

Adressierung im Internet

- Zusammengefasst ergibt sich folgendes Bild:

Application Layer	- symbolischer Domain-Name, z.B. in einer URL bei http
Transport Layer (TCP, UDP)	- Port-Nummer (2 Byte)
Network Layer (IP)	- IP-Adresse (4 Byte)
Link Layer Physical Layer	- z.B. Ethernet-Adresse (6 Byte)

- Hierbei sind die Pakete i.a. ineinander verschachtelt!

Namen und Adressen

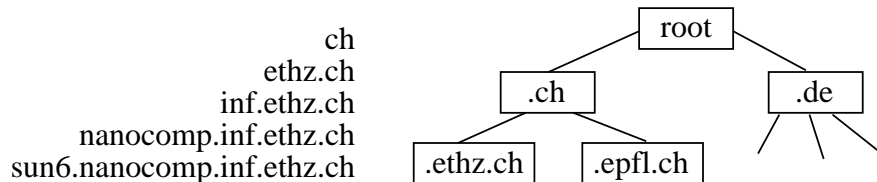
- *Namen* geben i.a. Aufschluss über die *Art* eines Objektes
 - Typ, Gestalt, Zweck... (falls Name sinnvoll gewählt!)
 - “Namen sind Schall und Rauch” oder “Nomen est Omen”?
- Namen dienen auch der *Bezeichnung* und *Identifizierung*
 - daher oft auch “Bezeichner” oder “Identifikator” für “Name”
 - es gibt auch *anonyme* Objekte (z.B. dynamisch erzeugte Variablen)
 - ein Objekt kann u.U. *mehrere Namen* haben (“alias”)
 - gleicher Name kann in verschiedenen Kontexten (“Namensraum”) unterschiedliche Objekte bezeichnen
- *Adresse* ermöglicht die *Lokalisierung* eines Objektes
- Adressen sind innerhalb eines Kontextes (“Adressraum”) eindeutig
- Adresse eines Objektes ist u.U. *zeitabhängig*
 - mobile Objekte
 - “relocatable”
- *Dagegen*: Name eines Objektes ändert sich i.a. nicht
 - vgl. aber: Namensänderung bei Heirat, Zuweisung eines Alias...!
- Entkoppelung von Namen und Adressen unterstützt die *Ortstransparenz*
- Daher dynamische Zuordnung Name --> Adresse nötig
 - vgl. persönliches Adressbuch
 - “Binden” eines Namens an eine Adresse

Internet Domain Name System (DNS)

- Jeder Rechner im Internet hat eine IP-Adresse
 - typischerweise als 4 Dezimalzahlen geschrieben (z.B. 192.130.10.121)
- Symbolische Namen sind besser
 - z.B. Domain-Namen wie www.nanocomp.inf.ethz.ch
 - gut zu merken; relativ unabhängig von spezifischer Maschine
 - muss bei *vor* Verwendung bei Internet-Diensten (telnet, ftp, Email, WWW...) in eine IP-Adresse umgesetzt werden
 - Umsetzung in IP-Adresse geschieht im Internet mit DNS

- Domains

- hierarchischer Namensraum der symbolischen Namen im Internet
- "Toplevel domains" ch, de, fr, nl (ISO 3166 Ländercodes); edu, com,...
- Domains (ggf. rekursiv) gegliedert in Subdomains

