SNMP
Simpel? – Nur Mut Paula!

Ein Protokoll, das ebenso alt wie unterschätzt ist und ebenso unberechtigt gerügt wie qualifiziert verachtet wird.

Linuxwochen Eisenstadt
5. April 2025
Goesta Smekal

Überblick

- **Archeologie**
  Ursprünge, Entwicklung und Irrwege eines gerne unterschätzten Protokolls
- **Architektur**
  Artefakte, Komponenten, Nachrichten und Begriffe
- **Anachronismen**
  Fallstricke, Leichen im Keller und übliche Missverständnisse
- **Anwendung**
  was man in der Praxis damit tun kann

Wer bin ich?

... und warum tue ich euch das an?

Goesta Smekal
Jahrgang 1972
Computer seit 1986
Linux seit ~1995
LUGA seit 2007
Beruf: IT-Verantwortlicher in einem Verlag

Fragen, die nicht beantwortet werden

- Warum hat das Gerät XY keine SNMP Unterstützung?
- Was hältst Du von der proprietären Management-Lösung des Herstellers ...?
- Wie bekomme ich Zugriff auf meinen Router zu Hause?
- Hast Du kein moderneres Thema gefunden? Etwas mit KI?
- Warum schauen Deine Folien wie Kleinbild-Negative aus?

Archeologie :: Ursprünge

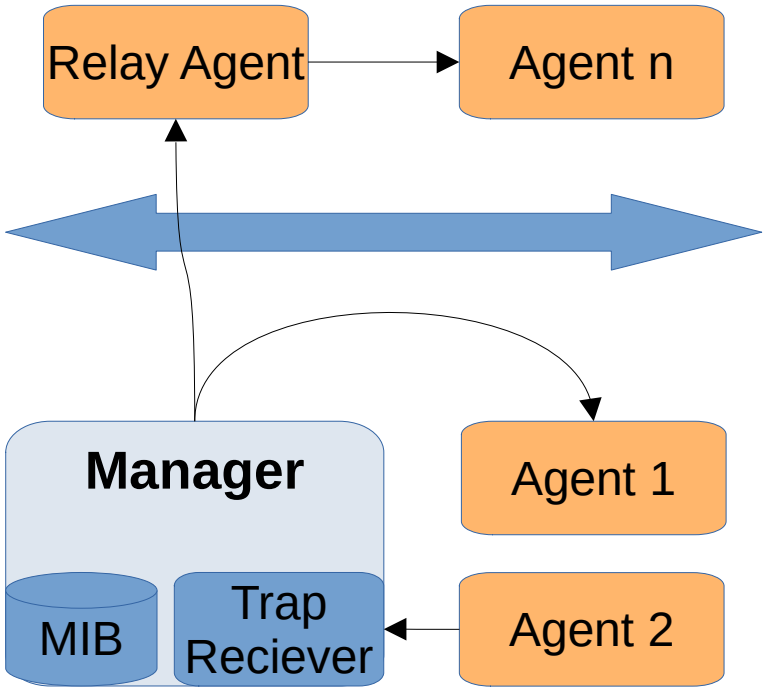
- Nachfolger des SGMP (Simple Gateway Monitoring Protocol)
- SNMPv1 spezifiziert in RFC 1067, 1988
- Ziele:
  - einheitliches Protokoll um Netzwerkdevices zu verwalten
  - einfach zu implementieren und in möglichst allen Geräten umgesetzt
- Umfeld
  - Netzwerke sind selten, überwiegend Point to Point, physischer Zugriff fällt auf
  - Ethernet war recht neu (BNC mit 2Mbps, 10BaseT kommt 1991)
  - Vertrauen dominiert
  - Geräte haben wenig Rechenleistung und wichtigere Aufgaben (als z.B. Crypto)
- „aktuell“: SNMPv3, 2002 https://datatracker.ietf.org/doc/html/rfc3411

Archeologie :: Versionen und Abwege

- 1988 SNMPv1
  - plaintext
  - keine Security (Community != Passwort)
- 1992 Secure SNMP, wurde nie umgesetzt
- 1993 SNMPv2 – nicht rückwärts kompatibel
  - … gleich drei davon:
    - SNMPv2p („party based", verschlüsselt community, pre shared secret)
    - SNMPv2u („user based" security, als zu komplex empfunden)
    - SNMPv2c = v1 mit optionaler Security – de facto Standard, aber ohne Security
  - 64Bit Counter (32Bit laufen bei 10Gbps < 1 min über)
  - neue RequestTypes: GetNext, GetBulk
  - Relay Agent
- 2002 SNMPv3
  - Security ernsthaft umgesetzt
  - nutzt halt niemand

