Internet Management

Kapitel 11

MNM TEAM

Internet Management

Kapitel: 11.1:

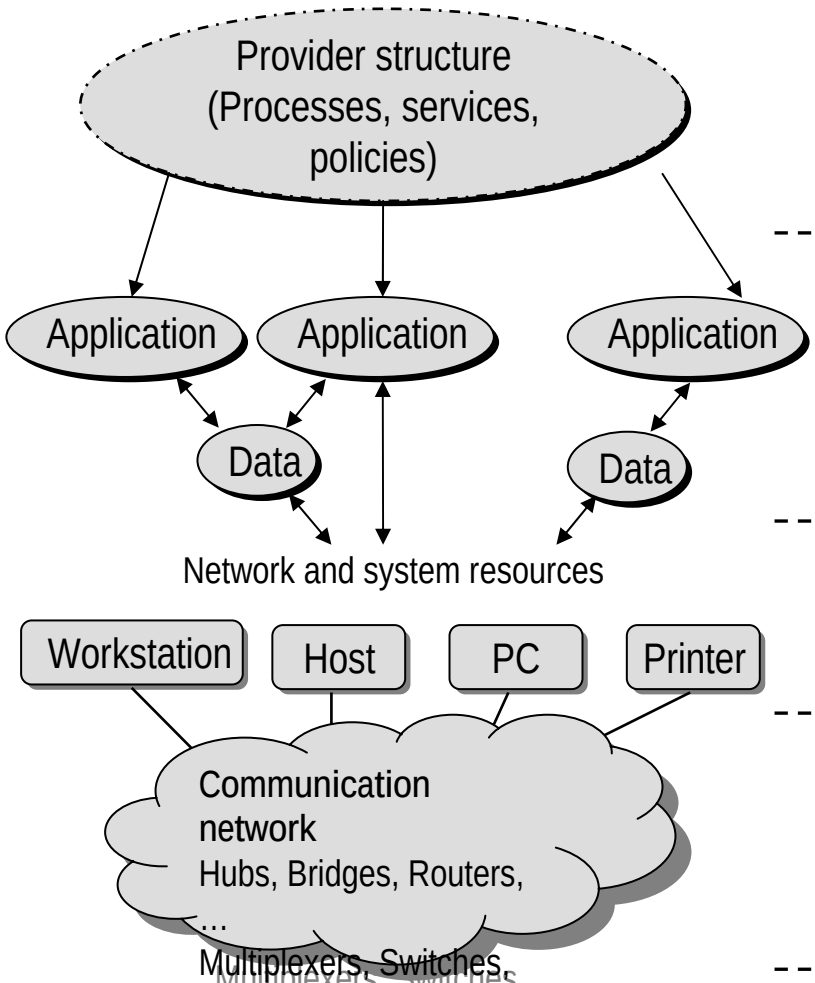
Motivation

Warum Management ?

- Bisher nur Nutzungsfunktionalität in Form von Protokollen und Diensten besprochen
- Ein Netz und seine Dienste müssen aber mit konkreten Ressourcen, mit steuerbaren Dienstgüten, in konkreten Organisationen und mit belastbaren Zielvereinbarungen betrieben werden.
- Managementobjekte sind u.a. Verbindungen (auf jeder Schicht), Koppelelemente auf verschiedenen Schichten wie z.B. Hubs, Bridges, Switches, Router, Gateways, Multiplexer, ferner Protokollinstanzen, Endsysteme, Softwarekomponenten, Dienste, Anwendungen
- Zielvorgaben: Verfügbarkeit, Zuverlässigkeit, Sicherheit, Durchsatz, Reaktionszeiten, Lastausgleich, Kosten

Umfeld für kooperative IT-Infrastruktur

Objects and resources to be managed Levels of integrated management



Service management

Enterprise management

Application management

Information management

System management

Network management

Netz-/Systemmanagement

- Gesamtheit aller Vorkehrungen und Aktivitäten zur Sicherstellung eines effektiven Einsatzes eines verteilten Systems und seiner Dienste bzw. Anwendungen
- Management ist betriebszielorientiert
- Management umfasst Personal, Verfahren, Programme, techn. Systeme
- Management betrifft Planung, Betrieb, Kontrolle, Einbettung in Organisationsformen

Internet Management

Kapitel: 11.2:

Funktionen

Netzmanagementdienste

- Benutzerverwaltung, Abrechnungsmanagement
- Sicherheitsmanagement
  (Bedrohungsanalyse, Sicherheitsmechanismen, Verschlüsselung, Authentifizierung, Zertifizierung)
- Fehlermanagement
  (Symptomerfassung, Eventkorrelation, Fehlerdiagnose, Fehlerbehebung, TT-Systeme)
- Konfigurationsmanagement
  (Generieren und Installieren von Systemen, Parameterfestlegung, Statusüberwachung, Versionsverwaltung, SW-Verteilung, Topologieplanung)
- Leistungsmanagement
  (Leistungsmessung, QoS-Parameter, Engpassanalysen, Auslastung, Kapazitätsplanung)
- Ressourcenmanagement (z.B. Bandbreiten, Wege)

Konfigurationsmanagement

- Konfigurieren heißt Anpassen von Systemen an Betriebsumgebungen
  - Neuinstallation von HW- und SW-Komponenten
  - Anpassen von SW:
    - patches, update, neue Versionen
  - Topologieänderungen bei Verbindungen und Geräten
  - Einstellen von Parametern
    - (Funktions-, Berechtigungs-, Last-, Protokoll-, Dienstgüte-, Anschlußparameter)

Fehlermanagement

- Überwachen des Netz-, System-, und Anwendungszustandes
- Entgegennehmen und Verarbeiten von Alarmen
- Feststellen von Fehlerfortpflanzungen / Eventkorrelation
- Diagnostizieren von Fehlerursachen
- Einleiten und überprüfen der Fehlerbehebung
- Betrieb eines Trouble Ticket Systems
- Führen eines User Help Desk

Leistungsmanagement

- Bestimmen von Dienstgüteparametern und Metriken
- Überwachen aller Ressourcen auf Leistungsengpässe
- Durchführen von Messungen
- Auswerten von History Logs
- Aufbereiten von Messdaten und Verfassen von Leistungsberichten
- Leistungsvorhersagen und Simulation
- Leistungs- und Kapazitätsplanung

Netzparameter für QoS

- **Bandbreite**
  - access speed - bit rate
  - abhängig von der Übertragungstechnik
- **Verzögerung**
  - access delay + transmission delay
  - = network transit delay (end-to-end delay)
- **Delay Jitter**
  - Puffer- u. Bearbeitungszeiten in Knoten
  - Phasenschwankungen in Schwingkreisen
  - Temperaturabhängigkeit der Bauteile
- **Fehlerraten**
  - Leitungsfehler, Paketfehler
- **Synchronisation**
  - Bandbreite + Delay + Jitter
- **Abhängig von der Verkehrssituation / Last**

