

Management vernetzter IT-Systeme

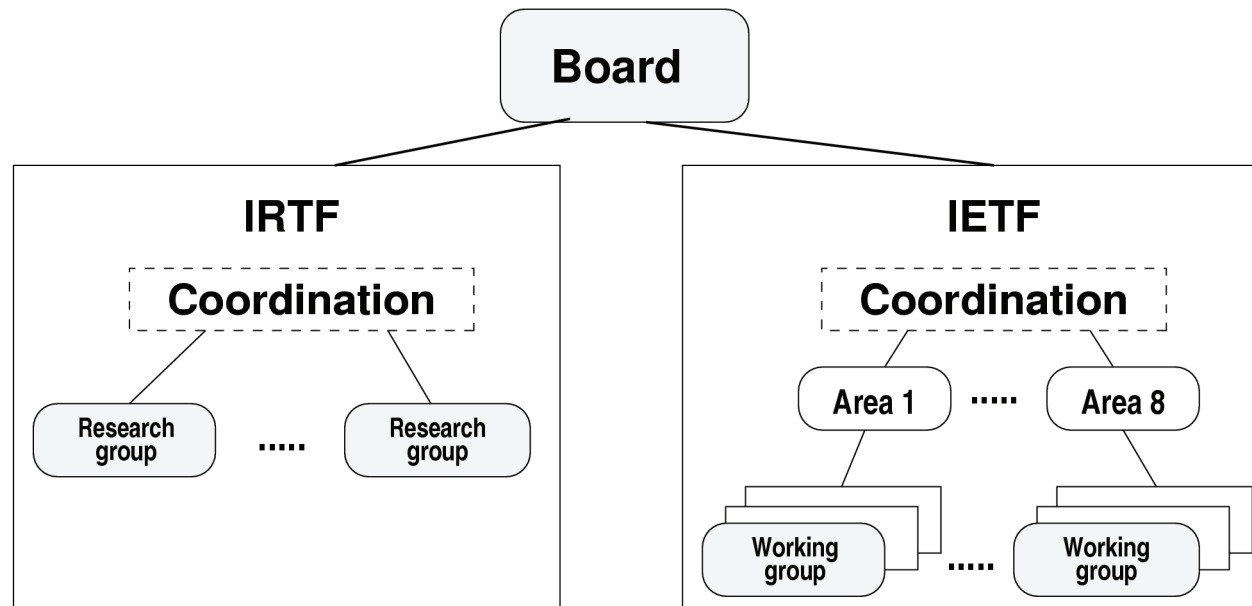
Kapitel: 5 Internet Management

Gliederung Kap. 5: Internet-Management

- Internet Informationsmodell (SMI und MIBs)
 - SNMPv1-SMI
 - SNMPv2-SMI
- Internet Kommunikationsmodell
 - SNMP Version 1
 - SNMP Version 2
- Remote Monitoring MIBs (RMON)
- weitere Entwicklungen
 - SNMP Version 3
 - DISMAN
 - AgentX

Internet management: Standardizing Process

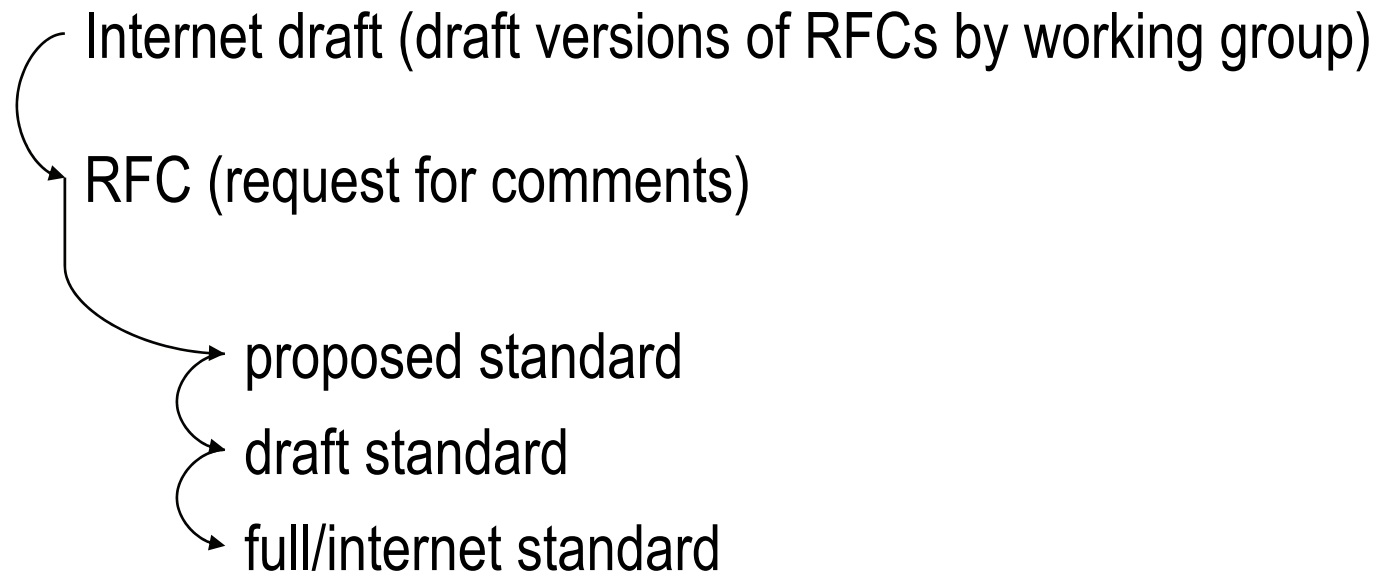
□ Internet Activities Board Organization



Internet Management: Standardizing Process

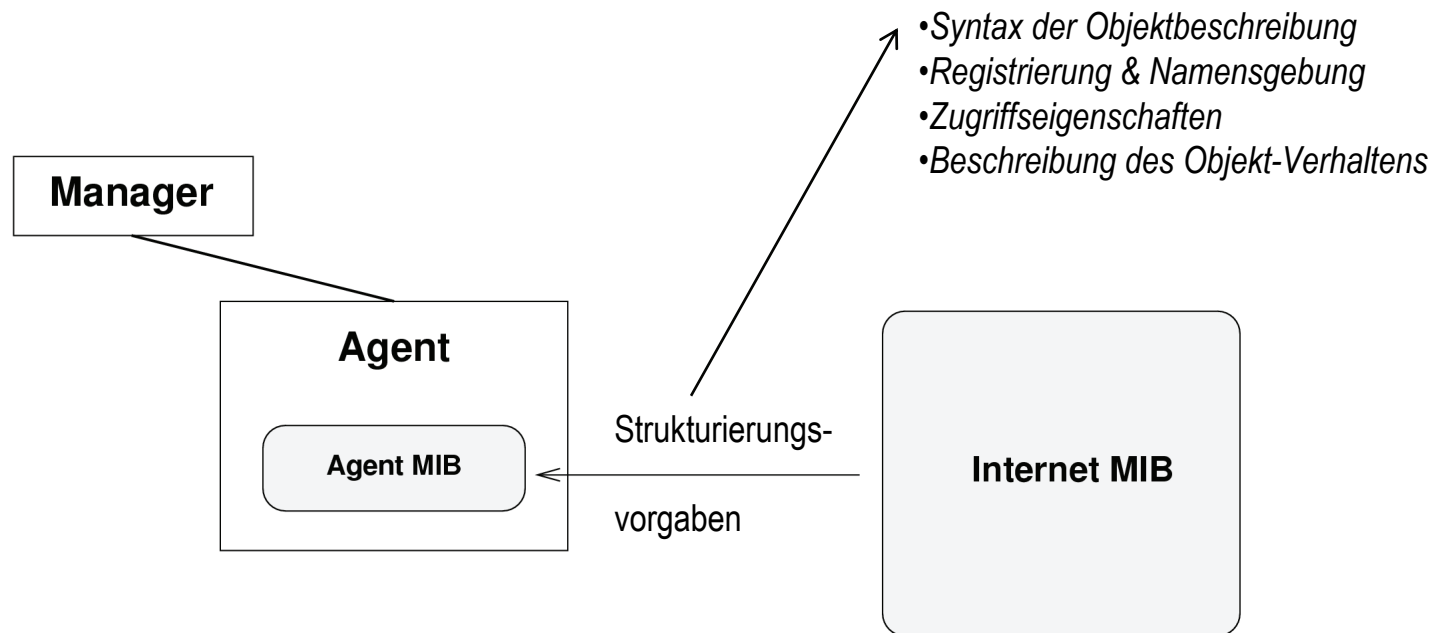
Kap. 05

Mgmt. vernetzter IT-Systeme



Internet-Informationsmodell (informell)

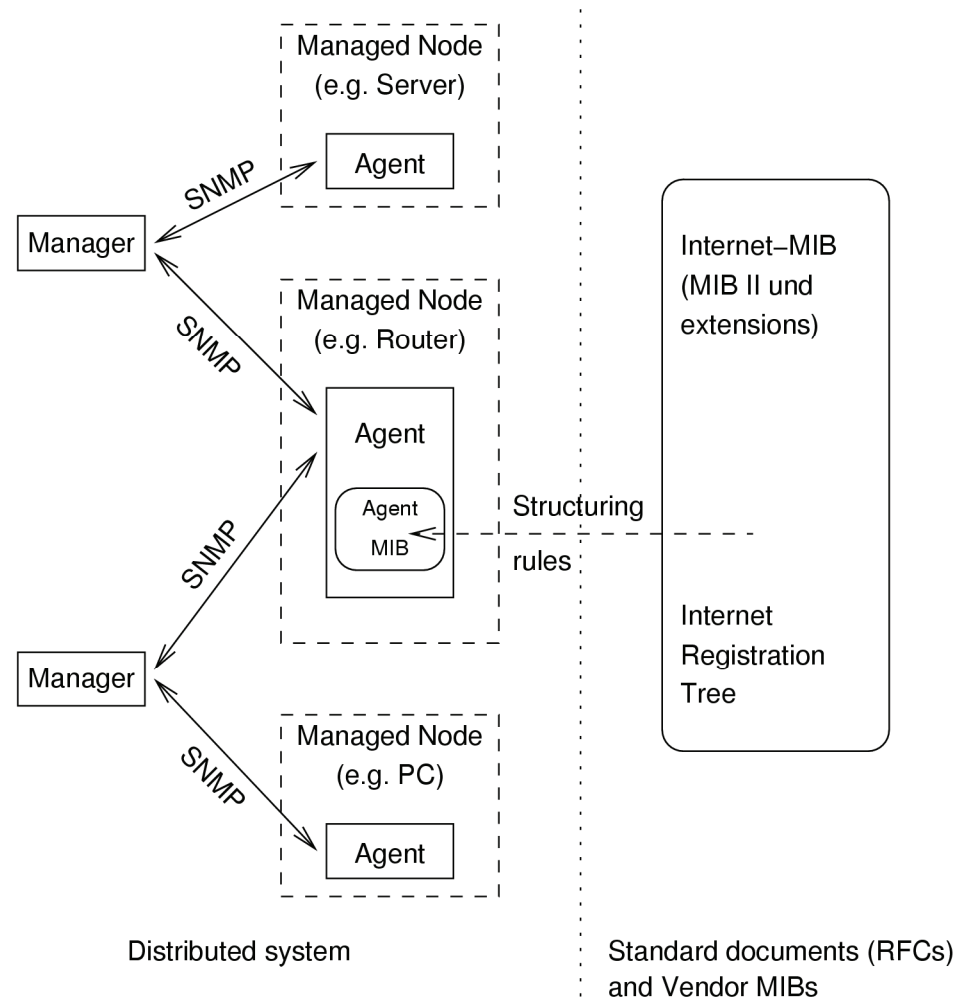
- ❑ Beschrieben im RFC 1155 (STD0016)
 - “Structure of Management Information“
- ❑ Problemstellung (informell)



