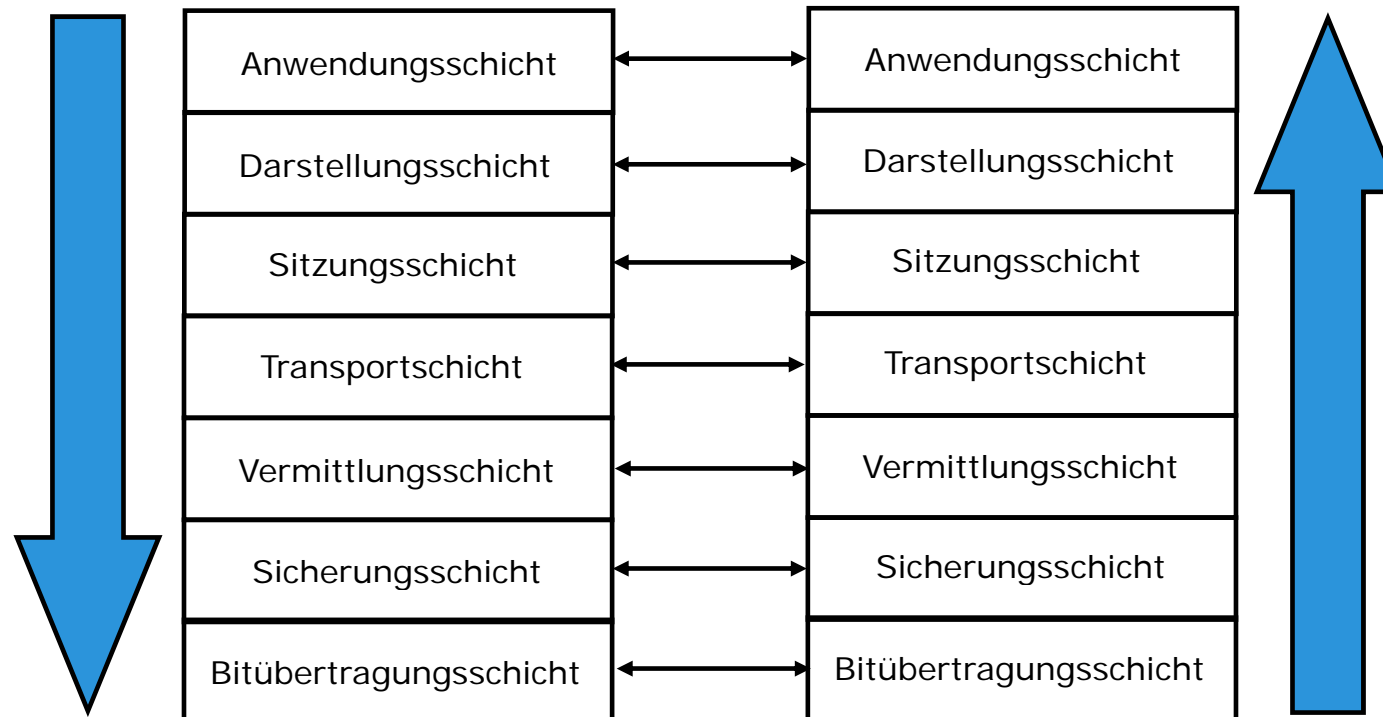


II. Kommunikationssysteme

Kapitel 2: ISO/OSI-Referenzmodell

- ISO/OSI-Referenzmodell

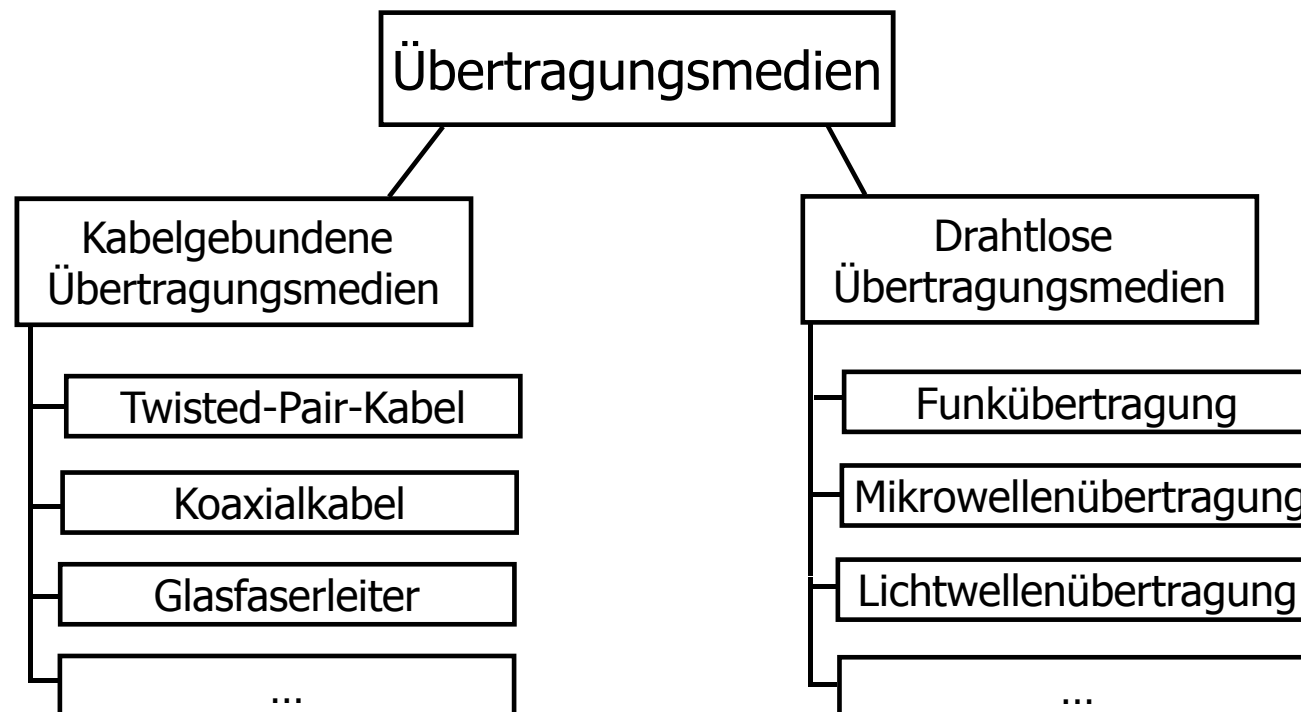


- 1. Bitübertragungsschicht
- 2. Sicherungsschicht
- 3. Vermittlungsschicht
- 4. Transportschicht
- 5. Sitzungsschicht
- 6. Darstellungsschicht
- 7. Anwendungsschicht

- Die Aufgabe der Bitübertragungsschicht ist die Beförderung **reiner Bitströme** von einem Knoten zum anderen Knoten.
- Für die eigentliche Übertragung können **verschiedene physikalische Medien** eingesetzt werden.
- Jedes Medium hat in Bezug auf **Bandbreite, Verzögerung, Kosten sowie Installationsfreundlichkeit und Wartung** seine eigenen Stärken und Schwächen.

- Durch die Bitübertragungsschicht werden u.a. die folgenden Festlegungen getroffen:
 - o Wie sind **Stecker** definiert?
 - o Wie sind **Pins** belegt?
 - o Welche **verschiedenen Übertragungsmedien** existieren?
(kabelgebunden oder drahtlos)
 - o Wann ist der **Einsatz** welches Übertragungsmedium sinnvoll?

- Die Auswahl verschiedener Übertragungsmedien kann wie folgt unterteilt werden.



Quelle: Tanenbaum (2006), S.110-130

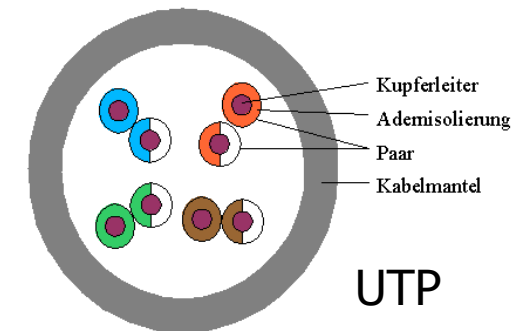
- Twisted Pair (verdrillte Leitungen)
 - ist das bekannteste und am häufigsten eingesetzte Kabel.
 - ein Twisted Pair Kabel besteht aus zwei isolierten Kupferdrähten (1mm dick)

 - Haupteinsatzgebiet:
 - o Telefonleitungen (ISDN)
 - o Verkabelung in Hochhäusern

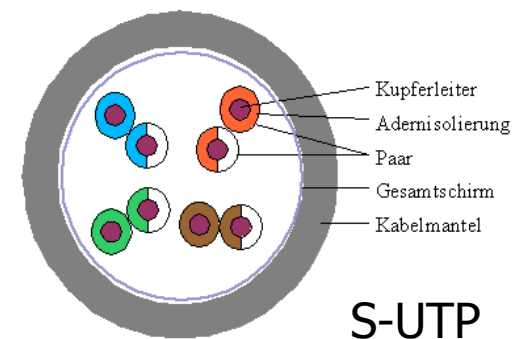
 - Es werden vier Varianten unterschieden:
 - o UTP (Unshielded Twisted Pair)
 - o STP (Shielded Twisted Pair)
 - o S/STP (Screened Shielded Twisted Pair)
 - o S/UTP (Screened Unshielded Twisted Pair)

- Unterschiede der Arten von Twisted-Pair-Kabeln:

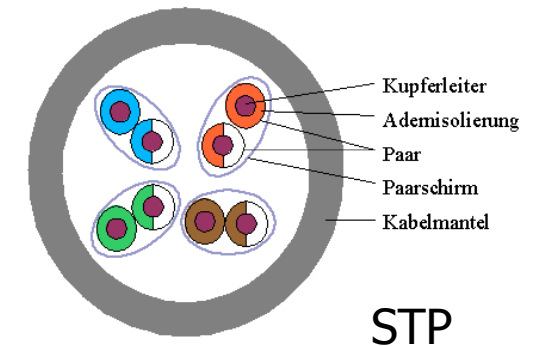
- o Unshielded Twisted Pair (UTP): Kabel, bei dem zwei Adern jeweils miteinander verdrillt sind.



