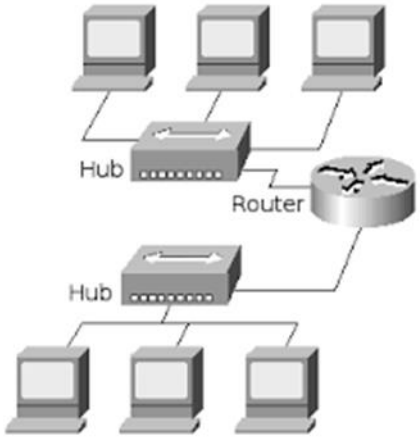
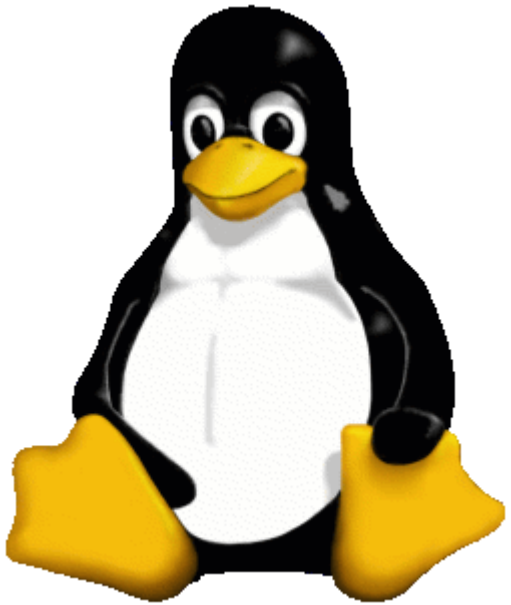
# Einführung in die Netzwerktechnik



## Ich

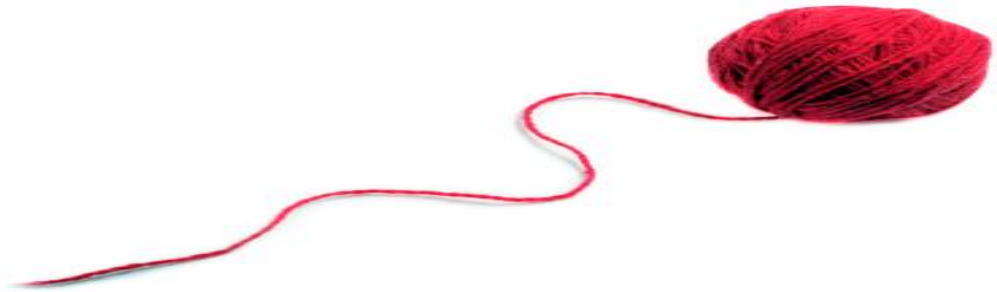

- Falk Schönfeld
- Seit 8 Jahren bei eurogard GmbH
- Entwickler für Remoteserviceprodukte
- Kernkompetenz Linux
- Mail: schoenfeld@eurogard.de
- Telefon: +49/2407/9516-15

# Einführung in die Netzwerktechnik

**Ablauf**:

- Was bedeutet Netzwerktechnik?
- Woher und wohin - historische Entwicklung
- Funktionsweise von Netzwerken – TCP/IP
- Virtuelle Private Netzwerke



