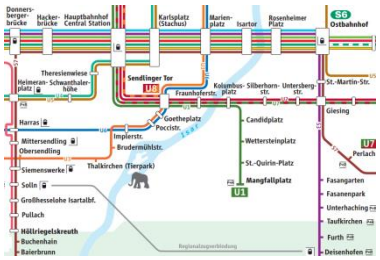
Die OSI-Schichten 3 und 4

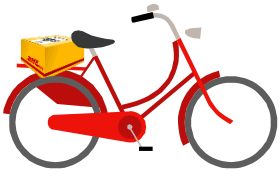


Bislang wurden Aufbau und Funktionsweise lokaler Netze auch an Hand des Modells eines Nahverkehrsnetzes geklärt. In diesem Kapitel wird die Kommunikation zwischen weiter entfernten Rechnern beschrieben.

Im Prinzip kann man sich das Senden von Daten ähnlich vorstellen wie das Versenden von Postpaketen:

1. Der zu versendende Inhalt wird in ein Paket gepackt und mit Absender- sowie Empfängeradresse versehen.

2. Die Pakete werden zur Postfiliale transportiert.

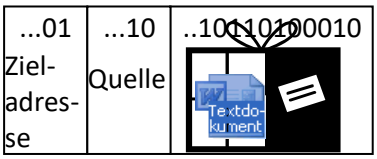


3. Alle eingegangenen Pakete werden zu Paketzentren transportiert und dort nach der Postleitzahl sortiert, um sie weiterleiten zu können.
Beschädigte Pakete werden repariert, unleserliche Adressen manuell ermittelt.

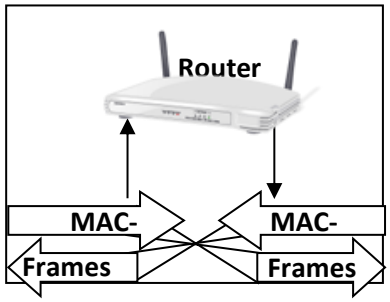
4. Die Pakete werden mit Hilfe geeigneter Transportmittel zu unterschiedlichen Paketzentren in der Nähe des Empfängers transportiert.
Von dort werden die Pakete an den Bestimmungsort gebracht.

Die zu versendenden Daten werden in mehrere Datenpakete gepackt und mit Quell- sowie Zieladresse versehen.
In Wirklichkeit handelt es sich natürlich um eine Bitfolge.

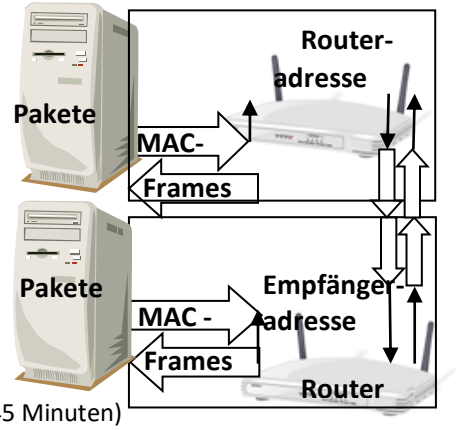
Die Pakete werden in MAC-Frames gesendet.



Router lesen die Adresse aus und leiten die Pakete weiter. Unleserliche Pakete werden verworfen und neu gesendet.

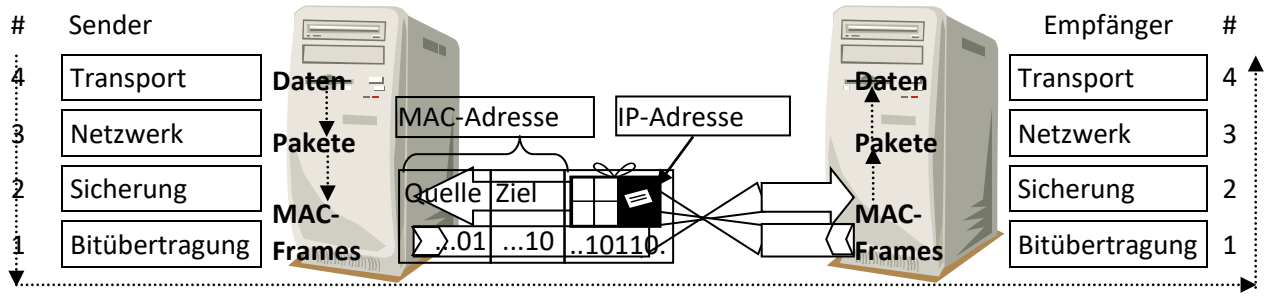


Die Pakete werden so lange von Router zu Router weitergeleitet, bis sie beim Empfänger ankommen.



Video von Ebay / DHL dazu: vgl. .\241-materialien\paketzustellung\ (Dauer: 8:45 Minuten)
Quelle: http://www.dhl.de/mlm.nf/dhl/images/images/dhl_de/dhl_relaunch/homepage/ebay_film/videoplayer.html

Die Kommunikation zwischen Computern verläuft folgendermaßen:
Der Sender teilt die Daten in Pakete auf, „übersetzt“ sie in MAC-Frames und sendet sie. Der Empfänger packt die Pakete aus und fügt den Inhalt wieder zu den ursprünglichen Daten zusammen:



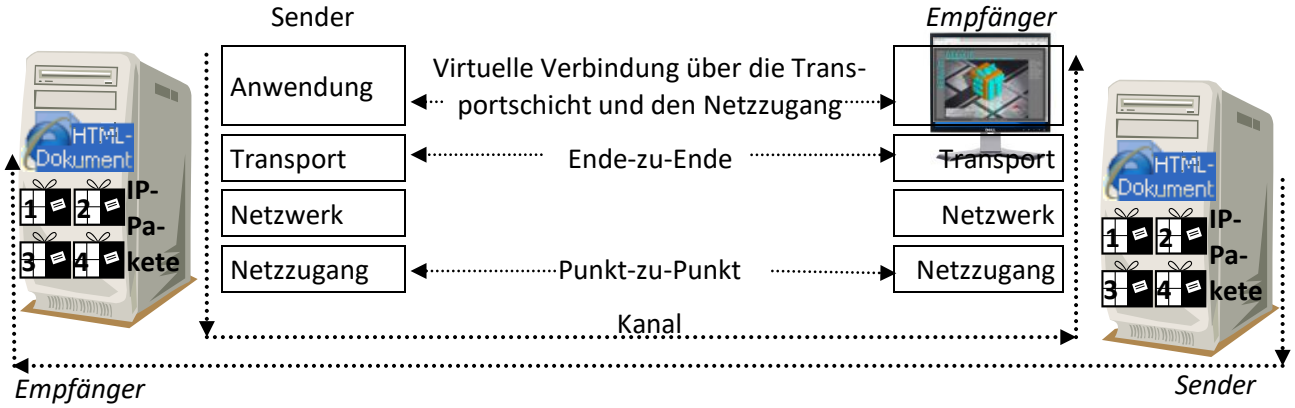
Die Datenübertragung kann man sich auch ähnlich wie beim Morsen vorstellen: Beim Übermitteln von Descartes‘ Zitat rechts finden im Zusammenhang mit dem Kommunikationsvorgang auch Datenverarbeitungsvorgänge statt:

Animation vgl. .\251-materialien\animationen\telegrafie2\telegrafie2.htm

- *Codierung*: Der Sender überträgt alphanumerische Zeichen in den Morsecode.
- *Übertragung*: Dabei sendet er die Binärzeichen in Form von Stromimpulsen.
- *Decodierung*: Der Empfänger überträgt Binärzeichen in alphanumerische Zeichen.

