Netzwerkmanagement

1. Aufgaben des Netzwerkmanagements
2. Der Standard SNMP
3. Die Management Information Base
4. Die Protokolle SNMP – SNMPv3
5. Management-Systeme

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Zum Inhalt

In diesem Kapitel lernen wir Netzwerkkomponenten von einer anderen Seite kennen – ihrem Management Interface. Alle Grundfunktionen spiegeln sich hier wider und tauchen unter eigenen ‚Management-Namen' auf. Dies ist u.a. deshalb interessant, weil wir so die Funktion der Router, Switches und Hosts in Aktion beobachen können.

Leider hat Tanenbaum dieses Thema übersprungen, im Meinel/Sack gibt es das kleine Unterkapitel 9.2 – Literatur gibt's am Ende des Abschnitts.

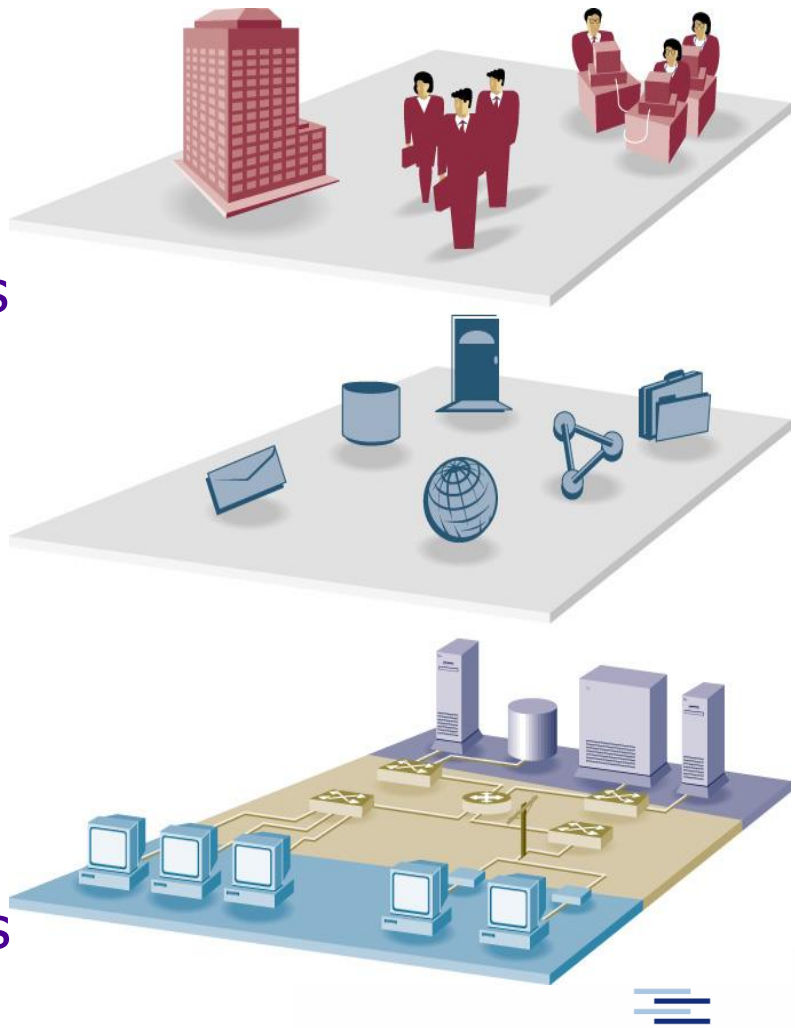
1. Motivation

- Große, räumlich verteilte Netze
- Viele, verschiedenartige Netzwerkkomponenten
- Funktionskritische Basisdienste
- Neue, leistungskomplexe Anwenderdienste
- Hohe Anforderungen an Sicherheit & Verfügbarkeit

⇒ Wir benötigen systemübergreifende, leistungsfähige Managementwerkzeuge

1. Wer benötigt Management ?

- Anwender & Rollen
  - Authentifikation & Identität
  - Addressierung
  - Roaming Profiles & Services
- Anwendungen & Dienste
  - Mail, DNS, …
  - IP Telefonie, Broadcasting
- Geräte & Infrastruktur
  - Router, Switches, Server, …
  - Bandbreite, Buffers, Policies



1. Aufgaben des Netzwerkmanagements

Fehlermanagement:

Erkennen, Isolieren und Beheben von Störungen

Konfigurationsmanagement:

Auslesen und Einstellen der Konfigurationsparameter

Performancemanagement:

Sammeln und Bewerten von Betriebsdaten

Accountingmanagement:

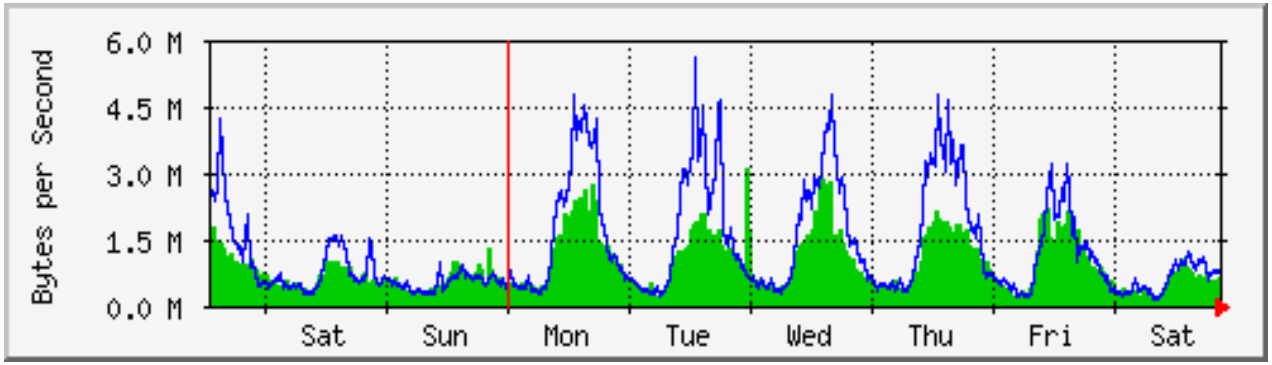
Nutzerbezogene Verbrauchsmessungen

Sicherheitsmanagement:

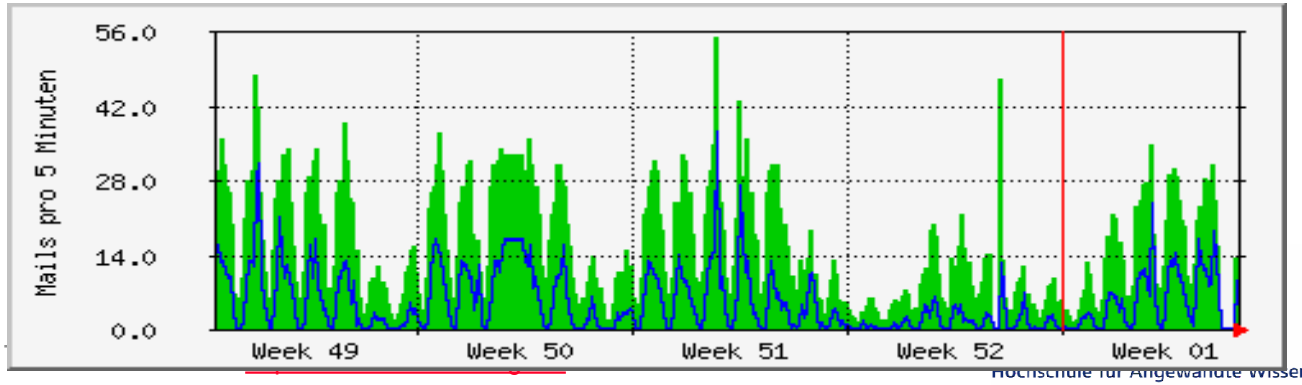
Dokumentation und Abwehr unerlaubter Zugriffe

