Netzwerktechnologien
3 VO

Univ.-Prof. Dr. Helmut Hlavacs
helmut.hlavacs@univie.ac.at

Dr. Ivan Gojmerac
gojmerac@ftw.at

Bachelorstudium Medieninformatik
SS 2012

Alles ist Vernetzt

- Weltweit Milliarden von vernetzten Terminals
- Internet:
  - globales Netzwerk
  - Eigentlich: eine Reihe von Protokollen
  - Verbinden von Netzwerken mit unterschiedlichen Technologien
    - Ethernet, Glasfaser, ADSL, Kabel, UMTS, LTE, Token Ring, MPLS, ATM, ...
- „Größte Maschine der Welt“
- Anwendungen hängen immer mehr davon ab
- Netzwerkausfall – was tun?

Transformation durch Vernetzung

- Traditionelle Sicht
  - Arbeitsplatzrechner, privater Rechner, Server
  - Lokal installierte Software
  - Wird über CD/DVDs installiert (Boxed, Retail Store)
- Heutige Sicht
  - Fixed und mobile Terminals (Phones, Pads, Netbooks, ...)
  - Appliances: digitaler Bilderrahmen, vernetzter Kühlschrank, Webcam, Sensoren, ...
  - Always On, mobile Dienste, location dependent, Ubiquitous Computing
  - Installation über das Netz (Appstore)
  - Remote Data, Remote Execution (Google Apps, Dropbox, Cloud Computing, Cloud Gaming)

Kapitel 1 – Computernetzwerke und das Internet

1.1 Was ist das Internet?
1.2 Der Netzwerkrand
1.3 Das Innere des Netzwerkes
1.4 Verzögerung, Verlust und Durchsatz in paketvermittelten Netzwerken
1.5 Protokollschichten und ihre Dienstmodelle
1.6 Sicherheit von Netzwerken
1.7 Geschichte der Computernetzwerke

1.1 Was ist das Internet ?

1.1.1 Technische Beschreibung:

- Millionen vernetzter Computer (genannt Hosts oder Endsysteme)
  - z.B.  PC  Server  Laptop  Smart-phone
- Verbunden durch Kommunikationsleitungen und Paket-Switches
  - z.B. Koaxial-, Glasfaserkabel, Kupferdrähte, Funk, Satellit

 Access Ponts —— Leitungen

- Übertragen Daten segmentiert in Form von Paketen (mit Header-Bytes)
  Wie Fahrzeuge in einem Autobahnnetz

1.1 Was ist das Internet?

- Endsysteme greifen über Internetdienstanbieter (*ISP – Internet Service Provider*) auf das Internet zu

- ISPs sind Netzwerke aus Paket-Switches und Kommunikationsleitungen

- Paket-Switches leiten Pakete weiter
  - Häufigste Typen im Internet: Router und Switches der Sicherungsschicht

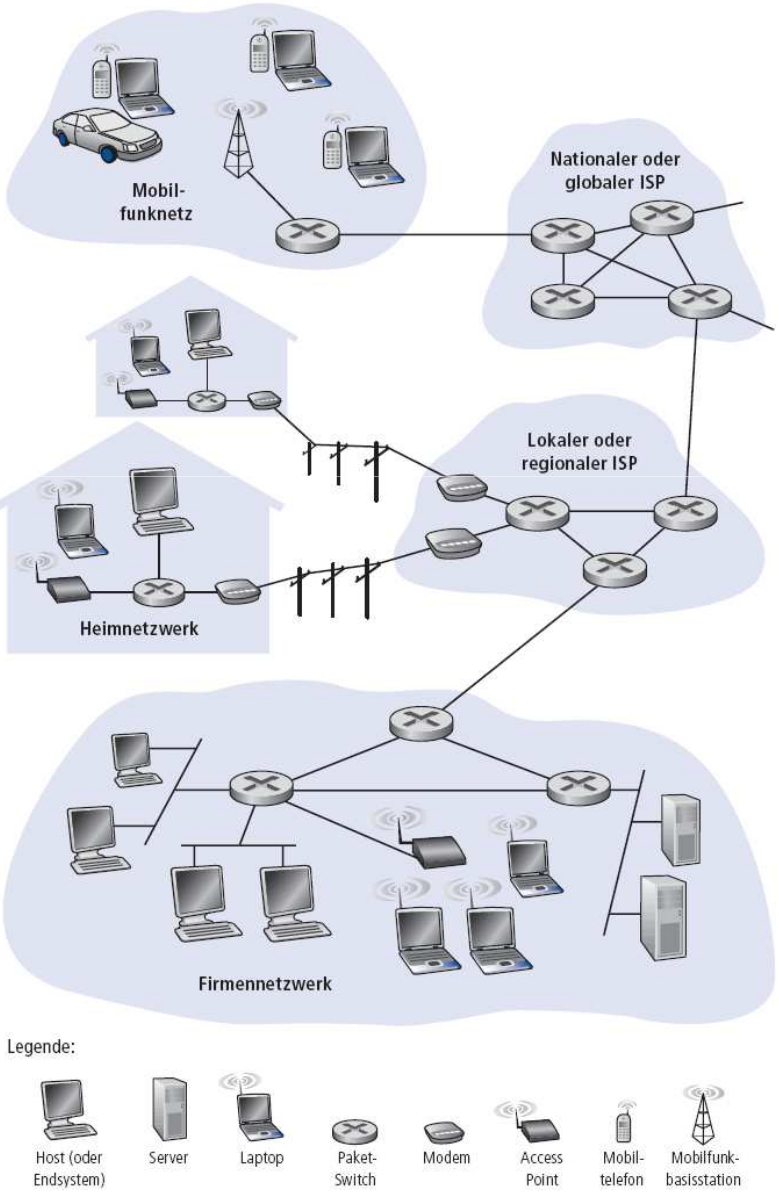
1.1 Was ist das Internet?

- „Netzwerk von Netzwerken“:

  Kleinere, lokale ISPs werden hierarchisch durch nationale und internationale ISPs miteinander verbunden

- Protokolle kontrollieren das Senden und Empfangen von Nachrichten
  - z.B., TCP, IP, HTTP, Skype, Ethernet Email, ...

- Internetstandards normieren Protokolle
  - Sie werden von der *Internet Engineering Task Force* (IETF) entwickelt
  - Die IETF-Normendokumente werden *Request for Comments* (RFC) genannt



1.1 Was ist das Internet?

1.1.2 Dienstbeschreibung:

- **Kommunikationsinfrastruktur**, die verteilte Anwendungen ermöglicht:
  - Web, VoIP, E-Mail, Spiele, eCommerce, File Sharing

- **Kommunikationsdienste**, die den Anwendungen zur Verfügung gestellt werden: Analogie zur Post
  - Unzuverlässige (“best effort”) Datenübertragung
  - Zuverlässige Datenübertragung von einer Quelle zu einem Ziel

- Programme nutzen APIs

1.1.3 Was ist ein Protokoll?

Protokolle zur Kommunikation zwischen Menschen:

- “Wie viel Uhr ist es?”
- “Ich habe eine Frage”
- Gegenseitiges Vorstellen

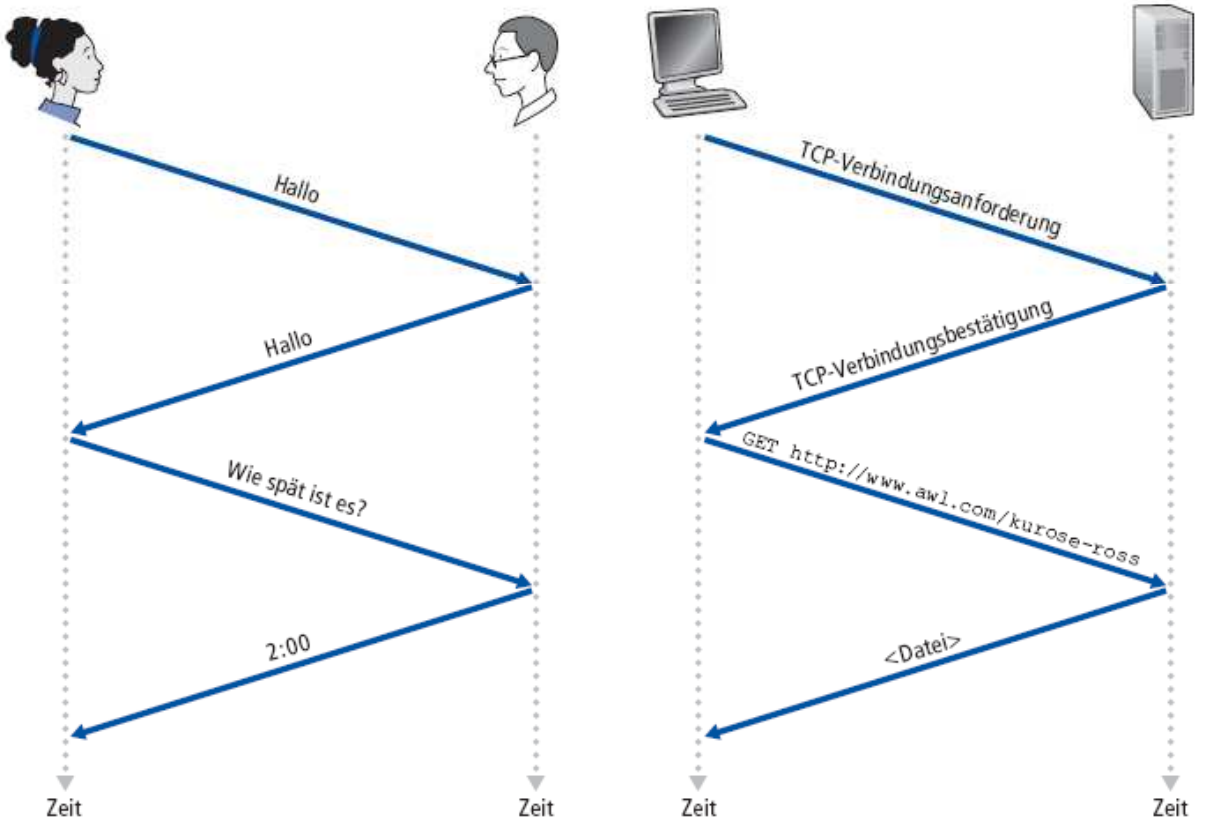
Netzwerkprotokolle:

- Maschinen statt Menschen
- Sämtliche Kommunikation im Internet wird durch Protokolle geregelt

→ Es werden „standardisierte“ Nachrichten übertragen
→ Durch den Empfang dieser Nachrichten werden „standardisierte“ Aktionen ausgelöst

*Protokolle definieren das **Format** und die **Reihenfolge**, in der **Nachrichten** von Systemen im Netzwerk gesendet und empfangen werden, sowie die **Aktionen**, welche durch diese Nachrichten ausgelöst werden.*

1.1.3 Was ist ein Protokoll?

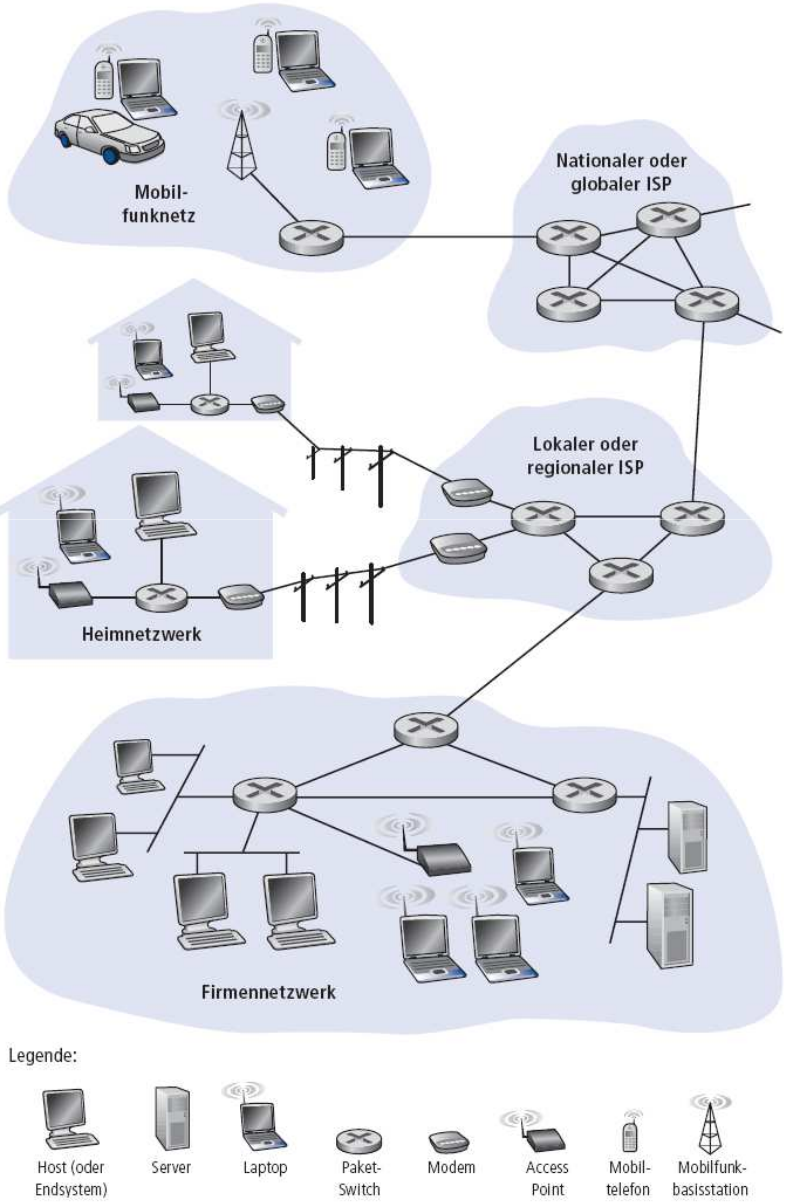


1.2 Der Netzwerkrand

- Den Netzwerkrand stellen je nach Zugangsnetz Endsysteme, Router und Accesspoints dar

1.2.2 Zugangsnetze

- *Heimzugänge* verbinden Endsysteme in einem privaten Haushalt mit dem Internet
- *Firmenzugänge* verbinden Endsysteme über ein lokales Netzwerk untereinander und mit einem Randrouter
- *Drahtlose Zugänge* verbinden (meist mobile) Endsysteme mit einer Basisstation