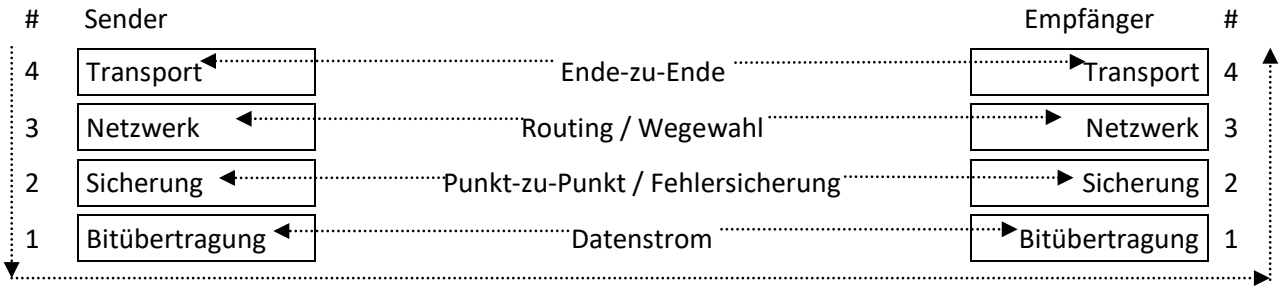
Du kennst bereits ein Modell für die Kommunikation zwischen Computern (vgl. Lerninhalte 1.4-04, Seite 2). Das nennt man ein **Schichtenmodell**: Der Ablauf wird in Schichten (*layer*) gegliedert, die von oben nach unten und wieder zurück abgearbeitet werden. Dieses Modell ist an das **TCP/IP-Referenzmodell** angelehnt. Bei diesem Modell wird vernachlässigt, wie die Daten technisch übertragen und wie übermittelte Daten weiterverarbeitet werden. Deshalb spricht man von einem **vereinfachten Schichtenmodell**:

- Der Sender zerlegt die Daten in *IP-Pakete* und übermittelt sie zum Empfänger.



Die vollständige Beschreibung des Kommunikationsvorgangs erfolgt in dem **OSI-Schichtenmodell**, wobei die Netzzugangsschicht in zwei Schichten aufgeteilt wird.
Die Anwendungsschicht wird hier noch ausgespart und das OSI-Modell um dieSchichten 3 und 4 erweitert:

- Auf der **Bitübertragungsschicht** (Schicht 1) wird die Technik zur Übermittlung der Signale festgelegt.
- Auf der OSI-Schicht 2 (**Sicherung**) wird das Zugriffsverfahren festgelegt und damit die Kommunikation zwischen zwei Rechnern gewährleistet, weshalb die Verbindung auch **Punkt-zu-Punkt** genannt wird.
- Für den Weg („die Route“) zwischen unterschiedlichen Netzwerken über weite Strecken hinweg ist die OSI-Schicht 3 (**Netzwerk**) zuständig.
- In der **Transportschicht** (OSI-Schicht 4)wird eine **Ende-zu-Ende**-Verbindung hergestellt: Hier ist das Übermitteln der Daten abgeschlossen und der fehlerfreie Datentransfer wird gewährleistet.



A Bearbeite das Arbeitsblatt 08: Simulation von Netzwerken mit FILIUS I

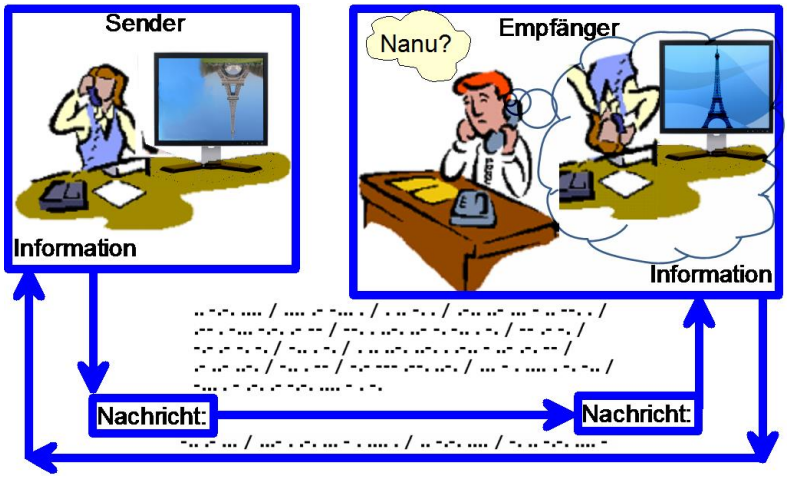
Protokolle

Jetzt gilt es zu betrachten, wie das „Übersetzen“ und Adressieren der Daten für den Transport funktioniert.

Ein Gespräch zwischen zwei Personen wird in einer für sie verständlichen Sprache geführt. Würden sie im Morsecode miteinander sprechen, wäre das nicht nur umständlich und langwierig. Die beiden würden sich wahrscheinlich auch nicht verstehen.

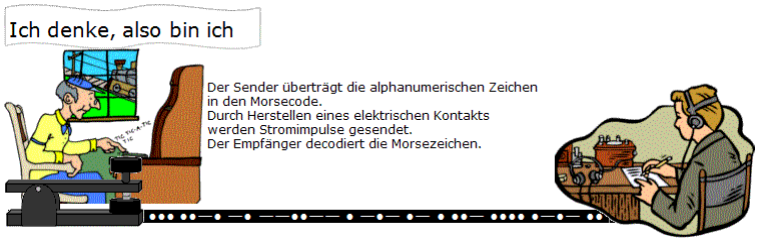
Für eine direkte Unterhaltung zwischen zwei Menschen ist eine natürliche Sprache angemessen.

Für die Übermittlung von Nachrichten über größere Entfernungen war lange Zeit die Telegrafie eine effektive technische Lösung.



„Unterhaltung“ im Morsecode (vgl. Lerninhalte 1.4-04 Kommunikation)

Bei der Telegrafie musste der Telegrafist den natürlichsprachlich vorgegebenen Text in den Morsecode übersetzen, um diesen übermitteln zu können.
Bei der Kommunikation zwischen Computern ist es naheliegend, zur Nachrichtenübermittlung ebenfalls einen Binärcode zu verwenden, da die Daten ohnehin binär codiert vorliegen.



Telegrafische Nachrichtenübermittlung

Wie in dem Beispiel oben „sprechen“ unterschiedliche Schichten in Computernetzen aber auch eine andere „Sprache“. Eine „Sprache“ im Computernetz wird Protokoll genannt.

