Basiskonzepte der TCP/IP-Protokollfamilie

Veranstaltung vom 28.5.98 im Rahmen der Vorlesung

Einführung in die Kommunikationstechnik

SS 1998 - Veranstaltungsnummer: 320131

Markus Speer

Universitätsrechenzentrum

Westfälische Wilhelms-Universität

Münster

E-Mail: speer@uni-muenster.de

Tel.: (0251) 83-31614, Fax: (0251) 83-31653

Themenübersicht

- Internet-Dokumente
- Überblick: TCP/IP und Internet, TCP/IP-Architektur
- TCP/IP-Protokollübersicht
  - Anwendungsprotokolle
  - Protokolle für Basisdienste
  - grundlegende Protokolle
- Basiskonzepte
  - Internet-Adressen
  - Subnetting
  - Port-Nummern
  - Domain Name System
- TCP/IP-Basiskonfiguration

Internet-Dokumente

- **RFCs (Request for Comments):** Originaldokumente der TCP/IP-Kommunikationsverfahren
  - 2292 Dokumente (Februar 1998)
  - Quellen: diverse FTP-Server, CD-ROMs
- **FYI (For Your Information):** ausgewählte RFCs mit Übersichtsdarstellungen
- **BCP (Best Current Practices):** ausgewählte RFCs mit Beschreibungen bewährter Verfahren
- **Internet Official Protocol Standards** (53 Standards bis Mai 1996): Durchlaufen eines standardisierten Verfahrens um zu einem Standardprotokoll erhoben zu werden

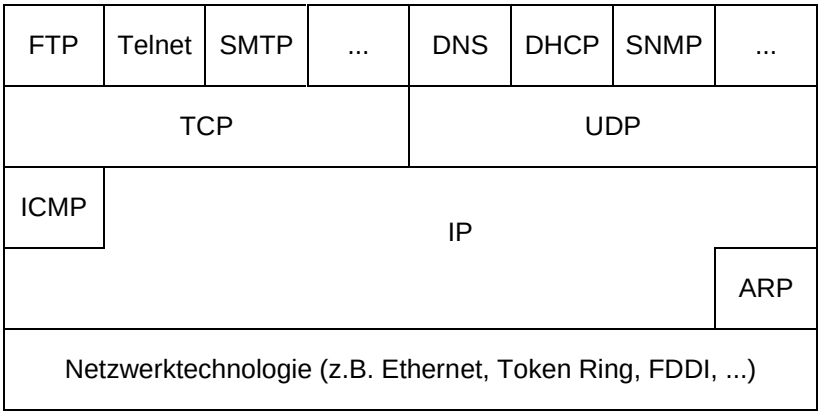
Überblick: TCP/IP und Internet

- **Protokoll:** Festlegung eines Kommunikationsverfahrens
- **herstellerunabhängige** Kommunikationsarchitektur, -protokolle
- **TCP (Transmission Control Protocol):** sichere Übertragung zwischen Endsystemen
- **IP (Internet Protocol):** Routing (Wegwahl), Vermittlung
- eine Vielzahl anderer Protokolle (auch **Anwendungsprotokolle**)
- **RFC-Dokumente (Request For Comment):** Festlegung der Protokolle
- **Internet:** weltweiter Verbund von Rechnern, in dem die TCP/IP-Protokollfamilie eingesetzt wird.

OSI-Schichtenmodell (ISO 7498)

7	Anwendungsschicht	Application Layer
6	Darstellungsschicht	Presentation Layer
5	Kommunikationssteuerungsschicht	Session Layer
4	Transportschicht	Transport Layer
3	Vermittlungsschicht	Network Layer
2	Sicherungsschicht	Data Link Layer
1	Bitübertragungsschicht	Physical Layer

Architektur der TCP/IP-Protokollfamilie



TCP/IP-Anwendungsprotokolle - 1

- **TELNET, RLOGIN:** Dialogzugang, Terminalemulation
- **FTP, TFTP, RCP:** Dateiübertragung
- **SMTP, MAIL, POP3:** E-Mail (elektronische Post)
- **NNTP:** NetNews (elektronische Diskussionsforen)
- Informationsdienste:
  - **WWW:** (ursprünglich) Hypertextinformationssystem
  - **Gopher:** menügeführtes, hierarchisches Informationssys.
  - **WAIS:** weltweit verteilte Datenbanken