SAIA BURGESS CONTROLS

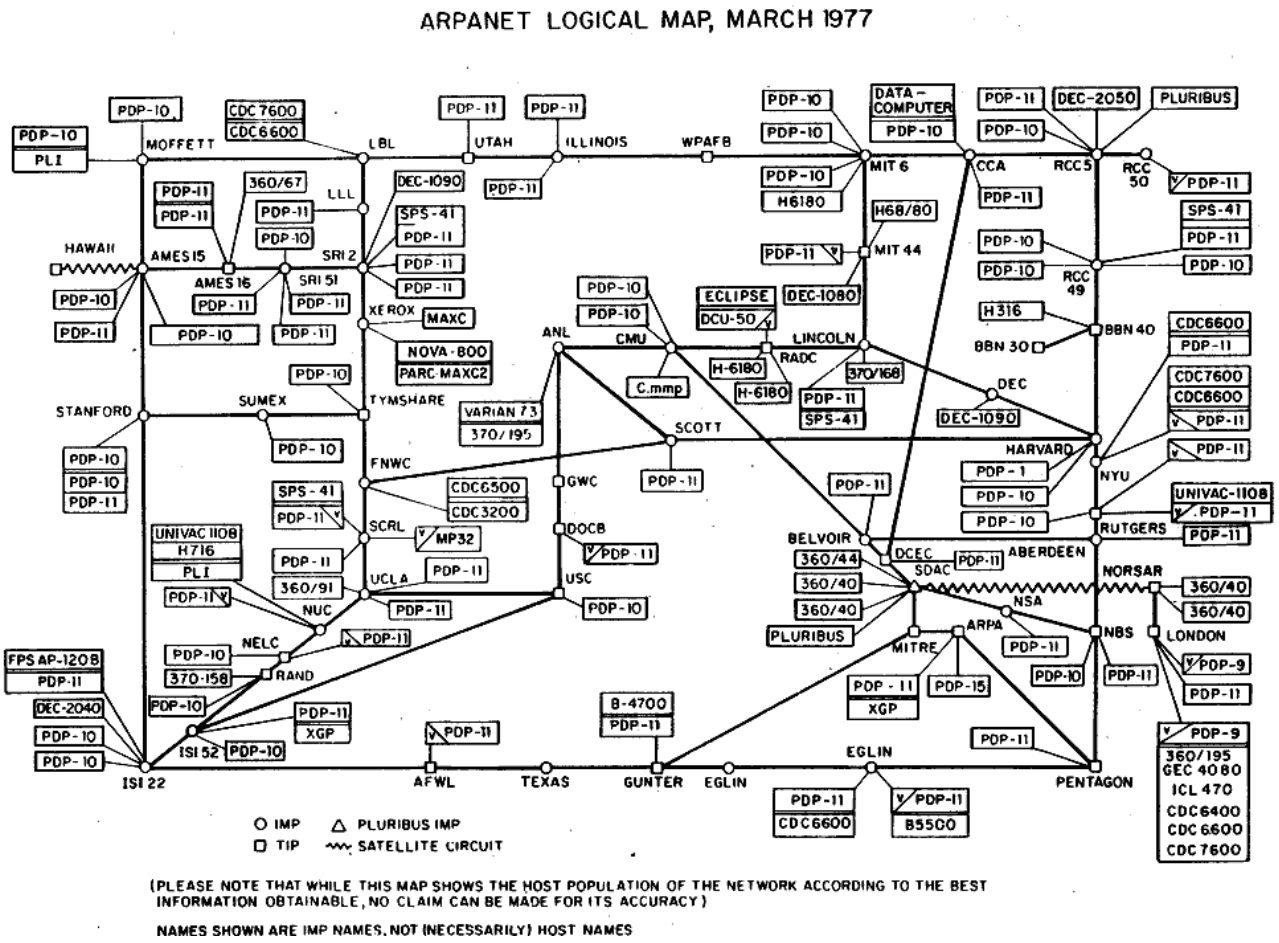
## 1. Netzwerke - Begriffsklärung

- Wir beziehen uns auf Rechnernetze
- Zusammenschluss von netzwerkfähigen Geräten zum Datenaustausch
- Netze sind Verbindungssysteme zur Datenkommunikation
- Teilnehmer müssen gleiche Sprache - Protokolle - sprechen
- Netze haben Topologie

## Geschichtliche Entwicklung

- Entwicklung begann in den 50‘er Jahren
- Ausgehend vom militärischen und universitären Bereich
- 2 verschiedene Ansätze: leitungs- und paketorientierte Verbindungen
- „Urvater“ des Internets -> Arpanet ca. 1970 – 1990
- Viele heute Konzepte z. B. TCP/IP, Unix, C

## Arpanet 1977




(PLEASE NOTE THAT WHILE THIS MAP SHOWS THE HOST POPULATION OF THE NETWORK ACCORDING TO THE BEST INFORMATION OBTAINABLE, NO CLAIM CAN BE MADE FOR ITS ACCURACY)

NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

## Funktionsweise von Netzwerken

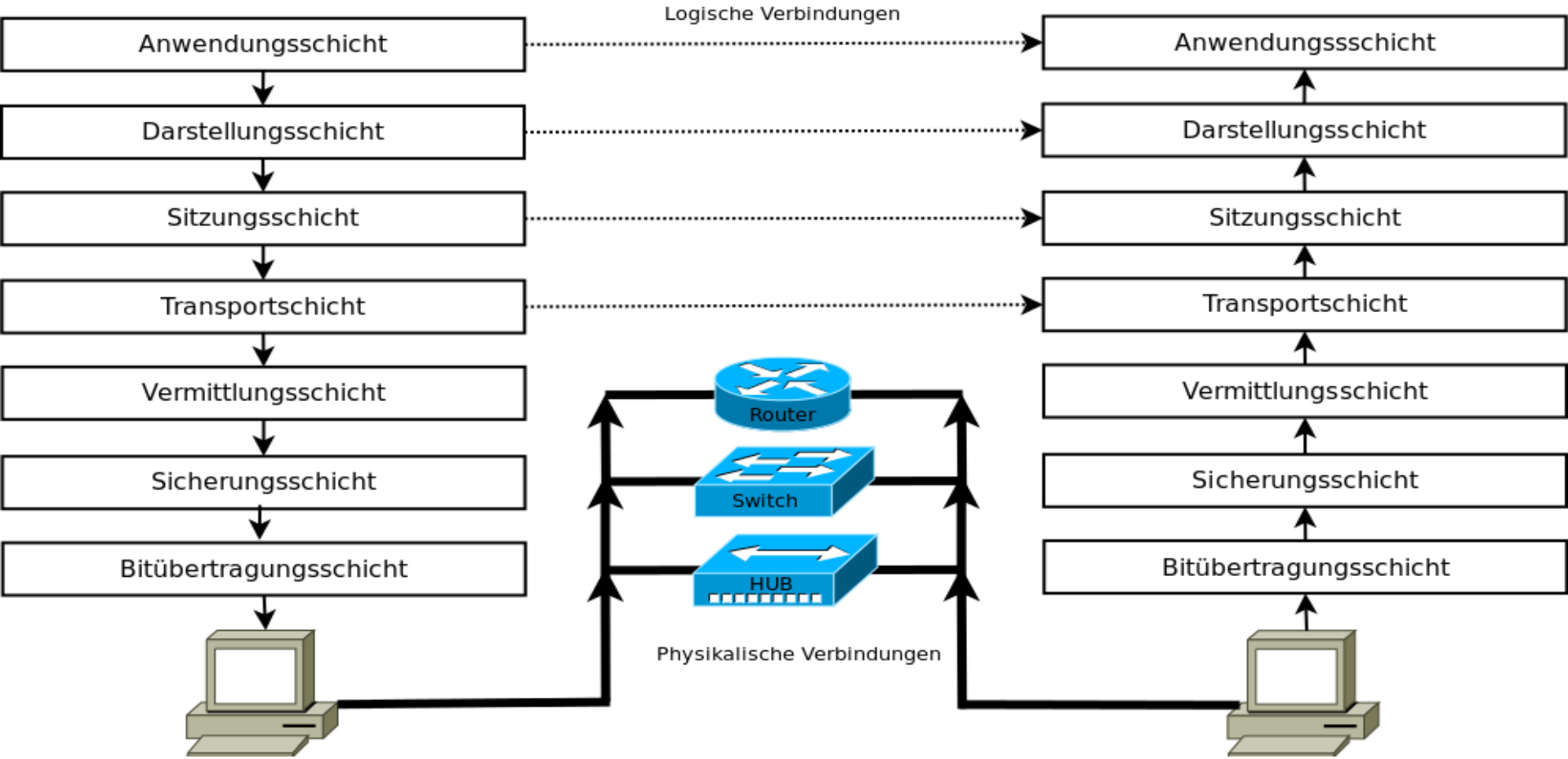
### Probleme und Anforderung

- Adressierung der Teilnehmer
- Geringer Overhead
- Effiziente Nutzung
- Sicherheit
- Fehlertoleranz