- Ein **Protokoll** ist in der Informationstechnik eine Zusammenstellung von Regeln, *die Kommunikation auf derselben Schicht ermöglichen.*

In einer natürlichen Sprache beinhalten diese Regeln vor allem die **Bedeutung von *Vokabeln*** und *grammatikalische* Festlegungen. Die Übertragung ergibt sich im Gespräch durch den Rede**fluss**.
Die Kommunikation in Computernetzen ist dagegen meist **paketorientiert**. Das bedeutet, dass die Daten in Dateneinheiten zerlegt und in einzelnen Paketen gesendet werden.
Bei Netzwerkprotokollen ist insbesondere der Aufbau eines Datenpakets festgelegt.
Ein Paket ist durchaus mit einem Frame vergleichbar, auch wenn die beiden Begriffe im OSI-Modell klar zu trennen sind. Darin sind insbesondere die folgenden Informationen enthalten:

- Absender und Empfänger
- Typ des Pakets (z. B. Nutzdaten; Verbindungsaufbau und -abbau)
- Paketgröße

Es gab bzw. gibt viele unterschiedliche Protokolle. Beispiele aus dem PC-Bereich sind:

- NetBIOS (von IBM - engl. Network Basic Input Output System): Dieses Protokoll wurde für die ersten Netzwerkfunktionen in MS-DOS verwendetet
- IPX/SPX (von Novell – engl. Internetwork Packet eXchange) war in den 80er und 90er Jahren das am häufigsten genutzte Protokoll für PC-basierte lokale Netze.
- Apple Talk (von Apple) wurde mittlerweile - wie die übrigen genannten Protokolle auch
- durch TCP/IP verdrängt, das hier zunächst besonders wichtig ist:

TCP/IP (Transmission Control Protocol / Internet Protocol)

In TCP/IP sind zwei Protokolle enthalten, die die Grundlage des Internet bilden: Das Übertragungssteuerungsprotokoll TCP und das Internet Protocol IP.

Die Aufgaben der Protokolle TCP und IP sind:

- Verbindungsaufbau zwischen Computern *(TCP)*
- Zerlegen der Daten in Pakete *(TCP)*
- Übertragung von Paketen *(IP)*
- Erkennen von Übertragungsfehlern durch die Prüfsumme *(in IP V4)*
- Wiederholtes Senden von Paketen, die den Empfänger nicht erreicht haben *(TCP)*
- Verschlüsselung der Daten
- Elektronische Signaturen verhindern die Manipulation der Daten
- Zusammenfügen übertragener Datenpakete in der richtigen Reihenfolge *(TCP)*

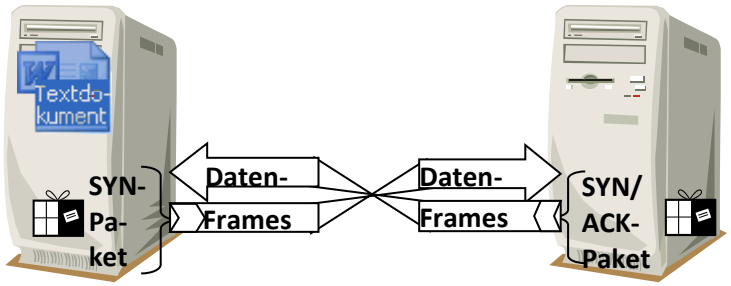
Die Aufgabenverteilung der beiden Protokolle ist mit dem Postweg vergleichbar:

- TCP ist für das Ein- und Auspacken sowie die Kontrolle des Inhalts zuständig.
- IP ersetzt den Postboten, der die Pakete transportiert und an die
- Empfängeradresse ausliefert.

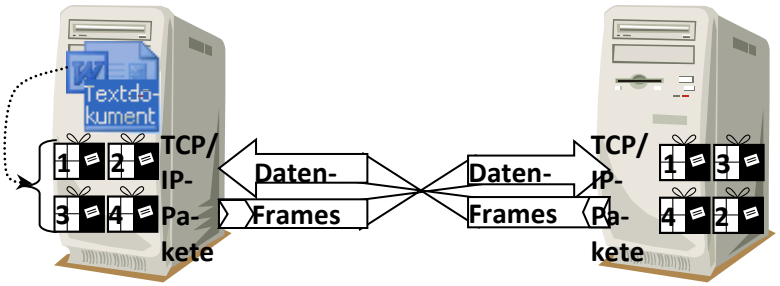
Beispiel:

Es soll ein Textdokument gesendet werden.

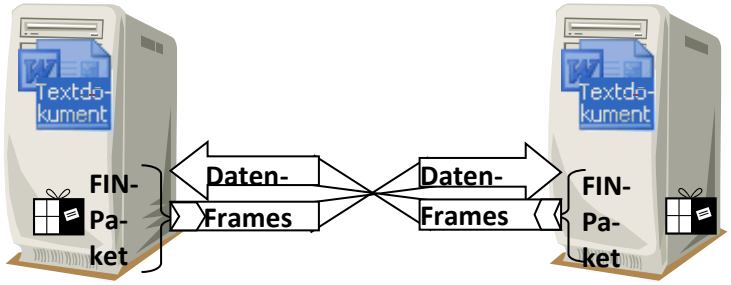
I. Verbindungsaufbau (TCP)
Der Client, der eine Verbindung aufbauen will, sendet dem Server ein SYN-Paket (von engl. synchronize). Der Server empfängt das Paket. Dann bestätigt er den Empfang und stimmt dem Verbindungsaufbau zu, indem er ein SYN/ACK-Paket zurückschickt (ACK von engl. acknowledgement = Bestätigung).



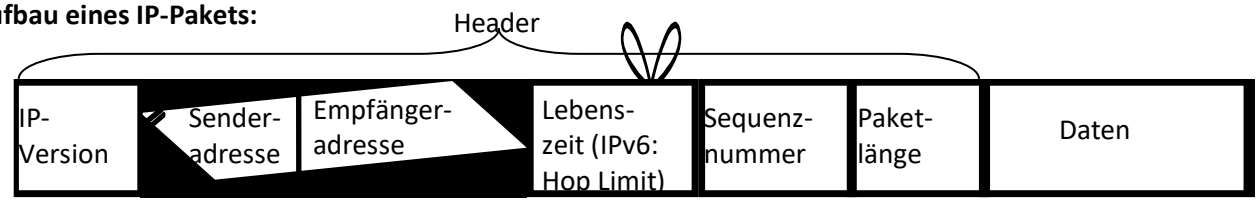
II. Datenübertragung
- Segmentierung: Der Sender zerlegt die Daten in Pakete (TCP).
- Versenden (IP):
Dazu werden die IP-Pakete in Frames verpackt und übertragen, wofür wiederum die Bitübertragungsschicht zuständig ist.
- Bestätigung der Sendung (TCP)
Die Datenframes – und damit die IP-Pakete - kommen beim Empfänger meist nicht in der Reihenfolge an, in der sie versendet wurden. Damit der Empfänger wieder die richtige Reihenfolge herstellen kann, werden die Pakete durchnummeriert.
IP-Pakete werden meistens über Ethernet übertragen. Weil ein MAC-Frame maximal 1500 Byte groß sein darf, wird üblicherweise für IP-Pakete diese Größe verwendet.



III. Verbindungsabbau (TCP)
Beendet wird die Übertragung durch Senden eines FIN-Pakets (von engl. finish = Ende, Abschluss). Der Empfänger des FIN-Pakets bestätigt den Erhalt mittels ACK und sendet ebenfalls FIN-Paket.



Aufbau eines IP-Pakets:

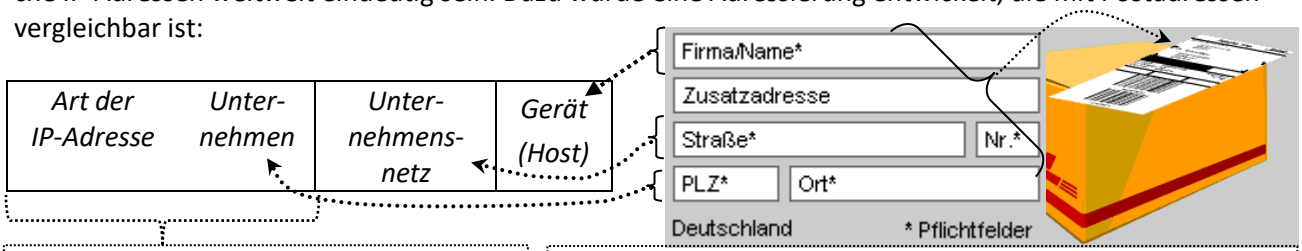


Lange Zeit war IP Version 4 Standard. Seit dem Jahr 2010 wurde auf IP Version 6 umgestellt.