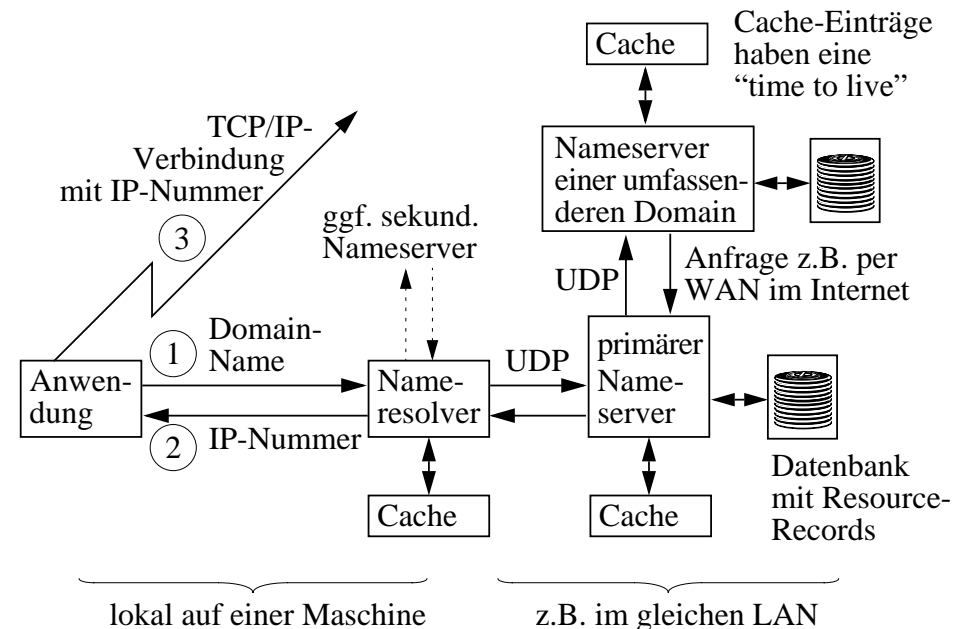


- Für einzelne Subdomains bzw. einer Zusammenfassung einiger Subdomains (sogenannte "Zonen") ist jeweils ein Domain-Nameserver zuständig

- primärer Nameserver
- optional zusätzlich einige weitere sekundäre Nameserver
- oft sind Primärservers verschiedener Zonen gleichzeitig wechselseitig Sekundärservers für die anderen
- Nameserver haben also nur eine Teilsicht!

Namensauflösung im Internet

- Historisch: Jeder Rechner hatte eine Datei hosts.txt, die jede Nacht von zentraler Stelle aus verteilt wurde
- Jetzt: lokaler Nameserver, der eine Zuordnungsdatei /etc/hosts für die wichtigsten Rechner enthält, und sich ansonsten an einen seiner nächsten Nameserver wendet
 - IP-Nummern der lokalen Nameserver stehen in der Datei resolv.conf



nslookup

NAME in.named, named

in.named is the Internet domain name server. It is used by hosts on the Internet to provide access to the Internet distributed naming database. See RFC 1034 and RFC 1035 for more details. With no arguments, in.named reads /etc/named.boot for any initial data, and listens for queries on a privileged port.

NAME nslookup - query name servers interactively

nslookup is an interactive program to query Internet domain name servers. The user can contact servers to request information about a specific host, or print a list of hosts in the domain.

```
> sun20
Name: sun20.nanocomp.inf.ethz.ch
Address: 129.132.33.79
Aliases: ftp.nanocomp.inf.ethz.ch

> altavista.com
Name: altavista.com
Addresses: 204.123.2.75, 204.123.2.66,
204.123.2.69

> altavista.com
Name: altavista.com
Addresses: 204.123.2.66, 204.123.2.69,
204.123.2.75

> cs.uni-sb.de
Name: cs.uni-sb.de
Addresses: 134.96.254.254, 134.96.252.31
```

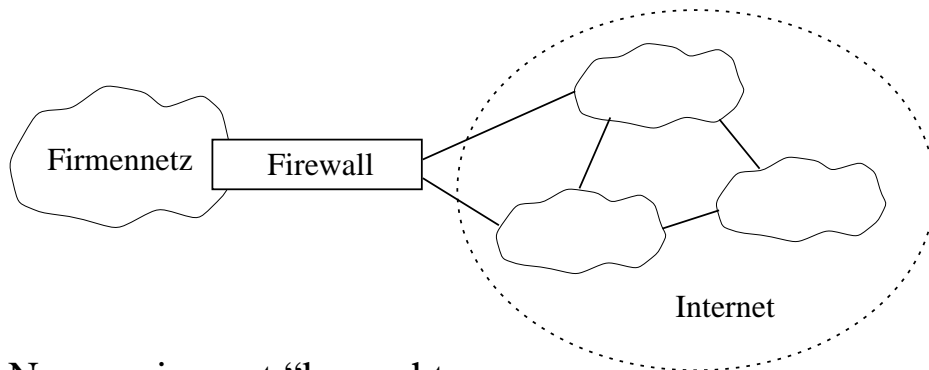
Dies deutet auf einen "round robin"-Eintrag hin: Der Nameserver von altavista.com ändert alle paar Minuten die Reihenfolge der Einträge, die bei anderen Nameservern auch nur einige Minuten lang gespeichert bleiben dürfen. Da Anwendungen i.a. den ersten Eintrag nehmen, wird so eine Lastverteilung auf mehrere Altavista-Server vorgenommen!

