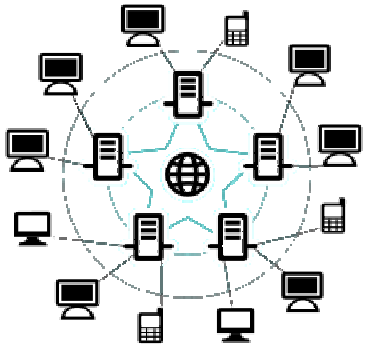
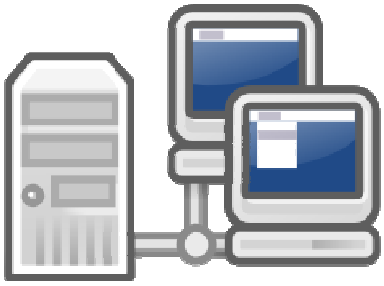
Netzwerkgrundlagen



Das **Internet** ist ein globales Netzwerk (**GAN** = Global Area Network), alle Computer die sich Zugang verschaffen (über Telefonleitung, Kabel- oder Handynetz, Standleitung …) sind ein Teil davon!

Ein Teilbereich des großen Internets (**GAN**) ist ein so genanntes **WAN** (Wide Area Network). **WAN** bedeutet nichts anderes als wie „weites Netzwerk" (Wide Area Network), es ist also eine Verbindung von vielen Computern, die sich über eine relativ große Fläche erstreckt, jedoch nur einen Teil des großen Internets ausmacht. Ein **WAN** könnten z.B. alle Internet - Benutzer in ganz Österreich sein, wir als Nation ergeben praktisch einen beträchtlichen Teil. Alle **WAN**s zusammengerechnet ergeben dann wiederum das Internet (= **GAN**!).



Wenn wir bei einer großen Fläche wie z.B. Österreich (WAN) nun noch weiter ins Detail gehen, kommen wir auf die einzelnen Gebäude, wo sich Menschen befinden, die zusätzlich ein kleines Netzwerk haben könnten (z.B. 2 oder mehr Computer, die miteinander verbunden sind!). Zu diesem kleinsten aller kleinen Netzwerke sagt man dann **LAN** (kabelgebundenes lokales Netzwerk), **WLAN** (drahtloses lokales Netzwerk im selben Gebäude) oder **Powerline** (lokales Netzwerk im selben Gebäude, welches über Stromleitungen verläuft!). Es wird nicht explizit eine der 3 Arten von lokalen Netzwerken vorgeschrieben, es können LANs/WLANs und Powerlines beliebig miteinander kombiniert werden!

GAN – WAN – LAN/WLAN/PowerLine → großes Netzwerk – ein kleiner Teil davon – ein noch kleinerer Teil

Jeder einzelne Computer, mit dem man Zugang zum Internet bekommt, ist ein Teil des gesamten großen Netzwerks (**GAN** = Internet). Und wie es in Wirklichkeit auch der Fall ist, haben einzelne Gebäude ja auch eine Adresse. Damit wir über Internet z.B. Nachrichten schicken, Bilder austauschen oder Informationen suchen können, muss auch jeder Computer der im Internet ist genauso über eine eigene **Adresse** verfügen. www.facebook.at ist eine Adresse oder www.google.at . Sobald man diese besucht, gelangt man vereinfacht erklärt auf den jeweiligen Computer im großen Netzwerk (**GAN**), auf dem die Website gespeichert ist. **MAN BESUCHT EINE ADRESSE!**

Zu **LAN/WLAN/Powerline** sagt man auch gerne **INTRANET,** weil sich das Netzwerk im selben Gebäude befindet (intern!)! **INTRANET** und **INTERNET** sind **NICHT** dasselbe, beide verwenden aber die gleichen Technologien! Das **Intranet** ist in einem Gebäude, das Internet umspannt die gesamte Erdkugel! Es handelt sich aber in beiden Fällen um **Netzwerke**!

Es kann keine 2 gleichen Adressen in einem **Netzwerk** geben, wenn **z.B.** jemand etwas bestellt, muss die Post auch genau wissen wo der Empfänger wohnt.