Abrechnungsmanagement, Benutzerverwaltung

- Namen- und Adressmanagement
- Autorisierung
- Accounting Management
  - Festlegen von Abrechnungsdaten
  - Erfassen von Verbrauchsdaten
  - Führen von Abrechnungskonten
  - Zuordnen Kosten zu Konten
  - Verteilen und Überwachen von Kontingenten
  - Führen von Verbrauchsstatistiken, Kundenprofilen
  - Festlegen von Abrechnungspolitiken und Tarifen

Beispiel: Web-Hosting (1)

- Abonnement-bezogene Parameter
  - Anzahl der einzurichtenden WWW Domänen
  - WWW Server (Anz. dedizierter Server, Anz. virtueller Server, Anz. v. Fremd-Werbe-Bannern)
  - Max. Datentransferrate im Monat
  - Max. verfügbarer Speicherplatz
  - Bandbreite der Anbindung an das Backbone
  - Max. Anz. der Benutzer für passwortgeschützte Seiten
  - Email: Max. Anzahl der Email-Aliases
  - Maximale Anz. gleichzeitiger Verbindungen
  - ...
- Nutzungsbezogene Parameter
  - Anz. der übertragenden Bytes/Pakete/Responses
  - Anzahl der Requests
  - Gesamtverweildauer (bezogen auf einen Nutzer)

Beispiel: Web-Hosting (2)

- Content-basiert
- FTP: Anzahl übertragener Bytes/Pakete, Content-basiert
- Email: Anz. geforwardeter Emails
- Dienstgüte:
  - Transaktionsdauer
  - Anzahl korrekt übertragener Responses
  - Anzahl der Verweise auf die Seite (Pflege von Suchmaschinen)
  - Downtime des Servers
- Management-bezogene Parameter
  - WWW Server (Detailgrad d. Statistiken, Anz. der Aktualisierungen)
  - WWW Seiten (Anzahl der WWW Seiten Updates durch den Kunden, Aufsatz für Web-Tools (z.B. Front-Page))
  - Sicherheit: Anz. Zertifikatgeschützter WWW Seiten, Gesamtanzahl der verwalteten Zertifikate, Anz. Neuausgestellter Zertifikate
  - ...

Sicherheitsmanagement: Teilaufgaben

- Durchführung von Bedrohungsanalysen
- Festlegung und Durchsetzen von Sicherheitspolitiken
- Überprüfen von Autorisierungen
- Feststellen einer Identität (Authentifizierung, Signaturen, Zertifizierung)
- Durchführen einer Zugriffskontrolle
- Sicherstellung der Vertraulichkeit und Datenintegrität
- Überwachung auf Sicherheitsangriffe
- Berichterstattung zur Sicherheit

Sicherheitsmanagement: Bedrohungen

- Passive Angriffe
  - Abhören von Informationen
  - Erstellen eines Nutzerprofils
  - unerwünschte Verkehrsanalyse
- Aktive Angriffe
  - Maskerade
  - Manipulation von Nachrichtensequenzen
  - Modifikation von Nachrichten
  - Manipulation von Ressourcen
- Fehlfunktion
- Fehlbedienung

Control and Monitoring

- operational data: instantaneous information about resources
- error data: recording and monitoring of error events
- traffic and load data: device and connection related information
- performance data: analysis of thresholds, etc.
- security data: auditing, logging, etc.
- accounting data: service and resource utilization

Weitere Managementfunktionen

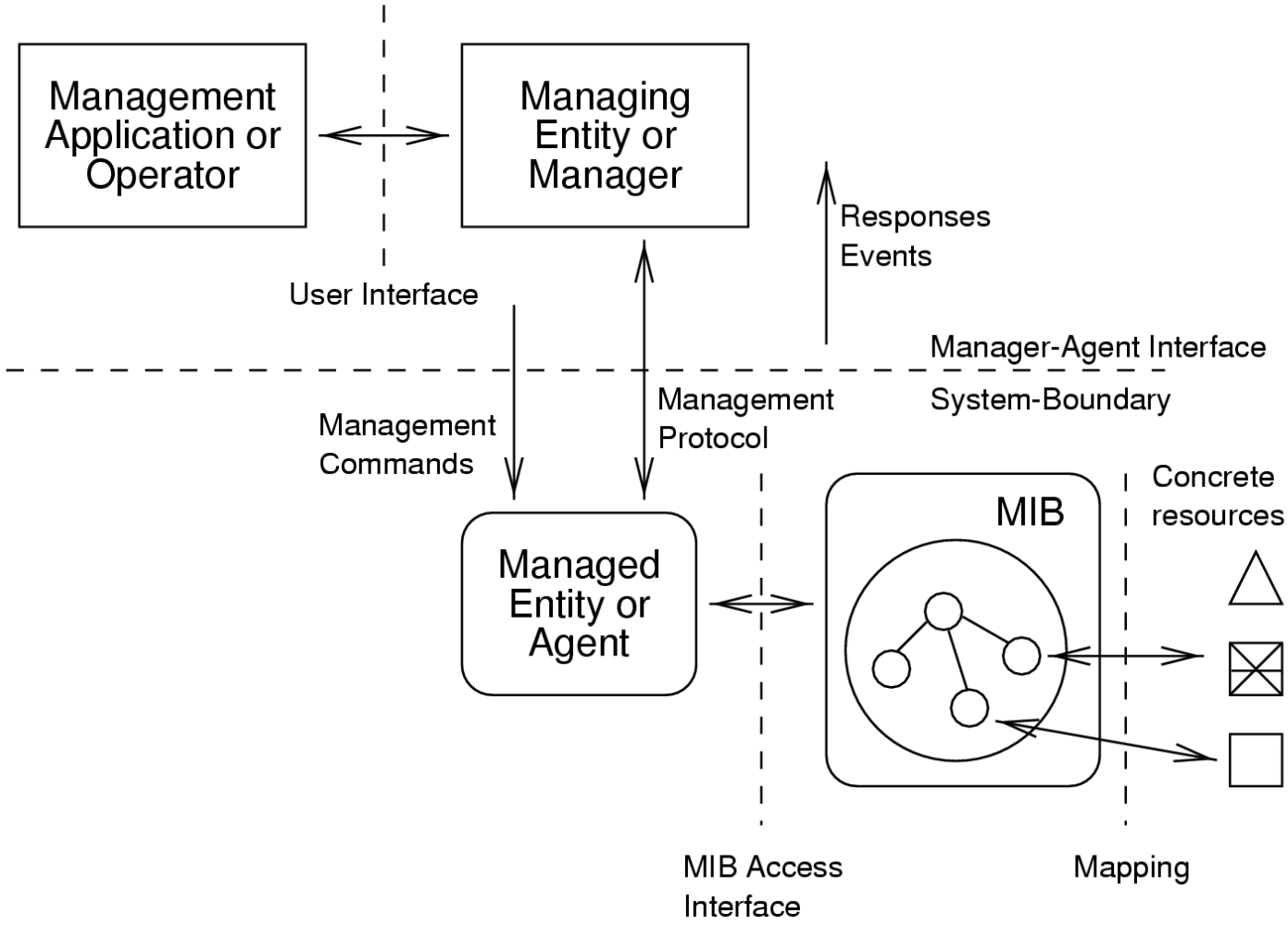
- Inventory Management, Asset Management
- Service Management (creation, provisioning, subscribing, operation)
- Change Management
- Maintenance, Training, Logistics
- Informationsdienste
  - Allg. Informationsdienste (Blackboard)
  - Directory Services (yellow pages, mailing lists, distribution lists)
  - Dynamic information about users, resources, usage, etc.
  - Support and advice information (Hotline, CCC)