- Die Angabe der Lebenszeit (IPv4: Time to live; IPv6: Hop Limit) ist erforderlich, damit Pakete nicht endlos kreisen, wenn sie keinen Empfänger erreichen.
- Mit der Sequenznummer werden die gesendeten Pakete durchnummeriert, damit der Empfänger sie wieder in der richtigen Reihenfolge zusammenfügen kann.

IP-Adressen

Die Zustellung von IP-Paketen muss weltweit organisiert werden. Wie Postadressen müssen auch öffentliche IP-Adressen weltweit eindeutig sein. Dazu wurde eine Adressierung entwickelt, die mit Postadressen vergleichbar ist:



Im linken Teil der IP-Adresse wird in Netzwerke eingeteilt („Netzwerkanteil“).

Im rechten Teil wird in Hosts eingeteilt („Hostanteil“). Hier wird die Adresse des Geräts im Netz angegeben.

Öffentliche IP-Adressen müssen in der Regel weltweit eindeutig zugeordnet werden können.
Für die Vergabe von Adressblöcken ist die Internet *Assigned Numbers Authority* (IANA) verantwortlich.
Die IP-Adressen werden von *Regional Internet Registries* (RIRs) verwaltet. Jede RIR ist für einen Teil der Welt verantwortlich, z. B. das *Réseaux IP Européens Network Coordination Centre* (RIPE NCC) für Europa.

IP Version 4

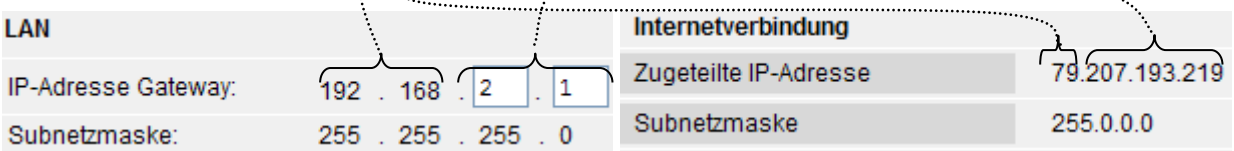
Eine IPv4-Adresse besteht aus vier 8 Bit großen Gruppen, die jeweils durch einen Punkt (dot) getrennt sind. Sie ist also insgesamt 32 Bit groß, der Adressbereich erstreckt sich von 0.0.0.0 bis 255.255.255.255 und umfasst damit im Prinzip 256^4 verschiedene Adressen.
In der Version 4 des Internet Protocols (IPv4-Adressen) wurden zur Verwendung innerhalb lokaler Netze *private Adressbereiche* reserviert, die im Internet nicht weitergeleitet werden:

192.168.0.0–192.168.255.255, 172.16.0.0–172.31.255.255 und 10.0.0.0–10.255.255.255

Beispiele für konkrete IP-Adressen:

Netzwerkteil		Lokaler Adressteil	
Art der IP-Adresse	Unternehmen	Subnetz	Gerät (Host)

I. Private IP-Adresse II. Öffentliche IP-Adresse

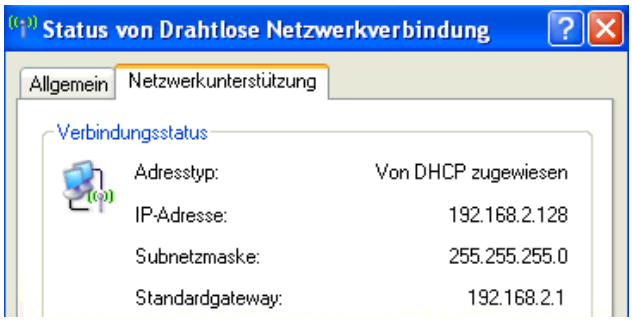


Die **private** IP-Adresse 192.168.2.1 ist nur innerhalb des lokalen Netzes sichtbar. Diese Adresse kann selbst vergeben werden und kommt weltweit häufig vor.

Die **öffentliche** IP-Adresse 79.207.193.219 wurde von dem Internetprovider zugewiesen und ist weltweit eindeutig. Diese Adresse kann nicht selbst geändert werden.

Die **Subnetzmaske** ermöglicht die Festlegung von Subnetzen innerhalb eines Unternehmens. Das verbessert die Effektivität von technischen Lösungen deutlich. Die Einrichtung ist aber recht kompliziert. Für den Normalgebrauch reicht es, folgendes zu wissen:

- Eine 0 im lokalen Adressteil der Subnetzmaske zeigt an, dass keine Subnetze existieren.
- Die Subnetzmasken innerhalb eines (Sub-) Netzes müssen immer identisch sein.



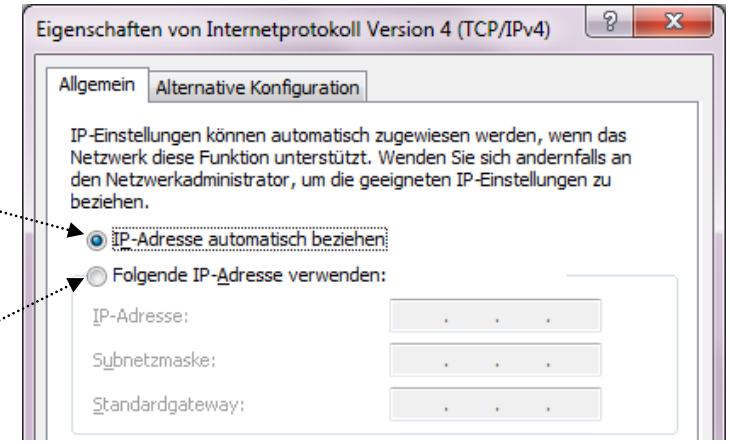
Das bedeutet für das Beispiel oben, dass alle PCs innerhalb des Netzes die Subnetzmaske 255.255.255.0 erhalten müssen. Dies ist eine Standardkonfiguration für kleinere Netze.

A Bearbeite das Arbeitsblatt 09: Beschreibung des Internetprotokolls Version 4

Das Dynamic Host Configuration Protocol (DHCP)

DHCP ermöglicht die Zuweisung von Einstellungen durch einen Server. Dadurch können Geräte automatisch konfiguriert werden.
Bei aktiviertem DHCP bezieht der Client beim Start des Rechners die IP-Adresse, die Netzmaske, das Gateway und den DNS-Server, sofern ein DHCP-Server erreichbar ist.

Selbstverständlich können die Daten für die Netzwerkverbindung auch manuell konfiguriert werden.



A Bearbeite das Arbeitsblatt 10: Simulation von Netzwerken mit FILIUS II

IP Version 6

A Bearbeite das Arbeitsblatt 11: Hexadezimalzahlen

Durch den zunehmenden Bedarf an IP-Adressen wurde der Adressraum von IPv4 zu klein.
Es gab Ansätze, das Internetprotokoll unter der Versionsnummer 5, vor allem in Bezug auf die Echtzeitfähigkeit, zu erweitern. Ein Protokoll IPv5 wurde aber nie standardisiert.

