# 1 Internetarchitekturen

Die allgemeine Architektur des Internets ist gegeben durch die Vernetzung von 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.

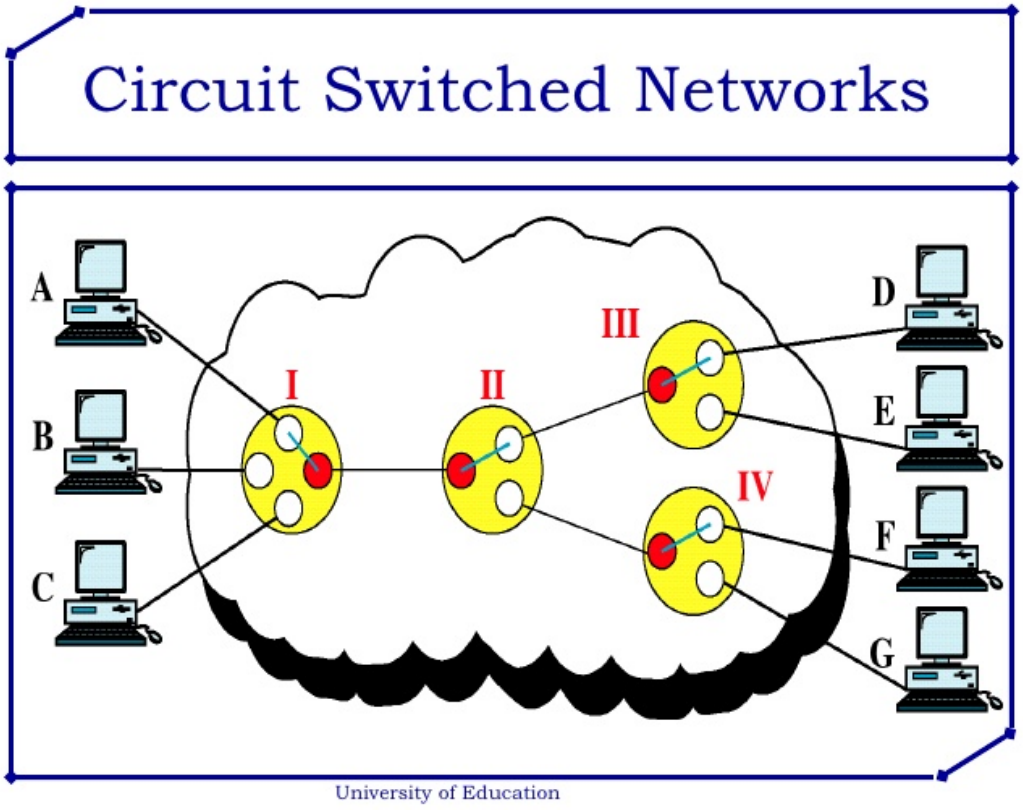
Weiters ist das Internet noch durch Protokolle untersttzt, um fehlerfreien Austausch zu garantieren, oft beschrieben mithilfe des ISO/OSI-Referenzmodells (siehe 2.3).

Mit den IX im Vordergrund, stehen im Hintergrund mehrere angewandte Techniken:
- *Verbindungsklassen*:
  - ◇ Point-to-Point: Ein Computer zum nchsten
  - ◇ Multi-Point: Mehrere Computer an einem Subnetwork
  - ◇ Switched Networks: Viele Computer in einem Network
  - ◇ Interconnected Networks: Mehrere Networks zusammen
- *Verbindungstypen*:
  - ◇ Simplex: bertragung in eine Richtung
  - ◇ Half-Duplex: bertragung von 2 Seiten bei asynchroner bertragung
  - ◇ Duplex: bertragung von 2 Seiten bei synchroner bertragung