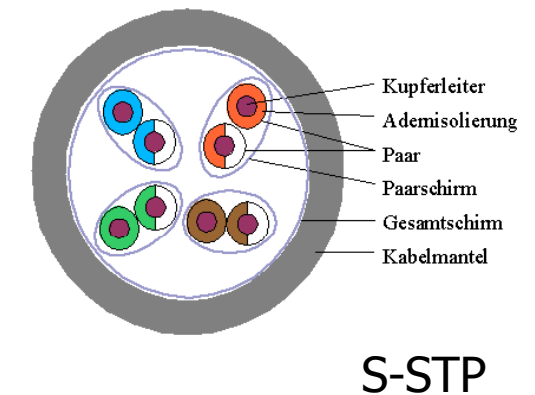
- o Screened UTP (S-UTP): wie UTP, aber es existiert ein Gesamtschirm für das Gesamtkabel.



- o Shielded Twisted Pair (STP): wie UTP, aber die Adernpaare sind zusätzlich gegeneinander abgeschirmt.



- o Screened STP (S-STP): Kombination aus STP und S-UTP.



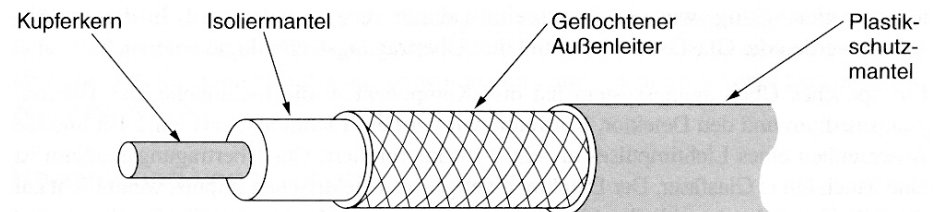
■ Koaxialkabel

- Besser abgeschirmt als ein Twisted-Pair-Kabel
- Gut geeignet für sehr große Entfernungen und hohe Geschwindigkeiten
- Besteht aus einem starren Kupferdraht als Kern, ummantelt mit einem Isoliermaterial. Der Isolator wird wiederum von einem zylindrischen Leiter umschlossen
- Bekannt als klassisches Fernsehantennenkabel

- Haupteinsatzgebiet:

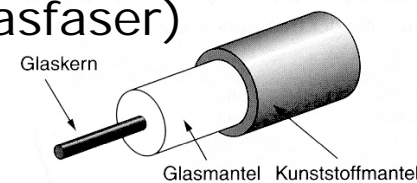
- o Digitale Übertragungen
- o Kabelfernsehen

- o War in den 80ern und Anfang der 90er Jahre das Standardkabel für Token-Ring-Netzwerke

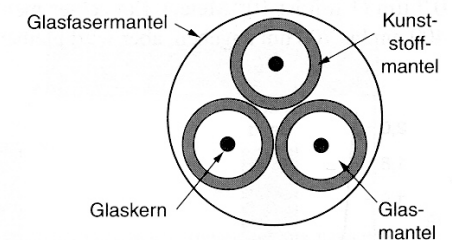


■ Glasfaserleiter

- Ein Glasfaserkabel besteht aus einem Glaskern (etwa die Stärke eines menschlichen Haars).
- Der Glaskern ist mit einem Glasmantel verkleidet.
- Darüber liegt ein dünner Kunststoffmantel zum Schutz des Glasmantels.
- Glasfaserleiter sind in Bündel gruppiert und werden von einem Außenmantel umgeben.
- Extrem hohe Datenraten vs. unflexible Kabelverlegung
- Haupteinsatzgebiet:
 - o Überseekabel für Datenkommunikation
 - o Netzwerke (Ethernet über Glasfaser)



(a)

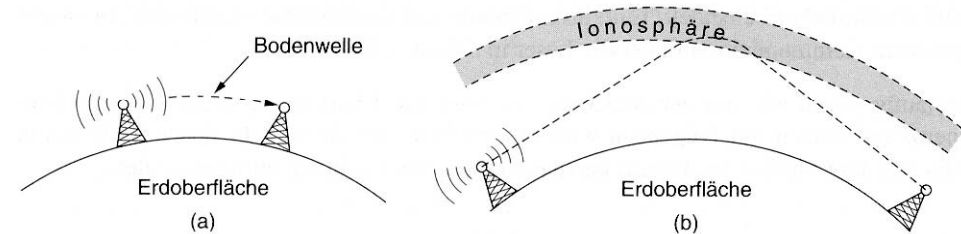


(b)

Quelle: Tanenbaum (2006), S.116

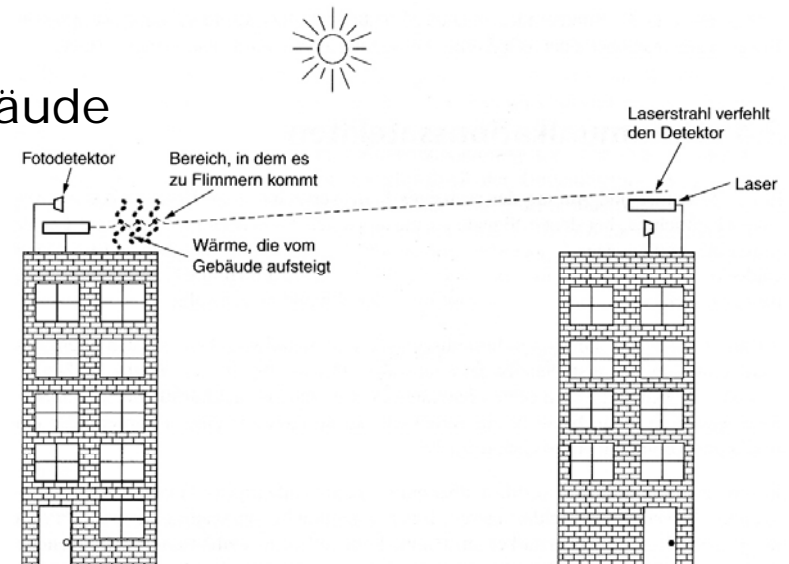
■ Funkübertragung

- Leicht zu realisieren
- Legen große Entfernungen zurück
- Dringen mühelos in Gebäude ein
- Sind rundstrahlend, d.h. eine Ausrichtung von Sender und Empfänger entfällt.
- Sind sehr störanfällig
 - o Beispiel: Cadillac Antiblockiersystem vs. Funksystem der Polizei aus Ohio.
- Funkübertragungen sind weltweit stark reguliert.
- Haupteinsatzgebiet:
 - o Bluetooth, WLAN, WiMAX, GSM, UMTS



■ Lichtwellenübertragung

- Für eine Lichtwellenübertragung wird ein Detektor und ein Laser benötigt, die beispielsweise auf dem Dach von Gebäuden zu installieren sind
- Die Lichtwellenübertragung ermöglicht eine hohe Bandbreite und erzeugt sehr geringe Kosten
- Regen und Nebel unterbrechen eine Lichtwellenübertragung
- Haupteinsatzgebiet:
 - o Verbindung von LANs zweier Gebäude



Quelle: Tanenbaum (2006), S.129

- 1. Bitübertragungsschicht
- 2. Sicherungsschicht
- 3. Vermittlungsschicht
- 4. Transportschicht
- 5. Sitzungsschicht
- 6. Darstellungsschicht
- 7. Anwendungsschicht

- Die Sicherungsschicht umfasst **Algorithmen, um eine effiziente und zuverlässige Kommunikation** zwischen zwei benachbarten Knoten sicherzustellen.
- Das Hauptziel der Sicherungsschicht besteht in der **reibungslosen Übertragung von Bits** von der Quelle zum Ziel, so dass eine von der Vermittlungsschicht initialisierte Übertragung an die gegenüber liegende Vermittlungsschicht übertragen werden kann.
- Die Sicherungsschicht stellt der Vermittlungsschicht Dienste zur reibungslosen Übertragung zur Verfügung.

