

Rechnernetze:

(9) Network Management



Prof. Dr. Klaus-Peter Kossakowski



Gliederung der Vorlesung

- Einführung und Historie des Internets
- Schichtenmodell, Netzwerk als Infrastruktur
- Layer 7: Anwendungsschicht
- Layer 7/4: Socket-Programmierung
- Layer 4: Transportschicht
- Layer 3: Netzwerkschicht
 - IPv4, ICMPv4, IPv6, Routing, ...
 - Firewalls
 - Management
- Layer 2: Sicherungsschicht



Inhalte dieses Kapitels

In diesem Kapitel wird auf das Netzwerk-Management eingegangen.

Das Simple Network Management Protocol (SNMP) wird als das Standardprotokoll angesprochen und kurz dargestellt.

Die besondere Problematik der unterschiedlichen Repräsentation von Daten (typen) und die gewählte Lösung per ASN.1 wird erklärt.



Ziele dieses Kapitels

Sie kennen die Aufgaben des Netzwerk-Managements.

Sie können das SNMP erklären und einzelne Abläufe, Komponenten und die Art der Kommunikation erläutern.

Sie kennen das grundlegende Konzept der ASN.1 und können erklären, welches Problem durch ASN.1 gelöst wird.



Was ist Netzwerkmanagement?

- **Autonome Systeme bestehen immer häufiger aus tausenden von interagierenden Hard- und Softwarekomponenten**
- **Komplexe Systeme benötigen Überwachungs- und Steuerungsfunktionen, z.B. findet man das in**
 - Transport (Flugzeugen, Schifffahrt, ...)
 - Energie (Kraftwerke, Überlandleitungen, ...)
- **Anforderung: Funktion & Verfügbarkeit**



Definition Netzwerkmanagement

“Netzwerkmanagement beinhaltet Einsatz, Integration und Koordination von Hardware, Software und menschlichen Beteiligten, um das Netzwerk und die Ressourcen, aus denen es besteht, zu überwachen, zu testen, abzufragen, zu konfigurieren, zu analysieren, auszuwerten und zu steuern,

um so die Leistung während des Betriebs in Echtzeit sowie die Dienstgüteanforderungen bei vernünftigen Kosten zu gewährleisten.”

gem. Kurose, Ross

Wer braucht Management ?



■ Anwender & Rollen

- Authentifikation & Identität
- Addressierung
- Roaming Profiles & Services

■ Anwendungen & Dienste

- Mail, DNS, ...
- IP Telefonie, Broadcasting

■ Geräte & Infrastruktur

- Router, Switches, Server, ...
- Bandbreite, Buffers, Policies



Aufgaben des Netzwerkmanagements



■ Fehlermanagement:

- Erkennen, Isolieren und Beheben von Störungen

■ Konfigurationsmanagement:

- Auslesen und Einstellen der Konfigurationsparameter

■ Performanzmanagement:

- Sammeln und Bewerten von Betriebsdaten

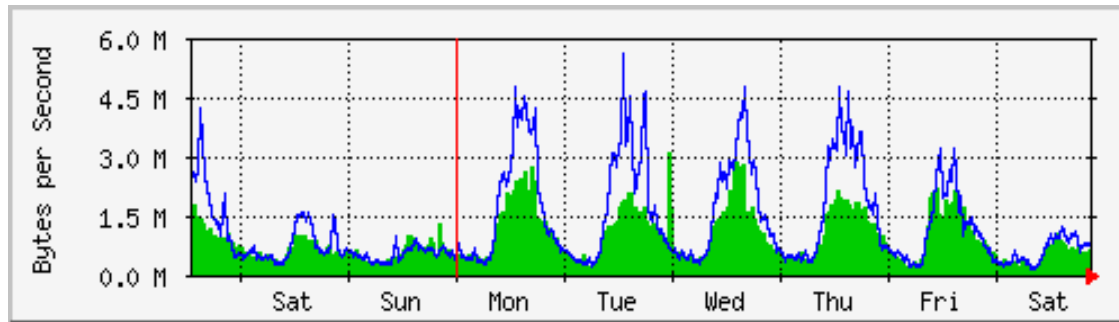
■ Accountingmanagement:

- Nutzerbezogene Verbrauchsmessungen

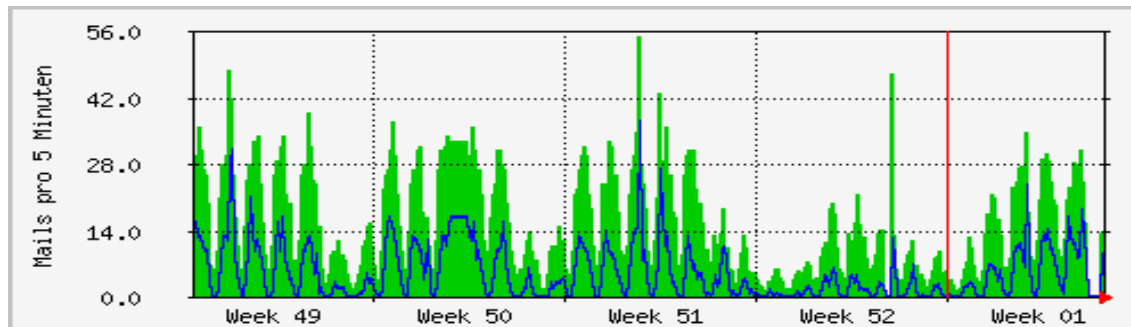
Relativ einfache Visualisierung



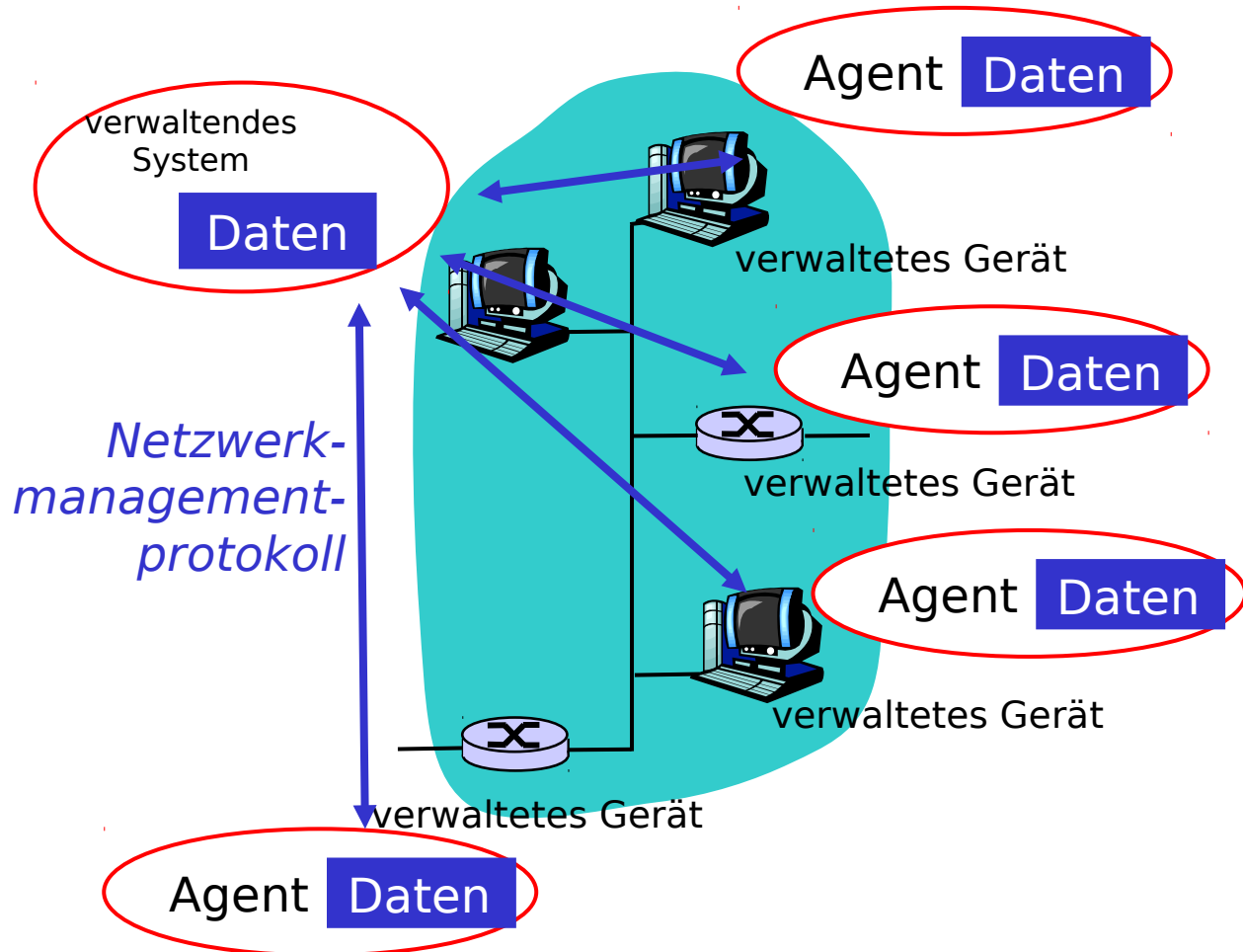
Internet Traffic Monitoring



Mailverkehr



Infrastruktur für das Netzwerkmanagement





Kernbegriffe

- **verwaltete Geräte** enthalten
- **verwaltete Objekte**, deren
- **Daten in einer sogenannte Management Information Base (MIB) gesammelt werden**

Ursprünge in dem OSI CMIP: Common Management Information Protocol

- In den 80er Jahren entworfen mit dem Ziel, einen einheitlichen Netzwerkmanagementstandard zu entwerfen
- Viel zu schleppend standardisiert und deswegen von weiteren Entwicklungen „überrollt“

SNMP:

Simple Network Management Protocol



- **Auch das Internet braucht ein Netzwerkmanagement**
 - kleine, bescheidene Anfänge
 - 1988 als Übergangslösung entworfen (RFC 1157)
 - schnelle Verbreitung
- **Zuwachs an Mächtigkeit und Komplexität bis heute zum aktuellen SNMPv3**
- **De-facto-Netzwerkmanagement-Standard**



SNMP-Protokoll



Zentrale Elemente des SNMP

■ Structure of Management Information (SMI)

- Datendefinitionssprache für MIB-Objekte zur Beschreibung der allgemeinen Struktur (Anordnung, Typen,...) von Informationen
- Generischer Typ: Managed Object
- Generische Datenstruktur: 2-dim. Table

■ Management Information Base (MIB)

- verteilter Speicher für Netzwerkmanagement-Daten
- Beschreibung der konkreten Objekte
- Offene Konzeption der Datenspeicherung



Zentrale Elemente des SNMP (2)

■ SNMP-Protokoll

- Regelt die Kommunikation zwischen Netzwerkmanagementsystem und Agenten
- Übertragung von Information zwischen verwaltender und verwalteter Einheit sowie von Befehlen

■ Sicherheit und Administration

- erst wesentliche Neuerung in SNMPv3



SNMP-Modell

- **Bestandteile des übergreifenden NMM-Modells:**
 - Leistungsfähige Network Management Station
 - Managed Nodes, ausgestattet mit SNMP Agenten
 - Proxy-Agents zur Einbindung von Nicht-SNMP-Systemen
- **Protokoll selbst benutzt einfachen Datagramm-Dienst zur Nachrichtenübermittlung**
- **Zielsystemunabhängige Strukturbeschreibung in ASN.1**



Netzwerkmanagementsysteme

Das Modell bietet den Managementrahmen, selbst aber keine Applikationen. Hierfür wird Netzwerkmanagementsoftware benötigt.

