

Kommunikation in Rechnernetzen

1 NETZWERKMODELLE

- 1.1 P2P (Peer to Peer)
- 1.2 Client-Server

2 GRÖßENORDNUNGEN

LAN / MAN / WAN

3 NETZWERKARCHITEKTUR

- 3.1 Netzwerktopologien
(Bus / Stern / Ring)
- 3.2 Übertragungsmedien
(NIC / BNC / UTP / STP)
- 3.3 Zugriffsverfahren
(CSMA/CD - TokenRing)

4 NETZWERKPROTOKOLLE

- 4.1 Leitungs-/ Paketvermittlung
- 4.2 OSI - Schichtenmodell
- 4.2 Adressierung
(TCP/IP - DNS - DHCP)

5 INTERNET und seine DIENSTE

- 5.1 FTP / Telnet / Email / News
- 5.2 WWW / Gopher / Wais

6 SICHERHEIT

- 6.1 Kryptographie
(DES / RSA / PGP)
- 6.2 Firewall / HTTPS

Netzwerk - Definition & Motivation

Netzwerk: Gruppe miteinander verbundener Systeme mit folgenden Komponenten:

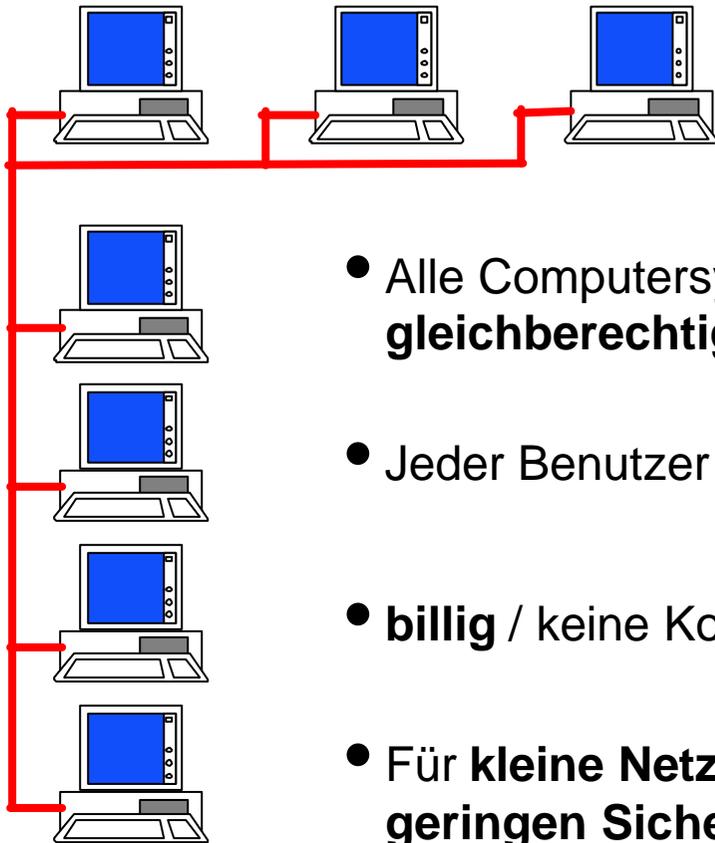
- **Gemeinsame Nutzung** von Daten, Software, Hardware
- **Übertragungsmedium** = Physikalische Verbindung
- **Protokolle** = Kommunikationsregeln

Vorteile einer Rechnernetzung / Motivation

- **Datenverbund** (Bibliotheken, Verwaltungsdaten)
- **Funktionsverbund** (gemeinsame Ressourcennutzung Software und Hardware)
- **Lastverbund** (Prozessorleistung)
- **Verfügbarkeitsverbund** (bei Ausfall eines Einzelsystems)
- **Kommunikation** (Informationsaustausch / Mail)
- **Datensicherung**
- **Systemwartung**

Netzwerkmodell P2P (Peer to Peer)

[Peer = Gleichwertiger]

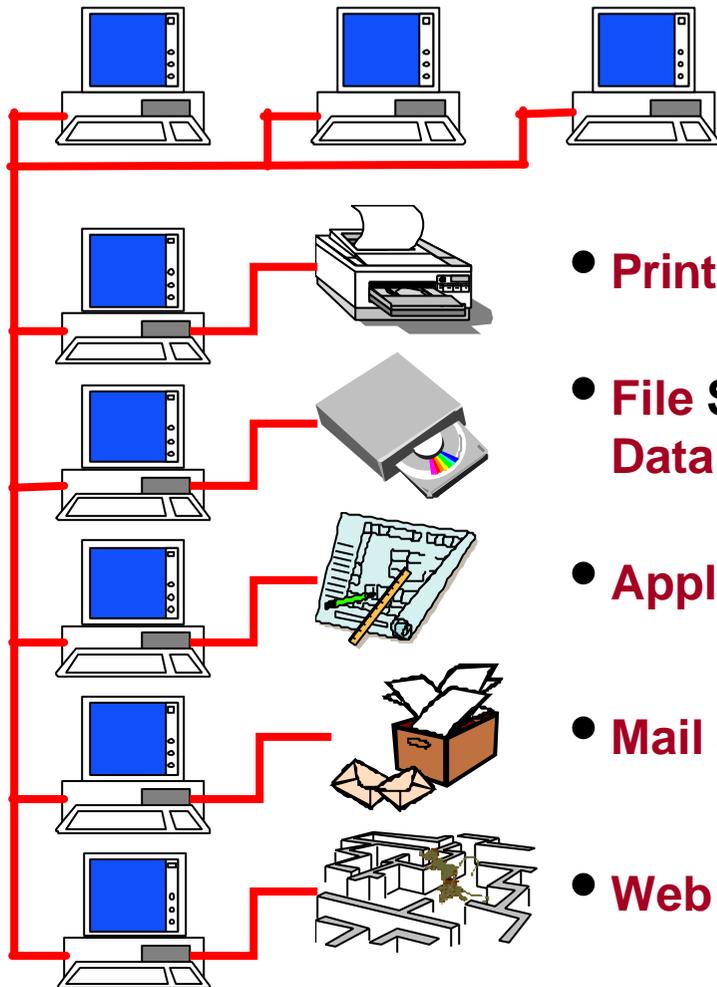


- Alle Computersysteme sind **gleichberechtigt (Workgroup)**
- Jeder Benutzer ist **eigenverantwortlich**
- **billig** / keine Kosten für Server & Administration
- Für **kleine Netze (<10)** mit **geringen Sicherheitsanforderungen)**

Beispiele: Windows for Workgroups, Win95, Windows NT Workstation, Novell Personal NetWare, Apple Talk, Atisoft LANtastic

Netzwerkmodell Client-Server

Spezialisierte Server [= Diener] stellen den mit ihnen verbundenen **Clients** [= Kunden] verschiedene Dienste zur Verfügung



- **Print Server**
 - **File Server**
 - **Data base Server**
 - **Application Server**
 - **Mail Server**
 - **Web Server**
- Großer **Arbeitsspeicher** RAM (Rand. Acc. Memory)
 - Hohe **Fehlertoleranz** RAID [Redundant Area of Inexpensive Disks]
 - Leistungsfähiger **Prozessor**

Bsp.: Windows NT Server, Novell NetWare, Unix, Linux, Open VMS, IBM OS/2 LAN Server

Netzwerktopologie (LAN): BUS

Vorteile

Niedrige Kosten,
da geringe Kabelmengen

Hohe Modularität
leichte Erweiterbarkeit

Ausfall einer Station
unproblematisch

Nachteile

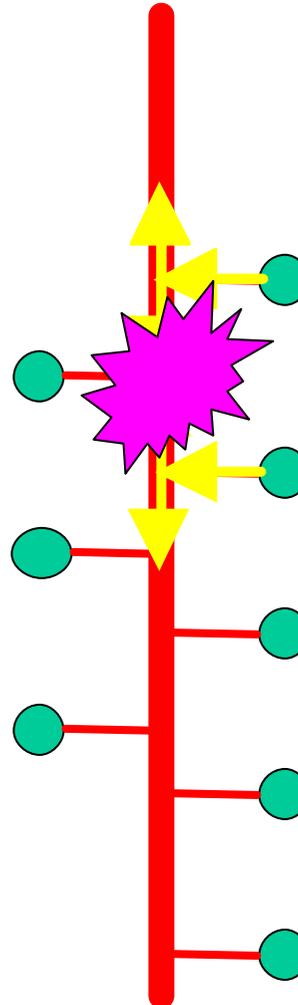
Hoher Datenverkehr,
da Diffusionsnetz

Hohe Kollisionsrate,
(überprop. zur Anz. d. Stationen)

