SNMP

Der vergessene Klassiker

Dr. Michael Schwartzkopff

Der Aufbau des Seminars

- Motivation für Netzwerk Management
- Grundlagen für SNMP (SMI, MIB und SNMP)
- SNMPv1
- `net-snmp`: Ein Agent mit Erweiterungen
- `net-snmp`: Die Kommandozeile
- Standard-MIBs von `net-snmp`
- Traps
- SNMPv3
- Netzwerk Management Systeme

SNMP: Teilnehmer im Netz

- Üblich ist Client/Server-Kommunikation im Netz.
- Bei SNMP heißen die Teilnehmer anders:
  - Der *Agent* ist der Teil, der die Informationen zur Verfügung stellt. Dieser Teil ist auf dem verwalteten Rechner installiert.
  - Der *Manager* sammelt die Informationen und wertet sie aus.
- Es gibt zwei Wege für die Kommunikation:
  - Der Manager fragt den Agenten nach Informationen (`get`).
  - Der Agent informiert den Manager über Ereignisse (`traps`).

SNMPv1 – Das Protokoll

- Folgende Nachrichten sind definiert:
  - `GetRequest`: Der Manager fragt nach einer Information.
  - `GetNextRequest`: Der Manager fragt nach der nächsten Information.
  - `GetResponse`: Der Agent stellt die angefragte Information zur Verfügung.
  - `SetRequest`: Der Manager schreibt Informationen auf den Agenten.
  - `Trap`: Der Agent informiert den Manager über Ereignisse.

SNMPv1 Paket

- Version: SNMP – Version. Bei v1 ist das „0“
- Community String geht in Klartext über die Leitung!
- SNMP PDU: Die Informationen.

SNMPv1 PDU

- Request – ID identifiziert die Anfrage / Antwort
- Error: Der Agent kann Fehlercodes senden.
- Error Index: Wo genau ist der Fehler aufgetreten?
- Varbind List: Eine Sequenz von Varbinds (Typ und Wert)

Varbind List

- Object Identifier
- Wert
  - Ist bei der Anfrage NULL. Der Agent setzt den Wert in der Antwort.

SNMPv3

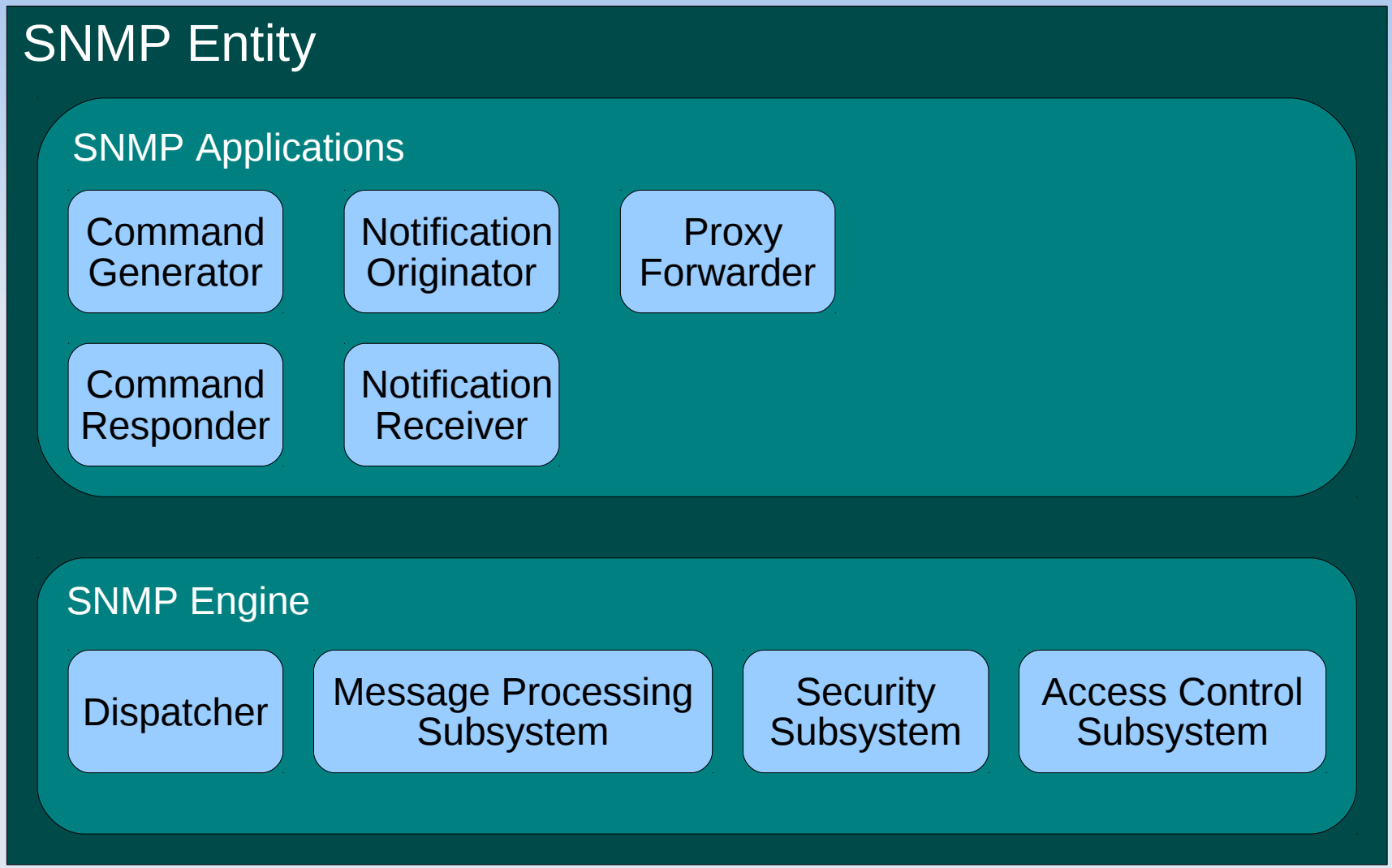
Warum SNMPv3?

