Simple Network Management Protocol

IT-Technik Netzwerkgrundlagen

Sebastian Meisel

26. Januar 2023

1 Simple Network Management Protocol (SNMP)

SNMP ist ein weitverbreitetes, weil einfaches Protokoll zur

- Überwachung von Netzwerkgeräten
- Fehlererkennung / ~benachrichtigung
- Remotekonfiguration / ~steuerung

1.1 Versionen

- **SNMPv1** (RFC 1155-1157): Das ursprüngliche Protokoll wird nicht benutzt
- **SNMPv2**: GetBulk-Befehl zum Abruf mehrerer *Tabellen* mit einem Befehl.
  - **(SNMPv2p)** (RFC 1441-1447): Verschlüsselung des *Community Strings*. **deprecated**
  - **(SNMPv2u)** (RFC 1909-1910): Authentifizierung durch Benutzernamen. **deprecated**
  - **SNMPv2c** (RFC 1901-1908): Keine Sicherheitsfunktionen.
- **SNMPv3** (RFC 3410-3418) : Authentifizierung und Verschlüsselung

Da Protokoll hat sich vor allem wegen seiner Einfachen Nutzung durchgesetzt. Versuche die Sicherheit des Protokolls zu erhöhen sind immer mit einer erhöhten Komplexität verbunden.
Das führt bis heute dazu, dass Verschlüsselung und Authentifizierung als minimale Sicherheitsfunktionen wenig Verbreitung finden. **SNMPv2p/u** sind gescheitert. **SNMPv3** wird zwar von den meisten neueren Geräten unterstützt aber zu wenig genutzt.
Böse Zungen meinen darum das Akronym des Protokolls stehe für:
Security is not my problem.
-**S** icherheit ist -**N** icht -**M** ein -**P** roblem.

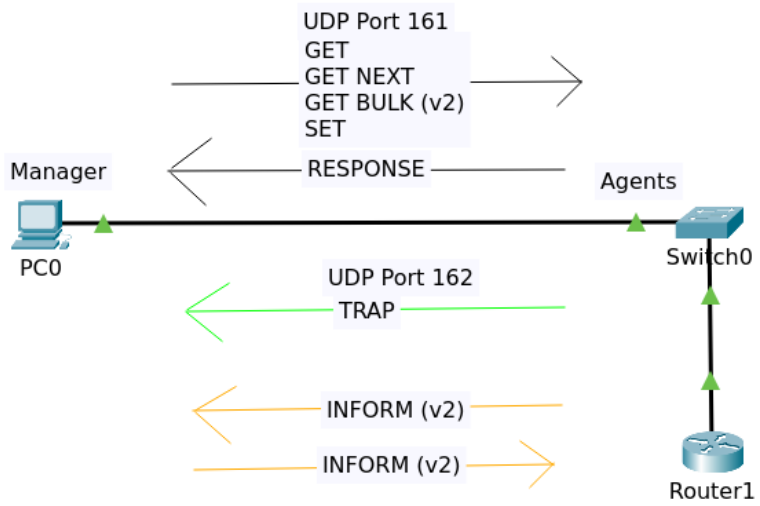

Abbildung 1: Funktionen des SNMP

2 Funktionsweise

Auf jedem Netzwerkgerät läuft ein **SNMP-Agent**, der:

1. vom **SNMP-Manager** auf einem zentralen Rechner mit einem der folgenden Befehle angesprochen werden kann:
   - GET: fragt Werte aus der Management Information Base (MIB) ab.
   - GET: fragt den nächsten Eintrag aus derselben Tabelle ab.
   - GET-BULK: (neu"ab Version 2) fragt alle Einträge einer Tabelle ab.
   - SET: wenn Schreibzugriff erlaubt ist, setzt dieser Befehl den Wert für einen Eintrag in **MIB**.
2. selbstständig Nachrichten an den **SNMP-Manager** sendet.

2.1 Management Information Base (MIB)

Die **MIB** ist eine Art simpler Datenbank in der Informationen, wie die IP oder der Status von Netzwerkschnittstellen von Netzwerkgeräten, wie Routern oder Switches gespeichert sind.
Diese Informationen nennt man **Managed Objects**. Diese sind in einer **standardisierten** Baumstruktur gespeichert. Jedes **Managed Object** kann über einen **Object Identifier (OID)** identifiziert werden. Dies ist eine Zahlenkette (z. B. .1.3.6.1.2.1.2.2.1.7) der ein Name zugeordnet ist (z. B. .iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifAdminStatus).
Der Befehl `GET-BULK .1.3.6.1.2.1.2.2.1.7` ruft den Status (Up/Down) aller Netzwerkschnittstellen eines Netzwerkgerätes ab. Der Befehl `GET .1.3.6.1.2.1.2.2.1.7` hingegen nur den der 1. Netzwerkschnittstelle. Die weiteren könnten dann nacheinander mit `GET-NEXT`

`.1.3.6.1.2.1.2.2.1.7` abgerufen werden. Mit `SET .1.3.6.1.2.1.2.2.1.7 up` könnte eine Netzwerkschnittstelle aktiviert werden (wenn der Schreibzugriff aktiviert ist).

2.2 Trap-Nachrichten

Folgende Nachrichten kann ein **SNMP-Agent** selbstständig senden:

Bedeutung	Nachricht	Wert
Kaltstart	caldStart	0
Warmstart	warmStart	1
Verbindung unterbrochen	linkDown	2
Verbindung hergestellt	linkUp	3
Authentifiierungsfehler	authentificationFailure	4
EPG-Nachbar verloren	epgNeighborLoss	5
firmenspezifisch	enterpriseSpecific	6