1. Beispiel: Lastvisualisierung

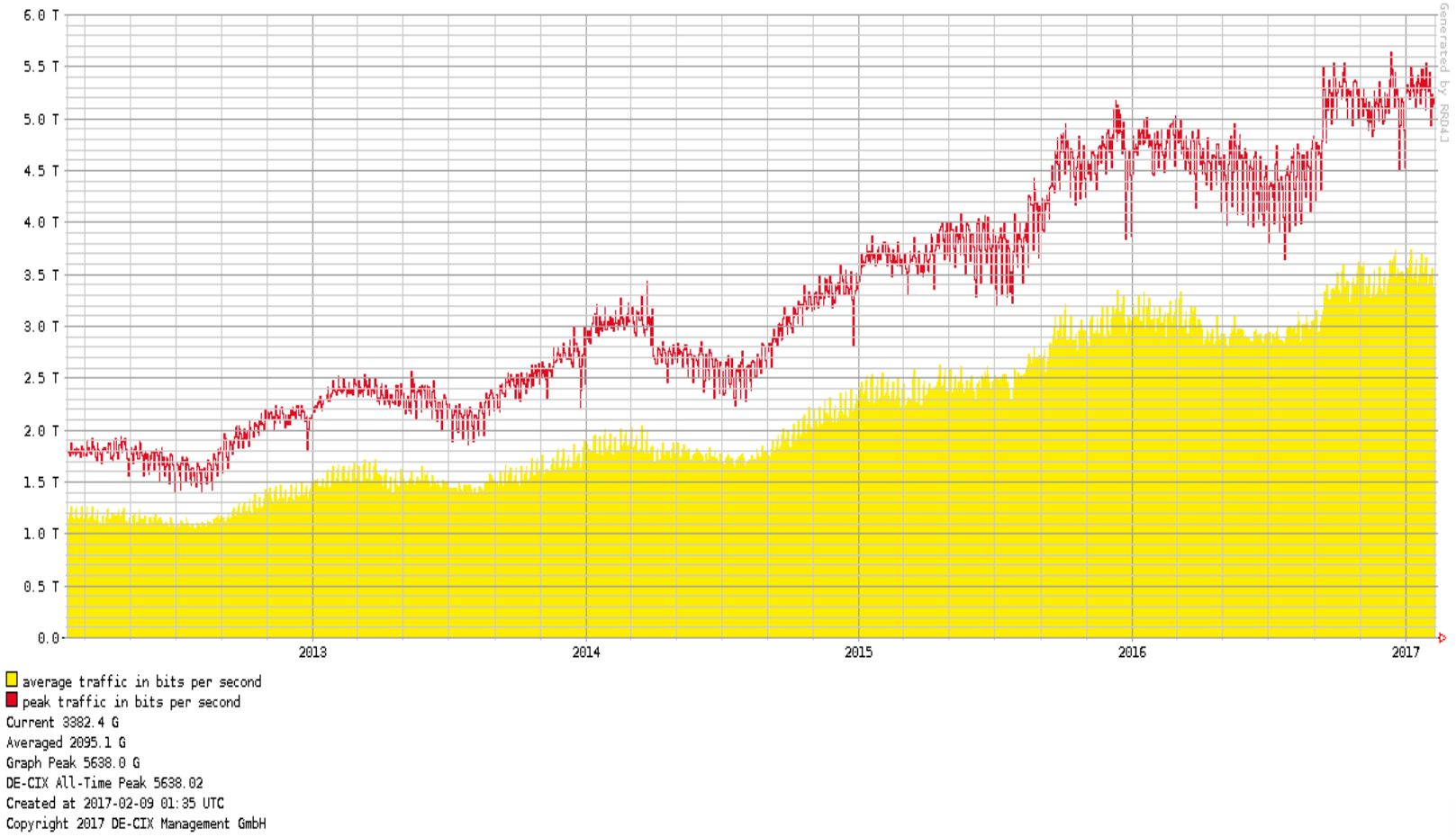
Internet Traffic Monitoring



Mailverkehr



1. Traffic Load @ DE-CIX Frankfurt



2. Der Standard SNMP

Der einzige ernst zu nehmende Standard für Managementaufgaben (auch für nicht primäre IP-Geräte): **S**imple **N**etwork **M**anagement **P**rotocol

- 1988 als Übergangslösung entworfen (RFC 1157)
- Gegenwärtig Version 2 (SNMPv3) (RFCs 3414, 3416)
- Benutzt einfachen Datagramm-Dienst zur Nachrichtenübermittlung
- SNMP Bestandteil eines übergreifenden NMM-Modells:
  - Managed Nodes, ausgestattet mit SNMP Agenten
  - Leistungsfähige Network Management Station
  - Proxy Agents zur Einbindung von Nicht-SNMP-Systemen
  - Zielsystemunabhängige Strukturbeschreibung in ASN.1

2. Struktur der Informationen

- **SMI: S**tructure and Identification of **M**anaged **I**nformation
  - Informationsmodell zur Beschreibung der allgemeinen Struktur (Anordnung, Typen,...) von Informationen
  - Generischer Typ: **Managed Object**
  - Generische Datenstruktur: **2-dim. Table**
- **MIB: M**anagement **I**nformation **B**ase
  - Beschreibung der konkreten Objekte
  - Offene Konzeption der Datenspeicherung
- **SNMP: S**imple **N**etwork **M**anagement **P**rotocol
  - Regelt die Kommunikation zwischen Netzwerkmanagementsystem und Agenten

2. SMI

Managed Objects repräsentieren verwaltete Ressourcen als Zustands- oder Ereignisvariablen

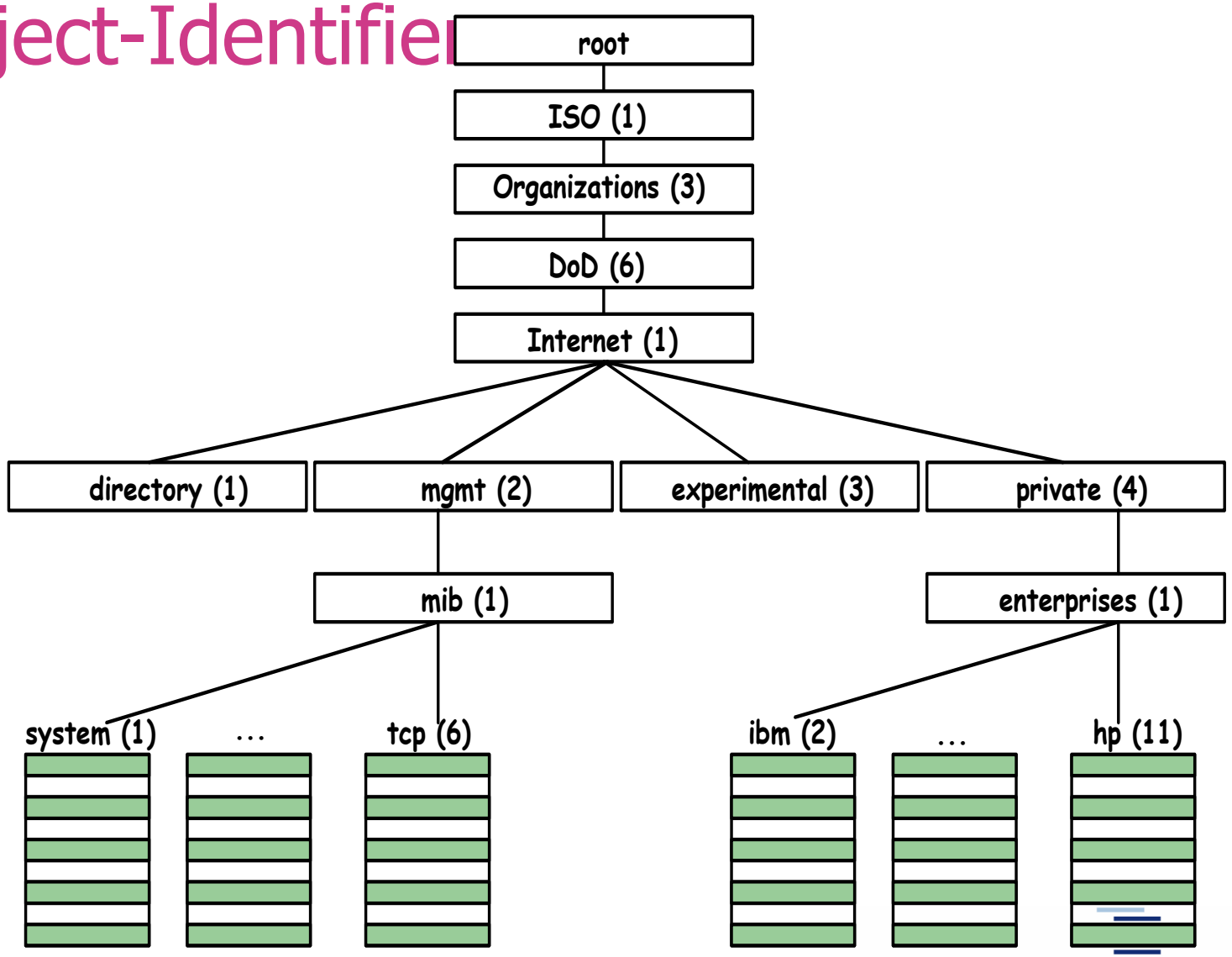
Probleme:

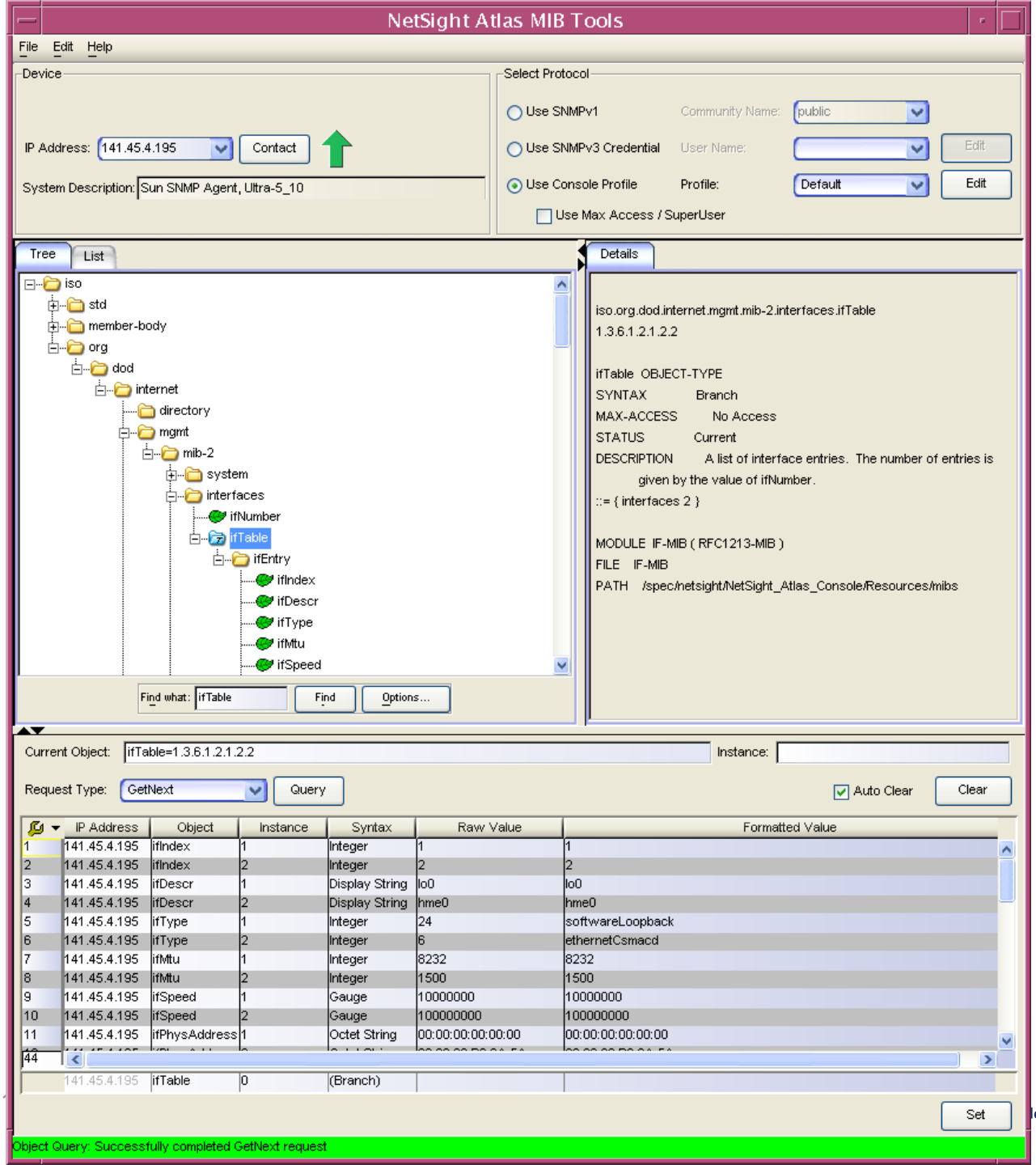
- Objekte zur Repräsentation von spezifischen Ressourcen müssen auf allen Systemen die gleichen sein
- Ein allgemeingültiges Schema zur Darstellung wird zur Interoperabilität benötigt

SMI beinhaltet

- eine standardisierte Technologie zur Strukturdefinition von individuellen MIBs
- eine standardisierte Technologie zur Definition individueller Objekte, einschließlich Syntax und (möglicher) Werte jedes Objekts
- eine standardisierte Technologie zur Enkodierung von Objektwerten

2. Baum-Struktur der Object-Identifier




NetSight Atlas MIB Tools
File Edit Help
Device
IP Address: 141.45.4.195
Contact
System Description: Sun SNMP Agent, Ultra-5_10
Select Protocol
Use SNMPv1
Community Name: public
Use SNMPv3 Credential
User Name:
Edit
Use Console Profile
Profile: Default
Edit
Use Max Access / SuperUser
Tree
List
iso
std
member-body
org
dod
internet
directory
mgmt
mib-2
system
interfaces
ifNumber
ifTable
ifEntry
ifIndex
ifDescr
ifType
ifMtu
ifSpeed
Find what: ifTable
Find
Options...
Details
iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable
1.3.6.1.2.1.2.2
ifTable OBJECT-TYPE
SYNTAX Branch
MAX-ACCESS No Access
STATUS Current
DESCRIPTION A list of interface entries. The number of entries is given by the value of ifNumber.
::= { interfaces 2 }
MODULE IF-MIB (RFC1213-MIB)
FILE IF-MIB
PATH /spec/netsight/NetSight_Atlas_Console/Resources/mibs
Current Object: ifTable=1.3.6.1.2.1.2.2
Instance:
Request Type: GetNext
Query
Auto Clear
Clear
IP Address | Object | Instance | Syntax | Raw Value | Formatted Value
1 | 141.45.4.195 | ifIndex | 1 | Integer | 1 | 1
2 | 141.45.4.195 | ifIndex | 2 | Integer | 2 | 2
3 | 141.45.4.195 | ifDescr | 1 | Display String | lo0 | lo0
4 | 141.45.4.195 | ifDescr | 2 | Display String | hme0 | hme0
5 | 141.45.4.195 | ifType | 1 | Integer | 24 | softwareLoopback
6 | 141.45.4.195 | ifType | 2 | Integer | 6 | ethernetCsmacd
7 | 141.45.4.195 | ifMtu | 1 | Integer | 8232 | 8232
8 | 141.45.4.195 | ifMtu | 2 | Integer | 1500 | 1500
9 | 141.45.4.195 | ifSpeed | 1 | Gauge | 10000000 | 10000000
10 | 141.45.4.195 | ifSpeed | 2 | Gauge | 100000000 | 100000000
11 | 141.45.4.195 | ifPhysAddress | 1 | Octet String | 00:00:00:00:00:00 | 00:00:00:00:00:00
44
141.45.4.195 | ifTable | 0 | (Branch)
Set
Object Query: Successfully completed GetNext request

3.

Die

MIB

3. Modellierung der Management-Informationen: MIB and SMI

Structure of Management Information (SMI) Management Information Base (MIB)

sysDescr OBJECT-TYPE

SYNTAX DisplayString (SIZE (0..255))

ACCESS read-only

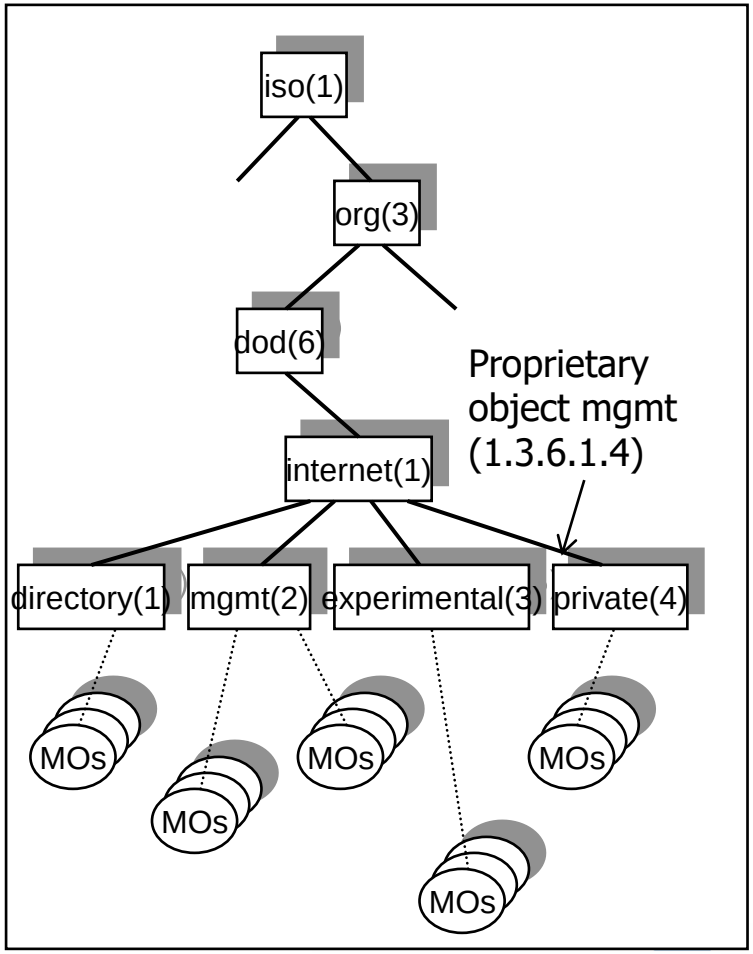
STATUS mandatory

DESCRIPTION

"A textual description of the entity. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software. It is mandatory that this only contains printable ASCII characters."