Router an zwei Netzen

Intranet

- Nutzung der Internet-Technologien und -Konzepte für firmeninterne Netze
 - TCP/IP-Protokoll (+ darauf aufbauende Dienste)
 - Web-Browser (+ http, html-Dokumente...)
 - ==> einheitliche Verfahren und Oberflächen, um von jedem Arbeitsplatz (PC, MAC, Workstation) aus an die Firmendaten zu kommen
- Aufgabe: Server und Clients "intranetfähig" machen, z.B.:
 - Java-Applets als lokal laufenden Anwendungen auf Client-Seite
 - Datenbank-Server mit http-Schnittstelle
- Intranet-Infrastruktur als Problem- und Geschäftsfeld
 - firmeninterne Suchmaschinen
 - Hochleistungs-Webserver
 - Sicherheitskonzepte
 - Datenbankanschluss
- Intranet ermöglicht relativ problemlose Verbindung privater Netze mit dem Internet
 - Lücke schliessen zwischen firmeneigenen Informationssystemen und dem Internet (--> electronic commerce...)
 - Sicherheitsproblematik:
 - Firmennetz als Teil des Internets?
 - Internet-Protokolle und -Dienste wurden nicht für sicherheitskritische Anwendungen entworfen!
 - Zauberwort "Firewall"

Firewall (1)



- Nur wenige gut "bewachte Übergangsstellen" in das Internet bereitstellen

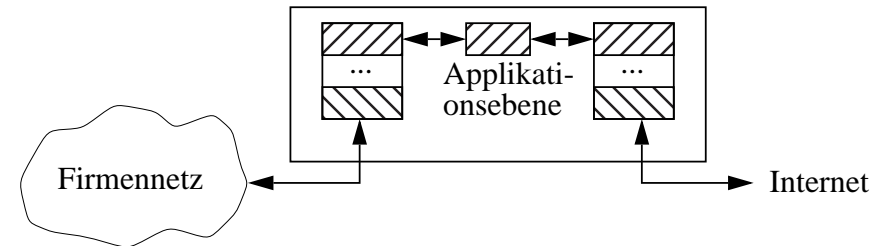
- vgl. Zugbrücke einer mittelalterlichen Burg
- Überprüfen von Datenpaketen, Verbindungswünschen, Adressen...
- Verhindern gewisser Kommunikationsmöglichkeiten
- Protokollierung, Alarmmeldungen etc.
- Beachte: Eine Firewall muss gut administriert werden!

- Typ "Paketfilter" (auf IP- und TCP-Ebene)

- typischerweise spezielle Router
- "Screening" durch definierbare Regeln
- Überprüfen von Quell- und Zieladresse
- Überprüfen von Port-Nummern
 - z.B. Telnet: 23; Finger: 79 etc.
 - dadurch z.B. verhindern, dass Telnet-Verbindungen von ausserhalb auf Firmenrechner möglich sind
- transparent für die Anwender (ausser bei "verbotener" Kommunikation!)
 - Nachteil: Unterscheidung zwischen Nutzern mit verschiedenen Rechten auf dieser Ebene kaum möglich
 - Nachteil: Es gibt Dienste mit dyn. Portnummern; es gibt sogar dynamische IP-Adressen...