Bus ist **Flaschenhals**

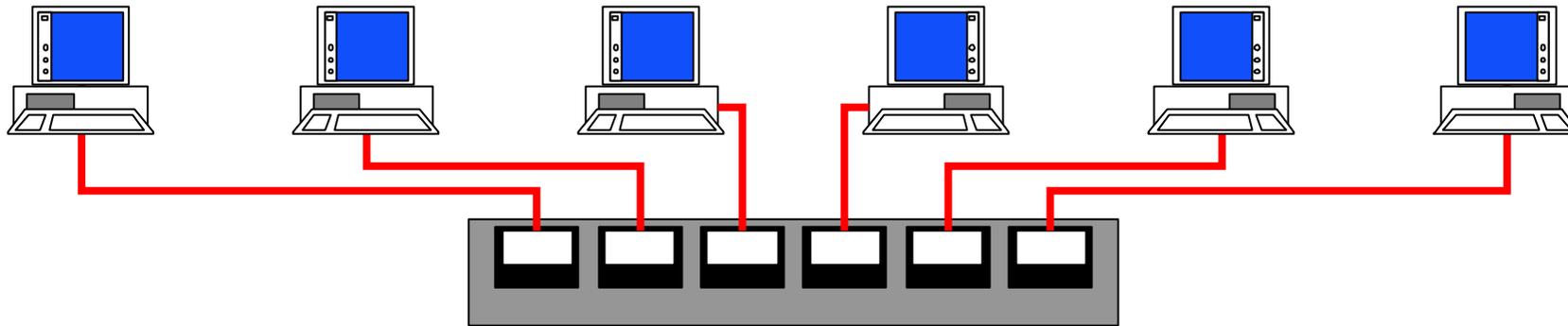
Busdefekt setzt Strang,
meist ganzes Netz lahm

Fehlersuche aufwendig



Netzwerktopologie (LAN): STERN

Punkt zu Punkt Verbindung jeder einzelnen Station mit einem



HUB

Vorteile

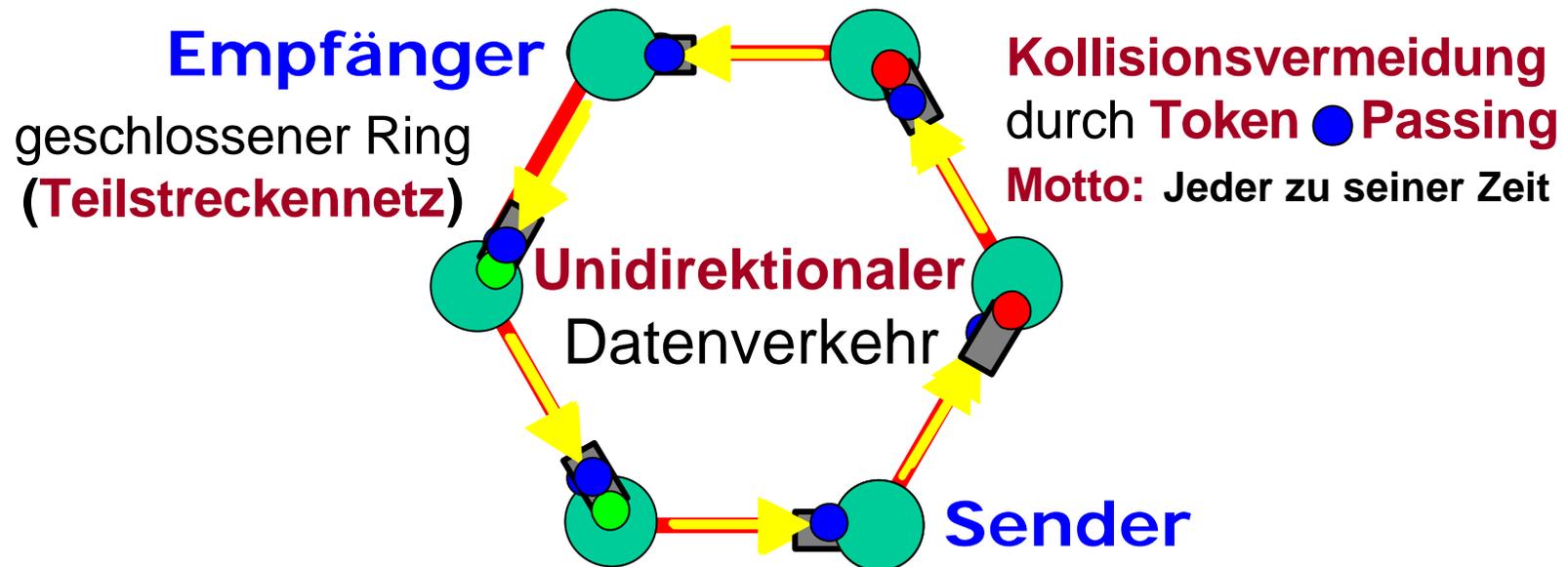
- **Ausfall einer Station unproblematisch**
- **leicht erweiterbar**
- **hohe Datendurchsatzraten**
- **Verteiler (Hub) wirkt auch als Verstärker (Repeater)**

Nachteile

- **Totalausfall des gesamten Netzes bei Ausfall des Verteilers (Hub)**
- **große Kabelmengen**
- **Hub ist Flaschenhals**
- **Weiterhin Kollisionen (Hub)**

Netzwerktopologie (LAN): RING

Punkt zu Punkt Verbindung zwischen benachbarten Stationen



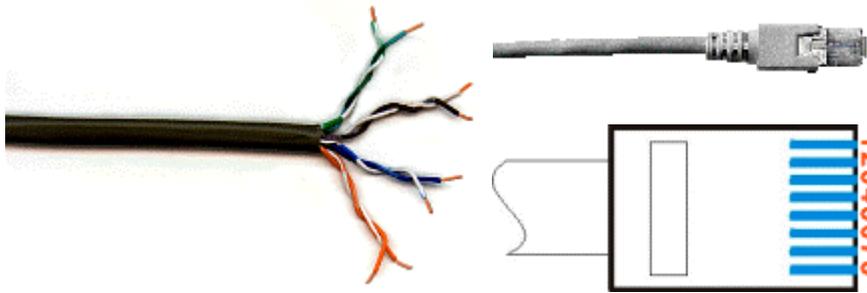
Nachteile = Nachteile des Bussystems

- **Totalausfall** des gesamten Netzes bei **Ausfall einer einzelnen Station**
- Aufgrund des **hohen Aufwands bei der Kabelverlegung** erscheint diese Topologie **physikalisch selten**, wird jedoch **logisch** durch zentralen **Ringverteilungsleiter** (IBM-Z-Ring / Token-Ring) realisiert.

physical layer / ethernet



BNC / 10Base2



**Twisted Pair
10BaseT (UTP/STP)
100BaseTX**



Fiber/ 100BaseFX



NIC Network Interface Card

- Ethernet Address bzw. MAC (media access control)

http://www.coffer.com/mac_find/

Netzwerk-/Übertragungsprotokolle

Def: Ein Protokoll ist ein **Regelwerk**, welches die **Kommunikation** zwischen Subjekten **steuert**.

Der Begriff stammt aus der Diplomatie und bezeichnet hier ein **diplomatisches Zeremoniell**:

- Reihenfolge der Begrüßung / Händeschütteln
- Vorstellung / Anredetitel etc...

Leitungs- / Nachrichten- / Paketvermittlung

Je nach **Aufbau / Ablauf / Beendigung** der Verbindung unterscheidet man

- **Leitungs-** vermittlung
- **Nachrichten-** vermittlung
- **Paket-** vermittlung

Netzwerk-/Übertragungsprotokolle

Leitungs- / Nachrichten- / Paketvermittlung

Leitungs- vermittlung (Telefon/Funk/Fax)

Def: **Stehende** Verbindung zwischen Sender und Empfänger während der **gesamten** Verbindungsdauer:

- **bidirektional** z.B. Telefon (**Protokoll ?**)
 - Hallo, hier ist ... ! (**Sender**)
 - Könnte ich ... (**Empfänger**) sprechen!
.....Gespräch.....
 - Danke! Auf Wiederhören ! (**Ende**)
- **unidirektional** z.B. Fax / Funk (**Protokoll ?**)
 - Whiskey, Alpha, Charly (**Sender**)
ruft ... (**Empfänger**)
 - Roger ! (**Empfangsbestätigung**)
 - Over ! (**Wechsel der Sprechrichtung**)
 - Over and Out ! (**Verbindungsende**)

Netzwerk-/Übertragungsprotokolle

Leitungs- / **Nachrichten-** / Paketvermittlung

Nachrichtenvermittlung (Post/Paketdienst)

Komplette Nachricht wird (unidirektional) auf den Weg geschickt.

- Brief oder Paket (**Nachrichtform** / **Verpackung**)
- Adressierung (**Empfänger** und **Absender**)
- Eilsendung / Luftpost (**Übertragungsform**)
- Post / DHL / Hermes (**Übertragungsdienst**)
- Zustellung (**Postlagernd** / **Briefträger**)
- Empfangsbestätigung (**Einschreiben** / **Nachnahme**)

Nachteile:

- **ineffiziente Nutzung**
der Leitungsbandbreite (Telefon)
- **hohe Sicherheitsmängel**
(Abhören, Abfangen, Manipulieren, Stören)
- **hohe Störanfälligkeit** insbesondere
bei Übertragung größerer Datenmengen

Netzwerk-/Übertragungsprotokolle

Exkurs: Kleine Geschichte des Internet

polemos pater panton
(Heraklit, 544-483 v. Chr.)

