Internet Management Standards

Quo Vadis?

Jürgen Schönwälder

Institut für Betriebssysteme und Rechnerverbund
TU Braunschweig
Bültenweg 74/75
38104 Braunschweig

E-mail: schoenw@ibr.cs.tu-bs.de

Überblick über den Vortrag

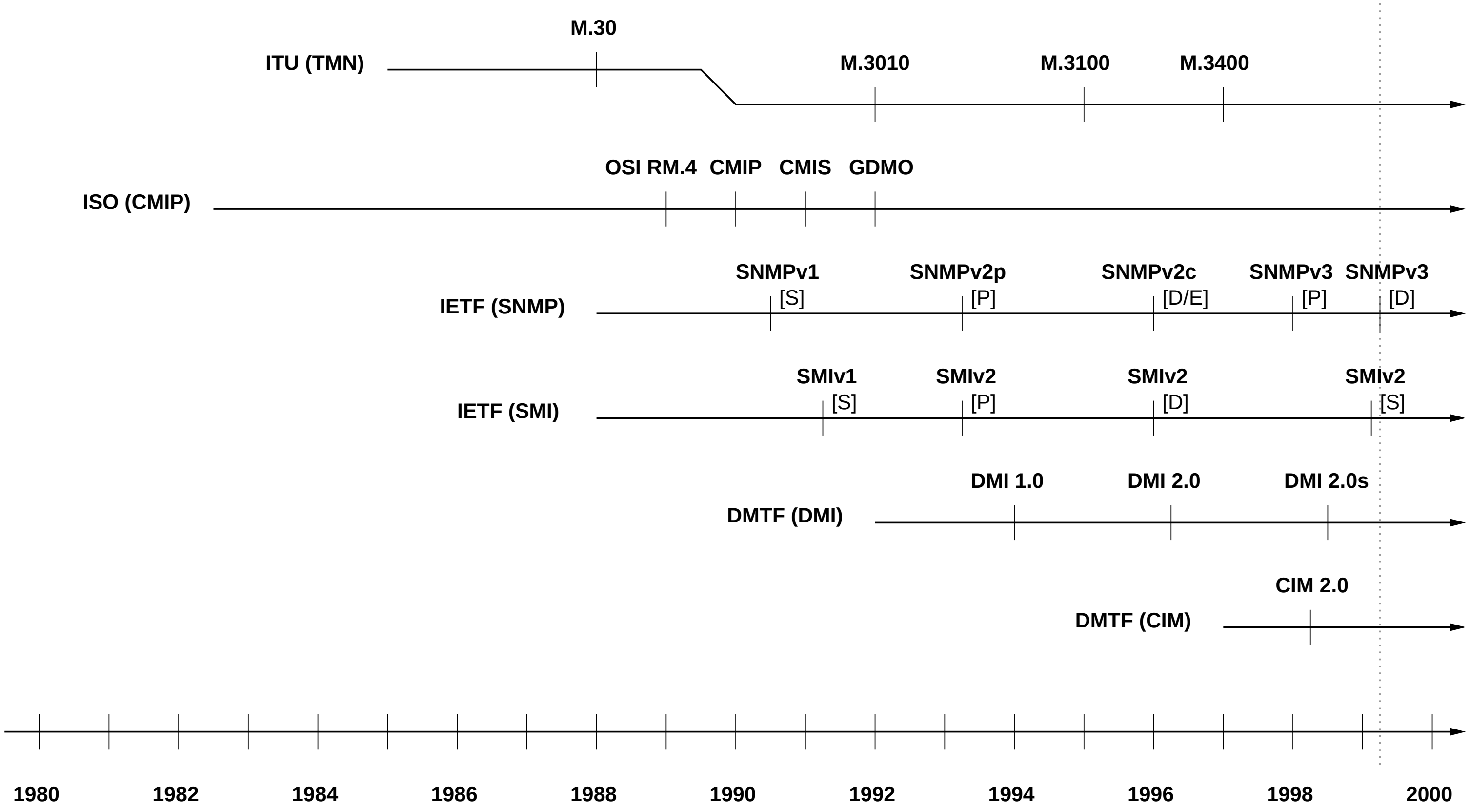
1. Aktuelle Entwicklungen innerhalb der IETF
   - SMI Version 2
   - SNMP Version 3
   - Erweiterbare Agenten (AgentX)
   - Verteiltes Management
   - Management von Applikationen

