Informatik 7bi Schuljahr 2018/2019 als PDF exportieren

Informatik 7. Klasse - Schuljahr 2018/19

Lehrinhalte

- Lehrplaninhalte

Remote-Zugriff auf Schulserver

Kapitel

- 1) Virtualisierung
- 2) CMS-Systeme
- 3) Netzwerke
- 4) Betriebssysteme
- 5) Datenbanken
- 6) PHP & MySQL
- 7) C++
- 8) Visual C++

Leistungsbeurteilung

- **Schularbeiten (SA)**
  - 2x SA (2h) pro Semester
- **Mitarbeit (MA)**
  - Aktive Mitarbeit im Unterricht (aMA)
  - Mündliche Stundenwiederholungen (mMA)
  - Schriftliche Stundenwiederholungen (sMA)
- **Praktische Arbeiten (PA)**
  - 1x praktischer Arbeitsauftrag pro Woche

- Aktueller Leistungsstand

Stoff für die 2. Schularbeit in Informatik – 7BI – ??.??.????

Stoff für die 1. Schularbeit in Informatik – 7BI – 09.11.2018

Was wird in der 7. Klasse gemacht?

Nachtrag aus der 6. Klasse (4. Semester)

Angewandte Informatik, Datenbanksysteme und Internet

Web-Techniken

- Das Editieren in einem Content-Management-System beherrschen

5. Semester

Sicherung der Nachhaltigkeit

- Notwendiges Vorwissens für die Kompetenzbereiche dieses Moduls wiederholen und aktivieren
- Grundlagen für die Kompetenzbereiche dieses Moduls ergänzen und bereitstellen

Gesellschaftliche Aspekte der Informationstechnologie

Verantwortung, Datenschutz und Datensicherheit

- Die Bedeutung von Informatik in der Gesellschaft beschreiben, die Auswirkungen auf die Einzelnen und die Gesellschaft einschätzen und Vor- und Nachteile an konkreten Beispielen abwägen können.
- Maßnahmen und rechtliche Grundlagen im Zusammenhang mit Datensicherheit, Datenschutz und Urheberrecht kennen und anwenden können.

Informatiksysteme – Hardware, Betriebssysteme und Vernetzung

Technische Grundlagen und Funktionsweisen (Hardware)

- Aktuelle Entwicklungen auf dem Hardwaresektor kennen
- Mit Hardware-Komponenten praktisch umgehen können

Virtualisierung

- Virtualisierungs-Software für Betriebssysteme und Server einsetzen können
- Betriebssysteme und Software virtualisieren können

Betriebssysteme (Linux)

- Die Arbeitsumgebung (Oberflächen, Tools, Script-Programmierung) von Linux einrichten können
- Anwenderprogramme unter Linux installieren und verwenden können
- Die Bedeutung von Linux als Betriebssystem für Internetdienst kennen
- Im LAN und im Internet mit Linux arbeiten können

Netzwerke

- Grundlagen der Vernetzung von Computern beschreiben und lokale und globale Computernetzwerke nutzen können.
- Netz-Topologien kennen
- Den Datenverkehr in Netzen simulieren und analysieren können
- Netzhardware kennen und praktisch damit umgehen können
- Protokolle und Adressierung kennen und anwenden können
- Sicherheitskonzepte für Netzwerke kennen
- Netztypen (Peer-to-Peer, Server-Client) kennen
- Peer-to-Peer und Server-Client-Netz installieren können
- Einfache Netzadministration durchführen können
- Programme für die Verwendung im Netz installieren können

Angewandte Informatik, Datenbanksysteme und Internet

Suche, Auswahl und Organisation von Information

- Informationsquellen erschließen, Inhalte systematisieren, strukturieren, bewerten, verarbeiten und unterschiedliche Informationsdarstellungen verwenden können.

Datenmodelle und Datenbanksysteme

- Datenbanken durch ein Programm ansteuern können
- Datenbanken benutzen und einfache Datenmodelle entwerfen können.
- Die Charakteristika von SQL kennen
- PHP-Scripts zur Anbindung einer Webseite an eine MySQL-Datenbank erstellen können

6. Semester

Sicherung der Nachhaltigkeit

- Notwendiges Vorwissens für die Kompetenzbereiche dieses Moduls wiederholen und aktivieren
- Grundlagen für die Kompetenzbereiche dieses Moduls ergänzen und bereitstellen

Angewandte Informatik, Datenbanksysteme und Internet

Web-Techniken

- PHP-Scripts zur Anbindung einer Webseite an eine MySQL-Datenbank erstellen können
- MySQL-Datenbank mittels PHP verwalten können

Gesellschaftliche Aspekte der Informationstechnologie

Verantwortung, Datenschutz und Datensicherheit

- Kommunikation mit einem externen Server herstellen können
- Die Bedeutung der Absicherung extern verwalteter Daten einschätzen können

Algorithmik und Programmierung

Algorithmen und Datenstrukturen

- Algorithmen erklären, entwerfen, darstellen können.
- Klassen und Objekte kennen und verwenden können
- Files kennen und einsetzen können
- Datenstrukturen Zeiger und Listen kennen und visualisieren können
- Algorithmen mit Zeigern und Listen erstellen können

Programmierung (Objektorientierte visuelle Programmiersprache)

- Weitere Komponenten der visuellen Programmierung kennen und anwenden können
- Mit einer visuellen Programmiersprache auf fortgeschrittenem Niveau arbeiten können
- Mit Files arbeiten können
- Graphikelemente einsetzen können
- Algorithmen in der visuellen Programmiersprache implementieren können
- Algorithmen mit Zeigern und Listen programmieren können

```
7. Klasse (3 Stunden,  je eine 2h Schularbeit pro Semester)
```

Virtualisierung

Definition

Bei der Virtualisierung handelt es sich um den Prozess der Erstellung einer **softwarebasierten (virtuellen) Komponente anstatt einer hardwarebasierten (physischen)**.

Virtualisieren lassen sich sowohl Anwendungen als auch Server, Storage und Netzwerke. Die Virtualisierung ist unabhängig von der Unternehmensgröße bei Weitem der effektivste Weg zur Reduzierung der IT-Ausgaben bei gleichzeitiger Steigerung der Effizienz und Agilität.

Gründe für Virtualisierung

Durch Virtualisierung kann die Agilität, Flexibilität und Skalierbarkeit der IT erhöht werden. Gleichzeitig werden deutliche Kosteneinsparungen ermöglicht. IT-Komponenten lassen sich einfacher verwalten und kostengünstiger betreiben, da Workloads schneller bereitgestellt, Performance und Verfügbarkeit optimiert sowie Betriebsabläufe automatisiert werden. Weitere Vorteile:

- Senkung der Investitions- und Betriebskosten
- Minimierung oder Vermeidung von Ausfallzeit
- Erhöhung der Produktivität, Effizienz, Agilität und Reaktionsfähigkeit der IT
- Beschleunigung und Vereinfachung des Anwendungs-Provisioning (Bereitstellung von Ressourcen)
- Nachhaltige Planung und einfache Wiederherstellung
- Vereinfachung des Managements von Rechenzentren
- Einfacher Austausch/Einfache Erweiterung von Software (da plattformunabhängig)

Virtualisierungsarten

Eine Einteilung in Gruppen bzw. Kategorien fällt nicht immer ganz leicht, da manche Virtualisierungstechnologien mehreren zugeordnet werden können. Hier findest du eine mögliche Einteilung:

1) Servervirtualisierung (auch Betriebssystemvirtualisierung genannt)

Die Virtualisierung von Servern bedient sich der Virtualisierung von Computern, die auch Hardware-Virtualisierung oder Betriebssystemvirtualisierung genannt wird. Hierbei wird auf physikalischer Computerhardware dem VM Host ein als sog. Hypervisor dienendes Betriebssystem installiert das vorhandene Hardwareressourcen intelligent auf virtuelle Maschinen verteilt. Dadurch ermöglicht diese Konstellation einem Serverbetriebssystem Teile der Vorhandenen Hardware, also Prozessor, Speicher und Anschlüsse, zu nutzen. Dabei wird einem Betriebssystem ein vorhandener Hardwarecomputer vorgespiegelt. Die gängigsten, kommerziellen Lösungen die von Herstellern verfügbar sind VMWare ESX, Citrix XEN, Microsoft Hyper-V sowie IBM MPAR bei professionellen Mainframe

Großrechnersystemen. Freie kostenlose Virtualisierungslösungen für Serverbetriebssysteme sind ebenfalls in großer Anzahl verfügbar. Die bekanntesten wären VMWare ESXi und VMWare Player, XEN, KVM und Oracle VirtualBox.

Man unterscheidet mehrere Arten der Servervirtualisierung:

1.1) Hardwarevirtualisierung

Die wohl am einfachsten zu verstehende Art ist die reine Hardwarevirtualisierung. Hierbei sind nicht die aktuelle Eigenschaften von Intel oder AMD-CPUs gemeint, sondern sogenannte Hardware-Partitions wie sie z. B. in IBMs System p oder Fujitsus Sparc Enterprise Serie realisiert sind. Vereinfacht ausgedrückt kauft der Kunde einen Schrank voller CPUs, Arbeitsspeicherriegel etc. Im Gegensatz zu normalen Servern muss jedoch bei der Erweiterung des Arbeitsspeichers nicht ein neues RAMModul aus dem Keller geholt und explizit in einen Server eingebaut werden. Vielmehr kann dies bei Hardware-Partitions „per Mausklick“ erfolgen, da die vorhandenen Ressourcen innerhalb des „Schranks“ frei auf die logischen Partitions verteilt werden können. Auf jeder so erstellten Partition kann dann ein entsprechendes Betriebssystem installiert werden. Die Virtualisierung erfolgt hierbei durch die Aufteilung der vorhandenen Hardware in kleinere Rechner (die erwähnten Partitions). Vollvirtualisierung

1.2) Vollvirtualisierung

Vollvirtualisierung bezeichnet eine in Software verwirklichte Technologie. Sie kann sowohl als Hypervisor realisiert werden, das heißt die Virtualisierungsschicht läuft direkt auf der Hardware, oder als Hosted-Lösung (siehe unten) In diesen Abschnitt wird erst einmal nur die HypervisorLösung betrachtet. Die Gast-Betriebssysteme müssen bei der Vollvirtualisierung nicht speziell angepasst werden, da diese in der virtuellen Umgebung bekannte Hardware vorfinden. Während das Gastbetriebssystem denkt, auf physikalische Geräte (wie zum Beispiel Netzwerkkarten) zuzugreifen, sind diese jedoch nur virtuell vorhanden. Wenn nun ein Gastbetriebssystem mit einem anderen Rechner kommunizieren will, so sendet es beispielsweise über seine virtuelle Intel EPro1000-Netzwerkkarte Daten ins LAN. Diese Daten müssen nun von der Virtualisierungsschicht über die physikalische Netzwerkkarte weitergeleitet werden („Virtualisierungsoverhead“ für Ein- und Ausgabeoperationen). Reine Rechenoperationen werden direkt auf den physikalischen CPUs ausgeführt. Die Problematik besteht hierbei darin, dass spezielle Befehle unterbunden werden müssen. Als Beispiel sei das Ausschalten einer virtuellen Maschine genannt. Um bei einem einfachen Modell zu bleiben, wird im Folgendem angenommen, dass hierfür das virtualisierte Betriebssystem den CPU-Befehl „Power-Off-Hardware“ ausführt. Würde dieser Befehl jedoch eins-zu-eins vom Hypervisor an den physikalischen Rechner weitergeleitet werden, würde der komplette Server mit allen VMs ausgeschaltet werden – anstatt einer einzelnen VM. Deshalb muss dieser Befehl abgefangen und anders verarbeitet werden – hier wird er durch den Befehl „Power-OffVM“ ersetzt. Dies bedeutet, dass grundsätzlich sämtliche von virtuellen Maschinen ausgeführte Befehle auf solche kritischen Kommandos hin untersucht und bei Bedarf umgeschrieben werden müssen. Dieser Vorgang wirkt sich entsprechend auf die Performance aus („Virtualisierungsoverhead“ für CPU-Befehle).

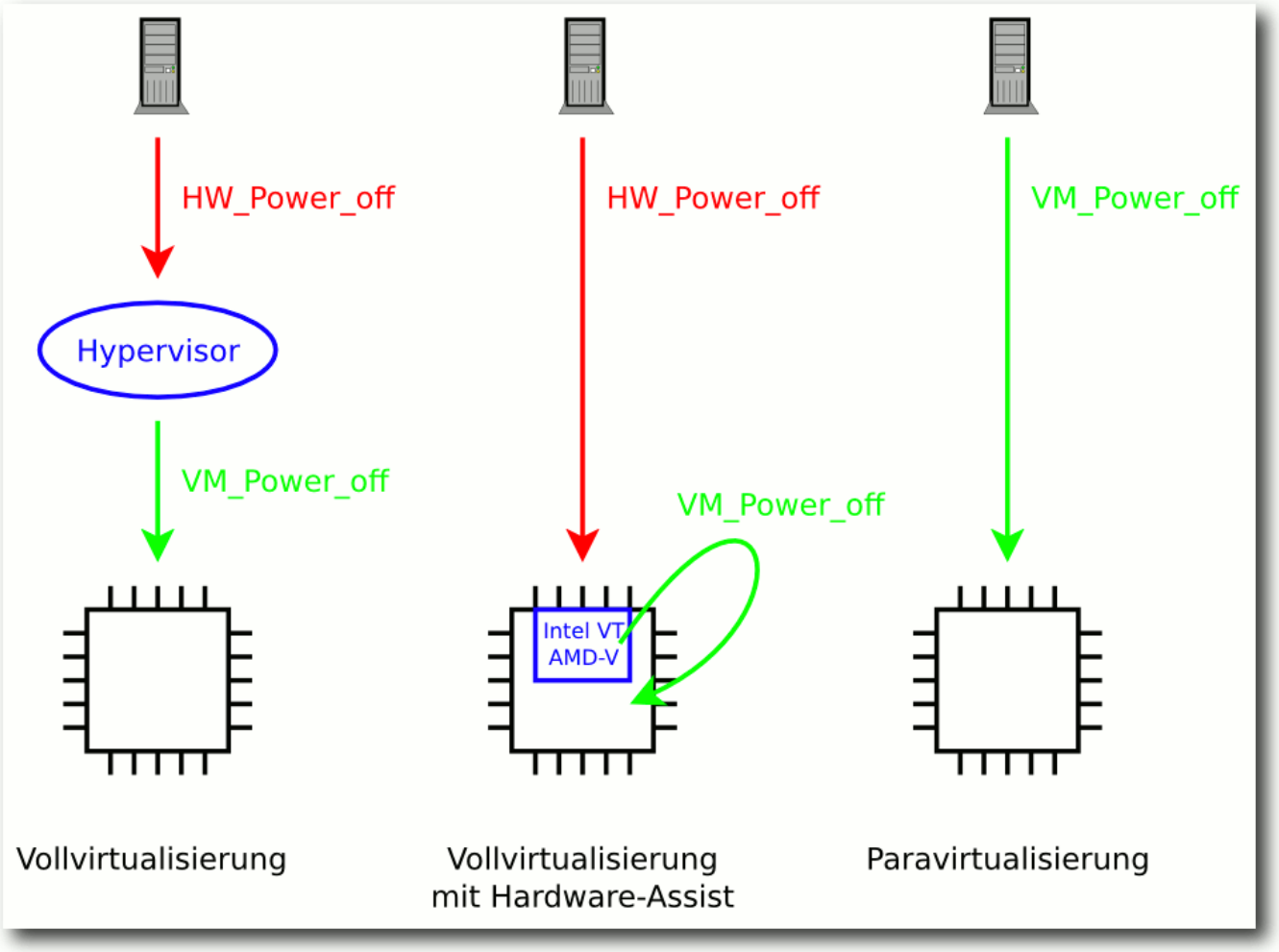
1.3) Hardware-Assisted-Virtualisierungen

Genau hier setzen Hardware-Assisted Virtualisierungen an. Bei diesen Lösungen übernimmt die

Hardware das Umsetzen der Befehle von „Power-Off-Hardware“ zu „Power-Off-VM“. Dies hat zur Folge, dass die Virtualisierungsschicht sich nicht mehr so intensiv um die Befehle der virtuellen Maschinen kümmern muss. Die Technologie wird bei Intel-CPUs als Vanderpool Technology „Intel VT-x“ 4 bzw. bei AMD als AMD-Virtualization „AMD-V“ 5 (früher Codename Pacifica) bezeichnet. In neueren Rechnergenerationen wird dieses Prinzip nicht mehr nur für CPUs sondern auch für Ein- und AusgabeBefehle verwendet (z. B. „Intel VT-d“).

1.4) Paravirtualisierung

Als letzte Technologie in diesem Abschnitt ist die Paravirtualisierung zu nennen. Der Unterschied zu den bisher genannten Techniken ist, dass hierbei das Gastbetriebssystem angepasst werden muss. Die Anpassung sorgt dafür, dass die virtuelle Maschine weiß, dass sie nicht auf physikalischer Hardware läuft und somit direkt den Befehl „Power-Off-VM“ ausführt. Deshalb erzeugt Paravirtualisierung weniger Overhead mit dem Nachteil der nötigen Anpassung des Gastes. Dadurch war diese Technologie zuerst nur Linux-Kernel basierten VMs vorenthalten. Microsoft hat mittlerweile auch für Windows Server 2008 solche Anpassungen entwickelt („Enlightenments“), welche jedoch ausschließlich Vereinfachtes Schema der Betriebssystemvirtualisierung. von Microsoft-Virtualisierungslösungen (sprich von Microsofts Hyper-V) verwendet werden dürfen, wenn nicht explizit ein Vertrag zusätzlich mit Microsoft ausgehandelt wurde. Es ist davon auszugehen, dass Microsoft sich dies entsprechend honorieren lässt. Um dieses Problem etwas zu mildern, wurden spezielle Treiber entwickelt, welche bei einem vollvirtualisierten Gast zumindest Teile paravirtualisiert betreiben können (z. B. der paravirtualisierte SCSI-Treiber derVMware Tools).



2) Desktop Virtualisierung

Die Virtualisierung von Desktop PCs entspricht technisch im weitest gehenden der Virtualisierungstechnik für Server. In der neuesten Generation der Desktop Virtualisierungen kann ein Virtualisierter PC auf beliebige Endgeräte der Anwender wie Laptops, Pads, Thin Clients oder PCs plattformübergreifend gestreamt werden. Für Desktopbetriebssysteme können die professionellen Virtualisierungslösungen für Server ebenfalls verwendet werden. Spezielle Softwarelösungen für Desktop Virtualisierung sind Microsoft Virtual PC; VMWare Workstation und Apple‘s Parallels Workstation. Konkret heißt das ein Windows 10 läuft nicht mehr am Arbeitsplatz-Rechner sondern innerhalb einer virtuellen Server-Infrastruktur (ESX, XenServer, Hyper-V). Die Benutzer verwenden entweder einen Terminal-Services-Client oder direkt einen ThinClient mit Hilfe dessen sie die virtuellen Clients steuern können.

Vorteile sind hierbei, dass sämtliche Server und Client-Betriebssysteme an einem zentralen Ort betrieben werden können (z. B. VMware vSphere-Umgebung im Serveraum). Somit ist eine zentrale Datenhaltung mit verbesserten Backup-, Performance- oder KostenersparnisMöglichkeiten gegeben. Für die Verwaltung der virtuellen Desktop-VMs wurden VMware View und Citrix XenDesktop entwickelt. Einen entscheidenden Nachteil teilen sich jedoch alle Virtualisierungslösungen, die für die (Client-)Benutzer-Interaktion ausgelegt sind: die Grafikkartenperformance. Bei einem physikalischen Client-PC ist die Grafikkarte direkt mit dem Monitor verbunden, während bei einer Client-VM die Daten von der virtuellen Grafikkarte im Serverraum erst über das Netzwerk zur lokalen Grafikkarte und letztlich zum Monitor übertragen werden müssen.

3) Applikations/Anwendungs-Virtualisierung

Die Virtualisierung von Applikationen erlaubt es Softwarepakete in komplexer Konfiguration zeitnah und unabhängig von Benutzerprofilen für Desktop PCs oder Notebooks bereitzustellen. Hierbei wird eine benötigte Anwendung inklusive aller konfigurierten Einstellungen in eine ausführbare .exe Datei umgewandelt. Durch die Bereitstellung der Datei im Netzwerk wird die Installation und Administration auf einzelnen Clients überflüssig was den administrativen Zeitaufwand erheblich verringert. Die entsprechende Software kann für den Außendienst oder das Homeoffice als portable Anwendungsdatei auf Computern gespeichert werden. Verfügbare Lösungen für die Software Virtualisierung sind VMWare ThinApp und Spoon Virtual Application Studio.

Man unterscheidet mehrere Arten der Anwendungsvirtualisierung:

3.1) Gehostete Vollvirtualisierung

Die gehostete Vollvirtualisierung wird in diesem Artikel der Gruppe der Anwendungsvirtualisierungen zugeordnet, während sie ebenfalls der Betriebssystemvirtualisierung zugeordnet werden könnte. Da jedoch die Virtualisierungsschicht nicht direkt auf der Hardware läuft, sondern vielmehr ein Basisbetriebssystem erforderlich ist, innerhalb dessen die Virtualisierung als normale Anwendung läuft, wird sie diesen Abschnitt zugeordnet. Als bekannte Vertreter dieser Gattung wären unter anderem VirtualBox, Microsoft VirtualPC und VMware Server/Workstation zu nennen. Die Vorteile liegen auf der Hand: Es ist nicht mehr die Virtualisierungsschicht für das Ansprechen der physikalischen Hardware verantwortlich, sondern das zu Grunde liegende Betriebssystem (z. B. Linux, Windows, Mac OS X). Somit müssen keine eigenen Treiber entwickelt werden. Beispielsweise unterstützt VMware ESX-Server 4 nur eine begrenzte Anzahl an Netzwerkkarten, während die Lösung

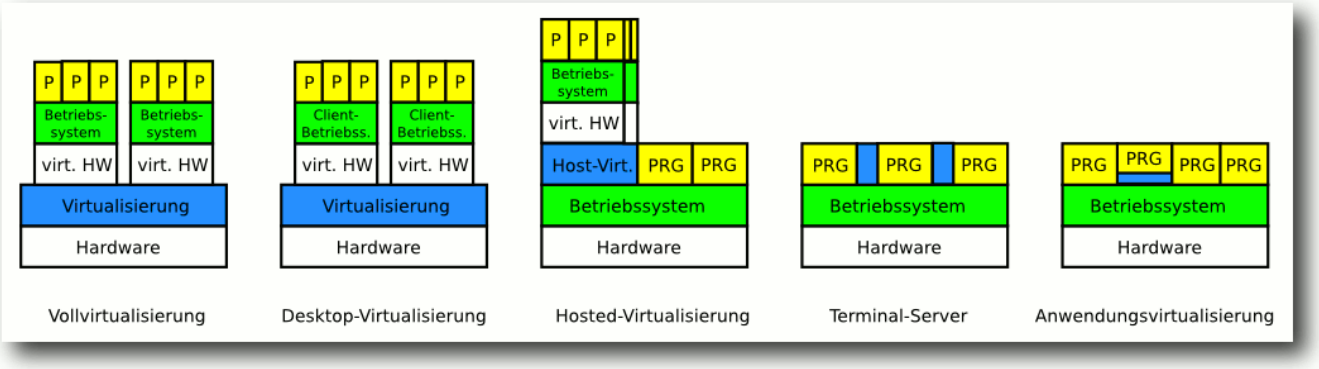
mit VMware Server sozusagen alle von Linux und Windows unterstützten Geräte verwenden kann. Auch Citrix XenServer, welches auf einem Linux-Kernel basiert und somit theoretisch sämtliche Linux-Treiber verwenden könnte, unterstützt nur einen Teil derer. Der Hauptnachteil von Hosted-Lösungen ist jedoch, dass das Virtualisierungsprogramm nur noch eines von vielen im Host-Betriebssystem ist und entsprechend auch als solches behandelt wird. Des Weiteren ist nicht garantiert, dass ein für Windows zertifizierter Treiber auch mit sämtlichen auf Windows ausführbaren Virtualisierungslösungen fehlerfrei funktioniert, während die Hersteller von Hypervisor-Produkten ihre Treiber genau für diesen Anwendungsfall testen.

3.2) Terminal-Server

Die wohl bekannteste Art der Anwendungsvirtualisierungen sind Terminal-Server. Hierbei werden nicht verschiedene Betriebssystem-Instanzen parallel auf einem Rechner ausgeführt, sondern nur parallele Sitzungen mehrere Nutzer innerhalb eines Betriebssystems. Unter Windows wären Microsofts Terminal Services und Citrix XenApp zu nennen, während Linux mit einer Vielzahl von Lösungen aufwarten kann. Dies liegt höchstwahrscheinlich daran, dass Linux schon immer als Mehrbenutzer-System entwickelt wurde. So können bereits die StandardDesktop-Manager (kdm, gdm) über XDMCP Sitzungen für Remote-Benutzer bereitstellen. Um Anwendungen in einer Mehrbenutzer-Umgebung von einander abzuschotten, wird normalerweise auf Home-Verzeichnissen und Variablen gesetzt. Dabei liegen die Programmdaten nur einmal vor (z. B. C:\Program Files\... bei Windows bzw. /usr/bin bei Linux), während für das Speichern der Dokumente eine Variable %HOMEPATH% (z. B. C:\Users\admin\) bzw. $HOME (z. B. /home/admin/) verwendet wird.

3.3) Anwendungsvirtualisierungen

Eine verwandte Art sind die (für viele Anwender missverständlich) direkt als Anwendungsvirtualisierungen betitelten Lösungen. Linux-Benutzer kennen ein ähnliches Verfahren seit Jahren. Gemeint ist eine chroot-Umgebung. Hierbei wird eine Anwendung in einer vom eigentlichen Betriebssystem abgekoppelten Umgebung („Sandbox“) ausgeführt. Die Technologien gehen hierbei heutzutage jedoch weiter und spiegeln eher das Verhalten von UnionFS wieder. Die Produkte der führenden Hersteller nennen sich VMware ThinApp, Citrix XenApp Streaming und Microsoft App-V . Alle beruhen auf dem Prinzip, dass ein Programm denkt, es laufe ungehindert im Betriebssystem, während in Wirklichkeit jedoch sämtliche Lese- und Schreiboperationen abgefangen und bei Bedarf umgebogen werden können. Einem Programm kann somit simuliert werden, dass es z. B. Daten von C:\temp nach D:\temp kopieren kann. In Wirklichkeit existieren jedoch die Ordner nicht einmal im Dateisystem sondern nur innerhalb der virtualisierten Anwendungsumgebung.



4) Storage Virtualisierung

Die Virtualisierung von Speichersystemen stellt die Zusammenfassung vorhandener Speicherressourcen wie Festplatten, NAS und SAN Systeme dar. Hierbei werden die vorhandenen Datenspeicher unterschiedlicher Technologien und Hersteller in einem gemeinsamen großen Speicherpool zusammengefügt. Einzelne, vorhandene Rechnersysteme können benötigten Speicherplatz in flexibler Größe aus dem virtuellen Speichersystem in Anspruch nehmen. Durch Hinzufügen weiterer Speicherhardware kann bei anwachsenden Datenmengen der Speicherpool im laufenden Betrieb beliebig vergrößert werden. Zusätzlich minimiert Storage-Virtualisierung den Aufwand zur Schaffung von Redundanz als Schutzmaßnahme gegen Datenverlust oder Betriebsausfälle. Man unterscheidet zwischen drei Arten der Storage-Virtualisierung. Die Hostbasierte Lösungen wie Datacore SANSymphony, Symantec Storage Foundation for Windows oder HPs LeftHand Virtual SAN laufen auf eigenen Rechnersystemen. Die zweite Möglichkeit findet direkt in Speicherhardware wie SAN Systemen statt bei denen weitere Geräte und Switches als zusätzliche vermittelnde Schicht ins SAN integriert werden. Der Storage Controller erkennt diese als Hostsystem während zugreifende Hosts diese als Storage erkennen. Die Produkte solcher kombinierter Systeme sind u.A. EMC Invista, LSI Logic StoreAge und HPs SVSP. Die dritte Möglichkeit ist Storage Virtualisierung die direkt in einem dedizierten Controller, der Anschlussmöglichkeiten für verschiedene Speichersysteme anbietet, stattfindet. Hierzu zählen IBM Systems SVC (Storage Virtualisierungs Controller) oder VMWare vSphere Storage Appliance.

5) Netzwerk Virtualisierung

Die Virtualisierung von Netzwerken bietet die Möglichkeit ein Firmennetzwerk über bauliche Abgrenzungen hinweg in mehrere Teilnetze aufzuteilen. Bei einer klassischen physikalischen Netzwerkinfrastruktur gilt ein Adressbereich für das ganze Unternehmen. Zugriffsberechtigungen und Netzwerkkontrolle kann bei dieser Konfiguration nur durch Dateiberechtigungen und komplizierte Firewall Lösungen ausgeübt werden. Eine physikalische Trennung einzelner Abteilungen ist bei dieser Konfiguration beinahe unmöglich. Bei einem virtualisierten Netzwerk können einzelne Clients sogar über Stockwerksgrenzen hinweg einer einzelnen Netzwerkgruppe zugeordnet werden. Jedes der so erstellten virtuellen Netzwerke hat einen eigenen Adressbereich obwohl sich diese im gleichen physikalischen Netzwerk befinden. Ressourcen der Entwicklungsabteilung z.B. sind somit vor ungewollten oder unautorisierten Zugriffen durch eine andere Abteilung auf unterster Ebene abgesichert. Mittlerweile implementiert fast jeder Hersteller von Netzwerkhardware die Möglichkeit zur Virtualisierung von Netzwerken in seine Produkte. Voraussetzung sind Layer2 oder Layer3 fähige Netzwerkswitche. Die besten Erfahrungen bei der Netzwerkvirtualisierung hatten wir mit Produkten der Hersteller Cisco, Extreme Networks, HP und Juniper.

VMNetwerkverbindungsarten

VMware Workstation bietet mehrere Möglichkeiten, die Netzwerkressourcen des Hosts zu nutzen. Je nach Anforderungen wird man eine dieser Möglichkeiten auswählen. Hier sind die wichtigsten erklärt:

Bridge

Hier benutzt der Gast die Netzwerkverbindung des Hosts mit einer eigenen IP in dessen lokalem Netz.

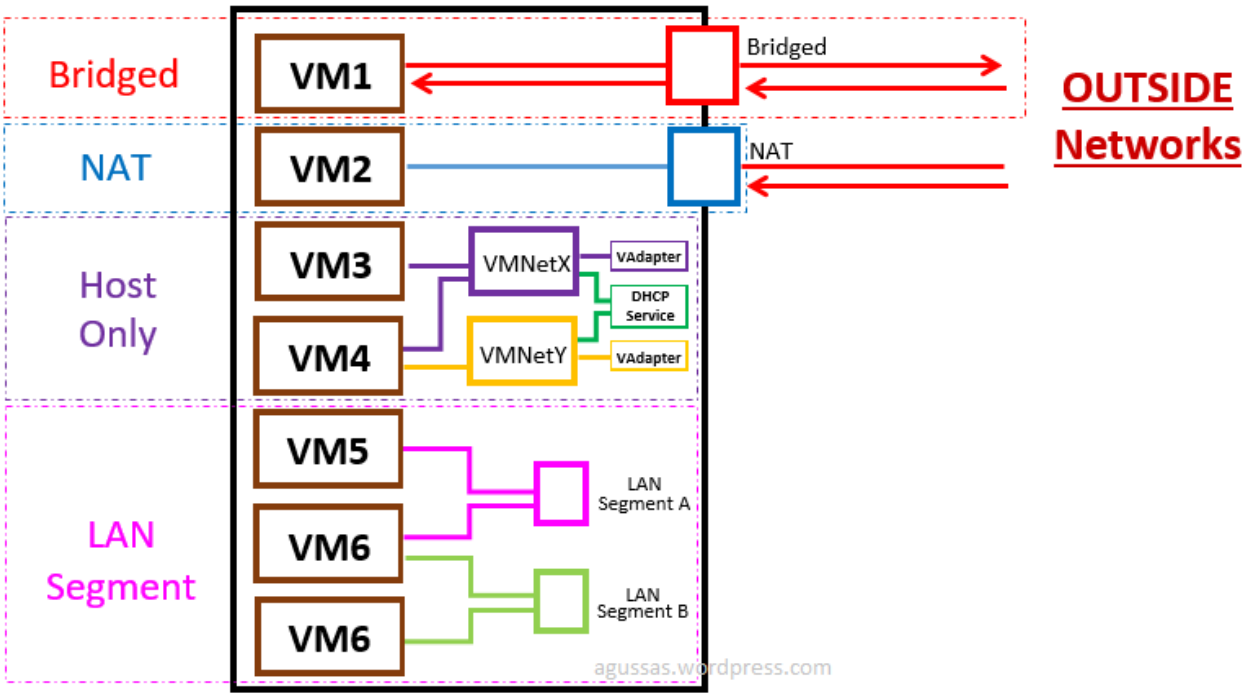
Das kommt der Installation eines separaten Rechners gleich – auch von außen her gesehen.

NAT

Der Gast bekommt eine IP in einem von VMware dafür eingerichteten privaten Netz, das vom physischen Netz des Hostrechners verschieden ist. Es kommt ein virtueller Netzwerkadapter zum Einsatz, den VMWare im Host einrichtet und mit einer weiteren IP des privaten Netzes konfiguriert; der Host wird auf Seite des Clients als Default-Gateway eingetragen. Via Adressübersetzung (NAT) kann der Gast nun das Host-Netz erreichen. Ressourcen des Gasts, z. B. Windows-Freigaben, sind nur vom Host aus unter der privaten IP des Gasts erreichbar. Von außen her ist nur eine IP sichtbar; dass sich dahinter mehrere Systeme befinden, kann nur durch Analyse des Datenverkehrs erkannt werden.

Host only

Auch hier richtet VMware ein privates Netz ein. Es werden jedoch keine Regeln definiert, die Datenpaketen des Gastes erlauben, dieses private Netz zu verlassen. Wenn zusätzliche Verbindungen gewünscht sind, müssen diese auf dem Host durch Routing (Forwarding) explizit hergestellt oder als Serverdienst (z. B. Proxy) realisiert werden. Diese Methode eignet sich vorzüglich, um einen dedizierten Server im lokalen Netz zu betreiben. Beispielsweise würde man für einen Terminalserver nur den Port für RDP freischalten. Damit wäre die Maschine für ihren eigentlichen Bestimmungszweck im Netz erreichbar, während z. B. Viren, die sich über andere Ports verbreiten, beim Host enden würden. Auch für private Zwecke eignet sich diese Methode, da damit verhindert werden kann, dass der Gast unerwünschte IP-Verbindungen (z. B. für Spamversand) aufbaut. Anmerkung: Mehrere Gastsysteme können separate private Netze nutzen, die nur miteinander kommunizieren können, wenn es jeweils im Hostsystem explizit konfiguriert ist.



CMS - Systeme

Ein CMS, ein **Content-Management- oder auch Redaktionssystem**, dient zur **Verwaltung der Inhalte (Einpflege von Texten, Bildern, Videos und Daten)** einer oder auch mehrerer **Websites**. Content-Management-Systeme sind **mandantenfähig**, d.h. sie können mehrere Kunden (Mandanten) bedienen, ohne dass diese Einblick in die Benutzerverwaltung des anderen haben. Ein typisches Feature eines CMS ist die **individualisierbare Rollenverteilung**: Unterschiedlichen Nutzern können unterschiedliche Rechte zugeteilt werden. Zudem gibt es meist **praktische Funktionen** für den Export und Import von Contents. Content-Management-Systeme sind **keine starren Gebilde**, sondern werden ständig **weiterentwickelt**. Das geschieht durch **Updates** oder sogenannte **Plugins**, die vom Nutzer relativ einfache heruntergeladen und installiert werden können.