::= { system 1 } ← Branch (mib.system) and identifier (OID)

meta data for the managed object



distributed database of MOs (a piece of it on each agent)

3. MIB-II (RFC 1213)

MIB-II ist die generische Management Information Base für jeden managebaren Internetknoten (generic SNMP device). Ihre Organisation:

iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1)

- system (1)
- interfaces (2)
- at (3)
- ip (4)
- icmp (5)
- tcp (6)
- udp (7)
- egp (8)
- transmission (10)
- snmp (11)

Erweiterungen/ zusätzliche Teilbäume können definiert werden unter

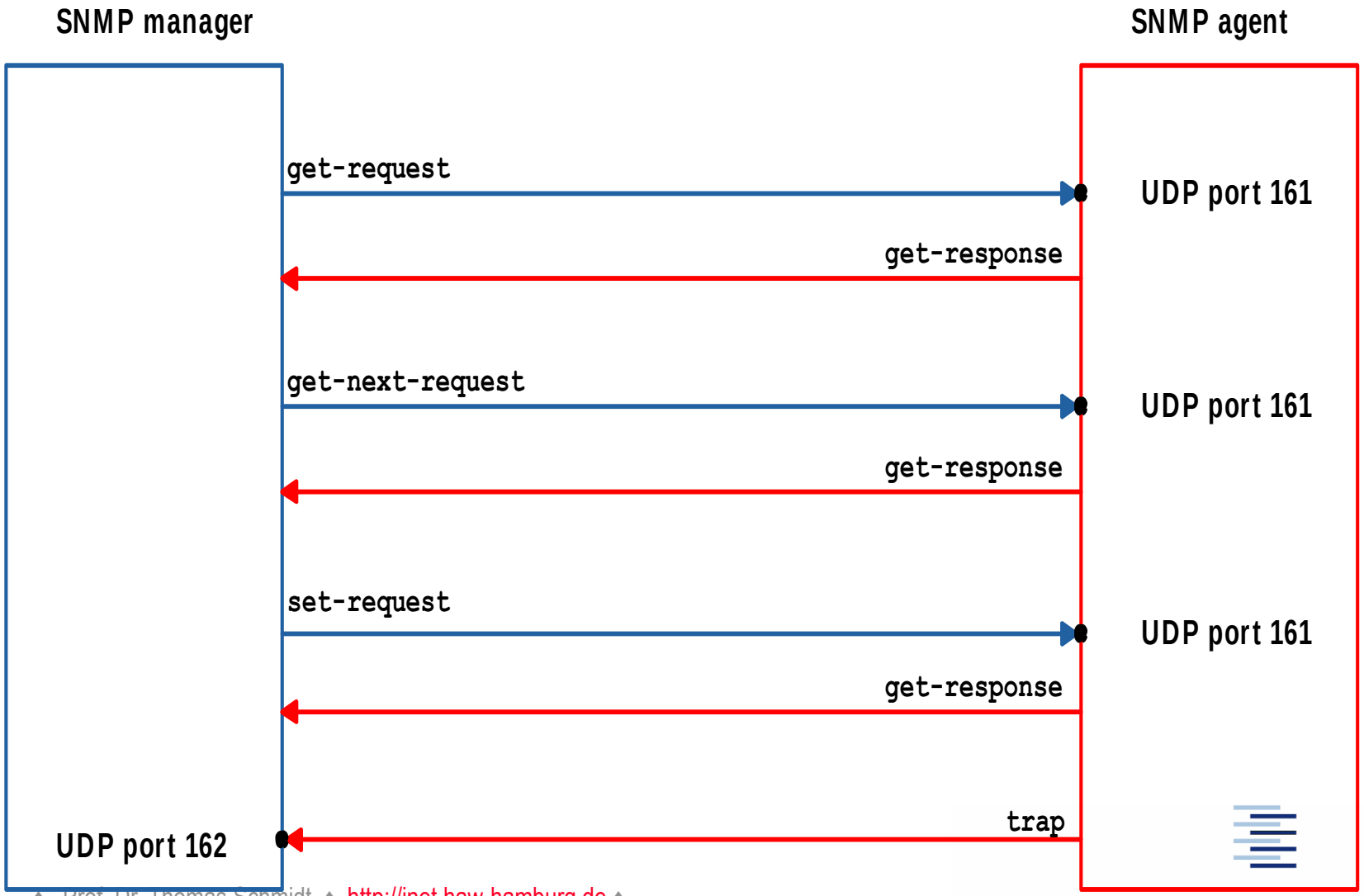
- mib-2 (Für allgemeine Standard-MIBs)
- mgmt oder experimental (für experimentelle MIBs)
- private (für herstellerprivate MIBs).

3. MIB Encoding in Abstract Syntax Notation One

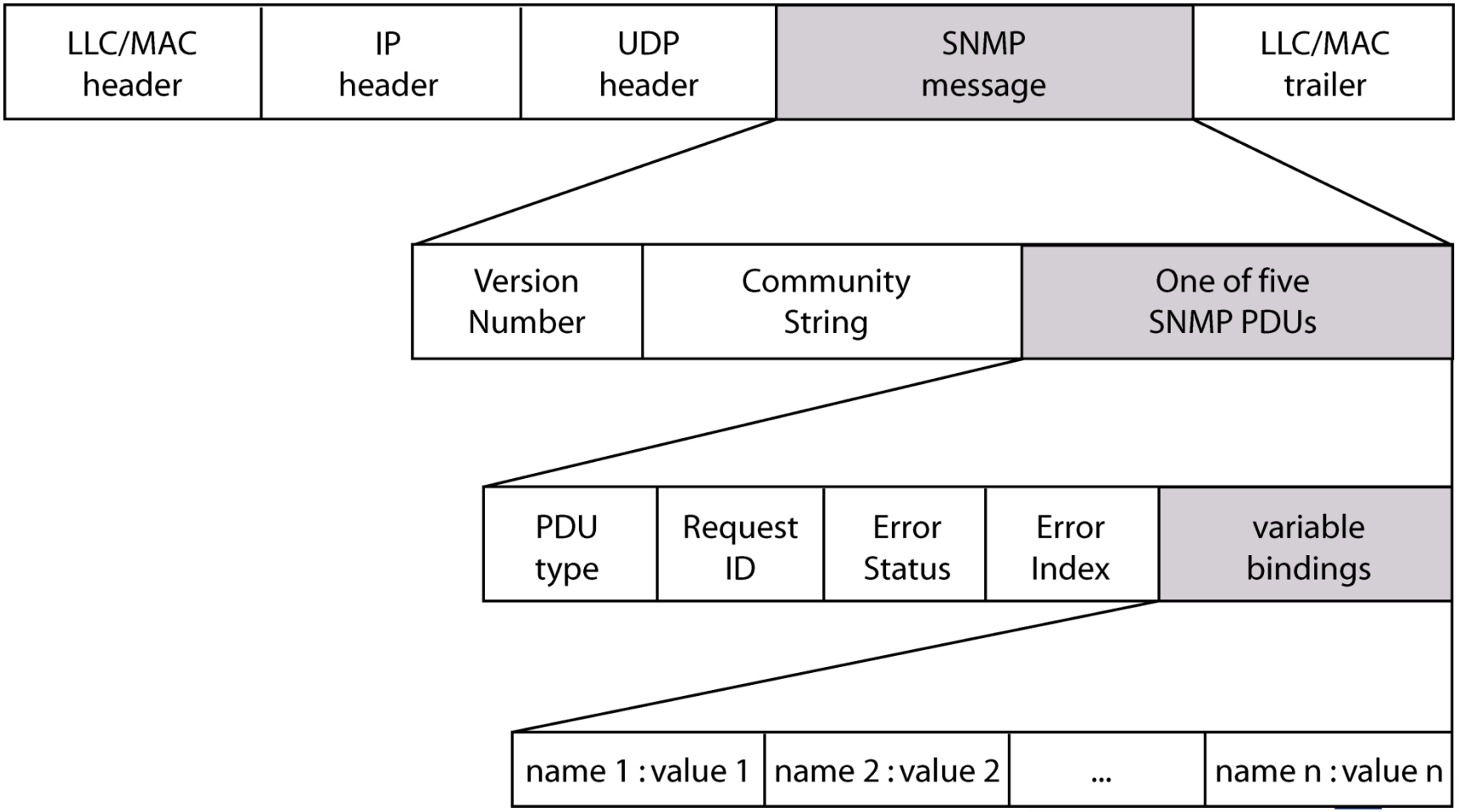
```
IF-MIB DEFINITIONS ::= BEGIN

 IMPORTS
     MODULE-IDENTITY, OBJECT-TYPE, Counter32, Gauge32, Counter64,
     [...]
 ifMIB MODULE-IDENTITY
     LAST-UPDATED "9611031355Z"
     ORGANIZATION "IETF Interfaces MIB Working Group"
     CONTACT-INFO
           "   Keith McCloghrie"
     DESCRIPTION
           "The MIB module to describe generic objects for
     [...]
     ::= { mib-2 31 }

 ifMIBObjects OBJECT IDENTIFIER ::= { ifMIB 1 }

 interfaces   OBJECT IDENTIFIER ::= { mib-2 2 }

 ifTable OBJECT-TYPE
     SYNTAX      SEQUENCE OF IfEntry
     MAX-ACCESS not-accessible
     [...]
     ::= { interfaces 2 }
....
```

```
....
ifTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF IfEntry
    MAX-ACCESS not-accessible
    [...]
    ::= { interfaces 2 }

ifEntry OBJECT-TYPE
    SYNTAX      IfEntry
    [...]
    INDEX   { ifIndex }
    ::= { ifTable 1 }

IfEntry ::= SEQUENCE {
    ifIndex     InterfaceIndex,
    ifDescr     DisplayString,
    ifType      IANAifType,
    ifMtu       Integer32,
    [...]
 }
```

4. SNMP


SNMP manager
SNMP agent
get-request
UDP port 161
get-response
get-next-request
UDP port 161
get-response
set-request
UDP port 161
get-response
trap
UDP port 162

