


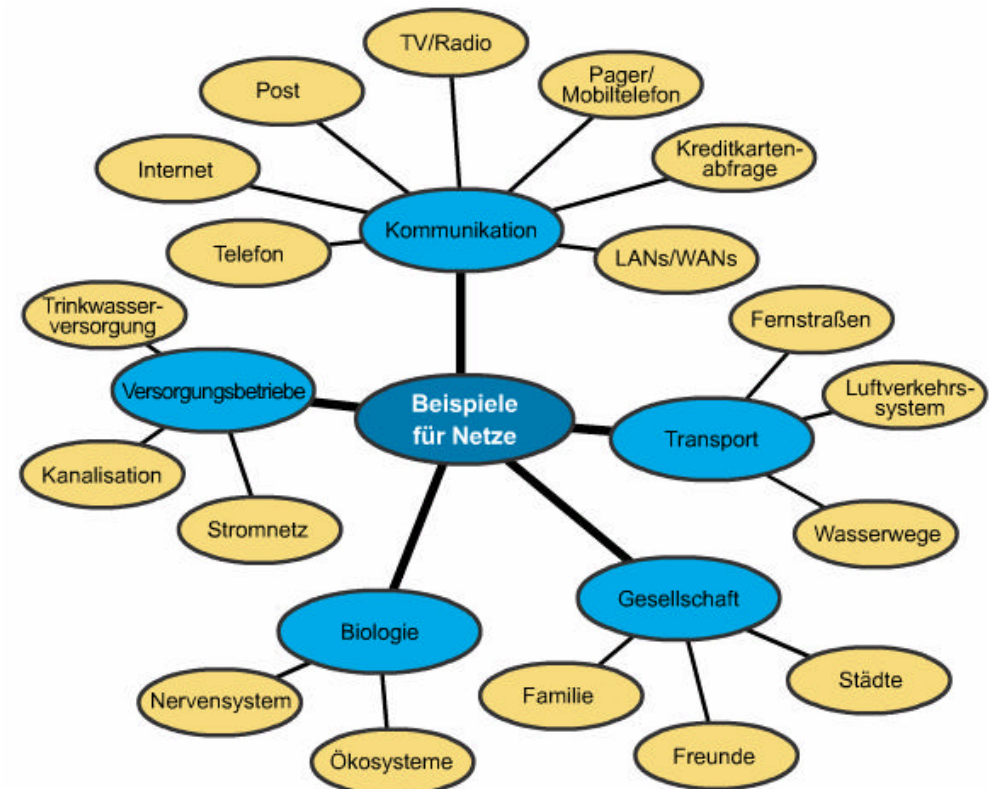
Computernetze – Einführung

Reiner Nitsch

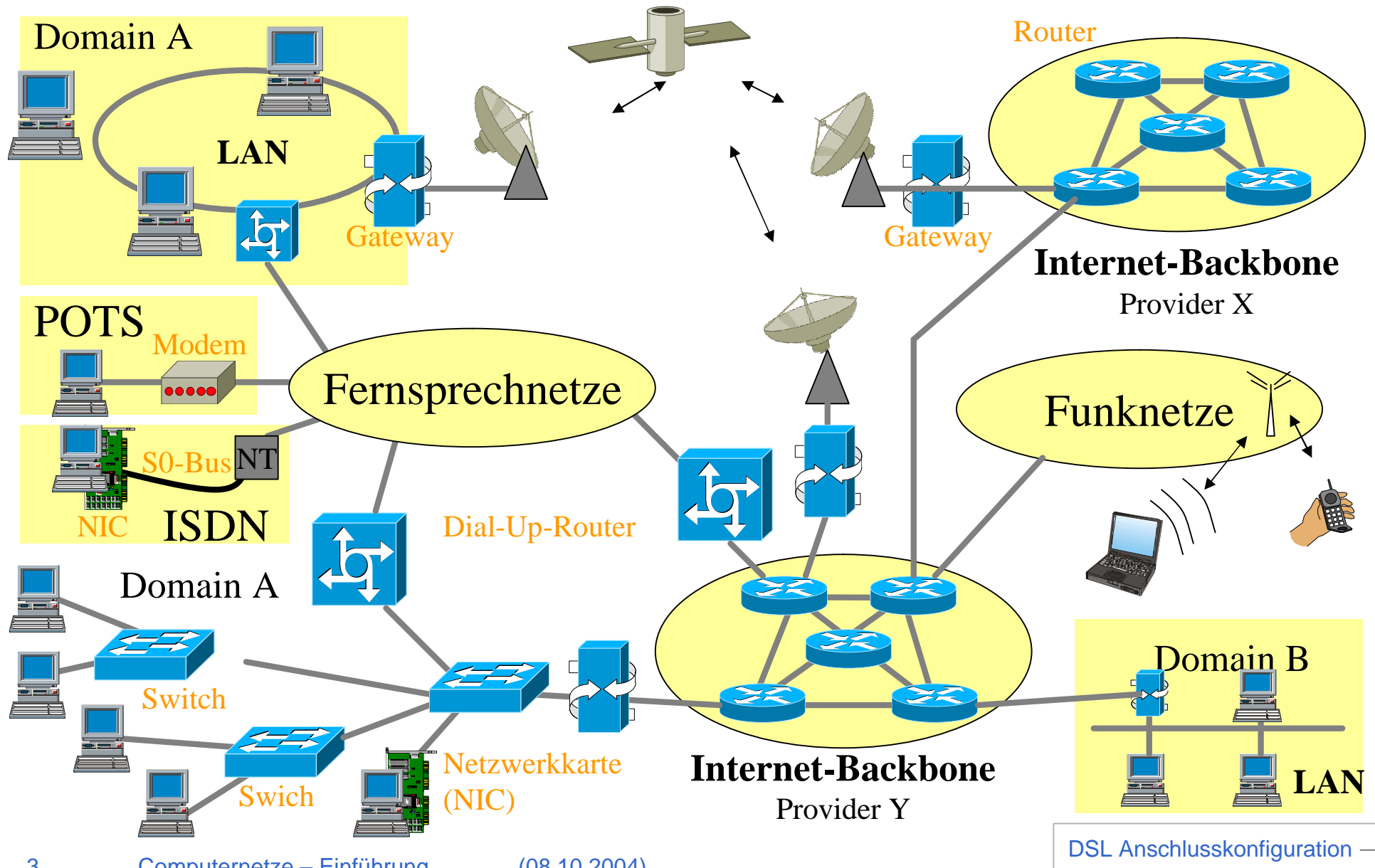
Raum 16c,  255

 r.nitsch@fbi.fh-darmstadt.de

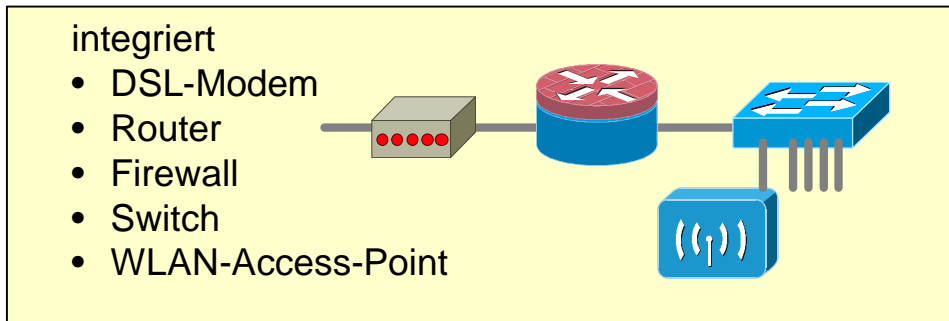
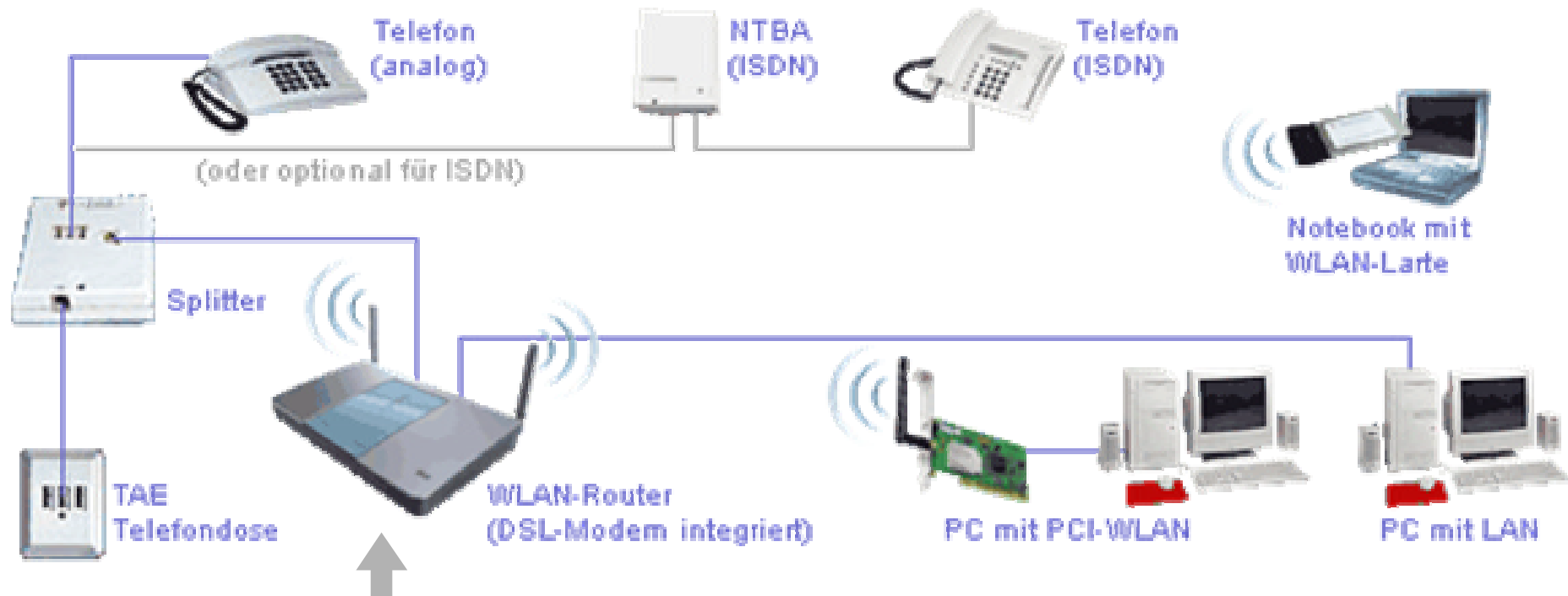
- Ein *Netz* ist ein stark verzweigtes System, das Objekte oder Menschen verbindet.
- Solche Netze decken i.d.R. einen Bedarf
- **Beispiele** sind
 - Kommunikationsnetze
 - Transportnetze
 - Soziale Netze
 - Biologische Netze
 - Öffentliche Versorgungsnetze
- Geforderte **Eigenschaften** sind
 - Zuverlässigkeit
 - Sicherheit
 - Effizienz
 - gutes Preis-Leistungs-Verhältnis
 - ressourcenschonend
 - Skalierbarkeit
 - Interoperabilität (Standardkonform)