Architektur :: Terminologie

- "managed device" – "agent"
- „relay agent“
- "network management station" - "manager"
- "management information base" - MIB
- "object identifier" - OID
- Get, Set, Trap, InformRequest
- Community (read, write, trap)



Architektur :: Netzwerk

- OSI Layer 7, Application Layer
- Transportprotokoll: UDP (sowie IPX aka Novell und AppleTalk)
  - Ports 161 (Get/Set Request/Response) und 162 (Traps)
    (oder 10161, 10162 bei TLS/DTLS)
  - gleich für alle Versionen v1, v2<x>, v3
- Request Types: Get, Set, GetNext, GetBulk, Response, Trap, Inform
- Paketaufbau
  - Paket Header enthält
    - Version
    - Community Name
  - PDU Header enthält
    - Get*/Set Request
      - Pakettyp, RequestID, Fehlerstatus, Fehlerindex
    - Trap
      - OID, Sender-IP, allg. TrapID, Firmen-TrapID, Timestamp (1/100s seit Agent Start)
  - PDU Data
    - VariableBinding1 … VariableBindingn

Architektur :: Datentypen

- IpAddress (IPv4, ab SMIv2 auch IPv6, 1999)
- Counter
  - 64bit ab v2c (laufen nach 133a bei 1,6Tbps)
  - z.B.: Packets total, Errors total, Pages printed, ...
- Gauge
  - momentaner Wert (32Bit)
  - z.B.: LinkSpeed, Memory used, Toner level, ...
- Opaque
  - Agent spezifisch
  - z.B.: Texte, Status, ...
- Table
  - komplexe Darstellung mehrerer Entitäten und deren Werte
  - z.B.: IfTable (ifIndex, ifDescr, ifType, ifMtu, ifSpeed, ifPhysAddress, ifAdminStatus, ifOperStatus, ifLastChange, ifInOctets …)
- TimeTicks
  - 1/100s seit Systemstart (wer braucht schon synchronisierte Uhren?)

Architektur :: MIB

- Management Information Base
- formuliert in ASN.1, nach SMIv2 (RFC 2578)
- Definiert die Datenstruktur für Agent-Typen
  - teilweise Standardisiert (IETF, IEEE)
    z.B.: https://netsnmp.org/mibs
  - überwiegend proprietär
    oft(!) auf Hersteller Websites zu finden
- Elemente sind hierarchisch organisiert über OIDs
  - OIDs sind numerisch und beginnen mit .1.3.6.1
    aka: iso.org.dod.internet
  - Abenteuer beginnen ab .1.3.6.1.4.1.xxx („enterprises“)
  - eigegen Zweig reservieren (PEN – private enterprise nr.):
    https://www.iana.org/assignments/enterprise-numbers

Architektur :: MIBs :: Beispiele

```
NET-SNMP-MIB DEFINITIONS ::= BEGIN
-- Top-level infrastructure of the Net-SNMP project enterprise MIB tree
IMPORTS
    MODULE-IDENTITY, enterprises FROM SNMPv2-SMI;
netSnmp MODULE-IDENTITY
    LAST-UPDATED "200201300000Z"
    ORGANIZATION "www.net-snmp.org"
    CONTACT-INFO
    "postal:   Wes Hardaker
          email:    net-snmp-coders@lists.sourceforge.net"
    DESCRIPTION
[...]
--  Net-SNMP enterprise-specific management objects
netSnmpObjects              OBJECT IDENTIFIER ::= {netSnmp 1}
-- netSnmpExamples             OBJECT IDENTIFIER ::= {netSnmp 2}
netSnmpEnumerations         OBJECT IDENTIFIER ::= {netSnmp 3}
netSnmpModuleIDs            OBJECT IDENTIFIER ::= {netSnmpEnumerations 1}
netSnmpAgentOIDs            OBJECT IDENTIFIER ::= {netSnmpEnumerations 2}
netSnmpDomains              OBJECT IDENTIFIER ::= {netSnmpEnumerations 3}
netSnmpExperimental         OBJECT IDENTIFIER ::= {netSnmp 9999}
```

