Simple Network Management Protocol (SNMP)

*Das **Simple Network Management Protocol** (englisch für "einfaches Netzwerkverwaltungsprotokoll", kurz SNMP), ist ein Netzwerkprotokoll, das von der IETF definiert wurden. Es wurde entwickelt um Netzwerkelemente (Router, Server, Switches, Drucker, Computer usw.) von einer zentralen Managementstation aus überwachen und steuern zu können. Es wird in einem PROFINET IO System zur Verwaltung der Netzwerkinfrastruktur und auch der IO-Controller und IO-Devices verwendet. Zu den Aufgaben des Netzwerkmanagement, die mit SNMP möglich sind, zählen:*

- ☐ *Überwachung von Netzwerkkomponenten.*
- ☐ *Fernsteuerung und Fernkonfiguration von Netzwerkkomponenten.*
- ☐ *Fehlererkennung und Fehlerbenachrichtigung.*

SNMP beschreibt hierbei den Aufbau der Datenpakete, die zwischen den überwachten Stationen und der Managementkonsole übertragen werden und den Kommunikationsablauf. Durch seine Einfachheit hat sich SNMP zum Standard entwickelt, der von den meisten Managementtools unterstützt wird.

Inhaltsverzeichnis

1 Beschreibung

1.1 Funktionsweise

Auf den überwachten Netzwerkelementen muss ein so genannter Agent laufen. Dabei handelt es sich um ein Programm, das die jeweilige Station überwacht und dessen Eigenschaften im Netz verfügbar macht. Managerprogramme können über diese Agenten auf die Stationen zugreifen um Daten abzufragen, Einstellungen vorzunehmen und Aktionen auszulösen.

Für die Kommunikation zwischen den Agenten und den Managern gibt es 6 verschiedene SNMP-Pakete:

GET	zum Anfordern eines Management Datensatzes
GETNEXT	um den nachfolgenden Datensatz abzurufen (um Tabellen zu durchlaufen)
GETBULK	um mehrere Datensätze auf einmal abzurufen, wie z. B. mehrere Reihen einer Tabelle (verfügbar ab SNMPv2)
SET	um einen Datensatz eines Netzelementes zu verändern.
RESPONSE	Antwort auf eines der vorherigen Pakete.
TRAP	unaufgeforderte Nachricht von einem Agenten an den Manager, dass ein Ereignis eingetreten ist.

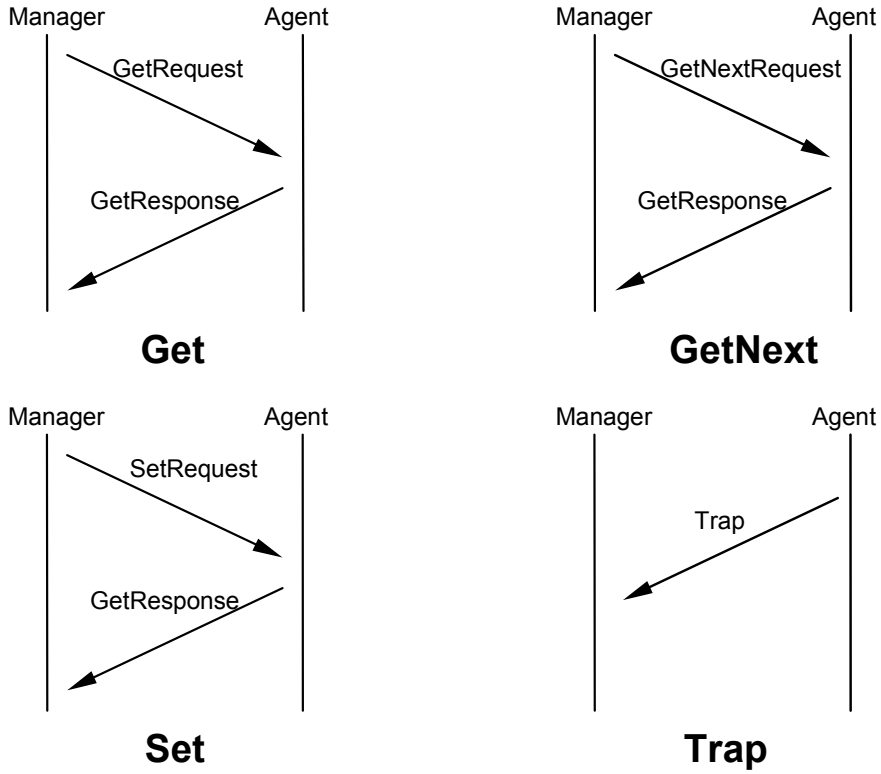

Abbildung 1 Die vier Grundfunktionen

Die drei Get-Pakete (Get, GetNext, GetBulk) können vom Manager zu einem Agenten gesendet werden um Daten über die jeweilige Station anzufordern. Dieser antwortet mit einem Response-Paket, das entweder die angeforderten Daten enthält oder eine Fehlermeldung.