Internet Management

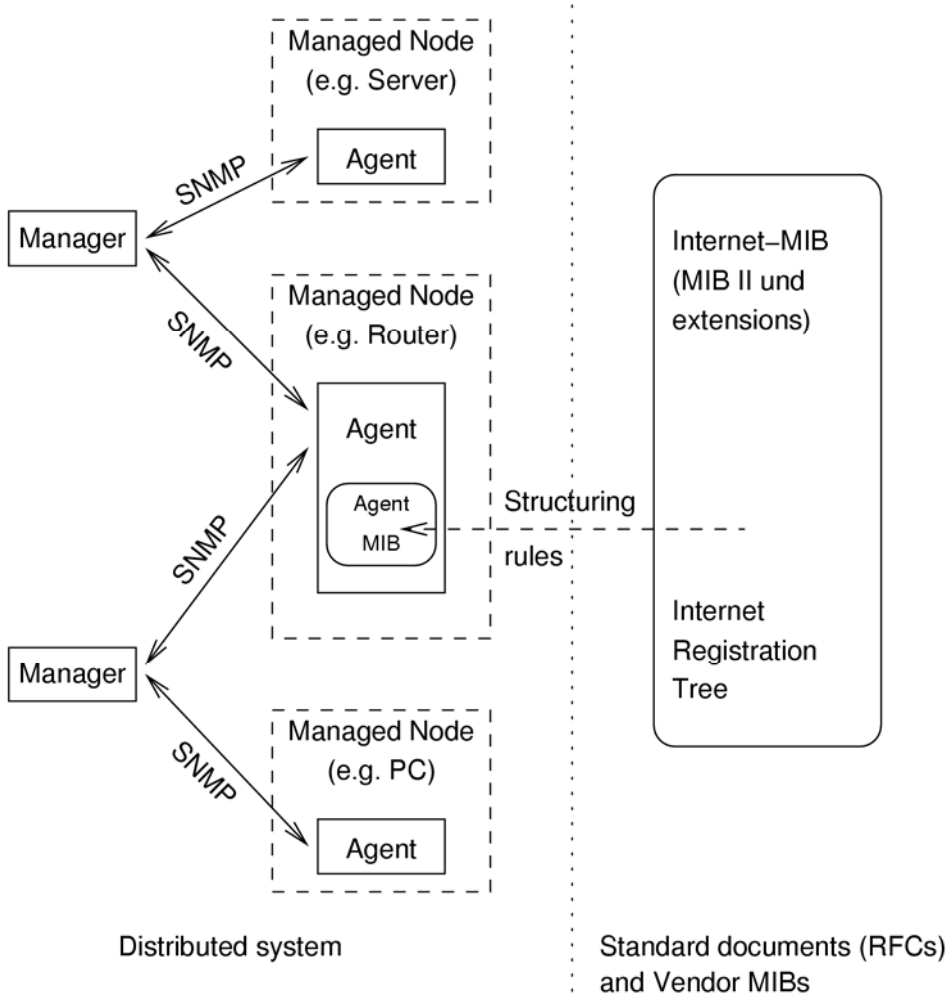
Kapitel: 11.3:

Managementinformation

Management via MIB Manipulation



Internet-Architekturmodell und MIBs



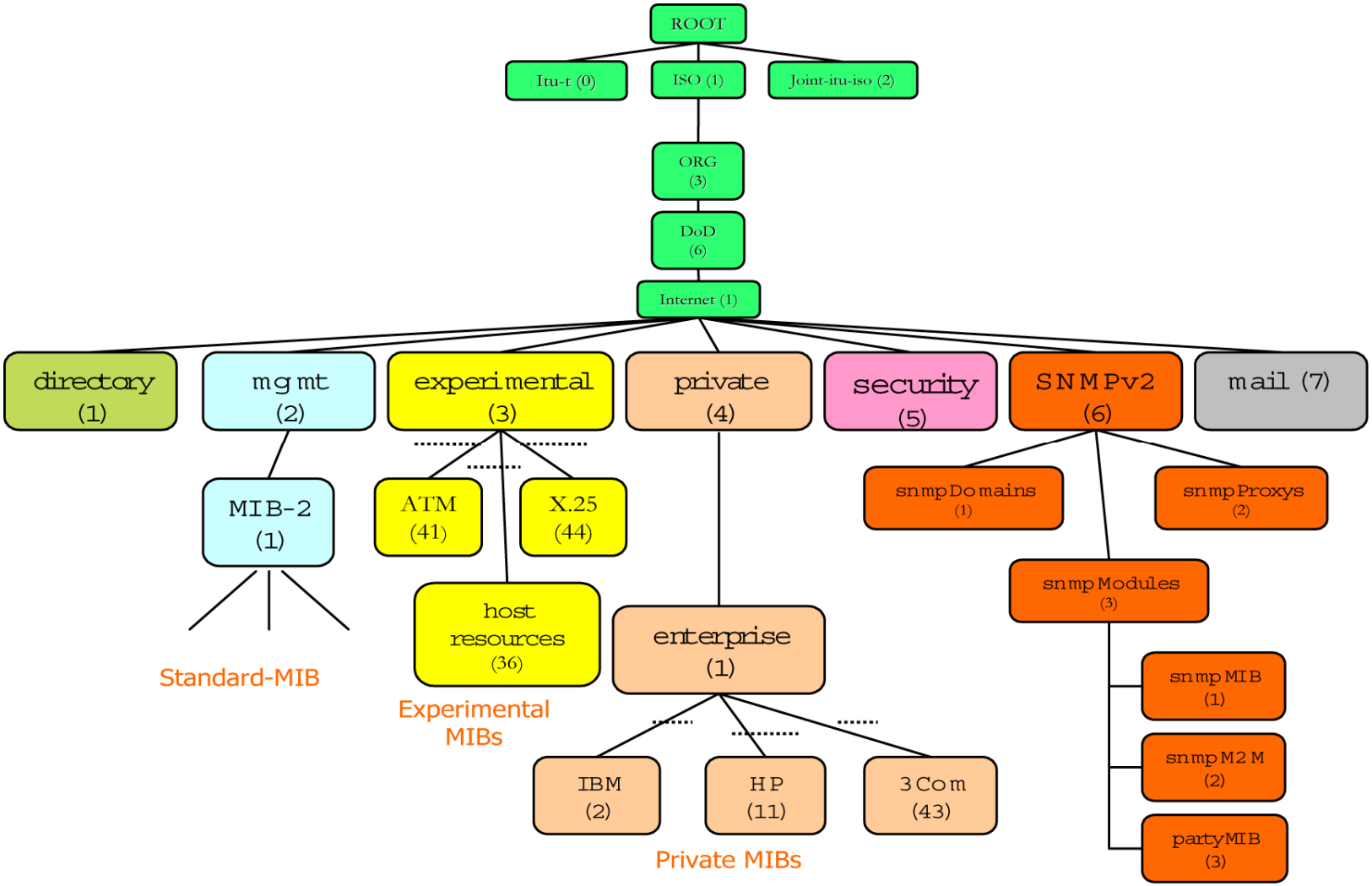
Internet-Informationsmodell

- Modellansatz:
  - Datentypansatz
- Informationseinheiten:
  - einfache und zusammengesetzte Variable
- Informationseinheiten:
  - „managed objects“

    (trotz Fehlens eines objektorientierten Ansatzes)
- Identifizierung, Benennung der Objekte über den “Internet-Registrierungsbaum”
- RFC 1155: „Structure of Management Information“

  (bzw. RFC 1442 für Version 2 des Internet Management)

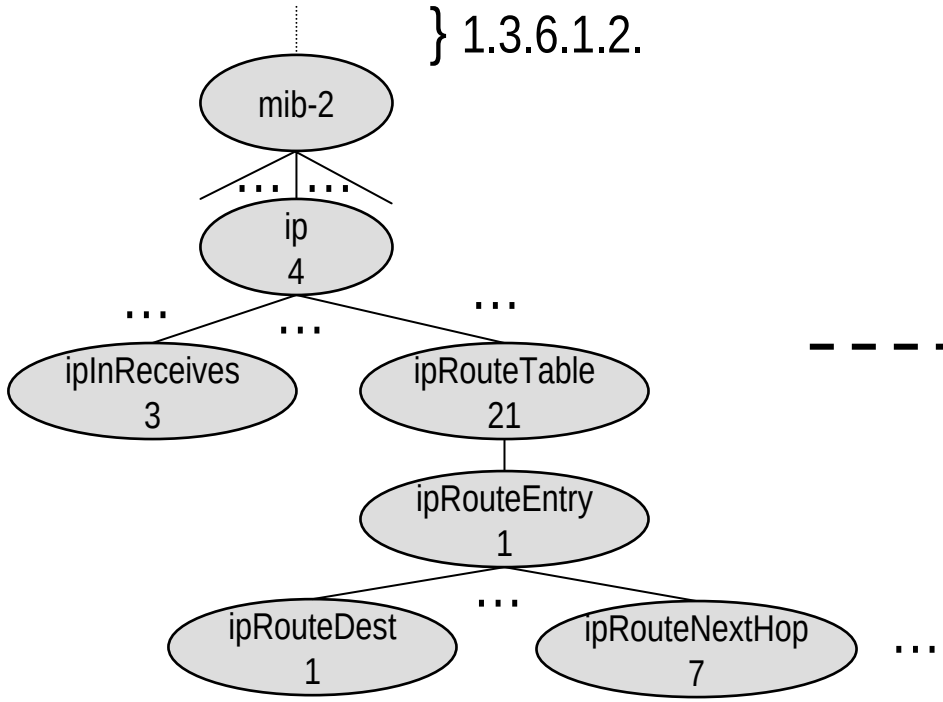
Internet Registrierungsbaum und Erweiterungen

