SNMP-basiertes Netzwerkmanagement

Markus Speer

Zentrum für Informationsverarbeitung

Westfälische Wilhelms-Universität

Münster

E-Mail: speer@uni-muenster.de

Tel.: (0251) 83-31614, Fax: (0251) 83-31653

Veranstaltung vom 22.05.2003 der Vorlesung

Rechnernetze und Internet –

Fortgeschrittene Themen

SS 2003 - Veranstaltungsnummer: 260 158

http://www.uni-muenster.de/ZIV/Lehre/2003-2/RechnernetzeFortgeschritteneThemen/

Themenübersicht

- **Funktionen des Netzwerkmanagement**
- SNMP: Simple Network Management Protocol
- MIB: Management Information Base
- RMON
- SNMP-basierte Managementwerkzeuge
- Reporting

Funktionen des Netzwerkmanagements

- **Konfigurations-Management:** Konfiguration, Initialisierung, Beenden, Kontrolle, Namensvergabe
- **Fehler-Management:** Versenden von Fehlermeldungen, Überwachung von Fehlerzählern, Test, Diagnose, Fehlerkorrektur
- **Performance-Management:** Überwachung des Durchsatzes, Überwachung des Antwortzeitverhaltens, Analyse der Auslastung
- **Sicherheits-Management:** Zugriffschutz, Zugangskontrolle, Überwachung von Zugriffen auf Netzkomponenten, Datenschutz
- **Abrechnungs-Management:** Benutzerverwaltung, Kosten und Rechnungsstellung bzgl. Netzressourcen, Nutzungsbeschränkung, Abrechnungsbereiche, Austausch von Kosteninformationen zwischen verschiedenen Bereichen
- **Netzdokumentation**

Wichtige TCP/IP-Netzwerkmanagement-Standards

- **SNMP:** A Simple Network Management Protocol (RFC 1157)
- **SMI:** Structure of Management Information (RFC 1155, RFC 1212)
- **MIB-II:** Management Information Base for Network Management of TCP/IP-based Internets (RFC 1213)
- **SMIv2:** Structure of Management Information Version 2 (RFC 2578, RFC 2579, RFC 2580)
- **RMON:** Remote Network Monitoring Management Information Base (RFC 2819)
- **SNMPv3:** Simple Network Management Protocol Version 3 (RFC 3411 – RFC 3418)

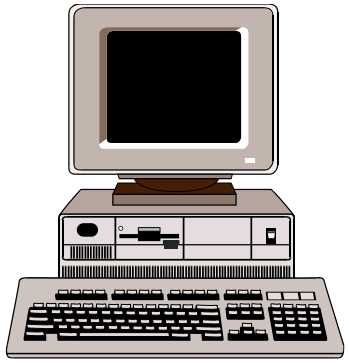
Themenübersicht

- Funktionen des Netzwerkmanagement
- **SNMP: Simple Network Management Protocol**
- MIB: Management Information Base
- RMON
- SNMP-basierte Managementwerkzeuge
- Reporting

SNMP - Komponenten

- **Agent:** Komponente auf dem zu managenden Gerät
- **Manager:** Management-System mit Management-Anwendung
- **MIB:** Management Information Base, Datenbasis auf dem Agenten
- **SNMP:** Simple Network Management Protocol für die Kommunikation zwischen Manager und SNMP-Agent

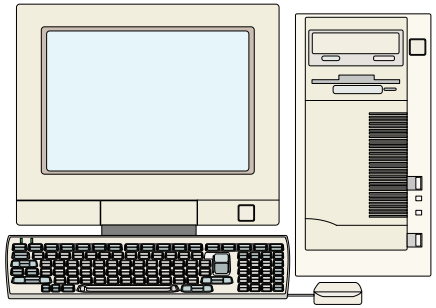
SNMP: Manager und Agent

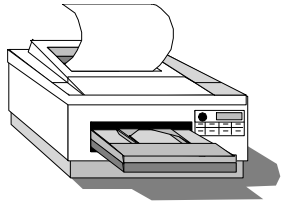


Manager
(z.B. Unix-System)

SNMP-Anfragen,
Antworten
und Traps

MIB auf **Agenten** (z.B. Hub, Switch,
Router, Server, Drucker, ...)

