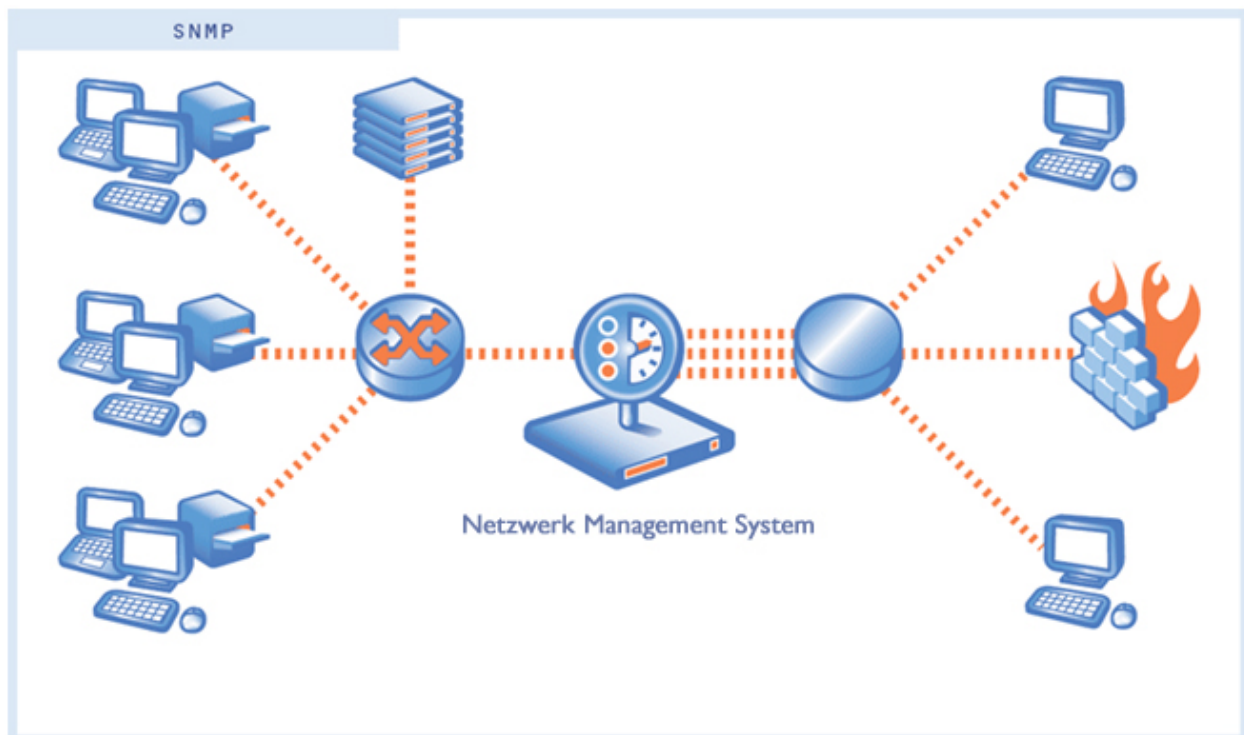



# Datenkommunikations-Protokolle

SNMP



<b>Modul: TeDKP</b>		<b>Datum: 07.06.2010</b>
	Name:	E-Mail:
Verfasser:	Manuel Mareischen	manuel.mareischen@tet.htwchur.ch
Dozent:	Bruno Wenk	bruno.wenk@htwchur.ch
	 <b>HTW</b> Chur Hochschule für Technik und Wirtschaft  Fachhochschule Ostschweiz University of Applied Sciences	



## INHALTSVERZEICHNIS

<b>Inhaltsverzeichnis .....</b>	<b>2</b>
<b>1. Einleitung .....</b>	<b>3</b>
1.1. <i>Netzwerk-Überwachung .....</i>	3
1.2. <i>Netzwerk-Konfiguration .....</i>	3
<b>2. Geschichte .....</b>	<b>4</b>
<b>3. Grundlagen .....</b>	<b>4</b>
3.1. <i>Versionen .....</i>	5
3.1.1. <i>Version 1 .....</i>	5
3.1.2. <i>Version 2 .....</i>	5
3.1.3. <i>Version 3 .....</i>	5
<b>4. OSI-Protokollstapel .....</b>	<b>6</b>
<b>5. Kommunikation .....</b>	<b>6</b>
5.1. <i>Befehle .....</i>	6
<b>6. Paketaufbau .....</b>	<b>8</b>
6.1. <i>Trap-Meldungen .....</i>	9
<b>7. SMI .....</b>	<b>10</b>
<b>8. MIB.....</b>	<b>10</b>
<b>9. Beispiel und Aufzeichnung mittels Wireshark .....</b>	<b>11</b>
9.1. <i>GET Anfrage an Windows XP Client .....</i>	11
<b>10. Abbildungsverzeichnis .....</b>	<b>13</b>
<b>11. Tabellenverzeichnis .....</b>	<b>13</b>
<b>12. Quellverzeichnis .....</b>	<b>13</b>