Firewall (2)

- Typ "Application Gateway"



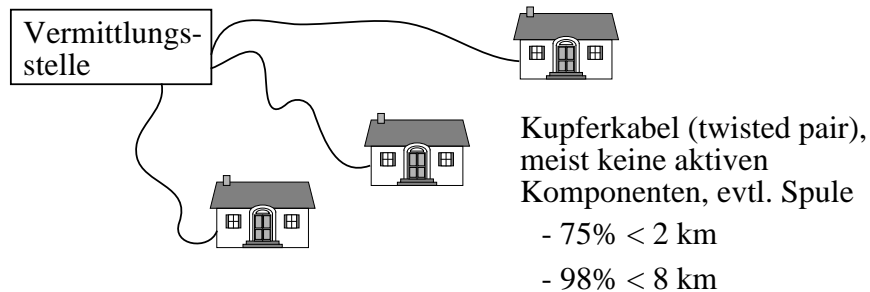
- Rechner mit zwei Netzzugängen ("dual-homed"), wobei das "IP-Forwarding" dazwischen deaktiviert ist
- Für spezielle Dienste (z.B. telnet, email, ftp, WWW...) sind im Gateway Stellvertreter-Services ("Proxies") realisiert
 - sowohl Client als auch Server wenden sich an den Proxy
 - direkte Kommunikation zwischen Client und Server ist unterbunden
 - Proxy sollte für Anwender transparent sein
 - Proxy-Software kann konfiguriert werden; damit z.B.:
 - Überprüfen von Adressen etc
 - Prüfen von Legitimation und Autorisierung
 - Authentifizierung, Einmalpasswörter, Verschlüsselung...
 - detaillierte Protokollierung
 - verbergen der firmeninternen Adressen, Netzstruktur etc.

- Es gibt weitere Sicherheitstechniken in Firewalls

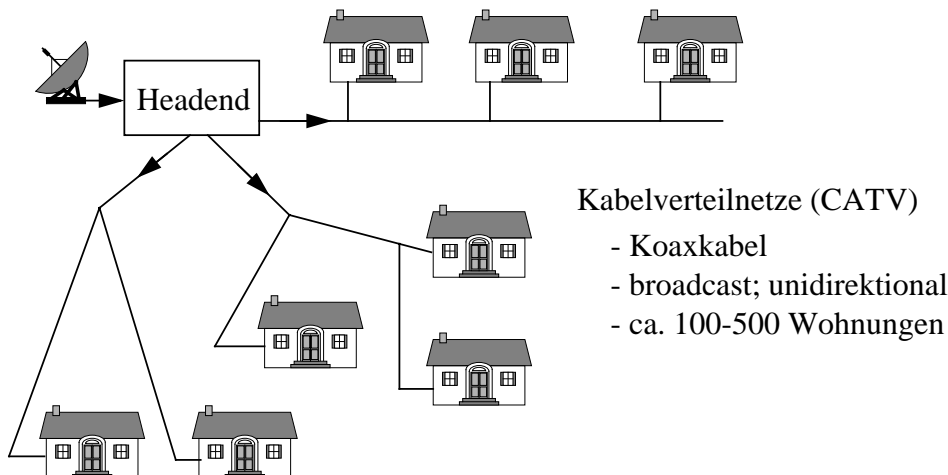
- z.B. "Policy Routing" (Wahl der Routen abhängig vom Absender etc.)

Hochgeschwindigkeit für alle!?

- “Residential Access Networks” möchten sich existierende Infrastruktur zunutze machen
- **Telefon-Infrastruktur** bietet **switching** (“Vermittlung”), aber nicht das geeignete **Medium** für hohe Bandbreiten



- **Kabel-TV-Infrastruktur** bietet **Medium**, aber kein “switching”



Potentielle Anwendungen von Hochgeschwindigkeitszugängen

- Schneller Zugang zu Internet-Provider
 - z.B. Informationsdienste über schnellen WWW-Zugang
- Electronic commerce (business - consumer)
 - home shopping
 - kostenpflichtige Informationsdienste
- Distance learning
- Fun, Entertainment, Infotainment
- Telecommuting; Teleworking (Heimarbeitsplätze)
- SOHO (Small Office / Home Office)
- (Near) Video on Demand
 - statt Video-Kassetten
 - auch Radio bzw. Audio on Demand (statt CDs)
- IP-Telefonie, Bildtelefon
- IP-Fernsehen, interactive TV, IP-Radio
- Applikationssoftware im Netz statt auf lokaler Platte
 - überhaupt: keine Festplatten am PC, sondern Speicherdienst des Netzes nutzen
- Neue Dienste im Netz
 - Terminkalender, Fotoalbum, ...
- ...