2. Einige offene Probleme und mögliche Lösungen
   - SMIng and libsmi
   - Bulk Transfer

3. Zukunft des Internet Managements

4. Diskussion

Historische Entwicklung der Management-Standards



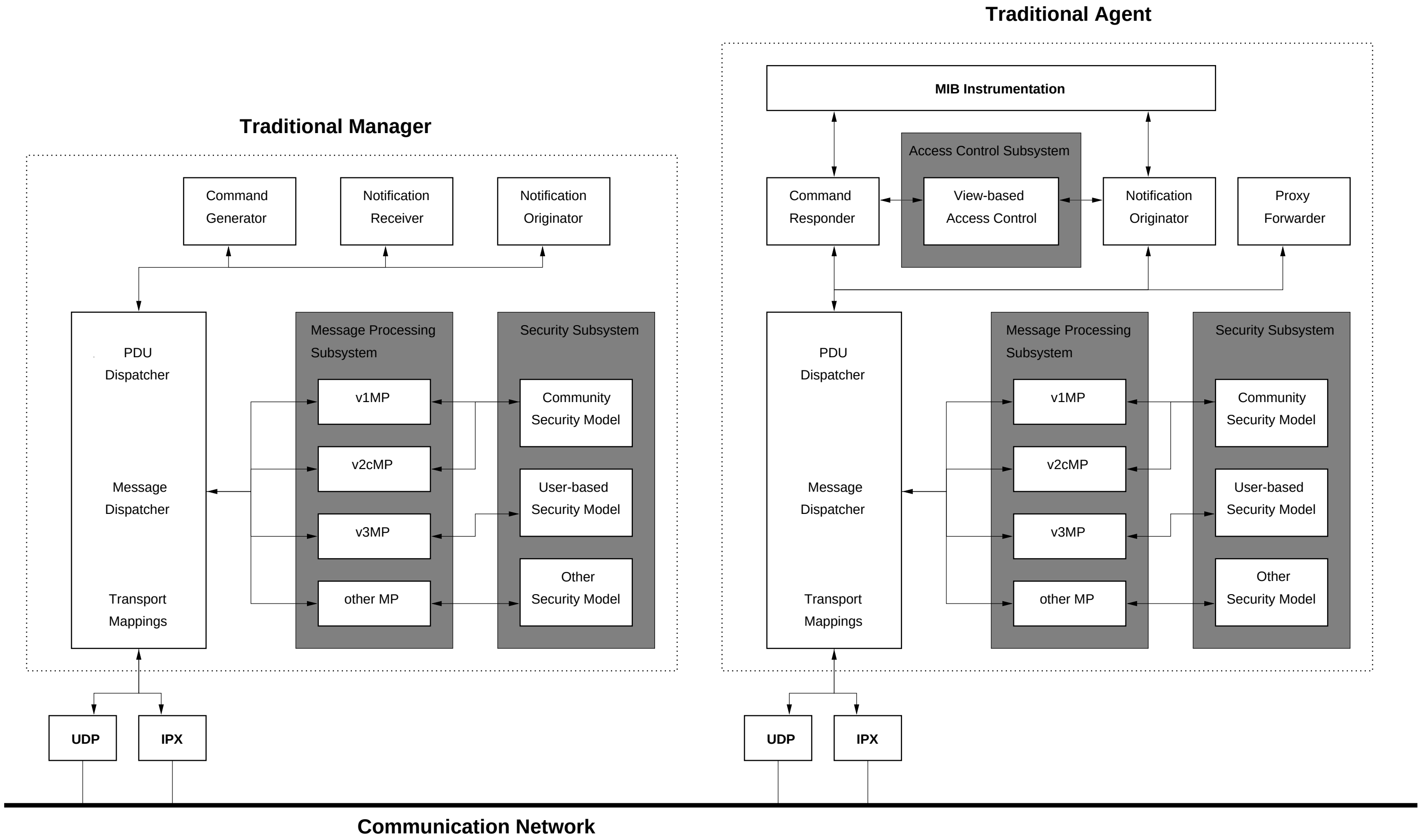
Structure of Management Information Version 2 (SMIv2)

- Bereits seit mehreren Jahren Grundlage aller IETF MIB Definitionen
- 1998 durch ein „Design Team“ überarbeitet (Klärungen, Fehlerkorrekturen)
- Publiziert als Internet Standard 58 (RFC 2578 – 2580) im April 1999
- SMIv2 wird SMIv1 demnächst ablösen, gute Unterstützung durch Hersteller
- Probleme durch die Abhängigkeit von ASN.1 (1988)
- Fehlende dringend benötigte Basis-Datentypen (z.B. Integer64)

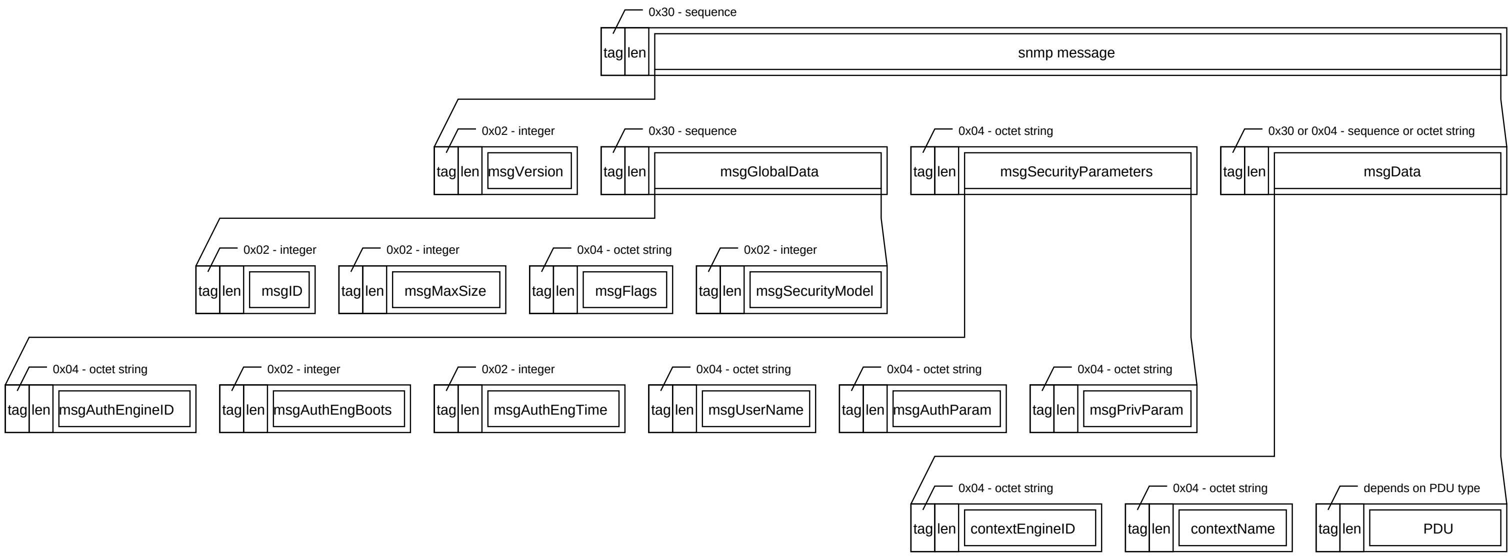
SNMP Version 3 (SNMPv3)

- Erweiterbarkeit durch ein modulares Architekturmodell
- Sicherer SNMPv3 Nachrichtenaustausch (Authentifikation und Verschlüsselung)
- Zugriffskontrolle auf MIB Objekte (Authorisierung)
- Eindeutige Identifikation von Management Informationen (ScopedPDU)
- MIBs zur Konfiguration von SNMP Entities via SNMP
- Gute Unterstützung durch SNMP Toolkit Hersteller
- IBM und CISCO liefern seit 1999 SNMPv3 in einigen Produkten aus