1957 Sputnikschock

Gründung der **ARPA**
(Advanced Research Projects Agency)

durch das **US-Verteidigungsministerium**
(Department of Defence)

mit der **Aufgabe**,
Universitäten und private Institute
bei Forschung und Entwicklung
von Technologien zu „unterstützen“,
die **von militärischem Nutzen** sind.

Netzwerk-/Übertragungsprotokolle

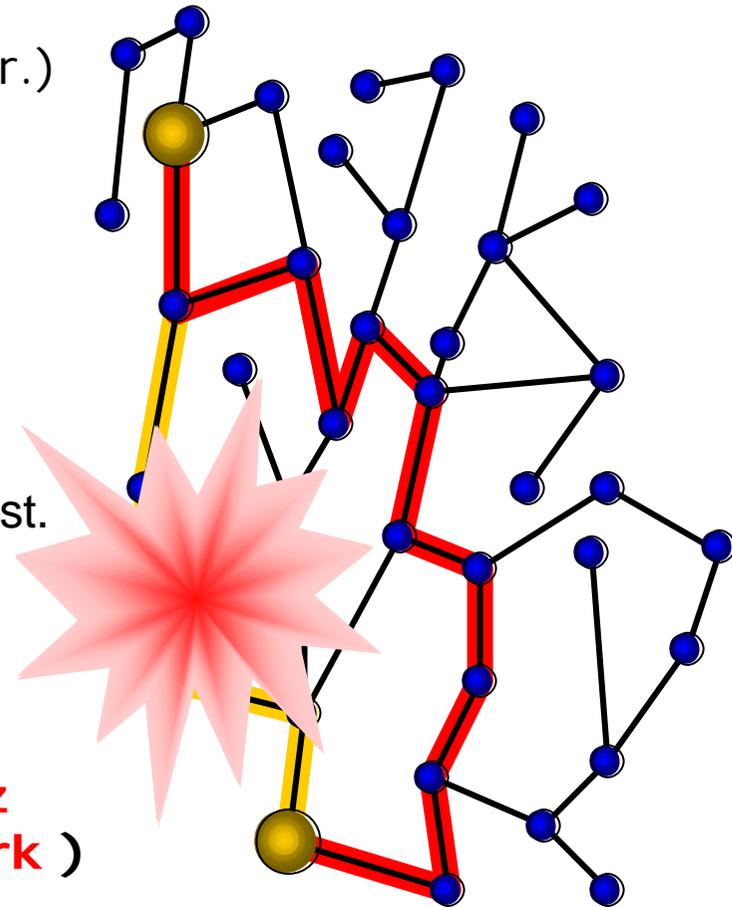
Exkurs: Kleine Geschichte des Internet

polemos pater panton
(Heraklit, 544-483 v. Chr.)

1969 Kalter Krieg

US-Verteidigungsministerium
(Department of Defence) fordert
Netzwerktechnologie,
die in einem hohen Maß
gegen Ausfälle sicher ist.

ARPANET wird von dem
Privatunternehmen BBN
(Bolt, Barenek & Newman)
als **paketvermitteltes Netz**
(**packet-switched network**)
entworfen und implementiert.



Netzwerk-/Übertragungsprotokolle

Leitungs- / Nachrichten- / **Paket**vermittlung

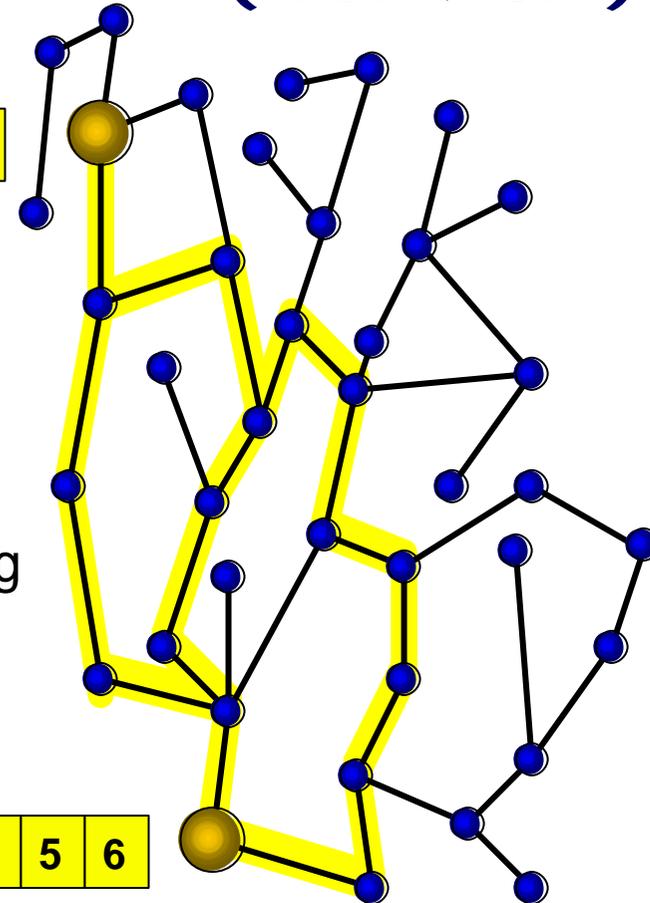
Paket-vermittlung (NCP)

(TCP / IP)

Zwei Partner werden während der Kommunikation nur virtuell miteinander verbunden.

Die zu übertragenden Daten werden vom Absender in **Pakete variabler oder fester Länge** zerlegt und über die virtuelle Verbindung übertragen;

Vom Empfänger werden diese Pakete nach dem Eintreffen **wieder zusammengesetzt**.



Netzwerk-/Übertragungsprotokolle

Exkurs: Kleine Geschichte des Internet

1969 ARPANET mit NCP (*Network Control Protocol*)

- University of California Los Angeles (UCLA)
- University of California Santa Barbara (UCSB)
- Stanford Research Institute (SRI)
- University of Utah

1974 Entwicklung der Protokollfamilie TCP/IP (*Transfer Control Protocol / Internet Protocol*)

Zielsetzung:

- Unabhängigkeit von Netzwerktypen („Netzwerk - Esperanto“)
- Gute Fehlerbehebung (Ausfall einzelner Knoten)
- Behandlung hoher Fehlerraten (Umleitung über andere Knoten)
- Anbindung neuer Subnetze zur Laufzeit
- sehr kleiner Datenüberhang (Header)

Netzwerk-/Übertragungsprotokolle

Exkurs: Kleine Geschichte des Internet

01.01.1983 ARPANET stellt die Annahme von **NCP (Network Control Protocol)** ein und akzeptiert **von nun an nur TCP/IP-Pakete.**

ARPANET wird aufgeteilt in

- einen militärischen Teil (*MILNET*) und
- einen Forschungsteil.

= offizieller Geburtstag des Internet

Durch die ausschließliche Verwendung von TCP/IP als offizielles Protokoll nimmt die Zahl der angeschlossenen Netze rapide zu.
Der Leim, der das Internet zusammenhält, sind die TCP/IP-Protokolle.

OSI Referenzmodell

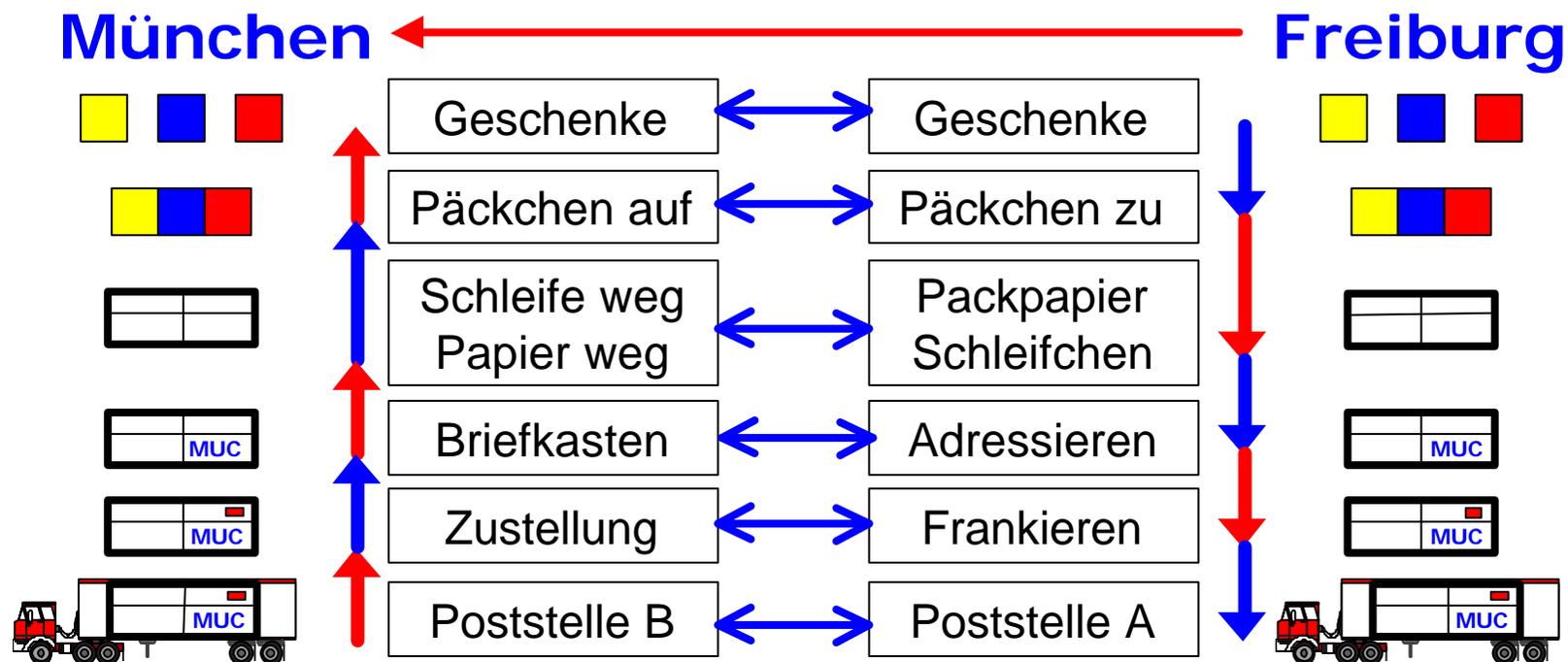
(Open Systems Interconnection)

