KOMMUNIKATION IN RECHNERNETZEN

HINTERGRUND ZUM UNTERRICHTSGANG

Thomas Schaller – E-Mail: t.schaller@gymnasium.ettenheim.de. – Februar 2018

Inhaltsverzeichnis

Einleitung

Bis in die späten sechziger Jahre hinein war jeder Computer eine in sich abgeschlossene Datenwelt. Man konnte seine Programme auf der Maschine seines Rechenzentrums laufen lassen, aber nicht seine Daten über eine elektrische Verbindung an einen anderen Computer oder gar ein anderes Rechenzentrum übertragen. Dann kam die Datenfernübertragung, mit der es möglich wurde, von einem Ein-Ausgabe-Gerät, das weit entfernt vom Rechner steht (womöglich in einem anderen Kontinent), über Telefonverbindungen mit dem Rechner zu kommunizieren: Daten in ihn einzugeben und Ergebnisse von ihm zurückzubekommen. Diese Technik ist auch heute noch in vollem Einsatz, wie man beim Bezahlen mit EC-Karten feststellen kann (es wird meist vor dem Bezahlen eine Telefonverbindung mit der Bank aufgebaut).

Wenn aber ein Rechner und ein Mensch (durch ein entfernt stehendes Ein-Ausgabe Gerät) auf diese Weise kommunizieren können, warum sollen es nicht auch zwei Rechner miteinander können? Und wenn es zwei können, dann müssten es doch auch zehn oder fünfzig können. Es entstand die Idee, mehrere Rechner über ein Verbindungsnetz so zusammenzuschalten, dass sie ein Rechnernetz bilden.

Seit den achtziger Jahren hat die Vernetzung der Computer einen unaufhaltsamen Siegeszug angetreten. Das ARPA-Net startete mit wenigen Rechnern. Schon 1985 waren es 2000 Rechner, 1990 über 300000, 2000 über 100 Millionen und 2013 etwa 1 Milliarde. Heutzutage sind Computernetze aus dem täglichen Leben nicht mehr wegzudenken. Neben Computern sind auch Handys, Fernseher, sogar Heizungen und vieles mehr an das Internet - das größte Computernetz - angeschlossen.

Was aber ist ein Rechnernetz genau? Wie sind solche Netze aufgebaut? Wie kommunizieren die Rechner miteinander? Wie anfällig sind solche Netze? Welchen Vorteil bringen sie und welche Gefahren können von ihnen ausgehen?

Nutzen eines Computernetzes

In einem Computernetz werden verschiedene eigenständige Geräte miteinander verbunden. Der Aufwand lohnt sich aber nur dann, wenn der Benutzer daraus einen Nutzen ziehen kann.

Man kann beispielsweise Drucker, Scanner oder externe Festplatten mit mehreren anderen Rechnern gemeinsam nutzen. Das senkt die Kosten und reduziert die Wartungsarbeiten. Eine Familie mit mehreren Rechnern kommt in aller Regel mit einem Drucker aus (gemeinsame Nutzung von Ressourcen). Ein solcher Netzdrucker kann darüber hinaus noch so eingerichtet werden, dass der 11-jährige Sprössling zum Beispiel maximal 100 Seiten pro Monat drucken darf (Verwaltung von Benutzerrechten).

Im Schulnetz ist es von Vorteil, wenn man auf seine Dokumente zugreifen kann, egal an welchem Rechner man arbeitet (gemeinsamer Fileserver). Im weltweiten Internet können alle Benutzer auf die zur Verfügung gestellten Dienste wie Webserver, Mailserver oder ähnliches zugreifen.

Die Grenzen zwischen lokalem Rechner und Rechnern im einem Netzwerk oder sogar im Internet verschwinden zunehmend. Bei der Benutzung von Laufwerken ist es kaum noch ersichtlich, auf welchem Rechner die Dateien gespeichert werden. Sogar Cloud-Speicher können als Unterordner in das eigene Dateisystem eingebunden werden. Das macht die verantwortungsvolle Nutzung dieser Dienste notwendig und setzt ein Verständnis für die Hintergründe voraus.

Ablauf der Kommunikation

Spätestens nachdem man sich über die Vorteile eines Rechnernetzes einig geworden ist, muss man die Frage beantworten, auf welche Weise die Rechner eigentlich miteinander kommunizieren sollen.

Im Alltag machen wir uns selten Gedanken darüber, was eigentlich die Voraussetzungen für eine erfolgreiche Kommunikation sind: wir reden einfach miteinander. Wenn wir aber verstehen wollen, wie Computer untereinander Informationen austauschen, dann müssen wir den Vorgang des Informationsaustauschs etwas genauer analysieren. Speziell müssen wir alle Voraussetzungen wegdenken, die zwar für die menschliche Kommunikation selbstverständlich sind, für die Computerkommunikation aber nicht zutreffen.

Kommunikationsmedium

Bei einem Gespräch zwischen Menschen ist die Luft die Überträgerin des Schalls. Welche Übertragungsmedien gibt es für Computer? Denkbar sind elektrische Kabel, Lichtwellenleiter, Funkverbindungen usw.

Ablauf des Kommunikationsprozesses

Der nächste zu klärende Punkt betrifft den Ablauf der Kommunikation: bei einem Telefongespräch kann immer nur einer der beiden Teilnehmer reden, der andere muss zuhören. Es ist also der eine der Sender der Information, der andere der Empfänger. Und natürlich gehört es zum guten Ton, dass die Rollen nach zumutbaren Zeitabschnitten getauscht werden. Beim Telefongespräch ergeben sich die Gelegenheiten für den Rollentausch sozusagen automatisch, z.B. dadurch, dass der momentane "Sender" eine Frage stellt oder eine Pause macht.

Schwieriger zu organisieren ist eine Kommunikation zwischen vielen Teilnehmern. Wenn wir Wert darauf legen, dass nach dem Ende der "Kommunikationssitzung" alle Teilnehmer über alle Informationen verfügen, die während der Sitzung genannt wurden, dann muss zumindest gewährleistet sein, dass stets nur einer der Teilnehmer spricht und alle anderen zuhören müssen! So sollte Schulunterricht eigentlich ablaufen... Wenn hingegen z.B. bei der Generalversammlung eines Vereins alle anwesenden Mitglieder dauernd munter durcheinanderreden, wird am Ende der Veranstaltung keiner der Anwesenden einen Überblick darüber haben, welche Argumente es für die vorgeschlagene Satzungsänderung gibt.

Für die Computerkommunikation muss man Vereinbarungen (=Protokolle) treffen, die die Regeln der Kommunikation genau festlegen.

Übertragungssicherheit

Woher weiß ich, ob die Information, die ich abgeschickt habe, auch unverfälscht beim Empfänger ankommt? Um im Bild sich unterhaltender Menschen zu bleiben: Bei Spielen von „stiller Post“ wird eine Nachricht von einer Person zur nächsten weiter geflüstert. Dabei kann es durchaus vorkommen, dass aus „Ich habe keinen Bock“ „Ich habe keinen Rock“ wird...

Diese Fehler können sowohl unabsichtlich sein als auch bewusst herbeigeführt. Vielleicht hat eine der Personen in der Reihe die Nachricht ausgetauscht. Außerdem besteht noch das Problem, dass man nicht bei jeder Nachricht möchte, dass alle Personen dazwischen die Nachricht erfahren. Und wer sagt, dass die Nachricht wirklich von der Person kommt, die angeblich der Absender ist?

Dies sind Probleme, die von der Kryptologie behandelt werden. Wie werden Nachrichten verschlüsselt oder signiert?

Bestandteile eines Netzwerks

Wikipedia definiert Rechnernetze so:

> „Ein Rechnernetz ist ein Zusammenschluss von verschiedenen technischen, primär selbstständigen elektronischen Systemen (insbesondere Computern, aber auch Sensoren, Aktoren, Funktechnologischen Komponenten usw.), der die Kommunikation der einzelnen Systeme untereinander ermöglicht.“[1]

Computernetze bestehen also üblicherweise aus Geräten (PCs, Laptops, Drucker, usw.), die mit Kabeln über Switches (=Gerät mit vielen Netzwerkanschlüssen, das Daten an die angeschlossenen Geräte innerhalb eines Netzwerks weiterleiten kann) verbunden sind, können aber auch andere Komponenten enthalten. Früher gab es neben Switches auch Hubs[2], die die Daten im Gegensatz zum Switch immer an alle angeschlossenen Geräte weitergeleitet haben.

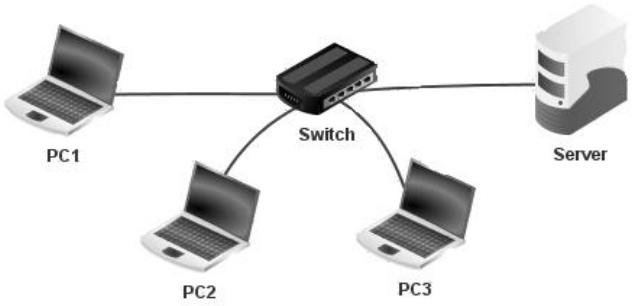


Bild "Lokales Netz", Schaller. Erstellt mit Filius-Netzwerksimulation, URL: http://www.lernsoftware-filius.de (November 2016)

Natürlich können statt Kabel auch WLAN-Funkverbindungen zum Einsatz kommen. Die in einem Netz verbundenen Rechner heißen

Netzknoten oder kurz **Knoten**. Ein derartiges Netzwerk (z.B. von einer Schule oder einer Firma) wird als Local Area Network (LAN) bezeichnet.

Ein spezieller Computer, der als Server fungiert, ist dabei nicht notwendig. Genau genommen kann jeder Computer spezielle Dienste bereitstellen (z.B. Dateien für die anderen Computer speichern). Diese Dienste werden als Server-Programme bezeichnet. Leider wird oft auch der Computer, der viele Server-Dienste bereitstellt, als Server bezeichnet. Dies trägt zur Verwirrung bei.

Topologie des Netzes

Wenn viele Geräte miteinander verbunden werden sollen, stellt sich die Frage, wie diese miteinander zu verbinden sind. Es geht hier nicht darum, ob mit oder ohne Kabel verbunden wird, sondern um einen rein topologischen (=die Anordnung im Raum betreffenden) Sachverhalt.

48-Port Switch

Bild „2550T-PWR-Front.jpg“, von Geek2003 [CC BY-SA 3.0 (https://creativecommons.org/licenses/by-sa/3.0)], via Wikimedia Commons (https://commons.wikimedia.org/wiki/File:2550T-PWR-Front.jpg) (abgerufen: Januar 2018)

1 Siehe Seite „Rechnernetz“. URL: https://de.wikipedia.org/wiki/Rechnernetz (abgerufen: 3. Mai 2018)

2 Dieses Verfahren wird noch bei USB-Hubs angewendet, die es ermöglichen mehrere USB-Geräte an einen einzigen USB-Port anzuschließen.

Es gibt folgende Netzwerk-Topologien:

Stern-Topologie

In der Stern-Topologie[3] unterhält eine zentrale Station die Verbindungen zu allen anderen Stationen. Jede Station ist über eine eigene physikalische Leitung an die zentrale Station angebunden. Es handelt sich im Regelfall um einen Switch, der die Verteilerfunktion für die Datenpakete übernimmt.

In vielen Haushalten steht ein Router, der vom Provider geliefert wird. Dieser erfüllt neben der Anbindung an das Internet die Funktion des zentralen Switches, an den die Endgeräte per Kabel oder WLAN angeschlossen sind.

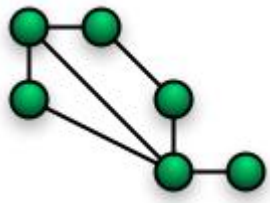
Baum-Topologie

Die Baum-Topologie ist eine erweiterte Stern-Topologie. Größere Netze nehmen eine solche Struktur an. An der Wurzel und jeder Verästelung befinden sich Switches. Dabei ist die Netzwerklast an der Wurzel des Baumes am höchsten. Dort muss ein leistungsfähiger Switch verwendet werden.

In den meisten Schulen wird diese Topologie verwendet. Der zentrale Server ist dabei direkt an der Wurzel des Baums angebunden. Von dort gehen Leitungen in die einzelnen Gebäude. Innerhalb dieser Gebäude werden die einzelnen Netzwerkanschlüsse über weitere Switches angeschlossen.

Vermaschte Topologie

In der vermaschten Topologie sind die einzelnen Knoten über mehrere Wege miteinander verbunden. Dadurch bleibt dieses Netz auch bei Ausfall einzelner Leitungen oder Knoten funktionsfähig.



Das Internet ist in weiten Teilen ein vermaschtes Netz. Es ist daher gegen den Ausfall einzelner Komponenten gesichert. Trotzdem gibt es "Hauptverkehrsadern" (die Backbone-Leitungen). Die Router an diesen Backbone-Leitungen sind für Abhöraktionen besonders interessant. Die einzelnen Knoten stellen dabei die Schnittstellen (Router) zu den lokalen Netzwerken dar, die in einer eigenen Topologie realisiert sind.

Geschwindigkeit der Datenübertragung

Bei der Planung eines Netzwerks spielt der erforderliche Datendurchsatz eine große Rolle. Neben der Topologie des Netzes ist dabei die Datenübertragungsgeschwindigkeit entscheidend. In vielen Werbebroschüren der Netzwerkprovider wird vor allem mit hohen Übertragungsgeschwindigkeiten geworben.

Normale Netzwerkkabel und Switches sind heute auf einen Datendurchsatz von 100 MBit/s (Megabit pro Sekunde) oder 1 GBit/s (Gigabit pro Sekunde) ausgelegt. Das entspricht 12,5 Megabyte/s, bzw. 125 Megabyte/s. Mit 100 MBit lässt sich ein Digitalbild hoher Auflösung in 0,25s oder ein Film (1,8 Gbyte) in 2,5min übertragen, wenn die volle Bandbreite zur Verfügung steht.

VDSL wird zurzeit (Januar 2018) mit einer Geschwindigkeit von max. 100 Mbit/s angeboten. Auch Funknetze bieten mit LTE (4G) heutzutage bis zu 100 MBit/s. Internet Backbones arbeiten mit 10 GBit/s bis max. 1 TBit/s. (vgl. Topologie des Baden-Württembergischen Forschungsnetzes Belwue, an das die meisten Schulen angeschlossen sind[4]).