Verbreitete CMS-Systeme

WordPress

Ursprünglich ein reines Blogsystem ist es heute mit über 70 Mio. Installationen das am weitesten verbreitete CMS.

Vorteile

- Installations- und Einrichtungsaufwand überschaubar
- Riesige Auswahl an kostenlosen bzw. -günstigen Designs
- Vielfältige Erweiterungsmöglichkeiten durch Plugins
- Ideal für SEO-Maßnahmen (sehr gute Tools: z.B. YOAST)

Nachteile

- WordPress braucht jede Menge Systemressourcen
- Ladegeschwindigkeit bei hohem Traffic oft langsam
- Viele Updates, teilweise mit Sicherheitsrisiken

TYPO3

Content-Management-Systeme: Typo3-LogoDas „Open Source Flaggschiff“ mit mehr als 9 Mio. Installationen und 500.000+ Websites.

Vorteile

- Weitverbreitet, viele Experten und Entwickler
- Viele Funktionen
- Erheblich schneller als WordPress, auch bei hoher Besucherfrequenz

Nachteile

- Das Setup ist komplex und für den Laien ungeeignet
- Auch bei Backend-Anpassungen sind profunde Kenntnisse im Administrationsbereich erforderlich

---

Joomla

Content-Management-Systeme: Joomla-LogoIst schon lange auf dem Markt und hat mit 1,2 Mio.+ Downloads eine eingeschworene Fangemeinde. Durch einen Entwicklungsstopp vor ein paar Jahren ist Joomla ein wenig ins Hintertreffen geraten. Derzeit holt dieses CMS allerdings wieder mächtig auf.

Vorteile

- Installation und Einrichtung einfach und gut dokumentiert
- Viele Erweiterungen und vorgefertigte Designs (ähnlich wie bei WordPress)

Nachteile

- Beliebtes Ziel von Hackern, nicht zuletzt aufgrund der vielen Erweiterungsmöglichkeiten (gilt übrigens auch für WordPress)
- Beim Rollen- und Rechtemanagement gibt’s Luft nach oben

⇒ 2.01) Joomla Installation

Drupal

Content-Management-Systeme: Drupal-LogoDrupal ist ein Baukaustensystem mit einer riesigen Auswahl an Features. Obwohl es unter die Content-Management-Systeme fällt, ist es eigentlich ein Content-Management-Framework (CMF). Drupal funktioniert im Grunde wie Lego – man kann alles damit bauen.

Vorteile

- Drupal verfügt über ein differenziertes Rollen- und Rechtesystem
- Es hat jede Menge Funktionen, die als Baustein in das System integriert werden können
- Das Backend ist voll individualisierbar

Nachteile

- Das Drupal-Setup ist vergleichsweise kompliziert
- Eingriffe im Backend und am Server erfordern Routine

JOOMLA Installation unter Ubuntu

Voraussetzungen

Einzige Voraussetzung ist ein Webserver (bspw. Apache) mit geladenem PHP5-Modul sowie MySQL als Datenbank. Eine Schnellanleitung zur Installation ist dem Artikel LAMP zu entnehmen. Detail-Informationen finden sich im Wiki in den folgenden Artikeln.

- Webserver (z.B. Apache)
- PHP
- MySQL

siehe https://wiki.ubuntuusers.de/Joomla%21/

Installation von Apache

- sudo apt-get install apache2
- Anleitung: https://wiki.ubuntuusers.de/Apache_2.4/
- Webverzeichnis liegt auf `/var/www/html`
- Server-Ip-Adresse anzeigen lassen mit `ifconfig`
- Überprüfung des Webservers durch Aufruf der IP-Adresse mit Browser

Installation von PHP

- sudo apt-get install php
- sudo apt-get install php-cli
- sudo apt-get install libapache2-mod-php7.0
- sudo apt-get install php-mysql
- Anleitung: https://wiki.ubuntuusers.de/PHP/
- Eventuell müssen Updates eingespielt werden: sudo apt-get update
- Überprüfung des Webserver-PHP-Moduls durch eine index.php Seite mit dem Befehl **phpinfo();**
- PHP-Version ermitteln –> php -v

Installation von MySQL

- sudo apt-get install mysql-server
- PW: schule
- Anleitung: https://wiki.ubuntuusers.de/MySQL/

Installation vom Modul PHP-MySQL

- sudo apt-get install php-mysql

Installation von Joomla

- Download von Joomla unter https://downloads.joomla.org/de/cms/joomla3/3-8-12/Joomla_3-8-12-Stable-Full_Package.zip?format=zip
- Entweder am Host-System downloaden und in die VM kopieren mittels WinScp über SSH (Dazu muss man vorher den Dienst ssh installieren) oder direkt mittels dem Befehl wget https://downloads.joomla.org/de/cms/joomla3/3-8-12/Joomla_3-8-12-Stable-Full_Package.zip?format=zip am Gastsystem downloaden
- Entpacken mittels unzip
- Rechte setzen für den Webuser www-data (chown www-data:www-data /var/www/html -R)

Mögliche Probleme

- sudo apt-get update
- sudo apt-get install php-xml
- Neustart des Servers: `init 6`

MySQL Root Passwort zurücksetzen

- Passwort des mysql-Users debian-sys-maint auslesen in der Datei /etc/mysql/debian.cnf
  - sudo less /etc/mysql/debian.cnf
    - Man „merkt“ sich die Buchstaben-Zahlenkolonne
- mysql -u debian-sys-maint -p
  - Passwort eingeben (gemerkte Buchstaben-Zahlenkolonne)
- Jetzt befindet man sich auf der mysql-Konsole, folgenden Befehl eingeben:
  - `UPDATE mysql.user SET authentication_string=PASSWORD('schule'), plugin='mysql_native_password' WHERE User='root' AND Host='localhost';`
  - `flush privileges;`
  - `exit;`
- mysql-Server neu starten:
  - `/etc/init.d/mysql restart`
- Jetzt kann man mit dem User root einsteigen:
  - `mysql -u root -p`
  - Passwort schule eingeben
- Jetzt kann Joomla installiert werden.

NETZWERKE

Allgemeine Netzwerkgrundlagen

Netzwerk-Grundlagen

Größenordnung von Netzwerken

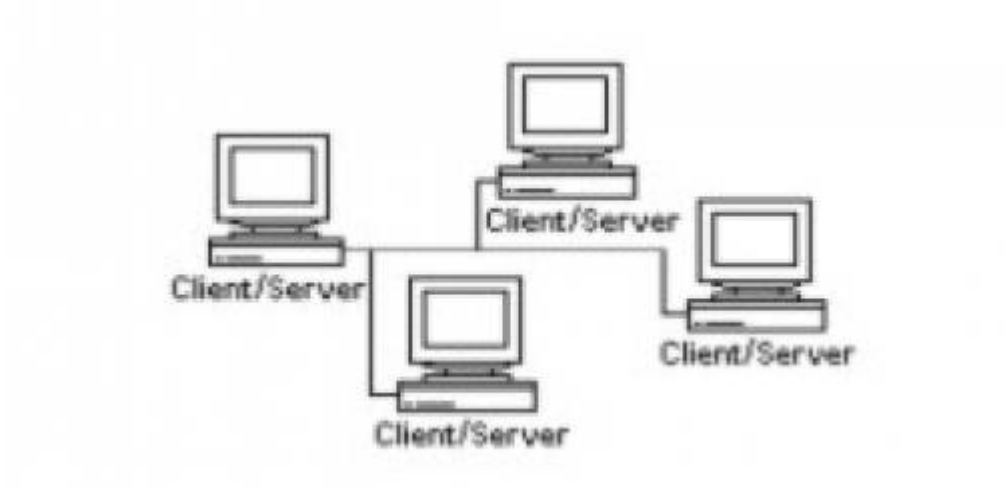
- **LAN** (Local Area Network): lokale Netze (meist innerhalb eines Gebäudekomplexes)
- **WAN** (Wide Area Network): große bis weltumspannende Netze; Beispiel: Telefonnetz, ISDN-Netz, VNET (IBM-eigenes Netzwerk)
- Der Begriff **MAN** (Metropolitan Area Network) ist eigentlich öffentlichen Netzen vorbehalten; in letzter Zeit verwenden aber auch Anwender mit vielen vernetzten Betriebsstellen (Banken) diesen Ausdruck.
- Netzwerke wie das Internet (die aus vielen, weltweit miteinander verbundenen Netzwerken bestehen), werden manchmal auch als **GAN** (Global Area Network) bezeichnet.

Peer-to-Peer-Netze und Client-Server-Architekturen

Man unterscheidet zwei „Philosophien“:

Peer-to-Peer-Netzwerke

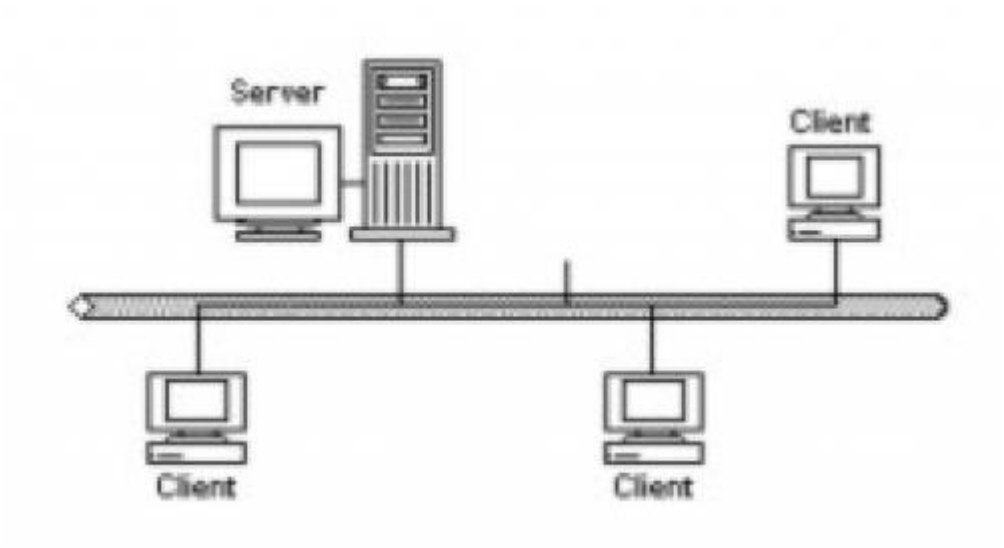
Bei einem solchen Netz können prinzipiell alle in das Netz eingebauten PCs ihre Ressourcen anderen PCs bzw. Anwendern zur Verfügung stellen. Typische Vertreter: NetWare Lite (Novell), Windows for Workgroups (Microsoft), LANtastic (Artisoft), Windows 95/98/ME (Microsoft), Windows NT Workstation (Microsoft), Windows 2000/XP Professional (Microsoft).



Peer-to-Peer-Netze brauchen keinen eigenen Server-Rechner, da jeder PC Server-Funktionen übernehmen kann.

Client/Server-Architekturen

Hier gibt es eine Trennung der Ein-/Ausgabefunktion von der eigentlichen Verarbeitung. Auf der Workstation laufen Programme, die nur für die Ein- und Ausgabe zuständig sind (Frontend-Software), während – unbemerkt vom Anwender – das entsprechende Backend-Programm auf dem Server seine Aufgaben erfüllt (z.B. Speicherung, Suche von Daten). Das grundlegendste Backend-Programm ist das Netzwerk-Betriebssystem.



Die meisten Netzwerke arbeiten so, dass der Server dabei seine Fähigkeiten den anderen Rechnern (Workstations) zur Verfügung stellt. Einen Server, der ausschließlich das Netzwerk und die Datenübertragungen im Netzwerk verwaltet und kontrolliert, bezeichnet man als Dedicated Server. Ist der Server selbst gleichzeitig als Workstation verwendet, so spricht man von einem Non-Dedicated Server.

Server-Betriebssysteme

Für einen Client/Server-Netzwerkbetrieb benötigt man für den Server eigene Betriebssysteme. Netzwerk-Betriebssysteme müssen Multiprocessing unterstützen.

Typische Netzwerk-Betriebssysteme

Novell Open Enterprise Server (früher NetWare)

Dieses Betriebssystem hat alle Kommunikationseigenschaften, die für Netzwerkbetrieb notwendig sind; außerdem werden verschiedenste Einzelplatz-Betriebssysteme unterstützt. Novell NetWare eignet sich daher besonders gut für heterogene Netzwerke. Die Grundidee ist, dass bei Novell NetWare meist dedicated servers eingesetzt werden, auf denen nicht gearbeitet werden kann. Versionen von Novell NetWare 2.11, 3.11 (Nachfolger 3.12), 4.x, 5.x, 6.x, OES1, NetWare for SAA (für Anbindung von Großrechnern wie AS/400)

Microsoft Windows-Serverbetriebssysteme

Typisch für die Microsoft-Serverproduktlinie ist die Möglichkeit, auch Anwendersoftware einsetzen zu können. Damit sind verbesserte Möglichkeiten der Protokollierung und Auswertung gegeben. Die aus den Microsoft Client-Betriebssystemen bekannte Oberfläche ermöglicht rasches Einarbeiten und die Konzentration auf die eigentlichen Systembetreuungsaufgaben. Versionen Windows NT 4.0 Server-Familie, Windows 2000 Server-Familie, Windows Server 2003-Familie

Unix Dialekte

SCO-Unix (SCO = Santa Cruz Operation), Xenix, Sinix, AIX, ULTRIX, Irix, Linux, ...
Auf den Unix-Dialekt Linux soll gesondert verwiesen werden, da es – im Vergleich zu den anderen Dialekten – sehr preisgünstig ist. Linux bietet (mit kleinen Einschränkungen) die volle Unix-Funktionalität!

Netzwerk-Topologien

Die Struktur eines Netzwerks bezeichnet man als Topologie. Wie wichtig die Struktur eines Netzwerks ist, merkt man bei einem Leitungsausfall: ein gutes Netzwerk findet bei einem Leitungsausfall selbstständig einen neuen Pfad zum Empfänger.

Physikalische und logische Topologie

Interessant ist, dass sich die **sichtbare Topologie** (also die physische Verkabelungsstruktur) vom tatsächlichen Datenfluss unterscheiden kann. Deshalb verwendet man für die hardwaremäßige Realisierung den Begriff **physikalische Topologie** während man für den tatsächlichen Datenfluss den Begriff „logische Topologie“ verwendet.

Die wichtigsten Netzwerktopologien sind:

Bus-Topologie

ALLE GERÄTE nutzen DASSELBE KABEL

Bei einem Bussystem sind alle Rechner hintereinander geschaltet und über Abzweige (T-Stücke) an das Netzwerkkabel angeschlossen. Problem: Eine Verbindungsunterbrechung betrifft den ganzen Bus!

Vorteile

- Relativ niedrige Kosten, da geringe Kabelkosten
- Ausfall einer Station führt zu keinem Netzausfall

Nachteile

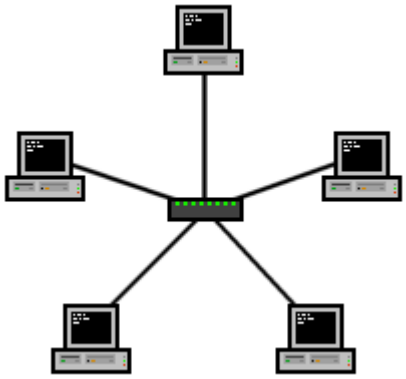
- Alle Daten über ein Kabel
- Nur eine Station kann senden. Alle anderen sind blockiert.
- Eine Störung an einer Stelle (z.B.: Defektes Kabel) führt zu einem Netzausfall (⇒ aufwendige Fehlersuche)
- Unverschlüsselter Netzwerkverkehr kann direkt am Bus (=Kabel) mitgelesen werden

Einsatzgebiet

Früher aufgrund der niedrigen Kosten häufig verwendet, heute spielt die Bus-Topologie keine Rolle mehr und wurde von der Stern-Topologie verdrängt.

Bus-Topologie - Details

Stern-Topologie



JEDES GERÄT nutzt EIN KABEL.
Damit ist es zu einem Verteiler verbunden. Es existiert eine Punkt-zu-Punkt Verbindung zwischen Verteiler und Gerät. Als Verteiler kann ein HUB oder ein SWITCH dienen.

Vorteile

- Ausfall einer Station oder eines Defekts an einem Kabel führt zu keinem Netzausfall
- Aktive Verteiler (Switch, Hub) dienen gleichzeitig als Signalverstärker
- Bei richtiger Konfiguration können zwei Stationen die volle Bandbreite des Übertragungsmediums für ihre Kommunikation nutzen, ohne andere Stationen dabei zu behindern. Diese physikalische Topologie erlaubt somit sehr hohe Datendurchsatzraten.
- Weitere Stationen oder Verteiler können einfach hinzugefügt werden. Sehr leicht skalierbar.

Nachteile

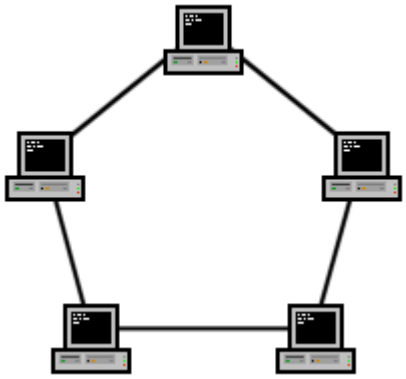
- Große Kabelmengen
- Beim Ausfall des Verteilers ist kein Netzverkehr mehr möglich

Einsatzgebiet

Im praktischen Einsatz bei lokalen Netzwerken findet die Stern-Topologie Verwendung. Häufigste Form der Verkabelung.

Stern-Topologie - Details

Ring-Topologie



JEDES GERÄT ist mit ZWEI NACHBARN verbunden.

Die Ring-Topologie ist eine geschlossene Form, es gibt keinen Kabelanfang und kein Kabelende.
Es handelt sich jeweils um eine Punkt-zu-Punkt Verbindung zwischen den Rechnern.
Jede Station hat genau einen Vorgänger und einen Nachfolger.
Datenverkehr findet immer nur in eine Richtung statt.

Vorteile

- Vorgänger und Nachfolger sind festgelegt
- Alle Stationen verstärken das Signal
- Alle Stationen haben gleiche Zugriffsmöglichkeit
- Leicht umsetzbar

Nachteile

- Ausfall einer Station oder eines Kabelteils führt zu einen Netzausfall
- Hoher Aufwand bei der Verkabelung (Jede Station braucht 2 Netzwerkkarten)
- Leicht abhörbar
- langsame Datenübertragung bei vielen Stationen

Einsatzgebiet

Physikalische Anwendung gibt es heute keine mehr.
Logische Anwendung findet sie im Token Ring.

W Ring-Topologie - Details

Mischformen

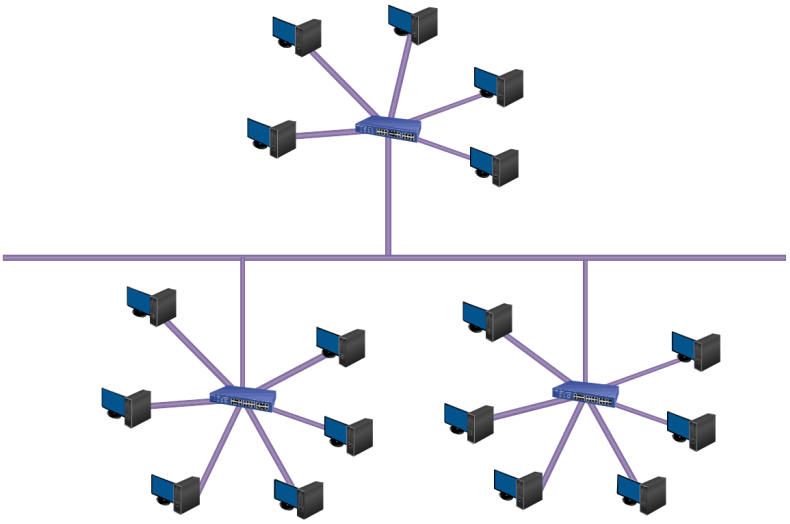
Sind zumeist **Kombinationen aus Bus, Stern und Ring**.

Backbone

Unter einem Backbone („Rückgrat“) wird die physikalische Verbindung zwischen einzelner Teilnetze verstanden. Es wird auch oft als Hintergrundnetz betitelt und verbindet z.B. mehrere Gebäude.

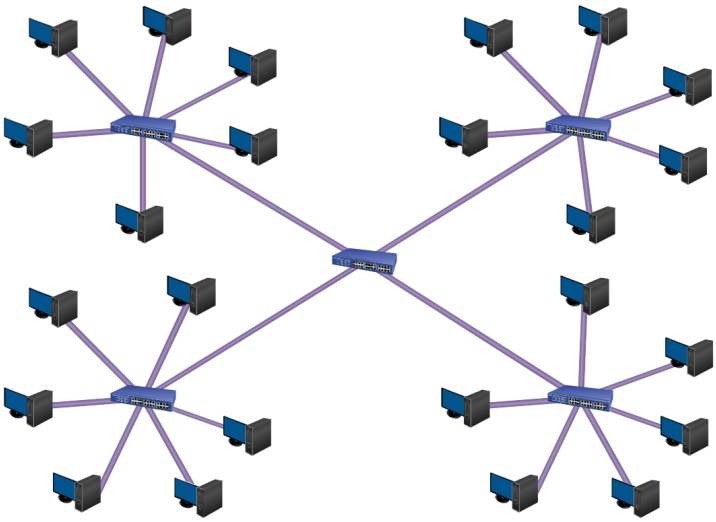
Stern-Bus-Netz

Ein Stern-Bus-Netz entsteht, wenn mehrere Verteiler über einen Bus miteinander verbunden sind. Häufig sind so mehrere Stockwerke miteinander verbunden.



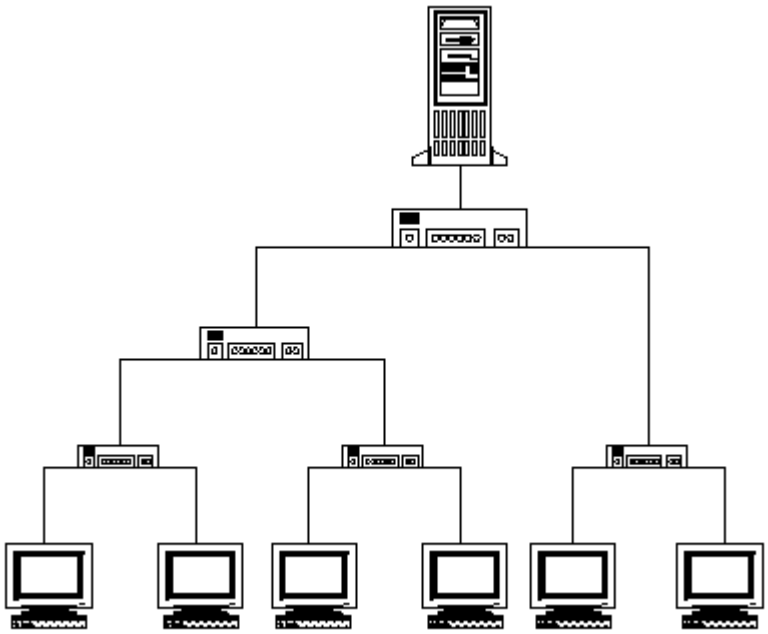
Stern-Stern-Netz

Ein Stern-Stern-Netz entsteht, wenn mehrere Verteiler wiederum über einen Verteiler verbunden sind. Häufigste Anwendung ist wiederum das Verbinden von mehreren Subnetzen (z.B. Netze in verschiedenen Stockwerken).
Fällt der Hauptverteiler aus, so kann zwischen den Stockwerken nicht mehr kommuniziert werden. Jedoch kann man auch die Hauptverteiler redundant auslegen.



Baum

Eine Baum-Topologie wird so aufgebaut, dass, ausgehend von der Wurzel, eine Menge von Verzweigungen zu weiteren Verteilungsstellen existiert.
Es handelt sich somit um eine Erweiterung der Stern-Stern-Topologie auf mehrere Ebenen.



Maschen-Topologie

Vorherrschende Netzstruktur in großflächigen Netzen (z.B. öffentliche Telekommunikationsnetze).
Maschen-Topologie - Details

Zell-Topologie

Die Zell-Topologie kommt hauptsächlich bei drahtlosen Netzen zum Einsatz. Eine Zelle ist der Bereich um eine Basisstation (z.B. Wireless Access Point), in dem eine Kommunikation zwischen den Endgeräten und der Basisstation möglich ist.
Zell-Topologie - Details

Übertragungsmedien

Die Übertragungsmedien sind die Straßen der Daten. Der Aufbau dieser Straßen muss sehr gut geplant werden, um alle aktuellen Anforderungen bzw. eventuelle zukünftige Anforderungen ohne großartige Veränderungen zu erfüllen.

Als **Maßeinheit für die Übertragungsgeschwindigkeit** werden die Werte in **bit/s, b/s bps, -> also Bit pro Sekunde** angegeben. Achtung: Nicht zu verwechseln mit **Byte/s -> Byte pro Sekunde**!!

`C= D/t` `(bits)/(s)`

1) Rechenbeispiel:

Es werden 100MB in 10s übertragen. Wie hoch ist die Übertragungsgeschwindigkeit?

- D=100MByte
- t=10s

Rechenschritt	**Berechnung**
D umwandeln in bits	`100*1024*1024*8 = 838860800` `bits`
C berechnen	`C=D/t=(838 860 800)/10=83886080` `(bit)/(s)`
C umwandeln in Mbit/s	`(83886080)/(1024)/(1024)=80` `(Mbit)/(s)`

2) Rechenbeispiel:

Max hat eine Datentransferrate von 10Mbit/s Download und 2Mbit/s Upload.

a) Wie lange braucht er, um 10MB runterzuladen?

- D=10MB
- C=10Mbit/s

Rechenschritt	**Berechnung**
D umwandeln in bits	`10*1024*1024*8 = 83886080` `bits`
C umwandeln in bit/s	`10*1024*1024=10485760` `(bit)/(s)`
Formel umformeln	`t=(D)/(C)` `(bits)/((bit)/s)`
In Formel einsetzen	`t=83886080/10485760=8` `s`

b) Wie lange braucht er, um 10MB hochzuladen?

Rechenschritt	**Berechnung**
D umwandeln in bits	`10*1024*1024*8 = 83886080` `bits`
C umwandeln in bit/s	`2*1024*1024=2097152` `(bit)/(s)`
Formel umformeln	`t=(D)/(C)` `(bits)/((bit)/s)`
In Formel einsetzen	`t=83886080/2097152=40` `s`

Leitergebundene Übertragung

Bei einer leitergebundenen Übertragung werden Medien in Form von Kabeln benötigt (Metallische Leiter, Glasfaser).
Ein Kabel besteht zumindest aus einer Ader (=Faser).
Mehrere Adern sind durch entsprechende Isolationssschichten getrennt.
Alle Adern wiederum werden von einem Mantel als Schutz umgeben.
Die Übertragung selbst erfolgt durch elektromagnetische Schwingungen.

Koaxialkabel

Das früher verwendete Koaxialkabel ist in modernen Netzen praktisch vollständig von Twisted Pair-Kabeln (TP) und Lichtwellenleiter (LWL) abgelöst worden.

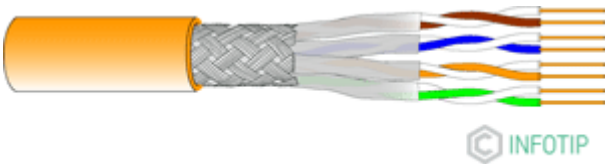
Es besteht aus

- einem Innenleiter (Kupfer, Stahlkupfer)
- einer Isolation (Dielektrikum)
- einer Abschirmung (Metallgeflecht schützt vor magnetischen Störungen –> Rauschen & Übersprechen)
- einem Mantel

Es waren bis zu 10Mbps möglich:

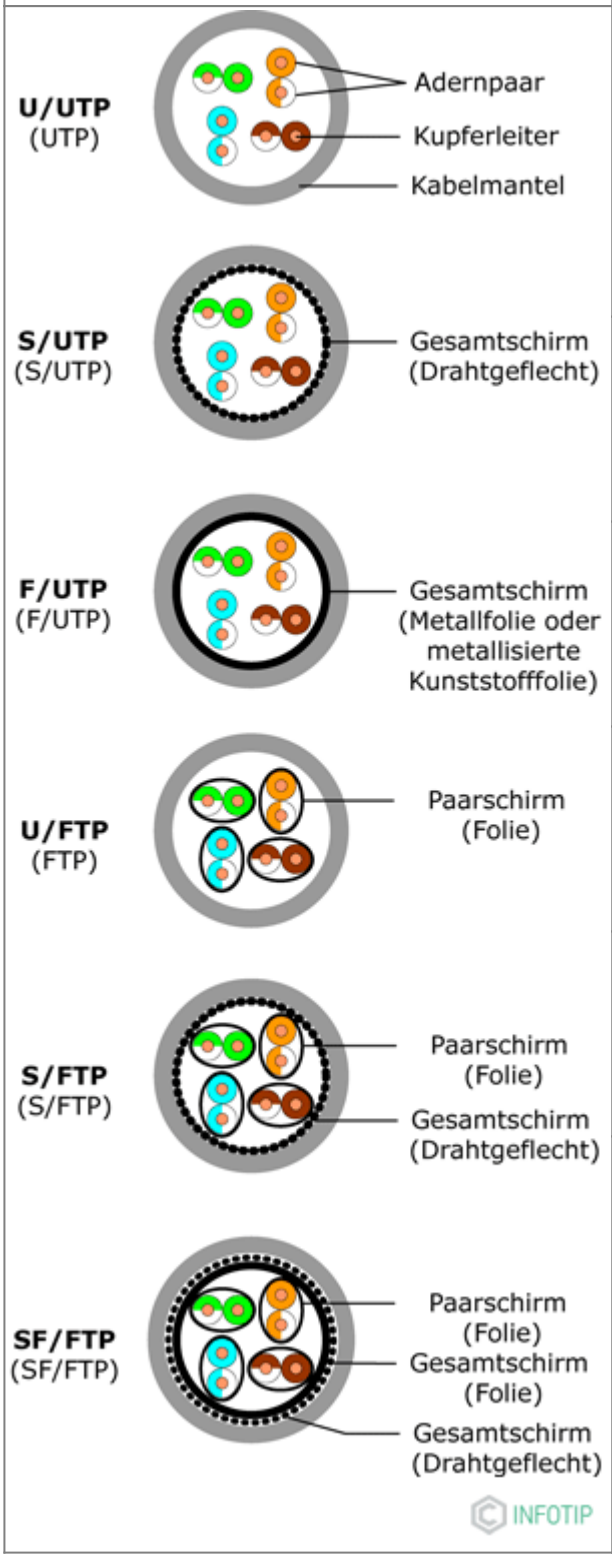
- Thicknet (10Base5)
- Thinnet (10Base2) - Heute noch bei Satellitenempfang im Einsatz

Twisted-Pair Kabel



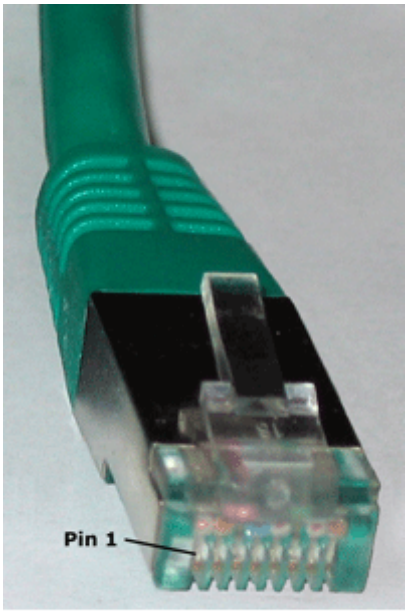
Twisted Pair ist ein vier-, acht- oder mehr-adriges Kupferkabel, bei dem jeweils zwei Adern miteinander verdrillt sind. Durch die Verdrillung kompensieren sich Leitungskapazität und -induktivität. Dadurch steigt die Übertragungsbandbreite und die mögliche Übertragungsreichweite wird praktisch nur durch die Dämpfung des Wirkwiderstandes begrenzt. Die Verwendung von symmetrischen Signalen (Differentialspannungen) erhöht die Festigkeit gegen elektromagnetische Störstrahlung.

Twisted Pair-Kabel gibt es in zahlreichen Varianten. Twisted Pair-Verbindungen werden außer in der Kommunikationstechnik (Netzwerkkabel, Telefonkabel) auch bei HDMI-, DVI- und LVDS-(in LCD/Plasma-TV zwischen Signalprozessor und Display) Verbindungen eingesetzt. Die Anzahl der Leiterpaare im Kabel hängt dabei von der benötigten Datenübertragungsrate ab. In Netzwerken wird für jede Übertragungsrichtung (senden, empfangen) wird jeweils ein Adernpaar (bei 100BaseT4 und 1000BaseT jeweils zwei) genutzt. Die Übertragungsreichweite ist abhängig vom Aufbau des Kabels, von der Dämpfung (=Länge) des Kabels und von den externen Störeinflüssen. Twisted Pair-Kabel für Netzwerke gibt es in zahlreichen Varianten:

Bild	Benennung	Beschreibung
	**U/UTP-Kabel**	**Unshielded/Unshielded Twisted Pair** sind nicht abgeschirmte verdrillte Leitungen und gehörten früher typischerweise der CAT3 an. UTP-Kabel sollten im industriellen Bereich oder in der Datentechnik mit hohen Datenraten nicht verwendet werden.
	S/UTP-Kabel	**Screened/Unshielded Twisted Pair** haben einen Gesamtschirm aus einem Kupfergeflecht zur Reduktion der äußeren Störeinflüsse
	F/UTP-Kabel	**Foilshielded/Unshielded Twisted Pair** besitzen zur Abschirmung einen Gesamtschirm, zumeist aus einer alukaschierten Kunststofffolie
	U/FTP-Kabel	**Unshielded/Foilshielded Twisted Pair** auch genannt **CAT5** oder **CAT5e**. Die Leitungsadern sind paarweise mit Folie abgeschirmt
	S/FTP-Kabel	**Screened/ Foilshielded Twisted Pair** auch genannt **CAT6** sollten in Bereichen mit hoher Störstrahlung (z.B. Büros mit mehreren PCs) eingesetzt werden.
	SF/FTP-Kabel	**Screened Foilshielded/Foilshielded Twisted Pair** auch genannt **CAT6e** oder **CAT7** besitzen eine Abschirmung für jedes Kabelpaar sowie eine doppelte Gesamtschirmung. Hierdurch kann eine optimale Störleistungsunterdrückung erreicht werden. Auch das Übersprechen zwischen den einzelnen Adernpaaren wird so wirksam unterdrückt

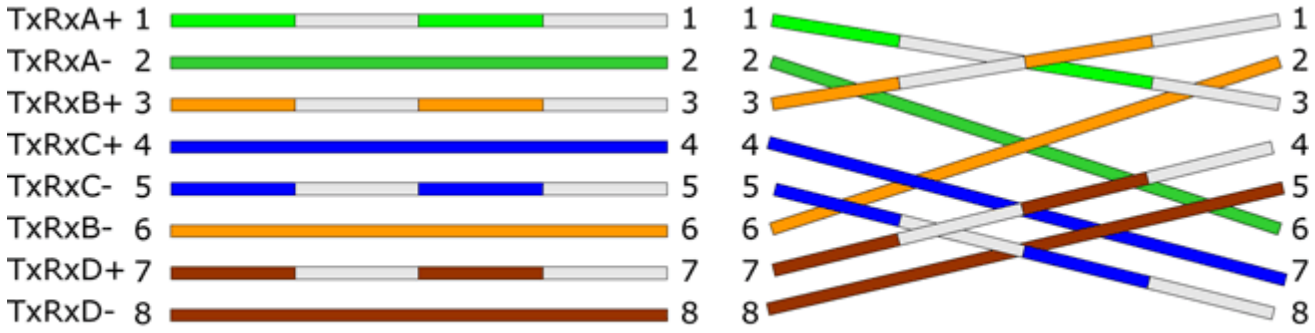
Die Preisunterschiede zwischen CAT-5e- Kabeln und CAT-7-Kabeln ist so gering, dass es sich bei Neuinstallation auf jeden Fall empfiehlt, CAT-7-Kabel einzusetzen. Dieses ist als einziges Kupfermedium in der Lage mit dem kommenden 10GBit-LAN verwendet zu werden.