Was ist das Internet? - Technik des Internet



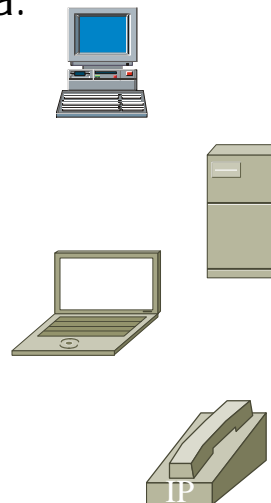
DSL Anschlusskonfiguration



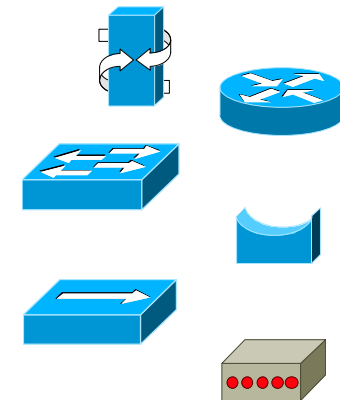
- Das **Internet** besteht aus vielen Einzelnetzen (z.B. **Lokale Netze** mit **Switches**, **Hosts**, **Routern** und **Dial-Up-Routern**) unterschiedlicher Technologien, die im Kern über **Backbonenetze** miteinander verbunden sind.
- Netzkomponenten, die Netze unterschiedlicher Technologien miteinander verbinden, werden auch als **Gateways** bezeichnet..
- Das Internet wurde Massenmedium durch **Wahlzugänge** (Dial-Up-Access).
- Der leistungsfähigste Teil des Internets ist in den USA und Europa installiert. Er basiert auf einem 2,5 - Gbit/s-Backbone (Kernnetz).
- Der DFN- Verein betreibt Backbone mit 2,5 Gbit/s. Die Fachhochschule Darmstadt ist mit 140 Mbit/s an das DFN angeschlossen.
- Werden Internetdienste (WWW, FTP, E- Mail usw.) innerhalb einer privaten Domäne genutzt, nennt man ein solches Netz auch „**Intranet**“.
- Hat ein „Intranet“ Zugang zu anderen Intranets werden diese als „**Extranet**“ bezeichnet.
- **POTS** (Plain Old Telephone Service) bezeichnet das analoge Fernsprechnet, **ISDN** (Integrated Services Digital Network) das digitale Fernsprechnet.

Was ist das Internet? – Sein Aufbau aus Peripherie und Kern

- Ein weltweites Computernetzwerk, das Millionen von Computergeräten, auch **Hosts** oder **Endsysteme** genannt, miteinander verbindet.
- Die Endgeräte bilden die **Peripherie des Internets**. Zu ihnen zählen u.a.
 - Traditionelle Desktop PCs
 - Unix-Workstations
 - Server (WWW, EMAIL, FTP)
 - Mobile Computer
 - Web-Fernseher
 - Personenrufgeräte (Pager)
 - IP-Phones, Haushaltsgeräte



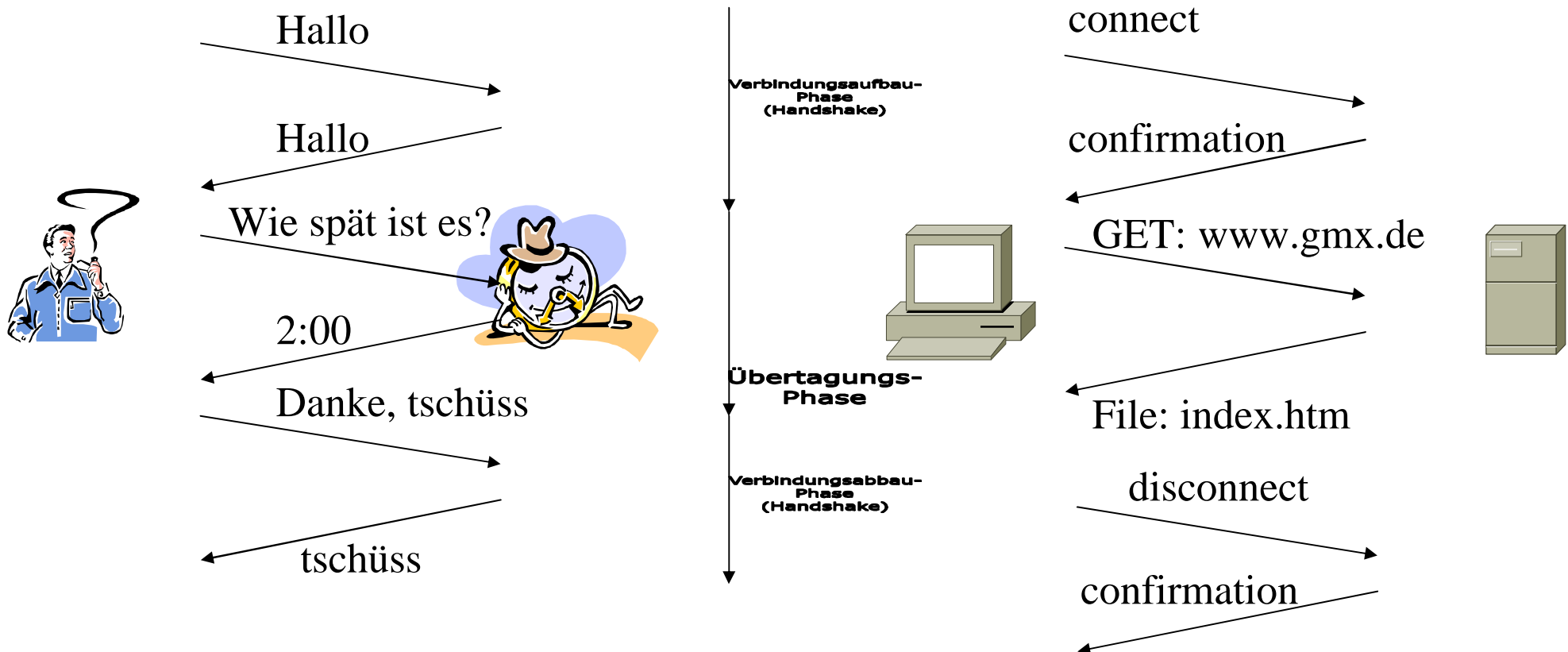
- Die Schaltstellen im **Kern des Internet** werden u.a. gebildet durch
 - Gateway
 - Router
 - Switch
 - Bridge
 - Hub, Repeater
 - Modem



- **Netzwerkanwendungen** (WWW, EMAIL, FTP,...) bestehen u.a. aus Software, die auf den Hosts ausgeführt wird.
- Die Kommunikation (Senden und Empfangen von Informationen) zwischen den Komponenten des Internets wird durch **Protokolle** gesteuert

Was ist ein Protokoll?

