Netzwerktechnologien
3 VO

Dr. Ivan Gojmerac
ivan.gojmerac@univie.ac.at

13. Vorlesungseinheit, 19. Juni 2013

Bachelorstudium Medieninformatik
SS 2013

Kapitel 8 - Netzwerksicherheit

8.7 Was ist Sicherheit auf der Netzwerkschicht?

Zwischen zwei Netzwerk-Entitäten...

- Die sendende Entität verschlüsselt den Datenteil der Datagramme
- Der Datenteil könnte sein:
  - Ein TCP oder UDP-Segment,
  - Eine ICMP Nachricht,
  - Eine OSPF Nachricht,
  - Usw.
- Alle Daten die von einer Entität zu einer anderen gesendet werden sind nun verborgen:
  - Webseiten, E-Mails, P2P Daten-Übertragungen, TCP SYN Pakete, usw.

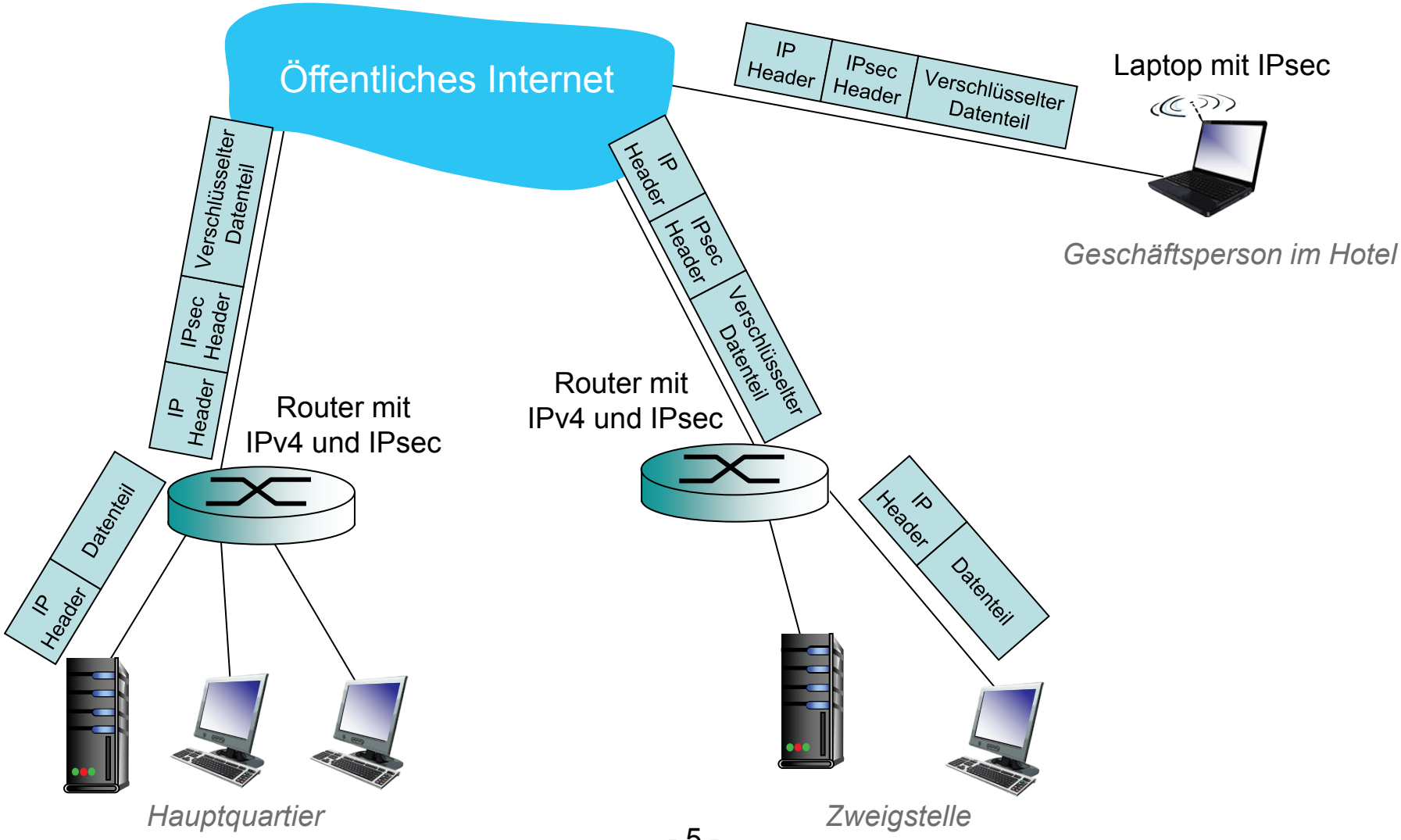
8.7 Virtual Private Networks (VPNs)

Motivation

- Institutionen richten oft aus Sicherheitsgründen eigene physikalische Netzwerke ein. Diese sind aber teuer im Aufbau und in der Wartung

- Statt dessen → **VPN**: Der interne Verkehr einer Institution wird bei VPN über das öffentliche Internet gesendet.
  - Der Verkehr wird vor dem Eintritt in das öffentliche Internet verschlüsselt
  - Der Verkehr ist (nur) logisch vom sonstigen Datenverkehr getrennt

8.7 Virtual Private Networks (VPNs)



8.7 IPsec: Sicherheit auf der Netzwerkschicht

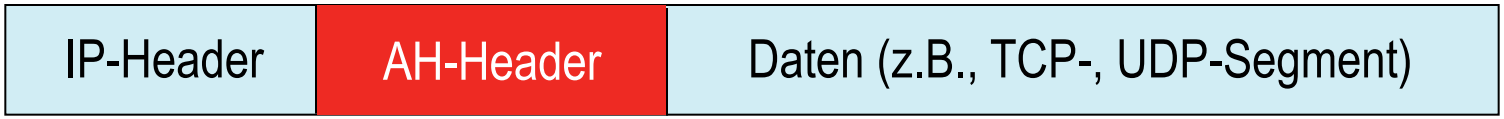
- Authentifizierung:
  - Zielhost kann Quell-IP authentifizieren
- Vertraulichkeit:
  - Sender verschlüsselt IP-Payload
- Zwei zentrale Protokolle:
  - Authentication-Header-Protokoll (AH)
  - Encapsulating-Security-Payload-Protokoll (ESP)
- Zwei Modi:
  - Transport-Modus
  - Tunnel-Modus
- Für AH ebenso wie für ESP: Handshake von Quelle und Ziel
  → logische Netzwerkschicht-Verbindung namens “Security Association (SA)”
- Jede SA ist unidirektional
  - Eindeutig bestimmt durch: Sicherheitsprotokoll (AH oder ESP), Quell-IP, 32-Bit-Verbindungs-ID