Architekturmodell von SNMPv3

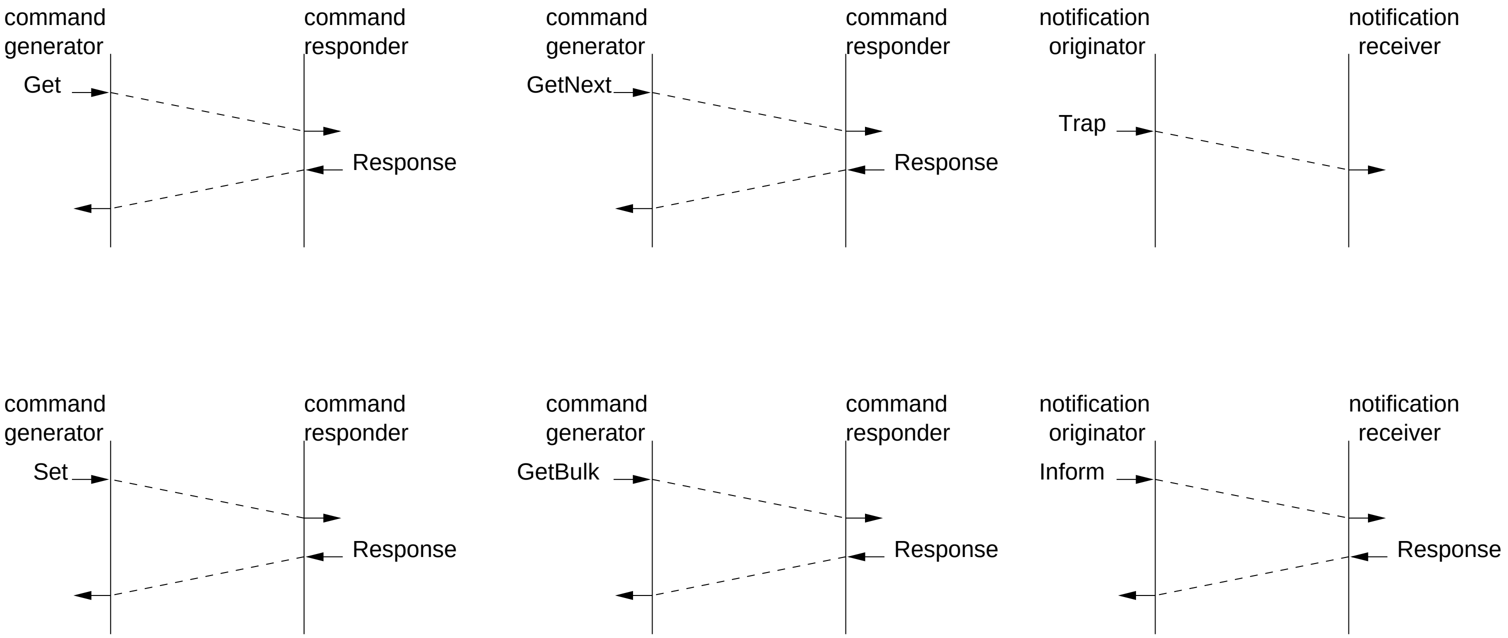


SNMPv3 Nachrichtenformat (User-based Security Model)



- `msgSecurityParameters` hängen vom `msgSecurityModel` ab
- `msgData` enthält entweder eine `scopedPDU` oder eine verschlüsselte `scopedPDU`

SNMPv3 Protokoll-Operationen



- Zusätzliche `Report` PDU zur Fehlerbehandlung und Uhrensynchronisation

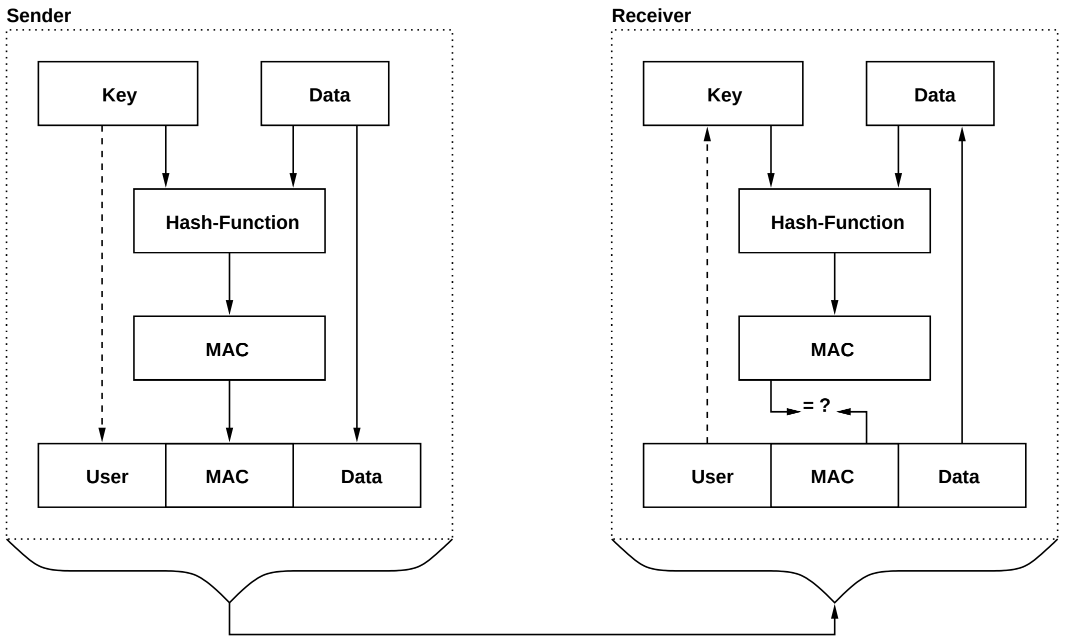
Sicherheitsproblematik

- Folgende Fragen müssen bei der Entscheidung, ob eine Operation auszuführen ist, beantwortet werden:

  1. Ist die empfangene Nachricht authentisch?
  2. Wer möchte die Operation ausführen?
  3. Welche Objekte sind von der Operation betroffen?
  4. Welche Rechte hat der Aufrufer einer Operation bezüglich der betroffenen Objekte?

