1 Internetarchitekturen

Die allgemeine Architektur des Internets ist gegeben durch die Vernetzung der Systeme auf unterschiedlichen Ebenen. Nutzer knnen ber Internet Exchange Points ("Internetknoten", IX or IXP, auch Network Access Point) verschiedenste Daten austauschen und generell werden diese von Providern (ISPs) zur Nutzung dargeboten.

Die meisten ISPs nutzen IX als Schnittstellen zwischen Rechnernetzwerken, wobei der gesamte Verbund aller autonomen Systeme das Internet bilden. Weltweit existieren ca. 340 IXPs, wobei kleinere Knotenpunkte als Uplink zu den 'Carriern', den ISPs, dienen. Die Vorteile mehrerer IX sind primr Effizienz und Ausfallsicherheit bei Datentransfer, wobei die Kosten fr den Betrieb eines IX von den dazugehrigen ISPs geteilt werden. Die Gebhren berechnen sich pro genutzten Port per eigenen IXP. Die Kosten fr den jeweiligen Port sind abhngig von dessen Transferrate - derzeit zwischen 10Mbps und 100 Gbps.

Bei den einzelnen ISPs unterscheidet man zwischen mehreren Kategorien (Tiers):

- Tier 1.: National & oftmals International, die grten Betreiber.
  z.B.: Deutsche Telekom, KPN, AT&T, Verizon, NTT, Telecom Italia,..
- Tier 2.: Transit Provider. Nehmen Downstream von Tier 1 in Anspruch und bieten Upstream fr Tier 3.
  z.B.: Vodafone, Tele2, Comcast
- Tier 3.: Lokale Provider. Sie verkaufen Transitmglichkeiten an Nutzer.

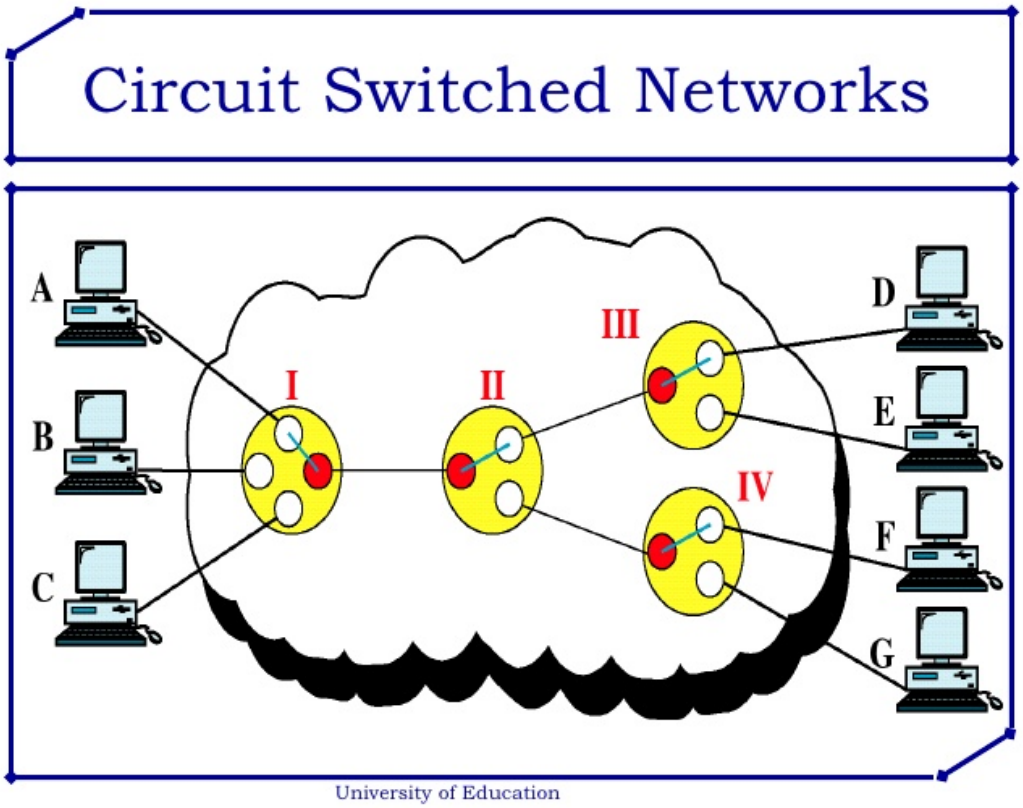
Es bleibt jedoch zu beachten dass die Kategorisierung regelrecht schwammig gefhrt wird.