8.7 Authentication Header Protokoll (AH)

- Bietet Quellauthentifizierung, Datenintegrität, keine Vertraulichkeit
- AH-Header zwischen IP-Header und Datenfeld
- IP-Protokollfeld: 51
- Router unterwegs behandeln das Datagramm wie üblich

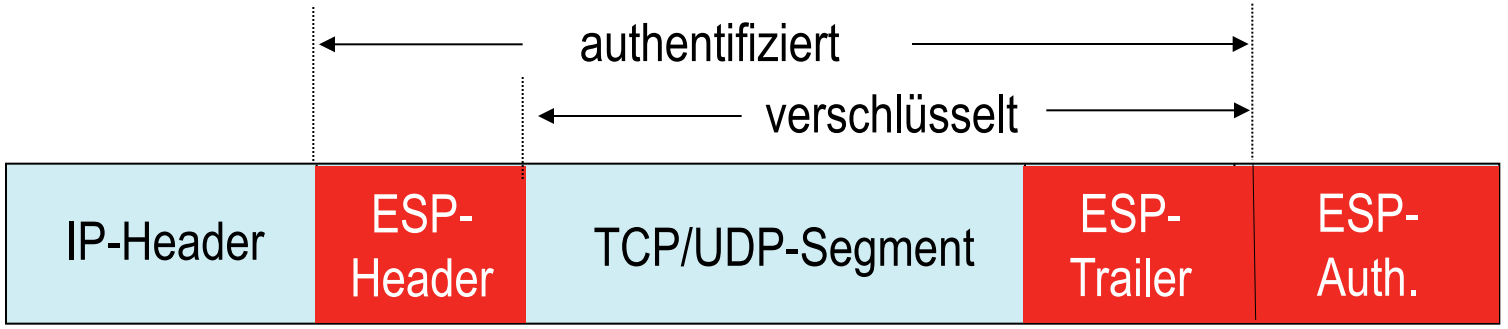
AH-Header umfasst:

- Verbindungs-ID
- Authentifizierungsdaten: Von der Quelle signierter Hashwert über das Original-Datagramm
- Next-Header-Feld: Payload-Typ (z.B., TCP, UDP, ICMP)



8.7 ESP-Protokoll

- Bietet Vertraulichkeit, Hostauthentifizierung, Datenintegrität
- Daten und ESP-Trailer sind verschlüsselt
- Next-Header-Feld im ESP-Trailer
- ESP-Authentifizierungsfeld funktioniert ähnlich wie das in AH
- IP-Protokollfeld: 50



Kapitel 8 - Netzwerksicherheit

8.8 IEEE-802.11-Sicherheit

- Viele WLAN Access Points werden befinden sich immer noch unverschlüsselt im Einsatz:
  - → WLAN / Internet Mitbenutzung (inkl. illegaler Aktivitäten!) möglich
  - → Paket-Sniffing ist sehr einfach

- **IEEE 802.11 WLAN sollte man absichern!**
  - Authentifizierung + Verschlüsselung notwendig!
  - Meistens *Pre-Shared Key* (PSK)-basiert
  - Erster Versuch, 802.11 sicher zu machen: Wired Equivalent Privacy (**WEP**) → Ein Fehlschlag
  - Neuer Anlauf: **WPA2** → gilt derzeit als sicher, unter der Voraussetzung, dass kryptographisch ausreichend starke Schlüssel verwendet werden!

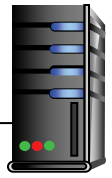
8.8 IEEE-802.11i: Verbesserte Sicherheit

- Starke Verschlüsselungsformen möglich
- Verwendet neben dem Zugangspunkt ins Netz einen separaten Server zur **dynamischen** Benutzer-Authentifizierung

  → Große Vorteile, wenn Benutzer laufend hinzugefügt und entfernt werden müssen, da Pre-Shared Keys (PSKs) in solchen Fällen ständig erneuert werden müssten!

8.8 IEEE-802.11i: 4-Way-Handshake

wired network



STA: Client Station

ZP: Zugangspunkt

AS: Authentifizierungsserver

1 Feststellung von Sicherungs-möglichkeiten

2 STA und AS authentifizieren einander und generieren einen **Master Key** (MKey). *Der ZP fungiert als "Durchgangspforte".*

3a STA leitet **Pairwise Master Key** (PMKey) ab.

3b AS leitet den selben PMKey ab und sendet diesen an den ZP.

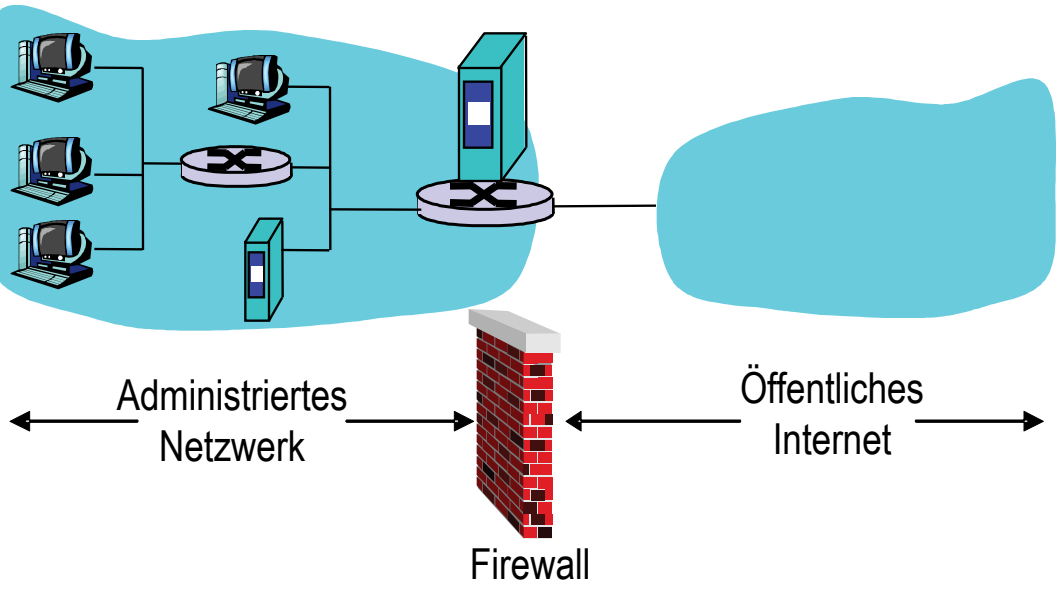
4 STA und ZP verwenden den PMKey um einen **Temporal Key** (TKey) abzuleiten, der für die Nachrichtenverschlüsselung und Überprüfung der Nachrichtenintegrität verwendet wird.

