

# SNMP - Der Weg zum Standard

Stephan Knabe

Hochschule Harz, Wernigerode

[stephan.knabe@desy.de](mailto:stephan.knabe@desy.de)

6. März 2004

# In der Praxis oft heterogene Umgebungen:

Beispiel:

- Workstations - MS Windows
- Server - Linux
- Drucker - HP
- Switches - 3Com
- Router - CISCO
- ...

Standardisierung ist nötig.

## Wichtige Ansätze waren:

- CMISE/CMI - Common Management Information Service Element / Common Management Information, hieraus CMOT (CMIP Over TCP)
- SNMP - Simple Network Management Protocol

SNMP hat sich durchgesetzt und gilt heute als quasi Standard.

## Timeline (1)

- Mai 1990 - Structure of Management Information, SMI (RFC 1155)
- Mai 1990 - Simple Network Management Protocol, SNMP (RFC 1157)
- März 1991 - MIB II (RFC 1212, 1213, 1215)

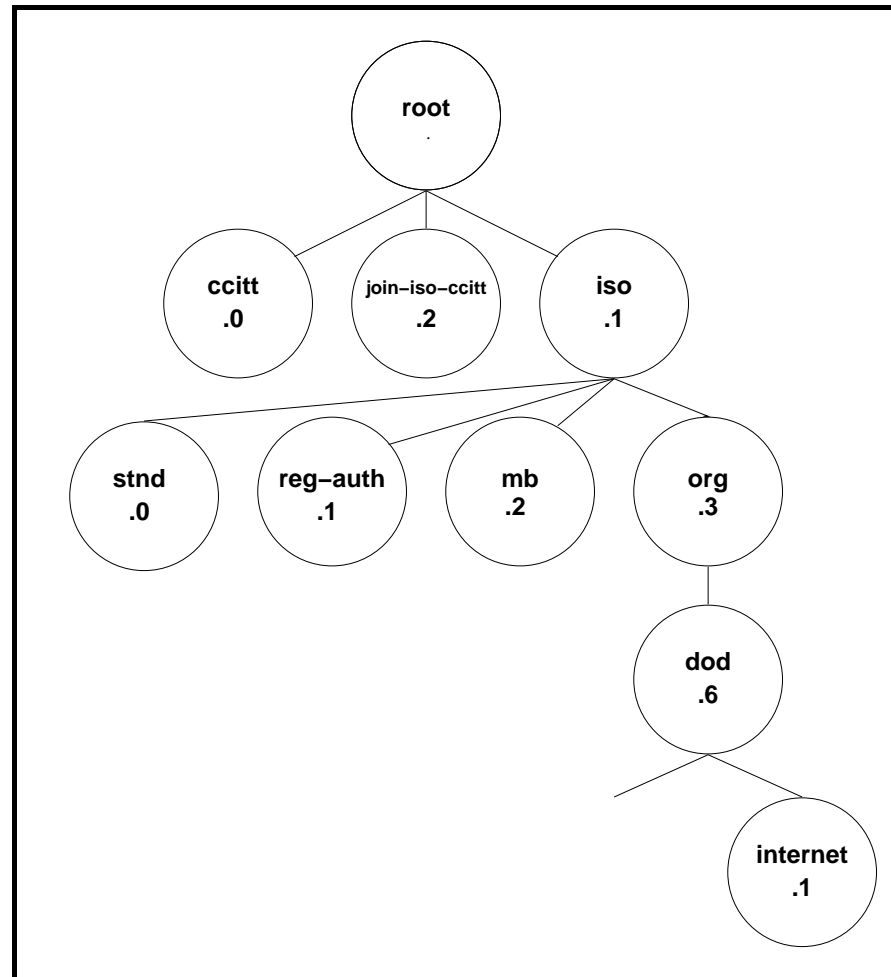
## Timeline (2)