Verbinder - RJ45



Der typische Standardverbinder für die Twisted-Pair-Verkabelung eines kupfergebundenen Ethernet-Netzwerkes ist der **8polige Western-Modularstecker RJ-45** (8P8C), auch RJ-48 oder RJ-49 genannt. RJ-45 Steckverbindungen können auf zwei Arten belegt sein, wobei die Belegung nach T568B am weitesten verbreitet zu sein scheint:

Belegung nach EIA/T-T568A		**Belegung nach EIA/T-T568B**	
Pin	**Farbe**	**Pin**	**Farbe**
1	weiß-grün	1	weiß-orange
2	grün	2	orange
3	weiß-orange	3	weiß-grün
4	blau	4	blau
5	weiß-blau	5	weiß-blau
6	orange	6	grün
7	weiß-braun	7	weiß-braun
8	braun	8	braun



Bei 1:1-Verbindungen sind beide Beschaltungen sind elektrisch zueinander kompatibel. Nur bei Erweiterungen von fest verdrahteten Netzen ist festzustellen, welche Belegung bereits vorgegeben ist. Normale Verbindungskabel („ Patchkabel“) mit RJ-45-Steckern sind 1:1 verschaltet, d.h. Pin 1 des einen Steckers geht auf den Pin 1 des anderen Steckers usw. Nur in besonderen Fällen, wenn z.B.

zwei Netzwerkkarten direkt miteinander verbunden werden sollen oder wenn Netzwerkkomponenten (z.B. Hubs älterer Bauart) über keinen dedizierten Uplink-Port verfügen, kann der Einsatz von Crossover-Kabeln notwendig werden.

LichtWellenLeiter (LWL)

Sind mit der Netzwerkverkabelung weite Strecken zu überwinden, z.B. zwischen einzelnen Gebäuden auf einem Fabrikgelände („Campusbereich“), sind sehr hohe Datenübertragungsraten (z.Zt. bis zu 170Gb/s) gefordert oder wenn sich die Datenübertragung per Kupferkabel aus technischen Gründen (z.B. bei extremer Störstrahlung) oder aus Gründen der Sicherheit verbietet, werden Lichtwellenleiter (LWL, Glasfasern) als Übertragungsmedium eingesetzt. Die Lieferprogramme der Hersteller erlauben mittlerweile die Übertragungsstrecken bis zum Einzelplatz komplett auf der Basis von LWL auszuführen.

Aufbau und Prinzip

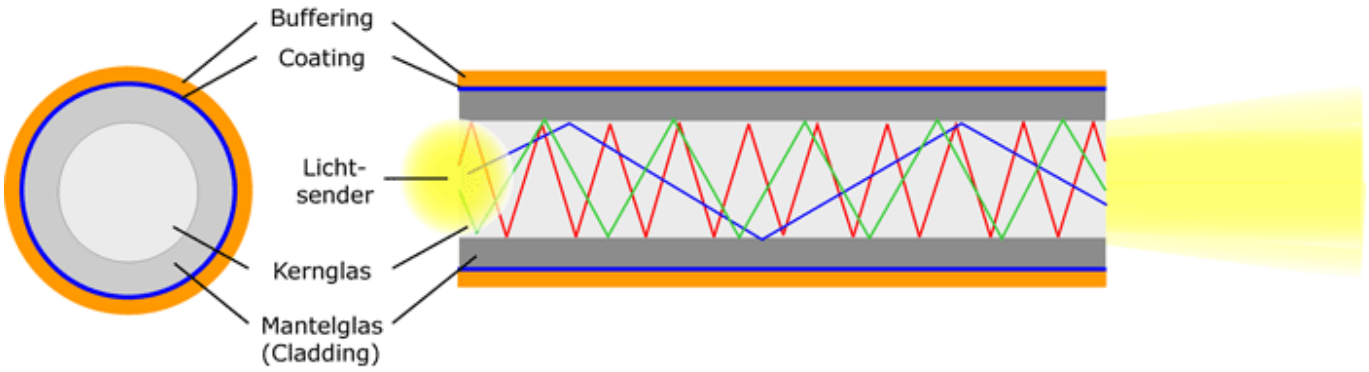
In einem LWL werden die Informationen nicht, wie in einem Kupferkabel, elektrisch übertragen, sondern mit **Licht**.
Der eigentliche LWL ist eine Faser aus Glas oder Kunststoff. Jede Faser besteht aus zwei Schichten. Der konzentrische Kern besteht aus einem optischen Material mit einem hohen Brechungsindex, das Mantelglas („ Cladding“) aus einem Material mit niedrigem. Licht, das in einem bestimmten Winkelbereich auf den Übergang von Kern zum Mantel trifft wird dort vollständig reflektiert. Über

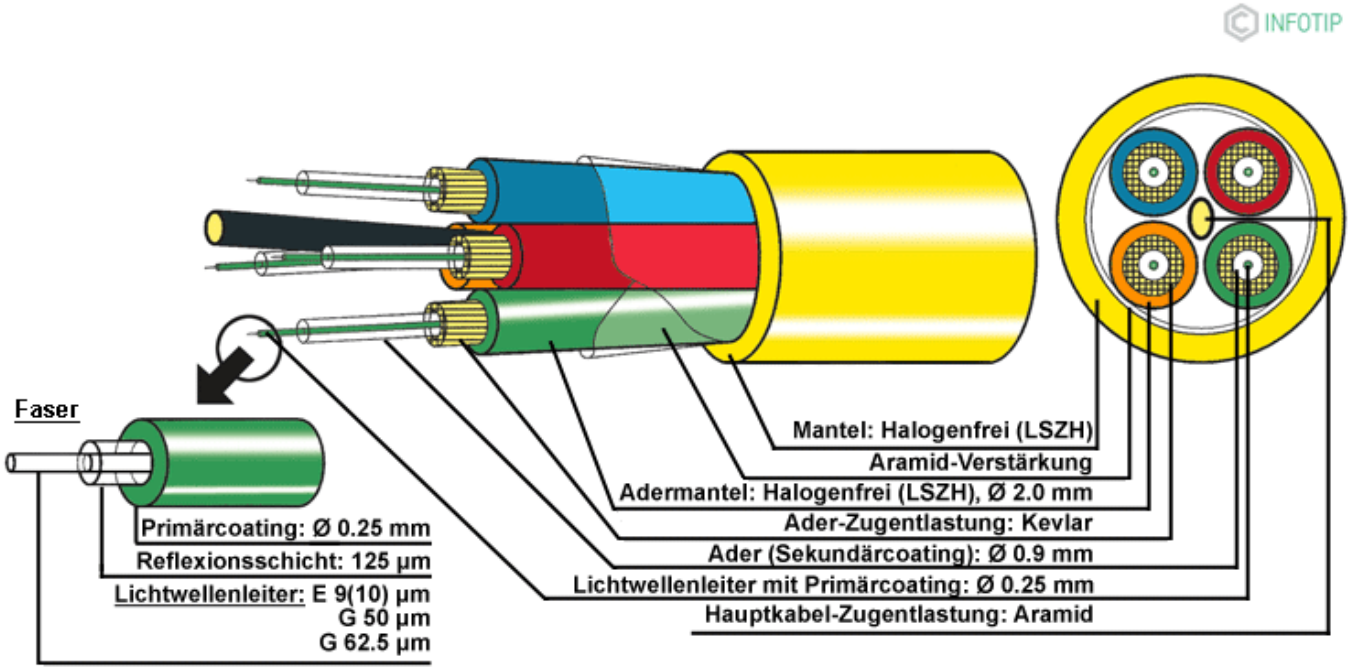
solche fortlaufenden Totalreflexionen pflanzt sich das Licht durch den LWL bis zum Ende der Faser fort.
Je steiler der Einfallswinkel des Lichts bei der Einspeisung in den LWL ist, desto häufiger wird die Lichtwelle reflektiert. Mit jeder Reflektion der Lichtwelle wird der Weg, des sogenannten Modes, länger.

Licht, das wenig häufig reflektiert wird, hat einen kürzeren Weg und durchläuft die Faser schneller. Es ist Licht niedrigen Modes.

Licht, das sehr häufig reflektiert wird, hat eine niedrige Ausbreitungsgeschwindigkeit in der Faser. Er ist Licht hohen Modes.

Erzeugt die Lichtquelle des Senders ein nicht-kohärentes Licht, tritt das Licht mit einer Vielzahl unterschiedlicher Winkel in die Faser ein. Dadurch entstehen natürlich durch die unterschiedlichen Moden Laufzeitunterschiede zwischen den Signalanteilen. Ein Eingangsimpuls mit steilen Flanken wird dadurch verschliffen und in seiner Breite gedehnt. Je länger ein Kabel ist, desto höher wird auch diese sog. Dispersion (Einheit: ns/km). Die Dispersion beeinflusst direkt die Übertragungsbandbreite der Glasfaserverbindung.

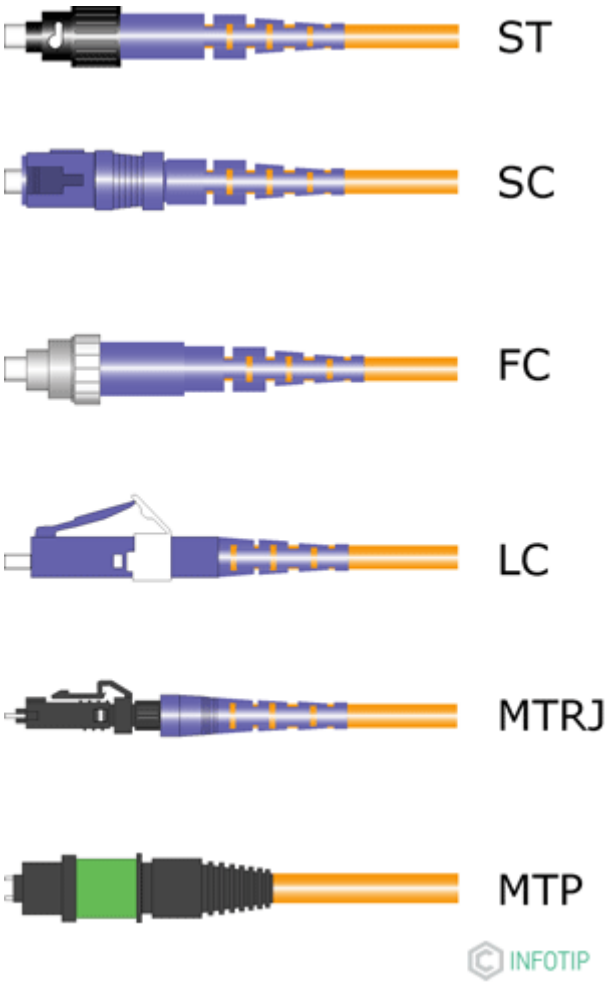




Da die Fasern sehr dünn und empfindlich sind, werden sie zum mechanischen Schutz mit einer Kunststoffbeschichtung („ Coating“) und einem Schutzüberzug versehen. In einem LWL-Kabel können mehrere Fasern, sogar in mehreren Bündeln, zusammen gefasst sein.

Verbinder

Die Hersteller von Netzwerkzubehör bieten konfektionierte Verbindungs- und Patchkabel mit einer Vielzahl von verschiedenen Steckerformen an. Meist sind die Kabel paarweise angelegt um beide Datenflussrichtungen (TX und RX) gleichzeitig herstellen zu können.



Vorteile

- hohe Reichweite
- hohe Übertragungsbandbreite
- Potentialfrei, daher auch für explosionsgefährdete Bereiche geeignet
- hohe Störfestigkeit, LWL können sogar zu Energieversorgungskabeln parallel verlegt werden
- hohe Abhörsicherheit

Nachteile

- Material für die Verkabelung ist teuer
- teure Verbindungstechnik
- Die Montagekosten sind wegen des höheren technischen Aufwandes höher
- komplexe und teure Messtechnik
- zusätzliche Kosten für Medienkonverter auf Kupfer-Ethernet

Leiterungebundene Übertragung

Als leiterungebundene Übertragung bezeichnet man eine Übertragung per

- Funk
- Ultraschall
- Infrarot
- Laser
- Licht

Drahtlose Übertragung (WLAN)

Die Übertragung von Informationen ohne Kabel ist mittlerweile in vielen Lebensbereichen als praktische Alternative eingezogen. Von der Fernbedienung eines Fernsehers über drahtlose Lautsprecher bis zum Smartphone gibt es viele Beispiele für die Umsetzung dieser Technik. Dabei werden Funksignale in frei verfügbaren Frequenzbändern anstelle von Kabeln für die Datenübertragung verwendet.

Vorteile

- Es sind keine baulichen Maßnahmen innerhalb eines Gebäudes nötig.
- Die baulichen Maßnahmen zwischen verschiedenen Gebäuden sind geringer als bei einer Verkabelung.
- Höhere Mobilität, da theoretisch jeder Punkt eines Firmengeländes drahtlos erreichbar ist.

Nachteile

- Oft geringere Datenübertragungsraten als bei Kabeln, die abhängig von Hindernissen sind.
- Anfällig für Störeinflüsse und Abhören durch Unbefugte.
- Probleme mit Ausleuchtung und Reflexionen.
- Bei vielen gleichzeitigen Nutzern an einem WLAN-Zugang bricht die Übertragungsrate ein (Shared Media).

Sicherheit als kritischer Bereich

Gerade im Bereich Sicherheit gibt es bei WLANs einige Punkte zu beachten, die sich auch in einem etwas größeren Konfigurationsaufwand äußern. Die sogenannte **SSID (Service Set Identifier)** kann eine eindeutige Identifikation (Firmenname etc.) enthalten, damit bei Problemen eine Kontaktaufnahme mit dem Betreiber möglich ist. Ein Verbergen bringt nicht viel, da die SSID in jedem Paket mitgeschickt wird und es Programme gibt, die auch verborgene SSIDs auslesen können. Eine versehentliche Verbindung durch Unbefugte ist bei verschlüsselten Zugängen nicht zu erwarten. Es gibt auch Empfehlungen, als SSID eine zufällige Zeichenfolge einzugeben, damit die SSID keine Rückschlüsse auf den Betreiber zulässt.

Letztendlich sollte die Übertragung im WLAN nur **verschlüsselt** erfolgen, wobei die Verschlüsselung mit **WEP (Wired Equivalent Privacy)** unsicher ist. Besser ist der Einsatz von **WPA (Wi-Fi**

Protected Access) bzw. der Nachfolgetechnologie **WPA2**, da hier deutlich stärkere Verschlüsselungsmechanismen mit **AES (Advanced Encryption Standard)** verwendet werden. Zusammen mit **TKIP (Temporal Key Integrity Protocol)** sind allerdings nur max. 54 Mbit/s möglich! Höhere Raten erreicht z. B. WPA2 zusammen mit CCMP (Counter-Mode/CBC-Mac Protocol)

Grundlegende Beschreibung

Kommunikation über WLAN erfolgt entweder als Punkt-zu-Punkt- oder als Mehrpunkt-Kommunikation. Die erste Variante dient z. B. der Überwindung größerer Distanzen durch den Einsatz zweier Richtantennen.

Bei der Mehrpunkt-Kommunikation werden ein oder mehrere sogenannte Access Points eingesetzt, die im Prinzip jeweils wie Zentralen (Verteiler) fungieren und die Datenströme mehrerer Clients koordinieren.

Diese Access Points können bei größeren Installationen über Kabel und geeignete Managed Switches eine Verbindung zu einem sogenannten RADIUS (Remote Authentication Dial-In User Service)-Server erhalten, um zwischen berechtigten und nicht berechtigten Sendern zu unterscheiden (Authentifizierung).

Eine Unterscheidung über die MAC-Adresse sollte nur den zum Zugang berechtigten Geräten vorbehalten bleiben, die sich nicht per RADIUS authentifizieren können. Dabei wird in einer Zugangsliste (Access Control Table) vom Managed Switch die MAC-Adresse eingetragen. Auf einem Access-Point bringt dies keine höhere Sicherheit, da per Funk eine MAC-Adresse unverschlüsselt verschickt wird und somit gefälscht werden kann. Die kleinste Einheit ist eine sogenannte Funkzelle, womit der Bereich gemeint ist, der von einem Sender (=Access Point) abgedeckt werden kann. Er umfasst ca. 30m im Gebäude und bis zu 300m im Freien. Mit speziellen Antennen können auch mehrere Kilometer überbrückt werden.

ISM-Frequenzbänder

In den meisten Fällen wird von den Herstellern ein sogenanntes **ISM-Band (Industrial, Scientific and Medical)** verwendet. Manchmal finden Sie auch die Abkürzung ISMO, wobei der letzte Buchstabe für den Begriff „Office“ (Büro) steht. Der Einsatz dieser Frequenzbänder bietet zwei Vorteile. Sie sind

- **gebührenfrei**
- **genehmigungsfrei**

Hierin liegt aber auch gleichzeitig der Nachteil. Sie werden von sehr vielen Herstellern für die unterschiedlichsten Zwecke genutzt, wie z. B. drahtlose Lautsprecher, elektronische Türöffnung bei Autos oder Garagen, und so ist die Gefahr, dass sich Geräte gegenseitig stören, relativ hoch.

Die für WLAN wichtigsten ISM-Bänder sind

- das **2,4-GHz-Band** (2,3995 bis 2,4845 GHz) mit max. **13 überlappenden Kanälen** von 20 MHz Bandbreite; auch 40 MHz Bandbreite ist möglich, dann aber mit weit weniger nutzbaren Kanälen. Es sind Geschwindigkeiten bis zu 300MBit/s möglich.
- das **5-GHz-Band** (5,150 bis 5,350 GHz für Kanalnummer 36–64 und 5,470 bis 5,725 GHz für Kanalnummer 100–140) mit Kanälen von 20, 40, 80 oder 160 MHz Bandbreite, wobei **max. 19**

Kanäle bei 20 MHz Bandbreite nicht überlappend nutzbar sind. Beim Funken mit 40 MHz Bandbreite sind 2 dieser Kanäle gebündelt erforderlich, mit 80 MHz 4 Kanäle usw. Die **Reichweite ist geringer** als im 2,4 GHz-Band. Es sind Geschwindigkeiten bis zu 600MBit/s möglich.

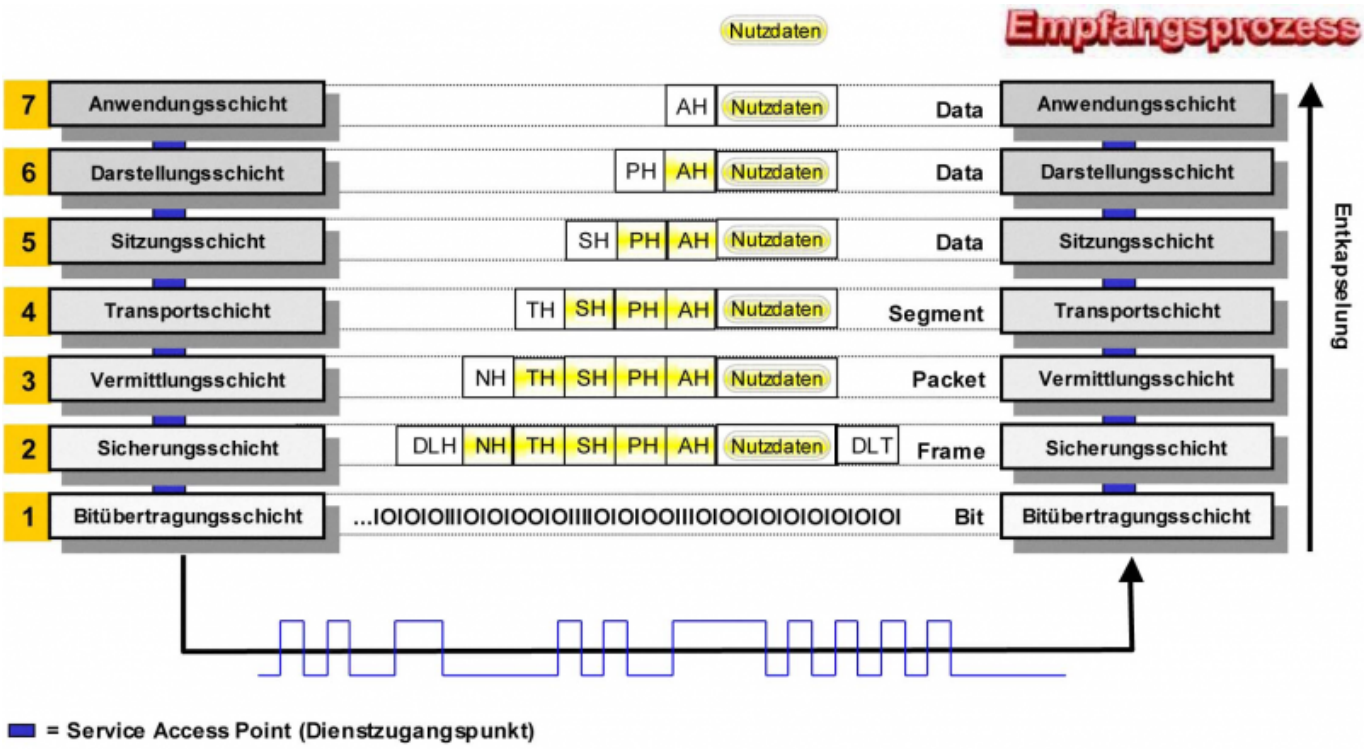
- zukünftig das 60-GHz-Band (57 bis 66 GHz) mit vier 2000 MHz breiten Funkkanälen für kurze Distanzen

OSI - Schichtenmodell

Das OSI-7-Schichtenmodell ist ein Referenzmodell für herstellerunabhängige Kommunikationssysteme bzw. eine Design-Grundlage für Kommunikationsprotokolle und Computernetze. OSI steht für Open System Interconnection (Offenes System für Kommunikationsverbindungen) und wurde von der ISO (International Organization for Standardization), das ist die Internationale Organisation für Normung, als Grundlage für die Bildung von offenen Kommunikationsstandards entworfen. Bei allen ISO-Standards handelt es sich um Handlungsempfehlungen. Die Einhaltung einer ISO-Norm ist freiwillig. In der Regel wird die Einhaltung der ISO-Standards von verschiedenen Seiten, zum Beispiel Kooperationspartnern, Herstellern und Kunden, gefordert.

Das Modell

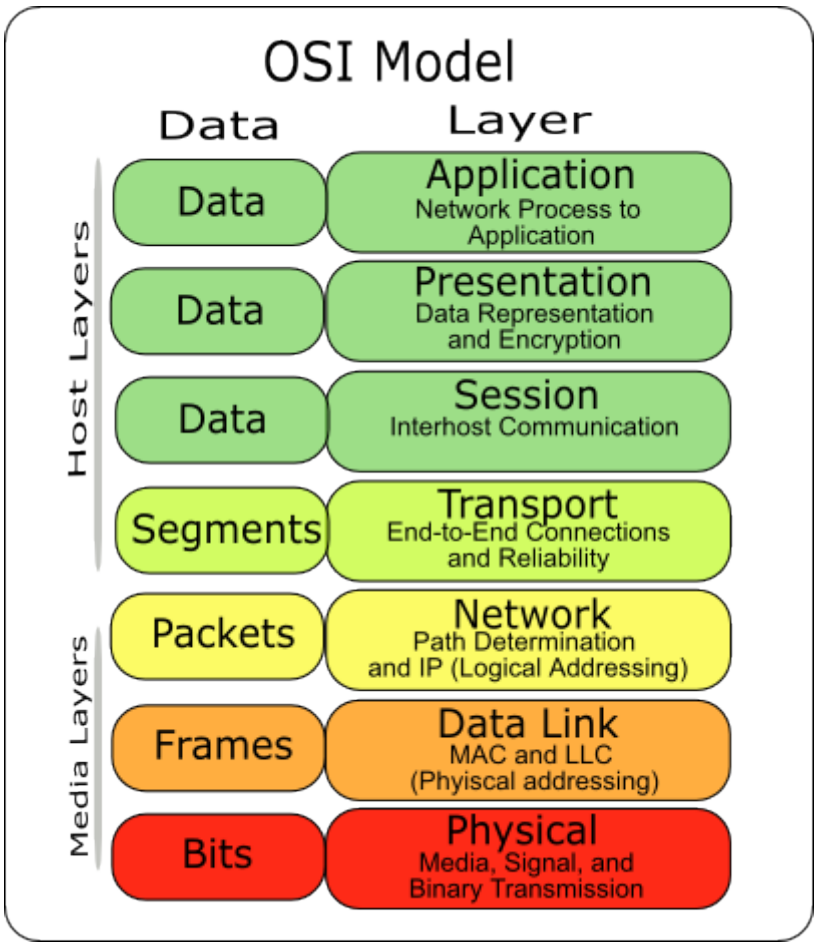
(Offenes System für Kommunikationsverbindungen) und wurde von der ISO (International Organization for Standardization), das ist die Internationale Organisation für Normung, als Grundlage für die Bildung von offenen Kommunikationsstandards entworfen. Bei allen ISO-Standards handelt es sich um Handlungsempfehlungen. Die Einhaltung einer ISO-Norm ist freiwillig. In der Regel wird die Einhaltung der ISO-Standards von verschiedenen Seiten, zum Beispiel Kooperationspartnern, Herstellern und Kunden, gefordert.



Die Schichten im Detail

Application Layer (Anwendungsschicht)	**Benutzerschnittstelle, Dienste, Anwendungen und Netzmanagement**
Schicht 7	Die Anwendungsschicht stellt Funktionen für die Anwendungen zur Verfügung. Diese Schicht stellt die Verbindung zu den unteren Schichten her. Auf dieser Ebene findet auch die Dateneingabe und -ausgabe statt.
Presentation Layer (Darstellungsschicht)	**Übersetzung, Verschlüsselung , Kompression in Standardformate**
Schicht 6	Die Darstellungsschicht setzt die Daten der Anwendungsebene in ein Zwischenformat um. Diese Schicht ist auch für Sicherheitsfragen zuständig. Durch sie werden Dienste zur Verschlüsselung von Daten bereitgestellt und gegebenenfalls Daten komprimiert.
Session Layer (Sitzungsschicht)	**Erstellung einer Verbindung, Freigabe von Verbindungen, Dialogsteuerung**
Schicht 5	Diese Schicht ermöglicht zwei Anwendungen auf verschiedenen Computern, eine gemeinsame Sitzung aufzubauen, damit zu arbeiten und sie zu beenden. Sie übernimmt ebenfalls die Dialogsteuerung zwischen den beiden Computern einer Sitzung und regelt, welcher der beiden wann und wie lange Daten überträgt.
Transport Layer (Transportschicht)	**Logische Ende-zu-Ende-Verbindungen (Transportkontrolle, Paketbildung)**
Schicht 4	Die Transportschicht stellt die zuverlässige Auslieferung der Nachrichten sicher und erkennt sowie behebt allfällige Fehler. Sie ordnet bei Bedarf auch die Nachrichten in Paketen neu, indem sie lange Nachrichten zur Datenübertragung in kleinere Pakete aufteilt. Am Ende des Weges stellt sie die kleinen Pakete wieder zur ursprünglichen Nachricht zusammen. Die empfangene Transportebene sendet auch eine Empfangs bestätigung.
Network Layer (Vermittlungsschicht)	**Routing (Internet), Datenflusskontrolle, Adressierung**

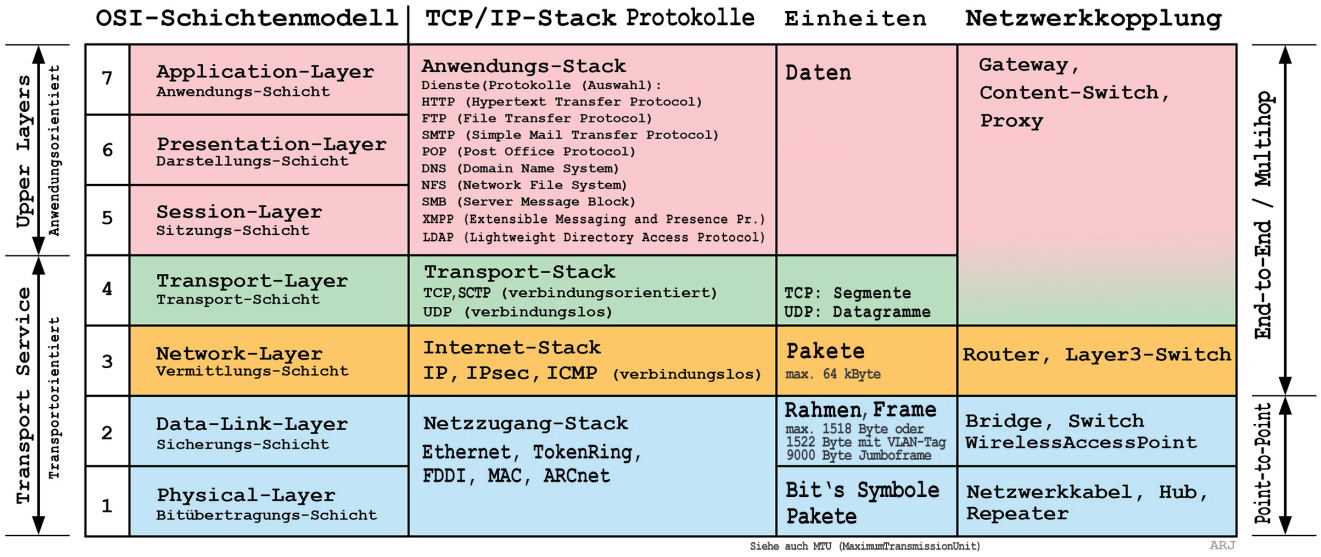
Application Layer (Anwendungsschicht)	**Benutzerschnittstelle, Dienste, Anwendungen und Netzmanagement**
Schicht 3	Die Vermittlungsschicht steuert die zeitliche und logische getrennte Kommunikation zwischen den Endgeräten, unabhängig vom Übertragungsmedium und der Topologie. Auf dieser Schicht erfolgt erstmals die logische Adressierung der Endgeräte. Die Adressierung ist eng mit dem Routing (Wegfindung vom Sender zum Empfänger) verbunden.
Data Link Layer (Sicherungsschicht)	**Logische Verbindungen mit Datenpaketen und elementare Fehlererkennungsmechanismen**
Schicht 2	Die Sicherungsschicht sorgt für eine zuverlässige und funktionierende Verbindung zwischen Endgerät und Übertragungsmedium. Zur Vermeidung von Übertragungsfehlern und Datenverlust enthält diese Schicht Funktionen zur Fehlererkennung, Fehlerbehebung und Datenflusskontrolle. Auf dieser Schicht findet auch die physikalische Adressierung von Datenpaketen statt.
Physical Layer (Physikalische Schicht)	**Maßnahmen und Verfahren zur Übertragung von Bitfolgen**
Schicht 1	Die Bitübertragungsschicht definiert die elektrische, mechanische und funktionale Schnittstelle zum Übertragungsmedium. Die Protokolle dieser Schicht unterscheiden sich nur nach dem eingesetzten Übertragungsmedium und -verfahren. Das Übertragungsmedium ist jedoch kein Bestandteil der Schicht 1.



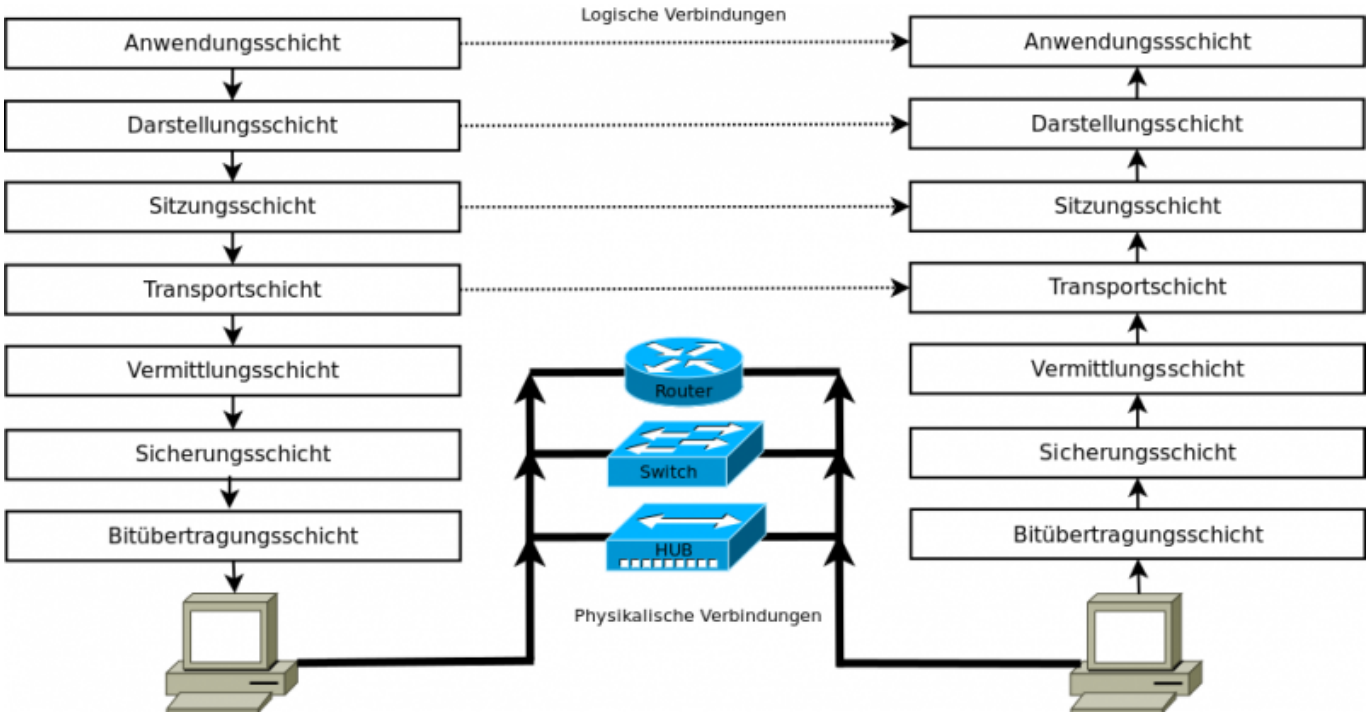
Protokolle

Protokolle sind eine **Sammlung von Regeln zur Kommunikation** auf einer bestimmten Schicht des OSI-Schichtenmodells. Die Protokolle einer Schicht sind zu den Protokollen der über- und untergeordneten Schichten weitestgehend transparent, so dass die Verhaltensweise eines Protokolls sich wie bei einer direkten Kommunikation mit dem Gegenstück auf der Gegenseite darstellt.