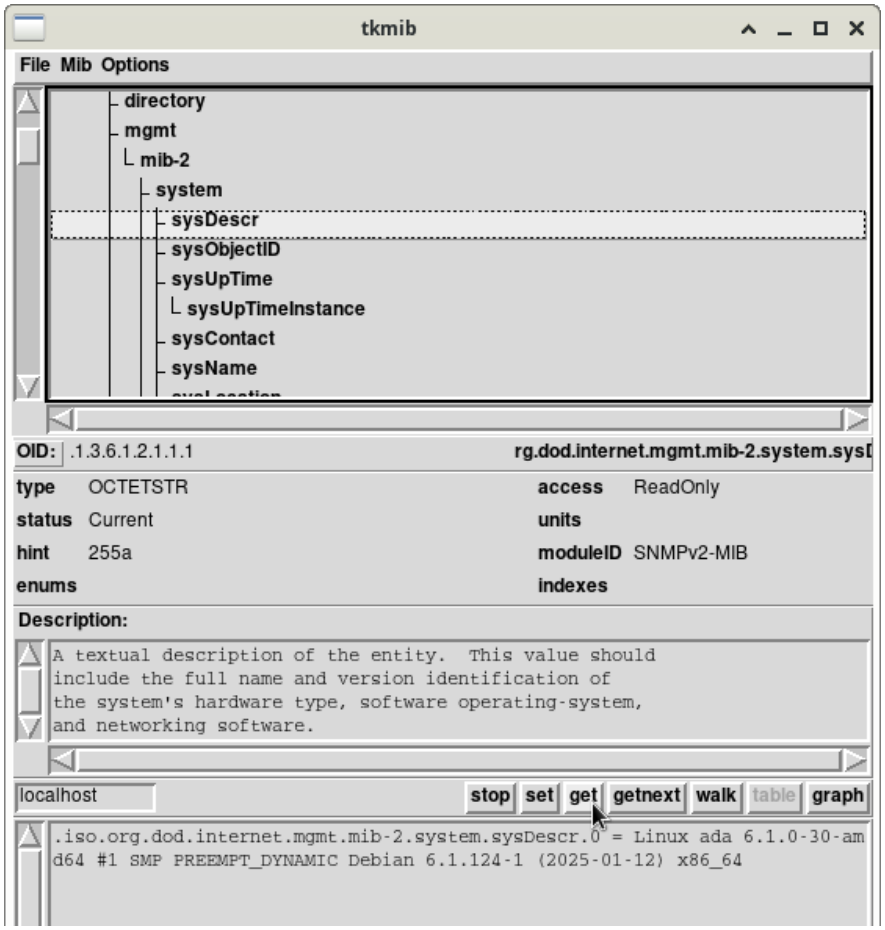
Architektur :: MIBs :: Beispiele

aus NET-SNMP-TC (text conventions):

```
-- SystemNET-SNMP-TC DEFINITIONS ::= BEGIN
--
-- Textual conventions and enumerations for the Net-SNMP project
--

IMPORTS

    netSnmpModuleIDs, netSnmpAgentOIDs, netSnmpDomains FROM NET-SNMP-MIB
    MODULE-IDENTITY, Opaque FROM SNMPv2-SMI
    TEXTUAL-CONVENTION FROM SNMPv2-TC;
[...]

--- Object ID values
--
--      XXX - do we want to distinguish between O/S versions ?
--      (as is currently done with HP-UX)
--

hpux9             OBJECT IDENTIFIER ::= { netSnmpAgentOIDs 1 }
[…]
openbsd           OBJECT IDENTIFIER ::= { netSnmpAgentOIDs 12 }
win32             OBJECT IDENTIFIER ::= { netSnmpAgentOIDs 13 } -- unlucky
hpux11            OBJECT IDENTIFIER ::= { netSnmpAgentOIDs 14 }
[...]
```

Architektur :: MIB :: Praxis

```
•
└── SNMPv2-MIB(.1.3.6.1.2.1)
    └── system(.1)
        ├── sysDescr (.1)
        ├── sysObjectID (.2)
        ├── sysUpTime (.3)
        ├── sysName (.5)
        ├── sysContact (.4)
        ├── sysLocation (.6)
        ├── sysServices (.7)
        ├── sysORLastChange (.8)
        └── sysORTable (.9)
            └── sysOREntry (.1)
                ├── sysORIndex (.1)
                ├── sysORID (.2)
                ├── sysORDescr (.3)
                └── sysORUpTime (.4)
```



Anachronismen :: Kritik

Security is **N**ot **M**y **P**roblem

- Community != Password
- SNMPv1 = plaintext
- Secure SNMP (1992) nie umgesetzt
- SNMPv2p (verschlüsselt community)
- SNMPv2u (user based security)
- SNMPv2c (1993) = v1 mit optionaler Security
- out of band Monitoring (Management VLAN)

Probleme in der Praxis

- SNMPv1 und v2c sind inkompatibel
- MIBs sind manchmal Geheimnisse
- Auslesen "großer" Devices ist komplex, oft mit wenig Prio am Device und dadurch langsam
- Implementierung oft schlampig und inkonsistent

Anwendungen :: wozu?