Kapitel 8 - Netzwerksicherheit

8.1 Was ist Netzwerksicherheit?
8.2 Grundlagen der Kryptographie
8.3 Endpunktauthentifizierung
8.4 Nachrichtenintegrität
8.5 Absichern von E-Mail
8.6 Absichern von TCP-Verbindungen: SSL
8.7 Sichern auf der Netzwerkschicht: Ipsec und VPNs
8.8 Sicherheit von Wireless LAN
8.9 Operative Sicherheit: Firewalls und IDS

8.9 Firewalls

Trennt das interne Netz der Organisation vom Rest des Internet; manche Pakete dürfen passieren, andere werden herausgefiltert.



8.9 Firewalls – Wozu?

Denial-of-Service-Angriffe abwehren:

- Angreifer bombardieren Sites mit nutzlosem Verkehr, es bleiben keine Ressourcen für die legitimen Verbindungen

Illegalen Zugriff auf oder Manipulation von internen Daten verhindern:

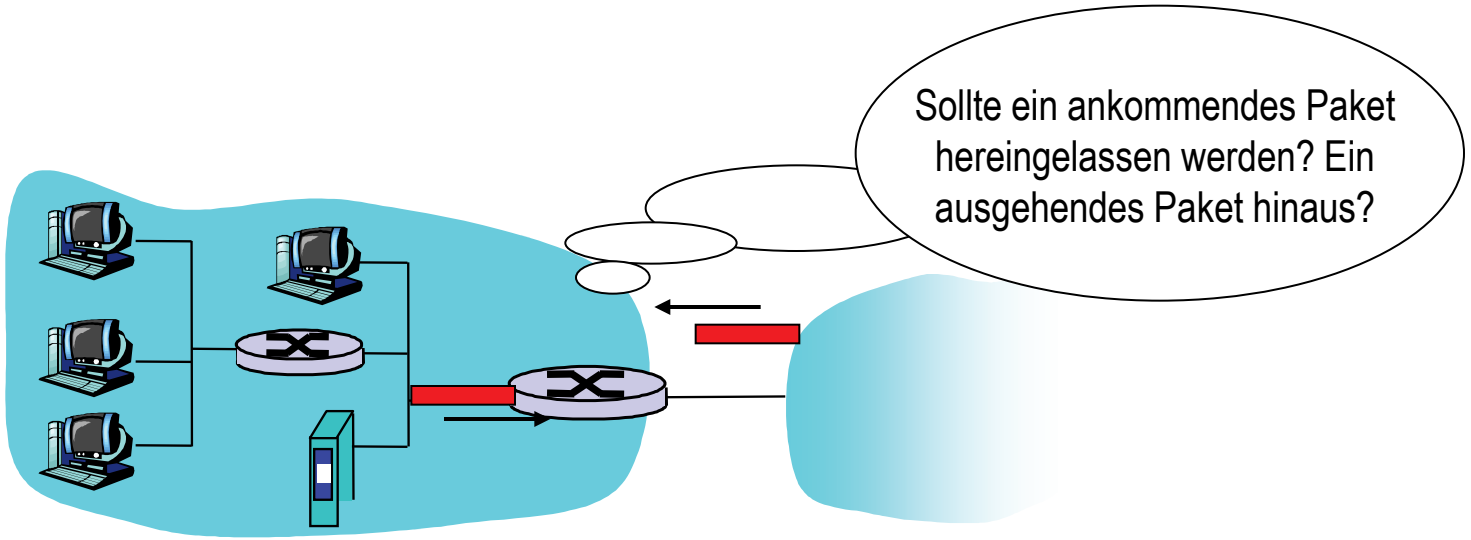
- Ein Angreifer könnte z.B. die Homepage der Organisation „hacken“

→ Nur autorisierten Zugriff auf das interne Netz erlauben (definierte Menge von autorisierten Hosts/Benutzern)

Drei Arten von Firewalls:

- **Zustandslose Paketfilter**
- **Zustandsbasierte Paketfilter**
- Anwendungs-Gateways

8.9 Zustandslose Paketfilter



- Internes Netz ist mit dem Internet über eine **Router-Firewall** verbunden
- Der Router **betrachtet jedes Paket für sich,** die Entscheidung, ob weitergeleitet wird, basiert auf :
  - Quell- und Ziel-IP
  - TCP/UDP-Quell- und Zielportnummern
  - ICMP-Nachrichtentyp
  - TCP-SYN- und ACK-Bits

8.9 Zustandslose Paketfilter

Beispiel 1:

Blockiere eingehende und ausgehende Datagramme mit IP-Protokollfeld 17 (UDP) wie auch jene Datagramme, die entweder Quell- oder Ziel-Port 23 (Telnet) haben.

- Alle ein- oder ausgehenden UDP-Flows **und** Telnet-Verbindungen werden blockiert.

Beispiel 2:

Eingehende TCP-Segmente mit ACK=0 blockieren.

- Hält externe Hosts davon ab, zu internen Hosts TCP-Verbindungen aufzubauen, erlaubt es aber internen Hosts, Verbindungen nach außen zu initiieren.

8.9 Zustandslose Paketfilter

Ziel	Firewall-Regel
Kein Web-Zugriff nach außen.	Alle ausgehenden Pakete zu jeder IP-Adresse und Port 80 oder 443 verwerfen.
Keine eingehenden TCP-Verbindungen, außer sie sprechen den eigenen Webserver an.	Alle eingehenden TCP-SYN-Pakete verwerfen, außer sie gehen an IP-Adresse 130.207.244.203, Port 80.
Vermeiden, dass Web-Radio die gesamte Bandbreite belegt.	Alle (eingehenden) UDP-Pakete verwerfen, außer DNS Verkehr.
Verhindern, dass das eigene Netz mit Traceroute untersucht wird.	Ausgehende ICMP-TTL-Expired-Pakete verwerfen.