Die **Übergänge zwischen den Schichten sind Schnittstellen**, die von den Protokollen verstanden werden müssen. Weil manche Protokolle für ganz bestimmte Anwendungen entwickelt wurden, kommt es auch vor, dass sich **Protokolle über mehrere Schichten** erstrecken und mehrere Aufgaben abdecken. Dabei kommt es vor, dass in manchen Verbindungen einzelne Aufgaben in mehreren Schichten und somit mehrfach ausgeführt werden.



Anmerkung zur Skizze: End-zu-End-Verbindungen finden laut Definition erst ab Schicht 4 statt.



Das wichtigste Protokoll im Netzwerkverkehr, ist das **TCP & IP Protokoll** (Transmission Control Protocol & Internet Protocol), welche sich heute als Standard durchgesetzt haben.

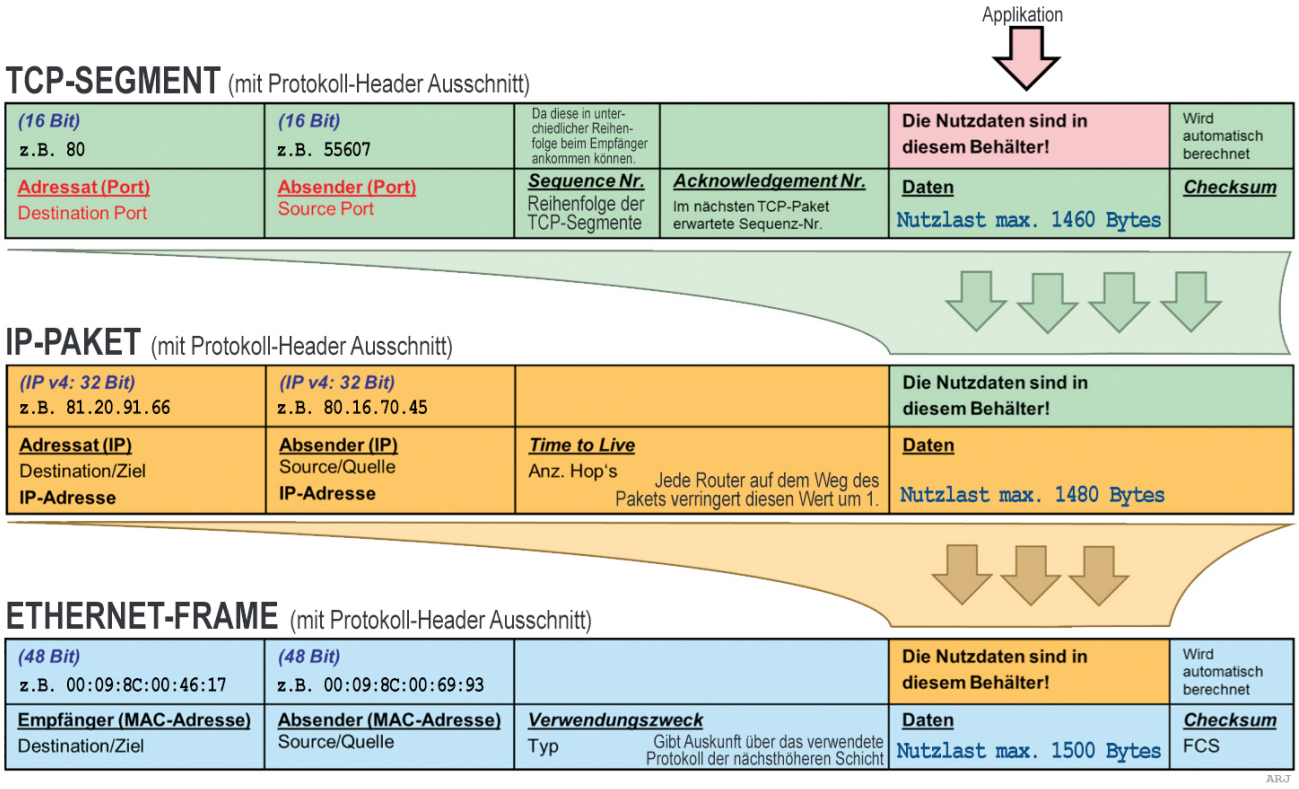
Neben TCP und IP gibt es natürlich noch viele weitere Protokolle, wie in der obigen Abbildung zu sehen ist.

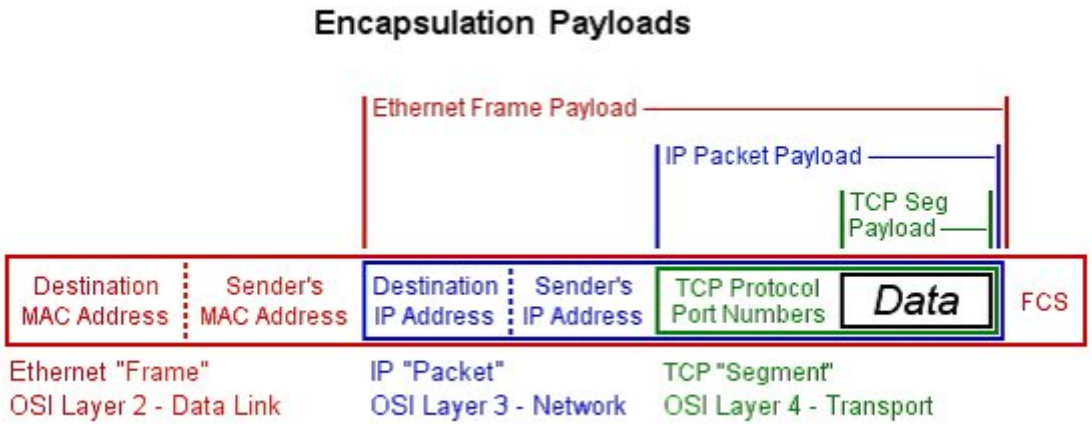
Die folgende Tabelle listet einige dieser Protokolle auf und ordnet sie ins obige Modell ein:

Protokoll	**Schicht**	**Name**	**Beschreibung**
FTP	5	File Transfer Protocol	Datenaustausch zwischen Rechnern
Telnet	5	Telecommunication Network Protocol	Terminalemulation zur Host-Kommunikation
SMTP	5	Simple Mail Transfer Protocol	Versenden von EMails
HTTP	5	Hypertext Transfer Protocol	Übertragen von HTML-Seiten
POP	5	Post Office Protocol	Abrufen von E-Mails
TCP	4	Transmission Control Protocol	Aufbau logischer Verbindungen zwischen Applikationen
UDP	4	User Datagram Protocol	Verbindungsloses Übertragungsprotokoll. Es ist nicht so gesichert wie TCP dafür aber schneller
IP	3	Internet Protocol	Verbindungsloses Protokoll zur Paketlenkung und Paketvermittlung über IP-Adressen
IPSec	3	IP Secure	Erweitert das reguläre IP-Protokoll um ein Bündel von Sicherheitsmechanismen
ARP	3	Address Resolution Protocol	Dien dazu logische IP-Adressen physikalischen MAC-Adressen zuzuordnen

Datenkapselung

Unter der Datenkapselung versteht man den Prozess im OSI-Modell und im TCP/IP-Referenzmodell, der die zu versendenden Daten im Header (und ggf. Trailer) der jeweiligen Schichten ergänzt. Im OSI-Modell betrifft dies die Datagramme der Schichten 2 bis 4, die gekapselt (verpackt) werden.





OSI-Schichtenmodell

TCP/IP-Referenzmodell

Netzwerkkomponenten

In der Netzwerktechnik unterscheidet man zwischen aktiven und passiven Netzwerk-Komponenten. Während **aktive Netzwerk-Komponenten eine eigene Logik haben**, zählen die passiven Netzwerk-Komponenten zur fest installierten Netzwerk-Infrastruktur. In der Regel dienen Netzwerk-Komponenten zur Kopplung der Netzwerk-Stationen. Man spricht deshalb auch von Kopplungselementen.

Passive Netzwerk-Komponenten

- Patchkabel und Installationskabel
- Anschlussdose
- Steckverbinder
- Patchfeld / Patchpanel
- Netzwerk-Schrank / Patch-Schrank

Hinweis: Zu den passiven Netzwerk-Komponenten zählen die Bestandteile der Verkabelung. Diese ist im OSI-Schichtenmodell nicht definiert.

Aktive Netzwerk-Komponenten

In kleinen privaten Netzwerken, haben Netzwerk-Komponenten noch klare Bezeichnung, wie Switch oder Router. In großen Unternehmensnetzwerken ist die Benennung der Kopplungselemente nicht immer eindeutig.

- Netzwerkkarte
- Repeater
- Hub
- Bridge
- Switch
- Router
- Gateway
- Server

Netzwerkkarte

Eine Netzwerkkarte wird auch als Netzwerkadapter bezeichnet. Die englische Bezeichnung ist Network Interface Card (NIC). Eine Netzwerkkarte ermöglicht es, auf ein Netzwerk zuzugreifen und arbeitet auf der Bitübertragungsschicht (Schicht 1) und der Datensicherungsschicht (Schicht 2) des OSI-Schichtenmodells. Jede Netzwerkkarte hat eine Hardware-Adresse (Format: XX-XX-XX-XX-XX-XX), die es auf der Welt nur einmal gibt. Anhand dieser Adresse lässt sich eine Station auf der Bitübertragungsschicht adressieren.

Im Falle von Ethernet-Netzen besteht die **MAC-Adresse aus 48 Bit (sechs Bytes)**. Die Adressen werden in der Regel **hexadezimal** geschrieben. Üblich ist dabei eine **byteweise Schreibweise**,

wobei die einzelnen Bytes durch Bindestriche oder Doppelpunkte voneinander getrennt werden, z. B. 00-80-41-ae-fd-7e oder 00:80:41:ae:fd:7e. Seltener zu finden sind Angaben wie 008041aefd7e oder 0080.41ae.fd7

In den **ersten 24 Bits** (Bit 3 bis 24) wird eine von der IEEE vergebene **Herstellerkennung** (auch OUI – Organizationally Unique Identifier genannt) beschrieben, die weitgehend in einer Datenbank einsehbar sind[6]. Die **verbleibenden 24 Bits** (Bit 25 bis 48) werden **vom jeweiligen Hersteller** für jede Schnittstelle individuell **festgelegt**.

Repeater

Ein Repeater ist ein Kopplungselement, um die Übertragungsstrecke innerhalb von Netzwerken, zum Beispiel Ethernet, zu verlängern. Ein Repeater empfängt ein Signal und bereitet es neu auf. Danach sendet er es weiter. Auf diese Weise verlängert der Repeater die Übertragungsstrecke und räumliche Ausdehnung des Netzwerks. Im einfachsten Fall hat ein Repeater zwei Ports, die wechselweise als Ein- und Ausgang funktionieren (bidirektional).

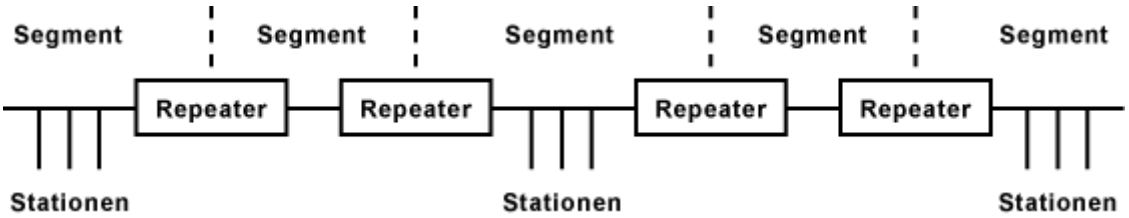
Repeater versteht man in der Regel als Verstärker von Übertragungsstrecken. Die weitere Beschreibung bezieht sich auf Repeater in kabelgebundenen Netzwerken, speziell in Ethernet-Netzwerken.

Ein Repeater arbeitet auf der Schicht 1, der Bitübertragungsschicht des OSI-Schichtenmodells. Der Repeater übernimmt keinerlei regulierende Funktion in einem Netzwerk. Er kann nur Signale empfangen und weiterleiten. Für angeschlossene Geräte ist nicht erkennbar, ob sie an einem Repeater angeschlossen sind. Er verhält sich völlig transparent.

Ein Repeater erweitert somit eine Kollisionsdomäne!!

Ein Repeater mit mehreren Ports wird auch als Hub (Multiport-Repeater) bezeichnet. Er kann mehrere Netzwerk-Segmente miteinander verbinden.

Die Repeater-Regel (5-4-3)



Um ein großes Netzwerk mit einer möglichst großen Reichweite aufzubauen, können mehrere Repeater hintereinandergeschaltet werden. Allerdings, nicht in beliebiger Anzahl. Der Grund liegt im Laufzeitverhalten und der Phasenverschiebung zwischen den Signalen an den Enden des Netzwerks. Deshalb gilt folgende Repeater-Regel:

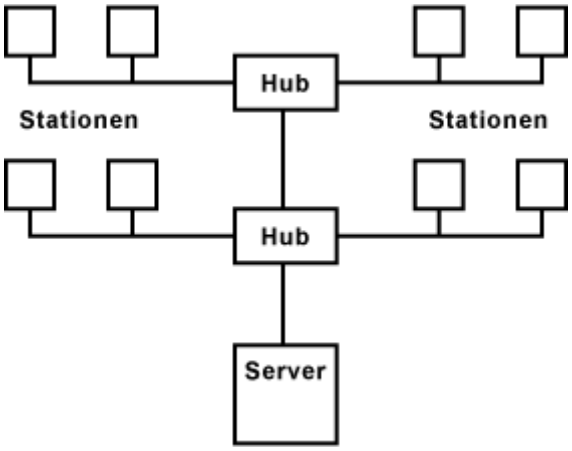
Es dürfen nicht mehr als fünf (5) Kabelsegmente verbunden werden. Dafür werden vier (4) Repeater eingesetzt. An nur drei (3) Segmenten dürfen Endstationen angeschlossen werden.

Diese **Repeater-Regel hat nur in den Ethernet-Netzwerken 10Base2 und 10BASE5** eine

Bedeutung. In Netzwerken, die mit Switches und Router aufgebaut sind, hat diese Repeater-Regel keine Bedeutung. Um die Nachteile von Repeatern in Ethernet-Netzwerken zu umgehen, werden generell Switches zur Kopplung der Hosts eingesetzt. In großen Netzwerken, insbesondere über unterschiedliche Übertragungssysteme hinweg, werden zusätzlich Router eingesetzt.

Hub

Ein Hub ist ein Kopplungselement, das mehrere Hosts in einem Netzwerk miteinander verbindet. In einem Ethernet-Netzwerk, das auf der Stern-Topologie basiert dient ein Hub als Verteiler für die Datenpakete. Hubs arbeiten auf der Bitübertragungsschicht (Schicht 1) des OSI-Schichtenmodells und sind damit auf die **reine Verteilfunktion** beschränkt. **Hubs erweitern somit die Kollisionsdomäne**. Ein Hub nimmt **ein Datenpaket entgegen und sendet es an alle anderen Ports** weiter. Das bedeutet, er **broadcastet**. Dadurch sind nicht nur **alle Ports**, sondern **auch alle Hosts belegt**. Sie bekommen alle Datenpakete zugeschickt, auch wenn sie nicht die Empfänger sind. Für die Hosts bedeutet das auch, dass sie nur dann senden können, wenn der Hub gerade keine Datenpakete sendet. Sonst kommt es zu Kollisionen.



Wenn die Anzahl der Anschlüsse an einem Hub für die Anzahl der Hosts nicht ausreicht, dann benötigt man noch einen zweiten Hub. Zwei Hubs werden über einen Uplink-Port eines der beiden Hubs oder mit einem Crossover-Kabel (Sende- und Empfangsleitungen sind gekreuzt) verbunden. Es gibt auch spezielle „stackable“ Hubs, die sich herstellerspezifisch mit Buskabeln kaskadieren lassen. Durch die Verbindung mehrerer Hubs lässt sich die Anzahl der möglichen Hosts im Netzwerk erhöhen. Allerdings ist die Anzahl der anschließbaren Hosts begrenzt. Hier gilt die Repeater-Regel.

Nachteile

- ineffizient
- unsicher (Jeder bekommt jede Nachricht)

Vorteile

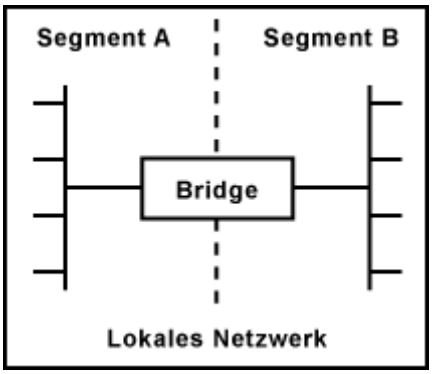
- zentraler Verteiler

Bridge

Eine Bridge ist ein Kopplungselement, das ein lokales Netzwerk in zwei Segmente aufteilt. Dabei

werden die Nachteile von Ethernet, die besonders bei großen Netzwerken auftreten ausgeglichen. Als Kopplungselement ist die Bridge eher untypisch. Man vermeidet die Einschränkungen durch Ethernet heute eher durch Switches.

Eine Bridge teilt eine Kollisionsdomäne!!

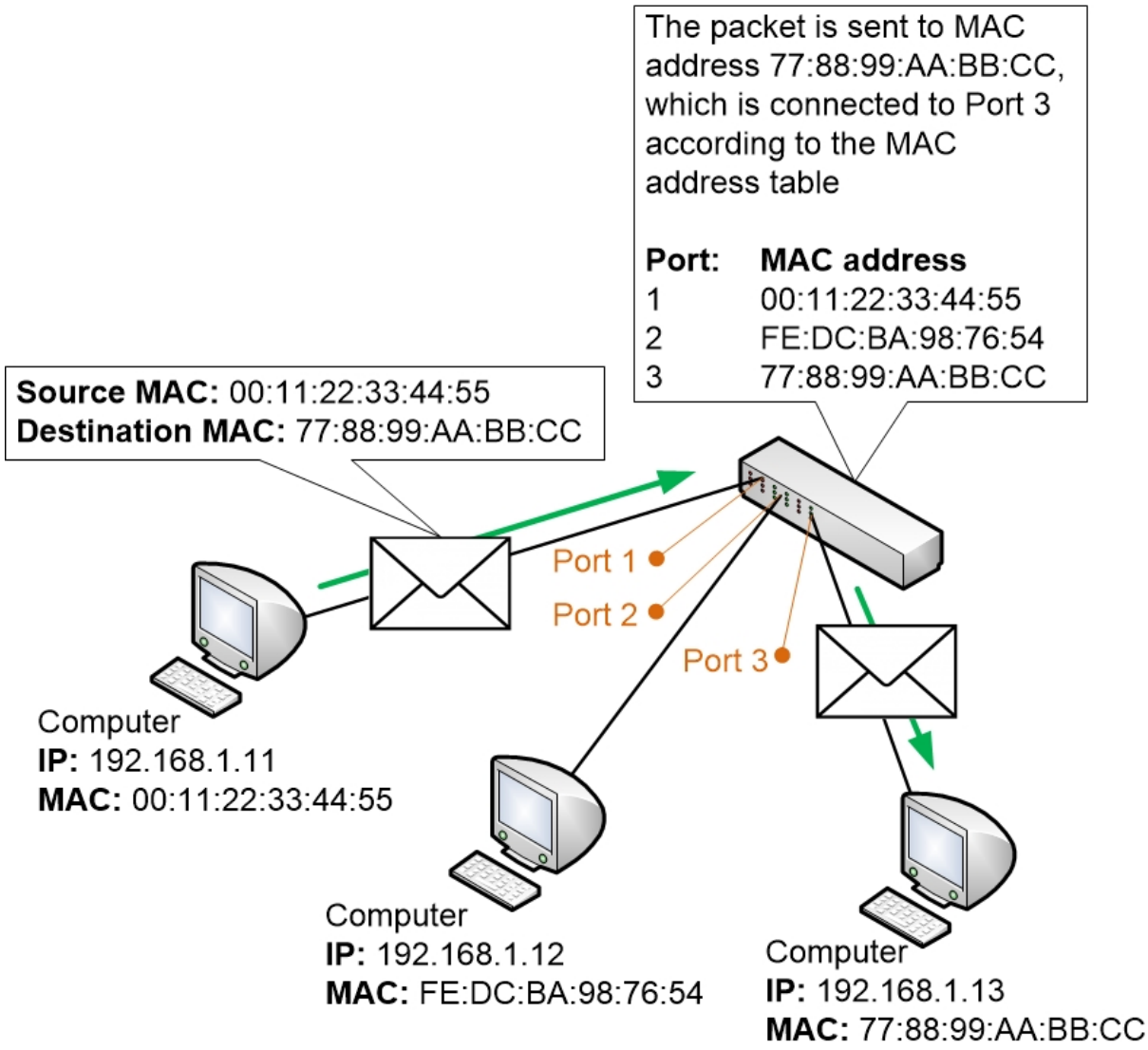


Switch

Ein Switch ist ein Kopplungselement, das mehrere Stationen in einem Netzwerk miteinander verbindet. In einem Ethernet-Netzwerk, das auf der Stern-Topologie basiert dient ein Switch als Verteiler für die Datenübertragung.

Die Funktion ist ähnlich einem Hub, mit dem Unterschied, das ein Switch direkte Verbindungen zwischen den angeschlossenen Geräten schalten kann, sofern ihm die Ports der Datenpaket-Empfänger bekannt sind. Somit kommunizieren wirklich nur jene miteinander, die auch miteinander reduzieren wollen. Wenn nicht, dann broadcastet der Switch die Datenpakete an alle Ports. Wenn die Antwortpakete von den Empfängern zurück kommen, dann merkt sich der Switch die MAC-Adressen der Datenpakete und den dazugehörigen Port und sendet die Datenpakete dann nur noch dorthin. Er baut also eine sogenannte MAC-Adressen-Tabelle auf:

Beispiel:



Während ein Hub die Bandbreite des Netzwerks limitiert, steht der Verbindung zwischen zwei Hosts, die volle Bandbreite der Ende-zu-Ende-Netzwerk-Verbindung zur Verfügung.

Ein Switch arbeitet auf der Sicherungsschicht (Schicht 2) de s OSI-Modells und arbeitet ähnlich wie eine Bridge. Daher haben sich bei den Herstellern auch solche Begriffe durchgesetzt, wie z. B. Bridging Switch oder Switching Bridge. Die verwendet man heute allerdings nicht mehr.

Switches unterscheidet man hinsichtlich ihrer Leistungsfähigkeit mit folgenden Eigenschaften:

- Anzahl der speicherbaren MAC-Adressen für die Quell- und Zielports
- Verfahren, wann ein empfangenes Datenpaket weitervermittelt wird (Switching-Verfahren)
- Latenz (Verzögerungszeit) der vermittelten Datenpakete

Ein Switch ist im Prinzip nichts anderes als ein intelligenter Hub, der sich merkt, über welchen Port welcher Host erreichbar ist. Teure Switches können zusätzlich auf der Schicht 3, der Vermittlungsschicht, des OSI-Schichtenmodells arbeiten (Layer-3-Switch oder Schicht-3-Switch). Sie sind in der Lage, die Datenpakete anhand der IP-Adresse an die Ziel-Ports weiterzuleiten. Im Gegensatz zu normalen Switche lassen sich auch ohne Router logische Abgrenzungen erreichen.

Switching-Verfahren

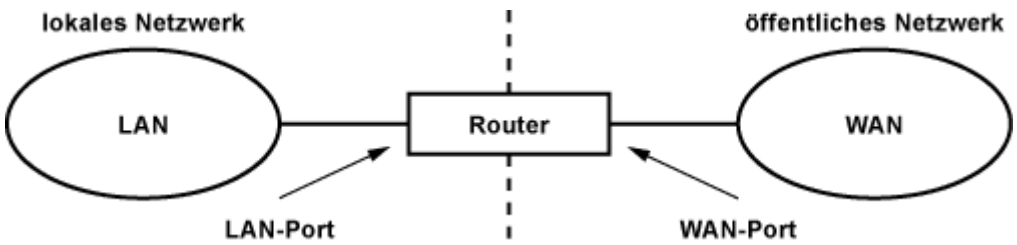
Switching-Verfahren	Beschreibung	Vorteile	Nachteile
Cut-Through	Der Switch leitet das Datenpaket sofort weiter, wenn er die Adresse des Ziels erhalten hat.	Die Latenz, die Verzögerungszeit, zwischen Empfangen und Weiterleiten ist äußerst gering.	Fehlerhafte Datenpakete werden nicht erkannt und trotzdem an den Empfänger weitergeleitet.
Store-and-Forward	Der Switch nimmt das gesamte Datenpaket in Empfang und speichert es in einem Puffer. Dort wird dann das Paket mit verschiedenen Filtern geprüft und bearbeitet. Erst danach wird das Paket an den Ziel-Port weitergeleitet.	Fehlerhafte Datenpakete können so im voraus aussortiert werden.	Die Speicherung und Prüfung der Datenpakete verursacht eine Verzögerung, abhängig von der Größe des Datenpaketes.
Fragment-Free	Der Switch empfängt die ersten 64 Byte des Daten-Paketes. Ist dieser Teil fehlerlos werden die Daten weitergeleitet. Die meisten Fehler und Kollisionen treten während den ersten 64 Byte auf. Dieses Verfahren wird trotz seiner effektiven Arbeitsweise selten genutzt.	sehr effizient	selten genutzt

Router

Ein Router verbindet mehrere Netzwerke mit unterschiedlichen Protokollen und Architekturen. Ein Router befindet sich häufig an den Außengrenzen eines Netzwerks, um es mit dem Internet oder einem anderen, größeren Netzwerk zu verbinden. Über die Routing-Tabelle entscheidet ein Router, welchen Weg ein Datenpaket nimmt. Es handelt sich dabei um ein dynamisches Verfahren, das Ausfälle und Engpässe ohne den Eingriff eines Administrators berücksichtigen kann. Ein Router hat mindestens zwei Netzwerkanschlüssen. Er arbeitet auf der Vermittlungsschicht (Schicht 3) des OSI-Schichtenmodells.

Die Aufgabe eines Routers ist ein komplexer Vorgang, der sich in 4 Schritte einteilen lässt:

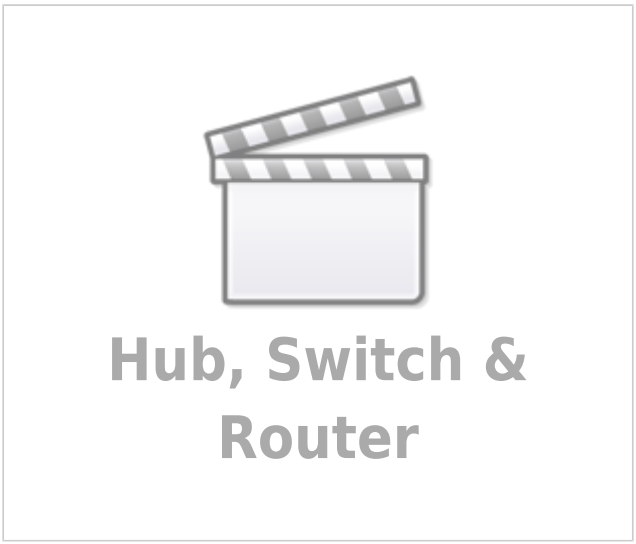
- Ermittlung der verfügbaren Routen
- Auswahl der geeignetsten Route unter Berücksichtigung verschiedener Kriterien
- Herstellen einer physikalischen Verbindung zu anderen Netzwerken
- Anpassen der Datenpakete an die Übertragungstechnik (Fragmentierung)



Ein Router hat in der Regel zwei Anschlüsse. Einen für die LAN-Seite und einen für die WAN-Seite.

Häufig sind die Ports mit der Bezeichnung LAN und WAN gekennzeichnet. Manchmal gibt es Port-Beschriftungen, bei denen nicht immer eindeutig ist, um was es sich handelt. Mit LAN ist immer das lokale Netzwerk mit privaten IP-Adressen gemeint, während die WAN-Seite das öffentliche Netzwerk kennzeichnet.

Zusammenfassung



IP-Adressen

Damit die Wegewahl in Netzwerken und im Internet zur Übermittlung von Datenpaketen vom Senden zum Empfänger funktioniert, wird jedem Rechner im **Internet eine weltweit eindeutige (und einmalige) Adresse (IP-Adresse)** zugeordnet.

Für Rechner die ohne Router direkt mit dem Internet verbunden sind, heißt das, das deren IP-Adressen weltweit eindeutig sind.

Standardmäßig haben diese IP-Adressen eine Länge von **32 Bit (4 x 8Bit)**.

Diese werden aus Gründen der **Übersichtlichkeit in 4 Zahlen zu je 1 Byte** aufgeteilt. Meist werden die einzelnen Bytes durch einen Punkt getrennt und dezimal dargestellt.

Öffentliche IP-Adressen

Wenn man von öffentlichen Adressen spricht, meint man die IP-Adressen, die im Internet erreichbar sind. Die Zuweisung einer öffentlichen IP-Adresse erfolgt in der Regel durch einen Provider (z.B. A1, Telekom, ...) welche diese wiederum in Europa durch die Organisation RIPE-NCC bekommt.

Private IP-Adressen

Private IP-Adressen (abgekürzt Private IP) sind IP-Adressen, die von der **IANA** nicht im Internet vergeben sind. Sie wurden für die **private Nutzung aus dem öffentlichen Adressraum ausgespart**, damit sie ohne administrativen Mehraufwand (Registrierung der IP-Adressen) in lokalen Netzwerken genutzt werden können. Als die **IP-Adressen des Internet Protokolls v4 knapp** wurden und dadurch eine **bewusste Einsparung öffentlicher IP-Adressen** notwendig wurde, war es umso wichtiger, private IP-Adressen in lokalen Netzwerken zur Verfügung zu haben, die **beliebig oft bzw. in beliebigen Netzwerken genutzt** werden können.

Netzklasse: Anzahl Netze (ohne Subnetting)	**Netzadressbereich**	**Subnetzmaske**	**CIDR-Notation**	**Anzahl Adressen**
Klasse A: 1 privates Netz mit 16.777.216 Adressen	10.0.0.0 bis 10.255.255.255	255.0.0.0	10.0.0.0/8	2^{24} = 16.777.216
Klasse B: 16 private Netze mit jeweils 65.536 Adressen	172.16.0.0 bis 172.31.255.255	255.240.0.0	172.16.0.0/12	2^{20} = 1.048.576
Klasse C: 256 private Netze mit jeweils 256 Adressen	192.168.0.0 bis 192.168.255.255	255.255.0.0	192.168.0.0/16	2^{16} = 65.536

Loopback Adresse

Die Class-A-Netzwerkadresse 127 ist weltweit reserviert für das sogenannte local loopback; sie dient zu Testzwecken der Netzwerkschnittstelle des eigenen Rechners. Die IP-Adresse **127.0.0.1** ist standardmäßig dem Loopback-Interface jedes Rechners zugeordnet.

Alle an diese Adresse geschickten Datenpakete werden nicht nach außen ins Netzwerk gesendet, sondern an der Netzwerkschnittstelle reflektiert. Die Datenpakete erscheinen, als kämen sie aus einem angeschlossenem Netzwerk.

Vergleich IP-Adresse vs. Telefonnummer

Ähnlich wie bei einer Telefonnummer setzt sich eine IP-Adresse aus mehreren Segmenten zusammen. Eine Telefonnummer besteht aus einer Vorwahl und einer Teilnehmernummer. Führen Sie ein Ortsgespräch, so muss die Vorwahl nicht angegeben werden. Ähnlich ist es bei IP-Adressen.

Diese bestehen auch aus zwei Teilen, wobei die ID für Identifikation steht:

- **Netzwerk-ID** im vorderen linken Teil entspricht der Vorwahl und gibt das entsprechende IP-Subnetz an.
- **Host-ID** im hinteren rechten Teil kennzeichnet eine einzelne Netzwerkkarte und entspricht dem Teilnehmernummer im Ortsnetz.

Entsprechend können Rechner im selben Subnetz direkt miteinander kommunizieren. Dagegen erfordert Kommunikation zischen Subnetzen eine Vermittlungsstelle, einen Router (Standardgateway), wo alle nicht im selben Netz adressierten Pakete hingeschickt werden.

Um zu erkennen, wo die Netzwerk-ID endet und die Host-ID beginnt, muss zusätzlich zur IP-Adresse zwingend eine sogenannte Subnetzmaske mit angegeben werden.

Subnetzmaske

Eine Subnetzmaske ist ein Bitmuster, das (von links nach rechts) Teile der IP-Adresse „maskiert“, um den Übergang zwischen Netz-ID und Host-ID zu kennzeichnen. Binär betrachtet besteht eine Subnetzmaske aus einer Folge von Einsen, die ab einer bestimmten Stelle umschlägt in eine Folge von Nullen. Dieser Umschlagpunkt gibt an, wie viele Bits zur Netzwerk-ID (Einsen) und zur Host-ID (Nullen) gehören.

Mögliche Subnetzmasken

Maske	Maske (kurze Schreibweise)	Anzahl Hosts pro Netz	Netze	Beispiel Klasse C-Netz (192.168.1.0)
255.255.255.0	/24	256	1	192.168.1.0 - 192.168.1.255
255.255.255.128	/25	128	2	192.168.1.0 - 192.168.1.127 192.168.1.128 - 192.168.1.255

Maske	Maske (kurze Schreibweise)	Anzahl Hosts pro Netz	Netze	Beispiel Klasse C-Netz (192.168.1.0)
255.255.255.192	/26	64	4	192.168.1.0 - 192.168.1.63 192.168.1.64 - 192.168.1.127 192.168.1.128 - 192.168.1.191 192.168.1.192 - 192.168.1.255
255.255.255.224	/27	32	8	192.168.1.0 - 192.168.1.31 192.168.1.32 - 192. 168.1.63 ... 192.168.192 - 192.168.1.223 192.168.1.224 - 192.168.1.255
255.255.255.240	/28	16	16	192.168.1.0 - 192.168.1.15 192.168.1.16 - 192.168.1.31 ... 192.168.1.224 - 192.168.1.239 192.168.1.240 - 192.168.1.255
255.255.255.248	/29	8	32	192.168.1.0 - 192.168.1.7 192.168.1.8 - 192.168.1.15 ... 192.168.1.240 - 192.168.1.247 192.168.1.248 - 192.168.1.255
255.255.255.252	/30	4	64	192.168.1.0 - 192.168.1.3 192.168.1.4 - 192.168.1.7 ... 192.168.1.248 - 192.168.1.251 192.168.1.252 - 192.168.1.255
255.255.255.254	/31	2	128	192.168.1.0 - 192.168.1.1 192.168.1.2 - 192.168.1.3 ... 192.168.1.252 - 192.168.1.253 192.168.1.254 - 192.168.1.255
255.255.255.255	/32	1	256	192.168.1.0 192.168.1.1 ... 192.168.1.254 192.168.1.255

Erklärung

Subnetting

Die Aufteilung eines zusammenhängenden Adressraums von IP-Adressen in mehrere kleinere Adressräume nennt man Subnetting. Ein Subnet, Subnetz bzw. Teilnetz ist ein physikalisches Segment eines Netzwerks, in dem IP-Adressen mit der gleichen Netzwerkadresse benutzt werden. Diese Teilnetze können über Routern miteinander verbunden werden und bilden dann ein großes zusammenhängendes Netzwerk.

