Netzwerkmanagement mit SNMP
→ Teil 1

Prof. Dr. Norbert Pohlmann
Fachbereich Informatik
Verteilte Systeme und Informationssicherheit

Fachhochschule Gelsenkirchen

Inhalt

- Ziele von SNMP
- Die Entwicklung von SNMP
- Die Architektur von SNMP
- Das Internet-Netzmanagement Rahmenwerk
- Structure of Management Informationen (SMI)
- Management Informationen Base II (MIB-II)

Inhalt

- **Ziele von SNMP**
- Die Entwicklung von SNMP
- Die Architektur von SNMP
- Das Internet-Netzmanagement Rahmenwerk
- Structure of Management Informationen (SMI)
- Management Informationen Base II (MIB-II)

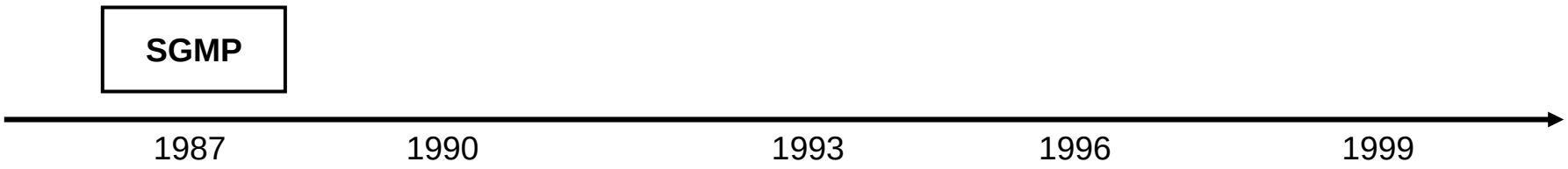
Ziele von SNMP
→ Simple Network Management Protocol

- Die Architektur des Simple Network Management Protocol basiert auf folgenden Zielen:
  - Die Management-Agent Software sollte so **einfach** wie möglich gehalten werden.
  - **Remote Management** Funktionen sollten unterstützt werden, um die Vorteile und Möglichkeiten des Internet nutzen zu können.
  - Die Architektur sollte so entwickelt werden, dass **Erweiterungen** in der Zukunft einfach durchzuführen sind.
  - Die SNMP-Architektur sollte **unabhängig** von speziellen Rechnern und Gateways sein.
- Die Idee hinter diesem Konzept ist, durch die **Begrenzung von Funktionalität** in SNMP letztlich die **Komplexität der Software zu begrenzen**.
- Dies ist wiederum Voraussetzung dafür, dass zum einen die Erweiterbarkeit und Ausbaufähigkeit der Software gegeben ist und zum anderen, dass die meisten Herstellern in der Lage und willens sind, SNMP zu unterstützen und für ihre Produkte Agenten zur Verfügung zu stellen.

Inhalt

- Ziele von SNMP
- **Die Entwicklung von SNMP**
- Die Architektur von SNMP
- Das Internet-Netzmanagement Rahmenwerk
- Structure of Management Informationen (SMI)
- Management Informationen Base II (MIB-II)

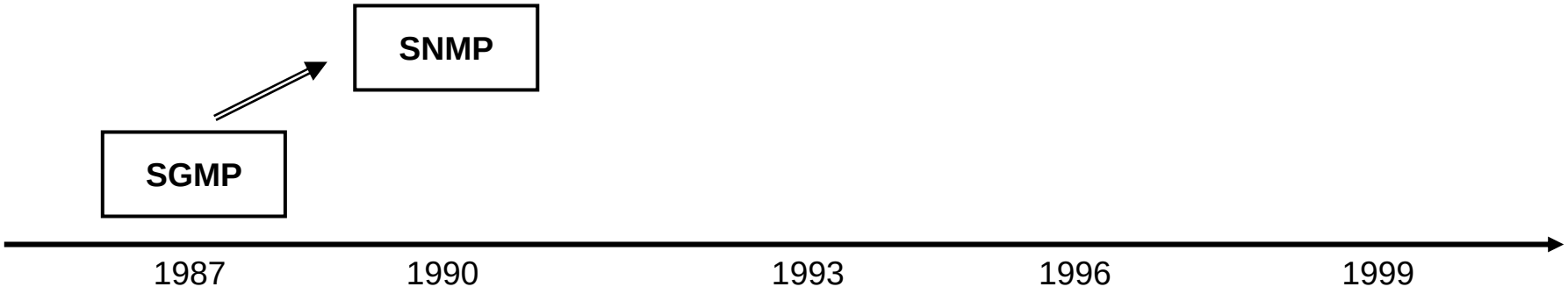
Die Entwicklung von SNMP (1/8)



Die Entwicklung des Netzwerkmanagements begann mit dem **Simple Gateway Monitoring Protocol (SGMP)**, das im Jahre 1987 aus der Taufe gehoben wurde.

Wie der Protokollname bereits ausdückt, beschränkt man sich zunächst auf das Management von Gateways.

Die Entwicklung von SNMP (2/8)

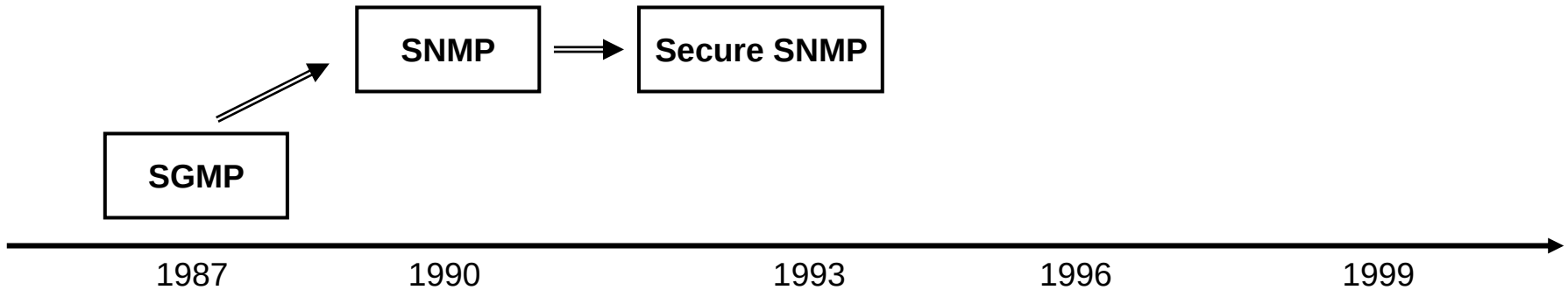


Aus diesem Protokoll entwickelt sich kurze Zeit später das **Simple Network Management Protocol (SNMP)** zur Verwaltung beliebiger Netzwerke.

Und im Mai 1990 wurde SNMP zum Internet Standard erhoben.

Aufgrund der einfachen Realisierung des Protokolls sowie der geringen Anforderung an die Hardware, fand SNMP rasch eine weite Verbreitung.

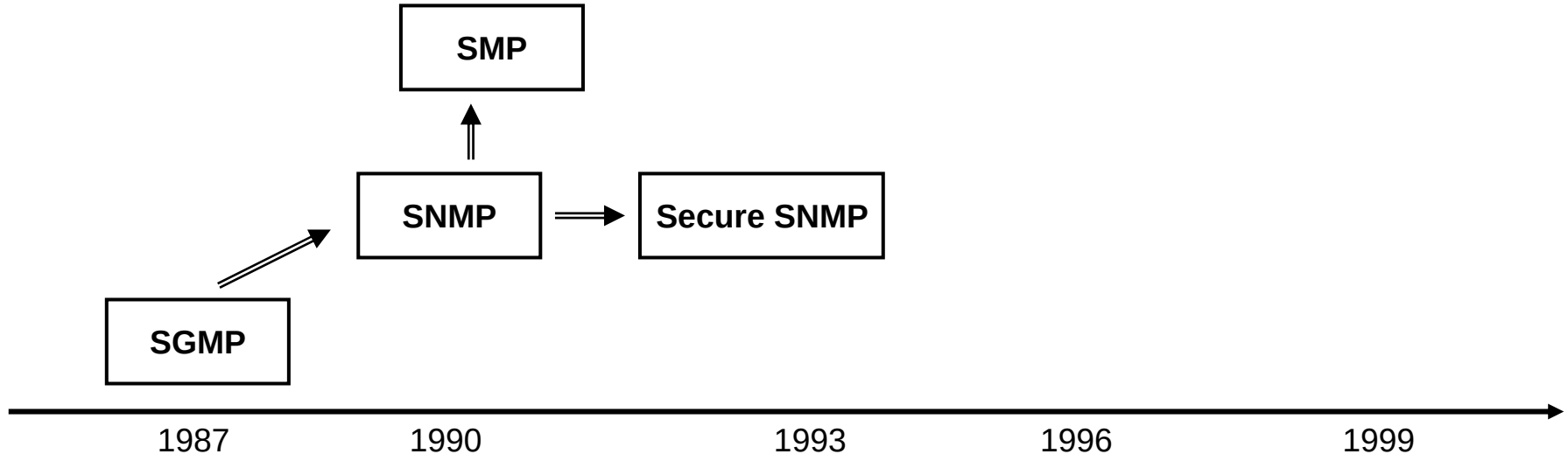
Die Entwicklung von SNMP (3/8)



Durch den umfangreichen praktischen Einsatz kristallisierten sich sehr bald auch die Schwächen von SNMP heraus, insbesondere was das Thema Sicherheit betraf.