xDSL (Digital Subscriber Line)

- Nutzung der Telefon-Kupferkabel
 - Sprachübertragung nutzt nur ca. 4 kHz
 - Kabel selbst "vertragen" aber ca. 1 MHz über typische Distanzen
- Digitale Modems an beiden Enden
- Technologievarianten "xDSL" (u.a.):
 - HDSL: High data rate SDL (1.5 Mb/s bei 80-240 kHz über ca. 3 km)
 - SDSL: Single line SDL (nutzt im Unterschied zu HDSL eine statt zwei Leitungen; dadurch Telefonie auf anderer Leitung gleichzeitig möglich)
 - VDSL: Very high data rate SDL (downstream 51.84 Mb/s über 300 m bzw. 12.96 Mb/s über 1500 m; upstream 1.6 - 19.2 Mb/s)
 - ADSL: Asymmetric SDL

Verwendung z.B.: Glasfaser bis zu einem Knotenpunkt; aber keine teure Neuverkabelung jedes einzelnen Haushaltes

- Unterschiedliche Gegebenheiten USA / Europa
 - USA: frühere Marktöffnung; ISDN wenig verbreitet; xDSL früher forciert; xDSL als Alternative zu ISDN
 - Europa: xDSL als Weiterentwicklung von ISDN

ADSL (Asymmetric DSL)

- Asymmetrie: Bandbreite upstream << downstream
 - viele Applikationen sind asymmetrisch ("Verbrauchen" von Information: Surfen im Internet, Video on Demand etc.)
 - aufgrund technischer Gegebenheiten (Dämpfung, Übersprechen) lassen sich Signale, die verschieden weit vom gemeinsamen Endpunkt entstehen (upstream!), bei gebündelten Leitungen nicht mit hoher Bitrate betreiben
- Maximale Entfernung ca. 7500 m
- Aufteilung in 4 gleichzeitig nutzbare Kanäle
 - in Europa Vielfache von E-1 (2.048 Mb/s)
 - in USA Vielfache von T-1 (1.536 Mb/s)

downstream	6.144 Mb/s	4.096 Mb/s	2.048 Mb/s
upstream	640 kb/s	608 kb/s	176 kb/s
Steuerkanal	64 kb/s	64 kb/s	16 kb/s
Telefonkanal	64 kb/s	64 kb/s	64 kb/s

- Tatsächliche Bitrate abhängig von Leitungslänge, Leitungsquerschnitt, Dämpfung etc.
 - z.B. 6.144 Mb/s bei 0.4 mm Kabeldurchmesser --> max. 2.7 km

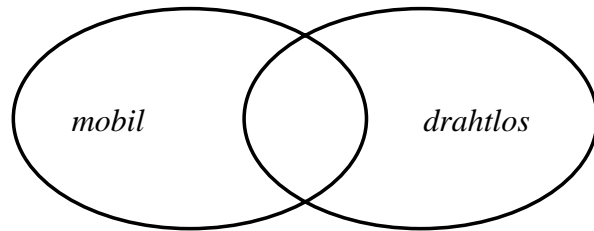
Kabelmodem

- Aus Sicht des Kunden: auf der einen Seite wie TV an Fernsehbuchse anschliessen, auf der anderen Seite den PC (z.B. über Ethernet-Anschluss)
- Umbau zu bidirektionalem Netz?
- Downstream in einem TV-Kanal von 6 MHz bei geeigneter Kodierung von 6 bits/Hz --> 30 Mb/s
- Upstream 1.5 bis ca. 3 Mb/s in einem 2 MHz-Band
 - dedizierter (logischer) Kanal auf Broadcast-Medium
 - redundantere Codierung, da upstream störanfälliger
 - Zugriffsverfahren notwendig (gemeinsames Medium!)
 - Verschlüsselung notwendig
 - Alternative: Schmalbandiger upstream-Kanal über Telefon-Netz
- Nachteil: Koaxkabel-Infrastruktur ist weniger stark verbreitet als Telefon-Infrastruktur
 - kaum in der Fläche (ländliche Gegenden)
 - auch kaum in Bürogebäuden
- Headend ist über Router etc. mit schnellerer Internet-Infrastruktur verbunden (i.a. über Glasfaser)