Beispiel 1:

IP-Adresse: 192.168.128.17

```
Dezimale Darstellung:           192.        168.        128.          17
Bit-Darstellung:          1100 0000   1010 1000    1000 0000   0001 0001
Hex-Darstellung:                C0          A8          80          11
```

Subnetzmaske: 255.255.255.0

```
Dezimale Darstellung:           255.        255.        255.          0
Bit-Darstellung:           1111 1111   1111 1111   1111 1111  0000 0000
Hex-Darstellung:                FF          FF          FF          00
```

Verknüpft man nun die binäre IP-Adresse mit der Subnetzmaske mit einem Logischen AND, so bekommt man die Netz-ID (=Netzadresse).

```
    <----------- NETZ-ID ------------><- HOST-ID ->
    1100 0000   1010 1000   1000 0000   0001 0001    (IP-Adresse)
AND 1111 1111   1111 1111   1111 1111   0000 0000    (Subnetzmaske)
    ---------------------------------------------------------------
    1100 0000   1010 1000   1000 0000   0000 0000    (Netz-ID)
Netz-ID in Dezimaldarstellung:
 192.168.128
```

Verknüpft man nun die binäre IP-Adresse mit der negierten Subnetzmaske mit einem Logischen AND, so bekommt man die Host-ID.

```
    <----------- NETZ-ID ------------><- HOST-ID ->
    1100 0000   1010 1000   1000 0000   0001 0001    (IP-Adresse)
AND 0000 0000   0000 0000   0000 0000   1111 1111    (negierte Subnetzmaske)
    ---------------------------------------------------------------------
-
    0000 0000   0000 0000   0000 0000   0001 0001    (Host-ID)
Host-ID in Dezimaldarstellung:
 17
```

Das heißt im Netzwerk 192.168.128.0 stehen theoretisch 256 (0-255) Adressen zur Adressierung von Netzwerkgeräten zur Verfügung. Praktisch sind es aber nur 254 Adressen, da zwei Adressen

- die **Netzadresse** (= 1. Adresse im Netz –> 192.168.128.0)
- die **Broadcastadresse** (= letzte Adresse im Netz –> 192.168.128.255)

reserviert sind.

Beispiel 2:

```
IP-Adresse 130.94.122.195/27

              Dezimal          Binär                                          
Berechnung

IP Adresse    130.094.122.195  10000010 01011110 01111010 11000011            
ip-adresse
Netzmaske     255.255.255.224  11111111 11111111 11111111 11100000      AND   
netzmaske
------------------------------------------------------------------------------
----------
Netzwerkteil  130.094.122.192  10000010 01011110 01111010 11000000   =       
netzwerkanteil

IP Adresse    130.094.122.195  10000010 01011110 01111010 11000011            
ip-adresse
Netzmaske     255.255.255.224  00000000 00000000 00000000 00011111  AND(NOT   
netzmaske)
------------------------------------------------------------------------------
----------
Geräteteil                  3  00000000 00000000 00000000 00000011       =   
geräteteil
```

Bei einer Netzmaske mit 27 gesetzten Bits ergibt sich ein Netzwerkteil von 130.94.122.192. Es verbleiben 5 Bits und damit `2^5=32` Adressen für den Geräteteil. Hiervon werden noch je 1 Adresse für das Netzwerk selbst und für den Broadcast benötigt, sodass 30 Adressen für Geräte zur Verfügung stehen.

Beispiel 3:

```
IP-Adresse 130.94.122.117/28

              Dezimal          Binär                                          
Berechnung

IP Adresse   130.094.122.117   10000010 01011110 01111010 01110101            
ip-adresse
Netzmaske    255.255.255.240   11111111 11111111 11111111 11110000      AND   
netzmaske
------------------------------------------------------------------------------
----------
Netzwerkteil 130.094.122.112   10000010 01011110 01111010 01110000   =       
netzwerkanteil
```

```
IP Adresse   130.094.122.117   10000010 01011110 01111010 01110101
ip-adresse
Netzmaske    255.255.255.240   00000000 00000000 00000000 00001111  AND(NOT
netzmaske)
-------------------------------------------------------------------------
----------
Geräteteil     0.  0.  0.  5   00000000 00000000 00000000 00000101       =
geräteteil
```

Bei einer Netzmaske mit 28 gesetzten Bits ergibt sich ein Netzwerkteil von 130.94.122.112. Es verbleiben 4 Bits und damit `2^4=16` Adressen für den Geräteteil. Hiervon werden noch je 1 Adresse für das Netzwerk selbst und für den Broadcast benötigt, sodass 14 Adressen für Geräte zur Verfügung stehen.

- Zusammenfassung zu Subnetzmasken

Übungen IP-Adressierung

Bsp 1

Befinden sich 192.168.0.93/27 und 192.168.0.97/27 im gleichen Netzwerk-Segment?

Lösung

```
1) NW-ID: 192.168.0.64
2) NW-ID: 192.168.0.96
=> Nein
```

Bsp 2

Wie lauten die Neztwerkadressen des ersten/letzten Hosts des Netzwerkes 192.168.0.96/27 und die Broadcastadresse?

Lösung

```
1. Host: 192.168.0.97
letzter Host: 192.168.0.126
BC: 192.168.0.127
```

Bsp 3

Das Netz 195.1.31.0 soll in 30 Subnetze aufgeteilt werden. Bestimme die Subnetzmaske, und die Anzahl Adressen pro Subnet!

Lösung

```
Subnetzmaske: 255.255.255.248
Adressen: 6
```

Bsp 4

Das Netz 10.0.0.0 soll in 200 Subnetze aufgeteilt werden. Bestimme die Subnetzmaske, und die Anzahl Adressen pro Subnet!

Lösung

```
Subnetzmaske: 255.255.0.0
```

```
Adressen: 65534
```

Bsp 5

Das Netz 192.168.1.0 soll in Subnetze mit je 18 Host-Adressen aufgeteilt werden. Bestimme die Subnetzmaske, und die Anzahl Subnetze!

Lösung

```
Subnetzmaske: 255.255.255.224
Subnetze: 6
```

Bsp 6

Das Netz 192.168.100.0 soll in Subnetze mit je 5 Host-Adressen aufgeteilt werden. Bestimmen Sie die Subnetzmaske, und die Anzahl Subnetze!

Lösung

```
Subnetzmaske: 255.255.255.248
Subnetze: 30
```

Bsp 7

Bestimme Netz- und Broadcastadresse des Subnets, in dem die Adresse 195.1.31.135 mit Netzmaske 255.255.255.128 liegt!

Lösung

```
NW-ID: 195.1.31.128
BC: 195.1.31.255
```

Bsp 8

Bestimme Netz- und Broadcastadresse des Subnets in dem die Adresse 195.1.31.135 mit Netzmaske 255.255.255.192 liegt!

Lösung

```
NW-ID: 195.1.31.128/26
BC: 195.1.31.191
```

Bsp 9

Bestimme Netz- und Broadcastadresse des Subnets in dem die Adresse 15.3.128.222 mit Netzmaske 255.255.255.240 liegt!

Lösung

```
NW-ID: 15.3.128.208
Broadcast: 15.3.128.223
```

Bsp 10

Gib den Bereich der Rechneradressen an, den das Teilnetz Nummer drei (132.45.96.0/19) hat.

Lösung

```
132.45.96.1
bis
132.45.127.254
```

Bsp 11

Berechne Netz-, Broadcast und Hostadressen des 0.,1.,15. und 31 Subnetz des Netzes 192.168.1.0/29

Lösung

```
0. Netz:
* NW-ID: 192.168.1.0
* BC: 192.168.1.7
* Hosts: 192.168.1.1-6
```

```
1. Netz:
* NW-ID: 192.168.1.8
* BC: 192.168.1.15
* Hosts: 192.168.1.9-14
```

```
15. Netz:
* NW-ID: 192.168.1.120
* BC: 192.168.1.127
* Hosts: 192.168.1.121-126
```

```
31. Netz:
* NW-ID: 192.168.1.248
* BC: 192.168.1.255
* Hosts: 192.168.1.249-254
```

Bsp 12

Vervollständige folgende Tabelle:

IP-Adresse	10.1.1.1	Netzwerkadresse des Subnet	. . .
Netmask	255.255.0.0	Broadcastadresse des Subnet	. . .
Anzahl Host pro Subnet		Anzahl Subnets in diesem Netz	

Lösung

IP-Adresse	10.1.1.1	Netzwerkadresse des Subnet	10.1.0.0
Netmask	255.255.0.0	Broadcastadresse des Subnet	10.1.255.255
Anzahl Host pro Subnet	65536	Anzahl Subnets in diesem Netz	256

Bsp 13

Vervollständige folgende Tabelle:

IP-Adresse	10.1.1.1/24	Netzwerkadresse des Subnet	. . .
Netmask	255.255.255.0	Broadcastadresse des Subnet	. . .
Anzahl Host pro Subnet		Anzahl Subnets in diesem Netz	

Lösung

IP-Adresse	10.1.1.1/24	Netzwerkadresse des Subnet	10.1.1.0
Netmask	255.255.255.0	Broadcastadresse des Subnet	10.1.1.255
Anzahl Host pro Subnet	254	Anzahl Subnets in diesem Netz	65536

IP-Routing

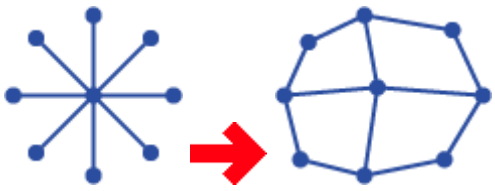
Das **Internet Protocol (IP)** ist ein **routingfähiges Protokoll** und sorgt dafür, dass **Datenpakete über Netzgrenzen** hinweg einen Weg zu anderen Hosts finden. Es kann die Daten über jede Art von physikalischer Verbindung oder Übertragungssystem vermitteln. Der hohen Flexibilität steht ein hohes Maß an Komplexität bei der Wegfindung vom Sender zum Empfänger gegenüber. Der **Vorgang der Wegfindung wird Routing** genannt

Wozu Routing?

Das grundlegende Verbindungselement in einem Ethernet-Netzwerk ist der Hub oder Switch. Daran sind alle Netzwerk-Teilnehmer angeschlossen. Wenn ein Host Datenpakete verschickt, dann werden die Pakete im Hub an alle Stationen verschickt und von diesen angenommen. Jedoch verarbeitet nur der adressierte Host die Pakete weiter. Das bedeutet aber auch, dass sich alle Hosts die Gesamtbandbreite dieses Hubs teilen müssen.

Um die Nachteile von Ethernet in Verbindung mit CSMA/CD auszuschließen, wählt man als Kopplungselement einen Switch und nutzt Fast Ethernet (kein CSMA/CD mehr). Der Switch merkt sich die Hardware-Adressen (MAC-Adressen) der Stationen und leitet die Ethernet-Pakete nur an den Port, hinter dem sich die Station befindet. Ist einem Switch die Hardware-Adresse nicht bekannt, leitet er das Datenpaket an alle seine Ports weiter (Broadcast) und funktioniert in diesem Augenblick wie ein Hub. Neben der begrenzten Speichergröße des Switches machen sich viele unbekannte Hardware-Adressen negativ auf die Performance eines Netzwerks bemerkbar.

Daher eignet sich zum **Verbinden großer Netzwerke** weder ein Hub noch ein Switch. Aus diesem Grund wird ein Netzwerk **durch Router** und IP-Adressen in **logische Segmente bzw. Subnetze** unterteilt. Die Adressierung durch das Internet Protocol ist so konzipiert, dass der Netzwerkverkehr innerhalb der Subnetze bleibt und erst dann das Netzwerk verlässt, wenn das Ziel in einem anderen Netzwerk liegt.



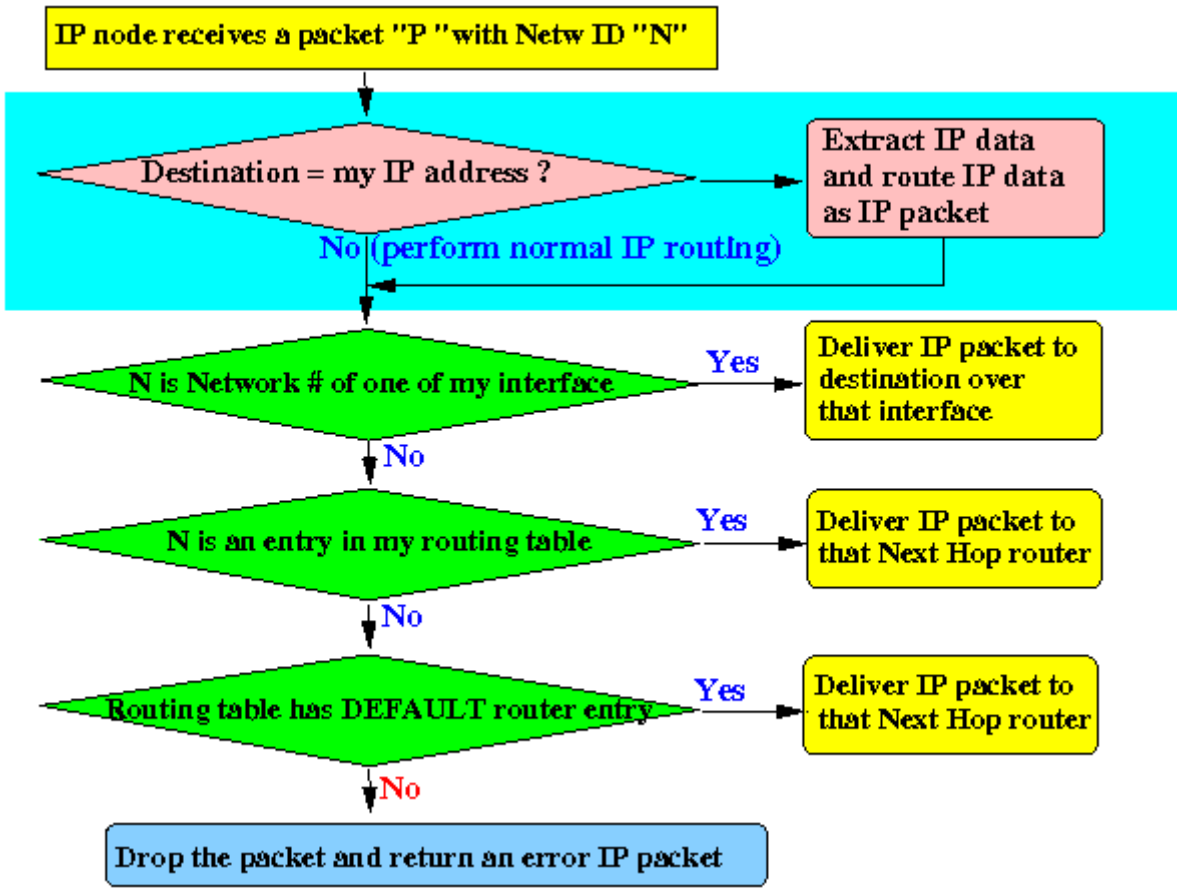
Insbesondere folgende **Probleme** in einem Ethernet-Netzwerk machen **IP-Routing notwendig**:

- **Vermeidung von Kollisionen und Broadcasts durch Begrenzung der Kollisions- und Broadcastdomäne**
- **Routing über unterschiedliche Netzarchitekturen und Übertragungssysteme**
- **Paket-Filter und Firewall**
- **Routing über Backup-Verbindungen bei Netzausfall**

IP-Routing-Algorithmus

Der IP-Routing-Algorithmus gilt nicht nur für IP-Router, sondern für alle Host, die IP-Datenpakete

empfangen können. Die empfangenen Datenpakete durchlaufen diesen Algorithmus bis das Datenpaket zugeordnet oder weitergeleitet werden kann.



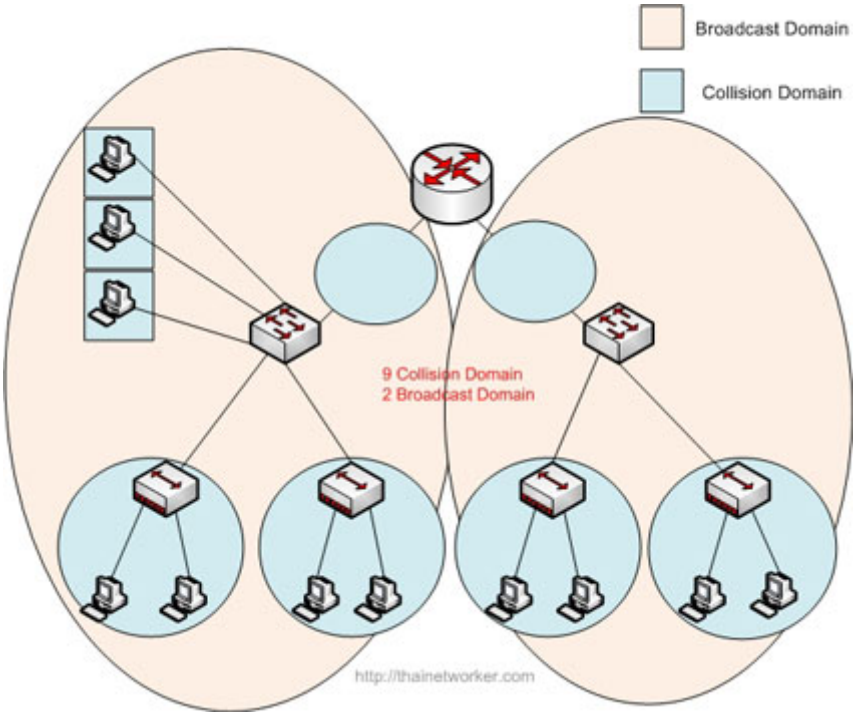
- Prüfe, ob das Datenpaket mir gehört?
  - Wenn ja, dann hat das Datenpaket sein Ziel erreicht und kann verarbeitet werden.
  - Wenn nein, prüfe ob das Datenpaket in mein Subnetz gehört?
    - Wenn ja, schick es in das eigene Subnetz weiter!
    - Wenn nein, prüfe ob die Route zum Empfänger bekannt ist?
      - Wenn ja, schicke es über die bekannte Route zum nächsten Router!
      - Wenn nein, prüfe ob es ein Standard-Gateway gibt?
        - Wenn ja, schick das Paket zum Standard-Gateway!
        - Wenn nein, schreibe eine Fehlermeldung und verwirf das Datenpaket!

Broadcastdomäne

Eine Broadcast-Domäne ist ein logischer Verbund von Netzwerkgeräten in einem lokalen Netzwerk, der sich dadurch auszeichnet, dass ein **Broadcast alle Domänenteilnehmer erreicht**.

Ein lokales Netzwerk auf der 2. Schicht des OSI-Modells (Sicherungsschicht) besteht durch seine Hubs, Switches und/oder Bridges aus einer Broadcast-Domäne. Erst durch die Unterteilung in VLANs oder durch den Einsatz von Routern, die auf Schicht 3 arbeiten, wird die Broadcast-Domäne aufgeteilt.

Eine Broadcast-Domäne besteht aus einer oder mehreren Kollisionsdomänen.



Netzwerkbefehle

Windows-Kommandos

Wichtige Netzwerkbefehle unter Windows XP

- ipconfig
  - /all ... detaillierte Informationen über Netzwerk-Konfiguration
  - /renew ... erneuert IP-Adressen
  - /release ... gibt IP-Adressen frei
- ping (sendet Datenpakete zu Rechner)
  - ping IP-Adresse
  - ping hostname
  - -n Anzahl ... Anzahl der Pakete
- tracert (Route zu Rechner)
- nslookup
  - nslookup (DNS-Abfragen)
  - nslookup IP-Adresse
  - nslookup Domain-Name

Linux-Kommandos

- ifconfig

Zeigt Informationen zu Netzwerk-Interfaces

- ping

```
ping -c 4 www.example.com
```

Pingt 4 mal www.example.com

- tracepath

```
tracepath www.example.com
```

Zeigt Hops zum Host an (benötigt eventuell SU-Rechte)

```
sudo tracepath www.example.com
```

- nslookup

```
nslookup www.example.com
```

Überprüft DNS-Eintrag

weitere hilfreiche Befehle:

- nmap (scannt („mappt“) das Netzwerk, führt Portscans aus und findet die Software eines fremden PCs heraus)
- mtr (kombiniert tracert (ohne su-Rechte) und ping, anschauliche Darstellung)

Fragen - Aufgaben - Arbeitsaufträge

Arbeitsaufträge:

1. Gib deiner/m Nachbarn/in die IP-Adresse deines Computers und notiere dir die IP-Adresse seines/ihres Computers.
2. Versuche deinen Nachbarcomputer anzupingen. Wie lange brauchte das Datenpaket zu diesem Rechner?
3. Gib deine IP-Adresse frei und versuche den Nachbarn anzupingen bzw. dich anpingen zu lassen. Erneuere anschließend deine IP-Adresse und überprüfe, wie sie nun lautet.
4. Versuche deinen Rechner (mit deiner IP-Adresse und der Loopback-Adresse) anzupingen.
5. Finde heraus, welche IP-Adresse der Domain-Name mail.bgamstetten.ac.at hat.
6. Finde einen Rechner im Internet, bis zu welchem ein Datenpaket sehr lange dauert und schicke zu diesem Rechner 20 Datenpakete hintereinander.
7. Finde heraus, welcher Domain-Name zu folgender IP-Adresse gehört 131.130.250.250
8. Lasse dir die Route zu www.yahoo.com anzeigen. Wie viele Rechner liegen zwischen dir und dem Webserver von www.yahoo.com ?
9. Versuche mit dem Internetexplorer die Website von www.google.at aufzurufen, indem du die IP-Adresse von Google in der Browserzeile eingibst.
10. Suche im Internet die Homepage von der australischen Regierung. Welche IP-Adresse hat der Rechner, auf dem die Homepage liegt? Wie viele Rechner liegen zwischen dir und diesem Rechner?
11. Finde einen Rechner im Internet, bis zu dem möglichst viele Hops dazwischen sind (Wer findet die meisten?).

Protokolle

Protokolle sind eine **Sammlung von Regeln zur Kommunikation** auf einer bestimmten Schicht des OSI-Schichtenmodells. Die Protokolle einer Schicht sind zu den Protokollen der über- und untergeordneten Schichten weitestgehend transparent, so dass die Verhaltensweise eines Protokolls sich wie bei einer direkten Kommunikation mit dem Gegenstück auf der Gegenseite darstellt.

Die **Übergänge zwischen den Schichten sind Schnittstellen**, die von den Protokollen verstanden werden müssen. Weil manche Protokolle für ganz bestimmte Anwendungen entwickelt wurden, kommt es auch vor, dass sich **Protokolle über mehrere Schichten** erstrecken und mehrere Aufgaben abdecken. Dabei kommt es vor, dass in manchen Verbindungen einzelne Aufgaben in mehreren Schichten und somit mehrfach ausgeführt werden.

Protokoll-Stack

Da sich ein einzelnes Protokoll immer nur um eine Teilaufgabe im Rahmen der Kommunikation kümmert, werden mehrere Protokolle zu Protokollsammlungen oder Protokollfamilien, den sogenannten Protokoll-Stacks, zusammengefasst. Die wichigsten Einzel-Protokolle werden dann oft stellvertertretend als Bezeichnung des gesamten Protokoll-Stapels genutzt.

Kommunikation zwischen Netzwerkkomponenten funktioniert nur dann, wenn sie denselben Protokoll-Stack benutzen oder wenn Geräte eingesetzt werden, die zwischen verschiedenen Stacks vermitteln können.

Portnummern (ab Layer 5)

Um die einzelnen Dienste (Protokolle), die bei einem Rechner über dieselbe IP-Adresse ausgeführt werden, voneinander zu differenzieren, wurden Portnummern eingeführt, um bei einer Anfrage deutlich zu machen, welcher Dienst gemeint ist.
Diese Portnummern, die im TCP- oder UDP Header angegeben werden, sind weltweit eindeutig festgelegt und können z.B. auf der Homepage der IANA eingesehen werden.
Allgemein lässt sich also sagen, dass die **IP-Adresse** den Rechner, **und** Die **Port-Nummer** den Dienst auf dem jeweiligen Rechner angibt. Diese beiden Informationen zusammen werden als **Socket** bezeichnet.

Wichtige Protokolle

OSI-LAYER	PROTOKOLL (Port)
5-7	DHCP (67+68/UDP)
	DNS (53/UDP)
	HTTP (80/TCP)
	HTTPS (443/TCP)
	FTP (20+21/TCP)
	SSH (22/TCP)
	SMTP (465 und 587 oder 25/TCP)
	POP3 (995 oder 110/TCP)
	IMAP (993 oder 143/TCP)
4	TCP
	UDP
3	IPv4
	IPv6
	NAT
	ICMP
2	Ethernet 802.3 , Wireless 802.x, MAC, ISDN,...
1	

Ethernet

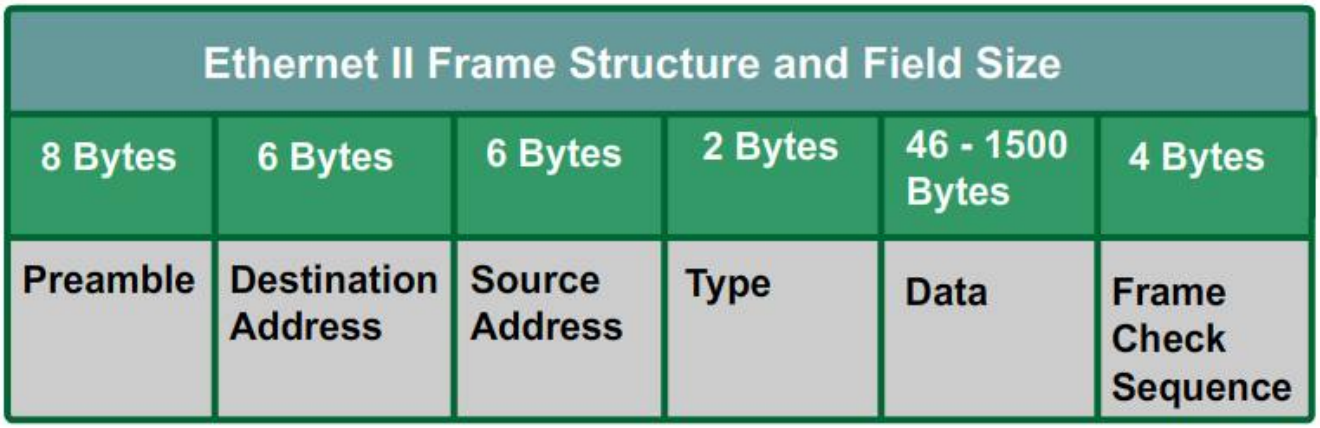
Erklärung

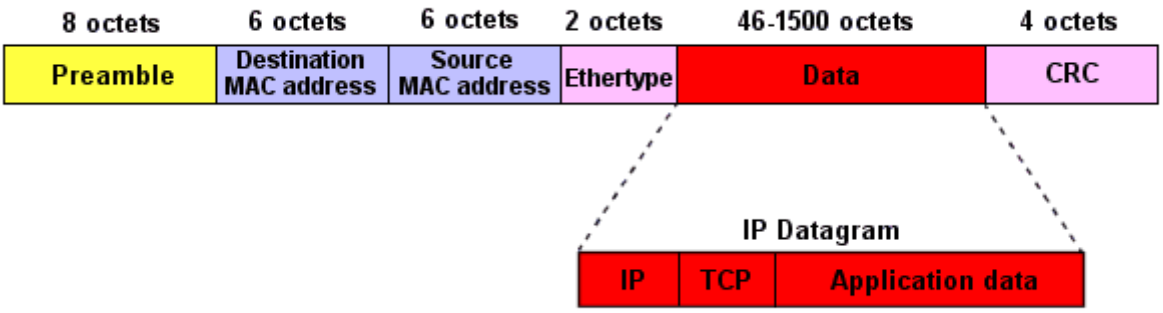
Ethernet ist eine Technik, die **Software (Protokolle usw.) und Hardware (Kabel, Verteiler, Netzwerkkarten usw.) für kabelgebundene Datennetze spezifiziert**, welche ursprünglich für lokale Datennetze (LANs) gedacht war und daher auch als LAN-Technik bezeichnet wird. Sie ermöglicht den Datenaustausch in Form von Datenframes zwischen den in einem lokalen Netz (LAN) angeschlossenen Geräten (Computer, Drucker und dergleichen). Derzeit sind Übertragungsraten von 1, 10, 100 Megabit/s (Fast Ethernet), 1000 Megabit/s (Gigabit-Ethernet), 2,5, 5, 10, 40, 50, 100, 200 und 400 Gigabit/s spezifiziert. In seiner ursprünglichen Form erstreckt sich das LAN dabei nur über ein Gebäude; Ethernet-Varianten über Glasfaser haben eine Reichweite von bis zu 70 km.

Die Ethernet-Protokolle umfassen Festlegungen für Kabeltypen und Stecker sowie für Übertragungsformen (Signale auf der Bitübertragungsschicht, Paketformate). Im OSI-Modell ist mit Ethernet sowohl die **physische Schicht (OSI Layer 1)** als auch die **Data-Link-Schicht (OSI Layer 2)** festgelegt.

Ethernet basiert auf der Idee, dass die Teilnehmer eines LANs Nachrichten durch Hochfrequenz übertragen, allerdings **nur innerhalb eines gemeinsamen Leitungsnetzes**. Jede Netzwerkschnittstelle hat **einen global eindeutigen 48-Bit-Schlüssel**, der als **MAC-Adresse** (=Media-Access-Control-Adress) bezeichnet wird. Das stellt sicher, dass alle Systeme in einem Ethernet unterschiedliche Adressen haben.

Ethernet Frame





CSMA/CD

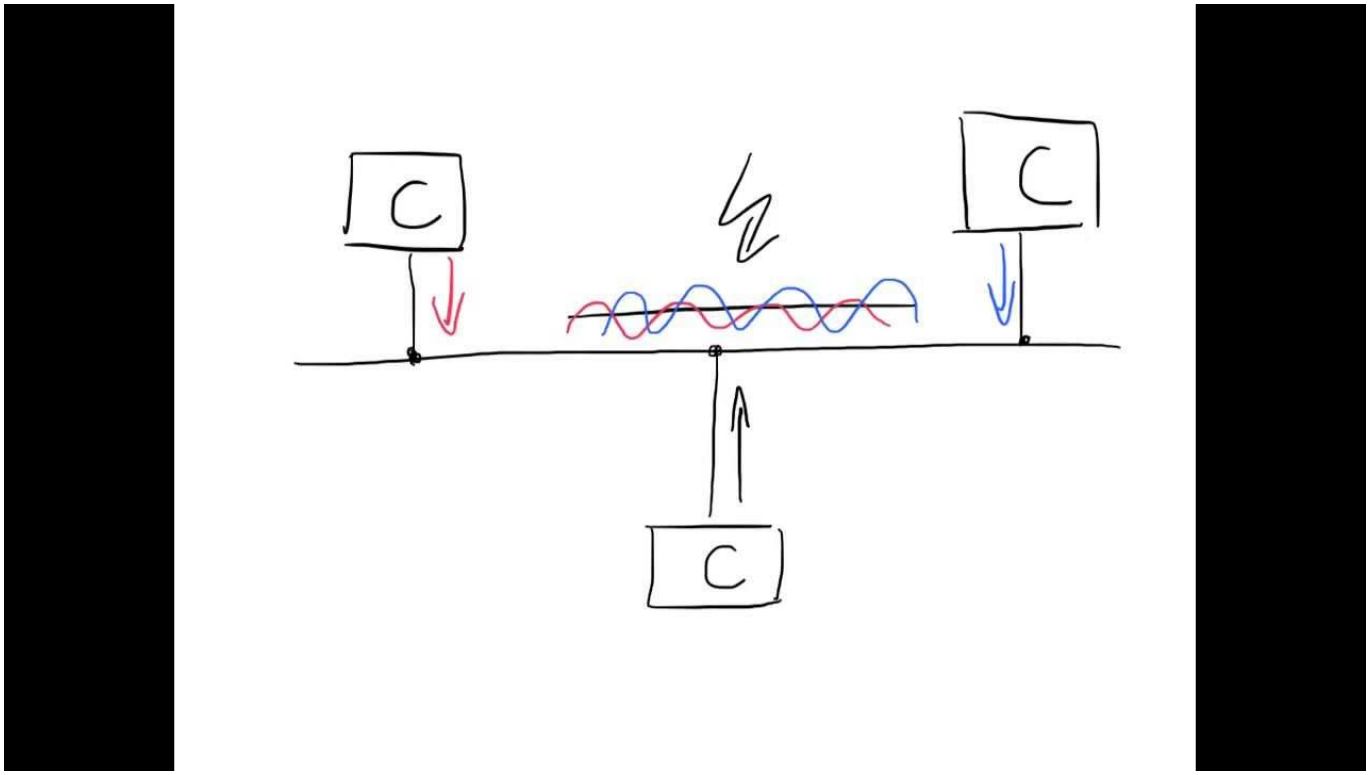
CSMA/CD (Carrier Sense Multiple Access with Collision Detection) ist das Zugriffsverfahren des Ethernets. Die Grundidee dabei ist, dass jede Station zu senden beginnen kann, wann sie will. Die einzelnen Stationen haben jederzeit und konkurrierend Zugang (Multiple Access) zum gemeinsamen Übertragungsmedium. Das grundlegende Motto könnte damit lauten:

Jeder darf, wann er will

Eingesetzt wird dieses Verfahren bei logischen Bus-Topologien. Dabei ist egal, ob physikalisch eine Bus- oder eine Stern-Topologie vorliegt.

Vorgehen

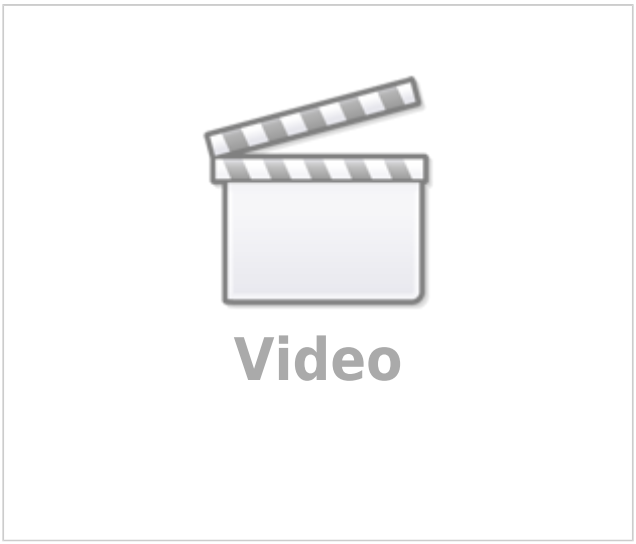
Durch Regelungen wird versucht, das Risiko zu minimieren, dass zwei Stationen ungünstigerweise gleichzeitig zu senden beginnen und somit die Signale auf dem Übertragungsweg zerstört/gestört werden **(=Kollision)**.