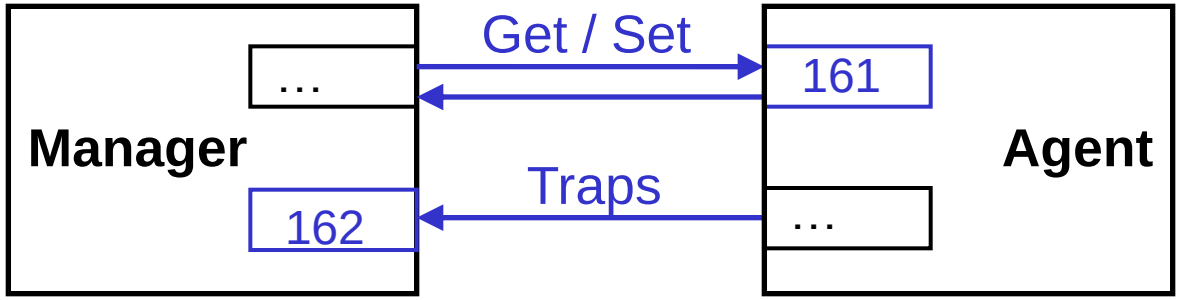




SNMP-Agent - Realisierungsmöglichkeiten

- sog. **Management-Modul** einer Netzkomponente
- **integriert** in Netzkomponente
- **Prozess** auf einem Server
- evtl. dedizierter **Management-Port**

SNMP-Protokoll: Überblick



- **UDP-basierend:**
  - Port 161: Get / Set -Operationen
  - Port 162: Traps (spontane Meldungen)
- **asynchrones** Frage-/Antwort-Protokoll
- Mit Get/Set werden Variable (z.B. Zähler, Konfigurations-parameter, Zustände, ...) von Netzkomponenten abgefragt oder gesetzt.

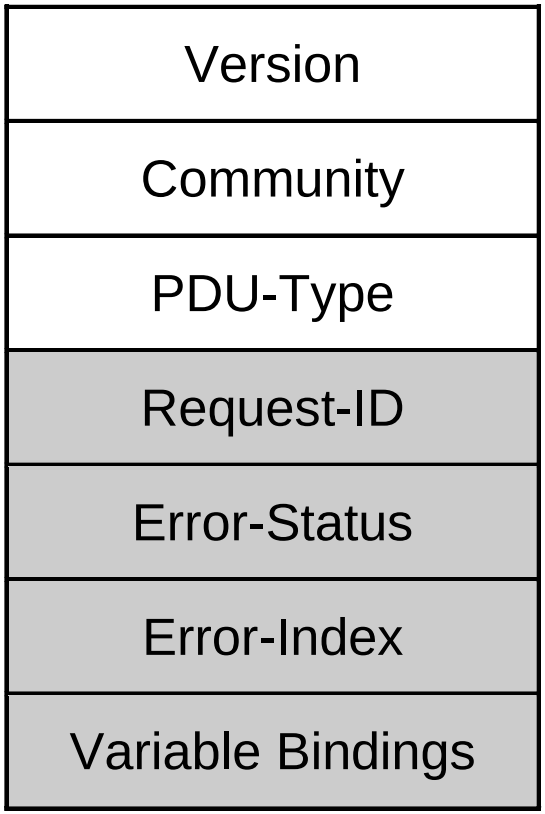
SNMP-Protokoll: Operationen

- **PDUs:** Protocol Data Units
- Operationen:
  - **Get-Request:** Lesen von Werten
  - **Get-Next-Request:** Lesen des nächsten Wertes (einer Tabelle)
  - **Set-Request:** Setzen von Werten
  - **Get-Response:** Antwort auf ein Get/Set-Request
  - **Trap:**
    - bei besonderen Ereignissen vom SNMP-Agenten unaufgefordert zum Manager geschickte Meldung (d.h. kein Polling erforderlich)
    - keine Empfangsbestätigung!

SNMP-Community

- Name, der eine Beziehung zwischen einem SNMP-Agenten und einer Menge von SNMP-Managern bezeichnet
- Verwendung für die Definition einer Zugriffskontrolle auf einem Agenten
- letztlich Funktion wie ein im Klartext übertragenes Passwords