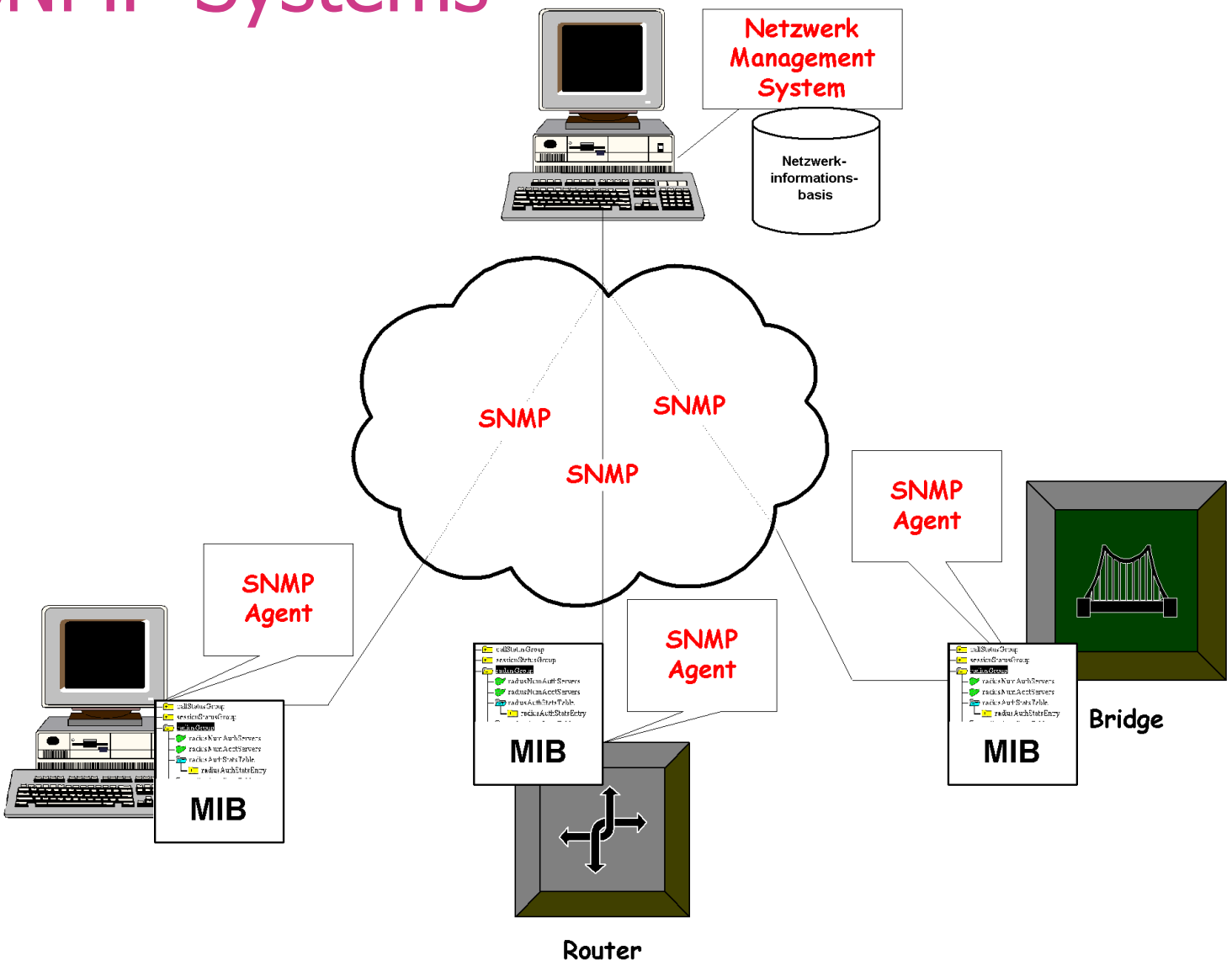
4. SNMP Message



4. SNMPv2/3

- SNMPv2 erweitert SNMPv1 um
  - Manager-Manager Messages (InformRequest)
  - GetBulkRequest PDU
  - Erweiterung der SMI
- SNMPv3 = SNMPv2 + Security + Administration
  - Vollständig aufwärtskompatibel zu SNMPv1 und SNMPv2*
  - User-based Security Model (USM): Authentication & Encryption
  - View-based Access Control (VACM): Reguliert Zugriff auf MIB

4. Architektur des SNMP-Systems



5. Netzwerkmanagementsysteme

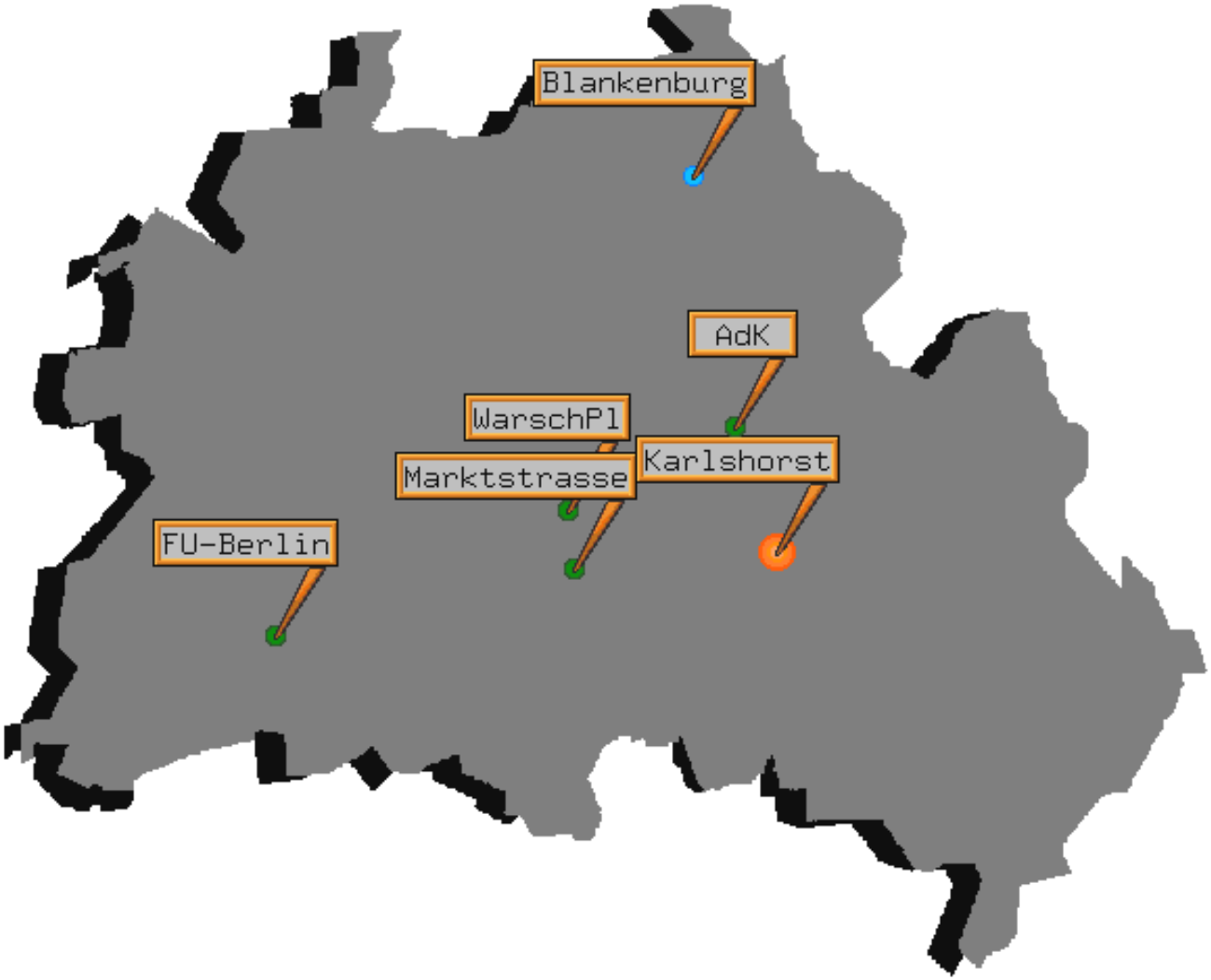
Das SNMP Modell bietet den Managementrahmen, aber keine Applikationen. Hierfür wird Netzwerkmanagementsoftware benötigt.