- Die verschiedenen Versionen 2 lösten unterschiedliche Probleme.
- SNMPv3 bietet eine generelle Lösung, die besonderen Werte auf Sicherheit und mögliche zukünftige Erweiterungen legt.
- Erst mit SNMPv3 gibt es eine Lösung, die
  - Verschlüsselung,
  - Authentifizierung und
  - Autorisierung bietet.
- SNMPv3 ist inzwischen alleine gültiger Standard der IETF!

Eine SNMPv3 - Einheit

- SNMPv3 spricht nicht mehr von Agent und Manager. Vielmehr werden „Einheiten“ definiert.
- Die Definition von SNMPv3 ist *modular*. Deshalb integrieren v1 und v2c in den Rahmen von v3.
- Die Modularität erlaubt auch zukünftige Erweiterungen.
  - Z.B. kann ein neuer Algorithmus zur Verschlüsselung problemlos integriert werden.
- Die Arbeit machen sog. Applikationen. Je nach Aufgabe der Einheit kommen unterschiedliche Applikationen zum Einsatz.

Modulare Architektur



Die Maschine

- Der *Dispatcher* erhält und versendet SNMP – Nachrichten. Er reicht die Daten ans Message Processing weiter.
- Das *Message Processing* besteht aus Modulen, die die Nachrichten erzeugen oder verarbeiten. Es gibt z. B. Module für v1, v2 oder v3 Requests.
- Das *Security Subsystem* authentifiziert oder verschlüsselt Nachrichten. Es gibt ein COMMUNITY (v1, v2c) und ein User Based Security Model (USM, v3).
- Das *Acces Control Subsystem* autorisiert Zugriffe auf Teile der MIBs (View Based Access Control Model, VACM).

Die Applikationen

- Der *Command Generator* erzeugt get, getnext und getbulk request sowie set requests. Er verarbeitet auch die Antworten. Dieses Modul ist zum Beispiel in Mangern / CLI aktiv.
- Der *Command Resonder* erzeugt Antworten auf Requests. Dieses Modul ist in Agenten aktiv.
- *Notification Originator* und *Receiver* erzeugen bzw. verarbeiten Notifications.
- Zusätzliche Applikationen haben im Rahmen von SNMPv3 auch noch Platz.

