Basistechnologien im Internet

Dr. Walter Ebner
Dr. Albert Weichselbraun

Wirtschaftsuniversität Wien

Inhalt

Ziel: Einführung in die Internet-Technologie

- Struktur des Internets
- Schichtenmodell
- TCP/IP Protokoll Suite
- Local Area Networks

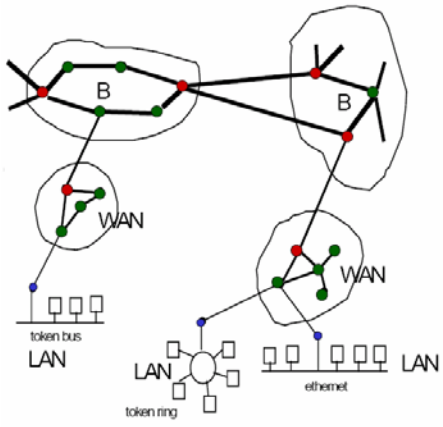
Definition

- Offizielle Definition:
  "Internet" refers to the ***global information system*** that -
  - is logically linked together by a ***globally unique address space*** based on the Internet Protocol (IP) or its subsequent extensions/follow-ons;
  - is able to support communications using the***Transmission Control Protocol / Internet Protocol (TCP/IP)*** suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and
  - provides, uses or makes accessible, either publicly or privately, ***high level services*** layered on the communications and related infrastructure described herein."

- Informationen über sämtliche Protokolle des Internets findet man in den **RFC**s „Requests for Comments“
  siehe: http://www.ietf.org/rfc.html

Struktur des Internet

- **Backbone**: “Internet-Kern” mit hoher Übertragungsbandbreite: mehrere Backbones verbunden durch Kabel hoher Kapazität und hoher Geschwindigkeit
- **Wide Area Network (WAN)**: nationale (A, D, F, GB,...) und regionale Netzwerke
- **Metropolitan Area Network (MAN)**:
  (kleinere) regionale Netzwerke (Wien, Berlin, New York City,...)
- **Local Area Network (LAN)**: Institut für Infw., PC7, ...
- verbunden durch
  - Network access points,
  - Router, und
  - Gateways



Quelle: AIFB Karlsruhe

Struktur des Internets

- Die Struktur des Internets
  - verschiedenartige Systeme
  - gleichberechtigte Teilnehmer
  - paketorientierte Datenübertragung
  - dynamisches Routing

"selbstorganisierendes Chaos"

- Notwendigkeit von Protokollen (z.B. Kommunikationsprotokoll) zur Regelung des Informationsflusses

Schichtenmodelle

- Jede Schicht eines Kommunikationssystems erfüllt bestimmte Aufgaben.
- Leistungen, welche eine Schicht für eine übergeordnete Schicht erbringen muss, werden als Dienst bezeichnet.
- Instanzen auf der selben Schicht, aber in unterschiedlichen Netzwerkknoten sind gleichberechtigt (Bezeichnung: peer entities). Sie kommunizieren über Protokolle.

- Eine Schicht hat also Schnittstellen zu ihren angrenzenden Schichten (zur oberen und unteren) und sie kommuniziert mit ihrer Peer-Schicht auf einen fremden Rechner.

Vorteile Schichtenmodelle

A Layered architecture is a conceptual blueprint of how communications should take place. It divides communication processes into logical groups called layers.

There are many reasons to use a layered architecture:

- To clarify the general functions of a communications process rather than focusing on the specifics of how to do it
- To break down complex networking processes into more manageable sublayers
- To enable interoperability by using industry-standard interfaces
- To change the features of one layer without changing all of the programming code in every layer
- To make for easier troubleshooting

OSI-Modell

Anfang 80er Jahre von ISO entwickelt.
Abstraktes 7-schichtiges Modell für offene Systeme. Beschreibt allgemeine Prinzipien der Vernetzung von offenen Systemen.

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

OSI – Open System Interconnection;
ISO – International Organization for Standardization

OSI-Modell: die oberen Schichten

- Provides a user interface
- Presents data
- Handles processing such as encryption
- Keeps different applications' data separate

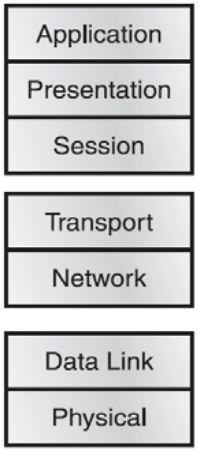
Quelle: Todd Lammle: *CCNA Study Guide*, 5th ed., Sybex 2005.