Mit dem Set-Paket kann ein Manager Werte beim Agenten verändern. Damit ist es möglich Einstellungen vorzunehmen oder Aktionen auszulösen. Der Agent bestätigt die Übernahme der Werte ebenfalls mit einem Response-Paket.

Wenn der Agent bei der Überwachung des Systems einen Fehler erkennt, kann er diesen mit Hilfe eines Trap-Paketes unaufgefordert an die Management-Station melden. Diese Pakete werden nicht vom Manager bestätigt. Der Agent kann damit nicht feststellen, ob der Trap beim Manager angekommen ist.

Damit die Netzwerkbelastung gering bleibt wird zum Versenden der Nachrichten das verbindungslose UDP-Protokoll verwendet. Der Agent empfängt dabei die Requests auf dem Port 161, während für den Manager der Port 162 zum Empfangen der Trap-Meldungen vorgeschrieben ist.

1.2 Management Information Base

Die Eigenschaften, die von einem Agenten über die gemanagte Netzwerkkomponente ausgelesen und verändert werden können, die so genannten 'Managed Objects', werden in der MIB (Management Information Base) festgelegt. Der Aufbau der MIB wird in Beschreibungsdateien, die in der abstrakten Beschreibungssprache ASN.1 (Abstract Syntax Notation One) geschrieben sind, definiert. Zu jedem Datum, das vom Agenten abgerufen oder verändert werden kann, werden in diesen Dateien eine Reihe von Informationen angegeben:

- ☐ Name
- ☐ Datentyp
- ☐ Zugriffsberechtigung (read-only, read-write, not-accessible)
- ☐ Status (Mandatory, Optional, Deprecated, Obsolete)
- ☐ Beschreibungstext

Mehrere solche MIBs wurden in RFCs definiert. Besonders hervorzuheben ist hierbei die MIB-2, die in der RFC 1213 definiert wurde und von allen Netzwerkkomponenten unterstützt wird. Neben dieser Standard-MIB existieren eine ganze Reihe von weiteren in RFCs definierten MIBs für verschiedene

Technologien (z. B. ISDN-MIB), Protokolle (z. B. OSPF-MIB) oder Komponenten (z. B. UPS-MIB). Sie enthalten jeweils allgemeine Objekte wie z. B. Portstatus, Router-Id, Ladezustand der Batterie und ähnliches.

Die Informationen der MIB sind in einer Art Baumstruktur organisiert, deren einzelne Zweige entweder durch Nummern oder alternativ durch alphanumerische Bezeichnungen dargestellt werden können. Die MIB-2 ist zum Beispiel unter "iso.org.dod.internet.mgmt.MIB-2" zu finden, das ebenso durch die Zahlenreihe 1.3.6.1.2.1 eindeutig bestimmt ist (1 für "iso", 3 für "org" usw.). Diese aus Punkten und Zahlen bestehende Zeichenkette nennt man OID (Object Identifier). In den MIBs wird dann weiter verzweigt bis zu den einzelnen Daten, die jeweils auch eine eigene OID besitzen und somit eindeutig identifiziert werden können.

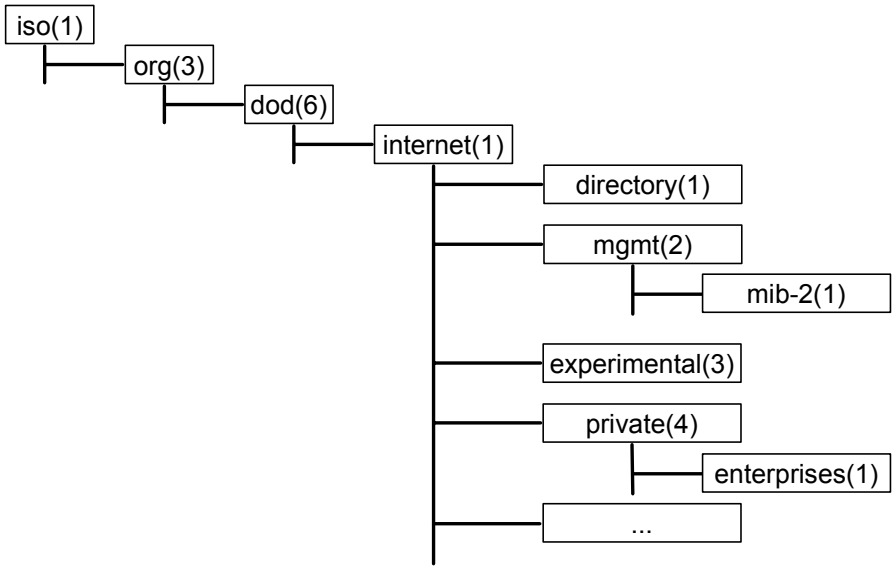

Abbildung 2 OID: iso.org.dod.internet.mgmt.mib-2.system.sysdescr = 1.3.6.1.2.1.1.1