3 Bilder „NetworkTopologies.png“, Foobaz. URL: *http://commons.wikimedia.org/wiki/File:NetworkTopologies.png* (Lizenz: gemeinfrei) (abgerufen: 4. Januar 2017)

4 Siehe Seite „Topologie des Baden-Württembergischen Forschungsnetz“. URL:

Anschluss an das Internet mittels Router

Im Gegensatz zu den Local Area Networks (LAN) ist das Internet ein globales, räumlich nicht beschränktes Netzwerk (WAN – Wide Area Network). Es entsteht durch die Verbindung vieler lokaler Netze. Um ein LAN an das Internet anzuschließen, ist ein Router erforderlich.

Dieser hat mehrere Netzwerkkarten. Jede dieser Netzwerkkarten ist dann Teil eines lokalen Netzwerks. Die Router sorgen dafür, dass der Datenaustausch zwischen diesen lokalen Netzwerken funktioniert. Die Router für Heimnetzwerke erfüllen meistens aber noch weitere Funktionen, die die eigentliche Routing-Funktion verschleiern:

- **VDSL-Modem:** Die Daten werden per VDSL an den Provider geschickt. Der private Router übernimmt das Versenden der Daten im VDSL-Format.
- **Switch:** Die meisten Router haben mehrere Netzwerkanschlüsse, um mehrere private Computer anschließen zu können. Oft ist auch noch eine WLAN-Funktionalität eingebaut. Dadurch spart man sich den Kauf eines separaten Switches.
- **DHCP-Server:** Der Router übernimmt die Konfiguration der Netzwerkkarten der privaten PCs, damit die User sich nicht darum kümmern müssen (die würden es in vielen Fällen auch gar nicht können...).
- **Firewall:** In der Regel ist eine Firewall in den Router integriert, die den Datenverkehr aus dem Internet in das private Netzwerk kontrolliert.
- **Network Adress Translation (NAT):** Der Internetprovider gibt uns für eine beschränkte Zeit eine IP-Adresse. Trotzdem können mehrere PCs gleichzeitig ins Internet gehen, da der Router die IP-Adresse des PCs bei Anfragen ins Internet gegen seine eigene ersetzt und dafür sorgt, dass die Antwort aus dem Internet an den richtigen PC weitergegeben wird.

Adressierung

MAC-Adressen

Damit jeder einzelne Rechner in einem Computernetz direkt angesprochen werden kann, muss er eindeutig gekennzeichnet sein. Solch ein individuelles Kennzeichen lässt sich leider nicht auf einfachem Wege aus der Hardware des Rechners ableiten: in früheren Zeiten wurde z.B. versucht, jede Netzwerkkarte durch eine eindeutige Nummer zu identifizieren. Diese Nummer wurde bei der Herstellung der Netzwerkkarte in einen ROM-Baustein auf der Karte "eingebrannt", und jedes Exemplar einer Netzwerkkarte sollte seine individuelle "MAC-Adresse" (**M**edia **A**ccess **C**ontrol Address) bekommen.

In alten "IPX/SPX-Netzen" wurden diese MAC-Nummern zur Identifikation der einzelnen Rechner eingesetzt. Recht bald tauchten aber Netzwerkkarten mit gleichen MAC-Adressen am Markt auf, was zu erheblichen Problemen in den Netzen führt. Daher werden die MAC-Adressen für den weltweiten Datenaustausch nicht mehr verwendet. Stattdessen kommen dort die IP-Adressen zum Einsatz. Nach wie vor werden aber die MAC-Adressen von den Netzwerkkarten für die Adressierung der Rechner im lokalen Netz genutzt. Bei einigen Funktionen im Netzwerk (z.B. Wake-On-Lan) muss auch der Benutzer die MAC-Adresse der Netzwerkkarte kennen. Daher muss sichergestellt sein, dass keine doppelten MAC-Adressen im Netzwerk existieren. Aber die MAC-Adressen müssen nicht mehr weltweit eindeutig sein.

http://www.belwue.de/fileadmin/belwue/topologie_bilder/2015-10-GESAMT.pdf (abgerufen: Mai 2018)

IP-Adressen

Jedes Haus braucht eine Adresse, damit der Briefträger die Post zustellen kann. Genauso braucht jeder Rechner eine Adresse: die IP-Adresse. Das Internet verwendet das "TCP/IP-Protokoll" (IPv4, zunehmend auch die neuere Version IPv6). Hier interessiert zunächst nur die dabei verwendete "IP-Adresse" (**I**nternet **P**rotocol - Adresse), welche nichts weiter ist als eine vier Byte lange Zahl, z.B.:

$$\text{IP-Adresse: } 192.168.123.137 = 11000000.10101000.01111011.10001001_b$$

An jeder der vier durch Punkte getrennten Stellen kann also eine ganze Zahl zwischen 0 und 255 stehen. Damit ist auch schon klar, wie viele Rechner es maximal im Internet geben darf, nämlich

$$(2^8)^4 = 2^{32} = 4\ 294\ 967\ 296.$$

Einige dieser Adressen sind für Spezialaufgaben reserviert und fallen daher für die Rechner-Kennzeichnung aus, sodass wir mit etwa 4 Milliarden IP-Adressen im Internet auskommen müssen. Daher sind die zur Verfügung stehenden Adressen bei IPv4 inzwischen nahezu verbraucht.

Ernste Befürchtungen, dass der IP-Adressraum schon sehr kurzfristig ausgehen könnte, wurden Anfang der neunziger Jahre des 20. Jahrhunderts laut. Der Internet-Boom setzte gerade ein und es entstand in kürzester Zeit weltweit ein riesiger Bedarf an IP-Adressen für Internet-Zugänge und Webserver. Hochrechnungen über den rasant wachsenden Bedarf ergaben einen Verbrauch aller bis dato freien IP-Adressen bis zum Jahr 1995.

Das Problem durch die beiden Hauptverursacher des steigenden Bedarfs an IP-Adressen, Internet-Zugänge und Webserver, wurde in kürzester Zeit durch neue Techniken entschärft: Für Internet-Zugänge wurde die **Network Address Translation** (siehe weiter unten) eingeführt und dem World Wide Web wurde eine überarbeitete Version des HTTP-Protokolls mit der Versionsnummer 1.1 verpasst, die so genannte **virtuelle Webserver** ermöglichte, also die Möglichkeit, auf einer IP-Adresse mehrere Webseiten mit unterschiedlichen Domain-Namen gleichzeitig betreiben zu können[5].

Der Bedarf an IP-Adressen ist zwar weiterhin steigend, jedoch bei weitem nicht mehr so drastisch wie in den neunziger Jahren. Zudem unterliegt heutzutage die Vergabe von IP-Adressen durch die **R**egional **I**nternet **R**egistries (RIR) recht strengen Vergaberichtlinien. Dennoch: Durch ungeschickte Vergabe von Adressbereichen (die University of California in Berkeley beispielsweise bekam 16,8 Millionen(!) IP-Adressen zugestanden) liegen große Bereiche des Adressraums brach. Eine Neuordnung wäre zwar theoretisch denkbar, die Fachwelt hält sie jedoch für nicht praktikabel.

Der langsam ausgehende Adressraum war nicht der einzige Grund, weshalb man sich ab 1995 daran setzte, die bisherige IP-Version (IPv4) aus den 70er Jahren durch den neuen Standard IPv6 zu ersetzen.

- **Größerer Adressraum** - IPv6 verwendet 16 Byte pro Adresse statt der bisher üblichen 4 Byte. Eine IPv6-Adresse sähe dann in Hexadezimaldarstellung zum Beispiel so aus:

  4003:0dc8:15a6:08d4:2319:3b2a:0040:3221

  •

  Es gibt dann $(2^8)^{16} = 2^{128} = 3{,}4 \cdot 10^{38} = 340$ Sextillionen Adressen. Kein Mensch weiß, was 340 Sextillionen sind! Drücken wir es daher etwas anders aus: Jedem Quadratmillimeter

5 Siehe Seite „IPv4“. URL: *http://de.wikipedia.org/w/index.php?title=IPv4&oldid=81059097* (abgerufen: Januar 2018)

der Erde inklusive Ozeane stehen dann 600 Billiarden Adressen zu! Das sollte für die Kühlschränke reichen.... IPv6 bietet damit genügend Möglichkeiten, um jedes Gerät im bestehenden und zukünftigen Internet mit einer eigenen, global gültigen Adresse auszustatten.

Durch die eindeutige Zuordnung des Interface-Identifiers zu einem Gerät geht allerdings die Anonymität im Internet verloren. Daher wurden die Privacy-Extensions[6] eingeführt, die regeln, dass sowohl der Interface-Identifier als auch das vom Provider zugewiesene Präfix regelmäßig wechseln sollen.

- **Netzwerksicherheit** - IPv6 integriert das IPsec Protokoll in den IP-Standard und ermöglicht dadurch eine erhöhte Netzwerksicherheit. IPsec stellt sicher, dass die versendeten Datenpakete vertraulich und authentifiziert sind. Zum Schlüsseltausch wird dabei das Diffie-Hellman-Verfahren verwendet.
- **Multicast** - Es ist möglich, Datenpakete nicht nur an einen oder alle Netzwerkteilnehmer zu senden, sondern auch an eine ausgewählte Teilmenge.
- **Effizienteres Routing** - Durch den überarbeiten IPv6-Header und das neue Adressierungsschema, das eine hierarchische Routing-Infrastruktur unterstützt, können IPv6-Router den entsprechenden Netzwerkverkehr schneller weiterleiten.

Verwaltung der Adressierung

Ein Problem der Adressierung ist die Verwaltung. Wer teilt IP-Adressen zu? Wer entscheidet über die Vergabe solcher Adressen? Wer bestimmt, nach welchen Kriterien die Zuteilung erfolgt?

Bis Anfang der 90er Jahre wurde dies alles vom **InterNIC** (= **Inter**net **N**etwork **I**nformation **C**enter) geleistet. Eine solche Zentralisierung birgt aber immer auch die Gefahr, dass die Institution träge und undurchschaubar wird. So auch beim InterNIC. Man beschloss daher, die Verwaltung für bestimmte Kontinente an eigenständige Institutionen zu übergeben. Außerdem wurden darüber hinaus damaligen Großunternehmungen eigene IP-Adressräume zugewiesen. So konnten diese Institutionen und Großunternehmungen ihre zugewiesenen IP-Adressräume autark verwalten.

IPv4:

Um IP-Adressräume dezentral verwalten zu können, wurde eine logische Aufteilung des IP-Adressraums notwendig. Diese logische Aufteilung wurde mit den so genannten Netzwerkklassen realisiert, mit denen auf diese Weise verschieden große Netzwerke gebildet wurden. Die eigentliche IP-Adresse wurde aufgeteilt in einen Netzteil und einen Hostteil.

Der Netzteil entspricht sozusagen der Adresse des Netzes, der Hostteil gibt einen bestimmten Rechner in diesem Netz an. Der Netzteil wird zentral von der IANA[7] verwaltet, der Hostteil darf vom Eigentümer eines Netzes frei an seine Rechner vergeben werden.

Dabei war diese Aufteilung standardisiert, es gab drei (später ein paar mehr) Netzklassen:

- Klasse A - Netze: Präfix 0.. , zusätzlich 7 Bit Netzteil, 24 Bit Hostteil
- Klasse B - Netze: Präfix 10.., zusätzlich 14 Bit Netzteil, 16 Bit Hostteil
- Klasse C - Netze: Präfix 110..., zusätzlich 21 Bit Netzteil, 8 Bit Hostteil

6 Privacy-Extensions (PEX, RFC 4911), https://tools.ietf.org/html/rfc4941 (abgerufen: Februar 2018)
7 IANA (Internet Assigned Numbers Authority), *http://www.iana.org/* (abgerufen: Dez. 2010)

Beispiel:

IP-Adresse:	192.168.123.137	
	= $11000000.10101000.1111011.10001001_b$	
Präfix (die ersten 3 Bits):	110	=> Klasse C Netz
Netzteil (insgesamt 24 Bit):	11000000.10101000.1111011	(von IANA vergeben)
Hostteil (8 Bit):	10001001	(vom Netzbetreiber vergeben)

Um die Nachteile der festen Netzklassen zu umgehen, wurde 1993 das Classless Inter-Domain Routing, kurz CIDR eingeführt. Mit CIDR entfällt die feste Zuordnung einer IP-Adresse zu einer Netzklasse. Es existiert jetzt eine Netzmaske (Subnet-Mask), welche die IP-Adresse in den Netzwerk- und Hostteil aufteilt. Dabei muss die Subnet-Mask mit Einsen beginnen und mit Nullen enden. Die Netzadresse ergibt sich dann durch eine bitweise UND-Verknüpfung[8] der IP-Adresse und der Subnet-Mask.

IP-Adresse	192.168.123.137	=	11000000 . 10101000 . 01111011 . 10001001
+ Subnetz-Maske	255.255.255.000	=	111111111 . 111111111 . 11111111 . 00000000
Netzwerk-Kennung	192.168.123.000	=	11000000 . 10101000 . 01111011 . 00000000
Computer-Kennung	137	=	10001001

Es ist dabei nicht notwendig (wenn auch häufig üblich), dass die Einsen am Ende eines Bytes enden. Der Wechsel zu den Nullen kann auch mitten im Byte liegen.

IP-Adresse	138.163.168.169	=	10001010 . 10100011 . 10101000 . 10101001
+ Subnetz-Maske	255.255.192.000	=	111111111 . 111111111 . 11000000 . 00000000
Netzwerk-Kennung	138.163.128.000	=	10001010 . 10100011 . 10000000 . 00000000
Computer-Kennung	40.169	=	101000 . 10101001

Ein Computernetzbetreiber bekommt nun also eine Netzwerkkennung und eine Subnetz-Maske von der IANA zugeteilt. Er kann dann die Computerkennungen seiner Rechner aus dem vorgegebenen Bereich frei wählen und erhält durch Kombination mit der Netzwerk-Kennung die IP-Adresse der Rechner. Je mehr Nullen die Subnetzmaske enthält, desto mehr Computerkennungen stehen dem Betreiber zur Verfügung (genau $2^{\text{Anzahl der Nullen}}$).