Quelle: Tanenbaum (2006), S.212

- Folgende Dienste bietet die Sicherungsschicht an:
 - Bietet Möglichkeiten zur **Fehlerbehandlung**
 - Ermöglicht eine **Flusskontrolle**
 - **Mehrfachzugriff**

- Man unterscheidet zwei grundlegende Strategien:
 - Mit jedem Datenblock genug redundante Informationen senden, so dass der Empfänger daraus ableiten kann, wie die zu übertragenden Daten ausgesehen haben müssen
 - **Fehlerkorrekturcodes** werden bei unzuverlässigen Verbindungen z.B. Funk eingesetzt um eine wiederholte Übertragung möglichst zu vermeiden
 - Nur so viel Redundanz senden, dass der Empfänger einen Fehler feststellen kann, aber nicht die Art des Fehlers
 - **Fehlererkennungscode**s werden bei sehr zuverlässigen Verbindungen z.B. Glasfaser eingesetzt da hier eine wiederholte Sendung nur selten vorkommt und daher der Overhead für redundante Informationen eingespart werden kann.

- Anwendungsgebiete:
 - o Bei Funkverbindungen finden auf Grund von Störungen oft Übertragungsfehler statt. Aus diesem Grund sind Fehlerkorrekturcodes besser geeignet, um Fehler direkt zu erkennen und zu beseitigen.
 - o Glasfaserverbindungen sind relativ zuverlässig, somit bieten sich Fehlererkennungscode an, da ein selten verlorenes Datenpaket schnell erneut gesendet werden kann.

- Der Hamming-Abstand DC eines Codes C ist definiert als die kleinste Anzahl von Positionen, an denen sich zwei beliebige, verschiedene Codewörter unterscheiden. Nur Codes mit $DC > 0$ sind sinnvoll, weil sich erst dann zwei Codewörter überhaupt unterscheiden:
 - $DC = 1$: Keine Fehlererkennung und keine Fehlerkorrektur möglich.
 - $DC = 2$: Fehler in einer Position sind erkennbar, aber nicht korrigierbar.
 - $DC > 3$: Fehler in zwei Positionen können erkannt, Fehler in einer Position können (nach der Wahrscheinlichkeit) korrigiert werden.
- Fehlererkennungscode: Cyclic Redundancy Check Code (CRC-Code), ...

Quelle: Eicker (2006a), Tannenbaum S.222

- Beispiel zum Hamming-Abstand $DC = 1$
 - o Ausgangspunkt:
 - Definiert ist eine Menge von Codewörtern eines Codes X
 - Codewort A = (repräsentiert durch) 0100
 - Codewort B = 0101
 - Codewort C = 0110

 - o Wie groß ist der Hamming-Abstand des Codes X ?
 - Der Hamming-Abstand des Codes X ist 1, da zwei beliebige Codewörter sich mindestens in einer Position von einander unterscheiden.
 - Hamming-Abstand zwischen Codewort A und B = 1
 - Hamming-Abstand zwischen Codewort A und C = 1
 - Hamming-Abstand zwischen Codewort B und C = 2

 - o Konsequenz bei der Anwendung (Beispiel)
 - Bei der Übertragung von Codewort A (0100) findet ein Übertragungsfehler statt und es wird 0110 übertragen was dem Codewort C (0110) entspricht. Der Fehler kann nicht erkannt werden, da das Codewort C ein gültiges Codewort des Codes X ist.

- Beispiel zum Hamming-Abstand $DC = 2$
 - o Ausgangspunkt:
 - Definiert ist eine Menge von Codewörtern eines Codes Y
 - Codewort A = (repräsentiert durch) 0001
 - Codewort B = 0010
 - Codewort C = 0111

 - o Wie groß ist der Hamming-Abstand des Codes Y ?
 - Der Hamming-Abstand des Codes Y ist 2, da zwei beliebige Codewörter sich mindestens in zwei Positionen von einander unterscheiden.
 - Hamming-Abstand zwischen Codewort A und B = 2
 - Hamming-Abstand zwischen Codewort A und C = 2
 - Hamming-Abstand zwischen Codewort B und C = 2

 - o Konsequenz bei der Anwendung (Beispiel)
 - Bei der Übertragung von Codewort A (0001) findet ein Übertragungsfehler statt und 0011 wird übertragen. Der Fehler kann erkannt werden, da ein Codewort mit der Darstellung 0011 nicht Bestandteil des Codes Y ist. Eine Korrektur ist nicht möglich, da dieses Codewort entweder Codewort A oder B gewesen sein könnte.

- Beispiel zum Hamming-Abstand $DC = 3$
 - o Ausgangspunkt:
 - Definiert ist eine Menge von Codewörtern eines Codes Z
 - Codewort A = (repräsentiert durch) 00010010
 - Codewort B = 00011001
 - Codewort C = 00001110
 - o Wie groß ist der Hamming-Abstand des Codes Z ?
 - Der Hamming-Abstand des Codes Z ist 3, da zwei beliebige Codewörter sich mindestens in drei Positionen von einander unterscheiden.
 - Hamming-Abstand zwischen Codewort A und B = 3
 - Hamming-Abstand zwischen Codewort A und C = 3
 - Hamming-Abstand zwischen Codewort B und C = 4

o Konsequenz bei der Anwendung (Beispiel)

- Bei der Übertragung von Codewort A (00010010) findet ein Übertragungsfehler statt und 00010110 wird übertragen. Der Fehler kann erkannt und korrigiert werden.
- Unterschied zwischen Codewort A (00010010) und 00010110 = 1
- Unterschied zwischen Codewort B (00011001) und 00010110 = 4
- Unterschied zwischen Codewort C (00001110) und 00010110 = 2
- Bei einem Übertragungsfehler in einer Position ist es wahrscheinlich, dass das ursprünglich zu übertragende Codewort, Codewort A (00010010) lautete. Der Fehler wurde erkannt und korrigiert.

■ Definition

- Bei der Datenkommunikation in einem Netzwerk kann es zum „Überlaufen“ des Empfängers kommen, wenn ein Knoten von einem oder mehreren Knoten mehr Datenpakete zugesendet bekommt, als er zu verarbeiten in der Lage ist. Um dieses zu verhindern, gibt es Maßnahmen zur Flusskontrolle.
- Unterschieden werden drei wesentliche Flusssteuerungstechniken.
 - **Isarithmische Flusskontrolle**
 - **Flusskontrolle auf Retransmissions-Basis**
 - Schiebefensterprotokoll

- Isarithmische Flusskontrolle
 - Die kommunizierenden Stationen vereinbaren, dass sie eine festzulegende Anzahl (**Credits** genannt) von Paketen senden dürfen, ohne dass sie über deren Empfang vom Kommunikationspartner eine Bestätigung erhalten müssen.
 - Die Anzahl der Credits werden bei jeder Übertragung heruntergezählt und bei jeder Bestätigung um einen in der Bestätigung angegebenen Wert erhöht (wobei dieser Wert nicht die zu Beginn vereinbarte Anzahl überschreiten darf).

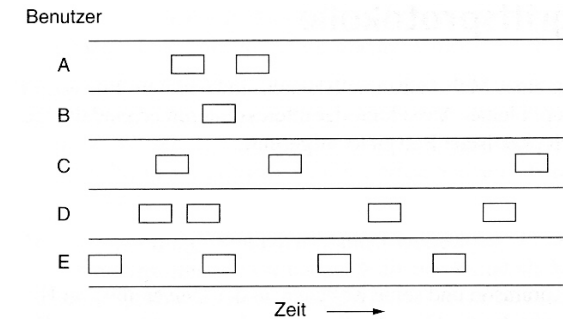
- Flusskontrolle auf Retransmissions-Basis
 - Dieses Verfahren arbeitet mit der „Brechstangen-Technik“:
 - o Kann ein Empfänger keine Nachrichten mehr aufnehmen, so weist er alle ankommenden Pakete ab.
 - o Die Sender bemerken dies durch das Ausbleiben von Empfangsbestätigungen.
 - o Sie reagieren mit der Herabsetzung der Sendegeschwindigkeit und warten auf die „Stauauflösung“.

- Die Kanalzuordnung beschäftigt sich mit der von mehreren Parteien gleichzeitigen Verwendung eines Kommunikationskanals.
 - Beispiel: Telefon
 - o Zwei Telefone sind mit einem Kabel verbunden.
 - o Die Personen am Ende der Leitung können problemlos ein Gespräch führen.
 - o Eine dritte Person schaltet sich dazu.
 - o Eine Abstimmung ist notwendig, wann wer mit wem telefonieren kann (Klingel-Ton, Besetzt-Zeichen).
 - Um dieses Verhalten im Intra- oder Internet zu ermöglichen, existieren verschiedene Verfahren zur Kollisionserkennung und -vermeidung.