OSI-Modell: die unteren Schichten

- Provides reliable or unreliable delivery
- Performs error correction before retransmit
- Provides logical addressing, which routers use for path determination
- Combines packets into bytes and bytes into frames
- Provides access to media using MAC address
- Performs error detection not correction
- Moves bits between devices
- Specifies voltage, wire speed, and pin-out of cables

Quelle: Todd Lammle: *CCNA Study Guide*, 5th ed., Sybex 2005.

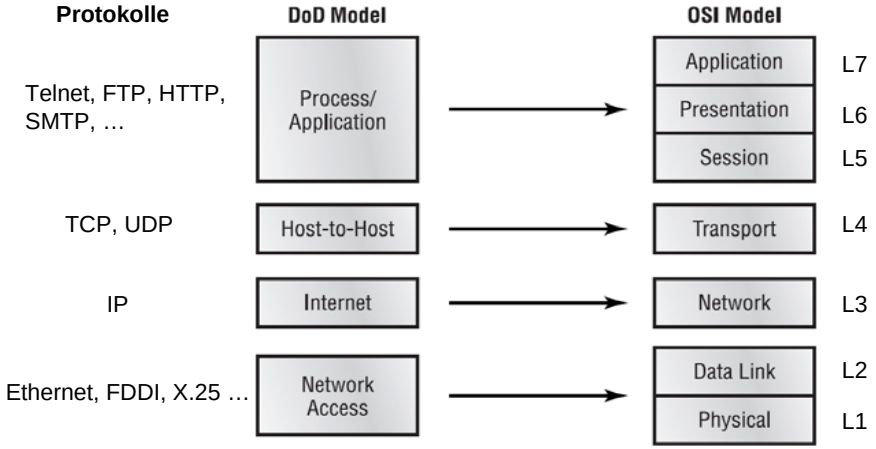
OSI-Modell: Schichtenfunktionen



- File, print, message, database, and application services
- Data encryption, compression, and translation services
- Dialog control
- End-to-end connection
- Routing
- Framing
- Physical topology

Quelle: Todd Lammle: *CCNA Study Guide*, 5th ed., Sybex 2005.