Wenn die Adresse nicht eindeutig ist, geht das Paket verloren bzw. der Absender bekommt es retour.

In Netzwerken spricht man von sogenannten **Datenpaketen**!

Das **WWW** (World Wide Web) ist ein **System,** welches einheitlich für alle Internet Seiten erfunden wurde. Durch das **WWW** können einzelne Websites erst besucht werden, das **HTTP** (Hyper Text Transfer Protocol) und **HTTPS** (Hyper Text Transfer Protocol Secure) überträgt für das WWW Informationen in unverschlüsselter oder verschlüsselter Form! Alles, was mit **WWW** beginnt, ist **eindeutig eine Website**! Solange man keine **Homepage** selbst erstellt hat, hat man auch keine Adresse wie www.facebook.at, sondern nur eine Zahl mit Punkten dazwischen, unter der man im Internet erkennbar ist → die sogenannte **IP – Adresse**!

Vergleichen wir das Ganze wieder mit der Realität, aber im direkten Zusammenhang mit Netzwerken! Wir fahren (**Clients**) jemanden besuchen (**Server**) und werden bei der Haustüre empfangen. Weil es der Hausbesitzer erlaubt (**Firewall**), dürfen wir eintreten und bekommen event. einen Kaffee und einen Kuchen (**Service**). Der Raum, in dem es die Verköstigung gibt, ist die Küche; wir gelangen über die Küchentür (**Port**) in die Küche. Um zum Gebäude zu gelangen, wo es Kaffee und Kuchen gibt, müssen wir auf alle Fälle auch die Adresse (**Webadresse/IP-Adresse**) wissen.

Abgekürzt: Adresse des Gebäudes und Raumname (Küche) müssen bekannt sein→ Wenn es der Firewall gestattet, werden wir durchgelassen und erhalten den **Service** (Kaffee und Kuchen) vom **Server** (Gebäude), der beim **Port Küche** (Küchentür) auf uns wartet (Kaffee und Kuchen)!

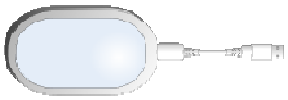
Wenn wir eine Internet - Seite wie z.B. www.facebook.at besuchen, ist das nichts anderes. Wir erhalten nur Zugang zum **Server** (Anbieter), wenn das für Gäste auch gestattet wird (**Firewall**)! Der Firewall muss uns einen Zugriff über Port 80 bei www.facebook.at gestatten! Sobald wir eintreten dürfen, bekommen wir zwar keine Verköstigung, aber dafür die nötigen Informationen (Text, Bilder, Musik, Videos), die wir benötigen (Service)! Erhaschen wir uns Informationen, obwohl wir nicht rein gelassen werden, sind wir ebenfalls Einbrecher wie bei einem richtigen fremden Gebäude, beim Computer heißen die Einbrecher jedoch **Hacker**!

Was den Computer vor unbefugtem Zugriff über das Internet und vor allem auch vor **Hackern** schützt, heißt **Firewall!** Wir stellen uns einen **Firewall** wie eine Mauer vor, die zerstört werden will, dies ist jedoch sehr schwer möglich! Schafft es doch jemand, ist er unerlaubt eingebrochen und kann z.B. Daten und/oder wichtige private Informationen von unserem PC stehlen!

Wie sieht es nun beim lokalen Netzwerk (LAN/WLAN/PowerLine) genauer aus bzw. wie funktioniert das alles im Detail?

Zu allererst müssen wir die wichtigsten Geräte aufzählen:

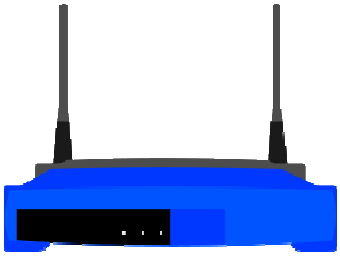
Modem → Das Modem ist ein Gerät, welches uns mit dem Internet verbindet! Die Verbindung wird über Telefonleitung, Kabelfernsehen, Internetstick (Verbindung über Handynetz), Standleitung … hergestellt)



Router → Der Router ist ein Gerät, welches verschiedene Netzwerke miteinander verbindet (z.B. Internet und lokales Netzwerk!)