- Die folgenden Verfahren seien beispielhaft genannt:
 - ALOHA-Prinzip
 - CSMA (**C**arrier **S**ense **M**ultiple **A**ccess)
 - CSMA-CD (**C**arrier **S**ense **M**ultiple **A**ccess – **C**ollision **D**etection)

- Grundidee:

- Jeder Teilnehmer kann jederzeit seine Datenpakete senden.
- Kollisionen sind unvermeidbar und werden erkannt.
- Bei einer Kollision wartet die sendende Station eine zufällige Zeitspanne ab und überträgt das Datenpaket erneut.



- CSMA steht für **C**arrier **S**ense **M**ultiple **A**ccess
 - Unter Carrier Sense ist zu verstehen, dass ein Kommunikationskanal abgehört wird, bevor die eigene Übertragung veranlasst wird.
 - Ist das Medium für eine bestimmte Zeitspanne nicht belegt, wird es als frei betrachtet und eine Transmission wird begonnen.
 - Kollisionen sind nicht erkennbar.
 - Das CSMA unterteilt sich, zum Zweck der Kollisionsbehandlung, in 2 weitere Verfahren:
 - **CSMA-CD (Collision Detection)**
 - CSMA-CA (Collision Avoidance)

- CSMA-CD steht für **C**arrier **S**ense **M**ultiple **A**ccess – **C**ollision **D**etection
 - Erweiterung gegenüber dem CSMA:
 - o Kollisionen werden erkannt.
 - o Bei Kollisionsauftreten wird der Abbruch der Kommunikation veranlasst.
 - o Jede an einer Kollision beteiligte Station wartet eine zufällige Zeitspanne ab, vergewissert sich, dass der Kommunikationskanal nicht verwendet wird, und startet eine erneute Übertragung.

- 1. Bitübertragungsschicht
- 2. Sicherungsschicht
- 3. Vermittlungsschicht
- 4. Transportschicht
- 5. Sitzungsschicht
- 6. Darstellungsschicht
- 7. Anwendungsschicht

- Die Vermittlungsschicht hat die Aufgabe, **Pakete von der Quelle zum Ziel zu übertragen**. Dazu kann auch das Durchqueren von Teilstrecken zwischen auf dem Weg liegenden Routern gehören.
 - Die Hauptaufgabe dieser Schicht besteht im **Routing**.
 - Darüber hinaus ist das Internet-Protokoll (IP) ein Protokoll der Vermittlungsschicht.

- Unter Routing versteht man die Aufgabe, dafür zu sorgen, dass ein Paket von der Quelle zum Ziel „bestmöglich“ weitergeleitet wird.

- Bestmöglich kann bedeuten:
 - geringe Transportkosten
 - schnellstmöglicher Transport
 - abhörsichere Übertragung
 - verfälschungssichere Übertragung
 - optimale Netzlast
 - eine (gewichtete) Kombination der o.g. Kriterien
 - etc.

- Es existieren zahlreiche Routingalgorithmen
 - Optimalitätsprinzip
 - **Dijkstra Algorithmus**
 - Ford Algorithmus
 - Distance Vector Routing
 - Link State Routing
 - Hierarchisches Routing
 - Broadcast Routing
 - Multicast Routing
 - ...

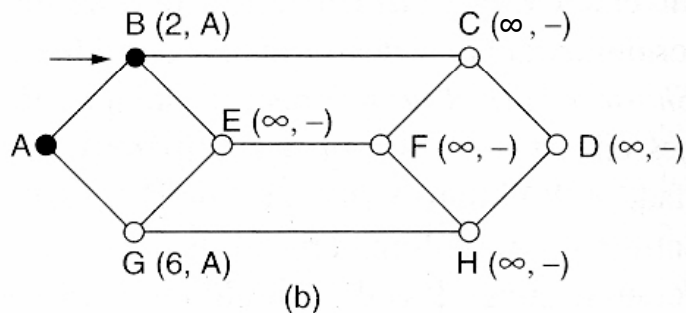
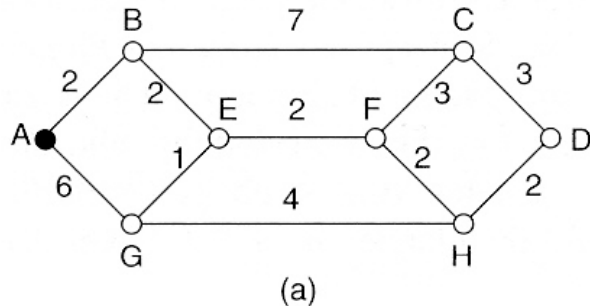
- Der Algorithmus wurde 1959 von Dijkstra entwickelt.
- Er dient zur Berechnung des kürzesten Pfades zwischen zwei Knoten eines Graphen.
- Bei diesem Konzept wird ein Graph des Teilnetzes erstellt, wobei jeder **Knoten** im Graphen einen **Router** und jede **Kante** eine **Übertragungsleitung** darstellt.
- Um einen Weg zwischen einem bestimmten Router-Paar auszuwählen, berechnet der Algorithmus anhand des Graphen den kürzesten Weg.
- Die **Beschriftung der Kanten** können Entfernung, Bandbreite, Durchschnittsverkehr, Übertragungskosten, mittlere Warteschlangelänge, gemessene Übertragungszeit oder andere Faktoren darstellen.
- Die **Gewichtung der Kanten** hat Einfluss auf den kürzesten Weg.

Quelle: Tanenbaum (2006), S.391-393

- Beispiel zum Dijkstra Algorithmus
 - Festlegungen:
 - o Gesucht ist der kürzeste Weg von A nach D.
 - o Jeder Knoten stellt einen Router da.
 - o Jedes Kantengewicht stellt die Entfernung zwischen zwei Routern dar.
 - o Zu Beginn ist der Pfad unbekannt, so dass alle Knoten die Bezeichnung „unendlich“ tragen.
 - o Je weiter der Algorithmus fortschreitet und Pfade gefunden werden, desto mehr ändert bzw. vervollständigt sich die Beschriftung.
 - o Eine Beschriftung kann provisorisch oder permanent sein.
 - o Zu Beginn sind alle Beschriftungen provisorisch.
 - o Wird festgelegt, dass eine Beschriftung den kürzesten Weg von der Quelle zum Ziel angibt, wird sie permanent gesetzt und danach nie mehr geändert.

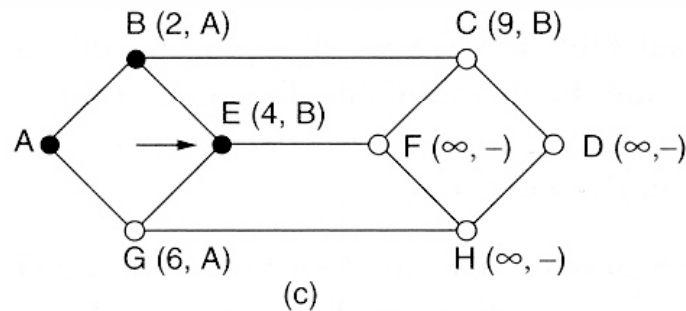
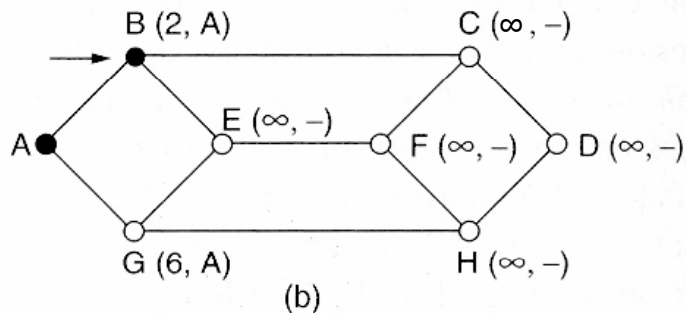
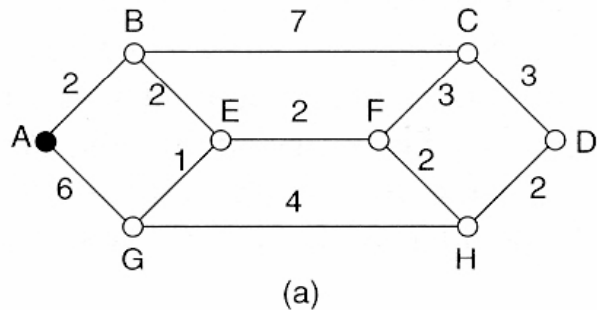
Quelle: Tanenbaum (2006), S.391-393

Routing – Dijkstra Algorithmus



- Es wird der kürzeste Weg von A nach D gesucht.
- Startknoten ist A.
- A ist Arbeitsknoten.
- Er wird als permanent markiert.
- Von A aus wird jeder benachbarte Knoten untersucht und mit seiner Entfernung zu A beschriftet.
- Jede Beschriftung enthält ebenfalls den Knoten von dem gemessen wurde, so dass der endgültige Pfad später rekonstruiert werden kann.
- Nach der Untersuchung jedes Nachbarknotens von A werden alle vorläufigen beschrifteten Knoten im Graphen untersucht.
- Die Knoten mit der jeweils kleinsten Beschriftung werden als permanent markiert.
- Neuer Start- und Arbeitsknoten ist jetzt Knoten B.