Internet-Architekturmodell und MIBs

Kap. 05

Mgmt. vernetzter IT-Systeme



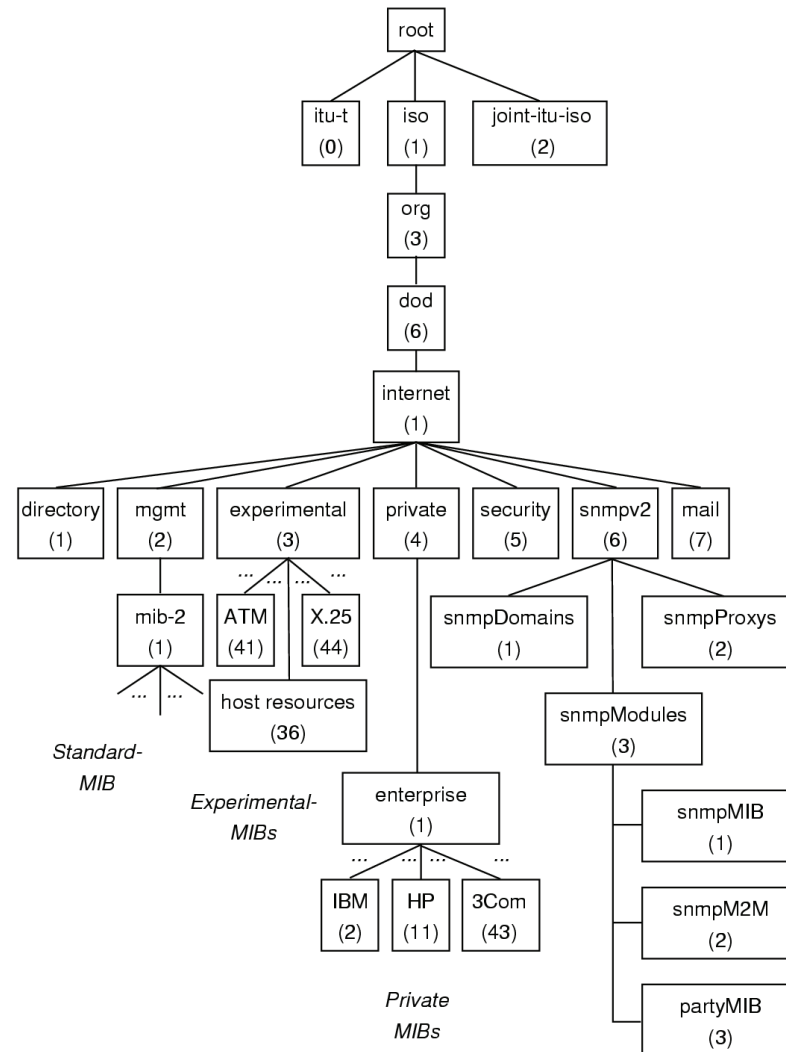
Internet-Informationsmodell

- ❑ 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 (STD 0016): „Structure of Management Information“
- ❑ RFC 2578, RFC 2579 (STD 0058): „Structure of Management Information Version 2“

Internet Registration Tree

Kap. 05

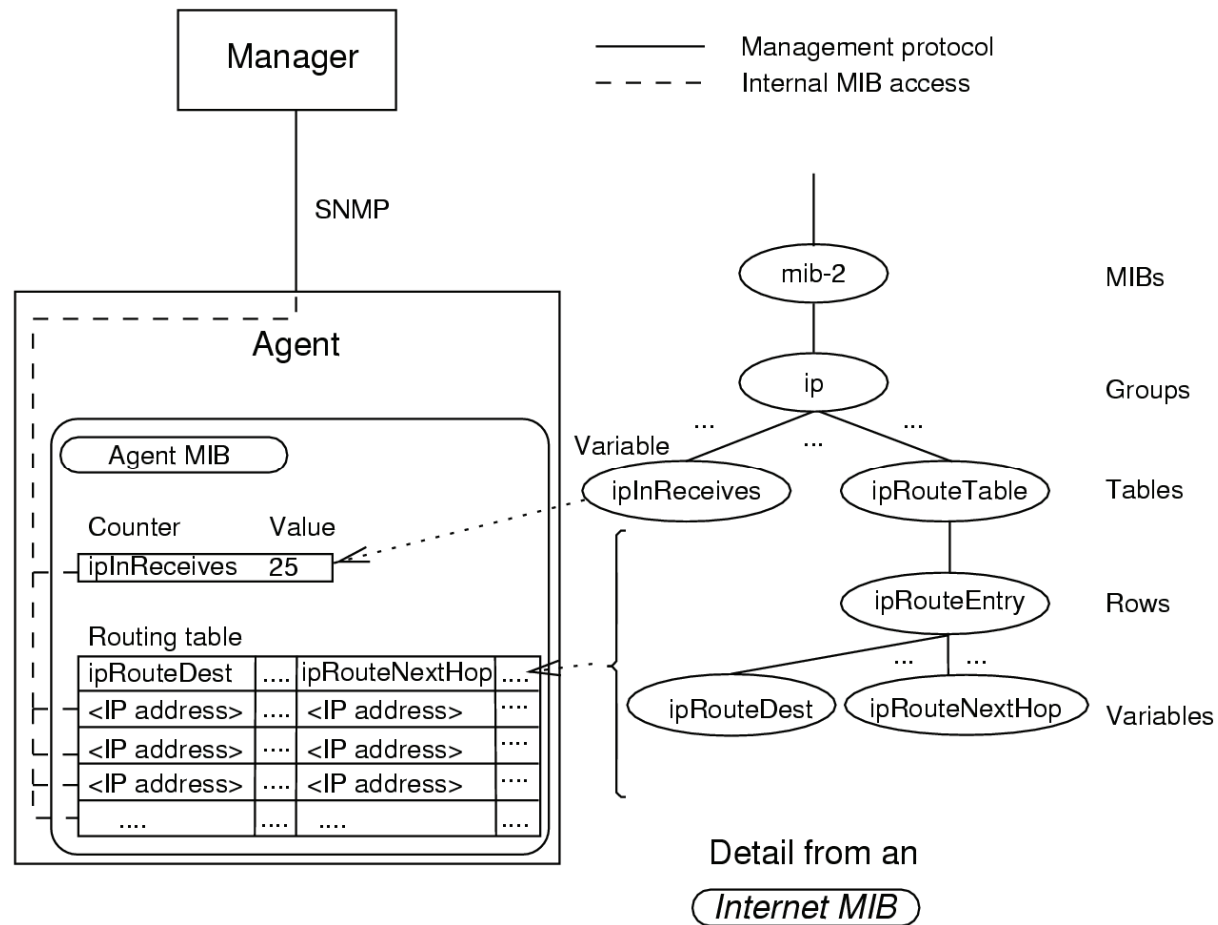
Mgmt. vernetzter IT-Systeme



Agenten- und Internet-MIB

Kap. 05

Mgmt. vernetzter IT-Systeme

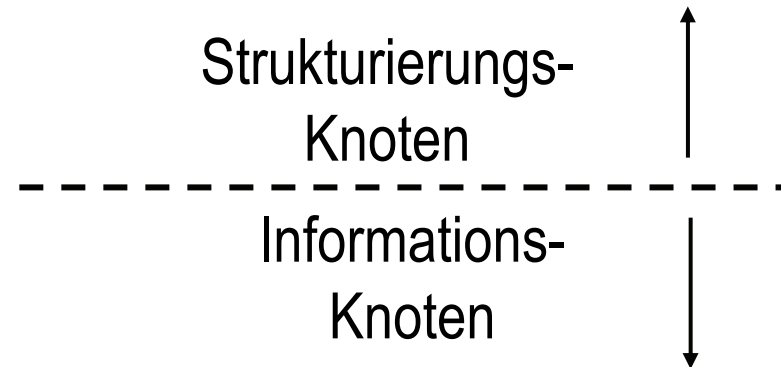
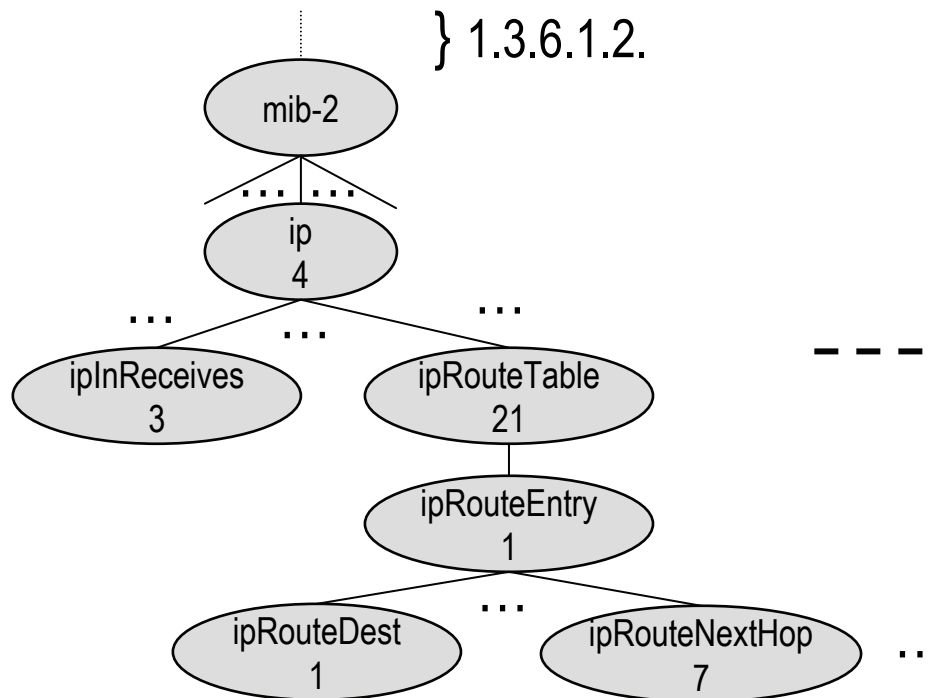


Knoten-Arten

□ Zwei Arten von Knoten im Registrierungsbaum

(1) „Strukturierungs“-Knoten

(2) „Informations“-Knoten



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 (1)

- ❑ Zähler ipInReceives

ipInReceives **OBJECT-TYPE**

SYNTAX Counter

ACCESS read-only

STATUS mandatory

DESCRIPTION

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

::= { ip 3 }

Mögliche Wertebelegungen

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

read-write, write-only, not-accessible

optional, obsolete

Syntax: Beispiel (2)

- 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

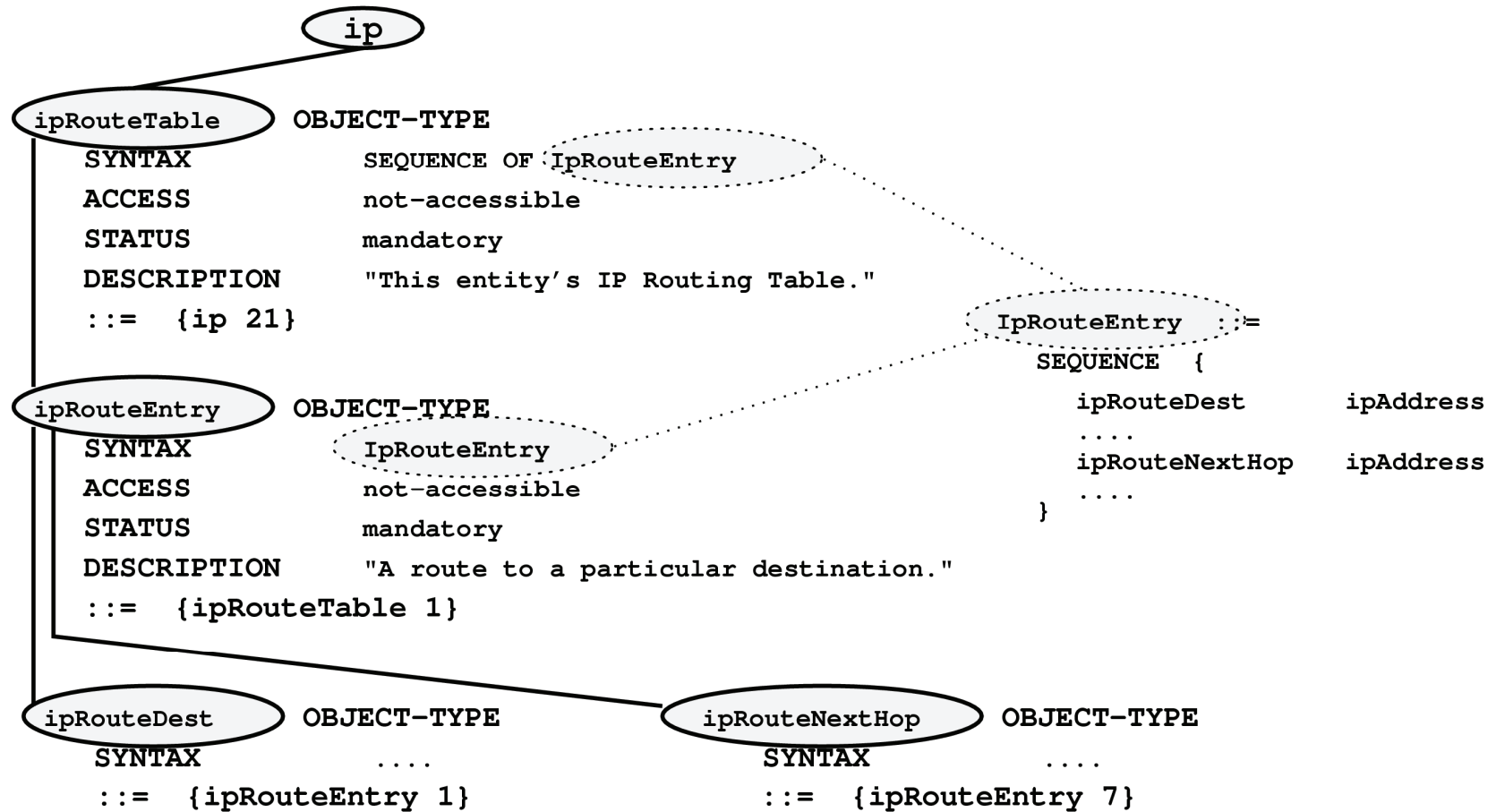
❑ Internet-Tabelle = SEQUENCE OF SEQUENCE (Einfacher Internet-Objektyp 1 ... Einfacher Internet-Objektyp N)