- Ein Protokoll definiert das **Format** und die **Reihenfolge** von Nachrichten, die zwischen zwei oder mehr kommunizierenden Einheiten ausgetauscht werden, sowie die **Aktionen**, die bei der Übertragung und/oder beim Empfang einer Nachricht oder eines anderen Ereignisses unternommen werden.
- **Beispiele:** Ein menschliches Protokoll und ein Netzwerkprotokoll

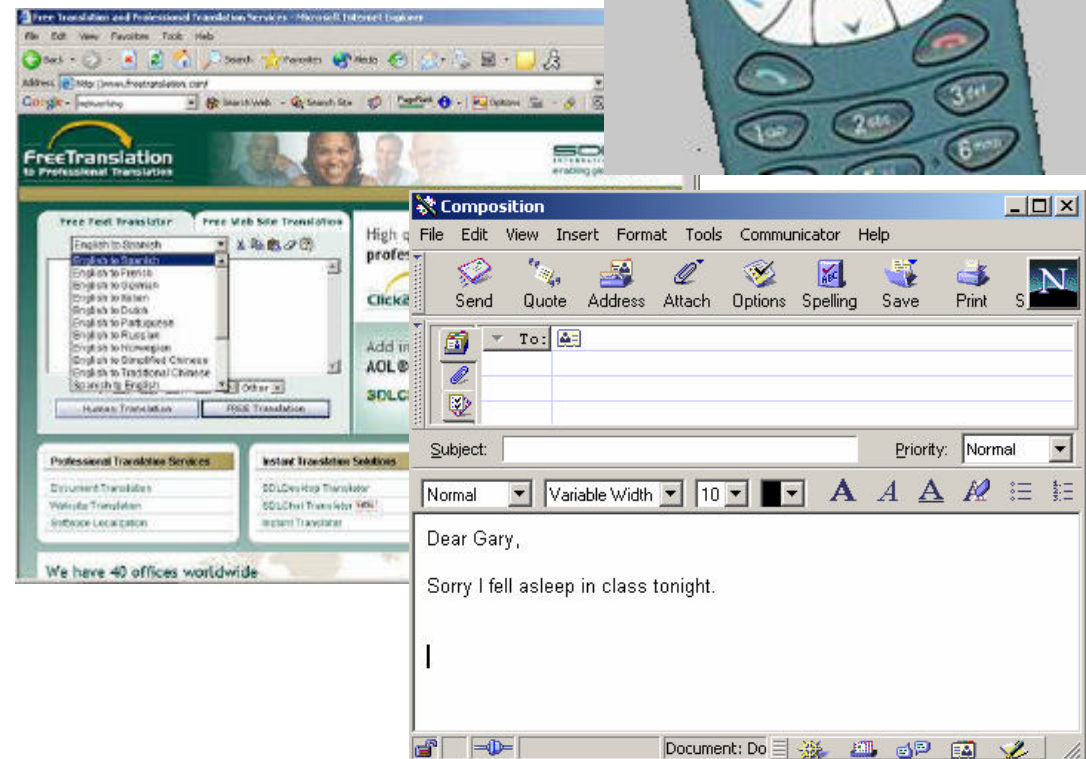


Was ist das Internet? – Seine Dienste

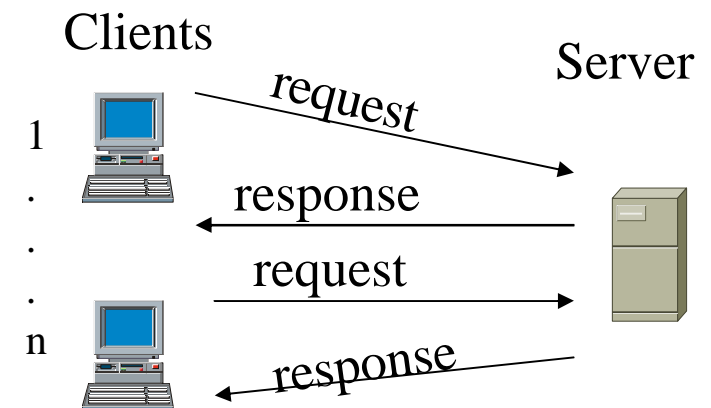
- Im Internet tauschen **verteilte Anwendungen** Daten miteinander aus. Verteilte Anwendungen sind Software, die auf den Endsystemen ausgeführt wird. **Beispiele** sind:

- Email
- World Wide Web
- File-Transfer
- Online-shops, -banking, -games, -auction (E-Commerce)
- Chat Rooms
- Voice over IP
- E-Government Anwendungen (ELSTER, Elektronischer Gesundheitsausweis, ...)
- Authentifizierung, Autorisierung
- Remote-Login

- Domain Name Service
- DHCP-Service
- File-Transfer



- Bei Hosts werden 2 Kategorien unterschieden: Clients und Server
 - **Server** (= Software auf einem Server-Host)
 - bieten einen Dienst an.
 - sind passiv, d.h. sie warten auf Anfragen (**Request**) von Clients
 - senden Antworten (**Response**)
 - **Clients** (= Software auf einem Client-Host)
 - sind aktiv, d.h. sie ergreifen die Initiative
 - senden Anfragen (**Requests**) an einen **Server**.
 - warten auf dessen Antwort
- Dieses **Client-Server-Modell** ist die vorherrschende Struktur von Internetanwendungen (Web, E-Mail, Filetransfer, Remote-Login z.B. mit Telnet, DNS, DHCP,...).
- Wegen der räumlichen Distanz zwischen Client und Server spricht man auch von **verteilten Anwendungen**. Das Netz selbst ist auf dieser Abstraktionsebene eine Blackbox, die einen **verbindungsorientierten Dienst** und/oder **einen verbindungslosen Dienst** bereit stellt. Übermittlungsdetails sind dabei verborgen.

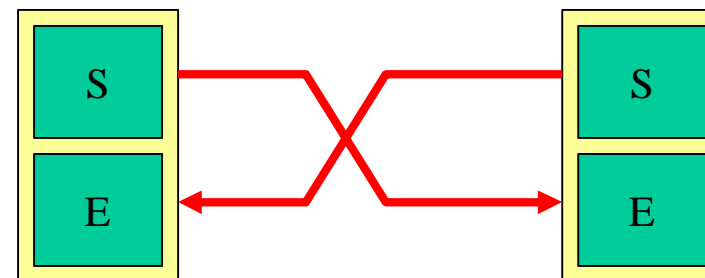
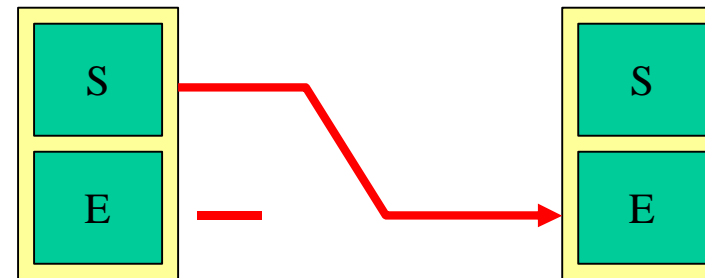


Ein Netzwerkkern stellt einer Anwendung verschiedene Dienste zur Verfügung:

- **Zuverlässiger Datenübertragungsdienst**: Daten kommen alle, ohne Fehler, nicht doppelt und in der richtigen Reihenfolge an.
- **Flusskontrolldienst (flow control)**: Stellt sicher, dass ein Sender einen langsamen Empfänger nicht durch zu schnelles Senden der Daten überfordert. Wird im Internet durch Sende- und Empfangs-Pufferspeicher in den Endsystemen und Zurückhalten von Bestätigungen realisiert.
- **Überlastkontrolldienst (congestion control)**: verhindert Daten-Staus im Netz, die entstehen, wenn Puffer in den Routern überlaufen und deswegen Nachrichten verloren gehen. Im Internet reduzieren dazu Endsysteme ihre Übertragungsrate indem Sie Daten-Bestätigungen kontrolliert zurückhalten.
- **Verbindungsorientierter Dienst (connection oriented service)** mit den Kennzeichen:
 - Ist ein zuverlässiger Datenübertragungsdienst
 - Abwicklung in 3 Verbindungsphasen: Aufbau (3-Wege-Handshake), Übertragung, Abbau (3-Wege-Handshake). Die Verbindung ist nur sehr locker: deshalb „verbindungsorientiert“. Die Router im Netz wissen nichts von den Verbindungen.
 - Im Internet realisiert als zuverlässiger Datenübertragungsdienst inklusive Flusskontrolle und Überlastkontrolle durch das **Transport Control Protocol (TCP)**
- **Verbindungsloser Dienst** mit den Kennzeichen:
 - keine Auf- und Abbauphase (kein Handshake). Daten werden daher schneller übertragen.
 - Keine Bestätigungen: Sender erfährt nicht, ob Nachricht den Empfänger erreicht hat (best effort)
 - Keine Flusskontrolle
 - Keine Überlastkontrolle
 - Wird im Internet vom **User Data Protocol (UDP)** bereitgestellt
 - Ist kein zuverlässiger Datenübertragungsdienst sondern arbeitet nach dem „best effort“-Prinzip

Was ist das Internet? – Seine Übertragungsbetriebsarten

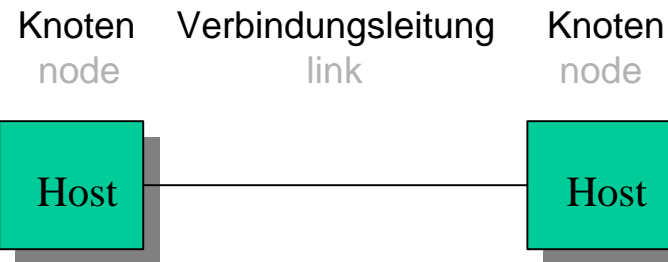
- **Simplex (sx)**, Richtungsbetrieb:
 - einer sendet, einer oder mehrere empfangen,
 - Zeitzeichensender, Rundfunk
- **Halbduplex (hx)**, Wechselbetrieb:
 - die Stationen senden wechselseitig, d.h. zeitlich nacheinander,
 - "normale" Fernsprechverbindung, Telexnetz,
- **Duplex (dx)**, Gegenbetrieb:
 - beide Stationen können gleichzeitig senden und empfangen,
 - Übertragungseinrichtungen im Fernnetz oder im Anschlußnetz, Modems, usw.