Im ersten Beispiel können die Computerkennungen von 0 bis 255 vergeben werden und man erhält die IP-Adressen von 192.168.123.0 - 192.168.123.255. Im zweiten Beispiel sind die Kennungen von 0.0 bis 63.255 möglich. Daraus ergeben sich dann die IP-Adressen von 138.163.128.0 – 138.163.191.255.

IPv6

Bei IPv6 ist das Verfahren sehr ähnlich. Eine IPv6-Adresse besteht aus 128 Bit (= 16 Byte). Die ersten 64 Bit bilden dabei den Präfix, die zweiten 64 Bit den Interface-Identifier, der das Gerät identifiziert. Dieser Interface-Identifier wird auch bei wechselnden Präfixen verwendet. Dadurch ist es möglich, dass ein Gerät mehrere IPv6-Adressen hat oder problemlos bei einem Wechsel des Netzes wiedererkannt werden kann (z.B. für mobile Endgeräte, die während eines Kommunikationsvorgangs zwischen WLAN-Netzen wechseln).

Der Präfix wird vom Provider vergeben. Der Provider selbst bekommt von der RIR einen

8 Bitweises UND: 1 + 1 = 1; 0 + 1 = 0; 1 + 0 = 0; 0 + 0 = 0

Adressbereich zugewiesen, in dem z.B. die ersten 32 Bit festgelegt sind. Er gibt dann einen kleineren Adressbereich an seine Kunden weiter.

Hat z. B. ein Netzwerkgerät die IPv6-Adresse

`2001:0db8:85a3:08d3:1319:8a2e:0370:7347`

so lautet das Präfix

`2001:0db8:85a3:08d3:`

und der Interface-Identifier

`1319:8a2e:0370:7347`.

Der Provider bekam von der *RIR* wahrscheinlich das Netz

`2001:0db8/32`

zugewiesen und der Endkunde vom Provider möglicherweise das Netz

`2001:0db8:85a3:0800/56`

Die Angabe nach dem Querstrich entspricht der Subnet-Mask von IPv4. Sie legt fest, wie viele Bits am Anfang der Adresse unveränderlich sind.

Ermitteln der Netzwerkkonfiguration

Die IP-Adresse und die Subnet-Mask eines Rechners mit Windows-Betriebssystem lassen sich leicht ermitteln. Öffnen Sie dazu ein DOS-Fenster (wählen Sie dazu im "Start-Menü" die "Eingabe-Aufforderung", oder geben Sie im "Ausführen"-Fenster "cmd" [ohne die Anführungszeichen] ein) und tippen Sie den Befehl

ipconfig –all

ein. Dann verrät Ihnen Windows die IP-Adresse dieses Rechners und noch vieles mehr. Sie sehen auch, dass Ihr Rechner vermutlich sowohl eine IPv4 als auch eine IPv6 Adresse hat. Die Bedeutung einiger der angegebenen Werte wird im Folgenden noch erklärt.

Vergleicht man in einem Netzwerk die IP-Adressen, kann man sehen, dass sie im Netzteil übereinstimmen und sich im Hostteil unterscheiden. Die Subnet-Mask (IPv4) muss bei allen Rechnern gleich sein.

Mit Hilfe der IP-Adresse kann man einen ersten Kontakt zum Nachbar-Rechner herstellen. Ein elementares Diagnose-Werkzeug für Netzwerker ist das Programm ***ping*****,** das den Informations-Kanal zu einem angegebenen Zielrechner testet. Dazu schickt das Programm eine Nachricht an den angegebenen Zielrechner und fordert ihn auf, zu antworten. Die Zeitdauer bis zum Eintreffen der Antwort und die Verlustrate der Pakete ist ein Maß für die Qualität der Verbindung: je kürzer die Antwortzeit und je weniger Paketverluste auftreten, desto schneller (d.h. "besser") ist die Verbindung.

z.B. ping 137.166.4.30 (Seite in Australien)

```
Ping wird ausgeführt für 137.166.4.30 mit 32 Bytes Daten:

Antwort von 137.166.4.30: Bytes=32 Zeit=511ms TTL=105
Antwort von 137.166.4.30: Bytes=32 Zeit=509ms TTL=105
Antwort von 137.166.4.30: Bytes=32 Zeit=512ms TTL=105
Antwort von 137.166.4.30: Bytes=32 Zeit=520ms TTL=104

Ping-Statistik für 137.166.4.30:  Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
Ca. Zeitangaben in Millisek.:  Minimum = 509ms, Maximum = 520ms, Mittelwert = 513ms
```

Dieser Computer ist mit einer guten Leitungsqualität (0% Verlust) aber einer recht langsamen Verbindung (0,5 sek) angebunden. Der Computer steht aber auf der anderen Seite der Welt. Für 40000 km sind 0,5 sek doch gar nicht so schlecht.

Ein Server, der zumindest ein Datenpaket als empfangen meldet, ist online. Hohe Antwortzeiten

bzw. verlorene Datenpakte deuten darauf hin, dass der Server aktuell überlastet oder die Leitung sehr schlecht ist.

In manchen Netzen wird der ping-Befehl bei Zugriffen auf externe Rechner nicht funktionieren: Wenn das lokale Netz durch eine entsprechend konfigurierte "Firewall" geschützt ist, wird ihre Anfrage durch die Firewall abgefangen. In diesem Fall liefert Ihnen das ping-Programm eine "Zeitüberschreitung".

Dynamische und statische IP-Adressen

Wenn man beim Booten von Computern etwas genauer hinsieht, kann man in vielen Netzwerken feststellen, dass wenige Sekunden nach dem Einschalten folgende Zeile einige Sekunden mit blinkendem Cursor stehen bleibt: „DHCP.....“

In diesem Moment wurde dem Computer eine IP verpasst. (Wie Sie diese herausfinden können, haben Sie oben gelernt.) Beim nächsten Bootvorgang wird dem Rechner erneut eine IP gegeben, aber nicht unbedingt dieselbe. Die IP ist also nicht statisch, sondern **dynamisch**. Zuständig hierfür ist ein Dienst, der auf dem Router oder Server läuft, das so genannte DHCP:

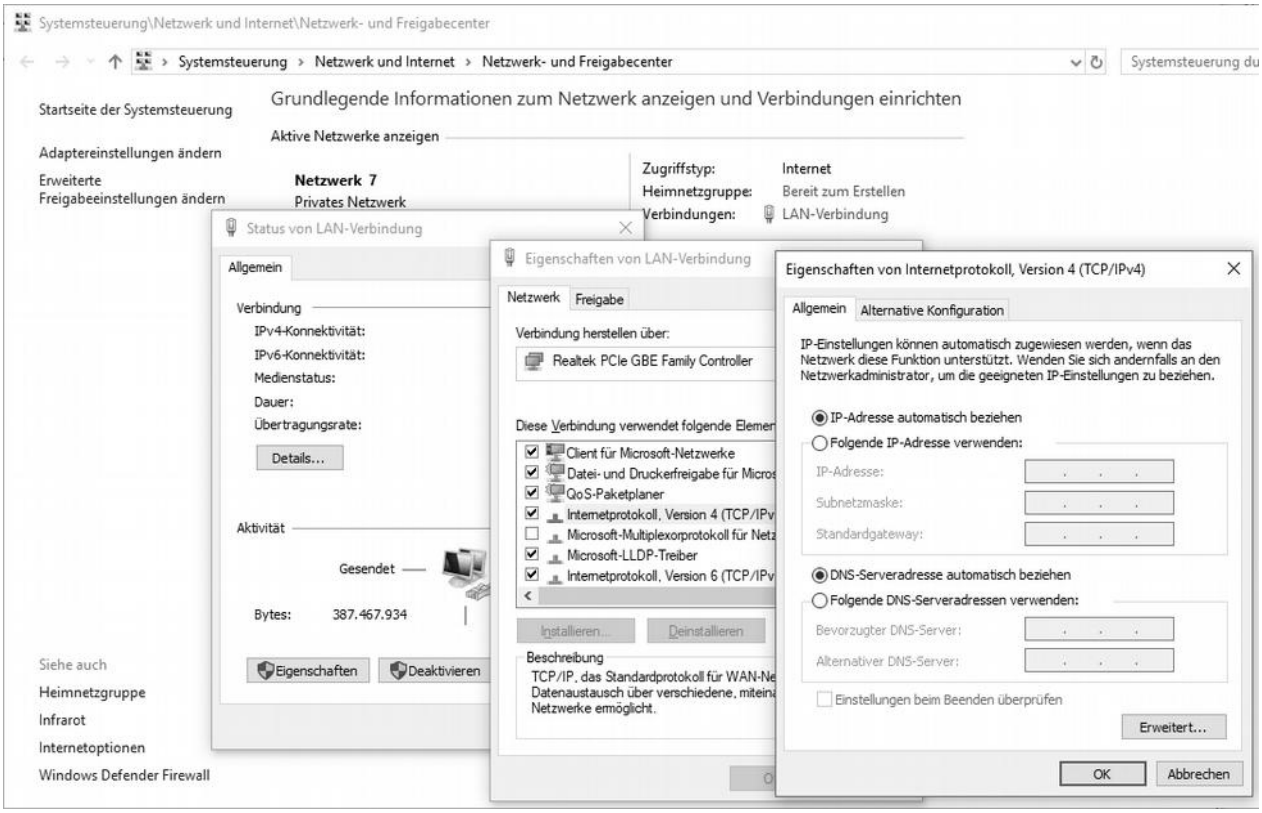


Abbildung: Konfiguration der IP-Einstellungen bei Windows 10.

Das **DHCP** (**D**ynamic **H**ost **C**onfiguration **P**rotocol) ermöglicht mit Hilfe eines entsprechenden Servers die dynamische Zuweisung einer IP-Adresse und weiterer Konfigurationsparameter (Subnet-Mask, DNS-Server, Gateway) an Computer in einem Netzwerk. Durch DHCP ist die Einbindung eines neuen Computers in ein bestehendes Netzwerk ohne weitere Konfiguration möglich. Ohne DHCP muss in der Netzwerkkartenkonfiguration die IP-Adresse, Netzmaske, Gateway, DNS-Server von Hand eingegeben werden. Und was passiert, wenn man mit einem Laptop immer wieder in verschiedenen Netzwerken arbeiten möchte...

Indem man „IP-Adresse automatisch beziehen“ wählt, erwartet man, dass der Rechner seine IP vom DHCP-Server erhält. In der Regel akzeptiert man diese Voreinstellung. Falls jedoch ein

bestimmtes Gerät immer die gleiche IP haben muss (Beispiel: Ein Multimedia-Server, da der Streaming-Client im Wohnzimmer seinen Server nur findet, wenn dieser die IP-Adresse nicht wechselt), dann wird man diesem Server eine statische IP geben.

Die dynamischen IPs sind aber nicht nur in LANs zu finden. Auch Ihr Provider wird Ihnen in der Regel eine dynamische IP geben, wenn Sie im Internet sind. Schauen Sie einfach zuhause im Abstand von mindestens 24 Stunden auf diese Seite „*http://www.wieistmeineip.de/*“[9]. Dort wird Ihnen die vom Provider zugeteilte Adresse mitgeteilt. Dies ist dann nicht die IP-Adresse ihres Rechners, sondern die im Internet gültige IP-Adresse Ihres DSL-Routers.

Selbst wenn man eine Flatrate mit dem Provider vereinbart hat und man daher die Verbindung zum Internet nicht trennt, so wird doch nach 24 Stunden die Leitung von Providerseite aus gekappt. Das ist nicht weiter tragisch, denn der Router oder Server baut binnen Sekunden die Verbindung wieder auf, - jetzt aber eventuell mit einer anderen IP-Adresse.

Falls man einen eigenen ftp- oder http-Server betreiben will, ist das schlecht. Man kann von außen nicht auf ihn zugreifen, da er ja beständig seine Adresse ändert und man die IP-Adresse für einen Zugriff benötigt. Es gibt aber Abhilfe, sofern man einen Router hat, der Dynamic DNS[10] in seinem Repertoire hat.

Das gleiche Problem hat man bei speziellen Geräten wie Drucker oder Server in einem Netzwerk. Diese dürfen auch keine dynamischen IP-Adressen haben, da die Arbeitsstationen wissen müssen, unter welcher Adresse diese Geräte erreichbar sind.

Ports

Möchte man jemand einen Brief schreiben, reicht es in der Regel nicht aus, die Adresse der Person anzugeben. Man muss auch den Namen des Empfängers mit angeben, wenn mehrere Personen in diesem Haus wohnen. Eventuell gibt es sogar mehrere Briefkästen für unterschiedliche Personen.

Auf den Computer übertragen, kann man sich das so vorstellen: Jeder Computer hat eine Adresse (IP-Adresse). Aber auf einem Computer können mehrere Programme gleichzeitig laufen (z.B. ein Browser, ein Computerspiel und ein Mailprogramm). Alle diese Programme greifen auf das Netzwerk zu und wollen Daten empfangen können. Daher erhält jedes Programm eine Portnummer. Diese entspricht dem Namen des Empfängers. Der Programmname wäre hier ungünstig, da man in der Regel gar nicht weiß, welches Programm z.B. auf einem Webserver läuft, dem man eine Anfrage senden möchte. Außerdem kann ein Programm mehrere Portnummern benötigen, wenn gleichzeitig mehrere Anfragen in das Internet gesendet werden (z.B. es sollen mehrere WWW-Seiten gleichzeitig geladen werden).