(Beliebig lange) Liste von
Tabellenzeilen

Beispiel: Tabelle

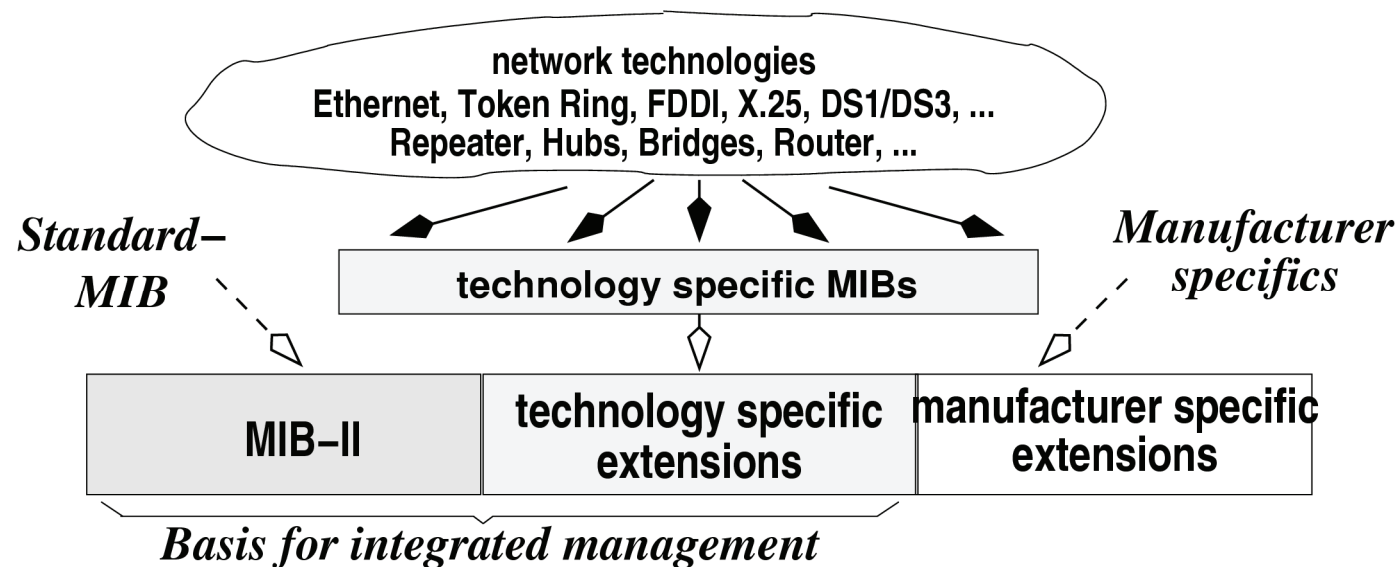
Kap. 05

Mgmt. vernetzter IT-Systeme



Internet-MIBs

- ❑ Auf der Grundlage des Informationsmodells sind konkrete Objekte zu definieren
- ❑ Internet-MIBs: Objektkataloge
- ❑ 3 Arten von Internet-MIBS:



MIB-II: Anforderungen

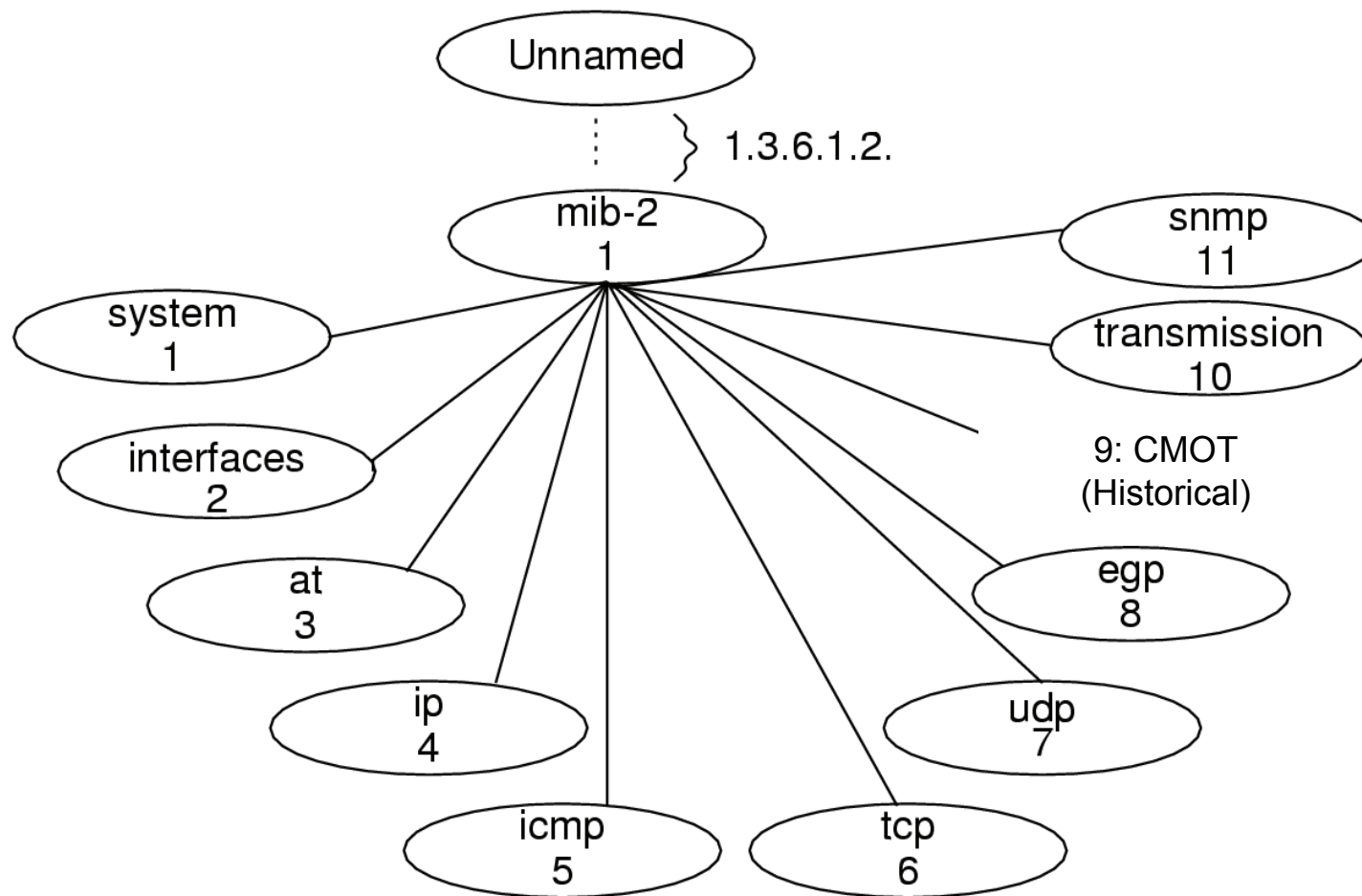
□ MIB-II

- RFC 1213 bzw. STD 0017, updated by RFCs 2011, 2012, 2013
- Basis-Objektkatalog im Internet-Management

□ Anforderungen an die Objekte der MIB-II

- Notwendigkeit für Fehler- oder Konfigurationsmanagement
- Wenig kritisch bzgl. Systemsicherheit
- Praktischer Nutzen offensichtlich, tatsächliche Nutzung absehbar
- Keine Redundanz
- Ausreichend allgemein
- Implementierungsfreundlich

Internet MIB-II: Überblick



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

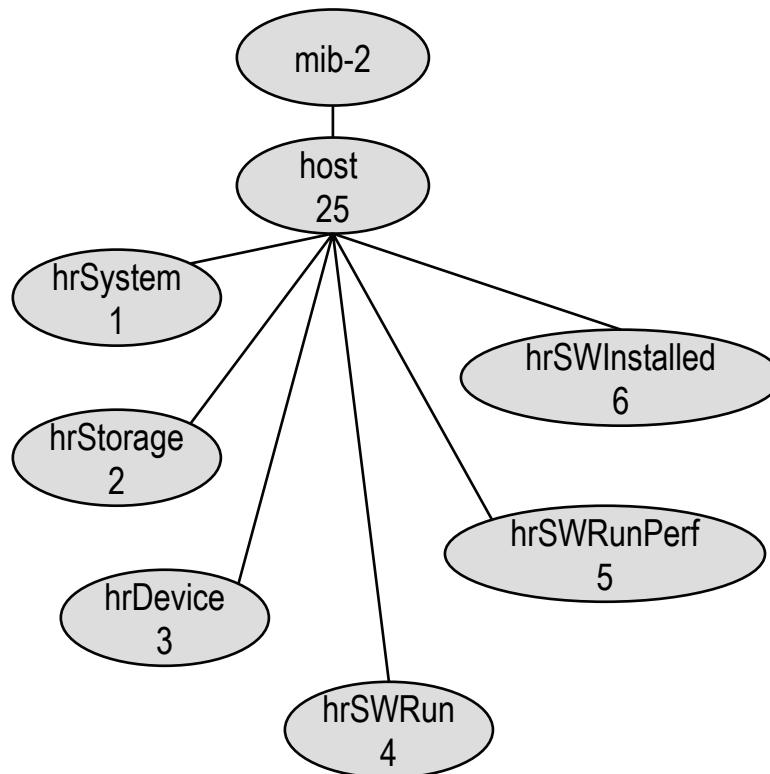
Beispiel: Bridge MIB (RFC 1493, 1525)

- ❑ Eine der ersten standardisierten Komponenten-MIBs
- ❑ Objektdefinitionen soweit möglich aus IEEE 802.1d abgeleitet
- ❑ Beziehungen zu MIB-II-Objekten präzise ausgearbeitet
 - Verhinderung von Redundanzen
- ❑ Beispiel für die Bridge-spezifische Objektdefinitionen
 - Bridge Port Table (dot1dBasePortTable)
 - Objekte zu Spanning Tree bzw. Source Routing
 - Trap bei Topologie-Änderung (topologyChange)

Internet MIBs für System und Application Mgmt.