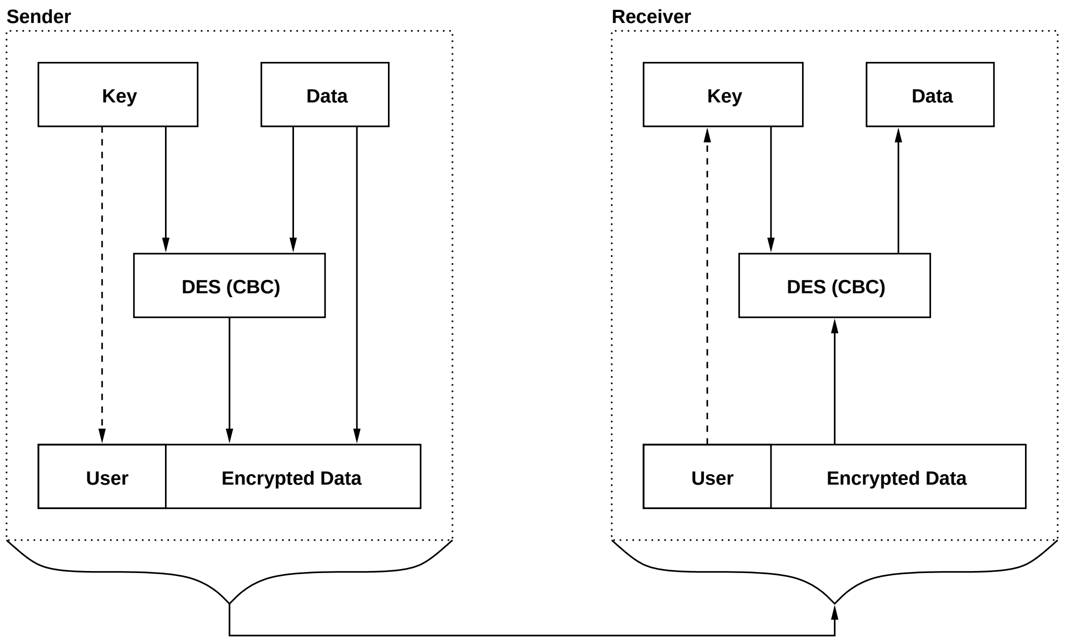
- Die Fragen 1 und 2 werden durch die Maßnahmen zur Sicherung der Nachrichten beantwortet (Authentifikation, Verschlüsselung).
- Die Fragen 3 und 4 werden durch die Zugriffskontrolle beantwortet.

SNMPv3 Authentifikation



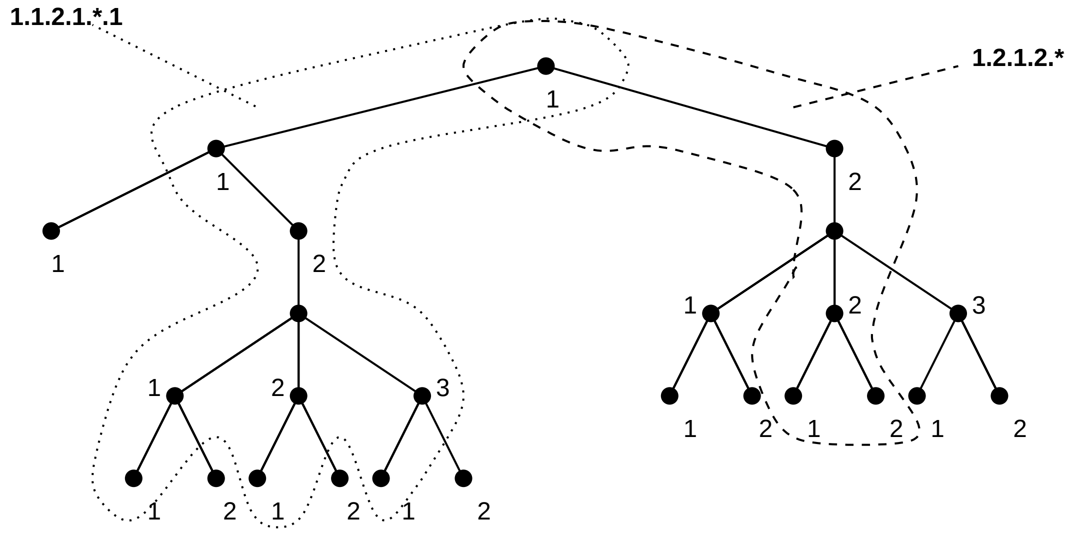
- Kryptographische Hash-Funktionen zur Bestimmung von Fingerabdrücken (HMAC-MD5-96, HMAC-SHA-96)
- Sicherung gegen Wiederholungen durch lose synchronisierte Uhren
- Erzeugung von Schlüsseln aus Passworten und „Lokalisierung" der Schlüssel

SNMPv3 Verschlüsselung



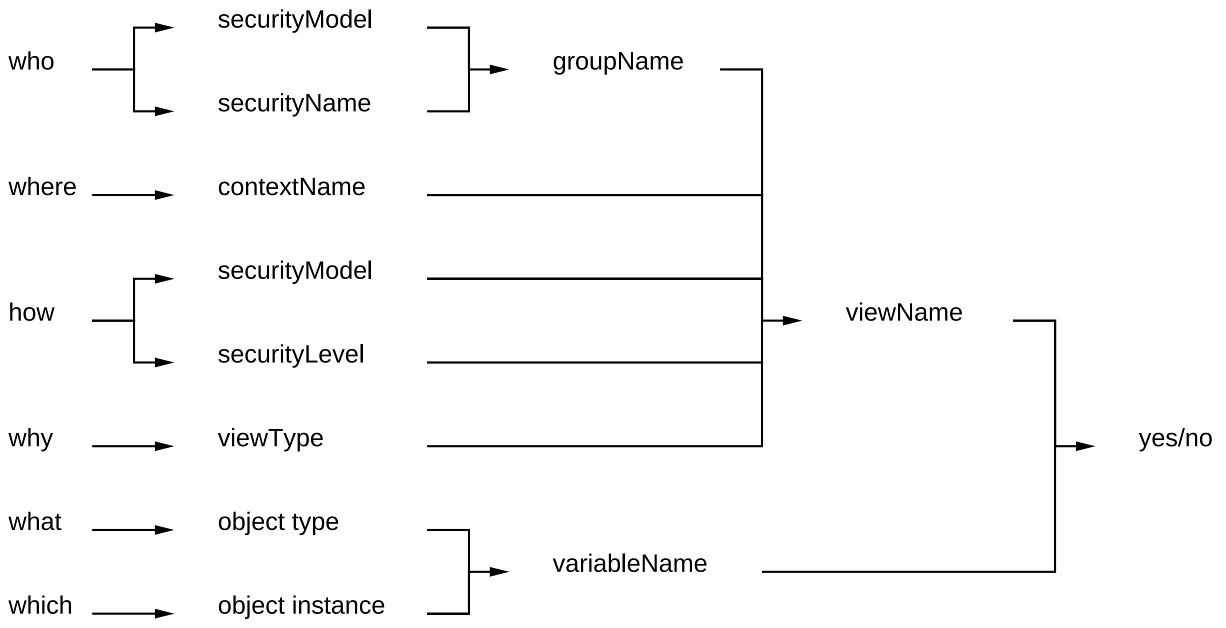
- Optionale Verschlüsselung der `ScopedPDU` (DES im CBC Modus)
- Verschlüsselung ist relativ aufwendig und daher sparsam zu verwenden.
- SNMPv3 erlaubt eine „relativ sichere“ Schlüsseländerung ohne Verschlüsselung