Die Portnummer ist eine 16-Bit (2 Byte) Zahl und kann daher Zahlenwerte zwischen 0 und 65535 (=2^{16}-1) annehmen. Manche Ports sind für spezielle Anwendungen reserviert. Web-Server erreicht man z.B. immer unter Port 80. Dies ist notwendig, damit ein Browser weiß, wohin er seine Anfrage senden muss. Möchte man Mails versenden, verwendet man den Mailserver-

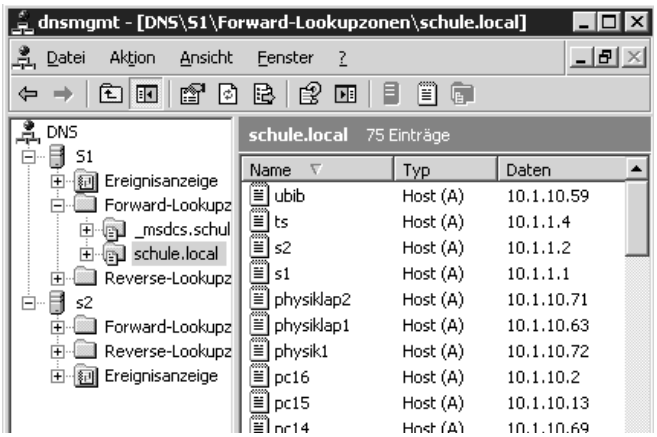
9 IP-Adresse ermitteln und DSL-Geschwindigkeitstest mit *http://www.wieistmeineip.de* von Computerbild. (abgerufen: Dez. 2010).
10 Mehr dazu unter *http://www.dyndns.com/* (abgerufen: Februar 2018)

Port 25. Möchte man Mails empfangen muss man den Port 110 verwenden[11].

Durch die Kontrolle dieser Ports kann der Datenaustausch eines Rechners mit dem Netzwerk überwacht werden. Diese Funktion übernimmt eine **Firewall**. Von außen werden nur Datenpakete an Ports erlaubt, unter denen ein Anwendungsprogramm eine Anfrage ins Internet gestellt hat oder die manuell vom Administrator freigegeben wurden, um einen Server betreiben zu können. Dies stellt sicher, dass keine unerwünschten Daten auf den eigenen Rechner gelangen. Dadurch werden viele Angriffe von Hackern abgewehrt.

Auch die Daten, die den eigenen Computer verlassen, werden kontrolliert. So kann der Administrator festlegen, dass nur bestimmte Zieladressen oder bestimmte Zielports zugelassen sind. Private Firewalls (z.B. Windows-Firewall) kontrollieren aber meist nur den Datenverkehr von außen nach innen.

Domain Name System



IP-Adressen sind für Menschen schwer zu merken. Leichter wäre es, wenn die Computer Namen hätten wie die Menschen auch. Daher hat man ein System eingeführt, mit dem man den Computern Namen geben kann und diese Namen dann automatisch in die richtigen IP-Adressen übersetzt werden. Dies bezeichnet man als Domain Name System (DNS).

Dabei verwaltet ein Domain Name Server-Programm eine Liste mit allen Namen und den zurzeit gültigen dazugehörigen IP-Adressen. Bei diesem Domain Name Server fragen die Clients dann nach, welches die richtige IP-Adresse ist, wenn nur der Name des gewünschten Rechners bekannt ist. Daher muss jeder Client die IP-Adresse des Domain Name Servers kennen. Sie wird daher in der Netzwerkkartenkonfiguration angegeben (vgl. *ipconfig*). Die dazugehörige Portnummer 53 ist immer gleich.

Im Internet ist das System komplizierter, da es dort sehr viele Domainnamen gibt und kein Server alle diese Domainnamen kennt. Im Kapitel „Dienste des Internets“ wird darauf näher eingegangen.

11 Liste mit vordefinierten Ports auf Seite „Port (Protokoll)“. In: Wikipedia, Die freie Enzyklopädie. URL: *http://de.wikipedia.org/w/index.php?title=Port_(Protokoll)&oldid=81798767* (abgerufen: Dez. 2010)

Client-Server-Prinzip

Nachdem die physikalische Verkabelung geplant ist und jeder Rechner eine Adresse bekommen hat, kann man sich nun Gedanken darüber machen, wie die Kommunikation zwischen den Rechnern abläuft. Wer stellt die „Frage“? Wer antwortet? Für die meisten Anwendungen hat sich das Client-Server-Prinzip als sinnvoll herausgestellt.

Die beiden Begriffe Client und Server sind umgangssprachlich leider nicht eindeutig.

Client-Server-Kommunikation

Ein **Server** (engl. „Diener“) ist in der Informatik ein Dienstleister, der in einem Computersystem Daten oder Ressourcen zur Verfügung stellt. Das Computersystem kann dabei aus einem einzelnen Computer oder einem Netzwerk mehrerer Computer bestehen. Zwei Bedeutungen werden unterschieden:

1. Server-Programm: Ein Computerprogramm, das einen Dienst (z. B. Fileserver: zentrale Speicherung von Dateien) bereitstellt.
2. Server-Computer: Der Computer auf dem ein oder mehrere Server-Programme laufen. Die ursprüngliche Bezeichnung für diesen physischen Rechner ist **Host**.

Genauso gibt es für das Gegenstück, den **Client** (engl. „Kunde"), zwei Bedeutungen:

1. Ein Client ist eine Anwendung, die in einem Netzwerk den Dienst eines Servers in Anspruch nimmt.
2. Der Begriff Client wird aber auch oft verwendet, um einen Computer in einem Netzwerk zu bezeichnen.

Der Client (Rechner und Programm) ist bei einer Datenübertragung für die Kontaktaufnahme verantwortlich und bestimmt deren Zeitpunkt. Das hat für den Client-Rechner den Vorteil, dass er erst zum Zeitpunkt der Kontaktaufnahme eine Netzverbindung benötigt. Dies wird als Client-Server-Prinzip bezeichnet: Der "Kunde" (Client) sagt, was er will, der "Dienstleister" (Server) erbringt (daraufhin) die gewünschte Leistung.

Der **Webbrowser** ist ein Beispiel für einen Client, denn er sendet bei jedem Aufruf einer Webseite eine Anfrage an einen **Webserver** und erhält dann von diesem eine Antwort. Der Webserver macht die meiste Zeit nichts anderes als warten. Er wird erst aktiv, wenn vom Client eine Anfrage eingeht.

Auch ein **Netzwerk-Drucker** ist ein Musterbeispiel für einen Server: er verhält sich zunächst gänzlich passiv und harrt still der Druckaufträge, die da kommen werden. Solange kein Druckjob kommt, tut er nichts (außer warten); wenn ein Druckauftrag ankommt, nimmt er die Daten entgegen und druckt sie aus. Danach fällt der Netzwerk-Drucker wieder in die passive Haltung zurück und beschränkt sich darauf, seine "Druckdienste" anzubieten.

Einige weitere Beispiele für Server-Anwendungen sind:

Serveranwendung	Funktion	Clientanwendung
Web-Server (z.B. Apache, Microsoft ISS)	Liefert HTML-Seiten aus	Web-Browser (z.B. Internet Explorer, Firefox, Crome,...)
FTP-Server (z.B. Filezilla)	Liefert Dateien aus (nimmt evtl. Dateien an)	FTP Client (z.B. WSFTP, Filezilla, SmartFTP,...)
Mail-Server (z.B. MS Exchange, JanaServer)	Speichert eingehende E-Mails und liefert sie aus	Mail-Programm (z.B. MS Outlook, Thunderbird)
Proxy-Server (z.B. MS ISA-Server, FreeProxy)	Liefert Internet-Dienste für mehrere Rechner	Ins Betriebssystem integriert
File-Server	Speichert Dateien und liefert sie zurück	Ins Betriebssystem integriert
Media-Server (z.B. TwonkyVision, TVersity)	Zentrale Speicherung von Videos und Musik	In Abspielgeräte integriert
Print-Server	Zwischenspeichern und Ausführen von Druckaufträgen	Ins Betriebssystem integriert
Chat-Server (ICQ-Server)	Verteilt Online-Nachrichten an die Teilnehmer	Chat-Client (ICQ, MS Messanger)

Client–Server–Anwendungen sind heute Standard. Meist werden viele Server-Anwendungen auf einem (oder einigen wenigen) Rechner konzentriert (In den meisten Schulnetzen gibt es einen Server, der DHCP-Server, Fileserver, DNS-Server, Mailserver, Windows-Updateserver und vieles mehr gleichzeitig ist). Die Konzentration der Funktionalität auf den Server verringert den Administrationsaufwand und macht den einzelnen Nutzer unabhängig von einer bestimmten Hardware. So kann der Nutzer den Arbeitsort bzw. den Computer wechseln, ohne auf „seine" Dateien etc. verzichten zu müssen.

In kleineren Netzen wird ein einziger Server genügen (**Ein-Server-Modell**). Alle bereits oben erwähnten zentralen Dienste werden also auf einem einzigen Gerät ausgeführt. Mit zunehmender Netzgröße wird ein einzelnes Gerät jedoch möglicherweise überlastet sein. Auch aus Sicherheitsgründen kann man sich für eine Verteilung der zentralen Dienste entscheiden (**Multi-Server-Modell**).

Das Internet: Verbindung mehrerer lokaler Netzwerke

Geschichte des Internet

Gegen Ende der 50er Jahre erhielt die ARPA (Advanced Research Projects Agency), eine Abteilung des US-amerikanischen Verteidigungsministeriums, den Auftrag, einen Ersatz für die bis dahin verwendete Art der Datenübertragung über fest vorgegebene Leitungen zu entwickeln. Diese leitungsorientierte Datenübertragung war störanfällig und nicht genügend zuverlässig. Die ARPA entwickelte daraufhin eine "paketorientierte" Form der Datenübertragung. Dabei wird die zu sendende Information in kleine Datenpakete aufgeteilt, die unabhängig voneinander zum Zielort übermittelt werden. Am Zielort werden diese Datenpakete wieder zur Information zusammengesetzt. Der größte Unterschied zur zuvor verwendeten Technologie war jedoch, dass für den Weg eines einzelnen Datenpakets nun nicht mehr fest vorgeschrieben war, über welche der möglichen Zwischenstationen es sein Ziel erreichen sollte! Die folgende Grafik zeigt als Beispiel drei verschiedene Wege, auf denen ein Datenpaket von A nach B gelangen könnte:

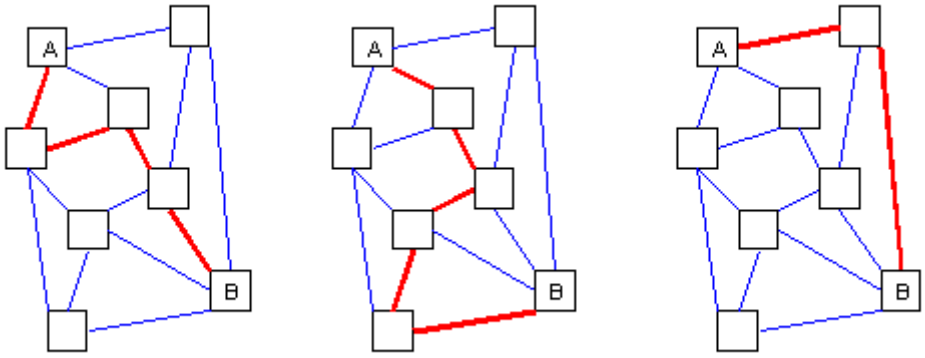


Bild „Routen im Internet“, Fortbildungsreihe Informatik – Teil A,
URL: http://www.gk-informatik.de/netze/internet.html (abgerufen: November 2016)

Wenn ein Datenpaket den Weg links gewählt hat, dann muss das nächste Paket nicht den gleichen Weg wählen. Mit anderen Worten: Die Gesamtinformation ist möglicherweise auf völlig verschiedenen Wegen ans Ziel gelangt!

Der Hintergrund dieses Projektes war eigentlich militärischer Natur: man wollte ein Informationsnetz haben, das ohne zentrale Steuerung auskommt und auch dann noch funktioniert, wenn Teile der Verbindungsleitungen oder einzelne Knotenrechner zerstört sind. Damit dies erreicht wird, muss sich ein Paket quasi seinen Weg durchs Netz "selber suchen", und zwar jeweils in Abhängigkeit davon, welche Verbindungen gerade verfügbar sind. Ein Nebeneffekt ist, dass man auf diese Art und Weise auch gleich noch eine gleichmäßige Lastverteilung auf die einzelnen Verbindungskanäle erreichen kann, indem man bei Stau auf der einen Leitung nachfolgende Pakete eben auf eine Umleitung schickt.

1969 startete dieses ARPA-Net als erstes paketorientiertes Netzwerk den Testbetrieb. Zu Beginn waren vier Universitäts- und Forschungsstandorte in den USA über Telefonleitungen miteinander verbunden. Es handelte sich dabei um die Universität von Kalifornien in Los Angeles (UCLA), die Universität von Kalifornien in Santa Barbara (UCSB), die Universität in Utah und das Stanford Research Institute.

Im Laufe der folgenden Jahre entstanden neben dem ARPAnet weitere paketorientierte Netzwerke. Diese unterschiedlichen heterogenen Netzwerke wurden auf der Grundlage eines

weiteren Forschungsauftrags Mitte der 70er Jahre miteinander verbunden. Das nun entstandene "Netz zwischen den Netzen" erhielt den Namen **Internet**.

Eigens für das Internet wurde ein neues Übertragungsprotokoll, das TCP/IP (Transport Control Protocol / Internet Protocol), entwickelt. Mit der Umstellung aller Rechner im ARPAnet auf TCP/IP Ende der 70er Jahre wurde dieses zum Standardübertragungsprotokoll erklärt. In dieser Zeit folgte die Aufteilung des sehr stark angewachsenen Netzes in einen rein militärischen (MilNet) und einen mehr forschungsorientierten Teil (ARPAnet), aus dem das jetzt bekannte Internet hervorging. Ende der 80er Jahre entstand das Hochgeschwindigkeitsnetz NSFnet (National Science Foundation - eine Behörde der US-Regierung), das sowohl die Wissenschaftszentren der USA als auch die Supercomputer miteinander verband. 1985 wurde der erste kommerzielle Internet-Knoten in Deutschland mit dem Internet verbunden.

Starken Auftrieb erhielt das Internet seit Anfang der 1990er durch das World Wide Web, kurz WWW. Es wurde im CERN (Genf) von Tim Berners-Lee entwickelt. Nun konnten mit Webbrowsern auch Laien auf das Netz zugreifen, was mit der wachsenden Zahl von Nutzern zu vielen kommerziellen Angeboten im Netz führte.