- Host Resources MIB (RFC 2790)
- Mail Monitoring MIB (RFC 2789)
- (X.500) Directory Server Monitoring MIB (RFC 2605)
- Network Services Monitoring MIB (RFC 2788)
- Relational Database Management System MIB (RFC 1697)
- System-Level MOs for Applications (RFC 2287)
- Application Management MIB (RFC 2564)
- WWW Service MIB (RFC 2594)
- Uninterruptible Power Supply MIB (RFC 1628)
- Lessons learned
 - DNS Server/Resolver MIB Extensions („frühere“ RFCs 1611/12, siehe RFC 3197)
 - Printer MIB (RFC 1759, siehe RFC 2707 Job Monitoring MIB)

Beispiel: Host Resources MIB (RFC 2790)



❑ hrSystem-Gruppe

- Allg. Information wie z.B. uptime, Anzahl eingeloggter User, max. Prozesszahl, Zeitzone etc.

❑ hrStorage-Gruppe

- Zu jedem Speichermedium Tabelle, die dessen Eigenschaften beschreibt: Typ, Kapazität, aktuell belegter Teil, Blockgröße etc.

❑ Software-Gruppen

(Run, RunPerf, Installed)

- Status, Pfad, CPU-Zeit, allokk. Speicher, Datum des letzten update, etc.

IETF: Host Resources MIB (1)

Variables of hrSWInstalledTable

Variable Name	Variable Function
hrSWInstalledIndex	This is a unique identifier for each piece of software installed on a system. The values assigned fall within the range of 1 to n , with 1 being the value assigned to the first piece of software installed.
hrSWInstalledName	As implied by the name of this variable, it contains the name of the software; however, it should also include the manufacturer, revision, and optionally, its serial number.
hrSWInstalledID	A unique identifier for a particular piece of software.
hrSWInstalledType	Indicates whether the software is an application, device driver, operating system, or an unknown type.
hrSWInstalledDate	This is the <i>last</i> date when there was a modification to this software. It is <i>not</i> the date when the software was originally installed.

IETF: Host Resources MIB (2)

Variables of hrSWRunTable

Variable Name	Variable Function
hrSWRunIndex	A unique identifier for each piece of software running on the host. Wherever possible, this should be the unique identification number assigned by the system.
hrSWRunName	A description of the running software, including the manufacturer, revision, and its name. If this software is installed (i.e., stored) on this system, this name should be the same as the name used in the Host Resources Installed Software Group.
hrSWRunID	The product identifier (ID) for this software.
hrSWRunPath	Indicates where the software is stored. That is, it should identify where the software is loaded from in order to run. For example, this might identify a particular disk drive on this system.
hrSWRunParameters	Identifies the parameters that are supplied to the software when it was first loaded.
hrSWRunType	Indicates whether the software is an application, device driver, operating system, or an unknown type.
hrSWRunStatus	In this table, there are four possible states for a piece of software: running, runnable (waiting for a resource, such as memory), notRunnable (loaded, waiting for some prerequisite event), and invalid.

IETF: sysAppl MIB (RFC 2287) and Appl MIB (RFC 2564)

- Unterstützen keine verteilten Anwendungen
- sysAppl MIB beobachtet die Anwendung nur von außen
- Appl MIB setzt Anwendungsinstrumentierung voraus
- sysAppl MIB
 - System Application Installed Group
 - System Application Run Group
 - System Application Map Group
- Appl MIB
 - Service-Level Tables
 - Service Instance / Running Application Element Table
 - Running Application Element Status/Control Tables
 - Open File Tables
 - Open Connections Tables
 - Transaction Statistics Tables

IETF: System Application MIB

Contents of sysAppElmtRunTable for a Single Element

Variable	Description
sysAppElmtRunInvocID	This will usually be the same as the index for the application to which this element belongs in the sysAppElmtRunInstallPkg table. If the application cannot be identified, the value of this field will be 0.
sysAppElmtRunIndex	As with the sysAppElmtRunInvocID, the value of this variable will be the same as the parent application's entry in the sysAppRunIndex table. Also, if the application cannot be identified, the value of this field will be 0.
sysAppElmtRunInstallID	A unique identifier for each element running on this system.
sysAppElmtRunTimeStarted	The date and time when this element began running on this system.
sysAppElmtRunState	The run state of the element: running, runnable but waiting for a resource (e.g., CPU, file, etc.), runnable but waiting for an event, exiting, or other.
sysAppElmtRunName	The name of the element plus complete path name indicating where this application is installed on this system.
sysAppElmtRunParameters	The starting parameters for this element.
sysAppElmtRunCPU	The CPU resources consumed by this element since it began running (measured in centiseconds).
sysAppElmtRunMemory	The amount of memory currently allocated to this element (in kilobytes).
sysAppElmtRunNumFiles	The number of files currently open by this element.
sysAppElmtRunUser	The login id of the owner of this instance of this element.

IETF: Application Management MIB

Running Application Element Status Table

Variable	Description
applElmtRunStatusSuspended	This field indicates whether the element has been suspended and if it has the source of the suspension.
applElmtRunStatusHeapUsage	This contains the approximate current heap usage by this application element.
applElmtRunStatusOpenConnections	This indicates the number of current open connections associated with this application element.
applElmtRunStatusLastErrorMsg	This indicates the nature of the last error message issued by this element.
applElmtRunStatusLastErrorTime	This contains the time when the last error message was issued by this element.

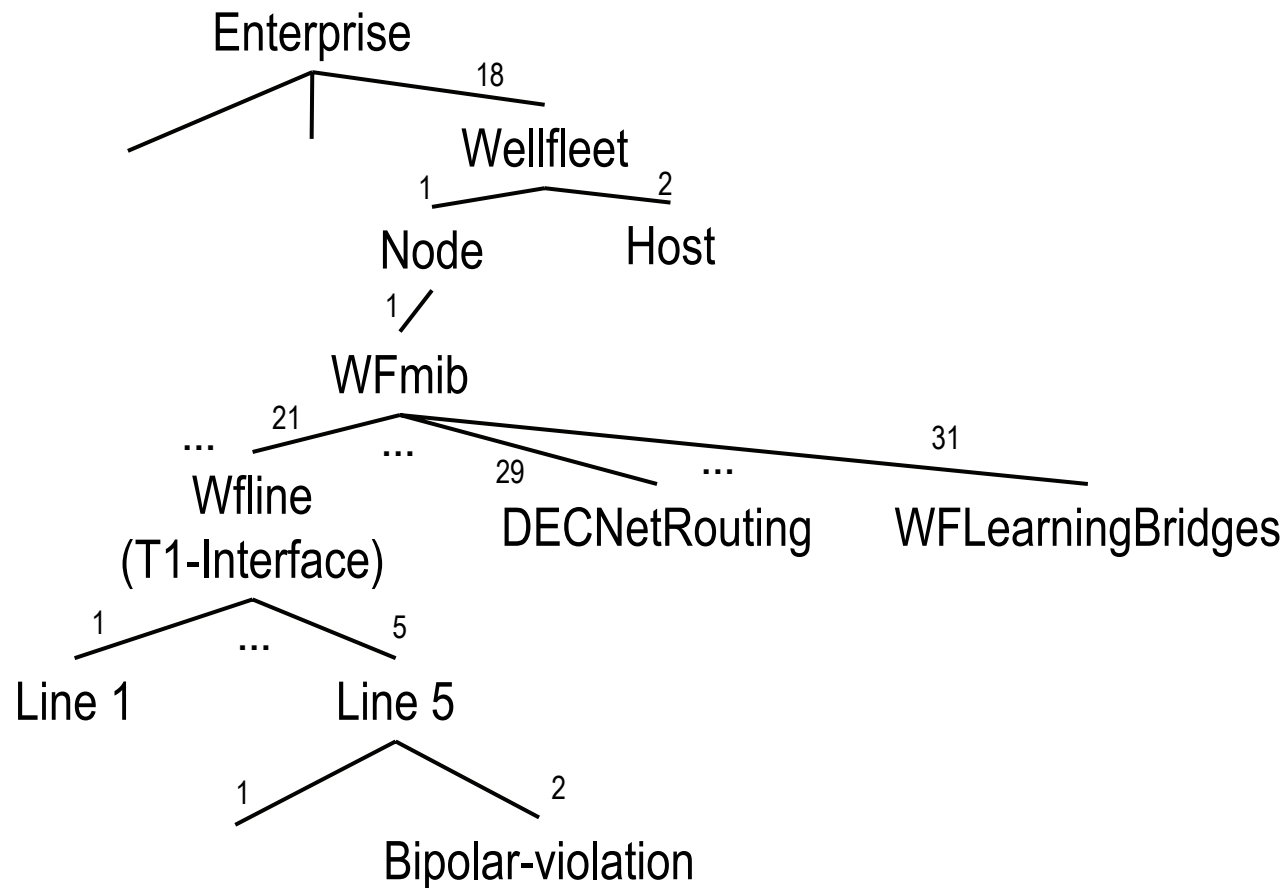
Running Application Element Control Table

Variable	Description
applElmtRunControlSuspend	Changing the setting of this variable will cause the element to be suspended if it is currently actively running. If it is currently suspended, it can be caused to resume processing by changing the setting of this variable.
applElmtRunControlReconfigure	This field can be used to instruct a running element to reload its configuration.
applElmtRunControlTerminate	This field can be utilized to cause a running application to go through a normal termination and exit.

Herstellerspezifische MIBs

- ❑ Bilden derzeit größten Anteil des Internet-Registrierungsbaums
- ❑ Die meisten herstellerepezifischen MIBs sind Komponenten-MIBs
- ❑ Ziel muss in Zukunft sein
 - Ersetzen von Teilen der herstellerepezifischen MIBs durch standardisierte Internet-MIBs
- ❑ Prozess behindert durch fehlendes Vererbungsprinzip im Internet-Informationsmodell
 - keine Verfeinerung → separate Teilbäume

Herstellerspezifische MIB (Beispiel)

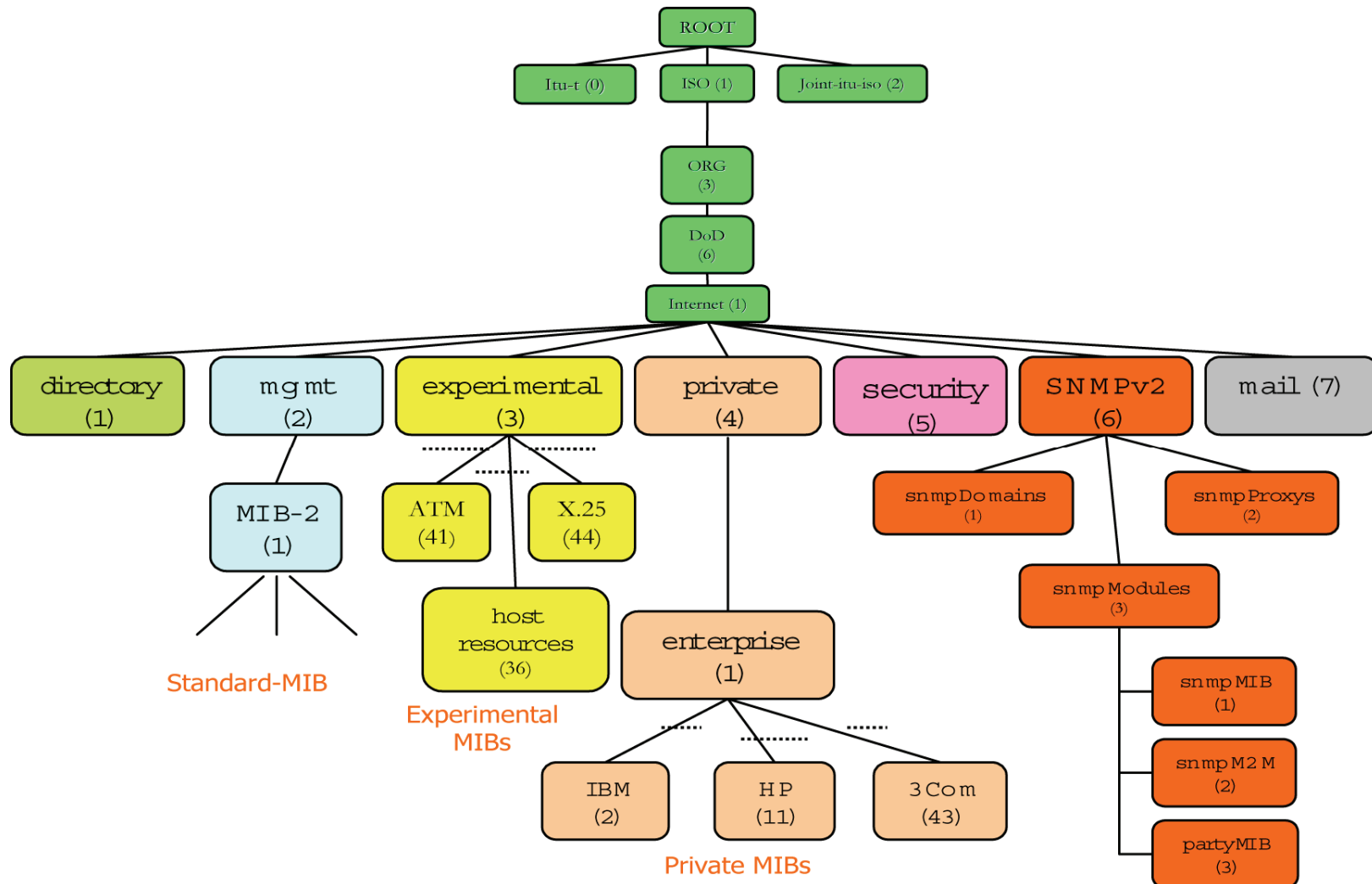


Insgesamt über 4000 Hersteller-MIBs !!