Maßeinheiten für die Datenrate

1 kbit/s = 1 kb/s = 1 kbps = 1.000 bit/s

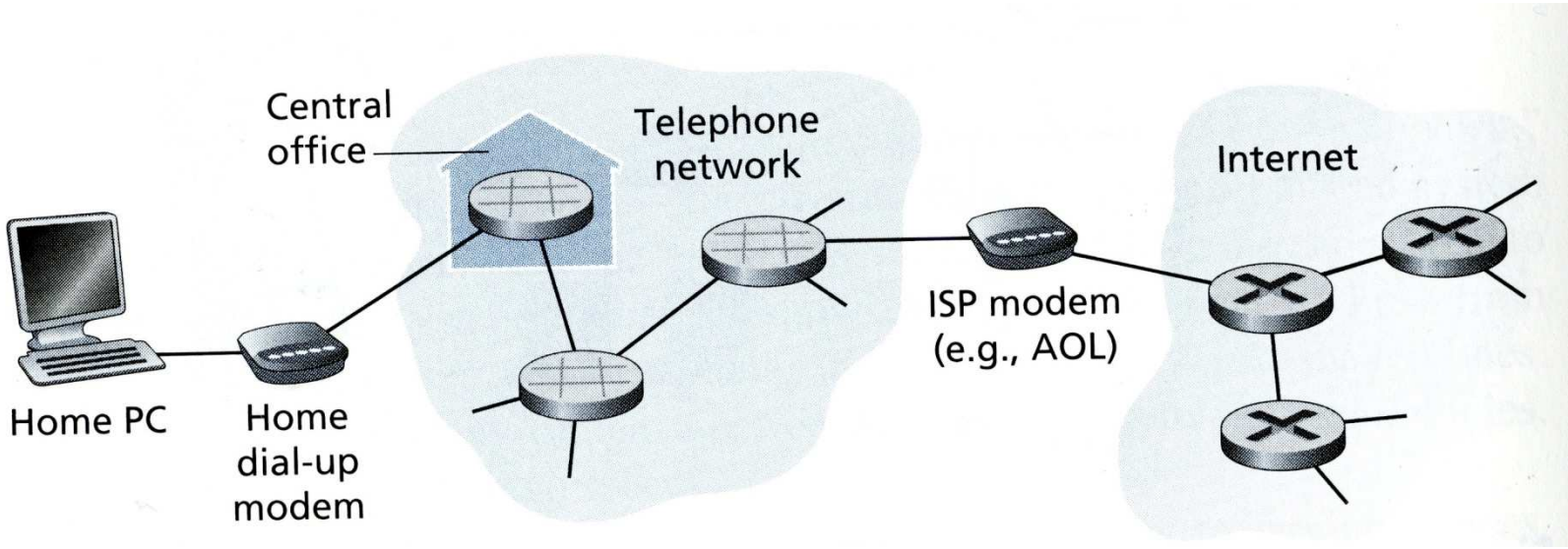
1 kBps = 8 kbps = 8000 bit/s

1 Mbit/s = 1 Mbps = 1.000.000 bit/s

1 Gbit/s = 1 Gbps = 1.000.000.000 bit/s

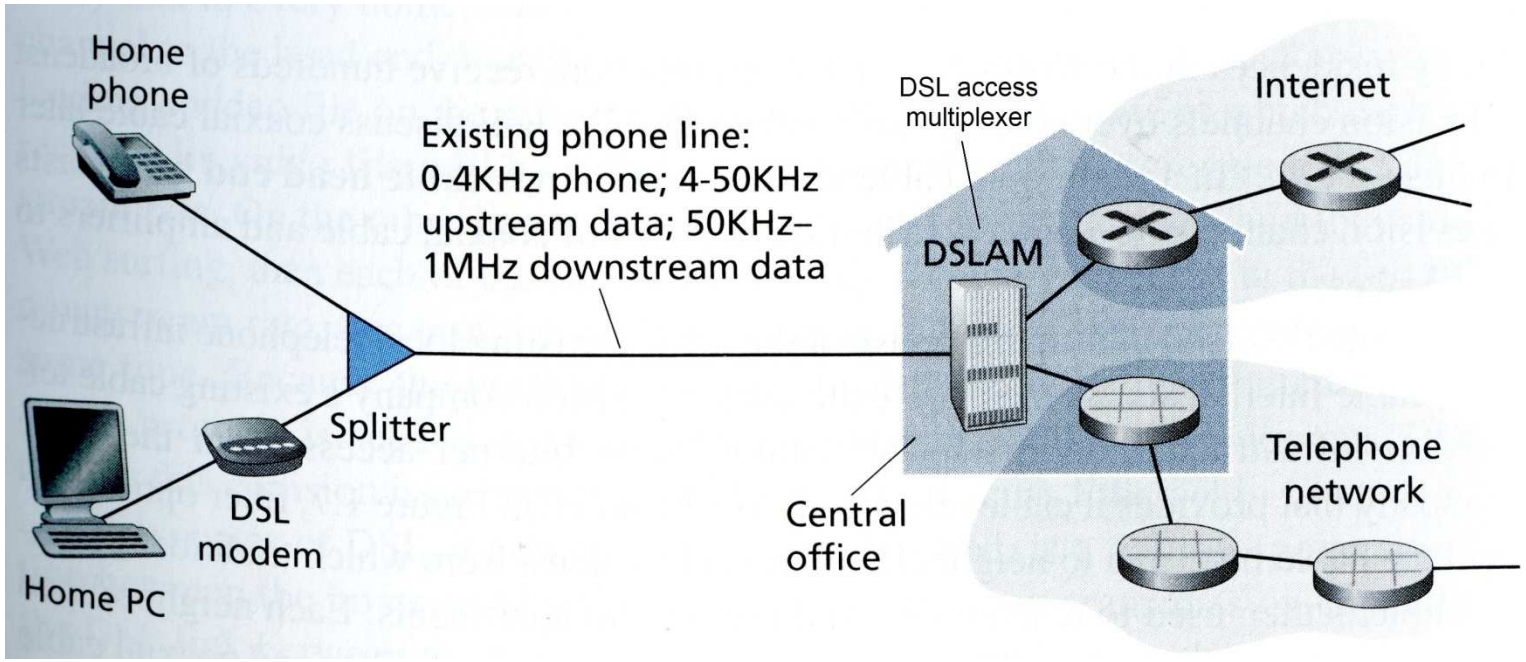
1.2.2 Zugangsnetze

Mögliche Verbindungsarten zum Netzwerk:



- Einwahlmodem
  - Verwendet Telefonleitungen
  - Bis zu 56 Kbps Übertragungsrate

1.2.2 DSL



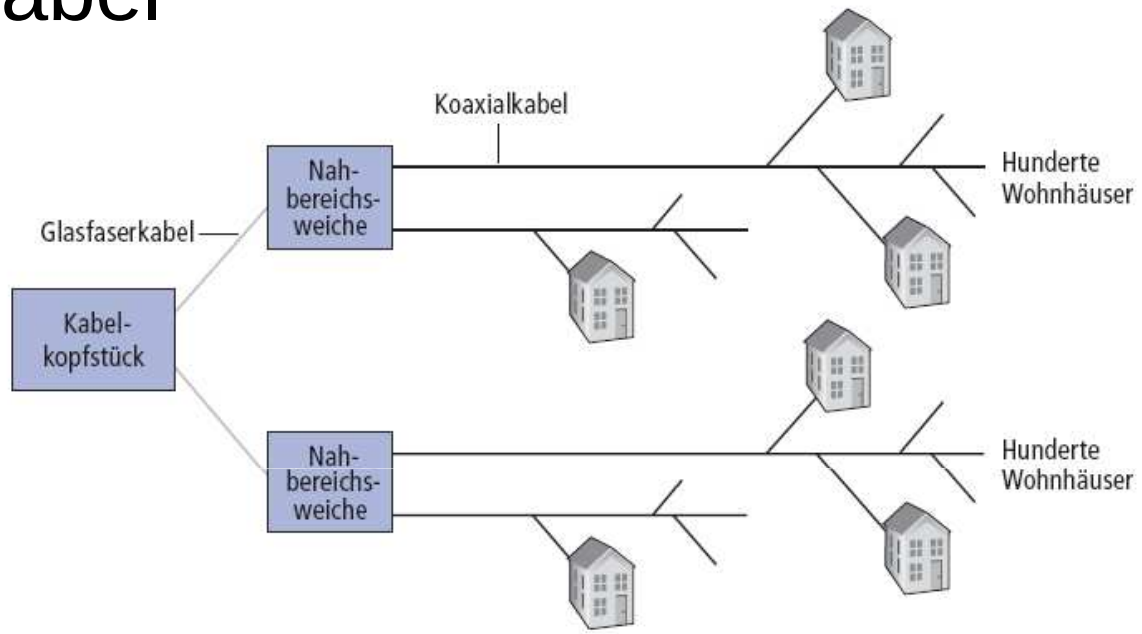
- Digital Subscriber Line (DSL)
  - Verwendet Telefonleitungen (Kupfer, twisted Pair)
  - Teilt Kommunikationsleitung in 3 Frequenzbänder: Telefon-, Up- und Downstream

1.2.2 DSL

- ADSL: Asymmetrische Übertragungsgeschwindigkeiten für Up- und Downstream (1:10)
- Ausschlaggebend für verfügbare Bandbreite:
  - Entfernung zur Vermittlungsstelle (Leitungsdämpfung)
  - Kabeldurchmesser
  - Übersprechen von Leitungen
- ADSL: 1.8 / 12 Mbit/s
- ADSL2/2+: 3 / 25 Mbit/s
- VDSL: 50 – 200 Mbit/s
- Zwangstrennung, dynamische IP

- Neue Technologien: Vectoring

1.2.2 Kabel



- Kabelverbindung (HFC - Hybrid Fiber-Coaxial-Cable)
  - Verwendet Kabelnetz
  - **Shared** Broadcast Medium: viele Haushalte sind an den selben Kabelkopf angeschlossen und teilen sich die Bandbreite
  - Teilt das Kommunikationsnetz in 2 Kanäle: Up- und Downstream-Kanal
  - Asymmetrische Übertragungsgeschwindigkeiten für Up- und Downstream (Downstream höher)

1.2.2 DSL vs. Kabel

- DSL PRO: Jeder Haushalt hat eine eigene Leitung zum Vermittlungsstelle
- DSL CON: Bandbreite durch Distanz limitiert

- Kabel PRO: Distanz zum Headend egal
- Kabel CON: Shared Medium (Dimensionierung wichtig)

1.2.2 FTTH

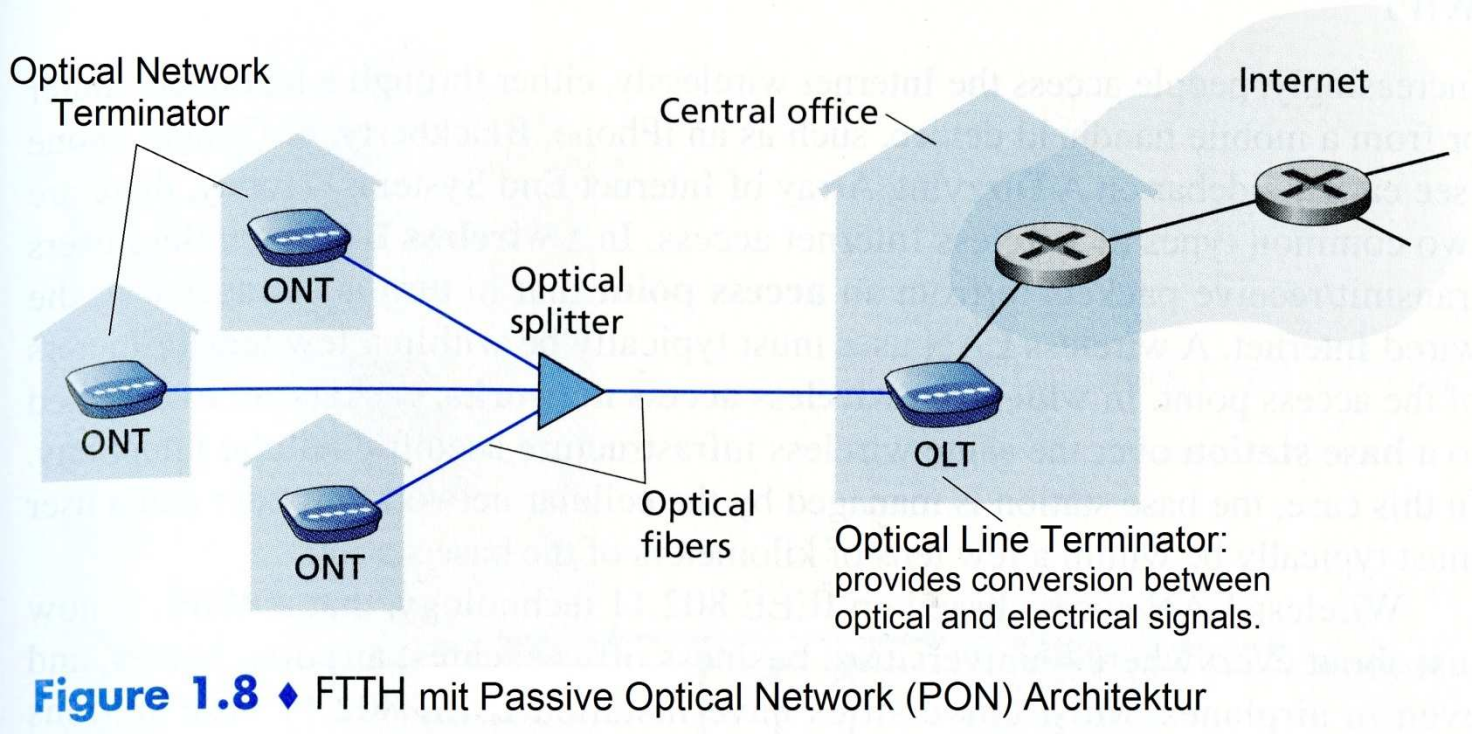
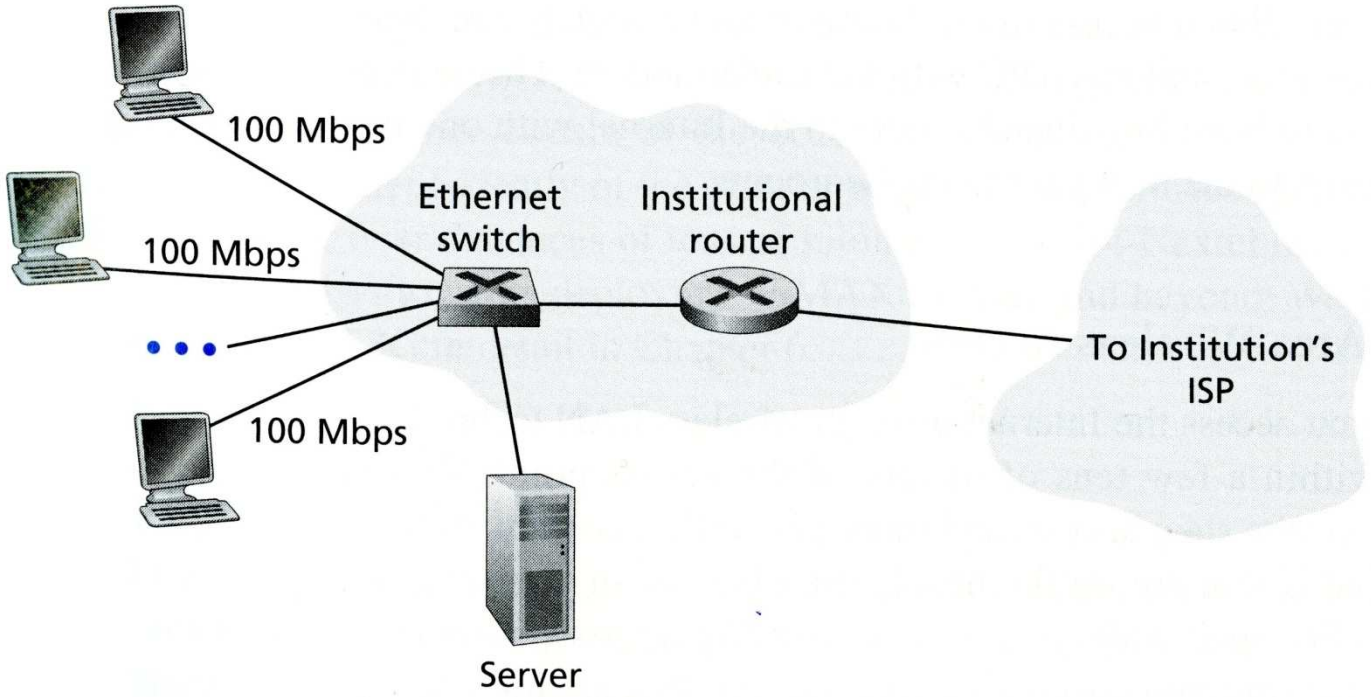