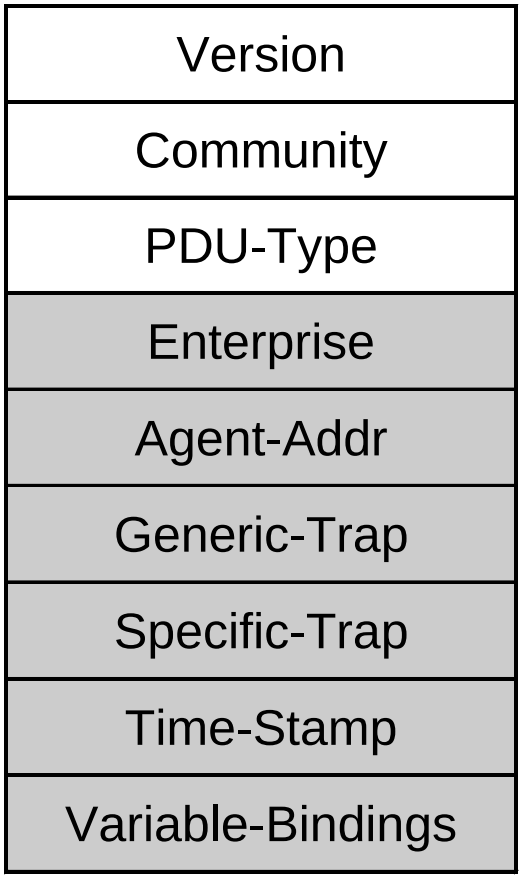
SNMP: Get und Set PDU-Format



SNMP Error-Status - Werte

- noError(0)
- tooBig(1)
- noSuchName(2)
- badValue(3)
- readOnly(4)
- genErr(5)