Schichtenweise Kommunikation

Zielsetzung:

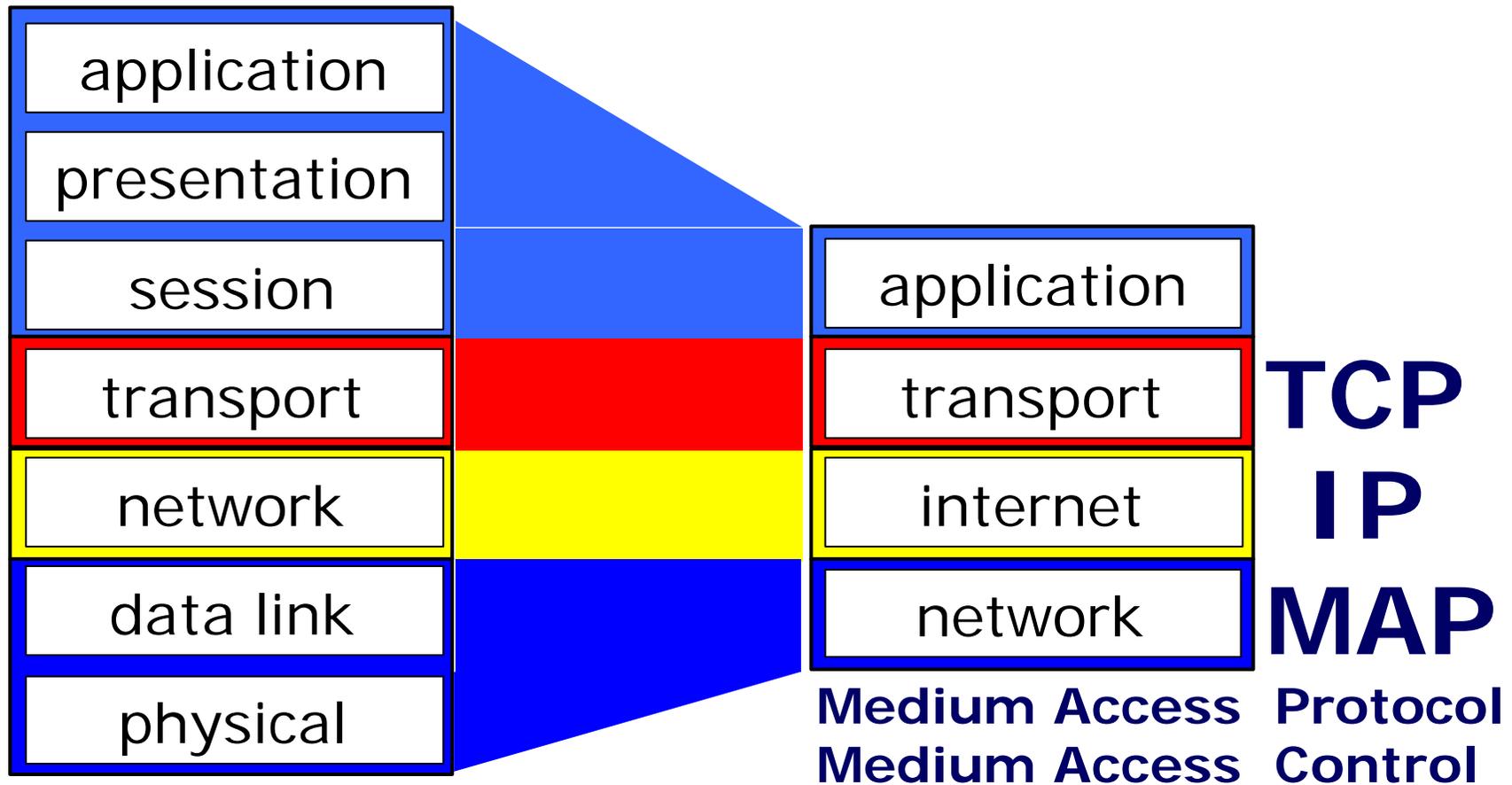
Unabhängigkeit von Netzwerktypen („**Netzwerk - Esperanto**“)
 durch **Modularisierung** der Protokolldienste (**Protokollstapel**)

Beispiel: Familie in Freiburg packt **Geschenkpaket** für die Oma



Übertragungsprotokolle TCP/IP

Ethernet-Frames / network layer

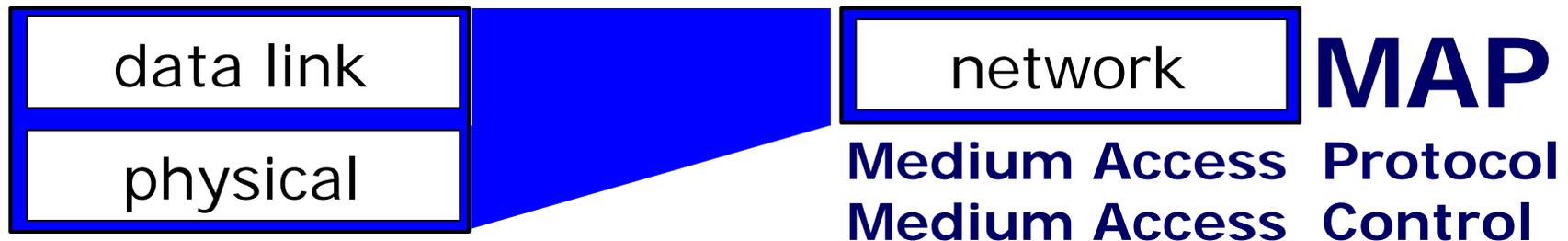


Übertragungsprotokolle TCP/IP

Ethernet-Frames / network layer

- Öffne ein DOS-Fenster: **Start > Ausführen > command**
- Gebe folgenden Befehl ein: **ipconfig/all**
- Notiere folgende Daten: Physikalische Adresse (Netzwerkkarte)
IP-Adresse (Rechner)

```
0 Ethernet Adapter :  
  
Beschreibung. . . . . : PPP Adapter.  
Physische Adresse . . . . . : 44-45-53-54-00-00  
DHCP aktiviert. . . . . : Ja  
IP-Adresse. . . . . : 0.0.0.0  
Subnet Mask . . . . . : 0.0.0.0  
Standard-Gateway . . . . . :  
DHCP-Server . . . . . : 255.255.255.255
```



Übertragungsprotokolle TCP/IP

Ethernet-Frames / network layer

Jede Netzwerkkarte (NIC) ist **weltweit eindeutig** identifizierbar durch die **MAC (Media Access Control) Adresse** = 6 Byte
(**Ethernet address / Token ring address**)

Vendor-ID			NIC-ID		
3 Byte (HEX)			3 Byte (HEX)		
00	20	AF	B7	32	29
00	50	04	8E	95	52
Xerox					
00	00	5A	5A	CD	D0
00	50	8E	8E	95	52