- Der Netzwerkkern ist realisiert als Direktverbindungsnetzwerk (**Direkte** oder **physikalische Konnektivität**) oder als vermitteltes Netz (**indirekte Konnektivität**). Die Vermittler im arbeiten dabei als **Leitungsvermittlung** oder **Paketvermittlung**
- In **leitungsvermittelten Netzen** werden die für eine Übertragung benötigten **Ressourcen** (Bandbreite) für die Dauer der Sitzung **reserviert**. Die Reservierung erlaubt es den Endsystemen, Daten mit einer **garantierten konstanten Rate** zu übertragen. Eine Überlast für bestehende Verbindungen ist nicht möglich.
Beispiele: Restaurant mit Tischreservierung, Telefonnetze
- In **paketvermittelten Netzen** werden Daten **ohne Reservierungen** in das Netz eingespeist und über eine Reihe von Verbindungsleitungen übertragen. Entsteht **Überlast**, weil gleichzeitig mehrere Pakete über die gleiche Leitung übertragen werden sollen, werden die Pakete in einer Warteschlange (Pufferspeicher) geparkt. Dadurch entsteht eine **Warteschlangenverzögerung**. Bei zu großer Überlast entsteht Datenverlust, weil die Puffer voll und die Pakete in der Folge verworfen werden.
Beispiele: Restaurant ohne Tischreservierung, Internet
- **Das Internet ist im wesentlichen ein paketvermitteltes System.** Es überträgt Daten nach „bestem Bemühen“ (**best effort**) möglichst schnell, macht aber keinerlei Zusicherungen.
- Es gibt paketvermittelte Netzwerke mit virtuellen Verbindungen (**virtual circuits**), die Charakteristika der Leitungs- und Paketvermittlung aufweisen (z.B. **Asynchronous Transfer Mode (ATM)**, **Frame Relay**)

Direkte Konnektivität = physikalische Konnektivität

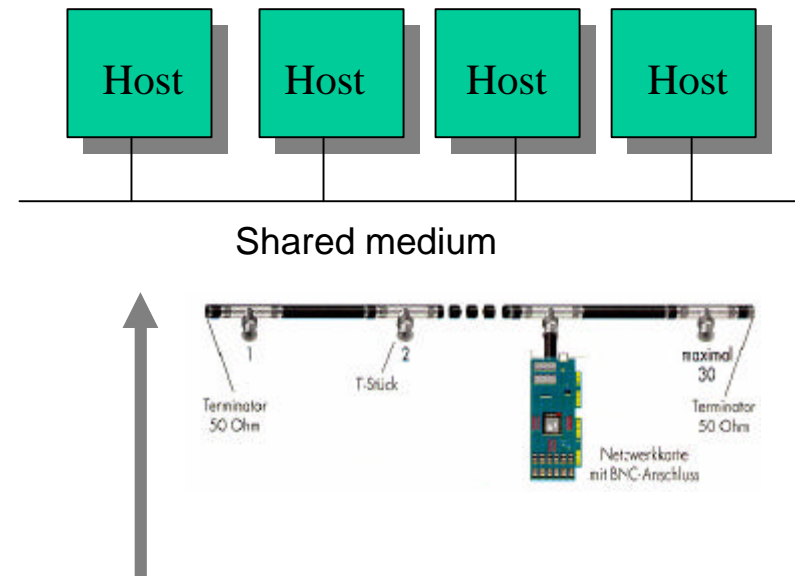
Punkt-zu-Punkt-Verbindung (point-to-point link)



Skalierungsproblem: In einer Gruppe von N PCs jeden mit jedem anderen zu verbinden erfordert $N(N-1)/2$ Punkt-zu-Punkt Verbindungen

- **Eingeschränkte Skalierbarkeit** wegen
 - Kabelmengen oder
 - max. Reichweite oder
 - begrenzter Anzahl anschließbarer Teilnehmer
- **Beispiele:** Local Area Networks (**LAN**), Rundfunk-/TV-Netze

Mehrfachzugriffs-Verbindung (multiple access link)

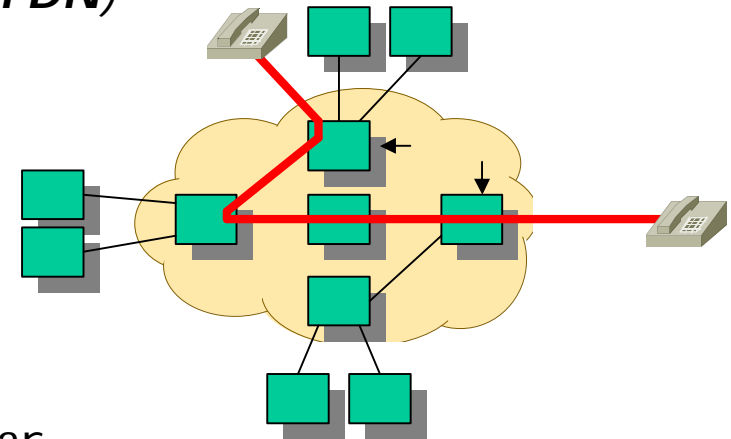


Man nennt das Senden einer Nachricht

- an einen bestimmten Host „**Unicast**“,
- an eine bestimmte Gruppe von Hosts „**Multicast**“ und
- an alle Hosts eines Netzwerkes „**Broadcast**“

Der Netzwerkkern - Indirekte Konnektivität - Leitungsvermittelltes Netz

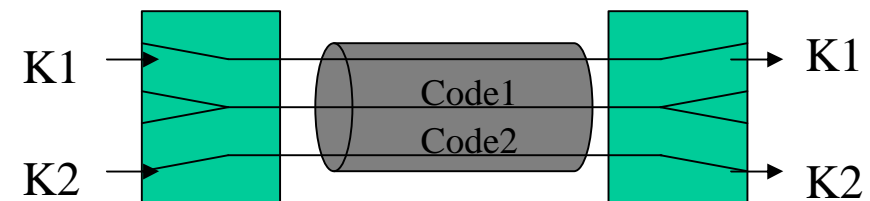
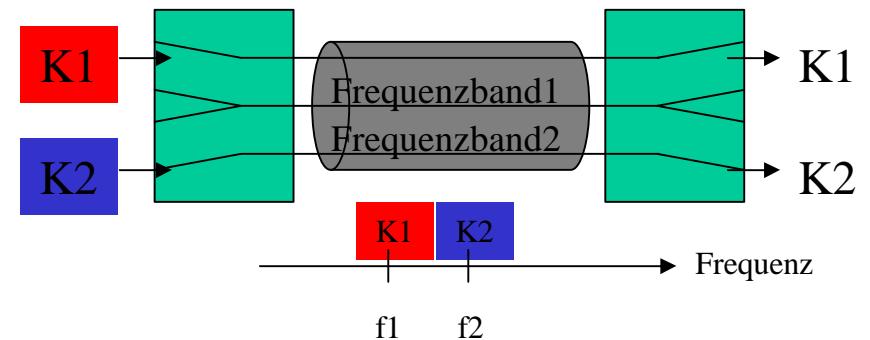
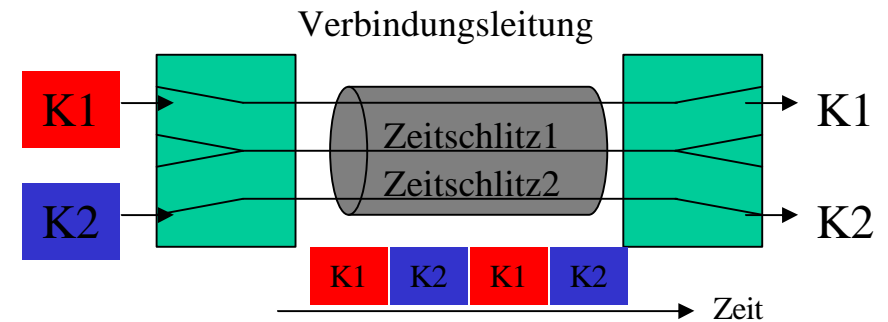
- *In Englisch: Circuit Switched Public Data Network (CSPDN)*
- 3 Verbindungsphasen
 - Verbindungsaufbau (evtl. mehrere Sekunden)
 - Signalübertragung
 - Verbindungsabbau
- Fest zugewiesener Weg zwischen 2 Endstationen
- Feste und gleiche Datenrate für beide Endstationen, auch dann, wenn gerade nicht benötigt (Nachteil!)
- Signallaufzeit in Verbindungsknoten ist vernachlässigbar
- Verbindung verhält sich wie bei durchgehendem Kabel (unveränderte Reihenfolge, Daten gehen nicht verloren und kommen nicht doppelt an)
- Keine Fehler- oder Flußkontrolle durch das Netzwerk
- Garantierte Dienstgüte (**Quality of Service QoS**): garantierte Bitrate und feste kleine Laufzeit
- **Gemeinsame Ressourcennutzung** auf den Verbindungsleitungen durch statische Multiplextechniken (TDM, FDM).
- **Beispiele:** Fernsprechnet, ISDN