# 2 Netzwerktypen

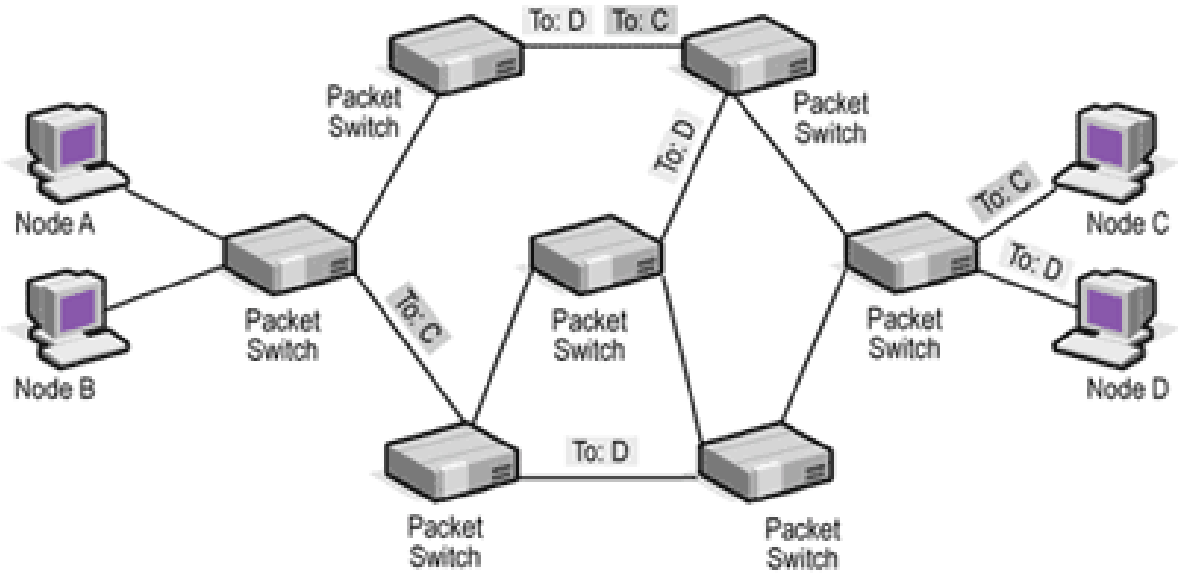
## 2.1 Leitungsvermittelnde Netzwerke

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.

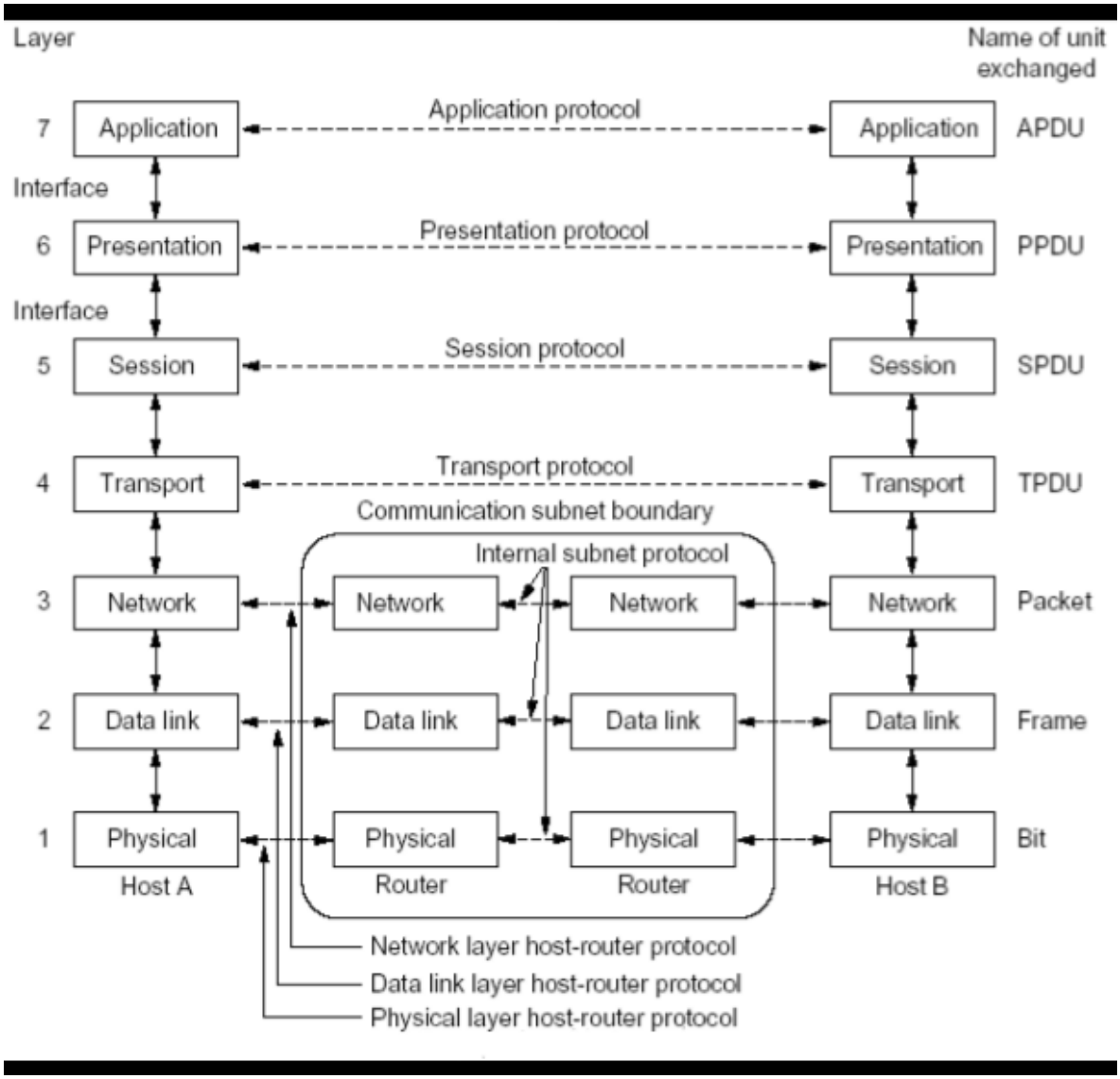



## 2.2 Paketvermittelnde Netzwerke

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 ermglicht Galvanische Trennung (blocken ungewollter Daten).