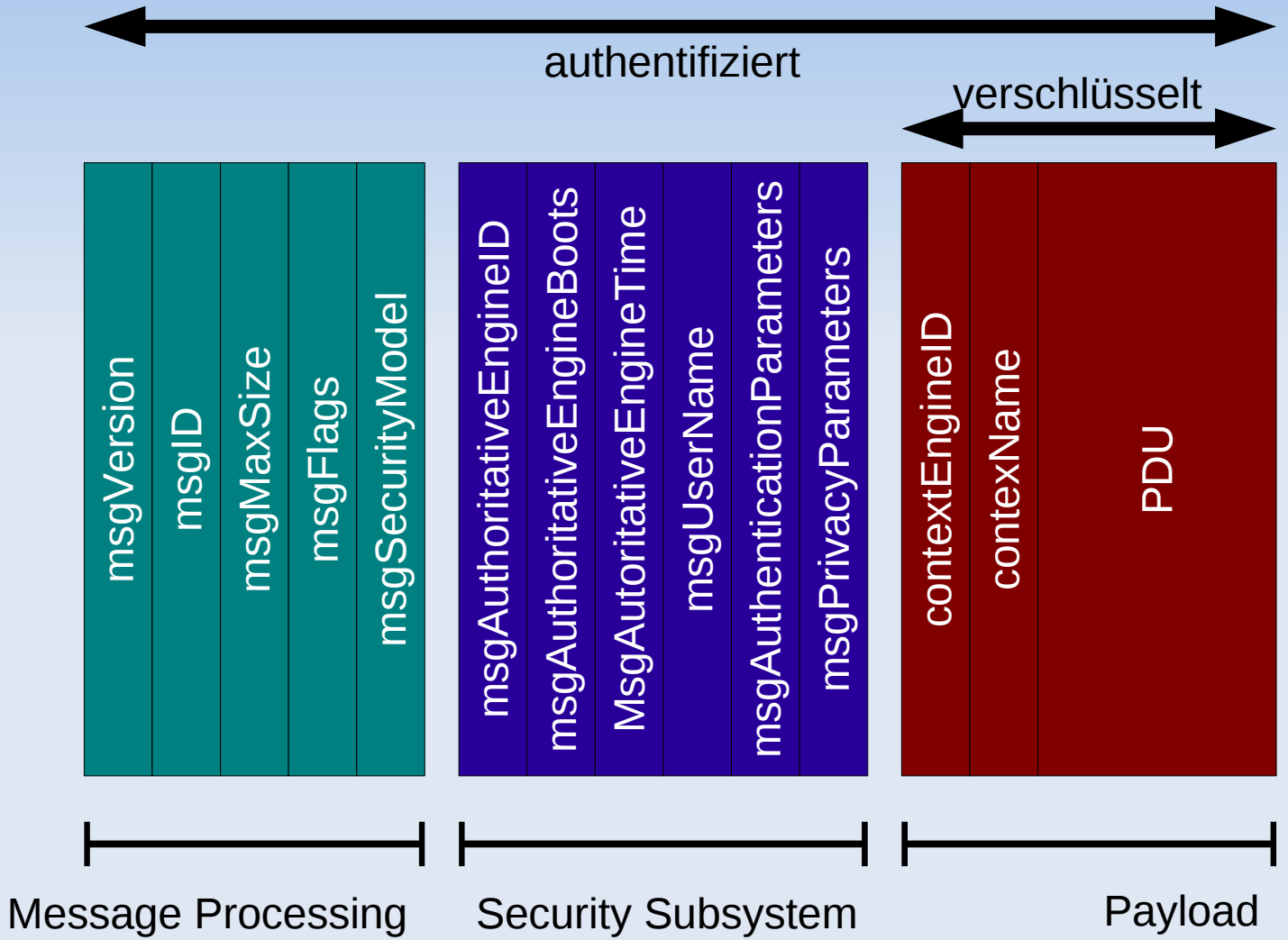
Die Einheiten

- In v3 wurden die Begriffe Agent und Manager durch „Entity“ ersetzt.
- Jede SNMP – Einheit ist durch ihre `snmpEngineID` definiert.
  - Damit diese im Netz eindeutig ist schlägt RFC 3411 Methoden vor, diese zu berechenen.
- Normalerweise berechnet jede Entity ihre ID selbst.
- Bevor zwei Einheiten Informationen austauschen können, müssen sei die `IDs` lernen. Dazu gibt es einen Autodiscovery Mechanismus.

Noch mehr Begriffe ...