Beispiele:

- **HP OpenView**
 - **IBM Tivoli**
 - **CA Unicenter TNG + Spectrum**
- ... und viele kleinere Lösungen**



Netzwerkmanagementsysteme (2)

Ihre Aufgaben sind:

- Sammeln und Verarbeiten der Netzwerkinformationen
- Visualisierung der Netzwerkstrukturen und -zustände
- Entdecken und Lokalisieren von Störungen/Alarmen
- Automatische Störungsbeseitigung (soweit möglich)
- Unterstützung bei der Netzwerkkonfiguration
- Netzwerk-Accounting
- ...



Netzwerkmanagementsysteme (3)

■ Discovery + Polling

- Erkennung und Überwachung der Netzstruktur via ICMP und SNMP

■ Standard MIB

- Erkennung und Verarbeitung der Standardfunktionen aller Geräte (z.B. Interfaces)

■ Private MIBs

- Erkennung und Verarbeitung geräte-spezifischer Funktionen (z.B. Cisco Router, ...)

Modellinformationen der Geräte/Hersteller werden im NMS benötigt!



Datendefinitionssprache

**Zweck: wohldefinierte
und eindeutige
Syntax und Semantik
von
Managementdaten**

■ **OBJECT-TYPE**

- Datentyp, Status
und Semantik

■ **MODULE-IDENTITY**

- zusammenfassen
von Objekten

■ **Basisdatentypen:**

Integer32

Unsigned32

OCTET STRING

OBJECT IDENTIFIED

IPAddress

Counter32

Counter64

Gauge32

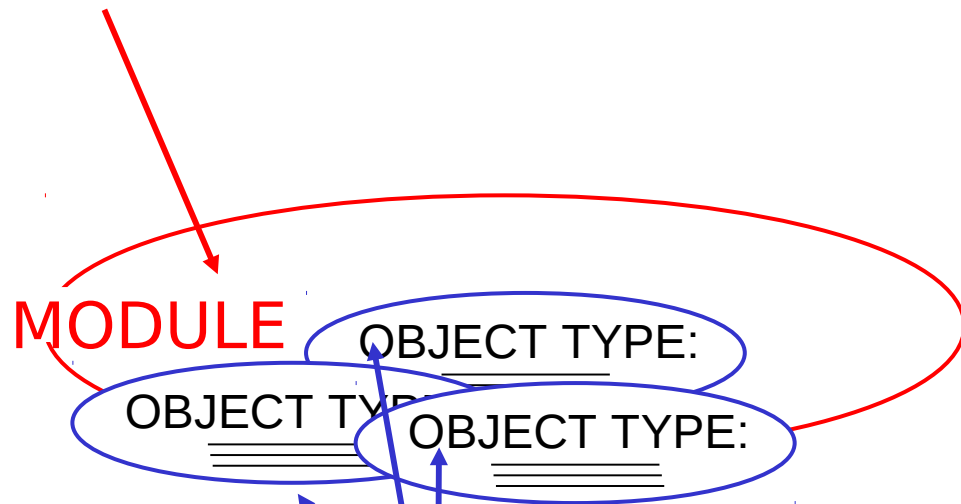
Time Ticks

Opaque



SNMP MIB

MIB-Modul, spezifiziert in der SMI die
MODULE-IDENTITY



ca. 100 Standard-MIBs plus
herstellerspezifische MIBs

Objekte
spezifiziert via SMIs
OBJECT-TYPE-Konstrukt



MIB-Beispiel: UDP-Modul

<u>Object ID</u>	<u>Name</u>	<u>Typ</u>	<u>Kommentar</u>
1.3.6.1.2.1.7.1	UDPInDatagrams	Counter32	Gesamtzahl zugestellter Datagramme an diesem Knoten
1.3.6.1.2.1.7.2	UDPNoPorts	Counter32	Gesamtzahl unzustellbarer Datagramme, keine Anwendung
1.3.6.1.2.1.7.3	UDInErrors	Counter32	Gesamtzahl unzustellbarer Datagramme, andere Gründe
1.3.6.1.2.1.7.4	UDPOutDatagrams	Counter32	Zahl gesendeter Datagramme
1.3.6.1.2.1.7.5	udpTable	SEQUENCE	Ein Eintrag pro verwendetem Port, Portnummer + IP