   *Protokolle*:

   Integrated Services Digital Network: Internationaler Standard fr Datenbertragung & Telefonie

Universal Serial Bus: Bussystem von Verbindungen um Daten zu bertragen
Bluetooth, Ethernet, ...

Grundstzlich wird alles Hardwaretechnische ber diese Schicht definiert - Kein Anschluss zum Router, eine unterbrochene Kabelverbindung, u.s.w..

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.

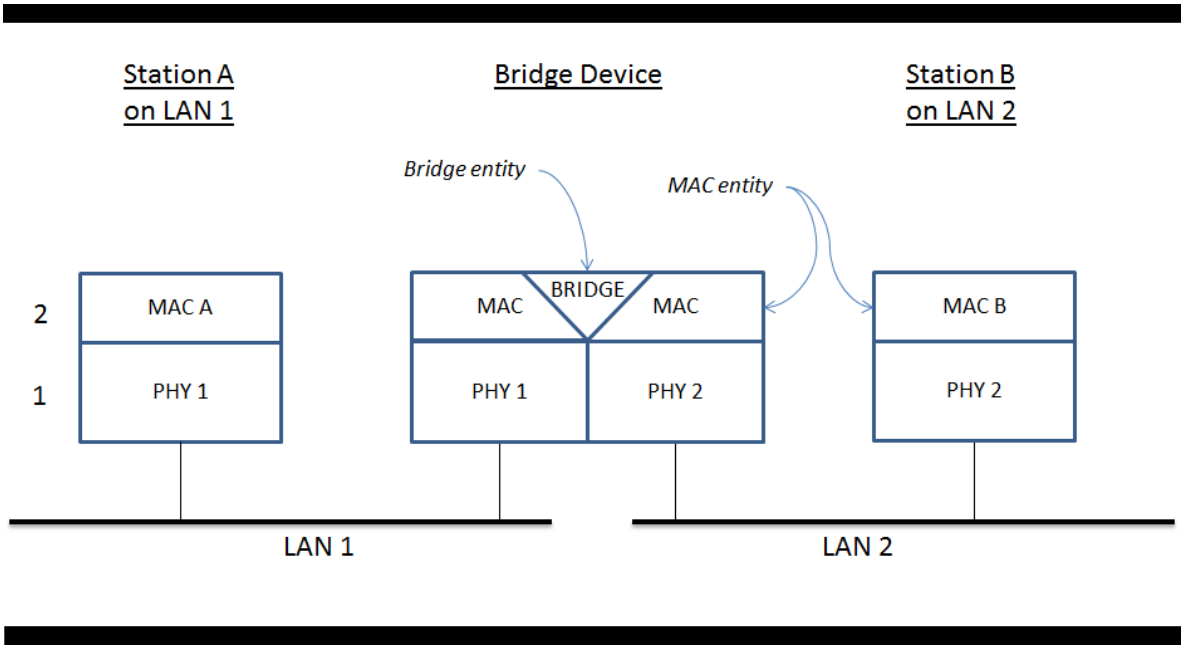
*Hardware*:

Bridges & Switches: 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).

*Protokolle*:

HDLC - High-Level Data Link Control: Transmition of sync/async frames
SDLC - Synchronous Data Link Control: Bitsynchron & Serielle bertragung
DDCMP - Digital Data Communications Message Protocol: Point-to-Point Transfer (Sicherheit)
SPB - Shortest Path Bridging: Aufbau & Konfig. + Multipath Routing

*Normen*: IEEE, FDDI (Fiber Distributed Data Interface), ISO




*Schemata of Bridge/Switch inside a Network*[1]

3. **Network Layer**
   Der "Network Layer", oder "the Routing Layer", behandelt die Weiterleitung und Routing durch multiple Zwischenmedien innerhalb eines Netzwerkes.

   *Funktionalitten*:

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

4. **Transport Layer**
   Dieser beschreibt den konkreten Datentransfer von A nach B, genannt "Windowing": Wieviele Daten geschickt oder empfangen werden, wann Daten gesendet werden, u.s.w..

   *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**
   Es beschreibt alles rund um das ffnen, schlieen und managen von Sessions zwischen

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

Usern. Es handelt sich dabei um einen anhaltenden Dialog der Gerte und behandelt Datensynchronisation und 'Checkpointing'[1].

*Protokolle*:

- ISO 8326 - OSI protocol suite: Neuverbindungsaufbau nach Strungen - ZIP - Zone Information Protocol (AppleTalk) - SMB - Server Message Block - RPC - Remote Procedure Call

Wenn man beispielsweise eine Website aufruft, so startet der Layer eine 'Session' mit dem jeweiligen Webserver.

6. **Presentation Layer**
   Die Prsentationsschicht dient der Darstellung der bertragenen Daten, auch 'Syntax Layer' genannt. Durch Konventionen wie ISO, ASCII oder EBCDIC werden die Bitcodes in erste Strukturen umgewandelt.

