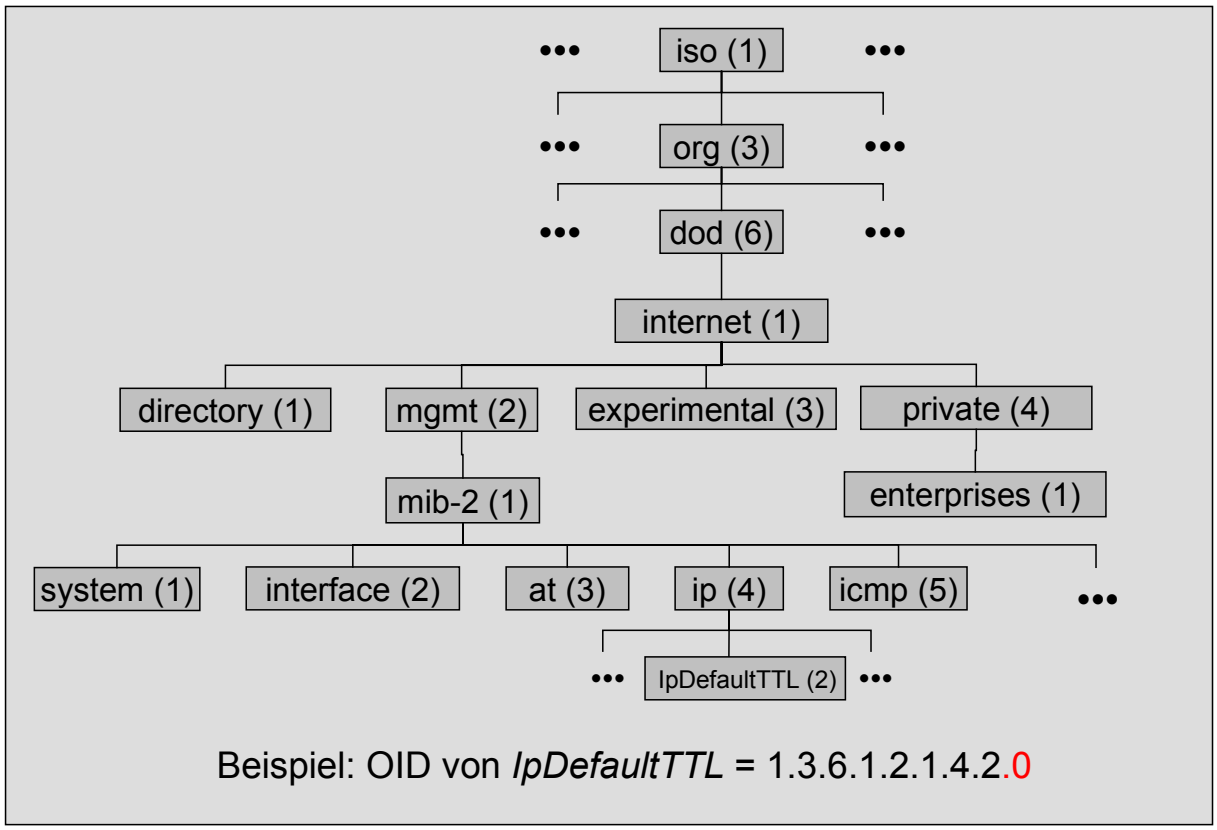



***Abbildung 3-4: Auszug aus der Management Information Base II***

Ein weiterer Begriff im Zusammenhang mit der Management Information Base ist der Begriff der Structure of Management Information (SMI). Die Structure of Management Information beschreibt den Aufbau der Management Information Base.
Sie beschreibt, z.B. was unterhalb des Internetknotens (1.3.6.1.) für weitere Knoten zu finden sind, welche Bedeutung er hat und wer für die Vergabe von weiteren Knotennamen verantwortlich ist. So legt die Structure of Management Information fest, daß innerhalb des oben bereits erwähnten Enterprises-Zweig Firmen eigene Knoten von der Internet Assigned Numbers Authority (IANA) erhalten und dort ihre eigenen MIBs anlegen dürfen.
Weiterhin wird mit Hilfe der Structure of Management Information festgelegt, daß Datentypen nur aus den Grunddatentypen Integer, Octet String, Object Identifier oder Null zusammengesetzt werden dürfen. Ein Datentyp *Counter* wird definiert als nichtnegativer Integer-Wert, der monoton heraufgezählt wird und bei Überschreiten seines Maximalwertes wieder bei Null beginnt. Der Maximalwert ist mit $2^{32} - 1$ angegeben.
Als Beschreibungssprache für die Structure of Management Information dient die Abstract Syntax Notation 1 (ASN.1). Diese spezifiziert Pakete und verwaltete Objekte, die nach ASN.1 aus einer Reihe von zu verwaltenden Eigenschaften bestehen.