## 1. EINLEITUNG

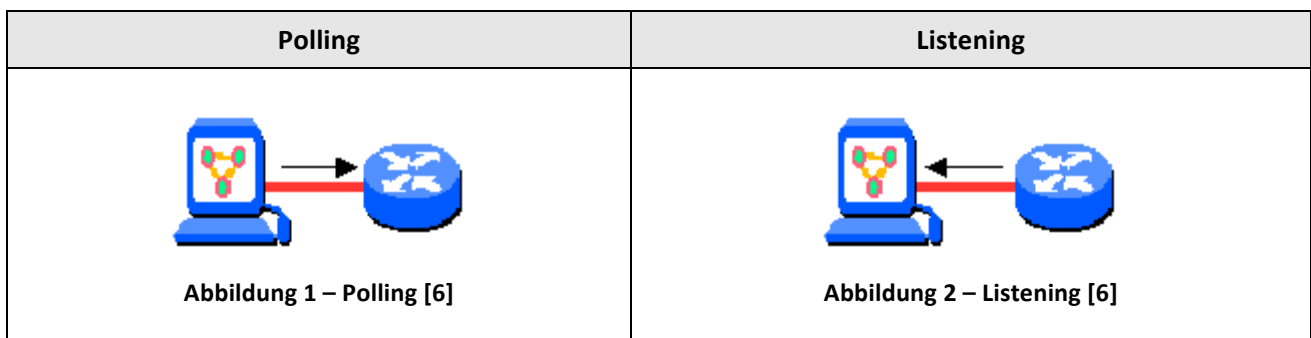
SNMP ist das Akronym für Simple Network Management Protokoll. Das Protokoll dient dem einfachen management eines Netzwerks. Unter Netzwerkmanagement wird in diesem Bezug hauptsächlich die Netzwerk-Konfiguration und -Überwachung verstanden.

Das Netzwerkmanagement stellt hohe Anforderungen an die Dienstgüte eines Netzwerks. Zur Erreichung dieser Anforderungen werden sogenannte Netzwerkmanagement-Systeme eingesetzt. Mit SNMP hat sich ein Industriestandard für die Kommunikation eines solchen Systems durchgesetzt.

### 1.1. Netzwerk-Überwachung

Unter Netzwerküberwachung versteht man die regelmässige Kontrolle eines Netzwerks, deren Hardware (z.B. Server, Router, Switches) sowie verschiedener Dienste (z.B. HTTP-Dienst, DNS-Dienst). Somit kann erkannt werden, ob nur ein gewisser Dienst auf einem Gerät nicht erreichbar ist, oder ob das ganze Gerät ausgefallen ist.

Im Grunde genommen gibt es zwei Möglichkeiten ein Netzwerk zu überwachen. Entweder geschieht dies **aktiv** oder **passiv**. Aktiv wird jedes Gerät in einem bestimmten zeitlichen Abstand abgerufen (Polling) und dem Gerät wird ein Paket zugeschickt. Dieses sendet anschliessend eine Antwort-Meldung zurück. SNMP unterstützt diese Funktionen. [1]



### 1.2. Netzwerk-Konfiguration

Das Konfigurationsmanagement dient dazu, das gesamte Netzwerk verfügbar zu machen. Hauptsächlich beinhaltet dieser Prozess die Abhandlung von Software-Konfigurationen sowie Einstellungsanpassungen sämtlicher Geräte innerhalb des Netzwerkes. [2]

## 2. GESCHICHTE

Das Protokoll entstand aus der Notwendigkeit heraus, die Komponenten in dem stetig wachsenden Internet einfacher konfigurieren zu können. Ein weiterer Punkt war, dass sich viele Hersteller mit der damaligen Marktlücke Internet versuchten und dies führte zu einem verbreiteten heterogenen Netz. Diesbezüglich wurde im Jahre 1987 ein Projekt gestartet, das Internet-Management auf ein einfaches Protokoll zu beschränken.

Der erste Versuch war SGMP (Simple Gateway Monitoring Protocol), welches das Management von Verbindungsknoten (Routern und deren Subnetze) beinhaltete. Ein anderer Versuch war HEMS (High Level Entity Management), welches jedoch nie den Weg in eine produktive Umsetzung fand. Der nächste Ansatz war, ein Protokoll gemäss des OSI-Modells zu verfolgen, welches dann schlussendlich als CMOT (CMIP over TCP; Common Management Information Protocol over Transmission Control Protocol) entstand.

Aus der Kombination von SGMP und CMOT entstand letztendlich das Protokoll SNMP, sowie die Informations-Standardisierungen SIM (Structure of Management Information) und MIB (Management Information Base). Mittels dieser Standardisierungen wird festgelegt wie Informationen, welches ein netzwerkfähiges Gerätes zur Verfügung stellt, gegliedert sind. Weitere Informationen unter Punkt 7 und 8.