   Alles was im Rahmen des eigenen Betriebssystemes passiert kann dieser Schicht zugeordnet werden: Protokollkonvertierung, Datenbersetzung, Kompression, Enkryption, Interpretation von graphischen Kommandos,...

7. **Application Layer**
   Die Anwendungsschicht spezifiziert den Zugriff auf das Netzwerk, beispielsweise Client/Server-Verbindung, P2P, etc.

   Es stellt sicher, dass eine Applikation auf System A genauso aussieht wie auf System B, was prinzipiell alles wiederspiegelt womit der User direkt arbeitet, z.B. FireFox, Chrome, Skype, Outlook, ...

Die Kommunikation derselben Schichten zwischen 2 Usern geschieht anhand der definierten Protokolle und dient grundstzlich dem Exception-Handling:

- ◇ Physical Layer: Verbindungsunterbruch auf Basis der Hardware
- ◇ Datalink Layer: Bitsynchrone bertragung, Serielle bertragung, Point2Point-Transfer, richtige MAC/LLC-Adressierung
- ◇ Network Layer: Verwerfen fehlerbehafteter Pakete, Routing
- ◇ Transport Layer: bertragungsprotokoll: TCP-IP oder UDP-IP
- ◇ Session Layer: Besttigung zum Datentransfer, Erhalt der Daten ist mglich, Verbindungsaufbau, Timeout-Handling
- ◇ Presentation Layer: Kodierungsformat, Enkryption, Dekryption
- ◇ Application Layer: Darstellung durch jeweilige User-Applikation.

Kurzum:
- Gleiche Schichten kommunizieren mittels Protokollen miteinander
- Zwischen den Schichten kommen Schnittstellen zum Einsantz
- Obere Schichten bauen auf den Unteren auf.

[1] Save states bei Fehler :: Laden bei Page 101 fhrt zu Fehler <=> Neuladen von 1-100 nicht notwendig

- Die 5. und 6. Schicht wird meist impliziert.

**Beispiel: Versenden einer E-Mail**

Das Senden einer Mail geschieht durch den User direkt im Application Layer.
Dieser gibt den Datensatz weiter an den Presentation Layer, welcher die Mail in eine systemunabhngige Datei umschreibt, inklusive dessen Codierungsform und Enkryption.
Weiter im Session Layer wird die Sitzung zum Zielempfnger spezifiziert, etwa @gmail.
Der Transport Layer definiert den Datenbertragungstyp, TCP/IP, UDP/IP.
Der Network Layer setzt anschlieend einen Pfad fest, auf welchem das Datenpaket zum Empfnger gesendet wird. Dies ist spter noch nderbar.
Der Datalink Layer formt aus dem oben erstellten, systemunabhngigen Dateiabbild die 'Frames'.
Via Bridge & Switch wird anhand MAC/LLC die Datenbertragung kontrolliert weitergegeben.
Die Physische Schicht gibt nun die Daten aus dem eigenen System einem Router, bzw. einem Bridge-Device, weiter.

Anhand des vorgegebenen Pfades werden nun die Daten von A nach B transferiert.

In System B treffen nun die Daten aus System A via physischen Layern ein. Der Datalinklayer setzt die Frames zusammen, der Network Layer besttigt die korrekte Adressierung, der Transport Layer kommuniziert entsprechend Protokolltypes zurck, der Sitzungslayer besttigt die erstellte Sitzung der Systeme. Der Presentation layer schreibt Frames in dasselbe Dateiabbild zurck wie vor der Transformierung in Bit und der Applikationslayer gibt die Daten dem Zieladdressaten wieder.

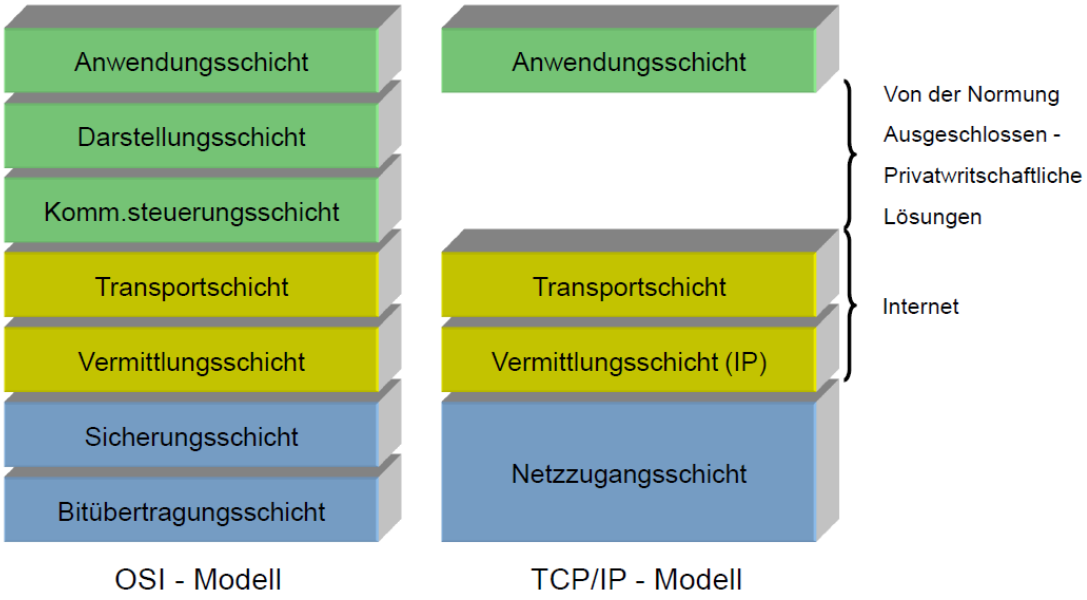
# 4 ISO/OIS Referenzmodel vs. TCP/IP-Referenzmodell