Firewall → Ein Firewall ist meist ein Programm auf einem Computer (muss nicht zwingend so sein!), welches alle anderen Computer im Netzwerk vor unbefugtem Zugriff über das Internet schützt!

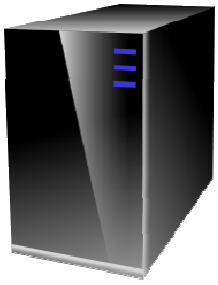
Switch → Der Switch ist ein intelligentes Gerät, welches vereinfacht erklärt, wie ein Stromverteiler arbeitet. In unserem Fall wird aber z.B. die Internetverbindung einfach auf mehrere Netzwerkkabel aufgeteilt! Der Switch merkt sich, welcher Client bei welchem Anschluss (Port) angeschlossen wurde und kann somit für jedes Gerät eine hohe Geschwindigkeit gewährleisten!



Access Point → Ein Access Point findet meist Verwendung, wenn ein Netzwerk auf einen größeren Bereich erweitert werden soll, z.B. Internetverbindung auch im Nebengebäude. Es kommt eine sogenannte **Wireless –Bridge** (drahtlose Brücke) per WLAN (Funk) zum Einsatz! **Access Points** werden auch oft dazu benutzt, um eine sogenannte **Demilitarized Zone (entmilitarisierte Zone)** zu erzeugen!

DMZ (demilitarized Zone) → Man spricht von einer **DMZ**, wenn ein Teil des Netzwerks nicht so sicher ist als wie der andere! Im öffentlicheren Teil werden die **Server** aufgestellt, im geschützten befinden sich die Computer (**Clients**) mit sensiblen, wichtigen Daten!

Repeater → Der **Repeater** kommt dann zum Einsatz, wenn ein Netzwerksignal über weite Strecken geschickt werden soll. Das Gerät verstärkt dieses –> die Funktion des Repeaters ist meist in APs (Access Points) bereits enthalten!

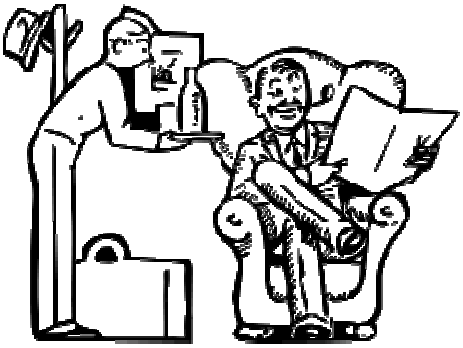


Server → Ein Server ist ein Computer, welcher verschiedenste Dienste für andere Computer zur Verfügung stellt (oft auch über das Internet, z.B. ein FTP – Server hält für alle Daten bereit, ein E-Mailserver verwaltet alle geschickten und empfangenen Nachrichten, ein Webserver speichert unsere Homepagedaten usw.)! Ein **Router** kann manchmal ebenso ein Server sein (z.B. wenn er bereits ein Modem verbaut hat, stellt er die Internet - Verbindung für alle Clients zur Verfügung!)!

Einfacher erklärt:

Ein **Server** ist ein Knotenpunkt in einem Netzwerk, der einen bestimmten Dienst für alle anderen Beteiligten zur Verfügung stellt wie z.B. Internet/Webseiten (Webserver), Programme/Musik /Bilder/Filme (FTP-Server) oder einfach Druckaufträge verwalten (Print-Server). Ein **Server** ist in der Realität mit einem Kellner zu vergleichen, der uns Essen und Trinken auf Wunsch bringt!

Client → Der Client (Klient) ist ein Computer, welcher die Dienste des Servers nutzt!