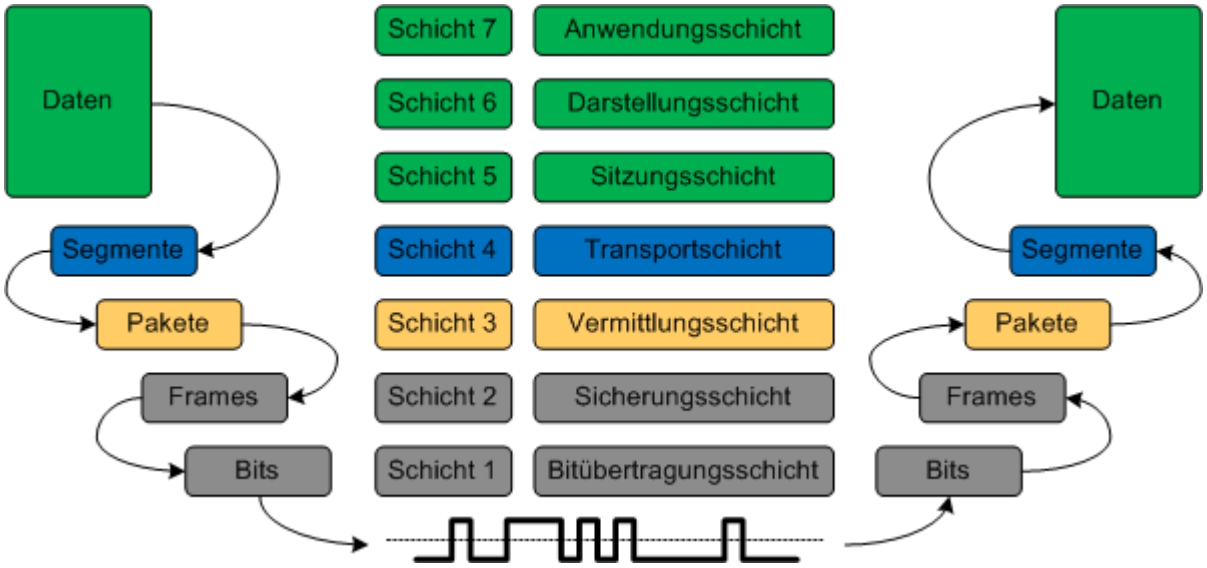
## Das OSI-Modell

- Standard von ISO und ITU aus den 1980‘er Jahren
- Ziel: Vereinfachung der Kommunikation verschiedener Systeme und der Weiterentwicklung
- OSI definiert 7 Schichten gemäß Anforderungen
- Eher akademischer Natur, typischerweise sind 5 abgebildet

## Das OSI-Modell



## Das OSI-Modell



## IP – Das Internet-Protokoll

- Wir reden von IP-Netzwerken
- IP – Internet Protokoll, hier in Version 4 -> IPv4
- IP stellt Verbindung zwischen Kommunikationsteilnehmern her
- Gewissermaßen das „Fräulein vom Amt“
- Teilnehmer (Hosts) finden sich durch eindeutige „IP-Adresse“ des Adapters
- Ein Teilnehmer kann mehrere Adapter (NIC‘s) haben

## IP-Adressen und Subnetzmasken

- Vergleichbar mit Telefonnummer oder Postadresse
- IP-Adressen (IP‘s) müssen (eigentlich) eindeutig sein
- Bestehen aus Netzwerk- und Hostanteil
- Durch Maske wird Netzwerk- und Hostanteil der IP spezifiziert
- Jedes gesetzte Bit in Maske steht für Netzanteil in IP-Adresse
- Host im gleichen Netzwerk können direkt untereinander kommunizieren
- Unterteilt in öffentliche und private Adressen
- Beide bestehen aus 32 Bit, der besseren Lesbarkeit
  byteweise Trennung durch Punkt
- 2 Adressen sind in jedem Netzwerk reserviert: Netzwerk und Broadcast
- Per Voreinstellung Netzwerk mit niedrigster und BC mit höchster Adresse

## Beispiele für IP-Adressen und Subnetzmasken

| IP-Adresse | Subnetzmaske |
|---|---|
| 192.168.1.8 | 255.255.255.0 |

Das heißt:

| | |
|---|---|
| Netzwerkanteil | 192.168.1 |
| Hostanteil | 8 |
| Netzwerk-IP | 192.168.1.0 |
| Broadcast-IP | 192.168.1.255 |

Alle Hosts deren IP‘s den Netzwerkanteil 192.168.1 haben, können direkt mit einander kommunizieren.