TCP/IP Referenzmodell basiert auf dem ISO/OSI-Modell, jedoch besteht es lediglich aus vier Schichten, da die Schichten 5 und 6 nicht verwendet werden. Es beruht auf Verbesserungen und Vorschlgen, welche bei der Weiterentwicklung des ARPANET's gemacht wurden.
Das TCP/IP-Referenzmodel ist zeitlich vor dem OSI-Referenzmodell entstanden, weshalb Erfahrungen und Ideen dieses Modells in die OSI-Standardisierung miteingeflossen sind.
TCP/IP bildet die Basis fr smtliche Netzwerke, sowie fr das OSI-Modell, wie wir es heute kennen.

Die IP tut hierbei nichts anderes als die Daten, mit bestimmten Ziel und Absender, zu verschicken. In Kombination mit TCP soll letztendlich gewhrleistet werden, dass die Daten ganzheitlich und fehlerfrei ankommen. Die Ziele der Architektur wurden bei der Entwicklung folglich 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, wie gesagt, im Gegensatz zum OSI-Modell aus nur vier Schichten.




## 4.1 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:*

- DNS (Domain Name System) - Umsetzung zwischen Domainnamen und IP-Adressen.
- DoIP (Diagnostic over IP) - Transportprotokoll fr Fahrzeugdiagnose.
- FTP (File Transfer Protocol) - Dateitransfer.
- HTTP (Hyper Text Transfer Protocol, WWW)
- HTTPS - (Hyper Text Transfer Protocol Secure)
- IMAP (Internet Message Access Protocol) - Zugriff auf E-Mails.
- IPFIX (Internet Protocol Flow Information Export)

- ◇ L2TP (Layer 2 Tunneling Protocol)
- ◇ LLMNR (Link-local Multicast Name Resolution)
- ◇ NDMP (Network Data Management Protocol)
- ◇ MBS/IP (Multi-purpose Business Security over IP)
- ◇ NNTP (Network News Transfer Protocol) - Diskussionsforen (Usenet)
- ◇ NTP (Network Time Protocol)
- ◇ POP3 (Post Office Protocol, Version 3) - E-Mail Abruf
- ◇ RTP (Real-Time Transport Protocol)
- ◇ SIP (Session Initiation Protocol) - Aufbau, Steuerung und Abbau von Kommunikationssitzung (VoIP).
- ◇ SNMP (Simple Network Management Protocol) - Verwaltung von Gerten im Netzwerk.
- ◇ SMTP (Simple Mail Transfer Protocol) - E-Mail Versand.
- ◇ SOCKS (Internet Sockets-Protokoll)
- ◇ SSH (Secure Shell) - verschlsselter REMOTE TERMINAL
- ◇ Telnet - unverschlsseltes Login auf entfernten Rechnern.
- ◇ XMPP (Extensible Message and Presence Protocol)
- ◇ Z39.50 - Abfrage von Informationssystemen

4.2 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)

  TCP ist ein zuverlssiges verbindungsorientiertes Protokoll, durch das ein Bytestrom fehlerfrei einem anderen Rechner im Internet bermittelt werden kann. Mittels virtuellem Handshake wird sichergestellt, dass die Daten fehlerfrei und ganzheitlich transferiert wurden.

- 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. Durch das ungecheckte Versenden knnen hierbei Datenstze verloren gehen.

*Protokolle:*

- ◇ TCP (Transmission Control Protocol) - bertragung von Datenstrmen (verbindungsorientiert, zuverlssig).
- ◇ UDP (User Datagram Protocol) - bertragung von Datenpaketen (verbindungslos, unzuverlssig, geringer Overhead).
- ◇ SCTP (Stream Control Transmission Protocol) - Transportprotokoll.
- ◇ TLS (Transport Layer Security) - Erweiterung von TCP um Verschlsselung.
- ◇ DTLS (Datagram Transport Layer Security) - Auf TLS basierendes Verschlsselungsprotokoll, das auch ber zustandslose Protokolle wie UDP bertragen werden kann.