Wir sind die Klienten/Kunden, also die Personen die sich alle Informationen vom Internet (dem großen Netzwerk) holen! Wie in einem Gasthaus: Es wird etwas vom Kellner (**Server**) angeboten und auf Wunsch gebracht! Genauso kann im lokalen Netzwerk ein **Server** dem **Client** (uns) nützlich sein! Ein sogenannter **Print – Server** verwaltet z.B. alle Druckaufträge in einer Firma! Ohne diesen wäre der Drucker sofort überfordert und würde abstürzen, wenn z.B. 20 Leute auf einmal drucken möchten!

Jedes Netzwerk basiert daher auf dem sogenannten Client – Server- Prinzip!

Nun ist es oft so, dass mehrere der aufgezählten Geräte bereits in einem vereint sind!

Deshalb müssen wir auch noch zwischen logical (logischen) und physical (physischen) devices (Geräten) unterscheiden!

Logical Devices sind z.B. im Einzelfall ein Firewall, ein Switch oder ein Modem!

Ein **physical device** vereint oft mehrere logical devices! Ein sogenannter **DSL - Router** verfügt z.B. in den meisten Fällen heutzutage bereits über alle genannte Funktionen (Modem, Router, Firewall, Switch)!

Wie erwähnt, können die Clients, Server, Router/Switches, Access Points usw. per Kabel (LAN), drahtlos (WLAN) oder über Stromleitungen (Powerline) verbunden werden! Auch die Kombination ist möglich, es können z.B. Teile drahtlos, Teile kabelgebunden und wiederum andere Teile über Stromleitungen verbunden werden!

Kommen wir zur Software:

IP - Adresse → Jedes Gerät in einem Netzwerk hat eine sogenannte **IP (Internet Protocol) - Adresse**. Im Normalfall ist eine gültige öffentliche **IP - Adresse** z.B. **173.194.39.183!** Im alltäglichen Leben könnte das genauso **8983 Bad Mitterndorf 450/6** bedeuten!

Es gibt verschiedene Adressbereiche für **Internet** und **Intranet (LAN/WLAN/PowerLine)**!

Im Internet ist man also unter einer anderen Adresse als im lokalen Netzwerk auffindbar!

z.B. die Internet IP ist **88.117.9.192** und die lokale (LAN /WLAN/Powerline) **192.168.0.100**!
Der **Router übernimmt die Aufgabe**, die öffentliche Internet IP mit der privaten ständig **abzugleichen**! Man spricht von der sogenannten **Network Adress Translation → NAT!**

Warum ist das überhaupt nötig? Würde jeder einzelne Client in einem lokalen Netzwerk eine öffentliche Internet - Adresse erhalten, wären diese schnell aufgebraucht!

TCP (Transmission Control Protocol = Übertragunsprotokoll): Alles, was z.B. per Mail über das Internet geschickt wird, soll auch genauso beim Empfänger ankommen. **TCP** überprüft das ganz genau (**TCP = Protokoll**)! Wenn man sich eine Homepage anschaut, möchte man ja auch alles sehen und nicht nur Teile davon!

Download: Von **Download** (herunterladen) spricht man, wenn von einem **Server** Daten (Informationen/Musik/Bilder/Filme usw.) auf einen lokalen Computer übertragen werden. Wenn man ein **E-Mail** bekommt, ist das z.B. auch ein **Download**! Nur das Betrachten einer Website ist bereits auch ein Download, da ja die angezeigten Texte, Bilder, Videos usw. übertragen werden müssen!

Upload: Upload ist das Gegenteil von Download. Wenn man z.B. ein E-Mail verschickt, handelt es sich um Upload! Wir werden beim Upload also sozusagen selbst zum „Anbieter"!

Die Summe aus verbrauchtem Down- und Upload ergibt den gesamten **Traffic** (Verkehr wie auf einer Straße), den wir verursachen. Umso mehr Verkehr durch **Down- und Upload** entsteht, umso mehr muss man in der Regel beim **Provider** (= **Internetanbieter**!) bezahlen. Es gibt aber sogenannte **FLAT RATES**, durch welche man so viel **Traffic** verursachen darf, wie man will und im Monat pauschal dafür bezahlt!