- April 1993 - SNMP v2 (RFC 1441, 1448-1450)
- Januar/Februar 1996 - Erweiterte Access Control Mechanismen (RFC 1901-1910)
- April 1999 - SNMP v3 (RFC 2570 - 2576)

# MIB's

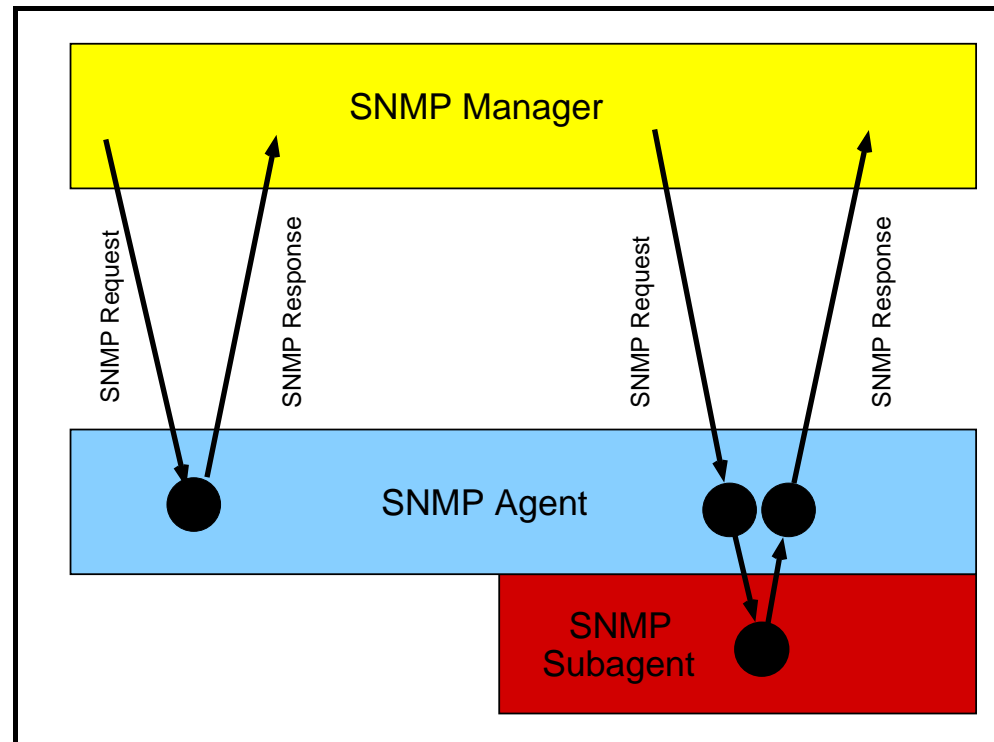
- SMI definiert, wie Objekte zu spezifizieren sind.
- Wichtigste Attribute sind Name, Syntax und Datentyp
- Name in numerischer und alphanumerischer Notation
- Zu managende Objekte werden in Management Information Bases (MIB's) zusammengefasst
- MIB's sind in Baum-Struktur gegliedert

# MIB Tree



# SNMP v1

## Austausch von Protocol Data Units (PDU's)





# Felder in PDU's

- Version (0 entspricht v1)
- Community
- Command (5 Typen)
- Request ID
- Error Status
- Variable Binding (varbind), Object Identifiers (OID's) und Werte

# Operationen (1)

## Get Request

- Einfache Anfrage nach den Werten von Objekten

## Get Response

- liefert verbind zurück

# Operationen (2)

## Getnext Request

- Browsen des MIB-Trees
- Anfrage unterscheidet sich im Kommando-Namen
- Response liefert varbind der lexigraphisch nächsten Variablen

