zurück

SNMP – Grundlagen

SNMP (**Simple Network Management Protocol**) ist ein Netzwerkprotokoll zur Überwachung, Verwaltung und Steuerung von Netzwerkgeräten.
Es wird auf Routern, Switches, Firewalls, Servern, Druckern, NAS-Systemen und vielen IoT-Geräten eingesetzt.

Warum SNMP?

Mit SNMP kann man:

- Gerätestatus abfragen (Online/Offline)
- CPU-, RAM- und Interface-Auslastung überwachen
- Temperatur, Lüfter, Stromversorgung prüfen
- Ports ein-/ausschalten (Managed Switch)
- Logs sammeln
- Warnungen erhalten (SNMP-Traps)

Es ist das Rückgrat vieler Monitoring-Systeme wie:

- Zabbix
- Icinga
- Nagios
- LibreNMS
- PRTG

SNMP Architektur

Es gibt zwei Rollen:

- **SNMP-Agent** → läuft auf dem Gerät (Switch, Server)
- **SNMP-Manager** → Monitoring-System, das Daten abfragt

ASCII:

```
[ Manager ] ↔ [ Agent auf Switch/Router ]
```

SNMP-Versionen

Version	Sicherheit	Beschreibung
———	———	———
SNMPv1	gering	klartext, kaum Schutz
SNMPv2c	mittel	klartext, aber schneller & erweitert
SNMPv3	hoch	Verschlüsselung, Authentifizierung

Empfehlung:
Nur SNMPv3 in produktiven Netzen benutzen.

Kommunities (Community Strings)

SNMPv1/v2c verwenden „Community Strings“ als einfache Passwörter.

Beispiele:

- `public` (lesen)
- `private` (schreiben)

Gefährlich:

- werden **klartext** übertragen
- häufig falsch konfiguriert
- beliebtes Angriffsziel

Mit SNMPv3 wird dieses Problem gelöst.

OIDs – Objekt-Identifikatoren

Jeder Wert in SNMP hat eine eindeutige Nummer, die **OID** genannt wird.

Beispiel:

```
1.3.6.1.2.1.1.1.0  → System-Info
1.3.6.1.2.1.2.2.1.10  → Interface RX Octets
```

Sie bilden einen Baum:

ASCII:

```
1.3 (ISO)
 └── 6 (DoD)
     └── 1 (Internet)
         └── 2 (Mgmt)
             └── 1 (MIB-2)
```

MIB – Management Information Base

Die MIB ist die „Wörterliste“ aller verfügbaren SNMP-Objekte.

Beispiele:

- **MIB-II** (Standardwerte)
- **HOST-RESOURCES-MIB**
- **IF-MIB** (Interfaces)
- herstellerspezifische MIBs (Cisco, HP, Mikrotik)

Wichtige Befehle (Linux)

SNMP-GET (Wert abfragen)

```
snmpget -v2c -c public 192.168.1.10 1.3.6.1.2.1.1.1.0
```

SNMP-WALK (kompletter Baum)

```
snmpwalk -v2c -c public 192.168.1.10
```

SNMPv3 Beispiel

```
snmpwalk -v3 -u admin -l authPriv \
-a SHA -A Passwort123 \
-x AES -X Geheim123 \
192.168.1.10
```

SNMP-Traps

Traps sind aktive Nachrichten, die ein Gerät **proaktiv** an den Manager sendet.

Beispiele:

- Lüfterfehler
- Port down/up
- Temperatur zu hoch
- CPU über 90%

ASCII:

```
[ Switch ] ---> "Trap: Port 5 down!" ---> [ Manager ]
```

Beispiel: Monitoring eines Switches

Über SNMP kannst du abfragen:

- Interface-Status (up/down)
- Speed (1G/10G)
- Errors, CRC, Drops
- Temperatur
- Uptime
- VLAN-Mitgliedschaften (per Hersteller-MIB)

Sicherheitsaspekte

SNMPv1/v2c:

- keine Verschlüsselung
- Passwörter (Community Strings) im Klartext
- anfällig für Abhören & Manipulation

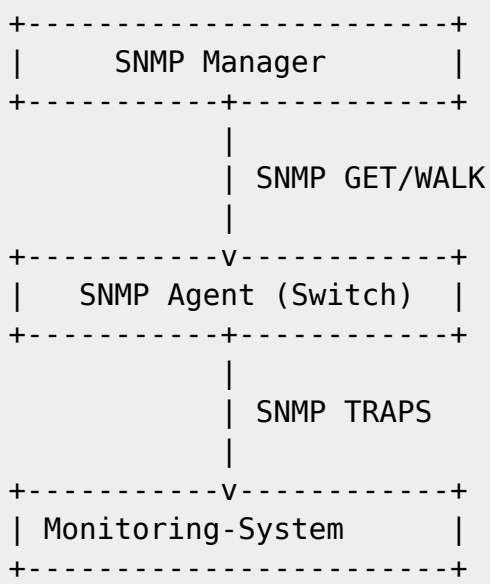
SNMPv3:

- Authentifizierung (SHA)
- Verschlüsselung (AES)
- starke Sicherheit

Best Practices

- SNMPv3, niemals v1/v2c für kritische Systeme
- Community Strings NICHT „public/private“
- nur Management-VLAN für SNMP zulassen
- Zugriff per ACL auf Monitoring-Server beschränken
- nur notwendige MIBs aktivieren
- Traps testen und Logging aktiv halten

ASCII-Übersichtsdiagramm



Zusammenfassung

- SNMP = Netzwerkmanagement-Protokoll
- Agent ↔ Manager Modell
- v1/v2c = unsicher, v3 = sicher
- nutzt OIDs, MIBs, GET, WALK, TRAPS
- essentiell für Überwachung von Switches, Routern, Servern, NAS, IoT
- nur im Management-VLAN und mit SNMPv3 nutzen