Internet Registrierungsbaum und Erweiterungen

Kap. 05

Mgmt. vernetzter IT-Systeme



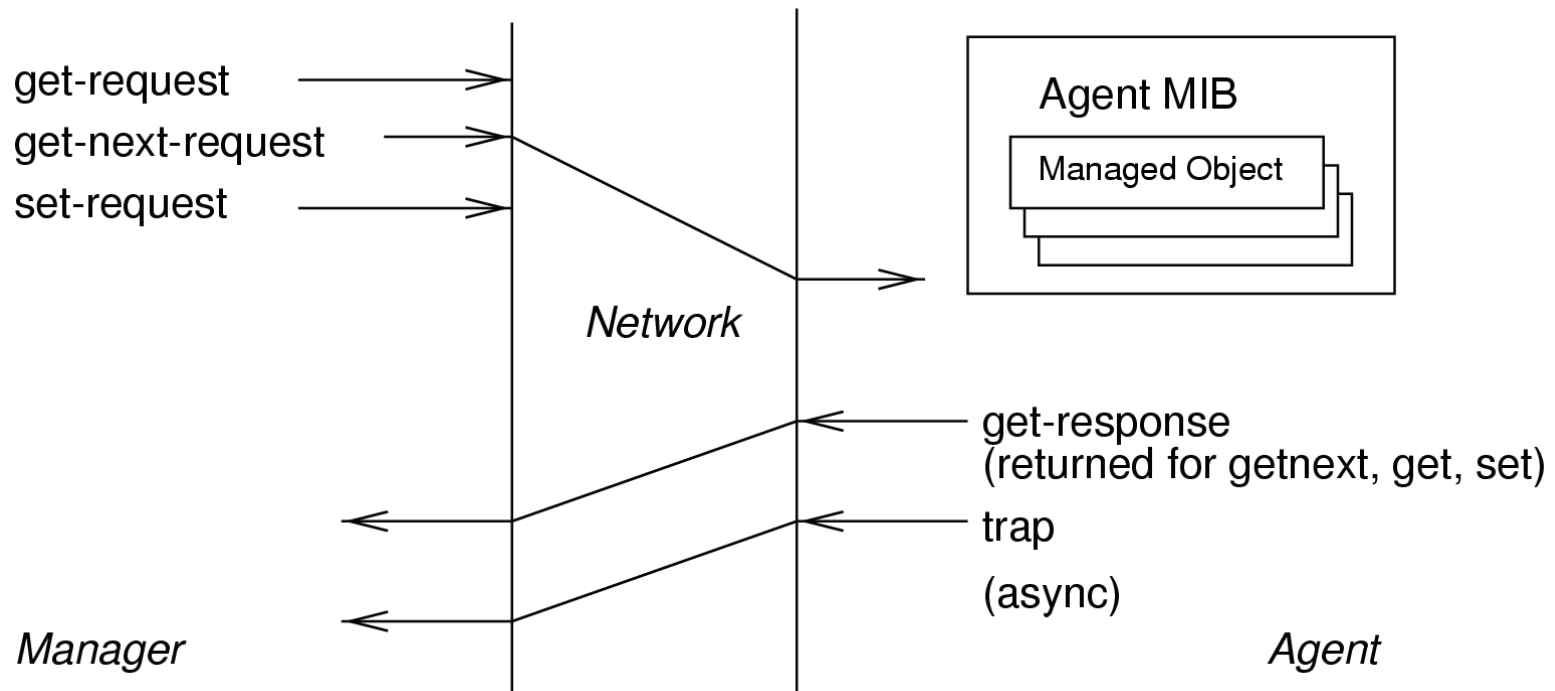
Internet-Kommunikationsmodell

- ❑ 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)

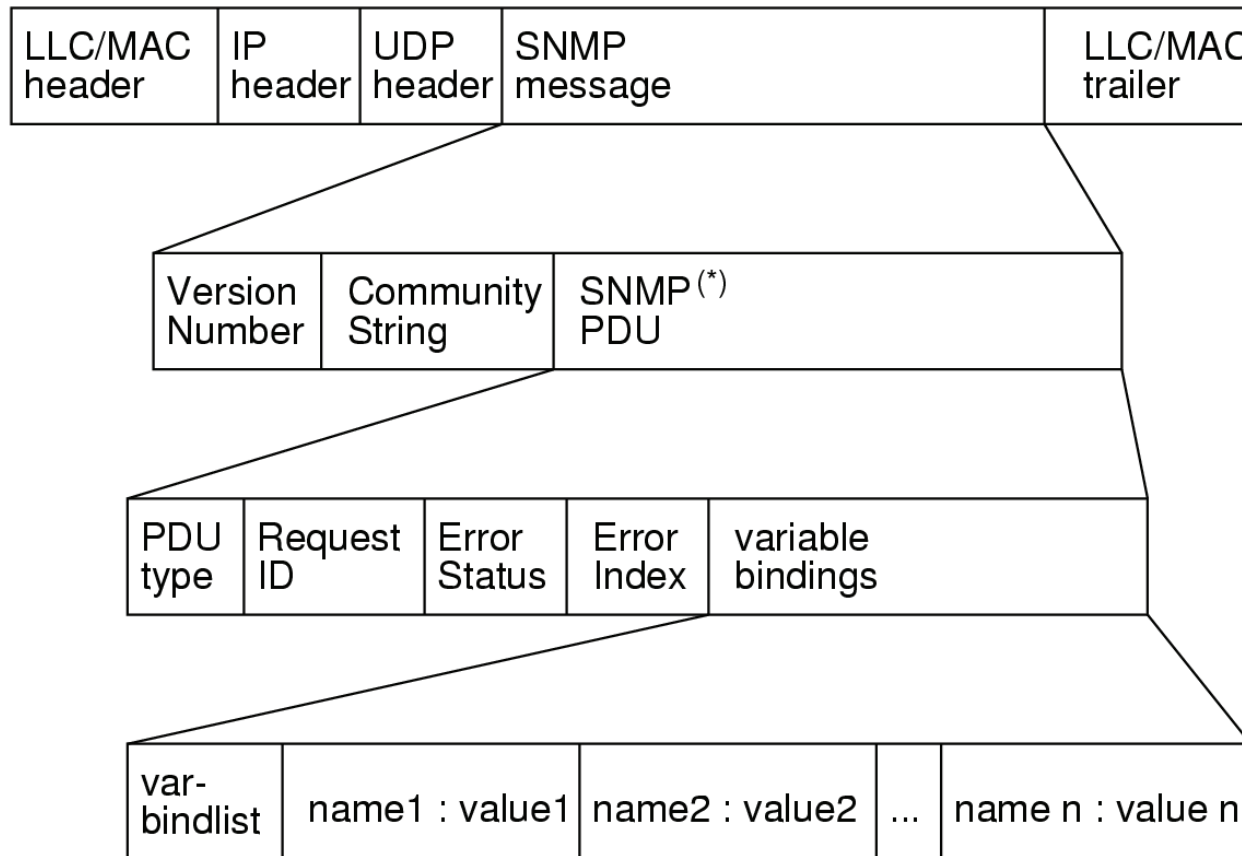
SNMP-Operationen

Kap. 05

Mgmt. vernetzter IT-Systeme



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

GetNext - Operation

- ❑ Ermöglicht den Zugriff auf eine Internet-MIB, ohne dessen Struktur im voraus genau kennen zu müssen
- ❑ Liefert als Resultat zu einem als Parameter angegebenen Objekt-Id.
 - lexikographisch nächsten Objekt-Identifikator + Wert des Objekts
- ❑ Besonders geeignet zum Auslesen einer Tabelle:

GetNextRequest (<Spaltenobjekte der Tabelle>)

GetResponse (<Objektid. + Werte der ERSTEN Zeile>)



GetNextRequest (< >)

GetResponse (<Objektid. + Werte der ZWEITEN Zeile>)

GetNext-Operation: Beispiel

ipRouteEntry	Index-Objektyp			{ipRouteEntry 7}		
	ipRouteDest	• • • •	ipRouteNextHop	• • •	• • •	• • •
	123.123.12.12		111.222.33.44		• • •	
	125.47.11.11		55.66.77.88			
	⋮	• • • •	⋮	⋮	• • •	

GetNextRequest (ipRouteDest, ipRouteNextHop)

GetResponse (ipRouteDest.123.123.12.12 = "123.123.12.12",
ipRouteNextHop.123.123.12.12 = "111.222.33.44")

GetNextRequest (ipRouteDest.123.123.12.12,
ipRouteNextHop.123.123.12.12)

GetResponse (ipRouteDest.125.47.11.11 = "125.47.11.11",
ipRouteNextHop.125.47.11.11 = "55.66.77.88")

GetNextRequest (ipRouteDest.125.47.11.11,)

SNMP Definitions in ASN.1 (RFC 1157)

```

RFC1157-SNMP DEFINITIONS ::= BEGIN

IMPORTS
    ObjectName, ObjectSyntax, NetworkAddress, IpAddress, TimeTicks
    FROM RFC1155-SMI;

-- top-level message
Message ::= SEQUENCE {version INTEGER {version-1(0) },          -- version-1 for this RFC
    community OCTET STRING,                                     -- community name
    data ANY             -- e.g., PDUs if trivial authentication is being used

-- protocol data units
PDU ::= CHOICE { get-request          GetRequest-PDU,
    get-next-request          GetNextRequest-PDU,
    get-response              GetResponse-PDU,
    set-request                SetRequest-PDU,
    trap                       Trap-PDU}

-- PDUs
GetRequest-PDU ::=          [0] IMPLICIT PDU
GetNextRequest-PDU ::=     [1] IMPLICIT PDU
GetResponse-PDU ::=        [2] IMPLICIT PDU
SetRequest-PDU ::=         [3] IMPLICIT PDU

PDU ::= SEQUENCE { request-id INTEGER,
    error-status INTEGER {
        noError(0),          -- sometimes ignored
        tooBig(1),
        noSuchName(2),
        badValue(3),
        readOnly(4),
        genErr(5)},
    error-index INTEGER,    -- sometimes ignored
    variable-bindings VarBindList}

Trap-PDU ::= [4] IMPLICIT SEQUENCE {
    enterprise OBJECT IDENTIFIER,    -- type of object generating
    agent-addr NetworkAddress,       -- trap, see sysObjectID in RFC 1155
    generic-trap INTEGER {          -- address of object generating trap
        coldStart(0),
        warmStart(1),
        linkDown(2),
        linkUp(3),
        authenticationFailure(4),
        egpNeighborLoss(5),
        enterpriseSpecific(6)},    -- generic trap type
    specific-trap INTEGER,          -- specific code, present even
    time-stamp TimeTicks,           -- if generic-trap is not enterpriseSpecific
    variable-bindings VarBindList}

-- variable bindings
VarBind ::= SEQUENCE {name ObjectName,
    value ObjectSyntax }

VarBindList ::= SEQUENCE OF VarBind

END