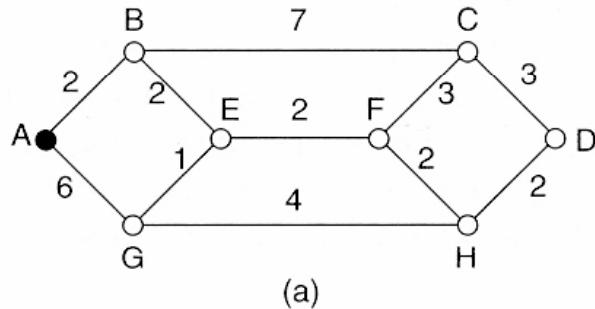
Routing – Dijkstra Algorithmus



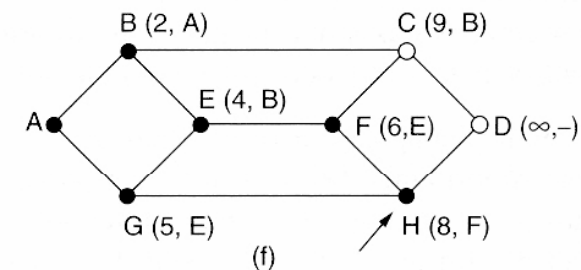
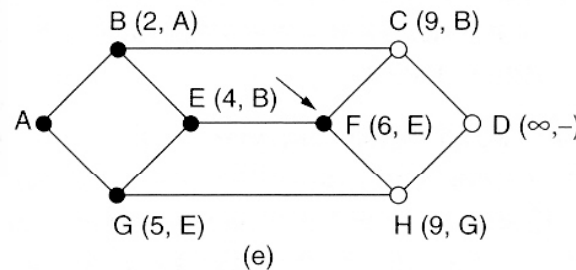
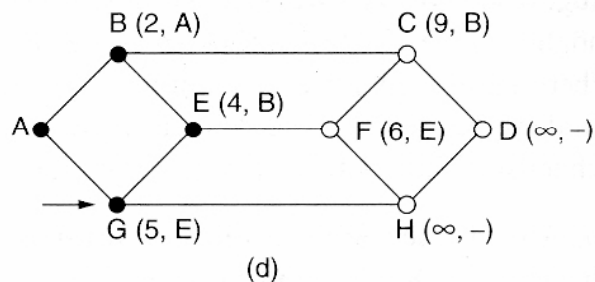
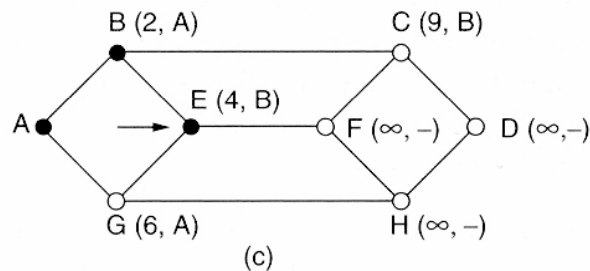
- Von B aus wird erneut jeder benachbarte Knoten untersucht.
- Sollte die Summe der Beschriftungen auf B und der Entfernung von B zu dem gerade untersuchten Knoten kleiner sein als die bisherige Beschriftung dieses Knotens, liegt ein kürzerer Pfad vor, also wird die Beschriftung geändert.
- In unserem Fall wird Knoten E neuer Start- und Arbeitsknoten.

Quelle: Tanenbaum (2006), S.391-393

Routing – Dijkstra Algorithmus



- Nachdem alle Nachbarn des Arbeitsknoten untersucht und die vollständigen Beschriftungen – soweit es möglich war – geändert wurden, wird der gesamte Graph nach dem vorläufig beschrifteten Knoten mit dem kleinsten Wert abgesucht.
- Der Knoten wird als permanent markiert und in der nächsten Runde als Arbeitsknoten deklariert.



Quelle: Tanenbaum (2006), S.391-393

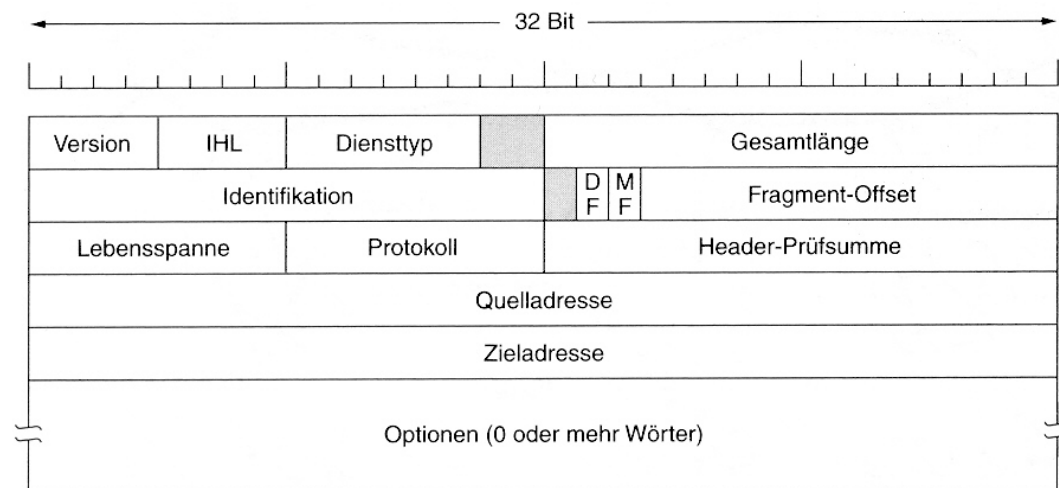
- Die Aufgabe des Internet-Protokolls (IP) besteht darin, Datenpakete von einem Sender über mehrere Netze hinweg zu einem Empfänger zu transportieren.
- Die Übertragung ist
 - paketorientiert,
 - verbindungslos und
 - nicht garantiert.
- IP ist spezifiziert im RFC 791.

- Begriffe:
 - **Paket:** Ein Paket ist ein Datenblock (eine festgelegte Anzahl von Bits) zusammen mit den Informationen, die notwendig sind, um diese dem Empfänger zuzustellen (Beispiel Postpaket).
 - **Datagramm:** Ein Datagramm ist das Paketformat, das durch das IP definiert ist. Es legt fest, wie die Bits angeordnet sein müssen, um als wohlgeformtes IP-Paket erkannt zu werden.
- Teilaufgaben des IP:
 - Übermittlung von Daten von der Transport- zur Vermittlungsschicht
 - Routing von Datagrammen durchs Netz
 - Fragmentierung und Zusammensetzung von Datagrammen
 - Definition der Adressierung von Hosts

■ Aufbau

- Ein IP-Header besteht aus folgenden Teilen:

- o Version
- o IHL (Headerlänge)
- o Diensttyp
- o **Gesamtlänge**
- o Identifikation
- o Flags (DF, MF)
- o Fragment-Offset
- o **Lebensspanne**
- o Protokoll
- o Header-Prüfsumme
- o **Quelladresse und Zieladresse**
- o Optionen



- Gesamtlänge
 - Die Gesamtlänge beinhaltet das komplette Datagramm: Header und Daten.

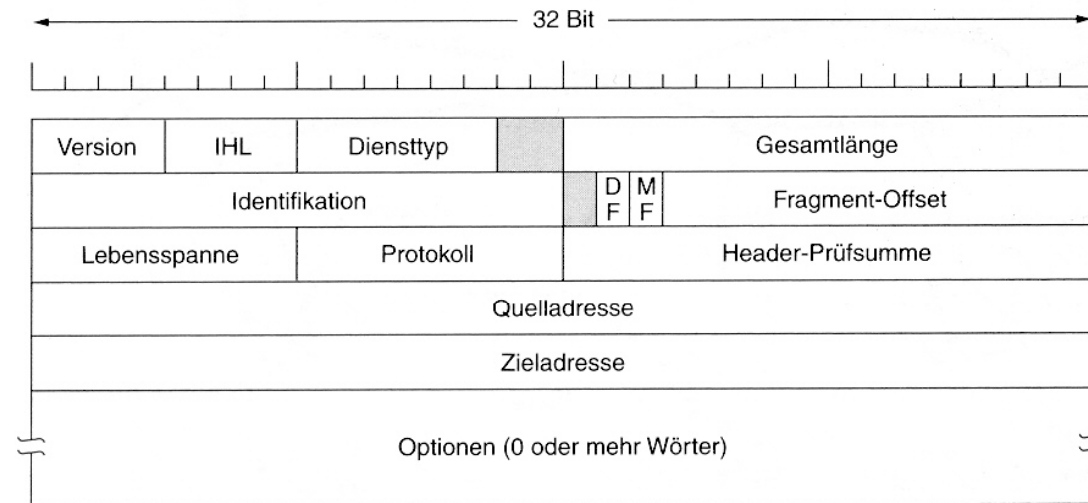
- Lebensspanne
 - Bestimmt die Lebensdauer eines IP-Paketes.
 - Die maximale Lebensdauer beträgt 255 Sekunden.