Um das Sicherheitsproblem in den Griff zu bekommen, wurde im Juli 1992 eine Reihe von RFCs (allgemein unter dem Namen **Secure SNMP** bekannt) als *Proposed Standard* veröffentlicht.

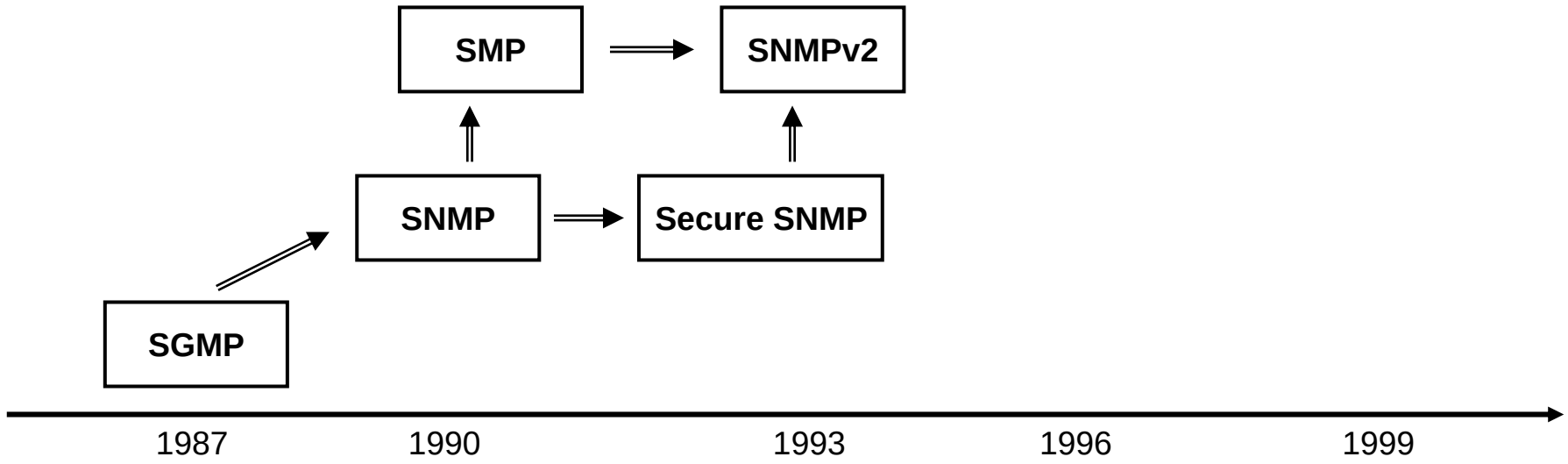
Die Entwicklung von SNMP (4/8)



Im selben Zeitraum wie Secure SNMP wurde eine Erweiterung von SNMP vorgeschlagen, die die funktionalen Schwachen von SNMP lösen sollte.

Diese erhielt die Bezeichnung **Simple Management Protocol (SMP)**.

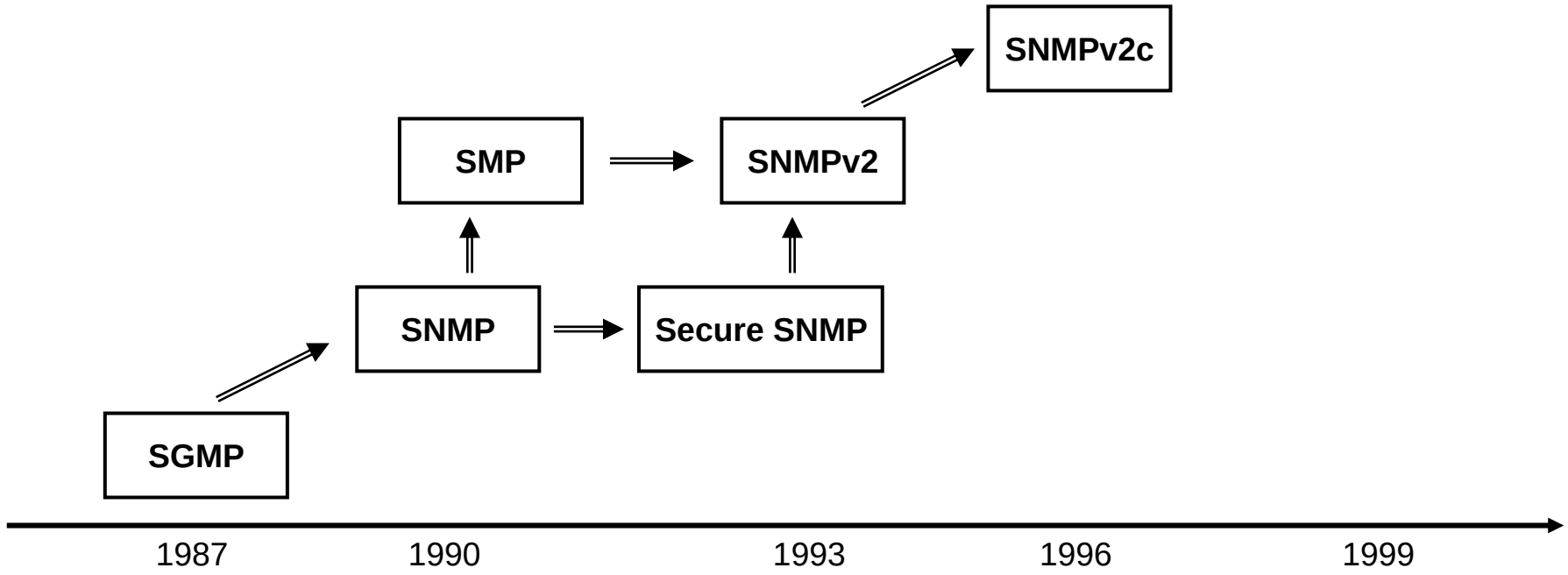
Die Entwicklung von SNMP (5/8)



Aus beiden Arbeiten von Secure SNMP und SMP entstand die offizielle Nachfolgeversion von SNMP: **SNMPv2**.

Im März 1993 wurde SNMPv2 zum *Proposed Internet Standard* erhoben.