Obwohl das Internet bereits 40 Jahre alt ist, ist es erst in den letzten 20 Jahren in das Bewusstsein der Öffentlichkeit gerückt. Von ca. 1 Mio. im Jahr 1993 ist die Zahl der registrierten Domains auf 1,1 Mrd. im Jahr 2016 gestiegen[12]. Die Anzahl der existierenden Web-Sites spiegelt das Interesse der Bevölkerung an diesem Medium sehr gut wieder. Vor 1996 war das Internet praktisch unbekannt.

Um die riesigen Datenmengen zu bewältigen, baut man einige wenige „Daten-Autobahnen“ (Glasfaser). Heute liegen die meisten europäischen Routen im Dreieck zwischen den Internet-Hauptstätten London-Paris-Frankfurt. Dies macht es allerdings leicht möglich, einen großen Teil des Datenverkehrs im Internet durch Überwachung dieser zentralen Knoten zu kontrollieren.

Router – die Verbindung zwischen den Netzen

Sollen mehrere lokale Netzwerke miteinander verbunden werden, benötigt man sogenannte Router. Diese sind im Prinzip Computer mit zwei oder mehr Netzwerkkarten. Jede Netzwerkkarte gehört zu einem der Netzwerke und muss dementsprechend konfiguriert sein. Der Router hat also mehrere IP-Adressen.

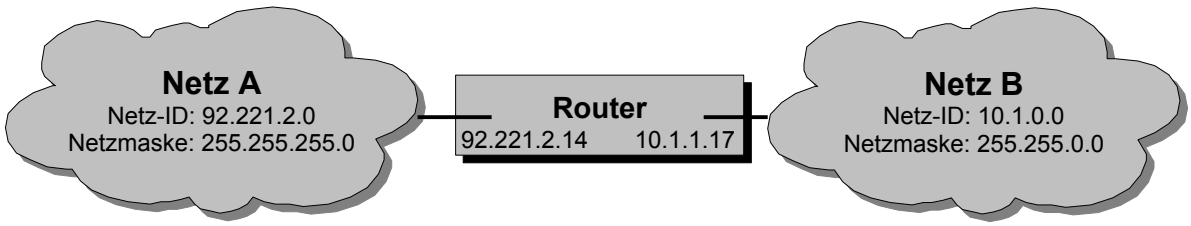


Bild "Verbindung von lokalen Netzen durch Router", Schaller (November 2017)

Router darf man nicht mit Switches verwechseln, die die Daten **innerhalb** eines Netzwerks weiterreichen und dafür auch mehrere Netzwerkanschlüsse bereitstellen.

Der gesamte Datenverkehr, der in andere Netze geht, muss über den Router gehen. Der Router verfügt über eine Tabelle (routing table), in der er nachschaut, wohin er die an ihn gerichteten Daten weiter senden muss.

Diese weitere Zustellung kann über eine Vielzahl von Routern gehen. Jeder Schritt von einem Router zum nächsten wird als „Hop“ bezeichnet. Man kann diesen Weg der Daten durch das Internet über verschiedene Router auch nachverfolgen:

12 Quelle: Internet Domain Survey, *https://www.isc.org/network/survey/* (abgerufen: Feb. 2018)

Trace Route

Mit diesem Tool bekommt man Informationen über die Netzwerkverbindung zwischen der lokalen Station und der entfernten Station. Mit Trace Route wird eine Routenverfolgung vorgenommen und sichtbar gemacht.

Trace Route steht auf der Kommandozeile/Konsole als Befehl traceroute unter Unix/Linux und tracert unter Windows zu Verfügung. Die entfernte Station kann unter der IP-Adresse oder dem Domain-Namen angesprochen werden.

Tracert nic1.belwue.de liefert z.B.:

```
Routenverfolgung zu nic1.belwue.de [129.143.2.9]  über maximal 30 Abschnitte:
  1   63 ms   46 ms   63 ms  217.5.98.84
  2   46 ms   63 ms   47 ms  217.237.154.110
  3   63 ms   62 ms   63 ms  ulm-ea1.ULM.DE.net.DTAG.DE [62.154.58.154]
  4   62 ms   63 ms   47 ms  ulm-eb1.ULM.DE.net.DTAG.DE [62.154.58.106]
  5   63 ms   62 ms   63 ms  Ulm2.BelWue.de [129.143.87.17]
  6   62 ms   47 ms   62 ms  Ulm1.BelWue.de [129.143.87.37]
  7   63 ms   62 ms   63 ms  Stuttgart1.BelWue.DE [129.143.1.17]
  8   62 ms   63 ms   62 ms  Stuttgart5.BelWue.DE [129.143.98.38]
  9   62 ms   63 ms   62 ms  nic1.belwue.de [129.143.2.9]
Ablaufverfolgung beendet.
```

Man erhält also Informationen über die Qualität der Leitungen (Antwortzeiten in Millisekunden) und über die IP-Adressen der Router. Da die Router oft auch mit Adressangaben registriert sind, kann auch der Weg auf einer Weltkarte verfolgt werden. Dazu gibt es Tools wie VisualRoute[13].

Die Route, die die Datenpakete nehmen, kann sich dabei häufig ändern, da die Router die günstigste Route ständig neu berechnen. Dadurch werden „Staus“ vermieden oder bei Routerausfällen andere Wege gewählt.

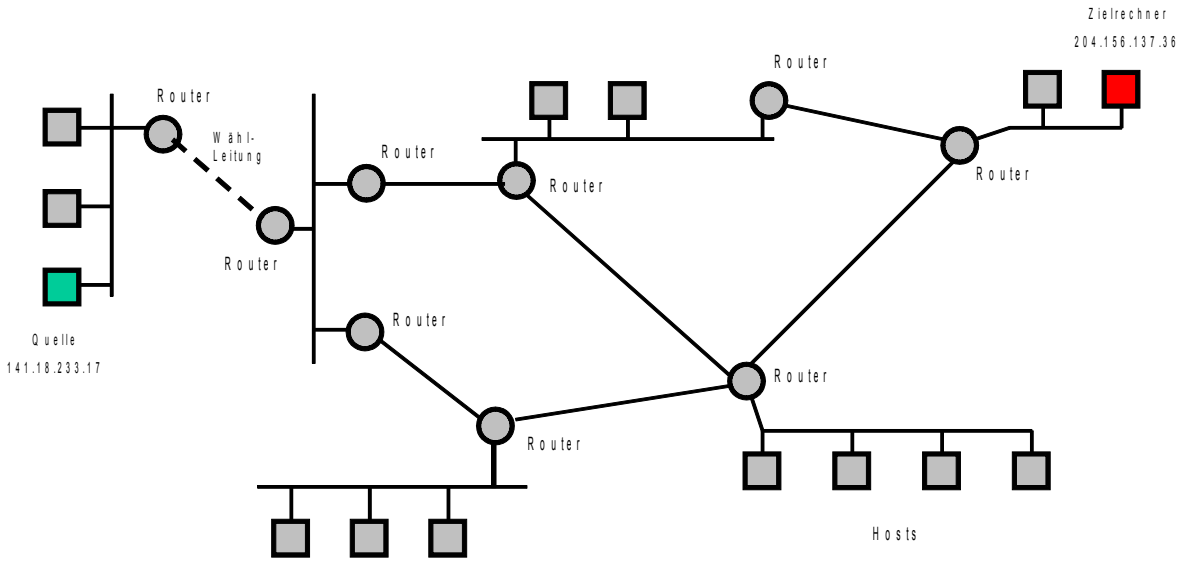


Bild „Vernetzte Router“, Fortbildungsreihe Informatik (BW) – Teil A

Network Address Translation (NAT)

Möchte man mehrere Rechner über einen einzelnen Internet-Zugang auf das Internet zugreifen lassen, taucht früher oder später die Frage auf, mit welchen IP-Adressen diese Rechner

13 Siehe Seite „Visual Traceroute“. URL: *http://www.dnstools.ch/visual-traceroute.html* (abgerufen: Feb. 2018)

ausgestattet werden sollen, da jeder Rechner im Internet eine IP-Adresse besitzen muss. Wenn also ein Unternehmen seine 200 Arbeitsplatzrechner mit Internet-Zugängen ausstatten möchte, wären hierfür mindestens 200 IP-Adressen notwendig.

Anfang der achtziger Jahre war dieser hohe Bedarf an IP-Adressen noch nicht vorstellbar. Universitäten und Institutionen, die am Internet angeschlossen waren, hatten meist nur wenige Großrechner am Netz, an denen die Anwender mit direkten Terminalverbindungen arbeiteten. Deshalb benötigte man nur für jeden Großrechner eine IP-Adresse.

Etwa zehn Jahre später, in den Anfängen des Internet-Booms, machten sich die ersten Experten Gedanken darüber, wie die bereits zu dem Zeitpunkt stark gestiegene Nachfrage nach IP-Adressen in der Zukunft aussehen würde. Selbst optimistischen Hochrechnungen ergaben damals, dass der gesamte IP-Adressraum in wenigen Jahren aufgebraucht sein würde.

Die Idee, die einige Experten unabhängig voneinander hatten, wurde im Mai 1994 durch sogenannte Network Address Translator realisiert. Dieser Adressübersetzer sollte als zusätzliches Modul in einem Internet-Router integriert werden. Im Gegensatz zu einem lokalen Netz, das hinter einem normalen Router an das Internet angebunden wird, kann ein Netz, das hinter einem NAT-fähigen Router steht, mit einem beliebigen IP-Adressbereich konfiguriert sein, da mit NAT eine strikte Trennung zwischen dem Internet und dem lokalen Netzwerk erfolgt. IPv6 wird diese Technik wieder überflüssig machen, da die Anzahl der verfügbaren IP-Adressen deutlich höher ist. Zur Zeit (Feb. 2018) nutzen allerdings noch weniger als die Hälfte der Hosts im Internet IPv6.

Initiiert ein Rechner im lokalen Netzwerk eine Verbindung zu einem Rechner im Internet, so werden die Datenpakete mit der Anfrage zunächst zum Router des Netzwerks übertragen. Dieser Router nimmt die Adressübersetzung der Absenderadresse vor, tauscht also die Adresse des internen Rechners gegen seine eigene im Internet gültige IP-Adresse aus und überträgt dann die Anfrage in das Internet. Der Router stellt sich somit gegenüber dem Internet als Absender der Anfrage dar.

Lokales Netz (LAN)	
Quelle	Ziel
192.168.2.1:8212	15.232.122.1:80
192.168.2.2:8810	16.23.110.3:80
192.168.2.16:211	15.232.122.1:80

NAT

$\longrightarrow$

Öffentliches Netz (Internet)	
Quelle	Ziel
202.1.2.22:9761	15.232.122.1:80
202.1.2.22:9762	16.23.110.3:80
202.1.2.22:9763	15.232.122.1:80

Gleichzeitig wird jede Adressübersetzung in einer NAT-Übersetzungstabelle gespeichert, um die Antwort aus dem Internet verarbeiten zu können.

NAT Übersetzungstabelle	
Port	Lokaler Rechner
9761	192.168.2.1:8212
9762	192.168.2.2:8810
9763	192.168.2.16:211

Jede Anfrage ins Internet bekommt dabei einen speziellen Port (z.B. in der Tabelle oben: 9761) zugewiesen. Daher kann der NAT-Router bei der Antwort aus dem Internet anhand der Portnummer wissen, welchem lokalen Rechner er die Daten weiterreichen muss. Er tauscht die Empfängeradresse der Datenpakete gegen die IP-Adresse des lokalen Rechners aus und gibt die Daten dann ins lokale Netzwerk weiter. Der lokale Rechner erhält diese Datenpakete und kann sie verarbeiten.

NAT ist vor allem für Szenarien gedacht, in denen ein einzelner Internet-Zugang, der nur eine einzelne öffentliche IP-Adresse zur Verfügung stellt, mit mehreren Rechnern gleichzeitig genutzt werden soll. Dies ist in Heimnetzen oder auch in den meisten Schulnetzen der Fall. Dazu ist NAT in den Router implementiert, der den Datenaustausch zum Internet regelt. Wenn zuhause ein DSL-Anschluss eingerichtet ist, so können alle Familienmitglieder gleichzeitig über den Router ins Internet gehen. Nicht viel anders ist es auch an der Schule. Auch hier sorgt ein Router dafür, dass alle Clients durch nur eine IP im Internet repräsentiert werden.

Theoretisch können so viele Anfragen von einem NAT-Router gleichzeitig ins Internet weitergeleitet werden wie es Portnummern gibt. Diese sind auf 16-Bit beschränkt. Man hat also ca. 65000 Verbindungen. Es können auf diese Weise also mehrere tausend Rechner mit einer einzigen IP-Adresse ins Internet gehen. Dies spart sehr viele IP-Adresse ein.

Private IP-Adressen für private Netzwerke

Ein Problem ergab sich bei der Verwendung von IP-Adressen für ein internes, durch NAT vom Internet getrennten Netzwerks: Welche IP-Adressen sollte man für so ein Netzwerk nutzen?

Anfänglich wurde dieses Problem quasi nach dem Lotterieprinzip gelöst: Der Administrator des betroffenen Netzwerks wählte einfach einen IP-Adressraum nach Gutdünken aus. Dies funktionierte normalerweise auch einwandfrei, erzeugte unter Umständen jedoch ein kleines Problem: Was tun, wenn jemand aus diesem lokalen Netzwerk einen Rechner im Internet erreichen muss, der im Internet eine IP-Adresse besitzt, die im lokalen Netzwerk ebenfalls verwendet wird? Sie ahnen es, dieser Rechner konnte so niemals erreicht werden, da die Netzwerkeinstellungen vorgaben, dass sich die die gesuchte IP-Adresse im lokalen Netzwerk angeblich befinden musste.

Deshalb wurden so genannte "private IP-Adressen" eingeführt, die genau diesen Umstand beheben sollten. Private IP-Adressen sind spezielle Adressbereiche im IP-Adressraum, die speziell für die Nutzung in lokalen Netzwerken vorgesehen sind und im öffentlichen Internet nicht verwendet oder geroutet werden.