## 3.4 Funktionen

Das Simple Network Management Protocol stellt folgende vier Befehle zur Verfügung, die es erlauben auf der Management Information Base zu operieren:

- *Get*
- *GetNext*
- *Set*
- *Trap*

Der *Get*-Befehl dient zum Lesen einer oder mehrerer Objektinstanzen.
Der *GetNext*-Befehl erlaubt das Lesen der nächsten Objektinstanz aus einer Liste/Tabelle der Management Information Base des Agenten. Weiterhin kann mit Hilfe aufeinanderfolgender *GetNext*-Operationen eine Management Information Base ohne Kenntnis der Struktur durchlaufen werden.
Der *Set*-Befehl schreibt Werte in eine oder mehrere Objektinstanzen. Zusätzlich dient er zum Erzeugen neuer Objektinstanzen, wobei nicht geregelt ist, wie dieser Vorgang stattzufinden hat. Aus sicherheitstechnischen Gründen (vgl. Kapitel 3.5) wird jedoch bei einigen Implementationen von SNMPv1 der Befehl Set nicht benutzt. Dadurch wird das Simple Network Management Protocol allerdings zu einem reinen Überwachungsinstrument.
Mit Hilfe des *Trap*-Befehls informiert ein Agent sein Network Management System über ein eingetretenes Ereignis, wie z.B. das Wiederhochfahren der Ressource nach einem Stromausfall. Der Empfang des *Trap*-Befehles wird vom Network Management System nicht bestätigt. Normalerweise können Agenten konfiguriert werden, ob und wohin Traps versendet werden. Allerdings gibt es in SNMPv1 kein Standardverfahren zur Konfiguration von Agenten.
Weitere Befehle sind bewußt nicht eingeführt worden, um das Protokoll einfach zu halten. Eine Möglichkeit weitere Befehle zu realisieren, kann durch definierte Variablen ersetzt werden. So kann z.B. „Gerät abschalten“ als Variable definiert sein, deren Wert die Zeit in Sekunden angibt nach der das Gerät abgeschaltet wird. Durch Setzen der Variableninstanz auf den Wert zehn würde sich das Gerät nach zehn Sekunden abschalten. Aufgrund der Sicherheitsproblematik bei SNMPv1 könnte damit ggf. Unbefugten weitreichende Möglichkeiten zur Manipulation der Netzressourcen gegeben werden.
Die Abbildung 3-5 zeigt das Schema des Nachrichtenaustausches der vier Grundbefehle. Der Manager bzw. der Agent kann in eine *Application Entity* und eine *Protocol Entity* unterteilt werden. Die *Application Entities* sind die Einheiten, die mit Hilfe des SNMP kommunizieren. Unterstützt werden sie durch die *Protocol Entities*, welche das eigentliche SNMP implementieren. Die *Protocol Entity* setzt das Nach-

richtenpaket des Managers zusammen bzw. nimmt es auf den Agenten auseinander, um die eigentlichen Informationen, wie z.B. die angefragte Objektinstanz, auszulesen.

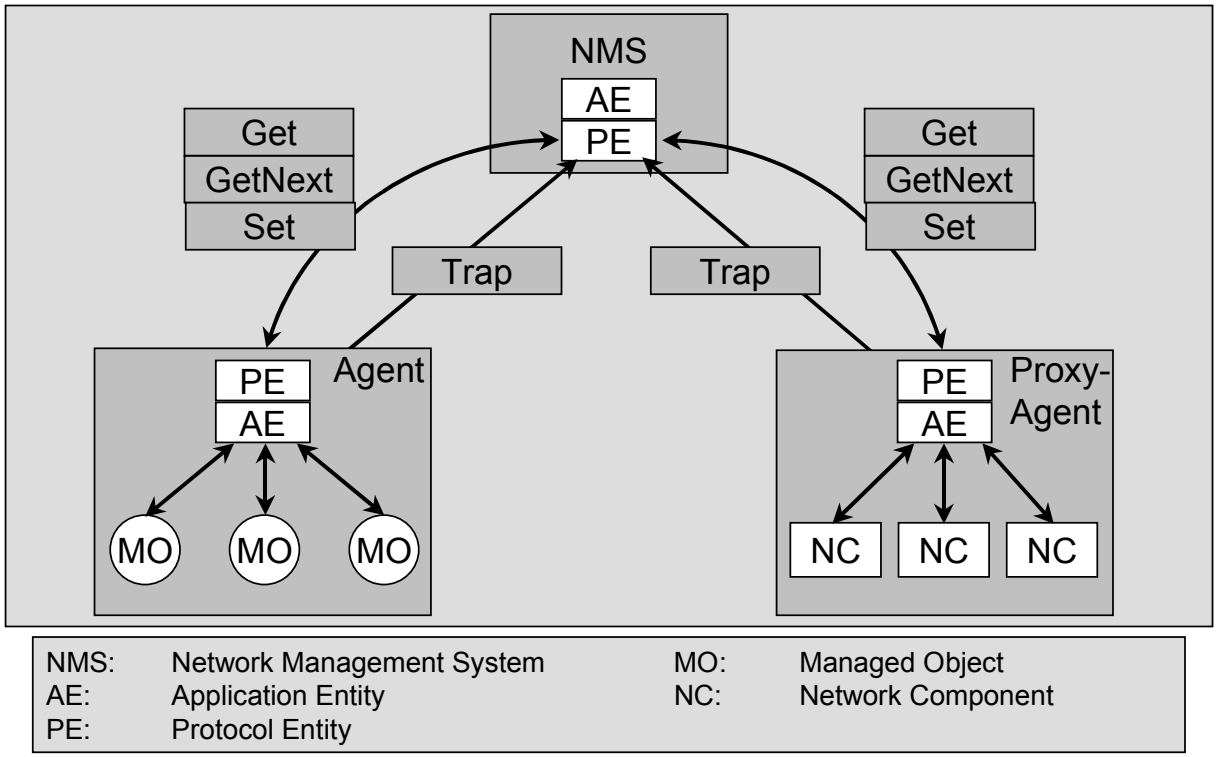



***Abbildung 3-5: Schema des Nachrichtenaustausches***

Für eine Anfrage schickt das Network Management System einen *Get*-, *GetNext*- oder *Set*-Befehl an den Agenten oder Proxy-Agenten. Je nach Befehl arbeitet der Agent diesen ab und schickt eine Antwort an das Network Management System zurück.
Alternativ sendet der Agent selbständig eine Benachrichtigung (*Trap*-Befehl) an das Network Management System, wenn ein besonderes Ereignis eingetreten ist.