CSPDN: Circuit Switched Private Data Network
ISDN: Integrated Services Digital Network

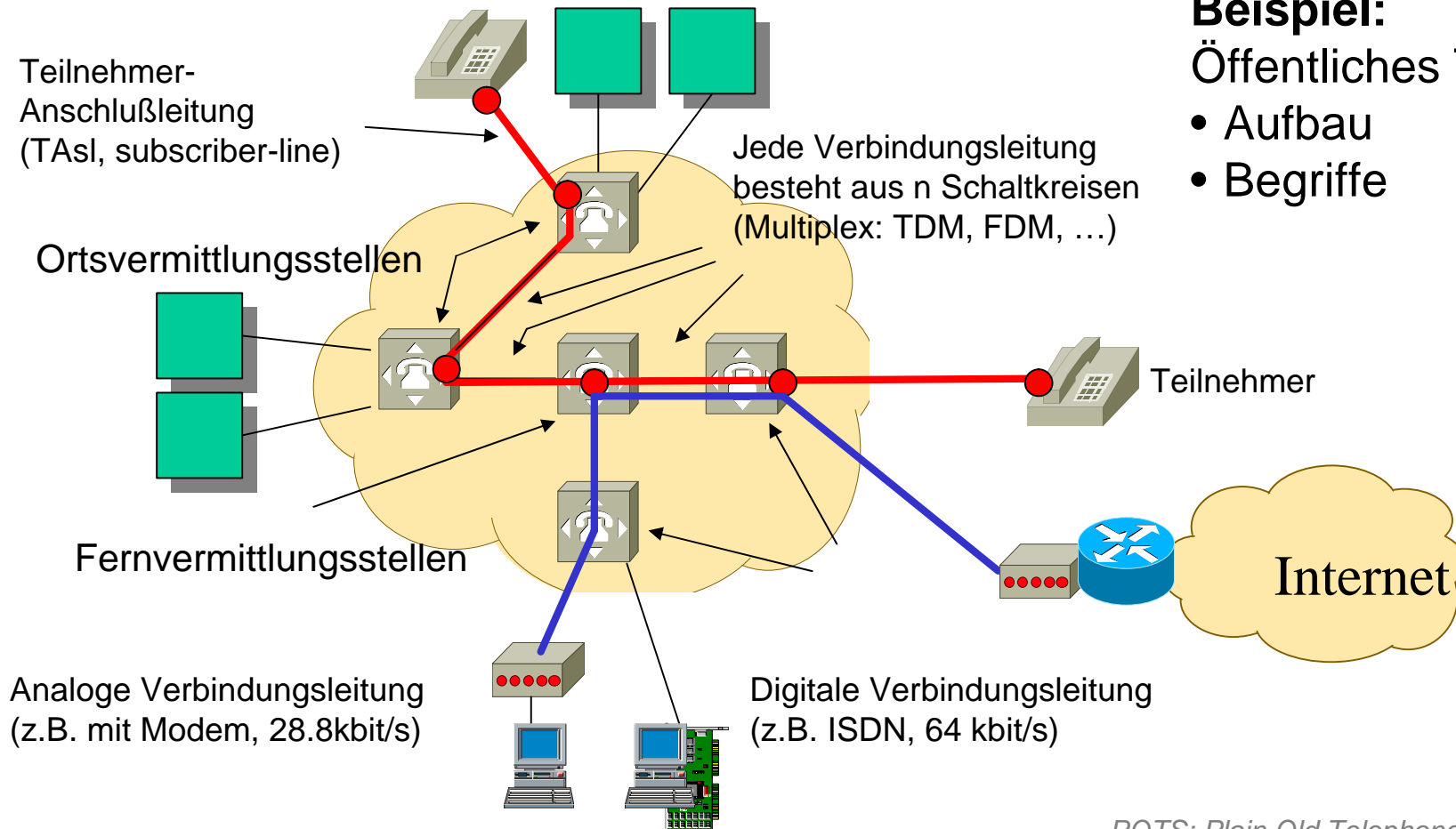
Gemeinsame Ressourcennutzung – Statische Multiplextechniken

- Ermöglicht mehreren Hosts dieselbe Verbindungsleitung gleichzeitig zu nutzen
- Multiplexprinzipien
 - **Zeitmultiplex**
(Time Division Multiplex – TDM)
 - **Frequenzmultiplex**
(Frequency Division Multiplex – FDM)
Beispiele: Rundfunk, TV,...
früher auch im Fernsprechnet
 - **Codemultiplex**
(Code Division Multiplex – CDM)



Beispiel POTS →

Der Netzwerkkern - Indirekte Konnektivität - Beispiel POTS



Beispiel: Öffentliches Telefon-Netz

- Aufbau
- Begriffe

*POTS: Plain Old Telephone Service
CSPDN: Circuit Switched Private Data Network
TAsl: Teilnehmer-Anschlußleitung
TDM: Time Division Multiplex
FDM: Frequency Division Multiplex*

- **Nachteile** von TDM, FDM und CDM:
Übertragungskapazität eines Kanals
 - wird auch belegt, wenn es nichts zu übertragen gibt
(**Beispiel**: Lesen einer Webseite)
 - kann nicht an den tatsächlichen Bedarf angepasst werden, sondern orientiert sich am Maximalbedarf
- TDM, FDM und CDM werden deshalb auch **statische Multiplextechniken** genannt.

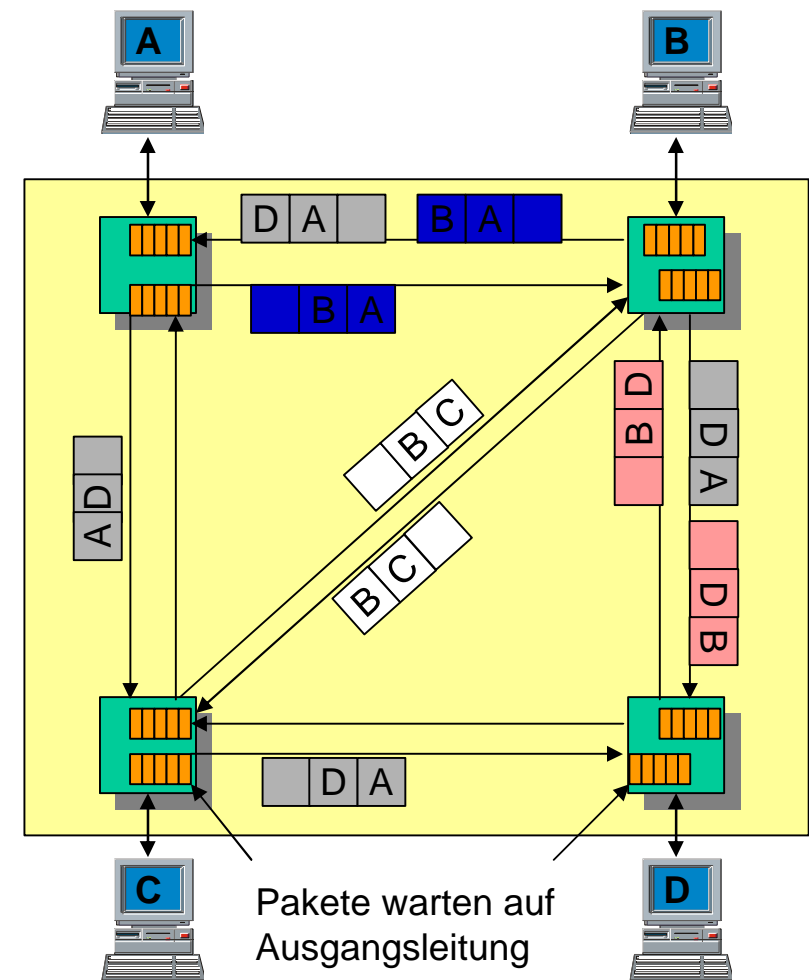
➤ **Statisches Multiplexen ist ineffizient, weil es Übertragungskapazität vergeudet!**

- **Wird in paketvermittelten Netzen angewendet.**
- **On Demand: Übertragungskapazität** wird erst **auf Anfrage** zugeteilt.
- **Wettbewerb:** Mehrere Hosts **konkurrieren** um dieselbe Übertragungskapazität.
- **Alles oder nichts:** Zugeteilt wird jeweils die gesamte (ungeteilte) Übertragungskapazität
- **Bitte warten:** Bei gleichzeitigem Übertragungswunsch mehrerer Hosts wird zeitlich nacheinander zugeteilt. Bis zur Zuteilung werden die Sendedaten gepuffert (Speichervermittlung, ungewisse Laufzeit!).
- **Scheibchenweise:** Faire Zuteilungschancen machen eine Segmentierung größerer Nachrichten erforderlich. Nachrichten werden paketweise übertragen.
- **Vorteile:**
 - Bedarfsgerechte Zuteilung (nur dann, wenn benötigt und soviel wie benötigt!)
 - Keine Ressourcenverschwendung
 - Optimale Nutzung der Übertragungskapazität
- **Nachteile:**
 - nicht vorhersagbare Laufzeit und Laufzeitschwankungen
 - Überlastungsgefahr