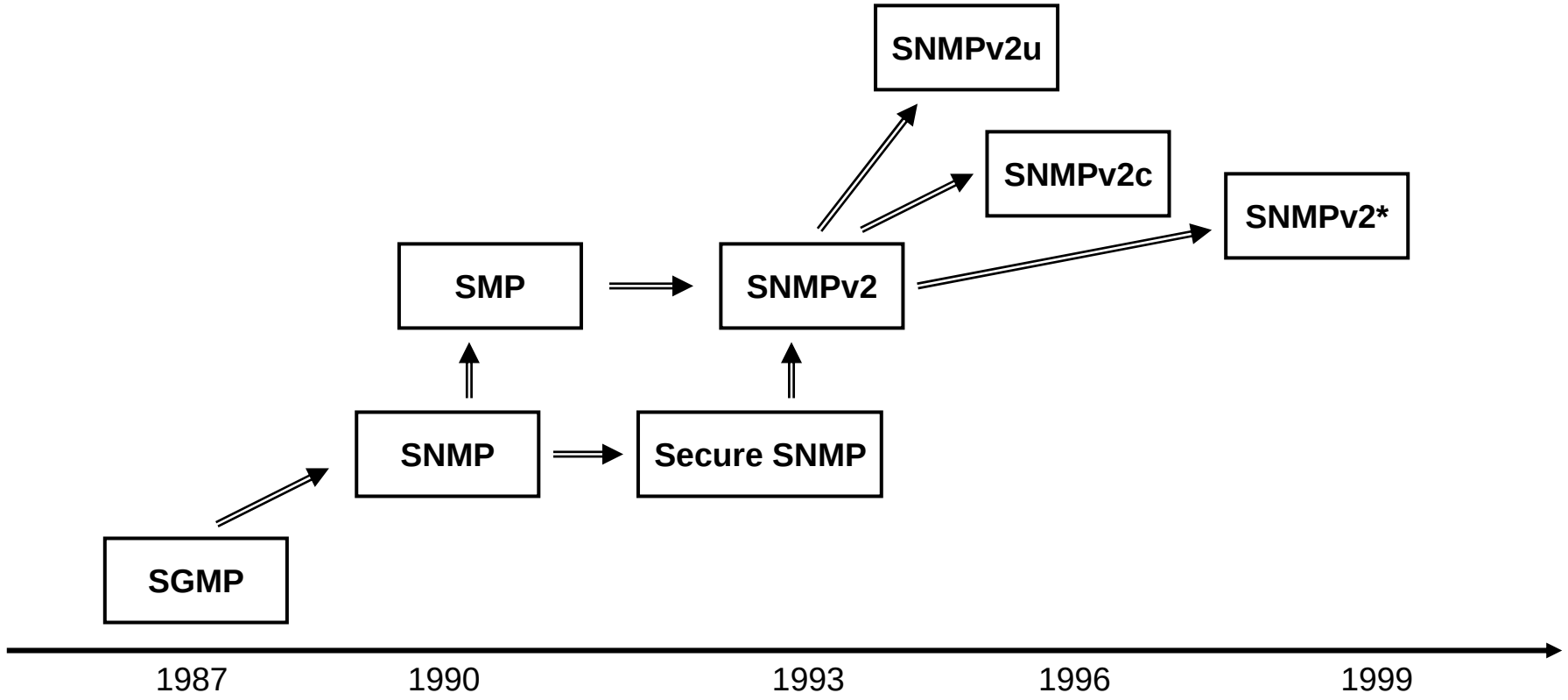
Die Entwicklung von SNMP (6/8)



Das Sicherheitskonzept in SNMPv2 wurde jedoch allgemein als zu komplex empfunden, so dass 1996 überarbeitete RFCs zu SNMPv2 veröffentlicht wurden.

Diese zweite Version von SNMPv2 wurde als **SNMPv2c** bezeichnet und verwendete das bei weitem nicht ausreichende Sicherheitskonzept von SNMPv1.

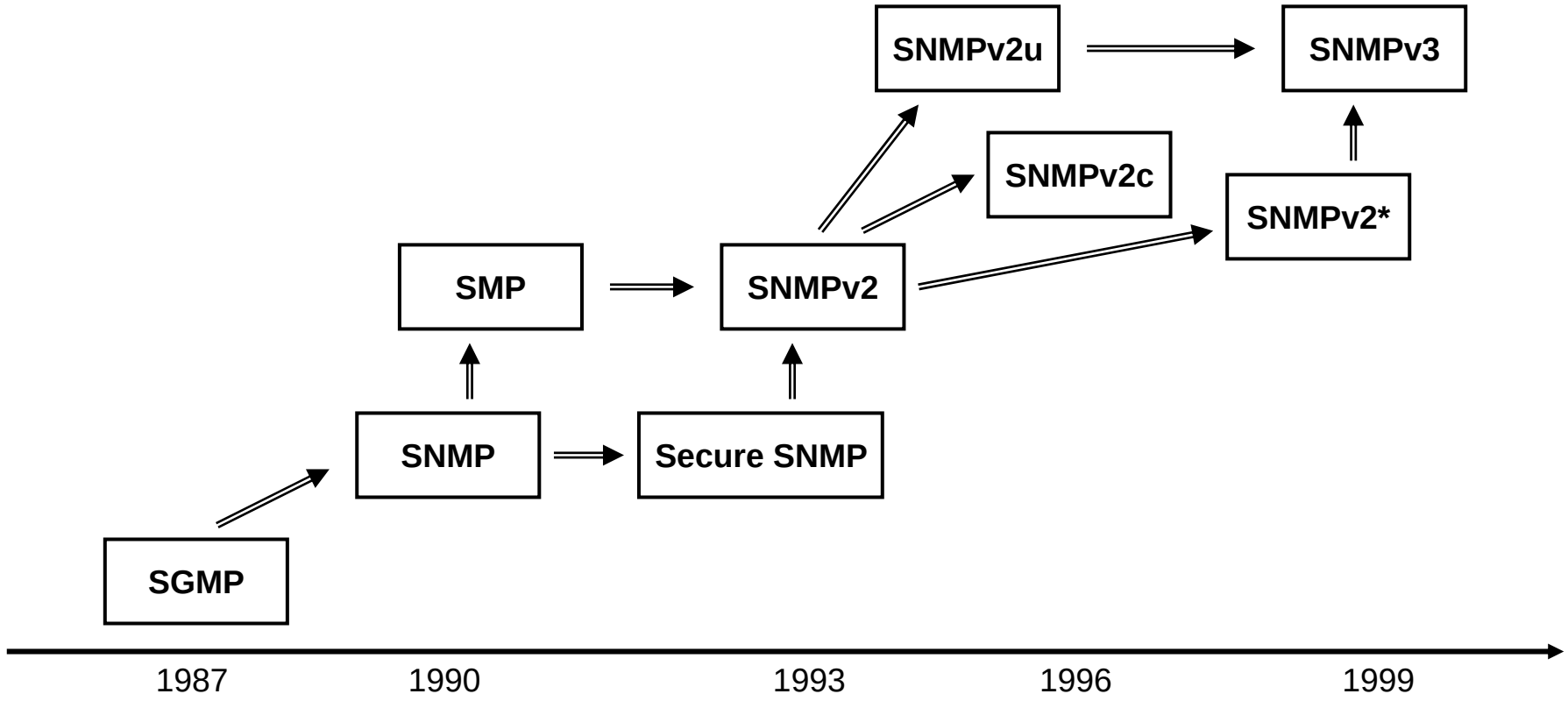
Die Entwicklung von SNMP (7/8)



Um die Sicherheitslücken von SNMPv2 zu schließen, begannen mehrere unabhängige Gruppen damit, an einem neuen Sicherheitskonzept zu arbeiten.

Daraus kristallisierten sich zwei Ansätze: **SNMPv2u und SNMPv2***.

Die Entwicklung von SNMP (8/8)



Damit gab es keinen einheitlichen Standard mehr, so dass im Jahre 1997 eine neue Arbeitsgruppe ins Leben gerufen wurde, die sich mit der Entwicklung von **SNMPv3** befassen sollte.

Die Arbeiten für SNMPv3 wurden im Januar 1998 als *Proposed Internet Standard* veröffentlicht und im März 1999 zum *Draft Internet Standard* erhoben.