Deshalb wurde IPv6 entwickelt. Hier werden **128 Bit** zur **Adressierung** verwendet, womit im Prinzip 2^{128} (= 340.282.366.920.938.463.463.374.607.431.768.211.456) - etwa 3,4 x 10^{38} - Adressen darstellbar sind. Damit kann theoretisch jeder Quadratmeter der Erdoberfläche mit etwa 6 x 10^{23} IP-Adressen versorgt werden. Dass tatsächlich nicht ganz so viele Adressen zur Verfügung stehen, liegt daran, dass für IPv6 einige Funktionalitäten zur Verfügung stehen, die es in IPv4 so noch nicht gab, zum Beispiel:

- In IPv6 gibt es keine statische Aufteilung mehr (Netz, Rechner).
- Jeder Adapter erhält mehrere IPv6-Adressen nach folgenden Vorgaben:
  - Die Schreibweise ist hexadezimal. IPv6-Adressen bestehen aus 8 Gruppen je 2 Byte, z.B.: fe80:0000:0000:0000:150c:dd53:b804:688
  - Führende Nullen können weggelassen werden, z.B. fe80:0:0:0:150c:dd53:b804:688.
  - Aufeinander folgende Blöcke, deren Wert 0 beträgt, dürfen einmal ausgelassen und durch zwei Doppelpunkte ersetzt werden, z.B. fe80::150c:dd53:b804:688.
  - Für die Eingabe von IPv6-Adressen in Browsern werden eckige Klammern verwendet, z.B. **http://[2a02:2e0:3fe:100::7]** könnte eine konkrete IPv6-Adresse sein.
  - Der Interface Identifier (ID) kann aus der MAC-Adresse erstellt werden.

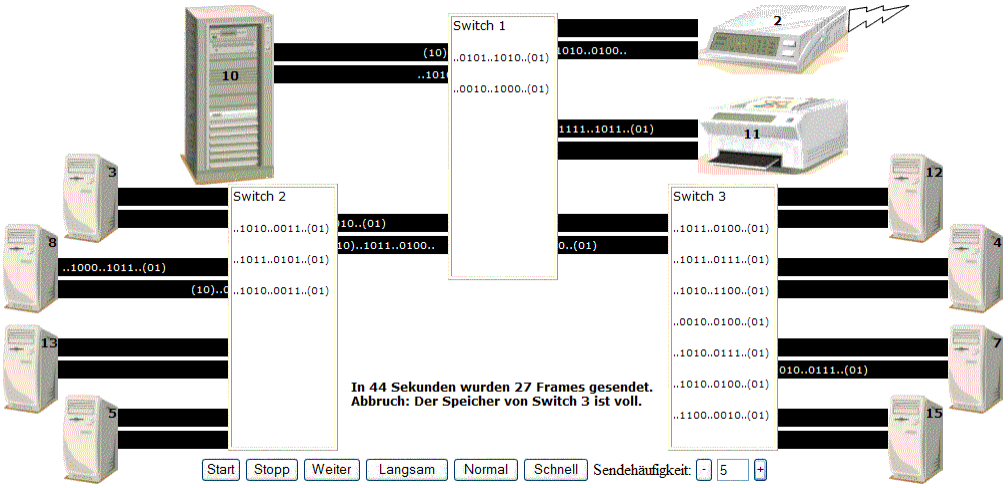
- Der binäre Präfix enthält Angaben zur Art der IP-Adresse:
  - Der Bereich FE80 bis FEBF ist zur automatischen Konfiguration reserviert: Jeder Host generiert eine lokale-Adresse, auch wenn keine Verbindung besteht, z. B.: fe80::150c:dd53:b804:688
  - Die Präfixe FC und FD kennzeichnen Unique Local Addresses (ULA) – private Adressen, z. B.: fd90:2906:4a75:0001::1.
  - Adressen, die keinem anderen Zweck dienen, sind weltweit eindeutig (Global Unicast), z. B.: 2003:0061:e87f:8202:7631:70ff:fee7:cb73/56
- IPv6-Adressen sind 128 Bit lang, die sich wie folgt strukturieren:

	Netzwerkteil			Lokal (64 Bit)
	Art der IP-Adresse	Unternehmen	Subnetz	Gerät (Host)
Unicast	010	(Provider-ID)	(Subnetz-ID)	(Interface-ID)
Link Local Unicast	1111 1110 10	*Die Netzmaske legt fest, wie viele Bit der 64 Bit des Netzwerkteils für Subnetze zur Verfügung stehen. Z. B. bei /56 sind 256 Subnetze möglich (8 Bit), bei /64 keines (0 Bit).*		
Unique Local Unicast	1111 1100 1111 1101			
Multicast	1111 1111			
IPv4-Adresse	0000 0000	(Nullen)	FFFF	(32 Bit IPv4)

  - Unicast-Adressen sind providerbasierte Adressen und gelten weltweit.
  - Link local Unicast: Verbindungsspezifische lokale Adressen sind nur im gleichen Teilnetz erreichbar. Sie dienen der Autokonfiguration.
  - Unique local Unicast: Unique Local Addresses (ULA) werden für private Adressen verwendet.
  - Multicast-Adressen sprechen eine ganze Gruppe von Rechnern an. Das spart Bandbreite, weil die Pakete nicht mehrfach an jeden einzelnen Empfänger gesendet werden müssen.
  - IPv4-Adressen werden von links mit Nullen aufgefüllt und FFFF vorangestellt.
    Eine IPv4-Adresse lautet also in IPv6 z. B. 192.168.2.1 -> [::FFFF:C0:A8:2:1].