# Bild Beispiel snmpwalk

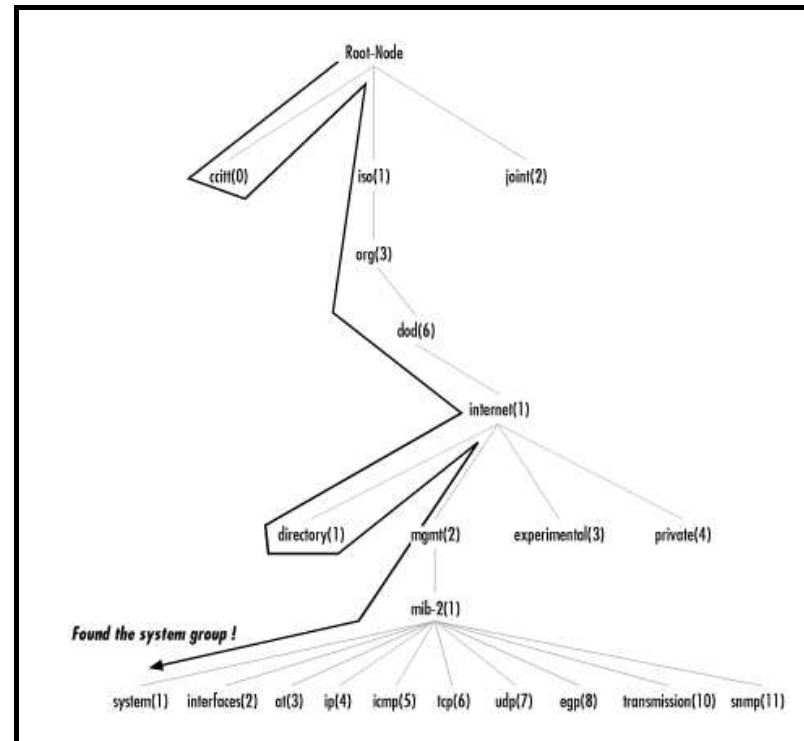


Bild aus „Essential SNMP“, Douglas Mauro & Kevin Schmidt, O'Reilly 2001

# Operationen (3)

## Set Request

- Setzen einer Variablen
- varbind enthält neben OLD auch neuen Wert
- Antwort mit Get Response und neuem Wert