MAC (media access control) lookup:

http://www.coffer.com/mac_find/

Übertragungsprotokolle TCP/IP

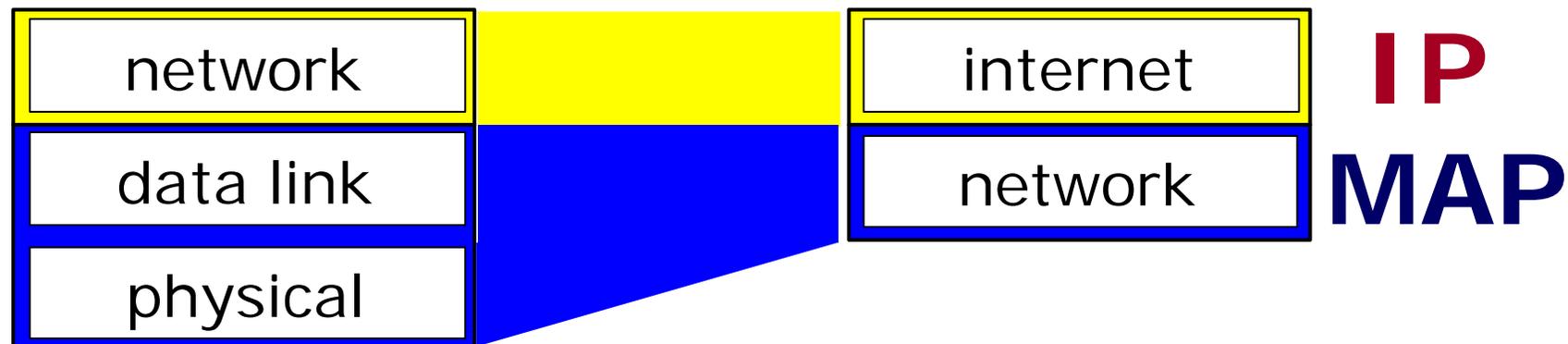
IP-Adressierung / internet layer

Separierung

- der **Netzwerkartenadresse** (**MAC**-address / layer 2 network)
- von **logischer Netzwerkstruktur** (**IP**-address / layer 3 internet)

durch die **IP-address**

32 bit = 4 byte = $4.3 \cdot 10^9$ (IPv4) Adressen



IP-Adressierung / internet layer

IP-Adresse	192	168	1	11
binär	1100 0000	1010 1000	0000 0001	0000 0101
Subnetzmaske	255	255	255	0
binär	1111 1111	1111 1111	1111 1111	0000 0000
Interpretation	192	168	1	11
	Netzwerk - Kennung (net-id)			Rechner- Kennung (host-id)

An den Stellen, wo die Binärdarstellung der **Subnetz-Maske Einsen** hat, stimmen die IP-Nummern von allen Rechnern in diesem Netz überein!

Dies ist die **Kenn-Nummer für das Netz: net - id**

An den Stellen, wo die Binärdarstellung der **Subnetz-Maske Nullen** hat, unterscheiden sich die IP-Nummer verschiedener Rechner dieses Netzes.

Dies ist die **Kenn-Nummer des Rechners: host - id**

IP-Adressierung / internet layer

Feste IP-Adresse

Dem Rechner ist eine feste IP-Adresse zugeordnet.

- Der Rechner kann immer unter derselben Adresse erreicht werden.

Dynamisch IP-Adresse

Bei jeder Einwahl bekommt der Rechner vom Provider eine neue IP-Adresse **zugeteilt**.

- Rechner sind nicht mehr eindeutig identifizierbar.
- Nicht geeignet für Webserver usw.

Adresstranslation (NAT)

Die Rechner im lokalen Netzwerk haben nicht öffentliche IP-Adressen.

Sie gehen **über einen Proxyserver ins Internet**. Der Proxyserver gibt die Anfrage unter seiner eigenen öffentlichen IP-Adresse weiter und leitet die eingehende Antwort wieder an den anfragenden Rechner weiter.

- Es wird **nur eine öffentliche IP-Adresse** für den Proxyserver benötigt.
- Die Rechner im lokalen Netz sind **von außen „unsichtbar“**.

IP-Adressierung / internet layer

IP network commands: **ping**

Untersuche deine Netzwerkverbindung:

Sende ein **ping** in der DOS-Eingabeaufforderung an:

- **localhost (127.0.0.1)**
- deine **eigene IP-Adresse**
- die IP-Adresse deines **Nachbarn**
- einen anderen **Rechner im Rechnerraum**
- an die Adresse des **DHG-Gateway (ipconfig)**
- an die IP-Adresse **209.85.135.99**
- an die IP-Adresse **129.143.236.13**

Untersuche mit deinem Webbrowser, wer sich hinter den letztgenannten IP-Adressen verbirgt: **http:// IP-address**

Routing im Internet

Wie findet ein IP Paket den Weg zum Zielrechner?

Bildung von **Subnetzen**, welche über **Router** miteinander verbunden sind.

Innerhalb einer Collision Domain (**eigenes Subnet**):

- Rechner startet eine **ARP (Address Resolution Protocol)-Anfrage** im lokalen Ethernet-Netzwerk, wer die Ziel-IP-Adresse besitzt (**ethereal: "Who ist IP 192.186.1.11?"**).
- Der Zielrechner meldet seine Netzwerkkartenadresse (MAC-Adresse).
- Datenpaket wird **direkt an die MAC-Adresse** (Netzwerkkarte) geschickt.

Zieladresse außerhalb des eigenen Subnet

Datenpaket wird mit der IP-Adresse des Zielrechners an die **MAC-Adresse des Routers (Standard-Gateway)** geschickt, der es dann weiterleitet.

Routing im Internet

Wie findet ein IP Paket den Weg zum Zielrechner?

1. Subnet von A bestimmen

A	192.168. 1.11		11000000	10101000	00000001	00000101
AND	<u>255.255.255. 0</u>	Mask	<u>11111111</u>	<u>11111111</u>	<u>11111111</u>	<u>00000000</u>
	192.168. 1. 0	Subnet	11000000	10101000	00000001	00000000

2. Ist B Teil des Subnet?

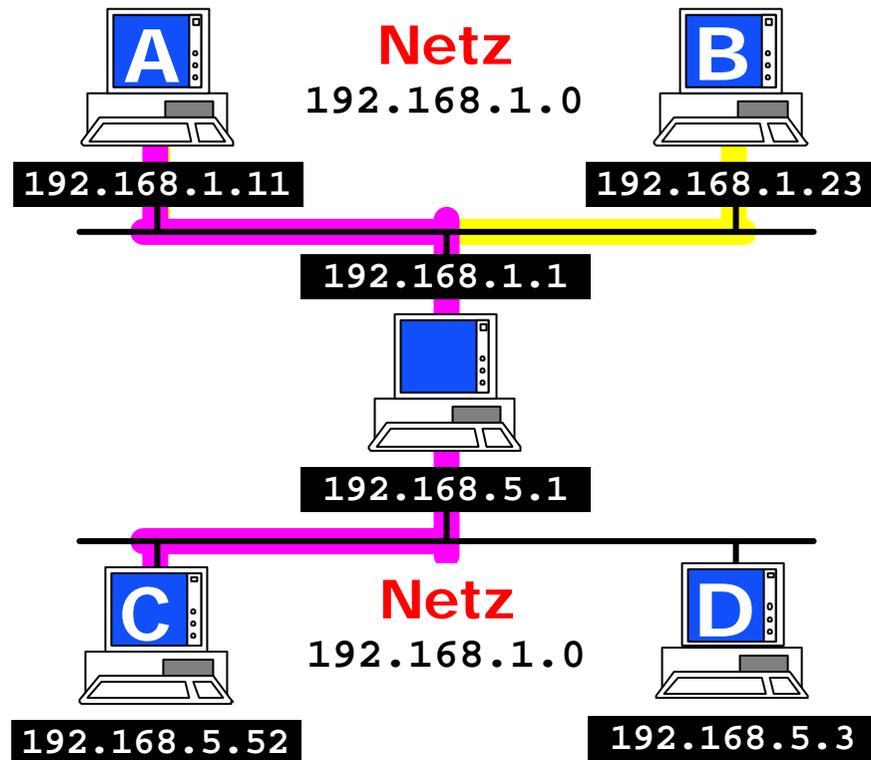
B	192.168. 1.23
AND	<u>255.255.255. 0</u>
	192.168. 1. 0