Weiters ist das Internet noch durch Protokolle untersttzt, um fehlerfreien Austausch zu garantieren, oft beschrieben mithilfe des ISO/OSI-Referenzmodells (siehe 2.3).

2 Netzwerktypen

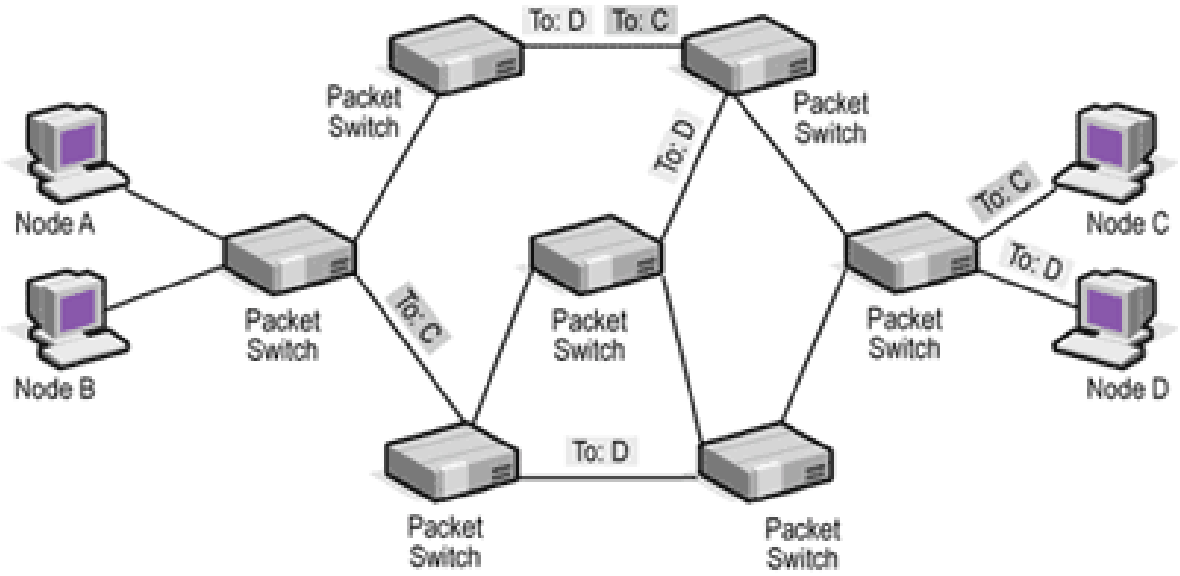
2.1 Leitungsvermittelnde Netzwerke

Leitungsvermittelnde Netzwerke, oder Circuit-Switch Networks, sind vergleichbar mit Telefonanrufen oder einem Schienennetz. Ein exklusiver logischer oder physikalischer Pfad wird zwischen Sender und Empfnger designiert, vergleichbar mit einer Krititschen Zone. Genutzte Ressourcen, benutzt oder nicht, stehen in dieser Zeit anderen Usern nicht zur Verfgung.