TCP/IP-Anwendungsprotokolle - 2

- verteilte Betriebssystemdienste
  - **NFS:** Netzwerkdateisystem
  - **NIS:** Verwaltung von Tabellen
  - **LPD:** Netzwerkdrucker
- verteilte Programmausführung
  - **REXEC, RSH:** auf Kommandobasis
  - **REXEC, RPC:** Programmierschnittstellen
- **X Windows-System**, kurz **X11**: grafische Anwendungen und Benutzeroberflächen im Netz

TCP/IP-Protokolle für Basisdienste

- **DNS:** Domain Name System
- **WINS:** Windows Internet Name Service
- **BOOTP/DHCP** (Bootstrap Protocol / Dynamic Host Configuration Protocol): Konfigurationsservice
- **IPCP** (Internet Protocol Control Protocol): Konfigurationsservice bei Einwahlzugängen
- Zeitservice
  - **TIME:** Setzen der Uhr
  - **NTP** (Network Time Protocol): Synchronisation von Uhren
- **SNMP:** Simple Network Management Protocol

TCP: Transmission Control Protocol

- **verbindungsorientiert**
- **Sicherung der Übertragung**
  - Prüfsumme (Checksum)
  - Paketfolgenummer (Sequence Number)
  - Empfangsbestätigung (Acknowledgement)
  - Übertragungswiederholung (Retransmission)
- **Datenflußsteuerung**
- Die TCP-Funktionen werden von den Endsystemen, zwischen denen die TCP-Verbindung besteht, abgewickelt.

UDP: User Datagram Protocol

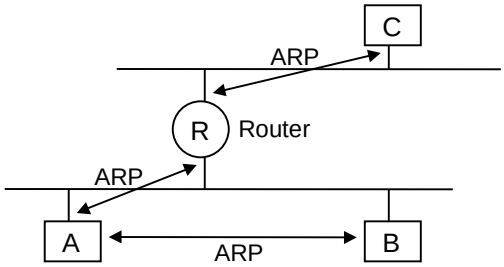
- **verbindungslos**
- **ungesicherte Übertragung**
- Datenzustellung nach dem **Best Effort-Prinzip**
- für Anwendungen mit einfachem Frage-/Antwortcharakter (z.B. Name Service)

IP: Internet Protocol

- **Adressierung**
- **Routing (Wegwahl)**
- **Vermittlung** zwischen verschiedenen Technologien
- **Fragmentierung, Reassemblierung**
- **Router:** Netzkomponente, in der diese Funktionen abgewickelt werden

ARP: Address Resolution Protocol

- **im LAN (Shared Medium**): Identifizierung der angeschlossenen Stationen über die LAN/MAC-Adresse (Adr. der Netzwerkkarte)
- Problem: Welche LAN-Adresse gehört zu einer bestimmten Internet-Adresse?
- ARP: Link Layer Protokoll zur dynamischen Ermittlung der LAN-Adresse zu einer Internet-Adresse über LAN-Broadcast



Internet-Adressen / IP-Adressen

- 32 Bits zur Rechneridentifizierung
- 4 Oktett-Schreibweise: dezimale numerische Werte der einzelnen Bytes durch Punkte getrennt
- Beispiel: 128.176.188.82 (www.uni-muenster.de)
- Unterteilung in
  - Netzwerkadresse (vgl. Telefon-Vorwahl)
  - Rechneradresse, Hostadresse (vgl. Tel.-Anschlußnummer)
- Möglichkeit des Subnetting
- Grundlage des Routings
- Broadcast- und Multicastadressierung
- 5 Klassen von Adressen