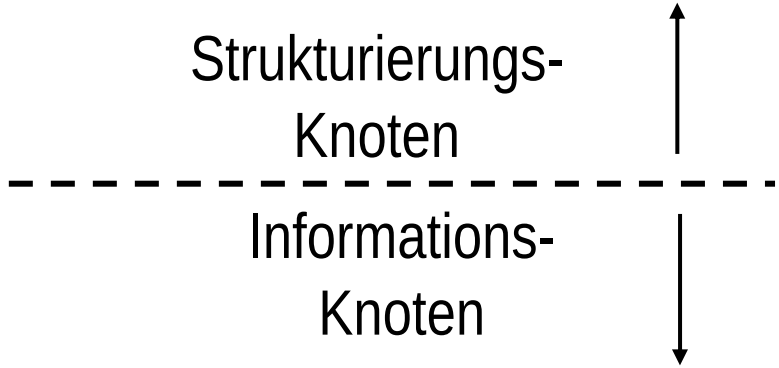


Knoten-Arten

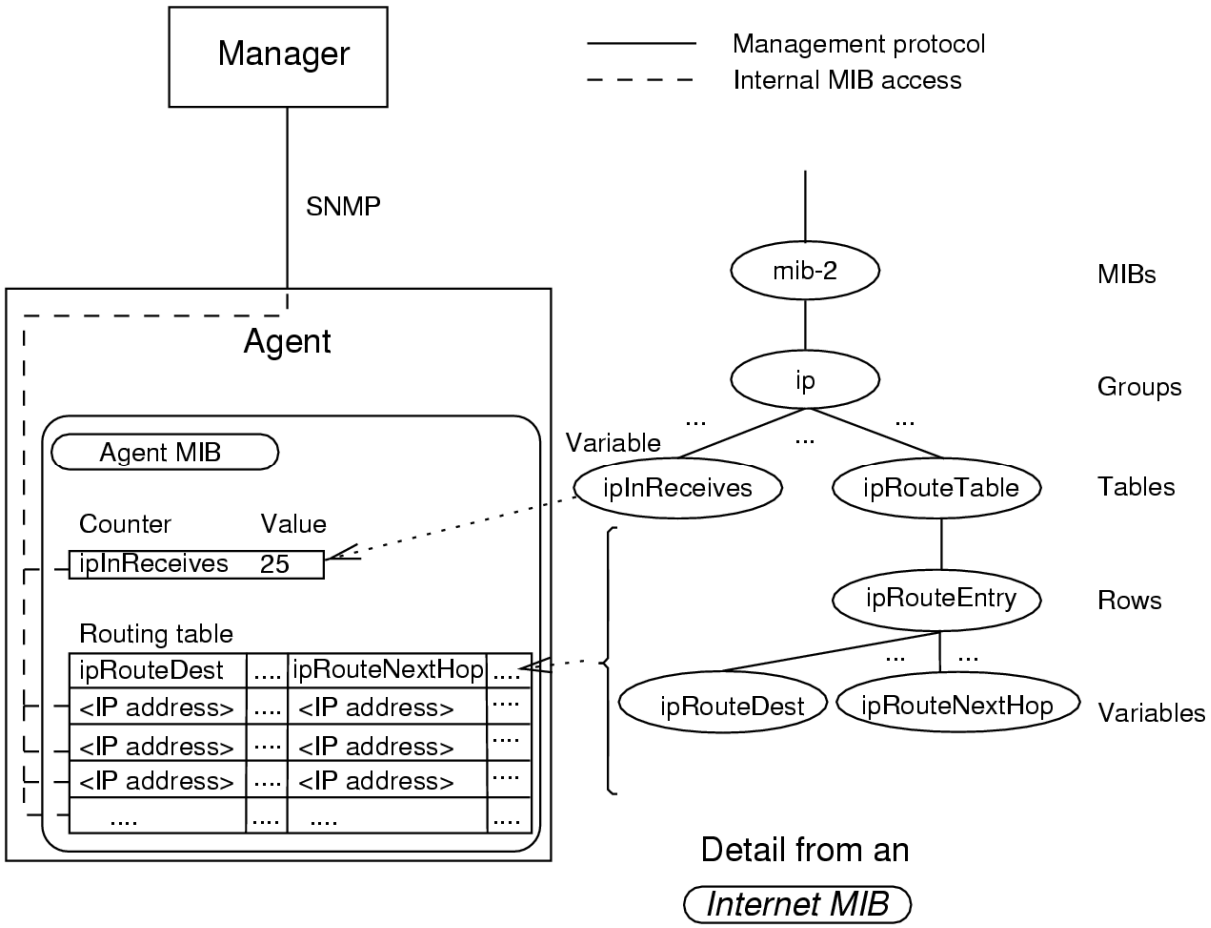
- Zwei Arten von Knoten im Registrierungsbaum

(1) „Strukturierungs“-Knoten (2) „Informations“-Knoten





Agenten- und Internet-MIB



Syntax

❑ Syntax der Strukturierungsknoten

mib-2 OBJECT IDENTIFIER : : = { iso(1) org(3) dod(6) internet(1) mgmt (2) 1 }

ip OBJECT IDENTIFIER : : = { mib-2 4 }

❑ Syntax der Informationsknoten

- ASN.1 – Makro OBJECT-TYPE

  <Objektname> OBJECT-TYPE

  SYNTAX *<Typangabe>*

  ACCESS *<Zugriffsmöglichkeiten>*

  STATUS *<Implementierungsanforderungen>*

  DESCRIPTION *<Informelle Semantik-Beschreibung>*

  : : = { *<Objektname des Vaterknotens>* *<laufende Nummer>* }
- Simple Object Types ⟶ z.B. Zähler oder Zeichenreihe
- Aggregate Object Types ⟶ Listen und Tabellen

Syntax: Beispiel

- Zähler ipInReceives

Mögliche Wertebelegungen

ipInReceives OBJECT-TYPE

SYNTAX Counter — Integer, Octet String, Object Identifier, Null, IpAddress, NetworkAddress, Counter, Gauge, Time Ticks, Opaque

ACCESS read-only — read-write, write-only, not-accessible

STATUS mandatory — optional, obsolete

DESCRIPTION

„The total number of input datagrams received from interfaces, including those received in error.“

: : = { ip 3 }

Syntax: Beispiel

- Knotenart-Indikator ipForwarding

```
ipForwarding   OBJECT-TYPE

    SYNTAX     Integer { gateway (1),  -- entity forwards datagrams
                         host (2)      -- entity does NOT forward datagrams }

    ACCESS     read-only

    STATUS     mandatory
               DESCRIPTION
               „The indication of this entity is acting as an IProuter in respect to the
    forwarding of datagrams received by, but not addressed to, this entity.“
: : = { ip 1 }
```

Zusammengesetzte Objekte

- Listen und Tabellen
- Informelle Beschreibung einer Tabelle

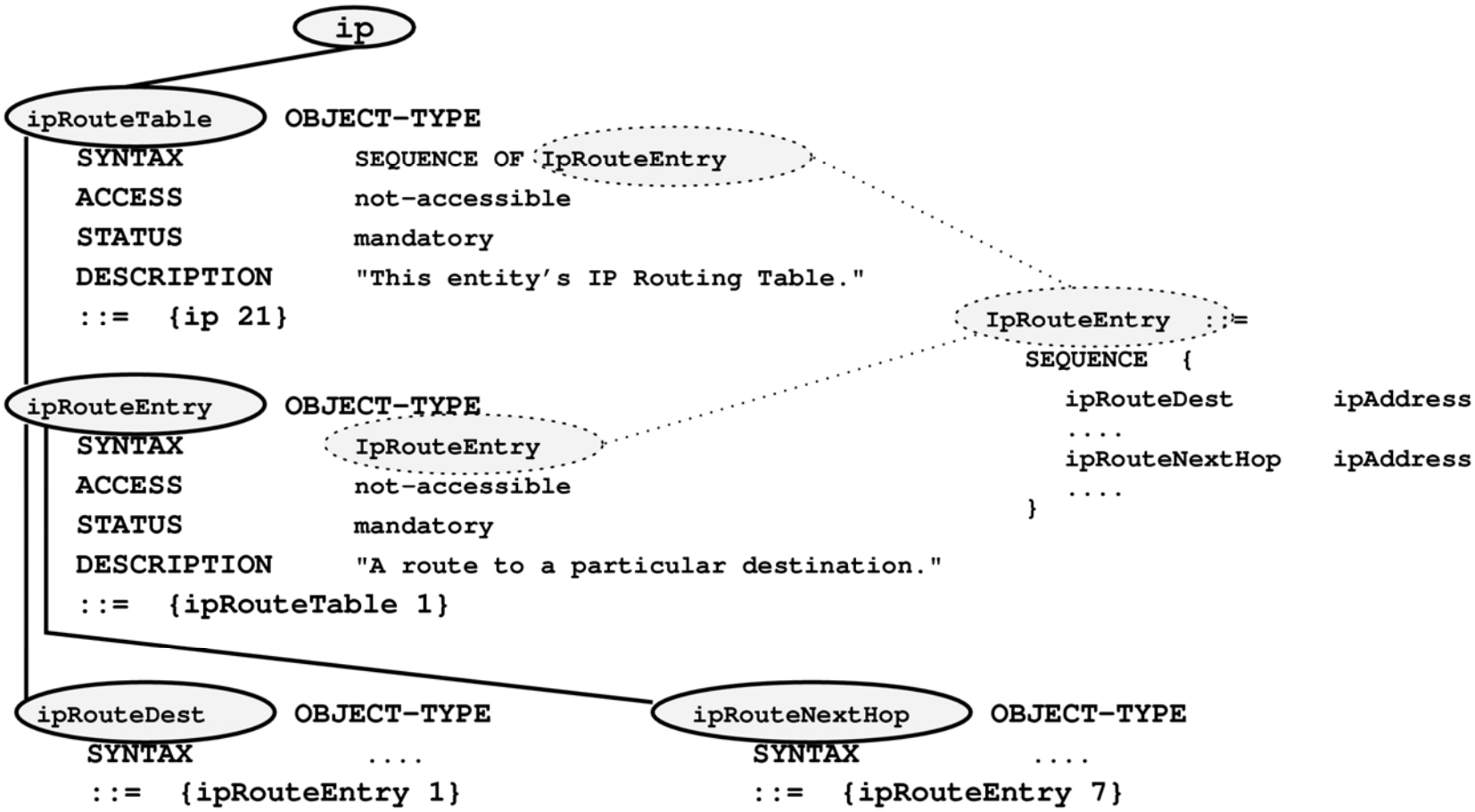
SEQUENCE OF { geordnete Liste beliebiger Länge von (gleichen) Tabellenzeilen,