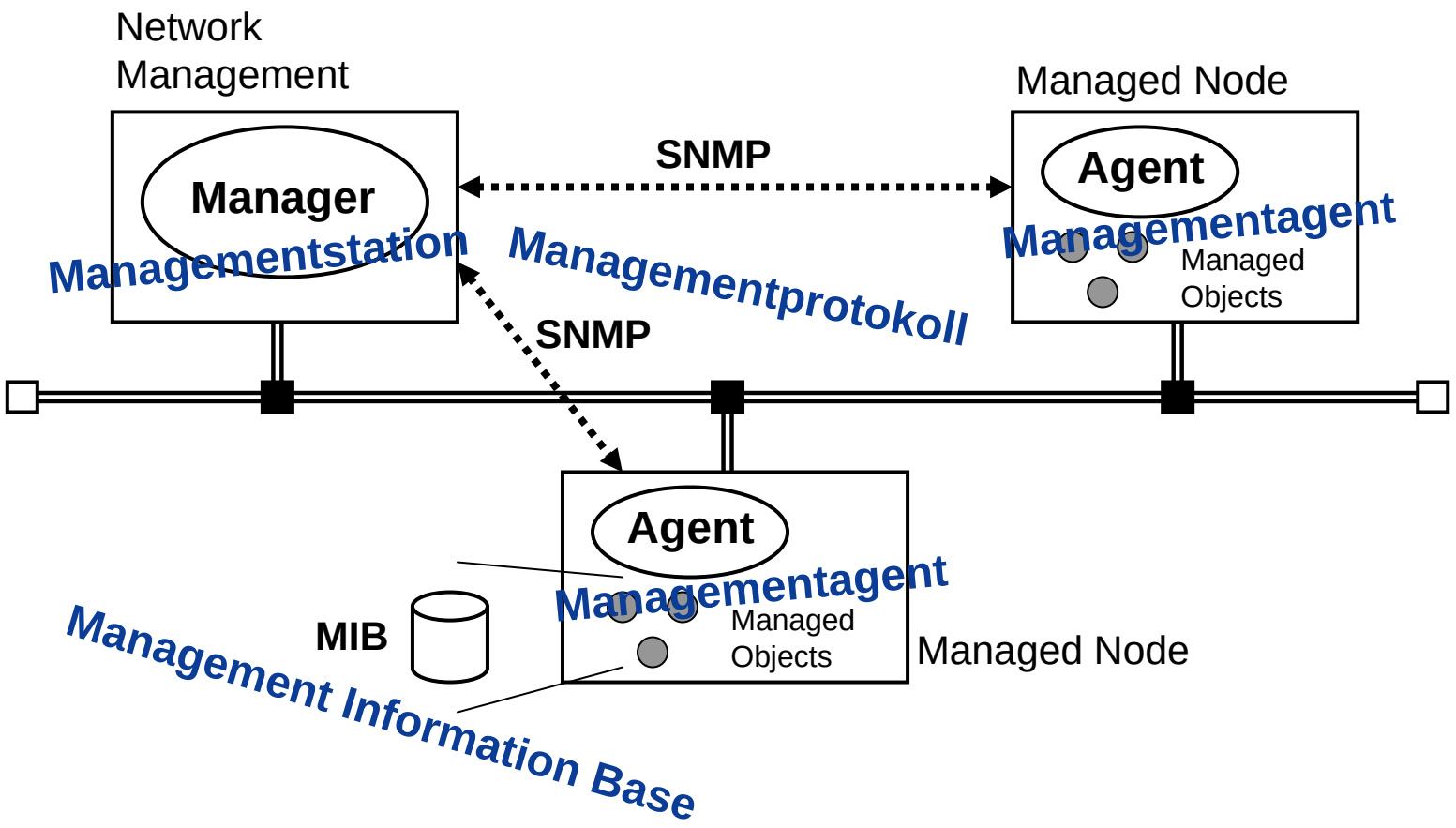
Inhalt

- Ziele von SNMP
- Die Entwicklung von SNMP
- **Die Architektur von SNMP**
- Das Internet-Netzmanagement Rahmenwerk
- Structure of Management Informationen (SMI)
- Management Informationen Base II (MIB-II)

Die Architektur von SNMP

- Die Architektur von SNMP basiert auf dem **Manager-Agent-Modell**, das auch als Grundlage für das OSI Netzwerkmanagement verwendet wurde.
- Dieses Modell definiert vier **Schlüsselelemente** für das Management von Netzen:
  - Managementstation
  - Managementagent
  - Management Informationen Base (MIB)
  - Managementprotokoll

Die Architektur von SNMP
→ Das Management-Agent Modell

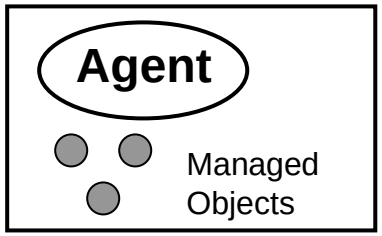


Die Architektur von SNMP
→ Managementstation

- Die Managementstation ist in der Regel ein einzelner Rechner, auf dem die Managementapplikation läuft.
- Die Managementapplikation stellt die Schnittstelle zwischen Netzadminstrator und dem Netzmanagementsystem dar.
- Im einfachsten Fall dient die Managementapplikation zur Aufbereitung und Darstellung der von dem Agent bereitgestellten Informationen.
- Allerdings können im Manager auch komplexe Managementanwendungen realisiert werden, durch die die Abläufe des Managements automatisiert und der Zustand des Netzes automatisch überwacht werden können.

Die Architektur von SNMP
→ Managementagent

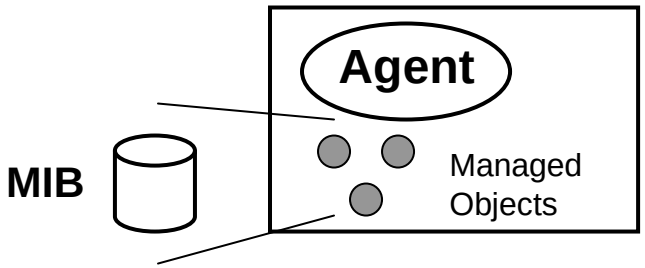
- Auf jedem zu verwaltenden Knoten (*Managed Node*) muss ein Managementagent installiert sein, der Managementinformationen über diesen Knoten für die Managementstation bereit hält und Anfragen von der Managementstation entsprechend bearbeitet.



- Ein Agent kann in Ausnahmefällen auch von sich aus Informationen an den Manager senden.
- Ein verwalteter Knoten kann z.B. ein Rechner, ein Gatewaysystem oder ein Netzelement (Hub, Switch, Router, ...) sein.
- Die zu verwaltenden Ressourcen oder Managementinformationen werden im Netzwerkmanagement als Objekt (**Managed Object**) dargestellt.
- Der Begriff **Objekt** wurde gewählte, da diese Informationen zu den Eigenschaften einer „normalen“ Variablen (wie Name, Typ und Wert) noch weitere Attribute besitzen.
- Man spricht deshalb auch nicht von Variablen sondern von **Instanzen**.

Die Architektur von SNMP
→ Management Information Base

- Die Ansammlung von *Managed Objects*, die von einem Agenten verwaltet wird, wird unter dem Begriff **Management Information Base (MIB)** zusammengefasst.
- Eine MIB enthält jedoch nicht die eigentlichen Managementinformationen, sondern beschreibt in einer **formalen Art und Weise**, welche Informationen der Agent bereitstellt und wie die Managementapplikation darauf zugreift.



Die Architektur von SNMP
→ Managementprotokoll

- Managementapplikation und Managementagent sind über ein Netzmanagementprotokoll verbunden.
- Das Protokoll für TCP/IP basierende Rechnernetze ist das **Simple Network Management Protocol (SNMP).**
- Die Architektur des SNMP Protokolls zielt darauf ab, die Anforderungen an die Netzknoten so gering wie möglich zu halten, um Managementfunktionalitäten auf vielen Netzknoten implementieren zu können.
- Die Philosophie lautet deshalb: Der Einfluß auf verwaltete Knoten durch das Hinzufügen von Netzverwaltung muss möglichst klein sein, also den kleinsten gemeinsamen Nenner darstellen.
- Als Folge dieser Maxime verlagert sich die Last auf die **Netzwerkmanagementstation**, die den **größten Teil der Funktionalität** bereitstellen muss.

Inhalt

- Ziele von SNMP
- Die Entwicklung von SNMP
- Die Architektur von SNMP
- **Das Internet-Netzmanagement Rahmenwerk**
- Structure of Management Informationen (SMI)
- Management Informationen Base II (MIB-II)

Das Internet-Netzmanagement Rahmenwerk

- Der Begriff **Simple Network Management Protocol** bezieht sich eigentlich auf eine Sammlung von Spezifikationen, die in RFCs abgelegt sind und verschiedene Teilaspekte des Netzwerkmanagement abdecken (unter anderen das SNMP-Protokoll).
- Diese Sammlung von Spezifikationen wird auch als das Internet-Netzmanagement Rahmenwerk bezeichnet und wächst weiterhin.
- Die drei wichtigsten Kerndokumente sind:
  - RFC1155 / RFC1212 — Structure of Management Informationen
  - RFC1213 — Management Informationen Base II (MIB-II)
  - RFC1157 — Simple Network Management Protocol (SNMP)

Inhalt

- Ziele von SNMP
- Die Entwicklung von SNMP
- Die Architektur von SNMP
- Das Internet-Netzmanagement Rahmenwerk
- **Structure of Management Informationen (SMI)**
- Management Informationen Base II (MIB-II)