Ein solcher reservierter Adressbereich, der sehr häufig für lokale Netzwerke verwendet wird, liegt zwischen 192.168.0.0 und 192.168.255.255. (Oft auch zwischen 10.1.0.0 und 10.1.255.255, wie in vielen Schulnetzen).

Internetdienste

Das Internet ist ein Transportmedium für digitale Daten, und gelegentlich wird es als "Daten-Autobahn" bezeichnet. Dieses Bild trifft es recht genau: So wie das Straßennetz vorhanden sein muss, wenn der Verkehr fließen soll, schafft das Internet die notwendigen Voraussetzungen für den weltweiten Datenaustausch. Allerdings ist damit noch nicht festgelegt, welche Daten transportiert werden können. Um im Bild zu bleiben: Es ist noch nicht darüber entschieden, welche LKWs auf unserer Autobahn nach welchen Verkehrsregeln fahren und welche Art von Waren sie transportieren.

Dies wird durch die Dienste geregelt, die auf dem Internet aufsetzen. Ein Anwenderprogramm, das Datenübertragung über das Internet benutzen will, muss als Client agieren: es muss eine Dienstleistung von einem entsprechenden (in der Regel weit entfernten) Server anfordern. Die Kommunikation zwischen Client und Server wird dabei über ein Protokoll abgewickelt, das für den jeweiligen Dienst charakteristisch ist und den Ablauf der Kommunikation regelt. Die folgende Tabelle zeigt einige Internet-Dienste und zugehörige Protokolle:

WWW (World Wide Web)	**Informationsangebot:**
HTTP (Hyper Text Transfer Protocol)	Dokumente im HTML-Format, die Texte und Bilder sowie Verweise auf andere HTML-Dokumente, aber auch auf beliebige andere Dateien enthalten können; durch entsprechende Programmierung sind auch interaktive Dokumente möglich, die auf Benutzereingaben reagieren ("aktive Seiten").
E-Mail	**Elektronische Post:**
z.B. SMTP + POP3 (Simple Mail Transfer Protocol, Post Office Protocol 3)	der Absender schreibt einen Brief und sendet ihn über das Internet zu einem "digitalen Postfach" des Empfängers. Dieser kann dann die dort lagernden Briefe auf seinen lokalen Rechner holen. Um die Beschränkung auf Texte zu umgehen, können einer E-Mail beliebige andere Dateien "angehängt" werden.
FTP	**Übertragung von Dateien:**
FTP (File Transfer Protocol)	Je nach Übertragungsrichtung unterscheidet man zwischen "Upload" (Dateien von meinem lokalen Rechner zu einem entfernten Computer senden) und "Download" (Dateien von einem entfernten Computer auf meinen lokalen Rechner holen).
Time	**Zeiteinstellung:**
SNTP (Simple Network Time Protocol)	Für viele Anwendungen (z.B. automatische Updates) ist es wichtig, dass alle Computer mit exakt der gleichen Uhrzeit arbeiten. Dafür liefert ein **SNTP-Server** eine hochgenaue Uhrzeit.
Domain Name System	**Übersetzung von Domain-Namen in IP-Adressen:**
DNS-Protocol	Werden vom Anwender statt IP-Adressen Domain-Namen eingegeben, müssen diese erst in IP-Adressen übersetzt werden. Diese Aufgabe leisten die DNS-Server.

Da das Internet laufend weiterentwickelt wird, ist damit zu rechnen, dass in Zukunft noch weitere Dienste eingerichtet werden. Es ist natürlich nicht möglich, hier alle Internetdienste zu beschreiben. Es werden hier daher nur zwei Dienste (WWW und E-Mail) und das für viele Dienste notwendige Domain Name System beschrieben.

World Wide Web

Der wohl bekannteste Internet-Dienst ist WWW, das "World Wide Web". Das zugehörige Protokoll nennt sich HTTP, was ein Akronym für "HyperText Transport Protocol" ist. Ein Programm, das HTTP verwendet, um Web-Seiten anzufordern, ist also ein "WWW-Client". Üblicherweise nennt man ein solches Programm einen "Browser" (engl. to browse = schmökern). Der bekannteste und am weitesten verbreitete Browser ist der Internet-Explorer (IE) von Microsoft. Diese Eigenschaften machen ihn allerdings zum einem bevorzugten Ziel von Hackerangriffen. Andere Firmen bieten Alternativen zum Internet Explorer, wie z.B. Firefox, Google Chrome oder Opera.

Der zugehörige HTTP-Server wird gewöhnlich einfach als "Web-Server" bezeichnet. In aller Regel ist dies ein Rechner, auf dem viele "Web-Seiten" gespeichert sind. Wie schon oben erwähnt, sind Web-Seiten Dokumente im HTML-Format. Damit der Client nun genau angeben kann, welche der zahlreichen HTML-Seiten er haben will, erhält jede Seite eine eindeutige Adresse:

z.B. http://www.gkinf.de/netze/internet.html

Eine so geformte Adresse nennt man einen "Universal Ressource Locator" oder kurz eine URL (was üblicherweise als Femininum verwendet wird). Eine URL ist aus vier Bestandteilen zusammengesetzt:

http://	Als erstes wird das zu verwendende Protokoll genannt.
www.gkinf.de	Sodann wird die Internet-Domain angegeben, auf der die gewünschte Seite lagert.
/netze/	Es folgt der Pfad auf dem Server bzw. der Ordner, in dem das gewünschte Dokument liegt.
internet.html	Abschließend wird der Dateiname des Dokuments angegeben.

Es sind nicht alle dieser Angaben immer unbedingt nötig:

- Wenn z.B. am Ende der URL der Dateiname fehlt und die URL mit dem Pfad aufhört, dann wird in diesem Ordner nach einem "Standard-Dokument" namens „index.htm", „index.html" oder „index.php“ gesucht. Wird kein solches Dokument gefunden, dann wird üblicherweise das Inhaltsverzeichnis dieses Ordners zurückgeliefert.
- Die meisten modernen Browser tolerieren es auch, wenn die einleitende Dienste-Angabe (http://) fehlt. Ist kein Dienst angegeben, wird HTTP als Standard angenommen.

  Warum wird dann überhaupt ein Dienst angegeben? Nun, die meisten Browser können nicht nur HTTP, sondern auch FTP, und es gibt viele FTP-Server im Internet, auf die man mit dem Browser zugreifen kann (zumindest lesend!). In diesem Fall ist dann aber die Angabe des Dienstes "ftp://" am Anfang der URL unbedingt erforderlich!

  ftp://meinftpsever.net, bzw. ftp://username@meinftpserver.net (mit Benutzeranmeldung)

  Wenn der username existiert, erscheint eine Anmeldemaske, in der man das Passwort eingeben muss.

HTML-Dokumente können nach den eigenen Wünschen mit Schriftarten, Schriftgrößen, Schriftfarben und natürlich auch eingebetteten Bildern gestaltet werden[14]. Die wichtigste Eigenschaft von HTML-Dokumenten im "Web" sind aber die "Links" (engl. to link = verbinden): jedes Dokument kann Verweise auf andere Dokumente, ja sogar beliebige andere Dateien enthalten.

Wie alle HTML-Formatanweisungen wird auch ein Link mit Hilfe eines entsprechenden "Tags" dargestellt:

Suso-Gymnasium

Unter href kann eine beliebige URL angegeben werden. Liegt das Verweisziel auf dem gleichen Web-Server, kann die Angabe einer Domain entfallen und nur der Dateiname des Dokumentes (samt Pfad) angegeben werden.

Durch die Verweise auf weitere Dokumente entsteht ein Verbund aus vielen Dokumenten, die untereinander verlinkt sind. Dies bezeichnet man als Hypertext-Struktur. Topologisch gesehen handelt es sich hier um einen vermaschten Graphen, bei dem die einzelnen Dokumente die Knoten und die Links gerichtete Kanten darstellen. Damit haben das Internet (die Computer und ihre physikalischen Leitungen) und das WWW (die Dokumente und ihre Links) die gleiche zugrunde liegende Struktur, aber die Bedeutung der Knoten und Kanten ist eine völlig andere.

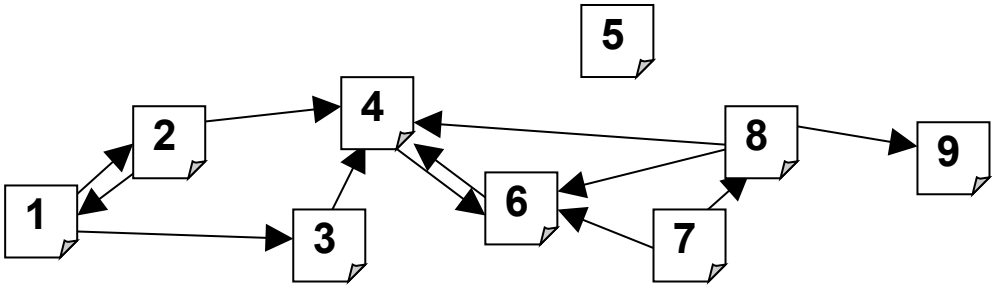


Bild "Verlinkung von Dokumenten", Schaller. (November 2016)

Protokollierung

Jeder Computer im Internet wird durch seine IP-Adresse identifiziert. Wenn man zuhause mit einem DSL-Anschluss oder mobil mit einem Smartphone ins Internet geht, erhält man vom Provider eine IP-Adresse zugewiesen. Der Provider hat einen Adressbereich, aus dem er Adressen verteilen kann. Diese IP-Adresse ist bis zum Trennen der Verbindung[15] gültig, beim nächsten Verbinden wird höchstwahrscheinlich eine neue IP-Adresse zugewiesen. Der Provider protokolliert, welcher Kunde in welchem Zeitraum welche IP-Adresse hatte.

Wenn ein Browser nun eine Anfrage an einen Webserver stellt, schickt er seine IP-Adresse mit: Der Server muss ja wissen, wohin er seine Antwort schicken muss. Die meisten Webserver sind so konfiguriert, dass sie ihrerseits ebenfalls ein Protokoll führen. Darin steht, welcher Client wann welche Seite aufgerufen hat.

14 Eine sehr gute Anleitung zur Erstellung von HTML-Seiten liefert SELFHTML: *http://de.selfhtml.org/*.
Zum Erstellen von HTML-Seiten ist z.B. Notepad++ geeignet: *https://notepad-plus-plus.org/* (abgerufen: Jan. 2017)

15 Die meisten DSL-Verträge enthalten eine Zwangstrennung nach 24 Stunden. Diese wird üblicherweise nachts automatisch vom Router durchgeführt.

Beispiel für einen Protokoll-Eintrag:

```
12.34.56.78 - - [05/Dec/2016:09:31:07 +0100] "GET /index.php HTTP/1.1" 200 3860
"https://www.server.de/" "Mozilla/5.0 (Windows NT 6.1; rv:50.0) Gecko/20100101
Firefox/50.0"
```

Es wird also zusätzlich zur IP-Adresse und dem genauen Zeitpunkt (am Anfang der ersten Zeile) gespeichert, welcher Browser und welches Betriebssystem verwendet werden.

Mit diesen Protokolldaten kann z.B. im Fall einer Straftat beim Provider erfragt werden, welcher Kunde zu einem bestimmten Zeitpunkt eine IP-Adresse besessen hat. Damit können dann juristische Schritte eingeleitet werden. Natürlich wird damit nur der Anschlussinhaber festgestellt – wie im Abschnitt „NAT“ beschrieben wurde, sind alle Teilnehmer hinter dem Router mit der gleichen IP-Adresse im Internet unterwegs. Daher sollte das private WLAN stets verschlüsselt werden, um zu verhindern, dass Fremde den Anschluss missbrauchen.

Cookies

Auch wenn keine Straftaten begangen werden, interessieren sich Internetanbieter dafür, wer welche Seiten im Internet anschaut. Zum Beispiel lässt sich aus den Internetsuchen ableiten, für welche Produkte sich ein Nutzer interessiert, so dass ihm maßgeschneiderte Werbung angezeigt werden kann.

Die IP-Adresse ist allerdings nur schlecht geeignet, einen Nutzer dauerhaft zu identifizieren: Sie wechselt täglich, und hinter einer IP-Adresse kann eine Vielzahl von Nutzern sitzen. Effektiver sind da Cookies: Ein Cookie ist eine kleine Textdatei, die der Browser auf Befehl vom Server hin auf dem Computer ablegen und wieder auslesen kann. Für den Nutzer zeigt sich der Vorteil darin, dass z.B. der Warenkorb eines Webshops auch dann weiterhin verfügbar ist, wenn man zwischendrin den Browser geschlossen hat oder dass man bei Facebook die Zugangsdaten nicht eingeben muss. Allerdings kann eine Website wie Facebook damit auch ein detailliertes Profil eines Nutzers erstellen, da der „Gefällt mir“-Button inzwischen auf vielen anderen Webseiten vertreten ist. Jedes Mal, wenn der Button angezeigt wird, kann Facebook versuchen, seinen Cookie auszulesen und kann damit eine weitere Information dem Profil des Nutzers hinzufügen.

Da es für die Funktionalität vieler Webseiten notwendig ist, dass Cookies gesetzt werden dürfen, sollten diese zumindest beim Schließen des Browsers automatisch gelöscht werden.

E-Mail Dienst

Der E-Maildienst ist neben dem World Wide Web (WWW) einer der bekannten, weit verbreiteten Dienste des Internets. Er wird durch Mailserver realisiert, die die Postfächer der Kunden verwalten und die ankommenden E-Mails entgegennehmen. Der Nutzer startet auf seinem Rechner ein Clientprogramm (z. B. Microsoft Outlook, Thunderbird) und lädt die E-Mails vom Server herunter oder verschickt E-Mails über den Server. Da das Clientprogramm die Anfrage sendet und der Server nur auf eingehende Anfragen reagiert, ist auch dies eine Client-Server-Anwendung.

Abgeschickte E-Mails werden vom Mailserver über viele Router an den entsprechenden Mailserver des Empfängers gesendet. Dadurch kann jeder die E-Mails mitlesen, der Zugriff auf einen der Router hat, sofern sie unverschlüsselt gesendet werden. Ein E-Mail entspricht somit einer Postkarte und sollte nie vertrauliche Daten enthalten.