SNMPv3 VACM MIB Views



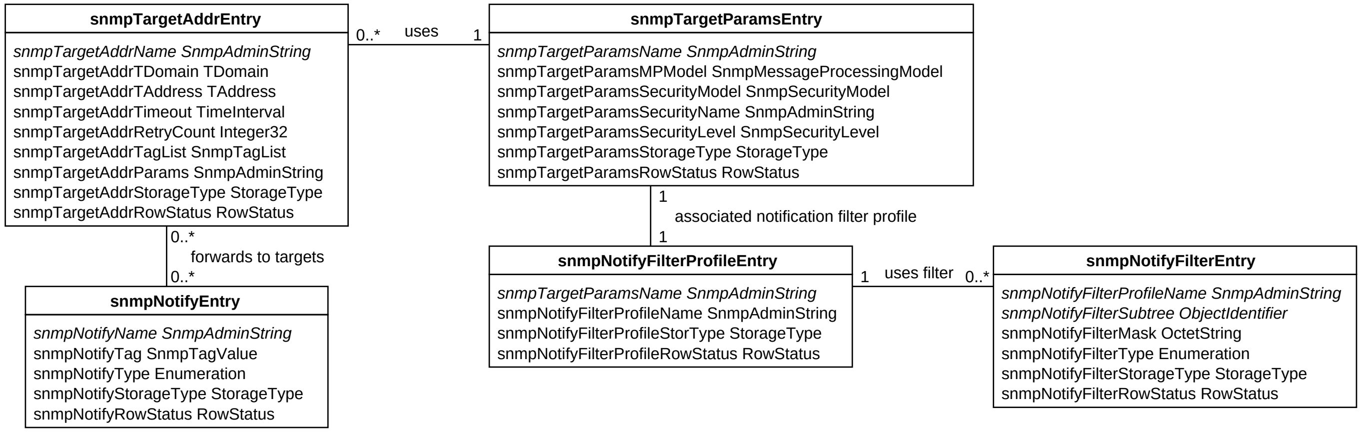
- Ein view subtree ist die Menge aller MIB-Objekte mit einem gemeinsamen Präfix
- Eine view tree family ist die Kombination von einem Präfix mit einer Bitmaske, die bestimmt, ob ein Element des Präfixes signifikant ist oder nicht
- Ein view setzt sich aus einer Menge von view tree families zusammen
- Zugriffsrechte werden durch einen read view, write view und notify view definiert

SNMPv3 Zugriffskontrolle



- Es gibt drei `securityLevel` (`noAuth/noPriv`, `auth/noPriv`, `auth/priv`)
- Der `securityName` ist ein vom `securityModel` unabhängiger Name

MIBs zur Konfiguration von SNMP Entities

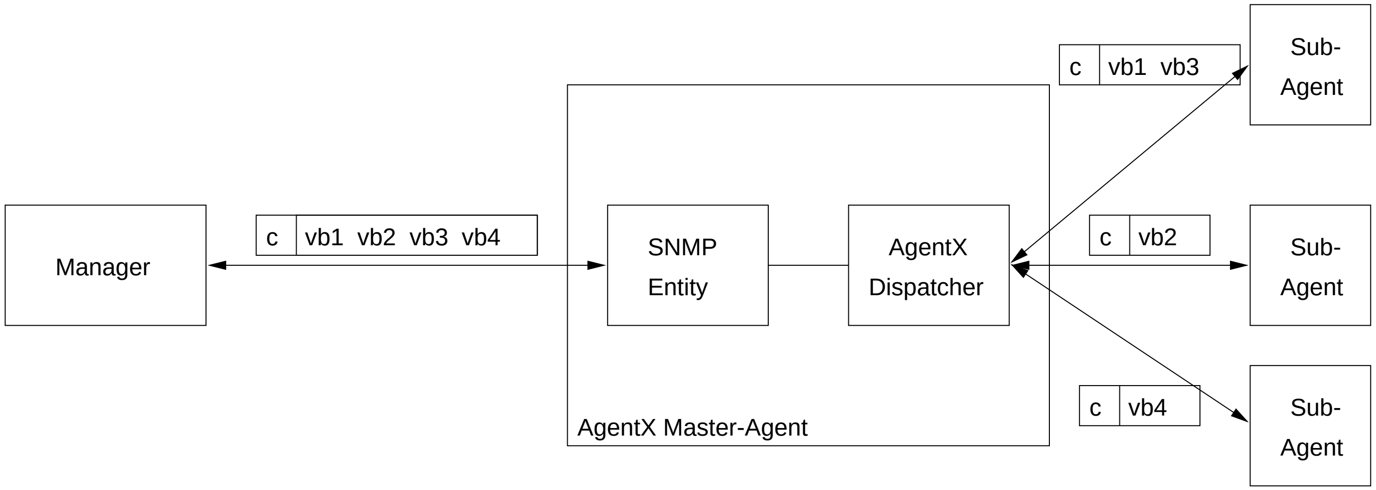


- SNMPv3 definiert eine Reihe von MIBs zur Konfiguration von SNMP Entities
- Einige der MIBs können auch zusammen mit SNMPv1/SNMPv2c genutzt werden
- Das Beispiel zeigt die Struktur der MIB-Tabellen zur Weiterleitung und Filterung von Ereignismeldungen (`Trap` und `Inform`)

Bekannte Probleme/Grenzen von SNMPv3

- Fehlende Erweiterbarkeit um weiterer Basis-Datentypen (z.B. Unsigned64)
- Fehlende Erweiterbarkeit um neue Protokoll-Operationen
- Geringe Flexibilität bei der Definition von VACM Zugriffskontrollregeln
- Asymmetrie beim Filtern von Notifications und der VACM Zugriffskontrolle
- Unterbringung der Sicherheitsinformationen innerhalb der Nachricht
- Unnötige Einhüllungen im SNMPv3 Nachrichtenformat
- Keine Effizienzverbesserungen gegenüber SNMPv2c