## 3.5 Nachrichtenformate

Das SNMPv1 unterscheidet zwei Nachrichtenformate: ein Format für den *Get*-, *GetNext*- und *Set*-Befehl bzw. die Antwort auf einen dieser drei Befehle (vgl. Abbildung 3-6) und ein Format zur Übersendung eines *Trap*-Befehles (vgl. Abbildung 3-7).
Wie bei den meisten Protokollen bestehen die Nachrichten auch bei SNMPv1 aus einem Kopf und einem Datenteil (PDU[1]).
Im Kopf stehen eine *Versions*-Nummer und der sogenannte *Community* Name. Dieser bewirkt, daß Geräte, die diesen Namen nicht kennen, von der Kommunikation mit dem Network Management System ausgeschlossen werden. Außerdem definiert er den

[1] PDU – Protocol Data Unit

Bereich, in dem ein Network Management System das Management übernimmt. Der *Community* Name ist auch der einzige Schutz vor unberechtigten Zugriffen. Nach Überprüfung der Sender- und Empfängeradresse sowie des *Community* Namens auf Korrektheit wird der Befehl ausgeführt. Hier ist der Angriffspunkt für unberechtigte Zugriffe auf das System, da es relativ leicht ist an die Sender- und Empfängeradressen zu gelangen und der Community Name ebenfalls unverschlüsselt übertragen wird.

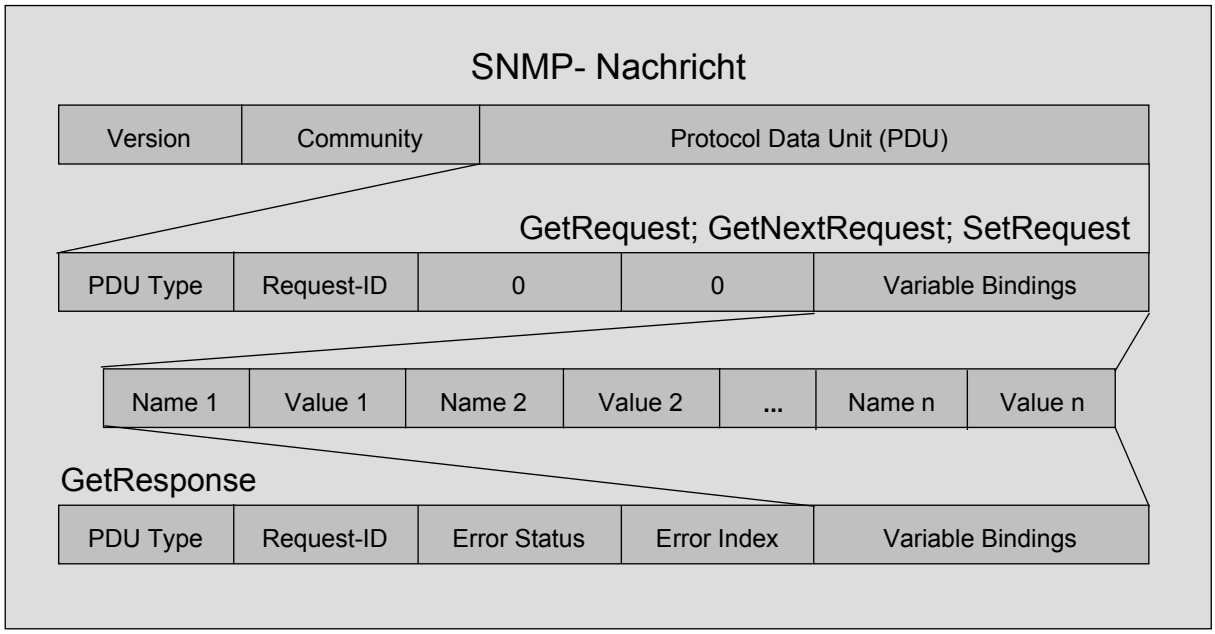



***Abbildung 3-6: Nachrichtenformat des Get-, GetNext- und Set-Befehles***

Der Datenteil unterteilt sich für das erste Nachrichtenformat wie folgt weiter:

- *PDU Type*
  Der *PDU Type* gibt den Typ des Befehls an, der übermittelt wird.
- *Request-ID*
  Die *Request-ID* ist eine ganze Zahl mit der das eindeutige Zuordnen von Anforderungen und Antworten möglich ist.
- *Error Status*
  Der *Error Status* informiert über etwaige Fehler und ihre Ursachen.
- *Error Index*
  Der *Error Index* ordnet den Fehler einer bestimmten Variablen zu.
- *Variable Bindings*
  *Variable Bindings* dient dazu, eine Zuordnung zwischen einer bestimmten Variablen und dem zugehörigen Wert herzustellen. Bei den Befehlen *Get* und *GetNext* wird der hier enthaltene Wert ignoriert.