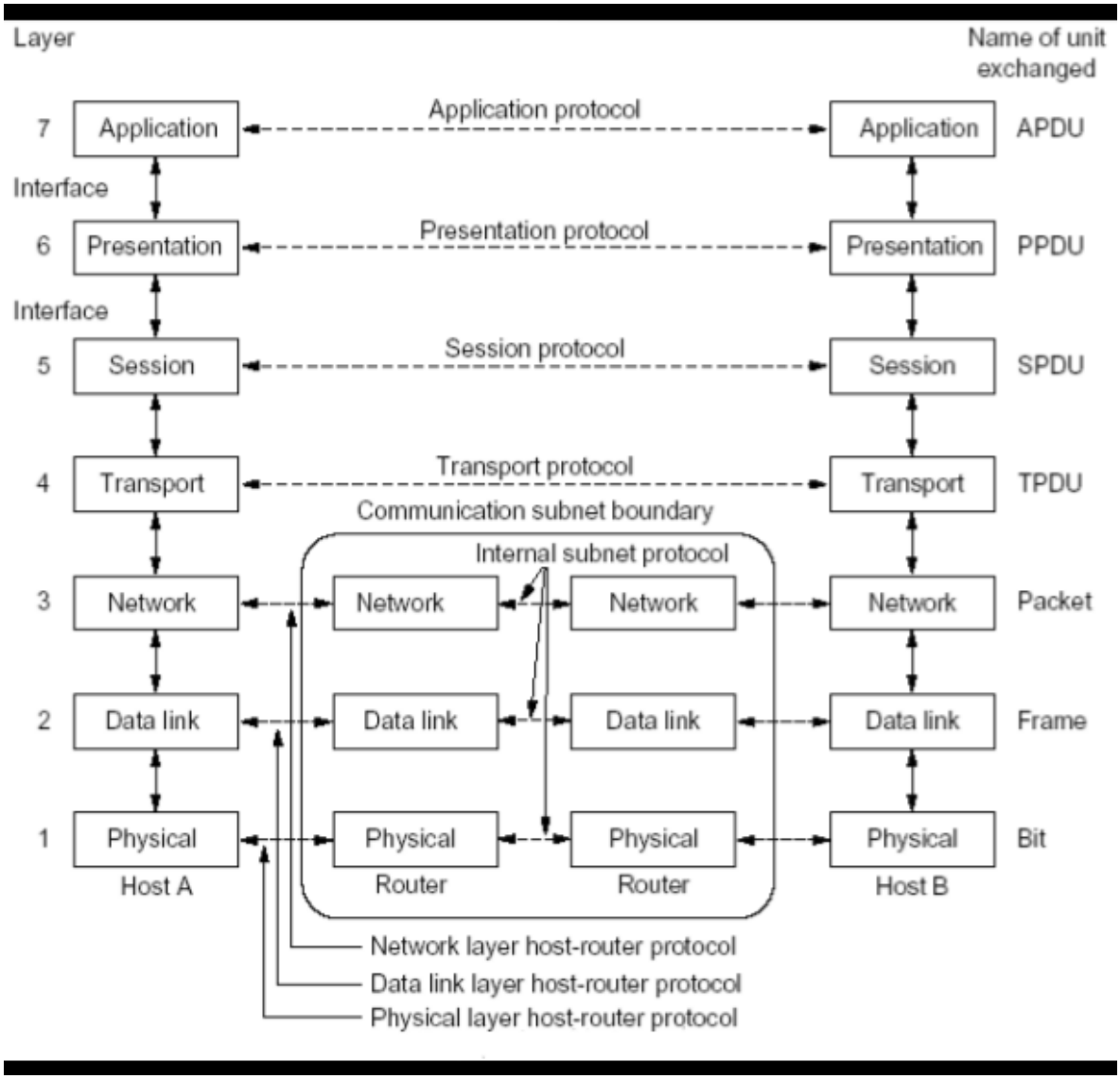


2.2 Paketvermittelnde Netzwerke

Paketvermittelnde Netzwerke, oder Packet-Switching Networks, sind charakteristisch gesehen wie E-Mails. Daten werden Bufferhnlich zu einem greren Datensatz zusammengeschrieben, welches das Datenpaket ausmacht. Diese werden vollstndig gesendet & vollstndig empfangen, wobei die Pakete ber dynamisch bestehende Pfade via Nodes verschickt wird. Dies ermglicht parallelen Transfer zwischen mehreren Usern und erhht die Ausfallsicherheit, da die Zielpfade der Pakete zur Laufzeit vernderbar sind.