Figure 1.8 ♦ FTTH mit Passive Optical Network (PON) Architektur

- Fiber-To-The-Home (FTTH)
  - Verwendet Glasfaserkabel
  - Oft teilen sich mehrere Haushalte ein Kabel vom Central Office
  - Asymmetrische Übertragungsgeschwindigkeiten für Up- und Downstream (Downstream höher)

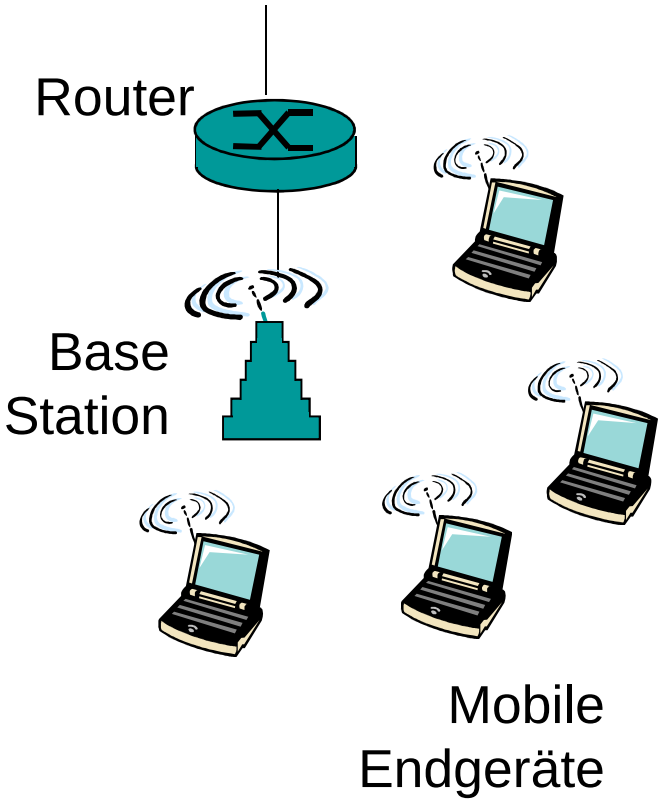
1.2.2 Firmenzugang



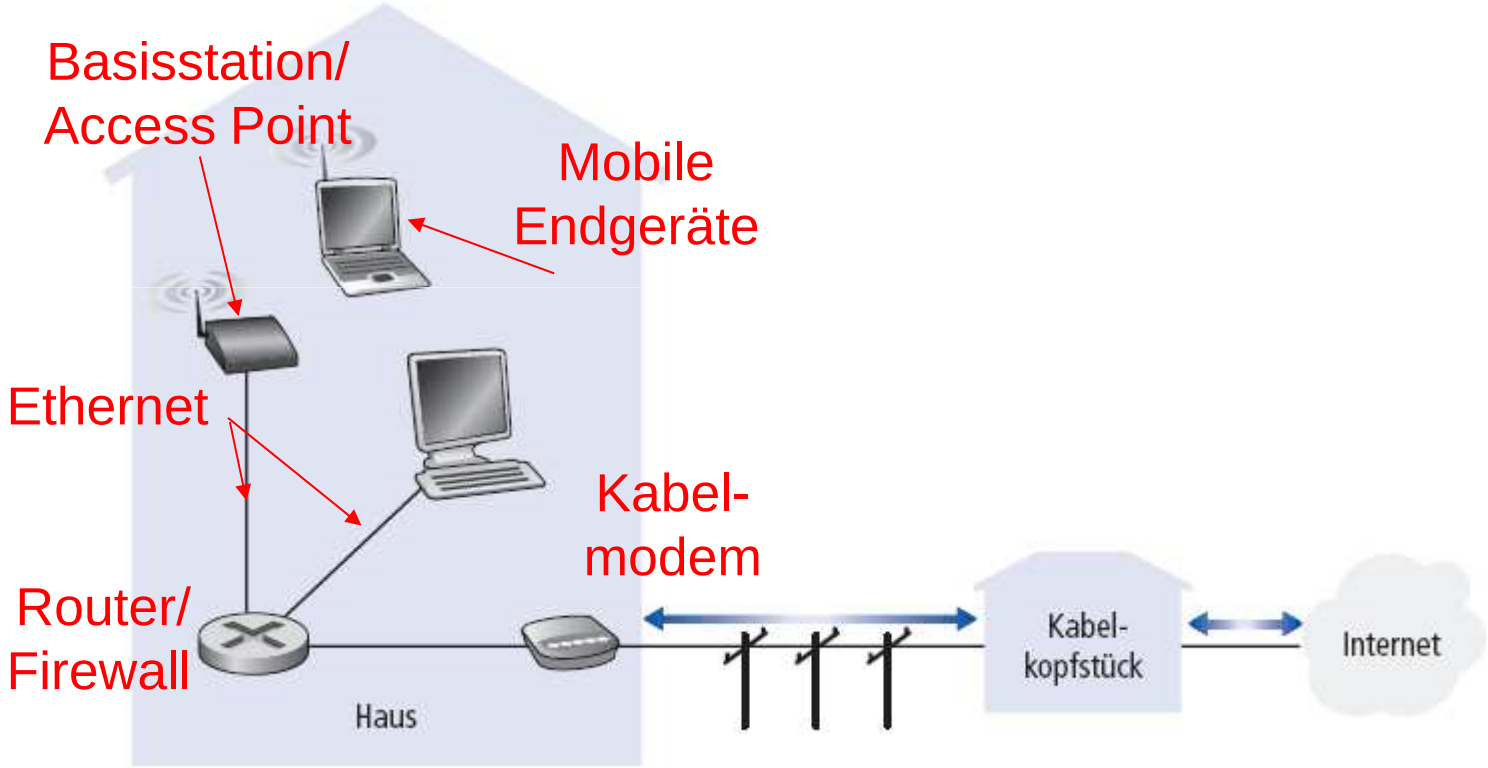
- Ethernet
  - Verwendet Twisted Pair Kupferkabel
  - 100 Mbit/s, 1 Gbit/s, 10 Gbit/s
  - Wird oft für das LAN auf Firmen- und Universitätsgeländen verwendet

1.2.2 Drahtlose Zugangsnetze

- Drahtlose Zugangsnetzwerke verbinden Endsysteme mit einem Router
  - Über eine Basisstation (auch „Access Point“)
- Wireless LANs: 802.11b/g (WiFi): 11/54 Mbit/s
- Drahtlose Weitverkehrsnetze
  - Durch Serviceprovider (z.B. A1, 3,) bereitgestellt
  - ~1 Mbit/s in zellulären Systemen (EVDO, HSDPA)
- In Zukunft:
  - WiMAX (mehrere 10 Mbit/s) im Weitverkehrsbereich (?)
  - Long Term Evolution (4G)



1.2.2 Heimnetzwerke



1.2.2 Ländliche Gegenden

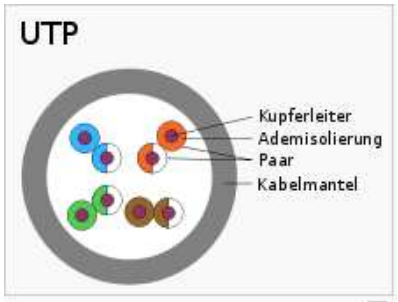
- Vergraben von Leitungen extrem teuer
- Entweder ADSL (lange Distanzen!)
- UMTS / LTE (?)
- WiMAX
- Satellit (Latenzzeit ˜250ms)

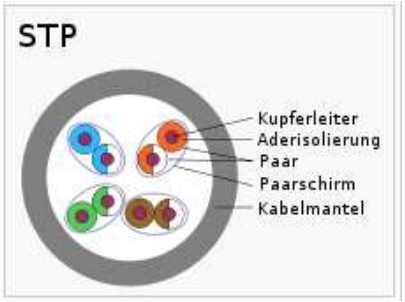
1.2.3 Trägermedien

- Geführte Medien: Signale breiten sich in festen Medien in eine Richtung aus
  - z.B. Kupfer-, Glasfaser-, Koaxialkabel
- Nichtgeführte Medien: Signale breiten sich frei aus
  - z.B. Funk, Mikrowellen

Twisted Pair (TP)

- Paarweise verdrillter isolierter Kupferdraht
  - TP Kategorie 3: Telefonkabel, 10 Mbit/s Ethernet
  - TP Kategorie 5: 100 Mbit/s Ethernet





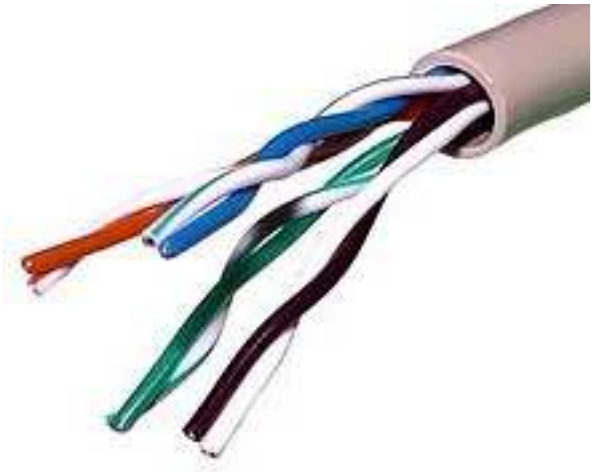
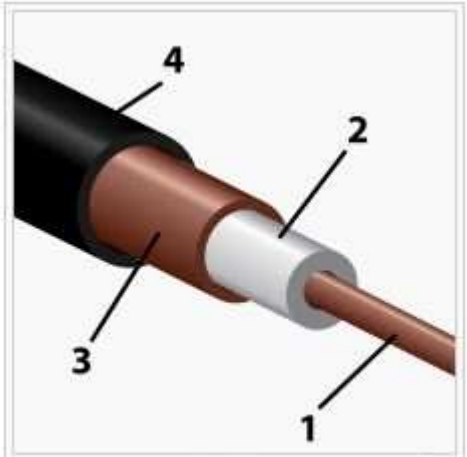


Bild von http://en.wikipedia.org /wiki/Twisted_pair am 26.02.2012.

1.2.3 Trägermedien



Koaxialkabel Schnittmodell:
1. Seele oder Innenleiter
2. Isolation oder Dielektrikum zwischen Innenleiter und Kabelschirm
3. Außenleiter und Abschirmung
4. Schutzmantel

Bild von http://de.wikipedia.org/wiki/Koaxialkabel am 26.02.2012

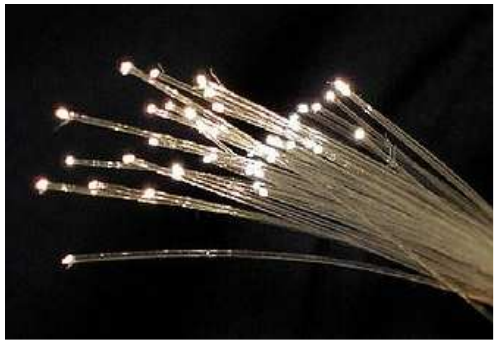
Koaxialkabel:

- Zwei konzentrisch angeordnete Kupferleiter (Innen- und Außenleiter)
- Bidirektional

Glasfaserkabel:

- Glasfaserkabel übertragen Lichtpulse, jeder Puls ist ein Bit
- Hohe Geschwindigkeit:
  - Üblicherweise zwischen 51,8 Mbps und 39,8 Gbps
- Unempfindlich gegen elektromagnetische Strahlung
- Auf Längen bis zu 100 km sehr niedrige Signalverluste
- Sind sehr schwer abzuhören

Bild von http://de.wikipedia.org/wiki/Glasfaserkabel am 26.02.2012



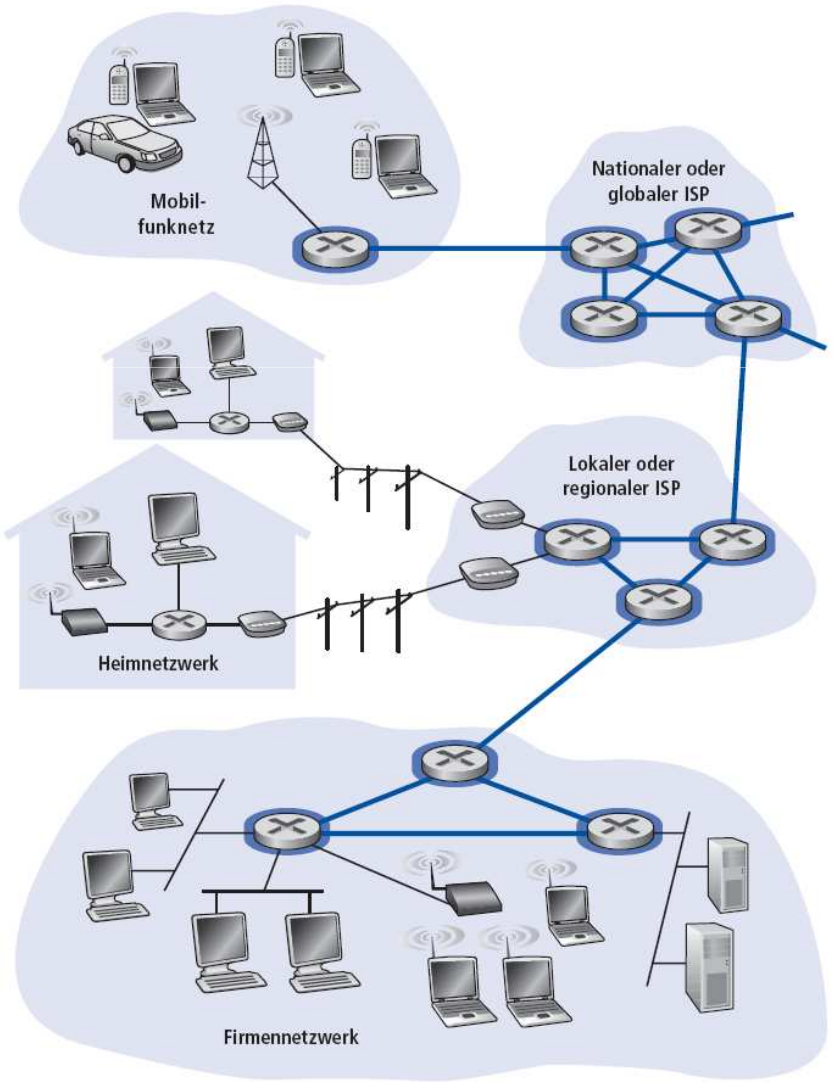
1.2.3 Trägermedien

Funk:

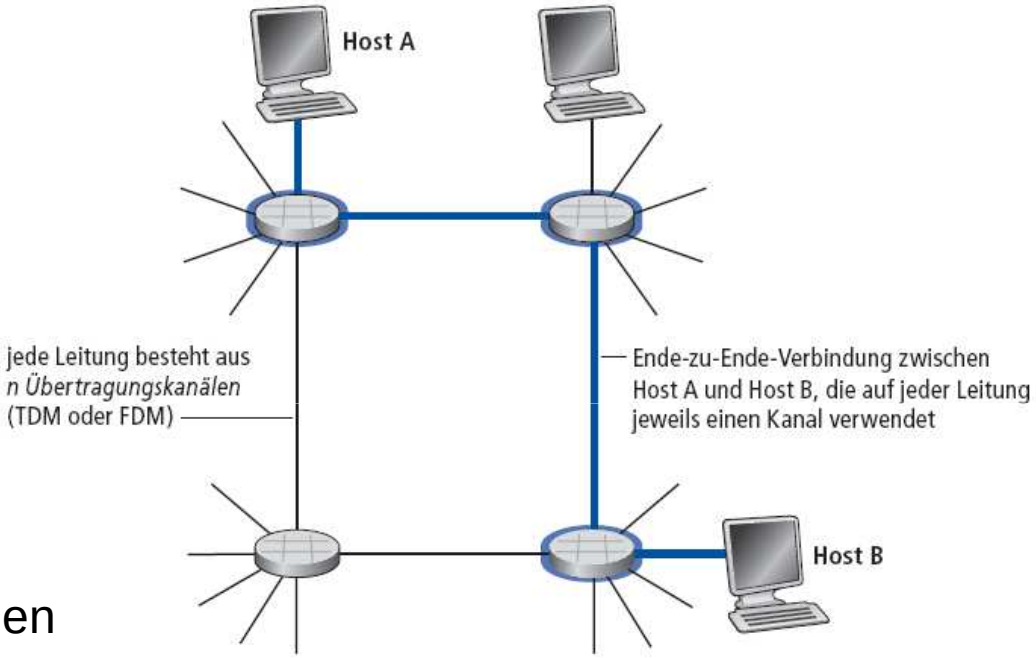
- Signal wird von elektromagnetischen Wellen übertragen
- Kein „Draht“, deswegen drahtlose Kommunikation
- Bidirektional
- EW sind ein shared Medium! (Aktuell: „Spin“ ermöglicht theoretisch unendlich viel Bandbreite)
- Unterschiede in der Reichweite (WLAN vs. UMTS)
- Signalausbreitung wird von der Umgebung beeinflusst:
  - Reflexion
  - Abschattung durch Hindernisse
  - Interferenz

1.3 Das Innere des Netzwerkes

- Viele, untereinander verbundene Router
- Die zentrale Frage: Wie werden Daten durch das Netzwerk geleitet?
  - **Leitungsvermittlung**: eine dedizierte Leitung wird für jeden Ruf geschaltet →Telefonnetz
  - **Paketvermittlung**: Daten werden in diskreten Einheiten durch das Netzwerk geleitet →Internet



1.3 Das Innere des Netzwerkes



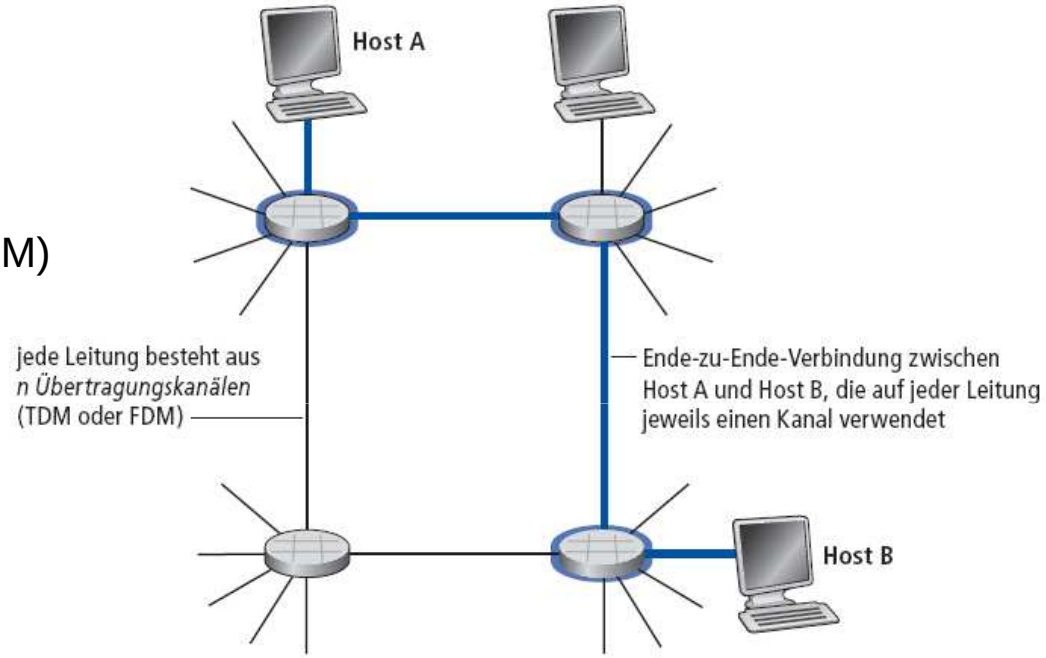
Leitungsvermittlung:

- Ende-zu-Ende-Ressourcen werden für einen Ruf reserviert:
  - Bandbreite auf Leitungen, Kapazität in Routern
  - Dedizierte Ressourcen: keine gemeinsame Nutzung
  - Garantierte Dienstgüte wie beim “Durchschalten” einer physikalischen Verbindung
  - Vor dem Austausch von Daten müssen die notwendigen Ressourcen reserviert werden

1.3 Das Innere des Netzwerkes

Wie teilt man die Bandbreite einer Leitung in Einheiten auf?

- *Frequenzmultiplex*
  (Frequency Division Multiplex,FDM)
- *Zeitmultiplex*
  (Time Division Multiplex, TDM)



Leitungsvermittlung:

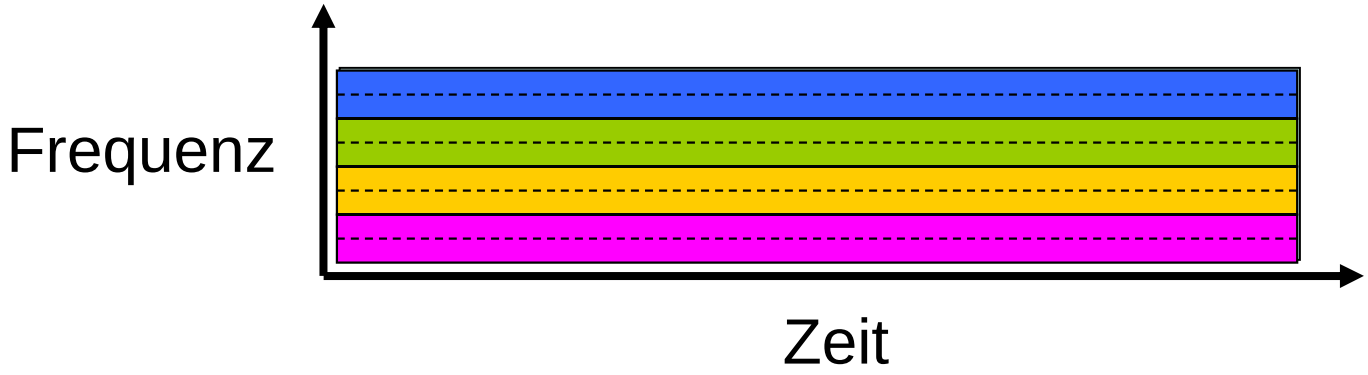
- Netzwerkressourcen (z.B. Bandbreite) werden in Einheiten (Kanäle) aufgeteilt
  - Kanäle werden Rufen (Calls) zugewiesen
  - Problem: **Kanäle bleiben ungenutzt**, wenn sie von ihrem Call nicht verwendet werden *(keine gemeinsame Nutzung von Ressourcen)*

1.3.1 FDM und TDM

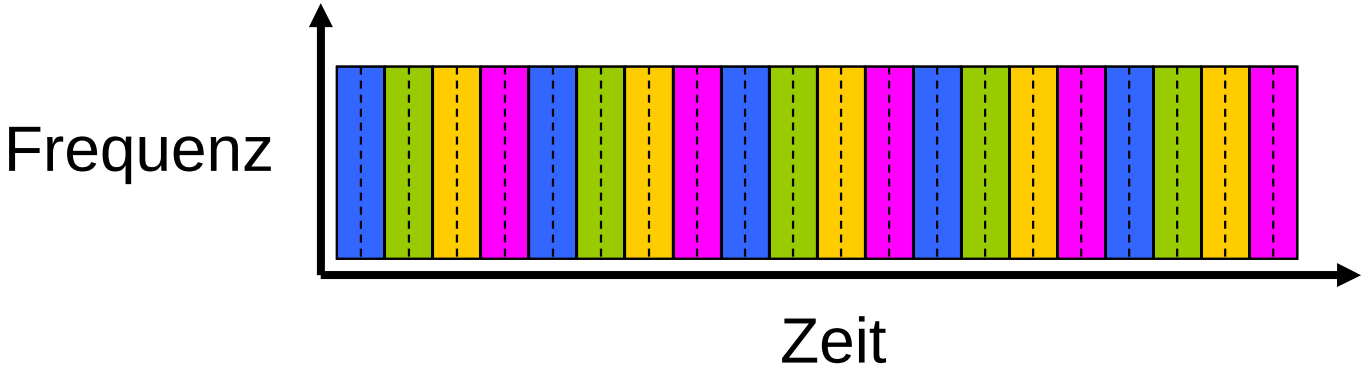
Beispiel:

4 Nutzer 

FDM



TDM



1.3.1 Ein Beispiel

- Wie lange dauert es, eine Datei mit 640.000 Bit von A nach B über ein leitungsvermitteltes Netzwerk zu übertragen?
- Alle Leitungen haben eine Bandbreite von 1.536 Mbit/s
- Alle Leitungen nutzen TDM mit 24 Zeitschlitzen/Sekunde
- 500 ms werden benötigt, um die Ende-zu-Ende-Leitung zu schalten

Antwort:

- 1.536.000 Bit/s / 24 = 64.000 Bit/s
- 640.000 Bit / 64.000 Bit/s = 10 s

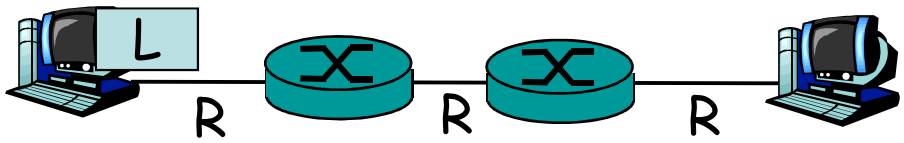
- Übertragungszeit = 10 + 0,5 = 10,5 s

1.3.1 Paketvermittlung

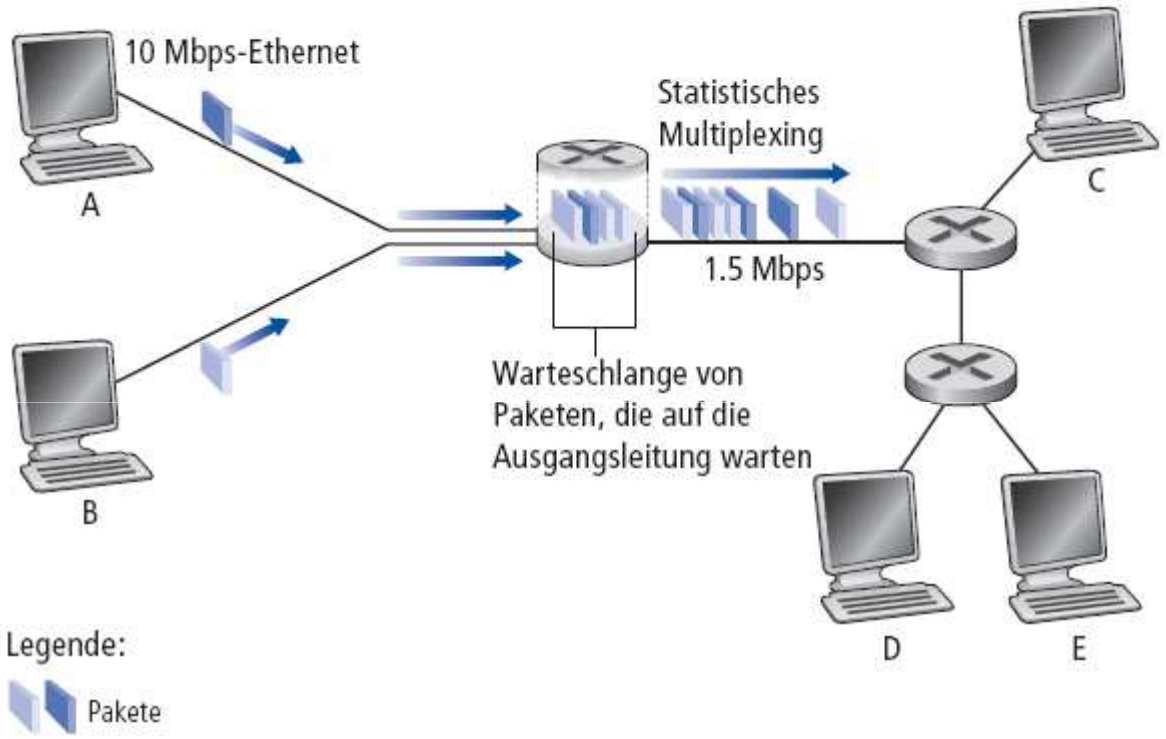
Paketvermittlung:

- Jeder Ende-zu-Ende-Datenstrom wird in Pakete aufgeteilt
  - Die Pakete aller Nutzer teilen sich die Netzwerkressourcen
  - Paket-Switches (Switches, Router) leiten die Pakete zum Ziel
- Store and Forward
  - Beispiel: Paket hat Länge L
  - Muss Q Leitungen überqueren
  - Jede Leitung hat Bandbreite R

  - Übertragungszeit (mindestens!) = L/R + L/R + ... + L/R = Q L /R



1.3.1 Wettbewerb um Ressourcen



Wettbewerb um Ressourcen:

- Die Nachfrage nach Ressourcen kann das Angebot übersteigen
- Überlast: Pakete werden zwischengespeichert (Puffer) und warten darauf, eine Leitung benutzen zu können

1.3.1 Statistisches Multiplexing

Die Folge von Paketen auf der Leitung hat kein festes Muster,
die Bandbreite wird nach Bedarf verteilt ➔ ***statistisches Multiplexing***

(Vergleiche TDM: Jede Verbindung erhält immer den gleichen Zeitrahmen in einem sich wiederholenden Muster)

1.3.1 Paketvermittlung VS. Leitungsvermittlung

Ist Paketvermittlung grundsätzlich besser?