1) Leitung prüfen (Carrier Sense)

Der erste Teil der Abkürzung steht für Kollisionsverhinderung. Dabei wird vor einer geplanten Sendung das Übertragungsmedium abgehört, ob dieses frei ist. Wenn das Medium frei ist, wird gesendet. **–> LISTEN BEFORE TALKING**

2) Erkennen von Kollisionen (Collision Detection) Kommt es trotzdem zu einer Kollision, weil zwei Stationen gleichzeitig zu senden beginnen (**Multiple Access**). dann muss diese Kollision erkannt (**Collision Detection**) und reagiert werden. Dabei müssen alle Stationen immer am Medium horchen, ob eine Kollision auftritt. Ist dies der Fall, so sendet die erste Station, die eine Kollision erkennt, ein sogenanntes JAM-Signal aus. Jede Station, die das JAM-Signal registriert, stoppt unmittelbar das Senden von Daten. Nach einer zufälligen Zeitspanne, wird das Medium wieder überprüft und anschließend wieder begonnen zu senden.



Frage: Wie kann bei einer physikalischen Stern-Topologie eine Kollision auftreten?

Vorteile

- Jeder kann zu jeder Zeit senden

Nachteile

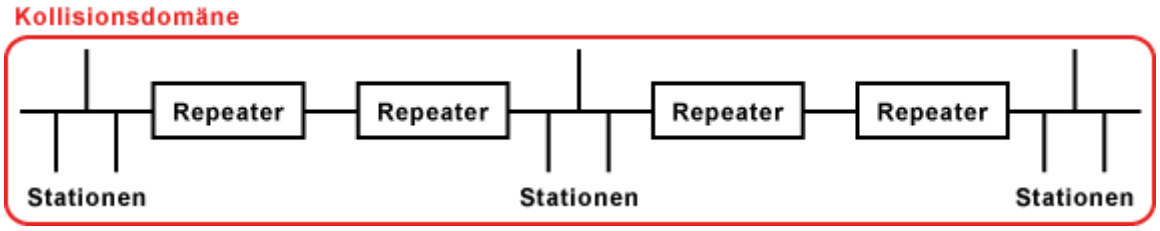
- Je mehr Stationen in einer Kollisionsdomäne, desto häufiger treten Kollisionen auf
- Der Zeitpunkt einer Sendung ist zufällig
- Das Verfahren ist ungeeignet für zeitkritischen Anwendungen

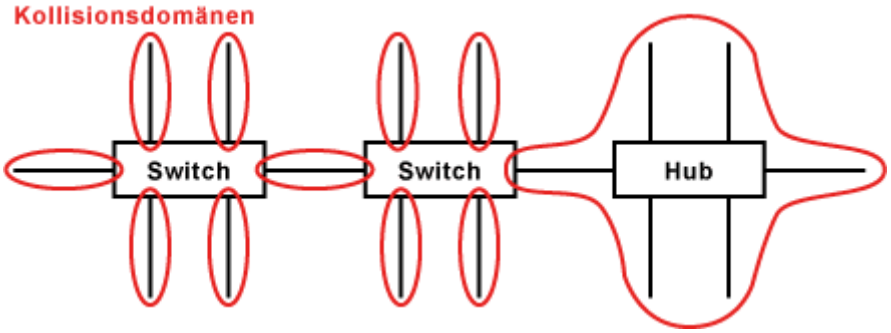
Kollisionsdomäne

Mit dem Begriff Kollisionsdomäne wird in einem Computernetz ein Teilbereich aus Teilnehmerstationen in derselben OSI-Modell-Schicht 1 bezeichnet. Eine Kollisionsdomäne umfasst alle Netzwerkgeräte, die um den Zugriff auf ein gemeinsames Übertragungsmedium konkurrieren. Das Übertragungsmedium ist daher eine zwischen allen Netzstationen geteilte Ressource. Grundlegende Vorstellung dabei ist, dass alle Netzwerkteilnehmer die Chance zur gleichberechtigten Nutzung des Netzwerkes besitzen.

Bei einem gemeinsamen Medium kann zu einer bestimmten Zeit nur jeweils eine Station Informationen übertragen, die an alle anderen Stationen übertragen bzw. von diesen empfangen wird. Fangen in einem derartigen gemeinsamen Schicht-1-Segment zwei Stationen gleichzeitig an zu senden, kommt es zu Kollisionen.

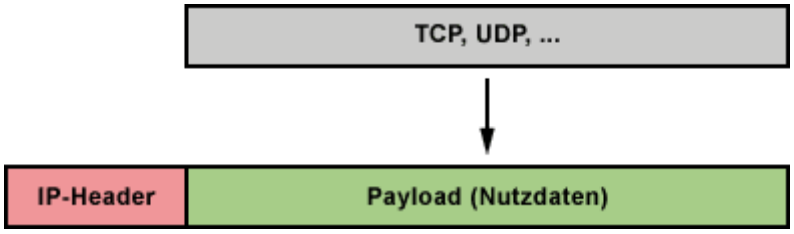
Beispiele für Kollisionsdomänen:





IPv4 - Internet Protocol Version 4 (Layer 3)

Das Internet Protocol, kurz IP, wird im Rahmen der Protokollfamilie TCP/IP zur Vermittlung von Datenpaketen verwendet. Es arbeitet auf der **Schicht 3 des OSI-Schichtenmodells** und hat maßgeblich die Aufgabe, **Datenpakete zu adressieren** und in einem dezentralen, **verbindungslosen und paketorientierten Netzwerk zu übertragen**. Dazu haben alle Netzwerk-Teilnehmer eine eigene IP-Adresse im Netzwerk. Sie dient nicht nur zur Identifikation eines Hosts, sondern auch des Netzes, in dem sich der jeweilige Host befindet.

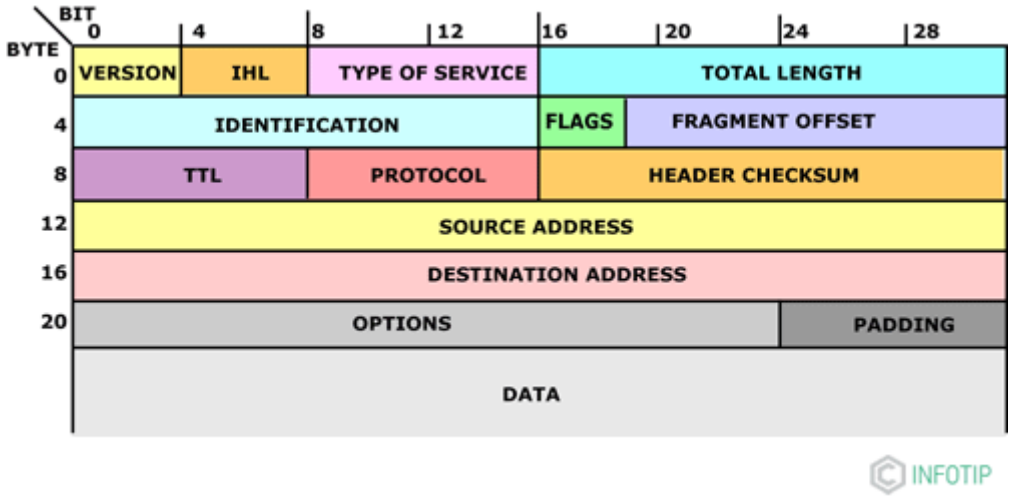


Aufgaben und Funktionen von IPv4

- Logische Adressierung (IPv4-Adresse)
- IPv4-Konfiguration
- IPv4-Header
- IP-Routing
- Namensauflösung (DNS-Dienst)

IPv4 Header

Jedes IPv4-Datenpaket besteht aus einem Header (Kopf) und dem Payload, in dem sich die Nutzdaten befinden. Der Header ist den Nutzdaten vorangestellt. Im IP-Header sind Informationen enthalten, die für die Verarbeitung durch das Internet Protocol notwendig sind.



Der Header ist in jeweils 32-Bit-Blöcke unterteilt. Dort sind Angaben zu Servicetypen, Paketlänge, Sender- und Empfängeradresse abgelegt. Ein IP-Paket muss mindestens 20 Byte Header und 8 Byte Nutzdaten bzw. Nutz- und Fülldaten enthalten. Die Gesamtlänge eines IP-Pakets darf 65.535 Byte nicht überschreiten.

IPv6 - Internet Protocol Version 6 (Layer 3)

IPv6 ist als Internet Protocol (Version 6) für die Vermittlung von Datenpaketen durch ein paketvermittelndes Netz, die Adressierung von Netzknoten und -stationen, sowie die Weiterleitung von Datenpaketen zwischen Teilnetzen zuständig. Mit diesen Aufgaben ist IPv6 der Schicht 3 des OSI-Schichtenmodells zugeordnet. Die Aufgabe des Internet-Protokolls besteht im Wesentlichen darin, Datenpakete von einem System über verschiedene Netzwerke hinweg zu einem anderen System zu vermitteln (Routing).

IPv6 ist der direkte Nachfolger von IPv4 und Teil der Protokollfamilie TCP/IP. Seit Dezember 1998 steht IPv6 bereit und wurde hauptsächlich wegen der Adressknappheit und verschiedener Unzulänglichkeiten von IPv4 entwickelt spezifiziert. Da weltweit immer mehr Menschen, Maschinen und Geräte an das Internet mit einer eindeutigen Adresse angeschlossen werden sollen, reichen die 4 Milliarden IPv4-Adressen nicht mehr aus.

Warum IPv6?

IPv6 gilt als Wunderwaffe gegen so manche Probleme mit Netzwerkprotokollen und gleichzeitig wird es als Teufelszeug verdammt, das wieder neue unbekannte Probleme hervorruft. Eine Tatsache ist, dass Administratoren, Programmierer und Hersteller IPv6 neu lernen müssen. Viele Rezepte aus der IPv4-Welt taugen unter IPv6 nicht mehr. Erschwerend kommt hinzu, dass es bei IPv6 allen Beteiligten an Erfahrung fehlt. IPv6-Gurus, die man bei einem großen Problem befragen kann, gibt es nicht so viele.

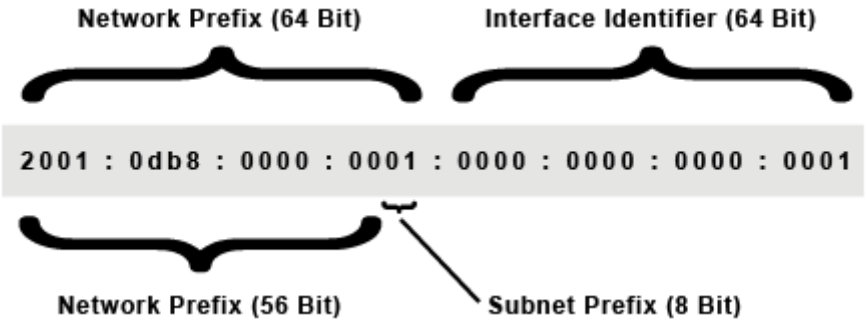
Bei IPv6 ist das Ende-zu-Ende-Prinzip konsequent weiter gedacht. Ein Interface kann mehrere IPv6-Adressen haben und es gibt spezielle IPv6-Adressen, denen mehrere Interfaces zugeordnet sind. IPv6 löst also nicht nur die Adressknappheit, sondern bietet auch Erleichterungen bei der Konfiguration und im Betrieb. Die zustandslose IPv6-Konfiguration und verbindungslokalen Adressen, die bereits nach dem Computerstart verfügbar sind, vereinfachen die Einrichtung und den Betrieb eines lokalen Netzwerks. Damit das gelingt sind Planer und Errichter von IP-Netzen gefordert sich eine neue Denkweise anzueignen.

IPv6 Adressen

Eine IPv6-Adresse ist eine Netzwerk-Adresse, die einen Host eindeutig innerhalb eines IPv6-Netzwerks logisch adressiert. Die Adresse wird auf IP- bzw. Vermittlungsebene (des OSI-Schichtenmodells) benötigt, um Datenpakete verschicken und zustellen zu können. Im Gegensatz zu anderen Adressen hat ein IPv6-Host mehrere IPv6-Adressen, die unterschiedliche Gültigkeitsbereiche haben. Konkret bedeutet das, dass wenn von IPv6-Adressen die Rede ist, dass nicht immer klar ist, welchen Gültigkeitsbereich diese IPv6-Adressen aufweisen. Grob unterscheidet man zwischen verbindungslokalen und globalen IPv6-Adressen. Die verbindungslokale IPv6-Adresse ist nur im lokalen Netzwerk gültig und wird nicht geroutet. Die globale IPv6-Adresse ist über das lokale Netzwerk hinaus im Internet gültig.

Eine IPv6-Adresse hat eine Länge von 128 Bit. Diese Adresslänge erlaubt eine unvorstellbare Menge von 2128 oder 3,4 x 1038 IPv6-Adressen. Das sind 340.282.366.900.000.000.000.000.000.000.000.000.000 IPv6-Adressen, also rund 340 Sextillionen Adressen. Bei IPv4 spricht man von rund 4,3 Milliarden Adressen. Der Adressraum von IPv6 reicht aus,

um umgerechnet jeden Quadratmillimeter der Erdoberfläche inklusive der Ozeane mit rund 600 Billiarden Adressen zu pflastern.



Eine IPv6-Adresse besteht aus 128 Bit. Wegen der unhandlichen Länge werden die 128 Bit in 8 mal 16 Bit unterteilt. Je 4 Bit werden als eine hexadezimale Zahl dargestellt. Je 4 Hexzahlen werden gruppiert und durch einen Doppelpunkt („:“) getrennt. Um die Schreibweise zu vereinfachen lässt man führende Nullen in den Blöcken weg. Eine Folge von 8 Nullen kann man durch zwei Doppelpunkte („::“) ersetzen.

Eine IPv6-Adresse besteht aus zwei Teilen. Dem Network Prefix (Präfix oder Netz-ID) und dem Interface Identifier (Suffix, IID oder EUI). Der Network Prefix kennzeichnet das Netz, Subnetz bzw. Adressbereich. Der Interface Identifier kennzeichnet einen Host in diesem Netz. Er wird aus der 48-Bit-MAC-Adresse des Interfaces gebildet und dabei in eine 64-Bit-Adresse umgewandelt. Es handelt sich dabei um das Modified-EUI-64-Format. Auf diese Weise ist das Interface unabhängig vom Network Prefix eindeutig identifizierbar.

NAT - Network Address Translation (Layer 3)

NAT (Network Address Translation) ist ein Verfahren, dass in **IP-Routern eingesetzt** wird, die lokale Netzwerke mit dem Internet verbinden. Weil Internet-Zugänge in der Regel nur über **eine einzige öffentliche** und damit routbare IPv4-Adresse verfügen, müssen sich alle anderen Hosts im lokalen Netzwerk mit privaten IPv4-Adressen begnügen. **Private IP-Adressen** dürfen zwar **mehrfach verwendet** werden, aber besitzen **in öffentlichen Netzen keine Gültigkeit**. Hosts mit einer privaten IPv4-Adresse können somit nicht mit Hosts außerhalb des lokalen Netzwerks kommunizieren.

NAT ist allerdings nur eine mittlerweile sehr lang andauernde Notlösung, um die Adressknappheit von IPv4 zu umgehen. Um die damit einhergehenden Probleme zu lösen muss langfristig auf ein Internet-Protokoll mit einem größeren Adressraum umgestellt werden. IPv6 ist ein solches Protokoll.

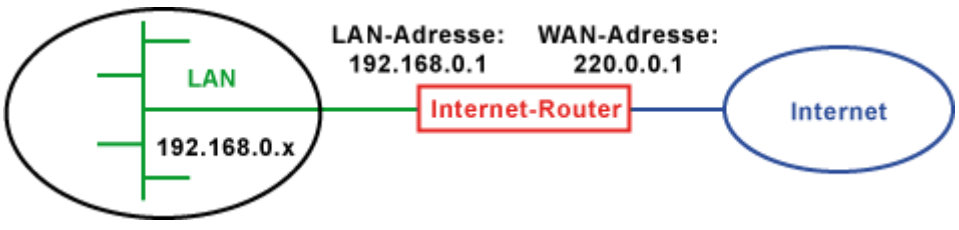
Warum NAT?

Die **ersten IPv4-Netze** waren **anfangs** eigenständige Netz **ohne Verbindung nach außen**. Hier begnügte man sich mit IPv4-Adressen aus den privaten Adressbereichen. Parallel dazu kam es bereits **Ende der 1990er** Jahre zu **Engpässen bei öffentlichen IPv4-Adressen**. Die steigende Anzahl der Einwahlzugänge über das Telefonnetz mussten mit IPv4-Adressen versorgt werden. Bis heute bekommt **ein Internet-Anschluss** nur eine **IPv4-Adresse für ein Gerät**. Damals war es undenkbar, dass an einem Internet-Anschluss ein ganzes Heimnetzwerk betrieben wird. Wenn ein Haushalt einen PC per Modem an das Telefonnetz angeschlossen und sich ins Internet eingewählt hat, dann war das schon etwas besonderes.

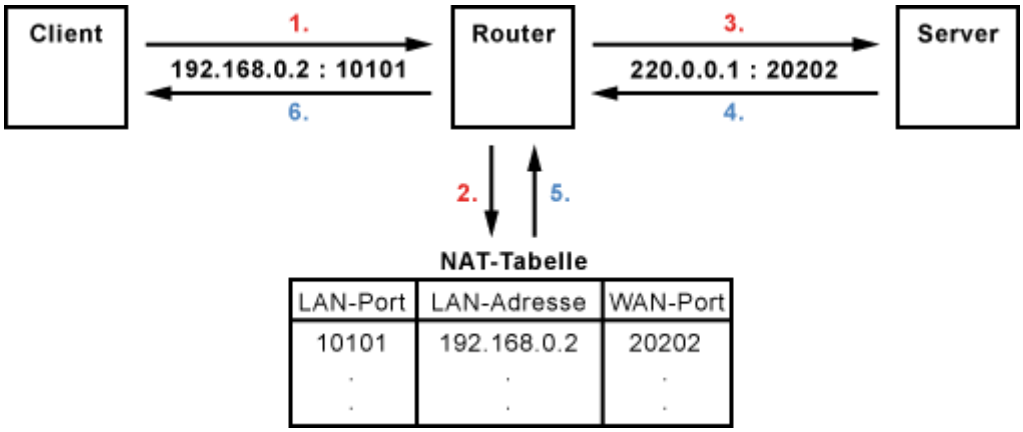
Internet in Österreich

NAT

Der Betrieb eines NAT-Routers ist üblicherweise an einem gewöhnlichen Internet-Anschluss. Zum Beispiel über DSL oder Kabelmodem. Der eingesetzte Router dient als Zugang zum Internet und als Standard-Gateway für das lokale Netzwerk. In der Regel wollen über den Router mehr Geräte ins Internet, als öffentliche IP-Adressen zur Verfügung stehen. In der Regel nur eine einzige. Beispielsweise bekommt der Router des lokalen Netzwerks die öffentliche IP-Adresse 222.0.0.1 für seinen WAN-Port vom Internet Service Provider (ISP) zugewiesen. Weil nur eine öffentliche IP-Adresse vom Internet-Provider zugeteilt wurde, bekommen die Stationen im LAN private IP-Adressen aus speziell dafür reservierten Adressbereichen zugewiesen. Diese Adressen sind nur innerhalb des privaten Netzwerks gültig. Private IP-Adressen werden in öffentlichen Netzen nicht geroutet. Das bedeutet, dass Stationen mit privaten IP-Adressen keine Verbindung ins Internet bekommen können. Damit das trotzdem funktioniert, wurde NAT entwickelt.



Ablauf von NAT



1. Der Client schickt seine Datenpakete mit der IP-Adresse 192.168.0.2 und dem TCP-Port 10101 an sein Standard-Gateway, bei dem es sich um einen NAT-Router handelt.
2. Der NAT-Router tauscht IP-Adresse (LAN-Adresse) und TCP-Port (LAN-Port) aus und speichert beides mit der getauschten Port-Nummer (WAN-Port) in der NAT-Tabelle.
3. Der Router leitet das Datenpaket mit der WAN-Adresse 220.0.0.1 und der neuen TCP-Port 20202 ins Internet weiter.
4. Der Empfänger (Server) verarbeitet das Datenpaket und schickt seine Antwort zurück.
5. Der NAT-Router stellt nun anhand der Port-Nummer 20202 (WAN-Port) fest, für welche IP-Adresse (LAN-Adresse) das Paket im lokalen Netz gedacht ist.
6. Er tauscht die IP-Adresse und die Port-Nummer wieder aus und leitet das Datenpaket ins lokale Netz weiter, wo es der Client entgegen nimmt.

Probleme

- Durch NAT können nur noch die, die über öffentliche IPv4-Adressen und in der Regel auch über das notwendige Kleingeld verfügen, Dienste im Internet anbieten.
- Die Einträge in der NAT-Tabelle des Routers sind nur für eine kurze Zeit gültig. Für eine Anwendung, die nur sehr unregelmäßig Daten austauscht, bedeutet das, dass ständig die Verbindung abgebrochen wird und dadurch die Erreichbarkeit eingeschränkt ist.

Vorteile

- Mehr Sicherheit - PCs im Netzwerk nicht direkt ansprechbar = mehr Privatsphäre
- Firewall - keine von außen eingehenden Verbindungen erlaubt, so fern keine Verbindung von intern aufgebaut wurde

ICMP - Internet Control Message Protocol (Layer 3)

Das Internet Control Message Protocol (ICMP) ist Bestandteil des Internet Protocols (IP). Es wird aber als eigenständiges Protokoll behandelt, das zur Übermittlung von Meldungen über IP dient. Hauptaufgabe von ICMP ist die **Übertragung von Statusinformationen und Fehlermeldungen der Protokolle IP, TCP und UDP**. Die ICMP-Meldungen werden zwischen Rechnern und aktiven Netzknoten, z. B. Routern, benutzt, um sich gegenseitig Probleme mit Datenpaketen mitzuteilen. Ziel ist, die Übertragungsqualität zu verbessert.

Jedes Betriebssystem mit TCP/IP hat Tools, die ICMP nutzen. Zwei bekannte Tools sind Ping und Trace Route. Beides sind sehr einfache Programme, die zur Analyse von Netzwerk-Problemen gedacht sind und damit wesentlich zur Problemlösung beitragen können.

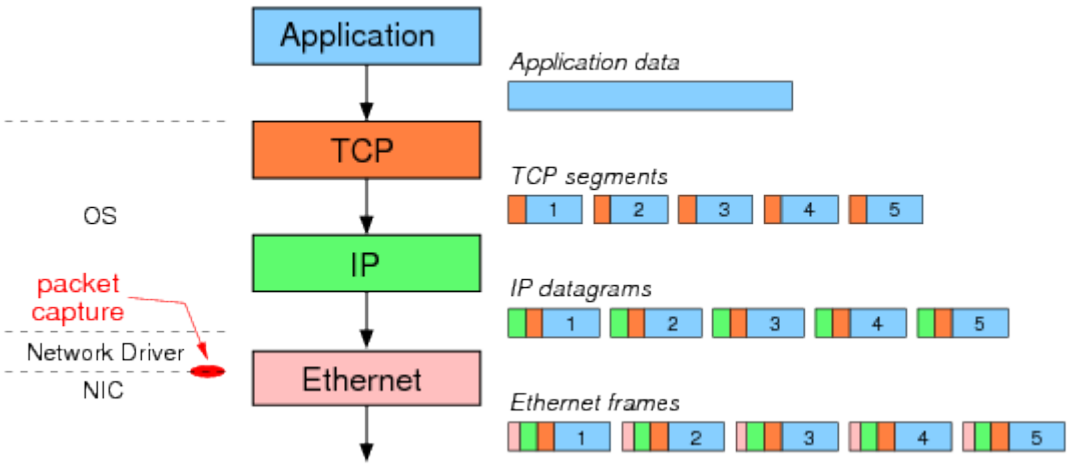
TCP - Transmission Control Protocol (Layer 4)

Das **Transmission Control Protocol** (=Übertragungssteuerungsprotokoll) ist ein Netzwerkprotokoll, das definiert, auf welche Art und Weise Daten zwischen Netzwerkkomponenten ausgetauscht werden sollen. Nahezu sämtliche aktuellen Betriebssysteme moderner Computer beherrschen TCP und nutzen es für den Datenaustausch mit anderen Rechnern. Das Protokoll ist ein zuverlässiges, verbindungsorientiertes, paketvermitteltes Transportprotokoll in Computernetzwerken. Es ist Teil der Internetprotokollfamilie, der Grundlage des Internets.

Aufgaben des TCP-Protokolls

Segmentierung (Data Segmenting)

Eine Funktion von TCP besteht darin, den von den Anwendungen kommenden **Datenstrom in Datenpakete bzw. Segmente aufzuteilen (Segmentierung)** und beim Empfang wieder zusammenzusetzen. Die Segmente werden mit einem **Header** versehen, in dem Steuer- und Kontroll-Informationen enthalten sind. Danach werden die **Segmente an das Internet Protocol (IP) übergeben**. Da beim IP-Routing die **Datenpakete unterschiedliche Wege** gehen können, entstehen unter Umständen **zeitliche Verzögerungen**, die dazu führen, dass die Datenpakete beim Empfänger in einer anderen Reihenfolge eingehen, als sie ursprünglich hatten. Deshalb werden die Segmente beim Empfänger auch wieder in die **richtige Reihenfolge** gebracht und erst dann an die adressierte Anwendung übergeben. Dazu werden die Segmente mit einer **fortlaufenden Sequenznummer** versehen (Sequenzierung).



Verbindungsmanagement (Connection Establishment and Termination)

Als **verbindungsorientiertes Protokoll** ist TCP für den **Verbindungsaufbau und Verbindungsabbau** zwischen zwei Stationen einer **Ende-zu-Ende-Kommunikation** zuständig. Durch TCP stehen Sender und Empfänger ständig in Kontakt zueinander (siehe TCP Kommunikation).

Fehlerbehandlung (Error Detection)

Obwohl es sich eher um eine virtuelle Verbindung handelt, werden während der Datenübertragung

ständig **Kontrollmeldungen** ausgetauscht. Der Empfänger bestätigt dem Sender jedes empfangene Datenpaket. Trifft keine Bestätigung beim Absender ein, wird das Paket noch mal verschickt. Da es bei Übertragungsproblemen zu doppelten Datenpaketen und Quittierungen kommen kann, werden alle TCP-Pakete und TCP-Meldungen mit einer **fortlaufenden Sequenznummer** gekennzeichnet. So sind Sender und Empfänger in der Lage, die Reihenfolge und Zuordnung der Datenpakete und Meldungen zu erkennen.

Flusssteuerung (Flow Control)

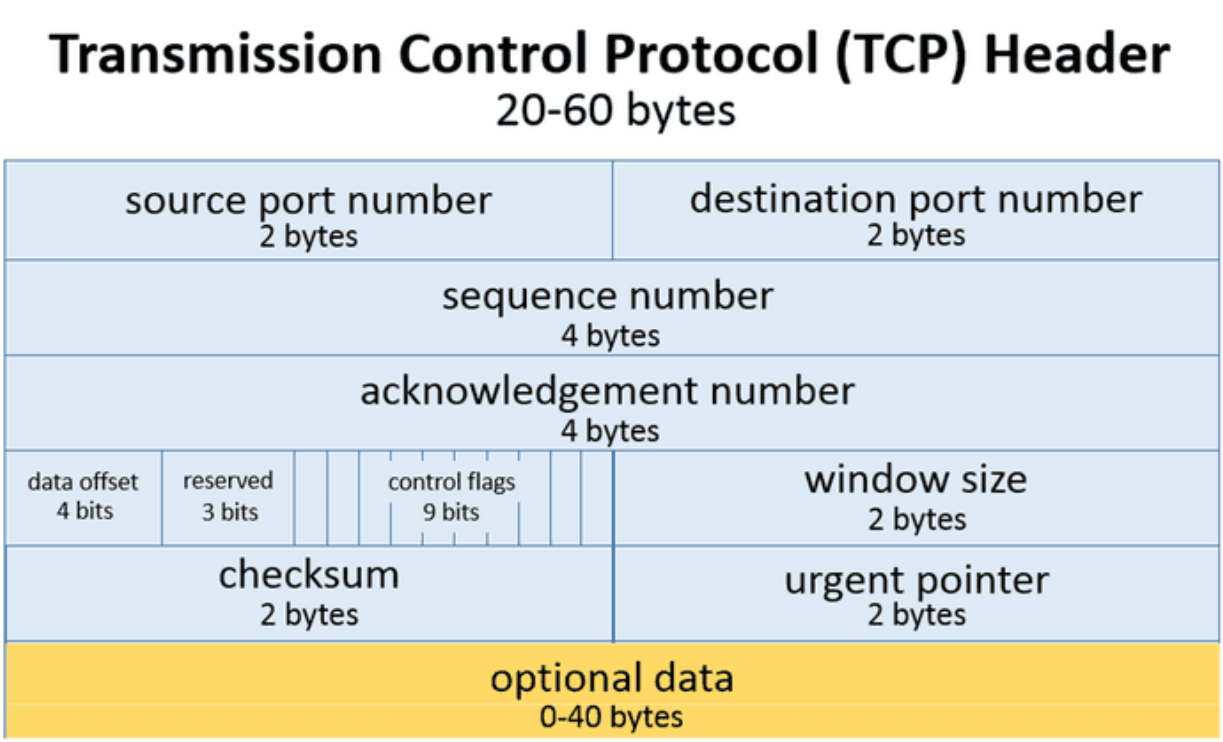
Bei einer paketorientierten Übertragung ohne feste zeitliche Zuordnung und ohne Kenntnis des Übertragungswegs erhält das Transport-Protokoll vom Übertragungssystem **keine Information über die verfügbare Bandbreite**. Mit der **Flusssteuerung** werden beliebig langsame oder schnelle **Übertragungsstrecken dynamisch auszulasten** und auch auf unerwartete Engpässe und Verzögerungen reagiert.

Anwendungsunterstützung (Application Support)

TCP- und UDP-Ports sind eine Software-Abstraktion, um Kommunikationsverbindungen voneinander unterscheiden zu können. Ähnlich wie IP-Adressen Rechner in Netzwerken adressieren, **adressieren Ports spezifische Anwendungen** oder Verbindungen, die auf einem Rechner laufen.

Aufbau eines TCP Headers

Aufbau des TCP-Headers TCP-Pakete setzen sich aus dem Header-Bereich und dem Daten-Bereich zusammen. Im Header sind alle Informationen enthalten, die für eine gesicherte TCP-Verbindung wichtig sind. Der TCP-Header ist in mehrere 32-Bit-Blöcke aufgeteilt. Mindestens enthält der Header 5 solcher Blöcke. Somit hat ein TCP-Header eine Länge von **mindestens 20 Byte**.

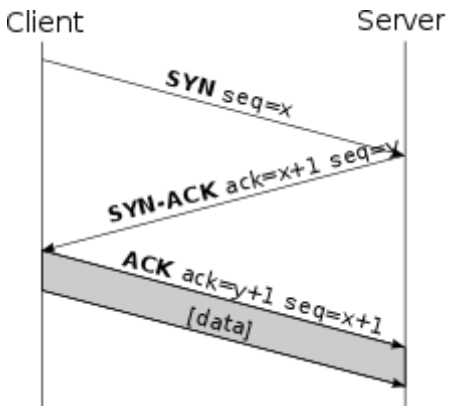


TCP Kommunikation

Verbindungsaufbau - 3-Way-Handshake

Der Client, der eine Verbindung aufbauen will, sendet dem Server ein **SYN-Paket** (von englisch synchronize) mit einer Sequenznummer x. Die Sequenznummern sind dabei für die Sicherstellung einer vollständigen Übertragung in der richtigen Reihenfolge und ohne Duplikate wichtig. Es handelt sich also um ein Paket, dessen SYN-Bit im Paketkopf gesetzt ist (siehe TCP-Header). Die Start-Sequenznummer ist eine beliebige Zahl, deren Generierung von der jeweiligen TCP-Implementierung abhängig ist. Sie sollte jedoch möglichst zufällig sein, um Sicherheitsrisiken zu vermeiden.

Der Server (siehe Abbildung) empfängt das Paket. Ist der Port geschlossen, antwortet er mit einem TCP-RST, um zu signalisieren, dass keine Verbindung aufgebaut werden kann. Ist der Port geöffnet, bestätigt er den Erhalt des ersten SYN-Pakets und stimmt dem Verbindungsaufbau zu, indem er ein **SYN/ACK-Paket** zurückschickt (ACK von engl. acknowledgement ‚Bestätigung'). Das gesetzte ACK-Flag im TCP-Header kennzeichnet diese Pakete, welche die Sequenznummer x+1 des SYN-Pakets im Header enthalten. Zusätzlich sendet er im Gegenzug seine Start-Sequenznummer y, die ebenfalls beliebig und unabhängig von der Start-Sequenznummer des Clients ist.

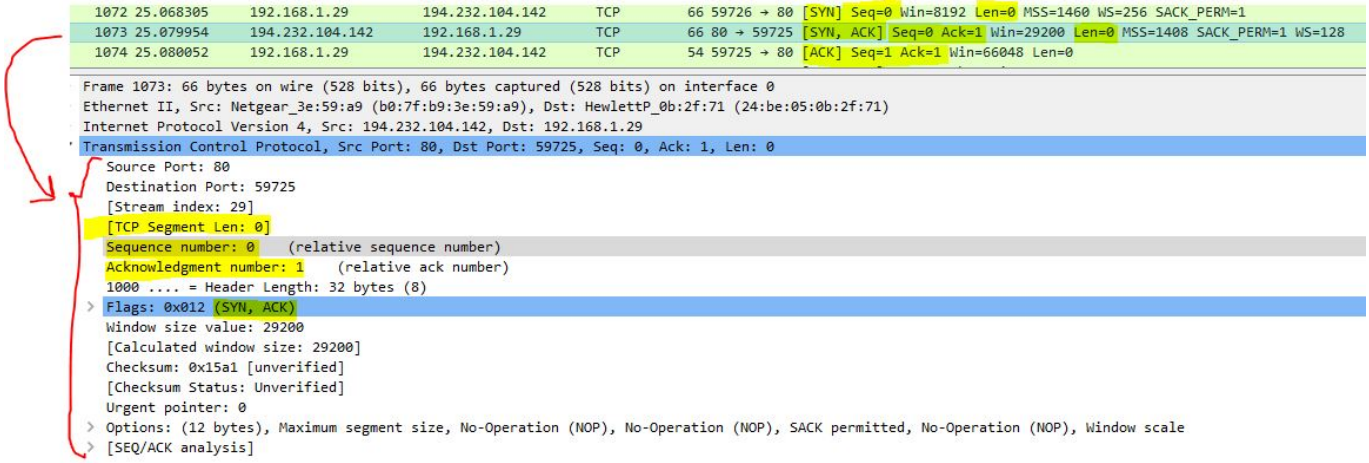


Der Client bestätigt zuletzt den Erhalt des SYN/ACK-Pakets durch das Senden eines eigenen **ACK-Paket**s mit der Sequenznummer x+1. Dieser Vorgang wird auch als **Forward Acknowledgement** bezeichnet. Aus Sicherheitsgründen sendet der Client den Wert y+1 (die Sequenznummer des Servers + 1) im ACK-Segment zurück. Die Verbindung ist damit aufgebaut. Im folgenden Beispiel wird der Vorgang abstrakt dargestellt:

```
1.  SYN-SENT            →    <SEQ=100><CTL=SYN>              →    SYN-RECEIVED
2.  SYN/ACK-RECEIVED    ←    <SEQ=300><ACK=101><CTL=SYN,ACK>    ←
SYN/ACK-SENT
3.  ACK-SENT            →    <SEQ=101><ACK=301><CTL=ACK>    →    ESTABLISHED
```

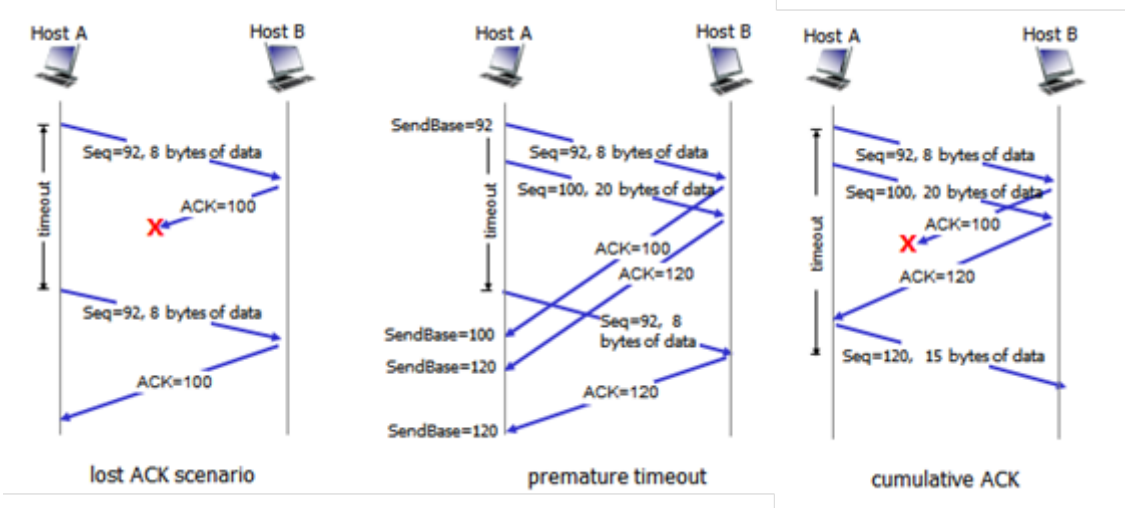
Einmal aufgebaut, ist die Verbindung für beide Kommunikationspartner gleichberechtigt, man kann einer bestehenden Verbindung auf TCP-Ebene nicht ansehen, wer der Server und wer der Client ist. Daher hat eine Unterscheidung dieser beiden Rollen in der weiteren Betrachtung keine Bedeutung mehr.