To: D
To: C
Packet Switch
Packet Switch
To: D
To: C
To: D
Node A
Node B
Packet Switch
Packet Switch
Packet Switch
Node C
Node D
To: D
Packet Switch
Packet Switch

3 ISO-OSI Referenzmodel



Das ISO-OSI Referenzmodell besteht aus verschiedenen Anwendungsschichten:

1. Physical Layer
   Dieser Layer beschreibt die fundamentale Netzwerkkommunikation. Datentransfer via physischem Layer sind reine Bitstreams.

   Hardware:

   PHY-Chip: Ein PHY implementiert die Funktionen Senden und Empfangen von Daten zwischen Gerten mithilfe des Datalink Layers (MAC, LLC). Es enkodiert und dekodiert einkommende bertragungen und Galvanische Trennung (Blockt ungewollten Datenempfang).

   Protokolle:

   Integrated Services Digital Network: Internationaler Standard fr Datenbertragung & Telefonie Universal Serial Bus: Bussystem von Verbindungen um Daten zu

bertragen Bluetooth, Ethernet, ...

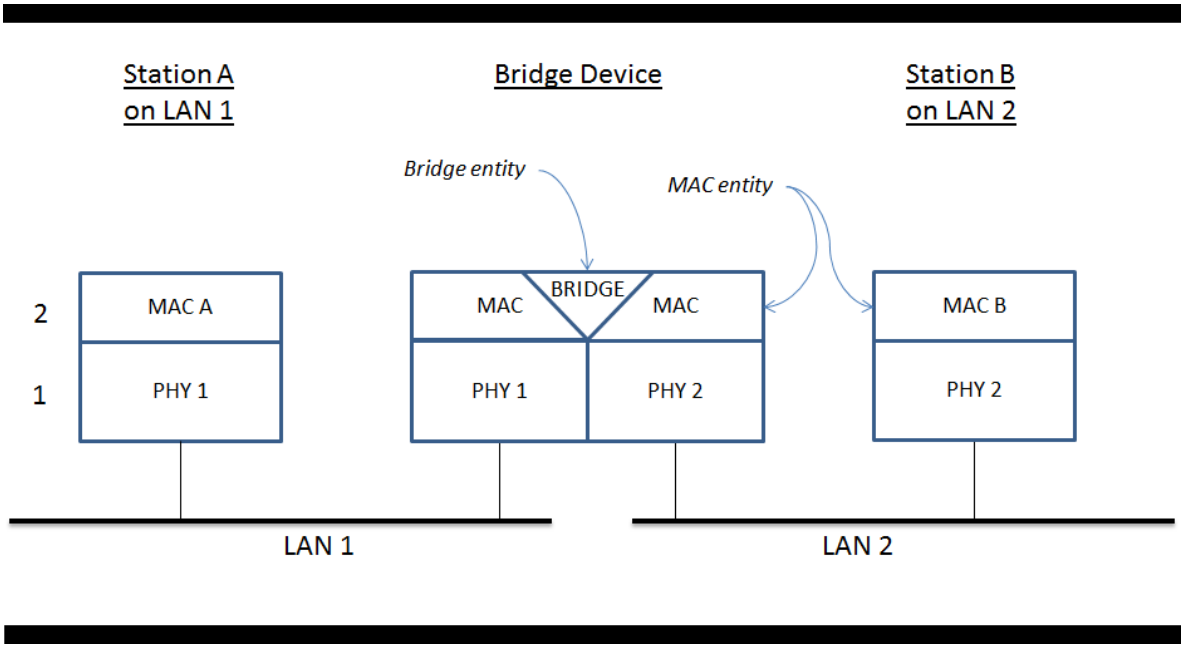
Normen:

2. Data Link Layer
   Der Datenlink nutzt Frames zur bertragung von Datenstzen. Frames bestehen aus einer gewissen Anzahl an Bit-Blcken und einer Prfsumme, welche die korrekte Datenflussbertragung gewhrleistet. Fehlerbehafte Frames knnen anhand dieser Summe erkannt werden und der DLL kann das jeweilige Paket verwerfen oder sogar korrigieren. Im Falle des Verwerfens ist es allerdings nicht vorgesehen das jeweilige Frame neu anzufordern.