Ihre Aufgaben sind:

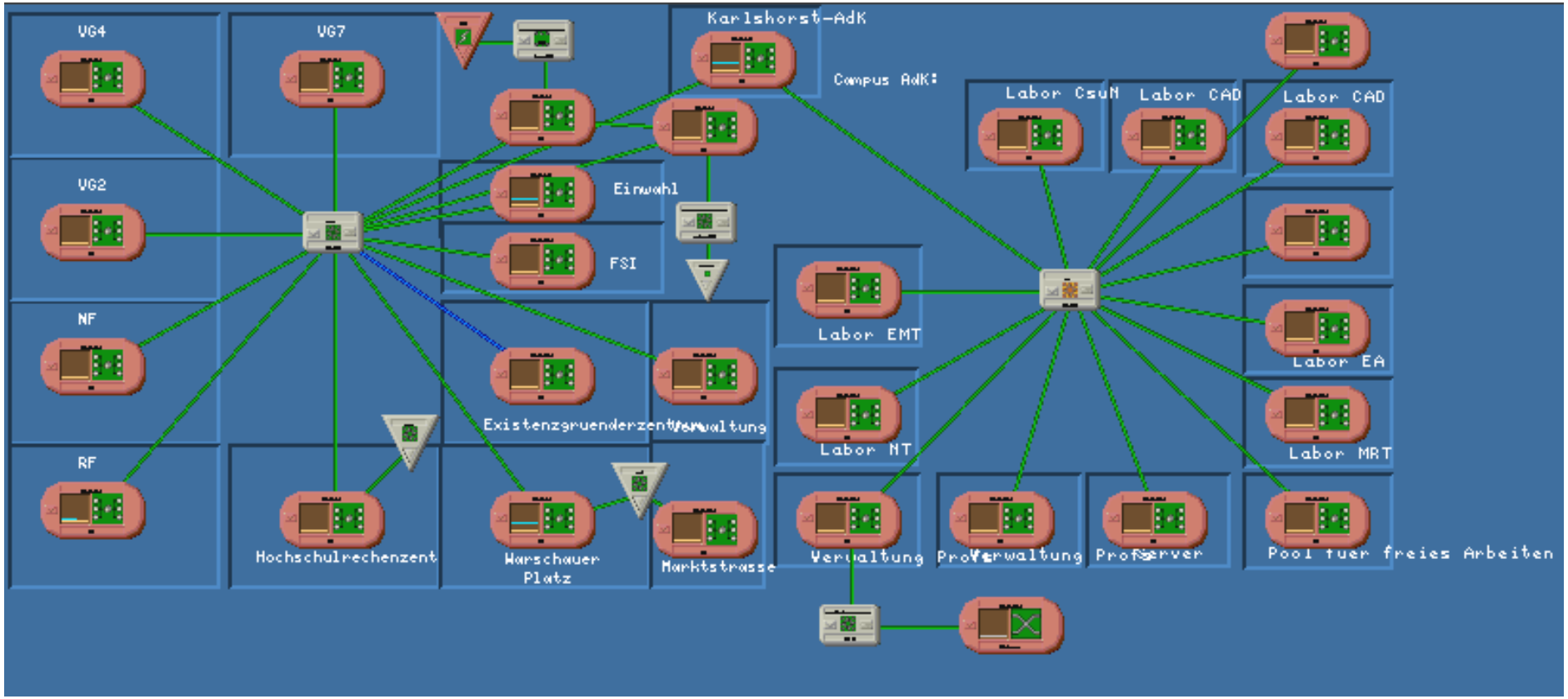
- Sammeln und Verarbeiten der Netzwerkinformationen
- Visualisierung der Netzwerkstrukturen und -zustände
- Entdecken und Lokalisieren von Störungen/Alarmen
- Automatische Störungsbeseitigung (soweit möglich)
- Unterstützung bei der Netzwerkkonfiguration
- Netzwerk-Accounting (ggf.)

Beispiele: CiscoWorks2000, HP Network Management Center (was OpenView), IBM Tivoli, CA Unicenter und viele kleinere Lösungen