- **Zuteilungsregeln** müssen faire Zuteilung der Leitungskapazität an mehrere konkurrierende Hosts gewährleisten.
 - **Zuteilungskriterien:**
 - First-In-First-Out (**FIFO**): Wer zuerst kommt mahlt zuerst!
 - Jeder Host bekommt eine bestimmte **mittlere Kapazität** zugeteilt.
 - Bestimmte Hosts bekommen eine **maximale Zuteilungswartezeit** garantiert.
 - Bestimmte Anwendungen werden bevorzugt bedient (**Priorität**)
- Netzwerke, die eine solche Sonderbehandlung gestatten, unterstützen Dienstgüte (Quality of Service; QoS)

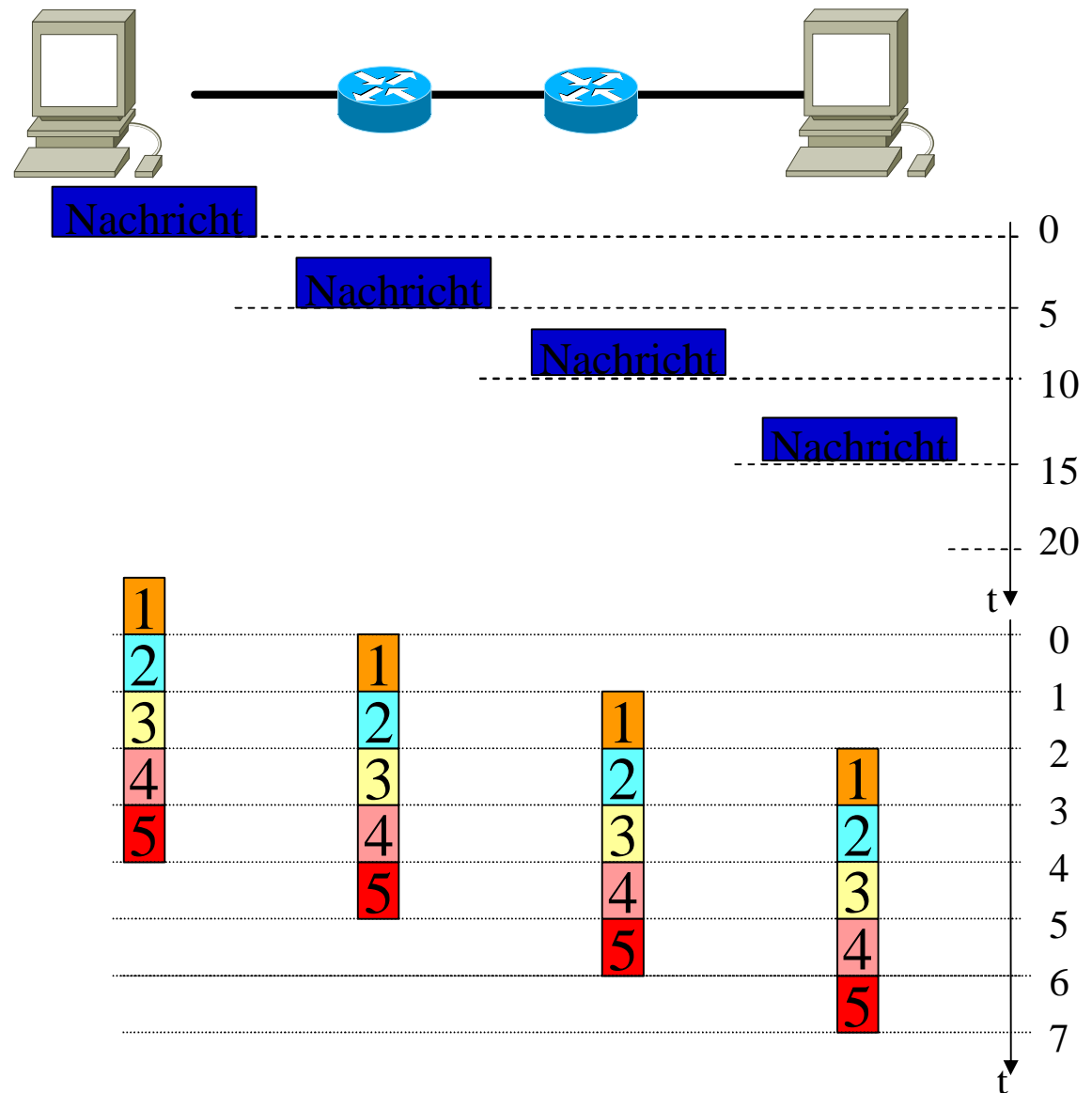
In Englisch: Paket Switched Public Data Network (PSPDN)

- Der Sender zerlegt (**segmentiert**) die Nachricht in mehrere kleinere Datenpakete (kommt gleich).
- Netzknoten empfangen und speichern die Pakete vollständig (**Store-and-Forward-Übertragung, Speichervermittlung**)
- Knoten/Netz bestimmt Weg für jedes Paket neu
- Der Empfänger **reassembliert** die Pakete zur Nachricht.
- + Kein Verbindungsauf- und -abbau
- + Netzressourcen werden nur bei Bedarf belegt
- Alle Pakete müssen Quell- und Zieladresse kennen (Overhead)
- Zusätzliche Laufzeit in Netzknoten durch Store-and-Forward-Prinzip und Warteschlangenverzögerung



Paketvermittelte Netze – Wozu segmentieren?

- **Beispiel:** 5-Mbit-Nachricht mit 1 Mbit/s übertragen dauert 5 Sekunden
- **Unsegmentierte Übertragung:** Sequentielle Übertragung der Nachricht von Hop zu Hop. Gesamtdauer hier 15 s.
- **Segmentierung** der Nachricht in 5 Segmente à 1 Mbit (Bild rechts unten). Jedes Segment wird in 1 s pro Hop übertragen. Gesamtdauer hier 7 s. Kleinere Übertragungszeit durch parallele Übertragung
- **Ausserdem:** Bei einem Bitfehler muss nur ein Segment und nicht die gesamte Nachricht neu übertragen werden.



In jedem Vermittlungsknoten einer paketvermittelten Netzes wird der Ausgangsport und damit der weitere Weg neu bestimmt.

Diese Aufgabe übernehmen sogenannte "**geroutete Protokolle**" (IP, IPX, Apple Talk, ...)

Die gerouteten Protokolle benutzen dazu die sogenannte **Routing-Tabelle**, die für alle Ziele den u.a. den besten Ausgangsport angibt.

Die Routing-Tabelle wird manuell durch Konfiguration (**statisches Routing**) oder durch sogenannte **Routing-Protokolle** erstellt und gepflegt (**dynamisches Routing**)

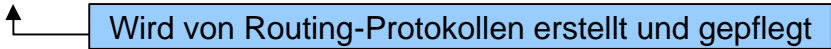
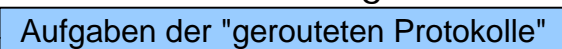



Vorteil: Ausfall von Netzressourcen führt automatisch zu einem Update der Routing Tabelle.

Nachteil: Die Routing-Protokolle konsumieren Rechenleistung und Übertragungskapazität.

Paketvermittelte Netze werden bezüglich Routing in **2 Klassen** eingeteilt:

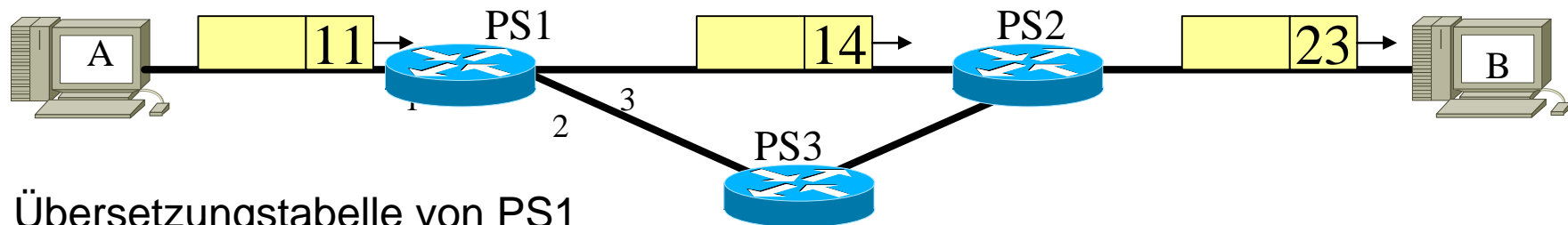
- Datagramm-Netzwerke und
- Virtual-Circuit(VC)-Netzwerke