- Monitoring – agentless … kind of
  - Link Auslastung, Status, Fehler, ...
  - Systemparameter (CPU, Memory, Temperatur, …)
- Inventarisierung
  - Gerätetypen, Seriennummern, Firmware, …
  - Topologie (über MAC Adressen pro Link)
  - Scan nach neuen/geänderten Geräten
- Konfiguration
  - Macht das wirklich jemand über SNMP?
- IoT
  - geringer Ressourcenverbrauch
  - über custom-OIDs vielfältig erweiterbar

Anwendung :: Tools

- Net-SNMP https://netsnmp.org
  - tkmib (GUI Tool, known Bugs seit ...)
  - snmpwalk
  - snmptable
- smitools, smistrip (manipulate and extract MIB fom RFCs)
- snmptrapd, snmptt (collect and process traps)

- LibreNMS (Observium), NeDi
- Torrus, Cacti, MRTG, …
- ntop

Anwendungen :: Praxis

Debian Pakete:

- snmp - Tools für den Manager
- snmpd - der Agent
- libsnmp-base - RFC MIBs
- libsmi2-common - nützliche Tools
- snmp-mibs-downloader - proprietäre MIBs (non-free section)

optional:

- snmptrapd – der Trap Collector
- snmptt – Trap Translator
- tkmib – GUI SNMP Manager

Anwendungen :: snmpd

/etc/snmp/snmpd.conf:

```
sysLocation  something meaningful
sysContact   me@example.com
agentaddress 127.0.0.1,[::1] # add interfaces as needed
# access based on OID
view   systemonly  included   .1.3.6.1.2.1.1 #
SystemInformation
view   systemonly  included   .1.3.6.1.2.1.2 # Interface MIB
view   systemonly  included   .1.3.6.1.2.1.25.1 # ifTable

rocommunity  public default -V systemonly
rocommunity6 public default -V systemonly
```

/etc/snmp/snmp.conf

```
# mibs : # comment out to allow loading proprietary MIBs
```

Anwendungen :: snmpd :: erweitern

- Scripts oder Programme lassen sich einfach einbinden
- custom OID sehr zu empfehlen
- Security!

in /etc/snmp/snmpd.conf:

```
# custom stuff
rocommunity custom
extend test /usr/bin/uptime
```

Abfrage:

```
goesta@ada:~$ snmpwalk -v 2c -c custom localhost nsExtendOutput1
NET-SNMP-EXTEND-MIB::nsExtendOutput1Line."test" = STRING:  17:03:16 up
234 days, 6:28,  2 users,  load average: 0.08, 0.03, 0.01
NET-SNMP-EXTEND-MIB::nsExtendOutputFull."test" = STRING:  17:03:16 up
234 days, 6:28,  2 users,  load average: 0.08, 0.03, 0.01
NET-SNMP-EXTEND-MIB::nsExtendOutNumLines."test" = INTEGER: 1
NET-SNMP-EXTEND-MIB::nsExtendResult."test" = INTEGER: 0
```

Anwendungen :: snmptrapd

- Trap-MIB passend zur Quelle erforderlich
- direkt durch snmptrapd behandeln lassen:

in /etc/snmp/snmptrapd.conf:

```
authCommunity log,execute,net public
## send mail when get linkDown
traphandle .1.3.6.1.6.3.1.1.5.3 /usr/bin/traptoemail -
s smtp.example.org foobar@example.org
```

- alternativ durch snmptt verarbeiten
  - kann Trap Messages umschreiben
  - kann anhand von Bedingungen Aktionen auslösen

Quellen

https://netsnmp.org/

https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

https://datatracker.ietf.org/doc/html/rfc3411

https://wiki.debian.org/SNMP

https://www.net-snmp.org/wiki/index.php/Tutorials

https://www.net-snmp.org/wiki/index.php/Tut:Extending_snmpd_using_shell_scripts