Inzwischen hat sich SNMP als „der Standard“ für das Netzwerkmanagement etabliert, so dass quasi alle verfügbaren Netzwerkgeräte via SNMP managebar sind. Der letzte Stand bei der Entwicklung von SNMP liegt bei SNMPv3 (Version 3) aus dem Jahre 2002. [3]

## 3. GRUNDLAGEN

SNMP basiert auf dem Client/Server Modell, wobei der Client dem **Manager** und der Server dem **Agenten** entspricht. Der Manager ist in den meisten Fällen ein mächtiges Netzwerkmanagement-System, und der Agent eine Netzwerkressource. [3]

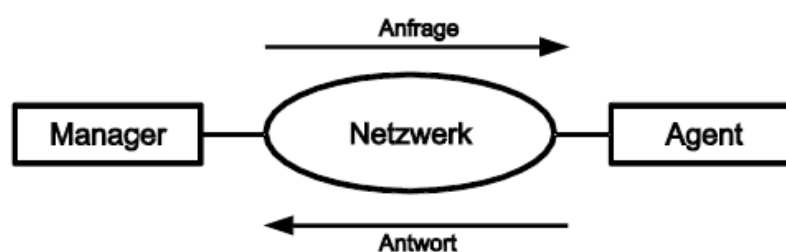


Abbildung 3 - Manager/Agent-Modell [3]



### 3.1. Versionen

SNMP wurde seit dessen Einführung stets weiterentwickelt, wobei hauptsächlich zusätzliche Sicherheitsmechanismen implementiert wurden. Die aktuell verbreitetste Variante ist die Version 2. Als nächstes folgt eine kurze Auflistung der verschiedenen Versionen.

#### 3.1.1. Version 1

Definiert in den RFC's:

- RFC 1155 – SMI
- RFC 1156 – MIB
- RFC 1157 – A Simple Network Management Protocol

Das Hauptproblem der ersten Version stellt die geringe, kaum vorhandene Sicherheit dar. Das Passwort (ein einfacher „Community-String“) wird im Klartext übertragen und kann somit leicht gesniffert werden.

#### 3.1.2. Version 2

Definiert in den RFC's:

- RFC 1901 – Introduction to Community-based SNMPv2
- RFC 1905 – Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2)
- RFC 1906 – Transport Mappings for version 2 of the Simple Network Management Protocol (SNMPv2)

SNMPv2 weist keine verbesserte Sicherheit bezüglich SNMPv1 auf. Das Protokoll wurde lediglich mit einigen nützlichen Funktionen erweitert, wie beispielsweise die Funktion GetBulk, welches mehrere Werte auf einmal abfragt.

#### 3.1.3. Version 3

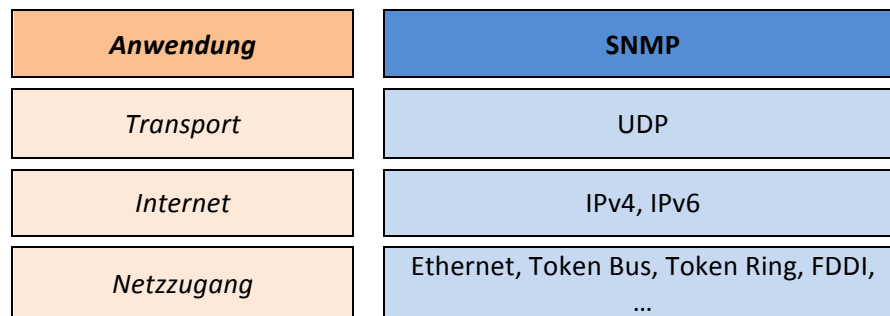
Etliche neue RFC's wurden für die sichere Version 3 definiert. Nur die wichtigsten werden folglich erwähnt:

- 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)

Wie bereits erwähnt bieten SNMP-Versionen 1 und 2 keine Sicherheitsmechanismen. So entstand auch die scherzhafte Deutung von SNMP als „Security is not my problem“. In der neusten und aktuellen Version 3 wurden die Sicherheitsmechanismen deutlich verbessert.

Jedoch führte die damit gestiegene Komplexität (wie beispielsweise eine Benutzer- und Passwortverwaltung) dazu, dass sich die Version 3 gegenüber Version 2 noch nicht durchsetzen konnte. [1]

## 4. OSI-PROTOKOLLSTAPEL



**Tabelle 1 - OSI-Protokollstapel**

SNMP baut auf das verbindungslose Transportprotokoll UDP auf. Somit wird das Netzwerk auf ein Minimum belastet. Die folgenden Ports sind für SNMP definiert: [1]

- 161/UDP
- 162/UDP (Traps)

## 5. KOMMUNIKATION

Via SNMP können Informationen abgerufen (GET), oder Konfigurationen abgeändert (SET) werden. Damit eine solche Kommunikation erfolgen kann sind auf dem betroffenen Gerät Community-Strings zu konfigurieren. Diese Community-Strings entsprechen Passwörtern.