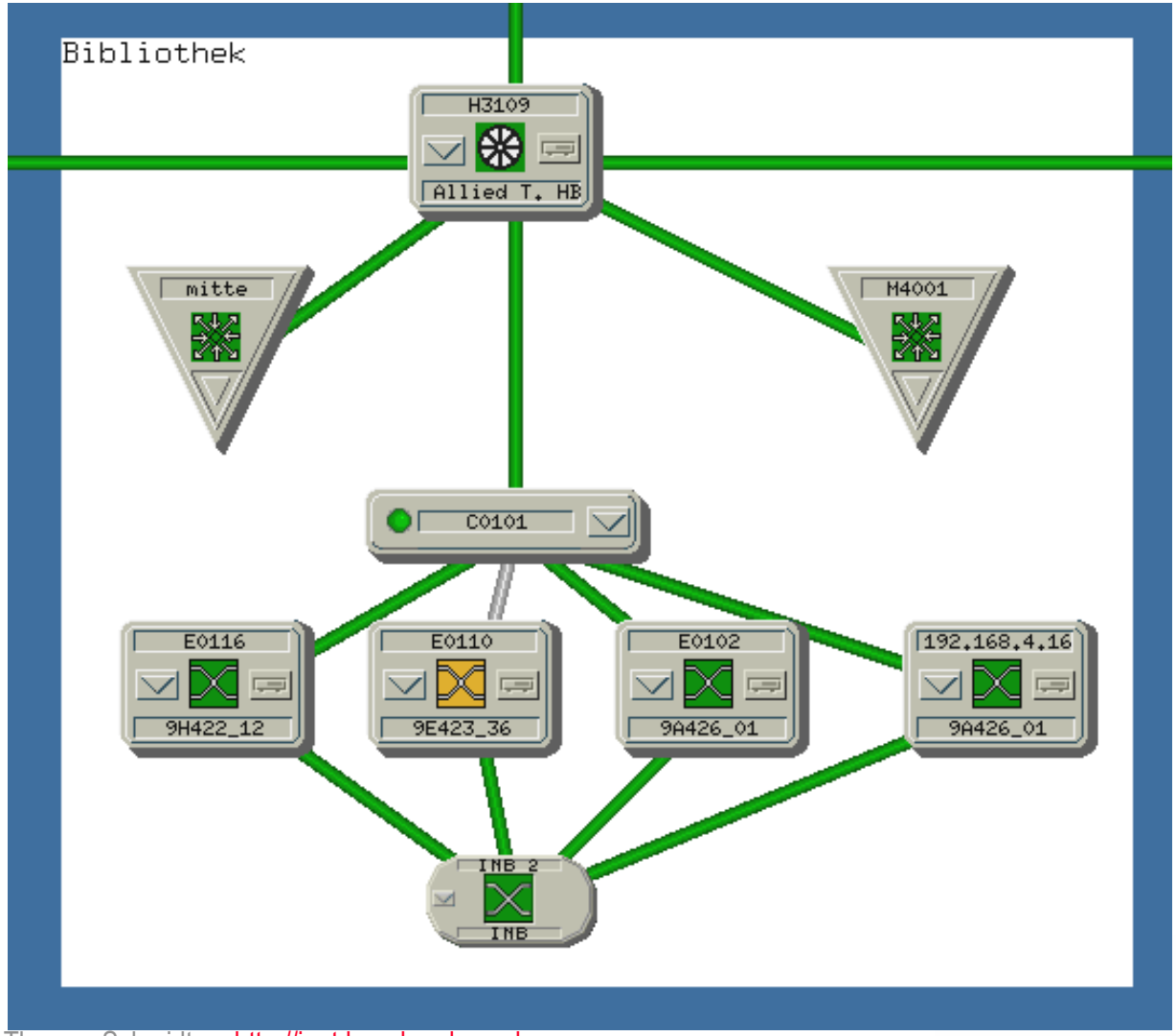
5. Beispiel CA Spectrum



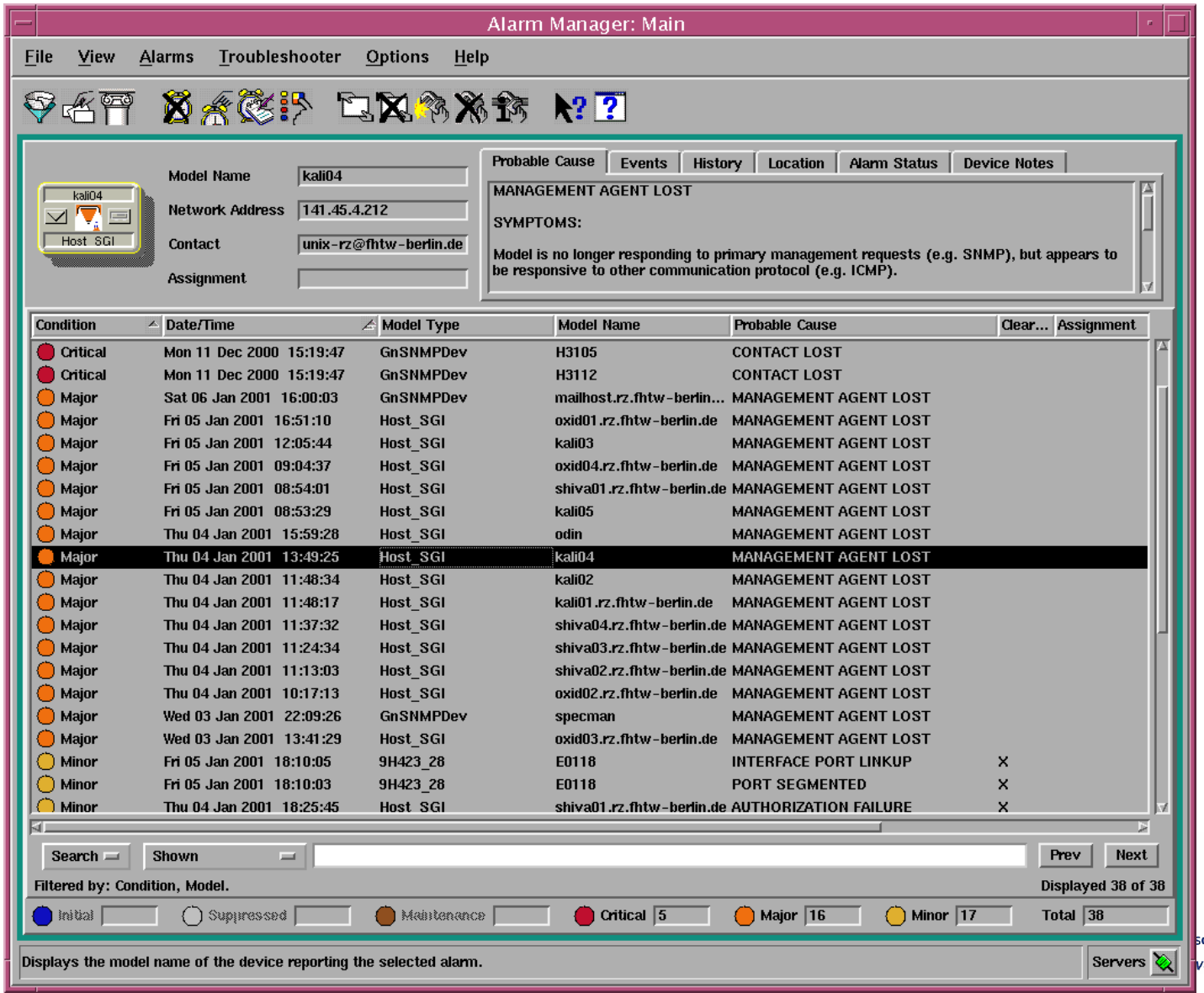
5. Netzübersicht



5. Detailansicht: Bibliothek



5. Alarmmanagement

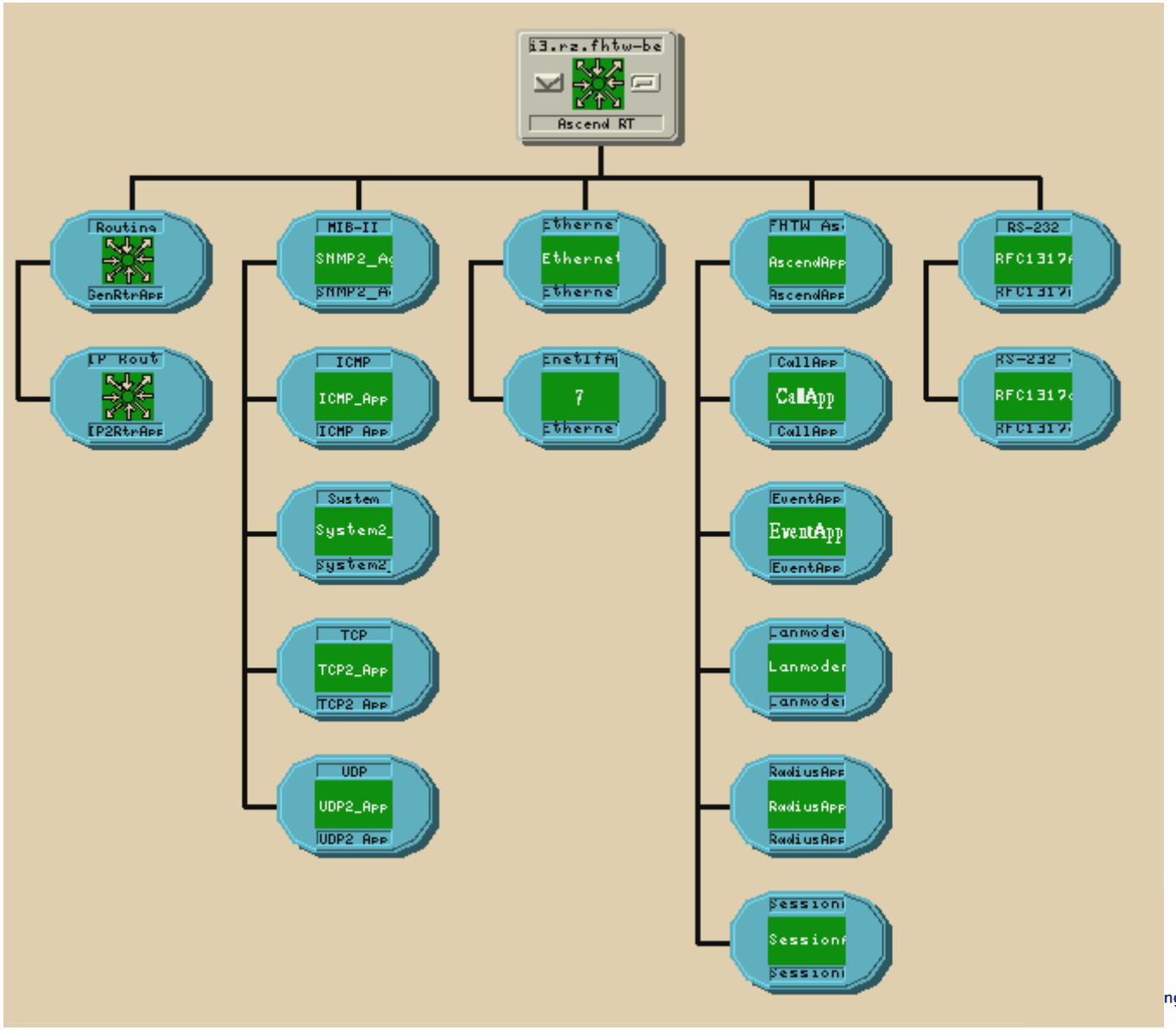


5. Netzwerkmanagementsysteme (2)

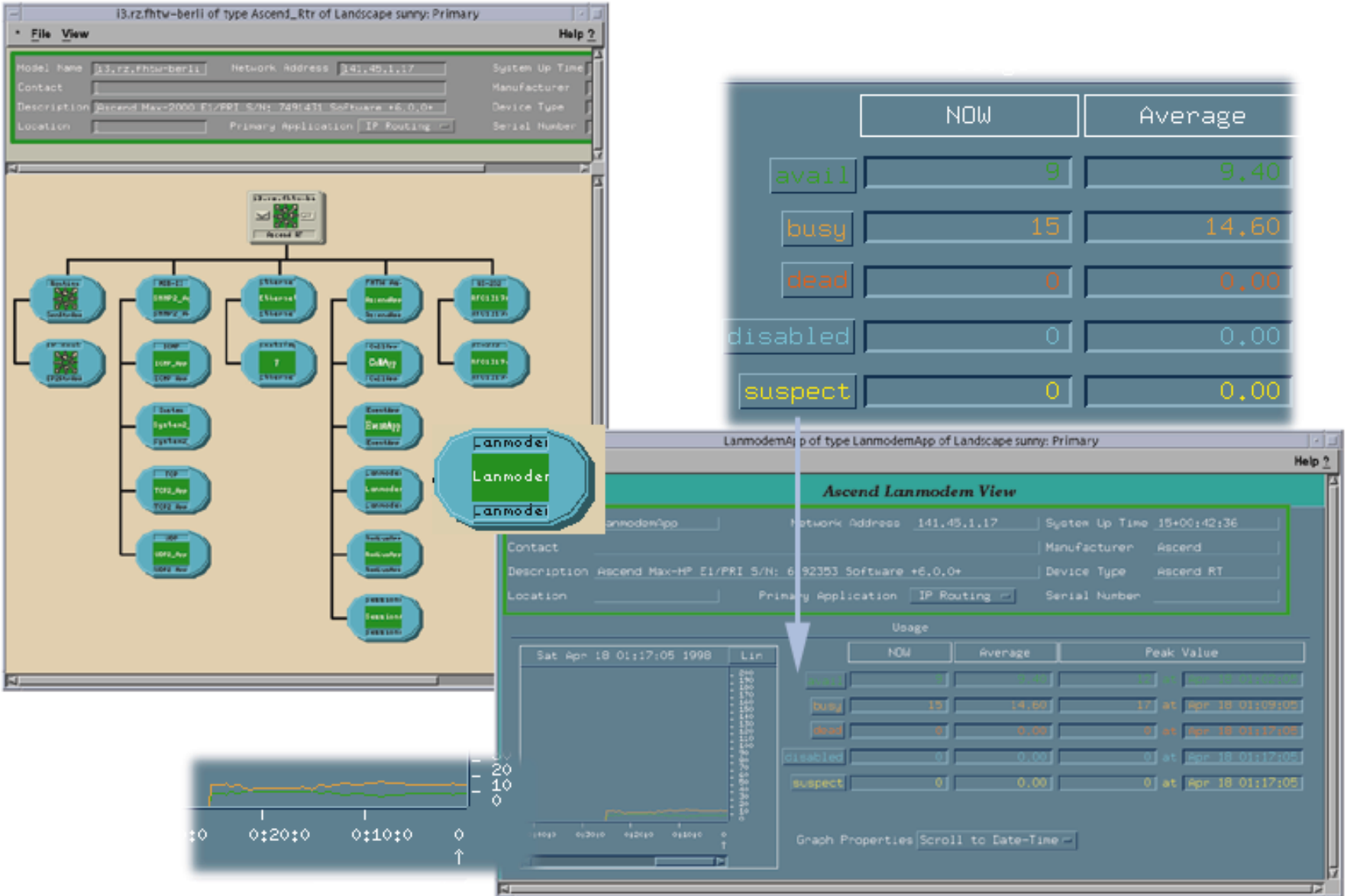
- **Discovery + Polling:** Erkennung und Überwachung der Netzstruktur via ICMP und SNMP
- **Standard MIB:** Erkennung und Verarbeitung der Standardfunktionen aller Geräte (z.B. Interfaces)
- **Private MIBs:** Erkennung und Verarbeitung geräte-spezifischer Funktionen (z.B. Cisco Router ...)