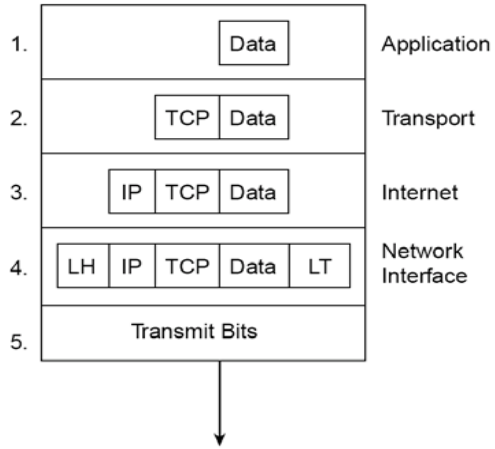
TCP/IP und OSI Modell



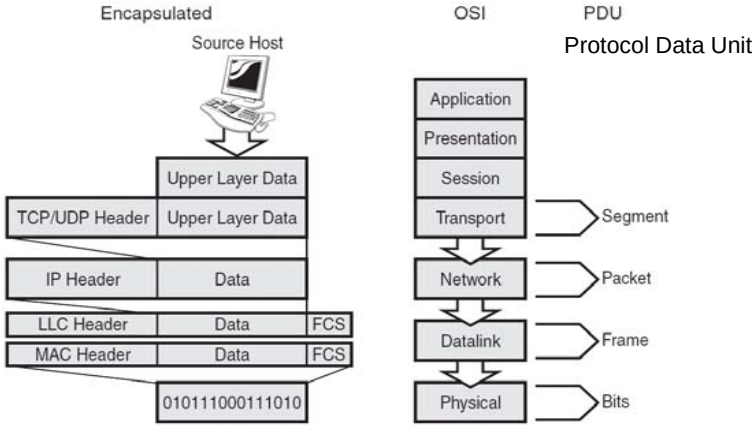
DoD: U.S. Department of Defence

Quelle: Cisco

Data Encapsulation in TCP/IP



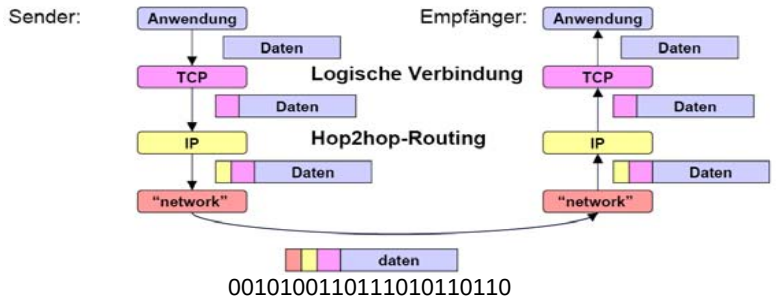
OSI Encapsulation



Kommunikation

Standardarchitektur für Kommunikation zwischen Rechnern ISO-OSI Modell reduziert auf:

- Application Layer L7 (Telnet, FTP, SMTP, HTTP, …)
- Transport Layer L4 (TCP, UDP)
- Network Layer L3 (IP)
- Data Link Layer L2 (Ethernet, FDDI, Token Ring, Frame Relay)



Übertragungsmedien

- Coaxial Kabel
  - Thin-Net 10Base-2
  - Thick-Net 10Base-5

- Verdrilltes Kupferkabel (UTP, STP)
  Verschiedene Kategorien:
  CAT-1 bis CAT-7

- Glasfaser-Kabel (engl: Fiber)
- Wireless (Funk, Mikrowelle, Infrarot, Laser)

Netzwerktopologie

- Bus-Topologie
- Star-Topologie
- Ring-Topologie
- Baum-Topologie
- Netz-Topologie

- Logische versus physische Topologie

Bus Topologie

- alle Netzwerkknoten werden direkt mit demselben Kabel verbunden
- jeder Knoten erhält eine ihn eindeutig identifizierende Adresse (Nachrichtenerkennung und Adressierung anderer Knoten)
- Netzwerkprotokoll regelt Erhalt der Nachrichten für die einzelnen Stationen
- Beispiele sind coax-basierte Netzwerke: 10Base-5, 10Base-2
  An den Enden gibt es einen Terminator

Bus Topologie

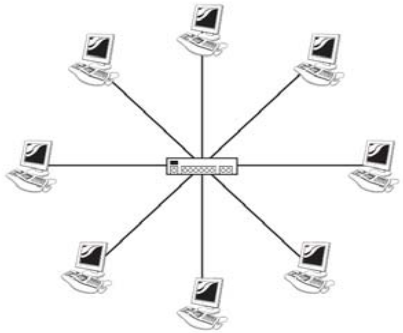
Vorteil:

- extrem einfache und effiziente Installation
- minimaler Verkabelungsaufwand, Netzwerkhardware billig

Nachteil:

- jede Komponente beeinflusst gesamtes Netzwerk
- Problem: Fehler bei Unterbrechung, Reflexion → Rauschen
- begrenzte Anzahl von Knoten pro Segment

Stern Topologie



- 10Base-T bzw. 100Base-T Ethernet mit Switch

Stern Topologie

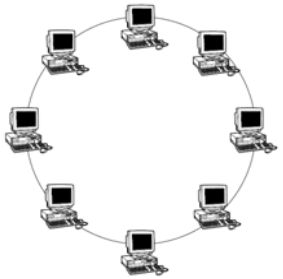
- es existiert ein zentrales System
- jeder Knoten wird durch ein eigenes Kabel an dieses System angeschlossen

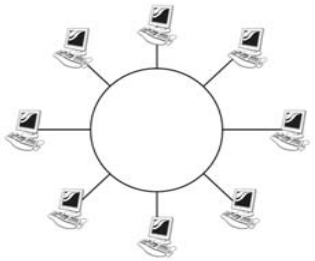
Nachteile: Kabelverbrauch, Kosten

Vorteile:

- Zuverlässigkeit, Ausfall nur eines Rechners bei Kabelbruch
- Netzwerkdiagnose in Zentralsystem einfacher