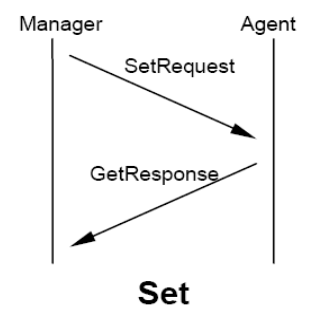
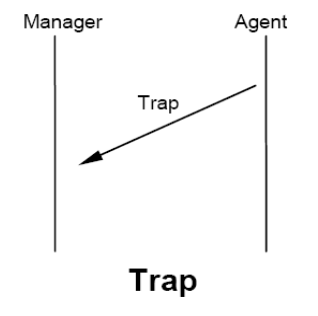
- Lesezugriff → Read Only-Community
- Schreibzugriff → Write-Community

Standardmässig sind die Community-Strings für den Lesezugriff auf „public“ und für den Schreibzugriff auf „private“ gesetzt. Es wird stark empfohlen diese Strings abzuändern, denn die Strings werden bei SNMPv1 und SNMPv2 in Klartext übertragen. Deshalb weist ein solcher Community-String keinerlei Sicherheit auf. Eine Protokollaufzeichnung mittels Wireshark wird in einem späteren Abschnitt dargestellt. Wenn der mit gesendete Community-String mit dem, auf dem Gerät konfigurierten String übereinstimmt, werden die Daten übermittelt. [1]

### 5.1. Befehle

Auf den Netzwerkkomponenten muss der so genannte "Agent" laufen. Dabei handelt es sich um eine Art Programm, welches das jeweilige Gerät überwacht und dessen Informationen im Netz zur Verfügung stellt. Ein „Manager“ (üblicherweise ein NMS) kann dann über diese Agenten auf die Geräte zugreifen um Daten abzurufen, sowie auch um Konfigurationsänderungen vorzunehmen. [5]

Die Kommunikation zwischen Agent und Manager kennt 6 verschiedene SNMP Befehle:

<b>GET</b>	Anfordern eines Management Datensatzes	
<b>GETNEXT</b>	Den nachfolgenden Datensatz abrufen	siehe GET-Befehl
<b>GETBULK</b>	mehrere Daten auf einmal abrufen	siehe GET-Befehl
<b>SET</b>	Den Datensatz einer Netzwerkkomponente verändern	
<b>RESPONSE</b>	Antwort auf eines der angeforderten GET-Pakete	
<b>TRAP</b>	Nachricht von einem Agenten an den Manager, dass ein Ereignis eingetreten ist	

**Tabelle 2 - Befehle**

## 6. PAKETAUFBAU

Das SNMP-Paket ist grundsätzlich wie folgt aufgebaut (Trap wird separat aufgeführt): [1]