> Modellinformationen der Geräte/Hersteller werden im NMS benötigt <

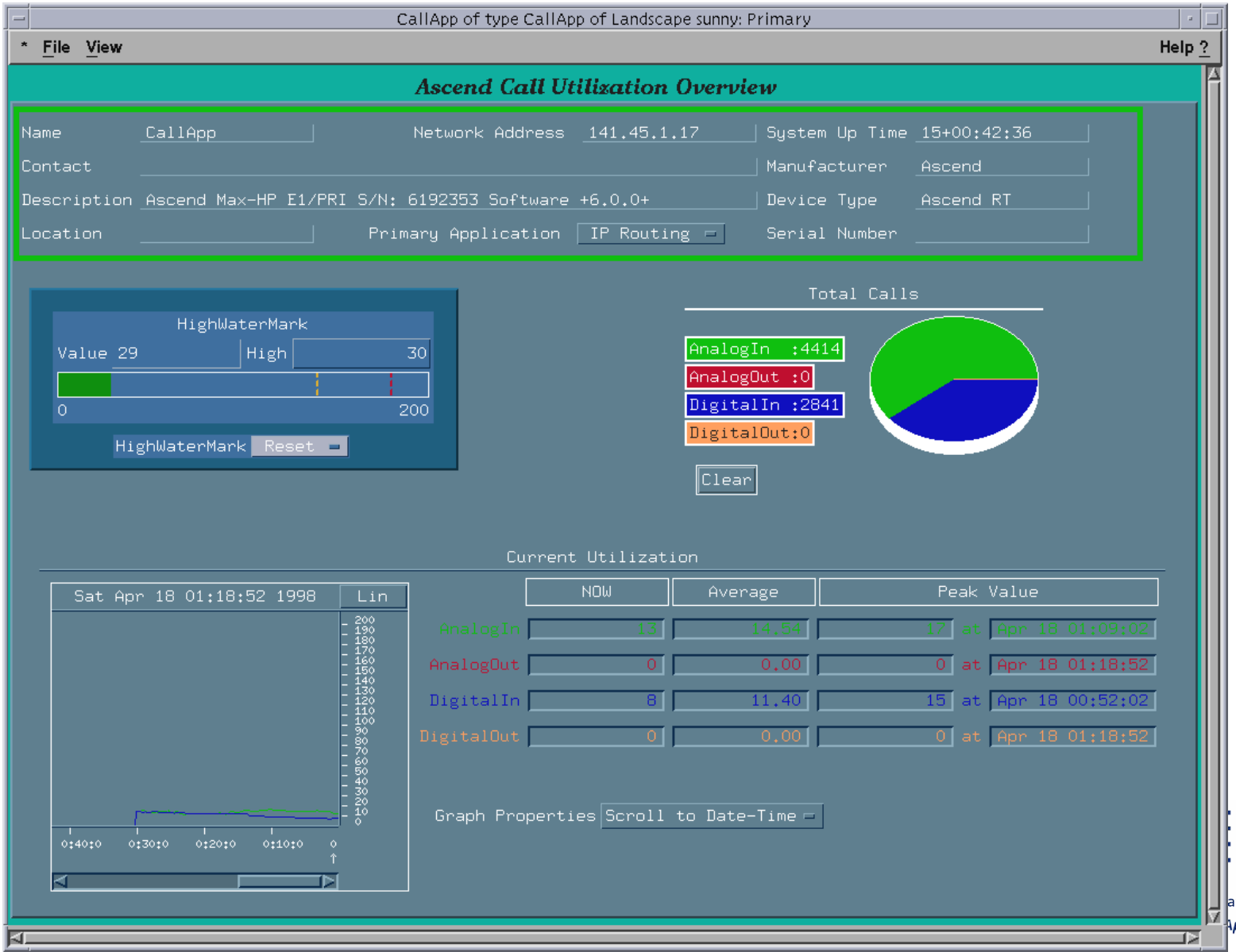
5. Beispiel Ascend Einwahlrouter



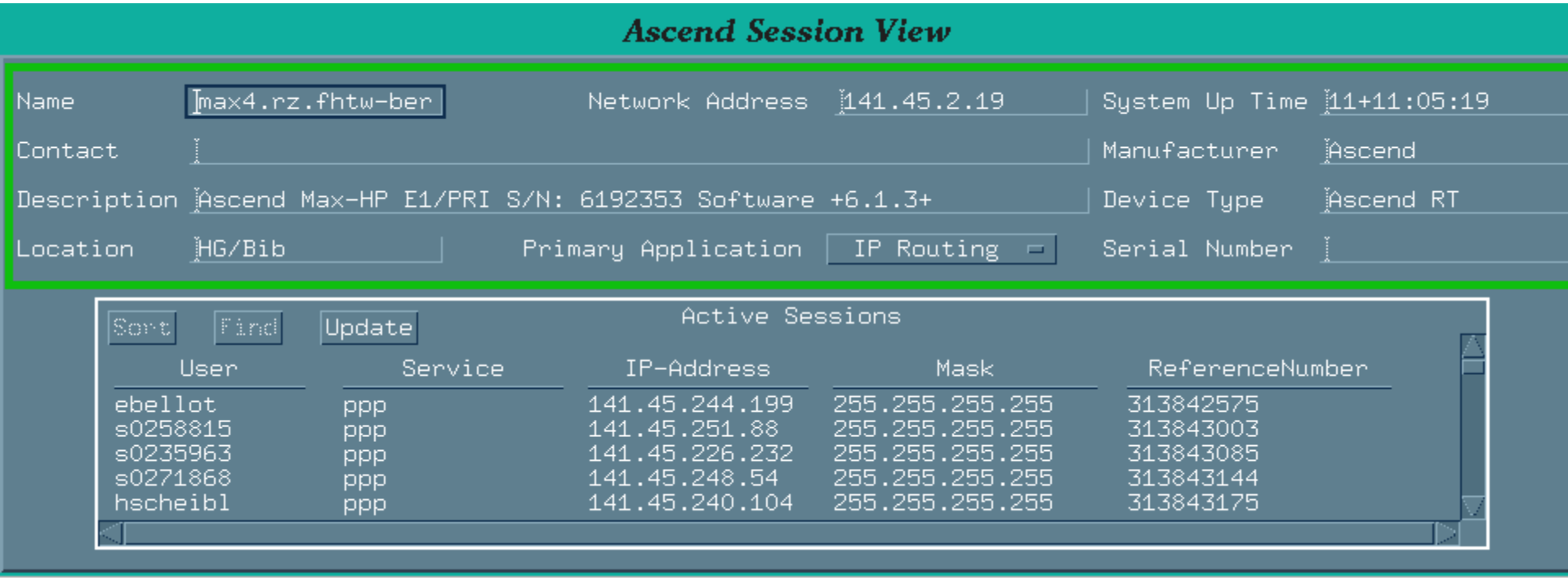
5. Navigation in Private MIB



5. Auslastungsübersicht



5. Teilnehmerübersicht



Zusammenfassung & Ausblick:

- Das SNMP-Konzept bietet einen einfachen Standard zum Management großer, heterogener Netze.
- Das Management lebt von der Bereitstellung ausreichender Informationen (MIB) und der Intelligenz des Netzwerkmanagementsystems.
- Weitergehende Informationen durch RMON (II) + SMON.
- Der technische Entwicklungsstand ist mit SNMPv3 einsatztauglich.
- Aktuelle Entwicklung der IETF: Netconf ersetzt SNMP, YANG Datenmodelle ersetzten die MIBs

Literatur:

- Rose, Marshall T.: *The Simple Book,* Pearson 1996.
- Stevens, Richard W.: *TCP/IP Illustrated, Vol 1,* Addison-Wesley 1994.
- Stallings, William: *SNMP, SNMPv2, SNMPv3 and RMON 1 and 2,* Addison-Wesley 2001.
- Simple Web: http://www.simpleweb.org

Selbsteinschätzungsfragen

1. Welche Betriebsaufgaben soll ein Netzwerkmanagement (teil-) automatisiert übernehmen?
2. Sie wollen den ‚Füllstand' der Mail-Warteschlangen überwachen und bei Auslastung > 80 % informiert werden. Wie gehen Sie vor?
3. Über welche gerätespezifischen Informationen verfügen SNMP Agent und Managementsystem gemeinsam? Wie werden diese kodiert?
4. Worin besteht die wesentliche Verbesserung von SNMPv3 gegenüber früheren Versionen?