- Quell- und Zieladresse
 - In diesem Feld werden die 32 Bit langen Internetadressen eingetragen.

- IP-Adressierung

- Jeder Host und Router im Internet hat eine IP-Adresse.
- Eine IP-Adresse ist eindeutig. Kein Rechner hat die gleiche IP-Adresse wie ein anderer Rechner (gilt für öffentliche IP-Adressen).
- Die Vergabe der IP-Adressen wird zentral organisiert durch:
 - o IANA (Internet Assigned Numbers Authority)
 - o ICANN (Internet Cooperation for Assigned Numbers and Names)

- Die Grundlage der Vergaben von IP-Adressen bildet der RFC 2050.



- Alle IP-Adressen (in IPv4) sind 32 Bit lang und werden in den Feldern Quelladresse und Zieladresse verwendet.
 - Beispiel: 140.212.54.123 wird in Binärdarstellung zu
 - 10001100-11010100-00110110-01111011

Adressklasse	Erstes Byte	Bytes für die Netzadresse	Bytes für die Hostadresse	Adressformat*	Anzahl Hosts
Klasse A	1-126	1	3	N.H.H.H	2^{24} (~16 Mio.)
Klasse B	128-191	2	2	N.N.H.H	2^{16} (~64.000)
Klasse C	192-223	3	1	N.N.N.H	254
Klasse D	224-239	Multicast-Adressen			
Klasse E	240-254	Experimentelle Adressen bzw. für zukünftige Nutzung reserviert			

*N steht für einen Teil der Netzadresse, H für einen Teil der Hostadresse.

- Es werden verschiedene Klassen von IP-Adressräumen unterschieden
 - o Klasse A
 - Das erste Byte hat einen Wert kleiner als 127
 - Das erste Byte ist die Netzwerknummer, die letzten drei Bytes identifizieren den Host.
 - Es gibt demnach 126 Klasse A-Netze mit bis zu 16 Millionen Hosts
 - Adressbereich: 0.0.0.0 bis 126.255.255.255
 - 127.0.0.0 bis 127.255.255.255 reserviert für loopback

- Klasse B
 - o Das erste Byte hat einen Wert im Bereich von 128 bis 191.
 - o Die ersten zwei Bytes identifizieren das Netzwerk, die letzten zwei Bytes den Host.
 - o Es gibt demnach 16.382 Klasse B-Netze mit bis zu 64.000 Hosts.
 - o Adressbereich: 128.0.0.0 bis 191.255.255.255
- Klasse C
 - o Das erste Byte hat einen Wert im Bereich von 192 bis 223.
 - o Die ersten drei Bytes identifizieren das Netzwerk, das letzte Byte den Host.
 - o Es gibt demnach 2 Millionen Klasse C-Netze mit bis zu 254 Hosts.
 - o Adressbereich: 192.0.0.0 bis 223.255.255.255
- Klasse D – Multicast-Adressen
 - o Adressbereich: 224.0.0.0 bis 239.255.255.255.
- Klasse E – Experimentelle Adressen bzw. für zukünftige Nutzung
 - o Adressbereich: 240.0.0.0 bis 247.255.255.255

- Beispiele:
 - Klasse A IP-Adresse: **10.5.5.1**
 - Klasse B IP-Adresse: **172.16.5.1**
 - Klasse C IP-Adresse: **192.168.5.1**

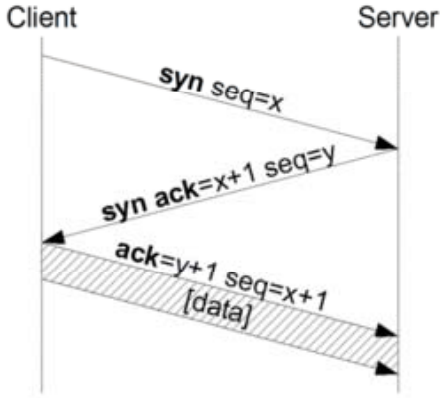
- Neuerung im IPv6
 - Eine IPv6-Adresse ist nun 128 Bit lang.
 - IPv6-Adressen werden nicht in dezimaler (zum Beispiel 80.130.234.185), sondern in hexadezimaler Notation mit Doppelpunkten geschrieben.
 - Beispiel: 2001:0db8:85a3:08d3:1319:8a2e:0370:7344
 - Notwendig aufgrund der geringen Anzahl verfügbarer IP-Adressen (IPv4)

- 1. Bitübertragungsschicht
- 2. Sicherungsschicht
- 3. Vermittlungsschicht
- 4. Transportschicht
- 5. Sitzungsschicht
- 6. Darstellungsschicht
- 7. Anwendungsschicht

- Die Transportschicht bildet die Schnittstelle zwischen transportorientierten und anwendungsorientierten Schichten.
- Sie hat die Aufgabe, den Transport der Daten von der Quelle zum Ziel (logische Ende-zu-Ende-Verbindung), unabhängig von den physikalischen Netzen zuverlässig und kosteneffizient (kürzester Weg) zu übernehmen.
- Die Transportschicht stellt den höheren Schichten u.a. folgende Dienste zur Verfügung:
 - **Geregelter Verbindungsaufbau (3-Wege-Handshake)**
 - Flusskontrolle und Pufferung
 - Multiplexing
- Wichtige Protokolle:
 - Transmission Control Protocol (TCP)
 - User Data Protocol (UDP)

- Beispiel aus dem Alltag - Terminvereinbarung per E-Mail
 - Prof. Rannenberg möchte sich mit Prof. König zu einer Besprechung verabreden.
 1. Prof. Rannenberg schickt Prof. König einen Terminvorschlag.
 2. Prof. König bestätigt Prof. Rannenberg den Termin mit einer Terminbestätigung.
 3. Prof. Rannenberg lässt Prof. König wissen, dass er seine Terminbestätigung erhalten hat.
 - Schritt 3 ist notwendig, damit Prof. König weiß, dass Prof. Rannenberg die Bestätigung erhalten hat. Nachricht Nummer 2 könnte verloren gegangen sein, und Prof. König würde alleine zu dem Treffen erscheinen.

Transmission Control Protocol (TCP) 3-Wege Handshake

- Aufbau einer TCP-Verbindung mittels 3-Wege-Handshake
 - Rechner (Client) sendet der Gegenstelle (Server) ein SYN-Paket (von engl. synchronize) mit Sequenznummer x .
 - Sequenznummern sind für die Sicherstellung einer vollständigen Übertragung in der richtigen Reihenfolge und ohne Duplikate wichtig.
- 
- Die Gegenstelle (Server) empfängt das Paket.
 - Ist der Port geschlossen, antwortet sie mit einem TCP-RST.
 - Ist der Port geöffnet, sendet sie ein eigenes SYN-Paket mit ihrer Start-Sequenznummer y . Zugleich bestätigt sie den Erhalt des ersten SYN-Pakets, indem sie die Sequenznummer x um eins erhöht und im ACK-Teil (von engl. acknowledgment = Bestätigung) des Headers zurückschickt.
 - Der Rechner (Client) empfängt SYN/ACK-Paket und bestätigt den Erhalt
 - Er sendet ein eigenen ACK-Paket mit der Sequenznummer $y+1$ (dieser Vorgang wird auch als „Forward Acknowledgement“ bezeichnet).
 - Außerdem sendet der Client den Sequenznummerwert $x+1$ zurück.
 - Dieses ACK-Segment erhält die Gegenstelle (Server); das ACK-Segment ist durch das gesetzte ACK-Flag gekennzeichnet.
 - Die Verbindung ist damit aufgebaut.

- Das Transmission Control Protocol (TCP) wurde speziell zum Transport eines **zuverlässigen verbindungsorientierten** Bytestromes (von einem Endpunkt zum anderen Endpunkt) in einem unzuverlässigen Netzwerk entwickelt.
- TCP ist im RFC 793 definiert.

- Eigenschaften

- Zuverlässig

- Eine Datenübertragung vom Sender zum Empfänger wird solange wiederholt, bis diese vom Empfänger bestätigt wird.

- Verbindungsorientiert

- In einem 3-Wege-Handshake wird eine logische Ende-zu-Ende-Verbindung zwischen Sender und Empfänger etabliert, bevor die eigentliche Datenübertragung beginnt.