Erweiterbare Agenten (AgentX Version 1)

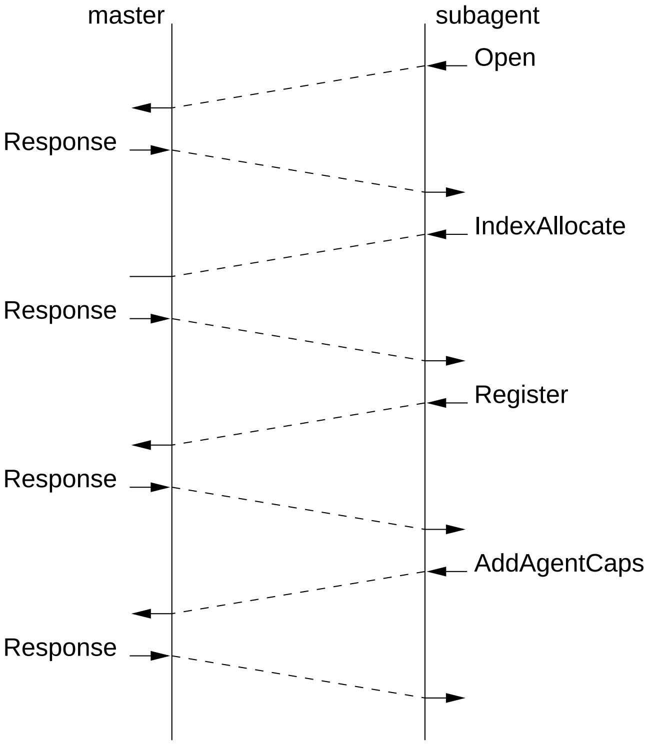


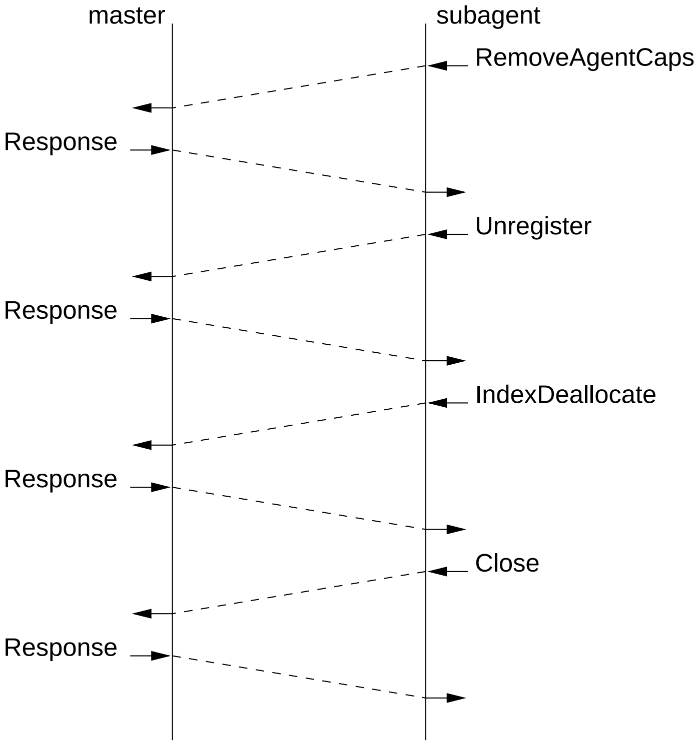
- Standard zur herstellerunabhängigen Implementation von erweiterbaren Agenten
- Unterstützung durch die meisten SNMP Toolkit Hersteller
- Voraussetzung zur portablen Instrumentierung von Applikationen und Diensten
- AgentX 1 (RFC 2257) beschränkt sich auf elementare Funktionen