```


SNMP-PDU Verarbeitung

```

procedure receive-getrequest;
begin
    if object not available for get then
        issue getresponse (noSuchName, index)
    else if generated PDU too big then
        issue getresponse (tooBig)
    else if value not retrievable for some other reason then
        issue getresponse (genErr, index)
    else issue getresponse (variablebindings)
end;

```

```

procedure receive-getnextrequest;
begin
    if no next object available for get then
        issue getresponse (noSuchName, index)
    else if generated PDU too big then
        issue getresponse (tooBig)
    else if value not retrievable for some other reason then
        issue getresponse (genErr, index)
    else issue getresponse (variablebindings)
end;

```

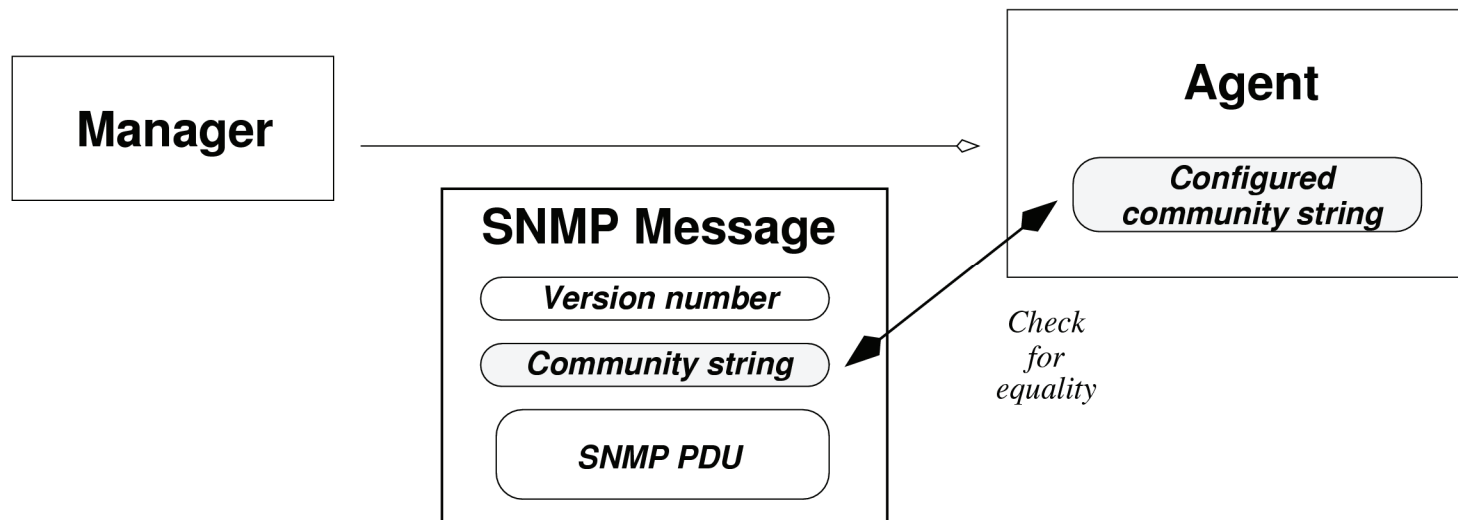
```

procedure receive-setrequest;
begin
    if object not available for set then
        issue getresponse (noSuchName, index)
    else if inconsistent object value then
        issue getresponse (badValue, index)
    else if generated PDU too big then
        issue getresponse (tooBig)
    else if value not settable for some other reason then
        issue getresponse (genErr, index)
    else issue getresponse (variablebindings)
end;

```

Internet Management: Communication model (1)

- ❑ Security aspects: Community string (SNMPv1)



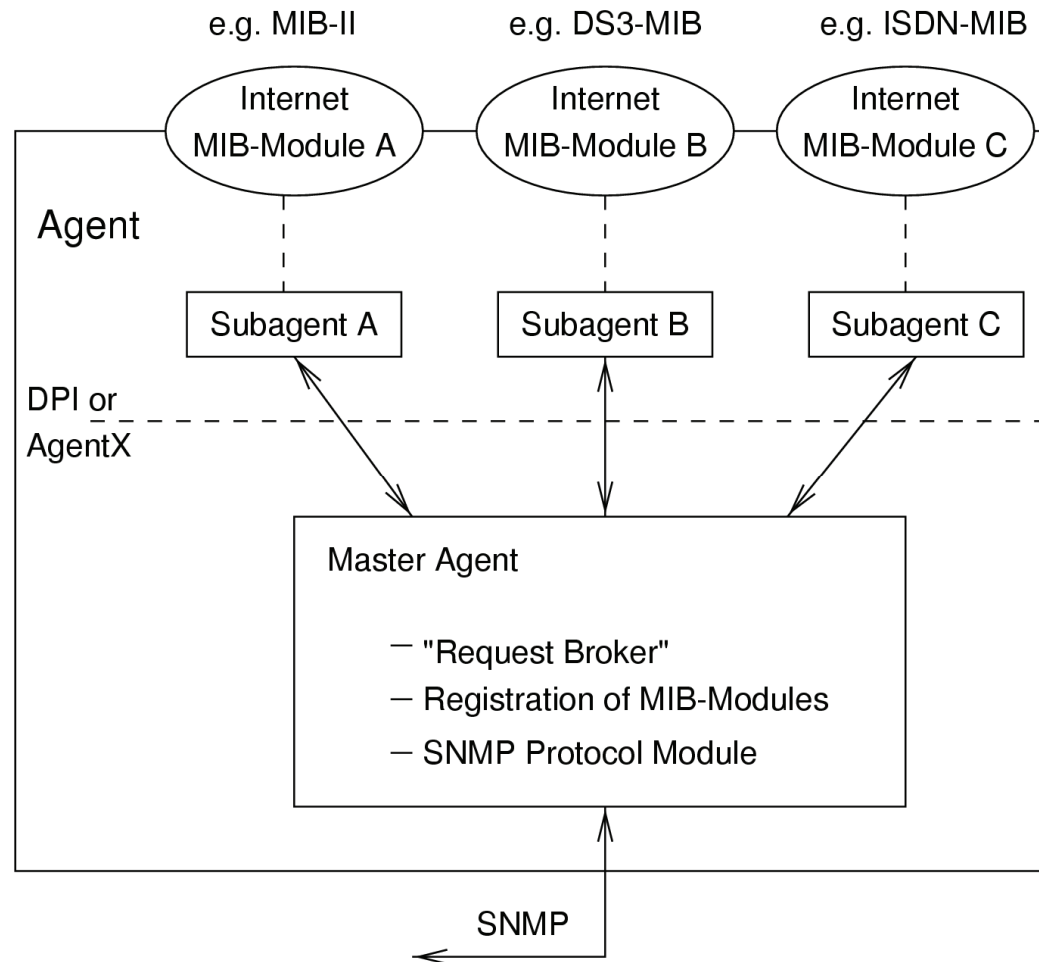
Internet Management: Communication model (2)

❑ 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

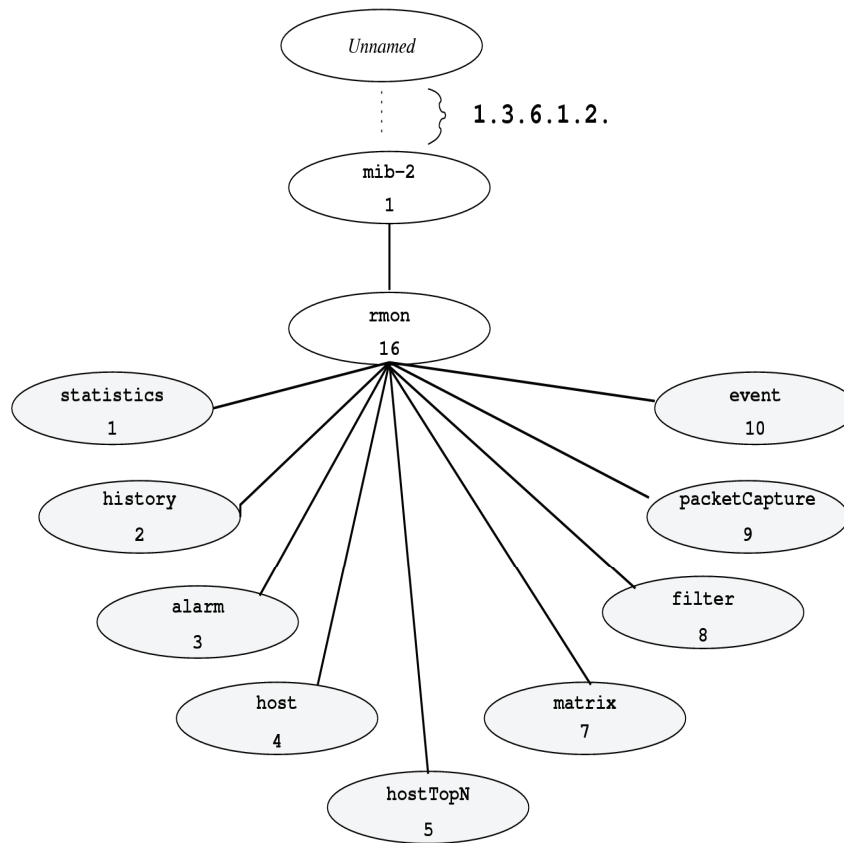
aber: community strings werden ungesichert übertragen!

AgentX und DPI (Distributed Protocol Interface)



Internet-Funktionsmodell

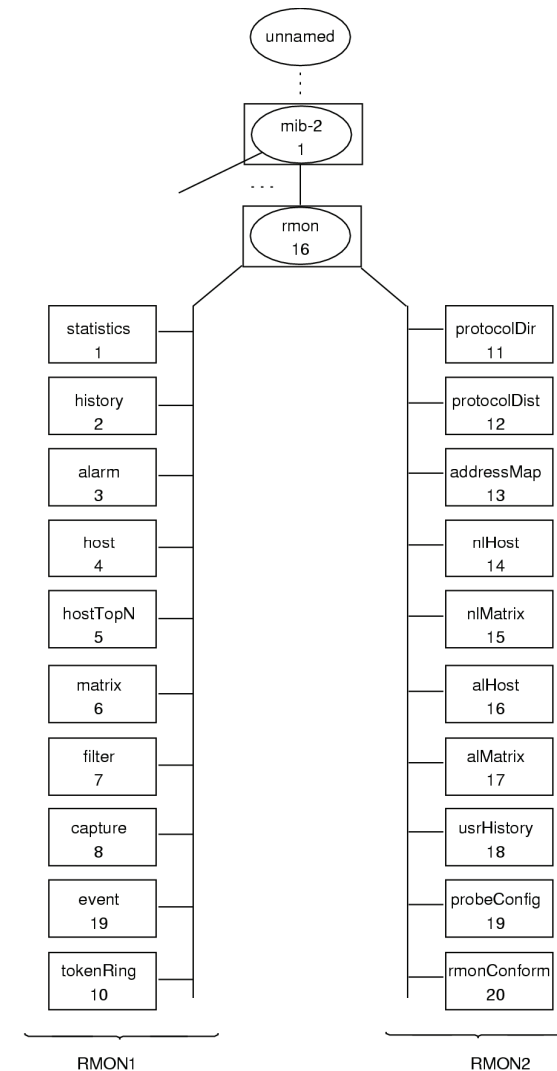
- ❑ Remote Network Monitoring MIB (RMON-MIB , RFC 2819, STD 59)