# Öffentliche und private IP-Adressen

## Private IP-Adressen

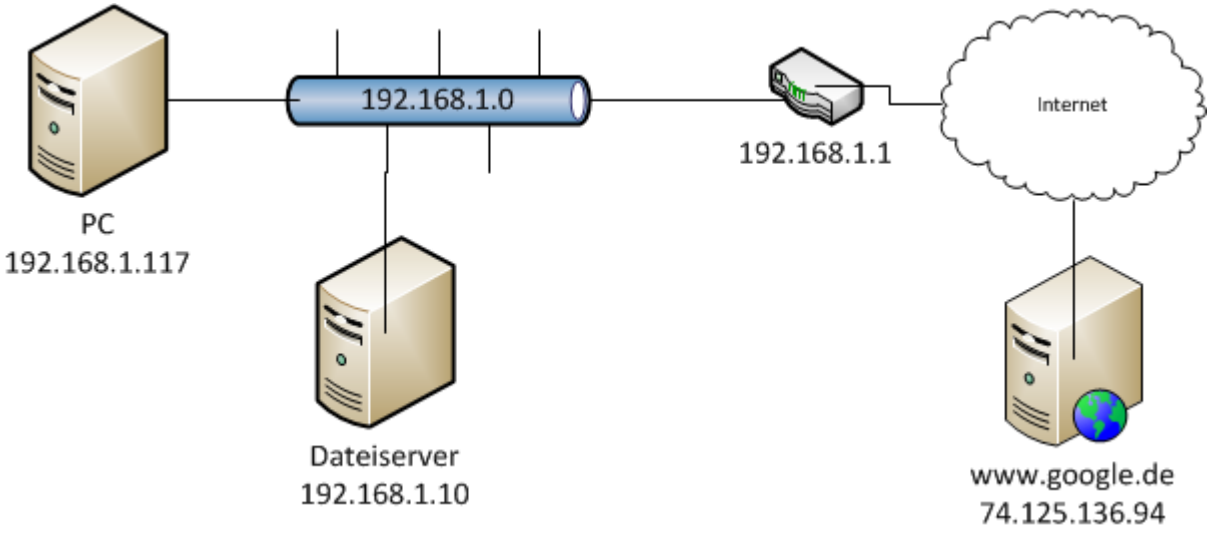
- Private IP‘s werden im Internet nicht transportiert
- Nur für den „Hausgebrauch“
- Bereiche 10.0.0.0/8, 172.16.0.0/16 und 192.168.0.0/24

## Öffentliche IP-Adressen

- Müssen registriert (und bezahlt) werden
- Müssen weltweit eindeutig sein
- Bereich ist alles ohne private IP‘s und besondere Anwendung, wie z.B. Multicast

## Hosts in unterschiedlichen Netzwerken

- Router verbinden mehrere Netzwerke
- Router haben mind. 2 NIC‘s  in verschiedenen Netzen
- Router müssen den Hosts bekannt sein
- Default-Gateway übernimmt falls keine Route bekannt



## Die „Paketdienste“

- Zum eigentlichen Datentransport wird TCP oder UDP benutzt

TCP
- Stellt den Empfang und Integrität der Daten sicher
- Mehr Overhead
- Z.B. Webseiten, Email,...