Überlaststeuerung

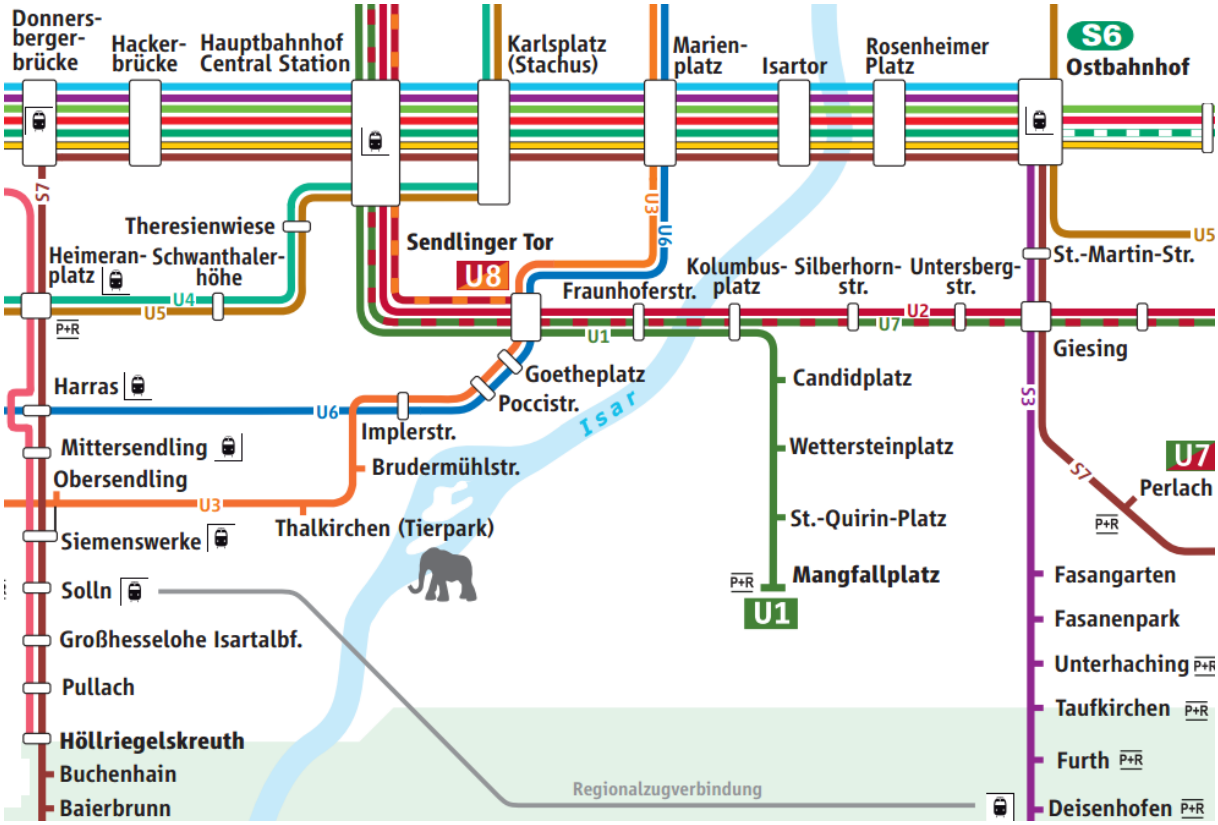
Der Verlust von Paketen wird festgestellt, wenn der Sender innerhalb einer bestimmten Zeit (Timeout) keine Bestätigung (ACK) erhält. Pakete können auf Grund eines „Staus“ bei hoher Netzlast verworfen werden. Diese Pakete werden erneut gesendet, was wiederum die Netzlast nochmals erhöht. Um den Stau zu beheben, reduzieren alle Sender ihre Netzlast, was aber die Wartezeiten (Latenz) erhöht. Das gilt in lokalen Netzen ebenso wie im Internet. Ein solcher „Propfen“ in der Kommunikation wird als *Bufferbloat* bezeichnet, der erstmals im Jahr 1986 das NSFnet von 32 kBit/s auf 40 Bit/s einbrechen ließ. Um das Problem zu beheben, können auch nicht einfach die Pufferspeicher beliebig vergrößert werden, weil dadurch die Latenzen zunehmen und durch wiederholtes Senden von Paketen die Netzlast weiter vergrößert wird.
In der Simulation zu dem Zugriffsverfahren CSMA/CD in Baumstrukturen wurde auf diesen Effekt zur Verdeutlichung mit einer Fehlermeldung hingewiesen. Diese Situation führt in der Wirklichkeit nicht zu einem Ausfall des Netzes. Bei hoher Netzlast sind Blockadesituationen möglich, die auch z. B. bei längeren Downloads beobachtet werden können.



Einordnung in das OSI-Schichtenmodell

Die Verkehrsnetze von S- und U-Bahn werden über ein gemeinsames Tarifsystem kombiniert: Ein Fahrgast, der ein Ticket des Verkehrsverbunds besitzt, kann sowohl die S-Bahn als auch die U-Bahn benutzen. Er muss lediglich etwas Zeit für das Umsteigen einkalkulieren.

- Der Fahrgast kann also den Weg mit dem entsprechenden Verkehrsmittel wählen.
- Insgesamt wird der Personentransport in unterschiedlichen Transportsystemen über das Tarifsystem gewährleistet – und damit durch eine über dem Zugverkehr liegende Schicht.



Genau diese beiden Schichten existieren auch in den **OSI-Schichten 3 und 4** für Datennetze:

#	Bezeichnung	Erläuterung	Protokolle / Geräte
4	Transport-schicht (transport layer)	Aufbau von Netzwerkverbindungen, Sicherstellung der *Weiterleitung* und Ankunft der Daten. Eine eventuelle *Wiederholung* der Datenübertragung kann veranlasst werden.	Das ***TCP*** (Transmission Control Protocol) beherrschen alle aktuellen Betriebssysteme.
3	Netzwerk-vermittlungs-schicht (network layer)	Nachrichten werden *adressiert* und die Paketleitwege vom *Sender* zum *Empfänger* festgelegt.	***IP*** (Internet Protocol) zur Bildung von Subnetzen. ***Router*** leiten Daten medienunabhängig aber protokollabhängig weiter.

Im Straßenverkehr wird häufig der Begriff *Route* verwendet:

- Man wählt eine bestimmte Route, um mit dem Auto den Urlaubsort zu erreichen
- Wenn man sich in einer Gegend oder in einer Stadt nicht auskennt, benutzt man einen Routenplaner.

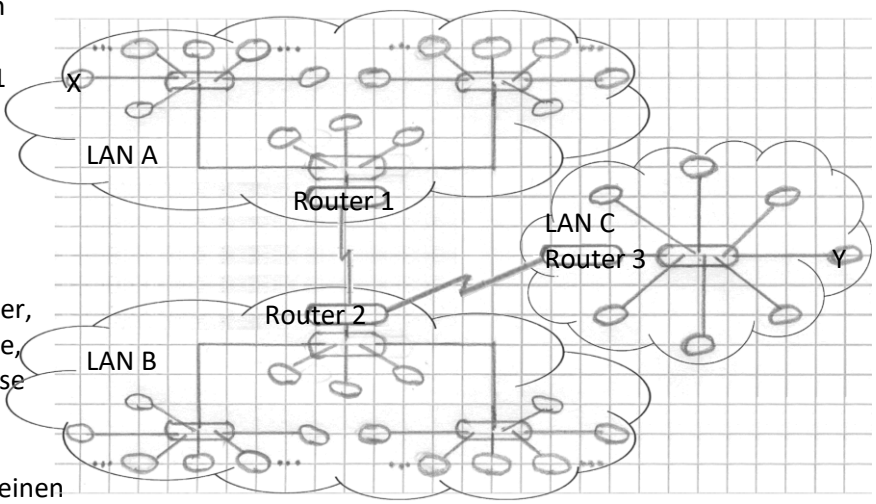
➢ Auch die Wahl des Wegs in Computernetzen wird als **Routing** bezeichnet.

A Bearbeite das Arbeitsblatt 12: Zusammenfassende Aufgaben zu den OSI-Schichten 3 und 4

Routing

Kenntnisse zum Ablauf des Routings sind wichtig, wenn mehrere Computernetze verbunden werden sollen. Im Beispiel unten sendet ein *Rechner X* aus dem *LAN A* Daten an einen *Rechner Y* im *LAN C*.
(Animation: .\251-materialien\animationen\routing1\routing1.htm)
Voraussetzung dafür ist,

- dass dem Rechner X (*MAC: 5*) die IP-Adresse des Rechners Y (*MAC: 6*) bekannt ist und
- der Rechner X die MAC-Adresse des Routers 1 (*MAC 1*) kennt.
- Der Quellrechner erstellt ein IP-Paket, das er in einem MAC-Frame an den Router 1 sendet:



Ziel:	Quelle:	
MAC 1	MAC 5	IP X | IP Y

- Der Router 1
  - prüft den Frame auf Fehler,
  - entfernt die MAC-Adresse,
  - ermittelt die IP-Zieladresse in der Routingtabelle.
- Besteht kein Eintrag, ermittelt der Router 1 über einen Rundruf die MAC-Adresse des Zielrechnersoder des nächsten Routers auf dem Weg zum Zielrechner.
- Dann packt der Router 1 das IP-Paket in einen neuen Datenframe, den er zum nächsten Netzknoten (Router 2) sendet. Die logischen IP-Adressen bleiben unverändert.