- Sehr gut für unregelmäßigen Verkehr (bursty traffic)
  - Gemeinsame Verwendung von Ressourcen, bessere Auslastung
  - Keine Verschwendung von ungenutzten Ressourcen
  - Einfacher, keine Reservierungen
- Problem Überlast: Verzögerung und Verlust von Paketen
  - Protokolle für zuverlässigen Datentransfer und Überlastkontrolle werden benötigt
- Frage: Wie kann man leitungsähnliches Verhalten bereitstellen?
  - Bandbreitengarantien werden gebraucht für Audio- und Videoanwendungen
  - -> Quality of Service

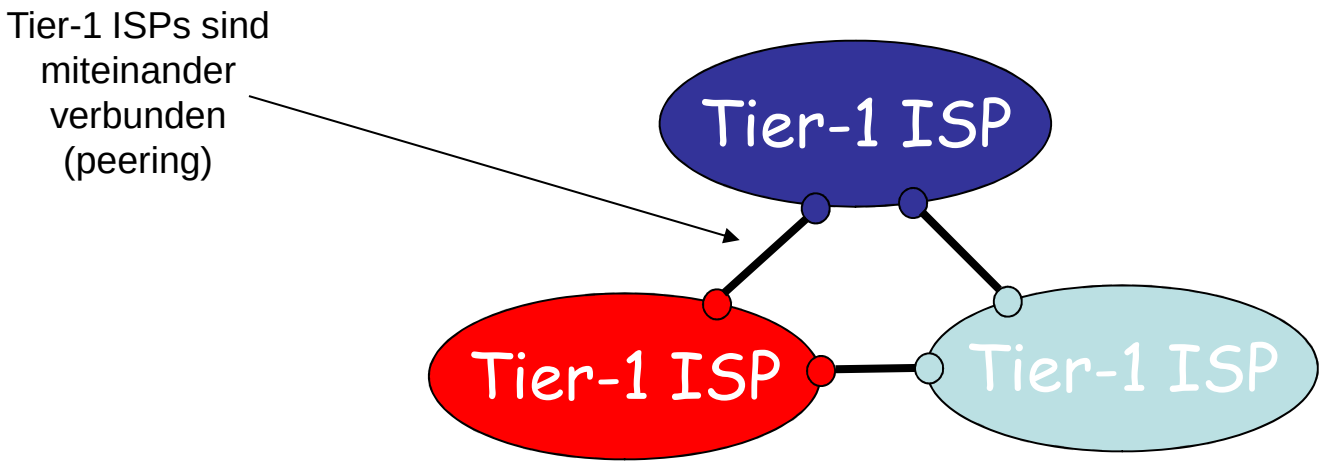
1.3.2 Wie gelangen Pakete zum Ziel?

1. Sender schreibt Zieladresse in den Paket-Header
2. Schickt es an den ersten Router
3. Router besitzt Weiterleitungstabellen
4. Lookup in der Tabelle
5. Wählt nächsten Router aus
6. Bis Paket beim Zielhost ankommt

Frage: wie werden diese Weiterleitungstabellen erstellt? (-> Kapitel 4)

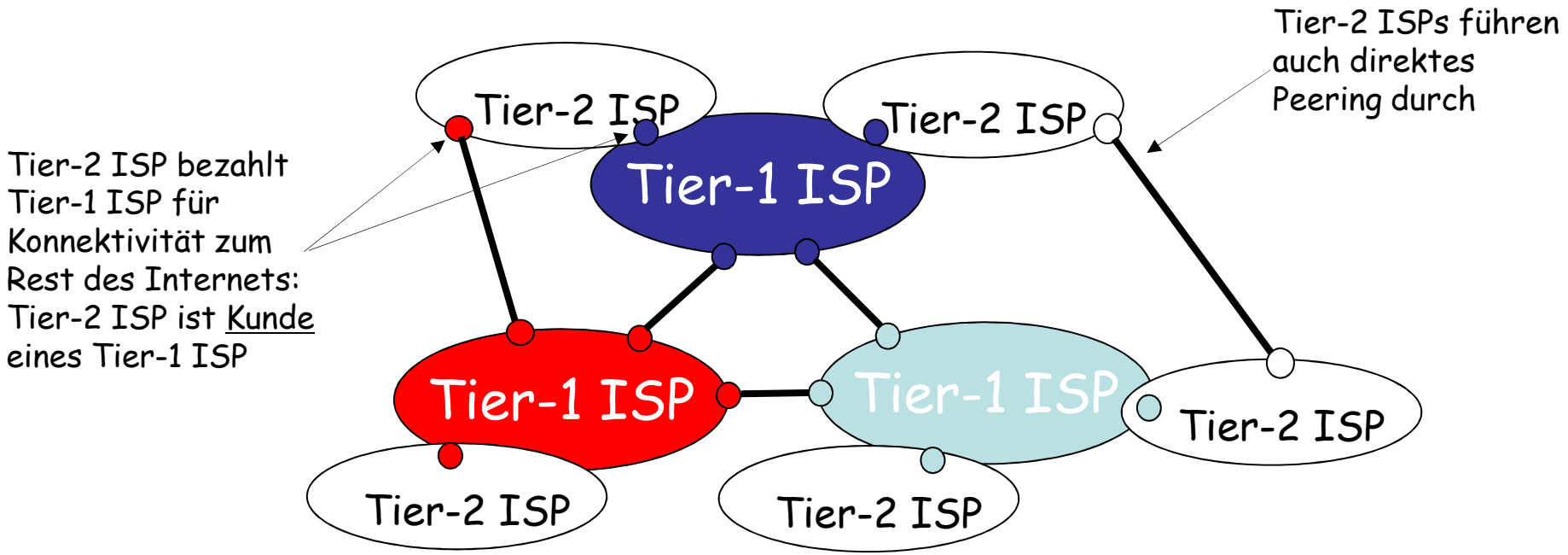
1.3.3 ISPs und Internet-Backbones

- Internet als „Netzwerk von Netzwerken“
- Grob hierarchisch
- Im Zentrum: “Tier-1” Internet Service Providers (ISPs)
  - „Internet Backbones“
  - Behandeln sich als gleichberechtigte Partner
  - Sind vollständig miteinander verbunden, sind mit vielen Tier-2 Netzen verbunden
  - Leitungen: 622 Mbps – 10 Gbps
  - Sprint, Verizon, Quest, AT&T, Level3, ...



1.3.3 ISPs und Internet-Backbones

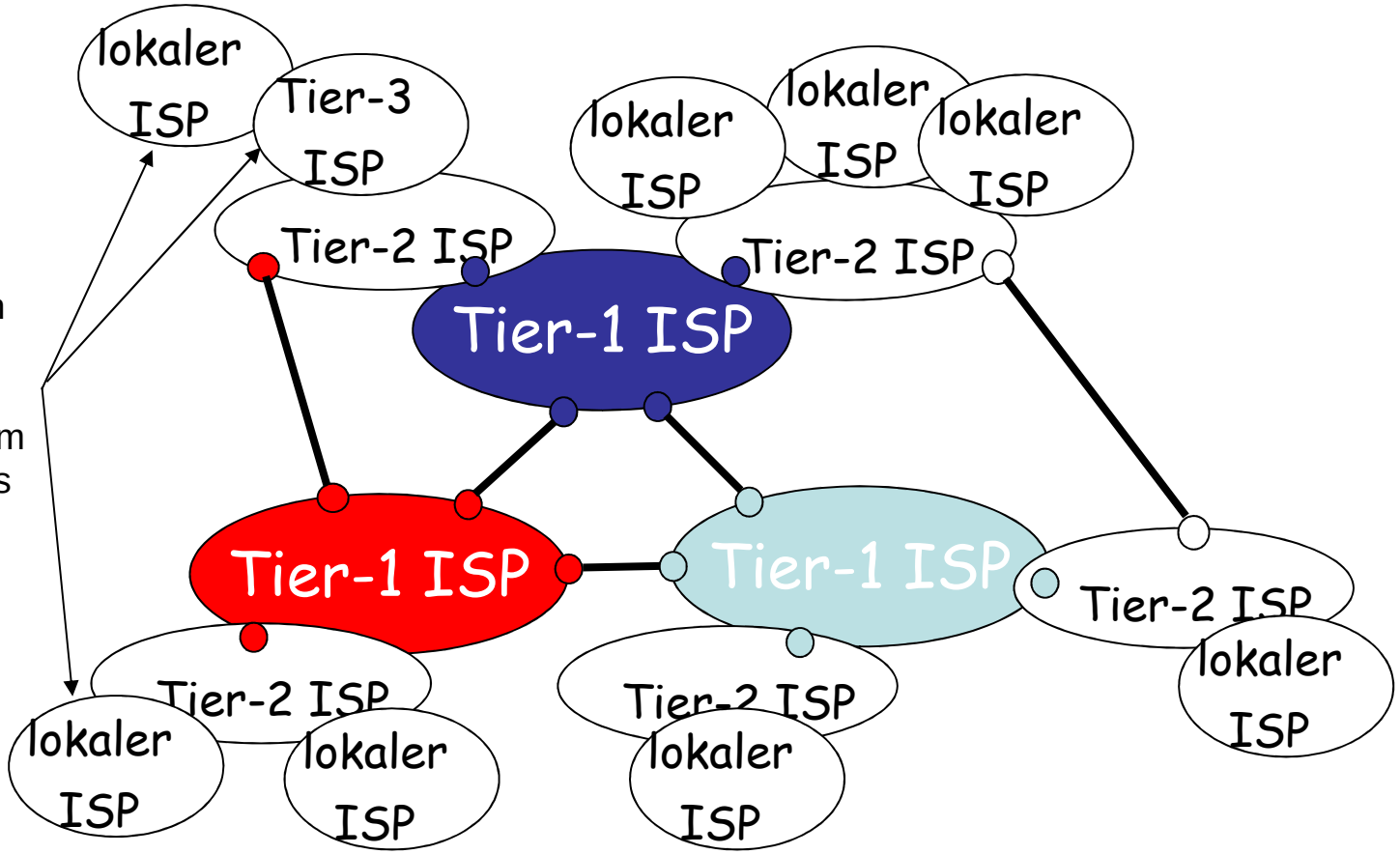
- "Tier-2" ISPs: kleinere, oft nationale oder regionale ISPs
  - Sind mit einem / mehreren Tier-1 ISPs verbunden, oft auch mit anderen Tier-2 ISPs
  - Sind **Kunden** von Tier-1 Netzen (zahlen für Leitung und Upstream Verkehr)
  - Manche Tier-2 ISPs sind auch Tier-1 ISPs (vertikale Integration)



1.3.3 ISPs und Internet-Backbones

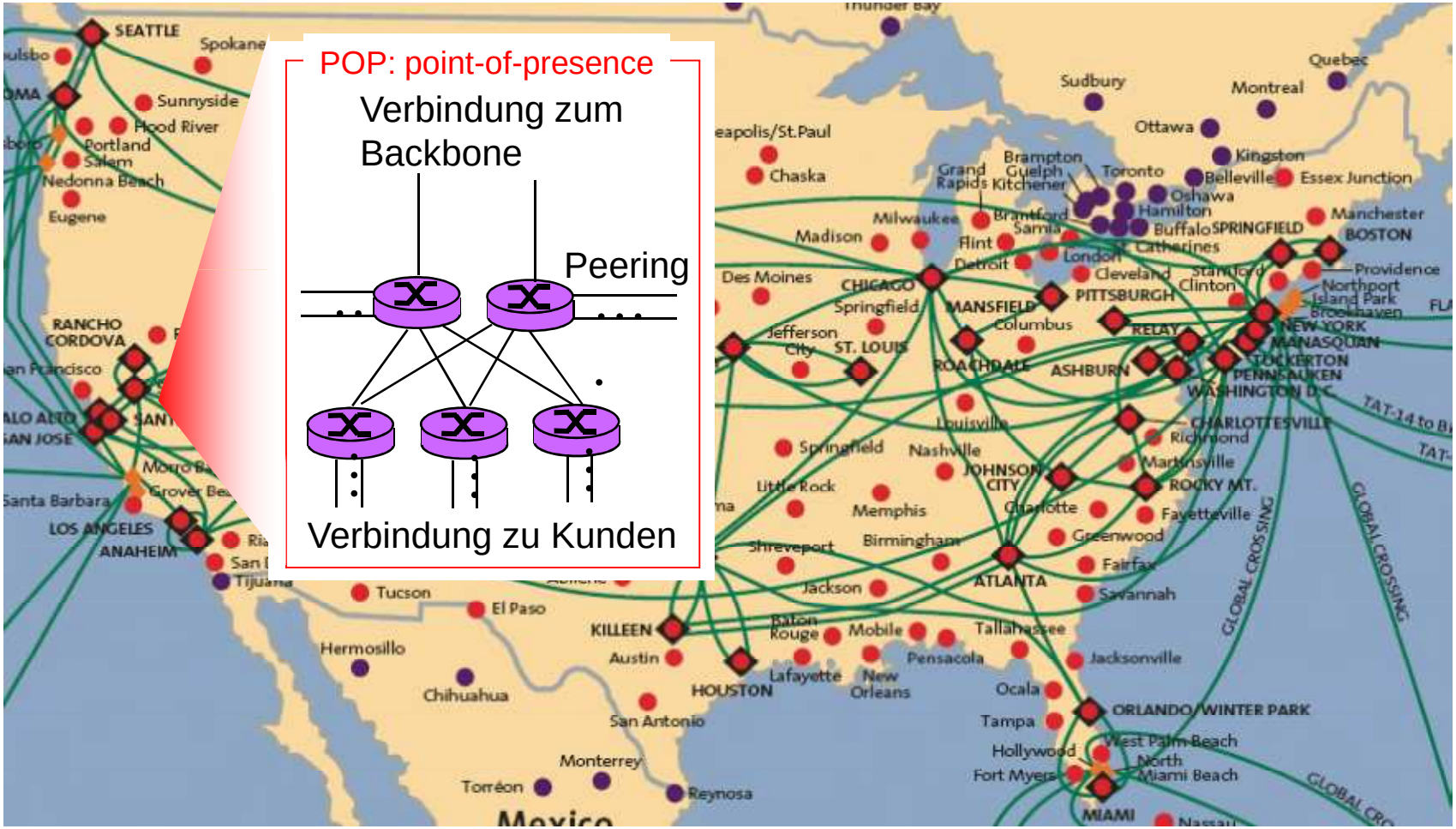
- "Tier-3" ISPs und lokale ISPs
  - Zugangsnetzwerke (last hop, access network)