ja \Rightarrow direkte MAC-Zustellung

3. Ist C Teil des Subnet?

C	192.168. 5.52
AND	<u>255.255.255. 0</u>
	192.168. 5. 0

nein \Rightarrow Sende an Router

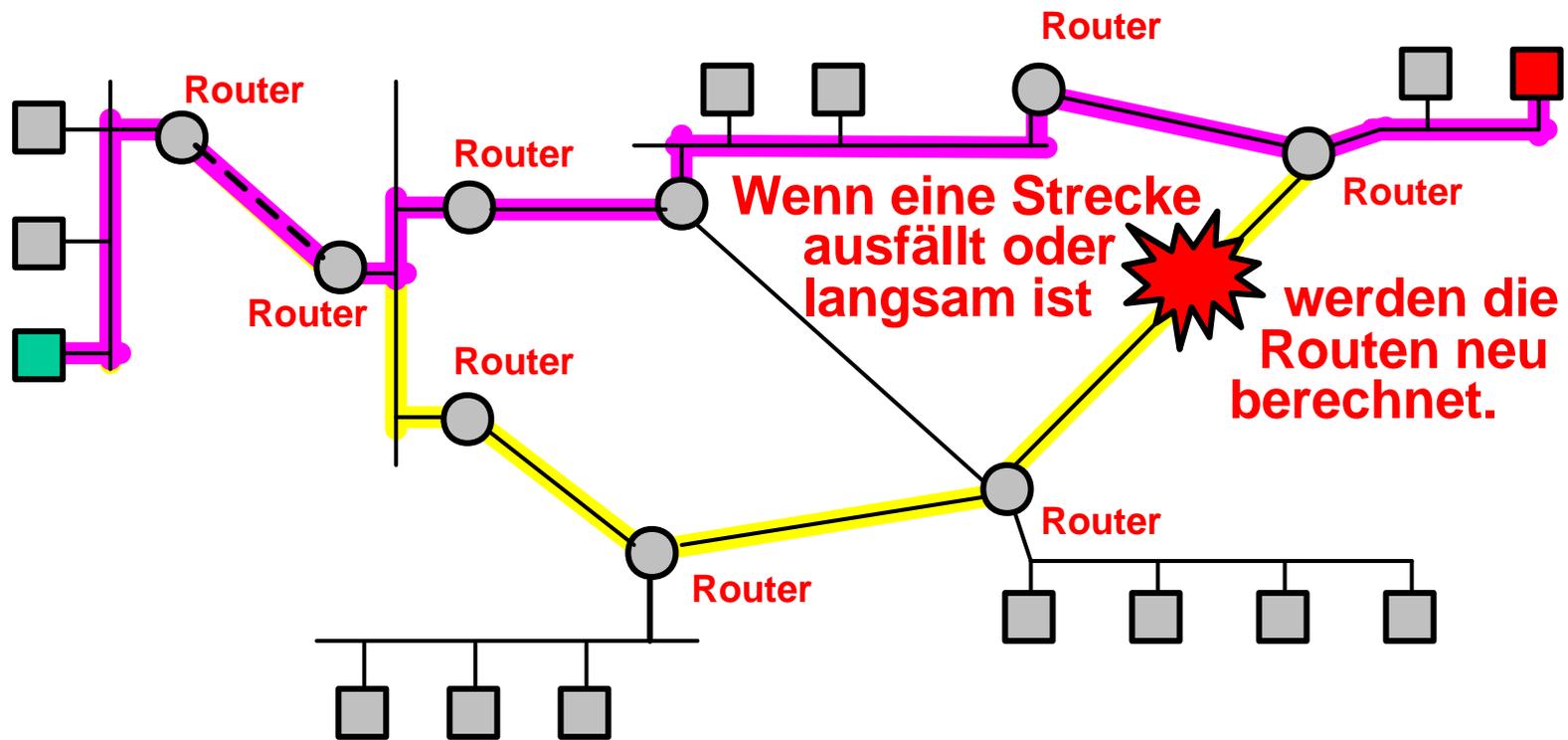


Routing im Internet

Wie findet ein IP Paket den Weg zum Zielrechner?

Die Frames müssen eventuell über viele Netzwerke geleitet werden.

Die **Router** berechnen hierbei **den günstigsten Weg**.



Routing im Internet

Wie findet ein IP Paket den Weg zum Zielrechner?

Die Router führen sogenannte Routingtabellen.

Statisches Routing

- Die **Routing Tabellen** werden von Hand erstellt.

Dynamisches Routing

- Benachbarte Router kommunizieren miteinander über spezielle Protokolle und tauschen dabei **Routinginformationen** aus.
- Nach speziellen Algorithmen berechnen sie gemeinsam den günstigsten Weg und speichern diesen in ihren Routingtabellen.
- Diese **Routingtabellen** können sehr umfangreich werden. Unter http://www.merit.edu/ipma/routing_table/ sind Snapshots von Routingtabellen einiger wichtiger Router abgelegt in die man somit einen Einblick nehmen kann.

DNS (Domain Name System)

Das Internet Telefonbuch

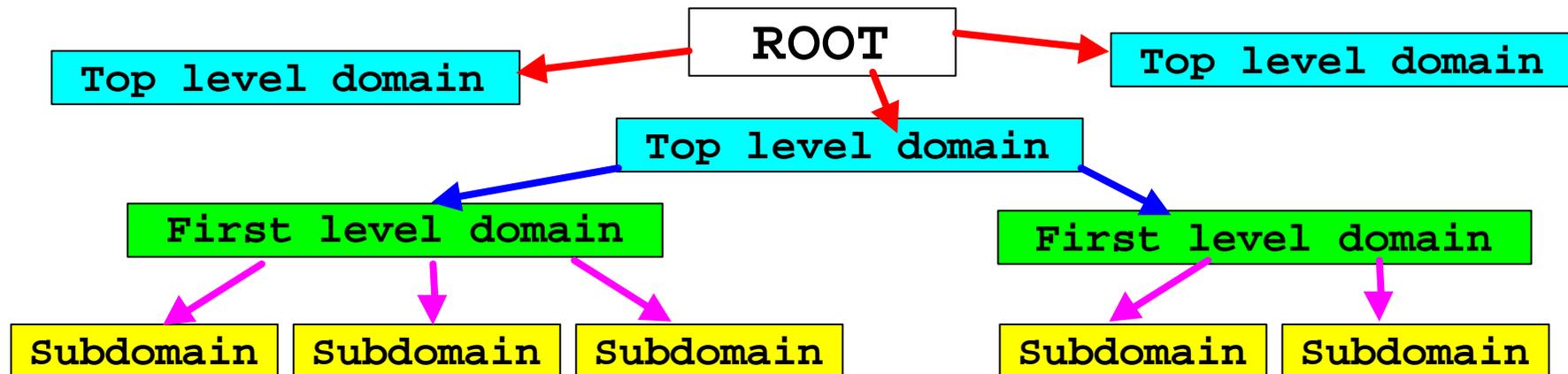
Menschen merken sich
Domain-Namen

Rechner verstehen nur
IP-Adressen

Die Zuordnung
www.schule.de ↔ **129.143.240.23**
erfolgt über das

Domain Name System:

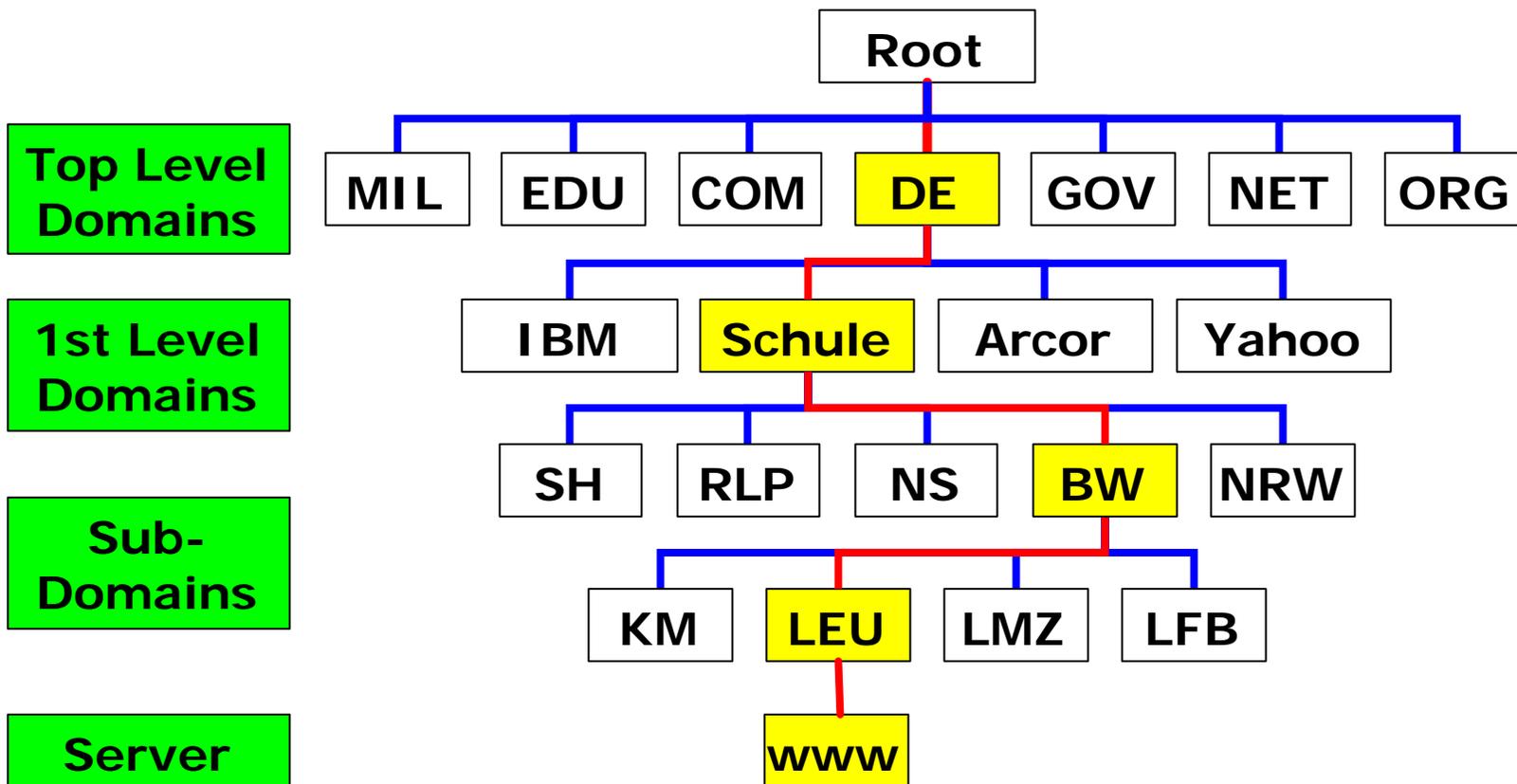
Hierarchischer Aufbau in Baum Struktur



DNS (Domain Name System)