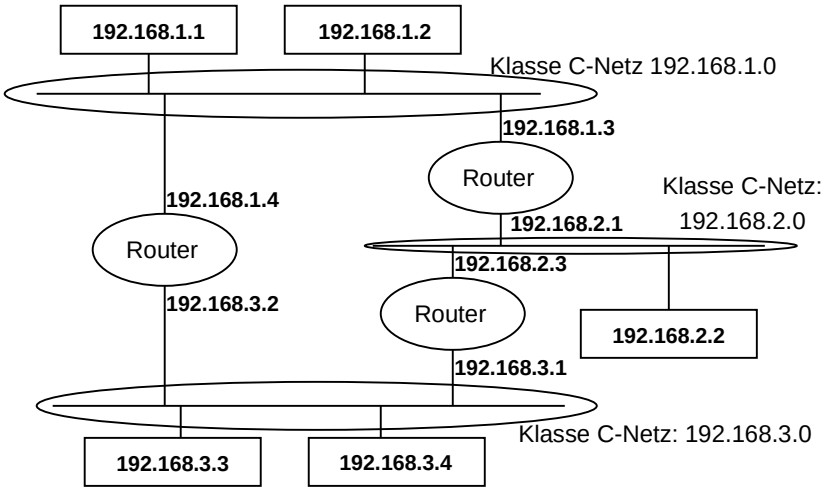
IP-Adressen: Adreßklassen

für bestimmte Netzgrößen

Klasse	führende Bits	Wert des 1. Bytes	Bits für Netz-adresse	Bits für Host-adresse	max. Rechner-zahl
A	0	1 – 126	7	24	ca. 16 Mill.
B	10	128 – 191	14	16	ca. 65000
C	110	192 – 223	21	8	ca. 250
D	1110	224 – 239	Multicast (Hostgruppe): 28 Bits		
E	1111	reserviert für Forschungszwecke			

neuere Entwicklungen: **CIDR** (Classless Inter-Domain Routing)

Beispiel: Kopplung von IP-Netzen mit Routern



spezielle reservierte IP-Adressen

- 0.0.0.0:
  - eigene (noch) unbekannte Adresse
  - sog. Default-Route (alle unbekannten Netze) in Routing-Tabellen
- 127.xxx.xxx.xxx: Adressen für **Loopbacktests (rechnerinterne Kommunikation),** z.B.
  - 127.0.0.1 (localhost): Adressierung der eigenen IP-Instanz ohne Kenntnis der IP-Adresse möglich
- **Broadcastadressen:**
  - 255.255.255.255: eigenes (unbekanntes) Netz
  - z.B. 128.176.255.255: Netzbroadcast
- Hostadresse 0.0.0 (bzw. 0.0 oder 0): Bezeichnung des Netzes, z.B. 128.176.0.0

IP-Adressen und Internet-Konnektivität

- **Internet-Konnektivität:** Verwendung registrierter (d.h. weltweit bekannter) IP-Adressen aus dem Kontingent des sog. **Internet-Providers**
- **keine Internet-Konnektivität:** Verwendung von reservierten IP-Adressen für den lokalen Gebrauch innerhalb einer Organisation möglich:
  - Klasse A Adreßbereich: 10.0.0.0 - 10.255.255.255 (1 Netz)
  - Klasse B Adreßbereich: 172.16.0.0 - 172.31.255.255 (16 Netze)
  - Klasse C Adreßbereich: 192.168.0.0 - 192.168.255.255 (256 Netze)

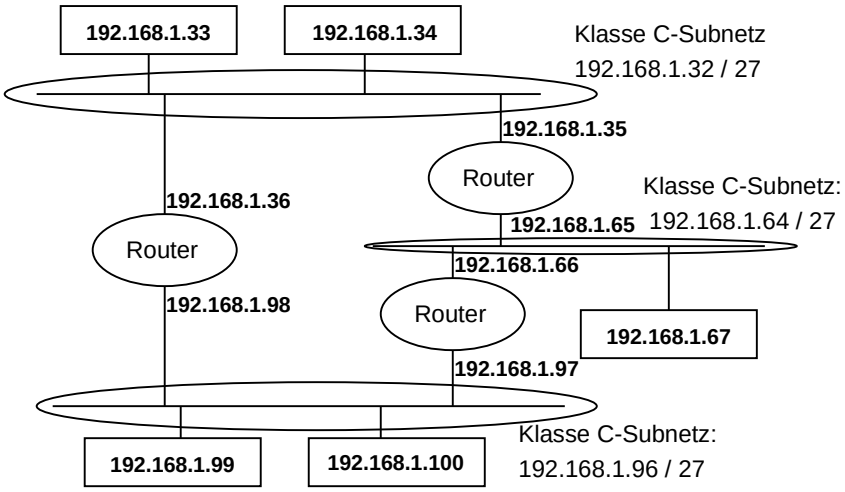
Subnetting / Subnetzmaske

- **Netzmaske:** Festlegung der die Netzadresse umfassenden Bits einer IP-Adresse
- Standardnetzmasken:
  - Klasse A: 255.0.0.0
  - Klasse B: 255.255.0.0
  - Klasse C: 255.255.255.0
- **Subnetting**: Unterteilung eines Klasse A, B oder C-Netzes in **Subnetze** mit Hilfe der Bits für die Hostadresse über die sog. **Subnetzmaske**