Lokale und Tier-3 ISPs sind Kunden von Tier-1 und Tier-2 ISPs, welche sie mit dem Rest des Internets verbinden



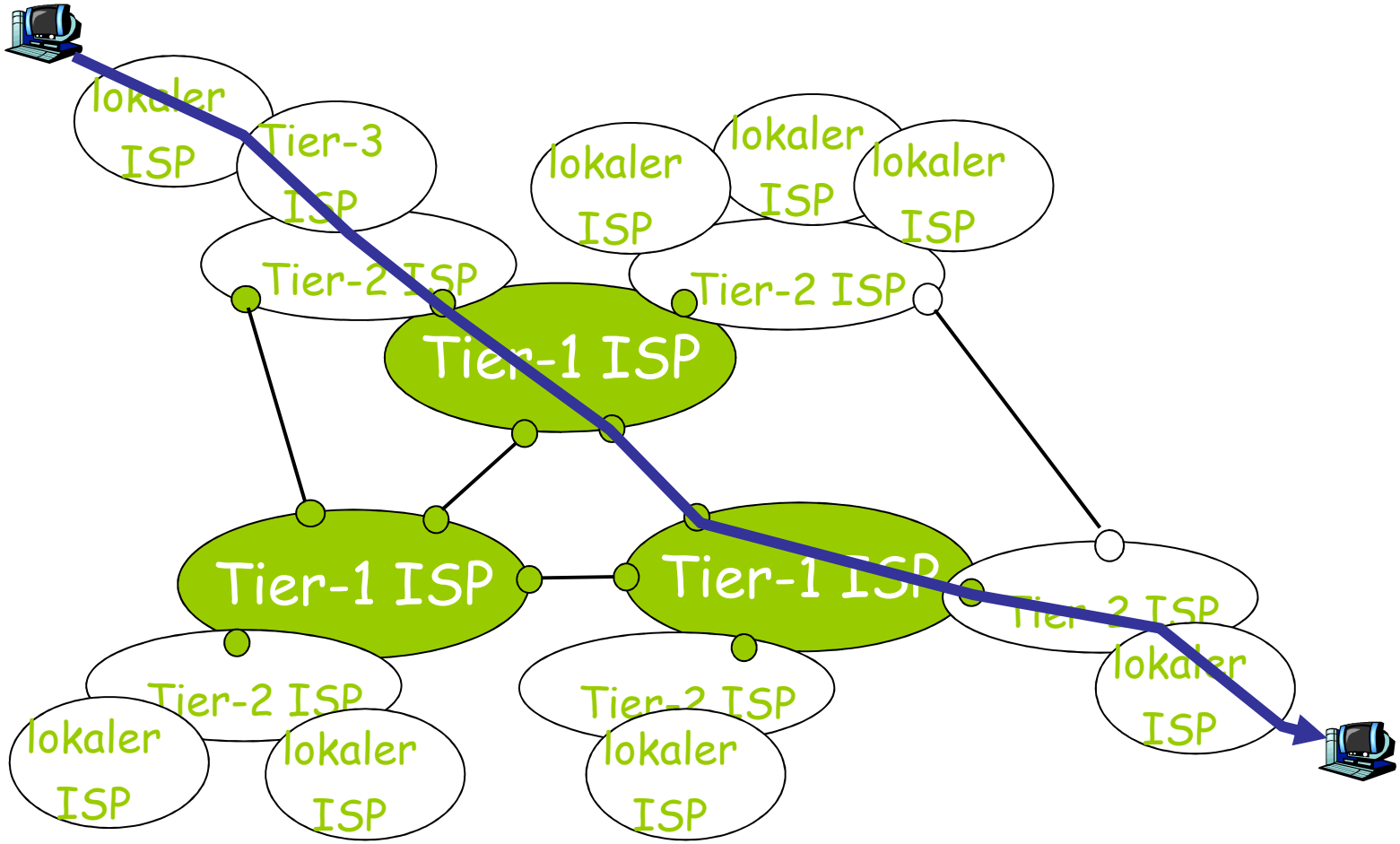
1.3.3 Point of Presence (POP)

- Ort an dem Router aufgestellt sind

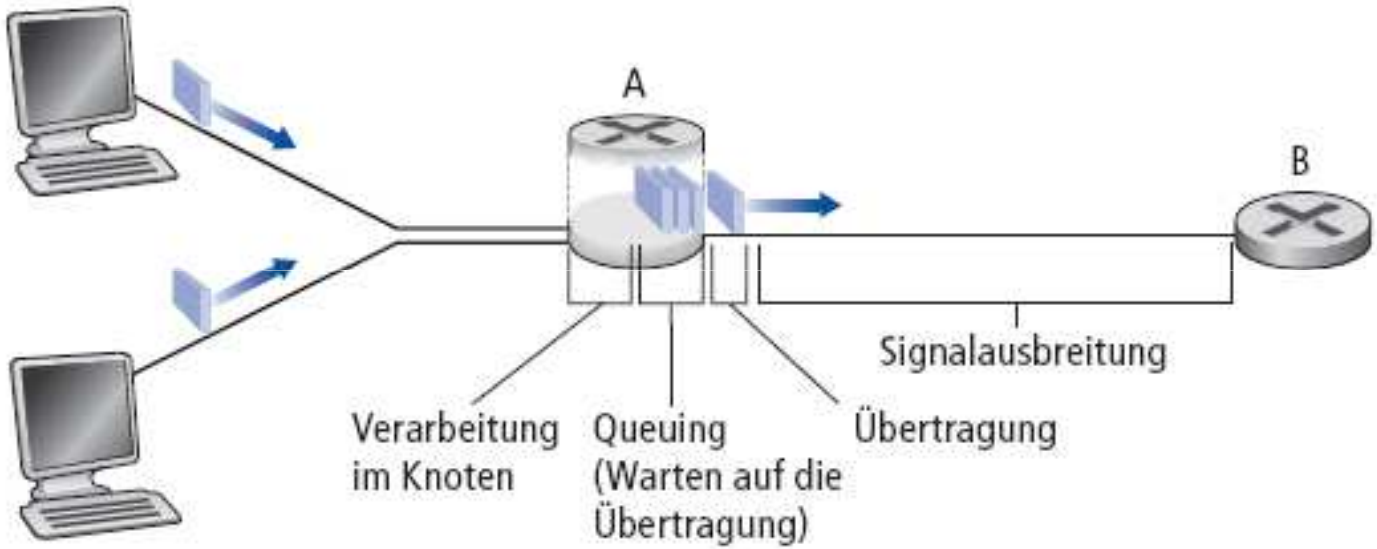


1.3.3 ISPs und Internet-Backbones

- Ein Paket durchquert viele Netzwerke!



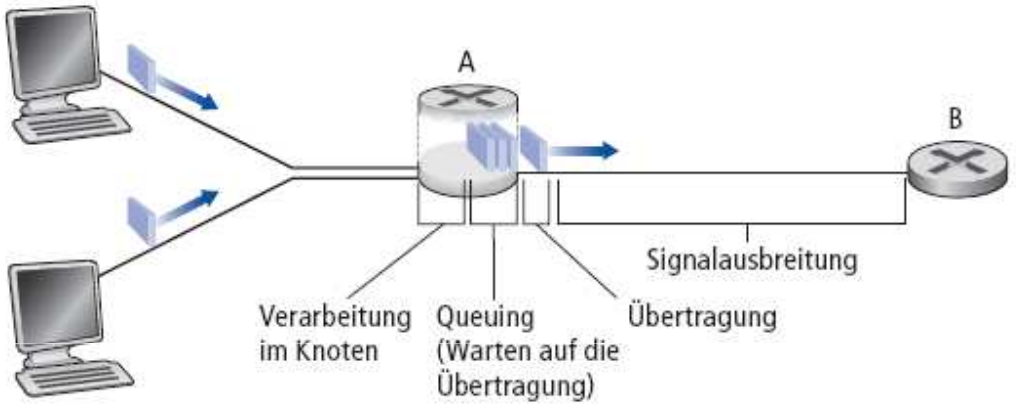
1.4 Verzögerung, Verlust und Durchsatz in paketvermittelten Netzen



Wie entstehen Paketverluste und Verzögerungen?
→Pakete warten in den Puffern von Routern wenn die Ankunftsrate die Kapazität der Ausgangsleitungen übersteigt.

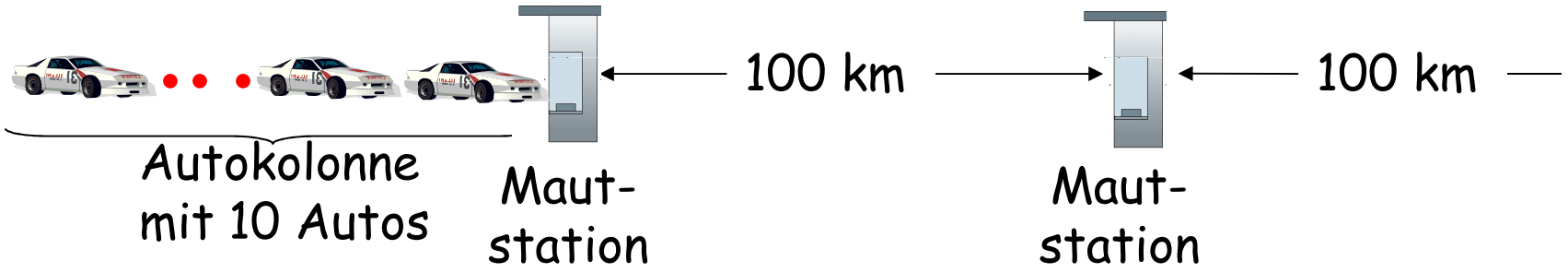
→ Ist die Warteschlange vor einer Leitung voll löscht der Router ankommende Pakete (da er keinen Platz hat um sie zu speichern), d.h. sie gehen verloren.

1.4.1 Arten der Verzögerung



1. Verarbeitung im Knoten:
   - Auf Bitfehler prüfen
   - Wahl der ausgehenden Leitung
2. Warten auf die Übertragung:
   - Wartezeit, bis das Paket auf die Ausgangsleitung gelegt werden kann
   - Hängt von der Last auf der Ausgangsleitung ab
3. Übertragungsverzögerung:
   - Wenn R = Bandbreite einer Leitung (Bit/s) und L = Paketgröße (Bit), dann ist die Übertragungsverzögerung = L/R
4. Ausbreitungsverzögerung:
   - Wenn d = Länge der Leitung und s = Ausbreitungsgeschwindigkeit des Mediums (~$2x10^8$ m/s), dann ist die Ausbreitungsverzögerung = d/s

1.4.1 Verhalten wie auf einer Autobahn



1.4.1 Verzögerung, Verlust und Durchsatz in paketvermittelten Netzen

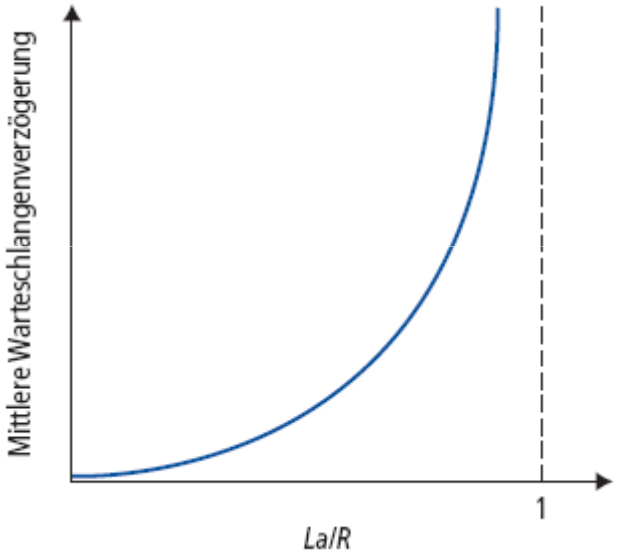
Gesamtverzögerung:

$$d_{\text{gesamt}} = d_{\text{Verarbeitung}} + d_{\text{Warten}} + d_{\text{Übertragung}} + d_{\text{Ausbreitung}}$$

- $d_{\text{Verarbeitung}}$ = Verarbeitungsverzögerung
  - Üblicherweise wenige Mikrosekunden oder weniger
- d_{Warten} = Wartezeit in Puffern
  - Abhängig von der aktuellen Überlastsituation
- $d_{\text{Übertragung}}$ = Übertragungsverzögerung
  - = L/R, signifikant wenn R klein ist
- $d_{\text{Ausbreitung}}$ = Ausbreitungsverzögerung
  - Wenige Mikrosekunden bis einige hundert Millisekunden

1.4.2 Warteschlangenverzögerung

- R = Bandbreite (Bit/s)
- L = Paketgröße (Bit)
- a = durchschnittliche Paketankunftsrate

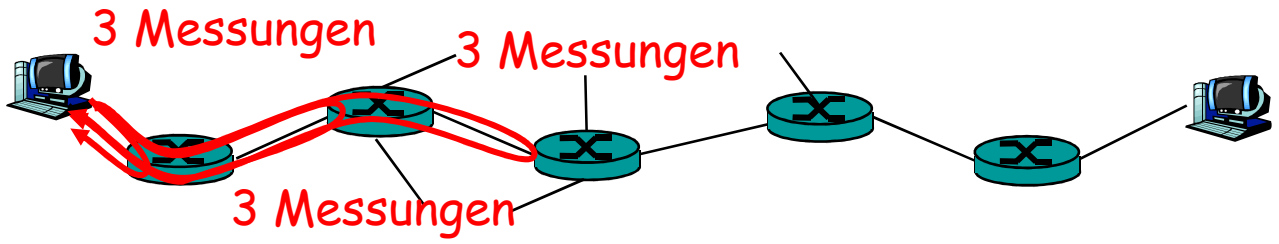


Verkehrswert (Last, Load) = L a/R

- La/R ~ 0: Wartezeit gering
- La/R -> 1: Wartezeit steigt stark an
- La/R > 1: durchschnittliche Wartezeit ist unendlich!