   Mithilfe der 'Data Flow Control' kann man die Dynamik der Framebertragung steuern, etwa wie schnell Blcke verschickt werden.

   Hardware:

   Bridge & Switch: Arbeiten via Media Access Control(Mac) oder Logical Link Control(LLC).
   Die MAC-Bridge schtzt gegen Kollisionen via Aufteilung des Netzes in verschiedene Kollisionsdomnen, d.H. ein Paket geht nur in das Netz, in welchem sich der tatschliche Empfnger befindet.
   Die LLC-Bridge dient der Koppelung zweier Teilnetze mithilfe verschiedener Zugriffsverfahren, wie Token-Passing (Tokens werden zwischen Sendern gewechselt und dementsprechend startet Datenverkehr) oder Carrier Sense Multiple Access/Collision Detection (CSMA/CD; Typischer Router mit x-Medien).



Schemata of Bridge/Switch inside a Network[1]

Protokolle:

HDLC - High-Level Data Link Control: Transmition of sync/async frames
SDLC - Synchronous Data Link Control: Bitsynchron & Serielle bertragung

[1] By Crvincenzi - MS Powerpoint, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=25610536

DDCMP - Digital Data Communications Message Protocol: Point-to-Point Transfer (Sicherheit)
SPB - Shortest Path Bridging: Aufbau & Konfig. + Multipath Routing

Normen: IEEE, FDDI, ISO

3. Network Layer Der Network Layer behandelt Weiterleitung und Routing durch multiple Zwischenmedien innerhalb eines Netzwerkes.

   Funktionen:

   - CL-mode: Verbindungslose Kommunikation, ber IP
   - Hostadressierung, jeder Host ist einzigartig identifizierbar
   - Weiterleitung: Partitionierung von Netzwerken in Subnetzwerke und Weiterleitung von Daten ber Gateways und Router

4. Transport Layer Die Transportschicht beschreibt den konkreten Datentransfer von A nach B.

   Protokolle:

   - Transmission Control Protocol: TCP/IP - Datentransfer wird kontrolliert weitergegeben. Wird das Paket falsch oder garnicht empfangen, so wird eine Anfrage geschickt welche das Datenpaket neu schickt. Es gibt Flow- und Congestioncontrol. Grundstzlich genutzt bei HTTP, FTP, SMTP.
   - User Datagram Protocol: UDP/IP - Datentransfer wird losgeschickt, ohne Kontrolle ob das Datenpaket tatschlich ankommt. Es gibt also weder Flow- noch Congestioncontrol.

5. Session Layer
6. Presentation Layer
7. Application Layer

Die 5. und 6. Schicht wird meist impliziert, bzw. wird von der Praxis nicht angenommen.