- SNMPv3 definiert sehr (!) viele Begriffe. Wichtige sind:
- Username
- Security Level
  Reicht von *noAuthNoPriv* bis *authPriv*.
- Authentication Protocol MD5 oder SHA1
- Authentication Passphrase für die Authentifizierung
- Privacy Protocol (DES, AES) und Passphrase

Das SNMPv3 Paket



Anlegen von Benutzern

- Erzeugen von Benutzern (=`secName`), bzw. Abbildung von Communities auf `secName`.
- USM – Option

```
createUser username (MD5|SHA) \
   authpassphrase [DES|AES] privpassphrase
```

  Beispiel:

```
createUser misch MD5 sehrgeheim
```

- v1 und v2c – Option

```
com2sec        SECNAME    SOURCE          COMMUNITY
z.B.: com2sec  readonly   192.168.1.0/24  public
```

Benutzer gruppieren

- Im nächsten Schritt fasst man Benutzer zu Gruppen zusammen:

```
group  GROUP     secModel   secName
```

- Beispiel:

```
group  MyROSystem   v1      readonly
group  MyROGroup    usm     misch
```

Views anleges

- Views definieren Ausschnitte aus dem OID – Baum.
- Bestimmte Gruppen erhalten Zugriff auf bestimmte Teilbäume.
- Teile können auch exclusiv definiert werden.

```
view   VNAME    TYPE   OID    [MASK]
```

- Beispiele:

```
view   all       included   .1   80
view system included .1.3.6.1.2.1.1
view interfaces included 1.3.6.1.2.1.2
```

Zugriff mit Access

- Alle Definitionen werden werden nun zusammengefasst:

```
access GROUP context secModel secLevel match read write notif
```

- Beispiel:

```
access MyROSystem „“ any noauth exact system none none
access MyROGroup „“ usm priv exact all none none
```

Konfiguration des Agenten

- Benutzer werden in SNMPv3 mit createUser angelegt. Format:

```
createUser username (MD5|SHA) authpassphrase\
[DES|AES] [privpassphrase]
```

- Wenn keine `privpassphrase` eingegeben wird nimmt der Agent die `authpassphrase`
- Passphrases mussen mindestens 8 Zeichen lang sein.

Einfache Benutzerverwaltung

- Mit den Optionen `rouser` und `rwuser` können Benutzern Rechte eingeräumt werden:

```
rouser USER [noauth|auth|priv [OID | …]]
```

- `noauth`: Der Benutzer muss sich nicht authentifizieren.
- `auth`: Der Benutzer muss sich Authentifizieren.
- `priv`: Die Kommunikation wird zusätzlich verschlüsselt.

v3 in snmpcmd

- Für die Kommandozeile gibt es eine Reihe von Optionen für v3.

```
-a authProtocol  MD5|SHA
-A authPassphrase

-x privProtocol  DES|AES
-X privPassphrase

-l secLevel    noAuthNoPriv … authPriv
-u secName
-v 3
```

v3 in der Konfigdatei

- Die Optionen auf jeder Kommandozeile einzutippen macht keinen Spass. Deshalb hinterlegen in *~/.snmp/snmp.conf*:

```
defAuthType             MD5|SHA
defAuthPassphrase       Passphrase
defSecurityLevel        noAuthNoPriv … authPriv
defSecurityName         Username
defVersion              3
defPrivType             DES|AES
defPrivPassphrase       Passphrase
```

- Auch möglich: `defPassphrase`

Simple ...

- Mit den Einträgen geht auch ein einfaches

  ```
  snmpwalk host .system
  ```

  … wieder.

- Also doch Simple Network Management!

SNMP Mythen

- „SNMP is not secure“
  - Ja. Das Design von SNMPv1 war nicht dazu gedacht sicher zu sein.
  - SNMPv3 ist sicher. Alle Nachrichten können verschlüsselt und authentifiziert werden.
  - SNMPv3 bietet ein rollenbasiertes Zugangsmodell.
- „SNMP is not safe“ (Traps werden nicht quittiert)
  - SNMPv3 bietet *Informs* die quittiert werden.
- „SNMP floods the net / overloads my router“
  - Hängt von der tatsächlichen Installation ab.
  - Auch ein falscher DNS-Server kann das Netz fluten.

Vielen Danke für die Aufmerksamkeit!

Fragen?