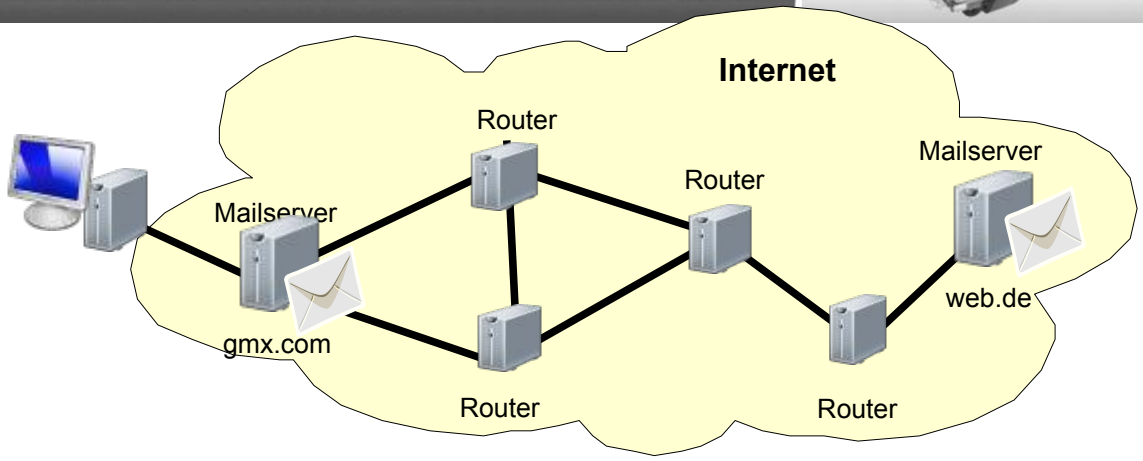


Bild "Mailversand", Schaller. Icons Monitor und Server aus dem Staz Hardware Icons von VisualPharm (Ivan Boyko) http://veryicon.com/icons/hardware/hardware-1/ und Umschlag von Clker-Free-Vector-Images https://pixabay.com/de/vectors/umschlag-e-mail-schreiben-luftpost-295411/ (abgerufen: Januar 2017)

Möchte man eine abhörsichere Kommunikation sicherstellen, müssen die E-Mails verschlüsselt werden. Dazu gibt es Programme wie zum Beispiel Pretty Good Privacy (PGP)[16], die eine sichere Verschlüsselung anbieten.

Die Kommunikation zwischen E-Mail-Client und Server umfasst im Gegensatz zum WWW zwei verschiedene Aktionen: das Empfangen und das Versenden von Briefen. Daher gibt es für die beiden Aktionen verschiedene Protokolle:

- SMTP (Simple Mail Transfer Protocol) zum Versenden
- POP3 (Post Office Protocol 3) oder IMAP (Internet Message Access Protocol) zum Empfangen. Im IMAP Protokoll ist neben dem Herunterladen der Mails auch die Verwaltung der Mails auf dem Server geregelt. Daher verwendet man es, wenn die Mails immer auf dem Server bleiben sollen und nur bei Bedarf heruntergeladen werden.

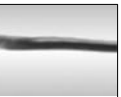
Es kann je nach Provider sogar verschiedene Server zum Versenden und zum Empfangen der Mails geben. Diese Server werden wie beim WWW auch durch Angabe eines Domain-Namens oder einer IP-Adresse festgelegt: z.B. smtp.web.de und pop3.web.de.

Domain Name System (DNS)

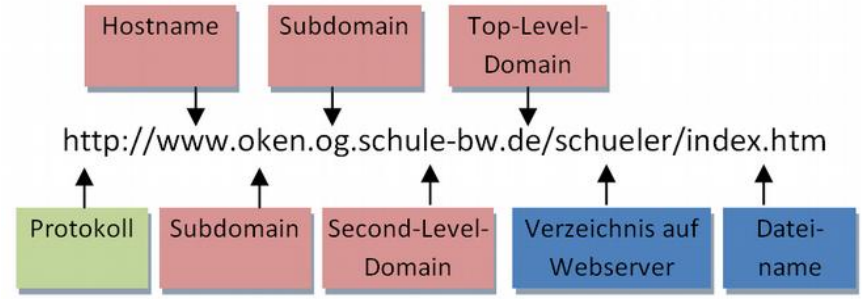
Im Internet werden die Computer von Menschen über ihre Namen und nicht ihre IP-Adresse identifiziert. Im Browser gibt man z.B. die URL (Uniform Resource Locator – z.B. http://www.gymnasium-ettenheim.de) der gewünschten Seite ein. Diese URL enthält die Bezeichnung der Domäne, die nichts anderes als der Name des Computers ist.

Jedem Domainnamen ist eine IP-Adresse zugeordnet. Dadurch erhält man eine lange Liste von Domainnamen mit den zugehörigen IP-Adressen. Zu Beginn der Entwicklung des Internet wurde auf jedem Client-Rechner eine derartige Tabelle geführt. Als das Internet aber immer weiter wuchs, wurde diese Methode zu unhandlich, weil dieselben Daten auf jedem einzelnen Client-Rechner ständig auf dem aktuellen Stand gehalten werden mussten - eine schier unlösbare Aufgabe! Also wurden diese Daten nur noch auf bestimmten Rechnern vorgehalten, die die Rolle von "Servern für die Adress-Ermittlung" übernahmen und so zu "Name-Servern" (wie üblich in englischer Aussprache!) wurden. Jetzt musste jeder Computer, der die zu einem Domainnamen gehörige IP-Adresse benötigte, bei diesen Servern anfragen. Es ist klar, dass bei den heutigen Zugriffszahlen dieses System zu einem Zusammenbruch der Nameserver führen würde. Außerdem müsste jeder neue Domainname den Betreibern dieser Server mitgeteilt werden. Und das sind mehrere Millionen pro Jahr!

16 Siehe Seite „Pretty Good Privacy“.
URL: *http://de.wikipedia.org/w/index.php?title=Pretty_Good_Privacy&oldid=82144865* (abgerufen: November 2016)



Daher hat man das System perfektioniert und ein hierarchisches System eingeführt. Ein Domainname wird daher in einzelne Teile gegliedert.



Die einzelnen Bestandteile der Domain-Bezeichnungen werden in den Domain-Namen in der Reihenfolge ansteigender Hierarchiestufen aufgeführt. Ganz am Ende des Namens steht die so genannte "top level domain". Dies ist die oberste Hierarchiestufe des DNS. Sie unterteilt das Web in thematisch ("com", "gov", "edu", "info", "berlin", "movie" usw.) oder geografisch ("de", "fr", "at", "us", usw.) abgegrenzte Bereiche. Jede dieser Top-Level-Domains wird von einer bestimmten Organisation verwaltet, bei der alle Domains unterhalb der jeweiligen Top-Level-Domain angemeldet werden müssen. So wird z.B. die Top-Level-Domain "de" vom "DEutschen Network Information Center", kurz "DENIC" verwaltet. Diese Organisation sorgt z.B. auch dafür, dass jeder mögliche Domain-Name nur einmal existiert!

Will man z.B. die Domain "wildbad-schule.de" für sich registrieren lassen, dann muss man sich an einen "Internet-Service-Provider" (ISP) wenden, der die Registrierung dieser Domain für Sie beim DENIC beantragt. Der ISP vermietet Ihnen dann üblicherweise auf einem seiner Server ein gewisses Kontingent an Festplattenplatz und gewährt Ihnen Schreibrechte in diesem Bereich, indem er Ihnen einen FTP-Zugang einrichtet. Darüber hinaus informiert er das DENIC darüber, wo genau diese Domain in Zukunft zu finden sein wird. Das DENIC wird seinerseits diese Information im Internet allgemein verfügbar machen, so dass Ihre Domain dann auch von einem beliebigen Rechner gefunden werden kann. Es ist klar, dass eine solche Dienstleistung Geld kostet - und mit diesem Geld wird letztendlich die Infrastruktur des Internets mitfinanziert!

Will nun ein Client-Rechner wissen, welche IP-Adresse zur Domain "www.pqr.xyz" gehört, fragt er bei einem Name-Server nach, und dieser liefert ihm die gesuchte IP-Adresse zurück. Wenn der ISP-Name-Server die Antwort auf die Anfrage nicht selbst kennt, dann erfragt er die Adresse bei weiteren Name-Servern. Das geht so lange weiter, bis ein Name-Server die richtige IP-Adresse zur gewünschten URL kennt. Diese Adresse liefert der Name-Server an den Client zurück.

Protokolle und OSI-Schichtenmodell

Damit die Kommunikation zwischen Sender und Empfänger funktioniert, müssen beide „dieselbe Sprache sprechen“. Sie müssen genau wissen, wer wann was sagen kann und darf. Nur wenn dies ganz exakt festgelegt ist, wird die Kommunikation zwischen Computern funktionieren. Diese Regeln werden in einem **Protokoll** festgelegt.

Bei "Protokoll" denken wir möglicherweise zunächst an das Protokoll einer Besprechung, also an ein Verlaufsprotokoll, dem nachträglich zu entnehmen ist, was in dieser Besprechung gesagt und beschlossen wurde. Darüber hinaus hat das Wort "Protokoll" aber auch im täglichen Leben noch eine andere Bedeutung: Es bezeichnet nämlich auch die Gesamtheit der im diplomatischen Dienst verwendeten Verhaltensregeln und Zeremonien. Diese Bedeutung kommt unserer informatischen Definition schon recht nahe, handelt es sich doch in beiden Fällen um eine Reihe von Vorschriften, die den Umgang verschiedener Teilnehmer regeln sollen.

Unter einem Protokoll verstehen wir also eine Menge von Regeln und Vorschriften, die genau festlegen, wie ein Kommunikationsprozess ablaufen soll. Im Alltag befolgen wir diese Regeln meist ganz "automatisch", d.h. ohne dass wir uns ihrer eigentlich bewusst sind:

1. Bei einem freien Gespräch zwischen mehreren Personen sollte stets nur einer reden. Also kann jeder der Teilnehmer nur dann mit seinem Beitrag beginnen, wenn gerade kein anderer redet. Starten zwei (oder mehrere) Teilnehmer gleichzeitig, kommt es zu einer Kollision, und die Verständlichkeit sinkt ab. Üblicherweise einigen sich die an der Kollision Beteiligten dann durch kurzen Blickkontakt, wer denn nun tatsächlich als nächster reden soll.
2. Bei einem moderierten Gespräch in einer Gruppe wird das Rederecht hingegen von einer zentralen Instanz, dem Diskussionsleiter, verwaltet: er führt eine Liste der Wortmeldungen, er erteilt dem einzelnen Teilnehmer das Rederecht und er wacht darüber, dass kein Teilnehmer länger als die ihm zugestandene Zeit redet. Das funktioniert natürlich nur dann, wenn sich alle Beteiligten an die Vorgaben des Diskussionsleiters halten.
3. Sollen wichtige Daten per Telefon übertragen werden, steht die Korrektheit der Datenübertragung im Mittelpunkt. Diese wird durch ein entsprechendes Übertragungsprotokoll gewährleistet: der Empfänger kann z. B. die übermittelte Information zur Kontrolle wiederholen, d.h. das, was er empfangen hat, gleich nochmal an den Sender zurückschicken, woraufhin dieser vergleichen kann, ob das, was da (zweimal!) über das Telefon übermittelt wurde, mit der ursprünglichen Nachricht übereinstimmt.
4. Sollen während einer Klassenarbeit verbotenerweise Informationen übertragen werden, ist der wichtigste Aspekt: Wie kann bei der Kommunikation verhindert werden, dass die Kommunikation an sich von einem Dritten bemerkt wird? Man erreicht dies gewöhnlich dadurch, dass man sehr leise redet, sodass die Kommunikation nur noch für den direkten Empfänger erkennbar ist. Damit steigt natürlich die Gefahr von Fehlern bei der Datenübermittlung an.

Zugriffsprotokolle

In den Situationen 1 (Freies Gespräch) und 2 (Moderiertes Gespräch) muss das Protokoll vor allem den zeitlichen Ablauf der Aktivitäten der Beteiligten regeln, also die Fragen: Wann redet wer und wie lange? Man redet hier von Zugriffs-Protokollen, die also den Zugriff der beteiligten Kommunikationspartner auf den "Informationskanal" regeln. Im Folgenden werden die beiden derzeit am häufigsten verwendeten Zugriffsprotokolle beschrieben, nämlich das Ethernet-Protokoll und das Token-Ring-Protokoll:

1. Das **Ethernet-Protokoll** funktioniert analog zum **freien Gespräch** zwischen mehreren Personen: will eine Station senden, wartet sie, bis gerade keine Übertragung im Netz stattfindet. Dann beginnt sie mit der Übertragung. Versuchen mehrere Stationen gleichzeitig zu senden, so kommt es zu einer Kollision, die von allen beteiligten Stationen erkannt wird. Nach einem zufällig gewählten Zeitraum versuchen die kollidierten Teilnehmer erneut zu übertragen. Kommt es noch mal zu einer Kollision, so wird schrittweise das Zeitintervall vergrößert. Die Wartezeit wird jedoch stets zufällig gewählt, um die Kollisionswahrscheinlichkeit insgesamt klein zu halten. Netze mit diesem Zugriffsverfahren sind einfach zu realisieren; allerdings kann nicht vorausgesagt werden, wie schnell die Datenübertragung vor sich gehen wird, speziell wenn viele Rechner auf das Netz zugreifen wollen.