Das gezeigte Format wird auch für die Antworten des Agenten benutzt. Bei der Übermittlung der Befehle *Get*, *GetNext* und *Set* werden die Felder *Error Status* und *Error*

*Index* auf Null gesetzt. Der entsprechende Fehlerstatus wird nur bei der Antwort des Agenten verwendet und eingetragen.

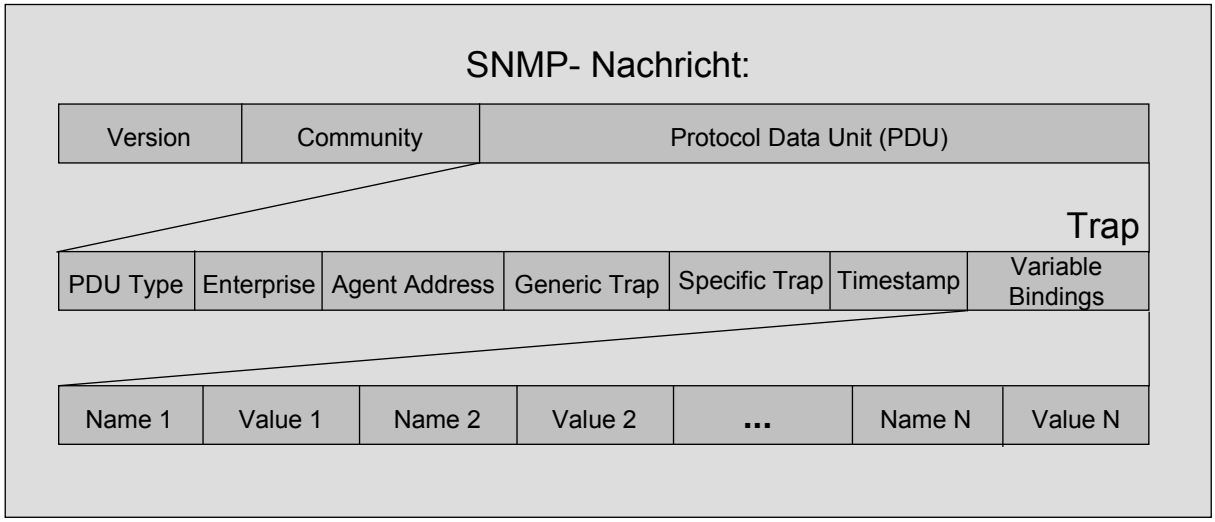



***Abbildung 3-7: Nachrichtenformat des Trap-Befehls***

Der Datenteil für den *Trap*-Befehl ist etwas anders aufgebaut (vgl. Abbildung 3-7):

- *Enterprise*
  Das Feld *Enterprise* gibt den Typ des Objektes an, das den Trap ausgelöst hat.
- *Agent Address*
  Im Feld *Agent Address* steht die Adresse des Agenten, von dem der Trap stammt.
- *Generic Trap*
  *Generic Trap* enthält den allgemeinen Typ des Traps.
- *Specific Trap*
  Im Feld *Specific Trap* ist ein Code enthalten, der den Typ genauer angibt.
- *Time Stamp*
  Das Feld *Timestamp* gibt die Zeit an, die zwischen der letzten Initialisierung des Netzwerkes und dem vorliegenden Trap verstrichen ist.
- *Variable Bindings*
  *Variable Bindings* enthält eine Liste von Variablen mit ergänzenden Informationen zum aktuellen Trap.

## 3.6 Vor- und Nachteile des SNMPv1

Die Vorteile des SNMP sind die geringen Ansprüche, die es an die Agenten stellt. Es ist einfach zu installieren und gleichfalls einfach zu bedienen. Die zusätzliche Belastung des Netzes bleibt marginal, da es im Regelfall nur einfache Variablen überträgt. Ein weiterer Vorteil ist seine weite Verbreitung und die damit verbundene Vielzahl an Anwendungen. Es kann als Quasi-Standard bezeichnet werden.

Der große Nachteil des Simple Network Management Protocols ist seine große Sicherheitsschwäche. Es bietet keine Möglichkeiten zur Authentifikation oder Verschlüsselung.
Ein weiterer Nachteil, der allerdings erst im Laufe der letzten Jahre entstanden ist als die Komponenten immer komplexer geworden sind, ist der Wunsch, die Daten noch detaillierter zu erhalten und noch feiner zu strukturieren.

# 4 Änderungen in SNMPv2 und SNMPv3

Dieses Kapitel beschreibt kurz die wichtigsten Änderungen der Nachfolger des SNMPv1. Im SNMP der Version 2 sind zwei neue Befehle zu den vier bereits bekannten Befehlen hinzugefügt worden: *GetBulk* und *Inform*

Der *GetBulk*-Befehl dient dem schnellen Auslesen großer Informationsblöcke, wie z.B. mehrere Spalten einer Tabelle. Es werden mehrere *GetNext*-Operationen automatisch hintereinander ausgeführt.

Der *Inform*-Befehl ermöglicht den Versand von *Trap*-Nachrichten von einem Network Management System zu einem anderen. Im Unterschied zum *Trap*-Befehl handelt es sich aber um einen bestätigten Befehl. Er dient weiterhin dem Nachrichtenaustausch zwischen Managern.