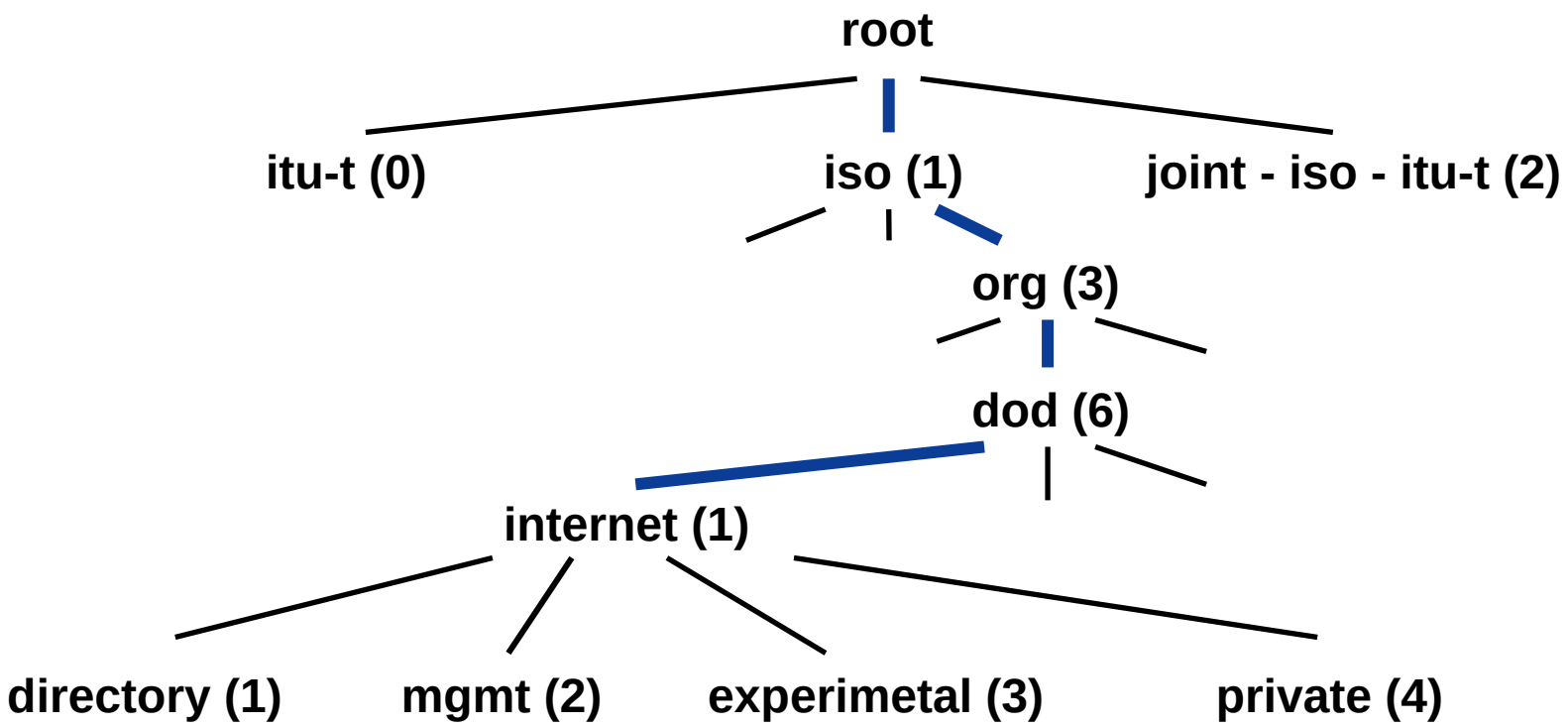
Structure of Management Information (SMI)

- Die Structure of Management Information (RFC1155 - SMI) definiert ein **allgemeines Rahmenwerk** mit Hilfe dessen *Managed Objects* innerhalb einer *Management Information Base* **formal** beschrieben werden können.

Struktur und Aufbau einer MIB

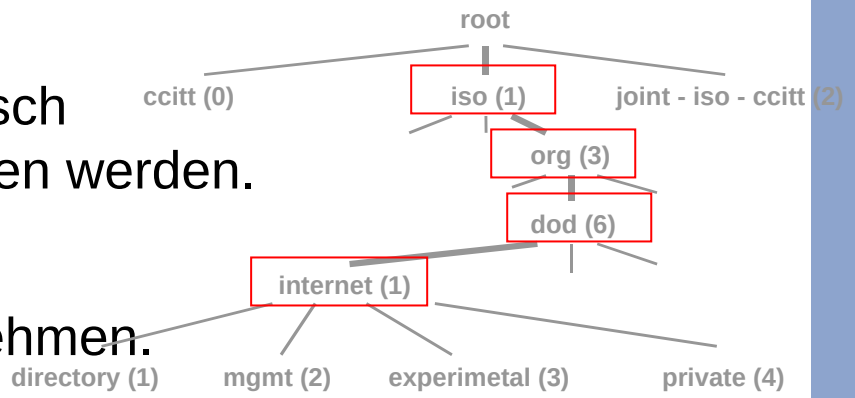
- Die Managementinformationen, die zwischen Management und Agenten ausgetauscht werden, müssen zunächst in einer ***Management Information Base (MIB)*** formal beschrieben werden.
- Eine MIB ist dabei als hierarchische Baumstruktur aufgebaut, wobei die *Managed Objects* (d.h. die zu verwaltenden Managementinformationen) als Blätter dieser Baumstruktur definiert werden.
- Jede MIB ist ihrerseits ein Unterbaum einer noch größeren, ebenfalls hierarchisch aufgebauten Struktur, die in der OSI-Welt als **Management Information Tree** und in der Internetwelt als **Domain Name System** bezeichnet wird.
- Diese Struktur bildet einen Namensbaum, in dem Objekte eindeutig mit Hilfe eines **Object Identifiers** angesprochen werden können.

Management Information Tree



Struktur und Aufbau einer MIB

- Direkt unterhalb der Wurzel des „Management Information Tree“ befinden sich drei Zweige: itu-t(0), iso(1) und joint-iso-ccitt(2).
- Diese Teilbäume gliedern sich in weitere Unterbäume auf, so dass eine baumartige Struktur entsteht.
- In diesem Baumkonzept können theoretisch beliebig viele Hierachieebenen vorgesehen werden.
- Damit ist diese Struktur geeignet, ein ganzes Universum von Objekten aufzunehmen.