8.9 Access Control Lists

ACL: Liste von Regeln, die von oben nach unten auf eingehende Pakete angewandt wird → Paare von Aktionen und Kriterien.

Aktion	Quell-IP	Ziel-IP	Protokoll	Quell-Port	Ziel-Port	Flags
erlaube	222.22/16	nicht in 222.22/16	TCP	> 1023	80	egal
erlaube	nicht in 222.22/16	222.22/16	TCP	80	> 1023	ACK
erlaube	222.22/16	nicht in 222.22/16	UDP	> 1023	53	---
erlaube	nicht in 222.22/16	222.22/16	UDP	53	> 1023	---
verbiete	alle	alle	alle	alle	alle	alle

8.9 Zustandsbehaftete Paketfilter

Zustandslose Paketfilter sind oft unbeholfen:

- Pakete werden zugelassen, die “keinen Sinn machen”, z.B. Quell-Port 80, ACK-Flag gesetzt, obwohl keine TCP-Verbindung existiert:

Aktion	Quell-IP	Ziel-IP	Protokoll	Quell-Port	Ziel-Port	Flags
erlaube	nicht in 222.22/16	222.22/16	TCP	80	> 1023	ACK

Zustandsbehafteter Paketfilter: Verfolgt den Zustand jeder TCP-Verbindung

- Liest den Verbindungsauf- (SYN) und –abbau (FIN) mit: Kann bestimmen, ob ein- und ausgehende Pakete “sinnvoll” sind
- Timeout für inaktive Verbindungen in der Firewall: Alte Verbindungen werden nicht mehr durchgelassen!

8.9 Zustandsbehaftete Paketfilter

ACL wird erweitert um anzuzeigen, ob es notwendig ist, die Zustandstabelle der Verbindungen ebenfalls zu prüfen.

Aktion	Quell-IP	Ziel-IP	Protokoll	Quell-Port	Ziel-Port	Flags	Verbindung prüfen
erlaube	222.22/16	nicht in 222.22/16	TCP	> 1023	80	egal	
erlaube	nicht in 222.22/16	222.22/16	TCP	80	> 1023	ACK	**JA**
erlaube	222.22/16	nicht in 222.22/16	UDP	> 1023	53	---	
erlaube	nicht in 222.22/16	222.22/16	UDP	53	> 1023	----	**JA**
verbiete	alle	alle	alle	alle	alle	alle	

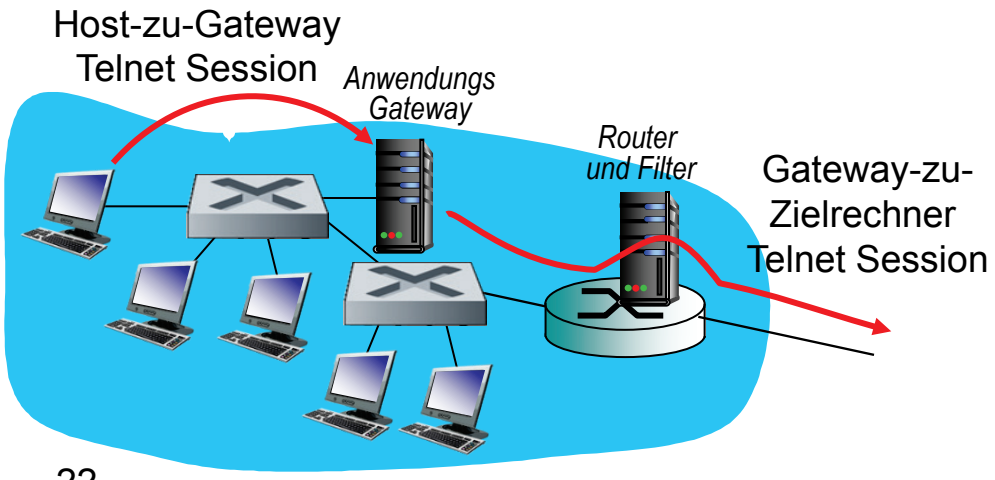
8.9 Anwendungs-Gateways

- Filtere Pakete nach Applikationsdaten und IP/TCP/UDP-Feldern

Beispiel

Einigen wenigen internen Benutzern die Verwendung eines Telnet-Dienstes erlauben:

1. Lasse Telnet Verbindungen nur über ein Gateway zu.
2. Für autorisierte Nutzer stellt das Gateway eine Verbindung zum Zielhost her. Das Gateway leitet die Daten zwischen den Verbindungen auf seinen beiden Seiten weiter.
3. Der Router-Filter blockiert alle Telnet Verbindungen, die nicht über das Gateway verlaufen.



8.9 Beschränkungen von Firewalls und Gateways

- IP Spoofing: Router können nicht wissen ob die Daten wirklich von der vorgegebenen Quelle kommen
- Wenn mehrere Anwendungen eine gesonderte Behandlung erfordern bekommt jede Anwendung ihr eigenes Gateway
- Die Client Software muss wissen, wie das Gateway zu erreichen ist
  - z.B. Die IP Adresse eines Proxy, die im Webbrowser eingestellt werden muss
- Kompromiss zwischen dem Grad der Kommunikation mit der Außenwelt und dem möglichen Sicherheitsniveau

→ Auch auf stark geschützte Sites werden immer wieder Angriffe verübt!