Auch die Nachrichtenformate in SNMPv2 sind geändert worden. Es existieren jetzt zwei Nachrichtenformate, eins für den *GetBulk*-Befehl und ein weiteres für alle anderen Befehle (*Get*, *GetNext*, *Set*, *Trap, Inform*). Weiterhin sind Möglichkeiten zur Verschlüsselung und Authentifikation hinzugefügt worden.

In der Version drei des SNMP ist ein neues Architekturmodell entwickelt worden, welches eine Modularisierung des Network Management Systems bzw. der Agenten vornimmt. Weiterhin sind die Sicherheitsfunktionen erweitert worden. So ist das User-based Security Model eingeführt worden, bei dem an einzelne Benutzer explizit Rechte vergeben werden können, ebenso ein Modell zur Zugriffskontrolle (View-based Access Control).

# 5 SNMPv3

## 5.1 Architekturmodel

Das neue Architekturmodell, welches für SNMPv3 entwickelt worden ist, unterteilt das Network Management System ebenso wie den Agenten in verschiedene Subsysteme. Diese werden weiter in einzelne Module unterteilt (vgl. Abbildung 5-1). Diese Modularisierung erlaubt es, einzelne Komponenten zu ersetzen oder zu erneuern, ohne das ganze Modell erneuern zu müssen. Beispielsweise kann ein Sicherheitsmodul ausgetauscht werden, in dem ein neuer stärkerer Verschlüsselungsalgorithmus implementiert ist, ohne das dies Einfluß auf die anderen Komponenten hat. Dies muß natürlich auf allen Ressourcen und Managern stattfinden.

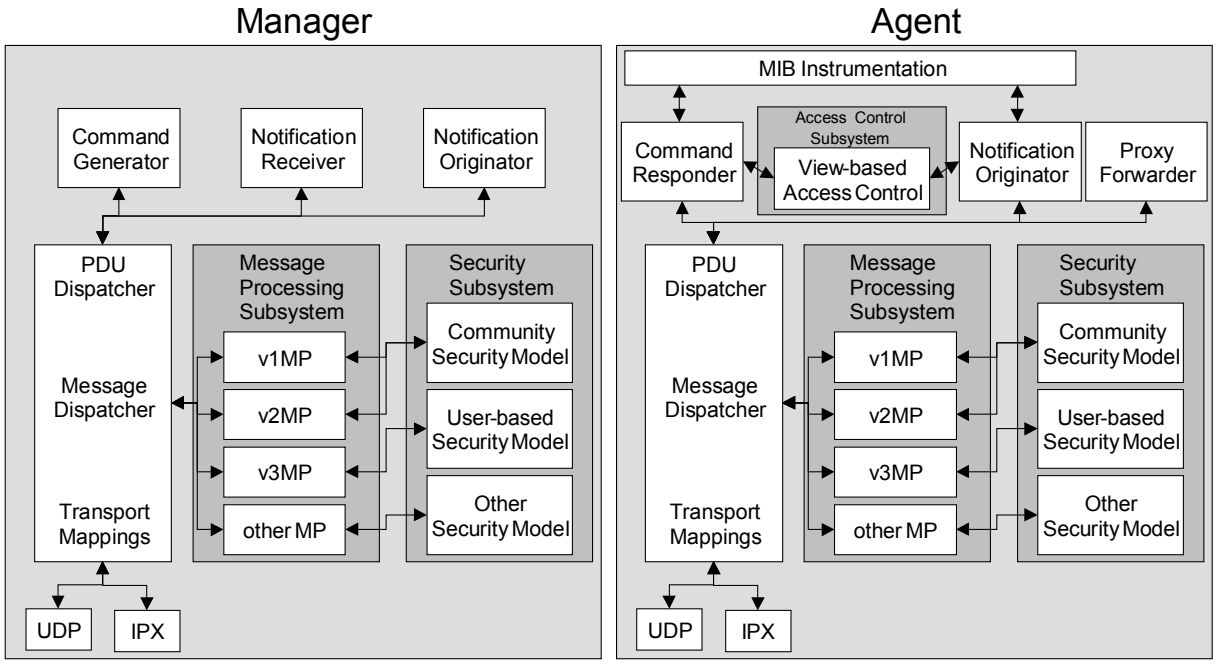



***Abbildung 5-1: Architekturmodel***

Der *Message Dispatcher* des Network Management Systems kümmert sich um den Empfang und das Versenden der Nachrichten. Er weist die Nachrichten dem richtigen Modul des *Message Processing Subsystem* zu. Das *Message Processing Subsystem* bereitet je nach ausgewähltem Managementprotokoll die Daten auf den Versand vor bzw. extrahiert die Daten aus einem eingetroffenen Paket. Das *Security Subsystem* stellt je nach Modell z.B. die Hilfsmittel zur Ver- bzw. Entschlüsselung oder Authentifizierung zur Verfügung. Die Module *Command Generator*, *Notification Receiver* und *Notification Originator* erledigen die weitere Verwendung der Daten.

Der *Agent* enthält ebenfalls alle bereits oben beschriebenen Module. Weitere Module sind die *MIB Instrumentation*, welche die Management Information Base beinhaltet, und ein *Access Control Subsystem*, in dem ein Modell zur Zugriffskontrolle implementiert ist, wie z.B. das *View-based Access Control Model* (vgl. Kapitel 5.3.3). Die *ProxyForwarder*-Komponente leitet Nachrichten an andere Agenten weiter.