Ring Topologie

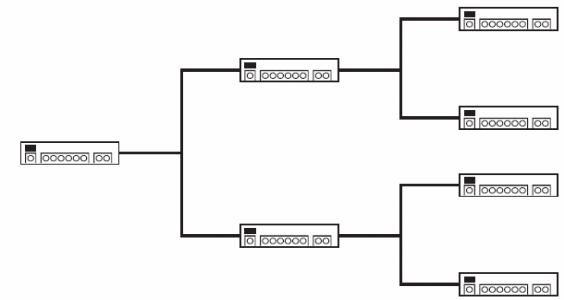




- Grundstruktur ist eine Kabelschleife
- die Signale werden von Knoten zu Knoten entlang des Rings übertragen (beachte Gegensatz zu Bus)

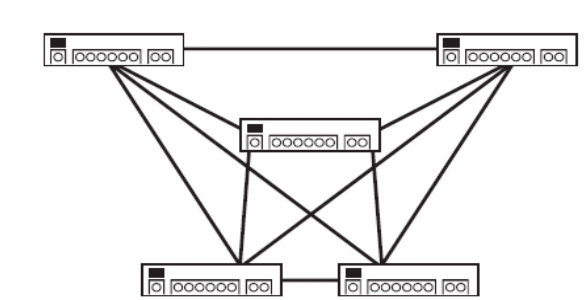
Beispiele: Token Ring, FDDI

Baum Topologie



- Mischung aus Bus und Star-Topologie

Netz Topologie



- Teilweise oder vollständig verbundenes Netz

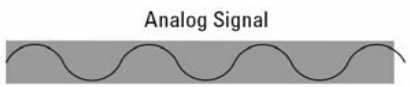
Übertragungstechniken

Basisband

- verwendet diskrete Signale (digitale Signalisierung)
- gesamte Kapazität des Übertragungskanals wird bereits für ein einzelnes Datensignal benutzt
- gemeinsame Kommunikation mehrerer Geräte durch Zeitmultiplex (TDM, Time-Division Multiplexing) möglich. die Übertragungszeit wird dabei in Zeitscheiben zerlegt

Breitband

- verwendet analoge Signale (Amplituden-, Frequenz- oder Phasenmodulation des Trägersignals)
- Frequenzmultiplex (FDM, Frequency-Division Multiplexing)



IEEE 802.3 Ethernet

- Geschwindigkeit von 10Mbps bis 10Gbps
- Adressierung im Ethernet über MAC-Adressen (**M**edia **A**ccess **C**ontrol)
- MAC Adressen sind hardwarebasiert und 6 Byte lang
- Da sich die Geräte ein Trägermedium teilen kommt es zu Kollisionen
- Lösung: **CSMA/CD** (Carrier Sense, Multiple Access with Collision Detection)

Netzwerkgeräte

- Repeater und Hub:
  - Arbeitet auf der ersten OSI-Schicht
  - Verstärkt alle empfangenen Signale (auch das Rauschen)
- Bridge und Switch:
  - Arbeiten auf der zweiten OSI-Schicht
  - Machen intelligente Entscheidungen durch Betrachtung der Ziel-Hardware-Adresse in Frames
- Router:
  - Arbeiten auf der dritten OSI-Schicht
  - Machen Entscheidungen aufgrund der Ziel-IP-Adresse
  - Ermittelt "beste" Route zwischen zwei oder mehr Netzwerken

TCP/IP Protokolle

Zur Protokollfamilie TCP/IP gehören u. a.:

- TCP: Transmission Control Protocol (L4)
- UDP: User Datagramm Protocol (L4)
- IP: Internet Protocol (L3)
- ARP: Address Resolution Protocol (L3)
- ICMP: Internet Control Message Protokoll (L3)

Die über ein IP-Netzwerk transportierten Daten werden in IP-Pakete eingekapselt.

IP ist ein routbares Protokoll:

Zwei über IP kommunizierende Knoten müssen nicht an dieselbe physische Leitung angeschlossen sein.