8.9 Intrusion-Detection-Systeme

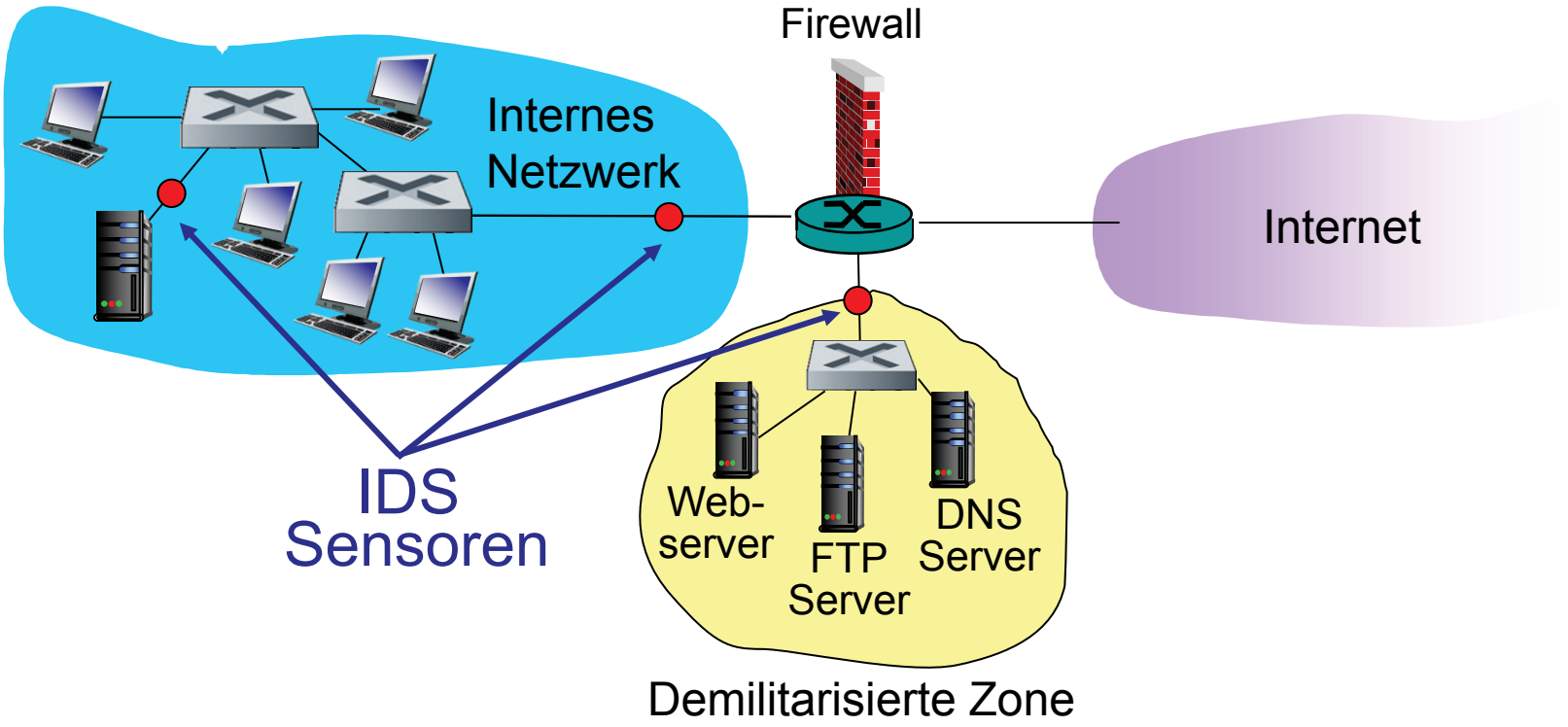
- Paketfilter:
  - Arbeiten nur auf den TCP/IP-Headern
  - Daten unterschiedlicher Sitzungen können nicht korreliert werden

- **IDS: Intrusion-Detection-System**
  - *Deep Packet Inspection:* Betrachtet den Paketinhalt (vergleicht z.B. ob im Paket Zeichenketten vorkommen, die in einer Datenbank bekannter Angriffe und Viren vorkommen)
  - Korrelation mehrerer Pakete, z.B. bei Port-Scanning

8.9 Intrusion-Detection-Systeme

Gängige IDS Deployments:

→ An verschiedenen Stellen wird der Verkehr aufgenommen, überprüft und gegebenenfalls korreliert.



Kapitel 9 - Netzwerkmanagement

9.1 Was ist Netzwerkmanagement?

Autonome Systeme (oder "Netzwerke"): Hunderte oder Tausende von interagierenden Hard- und Softwarekomponenten

- Komplexe Systeme benötigen Überwachungs- und Steuerungsfunktionen, man findet das z.B. in
  - Flugzeugen
  - Kernkraftwerken

*"**Netzwerkmanagement** beinhaltet Einsatz, Integration und Koordination von Hardware, Software und menschlichen Beteiligten um das Netzwerk und die Ressourcen, aus denen es besteht, zu überwachen, zu testen, abzufragen, zu konfigurieren, zu analysieren, auszuwerten und zu steuern, um so die Leistung während des Betriebs in Echtzeit sowie die Dienstgüteanforderungen bei vernünftigen Kosten zu gewährleisten."*

Kapitel 9 - Netzwerkmanagement

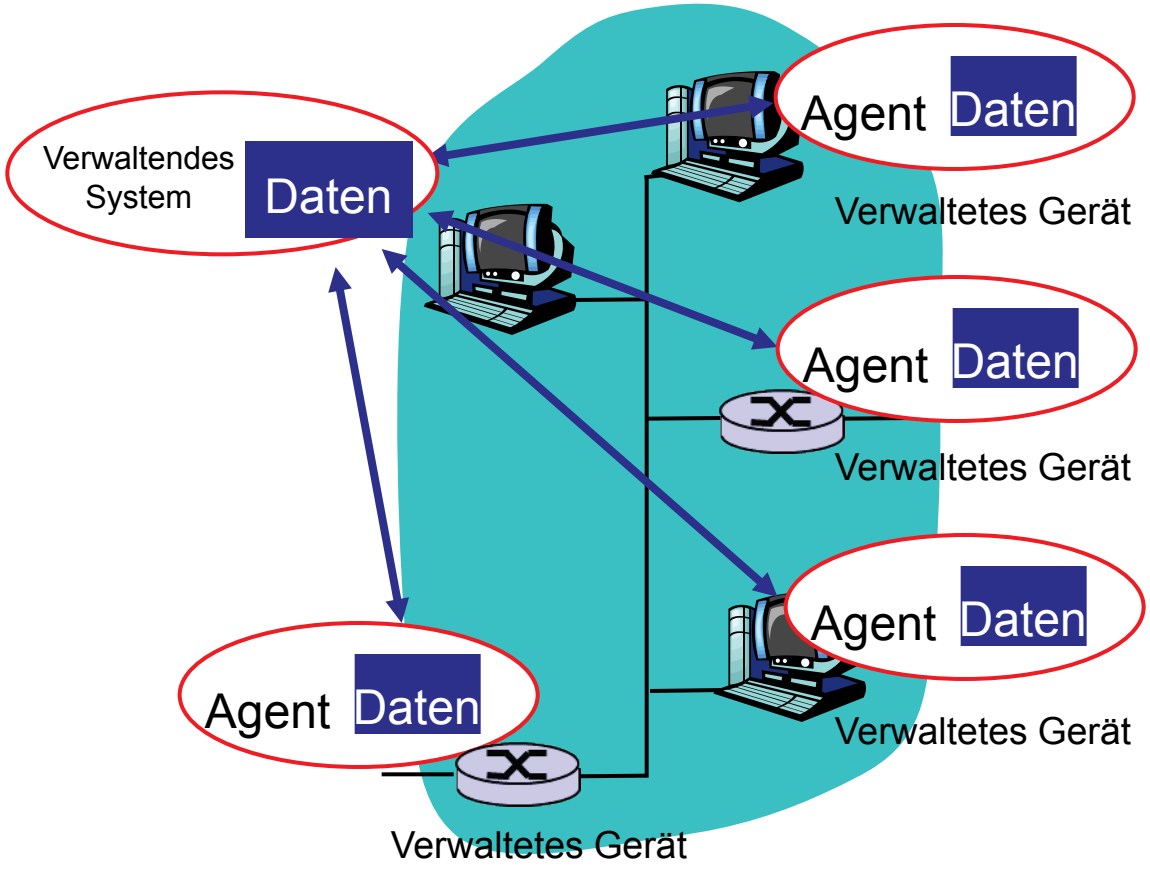
9.1 Was ist Netzwerkmanagement?