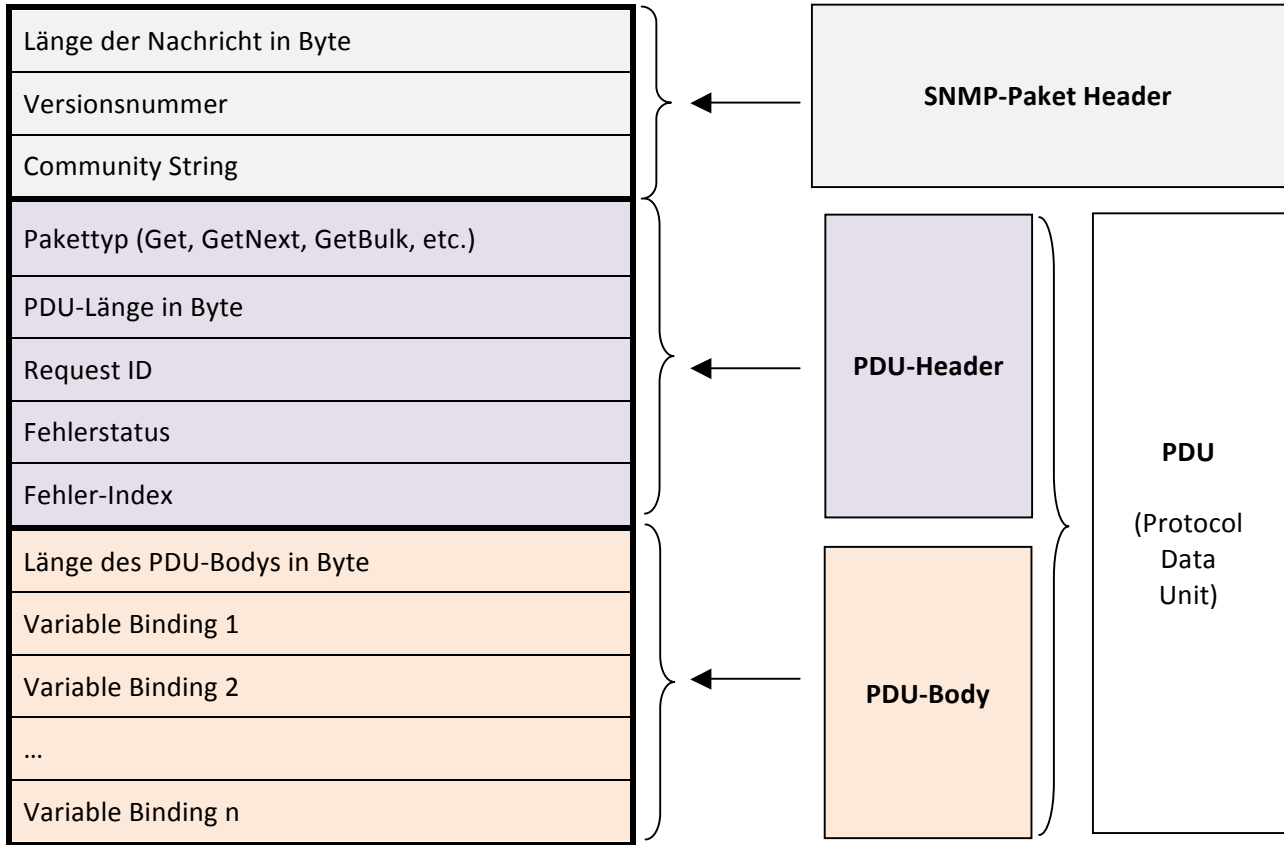


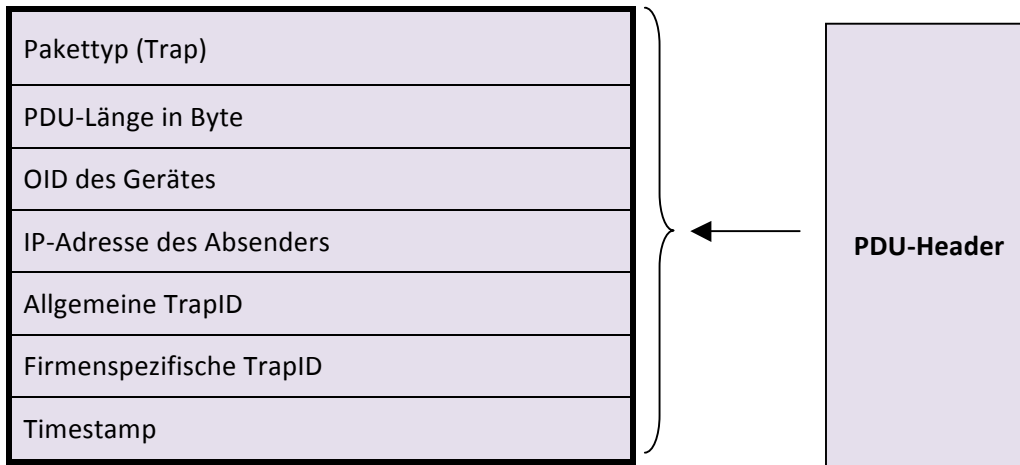
Tabelle 3 - Paketaufbau

Die Variable Bindings enthalten hierbei die angeforderten Objekte. [1]

Variable Binding 1		Variable Binding 2		....		Variable Binding n	
Name 1	Wert 1	Name 2	Wert 2	...	...	Name n	Wert n

## 6.1. Trap-Meldungen

Bei einer Trap Meldung ist der PDU-Header ein wenig anders aufgebaut:



**Tabelle 4 - PDU-Header Trap**

Um zu erkennen, von wem die Nachricht kommt, wird die IP-Adresse des Absenders, sowie dessen OID mitgesendet. Die OID gibt an, um was für ein Gerät es sich handelt. Anschliessend folgt die allgemeine TrapID. Es gibt sieben mögliche allgemeine TrapIDs:

- Kaltstart
- Warmstart
- Link Down
- Link Up
- Authentifizierungsfehler
- Nachbar verloren
- Firmenspezifisch

Wird in diesem Feld angegeben, dass es sich um einen firmenspezifischen Trap handelt, wird dessen ID im nachfolgenden Feld übertragen. [1]

## 7. SMI

Ein netzwerkfähiges Gerät hat tausende Informationen, welches es bereitstellt. Eine Strukturierung dieser Daten ist daher von grossem Vorteil. Diese Strukturierung ist gemäss der "Structure of Management Information" (SMI) definiert. Die Daten sind in Objekte (Managed Objects) eingeteilt und in einer hierarchischen Ordnung eingegliedert. Die Managed Objects sind wiederum in so genannten MIBs (Managed Information Bases) definiert. [5]

## 8. MIB

Abrufbare Informationen sind wie bereits erwähnt in den MIBs festgelegt (eine MIB kann man sich als eine Art Datenbank vorstellen). Mehrere MIBs wurden in RFCs (Request for Comments) als Standard definiert. Die Informationen einer MIB sind in einer Art Baumstruktur organisiert, deren einzelne Zweige entweder durch Nummern oder durch alphanumerische Bezeichnungen dargestellt werden können. Die MIB-2 (welche von allen netzwerkfähigen Geräten unterstützt wird) ist zum Beispiel unter "iso.org.dod.internet.mgmt.mib-2" zu finden. Sie ist sowohl auch durch die Zahlenreihe 1.3.6.1.2.1 eindeutig bestimmt (1 für "iso", 3 für "org" usw.). Diese, aus Zahlen bestehende Zeichenkette, nennt man OID (Object Identifier) und jede OID ist eindeutig. [5]

Herstellerspezifische Informationen sind unterhalb der MIB "enterprises" zu finden. Jedes Unternehmen, welches Hard- oder Software herstellt, kann dort eine eigene MIB veröffentlichen.