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

*Protokolle:*

- ◇ IP (Internet Protocol) - Datenpalet-bertragung (verbindungslos)
- ◇ IPsec (Internet Protocol Security) - Sichere Datenpaket-bertragung (verbindungslos)
- ◇ ICMP (Internet Control Message Protocol) - Kontrollnachrichten (zum Beispiel Fehlermeldungen), Teil jeder IP-Implementierung
- ◇ IGRP (Interior Gateway Routin Protocol) - Informationsaustausch zwischen Routern (Distanzvektor) (veraltet - ersetzt durch EIGRP)
- ◇ OSPF (Open Shortes Path First) - Informationsaustausch zwischen Routern (Linkzustand) via IP
- ◇ BGP (Border Gateway Protocol) - Informationsaustausch zwischen autonomen Systemen im Internet via TCP

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

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

4.4 Network Layer:

Unterhalb der Internetschicht befindet sich im TCP/IP-Modell eine groe 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:*

- ◇ Ethernet mit CSMA/CD - Netzwerkstandard IEEE 802.3

- ◇ WLAN - Netzwerkstandard IEEE 802.11

- ◇ PPP - Point-to-Point Protokoll

- ◇ Token Bus - Netzwerkstandard IEEE 802.4

- ◇ Token Ring - Netzwerkstandard IEEE 802.5

- ◇ FDDI - Fiber Distributed Data Interface

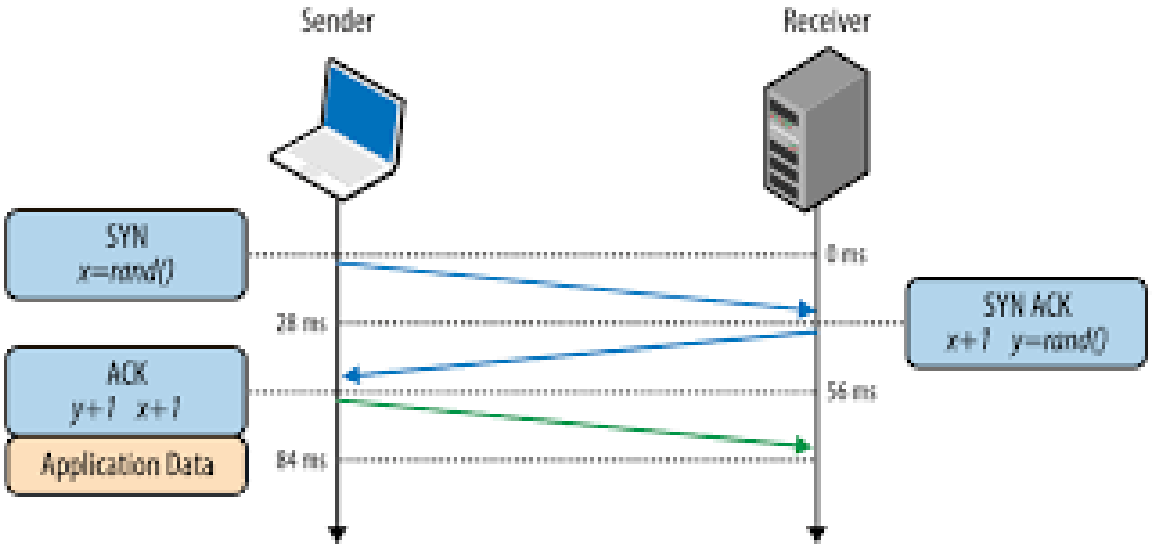
- ◇ ARP ( Adress Resolution Protocol) - Adressumsetzung zwischen IP- und Gerteadressen (MAC)

- ◇ 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.

Die Anwendungsprotokolle sind grundstzlich fr beide Arten dieselben.

◇ DNS - Domain Name Service

◇ Internet Control Message Protocol (ICMP)

◇ Telnet

◇ File Transfer Protocol (FTP, TFTP)