Subnetting / Subnetzmaske

- Beispiel:
  - Klasse C-Netz: 192.168.1.0
  - Subnetz: 192.168.1.32
  - Subnetzmaske: 255.255.255.224 (3 Subnetzbits, 32 Adressen umfassendes Subnetz: 192.168.1.32 - 192.168.1.63)
  - Schreibweisen:
    - 192.168.1.32 / 255.255.255.224
    - 192.168.1.32 / 27 (Anzahl der Netzmaskenbits)
- binäre Schreibweise:
  - **192. 168. 1. 32**
  - **1100 0000 1010 1000 0000 0001 0010 0000**
  - **255. 255. 255. 224**
  - **1111 1111 1111 1111 1111 1111 1110 0000**

Beispiel: Kopplung von IP-Subnetzen mit Routern

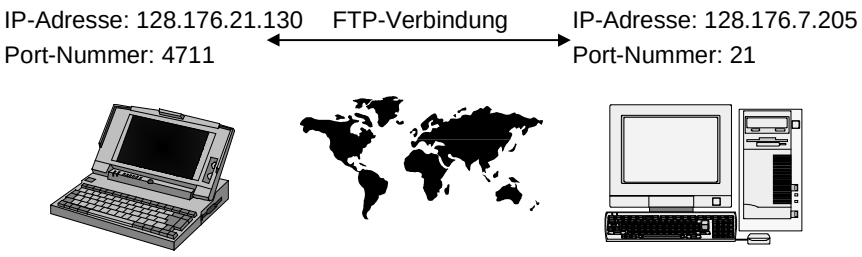


Port-Nummern

- **Adressierung innerhalb eines Rechners** zur Unterscheidung verschiedener Anwendungen (Anwendungsprozesse)
- **Well Known Port Numbers** für Standard-Anwendungen:
  - 21: FTP
  - 23: TELNET
  - 53: Domain Name Service
  - ...
- vgl. Unix-Datei **`/etc/services`**
- **Socket** (Kommunikationsendpunkt): IP-Adresse + Port-Nummer

Adressen einer TCP/IP-Rechnerverbindung

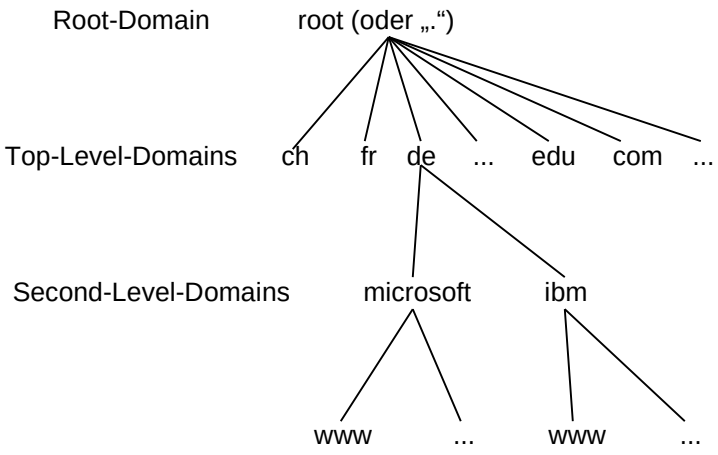
Eine Verbindung zwischen zwei Rechnern im weltweiten Internet ist eindeutig durch das Paar von Quell- und Zielsocket festgelegt.