SNMP: Trap PDU-Format



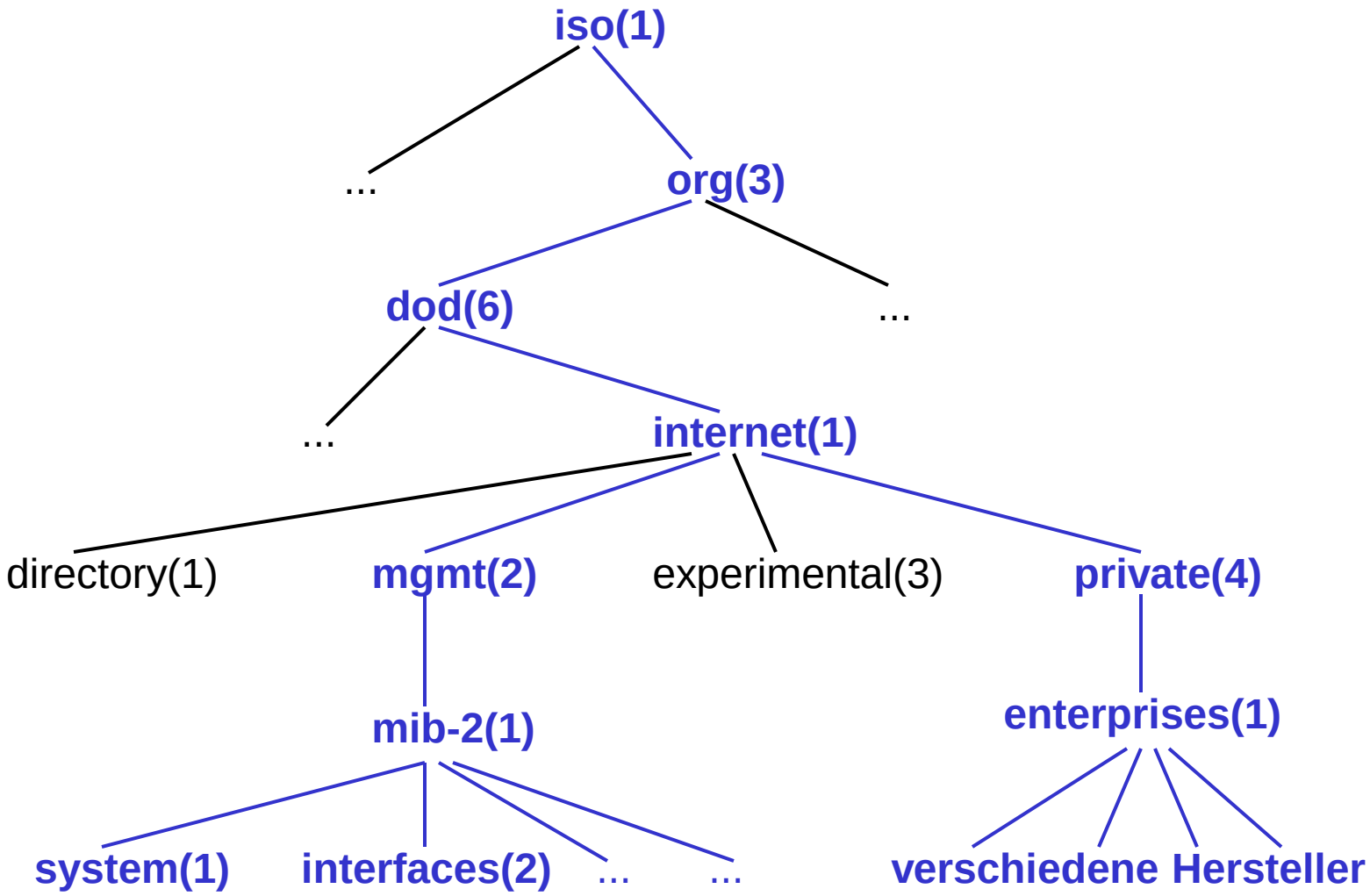
Themenübersicht

- Funktionen des Netzwerkmanagement
- SNMP: Simple Network Management Protocol
- **MIB: Management Information Base**
- RMON
- SNMP-basierte Managementwerkzeuge
- Reporting

SMI und MIB

- **SMI (Structure of Management Information):** Aufbau einer Datenbasis für das Netzwerkmanagement
- **MIB (Management Information Base):** hierarchische, baumartig angeordnete Datenbasis für Objekte des Netzwerkmanagements
- **MIB-II:** standardisierte Datenbasis für Standardobjekte (171 Objekte in 10 Gruppen)
- **MIBs für spezielle Netztechnologien, Netzfunktionen** in die MIB-II eingehängt
- **herstellerspezifische MIBs:** Unterstützung herstellerspezifischer Eigenschaften von Geräten

Aufbau der Standard MIB-II



MIB: Identifizierung von Objekten / Variablen

- Identifizierung von Objekten über:
  - durch Punkte getrennte Folge von Nummern von Unterbäumen z.B.: **1.3.6.1.2.1.1.1**
  - oder: durch Punkte getrennte Folge von Namen von Unterbäumen z.B.: ***.iso.org.dod.internet.mgmt.mib-2.system.sysDescr***
- **ASN.1 (Abstract Syntax Notation 1, ISO 8824):** Sprache zur Definition von Objekten in MIB-Unterbäumen
- **Instanzen** von Objekten
- **Tabellen** (z.B. Interfaces, Routing-Tabelle)
- **MIB-View:** Untermenge von Objekten in der MIB
- Enterprise-IDs: http://www.iana.org/assignments/enterprise-numbers

MIB-II: Unterbäume

- **system:** allgemeine Informationen
- **interfaces:** Netzwerk-Schnittstellen
- **at:** Address Translation (soll wegfallen)
- **ip**
- **icmp**
- **tcp**
- **udp**
- **egp:** Exterior Gateway Protocol
- **transmission:** Unterbäume für die Standard-Netztechniken (Ethernet, FDDI, ...)
- **snmp**

MIB-II: Objekte der System-Gruppe

- **sysDescr:** Beschreibung der Netzwerkkomponente
- **sysObjectID:** Bezeichnung für die Software des Agenten
- **sysUpTime:** Laufzeit des Agenten
- **sysContact:** Name der Kontaktperson
- **sysName:** Name des Gerätes
- **sysLocation:** Aufstellungsort des Gerätes
- **sysServices:** auf dem Gerät installierte Netzwerkdienste

MIB-II: Einige Objekte der Interfaces-Gruppe

- **ifIndex:** Nummer des Interfaces
- **ifDescr:** Beschreibung
- **ifSpeed:** Übertragungsgeschwindigkeit
- **ifPhysAddress:** physikalische Adresse
- **ifAdminStatus:** gewünschter Status
- **ifOperStatus:** tatsächlicher Status
- **ifInOctets:** Anzahl empfangener Bytes
- **ifInUcastPkts:** Anzahl empfangener Unicast-Pakete
- ...

gerätespezifische MIBs - Beispiele

- RFC 1515: Definitions of Managed Objects for IEEE 802.3 Medium Attachement Units (MAUs)
- RFC 1516, RFC 2108: Definitions of Managed Objects for IEEE 802.3 Repeater Devices
- RFC 1643: Definitions of Managed Object for the Ethernet-like Interface Types
- RFC 1493: Definition of Managed Objects for Bridges
- RFC 1215: FDDI MIB
- RFC 1628: UPS MIB
- RFC 1757, RFC 2819: Remote Network Monitoring MIB
- RFC 1317, RFC 1659: Definitions of Managed Objects for RS-232-like Hardware Devices