9.2 Die Infrastruktur des Netzwerkmanagements

9.3 Simple Network Management Protocol (SNMP)

9.2 Infrastruktur für das Netzwerkmanagement

Definitionen:



Verwaltete Geräte enthalten *verwaltete Objekte* deren Daten in einer **Management Information Base (MIB)** gesammelt werden.

9.2 Netzwerkmanagement-Standards

OSI CMIP

- Open Systems Interconnection – Common Management Information Protocol
- In den 1980ern entworfen: *Der* einheitliche Netzwerkmanagement-Standard
- Zu schleppend standardisiert

SNMP: Simple Network Management Protocol

- Wurzeln im Internet (SGMP – Simple Gateway Monitoring Protocol)
- Kleine, bescheidene Anfänge
- Schnelle Verbreitung
- Zuwachs an Mächtigkeit und Komplexität
- Aktuell: SNMP V3
- ***De-facto*-Netzwerkmanagement-Standard**

Kapitel 9 - Netzwerkmanagement

9.1 Was ist Netzwerkmanagement?

9.2 Die Infrastruktur des Netzwerkmanagements

9.3 Simple Network Management Protocol (SNMP)

9.3 SNMP-Überblick – 4 zentrale Elemente

- **Management Information Base (MIB):**
  - Verteilter Speicher für Netzwerkmanagement-Daten
- **Structure of Management Information (SMI):**
  - Datendefinitionssprache für MIB-Objekte
- **SNMP-Protokoll**
  - Übertragung von Informationen und Befehlen zwischen verwaltender und verwalteter Einheit
- **Sicherheit und Administration**
  - Die wesentliche Neuerung in SNMPv3

9.3 SMI – Datendefinitionssprache

Zweck: Syntax, Semantik von Managementdaten wohldefiniert und eindeutig

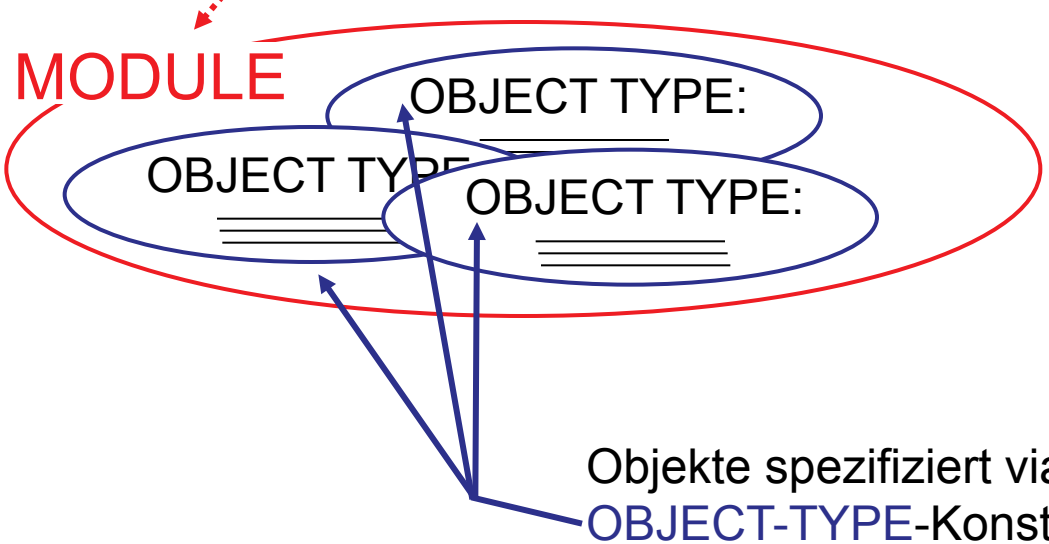
- Basisdatentypen
  - Simpel (siehe rechts)
- OBJECT-TYPE
  - Datentyp, Status und Semantik eines verwalteten Objektes
- MODULE-IDENTITY
  - Zusammenfassen von Objekten zu MIB-Modulen

Basisdatentypen:

- INTEGER
- Integer32
- Unsigned32
- OCTET STRING
- OBJECT IDENTIFIED
- IPaddress
- Counter32
- Counter64
- Guage32
- Time Ticks
- Opaque

9.3 SNMP MIB

MIB-Modul, spezifiziert in der SMI
MODULE-IDENTITY
(100 Standard-MIB-Module, zusätzlich noch herstellerspezifische weitere)



9.3 SMI – Beispiele für Objekte und Module

OBJECT-TYPE: ipInDelivers

```
ipInDelivers OBJECT-TYPE
   SYNTAX        Counter32
   MAX-ACCESS    read-only
   STATUS        current
   DESCRIPTION
       "The total number of input
        datagrams successfully
        delivered to IP user-
        protocols (including ICMP)"
   ::= { ipEntry   9}
```