AgentX Index-Allokation, OID-Registration und Scoping

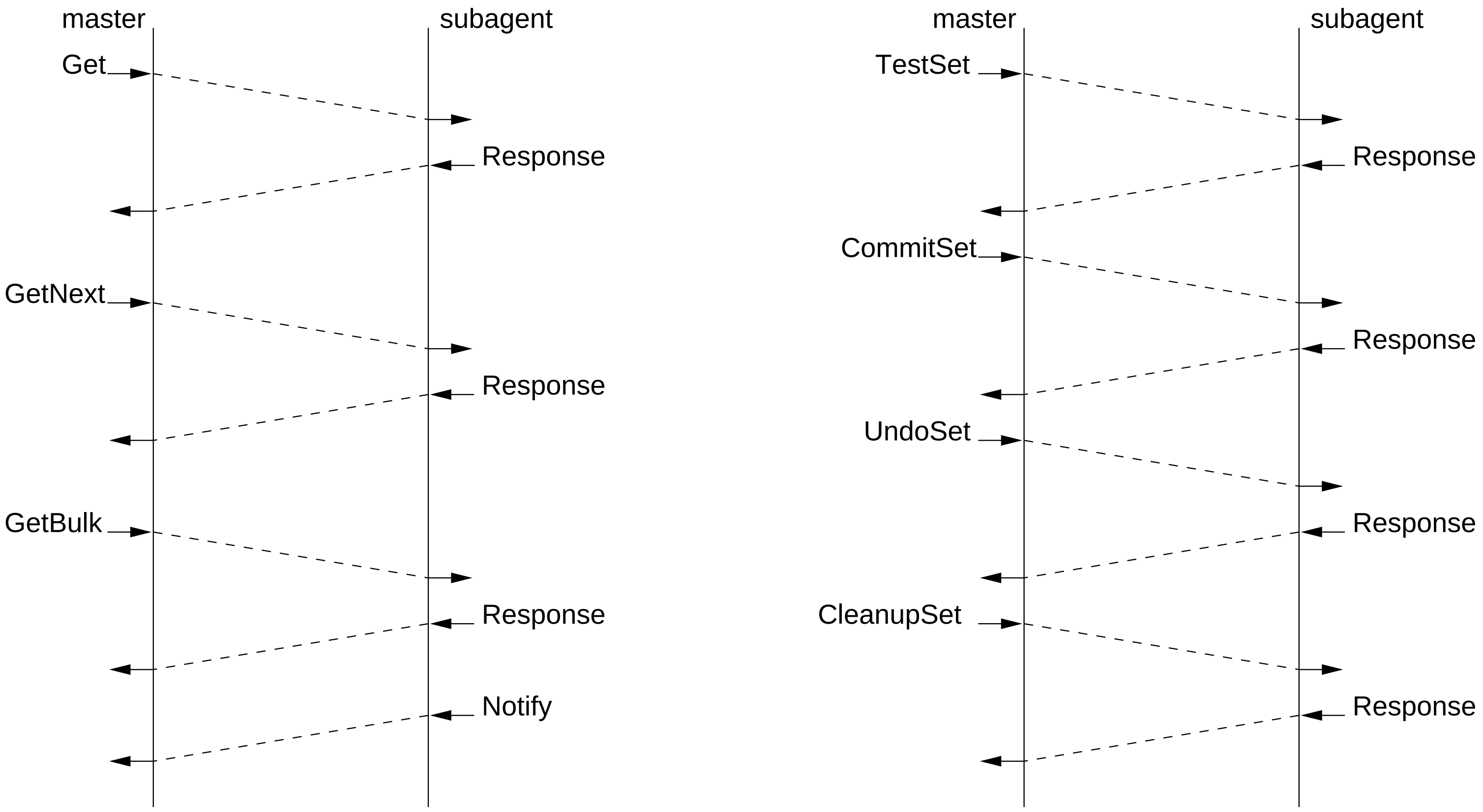
- Index-Allokation für gemeinsame Tabellen zwischen Sub-Agents
  - Allokation eines spezifischen Index-Wertes
  - Allokation eines Index-Wertes, der derzeit nicht benutzt wird
  - Allokation eines Index-Wertes, der noch niemals benutzt worden ist
- OID-Registration
  - Registration einzelner Instanzen:
    1.3.6.1.2.1.2.2.1.1.42 (ifIndex.42)
    1.3.6.1.2.1.2.2.1.2.42 (ifDescr.42)
  - Registration von Regionen:
    1.3.6.1.2.1.2.2.1.[1-22].42 (ifIndex.42 – ifSpecific.42)
- Scoping
  - Bei der AgentX GetBulk-Operation kann ein Scoping-Element angegeben werden, das die Bearbeitung an dem Object Identifier beendet.

AgentX Protokoll-Operationen





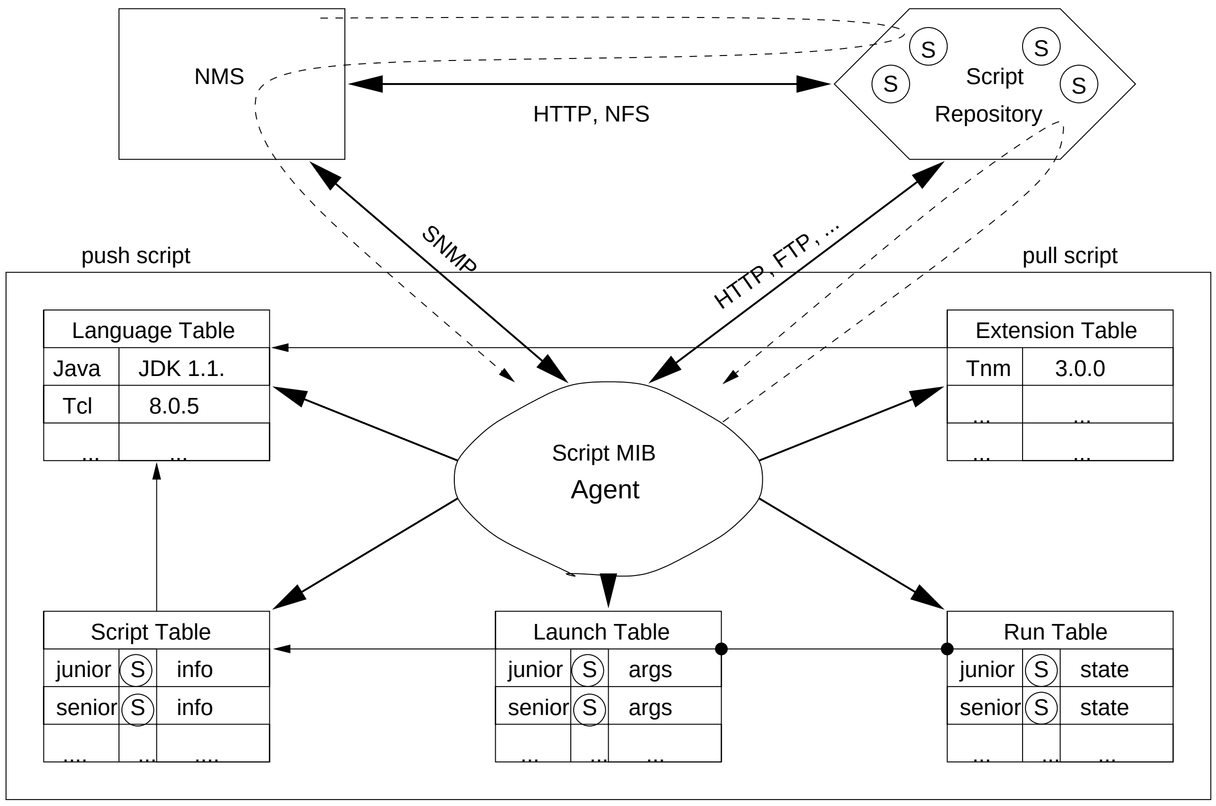
AgentX Protokoll-Operationen



Expression, Event und Scheduling MIB

- Expression MIB
  - Berechnung von Ausdrücken über MIB-Variablen
  - Wildcarding erlaubt Ausdrücke für mehrere Tabellenzeilen
  - Ergebnisse von Ausdrücken können in anderen Ausdrücken benutzt werden (Rekursionen sind allerdings nicht erlaubt!)
- Event MIB
  - Erzeugung von Ereignissen bei Über- oder Unterschreitung von Grenzwerten oder bei Änderung von MIB Variablen
- Scheduling MIB
  - Schreiboperationen auf MIB-Variablen nach einem gegebenen Zeitplan
  - Ermöglicht das Starten von Management-Funktionen oder die Statusänderung von Betriebsmitteln (z.B. Schnittstellen)