-> Warteschlangentheorie

1.4.3 Ende-zu-Ende-Verzögerung

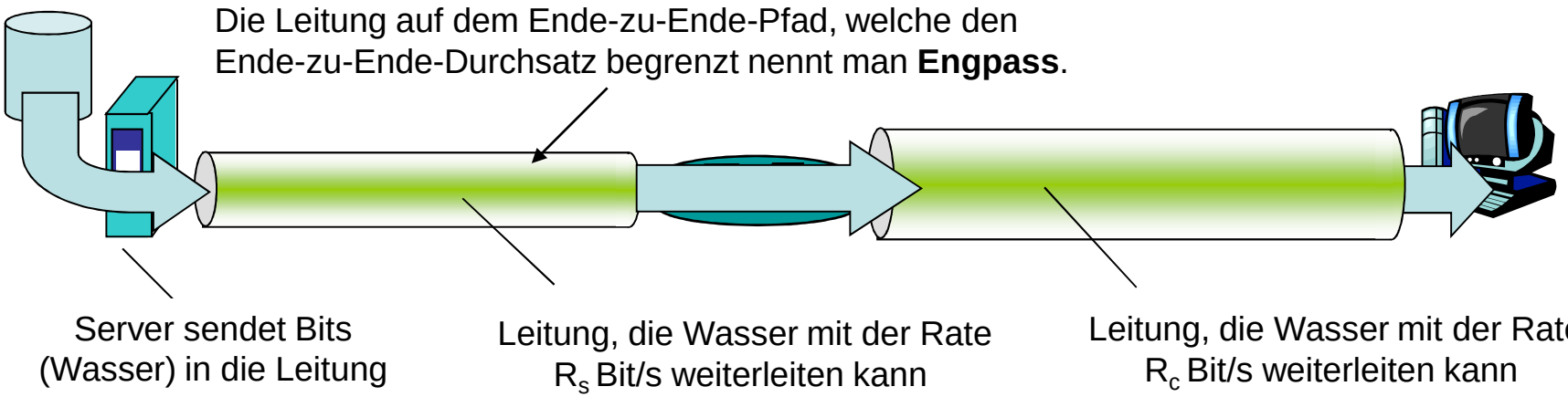


- **`Traceroute`**: Misst die Verzögerung von einer Quelle zu allen Routern auf dem Weg zu einem Ziel. Für alle Router i:
  - Sende drei Pakete, die i auf dem Pfad zum Sender erreichen
  - Router i schickt als Reaktion Pakete an den Sender
  - Sender misst die Zeit zwischen Senden des eigenen Paketes und Empfang des Paketes vom Router

1.4.4 Durchsatz in Computernetzwerken

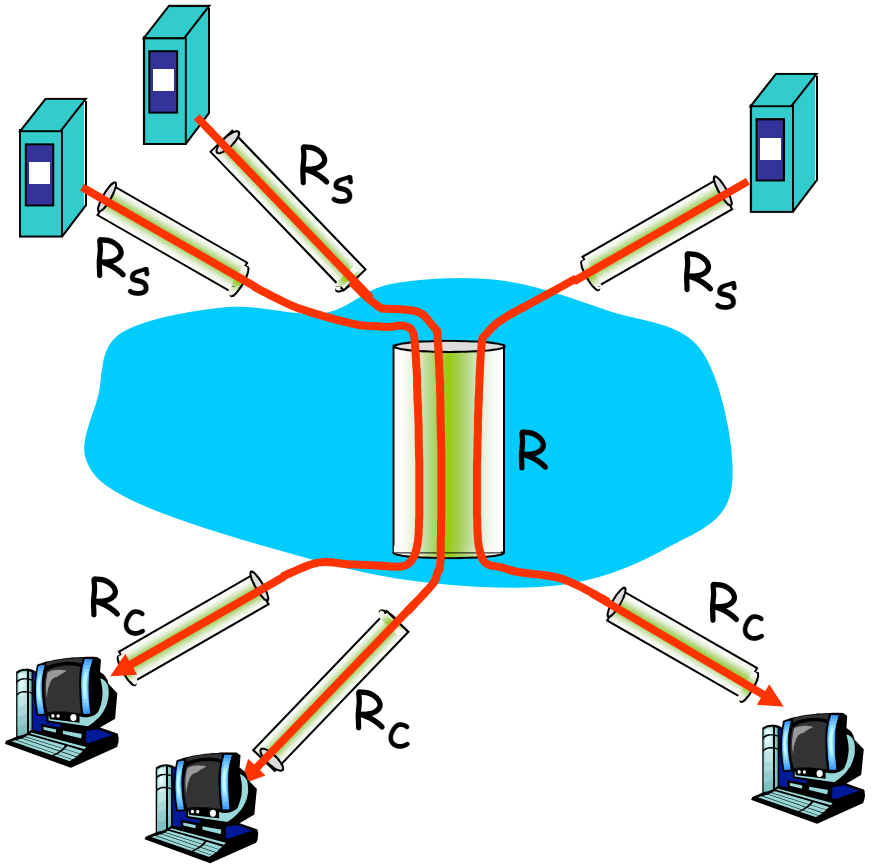
- *Durchsatz:* Rate (Bit/Zeiteinheit), mit der Daten zwischen Sender und Empfänger ausgetauscht werden
  - *Unmittelbar:* Rate zu einem gegebenen Zeitpunkt
  - *Durchschnittlich:* Rate über einen längeren Zeitraum

- Bits als Wasser vorstellbar und Kommunikationsleitungen als Rohre:



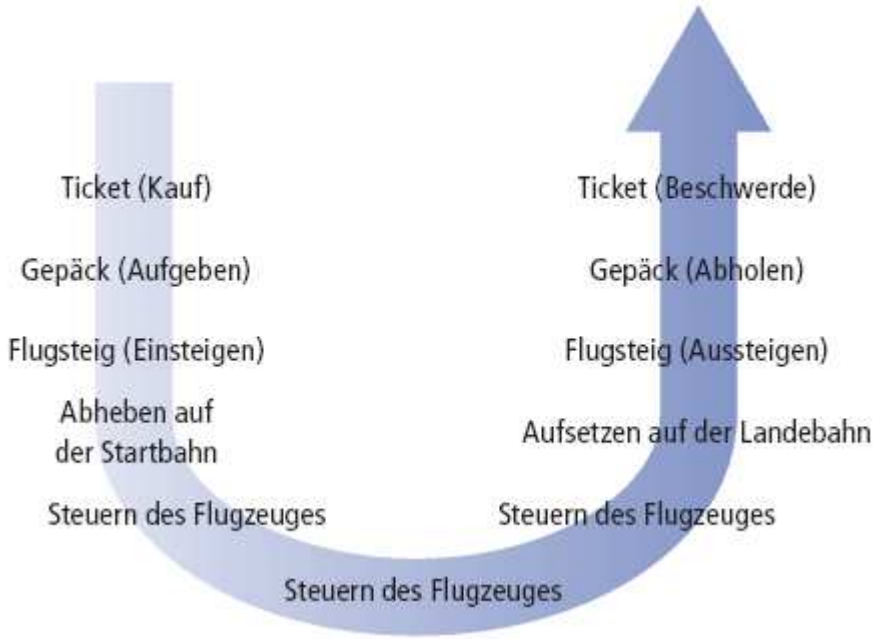
1.4.4 Durchsatz in Computernetzwerken

- Im Internet teilen sich Verbindungen den Engpass des Backbone-Netzwerkes
- Aber es hat sich gezeigt: Häufig sind R_c oder R_s die Engpässe

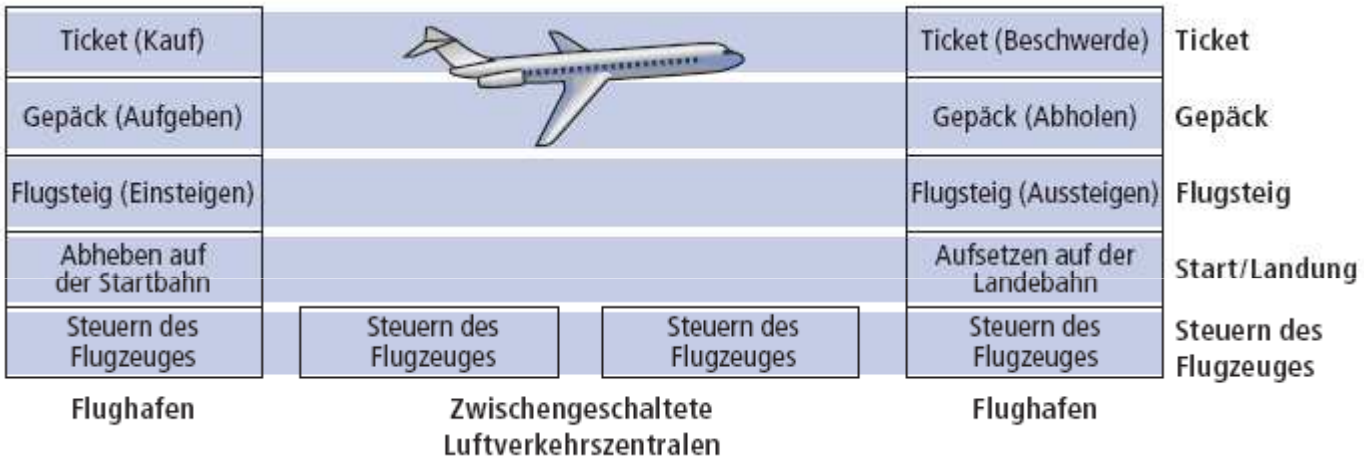


1.5 Protokollschichten und ihre Dienstmodelle

- Das Internet stellt ein äußerst kompliziertes System dar
  → schwierig zu strukturieren
- Die Internetarchitektur wird in Schichten gegliedert
- Zum besseren Verständnis die Analogie Luftverkehrssystem
  → eine Folge einzelner Schritte:



1.5 Protokollschichten und ihre Dienstmodelle



Schichten: Jede Schicht implementiert einen Dienst

- mit Hilfe von schichtinternen Aktionen
- unter Verwendung von Diensten der Schicht, die unter ihr liegt

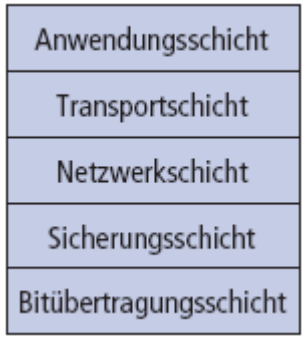
1.5 Protokollschichten und ihre Dienstmodelle

Schichten bieten folgende Vorteile beim Umgang mit komplexen Systemen:

- Strukturierung ermöglicht die Identifikation und das Verständnis des Zusammenspiels einzelner Bestandteile des Systems
  - Referenzmodell für die Diskussion des Systems
- Modularisierung vereinfacht die Wartung und das Arbeiten mit dem System:
  - Änderungen an der Implementierung einer Schicht sind transparent für den Rest des Systems

    Beispiel: Eine Veränderung der Einsteigeprozedur am Gate beeinflusst nicht den Rest des Systems

1.5 Internet Schichten



Protokollstapel des Internets:

- **Anwendungsschicht**: Unterstützung von Netzwerkanwendungen
  - FTP, SMTP, HTTP
- **Transportschicht**: Datentransfer zwischen Prozessen
  - TCP, UDP
- **Netzwerkschicht** (auch Vermittlungsschicht): Weiterleiten der Daten von einem Sender zu einem Empfänger
  - IP, Routing-Protokolle
- **Sicherungsschicht**: Datentransfer zwischen benachbarten Netzwerksystemen
  - PPP, Ethernet, WLAN
- **Bitübertragungsschicht**: Bits auf der Leitung

1.5.1 ISO/OSI Referenzmodell

Zwei zusätzliche Schichten:

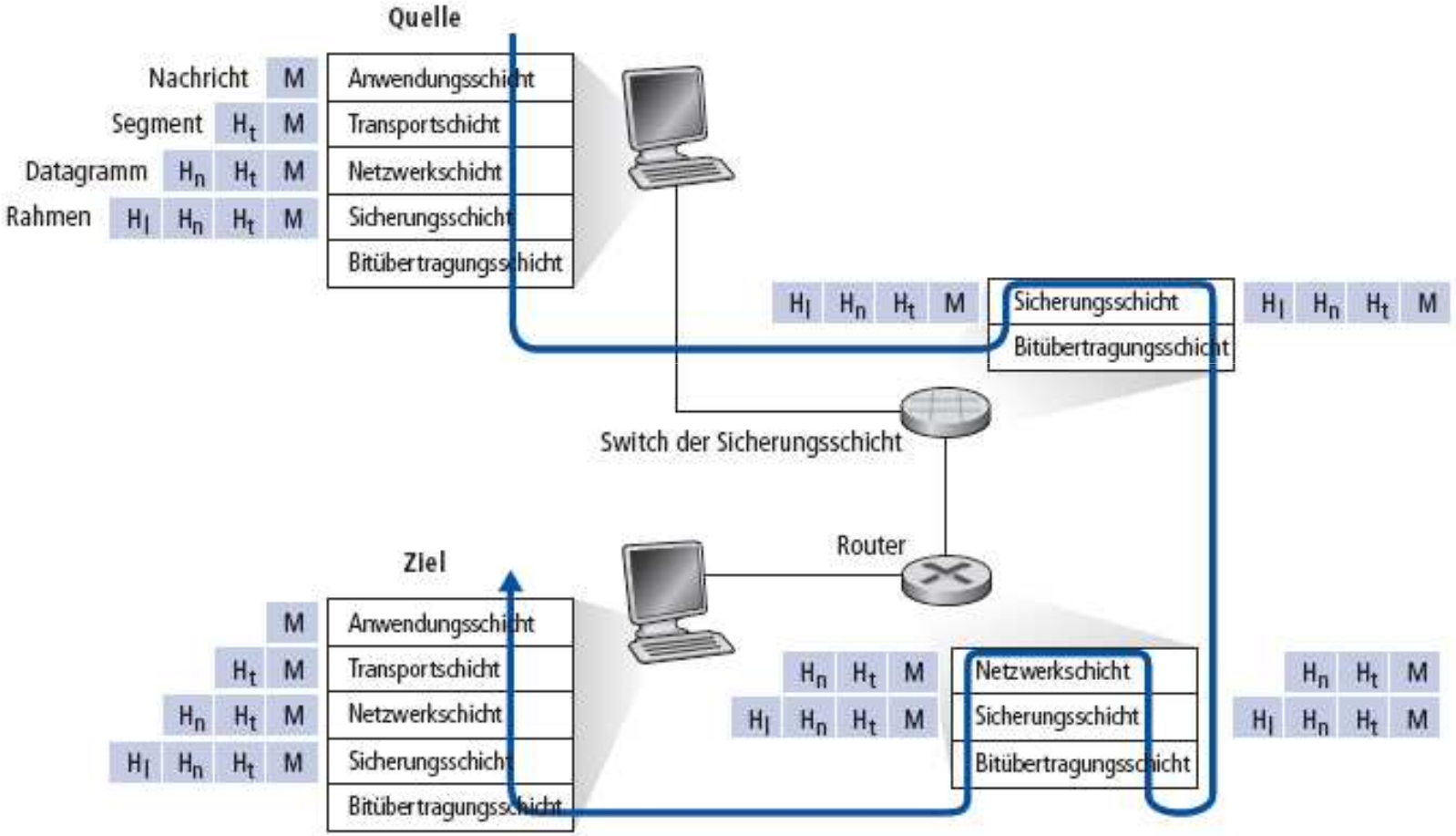
- **Darstellungsschicht**: Ermöglicht es Anwendungen, die Bedeutung von Daten zu interpretieren, z.B. Verschlüsselung, Kompression, Vermeidung systemspezifischer Datendarstellung
- **Kommunikationssteuerungsschicht***:* Synchronisation, Setzen von Wiederherstellungspunkten

Der Protokollstapel des Internets bietet diese Funktionalitäten nicht!