Ziel:	Quelle:	
MAC 2	MAC 1	IP X | IP Y

- Beim Router 2 wiederholt sich die Prozedur vom zweiten Schritt. Jeder Router verändert den Wert im Time to live (IPv4) bzw. Hop Limit (IPv6) – Feld. Zusätzlich muss ein Router noch überprüfen,
- ob sich der Zielrechner in demselben Netz (Subnetz) befindet – in diesem Fall wird der MAC-Frame geswitcht (Schicht 2)
- oder ob das IP-Paket geroutet werden muss (Schicht 3), weil sich der Zielrechner in einem anderen Netz befindet. Im Beispiel sendet der Router 2 einen MAC-Frame zum Router 3.

Ziel:	Quelle:	
MAC 3	MAC 2	IP X | IP Y

- Zu guter Letzt empfängt der Zielrechner den MAC-Frame, versehen mit der Quelladresse des letzten Routers und der Zieladresse des Rechners Y.

Im Nahverkehrsnetz enthalten Tabellen für mögliche Routen vor allem die Uhrzeit der Fahrten und Informationen zu Umsteigevorgängen.

Fahrtdaten

Fahrt	am	von	bis	Fahrtdauer	Umsteigen
1.	11.06.	09:40	10:12	00:32	1
2.	11.06.	09:57	10:21	00:24	1
3.	11.06.	10:10	10:41	00:31	1

Unterschiedliche Computernetze lassen sich wie Nahverkehrsnetze untereinander vernetzen.

- Informationen zur Weiterleitung von Daten zwischen unterschiedlichen Computernetzen werden in Routingtabellen gespeichert.

Routingtabellen in Computernetzen benötigen zwar keine Uhrzeiten, dafür aber die Information, über welchen weiteren Router die Zieladresse erreichbar ist:

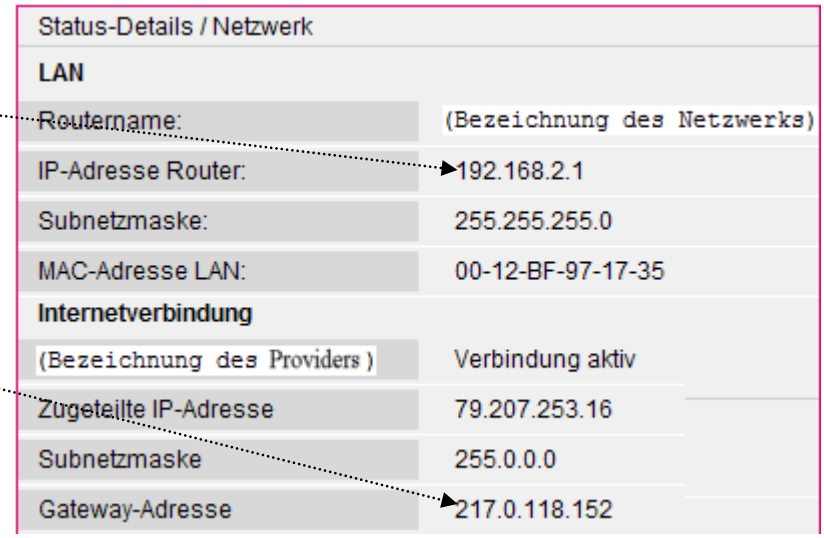
Netzadresse (Netzwerkziel)	Subnetzmaske (Netzwerkmaske)	Next Hop bzw. nächster Router (Gateway)	Metrik (Anzahl der Hops)

Bei Windows- und Unix-Rechnern kann die Routingtabelle des jeweiligen PC mit dem Befehl `netstat -r` angezeigt werden. Dazu ein Beispiel (IPv4):

```
C:\WINDOWS\system32\command.com
C:\>netstat -r

Routingtabelle
===========================================================================
Schnittstellenliste
0x1 ........................... MS TCP Loopback interface
0x2 ...00 13 ce 6a 64 11 ...... Intel(R) PRO/Wireless 2200BG Network Connection
- Paketplaner-Miniport
0x3 ...00 0f b0 a2 52 71 ...... Realtek RTL8139/810x Family Fast Ethernet NIC -
Paketplaner-Miniport
===========================================================================
===========================================================================
Aktive Routen:
     Netzwerkziel    Netzwerkmaske          Gateway   Schnittstelle  Anzahl
          0.0.0.0          0.0.0.0    192.168.2.1   192.168.2.102        25
        127.0.0.0        255.0.0.0      127.0.0.1       127.0.0.1         1
      192.168.2.0    255.255.255.0  192.168.2.102   192.168.2.102        25
    192.168.2.102  255.255.255.255      127.0.0.1       127.0.0.1        25
    192.168.2.255  255.255.255.255  192.168.2.102   192.168.2.102        25
        224.0.0.0        240.0.0.0  192.168.2.102   192.168.2.102        25
  255.255.255.255  255.255.255.255  192.168.2.102               3         1
  255.255.255.255  255.255.255.255  192.168.2.102   192.168.2.102         1
Standardgateway:       192.168.2.1
```

Der PC ist in dem Beispiel über einen „WLAN-Router“ mit dem Internet verbunden. IP-Pakete von diesem PC werden zunächst an die IP-Adresse weitergeleitet, unter der dieser WLAN-Router im lokalen Netz bekannt ist.
An diesem Beispiel erkennt man auch, warum man dabei nicht wirklich von einem Router sprechen kann:
Ein solches Gerät kennt nur die Adresse des Routers bei dem Internetanbieter. Daten werden dorthin gesendet bzw. von dort empfangen. Um die Weiterleitung der Daten im Internet kümmern sich die Router bei dem Provider.