4 ISO/OIS Referenzmodel vs. TCP/IP-Referenzmodell

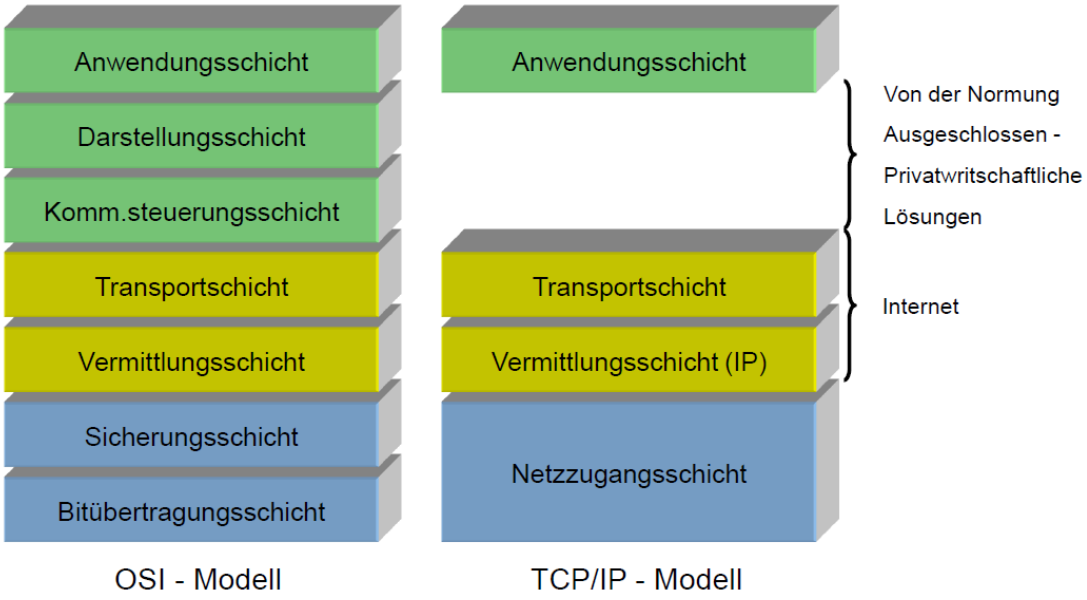
TCP/IP Referenzmodell besteht mehr oder weniger aus den gleichen Schichten wie das ISO/OSI-Referenzmodell, jedoch besteht es lediglich aus vier Schichten, da die Schichten 5 und 6 nicht verwendet werden.
Es beruht auf den Vorschlgen ,die bei der Fortentwicklung des ARPANET's gemacht wurden. Diese Art des Modells ist zeitlich vor dem OSI-Referenzmdell entstanden, weshalb auch die ERfahrungen dieses Modells in die OSI-Standardisierung miteingeflossen sind. Es bildet die Basis fr smtliche Netzwerke, sowie fr das OSI-Modell, wie wir es heute kennen.

IP tu hierbei nichts anderes, als die Daten, mit bestimmten Ziel und Absender, einfach nur zu

verschicken. In Kombination mit TCP soll letztendlich gewhrleistet werden, dass die Daten fehlerfrei ankommen. Als Ziele der Architektur wurden bei der Entwicklung definiert:

1. Unabhngigkeit von der verwendeten Netzwerk-Technologie
2. Unabhngigkeit von der Architektur der Hostrechner.
3. Universelle Verbindungsmglichkeiten im gesamten Netzwerk.
4. Ende-zu-Ende-Quittungen.
5. Standardisierte Anwendungsprotokolle.

Das TCP/IP-Referenzmodell besteht im Gegensatz zum OSI-Modell aus nur vier Schichten.



1. Application Layer

   Umfasst alle hherschichtigen Protokolle des TCP/IP-Modells. Zu den ersten Protokollen der Verarbeitungsschicht zhlen TELNET (fr virtuelle Terminals), FTP (Dateitransfer) und SMTP (zur bertragung von E-Mail). Im Laufe der Zeit kamen zu den etablierten Protokollen viele weitere Protokolle wie z.B. DNS (Domain Name Service) und HTTP (Hypertext Transfer Protocol) hinzu.

   Protokolle:

   (a) DNS (Domain Name System) - Umsetzung zwischen Domainnamen und IP-Adressen.

   (b) DoIP (Diagnostic over IP) - Transportprotokoll fr Fahrzeugdiagnose.

   (c) FTP (File Transfer Protocol) - Dateitransfer.

(d) HTTP (Hyper Text Transfer Protocol, WWW)

(e) HTTPS - (Hyper Text Transfer Protocol Secure)

(f) IMAP (Internet Message Access Protocol) - Zugriff auf E-Mails.

(g) IPFIX (Internet Protocol Flow Information Export)

(h) L2TP (Layer 2 Tunneling Protocol)

(i) LLMNR (Link-local Multicast Name Resolution)

(j) NDMP (Network Data Management Protocol)

(k) MBS/IP (Multi-purpose Business Security over IP)

(l) NNTP (Network News Transfer Protocol) - Diskussionsforen (Usenet)

(m) NTP (Network Time Protocol)

(n) POP3 (Post Office Protocol, Version 3) - E-Mail Abruf

(o) RTP (Real-Time Transport Protocol)

(p) SIP (Session Initiation Protocol) - Aufbau, Steuerung und Abbau von Kommunikationssitzung (VoIP).