Adressierung

- Adresse dient eindeutiger Identifizierung
- Adressen sind numerisch und besitzen ein wohldefiniertes Format.
- Jedes Gerät erhält eine eindeutige ID, die Adresse des Gerätes.
- In gerouteten Netzwerken besteht die Adresse aus mindestens zwei Komponenten: einer Netzwerk- (oder Bereichs-) Komponente und einer Knoten- (oder Host-) Komponente.
- Die Adressierung der Geräte in einem Netzwerk und der Netzwerke in einem Netzwerkverbund muss eindeutig sein.
- Broadcast- oder Multicast-Adressen: dienen dem gleichzeitigen Ansprechen mehrerer Knoten

IP: Internet Protocol

- Logische Adressierung im Internet

IPv4 (Internet Protocol version 4)
- 32-bit Adressen, z.B. 137.208.107.18
- Sind weltweit eindeutig (ausgenommen sind die privaten IP-Adressbereiche: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)
  Werden von der IANA (Internet Assigned Numbers Authority) bzw. deren Tochterorganisationen wie RIPE (Europa), ARIN (Nordamerica) etc. vergeben.
- lesbare Namen wie balrog.wu-wien.ac.at durch weltweit gültiges **Domain Name System** (DNS). .at-Domains werden von nic.at vergeben.
- früher eingeteilt in 5 verschiedene Klassen (A-E) zur (hierarchischen) Adressierung von Netzen, Subnetzen und Endgeräten (Hosts)
- jetzt Adressierung/Semantik gemäß dem Classless Interdomain Routing Protocol (CIDR)

IPv6: Erweiterung von IPv4
- 128-Bit Adressen (mehrere Tausend pro cm² Erdoberfläche)
- größere Funktionalität durch flexible, erweiterbare Header-Definition
- z.B.: 2001:3A01:0000:0056:0000:ABCD:EF12:1234

IP-Adressklassen

- 126 **Class A** Netzwerke:
  Erstes Oktet von 1 bis 126 (1.0.0.0-126.0.0.0)
  network.host.host.host (Maske: 255.0.0.0)
  max. Hostanzahl: 2^24-2=16,777.214
- 16384 **Class B** Netzwerke:
  Erstes Oktet von 128 bis 191 (128.0.0.0-191.255.0.0)
  network.network.host.host (Maske: 255.255.0.0)
  max. Hostanzahl: 2^16-2=65534
- Über 2 Mio **Class C** Netzwerke:
  Erstes Oktet von 192 bis 223 (192.0.0.0-223.255.255.0)
  network.network.network.host (Maske: 255.255.255.0)
  max. Hostanzahl: 2^8-2=254
- Class E
  Erstes Oktet von 224-239 (reserviert für Multicasting)
- Class F
  Erstes Oktet von 240-255 (experimentell)
- 127.0.0.1 ist reserviert für den **Loopback**

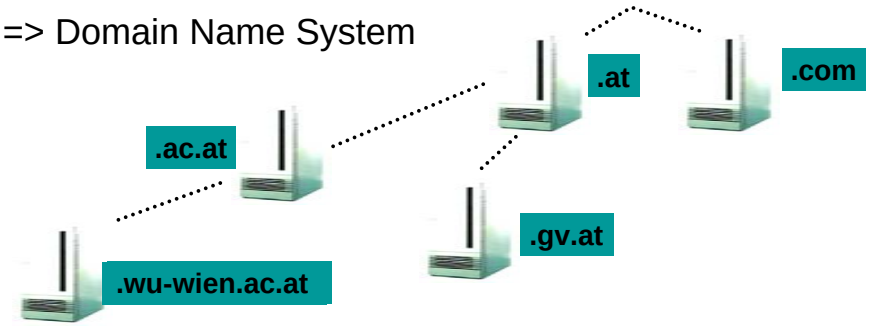
Private IP-Adressen

- Folgende IP-Adressbereiche sind laut RFC 1918 für den privaten Gebrauch bestimmt:
  - 1 Class A Netzwerk:
    10.0.0.0 (Maske: 255.0.0.0)
    max. Hostanzahl: 2^24-2=16,777.214
  - 16 Class B Netzwerke:
    172.16.0.0-172.31.0.0 (Maske: 255.255.0.0)
    max. Hostanzahl: 2^16-2=65534
  - 256 Class C Netzwerke:
    192.168.0.0-192.168.255.0 (Maske: 255.255.255.0)
    max. Hostanzahl: 2^8-2=254
- Private Adressen werden im Backbone nicht geroutet → Network Address (Port) Translation (NAT bzw NAPT)