→ Wenn benötigt, müssen sie von der Anwendung implementiert werden

→ Werden sie wirklich benötigt?

1.5 Protokollschichten und ihre Dienstmodelle



Weg, den Daten durch den Protokollstapel eines sendenden Endsystems nehmen.

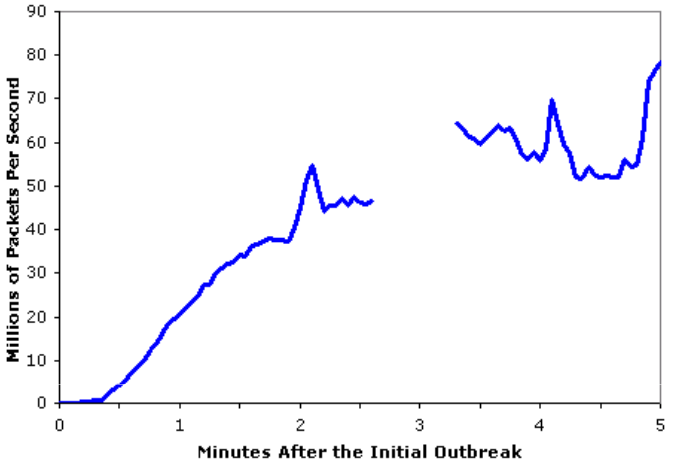
1.6 Sicherheit von Netzwerken

- Das Internet wurde nicht mit dem Ziel Sicherheit entworfen
  - Vision: *“Eine Gruppe von Benutzern, die sich gegenseitig vertrauen, sind über ein transparentes Netzwerk miteinander verbunden“*
  - Die Entwickler von Internetprotokollen versuchen, Sicherheit nachträglich einzubauen
  - Inzwischen: Sicherheit wird in allen Protokollschichten untersucht!

- Angriffe auf die Infrastruktur des Internets
  - Kompromittieren/Angreifen von Endsystemen: z.B. *Malware, Spyware, Würmer, unberechtigter Zugriff (Diebstahl von Daten und Accounts)*
  - Denial of Service: den Zugang zu Ressourcen verhindern

1.6 Sicherheit von Netzwerken

Sapphire-Wurm: scans/s in den ersten 5 Minuten des Ausbruchs (Daten von CAIDA, UWisc)



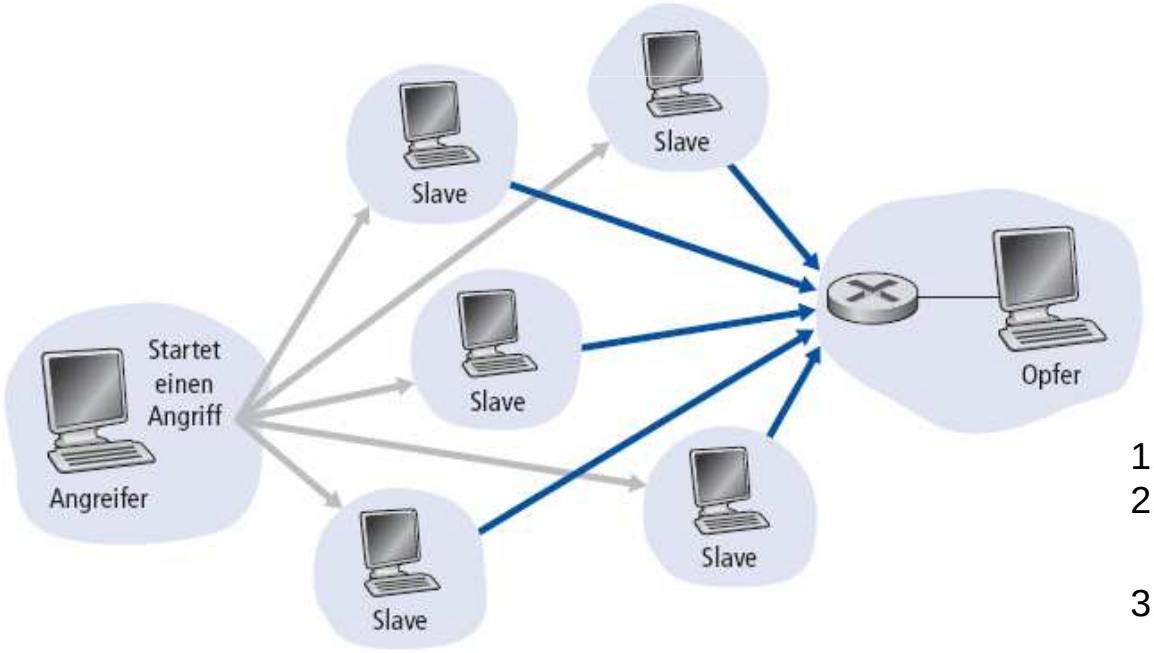
Malware:

- Spyware
  - Infektion durch Laden einer Webseite, die Spyware enthält
  - Aufzeichnen und Weitermelden von Tastenanschlägen, besuchten Websites etc.
- Virus
  - Infektionen über empfangene Objekte (z.B. per E-Mail), erfolgen aktiv
  - Selbst replizierende Viren verbreiten sich über weitere Endsysteme und Benutzer
- Würmer
  - Infektion durch Objekte, die ohne Benutzereingriff empfangen wurden
  - Selbst replizierende Würmer verbreiten sich über weitere Endsysteme und Benutzer

1.6 Sicherheit von Netzwerken

Denial-of-Service-Angriff (DoS Angriff):

- Angreifer verhindern den Zugriff von Benutzern auf Ressourcen (Server, Bandbreite), indem diese durch den Angreifer belegt werden

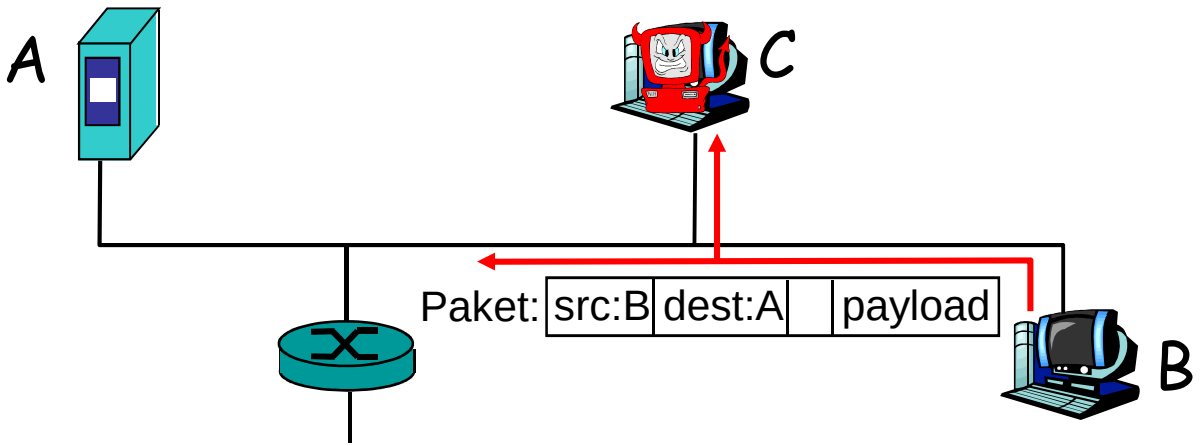


1. Wähle ein Ziel
2. Kompromittiere andere Systeme (z.B. durch Malware)
3. Sende eine sehr große Anzahl an Paketen von den kompromittierten Systemen an das Ziel

1.6 Sicherheit von Netzwerken

Mithören, Verändern und Löschen von Paketen:

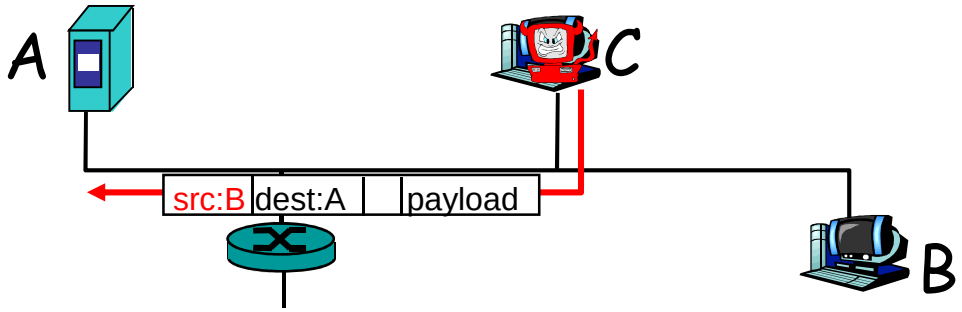
- *Mithören von Paketen, Man in the Middle:*
  - Broadcast-Medien (Ethernet, WLAN)
  - Netzwerkkarten im Promiscuous Mode zeichnen alle (!) Pakete auf, die sie hören können



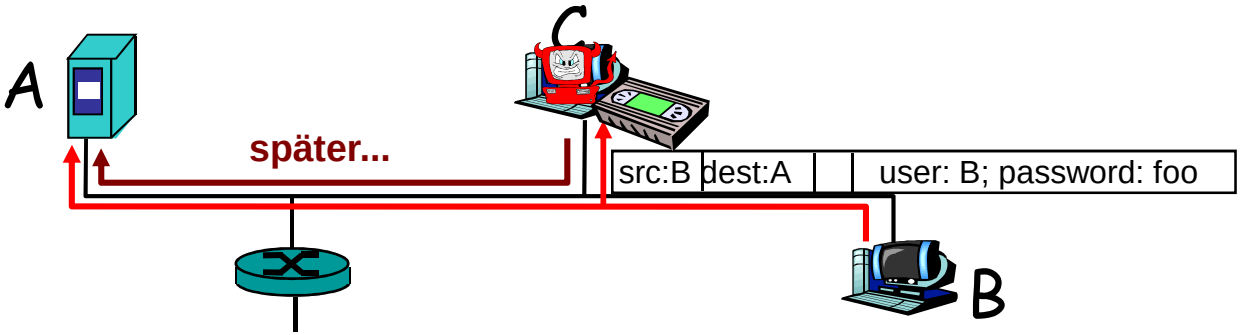
1.6 Sicherheit von Netzwerken

Eigene Identität fälschen:

- *IP-Spoofing:* Sende Pakete mit falscher Absenderadresse



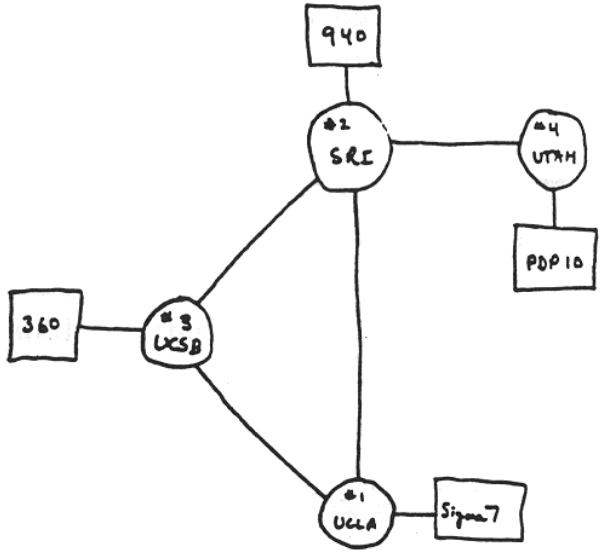
- *Aufzeichnen und Abspielen:* Sicherheitsrelevante Informationen (z.B. Passwort) mithören und später verwenden
  - Das System hält jemanden, der das Passwort eines Benutzers kennt, für den Benutzer!



1.7 Geschichte der Computernetzwerke

Geschichte des Internets: *1961–1972: Paketvermittlung*

- 1961: Kleinrock – Warteschlangentheorie zeigt die Effizienz der Paketvermittlung
- 1964: Baran – Paketvermittlung in Militärnetzen
- 1967: ARPAnet von der Advanced Research Projects Agency geplant
- 1969: erster ARPAnet-Knoten in Betrieb
- 1972:
  - ARPAnet, öffentliche Vorführung
  - NCP (Network Control Protocol), erstes Protokoll zwischen Hosts
  - Erstes E-Mail-Programm
  - ARPAnet hat 15 Knoten



THE ARPA NETWORK

1.7 Geschichte der Computernetzwerke

Geschichte des Internets: *1972–1980: Netzwerk von Netzwerken*

- 1970: ALOHAnet Satellitennetzwerk auf Hawaii
- 1974: Cerf und Kahn – Architektur für die Verbindung von Netzwerken
- 1976: Ethernet: Xerox PARC
- Späte 1970er: proprietäre Architekturen: DECnet, SNA, XNA
- Späte 1970er: Pakete fester Größe (später ATM)
- 1979: ARPAnet hat jetzt 200 Knoten

Cerf und Kahn: Prinzipien für die Verbindung von Netzen
- Minimalismus, Autonomie – keine internen Änderungen an den einzelnen Netzwerken
- Best-Effort-Dienst – keine Garantien
- Kein (Verbindungs-) Zustand in den Routern
- Dezentrale Kontrolle

→ Definition der aktuellen Internetarchitektur!

1.7 Geschichte der Computernetzwerke

Geschichte des Internets: *1980–1990: Neue Protokolle, Ausbreitung des Netzes*

- 1983: Einführung von TCP/IP
- 1982: Definition des SMTP-E-Mail-Protokolls
- 1983: Definition von DNS zur Übersetzung von Namen auf IP-Adressen
- 1985: Definition von ftp
- 1988: Überlastkontrolle in TCP

- Neue nationale Netzwerke: *Csnet, BITnet, NSFnet, Minitel*
- 100.000 Endsysteme sind an einen Verbund von Netzwerken angeschlossen

1.7 Geschichte der Computernetzwerke

Geschichte des Internets: *1990–20XX: Kommerzialisierung, WWW*

- Anfang 1990er Jahre: ARPAnet wird eingestellt
- 1991: NSF hebt die Einschränkungen bezüglich der kommerziellen Nutzung des NSFnet auf
- Anfang 1990er Jahre: Web
  - Hypertext [Bush 1945, Nelson 1960er]
  - HTML, HTTP: Berners-Lee
  - 1994: Mosaic, später Netscape
  - Späte 1990er Jahre: Kommerzialisierung des Web

Späte 1990er–20XX: Neue Anwendungen

- Mehr Killeranwendungen: Instant Messaging, P2P-Filesharing
- Netzwerksicherheit wird immer wichtiger
- Geschätzte 50 Millionen Endsysteme, 100 Millionen Anwender
- Backbone-Leitungen mit Gbit/s

Kapitel 1: Zusammenfassung

- Überblick über das Internet
- Was ist ein Protokoll?
- Rand des Netzwerkes, Zugangsnetze, das Innere des Netzwerkes
  - Paketvermittlung und Leitungsvermittlung
  - Struktur des Internets
- Leistungsgrößen: Verluste, Verzögerung, Durchsatz
- Schichten und Dienste
- Sicherheit
- Geschichte des Internets