# Operationen (4)

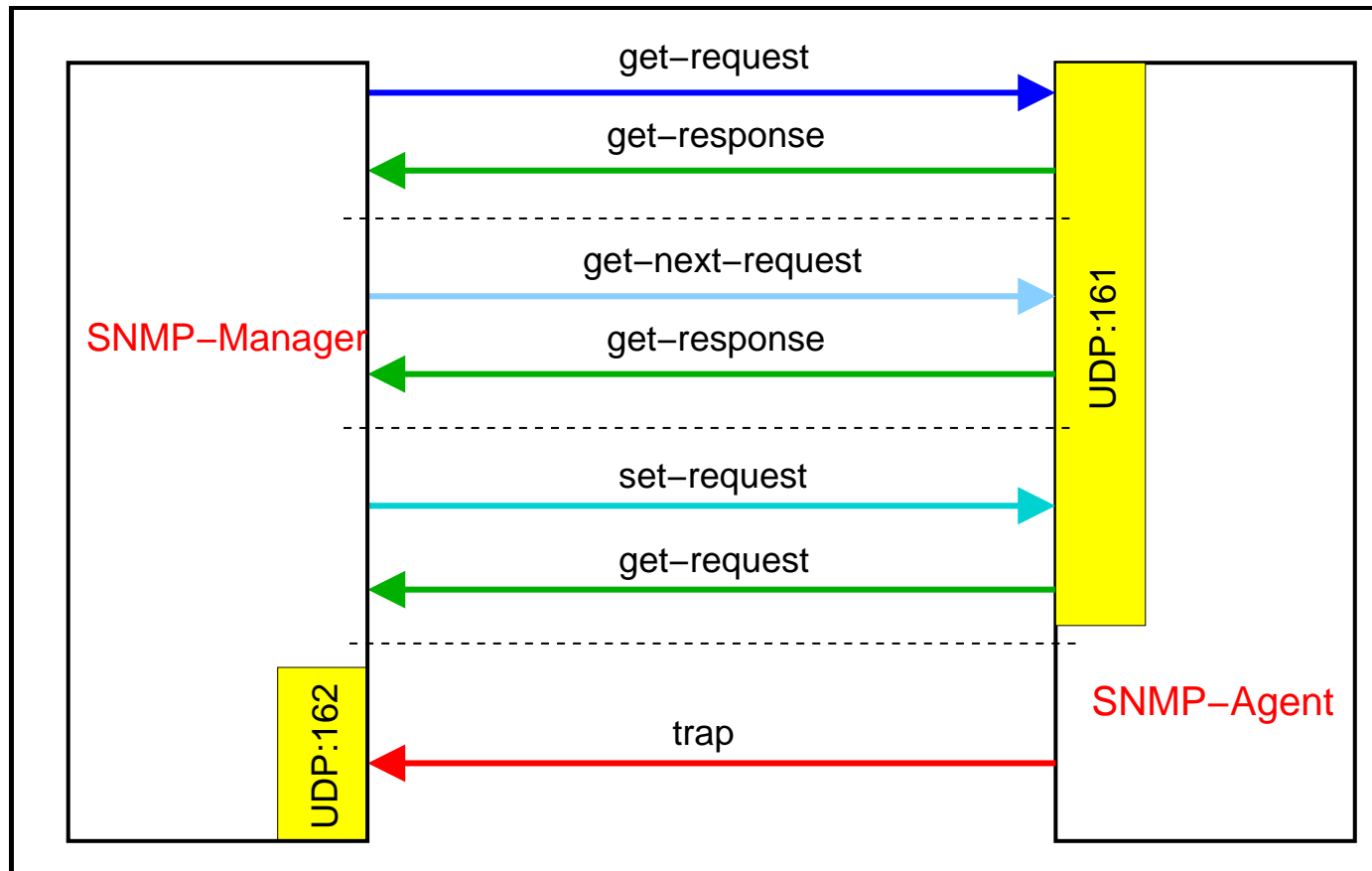
## Traps

- Asynchrone Messages
- 7 verschiedene Typen
- Typ 7 für eigene Definitionen
- Kann zusätzlich varbind enthalten

# Generic Traps

- coldStart (0)
- warmStart (1)
- linkDown (2)
- linkUp (3)
- authenticationFailure (4)
- egpNeighborLoss (5)
- enterpriseSpecific (6) - für eigene Implementierungen

# Kommunikation





# SNMPv1 Error Messages

noError(0)	Kein Fehler
tooBig(1)	Datenmenge im Response zu groß für eine Sequenz
noSuchName(2)	Nicht existierende OID im Request
badValue(3)	Inkonsistenter Schreibzugriff
readOnly(4)	Wird meist durch noSuchName ersetzt
genErr(5)	Sonstige Fehler

# SNMP v2

Erweiterung in verschiedenen Bereichen:

- Einführung verschiedener Security-Modelle
- Mangelnde Akzeptanz
- Versuch von Nachbesserungen
- Verschiedenste Versionen (v2p, v2\*, v2u)
- Akzeptierte Features als SNMP v2 Classic (v2c)

# SNMP v2c

- Keine erweiterten Sicherheitsmaßnahmen
- Erweiterungen in Syntax
- Neue Datentypen (u.a. größere Wertebereiche)
- Erweiterte Fehlermeldungen
- Änderungen am PDU Format

# Neue Operationen

- getbulk-Request - besseres Handling großer Datenmengen
- inform-Request - asynchrone Nachrichten mit Empfangsbestätigung

# SNMP v3

- Erweiterungen im Bereich Administration und Security
- User based Security Model (USM)
- View based Access Control Model (VACM)
- Nutzung von Authentisierungsprotokollen (z.B. MD5, SHA)
- Nutzung von Verschlüsselung (z.B. DES, AES)