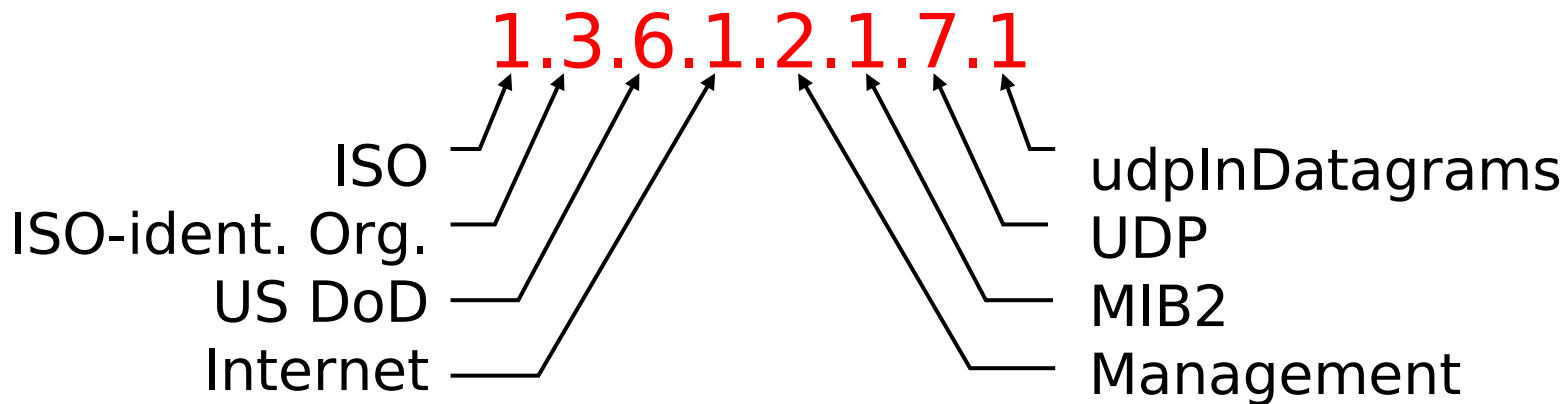
SNMP-Namensschema

Wie kann man jedes mögliche Standardobjekt (Protokoll, Daten,...) in jedem möglichen Netzwerkstandard eindeutig benennen?



SNMP-Namensschema

Wie kann man jedes mögliche Standardobjekt (Protokoll, Daten,...) in jedem möglichen Netzwerkstandard eindeutig benennen?





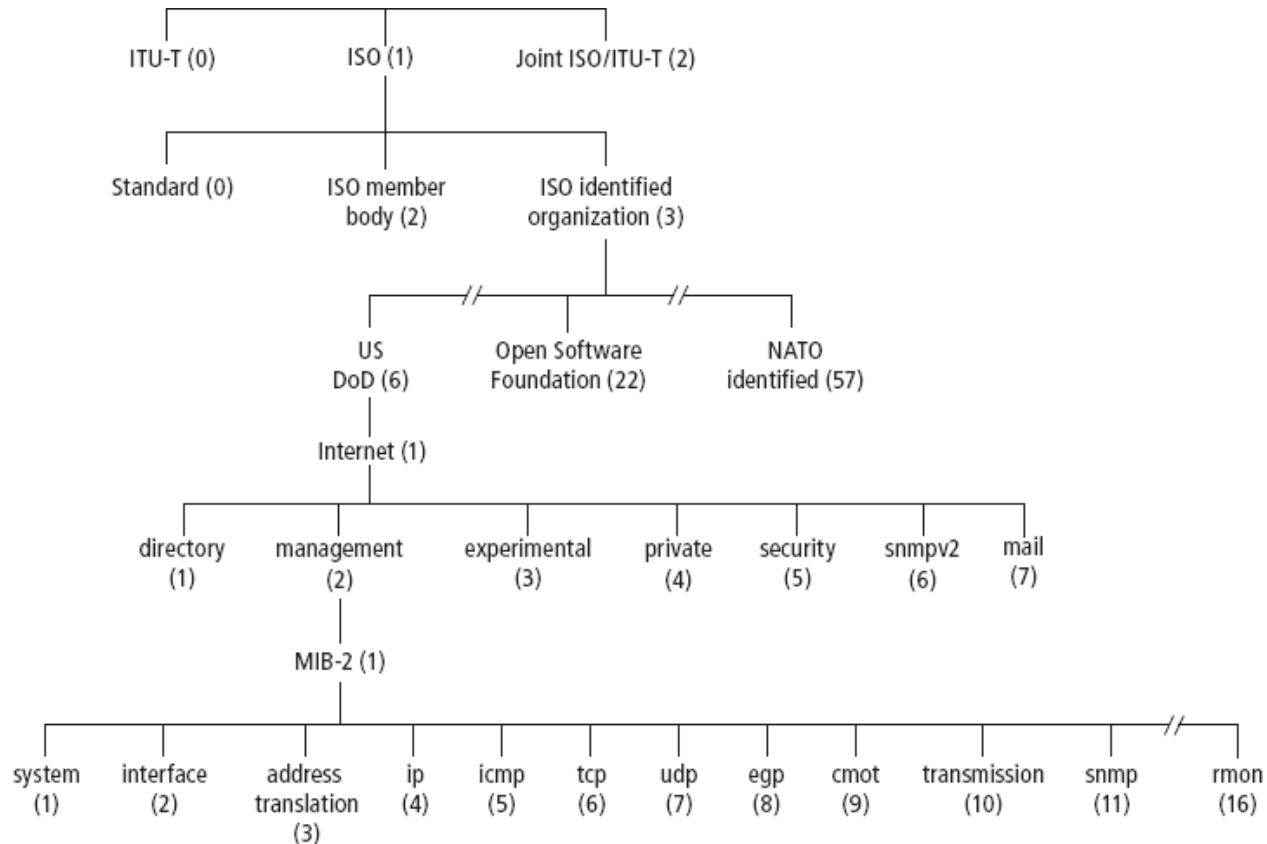
SNMP-Namensschema

Wie kann man jedes mögliche Standardobjekt (Protokoll, Daten,...) in jedem möglichen Netzwerkstandard eindeutig benennen?

- **Antwort: ISO-Objektkennzeichnungsbaum:**
 - hierarchische Benennung aller Objekte
 - jede Verzweigung hat einen Namen und eine Nummer