◇ HTTP

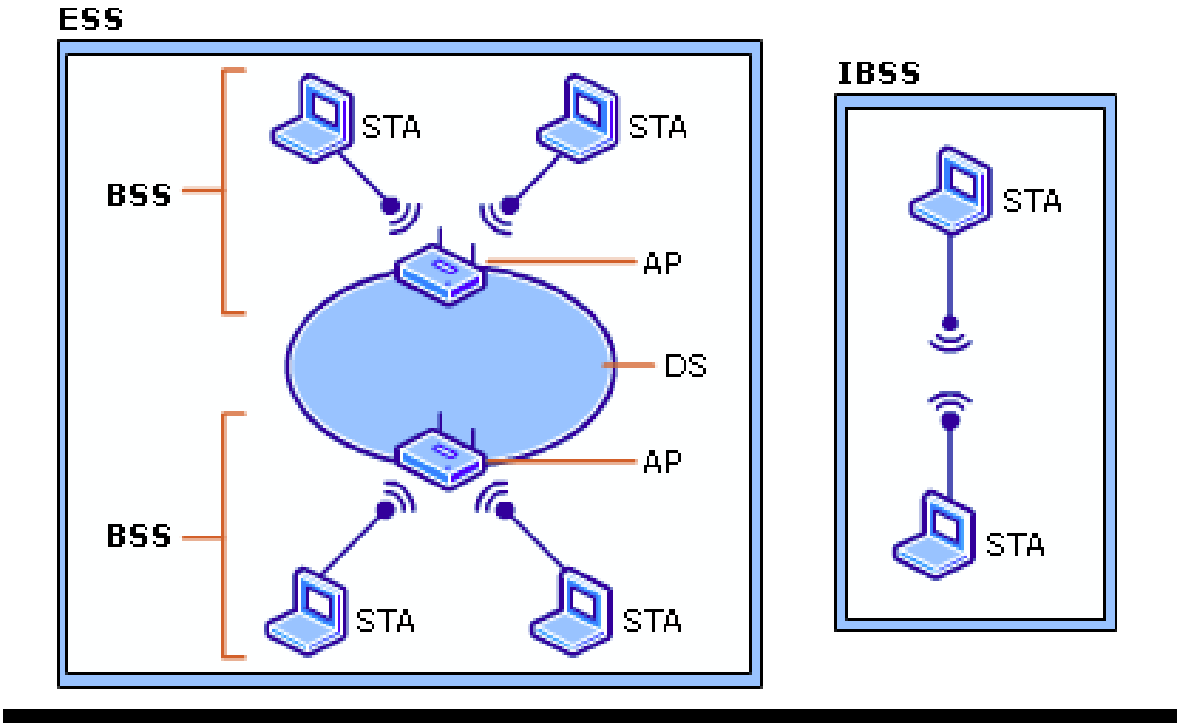
# 6 Die 802.11 Architektur

Das IEEE 802.11 Protokoll ist ein Netzwerkzugangs-Protokoll welches die Konnektivitt zwischen verschiedenen WLan-Gerten und Brcken sowie strukturierten, verkabelten Infrastrukturen sicherstellt. Man ermglicht den mobilen Zugriff der User in jeder Rumlichkeit der betreffenden Gebude - egal wo er oder sie sich gerade befinden. Auch verhelfen "Hot Spots" eine Erweiterung dieses Netzwerkes.

## 6.1 Logische Architektur

Die logische Architektur des 802.11 besteht aus mehreren Komponenten:

◇ (Wireless) Station (STA)
Die Station ermglicht die verbindungslose Konnektivitt zum Netzwerk. Dies kann sowohl Server als auch Gert eines Klienten sein.
◇ (Wireless) Access Point (WAP oder AP)
Der Access Point fungiert als Brcke zwischen STAs und dem gesamten Internet. Es ist quasi der jeweilige Router.
◇ Independent Basic Service Set (IBSS) Das IBSS besteht aus mindestens 2 STAs ohne Distribution System. Auch 'Ad Hoc Wireless Network'. Verbinden sich beispielsweise 2 Gerte mittels Server-Client-Configuration, so verbindet sich Gert A mit Gert B, ohne Zwischenstation.
◇ Basic Service Set (BSS) Das BSS besteht aus einem einzelnem AP, welcher mehrere STAs sttzt. Alle STAs innerhalb eines BSS kommunizieren mittels AP und der AP berbrckt die Verbindung zum DB und damit dem gesamten, gebudeinternen Netzwerk.
◇ Extended Service Set (ESS) Ein ESS ist die Gesamtheit eines kompletten Subnetworks. Es ist beispielsweise ein Set aus 2 oder mehreren APs im selben Netzwerk, an welchen die STAs hngen.
◇ Distribution System (DS) Das DS ist die Gesamtheit aller AP. Es erlaubt das Roaming der STAs zwischen APs.