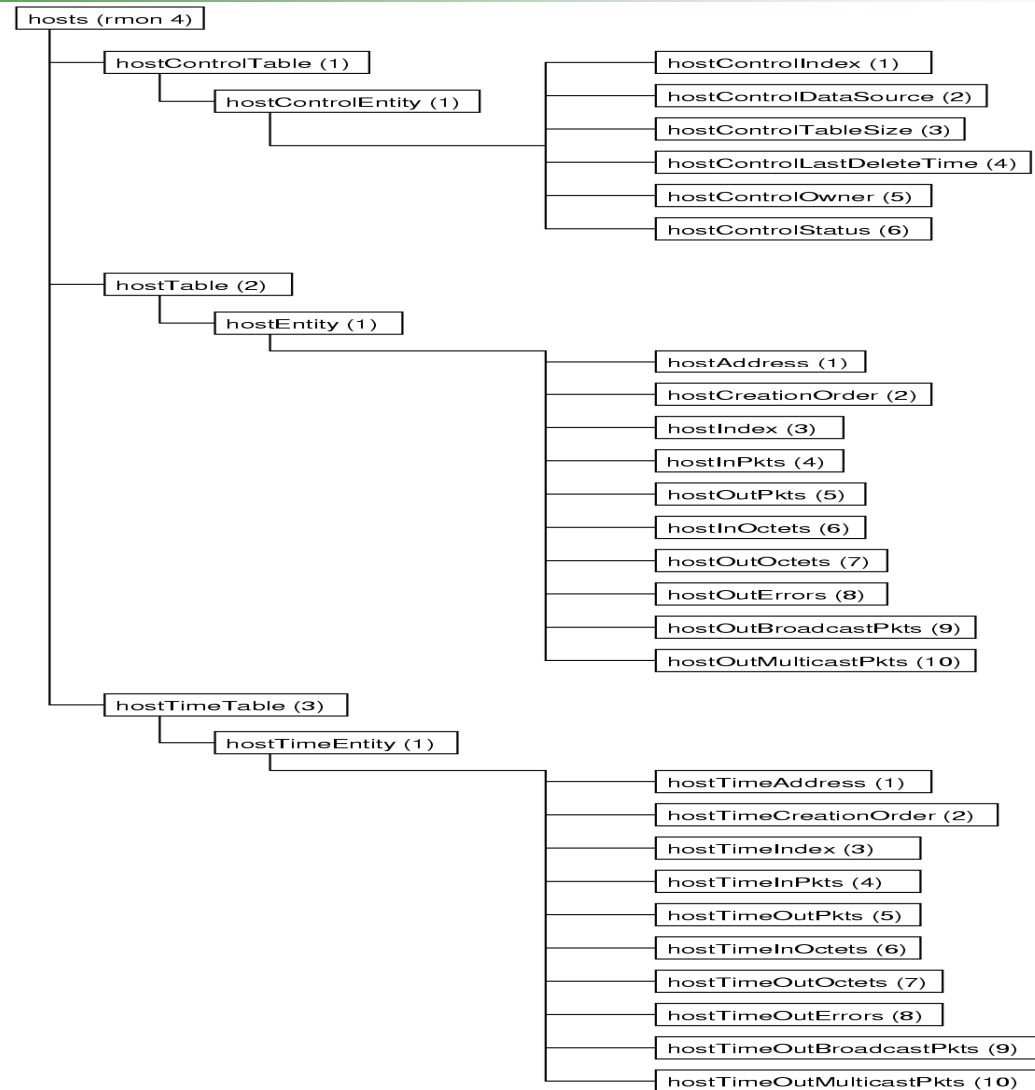
- RMON-MIB ist unterhalb des MIB-II-Knotens angeordnet
- Beinhaltet funktionale Elemente vergleichbar mit gewissen OSI Systems Management Functions (Metric Objects and Attributes, Event Report Management Function, Alarm Reporting Function)
- Hauptsächlich Performance-relevante Management-information
- Primärer Focus: OSI-Layer 1 und 2 (Ethernet)

RMON2-MIB (Internet Draft, August 2003)

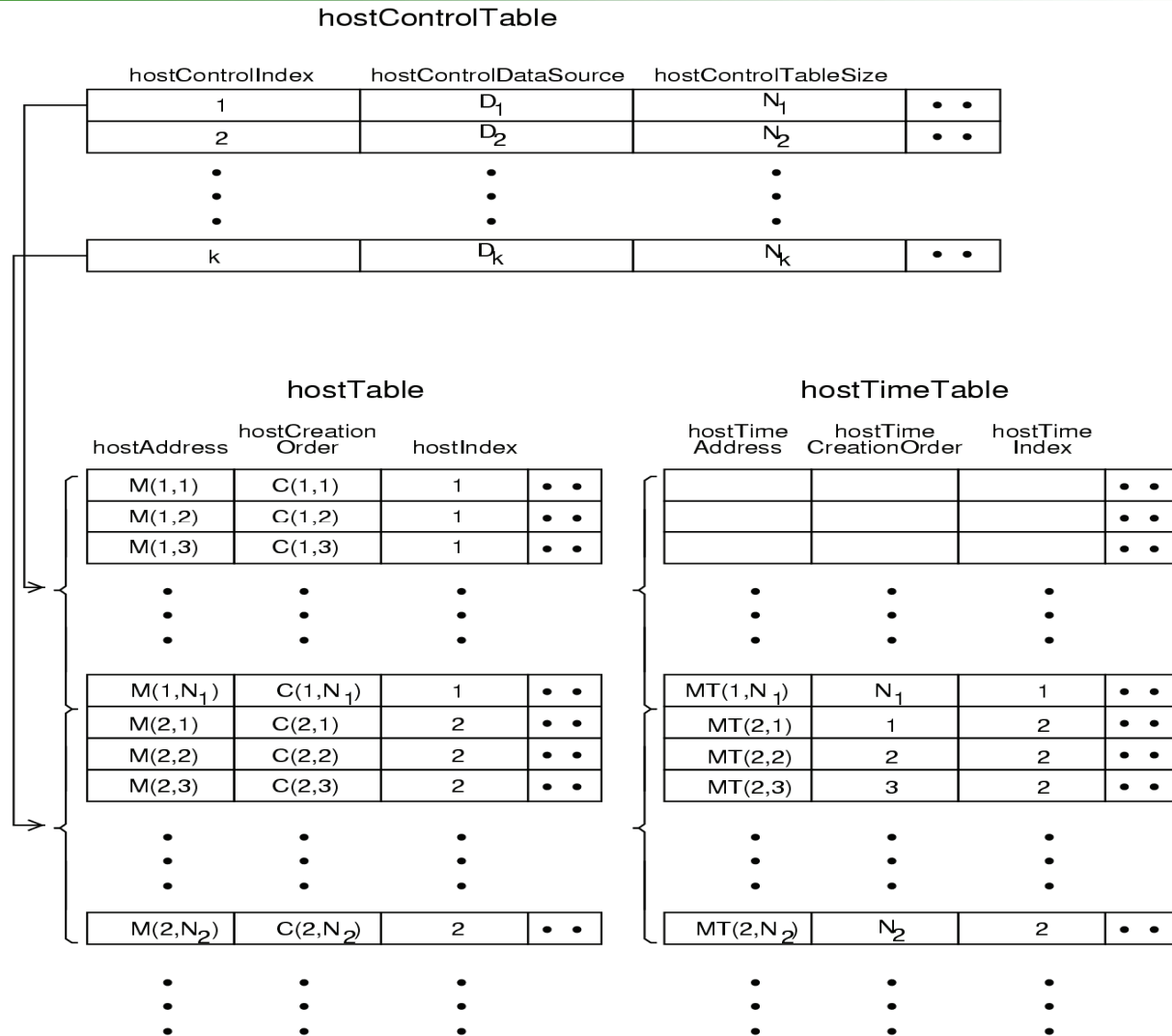
- Erweitert RMON-Ansatz um Monitoring für OSI-Laxer 3-7
- Flexibleres Arbeiten mit Tabellen
- 10 weitere Gruppen (al: application layer, nl : network layer)
- Adressabbildung
- Interoperabilität von RMON-Implementierungen und Konfiguration der Probes



RMON-MIB (Ausschnitt) (1)

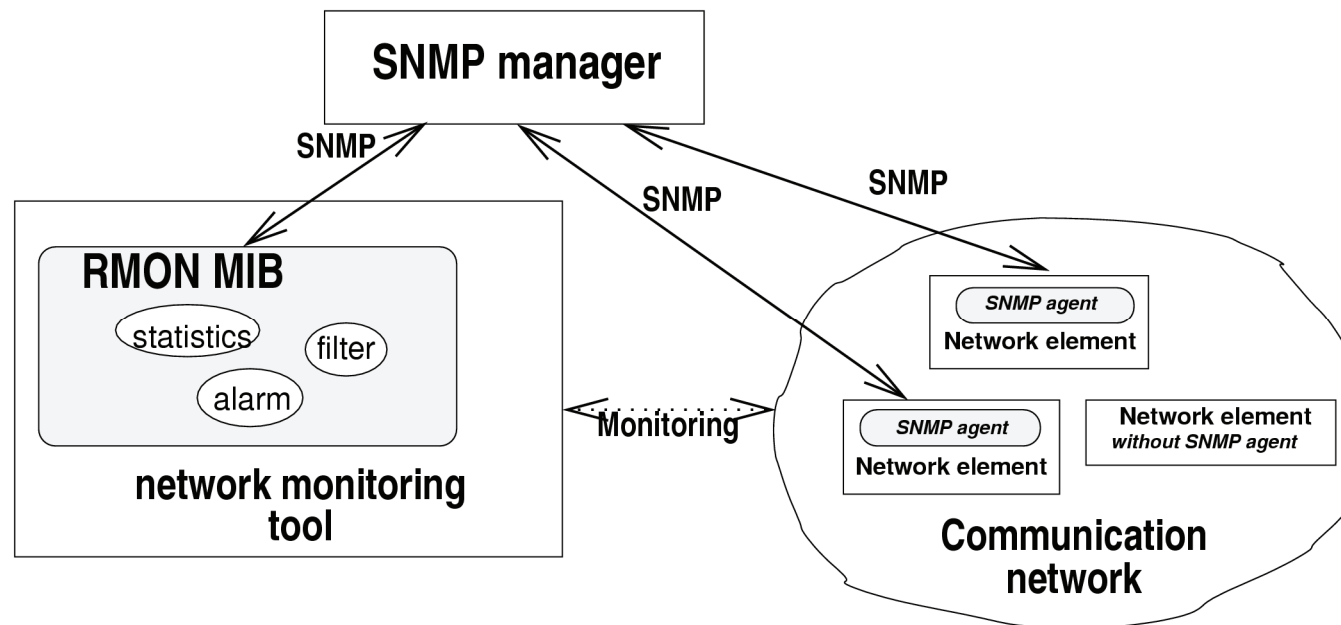


RMON-MIB (Ausschnitt) (2)



Einsatzbereich der RMON-MIB

- ❑ Integration von Netzüberwachungsgeräten (z.B. Protokollanalyatoren) in eine Management-Plattform
- ❑ Delegieren von Funktionalität in Mid-Level-Manager
- ❑ Nutzung der Möglichkeiten leistungsfähiger Agenten



SNMP Version 2 (und Version 3): Motivation

- ❑ Nachteile des Internet Management Version 1 (SNMPv1)
 - Überwachung der Ressourcen durch Polling
 - Geringe Unterstützung asynchroner events
 - Problematische Übertragung großer Datenmengen
 - Primitives Sicherheitskonzept: unverschlüsseltes Passwort
 - Managementfunktionalität liegt nur in den Anwendungen
 - Nur eingeschränkt nutzbar für Systemmanagement
 - Vielzahl herstellerspezifischer Erweiterungen
 - Datenverluste durch verbindungsloses Protokoll

Internet Management Version 2 und 3

□ Definition der Version 2:

- Informationsmodell-Erweiterungen
- Protokollverbesserungen
- Erweiterung der delegierbaren Funktionalität
- Aber: keine Einigung auf ein Sicherheitskonzept!