DNS: Domain Name System - 1

- Nutzung von **Rechnernamen** anstelle von IP-Adressen
- z.B. www.uni-muenster.de statt 128.176.188.82
- **DNS:** (weltweites, verteiltes) Datenbanksystem zur Übersetzung von Rechnernamen in IP-Adressen
- hierarchischer, baumartiger Aufbau des Namensraums
- **Domain:** Teilbaum des Namensraums
- eindeutige Namen innerhalb einer Domain

DNS: Domain Name System - 2

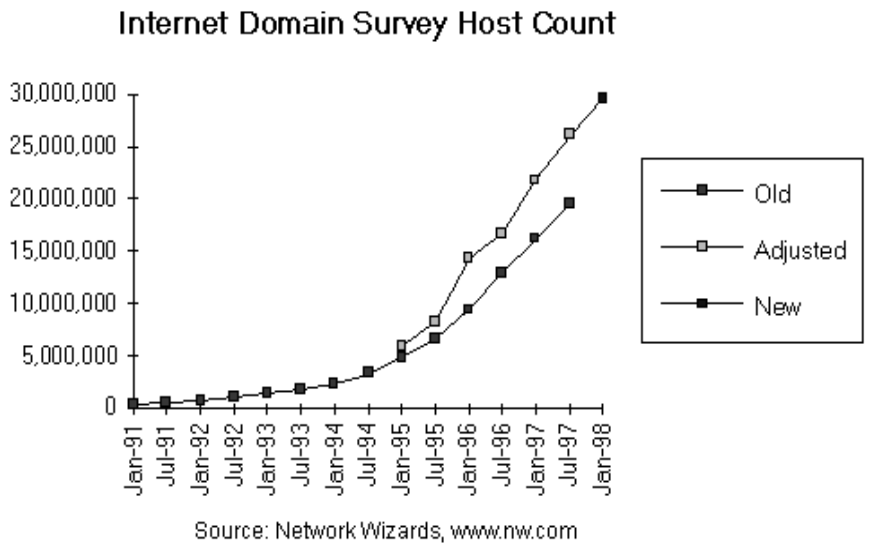


Domain Name Service - 3

- **Domain Name Server (DNS-Server):**
  - Verwaltung einer Domain
  - Kommunikation mit anderen Domain Name Servern
  - zur Erhöhung der Betriebssicherheit i.a. mehrere Server pro Domain:
    - **primärer DNS-Server**: mind. ein Server mit den Originaldaten
    - **sekundärer DNS-Server**: mehrere Server die vom primären Server (bei Änderung) die Originaldaten kopieren (sog. **Zonentransfer**)
- **dienstbezogene Rechnernamen:** www, ftp, mail, news, pop, ...

Top Level Domains

- **mil:** US-Militär
- **gov:** US-Regierung
- **edu:** US-Bildungswesen
- **com:** kommerzielle Einrichtungen
- **net:** Netzwerkorganisationen
- **org:** andere non-profit Organisationen
- **int:** internationale Organisationen
- **ch:** Schweiz
- **de:** Deutschland
- **fr:** Frankreich
- **uk:** Großbritanien
- ...



Top 100 Host Names (Jan 1998)

Quelle: Network Wizards, www.nw.com

614610	www	4037	ns2	2917	network	2407	pc27	1920	pc35
65109	host	4033	test	2889	mars	2388	ppp3	1917	host30
33672	mail	3932	pc11	2885	zeus	2385	free	1891	ws10
15614	router	3926	pc5	2882	pluto	2347	pc28	1888	ts1
10287	ns	3855	pc12	2880	ppp1	2302	saturn	1887	pc36
10001	user	3796	gate	2856	pc17	2298	admin	1887	apollo
9337	gw	3608	pc6	2848	pc18	2243	pc29	1886	mac
8710	ftp	3558	broadcast	2787	pc19	2233	mailhost	1879	mac1
6547	gateway	3466	pc13	2757	pc20	2192	orion	1870	pc32
6540	smtp	3394	pc7	2687	ppp2	2178	ws1	1868	ppp10
6421	server	3314	cisco	2678	pc21	2158	ppp4	1862	pc38
6065	ip	3304	pc8	2678	jupiter	2135	ws2	1858	pc33
5387	www2	3261	dummy	2634	pc22	2110	host29	1856	pc37
5199	pc1	3230	pc14	2571	pc23	2072	ws3	1838	ws11
4902	pc2	3164	pc9	2566	home	2034	ws4	1833	ppp6
4853	ns1	3115	dns	2529	pc24	2012	pc01	1819	pc40
4546	pc3	3022	pc15	2527	alpha	1976	ws5	1812	ws12
4270	news	3015	venus	2482	pc25	1937	ppp5	1801	pc39
4219	pc4	3014	proxy	2455	mercury	1937	pc31	1791	ppp11
4071	pc10	2938	pc16	2430	pc26	1925	pc34	1772	eagle

Die 28 **roten** Rechnernamen existieren auch im Rechnernetz der Universität Münster.