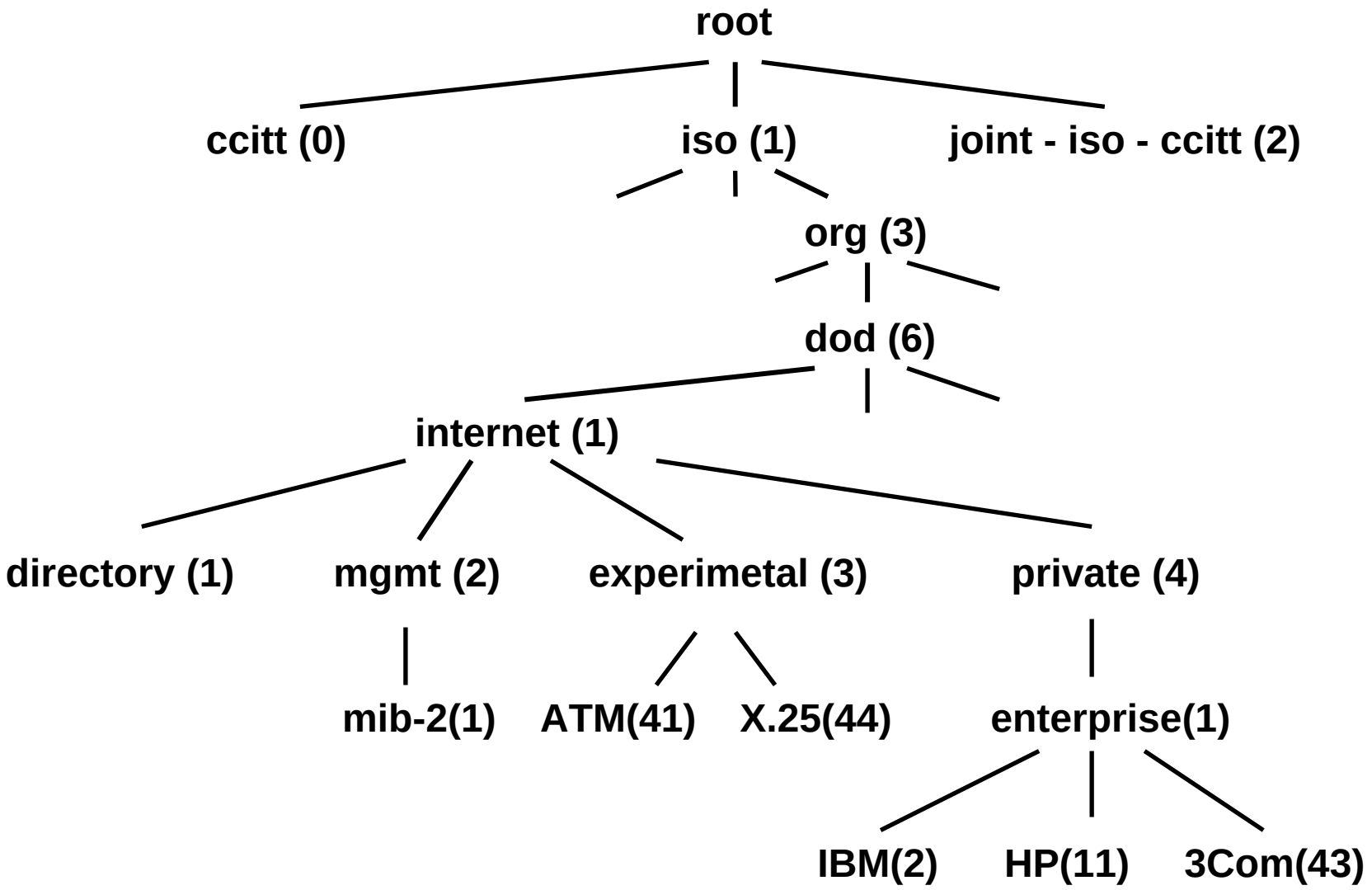


- Jedes Element einer Hierarchieebene wird durch eine eindeutige Zahl, sowie durch ein Kürzel beschrieben.
- Der eindeutige Bezeichner eines Objektes, der durch Aneinanderreihen dieser Zahl oder Kürzel entsteht, wird als **Object Identifier (OID)** bezeichet.
- Beispiele: 1.3.6.1 - iso.org.dod.internet - iso(1).org(3).dod(6).internet(1)

Struktur und Aufbau einer MIB

- Die SMI definiert vier weitere Knoten unter dem „internet“ Teilbaum.
  - Der „directory“ Unterbaum ist reserviert für zukünftige Erweiterungen und spielt für das Netzwerkmanagement zunächst keine Rolle.
  - Der „mgmt“ Unterbaum ist der Teilbaum, der sämtliche vom IAB standardisierte MIBs unter sich hat.
    Der „mgmt“ Teilbaum besitzt nur einen weiteren Unterbaum „mib-2“, der die *SNMP Standard Management Information Base MIB-II* enthält.
  - Unterhalb des „experimental“ Teilbaum befinden sich neu entwickelte MIBs, die vor ihrer Aufnahme in die Standard-MIB zunächst im „experimental“ - Zweig eingeführt und ausgiebig getestet werden.
  - Der „private“-Unterbaum enthält bis jetzt nur eine weitere Verzweigung, den „enterprises“-Unterbaum.
    - Dieser Teilbaum stellt für Unternehmen ein Möglichkeit dar, herstellerspezifische MIBs für ihre jeweiligen Produktfamilien zu entwickeln.
    - Alle namhaften Unternehmen, die im Netzbereich tätig sind, besitzen einen Unterbaum im „enterprises“ Zweig.

Management Information Tree



Definition von Objekten

- Für Beschreibungen der Objekte kommt die OSI Beschreibungssprache „Abstract Syntax Notation One“ (ASN.1) zum Einsatz.
- Jedes verwaltete Objekt wird mit Hilfe des OBJECT-TYPE Makros beschrieben, das im RFC1155-SMI definiert wurde.
- Dieses Makro wurde aktualisiert und im RFC-1212 erweitert
- OBJECT-TYPE MACRO::=

```
BEGIN
        TYPE NOTATION::=
                „SYNTAX“          type (ObjectSyntax)
                „ACCESS“          Access
                „STATUS“          Status
                „DESCRIPTION“     Text   |   empty
                „REFERENCE“       Text   |   empty
                „DEFVAL“          “{“  value “}“   |   empty
                „INDEX“           “{“  IndexTypes “}“   |   empty
                VALUE NOTATION  ::=  value (VALUE ObjectName)
END
```

Die Bestandteile des OBJECT-TYPE Makros (1/3)

- **SYNTAX**
  Die Syntax eines verwalteten Objekts entspricht dem ASN.1 Datentyp des Objektes.
  Der Ausdruck *ObjectSyntax* steht für einen *CHOICE* Datentyp, der alle im Internet-Netzmanagement definierten Datentypen enthält.

- **ACCESS**
  Definiert den erlaubten Zugriff auf ein verwaltetes Objekt.
  - read-only: Instanzen des Objektes können nur gelesen werden.
  - read-write: Instanzen des Objektes können sowohl gelesen als auch gesetzt werden.
  - write-only: Instanzen des Objektes können gesetzt, aber nicht gelesen werden.
  - not-accessible: Auf Instanzen des Objektes kann nicht zugegriffen werden.

Die Bestandteile des OBJECT-TYPE Makros (2/3)

- **STATUS**
  Das Status-Feld definiert eine der folgenden Anforderungen an die Implementierung von verwalteten Objekten:
  - mandatory: Der verwaltete Knoten muss dieses Objekt implementieren.
  - optional: Der verwaltete Knoten kann dieses Objekt implementieren.
  - obsolete: Der verwaltete Knoten sollte dieses Objekt nicht mehr implementieren.
  - deprecated: Das *Managed Object* ist überflüssig, kann aber aus Kompatibilitätsgründen implementiert werden.
- **DESCRPART**
  Hier kann optional eine textuelle Beschreibung des *Managed Object* angegeben werden.

Die Bestandteile des OBJECT-TYPE Makros (3/3)

- **REFERPART**
  Dieses Feld kann eine textuelle Referenz zu einem *Managed Object* in einer anderen MIB beinhalten.

- **DEFVALPART**
  In diesem Feld kann optional ein Defaultwert für das *Managed Object* festgelegt werden.

- **INDEXPART**
  Das Index-Feld bestimmt, welche Objekte innerhalb einer Tabelle als Schlüssel verwendet werden.
  Diese Index-Objekte müssen eine Tabellenzeile eindeutig identifizieren, wobei nur einfach Datentypen zugelassen sind.

- **Name(Wert)**
  Als Name wird der **OBJECT IDENTIFIER** angegeben.
  Durch diesen wird das *Managed Object* innerhalb des *Management Information Trees* eindeutig bestimmt.

Definition des Objektes sysDescr
→ Beispiel

- **sysDesc OBJECT-TYPE**
  SYNTAX OCTET STRING
  ACCESS read-only
  STATUS mandatory
  DESCRIPTION „A textual description of ...“
  ::= { system 1 }

- Da die Einträge von INDEX, REFERENCE und DEFVAL leer sind, werden sie für das sysDescr Objekt nicht aufgeführt.

- Der Ausdruck system ist eine Konstante von Typ OBJECT IDENTIFIER und besitzt den Wert.
  iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).system(1)

Definition von Tabellen (1/3)

- Die SMI erlaubt zusätzlich zu den einfachen Datentypen auch die Verwendung von zweidimensionalen Tabellen, die ihrerseits wieder nur einfache Datentypen enthalten dürfen.
- Für die Definition von Tabellen werden die ASN.1 Typen SEQUENCE und SEQUENCE OF verwendet.
- Bei der Definition von Tabellen legt die SMI folgende Konventionen fest:
- Für jede Tabelle wird ein Tabellenobjekt mit Hilfe des **OBJECT-TYPE** Makros definiert:

```
tabellenObjekt    OBJECT-TYPE
SYNTAX            SEQUENCE OF zeilenObjekt
ACCESS            not-accessible
...
::=    { any-mib 1 }
```

Definition von Tabellen (2/3)

- Das Zeilenobjekt wird unterhalb des Tabellenobjektes definiert als:

```
zeilenObjekt    OBJECT-TYPE
SYNTAX          ZeilenObjekt
ACCESS          not-accessible
INDEX           spaltenObjekt1..
::=   { tabellenObjekt 1 }
```

- Der Datentyp „ZeilenObjekt“ wird dabei definiert als:

```
ZeilenObjekt    ::=    SEQUENCE    {
                           <Typ von Spaltenobjekt1>
                           <Typ von SpaltenobjektN>
                               }
```

- Es ist zu beachten, dass ZeilenObjekt einen Datentyp darstellt (deshalb die Großschreibung) und zeilenObjekt ein *Managed Object*.
- Die Verwendung desselben Bezeichners für die Zeilenobjekte und dessen Syntax ist hierbei nicht zwingend vorgeschrieben, aber gängige Praxis.