(q) SNMP (Simple Network Management Protocol) - Verwaltung von Gerten im Netzwerk.

(r) SMTP (Simple Mail Transfer Protocol) - E-Mail Versand.

(s) SOCKS (Internet Sockets-Protokoll)

(t) SSH (Secure Shell) - verschlsselter REMOTE TERMINAL

(u) Telnet - unverschlsseltes Login auf entfernten Rechnern.

(v) XMPP (Extensible Message and Presence Protocol)

(w) Z39.50 - Abfrage von Informationssystemen

2. Transport Layer:

   Ermglicht wie im OSI-Modell die Kommunikation zwischen Quell- und Zielhost. Hierzu wurden zwei End-zu-End-Protokolle definiert:

   - Transmisstion Control Protocol (TCP)

     Ist ein zuverlssiges verbindungsorientiertes Protokoll, durch das ein Bytestrom fehlerfrei einem anderen Rechner im Internet bermittelt werden kann.

   - User Datagram Protocol (UDP)

     UDP ist ein unzuverlssiges Protokoll, welches vorwiegend in Client/Server-Umgebungen verwendet wird, in denen es in erster Linie nicht um eine sehr genaue, sondern schnelle Datenbertragung geht.

   Protokolle:

   (a) TCP (Transmission Control Protocol) - bertragung von Datenstrmen (verbindungsorientiert, zuverlssig).

   (b) UDP (User Datagram Protocol) - bertragung von Datenpaketen (verbindungslos, unzuverlssig, geringer Overhead).

   (c) SCTP (Stream Control Transmission Protocol) - Transportprotokoll.

   (d) TLS (Transport Layer Security) - Erweiterung von TCP um Verschlsselung.

   (e) DTLS (Datagram Transport Layer Security) - Auf TLS basierendes Verschlsselungsprotokoll, das auch ber zustandslose Protokolle wie UDP bertragen werden kann.

3. Internet Layer:

   Diese Schicht definiert nur ein Protokoll namens IP (Internet Protocol), das alle am Netzwerk beteiligten Rechner verstehen kann. Sie hat die Aufgabe IP-Pakete richtig zuzustellen. Dabei spielt das Routing der PAkete eine wichtige Rollen. Das Internet Control Message Protocol (ICMP) ist fester Bestandteil jedes IP-Implementierung und dient zur bertragung von Diagnose- und Fehlerinformation fr das Internet Protocol.

   Protokolle:

(a) IP (Internet Protocol) - Datenpalet-bertragung (verbindungslos)

(b) IPsec (Internet Protocol Security) - Sichere Datenpaket-bertragung (verbindungslos)

(c) ICMP (Internet Control Message Protocol) - Kontrollnachrichten (zum Beispiel Fehlermeldungen), Teil jeder IP-Implementierung

(d) IGRP (Interior Gateway Routin Protocol) - Informationsaustausch zwischen Routern (Distanzvektor) (veraltet - ersetzt durch EIGRP)

(e) OSPF (Open Shortes Path First) - Informationsaustausch zwischen Routern (Linkzustand) via IP

(f) BGP (Border Gateway Protocol) - Informationsaustausch zwischen autonomen Systemen im Internet via TCP

(g) RIP (Routing Information Protocol) - Informationsaustausch zwischen Routern vid UDP

(h) IGMP (Internet Group Management) - Organisation von Multicast-Gruppen, Bestandteil von IP auf allen Hosts, die den Empfang von IP-Multicast unterstzen

4. Network Layer:

Unterhalbe der Internetschicht befindet sich i TCP/IP-Modell eine gro0e Definitionslcke. Das Referenzmodell sagt auf dieser Ebene nicht viel aus, was hier passieren soll. Festgelegt ist lediglich, dass zur bermittlung von IP-Paketen ein Host ber ein bestimmtes Protokoll an ein Netz geschlossen werden muss. Dieses Protokoll ist im TCP/IP-Modell nicht weiter definiert und weicht von Netz zu Netz und Host zu Host ab. Dieses Modell macht an dieser Stelle vielmehr Gebrauch von bereits vorhandenen PRotokollen, wie z.B. Ethernet (IEE 802.3), Serial Line IP(SLIP), etc.