Nachfolgend die Struktur einer MIB:

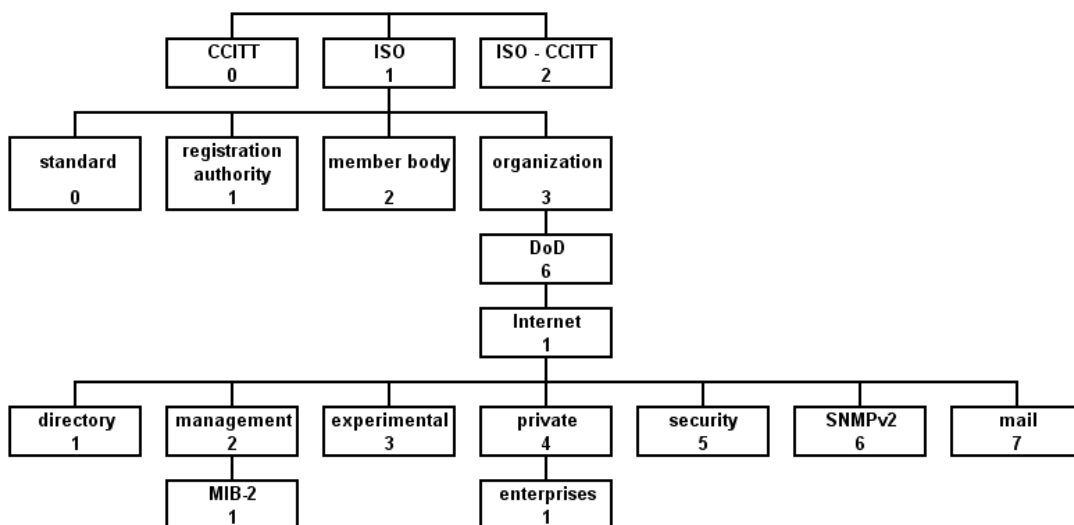


Abbildung 4 - MIB - Struktur [5]

## 9. BEISPIEL UND AUFEICHNUNG MITTELS WIRESHARK

Zur Verdeutlichung, wie eine Information abgerufen wird, ein Beispiel einer SNMP-Get Anfrage und der dazugehörigen SNMP Response:

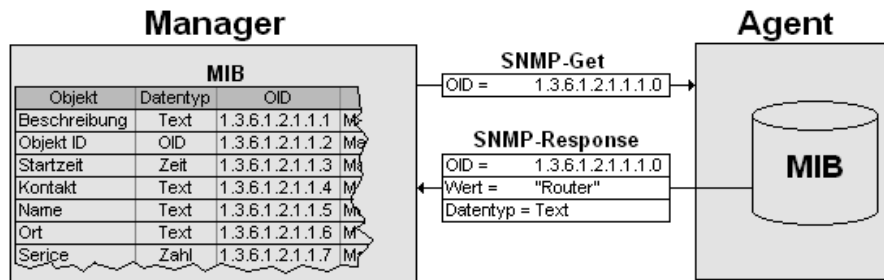


Abbildung 5 - SNMP-Get Anfrage [1]

### 9.1. GET Anfrage an Windows XP Client

Im Folgenden Beispiel wurde mittels der Software „iReasoning MIB-Browser“ eine SNMP-Anfrage an einen Windows XP Client gestartet und mittels Wireshark aufgezeichnet.

Manager (MIB Browser) - GET OID: .1.3.6.1.2.1.1.1.0 (SystemDescription):