SEQUENCE { wobei sich eine Tabellenzeile aus einer geordneten Liste fester Länge von einfachen Internet-Objekttypen ggf. unterschiedlichen Typs zusammensetzt

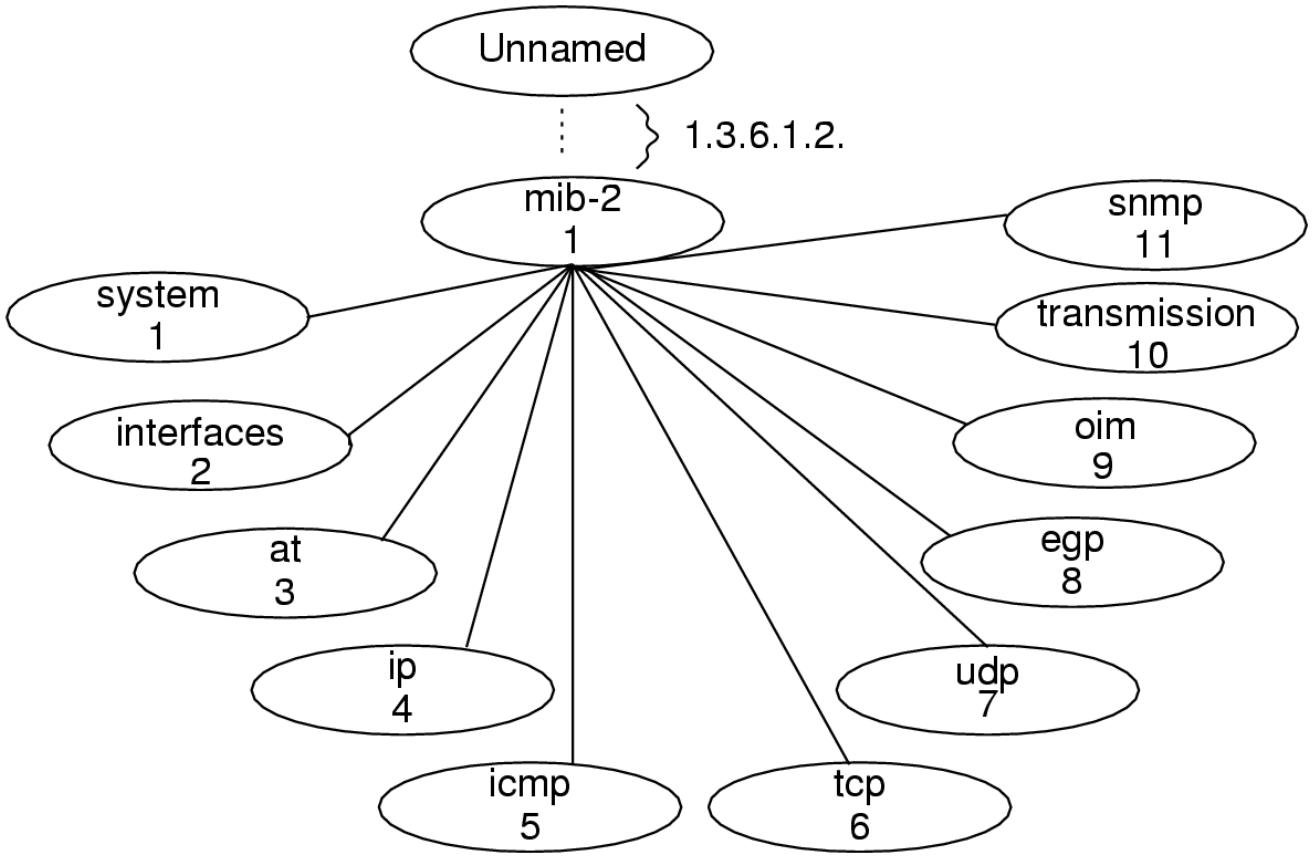
- Internet-Tabelle = SEQUENCE OF SEQUENCE (Einfacher Internet-Objekttyp 1 ... Einfacher Internet-Objekttyp N)

(Beliebig lange) Liste von Tabellenzeilen

Beispiel: Tabelle



Internet MIB-II



The Internet-standard MIB-II (1)

- System Group
  - The system group must be implemented by all managed nodes, and contains generic configuration information:

System OBJECT IDENTIFIER :: = { mib 1 }

sysDescr:	description of device
sysObjectID:	identity of the agent software
sysUpTime:	how long ago the agent started
sysContact:	name of contact person
sysName:	device name
sysLocation:	device physical‘s location
sysServices:	services offered by devices

The Internet-standard MIB-II (2)

- Beispiel:

sysDescr	„4BSD/ISODE SNMP“
sysObjectID	1.3.6.1.4.1.4.1.2.1
sysUpTime	45366736
	(5 days, 6 hours, 1 minutes, 7.36 seconds)
sysContact	„Marshall Rose mrose@psi.com“
sysName	wp.psi.com
sysLocation	„Troy machine room“
sysServices	0x48 (transport, application)

The Internet-standard MIB-II (3)