   In privaten Computernetzen und auch in den meisten Firmennetzen wird das Ethernetprotokoll verwendet, da die Konfiguration einfach ist.
2. Das **Token-Ring-Protokoll** funktioniert analog zum **moderierten Gespräch** in einer Gruppe, wo die Redeberechtigung von einer höheren Instanz verwaltet wird. Die Berechtigung zum Senden (also das "Rederecht") wird mit Hilfe eines sogenannten "Tokens" vergeben: dies ist ein Software-Kennzeichnung, von der es im Netz zu einer Zeit nur genau ein Exemplar geben darf, und das von der Station, die es gerade besitzt, spätestens nach einer festgelegten Zeit zur jeweils nächsten Station weitergereicht werden muss. Senden darf jeweils nur diejenige Station, die gerade das Token besitzt. Auf diese Weise werden Kollisionen vermieden. Das Zugriffsverfahren für einen Token-Ring ist wesentlich aufwändiger als das für ein Ethernet. So muss dafür gesorgt werden, dass beim An- und Abschalten von Stationen diese in den Tokenumlauf aufgenommen oder aus ihm gestrichen werden. Ebenso muss eine Regelung für einen Tokenverlust getroffen werden, wenn nämlich die Station, die gerade das Token besitzt, ausfällt. Im Gegensatz zum Ethernet kann aber bei Token-Ring-Netzen sehr genau vorausgesagt werden, wie schnell die Datenübertragung geschehen wird. Das ist besonders dann wichtig, wenn eine bestimmte Datenübertragungsrate eingehalten werden muss (z.B. bei der Übermittlung von Sprache oder Video-Daten in Echtzeit).

Übertragungsprotokolle

In Situation 3 (Übermittlung wichtiger Daten per Telefon) steht die Korrektheit der Datenübertragung im Mittelpunkt. Diese wird durch ein entsprechendes **Übertragungsprotokoll** gewährleistet: durch Überprüfung der Daten durch den Absender nach der doppelten Übertragung werden Fehler weitgehend ausgeschlossen.

Das **Transmission Control Protocol / Internet Protocol** (**TCP/IP**) hat Mechanismen eingebaut, die korrekte und vollständige Datenübermittlung sicherstellen sollen:

- Jedem Datenpaket wird eine Prüfsumme angehängt, mit der der Empfänger überprüfen kann, ob das Datenpaket fehlerfrei übertragen wurde. Ist dies nicht der Fall, löscht der Empfänger das Paket. Hat er das Paket korrekt erhalten, sendet er eine Empfangsbestätigung.
- Der Sender sendet die Datenpakete, für die er noch keine Empfangsbestätigung erhalten hat, so lange immer wieder, bis alle Empfangsbestätigungen eingetroffen sind.
- Alle gesendeten Daten werden in einzelne Pakete geteilt und dann nummeriert, damit nicht die gesamten Daten bei jedem Fehler erneut gesendet werden müssen. Große Pakete würden außerdem eine Datenleitung lange blockieren, so dass der Datenverkehr für andere Netzteilnehmer stocken würde.
- Der Empfänger setzt die Pakete wieder in der richtigen Reihenfolge zusammen. Fehlt ein Paket, werden die anderen Pakete so lange zwischengespeichert, bis es eingetroffen ist.

Dieses Verfahren stellt sicher, dass auch bei Verlust eines Datenpakets der Austausch korrekt funktioniert. Würde der Absender nur auf Anfrage des Empfängers die Daten erneut senden, käme der Datenaustausch nicht zustande, da der Empfänger gar nicht weiß, dass er Daten erhalten soll, wenn die Pakete verloren gegangen sind. Er kann daher die erneute Sendung nicht einfordern.

Neben TCP findet das **User Datagram Protocol (UDP)** häufig als Transportprotokoll Verwendung. Dabei schickt der Sender die Datenpakete der Reihe nach an den Empfänger. Eine Rückmeldung des Empfängers findet nicht statt. UDP bietet daher im Gegensatz zu TCP keinerlei Garantien, dass die Datenpakete in der richtigen Reihenfolge ankommen oder nicht verloren gehen. Selbst die Korrektheit der Datenpakete wird in der Regel nicht überprüft.

Dafür spart man auf diese Weise viele Nachrichten ein und das Protokoll arbeitet schneller. Es eignet sich daher für Datenübertragungen, bei denen es auf Geschwindigkeit ankommt (z.B. Audioübertragung bei VoIP, Videoübertragung bei Streaming, DNS-Abfragen), aber fehlerhafte Pakete keine große Rolle spielen (ein leichtes Knacken in der Leitung oder einige Pixelfehler spielen keine Rolle).

Protokolle für die geheime Datenübertragung

In der Situation 4 (verbotene Informationsübermittlung während einer Klassenarbeit) ist der wichtigste Aspekt die **geheime Datenübertragung**. Durch Verschlüsselung kann erreicht werden, dass die Daten von unbefugten Dritten nicht gelesen werden können. Hier geht es aber sogar darum, bei der Kommunikation zu verhindern, dass die Kommunikation an sich von einem Dritten bemerkt wird. Dies bezeichnet man als "Steganografie". Das ist die Technik des Verbergens der bloßen Existenz von Nachrichten.

OSI-Schichtenmodell

Es wurden im bisherigen Text schon viele Protokolle erwähnt: Ethernet-Protkoll, Transmission Control Protocol (TCP), Internet Protocol (IP-Protocol), Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), usw. Insgesamt gibt es über 500 Protokolle, die bei der Datenübertragung im Internet eine Rolle spielen.

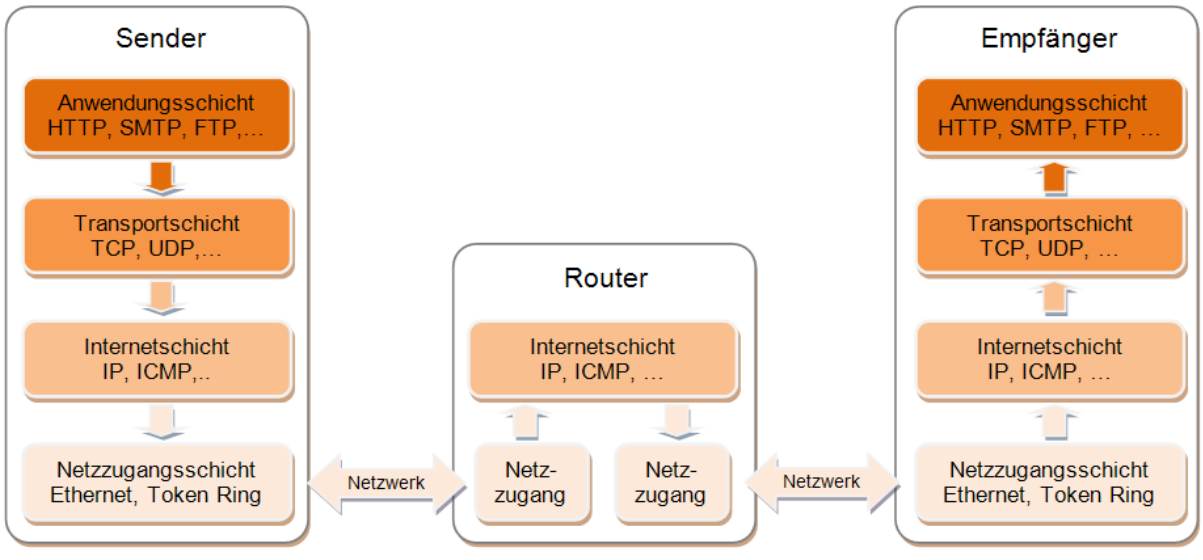


Bild: OSI-Schichtenmodell, Schaller

Bei der Informationsübermittlung in einem Rechner-Netz sind immer mehrere Protokolle beteiligt, wobei jedes Protokoll bestimmte Aufgaben hat. Man kann sich die Protokolle in Schichten übereinander angeordnet vorstellen. Ganz oben stehen die Protokolle der Anwendungen, die der Benutzer nutzt (z.B. HTTP hat jeder schon mal gehört). Ganz unten

stehen die Protokolle, die für den Datenaustausch auf Leitungsebene/Netzwerkkartenebene zuständig sind. Dazwischen gibt es weitere Protokolle des Betriebssystems, die der Programmierer einer Anwendung benutzen kann, um sich nicht selbst um die Funktionsweise einer Netzwerkkarte kümmern zu müssen. Wir wollen die im Detail ziemlich komplizierten Zusammenhänge (normalerweise 7 Schichten) im Folgenden anhand eines vereinfachten Modells (4 Schichten) erklären:

Abbildung 2 zeigt als oberste Schicht die **Anwendungsschicht**. Wenn z.B. ein Browser eine Internetseite aufrufen will, dann formuliert er einen entsprechenden Auftrag gemäß dem HTTP-Protokoll. Die Anfrage wird an die Transportschicht weitergegeben. Genauso gibt aber auch ein E-Mail-Client eine Anfrage an die Transportschicht weiter. Nur wurde diese Anfrage dann gemäß dem SMTP oder POP3-Protokoll formuliert.

Anfrage gemäß HTTP: *GET bild.png HTTP/1.1 Host: 141.23.2.222*

Anfrage gemäß POP3: *RETR 3* (Retrieve = Empfange Nachricht 3)

Das Betriebssystem des Rechners realisiert die **Transportschicht** und kennt das TCP-Protokoll. Geht also eine Anfrage von einer Anwendung ein, hält es sich an das TCP-Protokoll und verarbeitet die Daten dementsprechend:

Die zu sendenden Daten werden auf einzelne Pakete aufgeteilt, die häufig nicht größer als etwa ein KByte sind. Dann werden die Pakete durchnummeriert. Jedes einzelne Paket wird mit der IP-Nummer des Empfängers und der des Absenders versehen. Außerdem wird die Portnummer für die Anwendung des Empfängers (z.B. Port 80 => an Webserver gerichtet) und die Portnummer der Anwendung des Absenders angehängt. Die Portnummer des Absenders ist eine willkürliche Nummer, die notwendig ist, damit die Antwort an das richtige Anwendungsprogramm weitergeleitet werden kann.

Außerdem werden noch verschiedene Verwaltungsinformationen hinzugefügt, wie z.B. eine Prüfsumme, mit deren Hilfe ein Empfänger Übertragungsfehler erkennen kann.

Das IP-Protokoll hängt sehr stark mit dem TCP-Protokoll zusammen. Meist werden beide in einem Atemzug genannt (TCP/IP). Das Internet Protokoll regelt aber über das ganze Internet hinweg (**Internetschicht**), wie die Datenpakete vom Sender zum Empfänger gelangen sollen. Das Verfahren zum Routing der Datenpakete ist beispielsweise im IP festgelegt. Daher muss ein Router dieses Protokoll beherrschen. Diese Internetschicht heißt im OSI-Schichtenmodell **Vermittlungsschicht**.

Die unterste Schicht ist die **Netzzugangsschicht**. Die Daten werden an die Netzwerkkarte weitergereicht, die sie gemäß dem Ethernetprotokoll an eine andere Netzwerkkarte weiterreicht. Diese Netzwerkkarte gehört meistens nicht dem Empfänger, sondern stellt nur eine Zwischenstation dar. Davon hat die Netzzugangsschicht aber keine Ahnung. Sie kümmert sich nur um die Weitergabe von Netzwerkkarte zu Netzwerkkarte im eigenen Netzwerk. Ein Switch muss daher dieses Protokoll beherrschen. Für die korrekte Weiterleitung in andere Netzwerke sorgt die Vermittlungsschicht.

Beim Empfänger wird dieser ganze Prozess umgekehrt durchlaufen. Die Netzwerkkarte (Netzzugangsschicht) nimmt die Daten in Empfang und reicht sie an die Vermittlungsschicht weiter. Diese entscheidet, ob die Daten weitergeleitet werden müssen oder für diesen Rechner bestimmt sind. Die Transportschicht nimmt alle Pakete einzeln in Empfang, kontrolliert die Prüfsumme und sendet ggf. eine Empfangsbestätigung. Dann werden die Pakete in der richtigen Reihenfolge zusammengesetzt und an die Anwendungsschicht weitergegeben.

Die verschiedenen Schichten arbeiten auch mit unterschiedlichen Adressen:

- Anwendungsschicht: Domain-Namen oder IP-Adressen

- Transportschicht: IP-Adressen, Portnummern
- Vermittlungsschicht: IP-Adressen
- Netzzugangsschicht: MAC-Adressen

Der Vorteil dieses Schichtenmodells ist, dass die unterschiedlichen Funktionen auf verschiedene Programme verteilt und damit unabhängig voneinander sind. Dem Browser ist es völlig egal, ob auf der Netzzugangsschicht das Ethernet oder das Token Ring Protokoll verwendet wird. Er verlässt sich einfach darauf, dass es funktioniert. Auch die Umstellung von IPv4 auf IPv6 ist ohne Änderung des Browsers möglich. Ein Programmierer einer Internetanwendung muss sich keine Gedanken über den kompletten Datenverkehr machen. Er muss nur die Daten an die Transportschicht übermitteln, die sich um alles weitere kümmert.

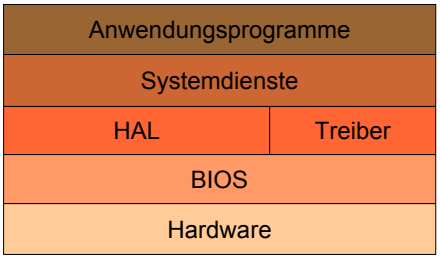


Bild Schichtenmodell, Schaller

Ähnliche Schichten gibt es auch bei Betriebssystemen. Ganz unten befindet sich die Hardware, die ja bei jedem Computer anders ist. Darüber liegt das BIOS (Basic Input Output System), das auf diese Hardware zugreift. Es ist fest auf einem Chip auf dem Motherboard gespeichert. Die Installation des Betriebssystems beginnt mit dem HAL (Hardware Abstraction Layer). Durch den HAL werden einheitliche Schnittstellen für die verschiedenen Komponenten eines Computers (incl. BIOS) bereitgestellt. Wenn im Computer spezielle Komponenten (z.B. Hochleistungsgrafikkarten) verbaut sind, deren Funktionen das Betriebssystem standardmäßig nicht alle kennt, dann werden spezielle Treiber in das Betriebssystem eingebunden, die dann die einheitliche Schnittstelle anbieten. Darüber werden verschiedene Systemdienste (z.B. Dateiverwaltung, Benutzerverwaltung, usw.) angeboten. Und erst ganz oben liegen die Anwendungsprogramme, die von der unterschiedlichen Hardware nicht mehr viel mitbekommen. Sie laufen auf jedem beliebigen Computer (zumindest im Prinzip).