## 5.2 Sicherheitsproblematik

Um mit Hilfe eines Netzwerkmanagement-Systems ein Netzwerk nicht nur zu überwachen sondern auch verantwortungsbewußt konfigurieren und managen zu können, muß die Sicherheitsproblematik geeignet gelöst werden.
Es stellen sich vier Fragen, die vor Ausführung einer Operation beantwortet werden müssen:

1) Ist die empfangene Nachricht authentisch?
2) Wer möchte die Operation ausgeführt bekommen?
3) Welche Objekte sind von der Operation betroffen?
4) Welche Rechte hat derjenige, der die Operation ausgeführt bekommen möchte in Bezug auf die betroffenen Objekte?

Die Fragen eins und zwei werden durch Maßnahmen zur Sicherung der Nachricht, also Authentifikation und Verschlüsselung, beantwortet. Die Lösung zu den Fragen drei und vier liegt in einem Modell zur Zugriffskontrolle. Das SNMPv3 stellt für alle vier Fragen Maßnahmen zur Verfügung, die im folgenden kurz vorgestellt werden.

## 5.3 Sicherheitsmechanismen

### 5.3.1 Datenintegrität und Authentifikation

Die Möglichkeit, die das SNMPv3 zur Authentifikation bietet, dient gleichzeitig zur Überprüfung der Datenintegrität, also der Überprüfung, ob die Nachricht unverändert ihr Ziel erreicht hat.
Die Abbildung 5-2 zeigt das Prinzip der Authentifikation einer Nachricht. Der Sender nimmt seinen Schlüssel und das zu übertragende Datenpaket und wendet darauf eine kryptographisch starke Hashfunktion (MD-5, SHA-1) an. Diese erzeugt eine Prüfsumme fester Länge, der Message Authentication Code (MAC), der mit den Daten zusammen übertragen wird. Der Empfänger wendet das Verfahren auf die gleiche Art und Weise an und überprüft anschließend, ob sein ermittelter MAC der gleiche ist wie der, der mit übertragen worden ist. Ein falscher Schlüssel oder eine geänderte Nachricht erzeugen einen anderen MAC, der nicht mit dem übertragenen MAC übereinstimmt.

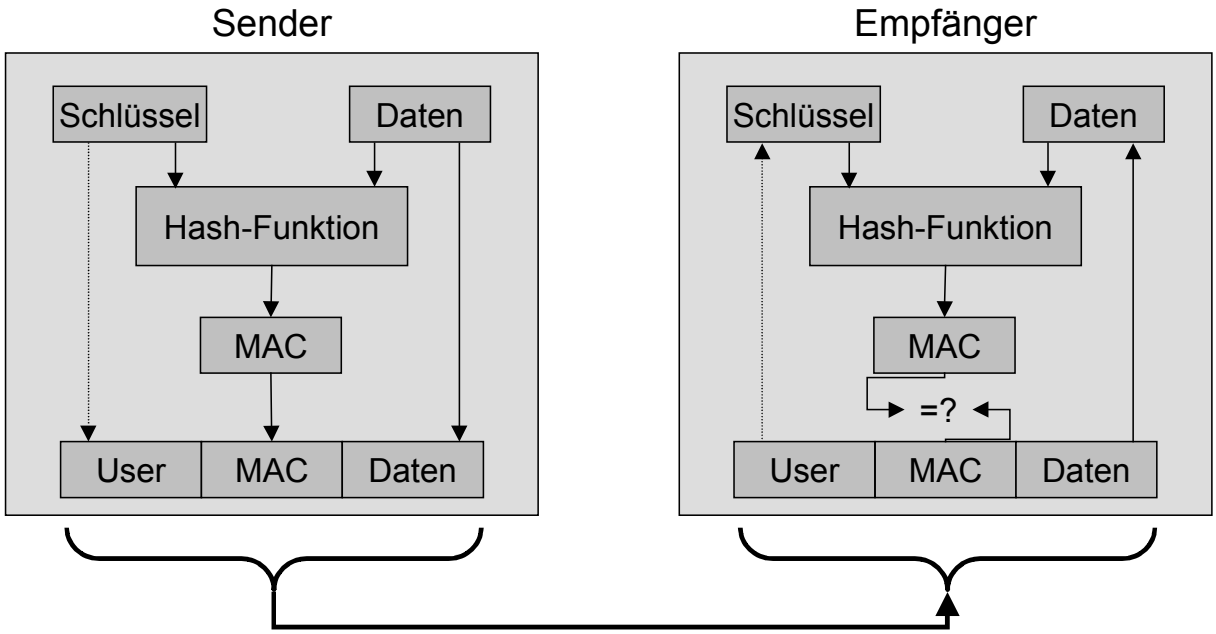



***Abbildung 5-2: Prinzip der Authentifikation***

Der benutzte Schlüssel ist sowohl dem Sender als auch dem Empfänger bekannt. Das SNMPv3 bietet aber auch die Möglichkeit den Schlüssel zu ändern, wodurch bei jeder neuen Nachricht theoretisch ein neuer Schlüssel benutzt werden kann. SNMPv3 stellt einen Algorithmus zum Ändern der Schlüssel zur Verfügung, der eine relativ sichere Schlüsseländerung ohne Verschlüsselung erlaubt, da beim Ändern der neue Schlüssel nicht direkt übertragen wird. Ist ein Schlüssel gebrochen und sind dem Angreifer alle Schlüsseländerungsnachrichten bekannt, so kann er den aktuellen Schlüssel errechnen.
Der Authentifikationsalgorithmus ist selbstverständlich nicht fest vorgegeben und kann, falls er z.B. unsicher geworden ist, durch einen anderen, sichereren ersetzt werden. Dies muß natürlich auf allen beteiligten Ressourcen geschehen.