- Interface Group (mandatory for all nodes)
  - Zahl der Interfaces, über die IP-Pakete kommen/gehen
  - Tabelle von Objekten für jedes Interface
    - Schnittstellenbeschreibung (Hersteller, Produkt, Version)
    - Typ (8.02.3/4/5, rfc 877-x25, lapb, T1, ...)
    - max IP-Paketlänge, Ü-Rate, Adresse
    - Status (up, down, testing)
    - diverse Zähler (received packets, faulty packets, …)
    - Länge Ausgabewarteschlange
    - …

Technologische MIBs (Experimental, Ausschnitt)

- LAN:
  - IEEE 802.3, 802.4, 802.5, 802.11, 802.12
  - Hub, Bridge
  - HIPPI, Fiber Channel
- MAN:
  - FDDI
- Internet:
  - PPP, OSPF, BGP, RSVP, IntServ, Diffserv, DNS
- WAN:
  - DS1/DS3, RS-232, SONET, SDLC, X.25, FR, ATM, SDMS,
- Sonstige:
  - Print, RDBMS

Internet MIBs für System und Application Mgmt.

- Host Resources MIB (RFC 1514)
- Mail Monitoring MIB (RFC 2249)
- X.500 Directory Monitoring MIB (RFC 1567)
- DNS Server/Resolver MIB Extensions (RFC 1611/12)
- Network Services Monitoring MIB (RFC 2248)
- Printer MIB (RFC 1759)
- Uninterruptable Power Supply MIB (RFC 1628)
- Relational Database Management System MIB (RFC 1697)
- System Application MIB (RFC 2287)
- Application Management MIB (RFC 2564)
- Application Performance Measurement MIB (Draft)
- WWW Service MIB (RFC 2594)

Internet Management

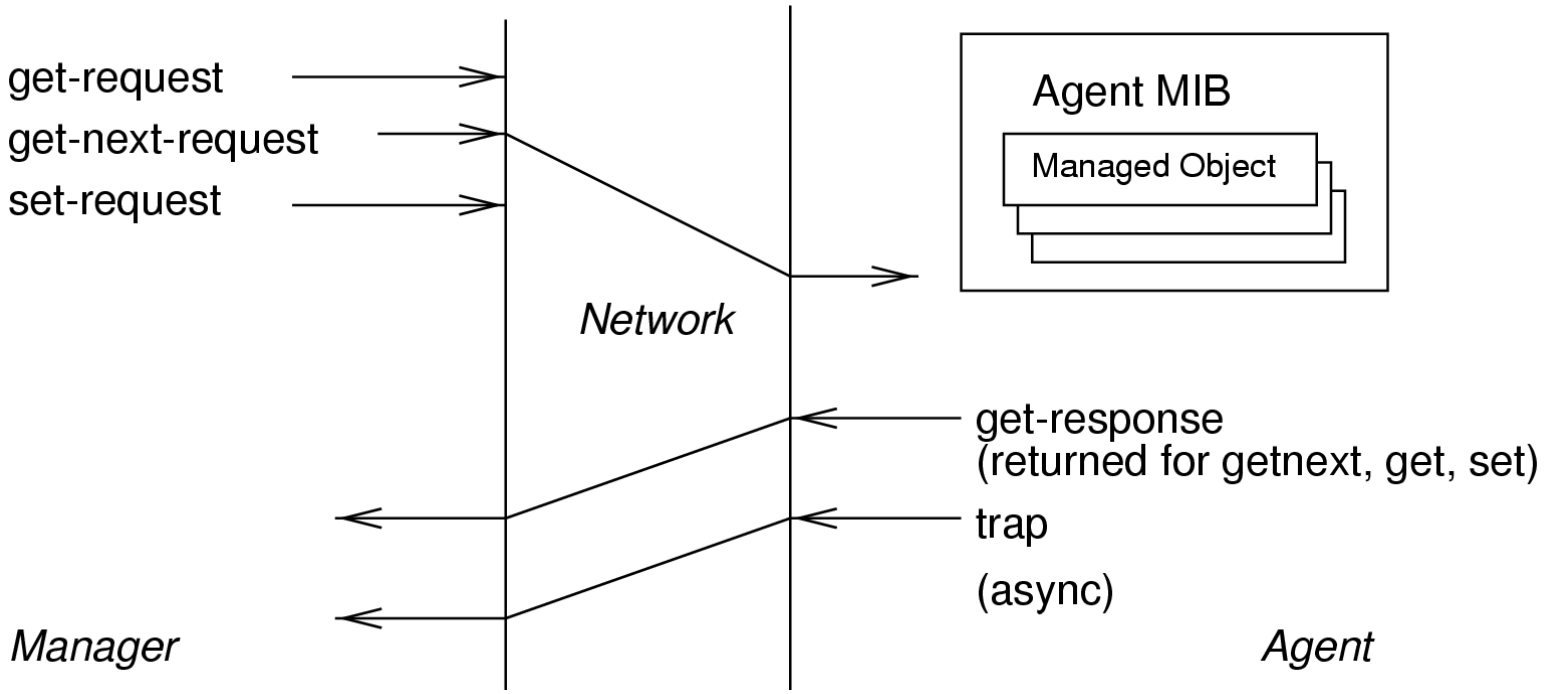
Kapitel: 11.4:

Simple Network Management Protocol

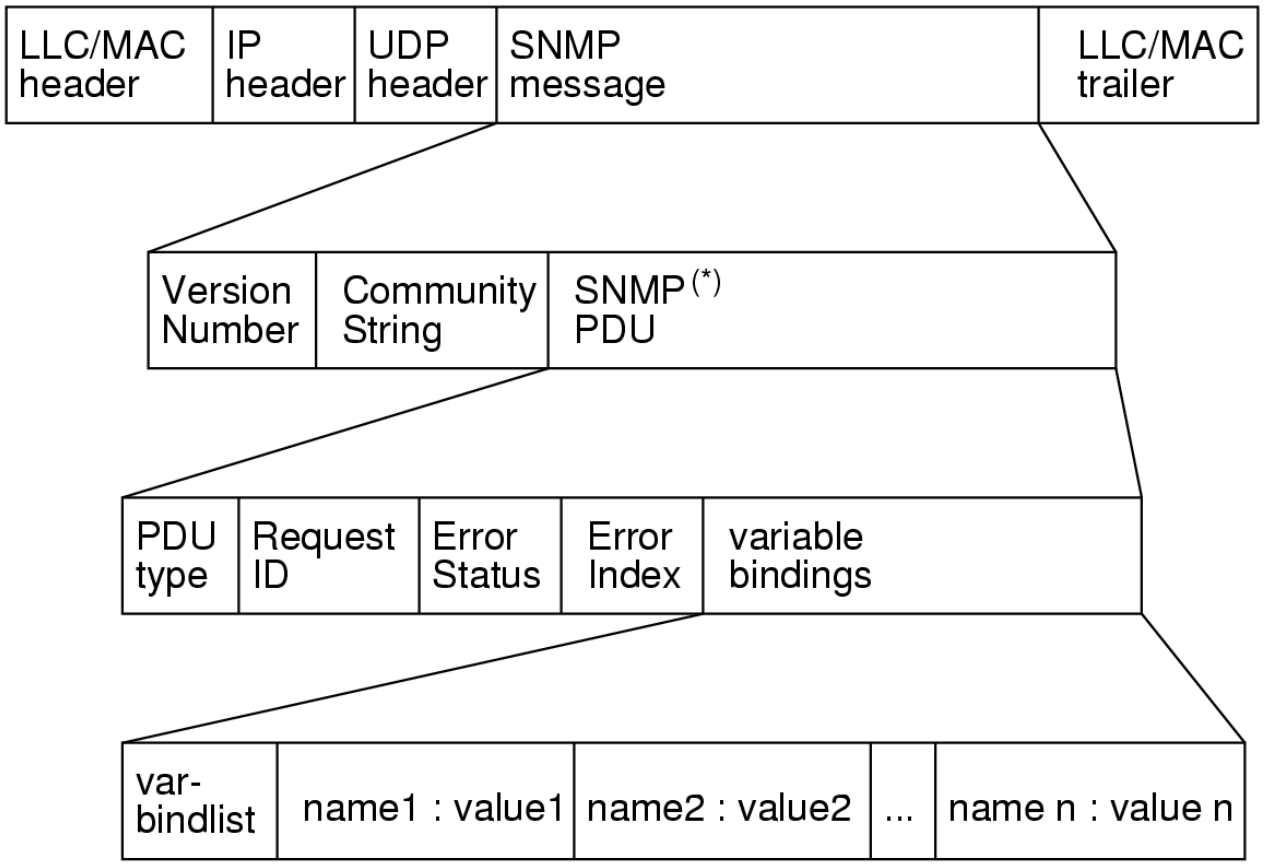
Internet-Kommunikationsmodell

- SNMP (Simple Network Management Protocol)
  - zentrale Bestandteil des Internet-Managements
    - Internet-Management = SNMP-Management
- Wesentliche Aufgabe von SNMP
  - Zugriff des Managers auf die vom Agenten bereitgestellte MIB (Get- und Set-Operation)
  - Informieren über Ereignisse, die im Agenten aufgetreten sind (Trap-Operation)

SNMP-Operationen



SNMP-Message Format



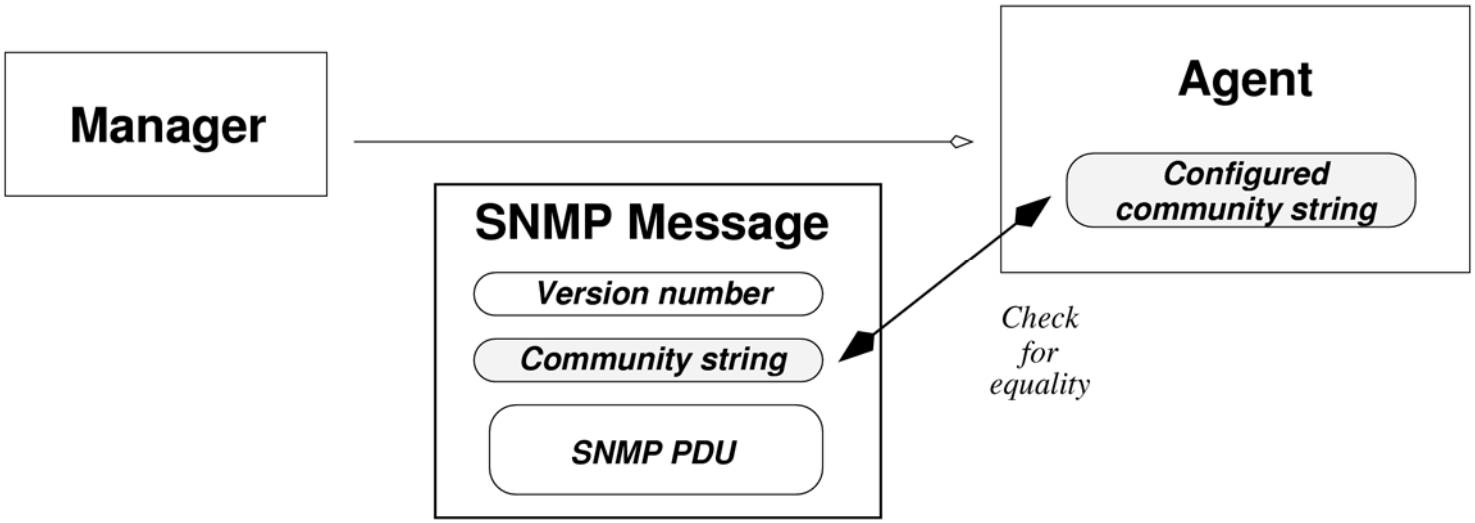
(*) Instead of a SNMP-PDU also a Trap-PDU may be contained in a SNMP-Message

Trap-PDU

- PDU-Type
  - 4
- Enterprise
  - OID des Trap erzeugenden Objekts
- Agent-address
  - Netzadresse des SNMP-Agenten
- Generic-trap
  - coldStart(0), warmStart(1),
  - linkDown(2), linkUp(3),
  - authenticationFailure(4),
  - egpNeighborLoss(5),
  - enterpriseSpecific(6)
- Specific-trap
  - weitere Informationen zu enterpriseSpecific
- Time-stamp
  - Zeit seit letzter Initialisierung
- Variable-bindings
  - Variablenwerte zum Trap

Internet Management: Communication model

- Security aspects: Community string (SNMPv1)



Internet Management: Communication model

- Security aspects: Community string (SNMPv1)

  - Mehrere Manager können auf einen Managed Node zugreifen
  - Community definiert Beziehung zwischen Agent und SNMP Application
  - Community Profile ist Paar aus MIB View und SNMP Access Rights
  - Authentifizierung über eindeutigen Community Name
  - Ermöglicht Festlegung administrativer Beziehungen zwischen SNMP Applikationen

  aber: community strings werden ungesichert übertragen!

Wertung Internet-Management

- dominant in der Datenkommunikation
- sehr einfacher Ansatz in Bezug auf Informations- und Kommunikationsmodell
- Managementobjekte nur repräsentiert über Einfachvariable und Tabellen, ist zu simpel für die heutige Managementwelt
- Neuere Entwicklungen (Version2 und 3) erhöhen Übertragungssicherheit und Effizienz von SNMP und erweitern das Konzept in Richtung Funktionsmodell