Fahren wir mit dem Auto zu schnell, dann müssen wir auch tief in die Tasche greifen; genauso ist es bei der Internet - Verbindungsgeschwindigkeit. Je schneller wir Informationen erhalten, desto mehr müssen wir bezahlen! **Die Internet –Verbindungsgeschwindigkeit wird in Megabit (MBIT) / Sekunde angegeben!** Um die maximale Geschwindigkeit in **Megabyte / Sekunde** zu errechnen, müssen wir den Wert **durch die Zahl 8 dividieren**, da 1 Byte ja 8 Bit enthält!

Eine 12 MBIT Internetverbindung kann also maximal 1,5 Megabyte in der Sekunde vom Server auf den Client übertragen!

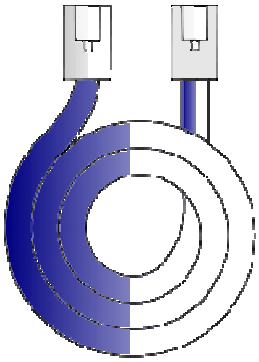
Wie bereits erwähnt, ist der **Provider** der **Internetanbieter**. In Österreich sind bekannte Provider, z.B. **A1, Tele 2, Drei** usw. Möchten wir selbst einen Server betreiben, der auch über das Internet erreichbar sein soll, benötigen wir unbedingt eine **statische Internet IP - Adresse**! Dadurch wird gewährleistet, dass der **Server** ständig erreichbar ist! Bei einer **dynamischen Adresse**, ändert sich diese nach jeder neuen Verbindung! Letzteres ist aber um einiges günstiger! Sollten wir z.B. einen Webserver mit einer eigenen Homepage betreiben, ist die statische Adresse aber unerlässlich!

Gateway: Der Gateway ist im Normalfall der Router (nicht zwingend!), es ist die IP - Adresse, über die wir aber im Normalfall Zugriff auf das Internet (nach außen) erlangen!

DNS (Domain Name System): Jeder Computer (Host) hat seinen eigenen Namen und DNS weist diesem die richtige IP – Adresse zu! Mit www.google.at kann ein Netzwerk prinzipiell nichts anfangen, erst durch das DNS wird eine „computerfreundliche“ IP - Adresse zugewiesen, und die Übermittlungen zwischen Server und Client können problemlos erfolgen. Im lokalen Netzwerk ist der DNS - Server meist ebenfalls der Router, er vergibt an den Client die lokale IP - Adresse!

DHCP: Jeder Client im Netzwerk hat eine IP – Adresse, entweder statisch (fest eingestellt) oder dynamisch (wird zugeteilt). Ist letzteres der Fall, kommt DHCP zum Einsatz. Dadurch wird eingestellt, welche IP - Adressen verwendet werden dürfen. Und sobald ein neuer Client sich per LAN/WLAN/PowerLine verbindet, wird automatisch eine IP Aus diesem „Adresspool“, der richtige Gateway, sowie DNS - Server zugewiesen! Bei statischen Adressen (z.B. bei einem Server!) müssen diese Einstellungen manuell erfolgen! Es ist wichtig, den Adresspool so einzustellen, dass keine IP - Adressen von z.B. einem wichtigen Server vergeben werden können (jede IP- Adresse kann es im selben Netzwerk nur einmal geben!)!

Port: Ein Port ist in der Realität ein Netzwerkanschluss für Netzwerkkabel. Es gibt jedoch auch virtuelle Ports im Internet; jeder Port ist einem Dienst zugewiesen. Z.B. Port 25 ist für das Empfangen von E-Mails ausgelegt, Port 20/21 für FTP – Verbindungen, Port 80 für http (Internet) usw.