### 5.3.2 Sicherung gegen unbefugtes Abhören

Das Verfahren zur Verschlüsselung einer Nachricht ist ähnlich dem zur Authentifikation (vgl. Abbildung 5-3).
Der Sender nutzt wieder seinen Schlüssel, um die Nachricht mit Hilfe eines Verschlüsselungsalgorithmus, dem Data Encryption Standard (DES) zu verschlüsseln. Dieses verschlüsselte Datenpaket wird an den Empfänger verschickt. Dort wird der Schlüssel dazu benutzt, die verschlüsselten Daten mit Hilfe des zugehörigen Entschlüsselungsalgorithmus zu entschlüsseln. Das Schlüsselmanagement entspricht dem bei der Authentifikation bereits beschriebenen Verfahren.
Der Verschlüsselungsalgorithmus ist nicht fest vorgegeben und kann bei Bedarf ersetzt werden.

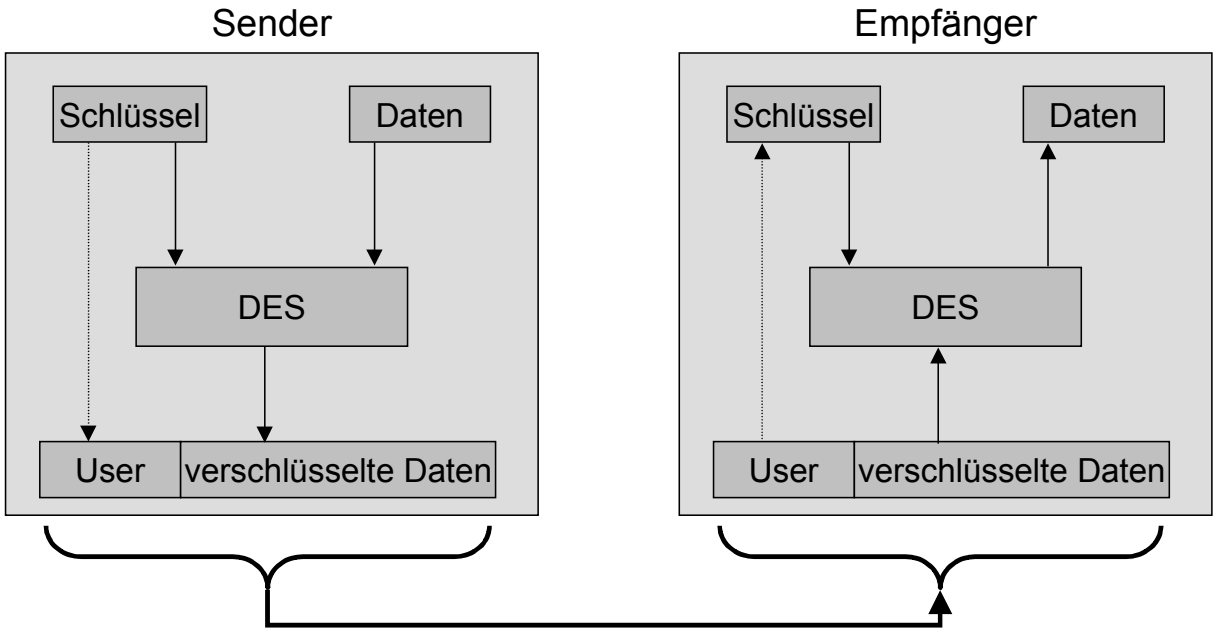



***Abbildung 5-3: Prinzip der Verschlüsselung einer Nachricht***

Da die Verschlüsselung relativ aufwendig ist, sollte sie nur in sicherheitskritischen Bereichen eingesetzt werden, in denen eine Verschlüsselung wirklich erforderlich ist.

### 5.3.3 View-based Access Control

Das View-based Access Control Model ist nach dem Schema in Abbildung 5-4 aufgebaut.