Script MIB (Management by Delegation)



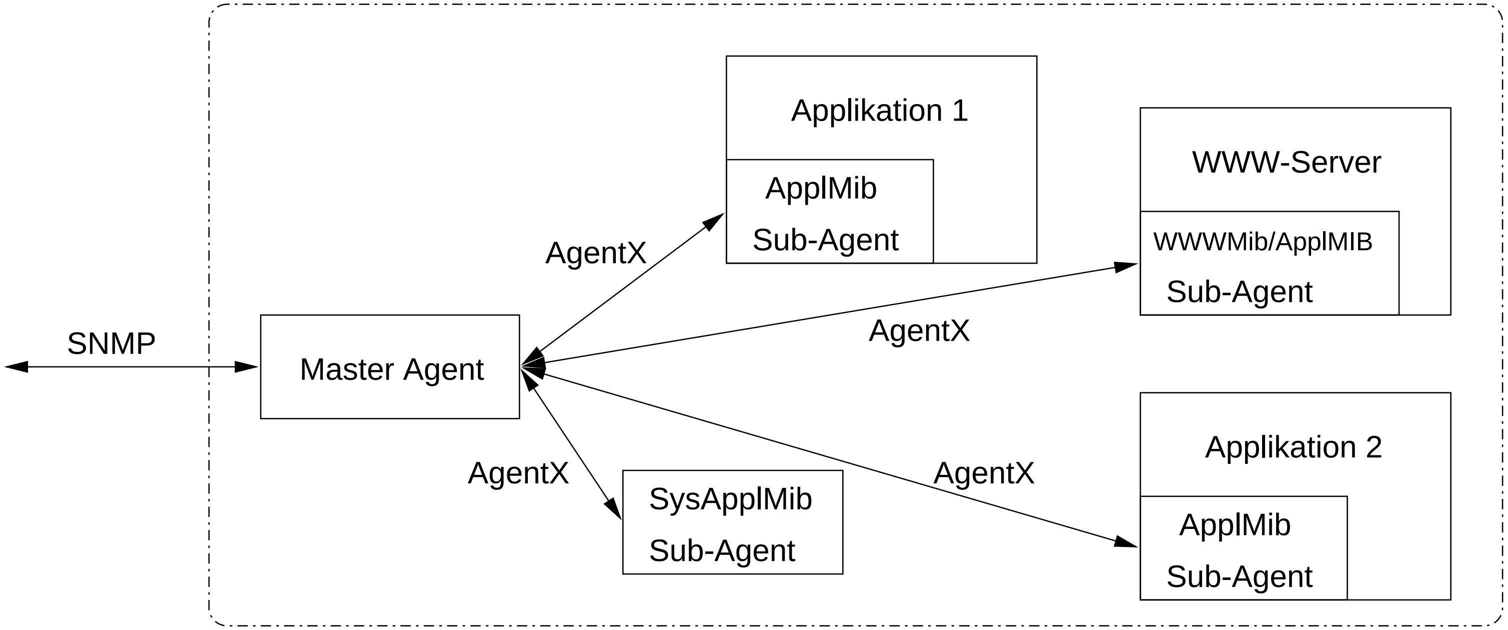
Management von Applikationen

- System Application MIB (RFC 2287)
  - Prozeßorientierte Sichtweise, Instrumentation auf Betriebssystemebene
  - Informationen über installierte und laufenden Applikationen und Prozesse

- Application MIB (to be published)
  - Prozeß- und dienstorientierte Sichtweise, Instrumentation in der Applikation
  - Statistiken über geöffnete Dateien oder etablierte Netzwerkverbindungen
  - Statistiken über Transaktionsströme auf den offenen E/A-Kanälen

- World-Wide Web MIB (to be published), ...
  - Statistiken über Request/Response Interaktionen (gemäß abstraktem DTP)
  - Informationen über die letzten N Zugriffe
  - Statistiken über die häufigsten Zugriffe in zurückliegenden Zeitintervallen

Management von Applikationen mit Hilfe von AgentX



- AgentX ist die Basis zur portablen Instrumentation von Applikationen

Zukunft der SMI – SMIng?

- Definition einer „einfacheren“ SMI unabhängig von ASN.1
- Einfaches und konsistentes Sprachkonzept, definiert in ABNF
- Vollständiger Satz von Basis-Datentypen (64-Bit Zahlen, Gleitpunktzahlen)
- Erweiterbarkeit durch `extension` und `annotation` Anweisungen
- Implementation von Konvertierern auf Basis einer `libsmi`
- Forschungsprojekt an der TU Braunschweig

Effizienter Transfer von MIB-Daten

1. Erweiterung von SNMP zur effizienten Übertragung von MIB-Daten:
   - Benutzung von TCP als Transportprotokoll
   - Komprimierung von SNMP Nachrichten mittles `gzip`
   - Einführung einer neuen `get-subtree` Protokolloperation

2. Benutzung von FTP:
   - MIB zur Speicherung von MIB Daten in lokalen Dateien
   - MIB zur Steuerung von FTP Übertragungen

3. Benutzung von alternativen Protokollen
   - Definition eines MIME-Typs zur Aufnahme von MIB-Daten
   - Transfer der MIB-Daten via HTTP oder SMTP

Zukunft des Internet Managements

- Standardisierte APIs für SNMP und zum Zugriff auf MIB-Informationen
- Protokolle und APIs zum Zugriff auf Topologie- und Konfigurationsinformationen
- Brauchen wir SNMP Version 4?
- Alternative Protokolle zum Zugriff auf Managementinformationen?
- Weniger Management ist mehr! $\Longrightarrow$ self-managing devices and protocols?
- Was sind die Alternativen? CORBA? CIM? CMIP/GDMO? Active Networks?

Weitere Informationen

- Internet Engineering Task Force (IETF) `http://www.ietf.org/`
- Internet Research Task Force (IETF) `http://www.irtf.org/`
- The SimpleTimes `http://www.simple-times.org/`
- The Simple Web `http://wwwsnmp.cs.utwente.nl/`
- OPS-Area Email-Liste `mailto:ops-area@ops.ietf.org`
- Vortragsfolien `http://www.ibr.cs.tu-bs.de/~schoenw/`

Diskussion

- Zeit für Fragen, Kommentare, Kritik, Wünsche oder andere Bemerkungen!