UDP
- Keine Sicherung gegen Verluste von Paketen
- Wenig Overhead
- Z.B. VoIP, Videostreaming

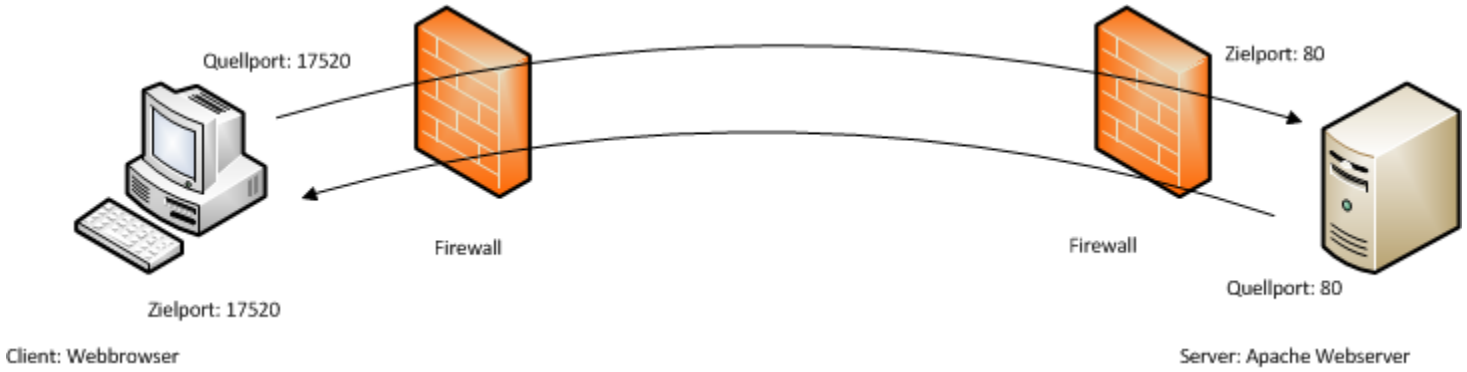
## Was sind Ports?

- Hosts können mehrere Verbindungen gleichzeitig geöffnet haben
- Das OS ordnet Verbindungen den Anwendungen durch Nummern zu
- Pro Verbindung sind immer 2 Ports beteiligt

Quellport
- Nummer der Verbindung vom anfragenden Gerät (Client)
- Meist nicht von Belang

Zielport
- Nummer der Verbindung auf Zielgerät (Server)
- Muss bekannt sein
- Für viele Anwendungen standardisiert z.B. FTP auf Port 21

## Beispiel Ports




Kommunikation zwischen Webbrowser und Webserver

## Virtuelle private Netzwerke

Grundsätzlich:

- Ein in sich geschlossenes Netz, das zum Transport auf bestehende – meist öffentliche und fremde – Netze zurück greift
- Verbinden räumlich und physisch getrennte Teilnehmer oder ganze Netze zu einem logischem Netz
- Dienen der vereinfachten Administration und Erreichbarkeit

Aber:

- Erhöhtes Schutzbedürfnis wegen Transport über öffentliche, bzw. fremde Netze

Unterscheidung in End-to-End, Site-to-Site,End-to-Site,…

## Virtuelle private Netzwerke

### Schutzbedarf

- Authentizität der Teilnehmer
- Integrität der Kommunikation
- Vertraulichkeit der Kommunikation
- Ev: Abstreitbarkeit der Kommunikation

# Virtuelle private Netzwerke

## Möglichkeiten der Realisierung

1. Authentizität

- Passwort
- Kryptografische Schlüssel oder Zertifikate
  z.B. PSK, X.509

## Virtuelle private Netzwerke

### Möglichkeiten der Realisierung

2. Integrität

- Hashfunktionen, z.B. md5, sha1

## Virtuelle private Netzwerke

### Möglichkeiten der Realisierung

3. Vertraulichkeit

- Verschlüsselung, z.B. 3DES, AES,RSA
- Kerckhoffs' Prinzip: Die Sicherheit rührt von der Geheimhaltung des Schlüssels, nicht von der des Algorithmus

## Virtuelle private Netzwerke

### Grundsätzliche Verfahren

1. Layer 2
   - IPsec, L2TP, PPTP
   - Auf Verbindungsschicht, IP-Ebene
   - Transparent, aber recht komplex

2. Layer 3
   - SSL-VPNs
   - Auf Transportschicht, TCP-/UDP-Ebene
   - Alle Anwendungsdaten werden in eine Verbindung getunnelt

# Geschafft ;-)