A Bearbeite das Arbeitsblatt 13: Ablauf des Routings

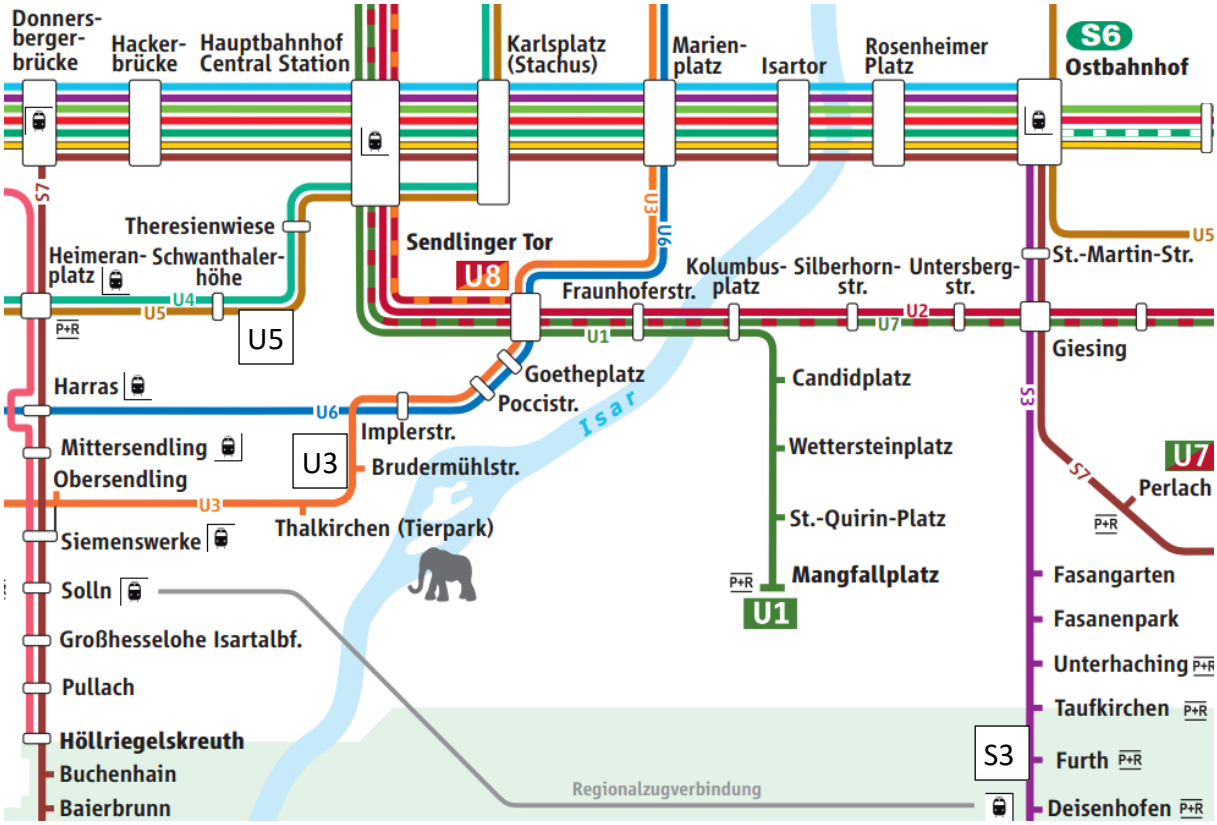
Netzwerkkategorien

Mit Hilfe des Routings lassen sich beliebig große Computernetze konfigurieren. Um einen Anhaltspunkt zur Größe eines Netzes zu erhalten, weden Netze nach ihrer Ausdehnung in Netzwerkkategorien klassifiziert:

- Ein **LAN** (Local Area Network) ist ein Computernetz, bei dem die Ausdehnung wesentlich kleiner ist als der Bereich einer Stadt. Ein LAN erstrecket sich meist über mehrere Räume, über Grundstücksgrenzen geht es aber selten hinaus. LANs werden innerhalb einer Institution verwendet, z. B. in einer Schule. Die Ausdehnung ist üblicherweise auf ca. 500 m beschränkt.
- **MAN**s (Metropolitan Area Network) sind Datennetze, die sich über mehrere Institutionen erstrecken. Aufbau und Verwaltung des Netzes bleibt im Prinzip unter eigener Kontrolle.
  Die Ausdehnung eines MAN liegt normalerweise unter 100 km.
- Ein **WAN** (Wide Area Network) verbindet unterschiedliche LANs verschiedener Unternehmen und Institutionen ohne geografische Beschränkung. Die Infrastruktur eines WAN wird von einem Dienstleister gesondert aufgebaut und gepflegt.

Vermaschte Struktur

Jetzt soll nicht nur die Topologie einzelner Linien des Nahverkehrsnetzes betrachtet werden, sondern im Prinzip das ganze Netz:



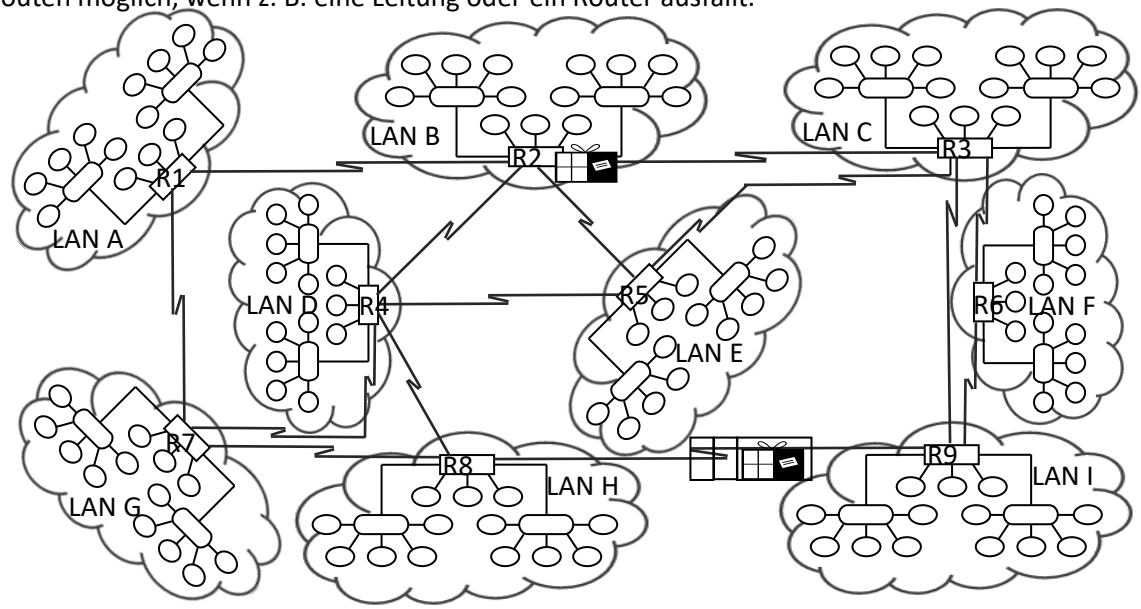
Mögliche Routen von der Haltestelle Deisenhofen zum Scheidplatz wären zum Beispiel:

Linie	*ab*	*an / ab*	*Linie*	*an / ab*	*an*	*umsteigen*
S3	*Deisenhofen*	*Marienplatz*	*U3*		*Scheidplatz*	*1*
S3	*Deisenhofen*	*Hauptbahnhof*	*U1*		*Scheidplatz*	*1*
Regionalzug	*Deisenhofen*	*Hauptbahnhof*	*U1*		*Scheidplatz*	*1*
S3	*Deisenhofen*	*Ostbahnhof*	*U5*	*Odeonsplatz*	*Scheidplatz*	*2*

- Die verschiedenen Netze sind untereinander und miteinander so vernetzt, dass Fahrten fast immer auf unterschiedlichen Routen möglich sind. Dabei werden Bus-, Stern- und Ringtopologien so vernetzt, dass eine vermaschte Struktur entsteht.

Der große Vorteil einer vermaschten Struktur ist, dass die Teilnehmer über viele unterschiedliche Wege erreichbar sind. Im Beispiel eines Nahverkehrsnetzes spielt es keine große Rolle, wenn Teilnetze ausfallen.
In Wirklichkeit gibt es neben U- und S-Bahn auch noch Straßenbahn und Bus. Die Linien all dieser öffentlichen Verkehrsmittel bilden ein komplexes Nahverkehrsnetz.

- Durch Routing ist die vermaschte Struktur auch in Computernetzen möglich.
  Das Prinzip des Routings in vermaschten Strukturen wird in der Flash-Animation *.\251-materialien\animationen\prinzipien\paketisierung.swf* aufgezeigt.
  Jeder Router hat eine MAC-Adresse und benötigt eine IP-Adresse. IP-Pakete können wie im vorigen Kapitel beschrieben zwischen verschiedenen lokalen Netzen geroutet werden. Durch die vermaschte Struktur sind unterschiedliche Routen möglich, wenn z. B. eine Leitung oder ein Router ausfällt.



  Simulation dazu vgl. .\251-materialien\animationen\routing2\routing2.htm
  Kollisionen können natürlich keine auftreten, weil für den Hin- und den Rückweg unterschiedliche Leitungen verwendet werden.
  Router arbeiten wie Switches üblicherweise mit dem Store-and-Forward-Verfahren. Sie speichern also IP-Pakete zwischen, die im Augenblick nicht gesendet werden können.

- Bearbeite das Arbeitsblatt 14: Routing in vermaschten Strukturen