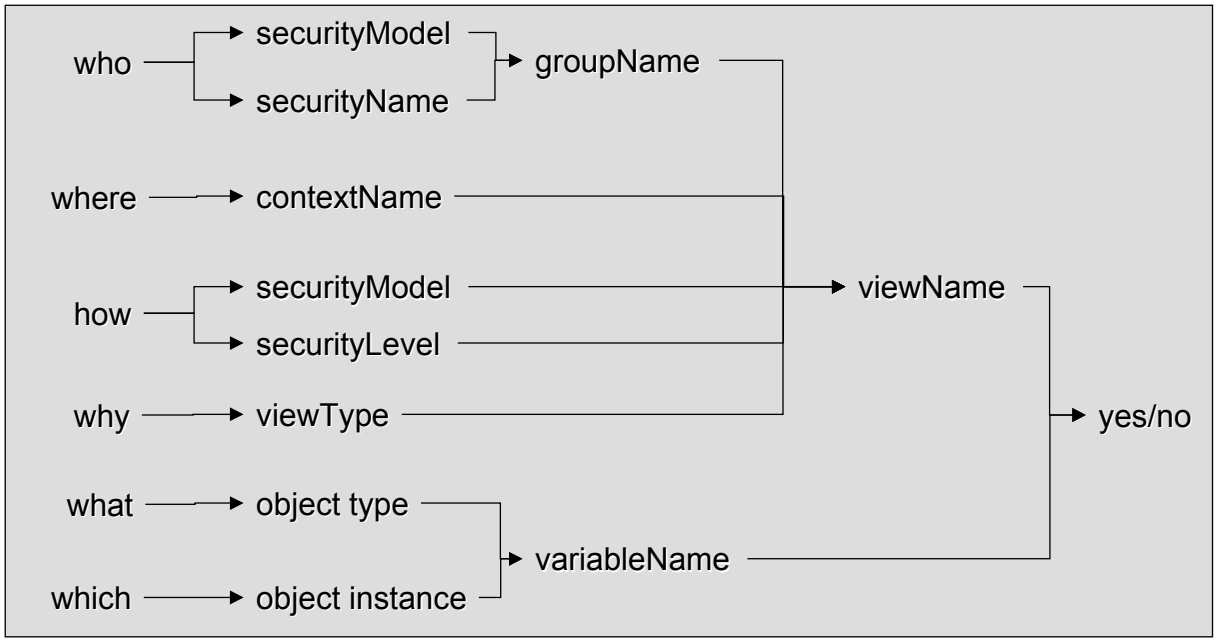



***Abbildung 5-4: Das View-based Access Control Model***

Als erstes wird überprüft, wer den Zugriff möchte. Das benutzte *securityModel* und der *securityName*, der den Manager identifiziert, werden zum *groupName* zusammengefaßt. Der *contextName* stellt anschließend den Zusammenhang zwischen der Ressource und dem betroffenen Objekt her, zur Klärung, wo der Zugriff erfolgen soll. Der *securityLevel* bestimmt, ob eine Nachricht ohne Authentifizierung, mit Authentifizierung, jedoch unverschlüsselt oder mit Authentifizierung und Verschlüsselung versendet wird. Schließlich wird noch überprüft, wie der Zugriff erfolgen soll, also z.B. schreibend oder lesend. Dies wird durch den *viewType* wiedergegeben. Alle vorhandenen Kombinationen besitzen einen eindeutigen *viewName*. Für diesen ViewName erfolgt nun die Überprüfung, ob der Zugriff auf den konkreten Objekttyp und seine Objektinstanz erlaubt ist oder nicht. Dementsprechend wird der Befehl anschließend weiterverarbeitet oder zurückgewiesen.

# 6 Zusammenfassung

Vor 10 Jahren ist das Simple Network Management Protocol (SNMP) entwickelt und standardisiert worden. SNMPv1 war sehr erfolgreich, da es eine zu der Zeit angemessene und von den Kosten her eine vertretbare und schnell umzusetzende Lösung darstellte. Da das SNMPv1 keine Sicherheitsmechanismen beinhaltet, wird es vorwiegend zum Monitoring eingesetzt. Es ist lange versucht worden dieses Problem zu beheben, ohne jedoch das Ziel mit SNMPv2 zu erreichen. Erst das SNMPv3, publiziert 1998 als Proposed-Standard, bietet neben der Lösung der Sicherheitsproblematik ein neues Architekturmodel, welches eine Modularisierung zuläßt. Dadurch ist eine Abwärtskompatibilität weiterhin gewährleistet.

# 7 Literatur

[BEC97] Beck, Holger
Grundlagen der Netzwerktechnik
Aufbau, Management, Nutzung
Gesellschaft für wissenschaftliche Datenverarbeitung mbH
Göttingen, Oktober 1997
http://www.gwdg.de/welcome_neu2.htm

[COH95] Cohen, Yoram
SNMP – Simple Network Management Protocol
http://www.rad.com/networks/1995/snmp/snmp.htm

[FAC98] Interest Verlag
Fachkompendium Protokolle und Dienste der Informationstechnologie
Interest Verlag GmbH, Augsburg 1999

[SCH98] Schönwälder, Jürgen
Vorlesung Netzwerkmanagement
Unterlagen zur Vorlesung Netzwerkmanagement
Technische Universität Braunschweig, Braunschweig 1998
http://www.ibr.cs.tu-bs.de/lehre/ws9899/nm/

[SCH99] Schönwälder, Jürgen
Internet Management Standards
Quo Vadis?
Technische Universität Braunschweig, Braunschweig 1999
http://snmp.cs.utwente.nl/bibliography/articles/general/index.html

[RFC1155] Rose, Marshall / McCloghrie, Keith
Structure and Identification of Management Information for TCP/IP-based Internets
RFC 1155, Mai 1990

[RFC1157] Case, Jeffrey / Fedor, Mark / Schoffstall, Martin / Davin, James
A Simple Network Management Protocol (SNMP)
RFC 1157, Mai 1990

[RFC1213] Rose, Marshall / McCloghrie, Keith
Management Information Base for Network Management of TCP/IP-based Networks
RFC 1213, März 1991

[RFC2271] Harrington, Dave / Presuhn, Randy / Wijnen, Bert
An Architecture for Describing SNMP Management Frameworks
RFC 2271, Januar 1998

[RFC2274] Blumenthal, Uri / Wijnen, Bert
User-based Security Model (USM) for version 3 of the Simple Network Management Protocol
RFC 2274, Januar 1998

[RFC2275] Wijnen, Bert / Presuhn, Randy / McCloghrie, Keith
View-based Access Control Model (VACM) for the Simple Network Management Protocol
RFC 2275, Januar 1998