Neben den in den RFCs definierten MIBs kann jeder Hersteller von Soft- oder Hardware eigene MIBs, so genannte private MIBs, definieren, die die speziellen Eigenschaften seines Produktes wiedergeben. Diese werden unter der OID iso(1).org(3).dod(6).internet(1).private(4).enterprises(1) bei der IANA registriert. Mittlerweile sind unter dieser OID mehrere tausend Firmen registriert (siehe private enterprise numbers). Ist einer OID einmal ein Objekt zugeordnet, so darf sich die Bedeutung dieser OID - sofern vom Gerät (dem SNMP-Agenten) unterstützt - nicht wieder ändern. Es darf auch keine Überschneidungen geben.

Mit Hilfe der MIB-Dateien sind die Managementprogramme in der Lage den hierarchischen Aufbau der Daten beim Agenten darzustellen und sie abzufragen, ohne dass der Benutzer die OID selber kennen muss.

2 Paketaufbau

Die meisten SNMP-Pakete sind identisch aufgebaut. Lediglich bei Trap-Meldungen werden im PDU-Header teilweise andere Informationen versendet.

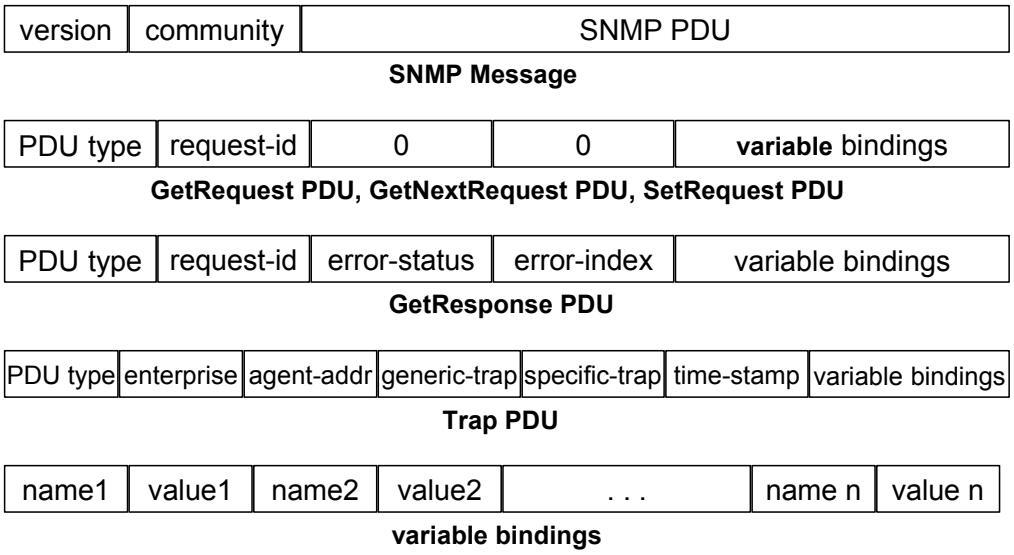

Abbildung 3 Die Paketformate

2.1 SNMP-Paket Header

Im Header wird die Gesamtgröße des Pakets, die Versionsnummer (SNMPv1, SNMPv2 oder SNMPv3) und der Community Name übertragen. Durch Zuweisen von Communitys sollten Zugriffsrechte vergeben werden. In den meisten Fällen wurde aber als Community Name „public“ gewählt für Lesezugriff und „private“ für Lese und Schreibzugriff. Sicherheit kann aber auch durch andere Namen nicht erreicht werden, da der Community Name im Klartext übertragen wird und von jedem im Netz mitgehört werden kann.

2.1.1 PDU-Header (Nicht-Trap-Pakete)

Im ersten Teil des PDU-Headers wird die Art des SNMP-Paketes und die Größe der PDU übertragen. Der Aufbau des zweiten Teils hängt von der Art des SNMP-Paketes ab.