WINS: Windows Internet Name Service

- sog. **NetBIOS-Namen** für spezielle Rechnerfunktionen
- NetBIOS-Namen werden beim **Windows-Netzwerk** bei der Nutzung von Netzwerkressourcen (z.B. Netzwerklaufwerk, Netzwerkdrucker, ...) verwendet. Die dort verwendeten Namen haben nichts mit den Standard Internet-DNS-Namen zu tun!
- Verschiedene **Typen von NetBIOS-Namen**, z.B.:
  - Server (eindeutiger Name)
  - Domain (Gruppenname)
- **WINS-Server:** Übersetzung von NetBIOS-Namen in IP-Adressen (bei Einsatz von NetBIOS über TCP/IP)
- Namensauflösung u.U. auch ohne WINS-Server möglich (über Broadcast-Adressierung)

TCP/IP-Basiskonfiguration eines Rechners

Die unten aufgelisteten Parameter müssen bei der Installation von TCP/IP-Software i.a. mindestens konfiguriert werden.

Möglichkeit der **automatischen Konfiguration** mit BOOTP/DHCP (oder IPCP: Internet Protocol Control Protocol)

- IP-Adresse
- Subnetzmaske (*)
- Default-Router (*)
- Domain Name Server
- Rechnername
- Internet-Domain
- WINS (nur bei Einsatz von NetBIOS über TCP/IP)

(*): Bei Einwahlzugängen Konfiguration nicht notwendig.

Automatische Konfiguration mit BOOTP/DHCP

- BOOTP: Bootstrap Protocol
- DHCP: Dynamic Host Configuration Protocol
- DHCP ist eine kompatible Weiterentwicklung von BOOTP.
- Funktion: automatische Konfiguration der wichtigsten TCP/IP-Parameter beim Rechnerstart
- Identifizierung der Rechner durch MAC/LAN-Adresse (Adresse der Netzwerkkarte) oder dynamische Vergabe freier IP-Adressen (nur bei DHCP)
- Vorteile der automatischen Konfiguration
  - Vereinfachung der Rechnerinstallation/-konfiguration
  - Vermeidung von doppelt verwendeten IP-Adressen
  - Änderung der Basisparameter nur einmal an zentraler Stelle

BOOTP/DHCP - Überblick

- **UDP-basierend**
  - Client: Port 68
  - Server: Port 67
- **Relay Agent** vorgesehen
  - nicht in jedem IP-Subnetz ein Server notwendig
  - Übersetzen eines Client-Broadcasts in ein oder mehrere Unicasts
- **DHCP-IP-Adreßvergabemodelle**
  - **dynamische,** vorübergehende Zuweisung (**lease time**)
  - **automatische,** dauerhafte Zuweisung (**infinite lease time**)
  - **statische** Zuweisung durch Administrator (wie bei BOOTP)
- DHCP: kein einfaches Frage-/Antwort-Protokoll wie BOOTP
- **7 DHCP-Nachrichtentypen**: DISCOVER, OFFER, REQUEST, ACK, NAK, DECLINE, RELEASE

IPCP - Internet Protocol Control Protocol

- Konfigurationservice bei Einwahlzugängen
- automatische Konfiguration von
  - IP-Adresse des einwählenden Rechners
  - IP-Kompressionsprotokoll (z.B. **Van Jacobson Header Compression**: Reduzierung des TCP/IP-Headers auf bis zu 3 Bytes)
  - Domain Name Server
  - evtl. WINS-Server

typische Fehler bei der Konfiguration von Internet-Adressen

- keine organisierte (zentrale) Vergabe und Kontrolle der IP-Adressen
- Konfiguration von Beispieladressen aus der Dokumentation
- Konfiguration durch Systemhaus ohne Kenntnis der Netzstruktur
- Kopieren der Konfiguration eines anderen Rechners
- Ableiten der zu konfigurierenden Adresse von den Adressen der benachbarten Rechner
- Default-Router nicht im eigenen Subnetz