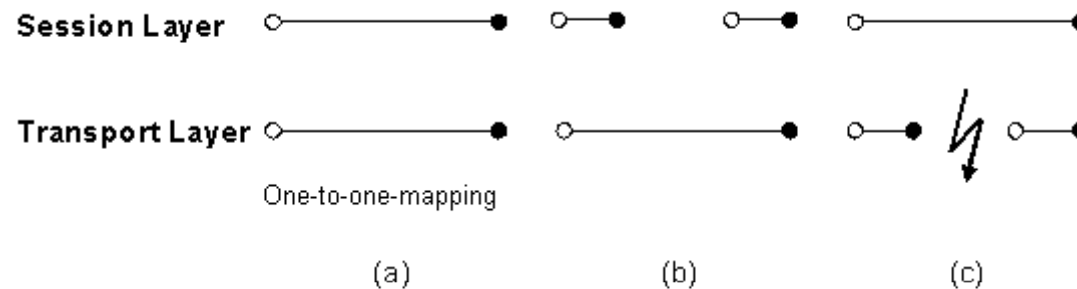
- Ermöglicht es, Informationen direkt an eine Anwendung zu leiten (Ports).

- Das User Data Protocol (UDP) ist ein verbindungsloses, unsicheres (keine Kontrolle, ob ein Datenpaket beim Empfänger angekommen ist) Transportprotokoll.
- UDP bietet gegenüber dem Transmission Control Protocol (TCP) den Vorteil eines geringen Protokolloverheads.
- UDP findet beispielsweise Anwendung bei DNS-Diensten.

- 1. Bitübertragungsschicht
- 2. Sicherungsschicht
- 3. Vermittlungsschicht
- 4. Transportschicht
- 5. Sitzungsschicht
- 6. Darstellungsschicht
- 7. Anwendungsschicht

- Die Sitzungsschicht stellt Mittel zur Verfügung, um einen organisierten und synchronisierten Datenaustausch zwischen Teilnehmern aufzubauen, geregelt durchzuführen und wieder geordnet zu beenden.
- Temporäre Teilnehmerverbindungen auf der Sitzungsschicht werden Sessions (Sitzungen) genannt.

- Einer Sitzung entspricht genau eine Transportverbindung und umgekehrt. (a)
- Mehrere Sitzungen werden über eine Transportverbindung abgewickelt. (b)



Bsp.: Ein Reisebüro ist per Minicomputer an die Flughafenauskunft angeschlossen. Bei jeder Flugreservierung für einen Kunden wird eine Anfrage gestartet, d.h. es finden viele Anfragen in kurzer Zeit statt. Es ist daher nicht sinnvoll, das Transportmedium freizugeben.

- Eine Sitzung wird (nacheinander) über mehrere Transportverbindungen durchgeführt. Dies ist dann der Fall, wenn ein Ausfall außerhalb des Hosts auftritt. Die Sitzung auf der Sitzungsschicht „überlebt“ den Ausfall auf dem Subnetz und ist somit die unterste Schicht, die den Aufbau einer neuen Transportverbindung übernehmen kann. (c)

- 1. Bitübertragungsschicht
- 2. Sicherungsschicht
- 3. Vermittlungsschicht
- 4. Transportschicht
- 5. Sitzungsschicht
- 6. Darstellungsschicht
- 7. Anwendungsschicht

- Die Darstellungsschicht wandelt systemspezifische Darstellungen von Daten in eine abstrakte Form um (Darstellungskonvertierung), so dass Daten in offenen Systemen ausgetauscht werden können.
- Weitere Aufgaben der Darstellungsschicht sind die
 - Datenkonvertierung,
 - Komprimierung und
 - Verschlüsselung

- Erforderlich sind:
 - o eine abstrakte Syntax zur Kommunikation ursprünglich systemspezifischer Datendarstellungen
 - o eine Syntax für die bitweise Codierung (Transfersyntax)
- Die standardisierte Beschreibungssprache ASN.1 (Abstract Syntax Notation) wurde als abstrakte Form der Syntaxbeschreibung definiert.
- Ihre Sprachkonstrukte ähneln den Sprachkonstrukten der Programmiersprache C.
 - o Basisdatentypen:
 - INTEGER, BITSTRING, OCTETSTRING, IA5STRING, REAL, OBJECT IDENTIFIER
 - o Aufzählungstyp, Zusammengesetzte Typen, ...

- Beispiel:

```

BEGIN
    Flugbuchung ::= SEQUENCE
    {
        passagier          Person
        flugbezeichnung    IA5STRING
        datum              IA5STRING
        abflug             Termin
        ankunft            Termin
    }
    Person ::= SEQUENCE
    {
        name               IA5STRING
        ...
    }
    Termin ::= SEQUENCE
    {
        Ort                IA5STRING
        Zeit               IA5STRING
    }

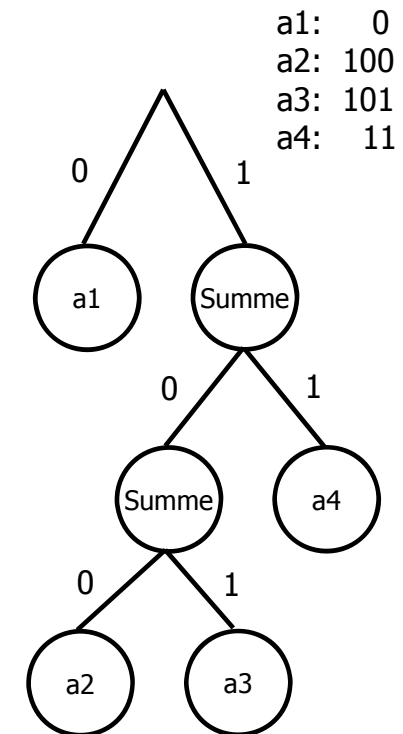
```

Quelle: Eicker (2006a)

- Um den immer höheren Datenaufkommen entgegen zu wirken, ist die Komprimierung von Daten bei der Datenübertragung unerlässlich (motiviert durch damalige geringe Bandbreiten).

- Komprimierungsverfahren sind u.a.:
 - Differenzialkodierung
 - Vektorkodierung
 - Umwandlungskodierung
 - Lauflängenkodierung
 - **Statistische Kodierung**
 - Kodierungstabellen

- Beispiel: Huffman-Kodierung (statistische Kodierung)
 - Geht auf Morse und sein Morse-Alphabet zurück
 - Häufiger auftretenden Symbole erhalten kürzere Codes.
 - Selten auftretende Symbole erhalten lange Codes.
 - Ein Huffman-Code-Baum ist ein spezieller Binärbaum. Jeder Ast führt entweder zu einer weiteren Verzweigung oder zu einem „Blatt“.
 - Die Codes erhält man, indem man dem entstehenden Code bei einer Verzweigung nach rechts eine 1, sonst eine 0 (oder vice versa) hinzufügt.



- Ein Verschlüsselungsalgorithmus muss in der Lage sein, einen Klartext in Chiffretext umzuwandeln, so dass ausschließlich der vorgesehene Empfänger in der Lage ist, den Klartext zu erzeugen.

- Unterschieden werden
 - Symmetrische Verschlüsselungsverfahren
 - Bei der symmetrischen Verschlüsselung verwenden Sender und Empfänger denselben Schlüssel.
 - Asymmetrische Verschlüsselungsverfahren
 - Bei der asymmetrischen Verschlüsselung werden zwei Schlüssel, ein privater und ein öffentlicher Schlüssel, verwendet.

- Einer der bekanntesten Algorithmen ist der DES (Data Encryption Standard), der in den siebziger Jahren von IBM für das National Bureau of Standards entwickelt wurde. Es ist ein „bewährtes“ symmetrisches Verschlüsselungsverfahren und wurde 1974 veröffentlicht und in den USA als ANSI-Standard genormt (ANSI X3.92-1981).

- Anwendungsgebiet:
 - Übertragung sensibler Daten, wie sie beispielsweise auf Kapitalmärkten vorgenommen werden.