Digital Powerline

- Internet-Zugang über **Niederspannungs-Stromnetze**
- Interesse der Energieversorgungsunternehmen
- Ca. **1 Mb/s** über **250 m** mit einer 230V-Leitung
- Idee: Einspeisung bei der **letzten Trafostation**
- 2 MHz breites Spektrum zwischen 2.2 und 10 MHz
- Problem: Alle Teilnehmer einer Versorgungsgebiets (z.B. eines Wohnblocks) **teilen sich die Bandbreite**
- **Bitfehlerrate** ist wesentlich höher als z.B. bei ADSL
- Elektronische Verbraucher (Leuchtstoffröhren, Schaltnetzteile) --> Verseuchung mit **Störsignalen**
- Nicht alle **elektronischen Geräte** vertragen hochfrequente Signale auf der Netzzuleitung (z.B. Fernsehgeräte)
- **Kurzwellen-Empfang** wird in der Umgebung erheblich beeinträchtigt (Stromkabel i.a. nicht geschirmt verlegt)
- Sogar Strassenlaternen können als Sendeantennen wirken!
- Allerdings ist diese Technik ggf. zur **“Vernetzung” eines Hauses** oder einer Wohnung geeignet
 - kein LAN, kein Telefonkabel (und kein TV-Kabel?) in der Wohnung...
 - Telefon (Internet-Telefonie!) hat einfach einen Stromstecker
 - ggf. als Alternative zu “wireless homes” (bzw. “offices”)
- **Europa** (ca. je 200 - 300 Wohnungen an Trafo) <--> **USA** (nur je ca. 6 - 8) --> untersch. Geschäftsmodelle

Mobile / drahtlose Kommunikation



- Mobil <--> stationär

↑
 Problem: Routing, Adressierung --> i.a. höhere Protokollebenen

- Drahtlos <--> drahtgebunden

↑
 Problem: media sharing --> i.a. niedrige Protokollebenen

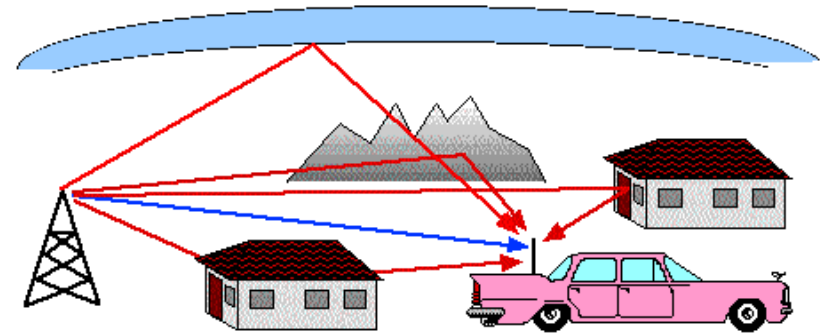


"... modem ... modem ... modem ..."

Drahtlose Kommunikation

- Probleme u.a.:

- Behinderung durch Schnee, Regen...
- atmosphärische Störungen
- Mehrwegausbreitung (--> Interferenzen, Fading)
- Abschattungen
- nahe Sender überdecken schwache Signale ferner Sender
- Zugriffskonflikte, da nicht alle von allen wissen / alle hören
- Energieverbrauch
- Abhörsicherheit
- Dopplereffekt



--> Andere Protokolle etc. erforderlich!

- z.B. Vorwärtskorrektur ("forward error recovery")
- z.B. bzgl. media access
- z.B. CDMA ("Code Division Multiple Access"): gleiches Frequenzband für alle Sender; XOR-verknüpft mit eindeutiger Pseudozufallsfolge; Empfänger kann daraus Originalsignal restaurieren (Vorteile: keine Frequenz-/Zeitscheibenplanung nötig; Vorwärtskorrektur und Verschlüsselung leicht integrierbar)

- Neue Aspekte, z.B. Handover, Roaming...