Damit Antwortpakete den vorherigen Anfragen zugeordnet werden können gibt es die Request ID, welche bei Anfrage und Antwort identisch sind. Damit ist es möglich mehrere Anfragen zu verschicken und die Antworten wieder richtig zu sortieren.

Der Fehlerstatus und -Index wird dazu verwendet bei Antwortpaketen mitzuteilen warum eine Anfrage nicht bearbeitet werden konnte. Solange kein Fehler auftritt sind die beiden Felder mit dem Wert Null belegt. Im Fehlerfall gibt der Fehlerindex an beim wievielten Datensatz der Fehler auftrat. Mit dem Fehlerstatus wird der Grund des Fehlers angegeben. Der Fehlerstatus kann bei SNMPv1 einen von 6 möglichen Werten haben:

- ☐ Kein Fehler
- ☐ Paket ist zu groß zum Versenden
- ☐ Die OID wird nicht unterstützt
- ☐ Falscher Datentyp oder Wert (nur als Antwort auf Set-Pakete möglich)
- ☐ Nur Lesezugriff (nur als Antwort auf Set-Pakete möglich)
- ☐ Unbekannter Generierungsfehler

2.1.2 PDU-Header (Trap-Pakete)

Die ersten beiden Felder des PDU-Header sind bei Traps identisch zu anderen SNMP-Paketen. Das Feld Pakettyp gibt an, dass es sich um einen Trap handelt. Ebenfalls wird hier die Größe der PDU angegeben. Im zweiten Teil werden andere Werte übertragen, die nur bei Traps benötigt werden.

Zum Erkennen von wem die Nachricht kommt wird eine OID des Gerätes mitgeschickt, dass den Trap generiert hat und die IP-Adresse des Absenders. Die OID gibt an um was für ein Gerät es sich handelt. Das ist wichtig zu wissen, wenn es sich um einen firmenspezifischen Trap handelt, die nur für diesen Gerätetyp gilt.

Danach folgt die allgemeine TrapID. Es gibt 7 mögliche allgemeine TrapIDs:

- ☐ Kaltstart
- ☐ Warmstart
- ☐ Link Down
- ☐ Link Up
- ☐ Authentifizierungsfehler
- ☐ EGP-Nachbar verloren
- ☐ firmenspezifisch

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

Da es möglich ist, dass Trap-Pakete nicht in der Reihenfolge eintreffen wie sie versendet wurden gibt es zusätzlich noch eine Zeitangabe, die auf hunderstel Sekunden genau angibt, wie lang der SNMP-Agent gelaufen ist, bis das Trap-Ereignis auftrat. Dadurch ist es möglich die Trap-Ereignisse in die zeitlich richtige Reihenfolge zu bringen.

2.1.3 PDU-Body

Im PDU-Body werden die eigentlichen Werte übertragen. Jeder Wert wird in einer sogenannten Variable Binding übertragen: Zu einer Variable Binding gehören deren OID, der Datentyp und der Wert selber.

Es gibt keine Vorgabe wie viele Variable Bindings im PDU-Body mitgeschickt werden dürfen. Es ist also möglich mehrere Werte mit einem Get-Befehl abzufragen. Wenn aber das Antwortpaket dabei zu groß wird, kann es passieren, dass die entsprechende Fehlermeldung im Antwortpaket zurück geschickt wird.

Bei Traps ist es auch möglich, dass keine Variable Bindings mitgeschickt werden. In dem Fall wird die TrapID als ausreichende Information angesehen.

Im SNMP-Paket ist keine Angabe vorgesehen, welche die Anzahl an mitgeschickten Variable Bindings angibt. Das lässt sich nur über die Größenangabe des PDU-Bodys und der Größenangabe der einzelnen Variable Bindings heraus finden.

3 Ethereal

3.1 Display Filter

Um nur SNMP Telegramme dazustellen kann der Filter „snmp“ verwendet werden.

3.2 Capture Filter

Um nur SNMP Telegramme aufzuzeichnen ist der Filter „udp port 161 or udp port 162“ geeignet.

4 Quellen und Literatur

Diese Kurzbeschreibung wurde unter der Verwendung der folgenden Unterlagen zusammengestellt:

[SNMP 1] Wikipedia: "http://de.wikipedia.org/wiki/Simple_Network_Management_Protocol"

Weitere hilfsreiche Programme findet man hier:

IANA Anmelden einer Firmen-OID

NET-SNMP Programme zum Auslesen und Anzeigen von SNMP-Daten

RMON-MIB MIB-Definitionsdatei für RMON

SNMPView Kostenloser SNMP Monitor für Windows

MIB-Browser Kostenloser MIB-Browser, java-basierend