Aufzeichnung mit Wireshark

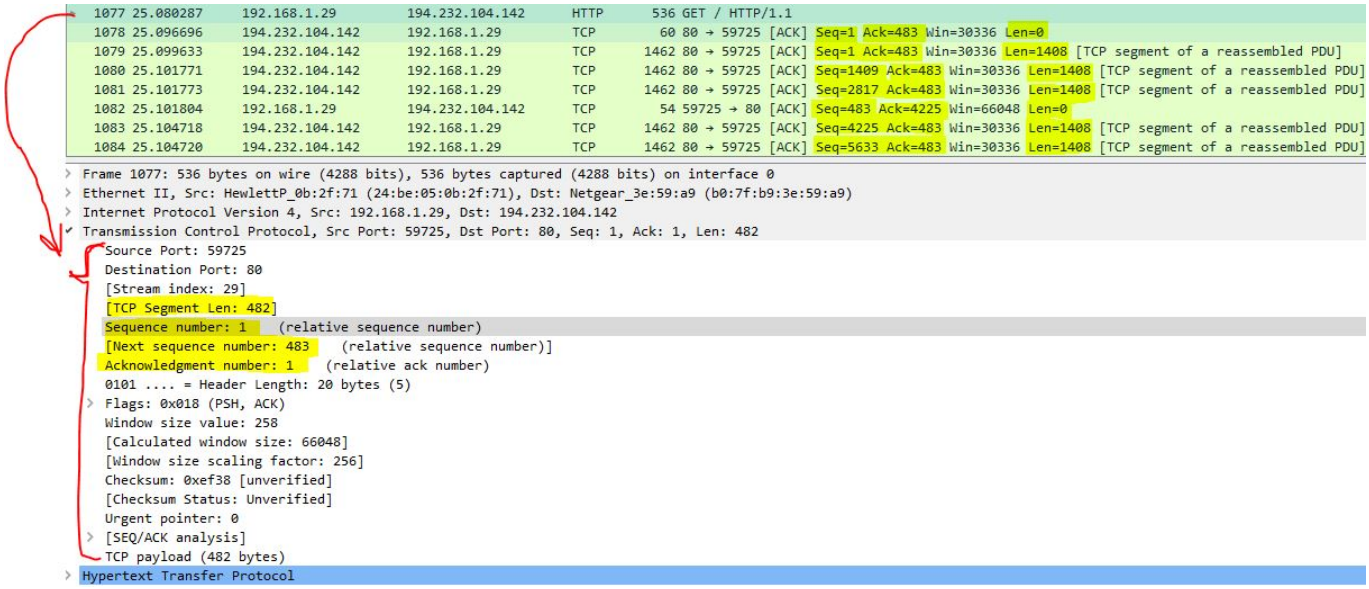


Datenaustausch

Der Sender beginnt mit dem Senden des ersten Datenpakets (Send Paket 1). Der Empfänger nimmt das Paket entgegen (Receive Paket 1) und bestätigt den Empfang (Send ACK Paket 1). Der Sender nimmt die Bestätigung entgegen (Receive ACK Paket 1) und sendet das zweite Datenpaket (Send Paket 2). Der Empfänger nimmt das zweite Paket entgegen (Receive Paket 2) und bestätigt den Empfang (Send ACK Paket 2). Der Sender nimmt die zweite Bestätigung entgegen (Receive ACK Paket 2). Und so läuft der Datenaustausch weiter, bis alle Pakete übertragen wurden.

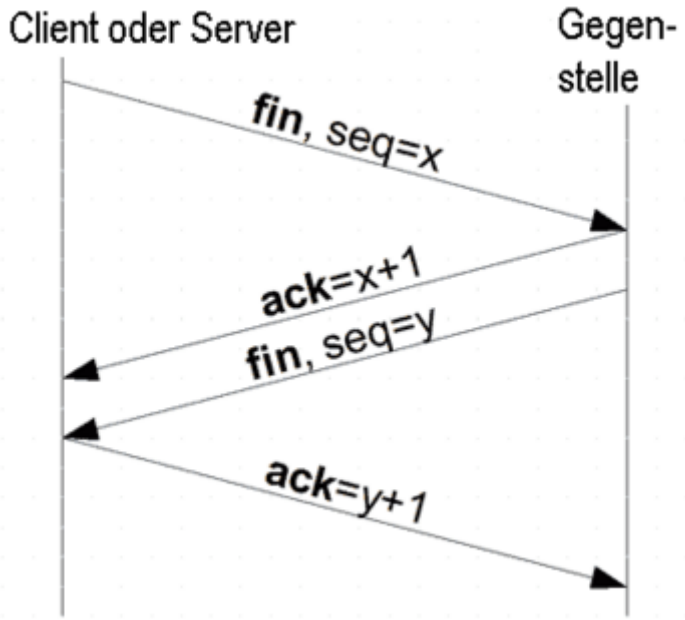


Aufzeichnung mit Wireshark

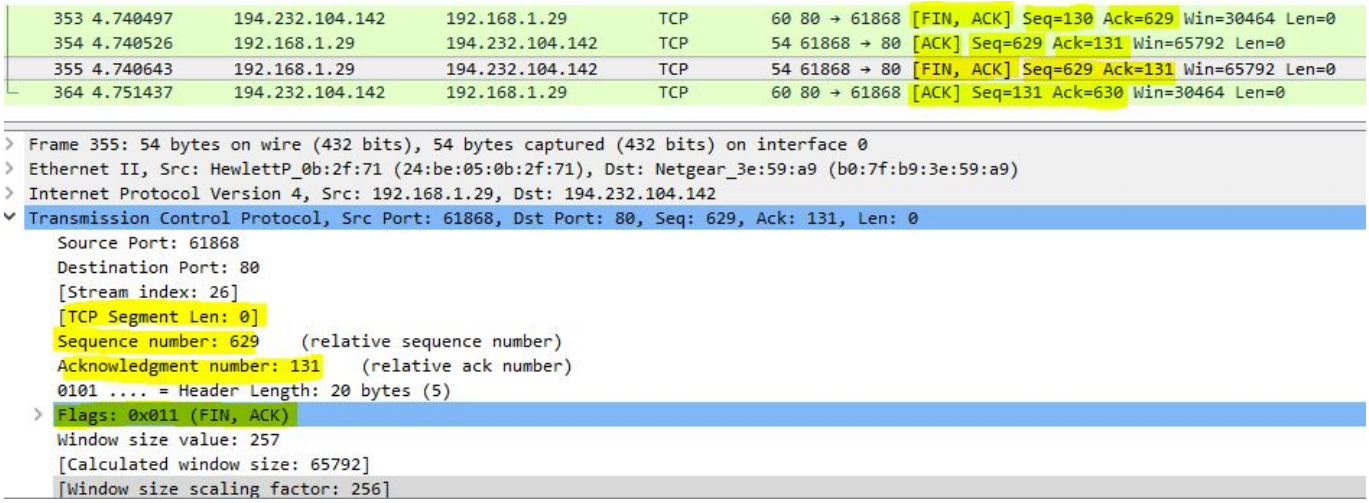


Verbindungsabbau

Der Verbindungsabbau kann sowohl vom Client als auch vom Server vorgenommen werden. Zuerst schickt einer der beiden der Gegenstelle einen Verbindungsabbauwunsch (**FIN**). Die Gegenstelle bestätigt den Erhalt der Nachricht (ACK) und schickt gleich darauf ebenfalls einen Verbindungsabbauwunsch (**FIN**). Danach bekommt die Gegenstelle noch mitgeteilt, dass die Verbindung abgebaut ist (**ACK**).



Aufzeichnung mit Wireshark



```
353 4.740497    194.232.104.142    192.168.1.29       TCP    60 80 → 61868 [FIN, ACK] Seq=130 Ack=629 Win=30464 Len=0
354 4.740526    192.168.1.29       194.232.104.142    TCP    54 61868 → 80 [ACK] Seq=629 Ack=131 Win=65792 Len=0
355 4.740643    192.168.1.29       194.232.104.142    TCP    54 61868 → 80 [FIN, ACK] Seq=629 Ack=131 Win=65792 Len=0
364 4.751437    194.232.104.142    192.168.1.29       TCP    60 80 → 61868 [ACK] Seq=131 Ack=630 Win=30464 Len=0

> Frame 355: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
> Ethernet II, Src: HewlettP_0b:2f:71 (24:be:05:0b:2f:71), Dst: Netgear_3e:59:a9 (b0:7f:b9:3e:59:a9)
> Internet Protocol Version 4, Src: 192.168.1.29, Dst: 194.232.104.142
v Transmission Control Protocol, Src Port: 61868, Dst Port: 80, Seq: 629, Ack: 131, Len: 0
    Source Port: 61868
    Destination Port: 80
    [Stream index: 26]
    [TCP Segment Len: 0]
    Sequence number: 629    (relative sequence number)
    Acknowledgment number: 131    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x011 (FIN, ACK)
    Window size value: 257
    [Calculated window size: 65792]
    [Window size scaling factor: 256]
```

UDP - User Datagram Protocol (Layer 4)

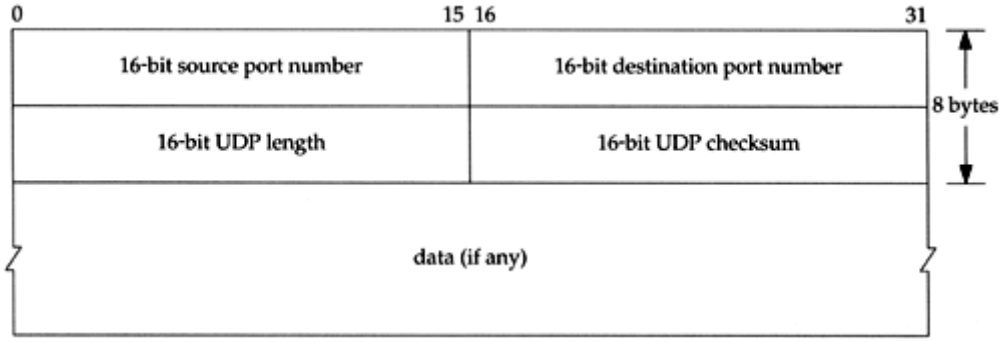
UDP ist ein **verbindungsloses Transport-Protokoll** und arbeitet auf der Schicht 4, der **Transportschicht**, des OSI-Schichtenmodells. Es hat damit eine vergleichbare Aufgabe, wie das verbindungsorientierte TCP. Allerdings arbeitet es **verbindungslos und damit unsicher**. Das bedeutet, der **Absender weiß nicht**, ob seine verschickten **Datenpakete angekommen sind**. Während TCP Bestätigungen beim Datenempfang sendet, verzichtet UDP darauf. Das hat den Vorteil, dass der Paket-Header viel kleiner ist und die Übertragungsstrecke keine Bestätigungen übertragen muss. Typischerweise wird UDP bei DNS-Anfragen, VPN-Verbindungen, Audio- und Video-Streaming verwendet.

Funktionsweise

UDP hat die selbe Aufgabe wie TCP, nur das nahezu alle Kontrollfunktionen fehlen, dadurch schlanker und einfacher zu verarbeiten ist. So besitzt UDP keinerlei Methoden die sicherstellen, dass ein Datenpaket beim Empfänger ankommt. Ebenso entfällt die Nummerierung der Datenpakete. UDP ist nicht in der Lage die Datenpakete in der richtigen Reihenfolge zusammenzusetzen. Statt dessen werden die UDP-Pakete direkt an die Anwendung weitergeleitet. Für eine sichere Datenübertragung ist deshalb die Anwendung zuständig. In der Regel wird UDP für Anwendungen und Dienste verwendet, die mit Paketverlusten umgehen können oder sich selber um das Verbindungsmanagement kümmern. UDP eignet sich auch für Anwendungen, die nur einzelne, nicht zusammenhängende Datenpakete transportieren müssen.

UDP Header

UDP-Pakete setzen sich aus dem Header-Bereich und dem Daten-Bereich zusammen. Im Header sind alle Informationen enthalten, die eine einigermaßen geordnete Datenübertragung zulässt und die ein UDP-Paket als ein solches erkennen lassen. Der UDP-Header ist in 32-Bit-Blöcke unterteilt. Er besteht aus zwei solcher Blöcke, die den Quell- und Ziel-Port, die Länge des gesamten UDP-Pakets und die Check-Summe enthalten. Der UDP-Header ist mit insgesamt 8 Byte sehr schlank und lässt sich mit wenig Rechenleistung verarbeiten.



TCP vs. UDP

DHCP - Dynamic Host Configuration Protocol (UDP, Ports 67 + 68, Layer 7)

DHCP ist ein Protokoll, um **IP-Adressen** in einem TCP/IP-Netzwerk **zu verwalten** und an die anfragenden Hosts zu verteilen. Mit DHCP ist jeder **Netzwerk-Teilnehmer** in der Lage sich selber **automatisch zu konfigurieren**.

Warum DHCP?

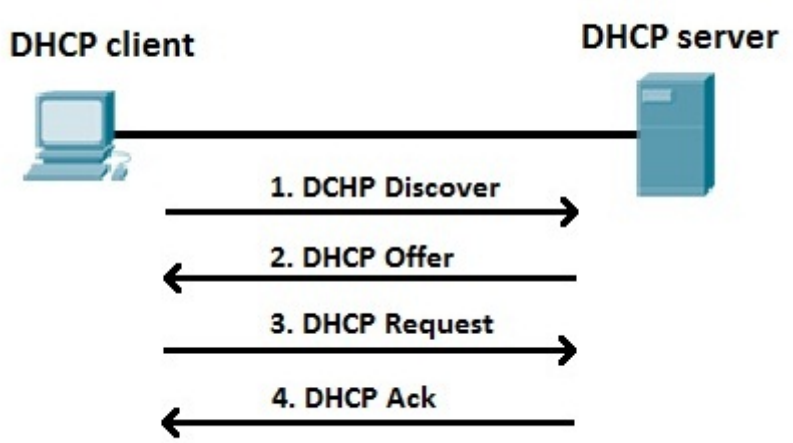
Um ein Netzwerk per TCP/IP aufzubauen ist es notwendig an jedem Host eine IP-Konfiguration vorzunehmen. Für ein TCP/IP-Netzwerk müssen folgende Einstellungen an jedem Host vorgenommen werden:

- Vergabe einer eindeutigen IP-Adresse
- Zuweisen einer Subnetzmaske (Subnetmask)
- Zuweisen des zuständigen Default- bzw. Standard-Gateways
- Zuweisen des zuständigen DNS-Servers

In den ersten IP-Netzen wurden IP-Adressen noch von Hand **aufwendig vergeben** und **fest** in die Systeme **eingetragen**. Die dazu **erforderliche Dokumentation** war jedoch nicht immer fehlerfrei und schon gar nicht aktuell und vollständig. Der Ruf nach einer einfachen und automatischen Adressverwaltung wurde deshalb besonders bei Betreibern großer Netze laut. Hier war durch die manuelle Verwaltung und Konfiguration sehr **viel Planungs- und Arbeitszeit** notwendig. Um für die Betreiber der immer größer werdenden Netze eine Erleichterung zu verschaffen wurde DHCP entwickelt. Mit DHCP kann jede IP-Host die IP-Adresskonfiguration von einem DHCP-Server anfordern und sich selber automatisch konfigurieren. So müssen IP-Adressen nicht mehr manuell verwaltet und zugewiesen werden.

Funktionsweise

1. Der DHCP-Client **schickt an alle Rechner** im Netzwerk (=Broadcast) eine **DHCP-Server-Suchanfrage (DHCP-Discover)**. Bis auf den DHCP-Server verwerfen alle Rechner das Datenpaket.
2. Nur der **DHCP-Server** empfängt den DHCP-Discover und bietet dem Client mittels Broadcast eine **freie IP-Adresse an (DHCP-Offer)**
3. Nur der **DHCP-Client** empfängt den DHCP-Offer und antwortet mit einer eine **DHCP-Anfrage (DHCP-Request)**. Alle anderen Clients verwerfen wiederum das DHCP-Angebot.
4. Der **DHCP-Server** empfängt den DHCP-Request und **bestätigt** dem DHCP-Client die angefragte IP-Adresse **mittels DHCP-ACK**.



DNS - Domain Name System (UDP, Port 53 , Layer 7)

Das Domain Name System, kurz DNS, wird auch als **Telefonbuch des Internets** bezeichnet. Ähnlich wie man in einem Telefonverzeichnis nach einem Namen sucht, um die Telefonnummer heraus zu bekommen, schaut man im DNS nach einem Computernamen, um die dazugehörige IP-Adresse zu bekommen. Die IP-Adresse wird benötigt, um eine Verbindung zu einem Server aufbauen zu können, über den nur der Computername bekannt ist.

Das Domain Name System ist ein System zur Auflösung von Computernamen in IP-Adressen und umgekehrt. DNS kennt keine zentrale Datenbank. Die Informationen sind auf vielen tausend Nameservern (DNS-Server) verteilt. Möchte man zum Beispiel die Webseite www.orf.at besuchen, dann fragt der Browser einen DNS-Server, der in der IP-Konfiguration hinterlegt ist. Das ist in der Regel der Router des Internet-Zugangs. Je nach dem, ob die DNS-Anfrage beantwortet werden kann oder nicht, wird eine Kette weiterer DNS-Server befragt, bis die Anfrage positiv beantwortet und eine IP-Adresse an den Browser zurück geliefert werden kann.

Wenn ein Computername oder Domain-Name nicht aufgelöst werden kann, dann kann auch keine Verbindung zu dem betreffenden Host aufgebaut werden. Es sei denn, der Nutzer verfügt über das Wissen der IP-Adresse. Das bedeutet, ohne DNS ist die Kommunikation im Netzwerk und im Internet praktisch nicht möglich. Deshalb existieren viele tausend DNS-Server auf der ganzen Welt, die zusätzlich hierarchisch angeordnet sind und sich gegenseitig über Änderungen informieren.

Top-Level-Domain & Second-Level-Domain

Domain-Namen sind hierarchisch von rechts nach links gegliedert. Der ganz rechte Abschnitt nach dem letzten Punkt heißt Top-Level-Domain (TLD), der davor Second-Level-Domain (SLD) oder einfach „Domain“. Alle weiteren Namensteile links davon sind jeweils Sub- bzw. Third-Level-Domains (Fourth Level, Fifth Level, Sixth Level usw.). Ein Beispiel verdeutlicht die Begrifflichkeiten: Der Name „www.example.com“ besteht aus drei Ebenen:

- „.com“: die erste Ebene, auch Top-Level-Domain oder Domain-Endung genannt
- „example“: die zweite Ebene, auch als Second-Level-Domain oder Domain bezeichnet
- „www“: die dritte Ebene, auch Sub- oder Third-Level-Domain genannt

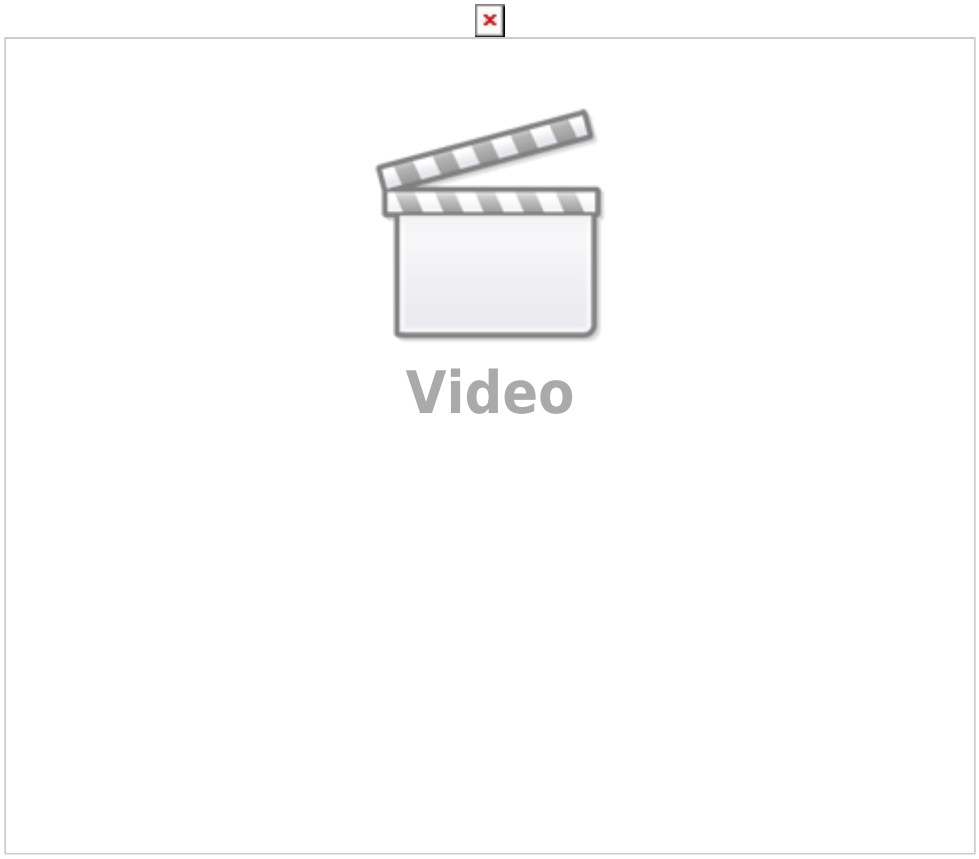
FQDN (Fully Qualified Domain Name)

Der vollständige Name einer Domain wird als ihr Fully Qualified Domain Name (FQDN) bezeichnet. Der Domain-Name ist in diesem Fall eine absolute Adresse.

Der FQDN www.example.com. ergibt sich durch:

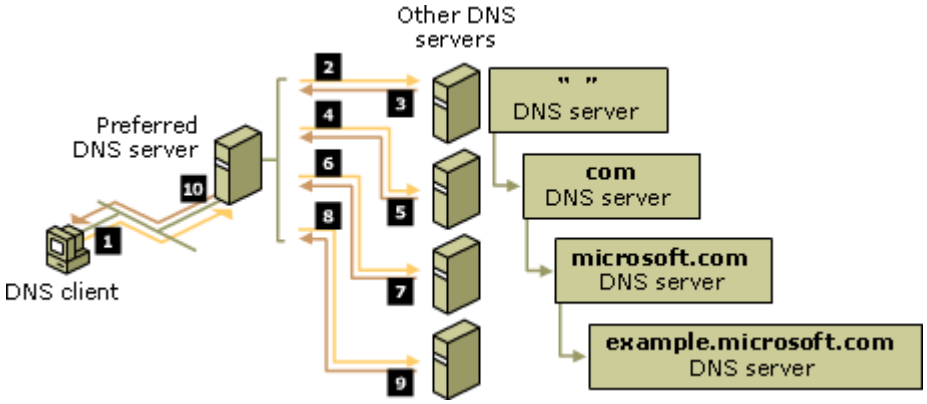
```
3rd-level-label. 2nd-level-label. Top-Level-Domain. root-label
```

Da das Root-Label immer leer ist (es besteht aus einer leeren Zeichenkette), wird bei den meisten Benutzer-Anwendungen (zum Beispiel Browsern) in der Regel auf die Eingabe des Punktes zwischen dem Label der Top Level Domain und dem root-label verzichtet. Streng genommen handelt es sich bei dieser Schreibweise nicht mehr um eine absolute, sondern um eine relative Adresse und damit nicht mehr um einen FQDN.

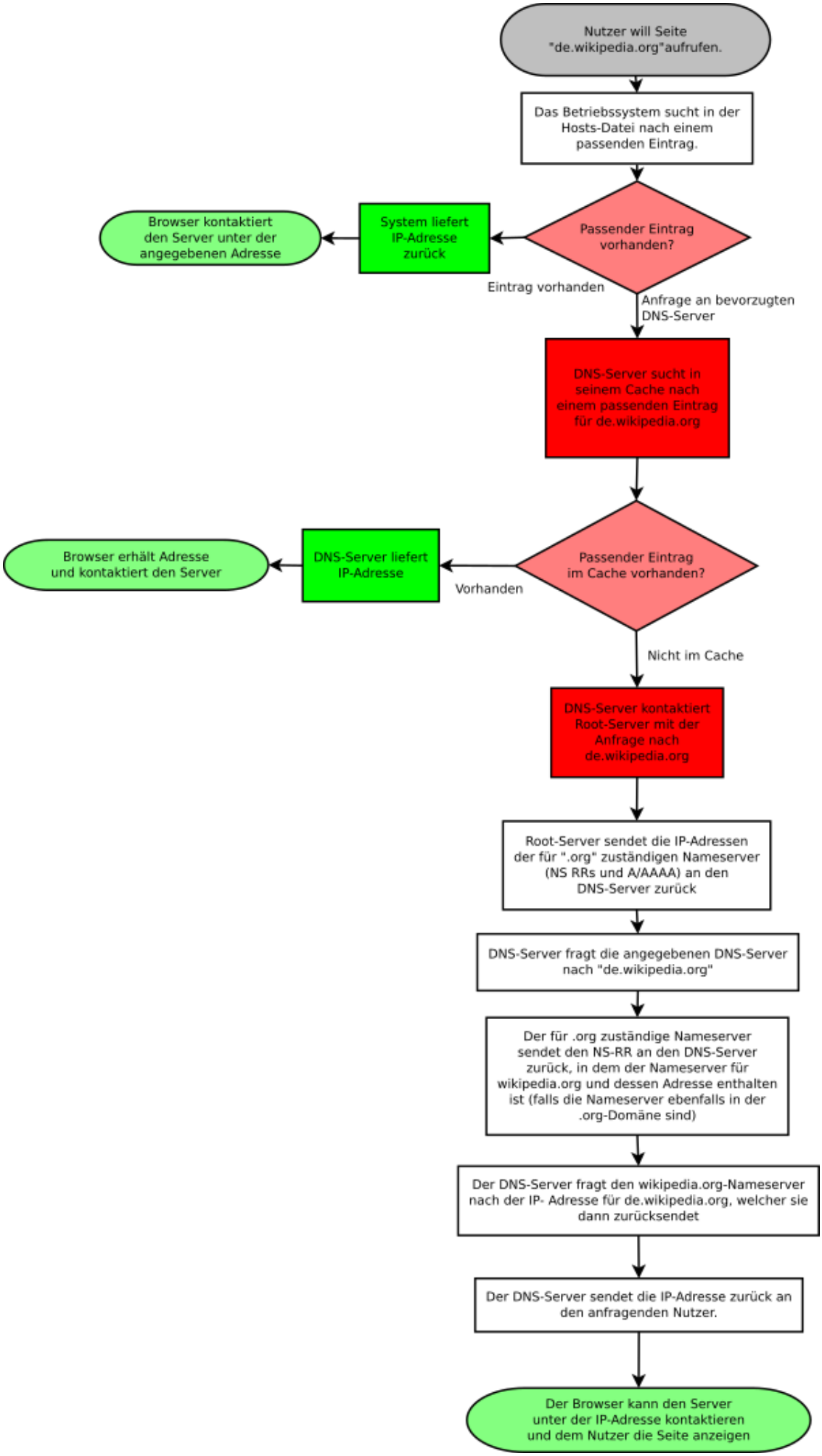


Rekursive Namensauflösung - Rekursive DNS-Serverstruktur

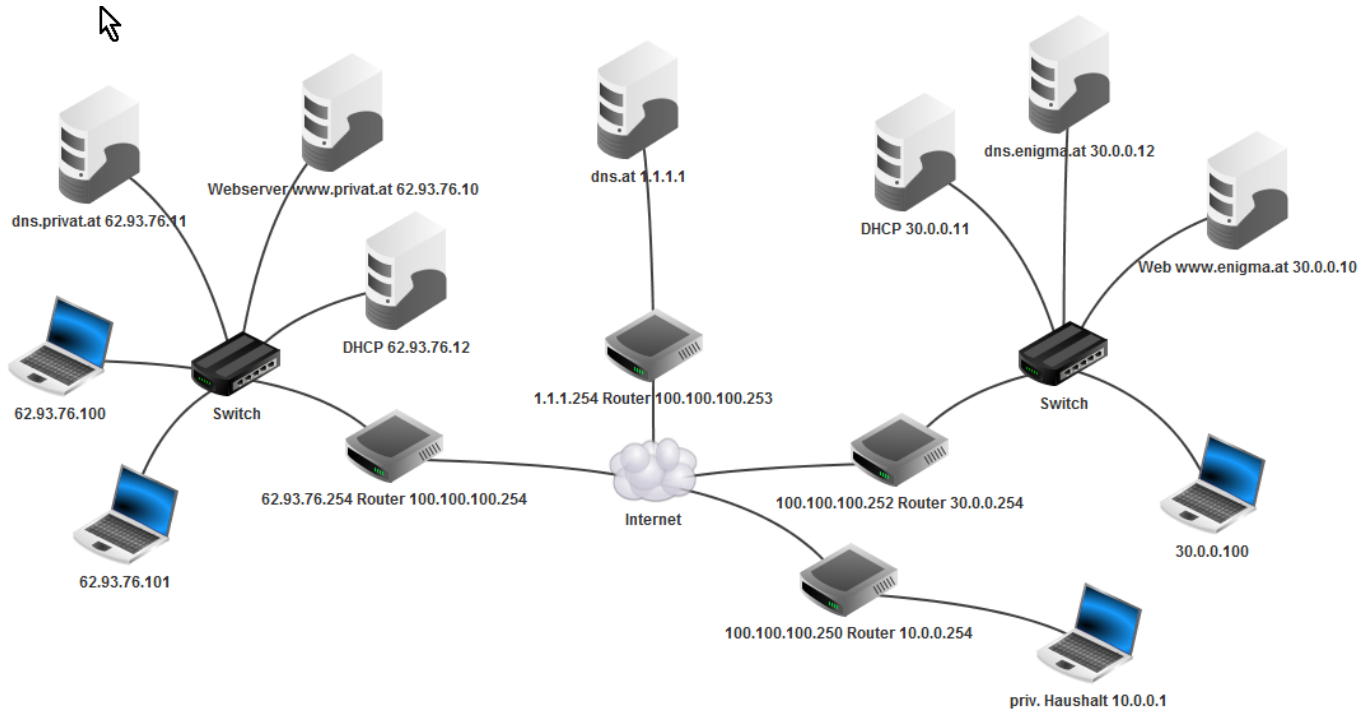
- Einzelne DNS-Server haben nicht jeden Domainnamen gespeichert. Informationen werden hierarchisch von übergeordneten DNS-Servern abgefragt. Die folgenden Grafiken sollen den Prozess veranschaulichen:



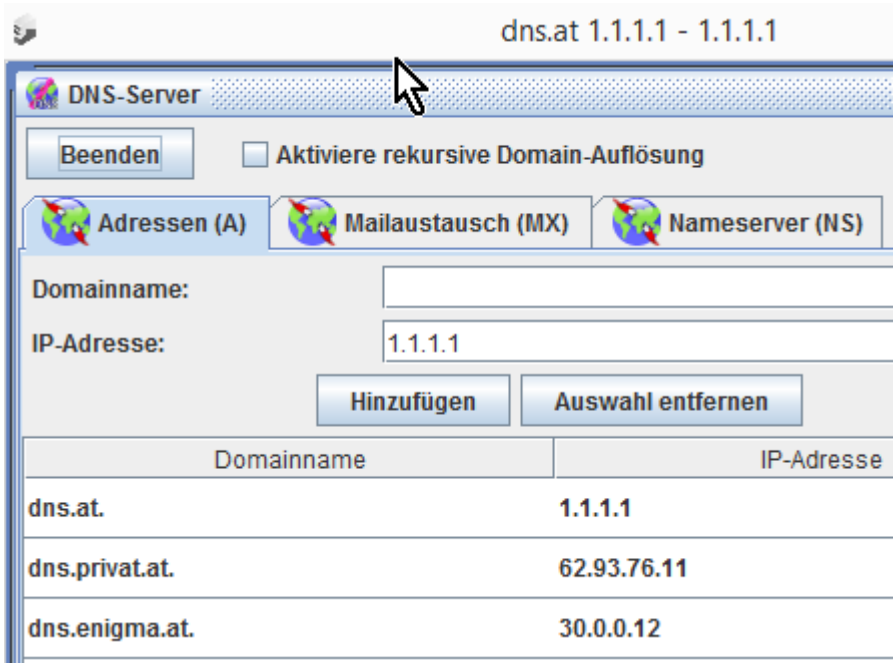
- Hier eine genauere Abfolge der Anfragen:

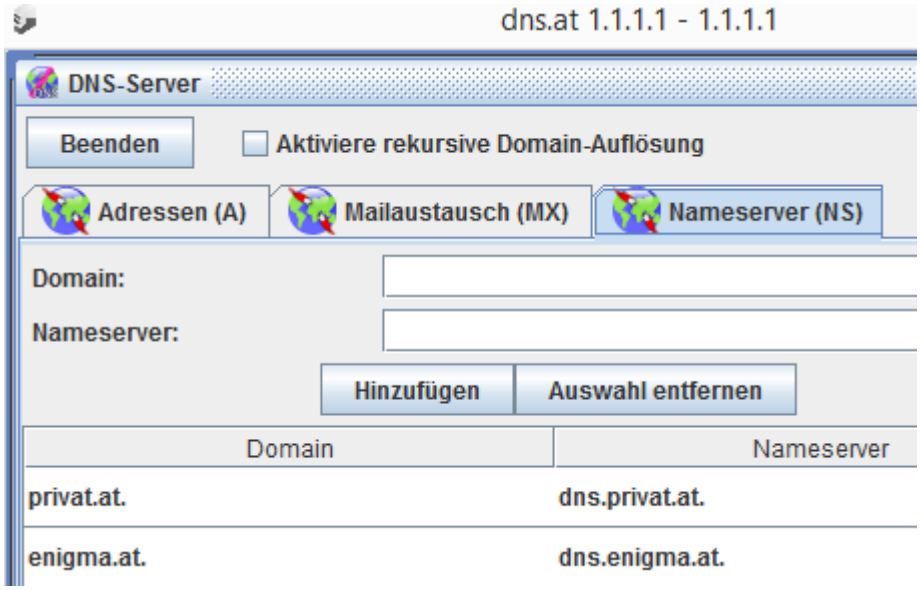

Nutzer will Seite "de.wikipedia.org"aufrufen.
Das Betriebssystem sucht in der Hosts-Datei nach einem passenden Eintrag.
Passender Eintrag vorhanden?
System liefert IP-Adresse zurück
Browser kontaktiert den Server unter der angegebenen Adresse
Eintrag vorhanden
Anfrage an bevorzugten DNS-Server
DNS-Server sucht in seinem Cache nach einem passenden Eintrag für de.wikipedia.org
Passender Eintrag im Cache vorhanden?
DNS-Server liefert IP-Adresse
Browser erhält Adresse und kontaktiert den Server
Vorhanden
Nicht im Cache
DNS-Server kontaktiert Root-Server mit der Anfrage nach de.wikipedia.org
Root-Server sendet die IP-Adressen der für ".org" zuständigen Nameserver (NS RRs und A/AAAA) an den DNS-Server zurück
DNS-Server fragt die angegebenen DNS-Server nach "de.wikipedia.org"
Der für .org zuständige Nameserver sendet den NS-RR an den DNS-Server zurück, in dem der Nameserver für wikipedia.org und dessen Adresse enthalten ist (falls die Nameserver ebenfalls in der .org-Domäne sind)
Der DNS-Server fragt den wikipedia.org-Nameserver nach der IP- Adresse für de.wikipedia.org, welcher sie dann zurücksendet
Der DNS-Server sendet die IP-Adresse zurück an den anfragenden Nutzer.
Der Browser kann den Server unter der IP-Adresse kontaktieren und dem Nutzer die Seite anzeigen

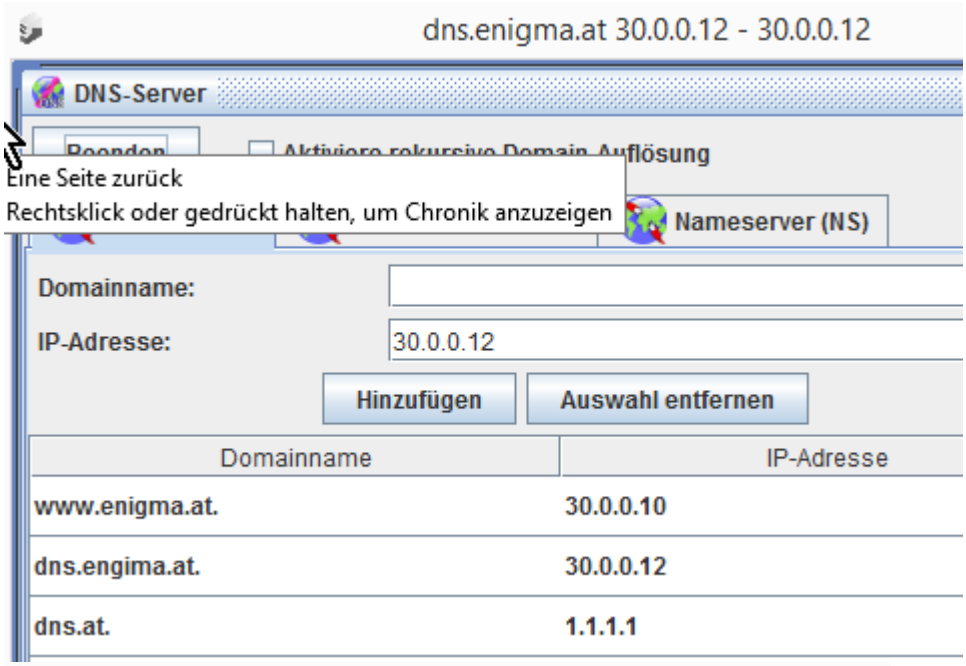
Mittels Filius kann eine hierarchische DNS-Serverstruktur aufgebaut werden:

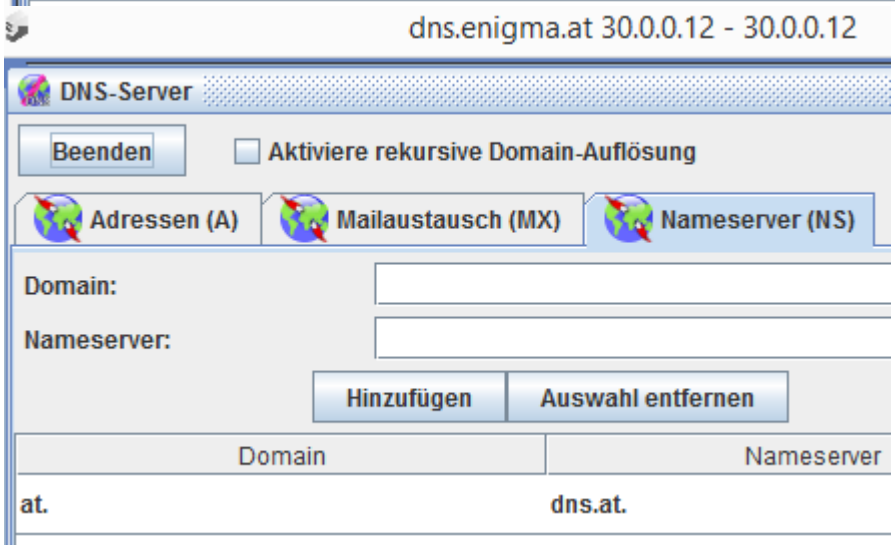


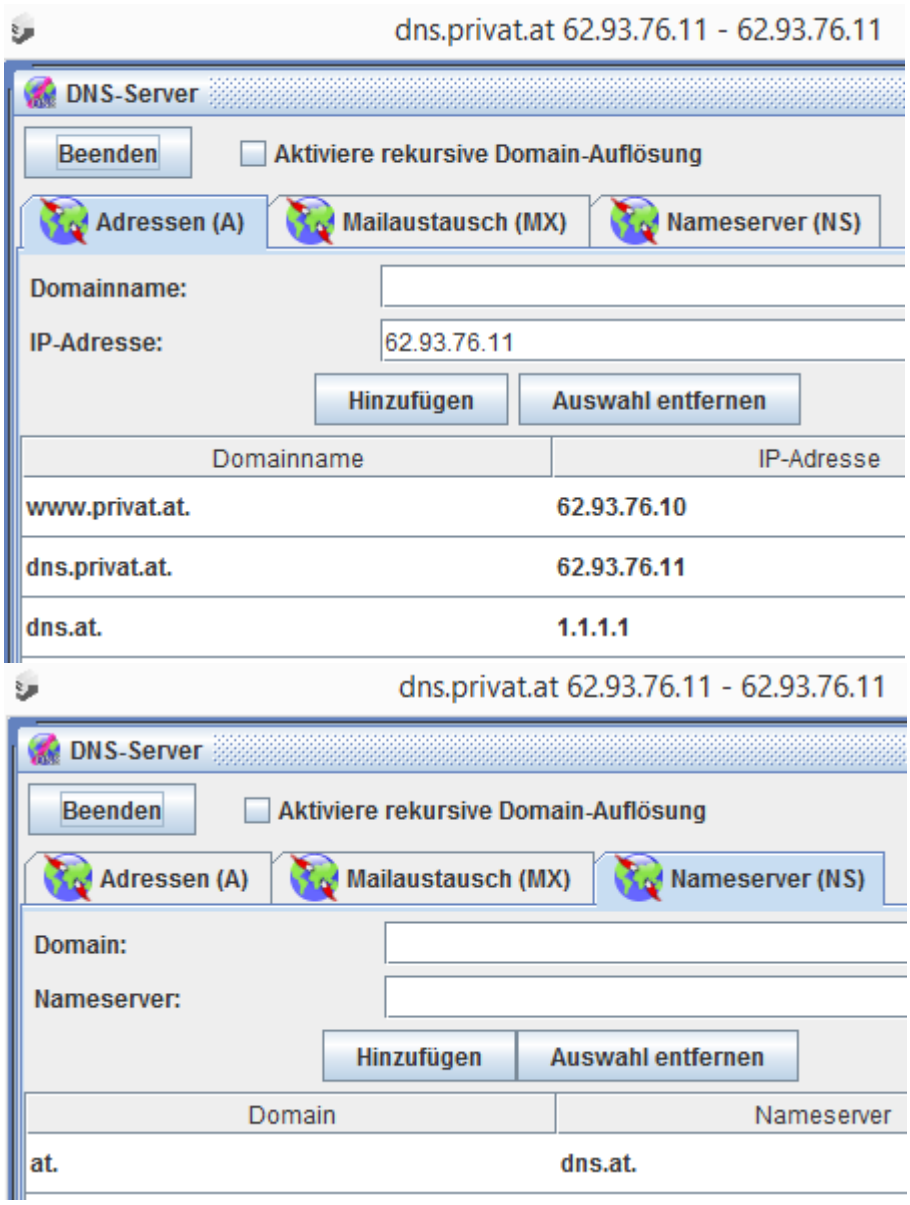
Hier die Screenshots über die entsprechenden Eintragungen in den Nameservern.




dns.at 1.1.1.1 - 1.1.1.1
DNS-Server
Beenden
Aktiviere rekursive Domain-Auflösung
Adressen (A)
Mailaustausch (MX)
Nameserver (NS)
Domain:
Nameserver:
Hinzufügen
Auswahl entfernen
Domain
Nameserver
privat.at.
dns.privat.at.
enigma.at.
dns.enigma.at.


dns.enigma.at 30.0.0.12 - 30.0.0.12
DNS-Server
Eine Seite zurück
Rechtsklick oder gedrückt halten, um Chronik anzuzeigen
Nameserver (NS)
Domainname:
IP-Adresse:
30.0.0.12
Hinzufügen
Auswahl entfernen
Domainname
IP-Adresse
www.enigma.at.
30.0.0.10
dns.engima.at.
30.0.0.12
dns.at.
1.1.1.1

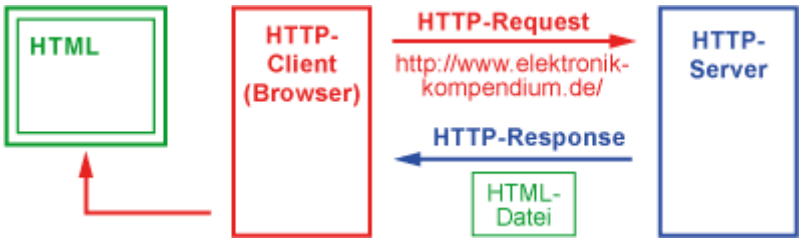

dns.enigma.at 30.0.0.12 - 30.0.0.12
DNS-Server
Beenden
Aktiviere rekursive Domain-Auflösung
Adressen (A)
Mailaustausch (MX)
Nameserver (NS)
Domain:
Nameserver:
Hinzufügen
Auswahl entfernen
Domain
Nameserver
at.
dns.at.



Hypertext Transfer Protocol (HTTP) (Port 80 - Layer 7)

HTTP ist das Kommunikationsprotokoll im World Wide Web (WWW). Die wichtigsten Funktionen sind Dateien vom Webserver anzufordern und in den Browser zu laden. Der Browser übernimmt dann die Darstellung von Texten und Bilder und kümmert sich um das Abspielen von Audio- und Video-Daten.

Funktionsweise



Die Kommunikation findet nach dem **Client-Server-Prinzip** statt. Der **HTTP-Client (Browser)** sendet seine **Anfrage (HTTP-Request)** an den **HTTP-Server (Webserver/Web-Server)**. Dieser bearbeitet die Anfrage und schickt seine **Antwort (HTTP-Response)** zurück. Nach der Antwort durch den Server ist diese Verbindung beendet. Typischerweise finden gleichzeitig mehrere HTTP-Verbindungen statt.

HTTP Adressierung

Damit der Server weiß, was er dem HTTP-Client schicken soll, adressiert der HTTP-Client eine Datei, die sich auf dem HTTP-Server befinden muss. Dazu wird vom HTTP-Client ein **URL (Uniform Resource Locator)** im HTTP-Header an den HTTP-Server übermittelt:

```
http://Servername.Domainname.Top-Level-Domain:TCP-Port/Pfad/Datei

z. B.
http://www.elektronik-kompendium.de:80/sites/kom/0902231.html
```

HTTP Request

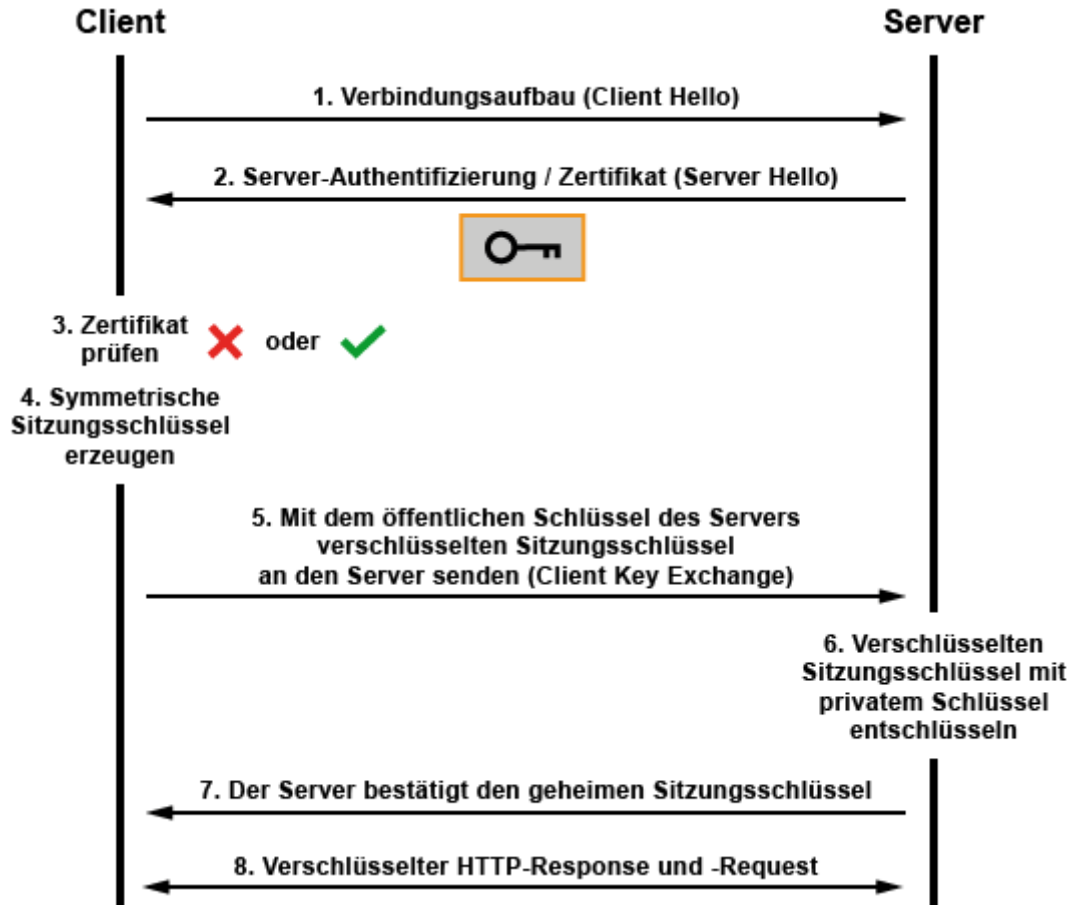
Der HTTP-Request ist die Anfrage des HTTP-Clients an den HTTP-Server. Ein HTTP-Request besteht aus den Angaben **Methode, URL und dem Request-Header**. Die häufigste Methoden sind **GET und POST**. Dahinter folgt durch ein Leerzeichen getrennt der URL und die verwendete HTTP-Version. In weiteren Zeilen folgt der Header und bei der Methode POST durch eine Leerzeile (!) getrennt die Formular-Daten.

HyperText Transfer Protocol Secure (HTTPS) (Port 443 - Layer 7)

HTTPS bzw. HTTP Secure ist die Anwendung von HTTP in **Verbindung mit Verschlüsselung und Authentifizierung**. Wobei in der Regel nur der **angefragte Webserver sich mit einem Zertifikat authentisieren** muss.

Eine **verschlüsselte Verbindung mit einem Browser** signalisiert man mit einem „https:“ *(TCP-Port 443) statt „http:*“ (TCP-Port 80). Dabei muss sich der Webserver dem Client gegenüber authentisieren, ob er tatsächlich der Webserver ist, der sich unter der eingegebenen Adresse befindet. Zusätzlich wird die **Verbindung bzw. Sitzung Ende-zu-Ende-verschlüsselt**. Das bedeutet, die **Stationen zwischen Client und Server** können die Kommunikation **nicht entschlüsseln**.

Für die Authentifizierung und Verschlüsselung ist SSL/TLS verantwortlich. Es schiebt sich zwischen HTTP und dem Transportprotokoll TCP. Damit steht SSL/TLS auch für andere Anwendungsprotokolle zur Verfügung. Beispielsweise SMTPS, IMAPS und FTPS. SSL arbeitet für den Anwender nahezu unsichtbar.



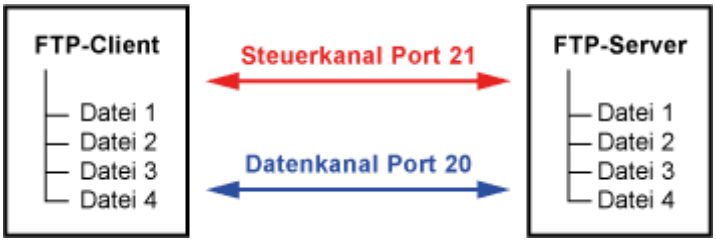
1. Client Hello: Der Client kontaktiert den Server über ein Protokoll mit Verschlüsselungsoptionen.
2. Server Hello, Certificate, Server Key Exchange, Server Hello Done: Der Server nimmt die Verbindung an und schickt sein Zertifikat mit dem öffentlichen Schlüssel seines Schlüsselpaares zur Authentifizierung an den Client.
3. Der Client überprüft das Server-Zertifikat und dessen Gültigkeit (Validierung). Erkennt der Client das Zertifikat als ungültig wird die Verbindung an dieser Stelle abgebrochen.
4. Erkennt der Client das Zertifikat als gültig erzeugt der Client den symmetrischen Sitzungsschlüssel.

5. Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message: Mit dem öffentlichen Schlüssel des Servers verschlüsselt der Client den Sitzungsschlüssel und schickt ihn an den Server.
6. Mit seinem privaten Schlüssel kann der Server den verschlüsselten Sitzungsschlüssel entschlüsseln.
7. Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Message: Der Server bestätigt den geheimen Sitzungsschlüssel.
8. Danach werden alle HTTP-Requests und -Responses verschlüsselt, bis die Verbindung abgebaut wird.

File Transfer Protocol (FTP) (Port 20 und 21 - Layer 7)

FTP ist ein Kommunikationsprotokoll, um Dateien zwischen unterschiedlichen Computersystemen zu übertragen. Die Übertragung findet nach dem Client-Server-Prinzip statt. Ein FTP-Server stellt dem FTP-Client Dateien zur Verfügung. Der FTP-Client kann Dateien auf dem FTP-Server ablegen, löschen oder herunterladen. Mit einem komfortablen FTP-Client arbeitet man ähnlich, wie mit einem Dateimanager.

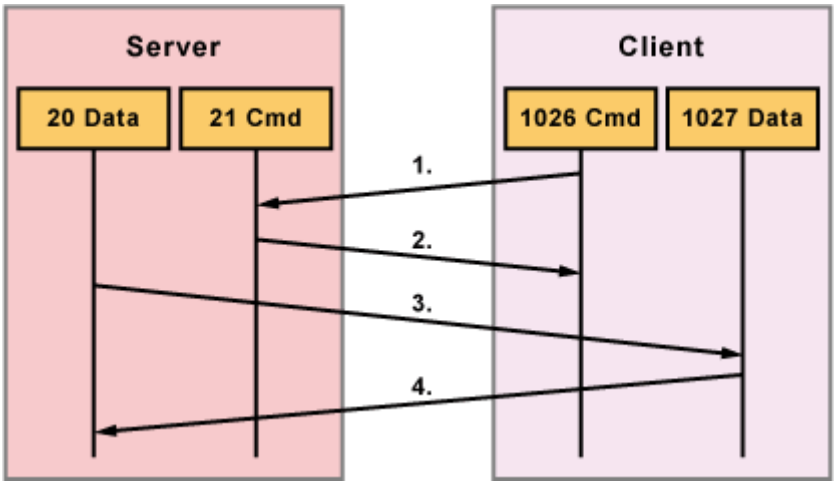
Funktionsweise

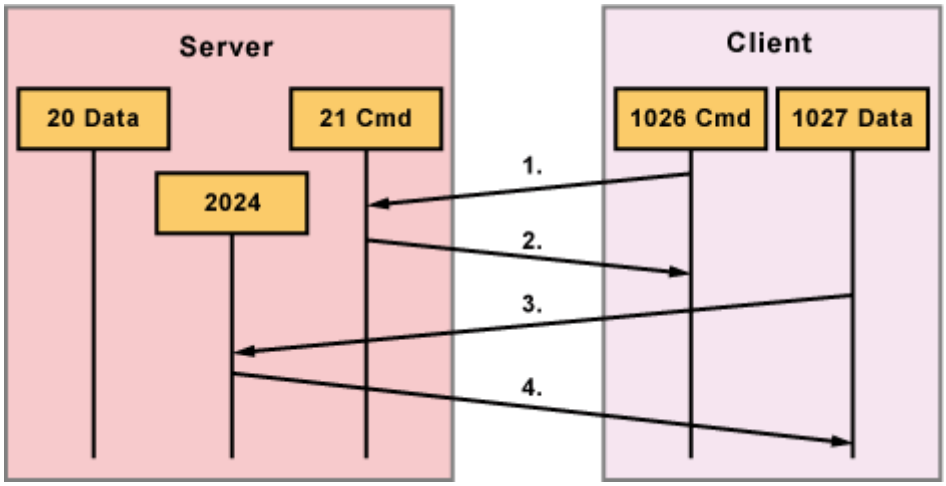


Die Kommunikation findet nach dem Client-Server-Prinzip statt. Wobei FTP zwischen Client und Server zwei logische Verbindungen herstellt. Eine Verbindung ist der Steuerkanal (command channel) über den TCP-Port 21. Dieser Kanal dient ausschließlich zur Übertragung von FTP-Kommandos und deren Antworten. Die zweite Verbindung ist der Datenkanal (data channel) über den TCP-Port 20. Dieser Kanal dient ausschließlich zur Übertragung von Daten. Über den Steuerkanal tauschen Client und Server Kommandos aus, die eine Datenübertragung über den Datenkanal einleiten und beenden.

Aktives vs. Passives FTP

Der FTP-Verbindungsaufbau sieht vor, dass der Steuerkanal vom FTP-Client zum FTP-Server aufgebaut wird. Steht der Steuerkanal wird der Datenkanal vom FTP-Server zum FTP-Client initiiert (aktives FTP). Befindet sich der FTP-Client hinter einem NAT-Router oder einer Firewall und verfügt parallel dazu nur über eine private IPv4-Adresse, dann kommt die Verbindung nicht zustande. Die Verbindungsanforderung vom Server an den Client wird von der Firewall bzw. dem Router abgeblockt, bzw. kann wegen der privaten IPv4-Adresse gar nicht geroutet werden. Für diesen Fall gibt es das passive FTP, bei dem auch der Client den Datenkanal initiiert.





Am Anfang jeder FTP-Verbindung steht die Authentifizierung des Benutzers. Danach erfolgt der Aufbau des Steuerkanals über Port 21 und des Datenkanals über Port 20. Wenn die Dateiübertragungen abgeschlossen sind, werden die Verbindungen vom Benutzer oder vom Server (Timeout) beendet.

Secure Shell (SSH) (Port 22 - Layer 7)

SSH bzw. Secure Shell ist ein **kryptografisches Protokoll** mit dem man auf einen entfernten Rechner mittels einer **verschlüsselten Verbindung über ein unsicheres Netzwerk** zugreifen kann.

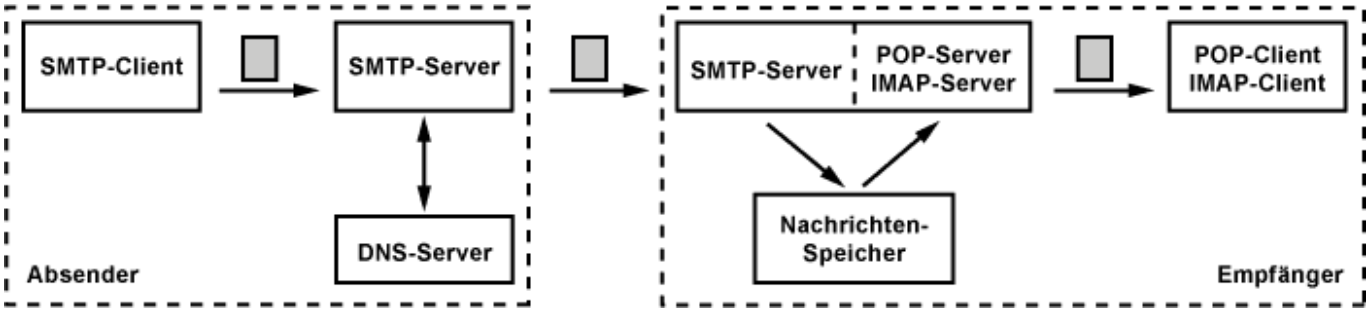
Die Shell (Kommandozeile) bietet **vollen Zugriff auf das Dateisystem und alle Funktionen** des Rechners.

Die Funktionen der Secure Shell beinhalten den Login auf entfernte Rechner, die interaktive und nicht interaktive Ausführung von Kommandos und das Kopieren von Dateien zwischen verschiedenen Rechnern eines Netzwerks. SSH bietet dazu eine kryptografisch gesicherte Kommunikation über das unsichere Netzwerk, eine zuverlässige gegenseitige Authentisierung, Verschlüsselung des gesamten Datenverkehrs auf Basis eines Passworts oder Public/Private-Key-Login-Methoden

Simple Mail Transfer Protocol (SMTP) (Port 25 - Layer 7)

SMTP ist ein **Kommunikationsprotokoll für die Übertragung von E-Mails**. Die **Kommunikation** erfolgt **zwischen** einem **E-Mail-Client und einem SMTP-Server (Postausgangsserver)** oder zwischen zwei SMTP-Server. Für den **Austausch** der E-Mails sind die **Mail Transfer Agents (MTAs)** zuständig. Untereinander verständigen sich die MTAs mit dem SMTP-Protokoll.

Neben SMTP gibt mit POP und IMAP noch zwei weitere Protokolle für den E-Mail-Austausch. Diese beiden Protokoll dienen jedoch nur dazu, um E-Mail abzuholen oder online zu verwalten. SMTP dagegen ist ein Kommunikationsprotokoll, das **E-Mails entgegennehmen und weiterleiten kann**.



Der Ablauf des E-Mail-Routings sieht in etwa so aus: Der SMTP-Server fragt einen DNS-Server ab und erhält eine Aufstellung von Mail-Servern, die E-Mails für den Ziel-SMTP-Server entgegennehmen. Jeder dieser Mail-Server (Mail Exchange) ist mit einer Priorität versehen. Der SMTP-Server versucht die Mail-Server in der vorgegebenen Reihenfolge zu kontaktieren, um die E-Mail zu übermitteln

Nachteile

- Für versendete E-Mails keine Versandbestätigung
- Geht eine E-Mail verloren, werden weder Sender noch Empfänger darüber informiert
- Nicht vorhandene Authentisierung des Benutzers beim Verbindungsaufbau zwischen SMTP-Client und SMTP-Server. Das führt dazu, dass eine beliebige Absenderadresse beim Versand einer E-Mail angegeben werden kann

Simple Mail Transfer Protocol Secure (SMTPS) (Port 465 und 587- Layer 7)

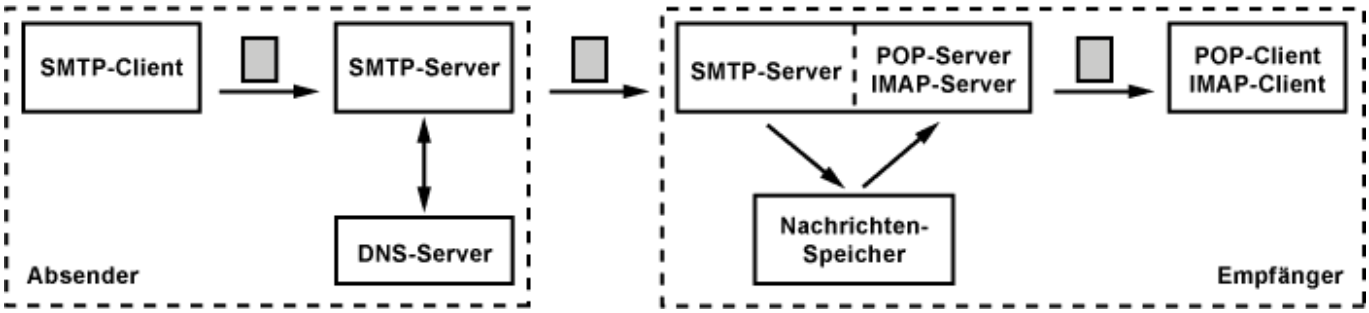
SMTPS (Simple Mail Transfer Protocol Secure) bezeichnet ein Verfahren zur **Absicherung der Kommunikation** beim E-Mail-Transport via **SMTP über SSL/TLS** und ermöglicht dadurch **Authentifizierung der Kommunikationspartner** auf Transportebene sowie **Integrität und Vertraulichkeit** der übertragenen Nachrichten.

SMTPS ist **kein eigenes Protokoll** und auch keine Erweiterung von SMTP, da es **vollkommen transparent und unabhängig** von diesem auf der Transportschicht arbeitet.

Das bedeutet, dass die Verbindung, über die SMTP abgewickelt wird, softwaremäßig mit den Verfahren **SSL oder TLS abgesichert** wird. Dies geschieht direkt beim Verbindungsaufbau, noch bevor irgendwelche Maildaten ausgetauscht werden. Da also die Verwendung der Sicherungsschicht nicht verhandelt wird, sind SMTPS-Dienste in der Regel auf einem eigenen TCP-Port erreichbar.

Post Office Protocol Version 3 (POP3) (Port 110 - Layer 7)

POP ist ein Kommunikationsprotokoll, um **E-Mails von einem Posteingangsserver (POP-Server) abzuholen**. Die **Kommunikation** erfolgt **zwischen** einem **E-Mail-Client** und einem **E-Mail-Server (Posteingangsserver)**. Das Protokoll, das diesen Zugriff regelt, nennt sich POP (aus dem Jahr 1984), das in der aktuellen Version 3 vorliegt, und deshalb manchmal auch als POP3 bezeichnet wird.



Per Fernzugriff werden die gespeicherten E-Mails abgerufen und auf dem lokalen Computer gespeichert. POP sieht das Prinzip der Offline-Verarbeitung von E-Mails vor. Online werden die E-Mails vom Posteingangsserver vom E-Mail-Client heruntergeladen. Wenn sich darunter E-Mails mit einem großen Dateianhang befinden, kann der Download schon mal etwas länger dauern. Erst nach erfolgreichem und vollständigem Zugriff werden die E-Mails auf dem Server gelöscht. Die Bearbeitung der eingegangenen E-Mails erfolgt anschließend auf dem lokalen Computer des Benutzers ohne Verbindung (offline) POP-Server.

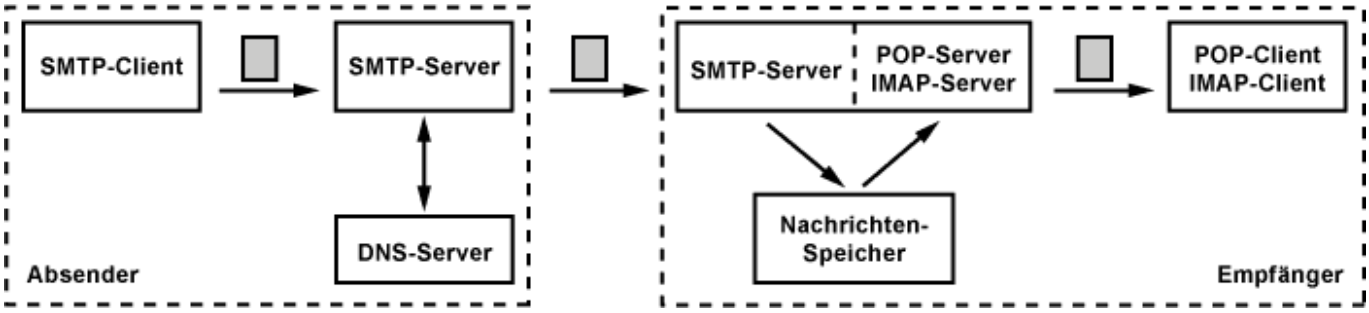
Die Verbindung zwischen POP-Server und E-Mail-Client erfolgt über TCP auf Port 110.

Post Office Protocol Version 3 Secure (POP3S) (Port 995 - Layer 7)

POP3S bezeichnet ein Netzwerkprotokoll zur Erweiterung des E-Mail-Übertragungsprotokolls POP3 um eine Verschlüsselung durch SSL/TLS. Üblicherweise wird für POP3S TCP auf Port 995 genutzt.

Internet Mail Access Protocol (IMAP) (TCP-Port 143 - Layer 7)

IMAP ist ein Kommunikationsprotokoll, um **E-Mails** auf einem **entfernten Server** ähnlich wie Dateien **zu verwalten**. Dabei **bleiben alle E-Mails auf dem IMAP-Server**. Erst wenn eine E-Mail gelesen werden soll, wird sie heruntergeladen.



IMAP erlaubt den Zugriff auf eine Mailbox, **ähnlich wie mit POP**. Der entscheidende **Unterschied** zwischen beiden Protokollen ist der **Online-Modus von IMAP**, über den der **E-Mail-Client ständig in Verbindung mit dem E-Mail-Server** steht. Während einer IMAP-Sitzung kann auf einzelne E-Mails zugegriffen werden, die so lange auf dem Server bleiben, bis sie gelöscht werden. Dadurch kann von überall auf dem Server zugegriffen werden. Auch mit einem Endgerät, das nur mit geringer Bandbreite am Netzwerk angeschlossen ist. Die **E-Mails werden nur dann heruntergeladen, wenn der Anwender diese Lesen will**. E-Mails mit einem großen Dateianhang verstopfen dann nicht mehr ungewollt den Zugang zum Netzwerk.

Internet Mail Access Protocol Secure (IMAPS) (TCP-Port 143 - Layer 7)

Bei der Verwendung von IMAPS wird die Verbindung zum Server bereits während des Verbindungsaufbaus durch SSL verschlüsselt. Damit der Server das erkennt, muss ein anderer Port verwendet werden. Dafür wurde der Port 993 reserviert.

Nach dem Aufbau der SSL-Verbindung wird IMAP verwendet. Die SSL-Schicht ist für das IMAP-Protokoll transparent, d. h., es werden keine Änderungen am IMAP-Protokoll vorgenommen.