Domain Name = URL (Uniform Resource Locator)

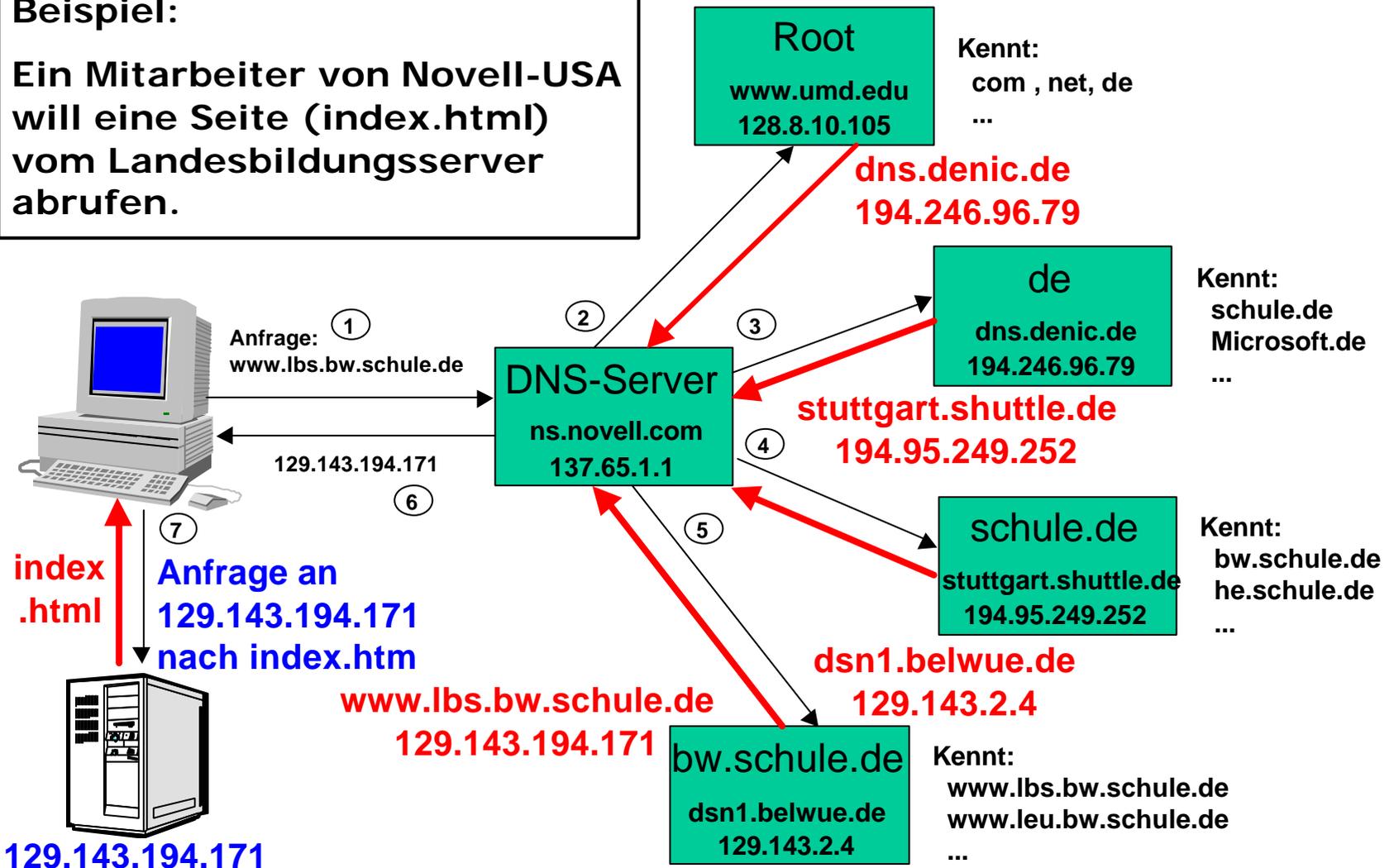
<http://www.leu.bw.schule.de>



DNS (Domain Name System) Abfrage

Beispiel:

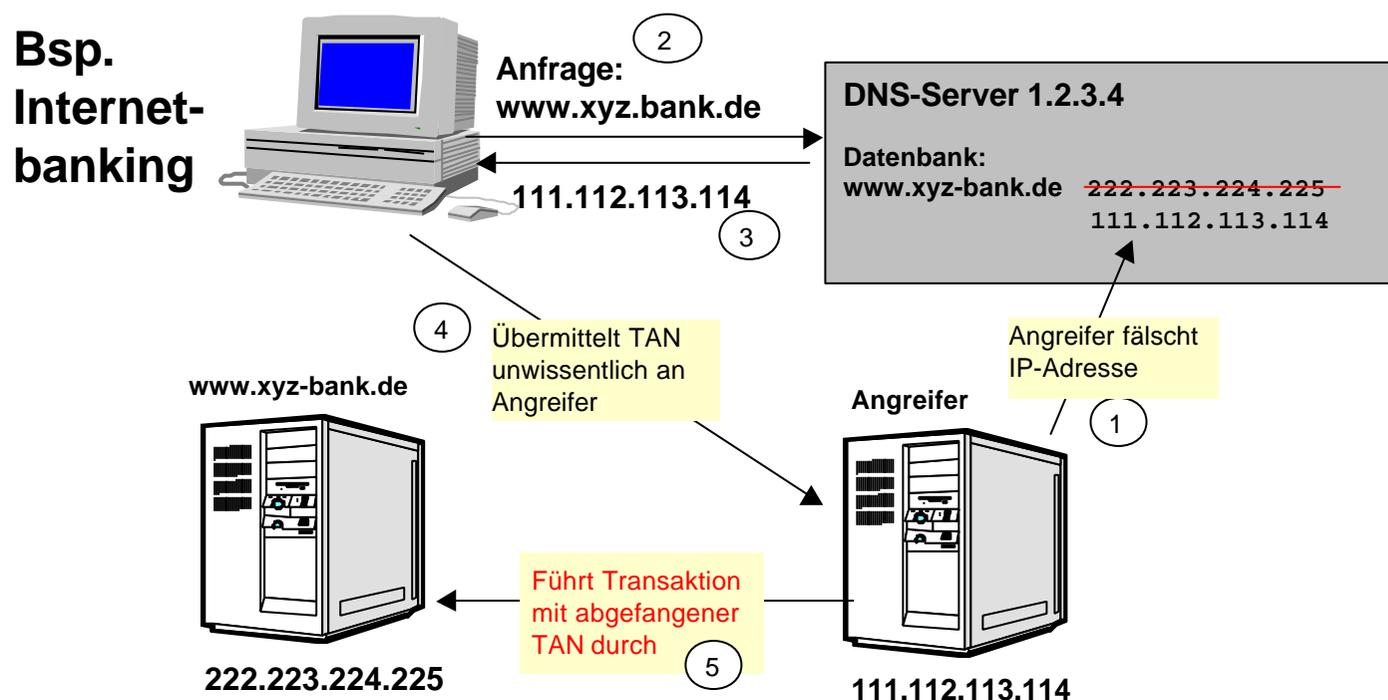
Ein Mitarbeiter von Novell-USA will eine Seite (index.html) vom Landesbildungsserver abrufen.



Sicherheitsaspekte beim DNS

Wenn es einem Eindringling gelingt, einen Adresseintrag in einem primären DNS Server zu verändern, so kann er eine Anfrage auf einen eigenen Web-Server umleiten. Dieser Vorgang wird als DNS-Spoofing bezeichnet.

Nameserver sind besonders sicherheitsrelevante Teile des Internets und müssen deshalb besonders geschützt sein.



Spuren im Netz: IP-Adresse / Domäne

Statische IP-Adressen sind dem **Rechner** zugeordnet
Dynamische IP Adressen werden für eine **temporäre Internetverbindung** vom Provider vergeben.

Sie werden vergeben von der

InterNIC *International Network Information Center*
<http://www.internic.net/>

und ihren regionalen Untergruppierungen:

RIPE *Reseaux IP Europeens*
<http://www.ripe.net/>

DeNIC *Deutsches Network Information Center*
<http://www.denic.de/>

Folgende Informationen können dort abgefragt werden:
Domaininhaber (Vertragspartner), administrativer (**admin-c**) und technischer (**tech-c**) Ansprechpartner sowie Zonenverwalter (**zone-c**)

Spuren im Netz: IP-Adresse / Domäne

z.B.: Abfrage über Domäne **schule.de** bei
DeNIC (Deutsches Network Information Center):

Domaindaten

Domainname: schule.de
Verein zur Foerderung eines Offenen Deutschen Schul-Netzes e.V.