1.3.6.1.2.1.7.1

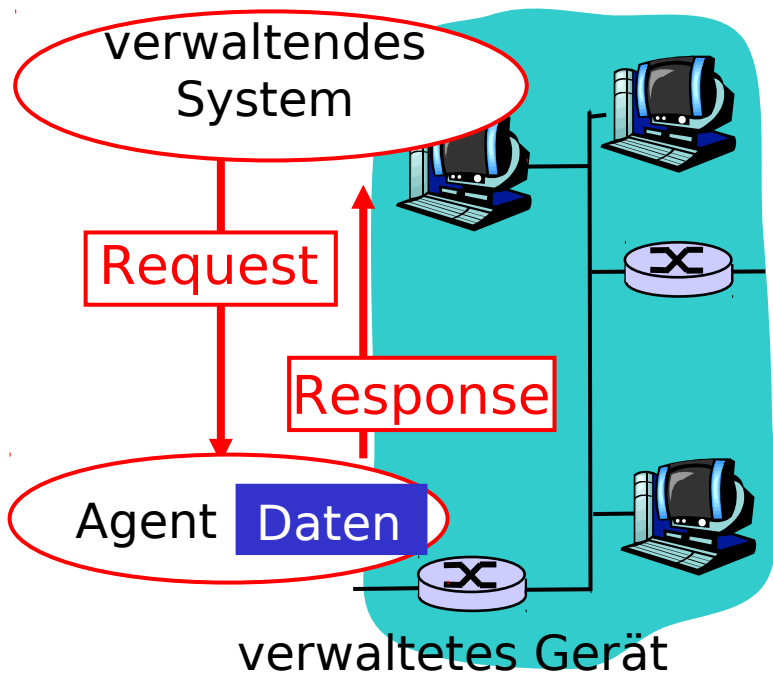
Objektkennzeichnungsbaum



Siehe auch: www.alvestrand.no/harald/objectid/top.html



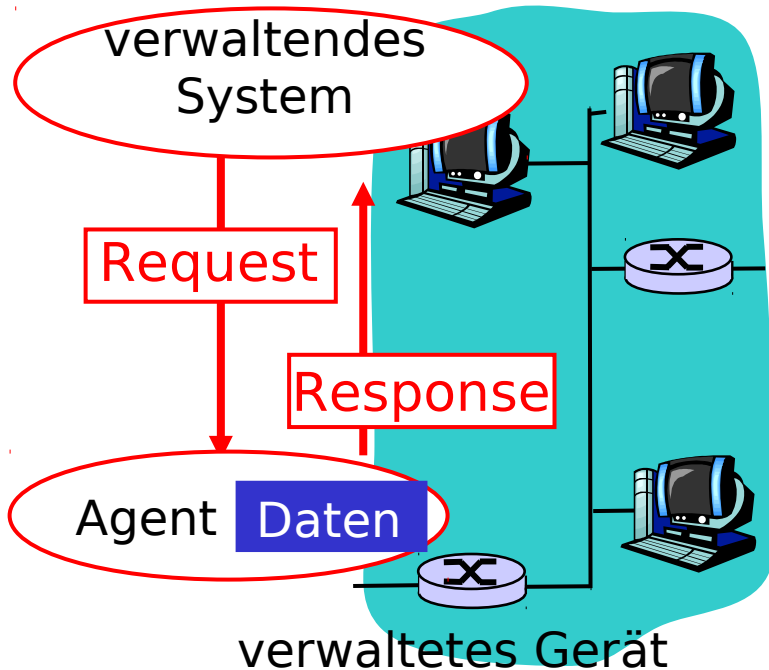
SNMP-Protokoll: MIB-Abfragen



Request-Response-Modus



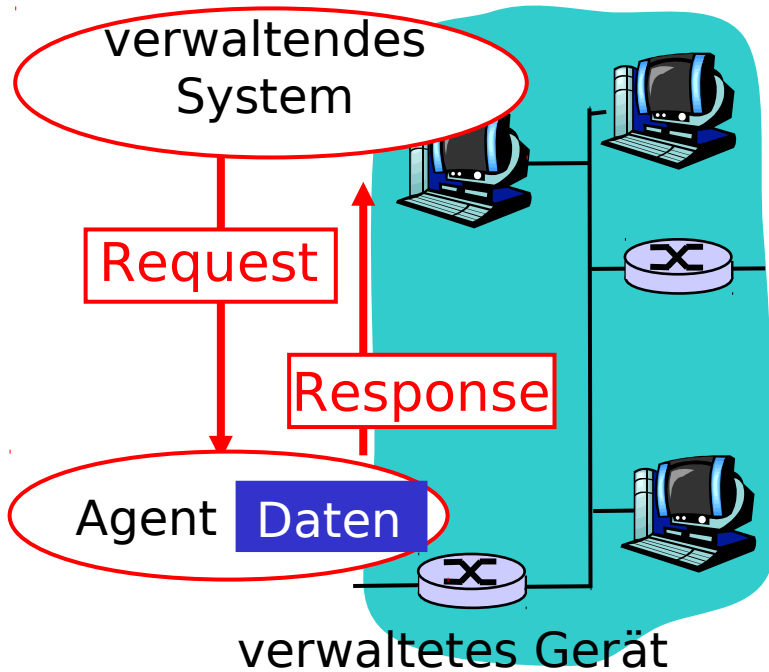
SNMP-Protokoll: MIB-Abfragen



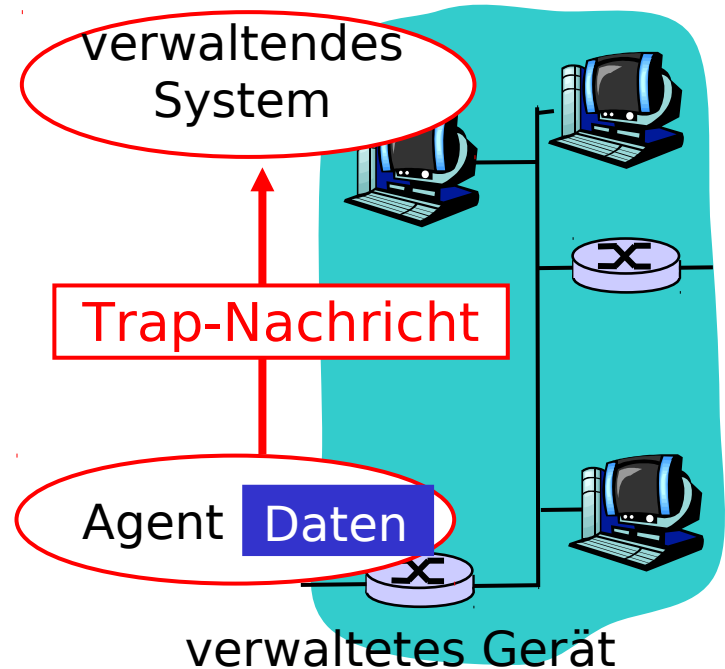
**... aber
immer
nur
pullen?**

Request-Response-Modus

SNMP-Protokoll: Nachrichten



Request-Response-Modus



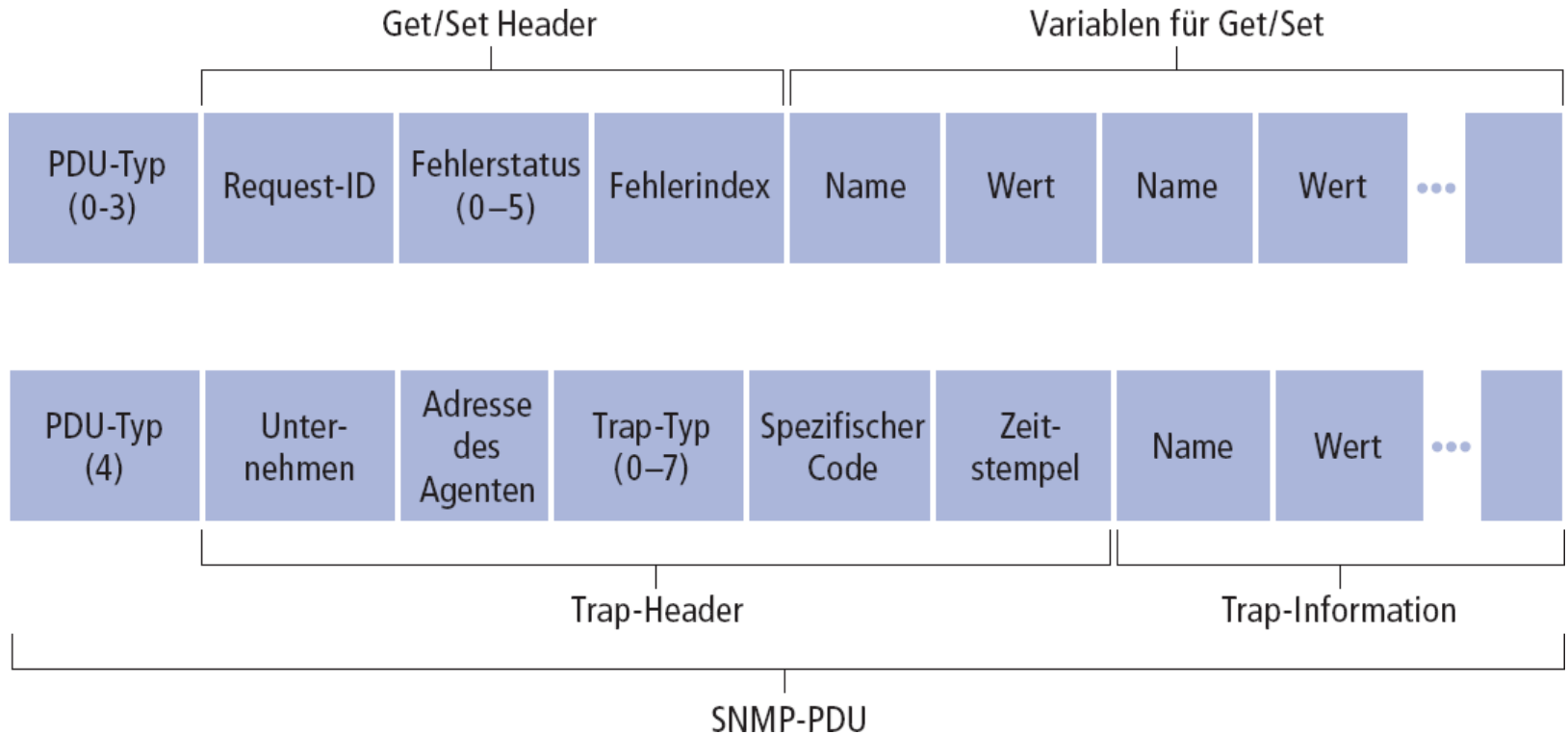
Trap-Modus

SNMP: Nachrichtentypen



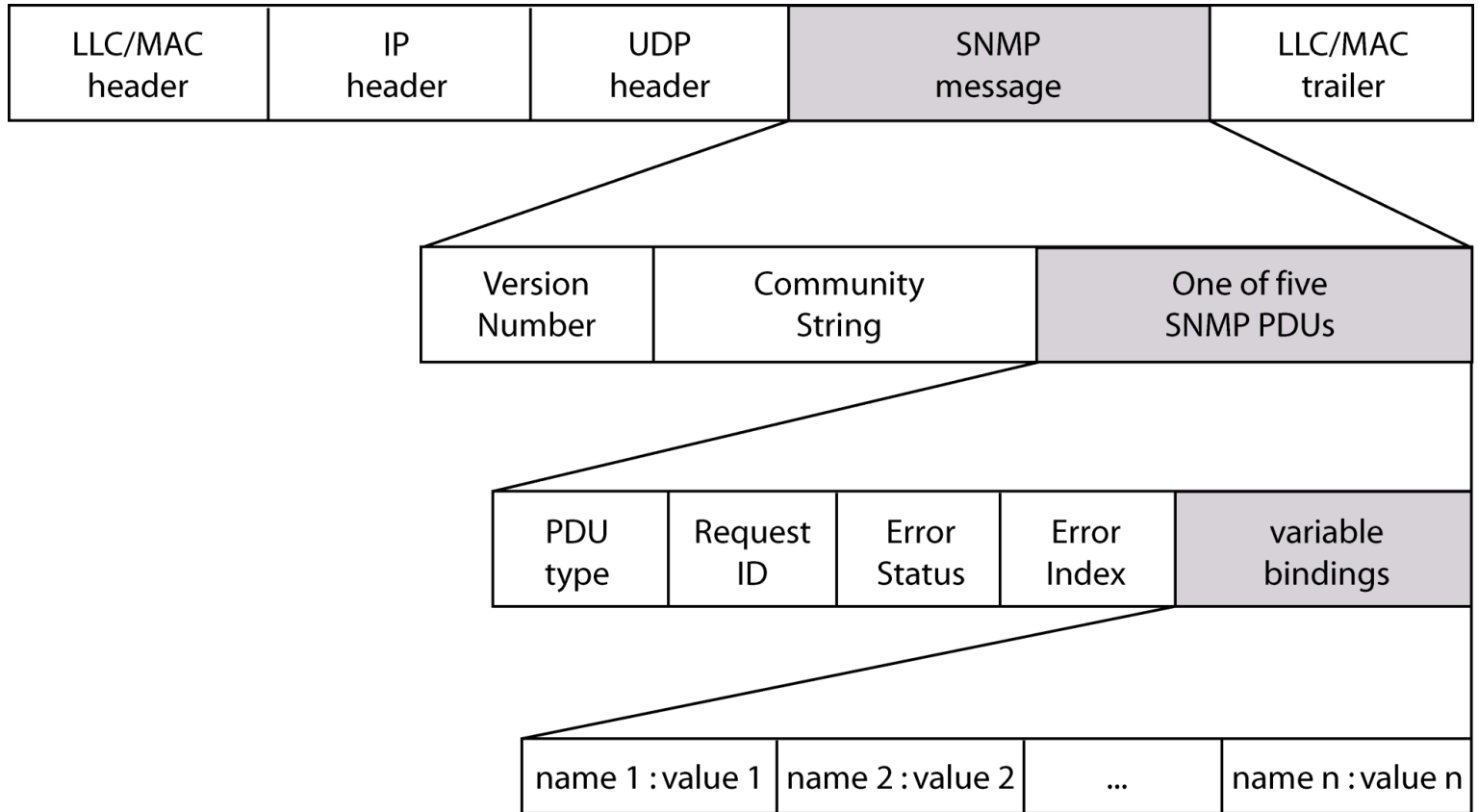
<u>Nachrichtentyp</u>	<u>Funktion</u>
GetRequest GetNextRequest GetBulkRequest	Verwaltendes System (Mgr) an Agent: "gib mir Daten" (Instanz, nächster in Liste, Block)
InformRequest	Mgr an Mgr: "hier ist ein MIB-Wert"
SetRequest	Mgr an Agent: "setze MIB-Wert"
Response	Agent an Mgr: "hier ist der angefragte Wert"