Protokolle:

(a) Ethernet mit CSMA/CD - Netzwerkstandard IEEE 802.3

(b) WLAN - Netzwerkstandard IEEE 802.11

(c) PPP - Point-to-Point Protokoll

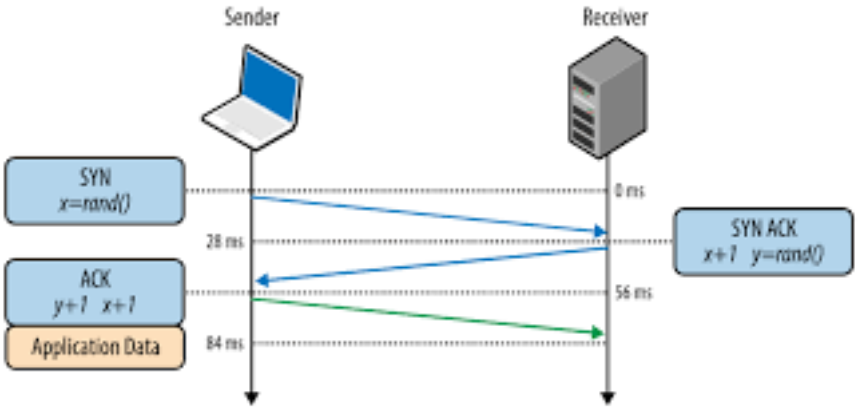
(d) Token Bus - Netzwerkstandard IEEE 802.4

(e) Token Ring - Netzwerkstandard IEEE 802.5

(f) FDDI - Fiber Distributed Data Interface

(g) ARP (Adress Resolution Protocol) - Adressumsetzung zwischen IP- und Gerteadressen (MAC)

(h) RARP (REverse Adress Resolution Protocol) - Adressumsetzung zwischen Gerte- (MAC) und IP-Adressen (veraltet - wird durch BOOTP ersetzt)



TCP Three-Way-Handshake:

1. Kontakt mit anderem Computer aufnehmen, indem Nachricht x gesendet wird.

2. Nun antwortet der Server mit der Sequenz, die er vom Client bekommen hatte, jedoch wurde zu dieser Sequenz plus eins dazu gerechnet.

3. Um Verbindung entgltig aufzubauen, antwortet der Client noch ein letztes mal.

5 TCP vs. UDP

Wie im OSI-Modell ermglicht die Transportschicht die Kommunikation zwischen den Quell- und Zielhosts. Auf dieser Schicht wurden zwei Ende-zu-Ende-Protokolle definiert:

- Transport Control Protocol (TCP)

- User Datagram Protocol (UDP)

1. User Datagram Protocol:

   Ist ein sogenannter Datagramm-Dienst, bei dem ledigliche Datenpakete verschickt werden. Hierbei muss sich das Applikationsprotokoll um Dinge wie Fehlerbehandlung, Quittierung kmmern.

2. Transport Control Protocol:

   TCP ist dagegen ein gesichertes, verbindungsorientiertes Protokoll: man ffnet zuerst eine "Verbindung" ber das dann die Daten bertragen werden. Hierbei wird garantiert, dass die Daten vollstndig, unverflscht und in der richtigen Reihenfolge ankommen. Auerdem funktioniert diese Verbindung in beide Richtungen. Anders als bei UDP kann man damt z.B. "Anfragen und Antworten" leicht zuordnen, weil sie ber dieselbe Verbindung geschickt werden.

Anwendungsprotokolle:

1. DNS
2. Internet Control Message Protocol (ICMP)
3. Telnet
4. File Transfer Protocol (FTP, TFTP)
5. HTTP