SNMP: Generic Traps (Standard-Traps)

- **ColdStart**: Neustart des SNMP-Agenten und der Objekte
- **warmStart**: nur Neustart des SNMP-Agenten
- **linkDown**: Ein Interface hat Zustand von *up* nach *down* verändert.
- **linkUp**: Ein Interface hat Zustand von *down* nach *up* verändert.
- **authenticationFailure**: falscher Community-Name
- **egpNeighborLoss**
- **enterpriseSpecific**: Anzeige eines herstellerspezifischen Traps

Konfiguration eines SNMP-Agenten

- Community Name
- Manager (DNS-Namen oder IP-Adressen)
- evtl. Einschränkung des Zugriffs / der Zugriffsart (Get/Set) auf Teile des MIB-Baumes (**View**)
- Empfänger für Traps (DNS-Namen oder IP-Adressen)
- Festlegung, welche Traps geschickt werden sollen
- Einträge im System-Unterbaum der MIB-II:
  - sysContact
  - sysName
  - sysLocation

SNMP Version 2: SNMPv2

- **Security**
  - **Authentisierung** zur Verhinderung der Datenverfälschung und Absenderimitation
  - **Privacy:** Unleserlichmachung der Daten
- **Manager-Manager-Kommunikation** zur Realisierung eines hierarchischen Managements
- **Get-Bulk-Request**: zusätzliches Protokollelement zum Auslesen großer Datenmengen
- **keine Kompatibilität** zwischen SNMPv1 und SNMPv2
- **strukturelle Änderung der MIB**
- **Definition einer Protokollumsetzung** zwischen einem SNMPv2-Manager und einem SNMPv1-Agenten
- **Festlegung der Umsetzung einer MIB** von SNMPv1-Format in SNMPv2-Format

Themenübersicht

- Funktionen des Netzwerkmanagement
- SNMP: Simple Network Management Protocol
- MIB: Management Information Base
- **RMON**
- SNMP-basierte Managementwerkzeuge
- Reporting

RMON-MIB: Remote Network Monitoring - 1

- **Probe**: Sensor zur Überwachung von Netzwerkanschlüssen, Sammlung von Daten, Langzeitstatistik
- **RMON-Agent**: SNMP-Schnittstelle zur Probe
- **Verlagerung der Management-Intelligenz** vom Manager auf RMON-Probe
- **Entlastung des Manager-Systems** von Routine-Überwachungsaufgaben
- z.T. **Ersatz für teure Protokollanalysatoren**

RMON-MIB: Remote Network Monitoring - 2

- RFC 2819: Remote Network Monitoring Management Information Base (**Ethernet**: neun Gruppen):
  - Statistik: Fehlerstatistik
  - Geschichte: periodische Musterstatistiken
  - Alarm: Schwellwerte für Zähler
  - Filter: Überwachung bestimmter Netzpakte
  - ...
- RFC 1513: **Token Ring** Extensions to the Remote Network Monitoring MIB

Themenübersicht

- Funktionen des Netzwerkmanagement
- SNMP: Simple Network Management Protocol
- MIB: Management Information Base
- RMON
- **SNMP-basierte Managementwerkzeuge**
- Reporting

SNMP-basierte Managementwerkzeuge

- **MIB-Browser:** Anzeige der MIB
- **grafische Darstellung** der zeitlichen Änderung von MIB-Variablen
- **Trap (Event-)Anzeiger**
- **Node Discovery**: autmatisches Entdecken der Stationen im Netz (Router, Hubs, Rechner, ...)
- **Topology-Discovery**: automatisches Erkennen der Netzstruktur
- **Netzeditor / Map**: Darstellung der Netzstruktur nach verschiedenen Aspekten
- **Konnektivitätsüberwachung**

Themenübersicht

- Funktionen des Netzwerkmanagement
- SNMP: Simple Network Management Protocol
- MIB: Management Information Base
- RMON
- SNMP-basierte Managementwerkzeuge
- **Reporting**

Reporting

- Abgrenzung gegenüber reinem Monitoring
- Kapazitätsüberwachung
- frühzeitige Erkennung von Engpässen
- Erkennung von Trends
- Planungsgrundlage
- Überwachung von SLAs: Service Level Agreements
- oft SNMP-basiert
- Reports des Netzes der Universität Münster unter **http://www.uni-muenster.de/ZIV/Content--NetzBetriebReports.html**