Definition von Tabellen (3/3)

- Anschließend werden alle Spaltenobjekte der Tabelle nacheinander mit Hilfe des OBJECT-TYPE Makros definiert.

```
spaltenObjekt1    OBJECT-TYPE
SYNTAX            <Typ von Spaltenobjekt 1>
ACCESS            not-accessible
. . .
::=    { zeilenObjekt 1 }
```

- Sowohl das Tabellen- wie auch das Zeilenobjekt sind als not-accessible gekennzeichnet, so dass auf diese Objekte nicht direkt zugegriffen werden darf.
- Bei der Definition eines Zeilenobjektes wird über das INDEX Feld definiert, welche(s) Spaltenobjekt(e) eine Tabellenzeile eindeutig identifiziert.

Datentypen für das Netzwerkmanagement (1/3)

- Jedem Objekt innerhalb einer MIB ist ein Datentyp zugeordnet.
- Um das Netzmanagement einfach zu halten, erlaubt die SMI nur die Verwendung eines Subset von ASN.1 Datentypen:
- Dies sind:

  INTEGER, OCTET STRING, OBJECT IDENTIFIER, SEQUENCE, SEQUENCE OF
- Basierend auf diesen Datentypen werden in der SMI sechs neue Typen für das Netzmanagement definiert.
- **IpAddress**
  Ein Datentyp, der eine IP-Adresse darstellt. Der Typ IPAddress ist als Untertyp definiert.

```
IpAddress          ::=          - - in network byte order
                  [ APPLICATION 0 ]
                              IMPLICIT OCTET STRING ( SIZE (4))
```

Datentypen für das Netzwerkmanagement (2/3)

- **NetworkAddress**
  Ein Datentyp, der die Netzwerkadresse darstellt. Diese kann von möglicherweise mehreren Protokollfamilien stammen. In SNMPv1 ist nur die Internetadresse als mögliche Netzadresse eingetragen.

```
NetworkAddress  ::=
        CHOICE          {
                integer             IpAddress   }
```

- **Counter**
  Ein Datentyp, der eine nicht negative Zahl darstellt, die monoton wächst, bis sie ihren höchsten Wert erreicht und dann wieder auf Null springt.

```
Counter  ::=
        [ APPLICATION 1 ]
                IMPLICIT INTEGER (0 ... 4294967295)
```

- **Gauge**
  Ein Datentyp, der eine nicht negative Zahl darstellt, die sowohl größer als auch kleiner werden kann, die aber bei einem bestimmten größten Wert festgehalten wird.

```
Gauge  ::=
        [ APPLICATION 2 ]
                IMPLICIT INTEGER (0 ... 4294967295)
```

Datentypen für das Netzwerkmanagement (3/3)

- **TimeTick**
  Ein Datentyp, der eine nicht negative Zahl darstellt, der die Zeit in 1/100 Sekunde seit einem früheren Ereignis zählt, allerdings auf die maximale Größe von 2^{32} beschränkt ist.

```
TimeTick  ::=
        [ APPLICATION 3 ]
                IMPLICIT INTEGER (0 ... 4294967295)
```

- **Opaque**
  Ein Datentyp, der eine beliebige Verpackung darstellt.

```
Opaque  ::=
        [ APPLICATION 4 ]
                IMPLICIT OCTET STRING
```

Inhalt

- Ziele von SNMP
- Die Entwicklung von SNMP
- Die Architektur von SNMP
- Das Internet-Netzmanagement Rahmenwerk
- Structure of Management Informationen (SMI)
- **Management Informationen Base II (MIB-II)**

Management Information Base (MIB)
→ Einführung (1/2)

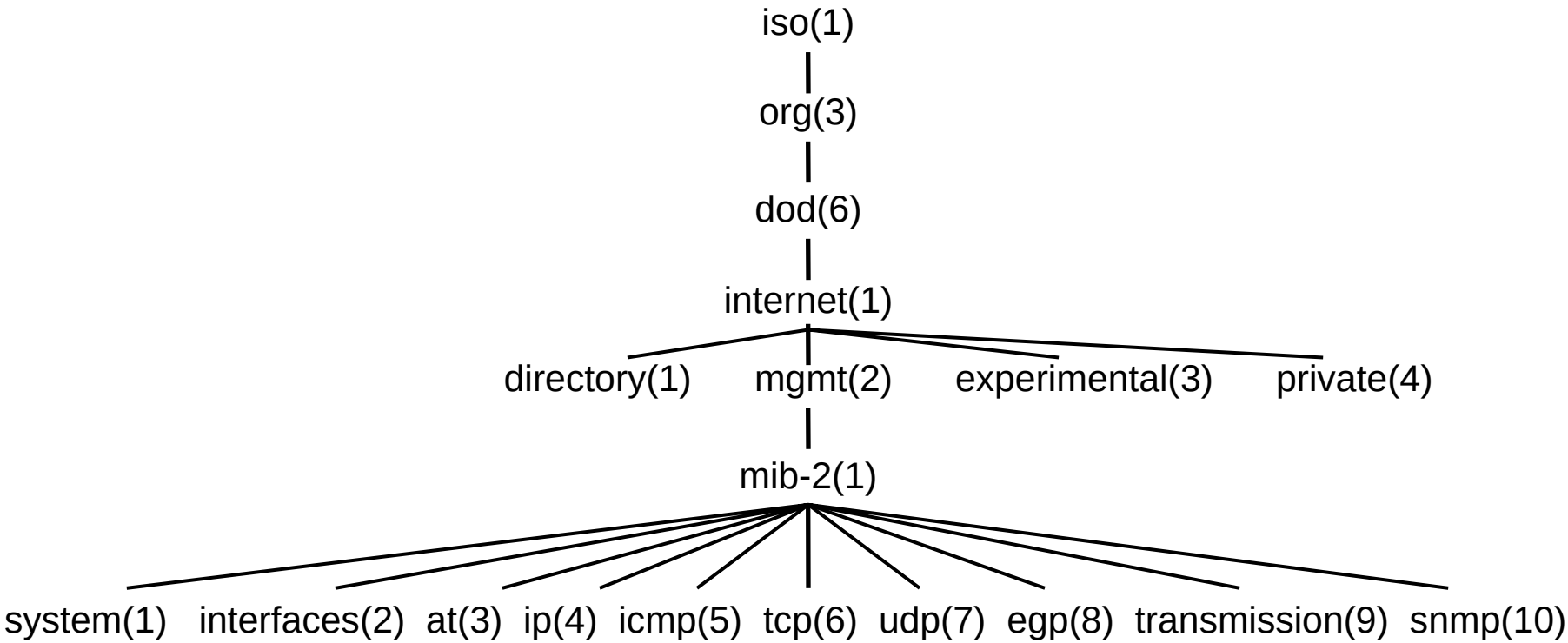
- Um die Anforderungen an die verwalteten Knoten so gering wie möglich zu halten, beschränkt sich das Internet-Netzmanagement auf die Abfrage allgemeiner, standardisierter Variablen, den **Managed Objects**.
- Diese Managementobjekte werden **formal** in einer **Management Informationen Base (MIB)** mit Hilfe des OBJECT-TYPE Makros beschrieben.
- Eine MIB stellt somit eine Zusammenfassung sämtlicher Managementinformationen dar, die zwischen Manager und Agent ausgetauscht werden können.
- Anhand der MIB besitzt der Manager sämtliche Informationen, die er für das Management eines Netzknoten benötigt.
- Ein Manager kennt je nach den zu verwaltenden Netzknoten eine Vielzahl von unterschiedlichen MIBs.