Funktionsweise und Eigenschaften

- Die Paket-Vermittler **speichern keine Zustandsinformationen** über die **über** sie laufenden **Verbindungen**. Sie kennen sie nicht einmal.
- Sie treffen die **Routing-Entscheidung unabhängig und neu für jedes Paket**.
- leiten Pakete anhand der **Hostzieladresse** weiter.
- Die Hostzieladresse wird jedem Paket in einem Kopfteil (**Header**) vorangestellt.
- Die Hostadresse muss **global eindeutig** sein und eine **hierarchische Struktur** haben.
- Jeder Paket-Vermittler (**packet switch**) hat eine **Routing-Tabelle**, die Zieladressen oder Teile davon einer Ausgangsleitung zuordnen. 
- Im Header ankommender Pakete wird die Zieladresse gelesen und in der Routing-Tabelle der passende Ausgang ermittelt (**route lookup**). 
- Dann wird das Paket in die Warteschlange dieser Ausgangsleitung eingefügt und abgesendet (**packet forwarding**). 
- Bei von Verbindungen oder Vermittlern kann sich auch der Weg zum gleichen Ziel für nachfolgende Pakete ändern (**dynamisches Routing**). 
- Bei mehreren gleichwertigen Wegen zum Ziel können die Pakete auch kontrolliert aufgeteilt werden (**load sharing**). 
- **Beispiele:** Postdienst, Internet

Paketvermitteltes Netz – Routing – VC-Netzwerke

- Jeder Packet-Switch kennt alle über ihn laufenden VCs und führt Zustandsinformationen
- VC-Netzwerke bilden virtuelle Schaltkreise aus
 - (1) einem Pfad zwischen dem Quell- und Ziel-Host der markiert wird mit
 - (2) Einträgen in den VC-Nummernübersetzungstabellen und der gefunden wird mit Hilfe von
 - (3) virtuellen Schaltkreisnummern im Header (eine Nummer pro Verbindungsabschnitt) in jedem Packet Switch auf dem Pfad.
- Ein VC hat auf jeder Verbindungsleitung eine neue Nummer. Die Packet-Switche müssen nach jedem Hop im Header die alte durch die neue Nummer ersetzen.



Übersetzungstabelle von PS1

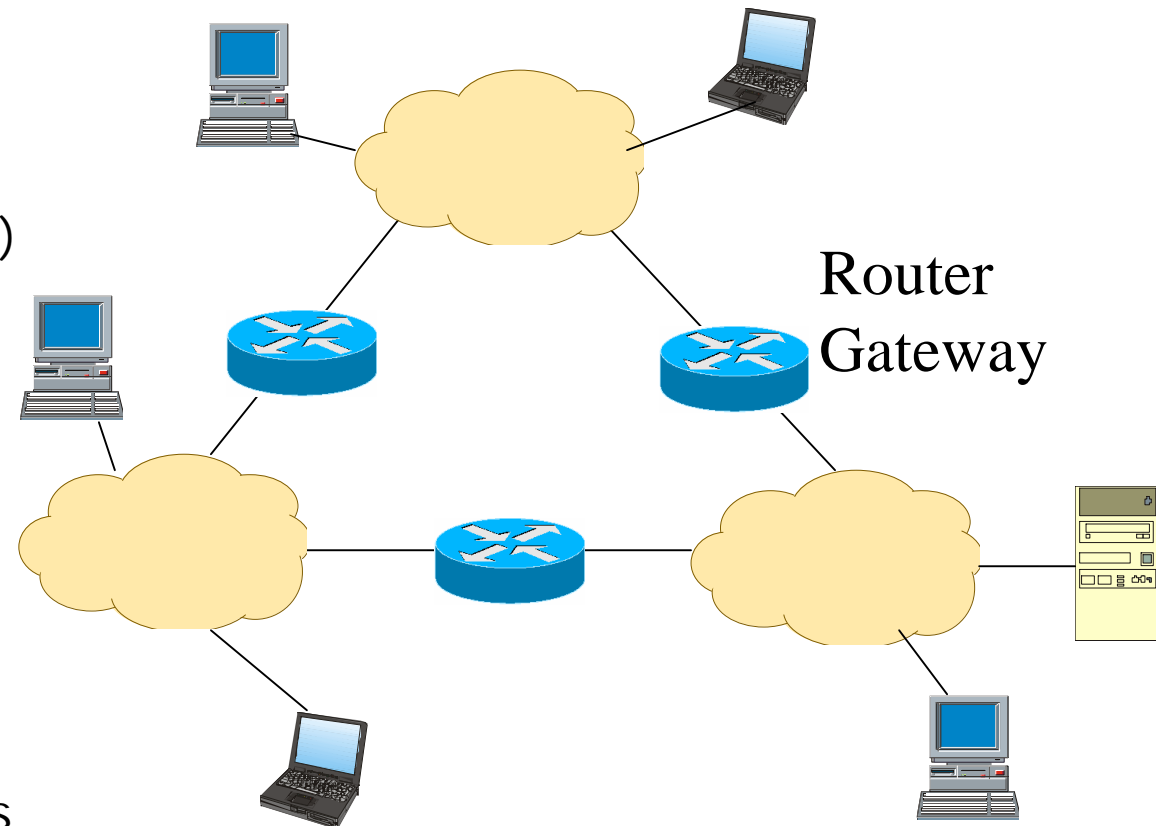
Eingangs-Schnittstelle	Nr. des Eingangs-VC	Ausgangs-Schnittstelle	Nr. des Ausgangs-VC
1	11	3	14
2	46	3	25
2	22	1	12
...

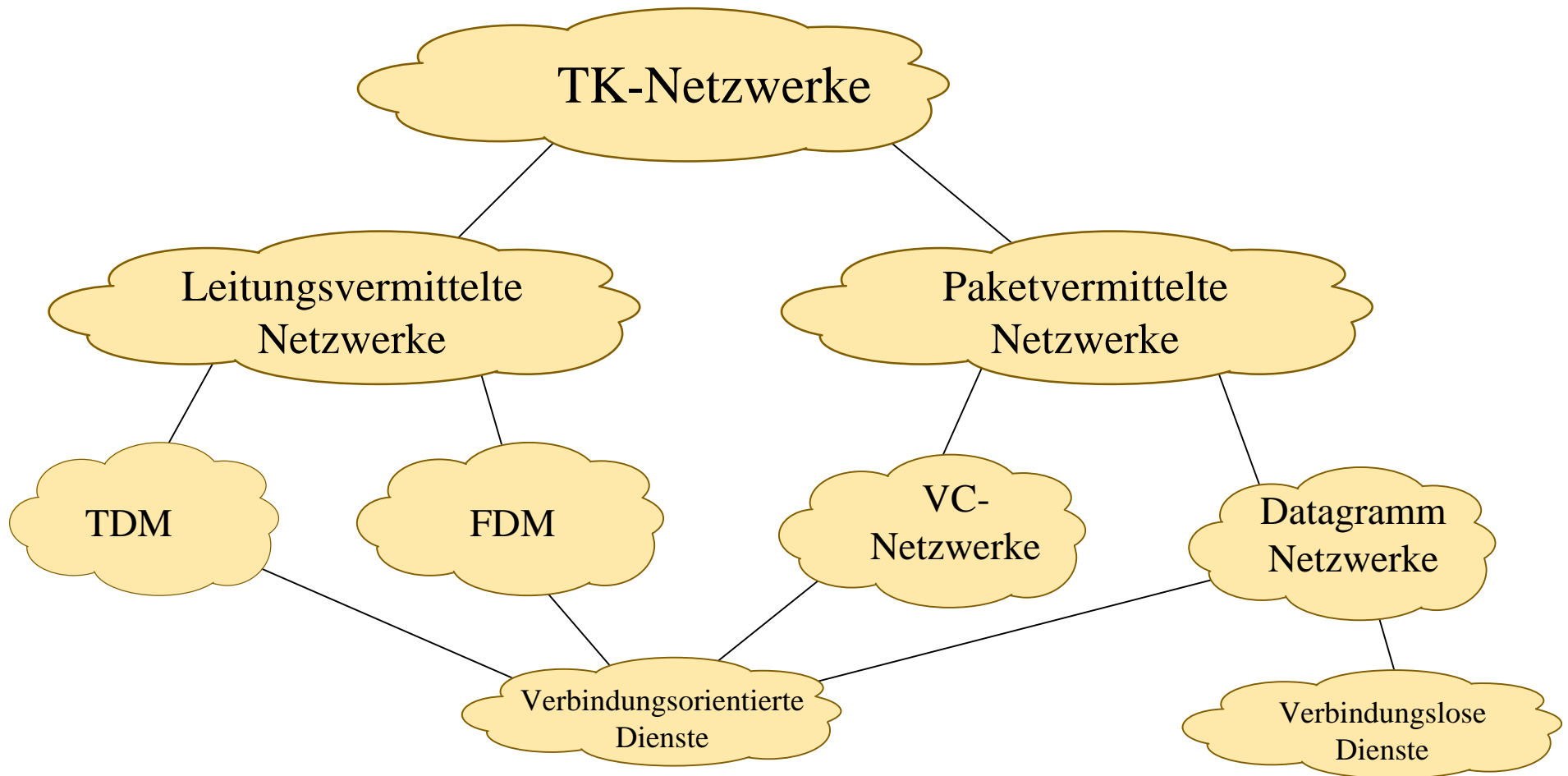
- VCs werden zu Beginn der Verbindung aufgebaut, indem die VC-Nummern in die Nummerntabellen aller beteiligten Switches eingetragen werden (**Verbindungsaufbauphase**)

VCs werden nach Verbindungsende abgebaut, indem die Einträge wieder entfernt werden (**Verbindungsabbauphase**)

- **Permanent Virtual Circuits (PVCs)** werden wie eine Festverbindung einmalig vom Netzadministrator oder einem Netzmanagementsystem aufgebaut.
- **Switched Virtual Circuits (SVCs)** werden bei jedem Verbindungswunsch neu aufgebaut.
- Dadurch, dass die **VC-Nummern nur von lokaler Bedeutung** sind, vereinfacht sich das Netzwerkmanagement erheblich.
- Alle **Switches verwalten Zustandsinformationen** über ihre Verbindungen.