Trap	Agent an Mgr: "hier gibt es ein außergewöhnliches Ereignis"

SNMP: Nachrichtenformate





SNMP: Nachrichtenformate (2)





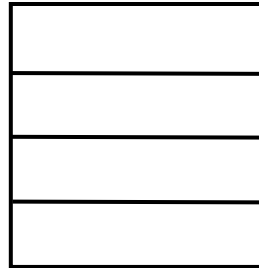
ASN.1



Das Darstellungsproblem

Frage: löst eine perfekte Speicher-zu-Speicher-Kopie das “Kommunikationsproblem”?

```
struct {  
    char code;  
    int x;  
} test;  
test.x = 256;  
test.code='a'
```





Das Darstellungsproblem

Frage: löst eine perfekte Speicher-zu-Speicher-Kopie das “Kommunikationsproblem”?

```
struct {  
    char code;  
    int x;  
} test;  
test.x = 256;  
test.code='a'
```

test.code	a
test.x	00000001
	00000011

Format von Host 1

Das Darstellungsproblem



Frage: löst eine perfekte Speicher-zu-Speicher-Kopie das “Kommunikationsproblem”?

■ Antwort: nicht immer!

```
struct {  
    char code;  
    int x;  
} test;  
test.x = 256;  
test.code='a'
```

test.code	a
test.x	00000001
	00000011

Format von Host 1

test.code	a
test.x	00000011
	00000001

Format von Host 2



**Wie geht denn das in
unserer Welt?**





Verfügbare Lösungsansätze

- **Sender informiert sich über Format des Empfängers, konvertiert die Daten in dieses Format, sendet dann.**
- **Sender sendet, Empfänger informiert sich über das Format des Senders, Empfänger konvertiert die Daten.**
- **Sender konvertiert in ein Host-unabhängiges Format, sendet dann, Empfänger konvertiert in sein eigenes Format.**



Genutzter Lösungsansatz

- ~~Sender informiert sich über Format des Empfängers, konvertiert die Daten in dieses Format, sendet dann.~~
- ~~Sender sendet, Empfänger informiert sich über das Format des Senders, Empfänger konvertiert die Daten.~~
- Sender konvertiert in ein Host-unabhängiges Format, sendet dann, Empfänger konvertiert in sein eigenes Format.