Administrativer Ansprechpartner, technischer Ansprechpartner, Zonenverwalter

Name: Ralph Ballier	admin-c Bevollmächtigter
Kontakttyp: Person	
Adresse: ODS-Verein e.V. - Vorstand - Goldrautenweg 1	tech-c technische Belange
Stadt: Berlin	
PLZ: 12357	zone-c Nameserver
Land: GERMANY	
Telefon: +49 30 6609 8116	
Telefax: +49 30 6609 8125	
E-Mail: ballier@ods.schule.de	

Spuren im Netz: IP-Adresse / Domäne

z.B.: Abfrage über **CallbyCall-Provider Easynet** bei **RIPE (Reseaux IP Europeens)**:

The screenshot shows the RIPE NCC website interface. The top left features the RIPE NCC logo. The main content area displays WHOIS data for the IP address 62.180.192.0 and the route 62.180.0.0/16. Two red circles highlight specific information: the route details and the role information for the customer care center.

```
inetnum: 62.180.192.0 - 62.180.192.255
netname: BT-IGNITE-DIAL-4
descr: BT-Ignite Dial-4
country: DE
admin-c: BCCC-RIPE
tech-c: BNMC-RIPE
status: ASSIGNED PA
remarks: was VIAG-DIAL-4
remarks: appr. RIPE-NCC-4
mnt-by: IGNITE-DE-MNT
changed: dave.pratt@viaginterkom.de 20070711
changed: katrin.bihlmayer@btignite.de 20070711
changed: hermann.maser@btignite.de 20070711
source: RIPE

route: 62.180.0.0/16
descr: DE-VIAG-980710
origin: AS8472
mnt-by: IGNITE-DE-MNT
changed: Kurt.Kayser@viaginterkom.de 19980711
source: RIPE

role: BT Ignite Customer Care Centre
address: Mergethaleralle 6-8,
address: 65760, Eschborn, Germany
phone: +49 69 3307 6611
fax-no: +49 69 3307 1111
e-mail: bccc.internet@btignite.de
trouble: SPAM/COMPLAINTS to: btignite-abuse@btignite.de
trouble: SPAM/COMPLAINTS to other addresses
admin-c: KM2133-RIPE
tech-c: HK376-RIPE
tech-c: ST378-RIPE
tech-c: SR1985-RIPE
notifv: ripe@de-ianite.net
```

Spuren im Netz: IP-Adresse / Domäne

Aufgabe:

Ermitteln Sie über eine **NIC-Anfrage** (Links unter <http://schreier.free.fr/dhg-info/> -> **Links** -> **Sicherheit**)

- den Geschäftssitz von Microsoft Deutschland GmbH (**microsoft.de**)
- Name und Tel.nr. des technischen Domänenbetreuers von (**uni-freiburg.de**)
- alle Informationen der Domäne **dhg-freiburg.de**.

Wer kümmert sich um den Internet-Auftritt des

- **Auswärtigen Amts** (**auswaertiges-amt.de**)
- **deutschen Bundestages:** (**bundestag.de**)
 - Welche Bundesbehörde nutzt denselben Anbieter ?
- **Bundeskanzlers:** (**bundeskanzler.de**)
 - Welche Bundesbehörden nutzen denselben Anbieter ?

Spuren im Netz: Web-Browser

Sehen Sie sich die **Informationen** an, welche **durch Ihren Browser** bei jeder Webanfrage mitgeschickt werden :



- **Welche Informationen bzw. Rückschlüsse** können damit über Sie gesammelt werden ?
- und
- **Welches Interesse** könnte daran bestehen ?

Spuren im Netz: Web-Browser

www.com-magazin.de/sicherheit

Information via HTTP

- Browser-History und Referrer
- Tracking-Cookies, Link Startin
- erster oder erneuter Besuch

Surfverhalten & Interessen:
Querverweise,
Suchmaschineneinträge

- IP-Adresse und Domain-Name
- Lokale Uhrzeit / Zeitzone
- Bildtypen, Zeichensätze

Herkunft / Zugehörigkeit
Domänen- / Firmenadresse
Herkunftsland / Sprache

- Browsersoftware, Versionsnummer
- Betriebssystem, Prozessor
- Java, JavaScript, VisualBasicScript
- installierte PlugIns, Macromedia Flash

Rechnerausstattung
Möglichkeiten
erweiterten Zugriffs,
Sicherheitsbewusstsein

Spuren im Netz: Cookies

Cookies

- enthalten Informationen, die der Betreiber einer Website **auf dem Rechner eines Besuchers** ablegen kann.
- Diese Informationen werden meist "nebenbei" (im HTTP-Response-Header "**SetCookie**") mitgeschickt.
- werden über Java-Scripte (-applets / cgi-Scripte) erzeugt.

Aufgabe:

```
<script language="JavaScript">
<!--
.....
function SetCookie (name,value,expires,path,domain,secure) {
    document.cookie = name + "=" + escape (value) +
        ((expire) ? "; expires=" + expires.toGMTString() : "") +
        ((path) ? "; path=" + path : "") +
        ((domain) ? "; domain=" + domain : "") +
        ((secure) ? "; secure" : "");
}
.....
// -->
</script>
```

Spuren im Netz: Cookies Summary

Verschiedene Einsatzmöglichkeiten:

- Persistent Cookies** = Anonymer Code zur Aufzeichnung der Zugriffshäufigkeit
- Registration Cookies** = Registrierungs-Formular kann verknüpft werden mit Surf- und Kaufverhalten, auch mit Information anderer Webseiten.
- Session Cookies** = Warenkorb von Versandhäusern, laufen nach der Sitzung aus.
- Preferences Cookies** = Persönliche Einstellungen

In welchen Fällen sind Cookies für den Surfer **von Nutzen bzw. unvermeidbar ??**

Was Cookies alles können: <http://www.cookiecentral.com/>

Spuren im Netz: **Webbugs**

Cookies können durch Surfer abgestellt (kontrolliert) werden.
Webbugs nicht !

Webbugs (Webbeacons)

- winzige (1x1 pixel) **transparente GIFs** („**clear GIFs**“), die auch in anderen Grafiken versteckt werden können.
- übermitteln **zusätzliche Informationen** zu denjenigen, die mit einem Cookie erfasst werden (DoubleClick).
- in **Emails mit HTML-Format**:
 - ob und wann die email gelesen wurde
 - Verknüpfung von Cookies mit Emailadresse möglich!
- möglich **in allen Dokumentarten**, die HTML-Code verarbeiten können (**Office 2000**).
- Dokument bzw. Email muss jedoch geöffnet werden, solange der **User noch online** ist.

Spuren im Netz: **Webbugs**

Web Bugs identifizieren:

- Informieren Sie sich über Einsatzmöglichkeiten von Web-Bugs:
<http://www.bugnosis.org/> (Alle Links zu diesem Thema gibt's
auf meiner homepage: schreier.free.fr)

Verwenden Sie im folgenden den **Internet Explorer**

- Aktivieren Sie in der Toolbar das **Tool Bugnosis** (rechts):
- Das Fenster ist nun **zweigeteilt**:
 - Im oberen Teil erscheint die Webpage unkommentiert
 - Im unteren Teil **Cookie (gelb) bzw. Webbug (rot)**-Warnungen

Surfen Sie nun auf folgende Seiten (Links unter Informatik / Sicherheit):

- www.tvtoday.de, www.teltarif.de, www.ivw.de, www.mtv.de,
www.pc-welt.de, www.finanztreff.de, www.vogue.com
- Achten Sie dabei insbesondere auf Links zu den Werbeagenturen
ivwbox.de, ad.de.doubleclick.net, adserv.quality-channel.de

Spuren im Netz: **Webbugs**

Web Bugs verhindern:

Da Sie Webbugs nicht intern durch Browser-Einstellungen verhindern können, sind Sie auf **externe Tools** angewiesen:

- Aktivieren Sie das **Tool Web-Washer** in der Schnellstart-Box. (WebWasher agiert als **lokaler Proxy-Server** auf dem Browser)
- Surfen Sie die **oben genannten Webseiten** nun noch einmal an und untersuchen Sie die Unterschiede.

Zusatzaufgaben:

Informieren Sie sich über die Verwendung von Cookies und Webbugs aus der Sicht von Webhändlern:

- <http://pages.ebay.de/help/myinfo/cookies.html>
- <http://www2.doubleclick.com/de/htm/corporate.asp>

und diskutieren Sie die konträren Argumente für / wider Cookies.

Spuren im Netz: **Spyware/Adware**

Bestimmte **Free- und Sharewareprogramme** installieren
zusätzlich und unbemerkt Spyware auf dem PC.
Die Programmierer finanzieren auf diesem Weg
(**Werbeeinblendung**) einen Teil ihrer Unkosten.

Spyware / Adware

- nimmt Kontakt zum Hersteller auf und überträgt Werbung, die auch als solche in einem **Werbefenster** sichtbar ist.
- **überträgt gleichzeitig statistische Daten** über den Benutzer, sein Surfverhalten und m.E. auch Dateiinformationen.
- kann sich **als Plugin im Browser oder der Autostartgruppe** einnisten und so ohne das Sharewareprogramm weiterarbeiten, d.h. selbst wenn das Sharewareprogramm nicht gestartet wird oder bereits wieder deinstalliert wurde