- Mehrere unabhängige Netze mit direkter oder indirekter Konnektivität (ggf. verschiedener Technologien) werden zu einem **Internetnetwork** verbunden
- Knoten, die an mehr als ein Netzwerk angeschlossen sind nennt man **Router** oder **Gateway** (Vermittlungsknoten)
- Alle Hosts müssen eine global eindeutige Netzwerkadresse haben
- Die systematische Ermittlung des optimalen Weges zum Ziel nennt man „**Routing**“



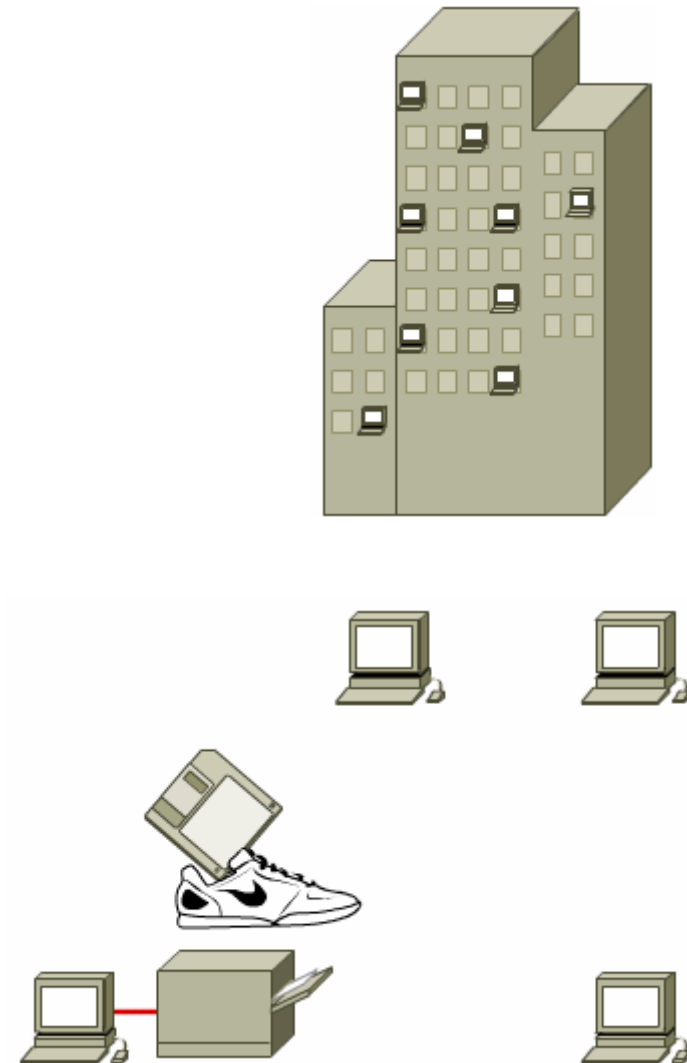


- 1969 wurde das ARPANET (Advanced Research Project Agency Network) aufgebaut. Drei Universitäten wurden über 56 kbit/ s- Mietleitungen vernetzt. Dienste: telnet, ftp
- Initiiert und bezahlt vom Department of Defense (DoD) . Ziel: robustes, leistungsfähiges und bezahlbares Netz.
- 1971: Email
- 1973: TCP/ IP- Protokolle
- 1983: Trennung in Milnet und Arpanet, Begriff Internet wird eingeführt und der Internetadressendienst Domain Name Service (DNS).
- 1988: erste Internetprovider in DE
- 1989: ARPANET wird aufgelöst, die National Science Foundation (NSF) übernahm die Verantwortung. Ziel: wissenschaftlichen Einrichtungen, Schulen und interessierten Bürgern einen Zugang zu diesen modernen Technologien möglich zu machen.
- In Deutschland betreibt der DFN- Verein (**D**eutsches **F**orschungs**N**etz <http://www.dfn.de/> ; 1984 vom BMFT gegründet) das sogenannte WIN (X. 25- basiertes Wissenschaftsnetz). Dieses Netz wird durch Hochschulen und andere wissenschaftliche Einrichtungen für Datenübertragung und als Internetzugang genutzt.

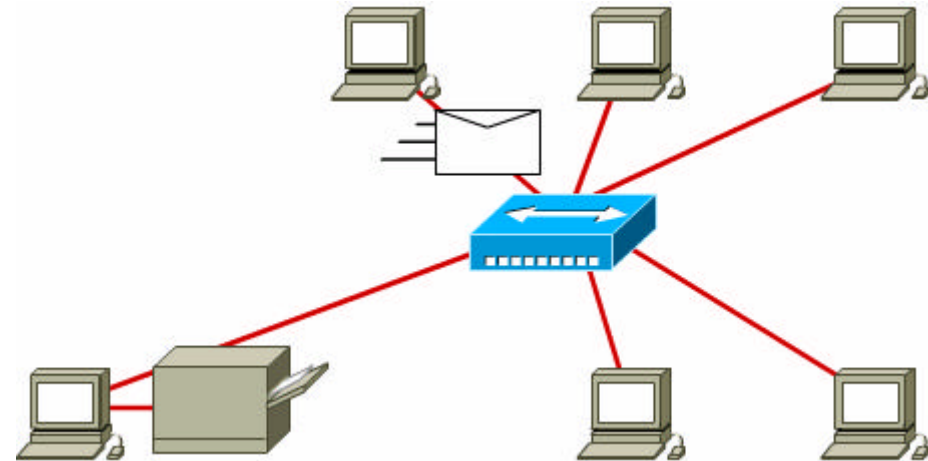
- 1992 Gründung der **Internet Society** (www.isoc.org):
 - Verband mit mehr als 150 Mitglieds-Organisationen und 16000 Mitgliedern in mehr als 180 Ländern
 - Verantwortlich für die Weiterentwicklung des Internet
 - Dachverband des IAB, IETF, IRTF, IESG
- **Internet Architecture Board** (www.iab.org)
- berät die ISOC
- beaufsichtigt das IETF (Standardisierungsprozeß, Protokollarchitekturen,...)
- schlichtet Beschwerden über Standardisierungsprozeß
- Herausgeber der RFCs
- verwaltet IETF Protokollparameter (RFC 1700)

- für die technische Weiterentwicklung zuständig. Im IAB gibt es zwei Gremien:
 - **Internet Engineering Task Force** (www.ietf.org) für kurzfristige technische Entwicklungen,
 - **IRTF** (Internet Research Task Force) für langfristige technische Entwicklungen.
 - **IANA** Internet Assigned Numbers Authority
 - **DENIC** (DE Network Information Center)
- Das Internet ist ein „anarchisches“ Netz, es wird nur reguliert und (im öffentlichen Teil) nicht reglementiert.
Verhaltenskodex: „Netiquette“.
- Technische Festlegungen werden als **RFCs** (Request for Comment) bezeichnet:
 - derzeit gibt es ca. 6000,
 - ~50 RFCs sind Internetstandards.
- RFC's sind frei verfügbar. Jeder kann RFC einreichen. Das IAB prüft.
 - Wenn sinnvoll: Proposed Standard
 - Liegen mindesten zwei unabhängige Implementierungen vor, die zusammenarbeiten: Draft Standard
 - Erfolgt nennenswerte Anwendung: Internetstandard

- Standalone-Geräte
- Zögernder Einsatz von PCs in Unternehmen
- Keine Vernetzung, Disketten dienten dem Datenaustausch (Turnschuhnetze, „Sneaker-Net“)
- Beschleunigtes Wachstum der Computerbranche durch erste Rationalisierungseffekte in den Unternehmen
- Aber: Viele neue, aber inkompatible Technologien (Chaos)



- Mitte 80er Jahre
 - Abteilungsweite lokale Netze (LANs) entstehen
 - Abteilungsintern gemeinsamer elektronischer Zugriff auf Dateien und Drucker
 - Ersatz von Standalone-Druckern durch schnelle Netzwerkdrucker
 - Aber: Immer noch Turnschuh-Vernetzung zwischen den Abteilungen/Standorten



- Gründe für Nachfrage nach Inter-LAN-Kommunikation (Internetworking):
 - Unmöglichkeit jederzeit mit jedem überall zu kommunizieren
 - Ineffektive Ressourcennutzung
 - Fehlen eines zentralen Netzwerkmanagements
- Deshalb seit Anfang 90er Jahre
 - Vernetzung der LAN-Inseln
 - Stadtnetze (Metropolitan Area Networks; MANs) und
 - Weitverkehrsnetze (Wide Area Networks; WANs)