ASN.1: Abstract Syntax Notation 1

- **ISO-Standard X.680**

- häufig im Internet benutzt, manchmal überraschend

- **definierte Datentypen, Objekt-Konstrukturen (ähnlich der SMI)**

- **BER: Basic Encoding Rules**

- legen fest, wie ASN.1-definierte Objekte übertragen werden
 - jedes übertragene Objekt verwendet TLV-Encoding (type, length, value)



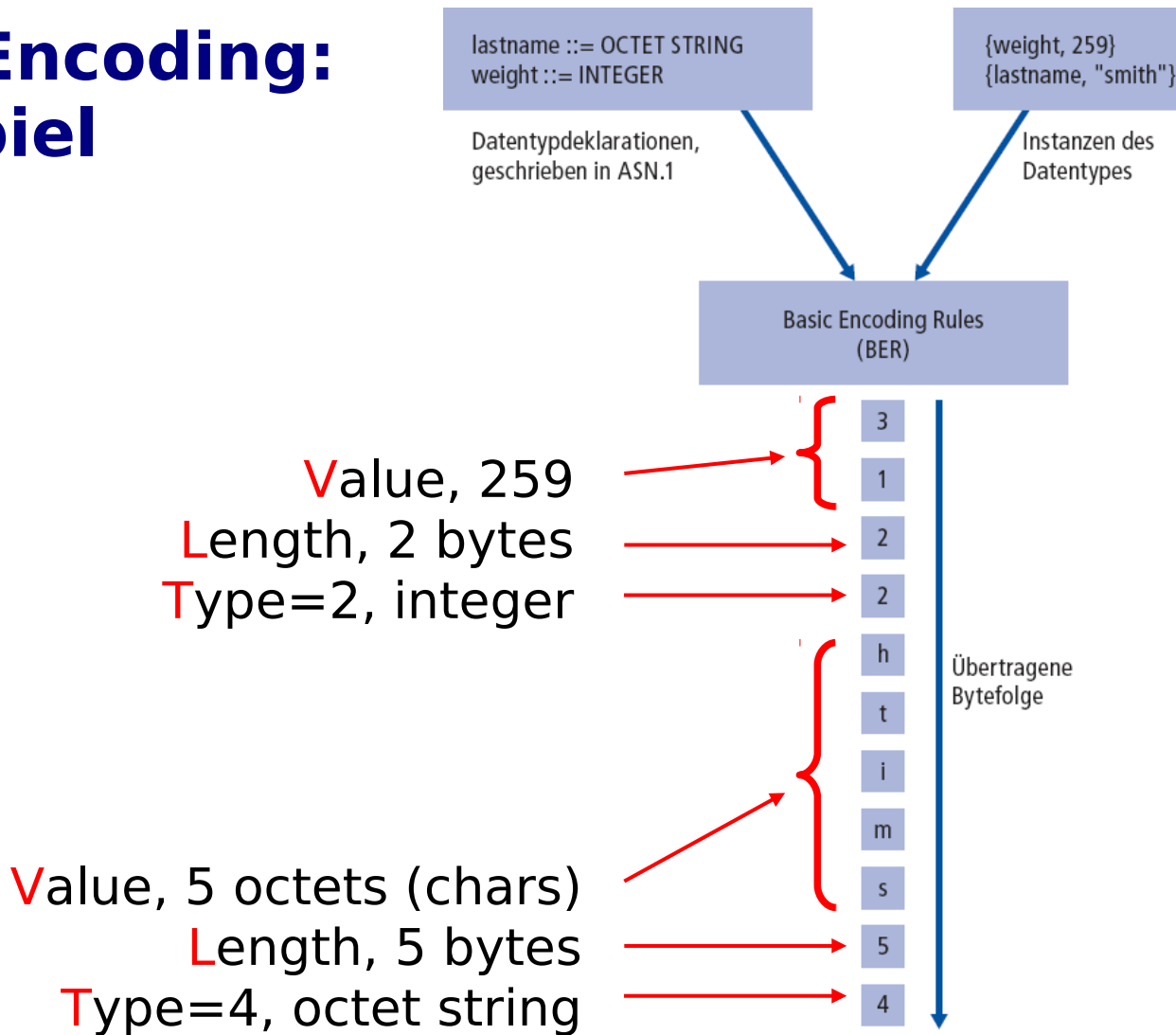
TLV-Encoding

Grundlegende Idee: die übertragenen Daten sind selbstspezifizierend!

- T: Datentyp, einer der von ASN.1 definierten Typen
- L: Länge der Daten in Bytes
- V: Wert, kodiert gemäß ASN.1-Standard

<u>Angabe</u>	<u>Type</u>
1	Boolean
2	Integer
3	Bitstring
4	Octet string
5	Null
6	Object Identifier
9	Real

TLV-Encoding: Beispiel





Updates durch SNMPv2

- **SNMPv2 erweitert SNMPv1 um**
 - Manager-Manager Messages (InformRequest)
 - GetBulkRequest PDU
 - Erweiterung der SMI



Updates durch SNMPv3

■ SNMPv3 ::=

SNMPv2 + Security + Administration

- Vollständig abwärtskompatibel zu SNMPv1 und SNMPv2*
- User-based Security Model (USM):
Authentifikation und Verschlüsselung
- View-based Access Control (VACM):
Reguliert Zugriff auf MIB



Bewertung

■ Netzwerkmanagement

- extrem wichtig: 80% der “Kosten” eines Netzwerks sind diesem Bereich zuzuordnen
- ASN.1 für die Datendarstellung
- SNMP-Protokoll zur Übermittlung

■ Noch immer eher Kunst als Wissenschaft

- was soll man messen oder beobachten?
- wie soll man auf Ausfälle reagieren?
- wie werden Alarme korreliert und gefiltert?



Bewertung (2)

- **Das SNMP-Konzept bietet einen einfachen Standard zum Management großer, heterogener Netze:**
 - Bereitstellung ausreichender Informationen (MIB)
 - „Intelligenz“ des Managementsystems
- **Der technische Entwicklungsstand ist (erst) mit SNMPv3 einsatztauglich**
- **Die Management-Aufgaben entwickeln sich in die Richtung eines Service-Managements**

Kontakt



Prof. Dr. Klaus-Peter Kossakowski

**Email: klaus-peter.kossakowski
 @haw-hamburg.de**

Mobil: +49 171 5767010

<https://users.informatik.haw-hamburg.de/~kpk/>