9.3 MIB-Beispiel – UDP-Modul

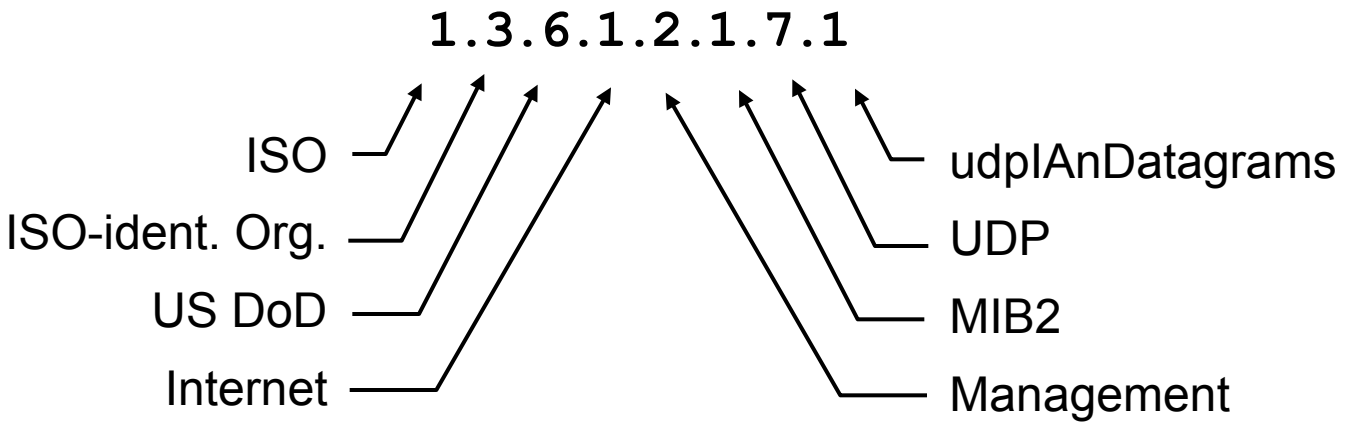
Object ID	Name	Typ	Kommentar
1.3.6.1.2.1.7.1	UDPInDatagrams	Counter32	Gesamtzahl zugestellter Datagramme an diesem Knoten
1.3.6.1.2.1.7.2	UDPNoPorts	Counter32	Gesamtzahl unzustellbarer Datagramme, keine Anwendung
1.3.6.1.2.1.7.3	UDInErrors	Counter32	Gesamtzahl unzustellbarer Datagramme, andere Gründe
1.3.6.1.2.1.7.4	UDPOutDatagrams	Counter32	Zahl gesendeter Datagramme
1.3.6.1.2.1.7.5	udpTable	SEQUENCE	Ein Eintrag pro verwendetem Port, Portnummer + IP

9.3 SNMP-Namensschema

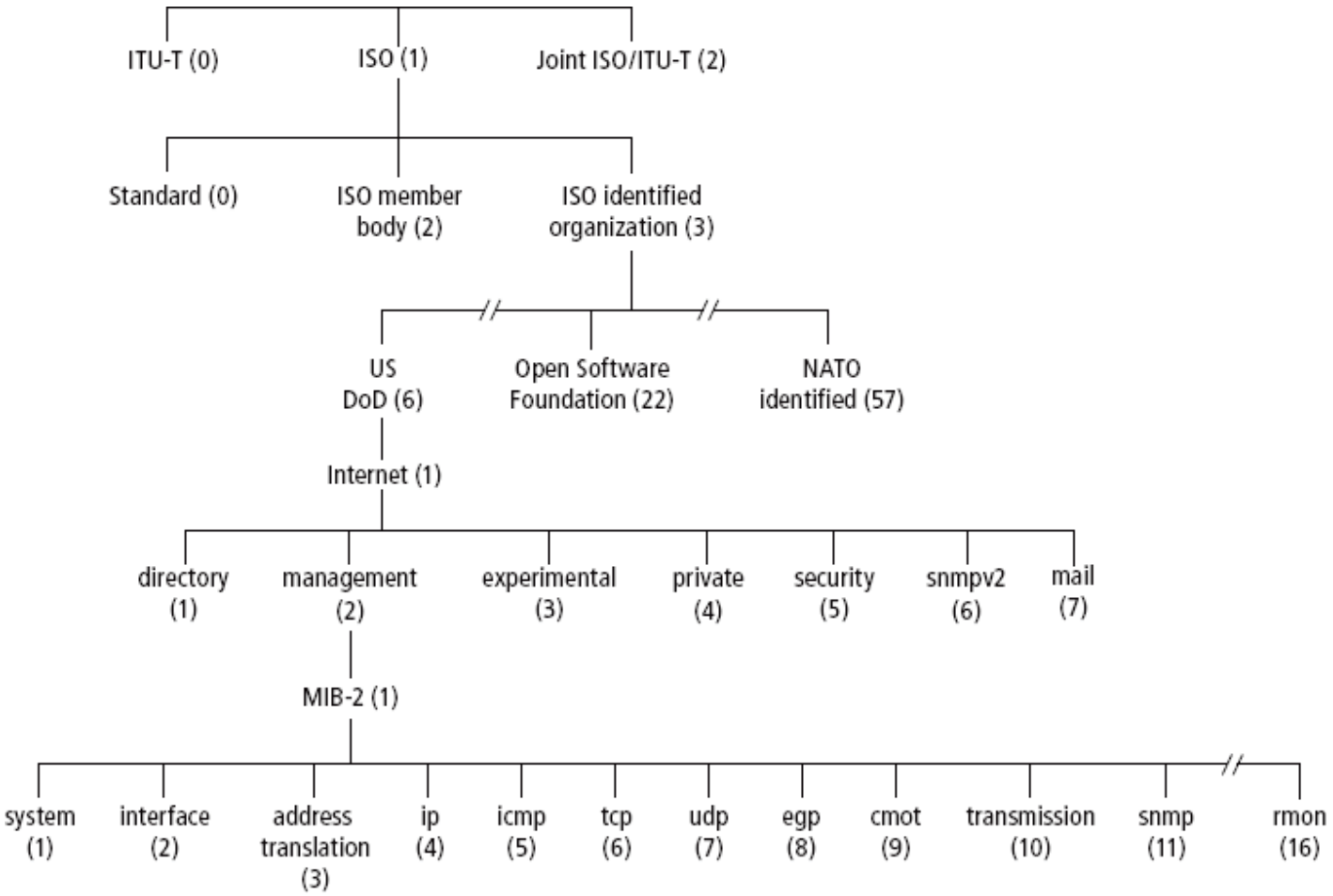
Frage: Wie kann man jedes mögliche Standardobjekt (Protokoll, Daten, usw.) in jedem möglichen Netzwerkstandard eindeutig benennen?