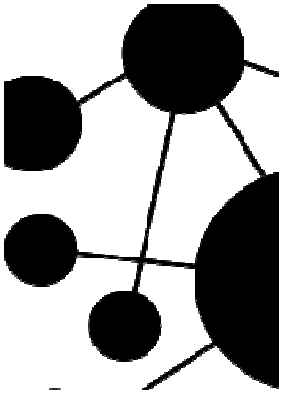


Port Forwarding: Ermöglicht es einzelne Dienste für bestimmte IPs (Clients) über Ports explizit durch den Firewall zu lassen! Es wird z.B dem Client 192.168.0.67 erlaubt, sich über das Programm Filezilla und die Ports 20/21 mit einem FTP – Server zu verbinden!

Generell ist es so, dass eingehende Verbindungen (Selbstschutz) im Firewall blockiert werden (hier kommt Port Forwarding ins Spiel!), ausgehende werden grundsätzlich erlaubt!

Ein praktisches Netzwerk - Beispiel zum Schluss:

Gehen wir nun von einem kleinen Betrieb mit rund 40 Mitarbeitern aus. Die Verbindung zum Internet wird über eine Telefonleitung hergestellt, dies geschieht im Normalfall per **DSL – Router**! Das Gerät verbindet sich per **Modem** mit dem Internet, stellt das lokale Netzwerk u. Internet mit allen IPs für die Clients (20 Mitarbeiter) zur Verfügung und schützt per **Firewall** vor Eindringlingen! Des Weiteren ist in den meisten Fällen beim Router ebenso bereits ein **Switch** mit 5 Ports (Anschlüssen) verfügbar und es können auch drahtlose (WLAN) Verbindungen vom **Client** (z.B. unserem Computer) zum **Server** (Router) aufgebaut werden! Damit wir nicht nur 5 Personen per Kabel einen Zugang ermöglichen können, sondern 20, schließen wir noch zwei 10 – Port Switches direkt an den DSL – Router an und verteilen mit weiteren Kabeln an die Clients. Computer/Laptops mit **WLAN** - Funktionen können auch drahtlos über eine sogenannte **SSID** (drahtloser Netzwerkname) und einem **Passwort** eine Verbindung herstellen. Die 20 Mitarbeiter im anderen Gebäude brauchen ebenfalls einen Internet - Zugang, also schließen wir an einen der Switches im Hauptgebäude einen **Access Point mit Bridge – Funktion** an und setzen im anderen Gebäude das gleiche Modell ein. Die beiden **APs (Access Points)** verbinden sich drahtlos (Bridge!)! Der **AP** im Nebengebäude wird wiederum mit einem **Router** verbunden - und so können auch in diesem Bereich Clients (PCs und Laptops) ins Internet sowie auf das Netzwerk zugreifen!



An den Router kommen wieder zwei **10 - Port Switches**, um die Verbindungen für die Clients aufzuteilen. Die Sicherheit der Firewall wird hier erhöht, wir haben eine **DMZ (!)** erzeugt bzw. alle PCs und Laptops, die am Router im Nebengebäude angeschlossen wurden bzw. sich per WLAN drahtlos den, sind ab nun ein Teil von dieser! Der Zugriff vom Nebengebäude ins Hauptgebäude ist möglich, Computer vom Hauptgebäude können sich aber nicht mit den Computern im Nebengebäude verbinden! Somit hätte es also ein Hacker noch schwerer, er müsste an der Firewall im Hauptgebäude bei und anschließend Zugriff auf das DMZ über noch einen Router mit Firewall erhalten. Eine **DMZ** ist also auch eine doppelte Absicherung!

Im Keller des Nebengebäudes kann keine WLAN – Verbindung aufgebaut werden, da hier Stahlbeton beim Bau verwendet wurde und somit der Funkbetrieb nicht möglich ist. Auch Kabel können nicht gelegt werden. Hier kommt eine **Powerline** zum Einsatz. Wir verbinden ein Kabel von einem Switch mit dem **Powerline - Adapter** in einer Steckdose. Im Keller haben wir ebenfalls einen Powerline Adapter in einer Steckdose und verbinden wiederum dieses Kabel mit einem weiteren Router oder Switch. Die weitere Verteilung des Signals ist also auch in diesem Bereich gewährleistet!

Ich hoffe, das Tutorial war für den Einstieg in die doch komplexe Materie hilfreich!