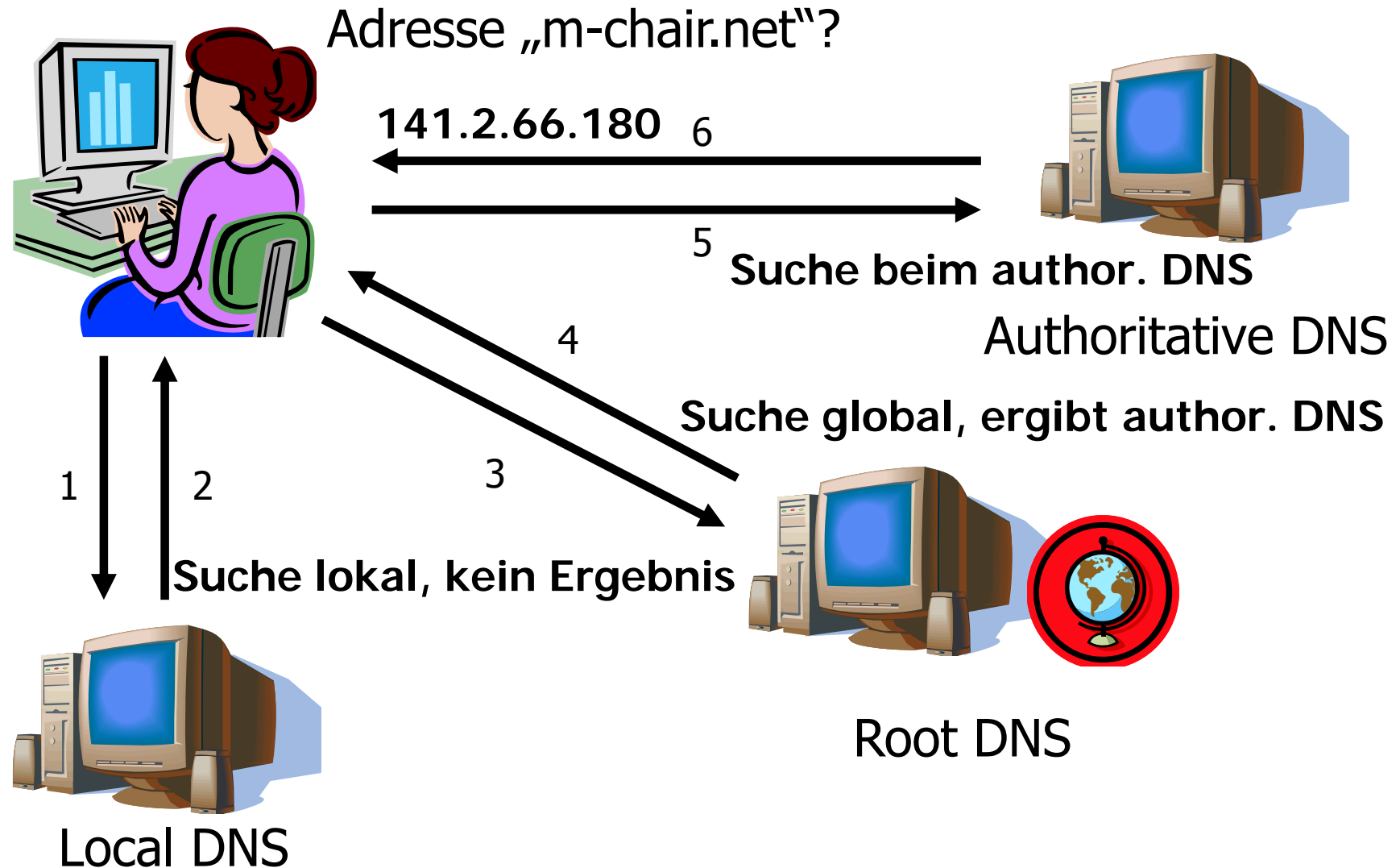
- 1. Bitübertragungsschicht
- 2. Sicherungsschicht
- 3. Vermittlungsschicht
- 4. Transportschicht
- 5. Sitzungsschicht
- 6. Darstellungsschicht
- 7. Anwendungsschicht

- Alle Schichten unterhalb der Anwendungsschicht dienen dazu, einen zuverlässigen Transport der Daten sicherzustellen, führen aber keine Aufgaben für den Benutzer durch.

- Auf der Anwendungsschicht werden unterstützende Protokolle eingesetzt, damit Anwendungen funktionieren. Sie bildet die Schnittstelle zu den Anwendungsprogrammen:
 - **DNS**
 - E-Mail
 - FTP
 - ...

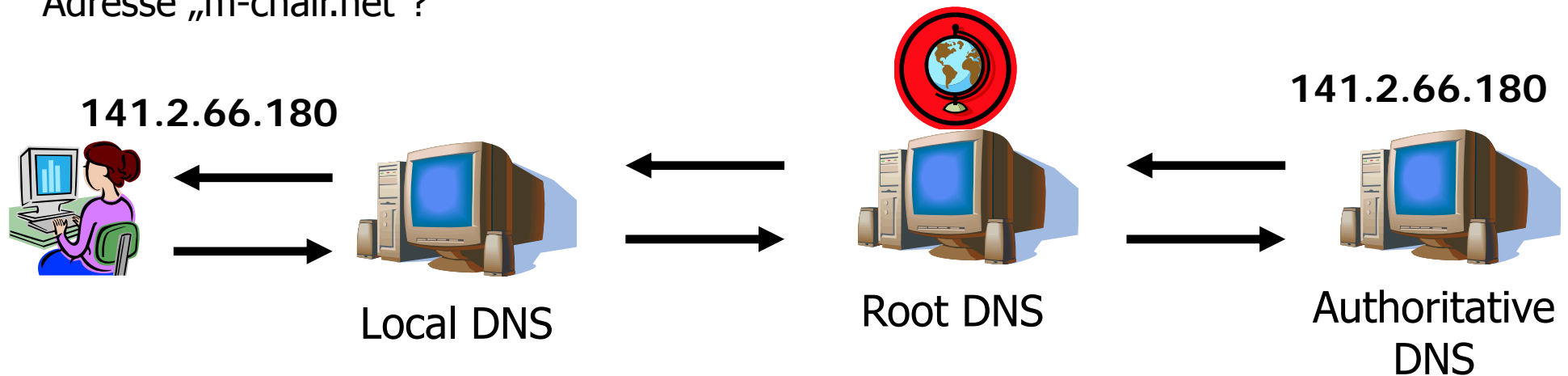
Quelle: Tanenbaum (2006)

- Einführung einer verteilten Datenbank, des „Domain Name Service“ oder DNS.
- DNS findet auf der Anwendungsschicht statt.
- DNS übersetzt Name in Adresse, Adresse in Name oder liefert den Mailserver einer Domäne (den Mail-Exchange oder MX-Record).
- Es gibt drei Arten von DNS:
 - Local: DNS innerhalb der eigenen Organisation
 - Root: Wurzel-DNS einer Domain
 - Authoritative: DNS, bei denen die Domains registriert sind



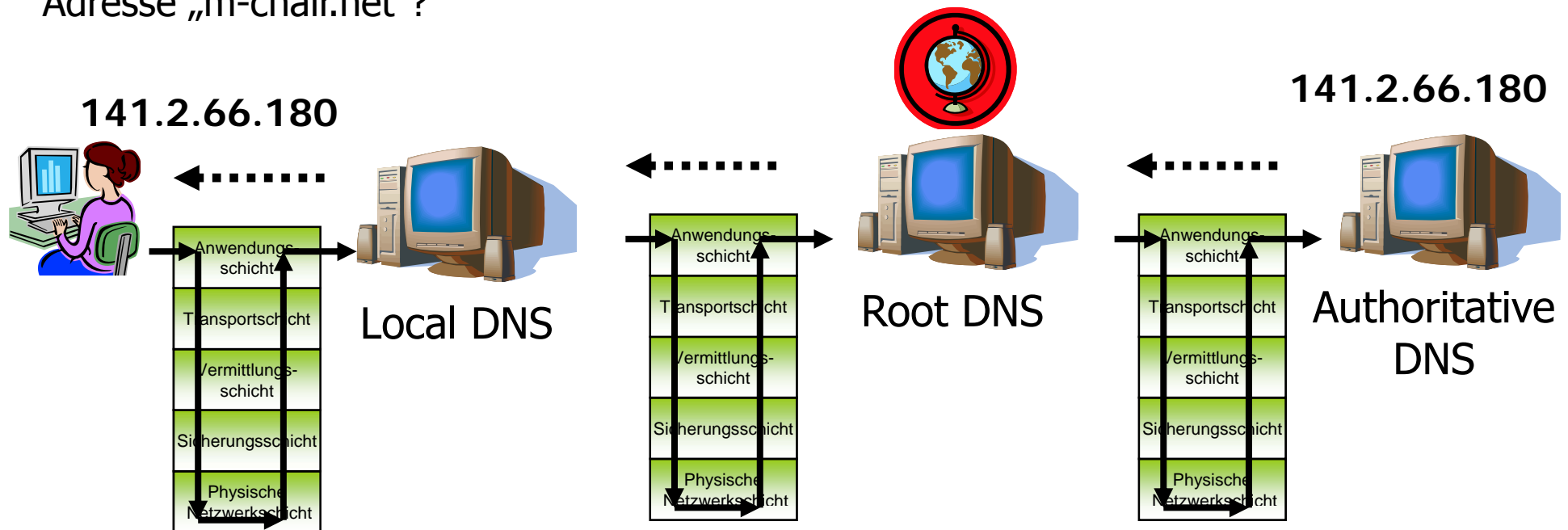
- Ziel: Last der DNS-Abfragen besser verteilen

Adresse „m-chair.net“?



- Bei den DNS-Abfragen werden die verschiedenen Schichten eines Netzwerks durchlaufen!

Adresse „m-chair.net“?



- DATACOM Buchverlag GmbH (2005) „IP-Protokoll“, <http://www.itwissen.info/>
- Eicker, S. (2006) „Grundlagen betrieblicher Kommunikationssysteme“, Skript Uni Duisburg-Essen.
- Holtkamp, H. (2002) „Einführung in TCP/IP“, <http://www.rvs.uni-bielefeld.de/~heiko/tcpip/>
- Tanenbaum, A.S. (2006) „Computernetzwerke“, ISBN-10: 3827370469