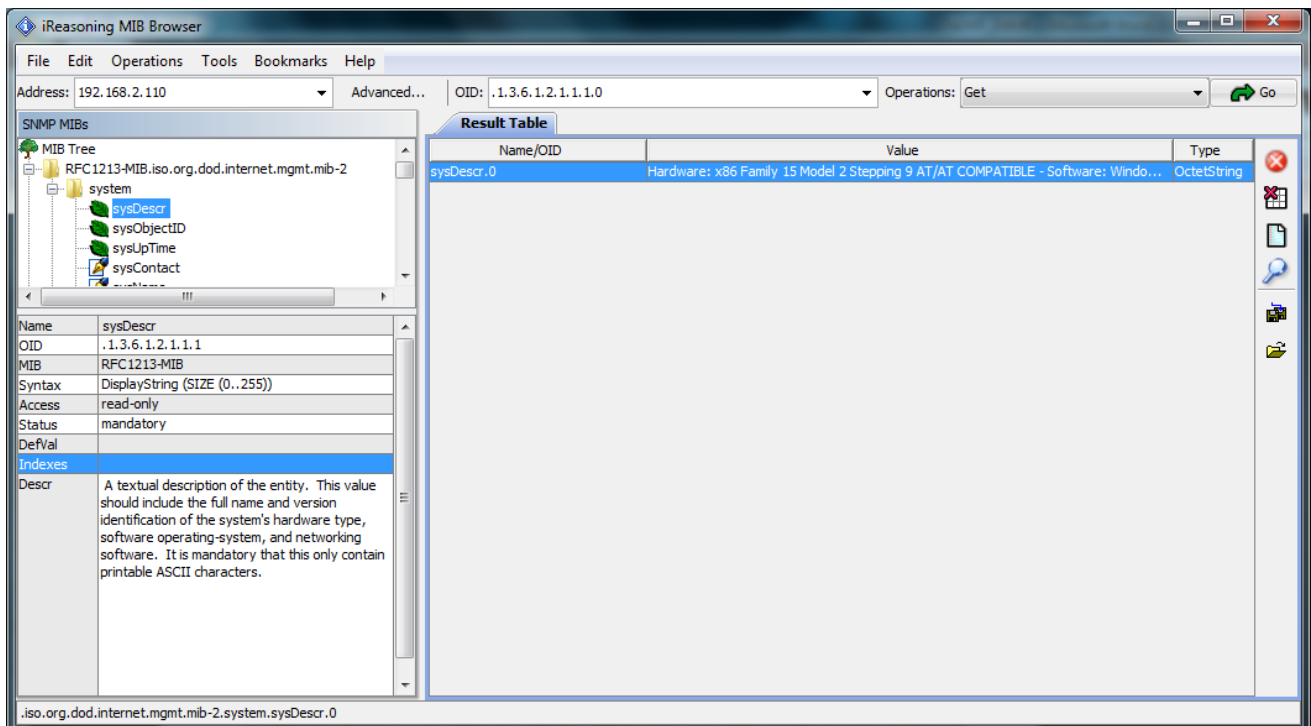


Abbildung 6 - MIB-Browser [6]

Kommunikationsaufzeichnung mit Wireshark:

• GET-Request

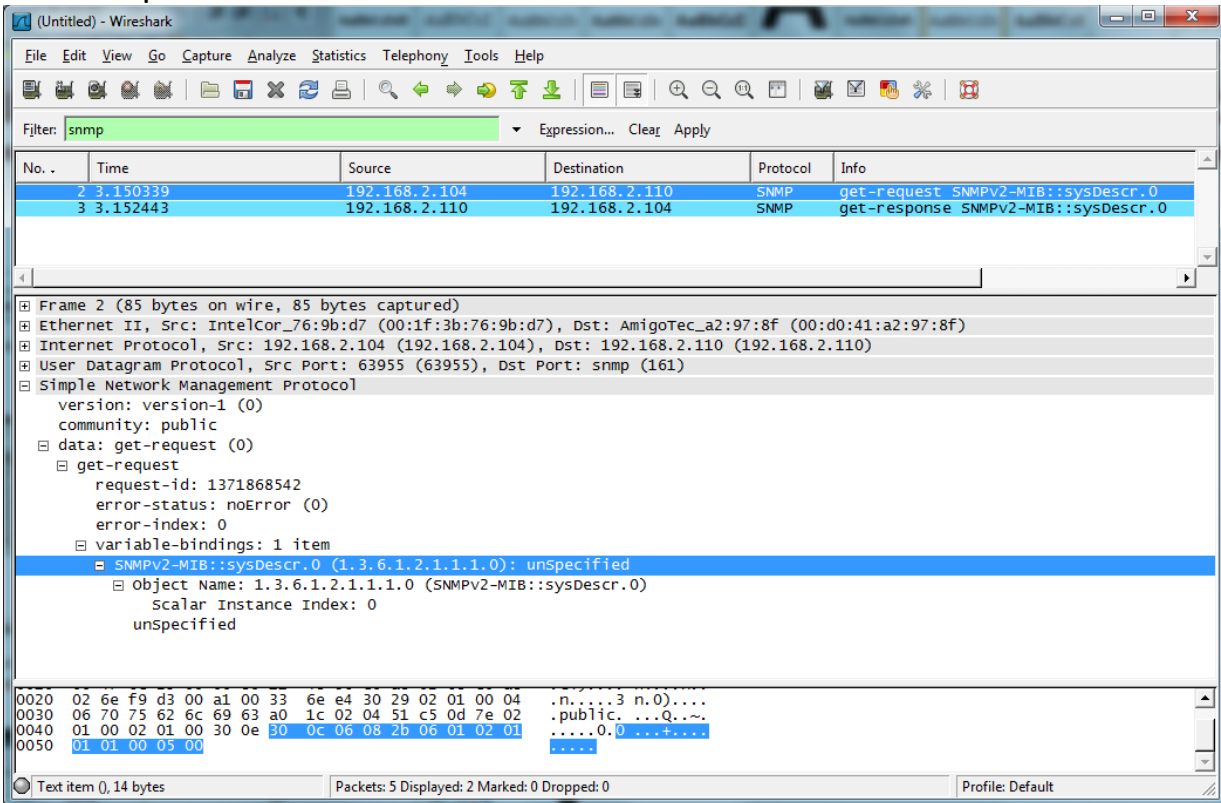


Abbildung 7 - GET-Request [6]