□ Version 3:

- übernimmt i.w. die Modelle von Version 2
- führt ein Sicherheitskonzept und Sicherheitsmechanismen ein

□ Zusätzliche Neuerungen in Version 3:

- Definition einer Architektur und der Komponenten (RFCs 3411, 3412, 3413)
- Definition von abstrakten Dienstprimitiven für den Zugriff auf Funktionen der Komponenten
- Vorkehrungen für Koexistenz von Version 1 und Version 2

SNMP Version 2 und 3: Verbesserungen

- ❑ Informationsmodell-Erweiterungen (RFCs 2578 - 2580, STD 58)
 - Notification-Definition, Agent-Capabilities-Makro
 - Neue Objekttypen (z.B. 64-bit counter)
 - Modularisierung der MI
- ❑ Protokoll-Verbesserungen (RFCs 3416, 3417, 3418, STD 62)
 - GetBulk-Operator (effiziente Übertragung großer Datenmengen)
 - Inform-PDU zur Meldung asynchroner Ereignisse
 - verbesserte Fehlerbehandlung
- ❑ Sicherheitskonzept (RFCs 3414, 3415, STD 62)
 - Authentifizierung mit HMAC-MD5-96 oder HMAC-SHA-96
 - Verschlüsselung mit CBC DES
 - Zugriffskontrolle: View-basiert (MIB-Teilbäume)
- ❑ Funktionsmodell-Erweiterungen
 - Laufende Erweiterung durch mehrere Arbeitsgruppen
 - Z.B.: Schwellwertüberwachung, Event-Forwarding, Alarm-Reporting

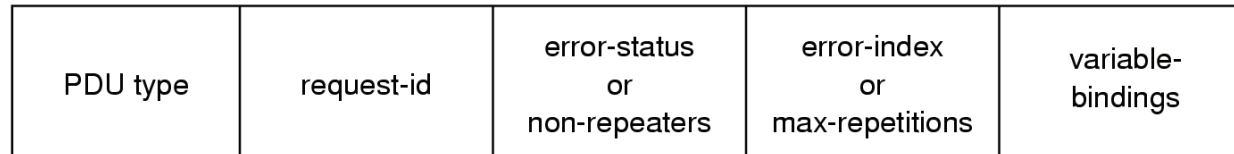
SMLv2 (Structure of Management Information Version 2): Makros

- Object Type Macro
- Notification Type Macro
 - Definition asynchroner Ereignismeldungen
 - Einheitliche Definition für Traps und InformRequests
- Module Identity Macro
 - Information zu Kontaktpersonen, Version des Moduls, ...
- Object Identity Macro
 - Information zur Wahl des Object Identifier

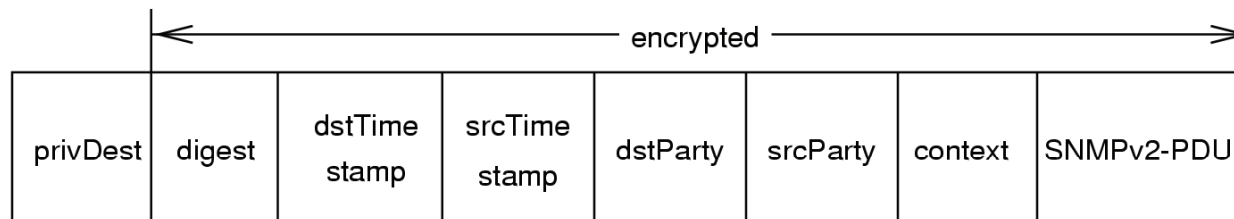
SNMPv2 Object Type Macro

- ❑ SYNTAX:
 - wie bei SNMPv1, zusätzlich Counter 64, Unsigned 32
- ❑ Unitsparts:
 - assoziierte Dimensionen (e.g. Sek, Nachrichten)
- ❑ MAX-ACCESS:
 - not-accessible, accessible-for-notify, read-only, read-write, read-create
- ❑ STATUS:
 - current, deprecated, obsolete
- ❑ Referpart:
 - Referenztext zu anderen Modulen
- ❑ Indexpart:
 - für flexible Tabellendefinitionen
- ❑ Valpart:
 - Default-Wert

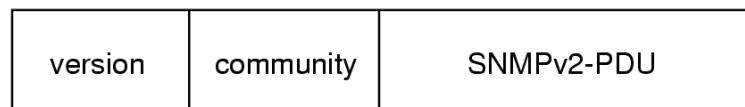
SNMP Message (Version 2)



SNMPv2-PDU



SNMPv2p-Message (private and authenticated)



SNMPv2c-Message

Funktionsmodell-Erweiterungen (1)

- ❑ Notification Log MIB (RFC 3014)
 - Logging transienter (Ereignis-)Information im Agenten
 - Sicherung gegen Verlust
 - Laufende Prüfung auf Informationsverluste durch Manager möglich
- ❑ Event MIB (RFC 2981)
 - Laufende Überwachung von MOs innerhalb des Agenten
 - Definition von Trigger-Bedingungen und resultierenden Aktionen (z.B. Auslösen von Notificationen)
- ❑ Script MIB (RFC 3165)
 - Delegation allgemeiner Management-Funktionalität (Scripts)
 - Steuerung der Ausführung
 - Sprachneutral
- ❑ Schedule MIB (RFC 3231)
 - Periodische/zeitgesteuerte Ausführung von Management-Aktionen im Agenten

Funktionsmodell-Erweiterungen (2)

- Alarm MIB, Alarm Reporting Control MIB
 - Internet Drafts, 11/03 bzw. 09/03
 - Management von Alarm-Bedingungen und Alarm-Reporting
 - Begriffsbildungen zu Alarmen und Fehlerzuständen
- Application Performance Measurement MIB
 - Internet Draft, 10/2003
 - Fortsetzung des RMON-Gedankens
 - (Entfernte) Messung der Performance „aus Anwendersicht“
- Real-time Application Quality-of-Service Monitoring
 - Internet Draft, 11/2003
 - (Entfernte) Messung der Performance von Hand-Helds, Mobile Phones etc.
- Policy Based Management MIB
 - Internet Draft, 09/2003

Weitere aktuelle Entwicklungen

- Unterstützung von Transaktionen in SNMP
 - Zusammenfassung des Diskussionsstands in RFC 3512 („Configuring Networks and Devices with SNMP“)
- Entity MIB (Version 2: RFC 2737)
 - Derzeit dritte Version in der Standardisierung
 - Unterstützung mehrerer Instanzen eines MIB-Moduls in einem Agenten
- SNMP Entity (Version 3)
- DISMAN

SNMP Entity (Version 3)

SNMP entity

SNMP engine (identified by snmpEngineID)

Dispatcher

Message
Processing
Subsystem

Security
Subsystem

Access
Control
Subsystem

Application(s)

Command
Generator

Notification
Receiver

Proxy
Forwarder

Command
Responder

Notification
Originator

Other

DISMAN

- Ansatz im Internet zum Management-by-Delegation
- Disman User sendet mittels Credentials abgesicherte Aufträge an einen Distributed Manager
Dieser koordiniert verteilte Ausführungen auf Management Targets
- Teilaufgaben sind Beschreibung von
 - Aufträgen, Domänen, Targets, Credentials, ferner sichere Delegation
- Zugehörige MIBs:
 - SERVICES MIB, TARGET MIB, SCRIPT MIB, EVENT MIB usw.

Internet-Management: Zusammenfassung (1)

□ Ansatz

- Pragmatischer, einfacher als der universelle, aber komplexe ISO-Ansatz
- Dadurch: seit geraumer Zeit im Einsatz, praktische Erfahrungen vorhanden
- Aufbauend auf Erfahrungen laufende Erweiterungen
- Damit zunehmende funktionale Ähnlichkeit zum ISO-Ansatz

□ Informationsmodell

- Einfach, wenig Strukturierungsmöglichkeiten, aber große Akzeptanz
- Wegen fehlender Strukturierung konkrete MI unübersichtlich, über Registrierungsbaum zersplittert
- Mit Version 2 und 3 diverse Erweiterungen
- Verbesserungen bringen größere Ähnlichkeit mit OSI-Management, z.B. freie Definition von Notificationen

Internet-Management: Zusammenfassung (2)

□ Kommunikationsmodell

- Basiert auf verbindungslosem, ungesichertem Transportdienst
- Kein scoping bzw. filtering
- Keine Unterstützung von Transaktionen
- Mit Version 2 und 3 Verbesserungen, speziell in Richtung Übertragungssicherung und Effizienz

□ Funktionsmodell

- Anfänglich kaum ausgeprägt (Ausnahme: RMON)
- Mit Version 2 und 3 diverse delegierbare Managementfunktionalität vorhanden, ähnlich zu (einfachen Varianten) von OSI System Management Functions
- Laufende Erweiterungen

ISO-NM versus Internet-NM

	OSI	IAB
Vorgehen	universeller Ansatz	Pragmatik, einfache Implementierbarkeit
Informationsmodell	objektorientiert (Vererbung, Allomorphie) gut strukturierte MIBs, Wiederverwendbare MOC-Def.	Datentypansatz, flacher Objektbaum keine generische Objektdefinition unstrukturierte MIB-Vielfalt
Organisationsmodell	Domänen als MOs	kein Domänen-Konzept
Funktionsmodell	ausgeprägt, SMFA, SMFs	Ansatz über RMON
Kommunikationsmodell	CMIP verbindungsorientiert (über ACSE, ROSE); zusätzlich: ACTION, CREATE Scoping, Filtering	SNMP verbindungslos (auf UDP)

Internet-Management: Dokumente (1)

RFC	STD	Titel	Datum	Ersetzte Dokumente
3410	INF	Introduction and Applicability Statements for Internet Standard Management Framework	12/2002	2570
3411	62	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks	12/2002	2271, 2571
3412	62	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)	12/2002	2272, 2572
3413	62	Simple Network Management Protocol (SNMP) Applications	12/2002	2273, 2573
3414	62	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)	12/2002	2274, 2574
3415	62	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)	12/2002	2275, 2575
3416	62	Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)	12/2002	1905, 1448
3417	62	Transport Mappings for the Simple Network Management Protocol (SNMP)	12/2002	1906, 1449
3418	62	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)	12/2002	1907, 1450
2578	58	Structure of Management Information Version 2 (SMIv2)	04/1999	1902, 1442
2579	58	Textual Conventions for SMIv2	04/1999	1903, 1443
2580	58	Conformance Statements for SMIv2	04/1999	1904, 1444
3584	BPC 74	Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework	08/2003	1908, 2089, 2576
1155	16	Structure and Identification of Management Information for TCP/IP-based Internets	05/1990	1065
1157	15	Simple Network Management Protocol (SNMP) (HISTORIC, see RFC 3416)	05/1990	1098
1213	17	Management Information Base for Network Management of TCP/IP-based internets:MIB-II (Updated by RFC2011, RFC2012, RFC2013)	03/1991	1158
2737	PS	Entity MIB (Version 2)	12/1999	2037
3512	INF	Configuring Networks and Devices with Simple Network Management Protocol (SNMP).	04/2003	
3577	INF	Introduction to the Remote Monitoring (RMON) Family of MIB Modul	08/2003	
2819	59	Remote Network Monitoring Management Information Base	05/2000	1757, 1271
2758	EXP	Definitions of Managed Objects for Service Level Agreements Performance Monitoring	02/2000	

Internet-Management: Dokumente (2)

RFC	STD	Titel	Datum	Ersetzte Dokumente
2981	PS	Event MIB	10/2000	
3014	PS	Notification Log MIB	11/2000	
3165	PS	Definitions of Managed Objects for the Delegation of Management Scripts	08/2001	2592
3231	PS	Definitions of Managed Objects for Scheduling Management Operations	01/2002	2591
1628	PS	UPS Management Information Base	05/1994	
1493	DS	Definitions of Managed Objects for Bridges	07/1993	1286
1525	PS	Definitions of Managed Objects for Source Routing Bridges	09/1993	1286
2788	PS	Network Services Monitoring MIB	03/2000	2248, 1565
2790	DS	Host Resources MIB	03/2000	1514
2287	PS	Definitions of System-Level Managed Objects for Applications	02/1998	
2564	PS	Application Management MIB	05/1999	
1697	PS	Relational Database Management System (RDBMS) Management Information Base (MIB) using SMv2	08/1994	
2594	PS	Definitions of Managed Objects for WWW Services	05/1999	
2789	PS	Mail Monitoring MIB	03/2000	2249, 1566
2605	PS	Directory Server Monitoring MIB	06/1999	1567
3197	INF	Applicability Statement for DNS MIB Extensions	11/2001	
1611	-	DNS Server MIB Extensions (HISTORIC, see RFC 3197)	05/1994	
1612	-	DNS Resolver MIB Extensions (HISTORIC, see RFC 3197)	05/1994	
1759	PS	Printer MIB	03/1995	
2707	INF	Job Monitoring MIB - V1.0	09/1999	