IP-Adressen/DNS

Numerische Adressen sind schwer zu merken

=> Domain Name System



IP-Adressen/DNS

- Der Nameserver verwaltet eine Liste von Adressen mit dazugehörigen Namen
- 137.208.8.18 www.wu-wien.ac.at
- 137.208.107.18 balrog.wu-wien.ac.at

Abfrage mit **host** *hostname*

oder ***dig*** *hostname*

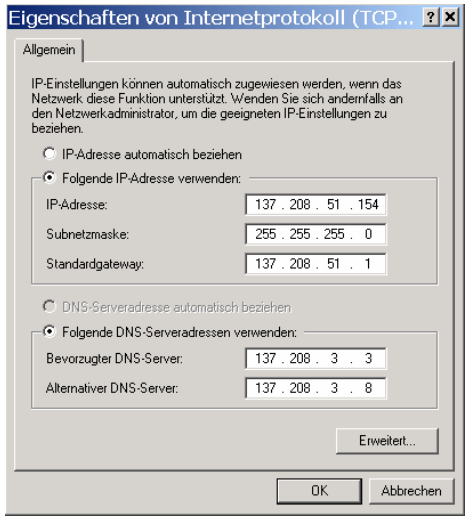
Übung: dig

MS Windows: Konfiguration

Jede Netzwerkkarte hat eine IP-Adresse:

Broadcast-Adresse: ?

Tipp: Überprüfung mit ipconfig /all



Routing Tabelle

- Windows Routing Tabelle:

```
===========================================================================
Aktive Routen:
Netzwerkziel        Netzwerkmaske          Gateway       Schnittstelle  Anzahl
0.0.0.0             0.0.0.0            137.208.51.1    137.208.51.154     1
127.0.0.0           255.0.0.0          127.0.0.1       127.0.0.1          1
137.208.51.0        255.255.255.0      137.208.51.154  137.208.51.154     1
137.208.51.154      255.255.255.255    127.0.0.1       127.0.0.1          1
137.208.255.255     255.255.255.255    137.208.51.154  137.208.51.154     1
224.0.0.0           224.0.0.0          137.208.51.154  137.208.51.154     1
255.255.255.255     255.255.255.255    137.208.51.154  137.208.51.154     1
Standardgateway:    137.208.51.1
===========================================================================
```

Anm: 137.208.51.154: die Adresse der Netzwerkkarte
127.0.0.1: loopback-Adresse

- Linux Routing Table:

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
0.0.0.0         192.168.1.1     0.0.0.0         UG    0      0        0 eth0
```

ARP

- ARP=Address Resolution Protocol (Layer 3)
- ARP ermittelt für eine bekannte IP-Adresse die hardwarebasierte Ethernet(MAC)-Adresse
- **ARP-Request** ist ein Broadcast an alle Knoten im LAN mit der Frage wer eine bestimmte IP-Adresse hat.
- **ARP-Reply:** Der Rechner mit der richtigen IP-Adresse antwortet und sind mit seiner Antwort gleichzeitig seine MAC-Adresse mit.
- Der **ARP-Cache** eines Betriebsystems speichert MAC-IP-Mappings für eine bestimmte Zeit um nicht für jedes gesendetes Paket diese Prozedur wiederholen zu müssen.
  Cache-Abfrage in Windows: arp –a, in Linux: arp

TCP (Transport Control Protocol)

Aufgaben von TCP

- **stellt eine logische, verlässliche Verbindung zwischen Sender und Empfänger her**.
- unterteilt den Datenstrom zwischen Sender und Empfänger in Segmente (L4 Pakete).
- Endpunkte der Verbindung heißen **Sockets**.
- Sockets sind **Ports** mit Nummern zwischen 0 und 2^{16} zugeordnet.
  Ports stellen die Verbindung zum Anwendungsprogramm (Dienst) her.
  Standarddienste wie FTP, HTTP,... sind Standardportnummern zugeordnet.
- TCP steuert den Datenfluss (Anzahl der Pakete/s) über die logische Verbindung durch das „Sliding Window Protocol“

  - Fenstergröße bestimmt, wie viele Bytes vor Erhalt einer Empfangsbestätigung versandt werden dürfen.
  - f wird dynamisch zwischen Sender und Empfänger ausgehandelt, abhängig von der aktuellen Pufferkapazität beim Empfänger (“maxwinsize”) und der aktuellen Transportleistung bzw. -qualität des Netzes.

UDP (User Datagram Protocol)

- **reicht den unzuverlässigen, verbindungslosen Dienst von IP an die Anwendungsschicht weiter**
- UDP wird beispielsweise für MultiMedia-Übertragungen eingesetzt, da es dort nicht darauf ankommt, jedes Datagramm zu erhalten, sondern möglichst viele pro Zeiteinheit.
- TCP könnte durch seine dynamische Flusssteuerung keinen gleichmäßigen Datenfluss gewährleisten.
- UDP verwendet ebenso Ports wie TCP (Ports sind aber voneinander unabhängig).
  z.B.: DNS Abfragen gehen an Port 53

TCP/UDP

TCP	UDP
• Sequenced	• Unsequenced
• Connection-oriented 3-Way Handshake	• Connectionless
• Reliable	• Unreliable (Best-effort)
• High overhead	• Low overhead
• Slower	• Fast

Analogie: Telefon versus Brief

ICMP

- ICMP=Internet Control Message Protocol
- Aufgabe:
  Transport von Fehler- und Diagnosemeldungen für das Internet Protokoll (IP), das User Datagram Protokoll (UDP) oder das Transmission Control Protokoll (TCP)
- ICMP-Meldungen werden in IP-Paketen verschickt.
- Beispiele:
  - Echo Request / Echo Reply / Network Unreachable / Host Unreachable / Port Unreachable / Redirect / Time to Live Exceeded

Ping

- **ping** *hostname* oder **ping** *ip_address*
  zur Überprüfung der Verbindung.
  sendet ICMP Echo Requests zum Host
- Bsp:

```
[ebner@lux7 ~]$ ping www.wu-wien.ac.at
PING www.wu-wien.ac.at (137.208.8.18) 56(84) bytes of data.
64 bytes from www.wu-wien.ac.at (137.208.8.18): icmp_seq=0 ttl=63 time=0.300 ms
64 bytes from www.wu-wien.ac.at (137.208.8.18): icmp_seq=1 ttl=63 time=0.271 ms
64 bytes from www.wu-wien.ac.at (137.208.8.18): icmp_seq=2 ttl=63 time=2.78 ms
64 bytes from www.wu-wien.ac.at (137.208.8.18): icmp_seq=3 ttl=63 time=0.270 ms

--- www.wu-wien.ac.at ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms

rtt min/avg/max/mdev  = 0.270/0.907/2.788/1.086 ms, pipe 2
```

Achtung: ICMP Echo Requests werden von vielen Firewalls gefiltert.

Traceroute

- **traceroute** (unter Windows: **tracert**)
  Darstellung der Route zum Zielrechner.
- Bsp:

```
[ebner@lux7 ~]$ traceroute www.orf.at
traceroute: Warning: www.orf.at has multiple addresses; using 194.232.104.29
traceroute to www.orf.at (194.232.104.29), 30 hops max, 38 byte packets
 1  gw-51.ai.wu-wien.ac.at (137.208.51.1)  0.504 ms  0.357 ms  0.292 ms
 2  box-1-19 (137.208.19.130)  4.186 ms  0.622 ms  0.379 ms
 3  ex-2-9 (137.208.9.22)  0.674 ms  0.773 ms  0.956 ms
 4  193.171.13.129 (193.171.13.129)  1.115 ms  1.555 ms  1.113 ms
 5  cvix2.apa.at (193.203.0.15)  1.695 ms  1.916 ms  1.140 ms
 6  cinter3-gig0-3.apa.net (194.158.154.249)  2.289 ms  2.356 ms  1.181 ms
 7  194.158.138.12 (194.158.138.12)  3.863 ms  2.323 ms  1.986 ms
 8  www.orf.at (194.232.104.29)  4.042 ms !<10>  13.829 ms !<10>  4.369 ms !<10>
```

Troubleshooting

Bei Connektivitätsproblemen werden diese vier Schritte von Cisco empfohlen:

1. Lokalhost pingen
   ping 127.0.0.1 (wenn ok - TCP-Stack ok)
2. Eigene IP-Adresse pingen (wenn ok - Netzwerkkarte funktioniert)
3. Default Gateway pingen (wenn ok - pysische Verbindung zwischen mir und dem default- Gateway ok)
4. Remote Host pingen

Achtung: nicht DNS-Namen verwenden