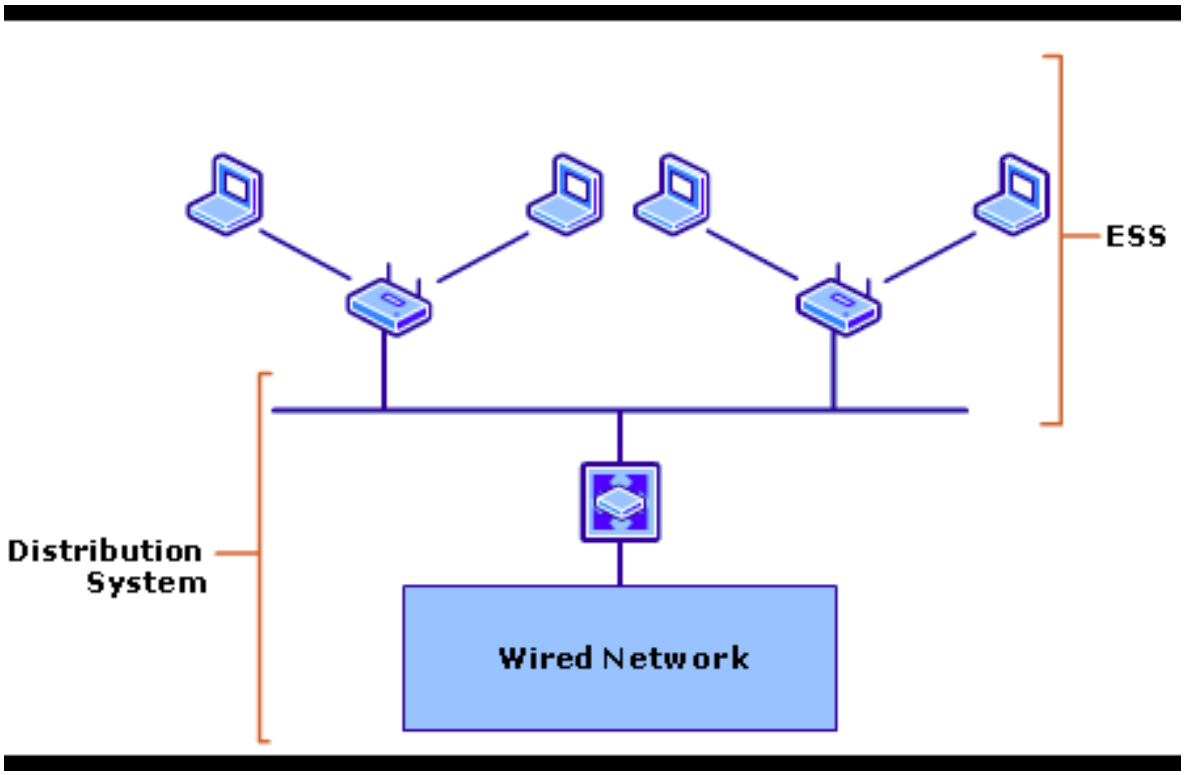

*Graphical Layout of the 802.11 Architecture*[1]

Es gilt dabei zu beachten: Die Operationsmodi sind bei IBSS und ESS grundstzlich unterschiedlich.

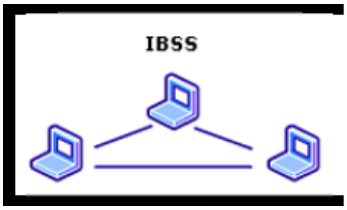
### 6.1.1 802.11 Infrastrukturmodus

Der Infrastrukturmodus beschreibt den Operationsmodus innerhalb des gesamten Subnets. Prinzipiell gibt es mindestens einen AP und einen STA, kurzum ein ESS. Der weitere Verbindungslauf wird entsprechend aufgerufener Ressource via AP und/oder DS geregelt.

[1]Source: https://i-technet.sec.s-msft.com/dynimg/IC196384.gif




### 6.1.2 802.11 Ad Hoc Modus




Der Ad Hoc Modus beschreibt die direkte Verbindung mehrerer STAs ohne Zwischenstationen. Es verluft also ein direkter Datenverkehr zwischen mehreren Medien.

## 6.2 Protokolle

- ◇ 802.11: IEEE Norm; Basiert auf OSI-Model und spezifiziert Datalink(=MAC) und Physical layer.
- ◇ 802.1X: IEEE Norm; definiert Port-basierte Zugangskontrolle
- ◇ EAPOL: Extensible Authentication protocol over Lan: Point-to-Point-Protocol fr LANs
- ◇ WEP: Wired Equivalent Privacy: Dekryption zwischen WLan Nodes.
- ◇ WPA: Wi-Fi Protected Access: Data Enkryption & Netzwerkauthentifizierung

### 6.3 Beispiel: Strukturierung des Heimnetzwerkes


## 7 Streaming

Grob gesagt meint Streaming das Abspielen von Inhalten ber das Internet bzw. ber ein Netzwerk. Hierbei werden whrend dem streamen fortlaufend Datenpakete bertragen und direkt verarbeitet. Wrde man zum Beispiel ein Video auf Youtube ansehen, wird die Videodatei in kleinen Teilen auf das Gert heruntergeladen und direkt abgespielt. Im Gegensatz zu einem herkmmlichen Download werden die Daten aber nicht dauerhaft gespeichert, sonden direkt wieder verworfen.

Das Streaming wird jedoch dann Problematisch, wenn die Internetverbindung zu langsam ist, da in diesem Fall das Video nhmlich stark stocken wrde. Der Grund dafr ist der, dass die nchsten Daten noch nicht heruntergeladen sind. Ein Stream kann natrlich auch von einem GErt auf ein anderes stattfinden. Beispielsweise knnen Medien von einem IPhone auf ein Apple TV gestreamt werden.

*Beispiele:*

1. *Netflix:*

Die Inhalte, also Serien und Filme, liegen auf den Netflix-Servern. Wird nun ein Video gestartet, so wird die Datei ber ihre Internetverbindung auf ihre nPC gestreamt. Um das Video ohne Probleme anzusehen, ist eine Internetverbindung mit einer Geschwindigkeit von mindestens 6000 Mbits pro Sekunde ntig.

2. *Amazon Prime Video:*

   Zum Streamen von Inhalten nutzt Amazon Video die Microsoft-Silverlight-Technologie und die Infrastruktur von Akamai. Zur Wiedergabe von HD-Inhalten wird eine Internetverbindung mit mindestens 3.5 MBits/s sowie eine HDCP-Untersttzung aller Gerte bentigt. Die Wiedergabe von SD-Inhalten bentigt jedoch mindestens eine 900 kBit/s schnelle Verbindung.