Antwort: **ISO-Objektkennzeichnungsbaum**

- Hierarchische Benennung aller Objekte
- Jede Verzweigung hat einen Namen und eine Nummer

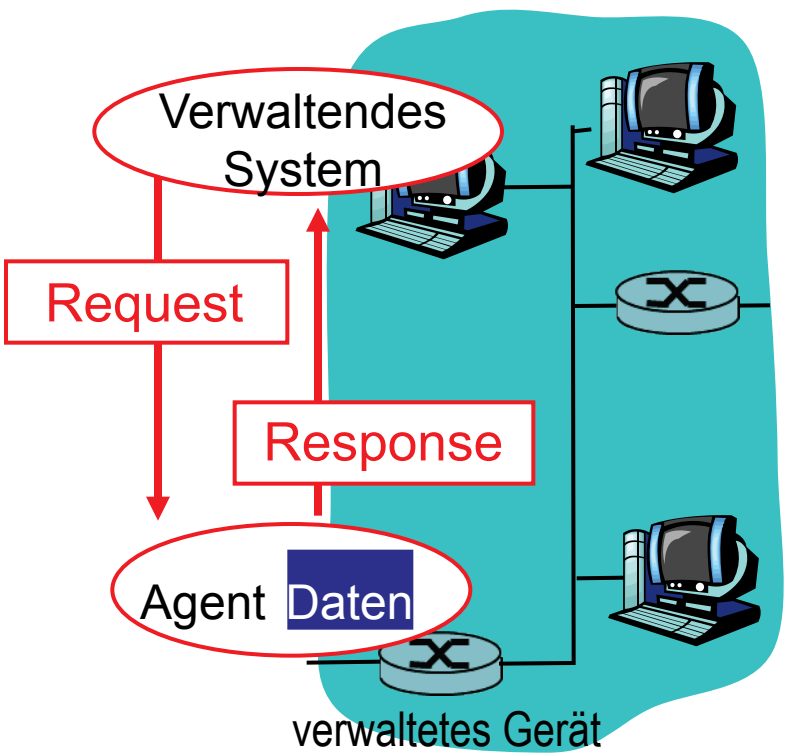


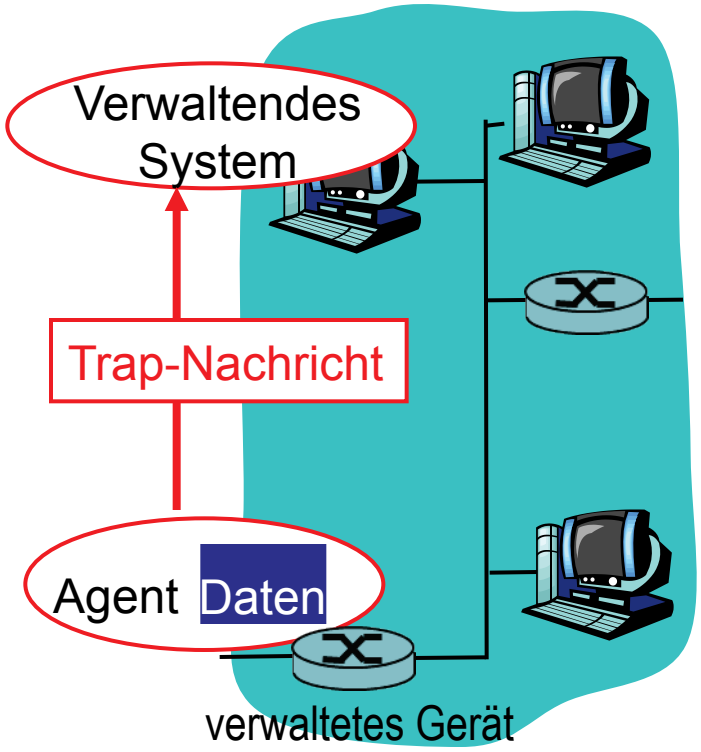
9.3 Objektkennzeichnungsbaum



9.3 SNMP-Protokoll

Zwei Modi um MIB-Information (und Kommandos) zu übertragen:





Request-Response-Modus:

Wird benutzt für das Abfragen oder für die Modifizierung von MIB-Werten im gemanagten Objekt.

Trap-Modus:

Wird benutzt für Benachrichtigungen über außergewöhnliche Ereignise, z.B. Überschreitung einer vordefinierten Schwelle bei einem Messwert.

9.3 SNMP-Protocol – Nachrichtentypen

Nachrichtentyp	Funktion
GetRequest GetNextRequest GetBulkRequest	Verwaltendes System (Manager – Mgr) an Agent: “Gib mir Daten” (Instanz, nächster in Liste, Block)
InformRequest	Mgr an Mgr: “Hier ist ein MIB-Wert”
SetRequest	Mgr an Agent: “Setze MIB-Wert”
Response	Agent an Mgr: Wert, Antwort auf Request
Trap	Agent an Mgr: Benachrichtige Mgr über außergewöhnliches Ereignis

9.3 SNMP – Sicherheit und Verwaltung

- **Verschlüsselung:** DES-Verschlüsselung von SNMP-Nachrichten
- **Authentifizierung:** Sichert die Nachrichten mittels MACs (Message Authentication Codes)
- **Schutz gegen Playback-Angriffe:** Nonce
- **Zugriffskontrolle:** SNMP-Entität enthält eine Datenbank mit Zugriffsrechten und Policies für Benutzer

Termine für die schriftliche Prüfung **Netzwerktechnologien (050019)** im Sommersemester 2013 und im Wintersemester 2013/14

- **1. Termin:** 26. Juni 2013, Beginn um 08:45 Uhr (Dauer: 100 Minuten), Ort: **HS1**
- **2. Termin:** 01. Oktober 2013, Beginn um 15:00 Uhr (Dauer: 100 Minuten), Ort: **HS1**
- **3. Termin:** 08. November 2013, Beginn um 15:00 Uhr (Dauer: 100 Minuten), Ort: **HS1**
- **4. Termin:** 13. Dezember 2013, Beginn um 15:00 Uhr (Dauer: 100 Minuten), Ort: **HS1**