• GET-Response

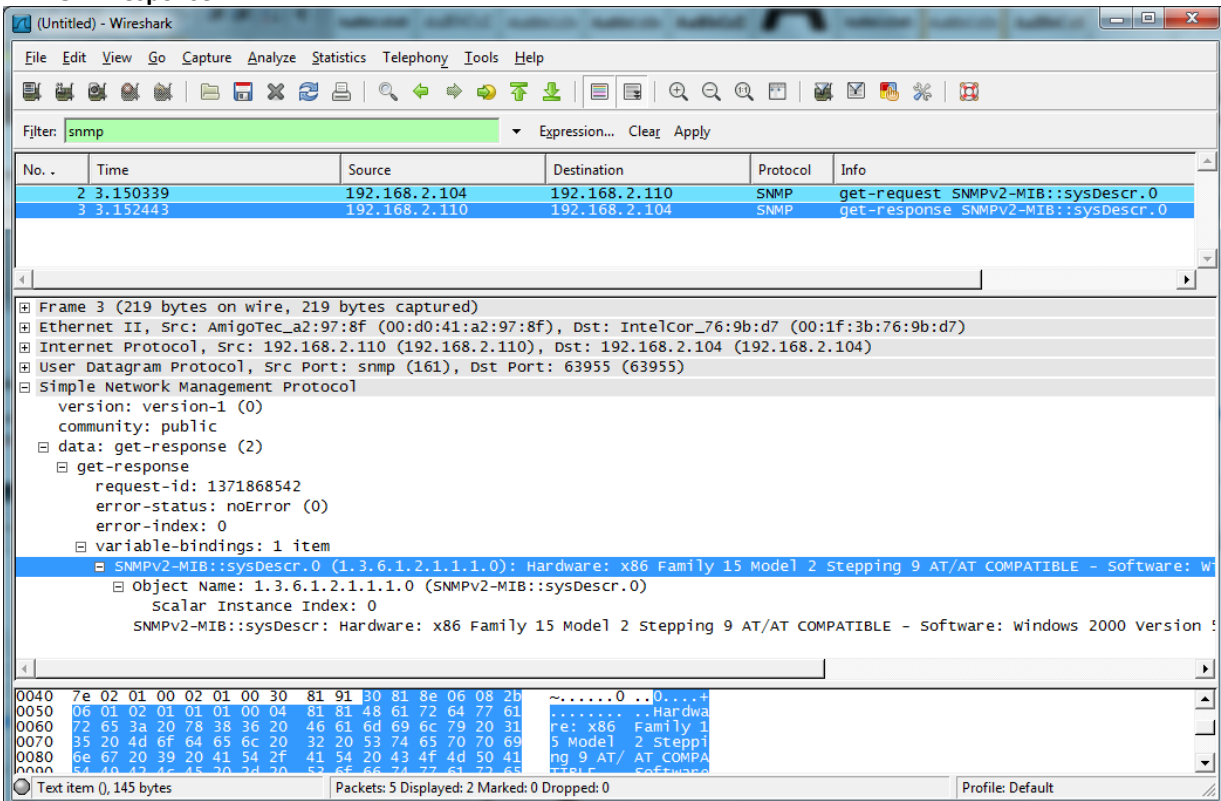


Abbildung 8 - GET-Response [6]



## 10. ABBILDUNGSVERZEICHNIS

Abbildung 1 – Polling [6].....	3
Abbildung 2 – Listening [6] .....	3
Abbildung 3 - Manager/Agent-Modell [3] .....	4
Abbildung 4 - GET-Befehl [5] .....	<b>Fehler! Textmarke nicht definiert.</b>
Abbildung 5 - SET-Befehl [5] .....	<b>Fehler! Textmarke nicht definiert.</b>
Abbildung 6 - TRAP-Befehl [5] .....	<b>Fehler! Textmarke nicht definiert.</b>
Abbildung 7 - MIB – Struktur [5].....	10
Abbildung 8 - SNMP-Get Anfrage [1].....	11
Abbildung 9 - MIB-Browser [6] .....	11
Abbildung 10 - GET-Request [6] .....	12
Abbildung 11 - GET-Response [6] .....	12

## 11. TABELLENVERZEICHNIS

Tabelle 1 - OSI-Protokollstapel .....	6
Tabelle 4 - Befehle .....	7
Tabelle 2 - Paketaufbau .....	8
Tabelle 3 - PDU-Header Trap .....	9

## 12. QUELLVERZEICHNIS

- [1] Wikipedia: Netzwerkmanagement; zuletzt besucht am 01.05.2010  
<http://de.wikipedia.org/wiki/Netzwerk-Monitoring>
- [2] Wikipedia: Systems Management; zuletzt besucht am 01.05.2010  
[http://en.wikipedia.org/wiki/Systems\\_management](http://en.wikipedia.org/wiki/Systems_management)
- [3] BTU Cottbus: Stanley Hammer: SNMP Netzwerkmanagement; zuletzt besucht am 04.05.2010  
<http://www-rnks.informatik.tu-cottbus.de/content/unrestricted/teachings/2005/SS/ProseminarInternet/Ausarbeitungen/SNMP.pdf>
- [4] Wikipedia: SNMP; zuletzt besucht am 04.05.2010  
<http://de.wikipedia.org/wiki/Snmp>
- [5] Profinet.ch: Kurzbeschreibung SNMP; zuletzt besucht am 04.05.2010  
<http://www.profinet.felser.ch/technik/SNMP.pdf>
- [6] eigene Unterlagen