Management Information Base
→ Einführung (2/2)

- Auf der andere Seite kann eine Agent auch mehrere MIBs implementieren.
- In der Regel wird die *Standard Internet MIB (MIB-II)* oder Teile daraus implementieren und zusätzliche herstellerspezifische Informationen in einer *privaten MIB* zur Verfügung stellen.
- Häufig wird die **MIB** auch als **verteilte, virtuelle Datenbank** bezeichnet.
- Die Betonung liegt hierbei auf **virtuell**, da eine MIB selbst keine Managementinformationen enthält, sondern nur im Sinne von Syntax, Status und Zugriffsmodus beschreibt.
- Es ist allein die Aufgabe der Agenten, die eigentlichen Managementinformationen zu ermitteln.

Die Standard Management Information Base → (MIB-II)

Standard Internet MIBs werden unter dem „mgmt“-Unterbaum definiert. Unter diesem ist bei SNMPv1 nur ein weiterer Unterbaum, der „mib-2(1)“-Unterbaum definiert.



Die Standard Management Information Base → (MIB-II)

- In der Standard *Management Information Base* wurden **grundlegende Objekte** für das Management TCP/IP basierender Rechnernetze definiert.
- Wenn ein Hersteller von seinem Produkt behauptet, dass es MIB-II fähig ist, dann muss dieses Gerät sämtliche Standard-MIB definierten Objekte kennen und bei Anfragen einer Managementstation entsprechende Informationen liefern können.
- Ausnahmen gibt es bei Netzknoten, die nicht alle Schichten des TCP/IP Protokollstacks implementieren.
- So ist zum Beispiel die Anfrage eines Repeaters nach Informationen über TCP oder UDP weniger sinnvoll.
- Wird ein Objekt nicht unterstützt, so darf die Abfrage jedoch nicht zu einem Fehler führen.

Gruppen der MIB-II

- Die Standard Management Information Base II besteht aus 10 Gruppen mit insgesamt 171 Objekten.
- Die Gruppen in der **MIB-II reflektieren im wesentlichen den TCP/IP Protokollstack**, indem für jede Protokollschicht Managementinformationen definiert wurden.

MIB-II
→ System Gruppe

- Die erste Gruppe mit dem Namen „system“ beinhaltet allgemeine Informationen zur Konfiguration, wie zum Beispiel eine Beschreibung des Gerätes, der Name und Aufstellungsort des Gerätes usw.
- Die Gruppe „system“ muss von **allen** verwalteten Knoten implementiert werden.

Aufbau:

sysDescr (1) :	textuelle Beschreibung des Knotens
sysObjectID (2) :	*Object Identifier*, der den Agent eindeutig identifiziert
sysUpTime (3) :	Zeit, die seit dem letzten Booten des Gerätes vergangen ist
sysContact (4) :	Name der Kontaktperson
sysName (5) :	Gerätenamen des Knotens
sysLocation (6) :	Standort des Knotens
sysServices (7) :	Protokollschicht, die der Knoten implementiert

Beispiel:

sysDescr	**Router 1 (Cisco)**
sysObjectID	**1.3.6.1.4.1.4.1.2.5**
sysContact	**Norbert Pohlmann**
sysLocation	**Raum 4.2.3.1 Gelsenkirchen**

MIB-II
→ Interfaces Gruppe

- Die Schnittstellengruppe enthält Grundinformationen über die Einheiten in der Schnittstellenschicht.
- Diese Gruppe enthält in der ersten Ebene zwei Objekte:
  - die Zahl der Schnittstellenanschlüsse des Knotens und
  - eine Tabelle mit Informationen über die Schnittstelle, wie z.B. die Anzahl der gesendeten und empfangenen Bytes.

MIB-II
→ AT Gruppe (address translation)

- Die Adressübersetzungsgruppe besteht aus einer Tabelle für die Abbildung von IP-Adressen auf Ethernet-Adressen.
- In der MIB-II wurde die Adressübersetzungsgruppe mit ***deprecate (***d.h. abgelehnt) markiert, da die Information über die Adressabbildung in die IP-Gruppe integriert wurden.

MIB-II
→ IP Gruppe

- Die IP Gruppe enthält Daten über das IP-Protokoll.
- Darin enthalten sind mehrere Zähler, z.B.
  - über die Anzahl der weitergeleiteten,
  - der verworfenen oder
  - der erfolgreich fragmentierten Datagramme.
- Außerdem enthält diese Gruppe noch drei Tabellen:
  - eine IP-Adresstabelle,
  - eine IP-Routingtabelle und
  - eine Adressübersetzungstabelle.
- Diese Gruppe muss von allen verwalteten Knoten implementiert werden.

MIB-II
→ ICMP Gruppe

- In der ICMP Gruppe sind für jeden Nachrichtentyp innerhalb des ICMP-Protokolls zwei Zähler definiert.
  - Der eine zählt, wie oft dieser Nachrichtentyp von der eigenen IP-Einheit erzeugt wurde;
  - der andere zählt, wie oft dieser Nachrichtentyp empfangen wurde.
- Diese Gruppe muss von allen Knoten implementiert werden.

MIB-II
→ TCP Gruppe

- Die TCP Gruppe enthält Informationen, die das Transportprotokoll betreffen.
- Dies sind vor allem Zähler, die z.B. die Anzahl der Verbindungen oder die Anzahl der gesendeten und empfangenen Segmente beinhalten.
- Die TCP Gruppe enthält aber auch eine Tabelle, in der alle derzeit bestehenden Verbindungen inklusive lokaler und entfernter IP-Adressen hinterlegt sind.
- Diese Gruppe muss von allen Knoten implementiert werden.

MIB-II
→ UDP Gruppe

- Die UDP Gruppe beinhaltet entsprechende Informationen für das verbindungslose Transportprotokoll UDP.
- Sie enthält mehrere Zähler und eine Tabelle, deren Einträge darüber Aufschluss geben, welche UDP-Ports derzeit in Verwendung sind.
- Diese Gruppe muss von allen Knoten implementiert werden.

MIB-II
→ EGP Gruppe

- Die EGP Gruppe ist neben der Übersetzungsgruppe die einzige Gruppe, die **nicht von allen** Knoten unterstützt werden muss.
- Diese Gruppe enthält spezifische Parameter über das *Exterior Gateway Protocol (EGP)* und muss somit nur auf Knoten implementiert werden, die dieses Protokoll unterstützen, also praktisch nur auf Gateways.

MIB-II
→ Transmission Gruppe

- Die Übersetzungsgruppe ist eigentlich überhaupt keine Gruppe, sondern ein Teilbaum, der media-abhängige MIBs enthalten soll.
- Zum Zeitpunkt der Definition der MIB-II war diese Gruppe leer.
- In der Zwischenzeit wurden für die MIBs für das Management von Ethernet-Netzen (RFC1643) und Token-Ring-Netzen (RFC1231) definiert.

MIB-II
→ SNMP Gruppe

- Als letzte Gruppe gibt es in der MIB-II noch die SNMP-Gruppe, die Informationen über das Simple Network Management Protocol beinhaltet.
- Dies sind beispielsweise Informationen über das Auftreten von Fehlern oder die Anzahl ausgelesener bzw. veränderter MIB-Objekte.
- Auch diese Gruppe muss von allen Knoten implementiert werden.

Erweiterung der MIB-II

- Neben den in RFC1213 beschriebenen Gruppen enthält der „mgmt“-Unterbaum mittlerweise eine ganze Reihe weiterer Gruppen, wie z.B. MIBs zum Management von Druckern oder Domain Name Services (DNS).
- Als eine weitere wichtige Gruppe ist die RMON-Gruppe (mib-2 16) zu nennen, die in RFC1757 *Remote Network Monitoring* spezifiziert wurde.
- Die herausragende Bedeutung der RMON-MIB besteht darin, dass sich das Netzmanagement nicht mehr nur auf die Verwaltung einzelner Knoten im Netz bezieht.
- Vielmehr ist es nun möglich, jedes beliebige Gerät, das einen RMON-Agent enthält, als Probe für einen Netzmonitor zu benutzen.
- Mit RMON können z.B. Daten über das derzeitige Verkehrsaufkommen an den einzelnen Interfaces oder die Anzahl der registrierten Kollisionen abgefragt werden.
- Damit ist es möglich, von der Netzwerkmanagementstation aus, Verkehrsdaten aus dem ganzen Netz zu sammeln.

Netzwerkmanagement mit SNMP
→ Teil 1

Vielen Dank für Ihre Aufmerksamkeit

Fragen ?

norbert.pohlmann@informatik.fh-gelsenkirchen.de

Fachhochschule Gelsenkirchen